



Documentazione del software StorageGRID 12.1

StorageGRID software

NetApp
July 22, 2026

This PDF was generated from <https://docs.netapp.com/it-it/storagegrid/index.html> on July 22, 2026.
Always check docs.netapp.com for the latest.

Sommario

Documentazione del software StorageGRID 12.1	1
Scopri l'hardware dell'appliance StorageGRID	2
Note di rilascio	3
Novità di StorageGRID 12.1	3
Capacità	3
Controllo accessi	3
Federazione	3
Gestibilità	3
S3	3
Sicurezza	4
Tenant	4
Aggiornamento	5
Interfaccia utente	5
Funzionalità e funzionalità rimosse o deprecate in StorageGRID	5
Definizioni	6
Fine del supporto delle funzionalità di StorageGRID	6
Modifiche all'API di gestione della griglia in StorageGRID	8
Nuovi endpoint per modificare la password BMC e le impostazioni IP della LAN	8
Modifiche all'API di gestione dei tenant in StorageGRID	8
Nuova API per la replicazione degli oggetti	9
Modifiche al supporto dell'API REST S3 di StorageGRID	9
Inizia subito con un sistema StorageGRID	14
Scopri di più su StorageGRID	14
Che cos'è StorageGRID?	14
Cloud ibridi con StorageGRID	16
Architettura StorageGRID e topologia di rete	17
Nodi e servizi Grid	20
Come StorageGRID gestisce i dati	33
Esplora StorageGRID	44
Linee guida per il networking	52
Linee guida di networking per StorageGRID	52
Tipi di rete StorageGRID	53
Esempi di topologia di rete	57
Requisiti di rete per StorageGRID	63
Requisiti specifici della rete per StorageGRID	65
Considerazioni di rete specifiche per l'implementazione	67
Installazione e provisioning di rete per StorageGRID	70
Linee guida post-installazione per StorageGRID	71
Riferimento porta di rete	71
Avvio rapido per StorageGRID	80
Installazione, aggiornamento e correzione rapida StorageGRID	83
Installare i nodi StorageGRID	83
Scopri l'hardware dell'appliance StorageGRID	83

Installare nodi basati su software	83
Configura la griglia e completa l'installazione	179
Scopri i passaggi obbligatori e facoltativi dopo l'installazione di StorageGRID	192
Aggiornare il software StorageGRID	193
Aggiornare il software StorageGRID	193
Pianificare e prepararsi per l'upgrade	194
Aggiornare il software	200
Risoluzione dei problemi di aggiornamento di StorageGRID	216
Applicare la correzione rapida StorageGRID	219
Procedura di hotfix StorageGRID	219
Come StorageGRID è influenzato quando si applica un hotfix	220
Procurare i materiali necessari per un hotfix StorageGRID	221
Scarica un file hotfix di StorageGRID	222
Verificare le condizioni del sistema prima di applicare un hotfix StorageGRID	222
Applicare un hotfix in StorageGRID	223
Configurare e gestire un sistema StorageGRID	228
Amministrare StorageGRID	228
Guida rapida per l'amministrazione di StorageGRID	228
Inizia subito con Grid Manager	229
Controllo dell'accesso a StorageGRID	256
USA la federazione di grid	327
Gestire la sicurezza	375
Gestire i tenant	448
Configurare le connessioni client	468
Gestire reti e connessioni	511
Gestire i nodi di storage	530
Gestire i nodi di amministrazione	544
Gestire gli oggetti con ILM	546
Gestisci gli oggetti con ILM in StorageGRID	546
ILM e ciclo di vita degli oggetti	546
Crea e assegna gradi di storage in StorageGRID	569
Utilizzare i pool di storage	572
Utilizza i Cloud Storage Pools	580
Gestisci i profili di codifica di cancellazione in StorageGRID	600
Configurare le regioni S3 per StorageGRID	603
Creare una regola ILM	605
Gestire le policy ILM	622
Lavora con le policy ILM e le regole ILM in StorageGRID	638
USA blocco oggetti S3	642
Esempio di regole e policy ILM	651
Hardening del sistema per StorageGRID	673
Scopri il rafforzamento del sistema per StorageGRID	673
Linee guida per il rafforzamento della sicurezza per gli aggiornamenti software StorageGRID	673
Linee guida per la protezione avanzata delle reti StorageGRID	674
Linee guida per la protezione avanzata dei nodi StorageGRID	675

Linee guida per l'hardening di TLS e SSH in StorageGRID	679
Linee guida per il rafforzamento della sicurezza per log, password e messaggi di audit in StorageGRID	681
StorageGRID con FabricPool	682
Flusso di lavoro di configurazione per l'utilizzo di StorageGRID con FabricPool	682
Informazioni necessarie per collegare StorageGRID come livello cloud FabricPool	684
Utilizzare l'installazione guidata di FabricPool	685
Configurare StorageGRID manualmente	698
Configura ONTAP System Manager per aggiungere StorageGRID come livello cloud FabricPool.	708
Configura le voci del DNS server per StorageGRID con FabricPool	710
Best practice StorageGRID per FabricPool	711
Rimuovere i dati FabricPool da StorageGRID	715
Utilizzare tenant e client StorageGRID	717
Utilizzare un account tenant	717
Utilizzare un account tenant StorageGRID	717
Come effettuare l'accesso e disconnettersi	718
Dashboard Tenant Manager in StorageGRID	720
API di gestione del tenant	723
Utilizzare connessioni di federazione di griglie	728
Gestire gruppi e utenti	737
Gestire le chiavi di accesso S3	755
Gestire i bucket S3	761
Gestire i servizi della piattaforma S3	792
UTILIZZARE L'API REST S3	826
Versioni e aggiornamenti supportati dall'API REST S3 di StorageGRID	826
Richieste API S3 supportate in StorageGRID	830
Testare la configurazione dell'API REST S3 di StorageGRID	849
Come StorageGRID implementa l'API REST S3	851
Supporto per Amazon S3 REST API	867
Operazioni personalizzate di StorageGRID	923
Gestire le policy di accesso	945
Operazioni S3 tracciate nei log di controllo StorageGRID	973
Utilizza Swift REST API (fine del ciclo di vita)	974
Supporto Swift REST API in StorageGRID	974
Monitorare e risolvere i problemi di un sistema StorageGRID	975
Monitorare il sistema StorageGRID	975
USA AutoSupport	975
Monitorare un sistema StorageGRID	989
Visualizza e gestisci la dashboard in StorageGRID	990
Visualizzare la pagina nodi	992
Informazioni da monitorare regolarmente	1022
Gestire gli avvisi	1050
Riferimenti ai file di log	1086
Configurare la gestione dei log e il server syslog esterno	1106
Configura il server di posta elettronica	1122

Utilizzare il monitoraggio SNMP	1124
Raccogliere dati StorageGRID aggiuntivi	1135
Risolvere i problemi relativi al sistema StorageGRID	1149
Risolvere i problemi di un sistema StorageGRID	1149
Risolvere i problemi relativi a oggetti e storage	1156
Risolvere i problemi relativi ai metadati in StorageGRID	1175
Risolvere gli errori dei certificati in StorageGRID	1177
Risolvi i problemi relativi al nodo di amministrazione e all'interfaccia utente in StorageGRID	1178
Risolvi i problemi di rete, hardware e piattaforma in StorageGRID	1181
Risoluzione dei problemi dei messaggi di errore del server syslog esterno per StorageGRID	1189
Scopri i problemi di memorizzazione nella cache del bilanciamento del carico in StorageGRID	1192
Esaminare i registri di audit	1193
Messaggi e registri di controllo	1193
Come i messaggi di controllo si spostano attraverso il sistema StorageGRID nel file di log audit.log per la conservazione	1193
Accedi ai file di log di audit dalla riga di comando del nodo Admin di StorageGRID	1196
Scopri la rotazione dei file di log di audit in StorageGRID	1197
Formato del file di log di audit	1198
Formato del messaggio di audit	1210
Messaggi di audit e ciclo di vita degli oggetti	1215
Messaggi di audit	1221
Espandi la capacità o le funzionalità del tuo sistema StorageGRID	1269
Scopri come espandere il tuo sistema StorageGRID	1269
Pianificazione dell'espansione	1270
Pianificazione dell'espansione per i dati replicati in StorageGRID	1270
Pianificazione dell'espansione per i dati con codice di cancellazione (EC) in StorageGRID	1271
Scopri di più sul ribilanciamento EC dopo l'espansione in StorageGRID	1272
Linee guida per l'espansione	1276
Linee guida per l'aggiunta di capacità di oggetti in StorageGRID	1276
Linee guida per l'aggiunta di capacità di metadati in StorageGRID	1278
Linee guida per l'aggiunta di nodi di griglia in StorageGRID	1280
Linee guida per l'aggiunta di un nuovo sito in StorageGRID	1280
Preparati ad espandere il tuo sistema StorageGRID	1281
Scaricare ed estrarre i file di installazione di StorageGRID	1282
Verificare l'hardware e il collegamento in rete	1288
Aggiunta di nodi o siti grid	1288
Riepilogo del flusso di lavoro per l'aggiunta di nodi della griglia o nuovi siti a StorageGRID	1289
Aggiungere o aggiornare le subnet alla rete Grid per l'espansione in StorageGRID	1289
Distribuisci nuovi nodi della griglia in StorageGRID	1290
Eseguire un'espansione StorageGRID	1294
Aggiungere volumi di storage	1299
Aggiungi volumi di archiviazione al tuo sistema StorageGRID	1299
Aggiungere volumi di archiviazione ai nodi di archiviazione VMware in StorageGRID	1302
Aggiungere volumi SAN o collegati direttamente ai nodi di archiviazione Linux in StorageGRID	1303
Configurare il sistema esteso	1307

Configurare i nodi e i siti appena aggiunti in StorageGRID	1307
Verificare che i nodi di archiviazione siano attivi dopo un'espansione StorageGRID	1308
Copia le metriche di Prometheus nei nuovi nodi amministrativi in StorageGRID	1309
Copia i registri di controllo nei nuovi nodi di amministrazione in StorageGRID	1310
Ribilancia i dati codificati in modo da essere cancellati dopo aver aggiunto nodi al tuo sistema StorageGRID	1312
Risoluzione dei problemi di espansione in StorageGRID	1315
Gestire un sistema StorageGRID	1316
Manutenzione della grid StorageGRID	1316
Prima di iniziare	1316
Procedure di manutenzione per le appliance	1316
Scarica il pacchetto di ripristino StorageGRID	1316
Decommissiona i nodi o il sito	1317
Decommissionare un nodo StorageGRID o un sito StorageGRID	1317
Decommissionamento dei nodi	1317
Decommissionamento del sito	1335
Rinominare la griglia, il sito o il nodo	1358
Utilizzare la procedura di ridenominazione di StorageGRID	1358
Aggiungi o aggiorna i nomi visualizzati di StorageGRID	1362
Procedure dei nodi	1368
Procedure di manutenzione dei nodi StorageGRID	1368
Spostare il servizio ADC in StorageGRID	1368
Convertire un nodo di storage StorageGRID in un nodo di soli dati	1369
Procedure di riavvio, spegnimento e alimentazione	1371
Procedure di rimappamento delle porte	1383
Procedure di Server Manager	1387
Procedure di rete	1396
Aggiorna le sottoreti per StorageGRID Grid Network	1396
Configurare gli indirizzi IP	1398
Aggiungere interfacce al nodo esistente	1417
Configurare i server DNS in StorageGRID	1421
Modificare la configurazione DNS per un singolo nodo StorageGRID	1422
Gestisci i server NTP in StorageGRID	1424
Ripristinare la connettività di rete per i nodi StorageGRID isolati	1425
Procedure host e middleware	1427
Migrare un nodo StorageGRID su un nuovo host Linux	1427
Configura una macchina virtuale VMware per il riavvio automatico in StorageGRID	1429
Recovery o sostituzione dei nodi	1430
Avvertenze e considerazioni per il ripristino dei nodi StorageGRID	1430
Condizioni preliminari per il ripristino dei nodi di rete	1430
Ordine di recovery del nodo in caso di guasto di un server che ospita più di un nodo griglia	1431
Indirizzi IP per i nodi ripristinati	1431
Raccogli il materiale necessario per il ripristino del nodo della griglia StorageGRID	1431
Scaricare ed estrarre i file di installazione di StorageGRID	1432
Selezionare la procedura di ripristino del nodo StorageGRID	1438

Ripristino da guasti del nodo di storage	1439
Ripristina dai guasti dei nodi di archiviazione StorageGRID	1439
Ripristinare il nodo storage dell'appliance	1440
Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto	1455
Ripristino in caso di guasto al disco di sistema	1463
Ripristino da errori del nodo di amministrazione	1475
Ripristino del nodo Admin primario o non primario in StorageGRID	1475
Riprendi dai guasti del nodo di amministrazione primario usando lo stesso nodo di amministrazione primario	1475
Ripristina dai guasti del nodo di amministrazione primario utilizzando un nodo di amministrazione non primario	1484
Ripristino da guasti non primari del nodo di amministrazione	1491
Ripristino da guasti del nodo gateway	1498
Sostituire il nodo gateway di StorageGRID	1498
Seleziona Avvia ripristino per configurare il nodo gateway di StorageGRID	1499
Ripristino da errori del nodo di archiviazione	1500
Ripristina dai guasti del nodo di archiviazione StorageGRID	1500
Sostituire il nodo Linux	1500
Sostituire un nodo Linux in StorageGRID	1500
Distribuisci nuovi host Linux per StorageGRID	1501
Ripristina i nodi StorageGRID sull'host	1502
Eseguire ulteriori passaggi di ripristino del nodo StorageGRID	1506
Sostituisci un nodo VMware in StorageGRID con un nodo di ripristino	1507
Sostituisci il nodo VMware in StorageGRID con SG1000 o SG100	1508
Passaggio 1: Sostituisci il nodo VMware	1509
Passaggio 2: Completa il ripristino del nodo	1514
Sostituire il nodo guasto con l'appliance di servizi	1514
Sostituire il nodo StorageGRID guasto con l'appliance di servizi	1514
Installare l'appliance di servizi StorageGRID (solo cambio di piattaforma)	1514
Preparare l'appliance StorageGRID per la reinstallazione (solo sostituzione della piattaforma)	1515
Avvia l'installazione del software StorageGRID su un'appliance di servizi	1516
Monitorare l'installazione degli appliance di servizi StorageGRID	1518
Come il supporto tecnico ripristina un sito StorageGRID	1519
Soluzioni e risorse StorageGRID	1522
Come gestire StorageGRID utilizzando NetApp Console	1523
Note legali	1524
Copyright	1524
Marchi	1524
Brevetti	1524
Direttiva sulla privacy	1524
licenza API	1524
Open source	1524

Documentazione del software StorageGRID 12.1

Scopri l'hardware dell'appliance StorageGRID

Vai su "[Documentazione dell'appliance StorageGRID](#)" per scoprire come installare, configurare e gestire gli appliance di storage e i servizi StorageGRID.

Note di rilascio

Novità di StorageGRID 12.1

StorageGRID 12.1 introduce le seguenti funzionalità e modifiche.

Per informazioni dettagliate sui problemi risolti e sui problemi noti nelle versioni recenti di StorageGRID 12.1, consultare le ["StorageGRID 12.1 Note di rilascio"](#). È necessario accedere con il proprio account NetApp o crearne uno per accedere alle note di rilascio.

Capacità

Il riequilibrio EC ora utilizza lo spazio libero

Il ribilanciamento EC ora utilizza lo spazio libero invece dello spazio utilizzato. Consulta ["Scopri di più sul ribilanciamento EC dopo l'espansione in StorageGRID"](#).

Spazio consentito per i metadati

Ora puoi aumentare il valore massimo consentito per i metadati da 3,96 TB a 7,92 TB. Consulta ["Spazio consentito di metadati"](#).

Controllo accessi

SSO tramite OIDC

Ora puoi ["Configura il single sign-on \(SSO\) in StorageGRID usando OpenID Connect \(OIDC\)"](#).

Federazione

Spazio dei nomi globale

Ora puoi configurare uno spazio dei nomi globale per consentire ai tenant di accedere ai bucket su più sistemi StorageGRID. Consulta ["Scopri lo spazio dei nomi globale"](#).

Gestibilità

Servizio di spostamento automatico ADC

["Quando richiesto per raggiungere il quorum dell'ADC"](#), il servizio ADC verrà ora spostato automaticamente quando sei ["conversione di un nodo di archiviazione in un nodo solo dati"](#) o ["disattivare un nodo di archiviazione"](#).

Ripristino del nodo amministratore primario

Ora puoi ripristinare qualsiasi nodo da un nodo Admin non primario. Consulta ["Ripristino da guasti del nodo Admin primario"](#).

S3

Abilita il blocco degli oggetti S3 sui bucket esistenti

Quando l'impostazione "Consenti blocco oggetti S3 per bucket esistenti" è abilitata, un account tenant S3 può abilitare il blocco oggetti S3 per un bucket esistente. Dopo che un account tenant S3 ha abilitato il blocco oggetti S3 per un bucket esistente, non può essere disabilitato.

Replica consentita per i bucket S3 con Object Lock abilitato

Ora puoi usare CloudMirror per replicare oggetti nei bucket S3 con Object Lock abilitato. Consulta ["Scopri i servizi della piattaforma"](#).

Abilita la replica cross-grid per i bucket non vuoti

Ora puoi abilitare la replica tra griglie per i bucket che non sono vuoti. Consulta ["Requisiti per la replica cross-grid"](#).

Operazioni batch S3 (solo FPVR)

Puoi usare le operazioni batch di S3 per replicare oggetti esistenti in un bucket con controllo delle versioni abilitato che vuoi configurare per la replica tra griglie.

Questa funzionalità richiede l'approvazione FPVR per StorageGRID 12.1. Per utilizzare questa funzionalità, contatta il tuo referente commerciale.

Intestazioni non funzionali delle API REST S3

Le `If-Match` e `If-None-Match` intestazioni sono accettate ma non funzionali per l'API REST S3 `"PutObject"`, `"CompleteMultipartUpload"`, `"Oggetto CopyObject"` e `"DeleteObject (Elimina oggetto)"`.

Per ulteriori informazioni, fai riferimento a ["Modifiche al supporto dell'API REST S3 di StorageGRID"](#).

Supporto per valori di checksum precalcolati

L'interfaccia S3 REST SPI ora supporta i valori di checksum precalcolati e l'``x-amz-checksum-type`` intestazione della richiesta. Consulta ["Aggiornamenti al supporto delle API REST"](#).

Sicurezza

Verifica multi-amministratore

La verifica multi-amministratore (MAV) aiuta a prevenire modifiche accidentali o non autorizzate al sistema StorageGRID. Fai riferimento a ["Scopri la verifica multi-amministratore di StorageGRID"](#).

Aggiornamenti delle policy di sicurezza per FIPS

I rigorosi criteri della politica FIPS sono stati aggiornati. Consulta ["Seleziona una policy di sicurezza in Gestisci la policy TLS e SSH"](#).

Tenant

Sincronizzazione account

La funzionalità *clonazione account* ora si riferisce a una clonazione una tantum delle informazioni di un account tenant specifico.

Account sync è una nuova funzionalità che ti permette di replicare automaticamente e continuamente tenant account, tenant group, tenant user e chiavi di accesso S3 tra i sistemi StorageGRID in una o più connessioni di federazione grid. Consulta ["Scopri la sincronizzazione degli account in StorageGRID"](#).

Endpoint Kafka e autenticazione mTLS

Il protocollo mTLS (Mutual Transport Layer Security) è ora supportato per gli endpoint Kafka. Fai riferimento a ["Configurare gli endpoint dei servizi della piattaforma"](#).

Numero massimo di bucket

Un sistema StorageGRID ora supporta un massimo di 20.000 bucket per ogni account tenant S3.

Aggiornamento

Il tempo per abilitare le funzionalità è aumentato

Durante l'aggiornamento di StorageGRID alla versione 12.1, il tempo necessario per abilitare le funzionalità è aumentato da meno di cinque minuti a un'ora. Consulta ["Stima il tempo necessario per completare un aggiornamento di StorageGRID"](#).

Interfaccia utente

Pagina delle impostazioni BMC

È stata aggiunta una nuova scheda BMC Settings alla pagina Nodes in Grid Manager per consentire il reset della password BMC e le modifiche alle impostazioni IP LAN del BMC. Consulta ["Cambia la password BMC dell'appliance"](#) e ["Modifica le impostazioni IP LAN del nodo BMC dell'appliance"](#). Sono stati aggiunti anche nuovi endpoint API per supportare queste funzioni. Consulta ["Nuovi endpoint per modificare la password BMC e le impostazioni IP della LAN"](#).

Notifiche email

Il Grid Manager ora dispone di una pagina e-mail comune per configurare e gestire le notifiche e-mail per gli avvisi, AutoSupport e la verifica multi-amministratore (MAV). Consulta ["Configura il server di posta elettronica"](#).

Aggiornamento della pagina dei costi del collegamento

StorageGRID 12.1 fornisce informazioni e impostazioni più dettagliate sui costi dei collegamenti. Consulta ["Gestire i costi di collegamento"](#).

controllo della porta USB

Ora puoi abilitare o disabilitare le porte USB tramite Grid Manager. Consulta ["Controlla l'accesso remoto tramite porte USB"](#).

Funzionalità e funzionalità rimosse o deprecate in StorageGRID

Scopri le funzionalità e le capacità rimosse o deprecate in StorageGRID 12.1.0. Prima di eseguire l'aggiornamento, verifica se le funzionalità rimosse o deprecate influiscono sulle applicazioni client o sulla configurazione della grid.

Definizioni

Obsoleto

Non dovresti utilizzare questa funzionalità nei nuovi ambienti di produzione. Gli ambienti di produzione esistenti possono continuare a utilizzare questa funzionalità.

Fine del ciclo di vita

Ultima versione fornita che supporta la funzione. In alcuni casi, la documentazione relativa alla funzione potrebbe essere rimossa in questa fase.

Rimosso

Prima versione che **non** supporta la funzione.

Fine del supporto delle funzionalità di StorageGRID

Le funzioni obsolete verranno rimosse nelle versioni principali N+2. Ad esempio, se una funzione è deprecata nella versione N (ad esempio, 6,3), l'ultima versione in cui la funzione esisterà è N+1 (ad esempio, 6,4). La versione N+2 (ad esempio, 6,5) è la prima versione quando la funzione non esiste nel prodotto.

Per ulteriori informazioni, vedere la ["Pagina supporto versione software"](#).



In alcune situazioni, NetApp potrebbe interrompere il supporto per determinate funzioni prima di quanto indicato.

Funzione	Obsoleto	Fine del ciclo di vita	Rimosso	Collegamenti alla documentazione precedente
Impostazione globale SSE per la crittografia AES-128	12,1	12,2	12,3	A partire da StorageGRID 12.1.0, il supporto per la crittografia AES-128 dei nuovi dati degli oggetti archiviati a riposo è deprecato. Il supporto continua per il recupero degli oggetti archiviati che erano stati originariamente crittografati con AES-128.
Allarmi, legacy (non Alerts)	11,7	11,8	11,9	"Riferimento allarmi (StorageGRID 11,8)"

Funzione	Obsoleto	Fine del ciclo di vita	Rimosso	Collegamenti alla documentazione precedente
Supporto nodo di archivio	11,7	11,8	11,9	"Considerazioni per il decommissionamento dei nodi di archivio (StorageGRID 11,8)" Nota: Prima di iniziare l'aggiornamento, è necessario: 1. Disattiva tutti i nodi di archivio. Consulta "Decommissionamento nodo griglia (sito doc StorageGRID 11,8)". 2. Rimuovi tutti i riferimenti ai nodi di archivio dai pool di archiviazione e dalle policy ILM. Consulta "Knowledge base 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 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 "requisiti software per i nodi basati su software" per un elenco delle versioni di Docker attualmente supportate.
Configurazione email (legacy)	11,9	12,0	12,1	"Configura le notifiche per gli allarmi (sistema legacy) (StorageGRID 11,8)"
Esportazione con audit NFS	11,8	11,9	12,0	"Configurare l'accesso al client di controllo per NFS (StorageGRID 11,8)"
Rimappatura delle porte	12,0	12,1	12,2	
Supporto API Swift	11,7	11,9	12,0	"Utilizzare l'API REST Swift (StorageGRID 11,8)"
RHEL 8,8	11,9	11,9	12,0	

Funzione	Obsoleto	Fine del ciclo di vita	Rimosso	Collegamenti 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	

Fare riferimento anche a:

- ["Modifiche all'API Grid Management"](#)
- ["Modifiche all'API di gestione del tenant"](#)

Modifiche all'API di gestione della griglia in StorageGRID

StorageGRID 12.1 utilizza la versione 4 della Grid Management API. La versione 4 rende obsoleta la versione 3; tuttavia, le versioni 1, 2 e 3 sono ancora supportate.



Puoi continuare a usare le versioni obsolete dell'API di gestione con StorageGRID; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una versione futura di StorageGRID. Dopo l'aggiornamento a StorageGRID 12.0 o versioni successive, puoi disattivare le API obsolete usando l'`PUT /grid/config/management` API.

Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Utilizzare l'API Grid Management"](#).

Nuovi endpoint per modificare la password BMC e le impostazioni IP della LAN

Il seguente endpoint è stato aggiunto per consentirti di ["cambia la password BMC di un appliance"](#).

```
PUT /bmc-configuration/root-password
```

Sono stati aggiunti i seguenti endpoint per consentirti di ["modificare o visualizzare le impostazioni IP LAN del BMC"](#).

```
PUT /grid/bmc/{node-id}/lan-ip-config
```

```
GET /grid/bmc/{node-id}/lan-ip-config
```

Modifiche all'API di gestione dei tenant in StorageGRID

StorageGRID 12.1 utilizza la versione 4 dell'API di gestione dei tenant. La versione 4 sostituisce la versione 3; tuttavia, le versioni 1, 2 e 3 sono ancora supportate.



Puoi continuare a usare le versioni obsolete della Tenant Management API con StorageGRID; tuttavia, il supporto per queste versioni dell'API verrà rimosso in una versione futura di StorageGRID. Dopo l'aggiornamento a StorageGRID 12.0 o versioni successive, puoi disattivare le API obsolete usando l' `PUT /grid/config/management` API.

Per ulteriori informazioni, visitare il sito Web all'indirizzo ["Comprendere l'API di gestione dei tenant"](#).

Nuova API per la replicazione degli oggetti

Puoi usare il `/org/cross-grid-replication/{versionId}/replicate` API per replicare manualmente gli oggetti su un bucket esistente con replica tra griglie appena configurata.

Modifiche al supporto dell'API REST S3 di StorageGRID

L'API REST S3 utilizzata da StorageGRID viene aggiornata regolarmente.

Rilasciare	Commenti
12.1.0	• <code>If-Match</code> L' <code>If-Match</code> intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l' <code>If-Match</code> intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented. • <code>If-None-Match</code> L' <code>If-None-Match</code> intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l' <code>If-None-Match</code> intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented. • Aggiunto il supporto per i valori di checksum precalcolati per le seguenti richieste e intestazioni supportate: ◦ <code>CompleteMultipartUpload</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, e <code>x-amz-checksum-crc64nvme</code> ◦ <code>CreateMultipartUpload</code>: <code>CRC32</code>, <code>CRC32C</code>, e <code>CRC64NVME</code> per <code>x-amz-checksum-algorithm</code> ◦ <code>CopyObject</code>: <code>CRC32</code>, <code>CRC32C</code>, <code>CRC64NVME</code>, e <code>SHA256</code> per <code>x-amz-checksum-algorithm</code> ◦ <code>PutObject</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, e <code>x-amz-checksum-crc64nvme</code> ◦ <code>UploadPart</code>: <code>x-amz-checksum-crc32</code>, <code>x-amz-checksum-crc32c</code>, e <code>x-amz-checksum-crc64nvme</code> • Aggiunto il supporto per <code>x-amz-checksum-type</code> per <code>CreateMultipartUpload</code> e <code>CompleteMultipartUpload</code>. • Aggiunto il supporto per la <code>s3:x-amz-copy-source</code> chiave della condizione di policy. • Consenti di abilitare S3 Object Lock sui bucket esistenti.
12,0	• Aggiunto il supporto per la condivisione delle risorse tra origini (CORS) per un'interfaccia di gestione, che consente a un altro dominio di accedere ai dati in StorageGRID utilizzando le API di gestione. "Scopri di più" . • Aggiunto il supporto per STS AssumeRole e le policy di sessione. Vedi "un esempio di politica di sessione". Puoi configurare AssumeRole nei gruppi tenant.

Rilasciare	Commenti
11,9	• Aggiunto supporto per valori checksum SHA-256 pre-calcolati per le seguenti richieste e intestazioni supportate. È possibile utilizzare questa funzione per verificare l'integrità degli oggetti caricati: ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ HeadObject (scarto capo): x-amz-checksum-mode ◦ ListParts ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • È stata aggiunta la possibilità per l'amministratore di grid di controllare le impostazioni di conservazione e conformità a livello di tenant. Queste impostazioni influiscono sulle impostazioni di blocco degli oggetti S3. ◦ Modalità di conservazione predefinita bucket e modalità di conservazione degli oggetti: Governance o conformità, se consentite dall'amministratore del grid. ◦ Periodo di conservazione predefinito del bucket e conservazione dell'oggetto fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia. • Supporto migliorato per la <code>aws-chunked</code> codifica del contenuto e i valori di streaming <code>x-amz-content-sha256</code>. 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 in modo che corrispondano ai nomi utilizzati in "Documentazione Amazon Web Services (AWS): Riferimento API Amazon Simple Storage Service" .
11,7	• Aggiunto "Riferimento rapido: Richieste API S3 supportate". • Aggiunto supporto per l'utilizzo della modalità DI GOVERNANCE con S3 Object Lock. • Aggiunto supporto per l'intestazione di risposta specifica di StorageGRID <code>x-ntap-sg-cgr-replication-status</code> per le richieste di oggetti GET e HEAD. Questa intestazione fornisce lo stato di replica di un oggetto per la replica cross-grid. • Le richieste SelectObjectContent ora supportano gli oggetti Parquet.

Rilasciare	Commenti
11,6	• Aggiunto il supporto per l'utilizzo del <code>partNumber</code> parametro di richiesta nelle richieste GET Object e HEAD Object. • Aggiunto supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock. • È stato aggiunto il supporto per <code>s3:object-lock-remaining-retention-days</code> la chiave della condizione della policy per impostare l'intervallo di periodi di conservazione consentiti per gli oggetti. • Modifica della dimensione massima <i>consigliata</i> per un'operazione di singolo oggetto PUT in 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.
11,5	• Aggiunto supporto per la gestione della crittografia bucket. • Aggiunto supporto per S3 Object Lock e richieste legacy di Compliance obsolete. • Aggiunto il supporto per l'utilizzo DELL'ELIMINAZIONE di più oggetti nei bucket con versione. • L'`Content-MD5` intestazione della richiesta è ora supportata correttamente.
11,4	• Aggiunto supporto per L'ELIMINAZIONE di tag bucket, L'AGGIUNTA DI tag bucket E L'AGGIUNTA di tag bucket. I tag di allocazione dei costi non sono supportati. • Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. • Aggiunto il supporto per le notifiche bucket sul <code>s3:ObjectRestore:Post</code> tipo di evento. • I limiti di dimensione AWS per le parti multipart vengono ora applicati. Ogni parte di un caricamento multiparte deve essere compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB. • Aggiunto supporto per TLS 1.3
11,3	• Aggiunto supporto per la crittografia lato server dei dati a oggetti con chiavi fornite dal cliente (SSE-C). • Aggiunto supporto per le operazioni di ELIMINAZIONE, RECUPERO e INSERIMENTO DEL ciclo di vita del bucket (solo azione scadenza) e per l'`x-amz-expiration` intestazione della risposta. • Aggiornamento DI PUT object, PUT object - Copy e Multipart Upload per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione. • Le crittografia TLS 1.1 non sono più supportate.

Rilasciare	Commenti
11,2	Aggiunto supporto per il ripristino POST-oggetto da utilizzare con i Cloud Storage Pools. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione dei criteri e variabili dei criteri in policy di gruppo e bucket. Le policy di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID continueranno a essere supportate. Nota: gli utilizzi di ARN/URN in altre configurazioni JSON/XML, inclusi quelli utilizzati nelle funzionalità personalizzate di StorageGRID, non sono cambiati.
11,1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per connessioni client S3 ai nodi di rete e impostazioni di conformità sui bucket.
11,0	Supporto aggiunto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. Inoltre, è stato aggiunto il supporto per i vincoli di posizione dei tag degli oggetti per i bucket e la coerenza disponibile.
10,4	Aggiunto supporto per le modifiche di scansione ILM alle versioni, agli aggiornamenti delle pagine dei nomi di dominio degli endpoint, alle condizioni e alle variabili nei criteri, agli esempi di policy e all'autorizzazione PutOverwriteObject.
10,3	Aggiunto supporto per il controllo delle versioni.
10,2	Aggiunto supporto per policy di accesso di gruppo e bucket e per copia multiparte (carica parte - Copia).
10,1	Aggiunto il supporto per il caricamento multipart, le richieste in stile virtual-hosted e l'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.

Consulta ["Versioni e aggiornamenti supportati dall'API REST S3"](#) per maggiori informazioni.

Inizia subito con un sistema StorageGRID

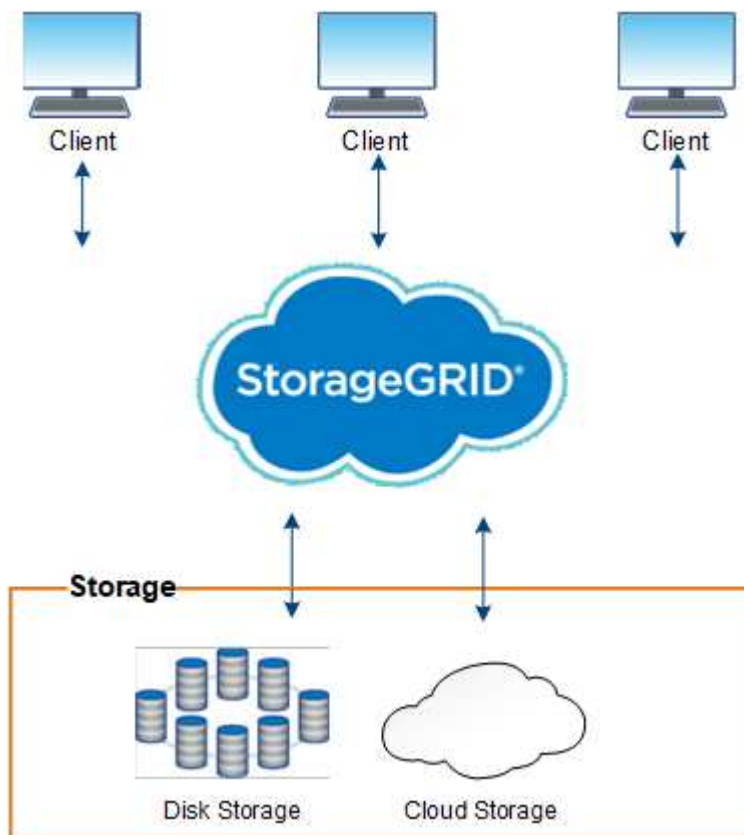
Scopri di più su StorageGRID

Che cos'è StorageGRID?

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

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

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



Il supporto per i nodi 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 cloud storage ILM", che offre più funzionalità.

Vantaggi di StorageGRID

I vantaggi del sistema StorageGRID includono:

- Un repository di dati distribuito geograficamente per dati non strutturati, estremamente scalabile e facile da utilizzare.
- Protocollo di archiviazione oggetti standard di Amazon Web Services Simple Storage Service (S3).
- Cloud ibrido abilitato. ILM (Information Lifecycle Management) basato su policy archivia gli oggetti nei cloud pubblici, tra cui Amazon Web Services (AWS) e Microsoft Azure. I servizi della piattaforma StorageGRID consentono la replica dei contenuti, la notifica degli eventi e la ricerca dei metadati degli oggetti archiviati nei cloud pubblici.
- Protezione flessibile dei dati per garantire durata e disponibilità. I dati possono essere protetti mediante replica e erasure coding a più livelli. La verifica dei dati a riposo e a bordo garantisce l'integrità per una conservazione a lungo termine.
- Gestione dinamica del ciclo di vita dei dati per aiutare a gestire i costi dello storage. È possibile creare regole ILM che gestiscono il ciclo di vita dei dati a livello di oggetto, personalizzando la posizione, la durata, le performance, i costi dei dati, e tempo di conservazione.
- Elevata disponibilità dello storage dei dati e di alcune funzioni di gestione, con bilanciamento del carico integrato per ottimizzare il carico dei dati tra le risorse StorageGRID.
- Supporto di più account tenant di storage per separare gli oggetti memorizzati nel sistema da diverse entità.
- Numerosi strumenti per il monitoraggio dello stato di salute del sistema StorageGRID, tra cui un sistema di avviso completo, una dashboard grafica e stati dettagliati per tutti i nodi e i siti.
- Supporto per l'implementazione basata su software o basata su hardware. Puoi implementare StorageGRID su una delle seguenti opzioni:
 - Macchine virtuali in esecuzione in VMware.
 - Motori container su host Linux.
 - Apparecchiature progettate da StorageGRID.
 - Le appliance di storage forniscono storage a oggetti.
 - Le appliance di servizi offrono servizi di gestione della griglia e bilanciamento del carico.
- Conforme ai requisiti di storage pertinenti delle seguenti normative:
 - Securities and Exchange Commission (SEC) in 17 cfr § 240.17a-4(f), che regola i membri di Exchange, gli intermediari o i rivenditori.
 - Financial Industry Regulatory Authority (FINRA) Rule 4511(c), che si difende ai requisiti di formato e supporti della norma SEC 17a-4(f).
 - Commodity Futures Trading Commission (CFTC) nel regolamento 17 cfr § 1.31(c)-(d), che regola il trading dei futures sulle commodity.
- Operazioni di upgrade e manutenzione senza interruzioni. Mantenere l'accesso ai contenuti durante le procedure di aggiornamento, espansione, decommissionamento e manutenzione.
- Gestione federata delle identità. Si integra con Active Directory, OpenLDAP o Oracle Directory Service per l'autenticazione degli utenti. Supporta il single sign-on (SSO) tramite Security Assertion Markup Language 2.0 (SAML 2.0) o OpenID Connect (OIDC) per lo scambio di dati di autenticazione e autorizzazione tra StorageGRID e un identity provider esterno come Active Directory Federation Services (AD FS).

Cloud ibridi con StorageGRID

Utilizza StorageGRID in una configurazione di cloud ibrido implementando la gestione dei dati basata su policy per memorizzare gli oggetti nei pool di storage cloud, sfruttare i servizi della piattaforma StorageGRID e tiering dei dati da ONTAP a StorageGRID con NetApp FabricPool.

Pool di cloud storage

I Cloud Storage Pools ti permettono di archiviare oggetti al di fuori del sistema StorageGRID. Ad esempio, potresti voler spostare oggetti a cui accedi raramente verso cloud storage a basso costo, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive in Microsoft Azure Blob Storage. Oppure, potresti voler mantenere un backup cloud degli oggetti StorageGRID, che può essere usato per recuperare dati persi a causa di un errore di un volume di archiviazione o di uno Storage Node.

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



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

Servizi della piattaforma S3

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

- Il servizio di replica CloudMirror esegue automaticamente il mirroring di oggetti specifici in un bucket S3 di destinazione, che può essere su Amazon S3 o su un secondo sistema StorageGRID.
- Il servizio di notifica degli eventi invia messaggi 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 di cercare, visualizzare e analizzare i metadati utilizzando strumenti di terze parti.

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

Tiering dei dati ONTAP con FabricPool

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

A differenza delle soluzioni di 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 un pool di storage cloud?"](#)
- ["Gestire i servizi della piattaforma"](#)
- ["Configurare StorageGRID per FabricPool"](#)

Architettura StorageGRID e topologia di rete

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

Scopri di più su ["tipi di nodi della griglia"](#) .

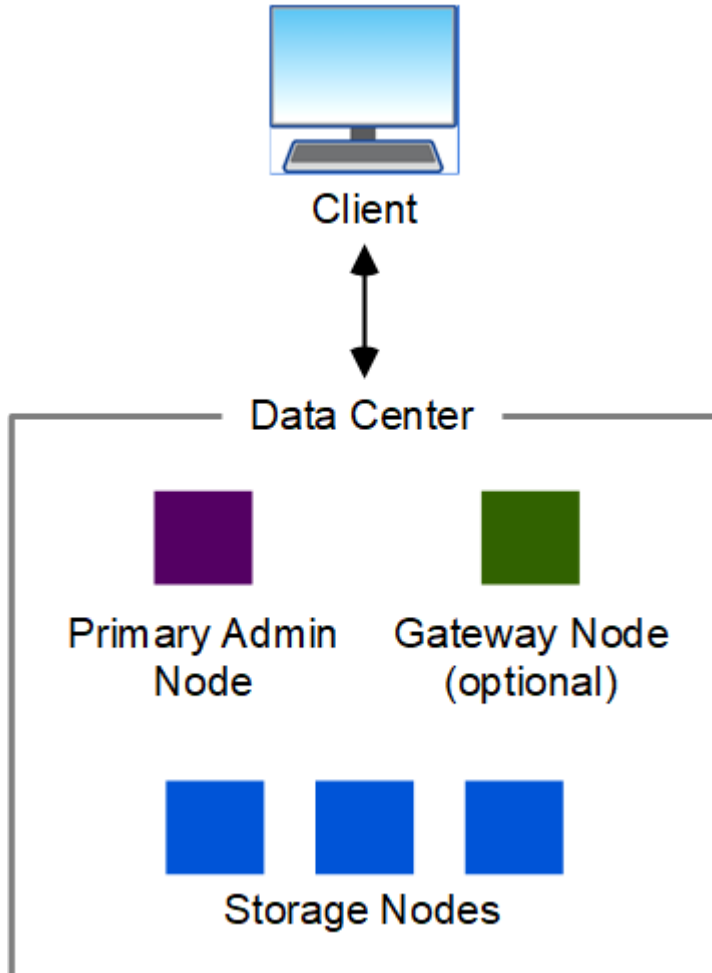
Per ulteriori informazioni sulla topologia di rete di StorageGRID, sui requisiti e sulle comunicazioni della griglia, consulta ["Linee guida per il networking"](#).

Topologie di implementazione

Il sistema StorageGRID può essere distribuito in un singolo sito di data center o in più siti di data center. Il numero massimo di siti per distribuzione è 16.

Sito singolo

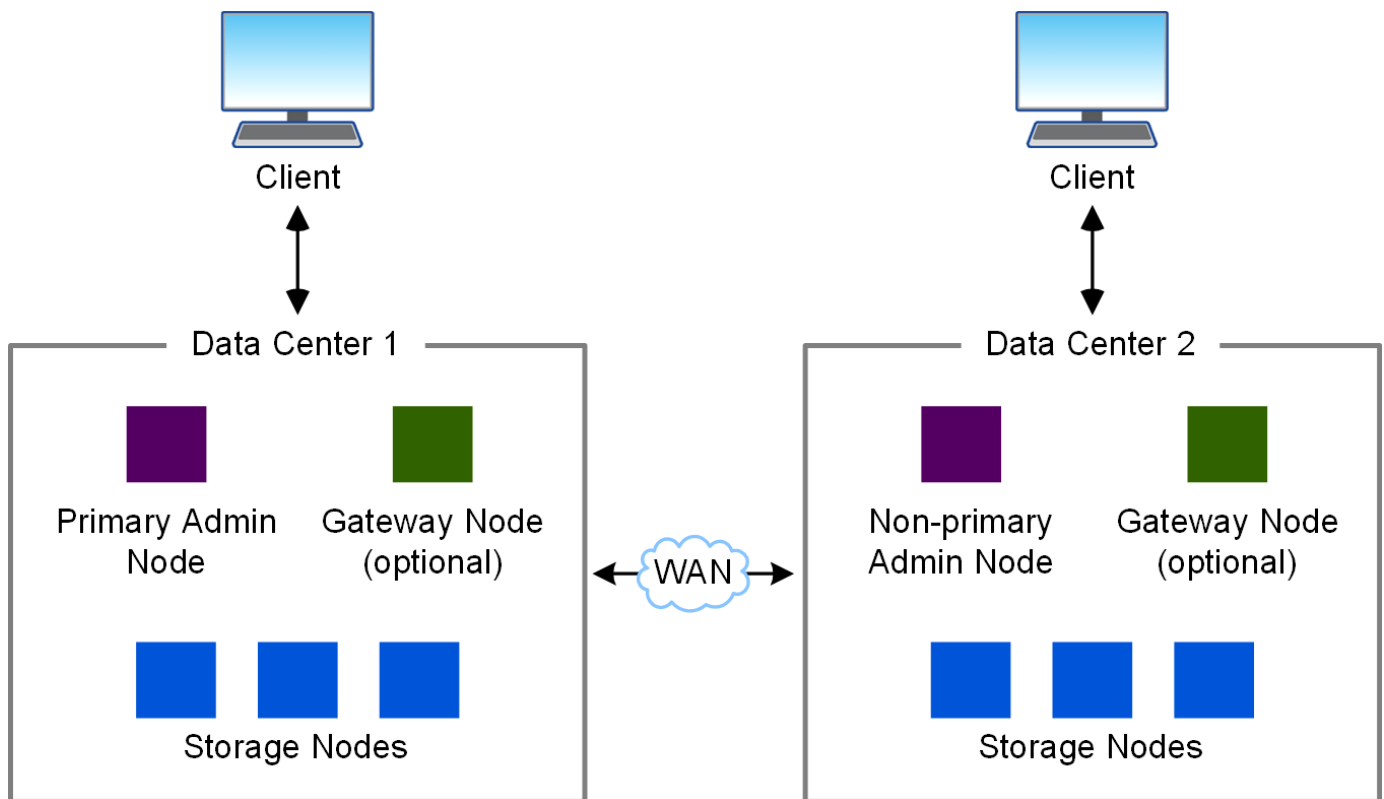
In un'implementazione con un singolo sito, l'infrastruttura e le operazioni del sistema StorageGRID sono centralizzate.



Più siti

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

Spesso i siti sono ubicati 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.



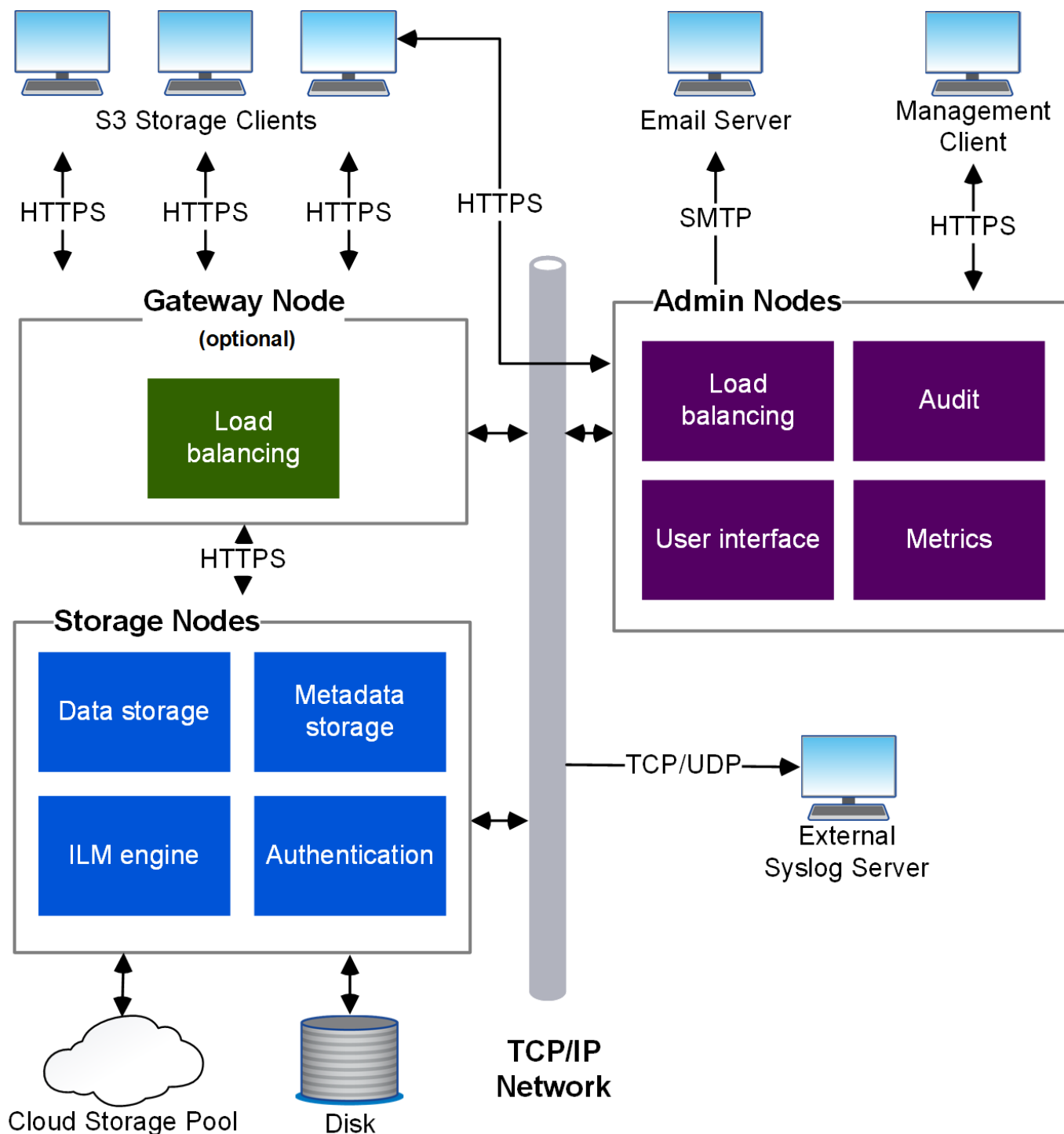
All'interno di un singolo data center possono esistere anche più siti logici per consentire l'uso della replica distribuita e della codifica di cancellazione per una maggiore disponibilità e resilienza.

Ridondanza del nodo di rete

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

Architettura di sistema

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



I client S3 archiviano e recuperano oggetti in StorageGRID. Altri client vengono utilizzati per accedere all'interfaccia di gestione di StorageGRID e, facoltativamente, alla condivisione di audit. Inoltre, StorageGRID può facoltativamente inviare avvisi via email tramite un server SMTP esterno.

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

Gli oggetti possono essere archiviati all'interno di StorageGRID su nodi di archiviazione basati su software o hardware, oppure in Cloud Storage Pools, che consistono in bucket S3 esterni o container Azure Blob Storage.

Nodi e servizi Grid

Nodi e servizi di griglia StorageGRID

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

Tipi di nodi della griglia

Il sistema StorageGRID utilizza tre tipi di nodi di griglia:

Nodi di amministrazione

Fornisci servizi di gestione come la configurazione del sistema, il monitoraggio e la registrazione. Quando accedi al Grid Manager, ti connetti a un Admin Node. Ogni grid deve avere un Admin Node primario e può avere Admin Node non primari aggiuntivi per la ridondanza. Puoi connetterti a qualsiasi Admin Node e ogni Admin Node mostra una vista simile del sistema StorageGRID. Tuttavia, devi eseguire la maggior parte delle procedure di manutenzione utilizzando l'Admin Node primario.

È possibile utilizzare i nodi amministrativi anche per bilanciare il carico del traffico client S3.

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

Nodi di storage

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

Durante l'installazione iniziale di un nuovo nodo di archiviazione, puoi specificare che venga utilizzato solo per ["memorizzare sia metadati che dati"](#).

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

Nodi gateway (opzionali)

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

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

Nodi hardware e software

I nodi StorageGRID possono essere distribuiti come nodi di appliance StorageGRID o come nodi basati su software. Il numero massimo di nodi (inclusi tutti i tipi di nodi) per sistema è 220.

Nodi appliance StorageGRID

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

Per ulteriori informazioni sulle appliance disponibili, vedere quanto segue:

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

- ["NetApp Hardware Universe"](#)

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. Vedere ["Installa StorageGRID sui nodi basati su software"](#).

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

Servizi StorageGRID

Di seguito viene riportato un elenco completo dei servizi StorageGRID.

Servizio	Descrizione	Posizione
Account Service Forwarder	Fornisce un'interfaccia per il servizio Load Balancer per eseguire query sull'account Service sugli host remoti e fornisce notifiche delle modifiche della configurazione degli endpoint del bilanciamento del carico al servizio Load Balancer.	Servizio di bilanciamento del carico su nodi amministrativi e nodi gateway
ADC (Administrative Domain Controller)	Mantiene le informazioni sulla topologia, fornisce servizi di autenticazione e risponde alle query provenienti dai servizi LDR e CMN.	Almeno tre nodi di archiviazione contenenti il servizio ADC in ciascun sito
AMS (Audit Management System)	Monitora e registra tutti gli eventi e le transazioni di sistema verificati in un file di log di testo.	Nodi di amministrazione
Demone Avahi	Gestisce mDNS, utilizzato per la risoluzione dei nomi e l'individuazione dei servizi all'interno della rete locale.	Tutti i nodi
Servizio cache	Viene eseguito sui nodi del bilanciamento del carico (Gateway) e gestisce una cache locale del contenuto degli oggetti.	Nodi gateway
Cassandra	Gestisce il database distribuito per i metadati degli oggetti.	Nodi di archiviazione (tranne quelli solo dati)
Cassandra Reaper	Esegue la riparazione automatica dei metadati degli oggetti.	Nodi di storage
Servizio a pezzi	Gestisce i dati con codifica erasure e i frammenti di parità.	Nodi di storage
CMN (nodo di gestione della configurazione)	Gestisce le configurazioni a livello di sistema e le attività di grid. Ogni griglia dispone di un servizio CMN.	Nodo amministratore primario

Servizio	Descrizione	Posizione
DDS (archiviazione dati distribuita)	Si interfaccia con il database Cassandra per gestire i metadati degli oggetti.	Nodi di storage
DMV (Data Mover)	Sposta i dati negli endpoint cloud.	Nodi di storage
Dynamic IP (dinamico)	Monitora la griglia per verificare la presenza di modifiche IP dinamiche e aggiorna le configurazioni locali.	Tutti i nodi
gdu-server	Il task runner di backend per le operazioni di manutenzione e provisioning della griglia. Accetta richieste da <code>mgmt-api</code> e da altri script di utilità, le convalida e inoltra ogni azione al gestore di attività GDU appropriato, come provisioning, espansione, decommission, e aggiornamenti.	Nodi di amministrazione
Grafana	Utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi di amministrazione
Alta disponibilità	Gestisce gli indirizzi IP virtuali ad alta disponibilità sui nodi configurati nella pagina Gruppi ad alta disponibilità. Questo servizio è anche noto come servizio <i>keepalived</i> .	Nodi Admin e Gateway
Identità (idnt)	Gestisce utenti e gruppi locali, l'autenticazione e federa le identità degli utenti da LDAP e Active Directory.	Nodi di storage che utilizzano il servizio ADC
Arbitro lambda	Gestisce le richieste S3 Select SelectObjectContent.	Tutti i nodi
Bilanciamento del carico (nginx-gw)	Bilanciamento del carico del traffico S3 fra i client e i nodi storage.	Nodi Admin e Gateway
LDR (router di distribuzione locale)	Gestisce lo storage e il trasferimento dei contenuti all'interno della griglia.	Nodi di storage
mgmt-api	L'API di backend di Grid Manager. Espone endpoint REST autenticati per l'amministrazione della grid (configurazione, monitoraggio e workflow di manutenzione), applica convalide e autorizzazioni e orchestra operazioni di lunga durata. L'API principale del control-plane utilizzata dall'interfaccia di Grid Manager e dai client di automazione.	Nodi di amministrazione

Servizio	Descrizione	Posizione
Daemon di controllo del servizio informazioni MISCd	Fornisce un'interfaccia per eseguire query e gestire servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio per eseguire query sullo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi
nginx	Agisce come meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynamic IP) per poter comunicare con servizi su altri nodi tramite API HTTPS.	Tutti i nodi
Bilanciatore del carico nginx-gw	Bilanciamento del carico del traffico S3 fra i client e i nodi storage.	Nodi Admin e Gateway
NMS (Network Management System, sistema di gestione della rete)	Alimenta le opzioni di monitoraggio, reporting e configurazione visualizzate tramite Grid Manager.	Nodi di amministrazione
Esportatore di nodi (raccolta dati Prometheus)	Pubblica statistiche a livello di sistema per la raccolta di metriche di serie temporali di Prometheus.	Tutti i nodi
NTP	Servizio NTP (Network Time Protocol).	Tutti i nodi
Persistenza	Gestisce i file sul disco root che devono persistere durante un riavvio.	Tutti i nodi
Prometheus	Raccoglie le metriche delle serie temporali dai servizi su tutti i nodi.	Nodi di amministrazione
RSM (macchina a stato replicato)	Garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.	Nodi di storage che utilizzano il servizio ADC
SSM (Server Status Monitor)	Monitora le condizioni dell'hardware e invia report al servizio NMS.	Un'istanza è presente su ogni nodo della griglia
Responsabile del server	Gestisce i servizi StorageGRID .	Tutti i nodi
Agente SNMP	Risponde alle richieste SNMP.	Nodi di amministrazione
Servizio di gestione delle porte SNMP	Gestisce la gestione dinamica delle porte SNMP.	Tutti i nodi

Servizio	Descrizione	Posizione
SSH (Secure Shell)	Gestisce l'accesso sicuro e la gestione remota del sistema.	Tutti i nodi
SSM (monitor dello stato del sistema)	Monitora le condizioni dell'hardware e invia report al servizio NMS.	Tutti i nodi
Statistica	Registra metriche aggiuntive relative ai bucket S3.	Nodi di storage
Agente di tracciamento (jaeger-agent)	Riceve ed elabora le informazioni di tracciamento inviate dal raccoglitore di tracce (jaeger-collector).	Tutti i nodi
Trace Collector (jaeger-collector)	Esegue la raccolta di tracce per raccogliere informazioni da utilizzare per il supporto tecnico. Il servizio di raccolta tracce utilizza il software open source Jaeger.	Nodi di amministrazione

Che cos'è un nodo di amministrazione StorageGRID?

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. È possibile utilizzare i nodi amministrativi anche per bilanciare il carico del traffico client S3. Ogni grid deve avere un nodo di amministrazione primario e può avere un numero qualsiasi di nodi di amministrazione non primari per la ridondanza.

Differenze tra i nodi amministrativi primari e non primari

Quando 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 devono essere eseguite dal nodo di amministrazione principale.

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

Funzionalità	Nodo amministratore primario	Nodo amministrativo non primario
Include il AMS servizio	Sì	Sì
Include il CMN servizio	Sì	No
Include il NMS servizio	Sì	Sì
Include il Prometheus servizio	Sì	Sì

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

nodo amministratore mittente preferito

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

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 Admin diventano "islanded" l'uno dall'altro, sia il mittente preferito che i mittenti in standby tenteranno di inviare notifiche e potrebbero essere ricevute più copie delle notifiche.
- Se un 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 verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività.

Servizi primari per nodi di amministrazione

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

Servizio	Funzione dei tasti
Audit Management System (AMS)	Tiene traccia dell'attività e degli eventi del sistema.
nodo di gestione della configurazione (CMN)	Gestisce la configurazione a livello di sistema.
[[alta disponibilità]]alta disponibilità	Gestisce gli indirizzi IP virtuali ad alta disponibilità per gruppi di nodi di amministrazione e nodi gateway. Nota: questo servizio si trova anche sui nodi gateway.
[[bilanciamento del carico]]bilanciamento del carico	Bilanciamento del carico del traffico S3 fra i client e i nodi storage. Nota: questo servizio si trova anche sui nodi gateway.
Management Application Program Interface (api di gestione)	Elabora le richieste provenienti dall'API Grid Management e dall'API Tenant Management.
Network Management System (NMS)	Fornisce funzionalità per Grid Manager.
Prometheus	Raccoglie e memorizza le metriche delle serie temporali dai servizi su tutti i nodi.
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

Che cos'è un nodo di archiviazione StorageGRID?

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

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

Tipi di nodi storage

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

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

Nodo di storage dati e metadati (combinato)

Per impostazione predefinita, tutti i nuovi Storage Node memorizzano sia i dati oggetto sia i metadati. Questo tipo di Storage Node viene chiamato Storage Node *combinato*.

Nodo storage solo metadati

L'utilizzo di un nodo di storage esclusivamente per i metadati può avere senso se il grid memorizza un numero molto elevato di piccoli oggetti. L'installazione della capacità di metadati dedicata fornisce un migliore equilibrio tra lo spazio necessario per un numero molto elevato di oggetti piccoli e lo spazio necessario per i metadati per tali oggetti. Inoltre, i nodi di storage solo per i metadati ospitati su appliance dalle performance elevate possono migliorare le performance.

I nodi di storage solo per metadati hanno requisiti hardware specifici:

- Quando usi le appliance StorageGRID, puoi configurare solo nodi esclusivamente per i metadati sulle appliance SGF6112 con dodici unità da 1,9 TB o dodici unità da 3,8 TB.
- Quando usi nodi basati su software, devi assicurarti che le risorse dei nodi solo metadati corrispondano alle risorse dei nodi di archiviazione esistenti. Per esempio:
 - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
 - 128 GB DI RAM
 - CPU a 8 core
 - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
 - Se il sito StorageGRID esistente utilizza nodi di archiviazione 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 dovrebbe, come minimo, corrispondere a quella dei siti esistenti. Le risorse in un nuovo sito devono corrispondere ai nodi di archiviazione nei siti esistenti.



Sebbene i nodi di storage solo per metadati contengano [Servizio LDR](#) e siano in grado di elaborare S3 richieste client, le performance di StorageGRID potrebbero non aumentare.

Nodo storage solo dati

L'utilizzo di un nodo di storage esclusivamente per i dati può essere utile se i nodi di storage hanno caratteristiche di prestazioni diverse. Ad esempio, per aumentare potenzialmente le performance, potrebbero esserci nodi di storage su disco rotante a elevata capacità e solo dati accompagnati da nodi di storage dalle performance elevate e solo metadati.

Inoltre, è possibile ottenere una maggiore capacità di metadati rimuovendo i nodi con poca RAM da Cassandra, il che aumenta il limite di capacità di metadati per nodo. Fare riferimento a ["Gestire lo storage dei metadati degli oggetti"](#).

Puoi convertire un nodo di archiviazione combinato in un nodo di archiviazione solo dati. Se il nodo di archiviazione contiene il [Servizio ADC](#) e vengono soddisfatti i prerequisiti per la conversione, il servizio viene spostato automaticamente in un altro nodo di archiviazione nello stesso sito durante la conversione. Per i prerequisiti e i passaggi dettagliati, consulta ["Convertire un nodo di archiviazione in un nodo solo dati"](#).

Nodi di archiviazione richiesti per griglia e per sito

Quando selezioni quali nodi di archiviazione utilizzare nella tua topologia, tieni presente che la griglia o ciascun sito nella griglia deve contenere quanto segue:

- Per sito (in una griglia a sito singolo o multiplo): tre [ADC](#) Nodi di archiviazione (possono essere qualsiasi combinazione di nodi di archiviazione combinati e solo metadati)
- Griglia a sito singolo: almeno due nodi di archiviazione di oggetti (possono essere qualsiasi combinazione di combinati e solo dati)
- Griglia multi-sito: almeno un nodo di archiviazione degli oggetti per sito (può essere combinato o solo dati)

Servizi primari per i nodi di storage

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



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

Servizio	Funzione dei tasti
Account (acct)	Gestisce gli account tenant. I nodi di archiviazione solo dati non ospitano questo servizio.

Servizio	Funzione dei tasti
Controller di dominio amministrativo (ADC)	Mantiene la topologia e la configurazione a livello di griglia. I nodi di archiviazione solo dati non ospitano questo servizio. Dettagli Il servizio ADC (Administrative Domain Controller) autentica i nodi della griglia e le relative connessioni tra loro. Il servizio ADC è ospitato su un minimo di tre nodi di storage in un sito. Il servizio ADC gestisce le informazioni sulla topologia, inclusi l'ubicazione e la disponibilità dei servizi. Quando un nodo della griglia necessita di informazioni da un altro nodo della griglia o di un'azione da eseguire da parte di un altro nodo della griglia, contatta un servizio ADC per individuare il nodo della griglia più adatto a elaborare la sua richiesta. Inoltre, il servizio ADC conserva una copia dei bundle di configurazione dell'implementazione StorageGRID, consentendo a qualsiasi nodo della griglia di recuperare le informazioni di configurazione correnti. Per facilitare le operazioni distribuite e islanded, ciascun servizio ADC sincronizza certificati, bundle di configurazione e informazioni sui servizi e sulla topologia con gli altri servizi ADC nel sistema StorageGRID. In generale, tutti i nodi di rete mantengono una connessione ad almeno un servizio ADC. In questo modo, i nodi della griglia accedono sempre alle informazioni più recenti. Quando i nodi di rete si connettono, memorizzano nella cache i certificati di altri nodi di rete, consentendo ai sistemi di continuare a funzionare con i nodi di rete noti anche quando un servizio ADC non è disponibile. I nuovi nodi di rete possono stabilire connessioni solo utilizzando un servizio ADC. La connessione di ciascun nodo di rete consente al servizio ADC di raccogliere informazioni sulla topologia. Queste informazioni sul nodo della griglia includono il carico della CPU, lo spazio su disco disponibile (se dotato di storage), i servizi supportati e l'ID del sito del nodo della griglia. Altri servizi richiedono al servizio ADC informazioni sulla topologia tramite query sulla topologia. Il servizio ADC risponde a ogni richiesta con le informazioni più recenti ricevute dal sistema StorageGRID.
Cassandra	Memorizza e protegge i metadati degli oggetti. I nodi di archiviazione solo dati non ospitano questo servizio.
Cassandra Reaper	Esegue la riparazione automatica dei metadati degli oggetti. I nodi di archiviazione solo dati non ospitano questo servizio.
Chunk	Gestisce i dati con codifica erasure e i frammenti di parità.

Servizio	Funzione dei tasti
Data Mover (dmv)	Sposta i dati nei pool di cloud storage.
Data store distribuito (DDS)	Monitora lo storage dei metadati degli oggetti. Dettagli Ogni nodo di storage include il servizio DDS (Distributed Data Store). Questo servizio si interfaccia con il database Cassandra per eseguire attività in background sui metadati degli oggetti archiviati nel sistema StorageGRID. Il servizio DDS tiene traccia del numero totale di oggetti acquisiti nel sistema StorageGRID e del numero totale di oggetti acquisiti tramite ciascuna delle interfacce supportate dal sistema (S3).
Identità (idnt)	Consente di federare le identità degli utenti da LDAP e Active Directory. I nodi di archiviazione solo dati non ospitano questo servizio.

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

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

Che cos'è un nodo gateway StorageGRID? I nodi di gateway forniscono un'interfaccia di bilanciamento del carico dedicata che le applicazioni client S3 possono utilizzare per la connessione a StorageGRID. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro tra più nodi di storage. I nodi del gateway sono opzionali. Il servizio di bilanciamento del carico StorageGRID viene fornito su tutti i nodi amministrativi e su tutti i nodi gateway. Esegue la terminazione TLS (Trasporto Layer Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Il servizio di bilanciamento del carico indirizza perfettamente i client a un nodo di storage ottimale, in modo che il guasto dei nodi o persino di un intero sito sia trasparente. È possibile configurare uno o più endpoint di bilanciamento del carico per definire la porta e il protocollo di rete (HTTPS o HTTP) utilizzati dalle richieste client in entrata e in uscita per accedere ai servizi di bilanciamento del carico sui nodi Gateway e Admin. L'endpoint di bilanciamento del carico definisce anche il tipo di client (S3), la modalità di associazione e, facoltativamente, un elenco di tenant consentiti o bloccati. Vedere "Considerazioni per il bilanciamento del carico". Se necessario, puoi raggruppare le interfacce di rete di più nodi di gateway e nodi amministrativi in un gruppo ad alta disponibilità (ha). In caso di guasto dell'interfaccia attiva nel gruppo di ha, un'interfaccia di backup può gestire il workload dell'applicazione client. Vedere "Gestire i gruppi ad alta disponibilità (ha)". Servizi primari per i nodi gateway La tabella seguente mostra i servizi primari per i nodi gateway, tuttavia, questa tabella non elenca tutti i servizi dei nodi.	Il servizio LDR gestisce le seguenti attività: • Query • Attività LLM (Information Lifecycle Management) • Eliminazione di oggetti • Trasferimenti di dati a oggetti da un altro servizio LDR (nodo di storage). • CS (Consistent Storage Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Il servizio di bilanciamento del carico indirizza perfettamente i client a un nodo di storage ottimale, in modo che il guasto dei nodi o persino di un intero sito sia trasparente. • Interfaccia protocollo S3 Il servizio LDR associa inoltre ciascun oggetto S3 al suo UUID univoco. Archivi di oggetti Gli archivi di oggetti in un nodo di storage sono identificati da un numero esadecimale compreso tra 0000 e 002F, noto come ID del volume. Lo spazio è riservato nel primo archivio di oggetti (volume 0) per i metadati degli oggetti in un database Cassandra; qualsiasi spazio rimanente in tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri archivi di oggetti vengono utilizzati esclusivamente per i dati degli oggetti, che includono copie replicate e frammenti con codifica di cancellazione. Per garantire un utilizzo uniforme dello spazio per le copie replicate, i dati

Servizio	Funzione dei tasti
Servizio cache	Gestisce una cache locale del contenuto dell'oggetto.
Alta disponibilità	Gestisce gli indirizzi IP virtuali ad alta disponibilità per gruppi di nodi di amministrazione e nodi gateway. Nota: questo servizio si trova anche nei nodi di amministrazione.
Bilanciamento del carico	Bilanciamento del carico Layer 7 del traffico S3 dai client ai nodi storage. Si tratta del meccanismo di bilanciamento del carico consigliato. Nota: questo servizio si trova anche nei nodi di amministrazione.

Servizio	Funzione dei tasti
Server Status Monitor (SSM)	Monitora il sistema operativo e l'hardware sottostante.

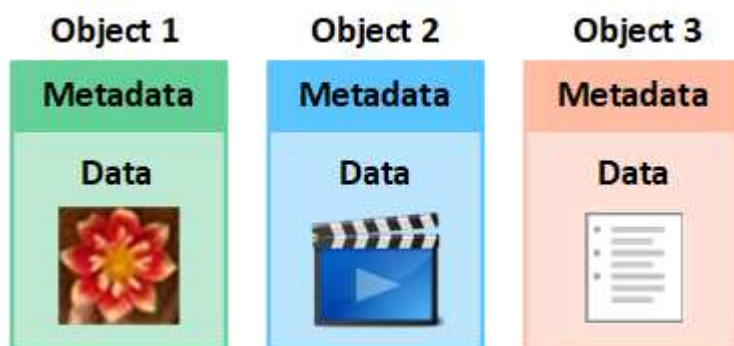
Come StorageGRID gestisce i dati

Che cos'è un oggetto StorageGRID

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

Lo storage a oggetti separa la posizione fisica dei dati dal metodo utilizzato per memorizzare e recuperare tali dati.

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



Che cos'è un dato a oggetti?

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

Che cos'è il metadata a oggetti?

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

I metadati dell'oggetto includono informazioni come:

- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3, il nome o l'ID dell'account tenant, le dimensioni logiche dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
- La posizione di storage corrente di ogni copia di oggetto o frammento con codifica di cancellazione.
- Qualsiasi metadati utente associato all'oggetto.

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

Per informazioni dettagliate su come e dove StorageGRID archivia i metadati degli oggetti, visitare il sito

"Gestire lo storage dei metadati degli oggetti".

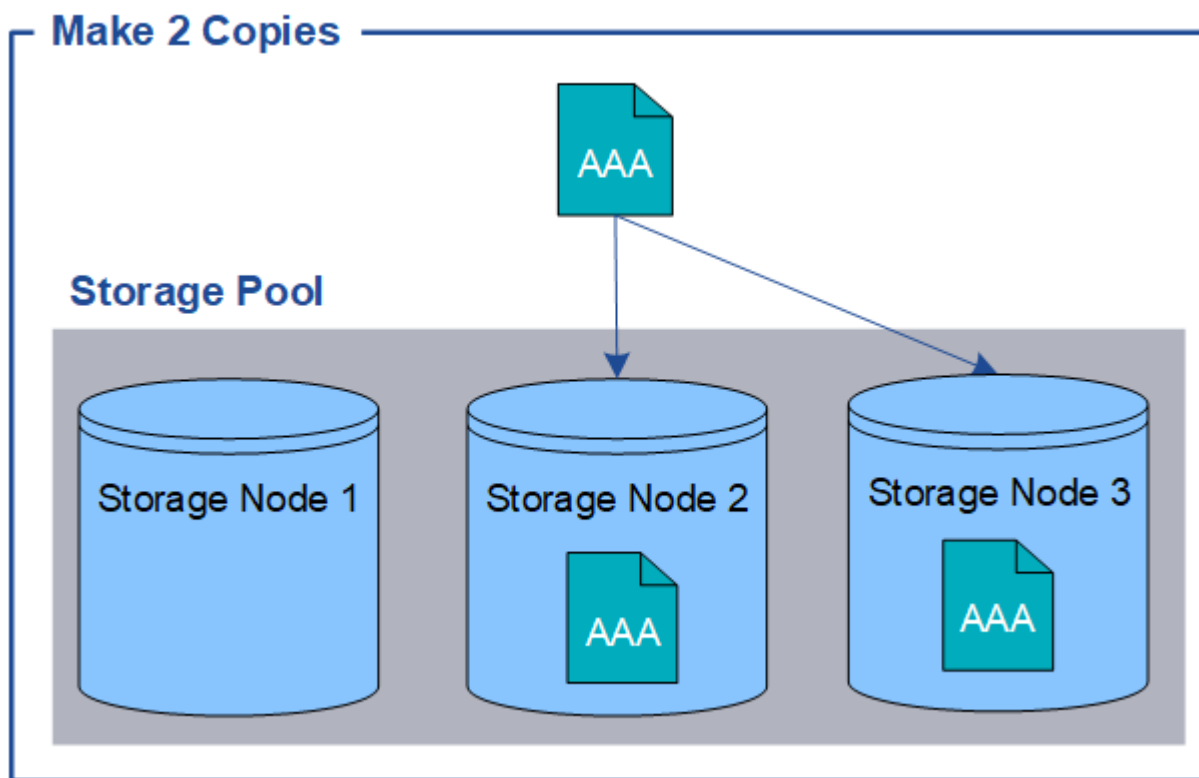
Come vengono protetti i dati a oggetti?

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

Replica

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

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

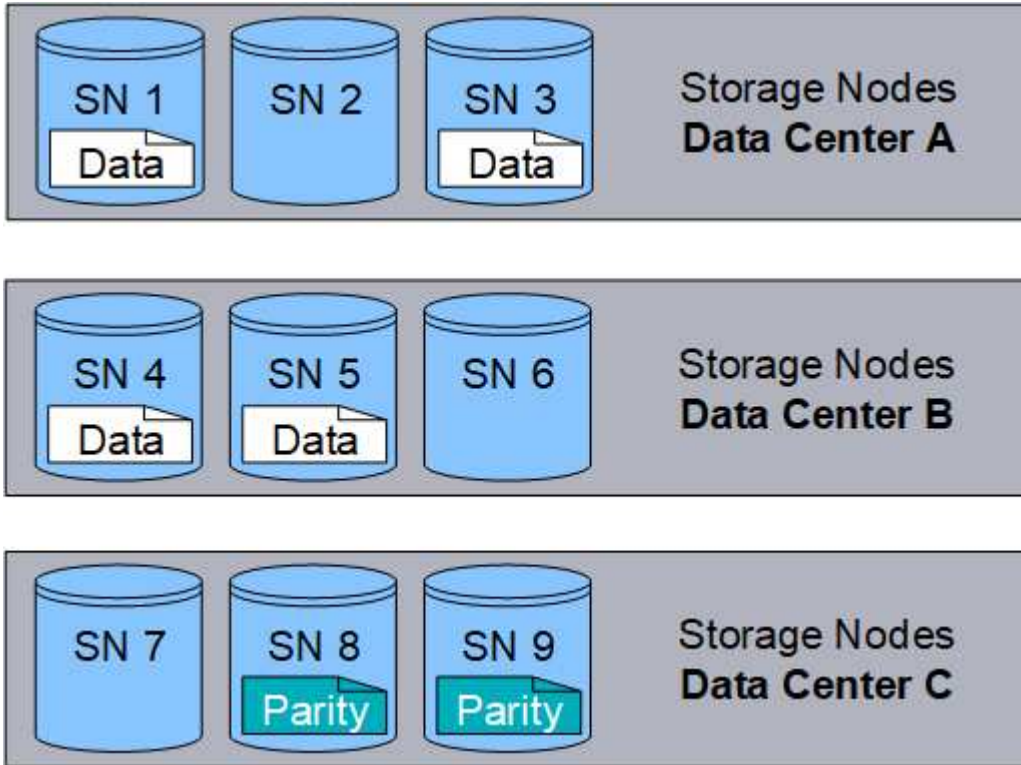


Erasure coding

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

Nell'esempio riportato di seguito viene illustrato l'utilizzo della codifica erasure sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto. Ciascuno dei sei

frammenti viene memorizzato su un nodo di storage diverso in tre data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.



Informazioni correlate

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

ciclo di vita degli oggetti in StorageGRID

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

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

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



Informazioni correlate

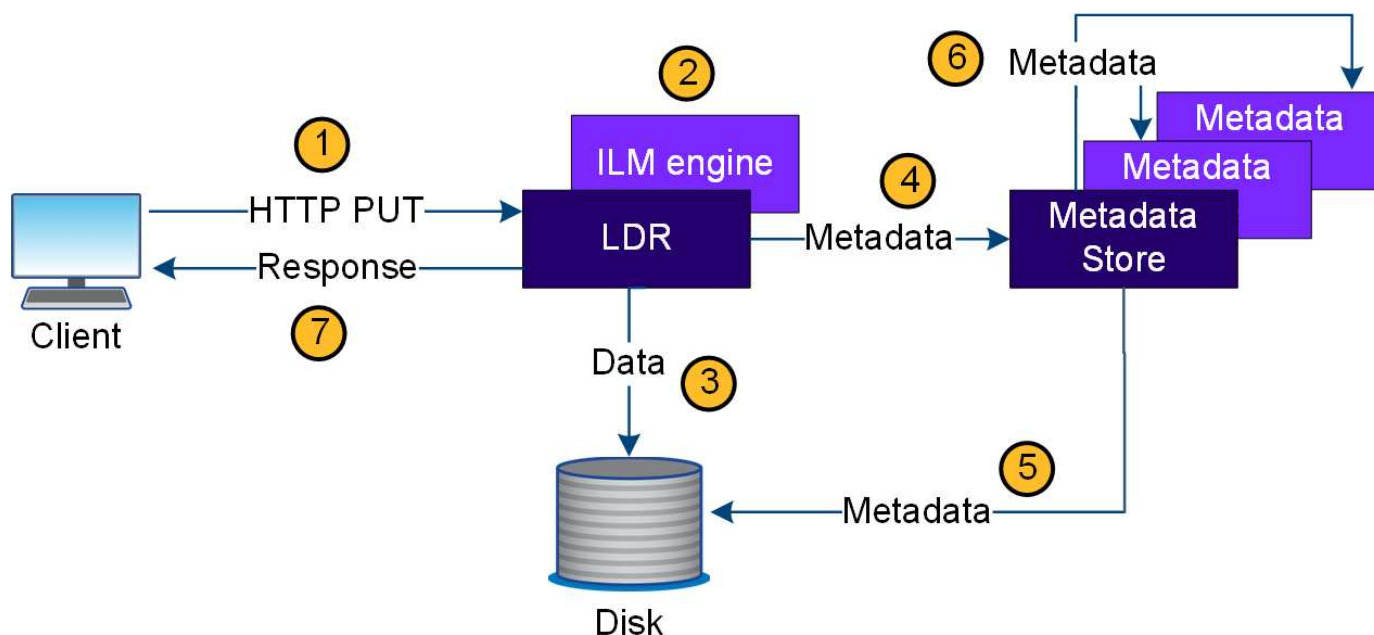
- ["Gestire gli oggetti con ILM"](#)
- ["Utilizza la gestione del ciclo di vita delle informazioni"](#)

Come StorageGRID gestisce l'ingestione degli oggetti

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

Flusso di dati

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



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

acquisito.

Come StorageGRID gestisce le copie degli oggetti

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

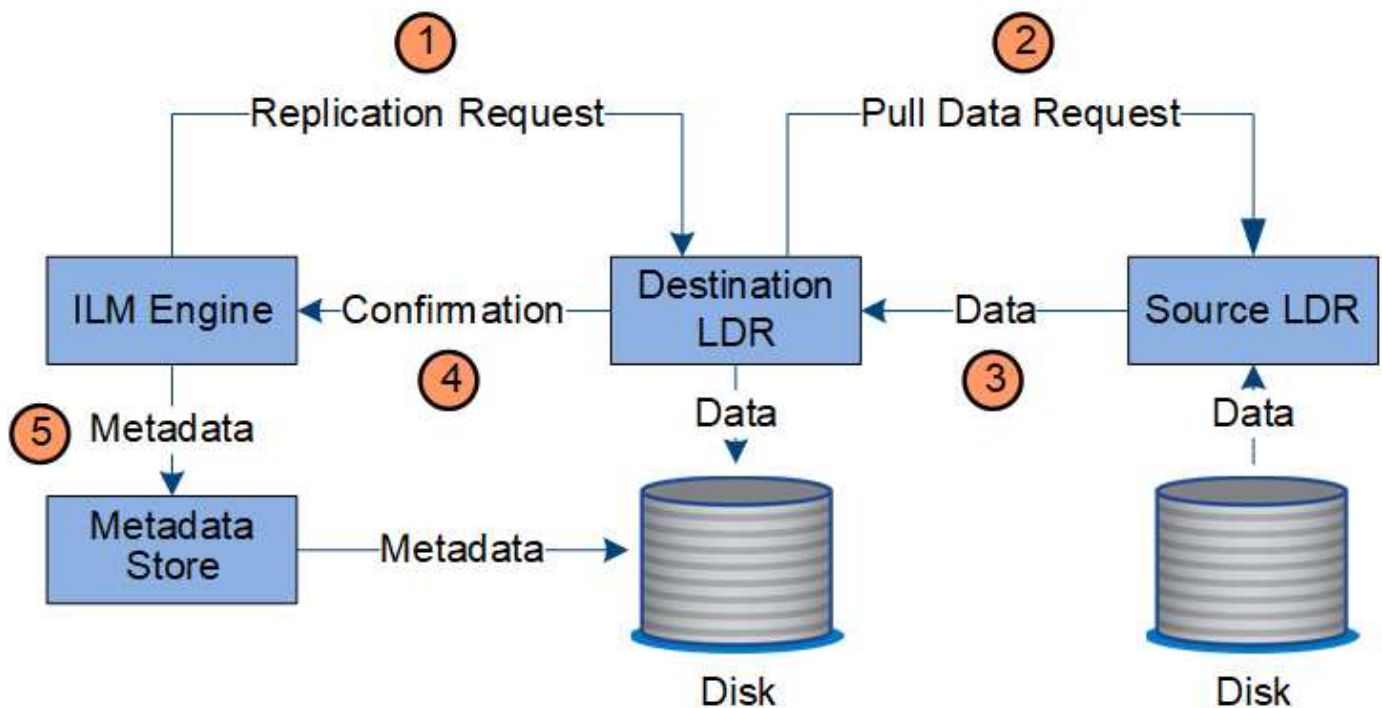
Potrebbero essere necessari diversi tipi o posizioni di copie di oggetti in momenti diversi della vita dell'oggetto. Le regole ILM vengono periodicamente valutate per garantire che gli oggetti vengano posizionati come richiesto.

I dati degli oggetti vengono gestiti dal servizio LDR.

Protezione del contenuto: Replica

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

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



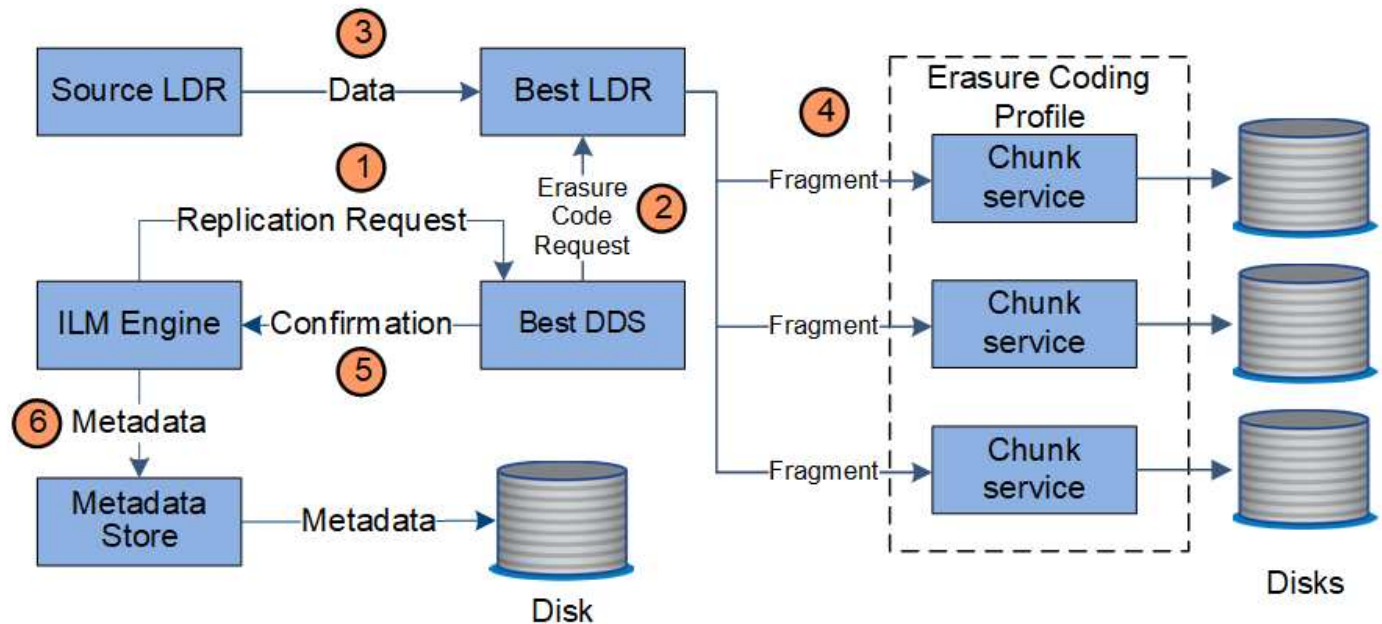
1. Il motore ILM interroga il servizio ADC per determinare il servizio LDR di destinazione migliore all'interno del pool di storage specificato dalla regola ILM. Quindi, invia al servizio LDR un comando per avviare la replica.
2. Il servizio LDR di destinazione interroga il servizio ADC per la migliore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

5. Il motore ILM aggiorna l'archivio di metadati con i metadati della posizione dell'oggetto.

Protezione del contenuto: Erasure coding

Se una regola ILM include istruzioni per creare copie codificate dei dati degli oggetti, lo schema di erasure coding applicabile suddivide i dati degli oggetti in fragment di dati e parità e distribuisce tali fragment nei nodi di storage configurati nel profilo di erasure coding.

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

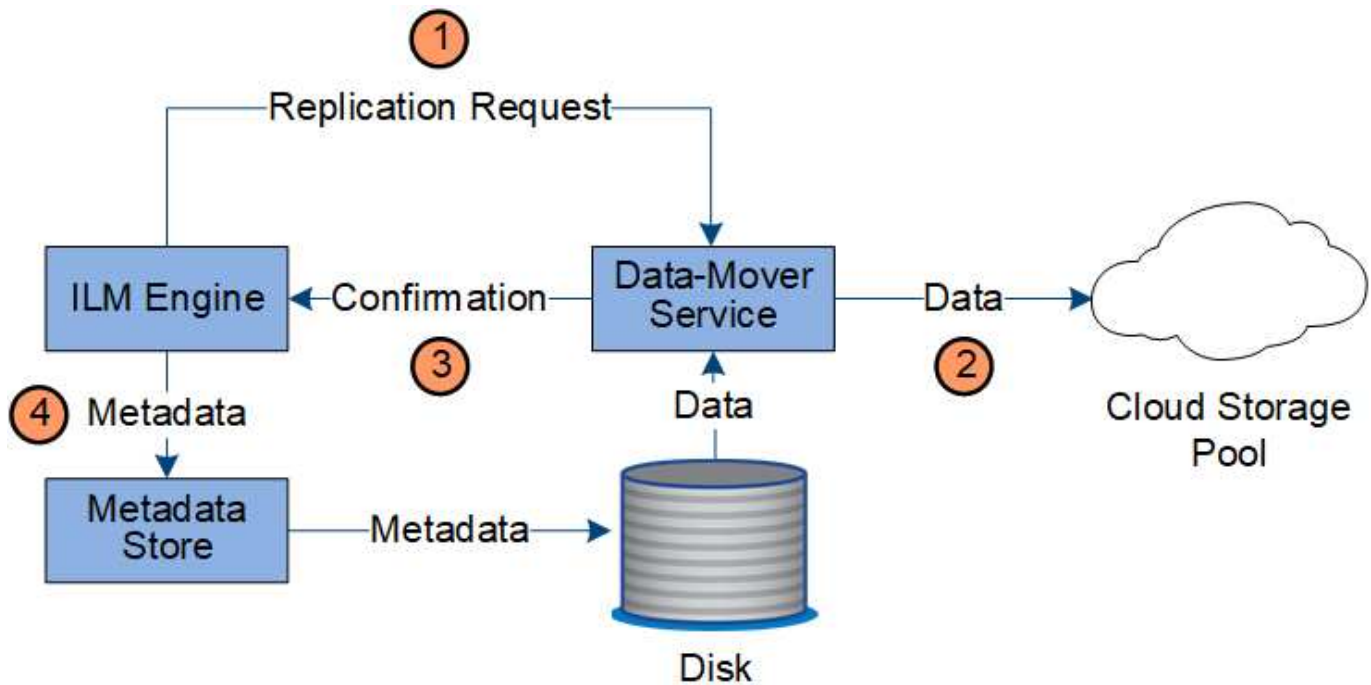


1. Il motore ILM interroga il servizio ADC per determinare quale servizio DDS può eseguire al meglio l'operazione di erasure coding. Una volta stabilito, il motore ILM invia una richiesta di "avvio" a tale servizio.
2. Il servizio DDS richiede a un LDR di eseguire la cancellazione del codice dei dati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

Protezione dei contenuti: Pool di storage cloud

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

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



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

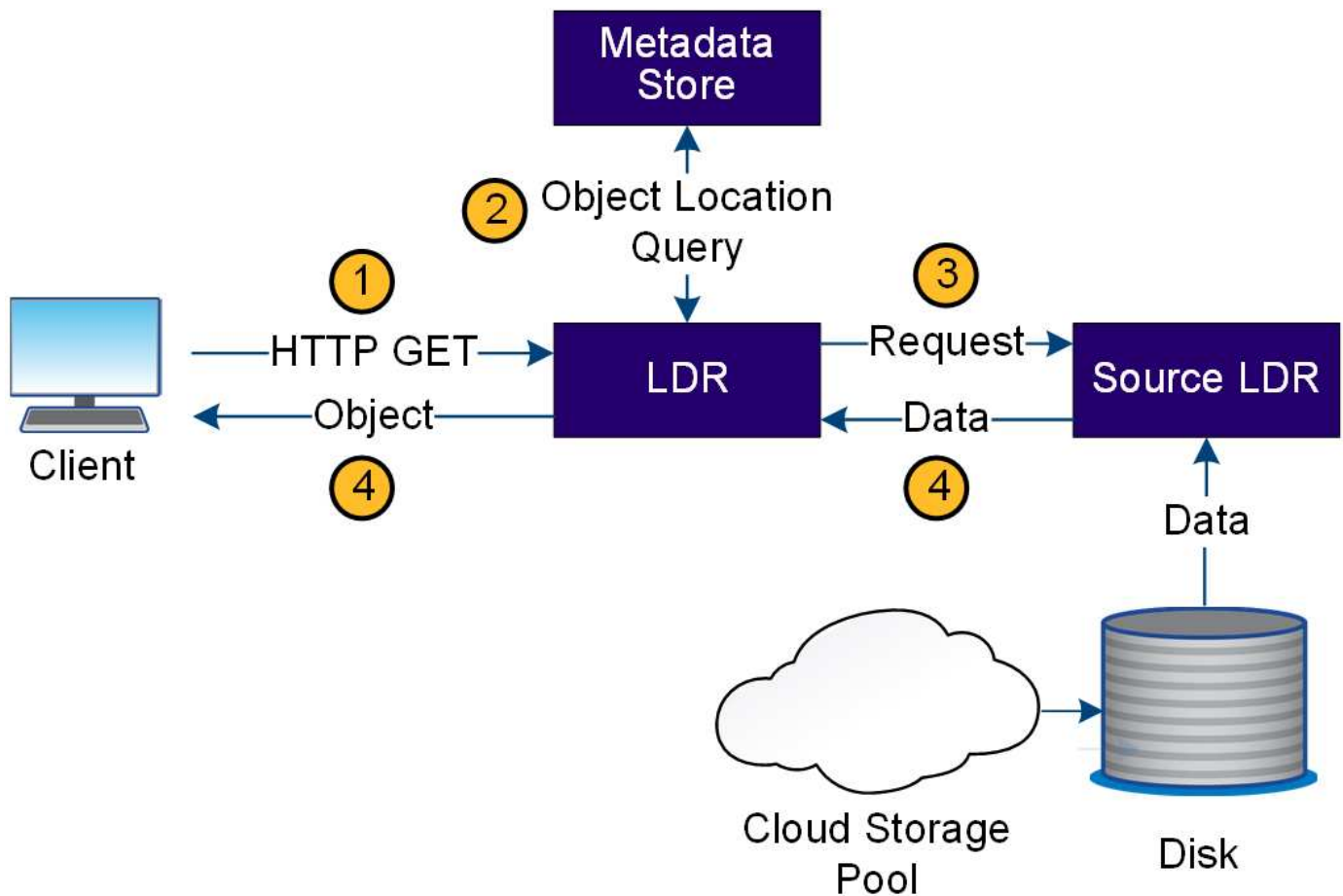
Come StorageGRID gestisce il recupero degli oggetti

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

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



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



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

Come StorageGRID gestisce l'eliminazione degli oggetti

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

Gerarchia di eliminazione

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

- **S3 Object Lock:** Se l'impostazione globale S3 Object Lock è attivata per la griglia, i client S3 possono creare bucket con S3 Object Lock abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data e conservazione legale per ogni versione di oggetto aggiunta a quel bucket.
 - Una versione dell'oggetto soggetta a blocco legale non può essere eliminata da alcun metodo.

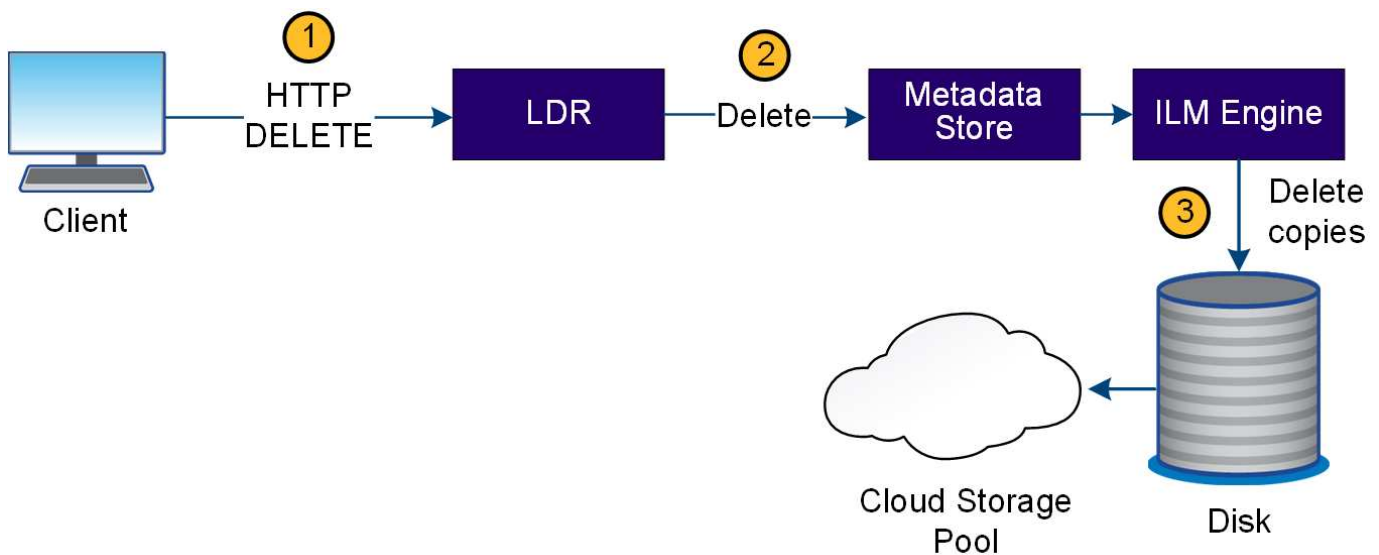
- Prima che venga raggiunta la data di conservazione di una versione a oggetti, tale versione non può essere eliminata da alcun metodo.
 - Gli oggetti nei bucket con blocco oggetti S3 abilitato vengono conservati da ILM "per sempre". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket.
 - Se i client S3 applicano al bucket una data di conservazione predefinita, non devono specificare una data di conservazione per ciascun oggetto.
- **Client delete request:** Un client S3 può emettere una richiesta di eliminazione degli oggetti. Quando un client elimina un oggetto, tutte le copie dell'oggetto vengono rimosse dal sistema StorageGRID.
 - **Elimina oggetti nel bucket:** Gli utenti di tenant Manager possono utilizzare questa opzione per rimuovere in modo permanente tutte le copie degli oggetti e delle versioni degli oggetti nei bucket selezionati dal sistema StorageGRID.
 - **Ciclo di vita del bucket S3:** I client S3 possono aggiungere una configurazione del ciclo di vita ai bucket che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID elimina automaticamente tutte le copie di un oggetto quando viene soddisfatta la data o il numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto.
 - **Istruzioni di posizionamento ILM:** Supponendo che il bucket non abbia attivato il blocco oggetti S3 e che non vi sia alcun ciclo di vita del bucket, StorageGRID elimina automaticamente un oggetto al termine dell'ultimo periodo di tempo della regola ILM e non vi sono ulteriori posizionamenti specificati per l'oggetto.



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

Per ulteriori informazioni, vedere ["Modalità di eliminazione degli oggetti"](#).

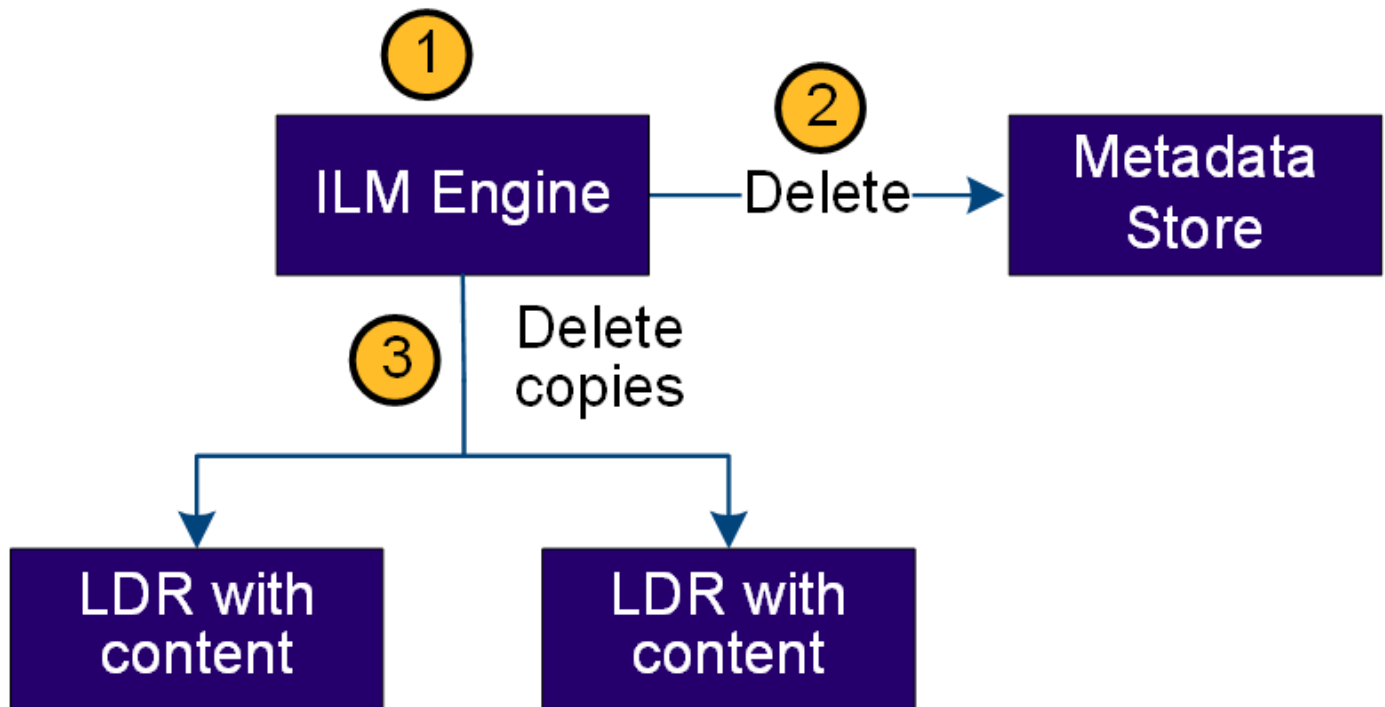
Eliminazione del flusso di dati per il client



1. Il servizio LDR riceve una richiesta di eliminazione dall'applicazione client.
2. Il servizio LDR aggiorna l'archivio di metadati in modo che l'oggetto venga cancellato dalle richieste del client e istruisce il motore ILM a rimuovere tutte le copie dei dati dell'oggetto.

3. L'oggetto viene rimosso dal sistema. L'archivio di metadati viene aggiornato per rimuovere i metadati degli oggetti.

Flusso di dati per l'eliminazione di ILM



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

Gestione del ciclo di vita delle informazioni in StorageGRID

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, bucket S3 specifici o valori di metadati specifici.
- Il tipo e la posizione di storage. Gli oggetti possono essere memorizzati sui nodi storage o nei pool di cloud storage.
- Il tipo di copie a oggetti eseguite. È possibile eseguire la replica o l'erasure coding.
- Per le copie replicate, il numero di copie eseguite.

- Per le copie con erasure coding, è stato utilizzato lo schema di erasure coding.
- Il cambia nel tempo nella posizione di storage di un oggetto e nel tipo di copie.
- Modalità di protezione dei dati degli oggetti durante l'acquisizione degli oggetti nella griglia (posizionamento sincrono o doppio commit).

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

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applicano solo agli oggetti appartenenti al tenant A.
- Eseguire due copie replicate di tali oggetti e memorizzare ciascuna copia in un sito diverso.
- Conserva le due copie "per sempre", il che significa che StorageGRID non le eliminerà automaticamente. Al contrario, StorageGRID conserverà questi oggetti fino a quando non saranno cancellati da una richiesta di eliminazione del client o dalla scadenza di un ciclo di vita del bucket.
- Utilizzare l'opzione bilanciato per il comportamento di acquisizione: L'istruzione di posizionamento a due siti viene applicata non appena il tenant A salva un oggetto in StorageGRID, a meno che non sia possibile eseguire immediatamente entrambe le copie richieste.

Ad esempio, se il sito 2 non è raggiungibile quando il tenant A salva un oggetto, StorageGRID eseguirà due copie intermedie sui nodi di storage nel sito 1. Non appena il sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta presso il sito.

Come un criterio ILM valuta gli oggetti

Le policy ILM attive del sistema StorageGRID controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti.

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

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

Esempio di policy ILM

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

- **Regola 1: Copie replicate per il tenant A**
 - Abbina tutti gli oggetti appartenenti al tenant A.

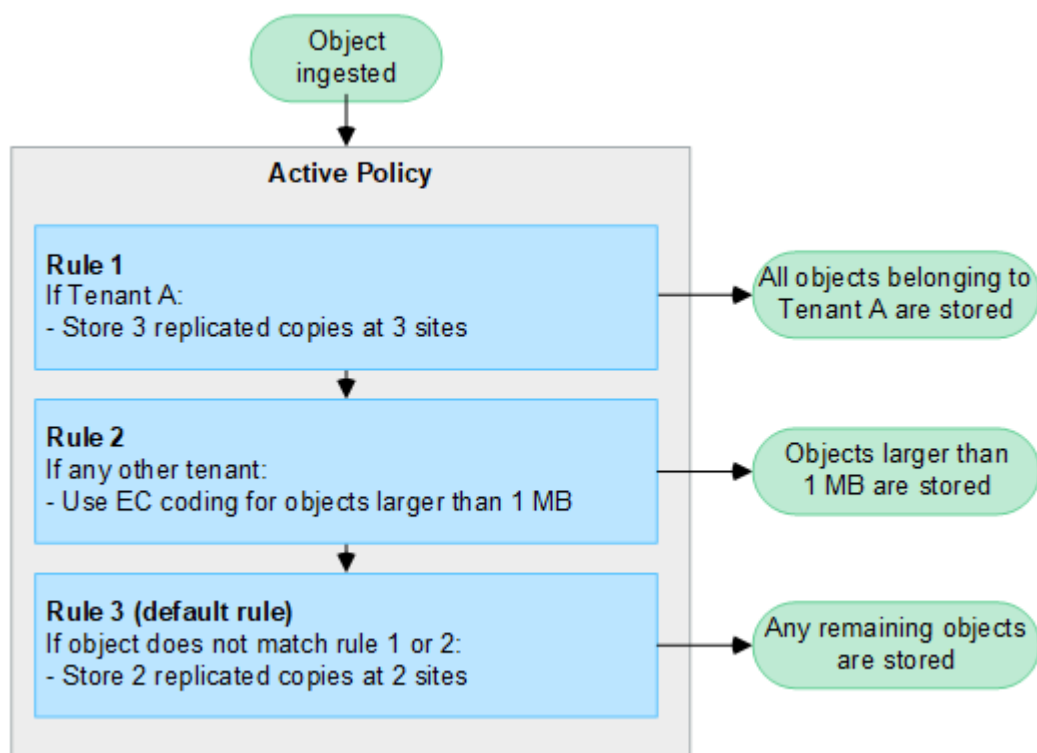
- Memorizzare questi oggetti come tre copie replicate in tre siti.
- Gli oggetti appartenenti ad altri tenant non corrispondono alla regola 1, quindi vengono valutati in base alla regola 2.

- **Regola 2: Erasure coding per oggetti superiori a 1 MB**

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

- **Regola 3: 2 copie 2 data center** (impostazione predefinita)

- È l'ultima regola predefinita del criterio. Non utilizza filtri.
- Creare due copie replicate di tutti gli oggetti non corrispondenti alla regola 1 o alla regola 2 (oggetti non appartenenti al tenant A di dimensioni pari o inferiori a 1 MB).



Informazioni correlate

- ["Gestire gli oggetti con ILM"](#)

Esplora StorageGRID

Esplora il StorageGRID Grid Manager

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



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

Quando si accede a Grid Manager, si sta effettuando la connessione a un nodo amministratore. Ogni sistema

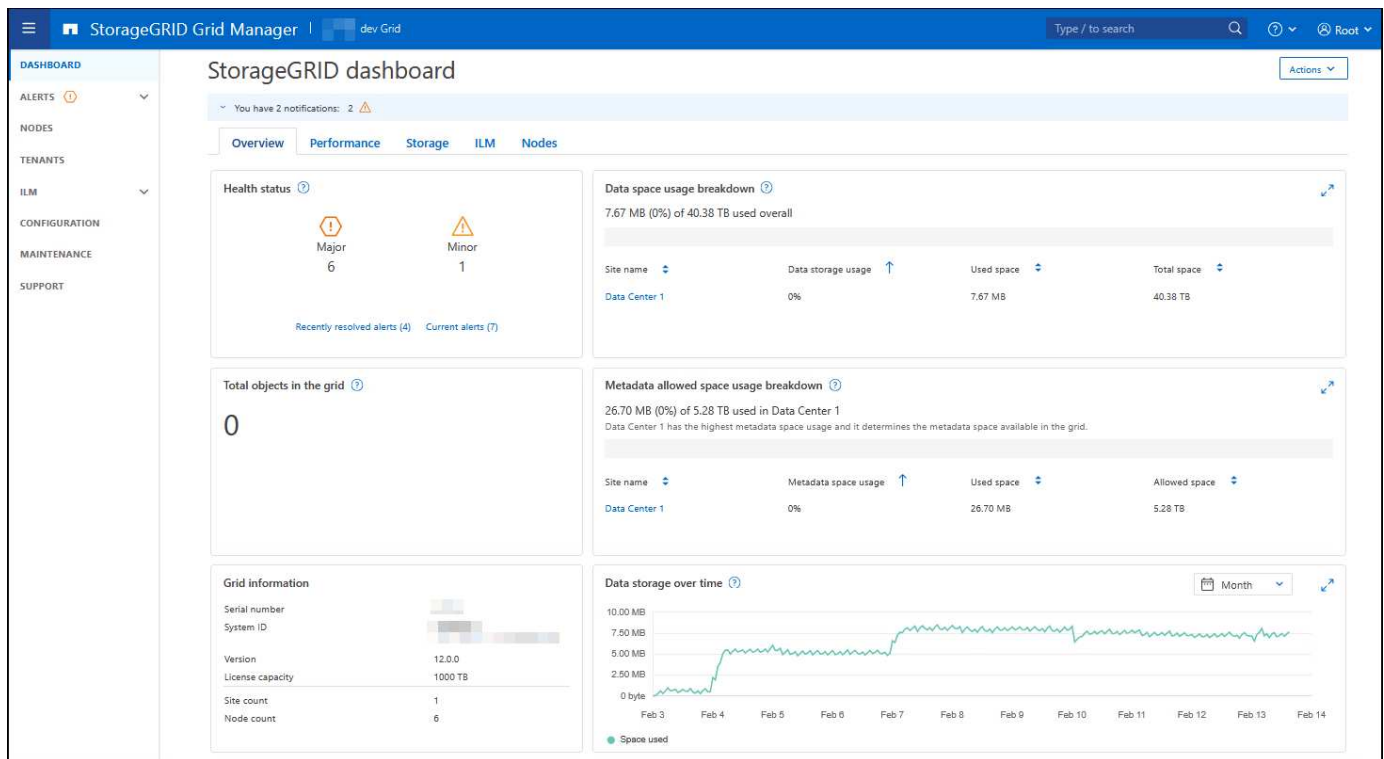
StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore visualizza una vista simile del sistema StorageGRID.

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

Dashboard di Grid Manager

Quando accedi per la prima volta al Grid Manager, puoi usare il dashboard per ["monitorare le attività del sistema"](#) dare un'occhiata.

La dashboard contiene informazioni su stato e performance del sistema, utilizzo dello storage, processi ILM, operazioni S3 e nodi nel grid. È possibile ["configurare il cruscotto"](#) selezionare da una raccolta di schede che contengono le informazioni necessarie per monitorare efficacemente il sistema.



Per una spiegazione delle informazioni visualizzate su ciascuna scheda, seleziona l'icona di aiuto (?) per quella scheda.

Campo di ricerca

Il campo **Search** nella barra di intestazione consente di accedere rapidamente a una pagina specifica all'interno di Grid Manager. Ad esempio, è possibile immettere **km** per accedere alla pagina del server di gestione delle chiavi (KMS).

È possibile utilizzare **Cerca** per trovare le voci nella barra laterale di Grid Manager e nei menu Configurazione, manutenzione e supporto. È inoltre possibile effettuare una ricerca per nome di elementi quali nodi griglia e account tenant.

Menu Guida

Il menu di aiuto (?) offre accesso a:

- IL ["FabricPool"](#) E ["Impostazione S3"](#) maghi
- Il sito della documentazione di StorageGRID per la versione corrente
- ["Documentazione API"](#)
- Informazioni sulla versione di StorageGRID attualmente installata

Menu Avvisi

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

Dal menu Avvisi, è possibile effettuare le seguenti operazioni ["gestire gli avvisi"](#):

- Rivedere gli avvisi correnti
- Esaminare gli avvisi risolti
- Configurare i silenzi per eliminare le notifiche di avviso
- Definire le regole di avviso per le condizioni che attivano gli avvisi
- Configura le notifiche e-mail per gli avvisi di StorageGRID

Pagina nodi

IL ["Pagina nodi"](#) visualizza informazioni sull'intera griglia, su ciascun sito nella griglia e su ciascun nodo in un sito. Per visualizzare le informazioni relative a un sito o a un nodo specifico, seleziona il sito o il nodo.

Pagina tenant

La ["Pagina tenant"](#) consente di ["creare e monitorare gli account tenant di storage"](#) utilizzare il sistema StorageGRID. È necessario creare almeno un account tenant per specificare chi può memorizzare e recuperare gli oggetti e quali funzionalità sono disponibili.

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

Menu ILM

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

Dal menu ILM è possibile visualizzare e gestire ILM:

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

Menu di configurazione

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

Attività di rete

Le attività di rete includono:

- ["Gestire i gruppi ad alta disponibilità"](#)
- ["Gestire gli endpoint del bilanciamento del carico"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)
- ["Gestire le policy di classificazione del traffico"](#)
- ["Configurare le interfacce VLAN"](#)
- ["Abilita StorageGRID CORS per un'interfaccia di gestione"](#)

Attività di sicurezza

Le attività di sicurezza includono:

- ["Gestire i certificati di sicurezza"](#)
- ["Gestire i controlli firewall interni"](#)
- ["Configurare i server di gestione delle chiavi"](#)
- Configurare le impostazioni di sicurezza, incluso il ["Policy TLS e SSH"](#), ["opzioni di protezione di rete e oggetti"](#), ["impostazioni di sicurezza dell'interfaccia"](#), E ["Opzioni di accesso SSH"](#)
- Configurare le impostazioni per un ["proxy di storage"](#) o un ["admin proxy \(proxy amministratore\)"](#)

Attività di sistema

Le attività di sistema includono:

- Usa ["federazione di grid"](#) per sincronizzare le informazioni dell'account del tenant e replicare i dati degli oggetti tra due sistemi StorageGRID
- Facoltativamente, abilitare l'opzione ["Compressione degli oggetti memorizzati"](#) opzione
- Facoltativamente, configurare il ["impostazione predefinita della coerenza del bucket"](#)
- ["Gestisci il blocco degli oggetti S3"](#)
- Comprendere le impostazioni di archiviazione come ["filigrane dei volumi di storage"](#)
- ["Gestire i profili di erasure coding"](#)

Attività di monitoraggio

Le attività di monitoraggio includono:

- ["Configura il server di posta elettronica"](#)
- ["Configurare la gestione dei log"](#)
- ["Utilizzare il monitoraggio SNMP"](#)

Attività di controllo degli accessi

Le attività di controllo degli accessi includono:

- ["Gestire i gruppi di amministratori"](#)
- ["Gestisci gli utenti amministratori"](#)
- [Cambia il "passphrase di provisioning" O "password della console dei nodi"](#)
- ["USA la federazione delle identità"](#)
- ["Configurare SSO"](#)
- ["Configura la verifica multi-amministratore"](#)

Menu di manutenzione

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

Attività

Le attività di manutenzione includono:

- ["Operazioni di decommissionamento"](#) per rimuovere i nodi e i siti della griglia inutilizzati
- ["Operazioni di espansione"](#) per aggiungere nuovi nodi e siti della griglia
- ["Procedure di ripristino del nodo Grid"](#) 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 degli oggetti"](#) per verificare l'esistenza (anche se non la correttezza) dei dati dell'oggetto
- Eseguire un ["riavvio in sequenza"](#) per riavviare più nodi della griglia
- Ripristino dei dati dell'oggetto
 - ["Ripristinare i dati dell'oggetto nel volume di storage per l'appliance"](#)
 - ["Ripristinare i dati degli oggetti nel volume di storage in cui il disco di sistema è intatto"](#)
 - ["Ripristinare i dati dell'oggetto nel volume di storage \(errore del disco di sistema\)"](#)

Sistema

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

- ["Visualizzare le informazioni sulla licenza StorageGRID" O "aggiornare le informazioni sulla licenza"](#)
- Generazione e download del ["pacchetto di recupero"](#)
- Esecuzione di aggiornamenti software StorageGRID, inclusi aggiornamenti software, hotfix e aggiornamenti del software SANtricity OS su alcune appliance
 - ["Procedura di aggiornamento"](#)
 - ["Procedura di hotfix"](#)
 - ["Aggiorna il sistema operativo SANtricity sugli storage controller SG6000 usando Grid Manager"](#)
 - ["Aggiorna il sistema operativo SANtricity sugli storage controller SG5700 usando Grid Manager"](#)

Rete

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

- ["Configurare i server DNS"](#)
- ["Aggiorna le subnet della rete Grid"](#)
- ["Gestire i server NTP"](#)

Menu Support (supporto)

Il menu Support (supporto) fornisce opzioni che consentono al supporto tecnico di analizzare e risolvere i problemi del sistema.

Strumenti

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

- ["Configurare AutoSupport"](#)
- ["Eseguire la diagnostica"](#) sullo stato corrente della griglia
- ["Raccogliere i file di log e i dati di sistema"](#)
- ["Rivedere le metriche di supporto"](#)



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

Altro

Dalla sezione Altro del menu supporto è possibile:

- Configurare ["Priorità I/O"](#)
- Gestione ["costo di collegamento"](#)
- Visualizza gli ID dei servizi dei nodi
- Gestione ["filigrane di archiviazione"](#)

Esplora il StorageGRID Tenant Manager

["Manager tenant"](#) È l'interfaccia grafica basata su browser a cui gli utenti del tenant accedono per configurare, gestire e monitorare i propri account di storage.



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

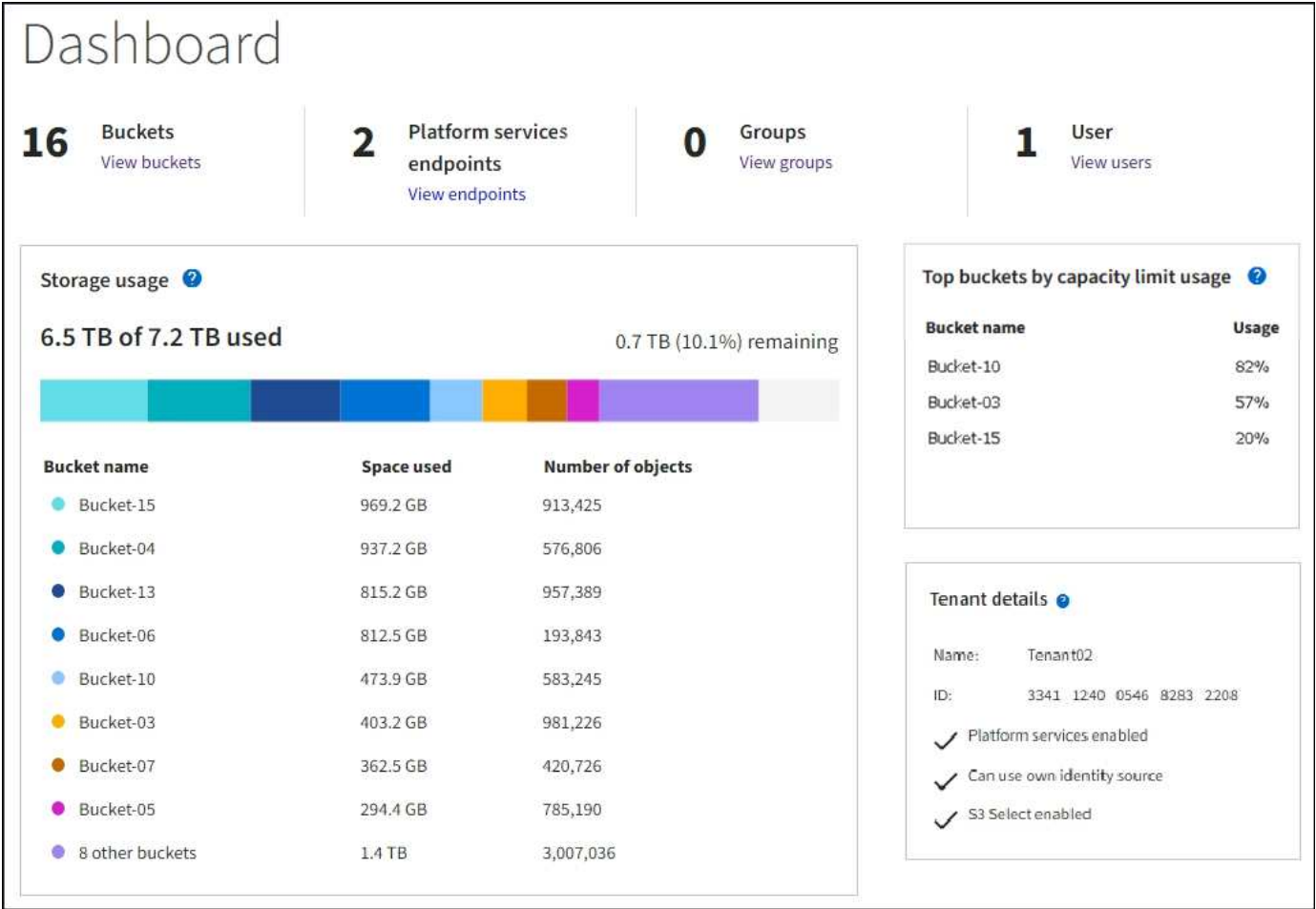
Quando gli utenti tenant accedono a Tenant Manager, si connettono a un nodo Admin.

Dashboard di tenant Manager

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

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



Menu Storage (S3)

Questo menu consente agli utenti S3 di:

- Gestisci le chiavi di accesso
- Crea, gestisci ed elimina i bucket
- Gestire gli endpoint dei servizi della piattaforma
- Visualizza tutte le connessioni di federazione della griglia che sono autorizzati a utilizzare

Chiavi di accesso personali

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

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

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



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

Bucket

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

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

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

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

Endpoint dei servizi di piattaforma

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

Connessioni a federazione di griglie

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

Accedere al menu Gestione

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

Linee guida per il networking

Linee guida di networking per StorageGRID

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

A proposito di queste istruzioni

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

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

- Memorizzare e recuperare i dati degli oggetti
- Ricevi notifiche via email
- Accedere all'interfaccia di gestione di StorageGRID (il gestore di griglia e il gestore dei tenant)
- Accesso alla condivisione dell'audit (opzionale)
- Fornire servizi come:
 - NTP (Network Time Protocol)
 - DNS (Domain Name System)
 - Server di gestione delle chiavi (KMS)

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

Prima di iniziare

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

Prima di configurare la rete, acquisire familiarità con l'architettura StorageGRID come descritto in ["Scopri di più su StorageGRID"](#).

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

Installare i nodi appliance

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

Installare nodi basati su software

- ["Installa StorageGRID sui nodi basati su software"](#)

Configurare e amministrare il software StorageGRID

- ["Amministrare StorageGRID"](#)
- ["Note di rilascio"](#). È necessario accedere con il proprio account NetApp o crearne uno per accedere alle note di rilascio.

Tipi di rete StorageGRID

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

Tipi di traffico

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

È possibile configurare la rete nei seguenti modi:

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

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

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

Interfacce di rete

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

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

Per i dettagli sulla mappatura delle porte virtuali o fisiche alle interfacce di rete dei nodi, vedere ["Installa StorageGRID sui nodi basati su software"](#).

Nodi appliance

- ["Appliance di storage SG6160"](#)
- ["Appliance di storage SGF6112"](#)
- ["Appliance di storage SG6000"](#)
- ["Appliance di storage SG5800"](#)
- ["Appliance di storage SG5700"](#)
- ["Appliance per i servizi SG110 e SG1100"](#)
- ["Appliance per i servizi SG100 e SG1000"](#)

Informazioni di rete per ciascun nodo

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

- Indirizzo IP
- Subnet mask
- Indirizzo IP del gateway

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

Gruppi ad alta disponibilità

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

Grid Network

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



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

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



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

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

- Il gateway Grid Network deve essere configurato se sono presenti più subnet Grid.
- Il gateway Grid Network è il gateway predefinito del nodo fino al completamento della configurazione della griglia.
- Le route statiche vengono generate automaticamente per tutti i nodi a tutte le subnet configurate nell'elenco globale delle subnet di rete Grid.
- Se viene aggiunta una rete client, il gateway predefinito passa dal gateway Grid Network al gateway Client Network una volta completata la configurazione della rete.

Admin Network (rete amministrativa)

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

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

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

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

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

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

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

Rete client

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

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

rete client non diventa operativa fino al completamento dell'installazione della griglia.

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

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

- Nodi di gateway, perché questi nodi forniscono l'accesso al servizio di bilanciamento del carico StorageGRID e all'accesso client S3 al grid.
- Nodi storage, perché questi nodi forniscono accesso al protocollo S3 e ai pool di cloud storage e al servizio di replica CloudMirror.
- Nodi amministrativi, per garantire che gli utenti tenant possano connettersi a Tenant Manager senza dover utilizzare la rete di amministrazione.

Tenere presente quanto segue per il gateway di rete client:

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

Reti VLAN opzionali

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

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

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

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



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

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

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

Esempi di topologia di rete

Topologia di rete Grid per StorageGRID

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

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

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

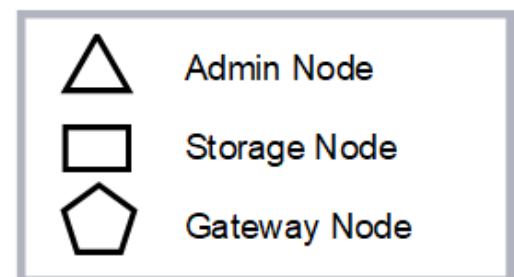
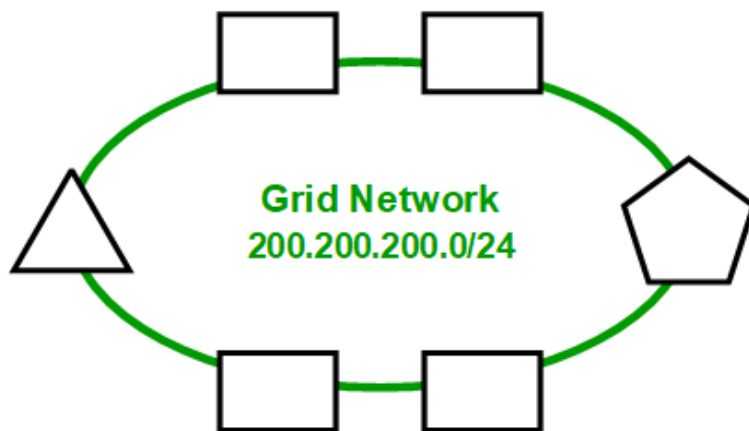
Al momento dell'installazione, l'interfaccia Grid Network applica route statiche per tutte le subnet in GNSL e imposta il percorso predefinito del nodo al gateway Grid Network, se configurato. GNSL non è richiesto se non esiste una rete client e il gateway Grid Network è il percorso predefinito del nodo.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

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



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

Topology example: Grid Network only



GNSL → 200.200.200.0/24

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

System Generated

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

Topologia di rete Admin per StorageGRID

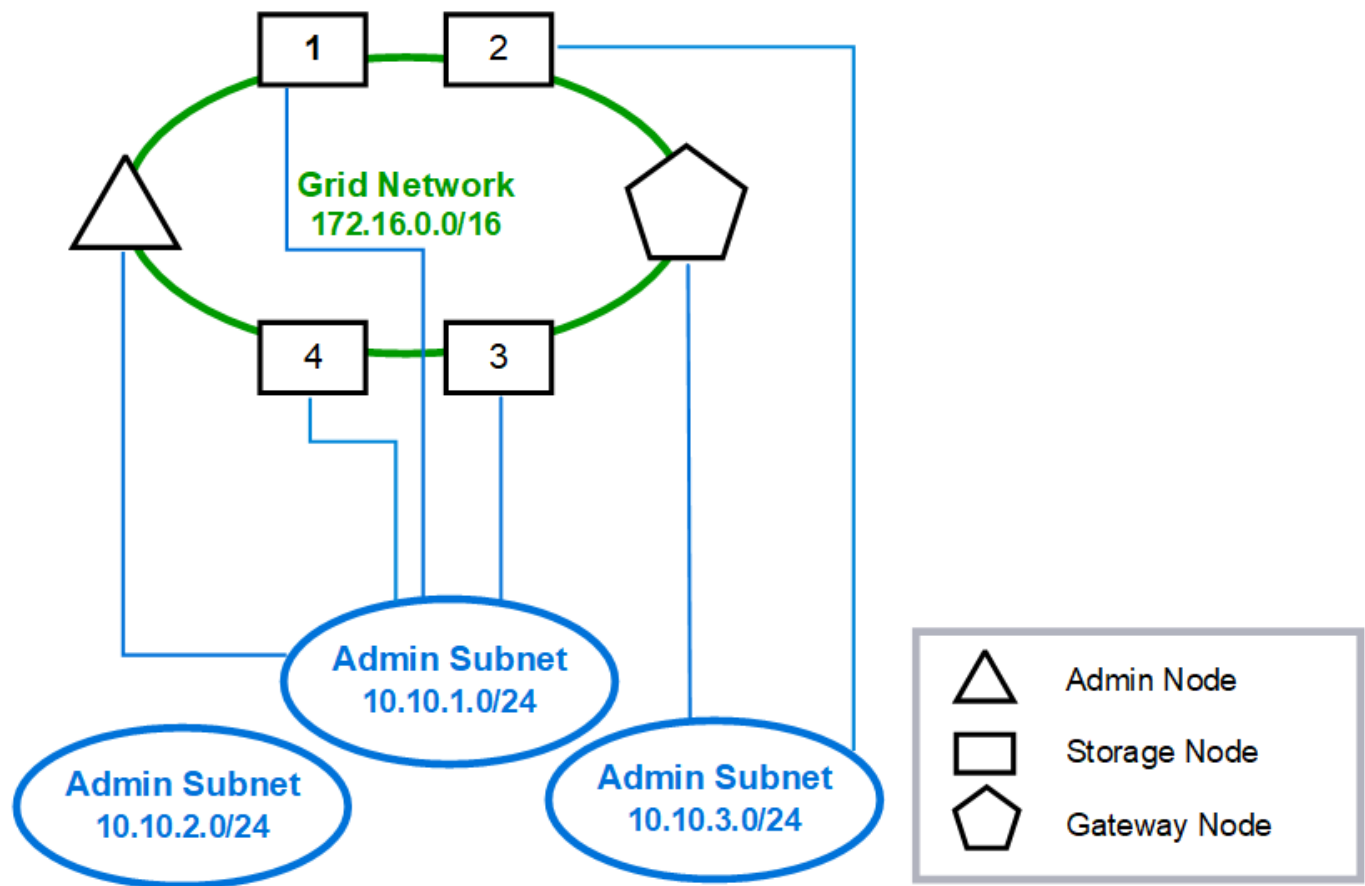
Disporre di una rete amministrativa è facoltativo. Un modo per utilizzare una rete amministrativa e una rete griglia consiste nel configurare una rete griglia instradabile e una rete amministrativa limitata per ciascun nodo.

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

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

In questo esempio, la rete Grid viene utilizzata per il traffico correlato alle richieste 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 di rete client per StorageGRID

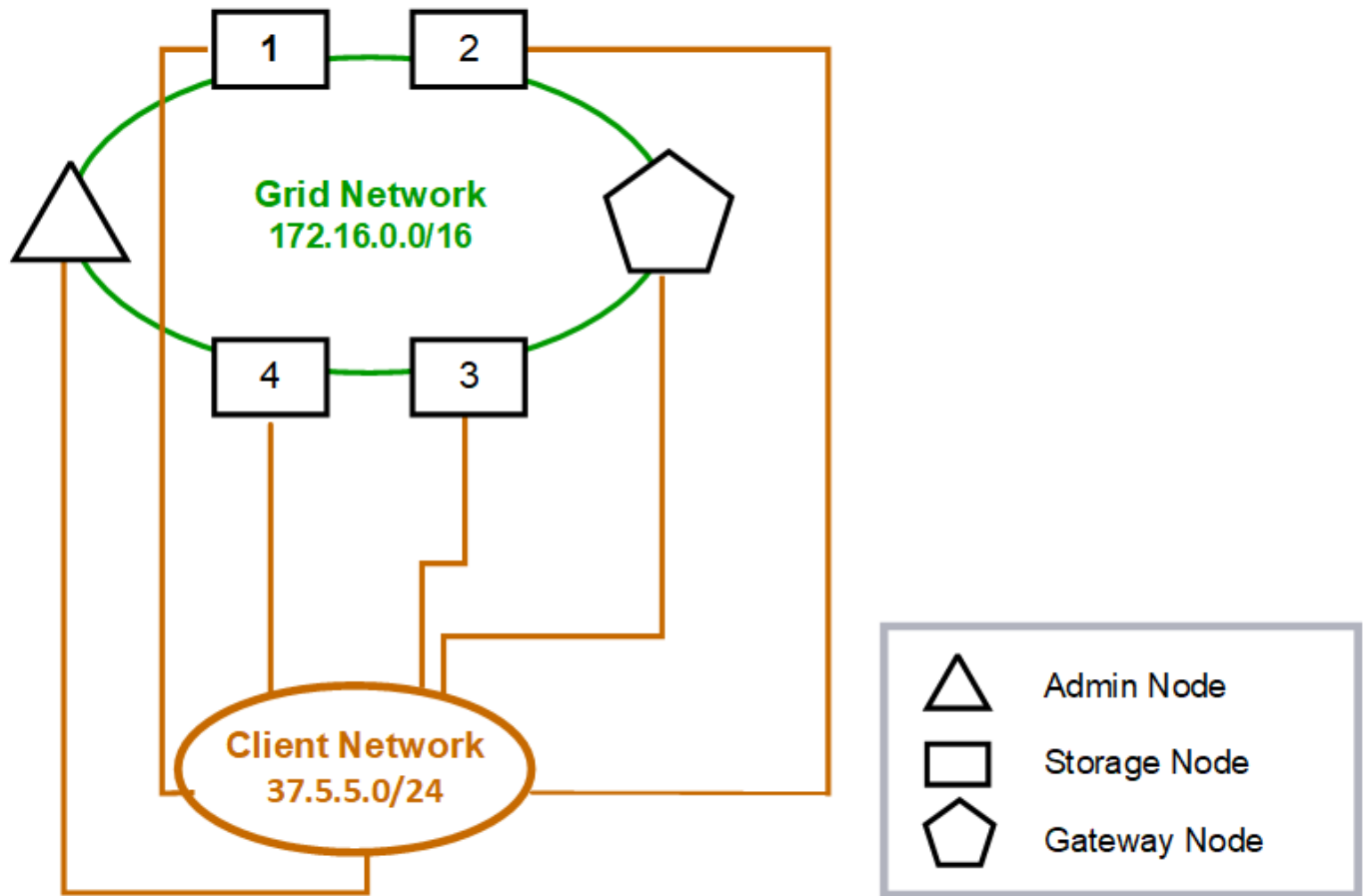
La disponibilità di una rete client è opzionale. L'utilizzo di una rete client consente di separare il traffico di rete client (ad esempio S3) dal traffico interno della rete, consentendo una rete più sicura. Il traffico amministrativo può essere gestito dal client o dalla rete griglia quando la rete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

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

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

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

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

["Modificare la configurazione di rete del nodo"](#)

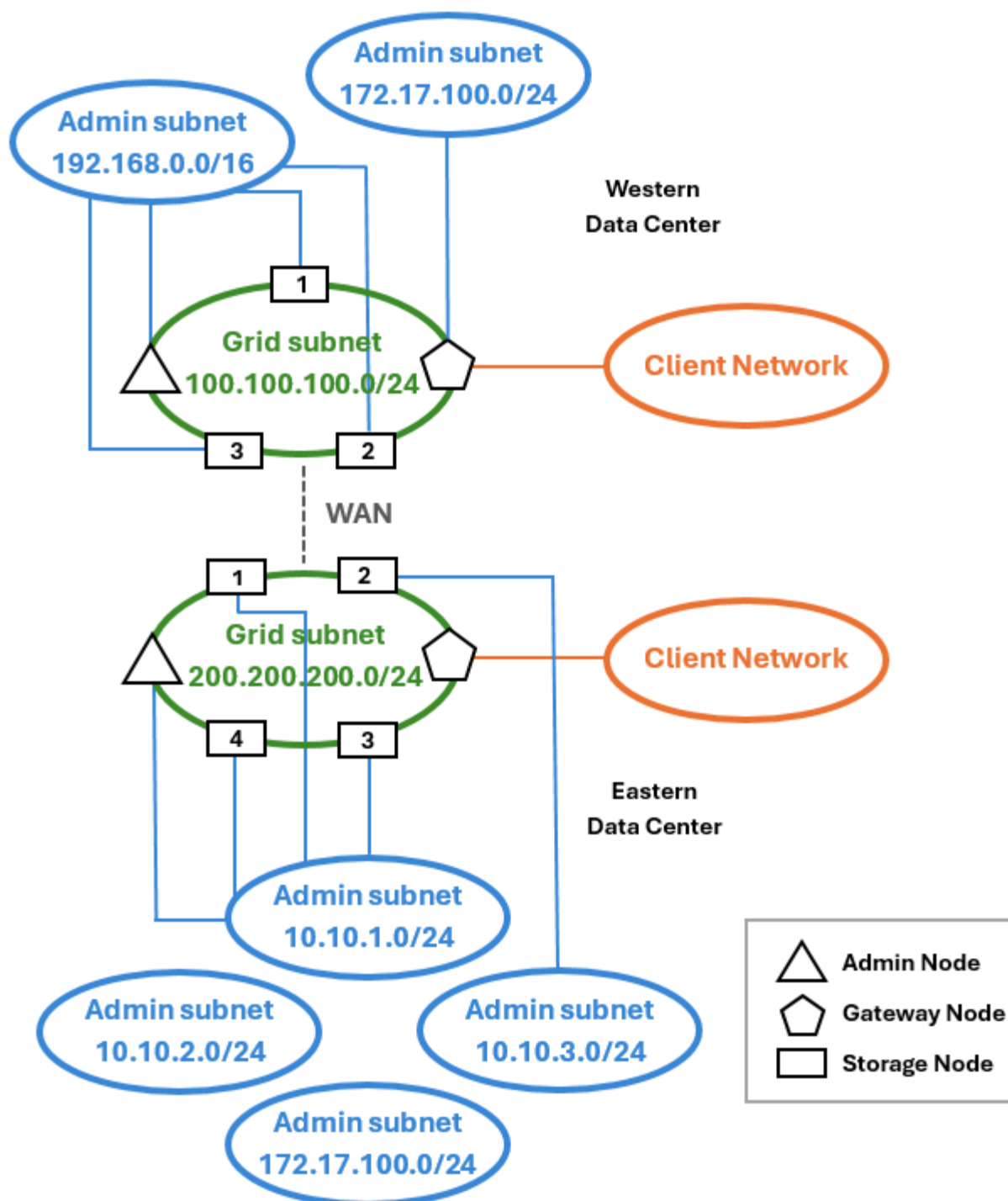
Topologia di rete per tutte e tre le reti StorageGRID

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

In questo esempio:

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

Esempio di topologia: Grid, Admin e Client Networks



Requisiti di rete per StorageGRID

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

Requisiti generali di rete

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

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

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

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

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



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

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

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

WAN (Wide Area Network) per più siti

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

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

Connessioni per nodi Admin e nodi Gateway

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

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

Utilizzo della NAT (Network Address Translation)

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

Requisiti specifici della rete per StorageGRID

Attenersi ai requisiti per ciascun tipo di rete StorageGRID.

Gateway e router di rete

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

Subnet



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

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

- La subnet mask per qualsiasi indirizzo IP di rete non può essere 255.255.255.254 o 255.255.255.255 (/31 o /32 nella notazione CIDR).
- La subnet definita da un indirizzo IP dell'interfaccia di rete e dalla subnet mask (CIDR) non può sovrapporsi alla subnet di qualsiasi altra interfaccia configurata sullo stesso nodo.
- Non utilizzare subnet che contengono i seguenti indirizzi IPv4 per la rete Grid, la rete di amministrazione o la rete client di alcun nodo:
 - 192.168.130.101
 - 192.168.130.121
 - 192.168.131.101
 - 192.168.131.121

- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4

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

- 192.168.130.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.130.101 e 192.168.130.102
- 192.168.131.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 192.168.131.101 e 192.168.131.102
- 198.51.100.0/24 perché questo intervallo di subnet contiene gli indirizzi IP 198.51.100.2 e 198.51.100.4
- La subnet Grid Network per ciascun nodo deve essere inclusa in GNSL.
- La subnet Admin Network non può sovrapporsi alla subnet Grid Network, alla subnet Client Network o a qualsiasi subnet in GNSL.
- Le subnet in AESL non possono sovrapporsi con le subnet in GNSL.
- La subnet della rete client non può sovrapporsi alla subnet della rete griglia, alla subnet della rete amministrativa, a qualsiasi subnet del GNSL o a qualsiasi subnet dell'AESL.

Grid Network

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



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

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

Admin Network (rete amministrativa)

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

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



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



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

Rete client

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

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

Informazioni correlate

["Modificare la configurazione di rete del nodo"](#)

Considerazioni di rete specifiche per l'implementazione

Configurazione di rete per le distribuzioni StorageGRID Linux

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

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



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

Vedi il ["Istruzioni di installazione"](#).

Configurazione della rete host per implementazioni di motori container

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

Host fisici

Se si utilizzano host fisici per supportare i nodi grid:

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



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

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Consigli sulla larghezza di banda minima

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

Tipo di nodo	Tipo di rete		
	Griglia	Amministratore	Client
	Larghezza di banda LAN minima	Amministratore	10 Gbps
1 Gbps	1 Gbps	Gateway	10 Gbps
1 Gbps	10 Gbps	Storage	10 Gbps
1 Gbps	10 Gbps	Archiviare	10 Gbps



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

Utilizzare la tabella per determinare il numero minimo di interfacce di rete da eseguire su ciascun host, in base

al numero e al tipo di nodi StorageGRID che si intende eseguire su tale host.

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

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

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

Per alcuni metodi consigliati per configurare le risorse fisiche e di rete sugli host nel cluster StorageGRID per preparare la distribuzione StorageGRID, vedere ["Configurare la rete host"](#).

Networking e porte per servizi di piattaforma e Cloud Storage Pool

Se si prevede di utilizzare i servizi della piattaforma StorageGRID o i pool di storage cloud, è necessario configurare il grid networking e i firewall per garantire che gli endpoint di destinazione possano essere raggiunti.

Networking per servizi di piattaforma

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

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

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

Networking per i Cloud Storage Pools

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

Porte per servizi di piattaforma e Cloud Storage Pools

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

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

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

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

VLAN, servizi di piattaforma e Cloud Storage Pool

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

Configurazione di rete per i nodi dell'appliance StorageGRID

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

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

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

Consultare le informazioni relative alle modalità di port bond dell'appliance:

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

Installazione e provisioning di rete per StorageGRID

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

Implementazione iniziale di un nodo

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

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

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

Registrazione automatica del nodo con nodo di amministrazione primario

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

Disattivazione della rete amministrativa o della rete client

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

Linee guida post-installazione per StorageGRID

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

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

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



I nodi si riavviano quando la configurazione della rete griglia viene modificata da DHCP, causando interruzioni nel caso in cui una modifica DHCP influisca su più nodi contemporaneamente.

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

Riferimento porta di rete

Comunicazioni interne dei nodi della griglia per StorageGRID

Il firewall interno di StorageGRID consente connessioni in entrata a porte specifiche della rete di rete. Le connessioni sono accettate anche sulle porte definite dagli endpoint del bilanciamento del carico.



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

Oltre a ICMP e alle porte elencate nella tabella, StorageGRID utilizza il protocollo di ridondanza del router virtuale (VRRP). VRRP è un protocollo Internet che utilizza il protocollo IP numero 112. StorageGRID utilizza VRRP solo in modalità unicast. VRRP è necessario 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 sui nodi basati su software"](#).



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a ["Rimuovere i rimaps delle porte sugli host bare metal"](#).

Linee guida per i nodi basati su VMware

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

Se i criteri di rete 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 le istruzioni per ["installazione di StorageGRID su VMware"](#).



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a ["Rimuovere i rimaps delle porte sugli host bare metal"](#).

Linee guida per i nodi appliance

Se i criteri di rete aziendali limitano l'accesso a una di queste porte, è possibile rimappare le porte utilizzando il programma di installazione dell'appliance StorageGRID. Vedere ["Opzionale: Consente di rimappare le porte di rete per l'appliance"](#).



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a ["Rimuovere le rimappature delle porte sugli apparecchi StorageGRID"](#).

Porte interne StorageGRID

Porta	TCP o UDP	Da	A.	Dettagli
22	TCP	Nodo amministratore primario	Tutti i nodi	Per le procedure di manutenzione, il nodo di amministrazione primario deve essere in grado di comunicare con tutti gli altri nodi utilizzando SSH sulla porta 22. Consentire il traffico SSH da altri nodi è facoltativo.
80	TCP	Appliance	Nodo Admin primario e nodo Admin non primario	Utilizzato dalle appliance StorageGRID per comunicare con il nodo di amministrazione principale per avviare l'installazione.

Porta	TCP o UDP	Da	A.	Dettagli
123	UDP	Tutti i nodi	Tutti i nodi	Servizio Network Time Protocol. Ogni nodo sincronizza il proprio tempo con ogni altro nodo utilizzando NTP.
443	TCP	Tutti i nodi	Nodo Admin primario e nodo Admin non 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 Admin primario e nodo Admin non primario	Traffico interno per l'installazione, l'espansione, il ripristino e altre procedure di manutenzione.
1139	TCP	Nodi di storage	Nodi di storage	Traffico interno tra nodi di storage.
1501	TCP	Tutti i nodi	Nodi di storage con ADC	Traffico interno di reporting, controllo e configurazione.
1502	TCP	Tutti i nodi	Nodi di storage	Traffico interno correlato a S3.
1504	TCP	Tutti i nodi	Nodi di amministrazione	Traffico interno di configurazione e reporting del servizio NMS.
1505	TCP	Tutti i nodi	Nodi di amministrazione	Traffico interno del servizio AMS.
1506	TCP	Tutti i nodi	Tutti i nodi	Traffico interno dello stato del server.
1507	TCP	Tutti i nodi	Nodi gateway	Traffico interno del bilanciamento del carico.
1508	TCP	Tutti i nodi	Nodo amministratore primario	Traffico interno della gestione della configurazione.
1511	TCP	Tutti i nodi	Nodi di storage	Traffico interno dei metadati.

Porta	TCP o UDP	Da	A.	Dettagli
5353	UDP	Tutti i nodi	Tutti i nodi	Fornisce il servizio DNS multicast (mDNS) utilizzato per le modifiche IP dell'intera griglia e per l'individuazione del nodo di amministrazione primario durante l'installazione, l'espansione e il ripristino. Nota: la configurazione di questa porta è facoltativa.
7001	TCP	Nodi di storage	Nodi di storage	Comunicazione cluster tra nodi Cassandra TLS.
7443	TCP	Tutti i nodi	Nodo Admin primario e nodo Admin non primario	Traffico interno per installazione, espansione, ripristino, altre procedure di manutenzione e segnalazione degli errori.
8011	TCP	Tutti i nodi	Nodo Admin primario e nodo Admin non primario	Traffico interno per l'installazione, l'espansione, il ripristino e altre procedure di manutenzione.
8443	TCP	Nodo amministratore primario	Nodi appliance	Traffico interno relativo alla procedura della modalità di manutenzione.
9042	TCP	Nodi di storage	Nodi di storage	Porta client Cassandra.
9999	TCP	Tutti i nodi	Tutti i nodi	Traffico interno per più servizi. Include procedure di manutenzione, metriche e aggiornamenti di rete.
10226	TCP	Nodi di storage	Nodo amministratore primario	Utilizzato dalle appliance StorageGRID per l'inoltro dei pacchetti AutoSupport da SANtricity System Manager di e-Series al nodo amministrativo primario.
10342	TCP	Tutti i nodi	Nodo Admin primario e nodo Admin non primario	Traffico interno per l'installazione, l'espansione, il ripristino e altre procedure di manutenzione.
18000	TCP	Tutti i nodi	Nodi di storage con ADC	Traffico interno del servizio account.
18001	TCP	Tutti i nodi	Nodi di storage con ADC	Traffico interno di Identity Federation.

Porta	TCP o UDP	Da	A.	Dettagli
18002	TCP	Tutti i nodi	Nodi di storage	Traffico API interno correlato ai protocolli a oggetti.
18003	TCP	Tutti i nodi	Nodi di storage con ADC	Traffico interno dei servizi della piattaforma.
18017	TCP	Nodi Admin/Storage	Nodi di storage	Traffico interno del servizio Data Mover per i pool di storage cloud.
18019	TCP	Tutti i nodi	Tutti i nodi	Traffico interno del servizio Chunk per la codifica di cancellazione e la replicazione
18082	TCP	Nodi Admin/Storage	Nodi di storage	Traffico interno correlato a S3.
18086	TCP	Tutti i nodi	Nodi di storage	Traffico interno relativo al servizio LDR.
18200	TCP	Nodi Admin/Storage	Nodi di storage	Statistiche aggiuntive sulle richieste dei client.
19000	TCP	Nodi Admin/Storage	Nodi di storage con ADC	Traffico interno del servizio Keystone.

Informazioni correlate

["Comunicazioni esterne"](#)

Comunicazioni esterne per StorageGRID

I client devono comunicare con i nodi grid per acquisire e recuperare contenuti. Le porte utilizzate dipendono dai protocolli di storage a oggetti scelti. Queste porte devono essere accessibili al client.

Accesso limitato alle porte

Se i criteri di rete aziendali limitano l'accesso a una delle porte, è possibile effettuare una delle seguenti operazioni:

- Utilizzare ["endpoint del bilanciamento del carico"](#) per consentire l'accesso alle porte definite dall'utente.
- Rimappare le porte durante la distribuzione dei nodi. Tuttavia, non è necessario rimappare gli endpoint del bilanciamento del carico. Consultare le informazioni relative alla rimappatura delle porte per il nodo StorageGRID:



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a ["Rimuovere le rimappature delle porte sugli apparecchi StorageGRID"](#) O ["Rimuovere i rimaps delle porte sugli host bare metal"](#).

- ["Chiavi di rimappatura delle porte per StorageGRID su Red Hat Enterprise Linux"](#)
- ["Rimappare le porte per StorageGRID su VMware"](#)
- ["Opzionale: Consente di rimappare le porte di rete per l'appliance"](#)

Porte utilizzate per le comunicazioni esterne

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



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

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
22	TCP	SSH	Laptop di assistenza	Tutti i nodi	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. Nota: questa porta è necessaria solo quando è necessario abilitare l'accesso SSH per determinate operazioni di manutenzione.
25	TCP	SMTP	Nodi di amministrazione	Server di posta elettronica	Utilizzato per avvisi e AutoSupport basato su e-mail. È possibile ignorare l'impostazione predefinita della porta 25 utilizzando la pagina Server di posta elettronica.
53	TCP/UDP	DNS	Tutti i nodi	Server DNS	Utilizzato per DNS.
67	UDP	DHCP	Tutti i nodi	Servizio DHCP	Utilizzato come opzione per supportare la configurazione di rete basata su DHCP. Il servizio dhclient non viene eseguito per le griglie configurate staticamente.
68	UDP	DHCP	Servizio DHCP	Tutti i nodi	Utilizzato come opzione per supportare la configurazione di rete basata su DHCP. Il servizio dhclient non viene eseguito per le griglie che utilizzano indirizzi IP statici.
80	TCP	HTTP	Browser	Nodi di amministrazione	La porta 80 reindirizza alla porta 443 per l'interfaccia utente del nodo di amministrazione.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
80	TCP	HTTP	Browser	Appliance	La porta 80 viene reindirizzata alla porta 8443 per il programma di installazione dell'appliance StorageGRID.
80	TCP	HTTP	Nodi di storage con ADC	AWS	Utilizzato per i messaggi dei servizi della piattaforma inviati ad AWS o ad altri servizi esterni che utilizzano HTTP. I tenant possono sovrascrivere l'impostazione predefinita della porta HTTP di 80 quando creano un endpoint.
80	TCP	HTTP	Nodi di storage	AWS	Le richieste dei Cloud Storage Pools vengono inviate alle destinazioni AWS che utilizzano HTTP. Gli amministratori della griglia possono ignorare l'impostazione predefinita della porta HTTP 80 quando configurano un Cloud Storage Pool.
123	UDP	NTP	Nodi NTP primari	NTP esterno	Servizio Network Time Protocol. I nodi selezionati come origini NTP primarie sincronizzano anche gli orari con le origini temporali NTP esterne.
161	TCP/UDP	SNMP	Client SNMP	Tutti i nodi	Utilizzato per il polling SNMP. Tutti i nodi forniscono informazioni di base, mentre i nodi amministrativi forniscono anche dati di avviso. Impostazione predefinita della porta UDP 161 quando configurata. Nota: questa porta è necessaria solo e viene aperta sul firewall del nodo solo se SNMP è configurato. Se si intende utilizzare SNMP, è possibile configurare porte alternative. Nota: per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il proprio rappresentante NetApp.
162	TCP/UDP	Notifiche SNMP	Tutti i nodi	Destinazioni di notifica	Per impostazione predefinita, le notifiche e i trap SNMP in uscita sono impostati sulla porta UDP 162. Nota: questa porta è necessaria solo se SNMP è attivato e le destinazioni di notifica sono configurate. Se si intende utilizzare SNMP, è possibile configurare porte alternative. Nota: per informazioni sull'utilizzo di SNMP con StorageGRID, contattare il proprio rappresentante NetApp.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
389	TCP/UDP	LDAP	Nodi di storage con ADC	Active Directory/LDAP	Utilizzato per la connessione a un server Active Directory o LDAP per Identity Federation.
443	TCP	HTTPS	Browser	Nodi di amministrazione	Utilizzato dai browser Web e dai client API di gestione per accedere a Grid Manager e Tenant Manager. 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 firewall" per configurare indirizzi IP privilegiati.
443	TCP	HTTPS	Nodi di amministrazione	Active Directory	Utilizzato dai nodi amministrativi che si connettono ad Active Directory se è attivato il Single Sign-on (SSO).
443	TCP	HTTPS	Nodi di storage con ADC	AWS	Utilizzato per i messaggi dei servizi della piattaforma inviati ad AWS o ad altri servizi esterni che utilizzano HTTPS. I tenant possono sovrascrivere l'impostazione predefinita della porta HTTP di 443 quando creano un endpoint.
443	TCP	HTTPS	Nodi di storage	AWS	Le richieste dei Cloud Storage Pools vengono inviate alle destinazioni AWS che utilizzano HTTPS. Gli amministratori della griglia possono ignorare l'impostazione predefinita della porta HTTPS 443 quando configurano un Cloud Storage Pool.
636	TCP/UDP	LDAP	Nodi di storage con ADC	Active Directory/LDAP	Utilizzato per la connessione a un server Active Directory o LDAP per Identity Federation.
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.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
5696	TCP	KMIP	Appliance	KM	Traffico esterno del protocollo KMIP (Key Management Interoperability Protocol) dalle appliance configurate per la crittografia del nodo al server di gestione delle chiavi (KMS), a meno che non sia specificata una porta diversa nella pagina di configurazione KMS del programma di installazione dell'appliance StorageGRID.
8443	TCP	HTTPS	Browser	Nodi di amministrazione	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 firewall" per configurare indirizzi IP privilegiati.
8443	TCP	HTTPS	Browser	Appliance	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	Laptop di assistenza	Appliance	Concede l'accesso alle appliance StorageGRID in modalità pre-configurazione per il supporto e la risoluzione dei problemi. Non è necessario che questa porta sia accessibile tra i nodi della griglia o durante le normali operazioni.
9091	TCP	HTTPS	Servizio Grafana esterno	Nodi di amministrazione	Utilizzato dai servizi esterni Grafana per un accesso sicuro al servizio StorageGRID Prometheus. Nota: questa porta è necessaria solo se è abilitato l'accesso Prometheus basato su certificato.

Porta	TCP o UDP	Protocollo	Da	A.	Dettagli
9092	TCP	Kafka	Nodi di storage con ADC	Cluster Kafka	Utilizzato per i messaggi di Platform Services inviati a un cluster Kafka. I tenant possono sovrascrivere l'impostazione predefinita della porta Kafka di 9092 quando creano un endpoint.
9443	TCP	HTTPS	Browser	Nodi di amministrazione	Opzionale. Utilizzato dai browser Web e dai client API di gestione per accedere a Tenant Manager. Può essere utilizzato per separare le comunicazioni tra Grid Manager e Tenant Manager.
18082	TCP	HTTPS	Client S3	Nodi di storage	Traffico client S3 direttamente verso i nodi di archiviazione (HTTPS).
18084	TCP	HTTP	Client S3	Nodi di storage	Traffico client S3 direttamente verso i nodi di archiviazione (HTTP).
23000-23999	TCP	HTTPS	Tutti i nodi della griglia di origine per la replica cross-grid	Nodi di amministrazione e nodi gateway nella griglia di destinazione per la replica cross-grid	Questo intervallo di porte è riservato alle connessioni a federazione di griglie. Entrambe le griglie di una determinata connessione utilizzano la stessa porta.

Avvio rapido per StorageGRID

Seguire questi passaggi per configurare e utilizzare qualsiasi sistema StorageGRID.

1

Apprendere, pianificare e raccogliere dati

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

- Quanti dati a oggetti prevedete di memorizzare inizialmente e nel tempo?
- Quanti siti sono necessari?
- Quanti e quali tipi di nodi sono necessari per ciascun sito?
- Quali reti StorageGRID utilizzerai?
- Chi utilizzerà la griglia per memorizzare gli oggetti? Quali applicazioni utilizzeranno?

- Hai requisiti di sicurezza o storage speciali?
- È necessario rispettare i requisiti legali o normativi?

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

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

2

Installazione dei nodi

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

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

Scopri come:

- ["Installare l'hardware dell'appliance"](#)
- ["Installa StorageGRID sui nodi basati su software"](#)

3

Accedere e controllare lo stato del sistema

Una volta completata l'installazione della griglia, è possibile 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:

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

4

Configurazione e gestione

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

Scopri come:

- ["Controllare l'accesso a StorageGRID"](#)
- ["Utilizzare l'installazione guidata S3"](#)

- ["Utilizzare l'installazione guidata di FabricPool"](#)
- ["Gestire la sicurezza"](#)
- ["Protezione avanzata del sistema"](#)

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) costituita da una o più regole ILM. Le regole ILM spiegano a StorageGRID come creare e distribuire copie di dati a oggetti e come gestirle nel tempo.

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

6

USA StorageGRID

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

Scopri come:

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

7

Monitoraggio e risoluzione dei problemi

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

Scopri come:

- ["Monitorare StorageGRID"](#)
- ["Risolvere i problemi relativi a StorageGRID"](#)

8

Espansione, manutenzione e ripristino

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

Scopri come:

- ["Espandere una griglia"](#)
- ["Mantenere la griglia"](#)
- ["Ripristinare i nodi"](#)

Installazione, aggiornamento e correzione rapida StorageGRID

Installare i nodi StorageGRID

Scopri l'hardware dell'appliance StorageGRID

Vai su ["Documentazione dell'appliance StorageGRID"](#) per scoprire come installare, configurare e gestire gli appliance di storage e i servizi StorageGRID.

Installare nodi basati su software

Avvio rapido per l'installazione di StorageGRID su un nodo basato su software

Per installare un nodo Linux o VMware StorageGRID , seguire questi passaggi generali.



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#) .

1

Preparazione

- Ulteriori informazioni su ["Architettura StorageGRID e topologia di rete"](#).
- Informazioni sulle specifiche di ["Networking StorageGRID"](#).
- Raccogliere e preparare il ["Informazioni e materiali richiesti"](#).
- (Solo VMware) Installa e configura ["Hypervisor di VMware vSphere, vCenter e host ESX"](#) .
- Preparare il necessario ["CPU e RAM"](#).
- Prevedere ["requisiti di storage e performance"](#).
- (Solo Linux) ["Preparare i server Linux"](#) che ospiterà i tuoi nodi StorageGRID .

2

Distribuzione

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

- (Solo Linux) 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 dei nodi"](#) .
- (Solo VMware) Utilizzare VMware vSphere Web Client, un file .vmdk e un set di modelli di file .ovf per ["Implementa i nodi basati su software come macchine virtuali \(VM\)"](#) sui server preparati nel passaggio 1.
- Per implementare i nodi di appliance StorageGRID, seguire la ["Avvio rapido per l'installazione dell'hardware"](#).

3

Configurazione

Una volta distribuiti tutti i nodi, utilizzare Grid Manager in ["configurare la griglia e completare l'installazione"](#).

Automatizzare l'installazione



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Linux

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

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

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

- Dopo aver distribuito i nodi 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 grid delle appliance"](#)
- Se si è uno sviluppatore avanzato di distribuzioni StorageGRID, automatizzare l'installazione dei nodi griglia utilizzando ["API REST di installazione"](#).

VMware

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

- ["Automatizza l'implementazione dei nodi con VMware vSphere"](#).
- Dopo aver implementato i nodi 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 grid delle appliance"](#)
- Se si è uno sviluppatore avanzato di distribuzioni StorageGRID, automatizzare l'installazione dei nodi griglia utilizzando ["API REST di installazione"](#).

Pianificare e preparare l'installazione su nodi basati su software

Informazioni e materiali necessari per StorageGRID

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

Informazioni richieste

Piano di rete

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

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

Informazioni di rete

Indirizzi IP da assegnare a ciascun nodo di rete e indirizzi IP dei server DNS e NTP.

Server per i nodi grid

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



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

Migrazione dei nodi (solo Ubuntu e Debian, se necessario)

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

Informazioni correlate

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

Materiali richiesti

Licenza NetApp StorageGRID

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



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

Archivio di installazione di StorageGRID

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

Laptop di assistenza

Il sistema StorageGRID viene installato tramite un laptop di assistenza.

Il laptop di assistenza deve disporre di:

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

Documentazione StorageGRID

- ["Note di rilascio"](#). È necessario accedere con il proprio account NetApp o crearne uno per accedere alle note di rilascio.
- ["Istruzioni per l'amministrazione di StorageGRID"](#)

Scaricare ed estrarre i file di installazione di StorageGRID

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

Fasi

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



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

5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
6. Nella colonna **Installa StorageGRID**, seleziona l'archivio di installazione .tgz o .zip per il tipo di nodo basato su software: RHEL, Ubuntu o Debian oppure VMware.



Utilizzare il .zip file se sul laptop di assistenza è in esecuzione Windows.

7. Salvare l'archivio di installazione.
8. La verifica della firma del codice è manuale su un nodo Linux. Facoltativamente, se è necessario verificare l'archivio di installazione:
 - a. Scaricare 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. Scegliere i file desiderati.

I file necessari dipendono dalla topologia della griglia pianificata e dalla modalità di distribuzione del sistema StorageGRID.



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

RHEL

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

Percorso e nome del file	Descrizione
	Uno script di supporto chiamato dallo script Python associato <code>storagegrid-ssoauth-azure.py</code> per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

Ubuntu o Debian

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	MD5 checksum 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.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.

Percorso e nome del file	Descrizione
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Uno script di supporto chiamato dallo script Python associato <code>storagegrid-ssoauth-azure.py</code> per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

VMware

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.

Percorso e nome del file	Descrizione
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file modello Open Virtualization Format (.ovf) e il file manifest (.mf) per la distribuzione del nodo amministrativo primario.
	Il file modello (.ovf) e il file manifesto (.mf) per la distribuzione di nodi Admin non primari.
	Il file modello (.ovf) e il file manifesto (.mf) per la distribuzione dei nodi Gateway.
	Il file modello (.ovf) e il file manifesto (.mf) per la distribuzione dei nodi di archiviazione basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
	Un file di configurazione di esempio da utilizzare con <code>deploy-vmware-ovftool.sh</code> lo script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando è attivato il Single Sign-on (SSO). È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.

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

Verificare i file di installazione di StorageGRID

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

Prima di iniziare

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

Fasi

1. Estrarre gli artefatti dal pacchetto di verifica:

```
tar -xf StorageGRID_12.1.0_Code_Signature_Verification_Package.tar.gz
```

2. Assicurarsi che questi artefatti siano stati estratti:

- Certificato Leaf: `Leaf-Cert.pem`
- Catena del certificato: `CA-Int-Cert.pem`
- Sequenza di risposta con indicazione temporale: `TS-Cert.pem`
- File checksum: `sha256sum`
- Firma checksum: `sha256sum.sig`
- File di risposta indicatore data e ora: `sha256sum.sig.tsr`

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

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

Uscita prevista: `Leaf-Cert.pem: OK`

4. Se il passaggio 2 non è riuscito a causa di un certificato foglia scaduto, utilizzare il `tsr` file per eseguire la verifica.

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

L'output previsto include: Verification: OK

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

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

Output previsto: *None*

6. Utilizzare la chiave pubblica per verificare il `sha256sum` file con `sha256sum.sig`.

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

Uscita prevista: Verified OK

7. Verificare il `sha256sum` contenuto del file in base ai checksum appena creati.

Esempio: `sha256sum -c sha256sum`

Output previsto: `<filename>: OK`

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

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

Requisiti software per StorageGRID

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

RHEL

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

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



Il supporto di Docker come motore container per implementazioni solo software è obsoleto. In una release futura, Docker sostituirà un altro motore per container.

Versioni Python testate

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

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

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1,5-2

Ubuntu e Debian

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

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

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



Il supporto di Docker come motore container per implementazioni solo software è obsoleto. In una release futura, Docker sostituirà un altro motore per container.

Versioni Python testate

- 3.5.2-2
- 3.6.8-2
- 3.6.8-38
- 3.6.9-1
- 3.7.3-1
- 3.8.10-0
- 3.9.2-1
- 3.9.10-2
- 3.9.16-1
- 3.10.6-1
- 3.11.2-6

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

- Docker-CE 20.10.7
- Docker-CE 20.10.20-3
- Docker-CE 23,0.6-1
- Docker-CE 24,0.2-1
- Docker-CE 24,0.4-1
- Docker-CE 24,0.5-1
- Docker-CE 24,0.7-1
- 1,5-2

VMware

VMware vSphere Hypervisor

È necessario installare VMware vSphere Hypervisor su un server fisico preparato. L'hardware deve essere configurato correttamente (incluse le versioni del firmware e le impostazioni del BIOS) prima di installare il software VMware.

- Configurare il collegamento in rete nell'hypervisor in base alle esigenze per supportare il collegamento in rete per il sistema StorageGRID che si sta installando.

["Linee guida per il networking"](#)

- Assicurarsi che l'archivio dati sia sufficientemente grande per le macchine virtuali e i dischi virtuali necessari per ospitare i nodi della griglia.
- Se si crea più di un datastore, assegnare un nome a ciascun datastore in modo da identificare facilmente quale datastore utilizzare per ciascun nodo della griglia quando si creano macchine virtuali.

Requisiti di configurazione dell'host ESX



È necessario configurare correttamente il protocollo NTP (Network Time Protocol) su ciascun host ESX. Se il tempo dell'host non è corretto, potrebbero verificarsi effetti negativi, inclusa la perdita di dati.

Requisiti di configurazione VMware

È necessario installare e configurare VMware vSphere e vCenter prima di implementare i nodi StorageGRID.

Per le versioni supportate di VMware vSphere Hypervisor e del software VMware vCenter Server, vedere ["Tool di matrice di interoperabilità NetApp"](#) .

Per informazioni sui passaggi necessari per l'installazione di questi prodotti VMware, consultare la documentazione VMware.

Requisiti di CPU e RAM per StorageGRID

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

Ogni nodo StorageGRID richiede le seguenti risorse minime:

- Core CPU: 8 per nodo
- RAM: A seconda della RAM totale disponibile e della 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
 - Se più tenant hanno ciascuno fino a 5.000 bucket, almeno 64 GB per nodo



Il sistema StorageGRID supporta un massimo di 20.000 bucket per ogni account tenant S3.

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

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#) .

Linux

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

VMware

VMware supporta un nodo per macchina virtuale. Assicurarsi che il nodo StorageGRID non superi la RAM fisica disponibile. Ciascuna macchina virtuale deve essere dedicata all'esecuzione di StorageGRID.



Monitora regolarmente l'utilizzo di CPU e memoria per assicurarti che queste risorse continuino a supportare il tuo carico di lavoro. Ad esempio, raddoppiare l'allocazione di RAM e CPU per i nodi di archiviazione virtuali fornirebbe risorse simili a quelle fornite per i nodi appliance StorageGRID. Inoltre, se la quantità di metadati per nodo supera 500 GB, valuta 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 di CPU e memoria, consulta le istruzioni per ["amministrazione"](#), ["monitoraggio"](#) e ["aggiornamento in corso"](#) StorageGRID.

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

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

(Solo RHEL, Debian e Ubuntu) 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.

Consulta ["Requisiti di storage e performance"](#).

Requisiti di storage e prestazioni per StorageGRID

Devi comprendere i requisiti di storage per i nodi StorageGRID per assicurarti di avere spazio sufficiente a supportare la configurazione iniziale e la futura espansione dello storage.

I requisiti di archiviazione e prestazioni variano in base all'implementazione del nodo basato su software.



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Categorie di archiviazione

I nodi StorageGRID richiedono tre categorie logiche di storage:

- **Pool di container** — Storage di livello prestazioni (10K SAS o SSD) per i container dei nodi, che viene assegnato al driver di storage del motore di container quando installi e configuri il motore di container sugli

host che supportano i tuoi nodi StorageGRID.

- **Dati di sistema** — Storage di livello prestazioni (SAS da 10K o SSD) per lo storage persistente per nodo dei dati di sistema e dei log delle transazioni, che i servizi host di StorageGRID consumano e mappano nei singoli nodi.
- **Dati oggetto** — storage di livello Performance (10.000 SAS o SSD) e storage bulk di livello capacità (NL-SAS/SATA) per lo storage persistente di dati oggetto e metadati oggetto.

Devi usare dispositivi a blocchi con supporto RAID per tutte le categorie di storage. Dischi non ridondanti, SSD o JBOD non sono supportati. Puoi usare storage RAID condiviso o locale per qualsiasi categoria di storage. Per migrare i nodi in StorageGRID, devi archiviare sia i dati di sistema che i dati degli oggetti su storage condiviso. Per ulteriori informazioni, vedi ["Requisiti per la migrazione dei container di nodi"](#).

Requisiti relativi alle performance

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

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

Requisiti degli host che utilizzano lo storage NetApp ONTAP

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



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

Numero di host richiesti

Ogni sito StorageGRID richiede almeno tre nodi di storage.



In un ambiente di produzione, non eseguire più di un Storage Node su un singolo host fisico o virtuale. Un host dedicato per ogni Storage Node fornisce un dominio di errore isolato.

Puoi distribuire altri tipi di nodi, come Admin Nodes o Gateway Nodes, sugli stessi host oppure su host dedicati, a seconda delle necessità.



Non puoi usare gli snapshot del disco per ripristinare i nodi della griglia. Invece, fai riferimento alle ["recovery del nodo grid"](#) procedure per ogni tipo di nodo.

Numero di volumi di archiviazione per ciascun nodo

La tabella seguente mostra il numero di volumi di storage (LUN) necessari per ciascun host e la dimensione minima richiesta per ciascun LUN, in base ai nodi distribuiti su tale host.

La dimensione massima del LUN testato è 100 TiB.



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

Scopo del LUN	Categoria di storage	Numero di LUN	Dimensione minima/LUN
Pool di storage del motore di container	Pool di container	1	Numero totale di nodi × 100 GB
/var/local volume	Dati di sistema	1 per ogni nodo su questo host	100 GB
Nodo di storage	Dati dell'oggetto	3 per ciascun nodo di storage su questo host Nota: Un nodo di storage basato su software Linux e un nodo di storage basato su software VMware possono avere da 1 a 48 volumi di storage. Sono consigliati almeno 3 volumi di storage.	12 TB (4 TB/LUN, minimo) Dimensione massima del LUN testato: 100 TiB. Consulta Requisiti di storage per i nodi di storage per maggiori informazioni.
Nodo di storage (solo metadati)	Metadati dell'oggetto	1	4 TB/LUN, minimo Dimensione massima del LUN testato: 100 TiB. Consulta Requisiti di storage per i nodi di storage per maggiori informazioni. Nota: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.
Registri di audit del nodo di amministrazione	Dati di sistema	1 per ogni nodo Admin su questo host	200 GB
Tabelle del nodo di amministrazione	Dati di sistema	1 per ogni nodo Admin su questo host	200 GB



A seconda del livello di audit configurato, delle dimensioni degli input utente come il nome della chiave dell'oggetto S3 e di quanta audit log data devi conservare, potresti dover aumentare le dimensioni del LUN del registro di audit su ciascun Admin Node. In genere, una grid genera circa 1 KB di dati di audit per ogni operazione S3, il che significa che un LUN da 200 GB supporterebbe 70 milioni di operazioni al giorno oppure 800 operazioni al secondo per due o tre giorni.

Spazio di storage minimo per un host

La tabella seguente mostra lo spazio di storage minimo richiesto per ogni tipo di nodo. Puoi usare questa tabella per determinare la quantità minima di storage che devi fornire all'host in ciascuna categoria di storage, in base ai nodi distribuiti su quell'host.



Non puoi usare gli snapshot del disco per ripristinare i nodi della griglia. Invece, fai riferimento alle ["recovery del nodo grid"](#) procedure per ogni tipo di nodo.

Ogni host nodo richiede una LUN da 100 GB per il sistema operativo.

Tipo di nodo	Pool di container	Dati di sistema	Dati dell'oggetto
Nodo di storage	100 GB	100 GB	4.000 GB
Nodo Admin	100 GB	500 GB (3 LUN)	<i>non applicabile</i>
Nodo gateway	100 GB	100 GB	<i>non applicabile</i>

Esempio: calcolo dei requisiti di archiviazione per un host o una macchina virtuale

Supponi di voler distribuire tre nodi sullo stesso host o macchina virtuale: un Storage Node, un Admin Node e un Gateway Node. Dovresti fornire all'host almeno nove volumi di storage. Ti servono almeno 300 GB di storage di livello prestazioni per i container dei nodi, 700 GB di storage di livello prestazioni per i dati di sistema e i log delle transazioni e 12 TB di storage di livello capacità per i dati a oggetti.

Esempio di host Linux

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensioni LUN
Nodo di storage	Pool di storage del motore di container	1	300 GB (100 GB/nodo)
Nodo di storage	/var/local volume	1	100 GB
Nodo di storage	Dati dell'oggetto	3	12 TB (4 TB/LUN)
Nodo Admin	/var/local volume	1	100 GB
Nodo Admin	Registri di audit del nodo di amministrazione	1	200 GB
Nodo Admin	Tabelle del nodo di amministrazione	1	200 GB
Nodo gateway	/var/local volume	1	100 GB
Totale		9	Pool di container: 300 GB Dati di sistema: 700 GB Dati oggetto: 12,000 GB

Esempio di macchina virtuale VMware

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensioni LUN
Nodo di storage	Volume del sistema operativo	1	100 GB
Nodo di storage	Dati dell'oggetto	3	12 TB (4 TB/LUN)
Nodo Admin	Volume del sistema operativo	1	100 GB
Nodo Admin	Registri di audit del nodo di amministrazione	1	200 GB
Nodo Admin	Tabelle del nodo di amministrazione	1	200 GB

Tipo di nodo	Scopo del LUN	Numero di LUN	Dimensioni LUN
Nodo gateway	Volume del sistema operativo	1	100 GB
Totale		8	Dati di sistema: 700 GB Dati oggetto: 12,000 GB

Requisiti di archiviazione specifici per i nodi di archiviazione

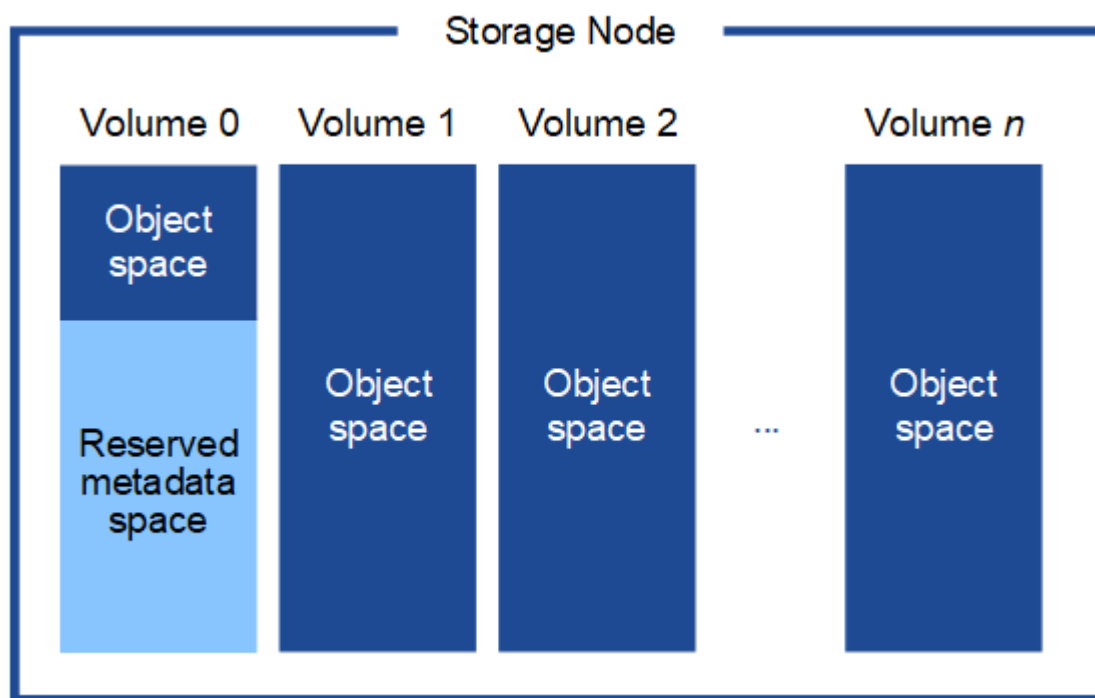
Linux e VMware hanno i seguenti requisiti di storage per i nodi di storage:

- Un nodo di storage basato su software Linux può avere da 1 a 48 volumi di storage.
- Un nodo di storage basato su software VMware può avere da 1 a 48 volumi di storage.
- Si consigliano tre o più volumi di stoccaggio.
- 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 storage 0 di ciascun nodo di storage. Qualsiasi spazio rimanente sul volume di storage 0 e qualsiasi altro volume di storage nel nodo di storage viene utilizzato esclusivamente per i dati a oggetti.



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

Quando installi una grid con Storage Node solo metadati, la grid deve anche contenere un numero minimo di nodi per lo storage a oggetti. Consulta ["Tipi di nodi storage"](#) per ulteriori informazioni sugli Storage Node solo metadati.

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

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

- È necessario assegnare almeno 4 TB al volume 0.



Se si utilizza un solo volume di 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 di archiviazione all'avvio e memorizzare solo i metadati dell'oggetto.



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

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

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

Per ulteriori informazioni, visitare il sito Web ["Gestire lo storage dei metadati degli oggetti"](#).

Requisiti di migrazione del container del nodo StorageGRID per Linux

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

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

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

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

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

Prima di eseguire la migrazione o la manutenzione dell'hypervisor, arrestare correttamente i nodi. Vedere le istruzioni per ["chiusura di un nodo di rete"](#).

VMware Live Migration non supportato

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

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

Nomi di interfaccia di rete coerenti

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

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

eth0 → bond0.1001

eth1 → bond0.1002

eth2 → bond0.1003

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

Supponiamo ora di voler migrare NodeA in Host2. Se l'host 2 ha anche interfacce denominate bond0.1001, bond0.1002 e bond0.1003, il sistema consentirà lo spostamento, supponendo che le interfacce con nome

simile forniscano la stessa connettività sull'host 2 di quella sull'host 1. Se l'host 2 non dispone di interfacce con gli stessi nomi, lo spostamento non sarà consentito.

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

Storage condiviso

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

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

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

Nell'esempio seguente viene illustrata una soluzione per la mappatura dei dispositivi di blocco per un nodo di storage StorageGRID, in cui il multipathing DM è in uso sugli host e il campo alias è stato utilizzato in `/etc/multipath.conf` per fornire nomi di dispositivi di blocco coerenti e facili 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 (Linux)

Come StorageGRID apporta modifiche alle impostazioni a livello di host

Sui sistemi bare metal, StorageGRID apporta alcune modifiche alle impostazioni a livello di host `sysctl`.



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere "[Tool di matrice di interoperabilità NetApp \(IMT\)](#)".

Vengono apportate le seguenti modifiche:

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

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

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

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

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

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

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

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

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

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

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

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

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

Installa StorageGRID su host grid Linux

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

Prima di iniziare

Verificare che il sistema operativo soddisfi i requisiti minimi di versione del kernel di StorageGRID, come indicato di seguito. Utilizzare il comando `uname -r` per ottenere la versione del kernel del sistema operativo o consultare il fornitore del sistema operativo.



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

RHEL

Versione RHEL	Versione minima del kernel	Nome del pacchetto 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
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

Ubuntu

Nota: il supporto per Ubuntu versione 18,04 e 20,04 è stato obsoleto e verrà rimosso in una versione futura.

Versione Ubuntu	Versione minima del kernel	Nome del pacchetto kernel
22.04.1	5.15.0-47-generic	linux-image-5.15.0-47-generic/jammy-updates,jammy-security,now 5.15.0-47,51
24,04	6,8.0-31-generic	linux-image-6,8.0-31-generic/noble,now 6,8.0-31,31

Debian

Nota: il supporto per Debian versione 11 è stato deprecato e sarà rimosso in una versione futura.

Versione Debian	Versione minima del kernel	Nome del pacchetto 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,now 6,1.27-1

Fasi

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



Non installare alcun ambiente desktop grafico.

- Se si utilizza il programma di installazione Linux standard durante l'installazione di RHEL, selezionare la configurazione software "compute node", se disponibile, oppure l'ambiente di base "minimal install".
 - 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, incluso il canale Extras per RHEL.
 3. Se lo swap è attivato:
 - a. Eseguire il seguente comando: `$ sudo swapoff --all`
 - b. Rimuovere tutte le voci di swap da `/etc/fstab` per mantenere le impostazioni.



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

Scopri i profili AppArmor per StorageGRID su Ubuntu e Debian

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

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

Esistono due opzioni per la gestione dei profili AppArmor:

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

Utilizzare i seguenti comandi:

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

Esempio:

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

- Disabilita AppArmor completamente. Per Ubuntu 9.10 o versioni successive, segui le istruzioni in ["Comunità online di Ubuntu"](#). Disabilitare completamente AppArmor potrebbe non essere possibile nelle versioni più recenti di Ubuntu.

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

indichi che AppArmor è attivato.

Configura la rete host StorageGRID per le distribuzioni Linux

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Prima di iniziare

- Hai esaminato le informazioni in ["Linee guida per il networking"](#).
- Sono state esaminate le informazioni su ["requisiti per la migrazione dei container di nodi"](#).
- Se si utilizzano host virtuali, è necessario leggere [Considerazioni e consigli per la clonazione degli indirizzi MAC](#) prima di configurare la rete host.



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

A proposito di questa attività

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

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

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

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



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

Considerazioni e consigli per la clonazione degli indirizzi MAC

La clonazione dell'indirizzo MAC fa sì che il container utilizzi l'indirizzo MAC dell'host e che l'host utilizzi l'indirizzo MAC di un indirizzo che specifichi tu o di uno generato casualmente.

Abilitazione della clonazione MAC

In determinati ambienti, la sicurezza può essere migliorata tramite la clonazione dell'indirizzo MAC perché ti permette di usare una scheda di rete virtuale dedicata per l'Admin Network, la Grid Network e la Client Network.



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



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

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

Per ogni rete è disponibile una chiave:

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

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

Casi di utilizzo della clonazione MAC

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

- Clonazione MAC non abilitata: quando la `_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 container avrà un MAC generato da StorageGRID, a meno che non venga specificato un MAC nella `_NETWORK_MAC` chiave. Se un indirizzo è impostato nella `_NETWORK_MAC` chiave, il container avrà l'indirizzo specificato nella

`\_NETWORK\_MAC` chiave.

- Clonazione MAC abilitata: quando la `_CLONE_MAC` chiave nel file di configurazione del nodo è impostata su "true", il container utilizza il MAC della NIC dell'host e l'host utilizza un MAC generato da StorageGRID, a meno che non sia specificato un MAC nella `_NETWORK_MAC` chiave. Se un indirizzo è impostato nella `_NETWORK_MAC` chiave, l'host utilizza l'indirizzo specificato invece di uno generato.



Se non vuoi usare la clonazione degli indirizzi MAC e preferisci permettere a tutte le interfacce di ricevere e trasmettere dati per indirizzi MAC diversi da quelli assegnati dall'hypervisor, assicurati che le proprietà di sicurezza a livello di switch virtuale e di port group siano impostate su **Accetta** per le modifiche degli indirizzi MAC e le trasmissioni falsificate. I valori impostati sullo switch virtuale possono essere sovrascritti dai valori a livello di port group, quindi assicurati che le impostazioni siano le stesse in entrambi i punti.

Per attivare la clonazione MAC, consultare la ["istruzioni per la creazione dei file di configurazione del nodo"](#).

Esempio di clonazione MAC

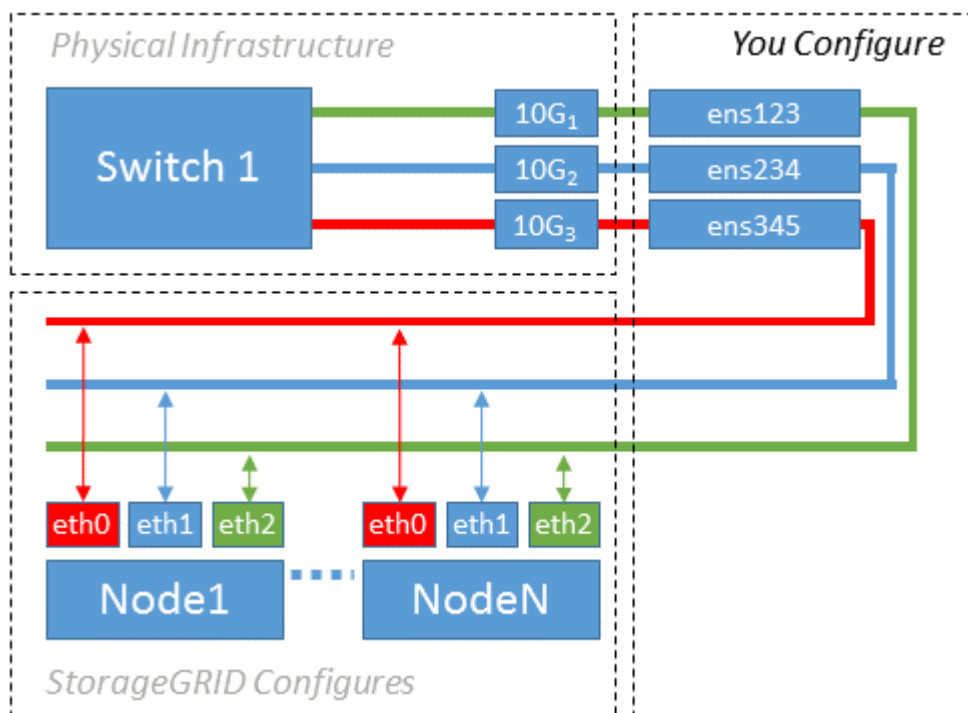
Esempio di clonazione MAC abilitata con un host con indirizzo MAC 11:22:33:44:55:66 per l'interfaccia ens256 e le seguenti chiavi nel file di configurazione del nodo:

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

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

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

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



Il sistema operativo Linux crea 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. 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 macchine virtuali a nodo singolo.

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

Esempio 2: Collegamento LACP con VLAN

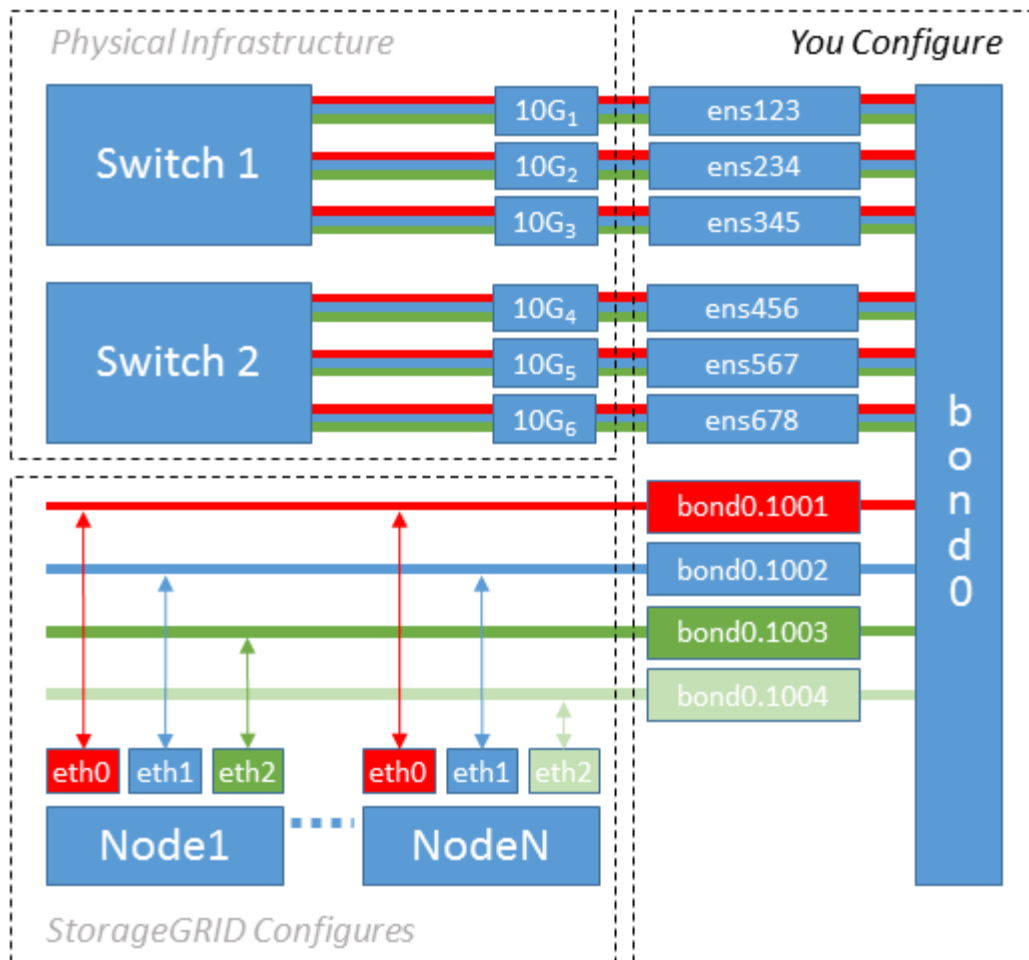
L'esempio 2 presuppone che si abbia familiarità con il bonding delle interfacce di rete e con la creazione di interfacce VLAN sulla distribuzione Linux in uso.

A proposito di questa attività

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

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

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



Fasi

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

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

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

I passi 1 e 2 richiedono una configurazione appropriata sugli edge switch che terminano le altre estremità dei collegamenti di rete. Le porte degli edge switch devono anche essere aggregate in un canale di porta LACP, configurate come trunk e in grado di passare tutte le VLAN richieste.

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

Informazioni correlate

- ["Esempio /etc/network/interfaces per Ubuntu e Debian"](#)
- ["Esempio /etc/sysconfig/network-scripts per RHEL"](#)

Configurare l'archiviazione host StorageGRID per le distribuzioni Linux

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

Prima di iniziare

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

- ["Requisiti di storage e performance"](#)
- ["Requisiti per la migrazione dei container di nodi"](#)



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

A proposito di questa attività

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

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

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



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



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

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

Ad esempio:

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

I risultati saranno diversi per ogni installazione.

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

Ad 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 di blocco nella `/dev/mapper` directory dell'host, consentendo di specificare un nome facile e facilmente validato ogni volta che un'operazione di configurazione o manutenzione richiede di specificare un volume di archiviazione del blocco.

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



Il supporto di Docker come motore container per implementazioni solo software è obsoleto. In una release futura, Docker sostituirà un altro motore per container.

Informazioni correlate

- ["Configurare il volume di storage del motore dei container"](#)
- ["Requisiti di storage e performance"](#)
- ["Requisiti per la migrazione dei container di nodi"](#)

Configura il volume di archiviazione del motore del container per StorageGRID su Linux

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



Il supporto di Docker come motore container per implementazioni solo software è obsoleto. In una release futura, Docker sostituirà un altro motore per container.



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

A proposito di questa attività

È possibile saltare questi passaggi se si prevede di utilizzare il volume root per il volume di archiviazione Docker o Podman e si dispone di spazio sufficiente sulla partizione host contenente:

- Podman: `/var/lib/containers`
- Docker: `/var/lib/docker`

Fasi

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

RHEL

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

Ubuntu o Debian

```
sudo mkfs.ext4 docker-storage-volume-device
```

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

RHEL

- 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
```

Ubuntu o Debian

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

- Per Podman:

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

3. Aggiungere una voce per il dispositivo del volume di archiviazione del contenitore a /etc/fstab.

- RHEL: dispositivo di archiviazione del volume del contenitore
- Ubuntu o Debian: docker-storage-volume-device

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

Installare Docker

Il sistema StorageGRID può essere eseguito su Linux come una raccolta di contenitori.

- Prima di poter installare StorageGRID per Ubuntu o Debian, è necessario installare Docker.
- Se hai scelto di utilizzare il motore del contenitore Docker, segui questi passaggi per installare Docker. Altrimenti, [Installare Podman](#).



Il supporto di Docker come motore container per implementazioni solo software è obsoleto. In una release futura, Docker sostituirà un altro motore per container.

Fasi

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



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

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

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

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

```
sudo docker version
```

Le versioni Client e Server devono essere 1.11.0 o successive.

Installare Podman

Il sistema StorageGRID funziona come una raccolta di contenitori. Se hai scelto di utilizzare il motore contenitore Podman, segui questi passaggi per installare Podman. Altrimenti, [Installare Docker](#).

Fasi

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



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

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

```
sudo docker version
```



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

Le versioni Client e Server devono essere 3.2.3 o successive.

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

Informazioni correlate

["Configurare lo storage host"](#)

Installare i servizi host StorageGRID su Linux

Per installare i servizi host StorageGRID , utilizzare il pacchetto StorageGRID adatto al tipo di sistema operativo in uso.



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#) .

RHEL

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

A proposito di questa attività

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

Fasi

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

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

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

```
sudo 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 immagini e poi il pacchetto servizi.



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

Ubuntu o Debian

Per installare i servizi host StorageGRID per Ubuntu o Debian, è possibile utilizzare il pacchetto StorageGRID DEB.

A proposito di questa attività

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

Fasi

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

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

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

È necessario installare prima il `images` pacchetto e il `service` secondo. Se i pacchetti sono stati inseriti in una directory diversa da `/tmp`, modificare il comando in modo che rifletta il percorso utilizzato.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```



Per poter installare i pacchetti StorageGRID, è necessario che Python 3 sia già installato. Il `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` il comando fallirà finché non lo avrai fatto.

Automatizza l'installazione dei nodi basati su software

Automatizza l'installazione del servizio host StorageGRID e la configurazione dei nodi grid su Linux

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



A proposito di questa attività

"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

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

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

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

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

StorageGRID fornisce script Python opzionali per automatizzare la configurazione delle appliance StorageGRID e dell'intero sistema StorageGRID (il "grid"). È possibile utilizzare direttamente questi script o controllarli per apprendere come utilizzare gli ["API REST per l'installazione di StorageGRID"](#) strumenti di distribuzione e configurazione della griglia sviluppati dall'utente.

Automatizzare l'installazione e la configurazione del servizio host StorageGRID

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

Il servizio host StorageGRID è confezionato in un DEB (Ubuntu o Debian) o in un RPM (RHEL) 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 la tua distribuzione Linux, aggiungere StorageGRID ai tuoi playbook o alle tue ricette dovrebbe essere semplice.

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

Esempio di Ansible role and playbook

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



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

RHEL

Per RHEL, 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`

Ubuntu o Debian

Per Ubuntu o Debian, le attività di installazione fornite `storagegrid` esempio di ruolo usa il `ansible.builtin.apt` modulo per eseguire l'installazione dai file DEB locali o da un repository apt 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 `ansible.builtin.apt` modulo:

- `roles/storagegrid/tasks/deb_install_from_repo.yml`
- `roles/storagegrid/tasks/deb_install_from_local.yml`

Automatizzare la configurazione di StorageGRID

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

Prima di iniziare

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

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

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



Memorizzare la password di gestione e la passphrase di provisioning dalla sezione password del file modificato `configure-storagegrid.json` file di configurazione in un luogo sicuro. Queste password sono necessarie per le procedure di installazione, espansione e manutenzione. Dovresti anche eseguire il backup del file modificato `configure-storagegrid.json` file di configurazione e salvarlo in un luogo sicuro.

A proposito di questa attività

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



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

Fasi

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

Ad esempio:

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

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

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

Ad esempio:

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

Risultato

Durante il processo di configurazione viene generato un file del pacchetto di ripristino `.zip` che viene scaricato nella directory in cui viene eseguito il processo di installazione e configurazione. È necessario

eseguire il backup del file del pacchetto di ripristino in modo da poter ripristinare il sistema StorageGRID in caso di guasto di uno o più nodi della griglia. Ad esempio, copiarla in una posizione di rete sicura e di backup e in una posizione di cloud storage sicura.



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

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

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

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

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

Automatizza la distribuzione dei nodi della griglia in StorageGRID con VMware vSphere

È possibile utilizzare lo strumento VMware OVF per automatizzare l'implementazione dei nodi grid. È inoltre possibile automatizzare la configurazione di StorageGRID.

Automazione dell'implementazione dei nodi grid

Utilizzare lo strumento VMware OVF per automatizzare l'implementazione dei nodi grid.

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 è installato e configurato correttamente.
- Si conoscono il nome utente e la password per accedere a VMware vSphere utilizzando lo strumento OVF
- Sono disponibili autorizzazioni sufficienti per implementare macchine virtuali da file OVF e attivarle, nonché per creare volumi aggiuntivi da collegare alle macchine virtuali. Per ulteriori informazioni, consultare la `ovftool` documentazione.
- Conosci l'URL dell'infrastruttura virtuale (VI) per la posizione in vSphere in cui desideri implementare le macchine virtuali StorageGRID. In genere, questo URL sarà un vApp o un pool di risorse. Ad esempio: `vi://vcenter.example.com/vi/sgws`



È possibile utilizzare l'utilità VMware `ovftool` per determinare questo valore (per ulteriori informazioni, consultare la `ovftool` documentazione).



Se si esegue la distribuzione su una vApp, le macchine virtuali non si avviano automaticamente la prima volta ed è necessario accenderle manualmente.

- Sono state raccolte tutte le informazioni necessarie per il file di configurazione della distribuzione. Per informazioni, vedere ["Raccogliere informazioni sull'ambiente di implementazione"](#).
- È possibile accedere ai seguenti file dall'archivio di installazione di VMware per StorageGRID:

Nome file	Descrizione
NetApp-SG-version-SHA.vmdk	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid. Nota: questo file deve trovarsi nella stessa cartella dei <code>.ovf</code> file e <code>.mf</code>
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Il file modello Open Virtualization Format (<code>.ovf</code>) e il file manifest (<code>.mf</code>) per la distribuzione del nodo amministrativo primario.
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Il file modello (<code>.ovf</code>) e il file manifesto (<code>.mf</code>) per la distribuzione di nodi Admin non primari.
vsphere-gateway.ovf vsphere-gateway.mf	Il file modello (<code>.ovf</code>) e il file manifesto (<code>.mf</code>) per la distribuzione dei nodi Gateway.
vsphere-storage.ovf vsphere-storage.mf	Il file modello (<code>.ovf</code>) e il file manifesto (<code>.mf</code>) per la distribuzione dei nodi di archiviazione basati su macchine virtuali.
deploy-vsphere-ovftool.sh	Lo script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
deploy-vsphere-ovftool-sample.ini	File di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> lo script.

Definire il file di configurazione per l'implementazione

È possibile specificare le informazioni necessarie per distribuire i nodi grid virtuali per StorageGRID in un file di configurazione, utilizzato dallo `deploy-vsphere-ovftool.sh` script Bash. È possibile modificare un file di configurazione di esempio, in modo da non dover creare il file da zero.

Fasi

1. Eseguire una copia del file di configurazione di esempio (`deploy-vsphere-ovftool.sample.ini`).
Salvare il nuovo file come `deploy-vsphere-ovftool.ini` nella stessa directory di `deploy-vsphere-ovftool.sh`.
2. Aprire `deploy-vsphere-ovftool.ini`.
3. Inserire tutte le informazioni necessarie per implementare i nodi virtual grid VMware.

Per informazioni, vedere [Impostazioni del file di configurazione](#).

4. Una volta inserite e verificate tutte le informazioni necessarie, salvare e chiudere il file.

Impostazioni del file di configurazione

Il `deploy-vsphere-ovftool.ini` file di configurazione contiene le impostazioni necessarie per distribuire i nodi griglia virtuali.

Il file di configurazione elenca prima i parametri globali, quindi i parametri specifici del nodo nelle sezioni definite dal nome del nodo. Quando si utilizza il file:

- I *parametri globali* vengono applicati a tutti i nodi della griglia.
- *Parametri specifici del nodo* sovrascrivono i parametri globali.

Parametri globali

I parametri globali vengono applicati a tutti i nodi della griglia, a meno che non vengano ignorati dalle impostazioni delle singole sezioni. Posizionare i parametri che si applicano a più nodi nella sezione Global Parameter (parametri globali), quindi eseguire l'override di queste impostazioni secondo necessità nelle sezioni relative ai singoli nodi.

- **OVFTOOL_ARGUMENTS:** È possibile specificare OVFTOOL_ARGUMENTS come impostazioni globali oppure applicare gli argomenti singolarmente a nodi specifici. Ad esempio:

```
OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=eagerZeroedThick
--datastore='datastore_name'
```

È possibile utilizzare le `--powerOffTarget` opzioni e `--overwrite` per arrestare e sostituire le macchine virtuali esistenti.



È necessario distribuire i nodi in diversi datastore e specificare OVFTOOL_ARGUMENTS per ciascun nodo, invece che globalmente.

- **SOURCE:** Il percorso del (`.vmdk`file StorageGRID virtual machine template` ) e dei `.ovf` file and `.mf` per i singoli nodi di griglia. Per impostazione predefinita, viene impostata la directory corrente.

```
SOURCE = /downloads/StorageGRID-Webscale-version/vsphere
```

- **TARGET:** URL dell'infrastruttura virtuale VMware vSphere (vi) per la posizione in cui verrà implementato StorageGRID. Ad esempio:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG:** Metodo utilizzato per acquisire indirizzi IP, STATICI o DHCP. L'impostazione predefinita è STATICO. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per l'acquisizione degli indirizzi IP, è possibile specificare questo metodo. È quindi possibile eseguire l'override

dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_CONFIG = STATIC
```

- **GRID_NETWORK_TARGET:** Il nome di una rete VMware esistente da utilizzare per Grid Network. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_TARGET = SG Admin Network
```

- **GRID_NETWORK_MASK:** La maschera di rete per Grid Network. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY:** Gateway di rete per Grid Network. Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU:** OPZIONALE. L'unità di trasmissione massima (MTU) sulla rete di rete. Se specificato, il valore deve essere compreso tra 1280 e 9216. Ad esempio:

```
GRID_NETWORK_MTU = 9000
```

Se omissso, viene utilizzato 1400.

Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito.



Il valore MTU della rete deve corrispondere al valore configurato sulla porta dello switch virtuale in vSphere a cui è connesso il nodo. In caso contrario, potrebbero verificarsi problemi di performance di rete o perdita di pacchetti.



Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete.

- **ADMIN_NETWORK_CONFIG:** Metodo utilizzato per acquisire gli indirizzi IP, DISABILITATI, STATICI o DHCP. L'impostazione predefinita è DISATTIVATA. Se tutti o la maggior parte dei nodi utilizzano lo stesso

metodo per l'acquisizione degli indirizzi IP, è possibile specificare questo metodo. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET:** Il nome di una rete VMware esistente da utilizzare per la rete di amministrazione. Questa impostazione è obbligatoria a meno che la rete amministrativa non sia disattivata. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. A differenza della rete Grid, non è necessario che tutti i nodi siano connessi alla stessa rete di amministrazione. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_TARGET = SG Admin Network
```

- **ADMIN_NETWORK_MASK:** La maschera di rete per la rete di amministrazione. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY:** Gateway di rete per la rete di amministrazione. Questa impostazione è necessaria se si utilizza un indirizzo IP statico e si specificano sottoreti esterne nell'impostazione ADMIN_NETWORK_ESL. (Ovvero, non è necessario se ADMIN_NETWORK_ESL è vuoto). Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL:** L'elenco di subnet esterne (route) per la rete amministrativa, specificato come elenco separato da virgole delle destinazioni di routing CIDR. Se tutti o la maggior parte dei nodi utilizzano lo stesso elenco di subnet esterne, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU:** OPZIONALE. L'unità di trasmissione massima (MTU) sulla rete di amministrazione. Non specificare se ADMIN_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omesso, viene utilizzato 1400. Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito. Se tutti o la maggior parte dei nodi utilizzano la stessa MTU per la rete di amministrazione, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG:** Metodo utilizzato per acquisire gli indirizzi IP, DISABILITATI, STATICI o DHCP. L'impostazione predefinita è DISATTIVATA. Se tutti o la maggior parte dei nodi utilizzano lo stesso metodo per l'acquisizione degli indirizzi IP, è possibile specificare questo metodo. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET:** Il nome di una rete VMware esistente da utilizzare per la rete client. Questa impostazione è obbligatoria a meno che la rete client non sia disattivata. Se tutti o la maggior parte dei nodi utilizzano lo stesso nome di rete, è possibile specificarlo qui. A differenza della rete Grid, non è necessario che tutti i nodi siano connessi alla stessa rete client. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_TARGET = SG Client Network
```

- **CLIENT_NETWORK_MASK:** La maschera di rete per la rete client. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico. Se tutti o la maggior parte dei nodi utilizzano la stessa maschera di rete, è possibile specificarla qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY:** Gateway di rete per la rete client. Questa impostazione è obbligatoria se si utilizza l'indirizzamento IP statico. Se tutti o la maggior parte dei nodi utilizzano lo stesso gateway di rete, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU:** OPZIONALE. L'unità di trasmissione massima (MTU) sulla rete client. Non specificare se CLIENT_NETWORK_CONFIG = DHCP. Se specificato, il valore deve essere compreso tra 1280 e 9216. Se omissso, viene utilizzato 1400. Se si desidera utilizzare i frame jumbo, impostare la MTU su un valore adatto per i frame jumbo, ad esempio 9000. In caso contrario, mantenere il valore predefinito. Se tutti o la maggior parte dei nodi utilizzano lo stesso MTU per la rete client, è possibile specificarlo qui. È quindi possibile eseguire l'override dell'impostazione globale specificando impostazioni diverse per uno o più singoli nodi. Ad esempio:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP:** Consente di rimappare qualsiasi porta utilizzata da un nodo per le comunicazioni interne al nodo di rete o esterne. Il rimapping delle porte è necessario se i criteri di rete aziendali limitano una o più

porte utilizzate da StorageGRID. Per l'elenco delle porte utilizzate da StorageGRID, vedere comunicazioni interne dei nodi di rete e comunicazioni esterne in ["Linee guida per il networking"](#).



Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico.



Se viene impostato solo PORT_REMAP, il mapping specificato viene utilizzato per le comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita.

Il formato utilizzato è: *network type/protocol/default port used by grid node/new port*, Dove il tipo di rete è grid, admin o client e il protocollo è tcp o udp.

Ad esempio:

```
PORT_REMAP = client/tcp/18082/443
```

Se utilizzata da sola, questa impostazione di esempio mappa simmetricamente le comunicazioni in entrata e in uscita per il nodo della griglia dalla porta 18082 alla porta 443. Se utilizzata in combinazione con PORT_REMAP_INBOUND, questa impostazione di esempio mappa le comunicazioni in uscita dalla porta 18082 alla porta 443.

È inoltre possibile rimappare più porte utilizzando un elenco separato da virgole.

Ad esempio:

```
PORT_REMAP = client/tcp/18082/443, client/tcp/18083/80
```

- **PORT_REMAP_INBOUND:** Consente di rimappare le comunicazioni in entrata per la porta specificata. Se si specifica PORT_REMAP_INBOUND ma non si specifica un valore per PORT_REMAP, le comunicazioni in uscita per la porta rimangono invariate.



Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico.

Il formato utilizzato è: *network type/protocol/_default port used by grid node/new port*, Dove il tipo di rete è grid, admin o client e il protocollo è tcp o udp.

Ad esempio:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

In questo esempio, il traffico inviato alla porta 443 passa attraverso un firewall interno e lo indirizza alla porta 18082, dove il nodo della griglia è in attesa delle richieste S3.

È inoltre possibile rimappare più porte in entrata utilizzando un elenco separato da virgole.

Ad esempio:

```
PORT_REMAP_INBOUND = grid/tcp/3022/22, admin/tcp/3022/22
```

- **TEMPORARY_PASSWORD_TYPE**: Il tipo di password di installazione temporanea da utilizzare quando si accede alla console VM o all'API di installazione StorageGRID, o utilizzando SSH, prima che il nodo si unisca alla griglia.



Se tutti o la maggior parte dei nodi utilizzano lo stesso tipo di password di installazione temporanea, specificare il tipo nella sezione Global Parameter (parametro globale). Quindi, facoltativamente, utilizzare un'impostazione diversa per un singolo nodo. Ad esempio, se si seleziona **Usa password personalizzata** a livello globale, è possibile utilizzare **CUSTOM_TEMPORARY_PASSWORD=<password>** per impostare la password per ciascun nodo.

TEMPORARY_PASSWORD_TYPE può essere uno dei seguenti:

- **Use node name**: Il nome del nodo viene utilizzato come password di installazione temporanea e fornisce l'accesso alla console VM, all'API di installazione StorageGRID e a SSH.
- **Disattiva password**: Non verrà utilizzata alcuna password di installazione temporanea. Se è necessario accedere alla VM per eseguire il debug dei problemi di installazione, vedere ["Risolvere i problemi di installazione"](#).
- **Usa password personalizzata**: Il valore fornito con **CUSTOM_TEMPORARY_PASSWORD=<password>** viene utilizzato come password di installazione temporanea e fornisce l'accesso alla console VM, all'API di installazione di StorageGRID e a SSH.



Facoltativamente, è possibile omettere il parametro **TEMPORARY_PASSWORD_TYPE** e specificare solo **CUSTOM_TEMPORARY_PASSWORD=<password>**.

- **CUSTOM_TEMPORARY_PASSWORD=<password>** opzionale. La password temporanea da utilizzare durante l'installazione quando si accede alla console VM, all'API di installazione StorageGRID e a SSH. Ignorato se **TEMPORARY_PASSWORD_TYPE** è impostato su **use node name** o **Disable password**.

Parametri specifici del nodo

Ogni nodo si trova nella propria sezione del file di configurazione. Ogni nodo richiede le seguenti impostazioni:

- L'Head della sezione definisce il nome del nodo che verrà visualizzato in Grid Manager. È possibile eseguire l'override di tale valore specificando il parametro **NODE_NAME** opzionale per il nodo.
- **NODE_TYPE**: **Nodo_Admin_VM**, **nodo_Storage_VM** o **nodo_Gateway_API_VM**
- **STORAGE_TYPE**: Combinato, dati o metadati. Se non viene specificato, per impostazione predefinita questo parametro opzionale per i nodi di storage viene utilizzato insieme (dati e metadati). Per ulteriori informazioni, vedere ["Tipi di nodi storage"](#).
- **GRID_NETWORK_IP**: L'indirizzo IP del nodo della rete Grid.
- **ADMIN_NETWORK_IP**: L'indirizzo IP del nodo nella rete di amministrazione. Obbligatorio solo se il nodo è collegato alla rete di amministrazione e **ADMIN_NETWORK_CONFIG** è impostato su **STATIC**.
- **CLIENT_NETWORK_IP**: L'indirizzo IP del nodo sulla rete client. Obbligatorio solo se il nodo è collegato alla rete client e **CLIENT_NETWORK_CONFIG** per questo nodo è impostato su **STATIC**.
- **ADMIN_IP**: L'indirizzo IP del nodo Admin primario sulla rete Grid. Utilizzare il valore specificato come **GRID_NETWORK_IP** per il nodo di amministrazione primario. Se si omette questo parametro, il nodo tenta

di rilevare l'IP del nodo di amministrazione primario utilizzando mDNS. Per ulteriori informazioni, vedere ["In che modo i nodi della griglia rilevano il nodo di amministrazione primario"](#).



Il parametro ADMIN_IP viene ignorato per il nodo di amministrazione primario.

- Tutti i parametri che non sono stati impostati globalmente. Ad esempio, se un nodo è collegato alla rete di amministrazione e non sono stati specificati i parametri ADMIN_NETWORK a livello globale, è necessario specificarli per il nodo.

Nodo amministratore primario

Per il nodo di amministrazione primario sono necessarie le seguenti impostazioni aggiuntive:

- **NODE_TYPE:** Nodo_amministrazione_VM
- **RUOLO_AMMINISTRATORE:** Primario

Questa voce di esempio si intende per un nodo amministratore primario che si trova su tutte e tre le reti:

```
[DC1-ADM1]
ADMIN_ROLE = Primary
NODE_TYPE = VM_Admin_Node
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 di amministrazione vengono assegnati due dischi rigidi aggiuntivi da 200 GB per l'audit e l'utilizzo del database. È possibile aumentare queste impostazioni utilizzando il parametro DISK. Ad esempio:

```
DISK = INSTANCES=2, CAPACITY=300
```



Per i nodi di amministrazione, LE ISTANZE devono sempre essere uguali a 2.

Nodo di storage

Per i nodi di storage è necessaria la seguente impostazione aggiuntiva:

- **NODE_TYPE:** Nodo_storage_VM

Questa voce di esempio si applica a un nodo di storage che si trova sulle reti Grid e Admin, ma non sulla rete client. Questo nodo utilizza l'impostazione ADMIN_IP per specificare l'indirizzo IP del nodo di amministrazione primario sulla rete di griglia.

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

Questo secondo esempio riguarda un nodo di storage su una rete client in cui la policy di rete aziendale del cliente afferma che un'applicazione client S3 è autorizzata ad accedere al nodo di storage solo utilizzando la porta 80 o 443. Il file di configurazione di esempio utilizza PORT_REMAP per consentire al nodo di storage di inviare e ricevere messaggi S3 sulla porta 443.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

L'ultimo esempio crea un remapping simmetrico per il traffico ssh dalla porta 22 alla porta 3022, ma imposta esplicitamente i valori per il traffico in entrata e in uscita.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

Le seguenti impostazioni aggiuntive sono opzionali per i nodi storage:

- **DISCO:** Per impostazione predefinita, ai nodi di storage vengono assegnati tre dischi da 4 TB per l'utilizzo di RangeDB. È possibile aumentare queste impostazioni con il parametro DISK. Ad esempio:

```
DISK = INSTANCES=16, CAPACITY=4096
```

- **STORAGE_TYPE:** Per impostazione predefinita, tutti i nuovi nodi di archiviazione sono configurati per

memorizzare sia i dati degli oggetti che i metadati, noti come *combined* Storage Node. È possibile modificare il tipo di nodo di archiviazione in modo che memorizzi solo dati o metadati con il parametro `STORAGE_TYPE`. Ad esempio:

```
STORAGE_TYPE = data
```

Nodo gateway

Per i nodi gateway è necessaria la seguente impostazione aggiuntiva:

- **NODE_TYPE:** GATEWAY VM_API

Questa voce di esempio è un nodo gateway di esempio su tutte e tre le reti. In questo esempio, nella sezione globale del file di configurazione non è stato specificato alcun parametro di rete client, pertanto è necessario specificarlo per il nodo:

```
[DC1-G1]
NODE_TYPE = VM_API_Gateway

GRID_NETWORK_IP = 10.1.0.5
ADMIN_NETWORK_IP = 10.3.0.5

CLIENT_NETWORK_CONFIG = STATIC
CLIENT_NETWORK_TARGET = SG Client Network
CLIENT_NETWORK_MASK = 255.255.255.0
CLIENT_NETWORK_GATEWAY = 10.4.0.1
CLIENT_NETWORK_IP = 10.4.0.5

ADMIN_IP = 10.1.0.2
```

Nodo amministrativo non primario

Per i nodi amministrativi non primari sono necessarie le seguenti impostazioni aggiuntive:

- **NODE_TYPE:** Nodo_amministrazione_VM
- **RUOLO_AMMINISTRATORE:** Non primario

Questa voce di esempio si trova per un nodo amministrativo non primario che non si trova nella rete client:

```
[DC2-ADM1]
ADMIN_ROLE = Non-Primary
NODE_TYPE = VM_Admin_Node

GRID_NETWORK_TARGET = SG Grid Network
GRID_NETWORK_IP = 10.1.0.6
ADMIN_NETWORK_IP = 10.3.0.6

ADMIN_IP = 10.1.0.2
```

La seguente impostazione aggiuntiva è facoltativa per i nodi di amministrazione non primari:

- **DISCO:** Per impostazione predefinita, ai nodi di amministrazione vengono assegnati due dischi rigidi aggiuntivi da 200 GB per l'audit e l'utilizzo del database. È possibile aumentare queste impostazioni utilizzando il parametro DISK. Ad esempio:

```
DISK = INSTANCES=2, CAPACITY=300
```



Per i nodi di amministrazione, LE ISTANZE devono sempre essere uguali a 2.

Eeguire lo script Bash

È possibile utilizzare `deploy-vsphere-ovftool.sh` lo script Bash e il file di configurazione `deploy-vsphere-ovftool.ini` modificato per automatizzare la distribuzione dei nodi StorageGRID in VMware vSphere.

Prima di iniziare

È stato creato un file di configurazione `deploy-vsphere-ovftool.ini` per il proprio ambiente.

È possibile utilizzare la guida disponibile con lo script Bash inserendo i comandi `help` (`-h`/`--help`). Ad esempio:

```
./deploy-vsphere-ovftool.sh -h
```

oppure

```
./deploy-vsphere-ovftool.sh --help
```

Fasi

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

Ad esempio:

```
cd StorageGRID-Webscale-version/vsphere
```

3. Per implementare tutti i nodi grid, eseguire lo script Bash con le opzioni appropriate per il proprio ambiente.

Ad esempio:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-  
vsphere-ovftool.ini
```

4. Se un nodo Grid non è riuscito a implementare a causa di un errore, risolvere l'errore ed eseguire nuovamente lo script Bash solo per quel nodo.

Ad esempio:

```
./deploy-vsphere-ovftool.sh --username=user --password=pwd --single  
-node="DC1-S3" ./deploy-vsphere-ovftool.ini
```

La distribuzione è completa quando lo stato per ogni nodo è "passato".

Deployment Summary

node	attempts	status
DC1-ADM1	1	Passed
DC1-G1	1	Passed
DC1-S1	1	Passed
DC1-S2	1	Passed
DC1-S3	1	Passed

Automatizzare la configurazione di StorageGRID

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

Prima di iniziare

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

Nome file	Descrizione
configure-storagegrid.py	Script Python utilizzato per automatizzare la configurazione

Nome file	Descrizione
configure-storagegrid.sample.json	File di configurazione di esempio da utilizzare con lo script
configure-storagegrid.blank.json	File di configurazione vuoto da utilizzare con lo script

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



Memorizzare la password di gestione e la passphrase di provisioning dalla sezione password del file modificato `configure-storagegrid.json` file di configurazione in un luogo sicuro. Queste password sono necessarie per le procedure di installazione, espansione e manutenzione. Dovresti anche eseguire il backup del file modificato `configure-storagegrid.json` file di configurazione e salvarlo in un luogo sicuro.

A proposito di questa attività

È possibile utilizzare `configure-storagegrid.py` lo script Python e il `configure-storagegrid.json` file di configurazione della griglia per automatizzare la configurazione del sistema StorageGRID.



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

Fasi

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

Ad esempio:

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

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

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

Ad esempio:

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

Risultato

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



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

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

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

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

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

Informazioni correlate

- ["Accedere a Grid Manager"](#)
- ["API REST di installazione"](#)

Distribuisce nodi di griglia virtuali

Raccogli informazioni sul tuo ambiente VMware per StorageGRID

Prima di implementare i nodi grid, è necessario raccogliere informazioni sulla configurazione di rete e sull'ambiente VMware.



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

Informazioni VMware

È necessario accedere all'ambiente di implementazione e raccogliere informazioni sull'ambiente VMware, sulle reti create per Grid, Admin e Client Network e sui tipi di volumi di storage che si intende utilizzare per i nodi di storage.

È necessario raccogliere informazioni sull'ambiente VMware, tra cui:

- Il nome utente e la password di un account VMware vSphere che dispone delle autorizzazioni appropriate per completare l'implementazione.
- Informazioni sulla configurazione di rete, datastore e host per ogni macchina virtuale a nodi StorageGRID.



VMware Live vMotion fa saltare il tempo di clock della macchina virtuale e non è supportato per i nodi grid di qualsiasi tipo. Anche se rari, tempi di clock errati possono causare la perdita di dati o aggiornamenti della configurazione.

Informazioni Grid Network

È necessario raccogliere informazioni sulla rete VMware creata per la rete grid StorageGRID (richiesta), tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare indirizzi IP, statici o DHCP.
 - Se si utilizzano indirizzi IP statici, i dettagli di rete richiesti per ciascun nodo della griglia (indirizzo IP, gateway, maschera di rete).
 - Se si utilizza DHCP, l'indirizzo IP del nodo amministrativo primario sulla rete Grid. Per ulteriori informazioni, vedere ["In che modo i nodi della griglia rilevano il nodo di amministrazione primario"](#).

Admin Network Information (informazioni di rete amministratore)

Per i nodi che saranno connessi alla rete amministrativa StorageGRID opzionale, è necessario raccogliere informazioni sulla rete VMware creata per questa rete, tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare indirizzi IP, statici o DHCP.
 - Se si utilizzano indirizzi IP statici, i dettagli di rete richiesti per ciascun nodo della griglia (indirizzo IP, gateway, maschera di rete).
 - Se si utilizza DHCP, l'indirizzo IP del nodo amministrativo primario sulla rete Grid. Per ulteriori informazioni, vedere ["In che modo i nodi della griglia rilevano il nodo di amministrazione primario"](#).
- L'elenco di subnet esterne (ESL) per la rete di amministrazione.

Informazioni di rete del client

Per i nodi che saranno connessi alla rete client StorageGRID opzionale, è necessario raccogliere informazioni sulla rete VMware creata per questa rete, tra cui:

- Il nome della rete.
- Metodo utilizzato per assegnare indirizzi IP, statici o DHCP.
- Se si utilizzano indirizzi IP statici, i dettagli di rete richiesti per ciascun nodo della griglia (indirizzo IP, gateway, maschera di rete).

Informazioni su interfacce aggiuntive

È possibile aggiungere interfacce di accesso o trunk alla macchina virtuale in vCenter dopo aver installato il nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha in Grid Manager.

- Se si aggiunge un'interfaccia di linea, configurare una o più interfacce VLAN per ogni nuova interfaccia principale. Vedere ["Configurare le interfacce VLAN"](#).
- Se si aggiunge un'interfaccia di accesso, è necessario aggiungerla direttamente ai gruppi ha. Vedere ["configurare i gruppi ad alta disponibilità"](#).

Volumi di storage per nodi di storage virtuali

Per i nodi di storage basati su macchine virtuali, è necessario raccogliere le seguenti informazioni:

- Il numero e le dimensioni dei volumi di archiviazione (LUN di archiviazione) che si intende aggiungere. Vedere ["Requisiti di storage e performance"](#).

Informazioni sulla configurazione della griglia

È necessario raccogliere informazioni per configurare la griglia:

- Licenza Grid
- Indirizzi IP del server NTP (Network Time Protocol)
- Indirizzi IP del server DNS

Creare file di configurazione del nodo StorageGRID per le distribuzioni Linux

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Posizione dei file di configurazione dei nodi

Posizionare il file di configurazione per ogni nodo StorageGRID nella `/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 sull'host, è necessario inserire tre file di configurazione del nodo nell'`/etc/storagegrid/nodes`host`.

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

Denominazione dei file di configurazione dei nodi

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

I nomi dei nodi devono seguire queste regole:

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

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

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

`site-nodetype-nodenumbers.conf`

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

Contenuto di un file di configurazione del nodo

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

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

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

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

Chiavi di rete Admin

ADMIN_IP

Valore	Designazione
Indirizzo IPv4 della rete Grid del nodo di amministrazione che si desidera utilizzare per installare il nodo basato su Linux. Per il ripristino, utilizzare l'IP del nodo di amministrazione primario, se disponibile; in caso contrario, utilizzare l'IP di un nodo di amministrazione non primario. Se si omette questo parametro, il nodo tenta di individuare un nodo amministrativo primario tramite mDNS. "In che modo i nodi della griglia rilevano il nodo di amministrazione primario"	Best practice

ADMIN_NETWORK_CONFIG

Valore	Designazione
DHCP, STATICO O DISATTIVATO	Opzionale

ADMIN_NETWORK_ESL

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

ADMIN_NETWORK_GATEWAY

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

ADMIN_NETWORK_IP

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

ADMIN_NETWORK_MAC

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

ADMIN_NETWORK_MASK

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

ADMIN_NETWORK_MTU

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

ADMIN_NETWORK_TARGET

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

ADMIN_NETWORK_TARGET_TYPE

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

ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare la chiave su "true" per fare in modo che il container StorageGRID utilizzi l'indirizzo MAC dell'interfaccia host di destinazione sulla rete di amministrazione. Per maggiori dettagli sulla clonazione MAC per Linux, vedere "Considerazioni e consigli per la clonazione degli indirizzi MAC"	Best practice

RUOLO_AMMINISTRATORE

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

Bloccare le chiavi del dispositivo

BLOCK_DEVICE_AUDIT_LOGS

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

BLOCK_DEVICE_RANGEDB_NNN

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per lo storage a oggetti persistente. Questa chiave è necessaria solo per i nodi con NODE_TYPE = VM_Storage_Node; non specificarla per altri tipi di nodo. È necessario solo BLOCK_DEVICE_RANGEDB_000; gli altri sono facoltativi. Il dispositivo a blocchi specificato per BLOCK_DEVICE_RANGEDB_000 deve essere di almeno 4 TB; gli altri possono essere più piccoli. Non lasciare lacune. Se si specifica BLOCK_DEVICE_RANGEDB_005, è necessario specificare ANCHE BLOCK_DEVICE_RANGEDB_004. Nota: Per la compatibilità con le implementazioni esistenti, sono supportate chiavi a due cifre per i nodi aggiornati. Esempi: <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>	Richiesti: BLOCK_DEVICE_RANGEDB_000 Opzionale: BLOCK_DEVICE_RANGEDB_001 BLOCK_DEVICE_RANGEDB_002 BLOCK_DEVICE_RANGEDB_003 BLOCK_DEVICE_RANGEDB_004 BLOCK_DEVICE_RANGEDB_005 BLOCK_DEVICE_RANGEDB_006 BLOCK_DEVICE_RANGEDB_007 BLOCK_DEVICE_RANGEDB_008 BLOCK_DEVICE_RANGEDB_009 BLOCK_DEVICE_RANGEDB_010 BLOCK_DEVICE_RANGEDB_011 BLOCK_DEVICE_RANGEDB_012 BLOCK_DEVICE_RANGEDB_013 BLOCK_DEVICE_RANGEDB_014 BLOCK_DEVICE_RANGEDB_015

BLOCK_DEVICE_TABLES

Valore	Designazione
Percorso e nome del file speciale del dispositivo a blocchi utilizzato da questo nodo per l'archiviazione persistente delle tabelle di database. Questa chiave è necessaria solo per i nodi con NODE_TYPE = VM_Admin_Node; non specificarla per altri tipi di nodo. Esempi: <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>	Obbligatorio

BLOCK_DEVICE_VAR_LOCAL

Valore	Designazione
Percorso e nome del file speciale del dispositivo di blocco utilizzato da questo nodo per l'`/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>	Obbligatorio

Chiavi di rete client

CONFIGURAZIONE_RETE_CLIENT

Valore	Designazione
DHCP, STATICO O DISATTIVATO	Opzionale

GATEWAY_RETE_CLIENT

Valore	Designazione

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

IP_RETE_CLIENT

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

CLIENT_NETWORK_MAC

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

CLIENT_NETWORK_MASK

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

MTU_RETE_CLIENT

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

DESTINAZIONE_RETE_CLIENT

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

TIPO_DESTINAZIONE_RETE_CLIENT

Valore	Designazione
DedicatedInterface (Questo è solo un valore supportato.)	Opzionale

CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare la chiave su "true" per fare in modo che il container StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete client. Per maggiori dettagli sulla clonazione MAC per Linux, vedere "Considerazioni e consigli per la clonazione degli indirizzi MAC"	Best practice

Chiavi di rete della griglia

GRID_NETWORK_CONFIG

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

GRID_NETWORK_GATEWAY

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

IP_RETE_GRIGLIA

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

GRID_NETWORK_MAC

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

GRID_NETWORK_MASK

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

GRID_NETWORK_MTU

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

GRID_NETWORK_TARGET

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

GRID_NETWORK_TARGET_TYPE

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

GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC

Valore	Designazione
Vero o Falso Impostare il valore della chiave su "true" per fare in modo che il contenitore StorageGRID utilizzi l'indirizzo MAC dell'interfaccia di destinazione host sulla rete di rete. Per maggiori dettagli sulla clonazione MAC per Linux, vedere "Considerazioni e consigli per la clonazione degli indirizzi MAC"	Best practice

Password di installazione (temporanea)

HASH_PASSWORD_TEMPORANEA_PERSONALIZZATA

Valore	Designazione
Per il nodo amministrativo primario, impostare una password temporanea predefinita per l'API di installazione StorageGRID durante l'installazione. Nota: Impostare una password di installazione solo sul nodo amministrativo primario. Se si tenta di impostare una password su un altro tipo di nodo, la convalida del file di configurazione del nodo non avrà esito positivo. 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 di StorageGRID. Deve essere un <code>crypt()</code> hash 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 il <code>openssl passwd</code> comando in modalità SHA-512.	Best practice

Interfaces key

INTERFACE_TARGET_nnnn

Valore	Designazione
Nome e descrizione opzionale per un'interfaccia aggiuntiva che si desidera aggiungere a questo nodo. È possibile aggiungere più interfacce aggiuntive a ciascun nodo. Per <i>nnnnn</i>, specificare un numero univoco per ogni voce di <code>INTERFACCIA_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 delle interfacce VLAN e nella pagina dei gruppi ha. Esempio: <code>INTERFACE_TARGET_0001=ens256, Trunk</code> Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.	Opzionale

Chiave RAM massima

MAXIMUM_RAM

Valore	Designazione
La quantità massima di RAM che questo nodo può consumare. Se questa chiave viene omessa, il nodo non presenta limitazioni di memoria. Quando si imposta questo campo per un nodo a livello di produzione, specificare un valore di almeno 24 GB e da 16 a 32 GB inferiore alla RAM totale di sistema. Nota: Il valore RAM influisce sullo spazio riservato ai metadati effettivi di un nodo. Consultare la "Descrizione di Metadata Reserved Space". Il formato di 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 gruppi di memoria.	Opzionale

Chiavi di tipo nodo

NODE_TYPE

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

TIPO_STORAGE

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

Tasti di rimappatura delle porte



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a "[Rimuovere i rimaps delle porte sugli host bare metal](#)".

PORT_REMAP

Valore	Designazione
Consente di rimappare qualsiasi porta utilizzata da un nodo per comunicazioni interne al nodo di rete o comunicazioni esterne. La rimappatura delle porte è necessaria se i criteri di rete aziendali limitano una o più porte utilizzate da StorageGRID, come descritto in "Comunicazioni interne al nodo di rete" o "Comunicazioni esterne". IMPORTANTE: Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico. Nota: Se è impostato solo PORT_REMAP, il mapping specificato viene utilizzato per le comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita. Il formato utilizzato è: <i>network type/protocol/default port used by grid node/new port</i>, Dove <i>network type</i> è grid, admin o client, ed è tcp o <i>protocol</i> udp. Esempio: PORT_REMAP = client/tcp/18082/443 È inoltre 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
Consente di rimappare le comunicazioni in entrata alla porta specificata. Se si specifica PORT_REMAP_INBOUND ma non si specifica un valore per PORT_REMAP, le comunicazioni in uscita per la porta rimangono invariate. IMPORTANTE: Non rimappare le porte che si intende utilizzare per configurare gli endpoint del bilanciamento del carico. Il formato utilizzato è: <i>network type/protocol/remapped port /default port used by grid node</i>, Dove <i>network type</i> è grid, admin o client, ed è tcp o protocol udp. Esempio: PORT_REMAP_INBOUND = grid/tcp/3022/22 È inoltre possibile rimappare più porte in entrata 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 in StorageGRID

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

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

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

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

Se si utilizza la ricerca automatica:



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

Distribuisce i nodi di griglia come macchine virtuali per StorageGRID con VMware vSphere

VMware vSphere Web Client consente di implementare ciascun nodo grid come macchina virtuale. Durante l'implementazione, ciascun nodo grid viene creato e connesso a una o più reti StorageGRID.

Se è necessario implementare qualsiasi nodo di archiviazione dell'appliance StorageGRID, vedere ["Implementare l'appliance Storage Node"](#).

In alternativa, è possibile rimappare le porte dei nodi o aumentare le impostazioni della CPU o della memoria per il nodo prima di accenderlo.

Prima di iniziare

- Avete esaminato come fare ["pianificare e preparare l'installazione"](#) e avete compreso i requisiti per software, CPU e RAM, storage e prestazioni.
- Hai familiarità con VMware vSphere Hypervisor e hai esperienza nell'implementazione di macchine virtuali in questo ambiente.



Il `open-vm-tools` pacchetto, un'implementazione open-source simile a VMware Tools, è incluso nella macchina virtuale StorageGRID. Non è necessario installare VMware Tools manualmente.

- È stata scaricata ed estratta la versione corretta dell'archivio di installazione di StorageGRID per VMware.



Se si implementa il nuovo nodo come parte di un'operazione di espansione o ripristino, è necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

- Si dispone del (`.vmdk` file disco della macchina virtuale StorageGRID):

```
NetApp-SG-version-SHA.vmdk
```

- Sono disponibili i `.ovf` file e `.mf` per ogni tipo di nodo griglia che si sta distribuendo:

Nome file	Descrizione
vsphere-primary-admin.ovf vsphere-primary-admin.mf	Il file di modello e il file manifest per il nodo di amministrazione primario.

Nome file	Descrizione
vsphere-non-primary-admin.ovf vsphere-non-primary-admin.mf	Il file di modello e il file manifest per un nodo di amministrazione non primario.
vsphere-storage.ovf vsphere-storage.mf	Il file modello e il file manifesto per un nodo di storage.
vsphere-gateway.ovf vsphere-gateway.mf	Il file di modello e il file manifest per un nodo gateway.

- I .vdmk file , , .ovf e .mf si trovano tutti nella stessa directory.
- Hai un piano per ridurre al minimo i domini di guasto. Ad esempio, non è consigliabile implementare tutti i nodi Gateway su un singolo host vSphere ESXi.



In una distribuzione di produzione, non eseguire più di un nodo di storage su una singola macchina virtuale. Non eseguire più macchine virtuali sullo stesso host ESXi se ciò creerebbe un problema inaccettabile del dominio di errore.

- Se si sta distribuendo un nodo come parte di un'operazione di espansione o ripristino, si dispone di ["Istruzioni per espandere un sistema StorageGRID"](#) o di ["Istruzioni per il ripristino e la manutenzione"](#).
- Se stai implementando un nodo StorageGRID come macchina virtuale con lo storage assegnato da un sistema NetApp ONTAP, hai verificato che il volume non disponga di una policy di tiering FabricPool abilitata. Ad esempio, se un nodo StorageGRID viene eseguito come macchina virtuale su un host VMware, assicurati che il volume che supporta l'archivio dati del nodo non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.



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

A proposito di questa attività

Seguire queste istruzioni per implementare inizialmente i nodi VMware, aggiungere un nuovo nodo VMware in un'espansione o sostituire un nodo VMware come parte di un'operazione di recovery. Ad eccezione di quanto indicato nelle fasi, la procedura di implementazione dei nodi è la stessa per tutti i tipi di nodi, inclusi nodi amministrativi, nodi storage e nodi gateway.

Se si sta installando un nuovo sistema StorageGRID:

- È possibile implementare i nodi in qualsiasi ordine.
- È necessario assicurarsi che ciascuna macchina virtuale possa connettersi al nodo di amministrazione primario tramite la rete di rete.
- È necessario implementare tutti i nodi della griglia prima di configurarla.

Se si sta eseguendo un'operazione di espansione o ripristino:

- È necessario assicurarsi che la nuova macchina virtuale possa connettersi a tutti gli altri nodi sulla rete Grid.

Se è necessario rimappare una delle porte del nodo, non accendere il nuovo nodo fino a quando la configurazione del rimappamento delle porte non è completa.



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a ["Rimuovere i rimaps delle porte sugli host bare metal"](#).

Fasi

1. Utilizzando vCenter, implementare un modello OVF.

Se si specifica un URL, selezionare una cartella contenente i seguenti file. In caso contrario, selezionare ciascuno di questi file da una directory locale.

```
NetApp-SG-version-SHA.vmdk  
vsphere-node.ovf  
vsphere-node.mf
```

Ad esempio, se si tratta del primo nodo che si sta implementando, utilizzare questi file per distribuire il nodo di amministrazione primario per il sistema StorageGRID:

```
NetApp-SG-version-SHA.vmdk  
vsphere-primary-admin.ovf  
vsphere-primary-admin.mf
```

2. Specificare un nome per la macchina virtuale.

La procedura standard consiste nell'utilizzare lo stesso nome sia per la macchina virtuale che per il nodo Grid.

3. Posizionare la macchina virtuale nella vApp o nel pool di risorse appropriato.
4. Se si sta implementando il nodo di amministrazione principale, leggere e accettare il Contratto di licenza con l'utente finale.

A seconda della versione di vCenter in uso, l'ordine dei passaggi varia in base all'accettazione del Contratto di licenza con l'utente finale, specificando il nome della macchina virtuale e selezionando un datastore.

5. Selezionare lo storage per la macchina virtuale.

Se si sta distribuendo un nodo come parte dell'operazione di ripristino, eseguire le istruzioni in [fase di recovery dello storage](#) per aggiungere nuovi dischi virtuali, ricollegare i dischi rigidi virtuali dal nodo griglia guasto o da entrambi.

Quando si implementa un nodo di storage, utilizzare 3 o più volumi di storage, con un volume di storage di 4 TB o superiore. È necessario assegnare almeno 4 TB al volume 0.



Il file .ovf del nodo di storage definisce diversi VMDK per lo storage. A meno che questi VMDK non soddisfino i requisiti di storage, è necessario rimuoverli e assegnare VMDK o RDM appropriati per lo storage prima di accendere il nodo. I VMDK sono più comunemente utilizzati negli ambienti VMware e sono più facili da gestire, mentre gli RDM potrebbero fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB).



Alcune installazioni StorageGRID potrebbero utilizzare volumi di storage più grandi e attivi rispetto ai carichi di lavoro virtualizzati tipici. Potrebbe essere necessario regolare alcuni parametri dell'hypervisor, come `MaxAddressableSpaceTB`, per ottenere prestazioni ottimali. In caso di performance scadenti, contatta la risorsa di supporto per la virtualizzazione per determinare se il tuo ambiente potrebbe trarre beneficio dall'ottimizzazione della configurazione specifica del carico di lavoro.

6. Selezionare reti.

Determinare quali reti StorageGRID utilizzare dal nodo selezionando una rete di destinazione per ciascuna rete di origine.

- La rete grid è obbligatoria. Selezionare una rete di destinazione nell'ambiente vSphere. + la rete di rete viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi nella grid, su 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 un'altra rete di destinazione nell'ambiente vSphere. Se non si utilizza la rete di amministrazione, selezionare la stessa destinazione selezionata per la rete di griglia.
- Se si utilizza la rete client, selezionare un'altra rete di destinazione nell'ambiente vSphere. Se non si utilizza la rete client, selezionare la stessa destinazione selezionata per la rete griglia.
- Se si utilizza una rete Admin o Client, i nodi non devono trovarsi sulle stesse reti Admin o Client.

7. Per **Personalizza modello**, configurare le proprietà del nodo StorageGRID richieste.

a. Inserire il nome del nodo.



Se si sta ripristinando un nodo Grid, è necessario immettere il nome del nodo che si sta ripristinando.

b. Utilizzare il menu a discesa **Password di installazione temporanea** per specificare una password di installazione temporanea, in modo da poter accedere alla console VM o 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 aver aggiunto un nodo alla griglia, è possibile accedervi utilizzando il **"password della console del nodo"**, che è elencato nel file nel `Passwords.txt` pacchetto di ripristino.

- **Usa nome nodo:** Il valore fornito per il campo **Nome nodo** viene utilizzato come password di installazione temporanea.
- **Usa password personalizzata:** Viene utilizzata una password personalizzata come password di installazione temporanea.
- **Disattiva password:** Non verrà utilizzata alcuna password di installazione temporanea. Se è

necessario accedere alla VM per eseguire il debug dei problemi di installazione, vedere ["Risolvere i problemi di installazione"](#).

- c. Se è stato selezionato **Usa password personalizzata**, specificare la password di installazione temporanea che si desidera utilizzare nel campo **Password personalizzata**.
- d. Nella sezione **Grid Network (eth0)**, selezionare STATIC (STATICO) o DHCP per la configurazione **Grid network IP (IP rete griglia)**.
 - Se si seleziona STATIC (STATICO), inserire **Grid network IP**, **Grid network mask**, **Grid network gateway** e **Grid network MTU**.
 - Se si seleziona DHCP, vengono assegnati automaticamente **Grid network IP**, **Grid network mask** e **Grid network gateway**.
- e. Nel campo **Primary Admin IP** (Indirizzo amministratore primario), immettere l'indirizzo IP del nodo di amministrazione primario per la rete di rete.

Se si omette l'indirizzo IP principale del nodo di amministrazione, l'indirizzo IP verrà rilevato automaticamente se il nodo di amministrazione primario, o almeno un altro nodo della griglia con ADMIN_IP configurato, è presente sulla stessa sottorete. Tuttavia, si consiglia di impostare qui l'indirizzo IP del nodo di amministrazione principale.

- f. Nella sezione **Admin Network (eth1)**, selezionare STATIC (STATICO), DHCP (DHCP) o DISABLED (DISATTIVATO) per la configurazione **Admin network IP (Indirizzo IP di rete amministratore)**.
 - Se non si desidera utilizzare la rete di amministrazione, selezionare DISABLED (DISATTIVATA) e immettere **0.0.0.0** come IP della rete di amministrazione. È possibile lasciare vuoti gli altri campi.
 - Se si seleziona STATICO, inserire **Admin network IP**, **Admin network mask**, **Admin network gateway** e **Admin network MTU**.
 - Se si seleziona STATICO, inserire l'elenco **Admin network external subnet list**. È inoltre necessario configurare un gateway.
 - Se si seleziona DHCP, vengono assegnati automaticamente **Admin network IP**, **Admin network mask** e **Admin network gateway**.
- g. Nella sezione **Client Network (eth2)**, selezionare STATIC (STATICO), DHCP (DHCP) o DISABLED (DISATTIVATO) per la configurazione **Client Network IP (IP di rete client)**.
 - Se non si desidera utilizzare la rete client, selezionare DISABLED (DISATTIVATA) e immettere **0.0.0.0** come IP di rete client. È possibile lasciare vuoti gli altri campi.
 - Se si seleziona STATIC (STATICO), inserire **Client network IP** (IP di rete client), **Client network mask** (maschera di rete client), **Client network gateway** e **Client network MTU**.
 - Se si seleziona DHCP, vengono assegnati automaticamente **IP di rete client**, **maschera di rete client** e **gateway di rete client**.
8. Esaminare la configurazione della macchina virtuale e apportare le modifiche necessarie.
9. Quando si è pronti per il completamento, selezionare **fine** per avviare il caricamento della macchina virtuale.
10. se questo nodo è stato implementato come parte dell'operazione di recovery e non si tratta di un recovery a nodo completo, attenersi alla seguente procedura al termine dell'implementazione:
 - a. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Edit Settings** (Modifica impostazioni).
 - b. Selezionare ciascun disco rigido virtuale predefinito designato per lo storage e selezionare **Rimuovi**.
 - c. A seconda delle circostanze di ripristino dei dati, aggiungere nuovi dischi virtuali in base ai requisiti di storage, ricollegare eventuali dischi rigidi virtuali conservati dal nodo Grid guasto precedentemente

rimosso o da entrambi.

Prendere nota delle seguenti importanti linee guida:

- Se si aggiungono nuovi dischi, è necessario utilizzare lo stesso tipo di dispositivo di storage utilizzato prima del ripristino del nodo.
- Il file .ovf del nodo di storage definisce diversi VMDK per lo storage. A meno che questi VMDK non soddisfino i requisiti di storage, è necessario rimuoverli e assegnare VMDK o RDM appropriati per lo storage prima di accendere il nodo. I VMDK sono più comunemente utilizzati negli ambienti VMware e sono più facili da gestire, mentre gli RDM potrebbero fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB).

11. se è necessario rimappare le porte utilizzate da questo nodo, procedere come segue.

Potresti dover rimappare una porta se le policy di rete aziendali limitano l'accesso a una o più porte utilizzate da StorageGRID. Consulta ["Linee guida per il networking"](#) per le porte utilizzate da StorageGRID.



Non rimappare le porte utilizzate negli endpoint del bilanciamento del carico.

- Selezionare la nuova VM.
- Dalla scheda Configura, selezionare **Impostazioni > Opzioni vApp**. La posizione di **vApp Options** dipende dalla versione di vCenter.
- Nella tabella **Proprietà**, individuare PORT_REMAP_INBOUND e PORT_REMAP.
- Per mappare simmetricamente le comunicazioni in entrata e in uscita per una porta, selezionare **PORT_REMAP**.



Il supporto per la rimappatura delle porte è obsoleto e verrà rimosso in una versione futura. Per rimuovere le porte rimappate, fare riferimento a ["Rimuovere i rimaps delle porte sugli host bare metal"](#).



Se viene impostato solo PORT_REMAP, il mapping specificato si applica alle comunicazioni in entrata e in uscita. Se VIENE specificato anche PORT_REMAP_INBOUND, PORT_REMAP si applica solo alle comunicazioni in uscita.

- Selezionare **Imposta valore**.
- Inserire la mappatura delle porte:

```
<network type>/<protocol>/<default port used by grid node>/<new port>
```

<network type> indica grid, admin o client, ed <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.

Ad 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. Inserire la mappatura delle porte:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound port  
used by grid node>
```

<network type> indica grid, admin o client, ed <protocol> è tcp o udp.

Ad esempio, per rimappare il traffico SSH in entrata inviato alla porta 3022 in modo che venga ricevuto alla porta 22 dal nodo della rete, immettere quanto segue:

```
client/tcp/3022/22
```

È possibile rimappare più porte in entrata utilizzando un elenco separato da virgole.

Ad esempio:

```
grid/tcp/3022/22, admin/tcp/3022/22
```

i. Selezionare **OK**

12. Se si desidera aumentare la CPU o la memoria per il nodo dalle impostazioni predefinite:

- Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Edit Settings** (Modifica impostazioni).
- Modificare il numero di CPU o la quantità di memoria secondo necessità.

Impostare **Memory Reservation** alle stesse dimensioni della **Memory** allocata alla macchina virtuale.

c. Selezionare **OK**.

13. Accendere la macchina virtuale.

Al termine

Se questo nodo è stato implementato come parte di una procedura di espansione o ripristino, tornare a queste istruzioni per completare la procedura.

File di configurazione di esempio per i nodi StorageGRID su Linux

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

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



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

Esempio per nodo amministratore primario

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

Esempio di contenuto del file:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
TEMPORARY_PASSWORD_TYPE = Use custom password
CUSTOM_TEMPORARY_PASSWORD = Passw0rd
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

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

Esempio per nodo di storage

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 Gateway Node

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/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Esempio di nodo amministrativo non primario

Nome file di esempio: /etc/storagegrid/nodes/dc1-adm2.conf

Esempio di contenuto del file:

```

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

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

```

Convalida la configurazione di StorageGRID su Linux

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

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

```
sudo storagegrid node validate all
```

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



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

```

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

```



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

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

```
Checking for misnamed node configuration files...
WARNING: ignoring /etc/storagegrid/nodes/dcl-adm1
WARNING: ignoring /etc/storagegrid/nodes/dcl-sn2.conf.keep
WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dcl-adm1...
ERROR: NODE_TYPE = VM_Foo_Node
      VM_Foo_Node is not a valid node type.  See *.conf.sample
ERROR: ADMIN_ROLE = Foo
      Foo is not a valid admin role.  See *.conf.sample
ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
      /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node 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
```

Avvia il servizio host StorageGRID su Linux

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

1. Eseguire i seguenti comandi su ciascun host:

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

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

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

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

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

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

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

Scopri l'API REST di installazione di StorageGRID

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

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



Tutte le operazioni API eseguite utilizzando la pagina Web documentazione API sono operazioni in tempo reale. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

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

API di installazione StorageGRID

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

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

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

- **config**: Operazioni relative alla release del prodotto e alle versioni dell'API. Puoi elencare la versione della release del prodotto e le versioni principali dell'API supportate da quella release.
- **griglia**: Operazioni di configurazione a livello di griglia. Puoi ottenere e aggiornare le impostazioni della griglia, inclusi i dettagli della griglia, le subnet della Grid Network, le password della griglia e gli indirizzi IP dei server NTP e DNS server.
- **nodi**: Operazioni di configurazione a livello di nodo. Puoi 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. Puoi avviare l'operazione di provisioning e visualizzarne lo stato.
- **recovery**: Operazioni di ripristino del nodo Admin primario. Puoi reimpostare le informazioni, caricare il Recovery Package, 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. Puoi creare, visualizzare, eliminare e modificare un sito.
- **password temporanea**: Operazioni sulla password temporanea per proteggere la mgmt-api durante l'installazione.

Risoluzione dei problemi di installazione di StorageGRID

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



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#) .

Linux

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

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

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

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

Per informazioni su come accedere ai file di registro, vedere ["Raccogliere i file di log e i dati di sistema"](#).

VMware

Di seguito sono riportati i principali file di log dell'installazione, che potrebbero essere necessari al supporto tecnico per risolvere i problemi.

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

La prenotazione delle risorse della macchina virtuale richiede una modifica

I file OVF includono una riserva di risorse progettata per garantire che ciascun nodo di griglia disponga di RAM e CPU sufficienti per funzionare in modo efficiente. Se si creano macchine virtuali implementando questi file OVF su VMware e il numero predefinito di risorse non è disponibile, le macchine virtuali non si avviano.

A proposito di questa attività

Se si è certi che l'host della macchina virtuale disponga di risorse sufficienti per ciascun nodo della griglia, regolare manualmente le risorse allocate per ciascuna macchina virtuale, quindi provare ad avviare le macchine virtuali.

Fasi

1. Nell'albero del client di VMware vSphere Hypervisor, selezionare la macchina virtuale non avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Edit Settings** (Modifica impostazioni).-
3. Dalla finestra Virtual Machines Properties (Proprietà macchine virtuali), selezionare la scheda **Resources** (risorse).
4. Regolare le risorse allocate alla macchina virtuale:
 - a. Selezionare **CPU**, quindi utilizzare il dispositivo di scorrimento Reservation (prenotazione) per regolare i MHz riservati per questa macchina virtuale.
 - b. Selezionare **memoria**, quindi utilizzare il dispositivo di scorrimento prenotazione per regolare il MB riservato per questa macchina virtuale.
5. Selezionare **OK**.
6. Ripetere la procedura secondo necessità per altre macchine virtuali ospitate sullo stesso host di macchine virtuali.

La password di installazione temporanea è stata disabilitata

Quando si implementa un nodo VMware, è possibile specificare facoltativamente una password di installazione temporanea. È necessario disporre di questa password per accedere alla console VM o utilizzare SSH prima che il nuovo nodo si unisca alla griglia.

Se si è scelto di disattivare la password di installazione temporanea, è necessario eseguire ulteriori operazioni per eseguire il debug dei problemi di installazione.

È possibile effettuare una delle seguenti operazioni:

- Ridistribuire la VM ma specificare una password di installazione temporanea in modo da poter accedere alla console o utilizzare SSH per eseguire il debug dei problemi di installazione.
- Utilizzare vCenter per impostare la password:
 - a. Spegnerne la macchina virtuale.
 - b. Vai su **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. Impostare la password temporanea:
 - Modificare **CUSTOM_TEMPORARY_PASSWORD** in un valore di password personalizzato.
 - Aggiornare **TEMPORARY_PASSWORD_TYPE** con il valore **use node name**.
 - f. Riavviare la macchina virtuale per applicare la nuova password.

Informazioni correlate

- Per informazioni su come accedere ai file di registro, vedere ["Riferimenti ai file di log"](#).
- ["Risolvere i problemi di un sistema StorageGRID"](#)
- Per ulteriore assistenza, contattare ["Supporto NetApp"](#).

Esempi di script

Esempio di consolidamento di quattro interfacce fisiche in un unico bond per StorageGRID su RHEL

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

Interfacce fisiche

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

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

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

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

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

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

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

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

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

Interfaccia bond

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

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

Interfacce VLAN

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

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

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

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

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

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

Esempio di aggregazione di interfacce fisiche per StorageGRID su Ubuntu e Debian

Il `/etc/network/interfaces` file comprende 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 aggrega quattro interfacce fisiche Linux in un singolo collegamento LACP e quindi stabilisce tre interfacce VLAN che sottintende il collegamento per l'utilizzo come interfacce di rete StorageGRID, amministratore e client.

Interfacce fisiche

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

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Interfaccia bond

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 ens224 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
```

Configura la griglia e completa l'installazione

Accedi a StorageGRID Grid Manager

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

Prima di iniziare

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

Fasi

1. Aprire il browser Web e accedere a:

`https://primary_admin_node_ip`

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

`https://primary_admin_node_ip:8443`

È possibile utilizzare l'indirizzo IP per l'indirizzo IP del nodo di amministrazione primario sulla rete griglia o sulla rete di amministrazione, a seconda della configurazione di rete. Potrebbe essere necessario utilizzare l'opzione Security/Advanced del browser per accedere a un certificato non attendibile.

2. Gestione di una password di installazione temporanea come necessario:

- Se una password è già stata impostata utilizzando uno di questi metodi, immetterla per continuare.
 - Un utente imposta la password durante l'accesso al programma di installazione in precedenza
 - Per Linux, la password è stata importata automaticamente dal file di configurazione del nodo in `/etc/storagegrid/nodes/<node_name>.conf`
 - Per VMware, la password SSH/console è stata importata automaticamente dalle proprietà OVF
- Se non è stata impostata una password, impostare una password per proteggere il programma di installazione di StorageGRID.

3. Selezionare **Installa un sistema StorageGRID**.

Viene visualizzata la pagina utilizzata per configurare una griglia StorageGRID.

NetApp® StorageGRID® Help ▾

Install

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

Specificare le informazioni sulla licenza StorageGRID

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

Fasi

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

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

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

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



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

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 in StorageGRID

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

Fasi

1. Nella pagina Siti, inserisci il **nome del sito**.
2. Per aggiungere altri siti, seleziona il segno più accanto all'ultima voce sito e inserisci il nome nella nuova casella di testo **Site name**.

Aggiungi tutti i siti aggiuntivi necessari per la topologia della 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 ✕

Site Name 2 + ✕

3. Selezionare **Avanti**.

Specificare le subnet della Grid Network per StorageGRID

È necessario specificare le subnet utilizzate nella rete Grid.

A proposito di questa attività

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

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

Fasi

1. Specificare l'indirizzo di rete CIDR per almeno una rete griglia nella casella di testo **Subnet 1**.
2. Seleziona il segno più accanto all'ultima voce per aggiungere un'altra voce di rete. Devi specificare tutte le sottoreti per tutti i siti nella Grid Network.
 - Se hai già distribuito almeno un nodo, seleziona **Scopri le sottoreti di Grid Networks** per popolare automaticamente l'elenco delle sottoreti di Grid Network con le sottoreti segnalate dai nodi grid che si sono registrati con Grid Manager.
 - È necessario aggiungere manualmente le sottoreti per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway di rete Grid.

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 (current step), 4. Grid Nodes, 5. NTP, 6. DNS, 7. Passwords, and 8. Summary. Step 3 is highlighted with a blue circle. Below the progress bar, the 'Grid Network' section is displayed. It contains a text box for 'Subnet 1' with the value '172.16.0.0/21' and a plus sign icon to its right. Below this, there is a button labeled 'Discover Grid Network subnets'.

3. Selezionare **Avanti**.

Approva i nodi della griglia in sospeso per StorageGRID

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

Prima di iniziare

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



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

Fasi

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



Se manca un nodo griglia, verificare che sia stato distribuito correttamente e che l'IP della rete griglia del nodo amministrativo primario sia impostato 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 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. Selezionare **approva**.
4. In General Settings (Impostazioni generali), modificare le impostazioni per le seguenti proprietà, in base alle necessità:
 - **Sito:** Il nome di sistema del sito per questo nodo della griglia.
 - **Name:** Il nome del sistema per il nodo. Il nome predefinito corrisponde al nome specificato al momento della configurazione del nodo.

I nomi di sistema sono necessari per le operazioni StorageGRID interne e non possono essere

modificati dopo aver completato l'installazione. Tuttavia, durante questa fase del processo di installazione, è possibile modificare i nomi di sistema in base alle esigenze.



Per un nodo VMware, è possibile modificare il nome qui, ma questa azione non cambierà il nome della macchina virtuale in vSphere.

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



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

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



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

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

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

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

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



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

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

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



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

Appliance: per un'appliance StorageGRID, se la rete amministrativa non è stata configurata durante l'installazione iniziale utilizzando il programma di installazione dell'appliance StorageGRID, non è possibile

configurarla in questa finestra di dialogo. È invece necessario attenersi alla seguente procedura:

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

Il riavvio può richiedere alcuni minuti.

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

Per ulteriori informazioni, consultare ["Avvio rapido per l'installazione dell'hardware"](#) le istruzioni per individuare l'apparecchio.

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



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

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

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

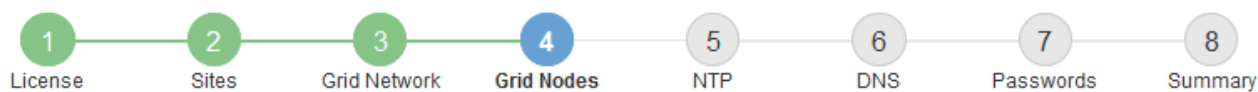
Il riavvio può richiedere alcuni minuti.

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

Per ulteriori informazioni, consultare ["Avvio rapido per l'installazione dell'hardware"](#) le istruzioni per individuare l'apparecchio.

8. Selezionare **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.

+ Approve

✕ Remove

Search

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.

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
☐	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 griglia in sospeso che si desidera approvare.

Devi approvare tutti i nodi che vuoi nella grid. Tuttavia, puoi tornare su questa pagina in qualsiasi momento prima di selezionare **Install** nella pagina Summary. Puoi modificare le proprietà di un nodo della grid approvato selezionando il suo pulsante di opzione e selezionando **Edit**.

10. Quando hai finito di approvare i nodi della griglia, seleziona **Avanti**.

Specificare le informazioni del server Network Time Protocol per StorageGRID

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

A proposito di questa attività

Specificare gli indirizzi IPv4 per i server NTP.

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

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



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

["Limite di supporto per tempi ad alta precisione"](#)

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



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

(Solo VMware) 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 .

Fasi

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

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**.

Informazioni correlate

Specificare le informazioni del DNS server per StorageGRID

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

A proposito di questa attività

La specifica "[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 si specificano più di tre, è possibile che ne vengano utilizzati solo tre a causa delle limitazioni del sistema operativo note su alcune piattaforme. Se nel proprio ambiente sono presenti restrizioni di routing, è possibile "[Personalizzare l'elenco dei server DNS](#)" che singoli nodi (in genere tutti i nodi di un sito) utilizzino un gruppo diverso di un massimo di tre server DNS.

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

Fasi

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

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 (currently selected), 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, there's a "Server 2" text box with the value "10.224.223.136" and a red "+ X" icon. The text below the text boxes reads: "Enter the IP address for at least one Domain Name System (DNS) server, so that server hostnames can be used instead of IP addresses. Specifying at least two DNS servers is recommended. Configuring DNS enables server connectivity, email notifications, and NetApp AutoSupport."

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

3. Selezionare **Avanti**.

Specificare le password di sistema di StorageGRID

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

A proposito di questa attività

Utilizzare la pagina Installa password per specificare la passphrase di provisioning e la password utente root di

gestione della griglia.

- La passphrase di provisioning viene utilizzata come chiave di crittografia e non viene memorizzata dal sistema StorageGRID.
- È necessario disporre della passphrase di provisioning per le procedure di installazione, espansione e manutenzione, incluso il download del pacchetto di ripristino. Pertanto, è importante memorizzare la passphrase di provisioning in una posizione sicura.
- È possibile modificare la passphrase di provisioning da Grid Manager, se si dispone di quella corrente.
- La password utente root della gestione della griglia può essere modificata utilizzando Grid Manager.
- La console della riga di comando generata casualmente e le password SSH sono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino.

Fasi

1. In **Passphrase di provisioning**, inserisci la passphrase di provisioning che sarà richiesta per apportare modifiche alla topologia della griglia del tuo sistema StorageGRID.

Memorizzare 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 **Grid Management Root User Password**, immettere la password da utilizzare per accedere al Grid Manager come utente "root".



Conservare la passphrase di provisioning in un luogo sicuro. È necessario per le procedure di installazione, ampliamento e manutenzione.

4. In **Confirm Root User Password** (Conferma password utente root), immettere nuovamente 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.

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

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



Ti viene richiesto di scaricare il file del Pacchetto di ripristino (sgws-recovery-package-id-revision.zip) dopo che selezioni **Installa** nella pagina Riepilogo. Devi ["scarica questo file"](#) per completare l'installazione. Le password necessarie per accedere al sistema sono memorizzate nel file Passwords.txt, contenuto nel Pacchetto di ripristino.

- Selezionare **Avanti**.

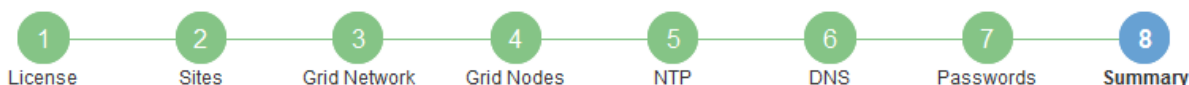
Rivedi la configurazione di StorageGRID

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

Fasi

- Visualizza la pagina **Riepilogo**.

Install



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

- Verificare che tutte le informazioni di configurazione della griglia siano corrette. Utilizzare i link Modify (Modifica) nella pagina Summary (Riepilogo) per tornare indietro e correggere eventuali errori.
- Seleziona **Installa**.



Se un nodo è configurato per utilizzare la Client Network, il gateway predefinito per quel nodo passa dalla Grid Network alla Client Network quando selezioni **Installa**. Se perdi la connettività, devi assicurarti di accedere al primary Admin Node tramite una subnet accessibile. Vedi "[Linee guida per il networking](#)" per i dettagli.

- Selezionare **Download recovery package** (Scarica pacchetto di ripristino).

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

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



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

6. Seleziona la casella di controllo **Ho scaricato e verificato correttamente il file del pacchetto di ripristino** e seleziona **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 completa per tutti i nodi della griglia, viene visualizzata la pagina di accesso per Grid Manager.

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

Requisiti di rete e DHCP dopo l'installazione di StorageGRID

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

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

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



I nodi si riavviano quando la configurazione della rete griglia viene modificata da DHCP, causando interruzioni nel caso in cui una modifica DHCP influisca su più nodi contemporaneamente.

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

Scopri i passaggi obbligatori e facoltativi dopo l'installazione di StorageGRID

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

Attività richieste

- (Solo VMware) Configurare VMware vSphere Hypervisor per il riavvio automatico.

È necessario configurare l'hypervisor per riavviare le macchine virtuali al riavvio del server. Senza un riavvio automatico, le macchine virtuali e i nodi della griglia rimangono spenti dopo il riavvio del server. Per ulteriori informazioni, consultare la documentazione di VMware vSphere Hypervisor.

- ["Creare un account tenant"](#) Per il protocollo client S3 che verrà utilizzato per memorizzare oggetti nel sistema StorageGRID.
- ["Controllare l'accesso al sistema"](#) configurando gruppi e account utente. In alternativa, è possibile ["configurare un'origine di identità federata"](#) (ad esempio Active Directory o OpenLDAP) importare gruppi e utenti di amministrazione. In alternativa, è possibile ["creare utenti e gruppi locali"](#).
- Integrare e testare le ["S3 API"](#) applicazioni client che verranno utilizzate per caricare oggetti sul sistema StorageGRID.
- ["Configurare le regole ILM \(Information Lifecycle Management\) e i criteri ILM"](#) ideale per la protezione dei dati degli oggetti.
- Se l'installazione include nodi di storage dell'appliance, utilizzare SANtricity OS per completare le seguenti operazioni:
 - Connessione a ogni appliance StorageGRID.
 - Verificare la ricezione dei dati AutoSupport.

Vedere ["Configurare l'hardware"](#).

- Esaminare e seguire la ["Linee guida per la protezione avanzata del sistema StorageGRID"](#) per eliminare i rischi per la sicurezza.
- ["Configurare le notifiche e-mail per gli avvisi di sistema"](#).

Attività facoltative

- ["Aggiornare gli indirizzi IP del nodo griglia"](#) se sono cambiati da quando hai pianificato la distribuzione e generato il pacchetto di ripristino.
- ["Configurare la crittografia dello storage"](#), se necessario.
- ["Configurare la compressione dello storage"](#) per ridurre le dimensioni degli oggetti memorizzati, se necessario.
- ["Configurare le interfacce VLAN"](#) per isolare e partizionare il traffico di rete, se necessario.
- ["Configurare i gruppi ad alta disponibilità"](#) Per migliorare la disponibilità delle connessioni per i client Grid Manager, Tenant Manager e S3, se necessario.
- ["Configurare gli endpoint del bilanciamento del carico"](#) Per la connettività client S3, se richiesta.

Aggiornare il software StorageGRID

Aggiornare il software StorageGRID

Seguire queste istruzioni per aggiornare un sistema StorageGRID a una nuova release.

Quando esegui l'upgrade, tutti i nodi del sistema StorageGRID vengono aggiornati.



Non avviare l'aggiornamento se hai urgente bisogno di espandere lo spazio di archiviazione per aumentarne la capacità (se lo spazio di archiviazione è quasi pieno). Completare la procedura di aggiornamento nei tempi previsti. Se è necessario un ripristino, contattare l'assistenza tecnica.

Prima di effettuare l'aggiornamento

Esamina questi argomenti per conoscere le nuove funzionalità e i miglioramenti di StorageGRID 12.1, verificare se alcune funzionalità sono state deprecate o rimosse e scoprire le modifiche apportate alle API di StorageGRID.

- ["Impatto del sistema durante l'aggiornamento"](#)
- ["Novità di StorageGRID 12.1"](#)
- ["Funzionalità rimosse o obsolete"](#)
- ["Modifiche all'API Grid Management"](#)
- ["Modifiche all'API di gestione del tenant"](#)

Pianificare e prepararsi per l'upgrade

Stima il tempo necessario per completare un aggiornamento di StorageGRID

Considerare quando eseguire l'aggiornamento, in base alla durata dell'aggiornamento. È importante sapere quali operazioni è possibile e non è possibile eseguire in ciascuna fase dell'aggiornamento.

A proposito di questa attività

Il tempo necessario per completare un aggiornamento di StorageGRID dipende da una varietà di fattori, come il carico del client e le performance dell'hardware.

La tabella riassume le principali attività di aggiornamento ed elenca il tempo approssimativo necessario per ciascuna attività. I passaggi successivi alla tabella forniscono le istruzioni da utilizzare per stimare il tempo di aggiornamento del sistema.

Attività di upgrade	Descrizione	Tempo approssimativo richiesto	Durante questa attività
Eseguire i controlli preliminari e aggiornare il nodo di amministrazione primario	Vengono eseguiti i controlli preliminari per l'aggiornamento e il nodo di amministrazione primario viene arrestato, aggiornato e riavviato.	da 30 minuti a 1 ora, con nodi di appliance di assistenza che richiedono la maggior parte del tempo. Gli errori di pre-controllo non risolti aumenteranno questo tempo.	Impossibile accedere al nodo di amministrazione primario. Potrebbero essere segnalati errori di connessione che è possibile ignorare. L'esecuzione dei controlli preliminari per l'aggiornamento prima di avviare l'aggiornamento consente di risolvere eventuali errori prima della finestra di manutenzione pianificata per l'aggiornamento.
Avviare il servizio di aggiornamento	Il file software viene distribuito e il servizio di aggiornamento viene avviato.	3 minuti per nodo di rete	

Attività di upgrade	Descrizione	Tempo approssimativo richiesto	Durante questa attività
Aggiornar e altri nodi grid	Il software su tutti gli altri nodi della griglia viene aggiornato nell'ordine in cui si approvano i nodi. Un nodo di amministrazione o gateway viene aggiornato contemporaneamente a un nodo di archiviazione.	da 15 minuti a 1 ora per nodo, con nodi appliance che richiedono il maggior numero di tempo Nota: Per i nodi appliance, il programma di installazione dell'appliance StorageGRID viene aggiornato automaticamente alla versione più recente.	• Non modificare la configurazione della griglia. • Non modificare la configurazione del livello di audit. • Non aggiornare la configurazione ILM. • Non è possibile eseguire altre procedure di manutenzione, ad esempio hotfix, decommissionare o espandere. Nota: Per eseguire un ripristino, contattare il supporto tecnico.
Abilitare le funzioni	Le nuove funzioni della nuova versione sono attivate.	Fino a 1 ora	• Non modificare la configurazione della griglia. • Non modificare la configurazione del livello di audit. • Non aggiornare la configurazione ILM. • Non è possibile eseguire un'altra procedura di manutenzione.
Fasi finali dell'upgrade	I file temporanei vengono rimossi e l'aggiornamento alla nuova release viene completato.	5 minuti	Una volta completata l'attività fasi finali dell'aggiornamento , è possibile eseguire tutte le procedure di manutenzione.

Stima del tempo per l'aggiornamento

Fasi

1. Stima del tempo necessario per l'aggiornamento di tutti i nodi della griglia.

a. Moltiplicare il numero di nodi nel sistema StorageGRID per 1 ora/nodo.

Come regola generale, l'aggiornamento dei nodi appliance richiede più tempo rispetto ai nodi basati su software.

b. Aggiungere 1 ora per tenere conto del tempo necessario per scaricare il .upgrade file, eseguire le convalide di controllo preliminare e completare le fasi finali dell'aggiornamento.

2. Se si dispone di nodi Linux, aggiungere 15 minuti per ciascun nodo per tenere conto del tempo necessario per scaricare e installare il pacchetto RPM o DEB.

3. Calcola il tempo totale stimato per l'aggiornamento aggiungendo i risultati dei passaggi 1 e 2.

Esempio: Tempo stimato per l'upgrade a StorageGRID 12.1

Si supponga che il sistema disponga di 14 nodi grid, di cui 8 nodi Linux.

1. Moltiplicare 14 per 1 ora/nodo.
2. Aggiungere 1 ora per tenere conto del download, del controllo preliminare e dei passaggi finali.

Il tempo stimato per l'aggiornamento di tutti i nodi è di 15 ore.

3. Moltiplicare 8 per 15 minuti/nodo per il tempo di installazione del pacchetto RPM o DEB sui nodi Linux.

Il tempo stimato per questa fase è di 2 ore.

4. Sommare i valori.

Dovresti prevedere fino a 18 ore per completare l'upgrade del tuo sistema a StorageGRID 12.1.0.



Se necessario, è possibile dividere la finestra di manutenzione in finestre più piccole approvando i sottoinsiemi di nodi della griglia da aggiornare in più sessioni. Ad esempio, si consiglia di aggiornare i nodi nel sito A in una sessione e quindi aggiornare i nodi nel sito B in una sessione successiva. Se si sceglie di eseguire l'aggiornamento in più sessioni, tenere presente che non è possibile iniziare a utilizzare le nuove funzionalità fino a quando tutti i nodi non sono stati aggiornati.

In che modo gli aggiornamenti di StorageGRID influiscono sul tuo sistema

Scopri in che modo il tuo sistema StorageGRID sarà influenzato durante l'aggiornamento.

L'accesso SSH esterno è consentito fino al completamento dell'aggiornamento

Durante l'aggiornamento è consentito l'accesso SSH esterno. Al termine dell'aggiornamento, l'accesso SSH esterno viene bloccato per impostazione predefinita. Dopo l'aggiornamento, puoi utilizzare la scheda **Blocca SSH** disponibile nella pagina **Gestione griglia > Impostazioni di sicurezza** per ["gestire l'accesso SSH esterno"](#). L'accesso SSH tra i nodi della griglia non è interessato.

Gli aggiornamenti di StorageGRID sono senza interruzioni

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante l'intero processo di aggiornamento. Se si approvano tutti i nodi dello stesso tipo per l'aggiornamento (ad esempio, i nodi di storage), i nodi vengono disattivati uno alla volta, in modo che non vi sia tempo in cui tutti i nodi di griglia o tutti i nodi di griglia di un determinato tipo non siano disponibili.

Per consentire la disponibilità continua, assicurarsi che il criterio ILM contenga regole che specificano la memorizzazione di più copie di ciascun oggetto. È inoltre necessario assicurarsi che tutti i client S3 esterni siano configurati per inviare richieste a uno dei seguenti:

- Un indirizzo IP virtuale del gruppo ad alta disponibilità (ha)
- Bilanciamento del carico di terze parti ad alta disponibilità
- Nodi gateway multipli per ogni client
- Più nodi di storage per ogni client

Le applicazioni client potrebbero riscontrare interruzioni a breve termine

Il sistema StorageGRID può acquisire e recuperare i dati dalle applicazioni client durante tutto il processo di upgrade, tuttavia le connessioni client a singoli nodi di gateway o nodi storage potrebbero essere temporaneamente interrotte se l'upgrade deve riavviare i servizi su tali nodi. La connettività viene ripristinata al termine del processo di upgrade e i servizi vengono ripristinati nei singoli nodi.

Potrebbe essere necessario pianificare i tempi di inattività per applicare un aggiornamento se la perdita di connettività per un breve periodo non è accettabile. È possibile utilizzare l'approvazione selettiva per pianificare l'aggiornamento di determinati nodi.



È possibile utilizzare più gateway e gruppi di alta disponibilità (ha) per fornire il failover automatico durante il processo di upgrade. Vedere le istruzioni per ["configurazione di gruppi ad alta disponibilità"](#).

Le riparazioni in background non verranno eseguite su griglie con nodi di versione mista

Le riparazioni in background non vengono eseguite durante l'aggiornamento quando la griglia contiene nodi con versioni miste. Eventuali incongruenze che si verificano durante un'interruzione del sito non verranno riparate fino al completamento dell'aggiornamento.

Il firmware dell'appliance viene aggiornato

Durante l'upgrade a StorageGRID 12.1:

- Tutti i nodi dell'appliance StorageGRID vengono aggiornati automaticamente al firmware StorageGRID Appliance Installer versione 12.1.
- Gli apparecchi SG6060 e SGF6024 vengono aggiornati automaticamente alla versione firmware BIOS 3B08.EX e alla versione firmware BMC 4.01.07.
- Gli apparecchi SG100 e SG1000 vengono automaticamente aggiornati alla versione firmware BIOS 3B13.EC e alla versione firmware BMC 4.75.07.
- Gli appliance SGF6112, SG6160, SG110 e SG1100 vengono aggiornati automaticamente alla versione firmware BIOS 3A14.QD e alla versione firmware BMC 3.21.07.

Le policy ILM vengono gestite in modo diverso in base al loro stato

- Il criterio attivo rimane lo stesso dopo l'aggiornamento.
- Solo le ultime 10 politiche storiche vengono mantenute al momento dell'aggiornamento.
- Se esiste una policy proposta, verrà eliminata durante l'aggiornamento.

Potrebbero essere attivati degli avvisi

Gli avvisi potrebbero essere attivati all'avvio e all'arresto dei servizi e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi di griglia che eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). Al termine dell'aggiornamento potrebbero essere attivati altri avvisi.

Ad esempio, potresti visualizzare l'avviso **Impossibile comunicare con il nodo** quando i servizi vengono arrestati, oppure l'avviso **Errore di comunicazione Cassandra** quando alcuni nodi sono stati aggiornati a StorageGRID 12.0 o versioni successive, ma altri nodi eseguono ancora una versione precedente di StorageGRID. In generale, questi avvisi si risolvono quando l'upgrade è completato.

L'avviso **Impossibile posizionare ILM** potrebbe essere attivato quando i nodi di archiviazione vengono

arrestati durante l'upgrade a StorageGRID 12.0 o versioni successive. Questo avviso potrebbe persistere per 1 giorno dopo il completamento dell'upgrade.

Una volta completato l'aggiornamento, è possibile rivedere gli avvisi relativi all'aggiornamento selezionando **Avvisi risolti di recente** o **Avvisi correnti** dalla dashboard di Grid Manager.

Le modifiche alla configurazione sono limitate



Le restrizioni relative alle modifiche di configurazione sono specifiche per ogni versione. Se stai eseguendo l'upgrade a un'altra release di StorageGRID, consulta l'elenco delle modifiche non consentite nelle istruzioni di upgrade per quella release.

Fino al completamento dell'attività **Enable New Feature**:

- Non apportare modifiche alla configurazione della griglia.
- Non attivare o disattivare nuove funzioni.
- Non aggiornare la configurazione ILM. In caso contrario, potrebbe verificarsi un comportamento ILM inconsistente e imprevisto.
- Non applicare una correzione rapida o ripristinare un nodo della griglia.



Contattare il supporto tecnico se è necessario ripristinare un nodo durante l'aggiornamento.

- Non dovresti gestire gruppi HA, interfacce VLAN o endpoint del bilanciatore di carico mentre stai eseguendo l'upgrade.
- Non eliminare alcun gruppo HA finché l'upgrade non è completato. Gli indirizzi IP virtuali in altri gruppi HA potrebbero diventare inaccessibili.

Fino al completamento dell'attività **fasi finali dell'aggiornamento**:

- Non eseguire una procedura di espansione.
- Non eseguire una procedura di decommissionamento.

Verificare la versione installata di StorageGRID prima dell'aggiornamento

Prima di avviare l'aggiornamento, verificare che la versione precedente di StorageGRID sia attualmente installata con la correzione rapida più recente disponibile applicata.

A proposito di questa attività

Prima di aggiornare a StorageGRID 12.1, sulla tua grid deve essere installato StorageGRID 12.0 o una versione successiva. Se stai utilizzando una versione precedente di StorageGRID, devi installare tutti i file di upgrade precedenti insieme ai relativi hotfix più recenti (fortemente consigliato) finché la versione attuale della tua grid non sarà almeno StorageGRID 12.0.0.

Un possibile percorso di aggiornamento è illustrato nella [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. Fare riferimento a "[Download NetApp: StorageGRID](#)" e le note di rilascio per ogni hotfix per saperne di più.

Verifica la versione installata

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Nella parte superiore di Grid Manager, selezionare **Guida > informazioni**.
3. Verificare che la **Versione** sia 11.9.0.8 o successiva.
4. Se la **Versione** non è 11.9.0.8 o successiva, vai a ["Download NetApp: StorageGRID"](#) per scaricare i file di aggiornamento e hotfix di cui hai bisogno.
5. ["Seguire le istruzioni per l'aggiornamento"](#) per ogni versione scaricata. ["Applica l'ultimo hotfix"](#) per ogni versione (fortemente consigliato).

Fare riferimento al seguente esempio di aggiornamento.

Esempio: aggiornamento a StorageGRID 12.0 dalla versione 11.8

L'esempio seguente mostra i passaggi per eseguire l'upgrade da StorageGRID versione 11.9 alla versione 12.0 in preparazione per un upgrade a StorageGRID 12.1.

Scaricare e installare il software nella sequenza seguente per preparare il sistema per l'aggiornamento:

1. Eseguire l'aggiornamento alla versione principale di StorageGRID 11.8.0.
2. Applicare la correzione rapida StorageGRID 11,8.0.y più recente.
3. Aggiorna alla versione principale StorageGRID 11.9.0.
4. Applicare l'hotfix StorageGRID 11.9.0.8 o versione successiva.

Ottieni i materiali necessari per un aggiornamento del software StorageGRID

Prima di iniziare l'aggiornamento del software, procurarsi tutto il materiale necessario.

Elemento	Note
Laptop di assistenza	Il laptop di assistenza deve disporre di: • Porta di rete • Client SSH (ad esempio, putty)
"Browser Web supportato"	Il supporto del browser in genere cambia per ogni release di StorageGRID. Assicurarsi che il browser sia compatibile con la nuova versione di StorageGRID.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è elencata nel <code>Passwords.txt</code> file.
Linux RPM o archivio DEB	Se qualsiasi nodo viene distribuito su host Linux, è necessario "Scaricare e installare il pacchetto RPM o DEB su tutti gli host" prima di avviare l'aggiornamento. Assicurati che il tuo sistema operativo Linux soddisfi i requisiti minimi di versione del kernel di StorageGRID. Vedere "Installa StorageGRID su host Linux" .

Elemento	Note
Documentazione StorageGRID	• "Note di rilascio". È necessario accedere con il proprio account NetApp o crearne uno per accedere alle note di rilascio. Assicurarsi di leggerle attentamente prima di iniziare l'aggiornamento. • "Guida alla risoluzione degli aggiornamenti del software StorageGRID" per la versione principale a cui stai eseguendo l'upgrade (accesso richiesto) • Altro "Documentazione StorageGRID", secondo necessità.

Controlla le condizioni del tuo sistema StorageGRID prima di eseguire l'aggiornamento

Prima di aggiornare un sistema StorageGRID, verificare che il sistema sia pronto per l'aggiornamento. Verificare che il sistema funzioni normalmente e che tutti i nodi della griglia siano operativi.

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Verificare la presenza di eventuali avvisi attivi e risolverli.
3. Consulta ["Comunicazioni interne al nodo di rete"](#) e ["Comunicazioni esterne"](#) per assicurarti che tutte le porte richieste per StorageGRID 12.1 siano aperte prima di eseguire l'upgrade.



Non sono necessarie porte aggiuntive per l'aggiornamento a StorageGRID 12.1.

Aggiornare il software

Avvio rapido per gli aggiornamenti di StorageGRID

Prima di iniziare l'aggiornamento, esaminare il flusso di lavoro generale. La pagina aggiornamento StorageGRID guida l'utente attraverso ogni fase di aggiornamento.

1

Preparare gli host Linux

Se un qualsiasi nodo StorageGRID viene distribuito su host Linux, ["Installare il pacchetto RPM o DEB su ciascun host"](#) prima di iniziare l'aggiornamento.

2

Caricare i file di aggiornamento e hotfix

Dal nodo di amministrazione principale, accedere alla pagina di aggiornamento StorageGRID e caricare il file di aggiornamento e il file di correzione rapida, se necessario.

3

Scarica il pacchetto di ripristino

Scaricare il pacchetto di ripristino corrente prima di avviare l'aggiornamento.

4**Eseguire controlli preliminari dell'aggiornamento**

I controlli preliminari dell'aggiornamento consentono di rilevare i problemi, in modo da poterli risolvere prima di avviare l'aggiornamento effettivo.

5**Avviare l'aggiornamento**

Quando si avvia l'aggiornamento, i controlli preliminari vengono eseguiti nuovamente e il nodo amministrativo primario viene aggiornato automaticamente. Impossibile accedere a Grid Manager durante l'aggiornamento del nodo di amministrazione primario. Anche i registri di controllo non saranno disponibili. L'aggiornamento può richiedere fino a 30 minuti.

6**Scarica il pacchetto di ripristino**

Dopo aver aggiornato il nodo di amministrazione primario, scaricare un nuovo pacchetto di ripristino.

7**Approva nodi**

È possibile approvare singoli nodi griglia, gruppi di nodi griglia o tutti i nodi griglia.



Non approvare l'aggiornamento per un nodo grid a meno che non si sia certi che il nodo sia pronto per essere arrestato e riavviato.

8**Riprendere le operazioni**

Una volta aggiornati tutti i nodi della griglia, vengono attivate nuove funzionalità ed è possibile riprendere le operazioni. È necessario attendere l'esecuzione di una procedura di decommissionamento o espansione fino al completamento dell'attività **Upgrade database** in background e dell'attività **Final upgrade steps**.

Informazioni correlate

["Stima del tempo necessario per completare un aggiornamento"](#)

Scarica e installa i pacchetti RPM o DEB su tutti gli host Linux per StorageGRID

Se un qualsiasi nodo StorageGRID viene distribuito su host Linux, scaricare e installare un pacchetto RPM o DEB aggiuntivo su ciascuno di questi host prima di avviare l'aggiornamento.

Scarica i file di aggiornamento, Linux e hotfix

Quando si esegue un aggiornamento StorageGRID da Grid Manager, viene richiesto di scaricare l'archivio di aggiornamento e le correzioni rapide necessarie come primo passaggio. Tuttavia, se è necessario scaricare i file per aggiornare gli host Linux, è possibile risparmiare tempo scaricando tutti i file richiesti in anticipo.

Fasi

1. Andare a ["Download NetApp: StorageGRID"](#).
2. Selezionare il pulsante per scaricare l'ultima versione oppure selezionare un'altra versione dal menu a discesa e selezionare **Go**.

Le versioni del software StorageGRID hanno questo formato: 11.x.y. Le hotfix StorageGRID hanno questo formato: 11.x.a. .z.

3. Accedi con il nome utente e la password del tuo account NetApp.
4. Se viene visualizzato un avviso di attenzione/MustRead, annotare il numero della correzione rapida e selezionare la casella di controllo.
5. Leggere il Contratto di licenza con l'utente finale (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 (**Upgrade StorageGRID**), scaricare due file:
 - L'archivio di aggiornamento per l'ultima release (questo è il file nella sezione denominata **VMware, SG1000 o SG100 Primary Admin Node**). Sebbene questo file non sia necessario fino a quando non si esegue l'aggiornamento, il download di questo file consente di risparmiare tempo.
 - Un archivio RPM o DEB in .tgz formato o. .zip Selezionare il .zip file se sul laptop di assistenza è in esecuzione Windows.
 - RHEL
StorageGRID-Webscale-version-RPM-uniqueID.zip
StorageGRID-Webscale-version-RPM-uniqueID.tgz
 - Ubuntu o Debian +
StorageGRID-Webscale-version-DEB-uniqueID.zip
StorageGRID-Webscale-version-DEB-uniqueID.tgz
7. Se è necessario accettare un avviso di attenzione/MustRead a causa di una correzione rapida richiesta, scaricare la correzione rapida:
 - a. Tornare a ["Download NetApp: StorageGRID"](#).
 - b. Selezionare il numero della correzione rapida dall'elenco a discesa.
 - c. Accettare nuovamente l'avviso di attenzione e l'EULA.
 - d. Scaricare e salvare la correzione rapida e il relativo README.

Quando si avvia l'aggiornamento, viene richiesto di caricare il file hotfix nella pagina aggiornamento StorageGRID.

8. La verifica della firma del codice è manuale su un nodo Linux. Facoltativamente, verificare l'archivio di installazione:
 - a. Scaricare 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"](#).

Installare l'archivio su tutti gli host Linux

Eseguire questa procedura prima di aggiornare il software StorageGRID.

Fasi

1. Estrarre i pacchetti RPM o DEB dal file di installazione.

2. Installare i pacchetti RPM o DEB su tutti gli host Linux.

Consultare i passaggi per l'installazione dei servizi host StorageGRID per Linux in ["Installare 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, è possibile rimuovere gli archivi di installazione delle versioni precedenti di StorageGRID che non sono più necessari.

Fasi

1. Rimuovere i vecchi archivi di installazione di StorageGRID.

RHEL

1. Catturare 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 intende eseguire l'aggiornamento.

È possibile ignorare in modo sicuro gli avvisi visualizzati. 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. Acquisire 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 intende 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. Acquisire l'elenco delle immagini contenitore 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 contenitore per le versioni precedenti di StorageGRID: `docker rmi image id`



Non rimuovere le immagini contenitore per la versione di StorageGRID attualmente in esecuzione o per le versioni di StorageGRID a cui si intende eseguire l'aggiornamento.

Esempio:

```
[root@docker-example ~]# docker rmi cb480ed37eea
Untagged: storagegrid-11.6.0:API_Gateway
Deleted:
sha256:cb480ed37eea0ae9cf3522de1dadfbff0075010d89c1c0a2337a3178051ddf02
Deleted:
sha256:5f269aabbf15c32c1fe6f36329c304b6c6ecb563d973794b9b59e8e5ab8ccc
afa
Deleted:
sha256:47c2b2c295a77b312b8db69db58a02d8e09e929e121352bec713fa12dae66
bde
[root@docker-example ~]#
```

Podman

1. Acquisire l'elenco delle immagini contenitore installate: `podman images`

Esempio:

```
[root@podman-example ~]# podman images
```

REPOSITORY SIZE	TAG	IMAGE ID	CREATED
localhost/storagegrid-11.8.0 ago 2.57 GB	Storage_Node	7125480de71b	7 months
localhost/storagegrid-11.8.0 ago 2.67 GB	Admin_Node	404e9f1bd173	7 months
localhost/storagegrid-11.8.0 ago 2.42 GB	Archive_Node	c3294a29697c	7 months
localhost/storagegrid-11.8.0 ago 1.77 GB	API_Gateway	1f88f24b9098	7 months
localhost/storagegrid-11.7.0 ago 2.54 GB	Storage_Node	1655350eff6f	16 months
localhost/storagegrid-11.7.0 ago 2.51 GB	Admin_Node	872258dd0dc8	16 months
localhost/storagegrid-11.7.0 ago 2.44 GB	Archive_Node	121e7c8b6d3b	16 months
localhost/storagegrid-11.7.0 ago 1.8 GB	API_Gateway	5b7a26e382de	16 months
localhost/storagegrid-11.6.0 ago 2.42 GB	Admin_Node	ee39f71a73e1	2 years
localhost/storagegrid-11.6.0 ago 2.11 GB	Storage_Node	f5ef895dcad0	2 years
localhost/storagegrid-11.6.0 ago 1.98 GB	Archive_Node	5782de552db0	2 years
localhost/storagegrid-11.6.0 ago 1.38 GB	API_Gateway	cb480ed37eea	2 years

```
[root@podman-example ~]#
```

2. Rimuovere le immagini contenitore per le versioni precedenti di StorageGRID: `podman rmi image id`



Non rimuovere le immagini contenitore per la versione di StorageGRID attualmente in esecuzione o per le versioni di StorageGRID a cui si intende eseguire l'aggiornamento.

Esempio:

```
[root@podman-example ~]# podman rmi f5ef895dcad0
Untagged: localhost/storagegrid-11.6.0:Storage_Node
Deleted:
f5ef895dcad0d78d0fd21a07dd132d7c7f65f45d80ee7205a4d615494e44cbb7
[root@podman-example ~]#
```

Eseguire un aggiornamento StorageGRID

Puoi eseguire l'upgrade a StorageGRID 12.1 e applicare l'ultimo hotfix per quella release contemporaneamente. La pagina di upgrade di StorageGRID fornisce il percorso di upgrade consigliato e i link diretti alle pagine di download corrette.

Prima di iniziare

Hai esaminato tutte le considerazioni e completato tutte le fasi di pianificazione e preparazione.



Non avviare l'aggiornamento se hai urgente bisogno di espandere lo spazio di archiviazione per aumentarne la capacità (se lo spazio di archiviazione è quasi pieno). Completare la procedura di aggiornamento nei tempi previsti. Se è necessario un ripristino, contattare l'assistenza tecnica.

Accedere alla pagina aggiornamento StorageGRID

Come primo passo, accedi alla pagina aggiornamento StorageGRID in Gestione griglia.

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Selezionare **Manutenzione > Sistema > Aggiornamento software**.
3. Dal riquadro di aggiornamento di StorageGRID, selezionare **Aggiorna**.

Selezionare file

Il percorso di upgrade nella pagina Upgrade di StorageGRID indica quali versioni principali (per esempio, 12.1.0) e hotfix (per esempio, 12.1.0.1) devi installare per arrivare all'ultima release di StorageGRID. Dovresti installare le versioni e gli hotfix raccomandati nell'ordine mostrato.



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.

Fasi

1. Per l'operazione **Select Files**, esaminare il percorso di aggiornamento.
2. Dalla sezione Download Files (Scarica file), selezionare ciascun collegamento **Download** per scaricare i file richiesti dal NetApp Support Site.

Se non viene visualizzato alcun percorso di aggiornamento, andare al ["Download NetApp: StorageGRID"](#) per determinare se è disponibile una nuova versione o correzione rapida e scaricare i file necessari.



Se è necessario scaricare e installare un pacchetto RPM o DEB su tutti gli host Linux, è possibile che i file di aggiornamento e hotfix di StorageGRID siano già elencati nel percorso di aggiornamento.

3. Seleziona **Sfoglia** per caricare il file di upgrade della versione su StorageGRID:
`NetApp_StorageGRID_12.1.0_Software_uniqueID.upgrade`

Una volta completato il caricamento e la verifica della firma del codice, accanto al nome del file appare un segno di spunta verde.

4. Se è stato scaricato un file di hotfix, selezionare **Sfoggia** per caricarlo. La correzione rapida verrà applicata automaticamente come parte dell'aggiornamento della versione.
5. Selezionare **continua**.

Eeguire i controlli preliminari

L'esecuzione dei controlli preliminari consente di rilevare e risolvere eventuali problemi di aggiornamento prima di iniziare l'aggiornamento del grid.

Fasi

1. Per il passaggio **Esegui controlli preliminari**, iniziare inserendo la passphrase di provisioning per la griglia.
2. Selezionare **Download recovery package** (Scarica pacchetto di ripristino).

Prima di aggiornare il nodo di amministrazione primario, è necessario scaricare la copia corrente del file del pacchetto di ripristino. Il file del pacchetto di ripristino consente di ripristinare il sistema in caso di guasto.

3. Una volta scaricato il file, confermare di poter accedere al contenuto, incluso il `Passwords.txt` file.
4. Copiare il file scaricato (.zip) in due posizioni sicure, sicure e separate.



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

5. Selezionare **Esegui pre-controlli** e attendere il completamento dei controlli preliminari.
6. Esamina i dettagli di ogni precontrollo segnalato e risolvi eventuali errori. Consulta la ["Guida alla risoluzione degli aggiornamenti del software StorageGRID"](#) per la release StorageGRID 12.1.

Prima di poter aggiornare il sistema, è necessario risolvere tutti gli errori di pre-controllo. Tuttavia, non è necessario eseguire il controllo preliminare *warnings* prima di eseguire l'aggiornamento.



Se sono state aperte porte firewall personalizzate, viene inviata una notifica durante la convalida del controllo preliminare. È necessario contattare il supporto tecnico prima di procedere con l'aggiornamento.

7. Se sono state apportate modifiche alla configurazione per risolvere i problemi segnalati, selezionare di nuovo **Esegui controlli preliminari** per ottenere risultati aggiornati.

Se tutti gli errori sono stati risolti, viene richiesto di avviare l'aggiornamento.

Avviare l'aggiornamento e aggiornare il nodo di amministrazione primario

Quando si avvia l'aggiornamento, i controlli preliminari dell'aggiornamento vengono eseguiti di nuovo e il nodo di amministrazione primario viene aggiornato automaticamente. Questa parte dell'aggiornamento può richiedere fino a 30 minuti.



Non sarà possibile accedere ad altre pagine di Grid Manager durante l'aggiornamento del nodo di amministrazione primario. Anche i registri di controllo non saranno disponibili.

Fasi

1. Selezionare **Avvia aggiornamento**.

Viene visualizzato un avviso per ricordare che l'accesso a Grid Manager verrà temporaneamente perso.

2. Selezionare **OK** per confermare l'avviso e avviare l'aggiornamento.

3. Attendere l'esecuzione delle verifiche preliminari dell'aggiornamento e l'aggiornamento del nodo di amministrazione primario.



Se vengono segnalati errori di pre-controllo, risolverli e selezionare di nuovo **Avvia aggiornamento**.

Se la griglia dispone di un altro nodo Admin in linea e pronto, è possibile utilizzarlo per monitorare lo stato del nodo Admin primario. Non appena il nodo di amministrazione primario viene aggiornato, è possibile approvare gli altri nodi della griglia.

4. Se necessario, selezionare **continua** per accedere alla fase **Aggiorna altri nodi**.

Aggiornare altri nodi

È necessario aggiornare tutti i nodi grid, ma è possibile eseguire più sessioni di aggiornamento e personalizzare la sequenza di aggiornamento. Ad esempio, si consiglia di aggiornare i nodi nel sito A in una sessione e quindi aggiornare i nodi nel sito B in una sessione successiva. Se si sceglie di eseguire l'aggiornamento in più sessioni, tenere presente che non è possibile iniziare a utilizzare le nuove funzionalità fino a quando tutti i nodi non sono stati aggiornati.

Se l'ordine in cui i nodi vengono aggiornati è importante, approvare i nodi o i gruppi di nodi uno alla volta e attendere il completamento dell'aggiornamento su ciascun nodo prima di approvare il nodo o il gruppo di nodi successivo.



Quando l'aggiornamento inizia su un nodo grid, i servizi su quel nodo vengono interrotti. In seguito, il nodo Grid viene riavviato. Per evitare interruzioni del servizio per le applicazioni client che comunicano con il nodo, non approvare l'aggiornamento per un nodo a meno che non si sia certi che il nodo sia pronto per essere arrestato e riavviato. Se necessario, pianificare una finestra di manutenzione o avvisare i clienti.

Fasi

1. Per la fase **Upgrade other Nodes** (Aggiorna altri nodi), consultare il Riepilogo, che fornisce l'ora di inizio dell'aggiornamento nel suo complesso e lo stato di ogni importante attività di upgrade.
 - **Avvia servizio di aggiornamento** è la prima attività di aggiornamento. Durante questa attività, il file software viene distribuito ai nodi grid e il servizio di aggiornamento viene avviato su ciascun nodo.
 - Una volta completata l'attività **Avvia 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 pacchetto di ripristino.



Dopo aver aggiornato il nodo di amministrazione primario, è necessario scaricare una nuova copia del file del pacchetto di ripristino. Il file del pacchetto di ripristino consente di ripristinare il sistema in caso di errore.

3. Esaminare le tabelle di stato per ciascun tipo di nodo. Sono presenti tabelle per i nodi amministrativi non primari, i nodi gateway e i nodi storage.

Un nodo della griglia può trovarsi in una di queste fasi quando le tabelle vengono visualizzate per la prima volta:

- Disimballaggio dell'aggiornamento
- Download in corso
- In attesa di approvazione

4. quando sei pronto a selezionare i nodi di griglia per l'upgrade (o se devi annullare l'approvazione dei nodi selezionati), utilizza queste istruzioni:



Per un upgrade a StorageGRID 12.1, se vuoi approvare singoli nodi invece di tutti i nodi, la best practice è aggiornare un intero sito prima di passare al sito successivo.

Attività	Istruzioni
Cercare nodi specifici da approvare, ad esempio tutti i nodi di un determinato sito	Inserire la stringa di ricerca nel campo Search
Selezionare tutti i nodi per l'aggiornamento	Selezionare approva tutti i nodi
Selezionare tutti i nodi dello stesso tipo per l'aggiornamento (ad esempio, tutti i nodi di storage)	Selezionare il pulsante approva tutto per il tipo di nodo Se si approvano più nodi dello stesso tipo, questi verranno aggiornati uno alla volta.
Selezionare un singolo nodo per l'aggiornamento	Selezionare il pulsante approva per il nodo
Posticipare l'aggiornamento su tutti i nodi selezionati	Selezionare Annulla approvazione di tutti i nodi
Posticipare l'aggiornamento su tutti i nodi selezionati dello stesso tipo	Selezionare il pulsante Annulla approvazione tutto per il tipo di nodo
Posticipare l'aggiornamento su un singolo nodo	Selezionare il pulsante Annulla approvazione per il nodo

5. Attendere che i nodi approvati procedano con le seguenti fasi di aggiornamento:

- Approvato e in attesa di aggiornamento
- Interruzione dei servizi



Non puoi rimuovere un nodo quando il suo Stage raggiunge **arresto dei servizi**. Il pulsante **Annulla approvazione** è disattivato.

- Arresto del container
- Pulizia delle immagini Docker
- Aggiornamento dei pacchetti del sistema operativo di base



Quando un nodo appliance raggiunge questa fase, il software di installazione dell'appliance StorageGRID viene aggiornato. Questo processo automatizzato garantisce che la versione del programma di installazione dell'appliance StorageGRID rimanga sincronizzata con la versione del software StorageGRID.

- Riavvio in corso



Alcuni modelli di appliance potrebbero riavviarsi più volte per aggiornare il firmware e il BIOS.

- Esecuzione dei passaggi dopo il riavvio
- Avvio dei servizi
- Fatto

6. Ripetere il [fase di approvazione](#) tutte le volte necessarie fino a quando tutti i nodi della griglia non sono stati aggiornati.

Aggiornamento completo

Quando tutti i nodi della griglia hanno completato le fasi di aggiornamento, l'attività **Upgrade other grid Node** (Aggiorna altri nodi della griglia) viene visualizzata come completata. Le restanti attività di aggiornamento vengono eseguite automaticamente in background.

Fasi

1. Non appena l'attività **Abilita funzionalità** sarà completata (fino a un'ora), puoi iniziare a usare la ["nuove funzionalità"](#) nella versione aggiornata di StorageGRID.

Una volta completate le **fasi finali dell'aggiornamento**, l'aggiornamento viene eseguito. Il primo passaggio, **Select Files**, viene visualizzato nuovamente con un banner verde di successo.

2. Verificare che le operazioni della griglia siano tornate alla normalità:
 - a. Verificare che i servizi funzionino normalmente e che non siano presenti avvisi imprevisti.
 - b. Verificare che le connessioni client al sistema StorageGRID funzionino come previsto.

Informazioni correlate

["Impatto del sistema durante l'aggiornamento"](#)

Risoluzione dei problemi di aggiornamento di StorageGRID

Se si verifica un errore durante l'esecuzione di un aggiornamento, potrebbe essere possibile risolvere il problema da soli. Se non riesci a risolvere un problema, raccogli tutte le informazioni possibili e contatta il supporto tecnico.

L'aggiornamento non viene completato

Le sezioni seguenti descrivono come eseguire il ripristino da situazioni in cui l'aggiornamento non è riuscito parzialmente.

Errori di controllo preliminare dell'aggiornamento

Per rilevare e risolvere i problemi, è possibile eseguire manualmente i controlli preliminari dell'aggiornamento

prima di avviare l'aggiornamento effettivo. La maggior parte degli errori di pre-controllo fornisce informazioni su come risolvere il problema.

Errori di provisioning

Se il processo di provisioning automatico non riesce, contattare il supporto tecnico.

Il nodo Grid si blocca o non si avvia

Se un nodo grid si blocca durante il processo di aggiornamento o non si avvia correttamente al termine dell'aggiornamento, contattare il supporto tecnico per investigare e correggere eventuali problemi sottostanti.

L'acquisizione o il recupero dei dati viene interrotto

Se l'acquisizione o il recupero dei dati viene interrotto inaspettatamente quando non si aggiorna un nodo di griglia, contattare il supporto tecnico.

Errori di aggiornamento del database

Se l'aggiornamento del database non riesce e viene visualizzato un errore, riprovare. Se il problema persiste, contattare il supporto tecnico.

Informazioni correlate

["Verifica delle condizioni del sistema prima dell'aggiornamento del software"](#)

Problemi dell'interfaccia utente

Potrebbero verificarsi problemi con Grid Manager o con il tenant Manager durante o dopo l'aggiornamento.

Grid Manager visualizza più messaggi di errore durante l'aggiornamento

Se si aggiorna il browser o si accede a un'altra pagina di Grid Manager mentre il nodo amministrativo principale viene aggiornato, è possibile che vengano visualizzati più messaggi "503: Servizio non disponibile" e "problema di connessione al server". È possibile ignorare questi messaggi in modo sicuro, che smetteranno di essere visualizzati non appena il nodo viene aggiornato.

Se questi messaggi vengono visualizzati per più di un'ora dopo l'avvio dell'aggiornamento, potrebbe essersi verificato un problema che ha impedito l'aggiornamento del nodo di amministrazione primario. Se non riesci a risolvere il problema da solo, contatta il supporto tecnico.

L'interfaccia Web non risponde come previsto

Dopo l'aggiornamento del software StorageGRID, il gestore di rete o il tenant manager potrebbero non rispondere come previsto.

In caso di problemi con l'interfaccia Web:

- Assicurarsi di utilizzare un ["browser web supportato"](#).



Il supporto del browser in genere cambia per ogni release di StorageGRID.

- Cancellare la cache del browser Web.

La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare nuovamente correttamente. Per istruzioni,

consultare la documentazione del browser Web.

Messaggi di errore "controllo disponibilità immagine Docker"

Quando si tenta di avviare il processo di upgrade, potrebbe essere visualizzato un messaggio di errore che indica che la suite di convalida del controllo di disponibilità dell'immagine Docker ha identificato i seguenti problemi. Tutti i problemi devono essere risolti prima di poter completare l'aggiornamento.

In caso di dubbi sulle modifiche necessarie per risolvere i problemi identificati, contattare il supporto tecnico.

Messaggio	Causa	Soluzione
Impossibile determinare la versione dell'aggiornamento. Il file di informazioni sulla versione di aggiornamento {file_path} non corrisponde al formato previsto.	Il pacchetto di aggiornamento è corrotto.	Caricare nuovamente il pacchetto di aggiornamento e riprovare. Se il problema persiste, contattare il supporto tecnico.
Impossibile trovare il file di informazioni sulla versione di aggiornamento {file_path}. Impossibile determinare la versione dell'aggiornamento.	Il pacchetto di aggiornamento è corrotto.	Caricare nuovamente il pacchetto di aggiornamento e riprovare. Se il problema persiste, contattare il supporto tecnico.
Impossibile determinare la versione della release attualmente installata su {node_name}.	Un file critico sul nodo è corrotto.	Contattare il supporto tecnico.
Errore di connessione durante il tentativo di elencare le versioni su {node_name}	Il nodo è offline o la connessione è stata interrotta.	Verificare che tutti i nodi siano in linea e raggiungibili dal nodo di amministrazione primario e riprovare.
L'host per il nodo {node_name} non ha caricato l'immagine StorageGRID {upgrade_version}. Prima di procedere con l'aggiornamento, è necessario installare immagini e servizi sull'host.	I pacchetti RPM o DEB per l'aggiornamento non sono stati installati sull'host in cui è in esecuzione il nodo oppure le immagini sono ancora in fase di importazione. Nota: questo errore si applica solo ai nodi in esecuzione come container su Linux.	Assicurarsi che i pacchetti RPM o DEB siano stati installati su tutti gli host Linux in cui sono in esecuzione i nodi. Assicurarsi che la versione sia corretta sia per il servizio che per il file di immagini. Attendere alcuni minuti e riprovare. Vedere "Linux: Installare il pacchetto RPM o DEB su tutti gli host" .
Errore durante il controllo del nodo {node_name}	Si è verificato un errore imprevisto.	Attendere alcuni minuti e riprovare.

Messaggio	Causa	Soluzione
Errore non rilevato durante l'esecuzione di controlli preliminari. {error_string}	Si è verificato un errore imprevisto.	Attendere alcuni minuti e riprovare.

Applicare la correzione rapida StorageGRID

Procedura di hotfix StorageGRID

Potrebbe essere necessario applicare una hotfix al sistema StorageGRID se vengono rilevati e risolti problemi relativi al software tra una versione e l'altra.

Le hotfix StorageGRID contengono modifiche software rese disponibili al di fuori di una release di funzionalità o patch. Le stesse modifiche sono incluse in una release futura. Inoltre, ogni release di hotfix contiene un rolup di tutti gli hotfix precedenti all'interno della funzionalità o della release di patch.

Considerazioni per l'applicazione di una correzione rapida

Non è possibile applicare una correzione rapida StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare una correzione rapida mentre è in esecuzione una procedura di decommissionamento, espansione o ripristino.



Se la procedura di decommissionamento di un nodo o di un sito è in pausa, è possibile applicare una correzione rapida in tutta sicurezza. Inoltre, potrebbe essere possibile applicare una correzione rapida durante le fasi finali di una procedura di aggiornamento di StorageGRID. Per ulteriori informazioni, consultare le istruzioni per l'aggiornamento del software StorageGRID.

Dopo aver caricato la correzione rapida in Grid Manager, la correzione rapida viene applicata automaticamente al nodo di amministrazione primario. Quindi, è possibile approvare l'applicazione della correzione rapida agli altri nodi nel sistema StorageGRID.

Se una correzione rapida non viene applicata a uno o più nodi, il motivo dell'errore viene visualizzato nella colonna Dettagli della tabella di avanzamento della correzione rapida. È necessario risolvere i problemi che hanno causato gli errori e riprovare l'intero processo. I nodi con un'applicazione della correzione rapida precedentemente riuscita verranno ignorati nelle applicazioni successive. È possibile riprovare il processo di hotfix tutte le volte necessarie fino a quando tutti i nodi non sono stati aggiornati. Per completare l'applicazione, la correzione rapida deve essere installata correttamente su tutti i nodi della griglia.

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

Modalità di applicazione degli hotfix per il ripristino e l'espansione

Dopo che un hotfix è stato applicato alla tua grid, il nodo Admin primario o un nodo Admin non primario installa automaticamente la stessa versione dell'hotfix su qualsiasi nodo ripristinato tramite operazioni di recovery o aggiunto in un'espansione. Puoi recuperare qualsiasi nodo (incluso il nodo Admin primario) quando hai effettuato l'accesso a un nodo Admin non primario. Se recuperi un nodo da un nodo Admin non primario, quel nodo Admin applica l'hotfix al nodo recuperato.

Se devi ripristinare il nodo Admin primario dal suo programma di installazione di StorageGRID, devi installare

manualmente la versione corretta di StorageGRID e poi applicare l'hotfix. La versione finale di StorageGRID del nodo Admin primario deve corrispondere alla versione degli altri nodi nella grid.

L'esempio seguente illustra come applicare una hotfix durante il ripristino del nodo Admin primario mentre sei connesso al nodo Admin non primario:

1. Si supponga che la griglia stia eseguendo una versione di StorageGRID 11.A.B con la correzione rapida più recente. La "versione griglia" è 11.A.B.y.
2. Si verifica un errore nel nodo di amministrazione primario.
3. Il nodo di amministrazione primario viene ridistribuita utilizzando StorageGRID 11.A.B ed è possibile eseguire la procedura di ripristino.



In base alle esigenze della versione grid, è possibile utilizzare una release minore durante la distribuzione del nodo; non è necessario implementare prima la release principale.

4. Quindi, applicare la correzione rapida 11.A.B.y al nodo di amministrazione primario.

Come StorageGRID è influenzato quando si applica un hotfix

Quando si applica una hotfix, è necessario comprendere in che modo il sistema StorageGRID verrà influenzato.

Le correzioni rapide di StorageGRID non provocano interruzioni

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante tutto il processo di hotfix. Se si approvano tutti i nodi dello stesso tipo per la correzione rapida (ad esempio, nodi di archiviazione), i nodi vengono abbassati uno alla volta, quindi non c'è tempo quando tutti i nodi della griglia o tutti i nodi della griglia di un determinato tipo non sono disponibili.

Per consentire la disponibilità continua, assicurarsi che il criterio ILM contenga regole che specificano la memorizzazione di più copie di ciascun oggetto. È inoltre necessario assicurarsi che tutti i client S3 esterni siano configurati per inviare richieste a uno dei seguenti:

- Un indirizzo IP virtuale del gruppo ad alta disponibilità (ha)
- Bilanciamento del carico di terze parti ad alta disponibilità
- Nodi gateway multipli per ogni client
- Più nodi di storage per ogni client

Le applicazioni client potrebbero riscontrare interruzioni a breve termine

Il sistema StorageGRID è in grado di acquisire e recuperare i dati dalle applicazioni client durante l'intero processo di hotfix; tuttavia, le connessioni client a singoli nodi gateway o nodi di storage potrebbero essere temporaneamente interrotte se la hotfix deve riavviare i servizi su tali nodi. La connettività verrà ripristinata al termine del processo di hotfix e i servizi riprenderanno sui singoli nodi.

Potrebbe essere necessario pianificare il downtime per applicare una correzione rapida se la perdita di connettività per un breve periodo non è accettabile. È possibile utilizzare l'approvazione selettiva per pianificare l'aggiornamento di determinati nodi.



È possibile utilizzare più gateway e gruppi ad alta disponibilità (ha) per fornire il failover automatico durante il processo di hotfix. Vedere le istruzioni per ["configurazione di gruppi ad alta disponibilità"](#).

Potrebbero essere attivati avvisi e notifiche SNMP

Gli avvisi e le notifiche SNMP potrebbero essere attivati al riavvio dei servizi e quando il sistema StorageGRID funziona come ambiente a versione mista (alcuni nodi di griglia che eseguono una versione precedente, mentre altri sono stati aggiornati a una versione successiva). In generale, al termine della correzione rapida, gli avvisi e le notifiche verranno deselezionati.

Le modifiche alla configurazione sono limitate

Quando si applica una correzione rapida a StorageGRID:

- Non apportare modifiche alla configurazione della griglia (ad esempio, specificando subnet Grid Network o approvando i nodi della griglia in sospeso) fino a quando la correzione rapida non è stata applicata a tutti i nodi.
- Non aggiornare la configurazione ILM fino a quando la correzione rapida non è stata applicata a tutti i nodi.

Procurare i materiali necessari per un hotfix StorageGRID

Prima di applicare una hotfix, è necessario procurarsi tutti i materiali necessari.

Elemento	Note
File di hotfix StorageGRID	È necessario scaricare il file di hotfix StorageGRID.
• Porta di rete • "Browser Web supportato" • Client SSH (ad esempio, putty)	
File del pacchetto di ripristino (.zip)	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 del pacchetto di ripristino e salvarla in un luogo sicuro. Il file del pacchetto di ripristino 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 <code>Passwords.txt</code> il file fa parte del pacchetto di ripristino .zip file.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è elencata nel <code>Passwords.txt</code> file.
Documentazione correlata	<code>readme.txt</code> file per la correzione rapida. Questo file è incluso nella pagina di download della correzione rapida. Assicurarsi di esaminare attentamente il <code>readme</code> file prima di applicare la correzione rapida.

Scarica un file hotfix di StorageGRID

Prima di applicare la correzione rapida, è necessario scaricare il file della correzione rapida.

Fasi

1. Andare a ["Download NetApp: StorageGRID"](#).
2. Selezionare la freccia verso il basso sotto **Software disponibile** per visualizzare un elenco di hotfix disponibili per il download.



Le versioni dei file hotfix hanno il formato: 11.4.x.y.

3. Esaminare le modifiche incluse nell'aggiornamento.



Se si dispone di ["Ripristinato nodo amministratore primario"](#) una correzione rapida ed è necessario applicarla, selezionare la stessa versione di correzione rapida installata sugli altri nodi della griglia.

- a. Selezionare la versione della correzione rapida che si desidera scaricare e selezionare **Go**.
- b. Accedi utilizzando il nome utente e la password del tuo account NetApp.
- c. Leggere e accettare il Contratto di licenza con l'utente finale.

Viene visualizzata la pagina di download della versione selezionata.

- d. Scaricare il file della correzione rapida `readme.txt` per visualizzare un riepilogo delle modifiche incluse nella correzione rapida.

4. Selezionare il pulsante di download per la correzione rapida e salvare il file.



Non modificare il nome del file.



Se si utilizza un dispositivo macOS, il file della correzione rapida potrebbe essere salvato automaticamente come `.txt` file. In tal caso, è necessario rinominare il file senza l' `.txt` estensione.

5. Selezionare una posizione per il download e selezionare **Salva**.

Verificare le condizioni del sistema prima di applicare un hotfix StorageGRID

Verificare che il sistema sia pronto per la correzione rapida.

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Se possibile, assicurarsi che il sistema funzioni correttamente e che tutti i nodi della rete siano collegati alla rete.

I nodi connessi presentano un segno di spunta verde  nella pagina Nodi.

3. Controllare e risolvere eventuali avvisi correnti, se possibile.

4. Assicurarsi che non siano in corso altre procedure di manutenzione, ad esempio una procedura di upgrade, recovery, espansione o decommissionamento.

Prima di applicare una correzione rapida, attendere il completamento delle procedure di manutenzione attive.

Non è possibile applicare una correzione rapida StorageGRID quando è in esecuzione un'altra procedura di manutenzione. Ad esempio, non è possibile applicare una correzione rapida mentre è in esecuzione una procedura di decommissionamento, espansione o ripristino.



Se si ["la procedura di decommissionamento è in pausa"](#) tratta di un nodo o di un sito, è possibile applicare una correzione rapida. Inoltre, potrebbe essere possibile applicare una correzione rapida durante le fasi finali di una procedura di aggiornamento di StorageGRID. Vedere le istruzioni per ["Aggiornamento del software StorageGRID"](#).

Applicare un hotfix in StorageGRID

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

Prima di iniziare

- È stata esaminata la ["considerazioni per l'applicazione di una correzione rapida"](#).
- Si dispone della passphrase di provisioning.
- Si dispone dell'autorizzazione di accesso root o di manutenzione.

A proposito di questa attività

- È possibile ritardare l'applicazione di una hotfix a un nodo, ma il processo di hotfix non viene completato fino a quando non si applica la hotfix a tutti i nodi.
- Non è possibile eseguire un aggiornamento del software StorageGRID o del sistema operativo SANtricity fino a quando non viene completata la procedura di correzione rapida.

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Selezionare **Manutenzione > Sistema > Aggiornamento software**.

Viene visualizzata la pagina Software Update (aggiornamento software).

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 **Apply Hotfix** (Applica correzione rapida).

Viene visualizzata la pagina Hotfix StorageGRID.

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. Selezionare il file hotfix scaricato dal NetApp Support Site.

- a. Selezionare **Sfoglia**.
- b. Individuare e selezionare il file.

`hotfix-install-version`

- c. Selezionare **Apri**.

Il file viene caricato. Al termine del caricamento, il nome del file viene visualizzato nel campo Dettagli.



Non modificare il nome del file perché fa parte del processo di verifica.

5. Inserire la passphrase di provisioning nella casella di testo.

Il pulsante **Start** viene attivato.

6. Selezionare **Start**.

Viene visualizzato un avviso che indica che la connessione del browser potrebbe andare persa temporaneamente quando i servizi sul nodo di amministrazione primario vengono riavviati.

7. Selezionare **OK** per avviare l'applicazione della correzione rapida al nodo di amministrazione primario.

All'avvio della correzione rapida:

a. Vengono eseguite le convalide degli hotfix, inclusa la verifica della firma del codice.



Se vengono segnalati errori, risolverli, caricare nuovamente il file di correzione rapida e selezionare di nuovo **Avvia**.

b. Viene visualizzata la tabella di avanzamento dell'installazione della correzione rapida.

Questa tabella mostra tutti i nodi della griglia e la fase corrente dell'installazione della correzione rapida per ciascun nodo. I nodi nella tabella sono raggruppati per tipo (nodi amministrativi, nodi gateway e nodi storage).

c. La barra di avanzamento raggiunge il completamento, quindi il nodo amministrativo primario viene visualizzato come "completo".

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, ordinare gli elenchi di nodi in ciascun raggruppamento in ordine crescente o decrescente per **Sito**, **Nome**, **avanzamento**, **fase** o **Dettagli**. In alternativa, inserire un termine nella casella **Search** per cercare nodi specifici.

9. Approvare i nodi della griglia pronti per l'aggiornamento. I nodi approvati dello stesso tipo vengono aggiornati uno alla volta.



Non approvare la correzione rapida per un nodo a meno che non si sia certi che il nodo sia pronto per l'aggiornamento. Quando la correzione rapida viene applicata a un nodo Grid, alcuni servizi su tale nodo potrebbero essere riavviati. Queste operazioni potrebbero causare interruzioni del servizio per i client che comunicano con il nodo.

- Selezionare uno o più pulsanti **approva** per aggiungere uno o più singoli nodi alla coda degli aggiornamenti rapidi.
- Selezionare il pulsante **approva tutto** all'interno di ciascun gruppo per aggiungere tutti i nodi dello stesso tipo alla coda degli hotfix. Se sono stati immessi criteri di ricerca nella casella **Cerca**, il pulsante **approva tutto** si applica a tutti i nodi selezionati dai criteri di ricerca.



Il pulsante **approva tutto** nella parte superiore della pagina approva tutti i nodi elencati nella pagina, mentre il pulsante **approva tutto** nella parte superiore di un raggruppamento di tabelle approva solo tutti i nodi di quel gruppo. Se l'ordine in cui i nodi vengono aggiornati è importante, approvare i nodi o i gruppi di nodi uno alla volta e attendere il completamento dell'aggiornamento su ciascun nodo prima di approvare i nodi successivi.

- Selezionare il pulsante di primo livello **approva tutto** nella parte superiore della pagina per aggiungere tutti i nodi della griglia alla coda degli aggiornamenti rapidi.



È necessario completare la correzione rapida StorageGRID prima di poter avviare un aggiornamento software diverso. Se non si riesce a completare la correzione rapida, contattare il supporto tecnico.

- Selezionare **Remove** o **Remove All** per rimuovere un nodo o tutti i nodi dalla coda di hotfix.

Quando Stage va oltre "in coda", il pulsante **Rimuovi** è nascosto e non è più possibile rimuovere il nodo dal processo di correzione rapida.

Storage Nodes - 1 out of 9 completed						Approve All	Remove All
						Search 	
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. Attendere che la correzione rapida venga applicata a ciascun nodo della griglia approvato.

Una volta che la correzione rapida è stata installata correttamente su tutti i nodi, la tabella di avanzamento

dell'installazione della correzione rapida si chiude. Un banner verde mostra la data e l'ora in cui la correzione rapida è stata completata.

11. Se la correzione rapida non può essere applicata a nessun nodo, esaminare l'errore per ciascun nodo, risolvere il problema e ripetere la procedura.

La procedura non è completa fino a quando la correzione rapida non viene applicata correttamente a tutti i nodi. È possibile riprovare il processo di correzione rapida tutte le volte necessarie fino al completamento.

Configurare e gestire un sistema StorageGRID

Amministrare StorageGRID

Guida rapida per l'amministrazione di StorageGRID

Seguire queste istruzioni per configurare e amministrare un sistema StorageGRID.



Assicurati di avere una conoscenza generale del sistema StorageGRID e una conoscenza piuttosto approfondita delle shell dei comandi Linux, delle reti e della configurazione dell'hardware del server.

1

Inizia a usare Grid Manager

- ["Scopri i passaggi fondamentali per utilizzare l'interfaccia utente di Grid Manager"](#)
- ["Scopri le informazioni sulla licenza"](#)
- ["Scopri come utilizzare l'API di gestione della griglia"](#)

2

Controlla l'accesso a StorageGRID

- ["Scopri passphrase, password e autorizzazioni"](#)
- ["Configura identity federation"](#)
- ["Gestire i gruppi di amministratori"](#)
- ["Gestire gli utenti"](#)
- ["Configura il single sign-on \(SSO\)"](#)

3

Usa la federazione di grid

- ["Configura le connessioni della federazione di griglia"](#)
- ["Scopri la sincronizzazione dell'account"](#)
- ["Scopri la replica cross-grid"](#)
- ["Configura lo spazio dei nomi globale"](#)

4

Gestisci la sicurezza

- ["Esaminare i metodi di crittografia StorageGRID"](#)
- ["Gestire i certificati"](#)
- ["Configurare le impostazioni di sicurezza"](#)
- ["Configurare i server di gestione delle chiavi"](#)
- ["Gestire le impostazioni del proxy"](#)
- ["Firewall di controllo"](#)

5**Gestisci i tenant**

- ["Scopri e gestisci gli account tenant"](#)
- ["Gestire i servizi della piattaforma per i tenant"](#)
- ["Manage S3 \(Gestisci S3\): Selezionare per gli account tenant"](#)

6**Configura le connessioni client**

- ["Scopri la sicurezza per i client S3"](#)
- ["Utilizzare l'installazione guidata S3"](#)
- ["Gestire i gruppi ad alta disponibilità"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

7**Gestisci reti e connessioni**

- ["Configurare le impostazioni di rete"](#)
- ["Configurare le interfacce VLAN"](#)
- ["Gestire le policy di classificazione del traffico"](#)
- ["Gestire i costi di collegamento"](#)

8**Gestisci i nodi**

- ["Gestire i nodi di storage"](#)
- ["Gestire i nodi di amministrazione"](#)

Inizia subito con Grid Manager**Requisiti del browser web per StorageGRID**

È necessario utilizzare un browser Web supportato.

Browser Web	Versione minima supportata
Google Chrome	138
Microsoft Edge	138
Mozilla Firefox	140

Imposta la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024

Larghezza del browser	Pixel
Ottimale	1280

Sign in al StorageGRID Grid Manager

Per accedere alla pagina di accesso di Grid Manager, immettere il nome di dominio completo (FQDN) o l'indirizzo IP di un nodo amministratore nella barra degli indirizzi di un browser Web supportato.

Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. Per gestire il sistema StorageGRID, è possibile accedere a Grid Manager da qualsiasi nodo amministrativo. Tuttavia, alcune procedure di manutenzione possono essere eseguite solo dal nodo amministrativo primario.

Connettersi al gruppo ha

Se i nodi di amministrazione sono inclusi in un gruppo ad alta disponibilità (ha), la connessione viene eseguita utilizzando l'indirizzo IP virtuale del gruppo ha o un nome di dominio completo che viene mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario deve essere selezionato come interfaccia principale del gruppo, in modo che quando si accede a Grid Manager, si accede al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile. Vedere ["Gestire i gruppi ad alta disponibilità"](#).

Utilizzare SSO

I passaggi di accesso sono leggermente diversi se ["È stato configurato Single Sign-on \(SSO\)"](#).

Accedi a Grid Manager sul primo nodo di amministrazione

Prima di iniziare

- Si dispone delle credenziali di accesso.
- Si sta utilizzando un ["browser web supportato"](#).
- I cookie sono attivati nel browser Web.
- L'utente appartiene a un gruppo di utenti che dispone di almeno un'autorizzazione.
- Hai l'URL per Grid Manager:

```
https://FQDN_or_Admin_Node_IP/
```

È possibile utilizzare il nome di dominio completo, l'indirizzo IP di un nodo amministratore o l'indirizzo IP virtuale di un gruppo ha di nodi amministratore.

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/
```

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per Grid Manager.

3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser. Vedere ["Gestire i certificati di sicurezza"](#).
4. Accedi a Grid Manager.

La schermata di accesso visualizzata dipende dalla configurazione di SSO (Single Sign-on) per StorageGRID.

Non si utilizza SSO

- a. Immettere il nome utente e la password per Grid Manager.
- b. Selezionare **Accedi**.

Utilizzo di SSO

- Se StorageGRID utilizza SSO ed è la prima volta che si accede all'URL dal browser:
 - i. Selezionare **Accedi**. È possibile lasciare lo 0 nel campo account.
 - ii. Inserisci le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Ad esempio, se StorageGRID utilizza SSO e in precedenza hai effettuato l'accesso a Grid Manager o a un account tenant:

- A. Inserire **0** (l'ID account per Grid Manager) o selezionare **Grid Manager** se compare nell'elenco degli account recenti.
- B. Selezionare **Accedi**.
- C. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Una volta effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per informazioni sulle informazioni fornite, vedere ["Visualizzare e gestire la dashboard"](#).

Accedere a un altro nodo amministratore

Per accedere a un altro nodo amministratore, procedere come segue.

Non si utilizza SSO

Fasi

1. Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta come richiesto.
2. Immettere il nome utente e la password per Grid Manager.
3. Selezionare **Accedi**.

Utilizzo di SSO

Se StorageGRID utilizza SSO ed è stato effettuato l'accesso a un nodo amministratore, è possibile accedere ad altri nodi amministrativi senza dover effettuare nuovamente l'accesso.

Fasi

1. Inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione nella barra degli indirizzi del browser.
2. Se la sessione SSO è scaduta, immettere nuovamente le credenziali.

Disconnettiti da StorageGRID Grid Manager

Una volta terminato l'utilizzo di Grid Manager, è necessario disconnettersi per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Selezionare il nome utente nell'angolo in alto a destra.
2. Selezionare **Disconnetti**.

Opzione	Descrizione
SSO non in uso	Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid Manager. Nota: se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.
SSO attivato	Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. Grid Manager è elencato come predefinito nell'elenco a discesa Recent Accounts (account recenti) e il campo account ID (ID account) mostra 0. Nota: se l'SSO è abilitato e hai effettuato l'accesso anche a Tenant Manager, devi anche "disconnettersi dall'account tenant" A "Disconnettersi da SSO" .

Cambia la password di StorageGRID Grid Manager

Gli utenti locali di Grid Manager possono modificare la propria password.

Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

Se si accede a StorageGRID come utente federato o se è attivato il Single Sign-on (SSO), non è possibile modificare la password in Grid Manager. È invece necessario modificare la password nell'origine dell'identità esterna, ad esempio Active Directory o OpenLDAP.

Fasi

1. Dall'intestazione Grid Manager, selezionare **Nome > Modifica password**.
2. Inserire la password corrente.
3. Digitare una nuova password.

La password deve contenere almeno 8 e non più di 32 caratteri. Le password distinguono tra maiuscole e minuscole.

4. Immettere nuovamente la nuova password.
5. Selezionare **Salva**.

Visualizzare le informazioni sulla licenza StorageGRID

Se necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID, ad esempio la capacità di storage massima del grid.

Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

In caso di problemi con la licenza software per questo sistema StorageGRID, la scheda di stato dello stato di salute sul dashboard include un'icona di stato della licenza e un collegamento **licenza**. Il numero indica il numero di problemi relativi alla licenza.



Fasi

1. Accedere alla pagina License (licenza) effettuando una delle seguenti operazioni:
 - Selezionare **Manutenzione > Sistema > Licenza**.
 - Dalla scheda Health status (Stato) sul dashboard, selezionare l'icona License status (Stato licenza) o il collegamento **License** (licenza).

Questo collegamento viene visualizzato solo in caso di problemi con la licenza.

2. Visualizzare i dettagli di sola lettura per la licenza corrente:
 - ID sistema StorageGRID, che è il numero di identificazione univoco per l'installazione di StorageGRID
 - Numero di serie della licenza
 - Tipo di licenza, **Perpetual** o **Subscription**
 - Capacità di storage concessa in licenza del grid
 - Capacità di storage supportata
 - Data di fine della licenza. **N/A** appare per una licenza perpetua.
 - Data di fine supporto

Questa data viene letta dal file di licenza corrente e potrebbe non essere aggiornata se hai esteso o rinnovato il contratto di supporto dopo aver ottenuto il file di licenza. Per aggiornare questo valore, consulta ["Aggiornare le informazioni sulla licenza StorageGRID"](#). Puoi anche visualizzare la data di fine contratto effettiva utilizzando Digital Advisor.

- Contenuto del file di testo della licenza

Aggiornare le informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni di licenza per il sistema StorageGRID in qualsiasi momento in cui i termini della licenza cambiano. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista ulteriore capacità di storage per il grid.

Prima di iniziare

- Si dispone di un nuovo file di licenza da applicare al sistema StorageGRID.
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Si dispone della passphrase di provisioning.

Fasi

1. Selezionare **Manutenzione > Sistema > Licenza**.
2. Nella sezione Aggiorna licenza, selezionare **Sfoglia**.
3. Individuare e selezionare il nuovo file di licenza (.txt).

Il nuovo file di licenza viene validato e visualizzato.

4. Inserire la passphrase di provisioning.
5. Selezionare **Salva**.

Utilizzare la API

Utilizzare l'API di gestione della griglia StorageGRID

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management invece dell'interfaccia utente di Grid Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

Risorse di alto livello

L'API Grid Management fornisce le seguenti risorse di primo livello:

- `/grid`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate.
- `/org`: L'accesso è limitato agli utenti che appartengono a un gruppo LDAP locale o federato per un account tenant. Per ulteriori informazioni, vedere ["Utilizzare un account tenant"](#).
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

Emettere richieste API

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di eseguire operazioni in tempo reale in StorageGRID con l'API.

L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).



Tutte le operazioni API eseguite utilizzando la pagina Web documentazione API sono operazioni in tempo reale. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Dall'installazione di Grid Manager, seleziona l'icona di aiuto  e seleziona **Documentazione API**.
2. Per eseguire un'operazione con l'API privata, selezionare **Vai alla documentazione API privata** nella pagina API di gestione StorageGRID.

Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Selezionare l'operazione desiderata.

Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, ad esempio GET, PUT, UPDATE ed DELETE.

4. Selezionare un'azione HTTP per visualizzare i dettagli della richiesta, tra cui l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le

possibili risposte.

groups Operations on groups

GET

/grid/groups

Lists Grid Administrator Groups

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>

- Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
- Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.
- Selezionare **Provalo**.
- Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
- Selezionare **Esegui**.

10. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Operazioni Grid Management API in StorageGRID

L'API Grid Management organizza le operazioni disponibili nelle seguenti sezioni.



Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **Account:** Operazioni per la gestione degli account del tenant di storage, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.
- **Alert-history:** Operazioni su avvisi risolti.
- **Ricevitori di avvisi:** Operazioni sui destinatari di notifiche di avvisi (e-mail).
- **Alert-rules:** Operazioni sulle regole di allerta.
- **Silenzi di allerta:** Operazioni di silenzi di allerta.
- **Alerts:** Operazioni sugli avvisi.
- **Audit:** Operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth:** Operazioni per l'autenticazione della sessione utente.

L'API Grid Management supporta lo schema di autenticazione del token del bearer. Per accedere, 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 richieste API successive ("Authorization: Bearer *token*"). Il token scade dopo 16 ore.



Se per il sistema StorageGRID è attivato il single sign-on, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "autenticazione nell'API se è attivato il single sign-on".

Per informazioni sul miglioramento della protezione dell'autenticazione, vedere "protezione contro la contraffazione delle richieste tra siti".

- **Certificati-client:** Operazioni per configurare i certificati client in modo che sia possibile accedere in modo sicuro a StorageGRID utilizzando strumenti di monitoraggio esterni.
- **Config:** Operazioni relative alla release del prodotto e alle versioni dell'API Grid Management. È possibile elencare la versione del prodotto e le principali versioni dell'API Grid Management supportate da tale release ed è possibile disattivare le versioni obsolete dell'API.
- **Disattivato-funzioni:** Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **dns-servers:** Operazioni per elencare e modificare i server DNS esterni configurati.
- **Dettagli unità:** Operazioni su unità per modelli di appliance di archiviazione specifici.
- **Nomi-dominio-endpoint:** Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **Erase coding:** Operazioni sui profili di erasure coding.
- **Espansione:** Operazioni di espansione (a livello di procedura).
- **Expansion-node:** Operazioni di espansione (a livello di nodo).
- **Expansion-sites:** Operazioni di espansione (a livello di sito).
- **Grid-networks:** Operazioni per elencare e modificare l'elenco Grid Network.
- **Grid-password:** Operazioni per la gestione delle password grid.

- **Gruppi:** Operazioni per gestire i gruppi di amministratori di griglia locali e recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **Identity-source:** Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm:** Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **Procedure in corso:** Recupera le procedure di manutenzione attualmente in corso.
- **Licenza:** Operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs:** Operazioni per la raccolta e il download dei file di log.v
- **Metriche:** Operazioni su metriche StorageGRID, incluse query metriche istantanee in un singolo punto nel tempo e query metriche di intervallo in un intervallo di tempo. L'API Grid Management utilizza lo strumento di monitoraggio dei sistemi Prometheus come origine dei dati back-end. Per informazioni sulla creazione di query Prometheus, visitare il sito Web Prometheus.



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

- **Node-details:** Operazioni sui dettagli del nodo.
- **Node-Health:** Operazioni sullo stato di salute del nodo.
- **Node-storage-state:** Operazioni sullo stato dello storage del nodo.
- **ntp-servers:** Operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects:** Operazioni su oggetti e metadati di oggetti.
- **Recovery:** Operazioni per la procedura di recovery.
- **recovery-package:** Operazioni per scaricare il pacchetto di ripristino.
- **Regioni:** Operazioni per visualizzare e creare regioni.
- **s3-Object-lock:** Operazioni sulle impostazioni generali di blocco oggetti S3.
- **Server-certificate:** Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp:** Operazioni sulla configurazione SNMP corrente.
- **Filigrane-archiviazione:** Filigrane del nodo di archiviazione.
- **Classi di traffico:** Operazioni per le policy di classificazione del traffico.
- **Untrusted-client-network:** Operazioni sulla configurazione Untrusted Client Network.
- **Utenti:** Operazioni per visualizzare e gestire gli utenti di Grid Manager.

Versioning dell'API Grid Management in StorageGRID

L'API Grid Management utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate

modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.



È possibile configurare le versioni supportate. Per ulteriori informazioni, vedere la sezione **config** della documentazione Swagger API "[API di Grid Management](#)". È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare la GET `/versions` richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione API utilizzando un parametro di percorso (/api/v4) o un'intestazione (Api-Version: 4. Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Proteggi contro gli attacchi Cross-Site Request Forgery (CSRF) in StorageGRID

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare il `csrfToken` parametro su `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 true, un `GridCsrfToken` cookie viene impostato con un valore casuale per i login al Grid Manager e il `AccountCsrfToken` cookie viene impostato con un valore casuale per i login al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- L' `X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo codificato in forma: Un `csrfToken` parametro del corpo della richiesta codificato in forma.

Per ulteriori esempi e dettagli, consultare la documentazione API online.



Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione `"Content-Type: Application/json"` per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare l'API se è attivato il Single Sign-on

Utilizzare l'API StorageGRID se il single sign-on è abilitato (Active Directory)

Se hai [SSO \(Single Sign-on\) configurato e abilitato](#) 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.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(`./rpms` per RHEL, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).
- Un esempio di workflow di richieste di curl.

Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: A valid SubjectConfirmation was not found on this Response.



L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: Unsupported SAML version.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare `storagegrid-ssoauth.py` lo script Python. Andare alla fase 2.
 - USA richieste di curl. Andare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` lo script, passare lo script all'interprete Python ed eseguire lo script.

Quando richiesto, inserire i valori per i seguenti argomenti:

- Il metodo SSO. Immettere ADFS o adfs.
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID
- L'indirizzo per StorageGRID
- L'ID account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```



Per accedere all'API Grid Management, utilizzare 0 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 con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
  sSl%2BfQ33cvfwA%3D&RelayState=12345",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

- d. Ottenere un URL completo che includa l'ID della richiesta del client da ad FS.

Un'opzione consiste nel richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRTOMwFIZfhh...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salvare l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Inviare le credenziali all'azione del modulo della risposta precedente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.



Se l'autenticazione a più fattori (MFA) è attivata per il sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTOMwFIZfhh...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. Salvare il MSISAuth cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

- h. Inviare una richiesta GET alla posizione specificata con i cookie del POST di autenticazione.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni delle risposte conterranno le informazioni della sessione di ad FS per un utilizzo successivo della disconnessione e il corpo della risposta conterrà la risposta SAMLin un campo di forma nascosto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFXVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThtMDgtNDRkZC04Yzg5LTQ3ND
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="PHNhbWxwOlJlc3Bvb3N1scDpsZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

- i. Salvare il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```


- j. Utilizzando il salvato `SAMLResponse`, eseguire una richiesta `StorageGRID/api/saml-response` per generare un token di autenticazione `StorageGRID`.

Per `RelayState`, utilizzare l'ID `account tenant` o 0 se si desidera accedere all'API di gestione 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. Salvare il token di autenticazione nella risposta come `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

È ora possibile utilizzare `MYTOKEN` per altre richieste, in modo simile a come si userebbe l'API se non fosse utilizzato SSO.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management. Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API `StorageGRID` disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da `StorageGRID`, che richiede un token bearer `StorageGRID` valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
  "apiVersion": "3.0",
  "data":
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2018-11-20T22:20:30.839Z",
  "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018 22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

Una 204 No Content risposta indica che l'utente è stato disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzare l'API StorageGRID se single sign-on è abilitato (Entra ID)

Se hai [SSO \(Single Sign-on\) configurato e abilitato](#) e utilizzi Entra ID come provider SSO, puoi utilizzare due script di esempio per ottenere un token di autenticazione valido per la Grid Management API o la Tenant Management API.

Sign in all'API se è abilitato l'accesso singolo dell'ID Entra

Queste istruzioni si applicano se si utilizza Entra ID come provider di identità SSO

Prima di iniziare

- Si conoscono l'indirizzo e-mail SSO e la password di un utente federato che appartiene a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- ``storagegrid-ssoauth-azure.py`` Lo script Python
- `Lo storagegrid-ssoauth-azure.js` script Node.js

Entrambi gli script si trovano nella directory dei file di installazione StorageGRID(`./rpms` per RHEL, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).

Per scrivere la tua integrazione API con Entra ID, 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 Entra ID 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 estrarre l'interfaccia Entra ID SSO.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version.`

Fasi

1. Installare le dipendenze richieste, come indicato di seguito:

- a. Installare Node.js (vedere "<https://nodejs.org/en/download/>").
- b. Installare i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO dell'ID Entra.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):
 - L'indirizzo email SSO utilizzato per accedere a Entra ID
 - L'indirizzo per StorageGRID
 - L'ID account tenant, se si desidera accedere all'API di gestione tenant
4. Quando richiesto, inserisci la password e preparati a fornire un'autorizzazione MFA a Entra ID, 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 utilizzando Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'immissione di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

Utilizzare l'API StorageGRID se il single sign-on è abilitato (PingFederate)

Se hai "[SSO \(Single Sign-on\) configurato e abilitato](#)" 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.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- IL `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione StorageGRID(`./rpms` per RHEL, `./debs` per Ubuntu o Debian, e `./vsphere` per VMware).
- Un esempio di workflow di richieste di curl.

Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: `A valid SubjectConfirmation was not found on this Response.`



L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version.`

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare `storagegrid-ssoauth.py` lo script Python. Andare alla fase 2.
 - USA richieste di curl. Andare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` lo script, passare lo script all'interprete Python ed eseguire lo script.

Quando richiesto, inserire i valori per i seguenti argomenti:

- Il metodo SSO. È possibile inserire qualsiasi variazione di "pingfederate" (PINGFEDERATE, pingfederate e così via).
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID. Questo campo non viene utilizzato per PingFederate. È possibile lasciare vuoto il campo o inserire un valore qualsiasi.
- L'indirizzo per StorageGRID
- L'ID account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****

*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Per accedere all'API Grid Management, utilizzare 0 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 con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
  "apiVersion": "3.0",
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
  "responseTime": "2018-11-06T16:30:23.355Z",
  "status": "success"
}
```

- c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Esportare la risposta e il cookie e visualizzare la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Esportare il valore 'pf.adapterId' e visualizzare la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esportare il valore 'href' (rimuovere la barra finale /) e visualizzare la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esportare il valore "azione":

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia cookie con credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salvare il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbwXwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato SAMLResponse, eseguire una richiesta StorageGRID/api/saml-response per generare un token di autenticazione StorageGRID.

Per RelayState, utilizzare l'ID account tenant o 0 se si desidera accedere all'API di gestione 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. Salvare il token di autenticazione nella risposta come MYTOKEN.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

È ora possibile utilizzare MYTOKEN per altre richieste, in modo simile a come si userebbe l'API se non fosse utilizzato SSO.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management. Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API StorageGRID disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```


2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-  
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found  
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-  
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256  
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \  
-H "accept: application/json" \  
-H "Authorization: Bearer $MYTOKEN" \  
--include
```

Una 204 No Content risposta indica che l'utente è stato disconnesso.

```
HTTP/1.1 204 No Content
```

Disattiva le funzionalità di StorageGRID tramite l'API

È possibile utilizzare l'API di gestione griglia per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzione viene disattivata, non è possibile assegnare a nessuno le autorizzazioni per eseguire le attività correlate a tale funzione.

A proposito di questa attività

Il sistema Disattivato consente di impedire l'accesso a determinate funzioni del sistema StorageGRID. La disattivazione di una funzione è l'unico modo per impedire all'utente root o agli utenti appartenenti a gruppi di amministratori con autorizzazione **Root Access** di utilizzare tale funzione.

Per comprendere come questa funzionalità potrebbe essere utile, considerare il seguente scenario:

L'azienda A è un provider di servizi che affitta la capacità di storage del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei titolari di leasing, la Società A desidera garantire che i propri dipendenti non possano mai accedere a alcun account tenant dopo l'implementazione dell'account.

*L'azienda A è in grado di raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API Grid Management. Disattivando completamente la funzione **Cambia password root tenant** in Grid Manager (sia l'interfaccia utente che l'API), l'azienda A garantisce che gli utenti Admin, inclusi l'utente root e gli utenti appartenenti a gruppi con autorizzazione **root access**, non possano modificare la password per l'utente root di qualsiasi account tenant.*

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia. Vedere ["Utilizzare l'API Grid Management"](#).
2. Individuare l'endpoint Deactivate Features.
3. Per disattivare una funzione, ad esempio Modifica password root tenant, inviare un corpo all'API come segue:

```
{ "grid": { "changeTenantRootPassword": true } }
```

Al termine della richiesta, la funzione Modifica password root tenant viene disattivata. L'autorizzazione di gestione **Modifica password principale tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password principale per un tenant non riesce con "403 Proibito".

Riattivare le funzioni disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzione disattivata. Tuttavia, se si desidera evitare che le funzioni disattivate vengano riattivate, è possibile disattivare la funzione **ActivateFeatures**.



Impossibile riattivare la funzione **ActivateCaratures**. Se decidi di disattivare questa funzione, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzione disattivata. È necessario contattare il supporto tecnico per ripristinare eventuali funzionalità perse.

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia.
2. Individuare l'endpoint Deactivate Features.
3. Per riattivare tutte le funzioni, inviare un corpo all'API come segue:

```
{ "grid": null }
```

Una volta completata la richiesta, tutte le funzioni, inclusa la funzione Change tenant root password, vengono riattivate. L'autorizzazione di gestione **Change tenant root password** viene ora visualizzata nell'interfaccia utente e tutte le richieste API che tentano di modificare la password root per un tenant avranno esito positivo, presupponendo che l'utente disponga dell'autorizzazione di gestione **Root access** o **Change tenant root password**.



L'esempio precedente causa la riattivazione di *tutte* le funzioni disattivate. Se sono state disattivate altre funzioni che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzione Cambia password root tenant e continuare a disattivare l'autorizzazione di gestione storageAdmin, inviare la richiesta PUT:

```
{ "grid": {"storageAdmin": true} }
```

Controllo dell'accesso a StorageGRID

Controllare l'accesso a StorageGRID

Puoi controllare chi può accedere a StorageGRID e quali attività gli utenti possono svolgere creando o importando gruppi e utenti e assegnando le autorizzazioni a ciascun gruppo. Inoltre, puoi abilitare il single sign-on (SSO), creare certificati client, cambiare le password della grid e usare la verifica multi-admin.

Controlla l'accesso a Grid Manager

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

L'utilizzo di ["federazione delle 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 il supporto tecnico.

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

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

Attiva single sign-on

Il sistema StorageGRID supporta il single sign-on (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0) o OpenID Connect (OIDC). Dopo che ["Configurare e abilitare SSO"](#), tutti gli utenti devono essere autenticati da un identity provider esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.

Modificare la passphrase di provisioning

La passphrase di provisioning è necessaria per 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 ["modificare la passphrase"](#) come richiesto.

Modificare le password della console dei nodi

Ogni nodo nella griglia ha una password per la console del nodo, necessaria per accedere al nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. Se necessario, puoi ["modificare la password della console del nodo"](#) per ogni nodo.

Usa la verifica multi-amministratore

Puoi usare la verifica multi-amministratore (MAV) per assicurarti che alcune operazioni di StorageGRID possano essere eseguite solo dopo l'approvazione degli amministratori designati. MAV impedisce ad amministratori compromessi, malintenzionati o inesperti di apportare modifiche indesiderate o eliminare dati.

Modificare la passphrase di provisioning di StorageGRID

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 dei pacchetti 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

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone delle autorizzazioni di accesso Maintenance o Root.
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

La passphrase di provisioning è 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.

Fasi

1. Selezionare **Configurazione > Controllo accessi > Password griglia**.
2. In **Cambia passphrase di provisioning**, selezionare **effettua una modifica**
3. Inserire la passphrase di provisioning corrente.
4. Inserire la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili al maiuscolo/minuscolo.



Conservare la passphrase di provisioning in un luogo sicuro. È necessario per le procedure di installazione, ampliamento e manutenzione.

5. Immettere nuovamente la nuova passphrase e selezionare **Save** (Salva).

Al termine della modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo.



Provisioning passphrase successfully changed. Go to the [Recovery Package](#) to download a new Recovery Package.

6. Selezionare **Recovery Package** (pacchetto di ripristino).
7. 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 del pacchetto di ripristino consente di ripristinare il sistema in caso di errore.

Modificare le password della console dei nodi in StorageGRID

Ogni nodo della griglia ha una password della console del nodo, che puoi utilizzare per accedere al nodo. Per impostazione predefinita, ogni nodo ha una password univoca. È possibile modificare ciascuna password con una nuova password univoca oppure è possibile modificare la password di ogni nodo per utilizzare una password globale. Le password vengono memorizzate nel pacchetto di ripristino.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

Si utilizza una password della console del nodo per accedere a un nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. È possibile modificare le password della console del nodo utilizzando una di queste opzioni:

- Applica automaticamente password casuali a ciascun nodo
- Specificare e applicare una password globale a tutti i nodi
- Specificare e applicare una password univoca a uno o più nodi

Le password vengono memorizzate in un file aggiornato `Passwords.txt` file nel pacchetto di ripristino. Le password sono elencate nella colonna Password del file.



IL ["Password di accesso SSH"](#) poiché le chiavi SSH utilizzate per la comunicazione tra i nodi sono separate dalle password della console del nodo. Questa procedura non modifica le password di accesso SSH.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Controllo accessi > Password griglia**.
2. In **Cambia password console nodo**, selezionare **effettua una modifica**.

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.

Fasi

1. Inserire la passphrase di provisioning per la griglia.
2. Selezionare **Download recovery package** (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**.

Fornire nuove password

1. Seleziona il metodo di modifica della password che desideri utilizzare.
 - **Automatico**: StorageGRID assegna automaticamente una nuova password casuale della console a tutti i nodi.
 - **Personalizzato**: fornisci le password della console.

Automatico

1. Selezionare **continua**.

Personalizzato

1. Selezionare una delle seguenti opzioni:
 - **Password console globale**: applica la stessa password console a tutti i nodi.
 - **Password univoche della console**: applica una password diversa su uno o più nodi.
2. Se hai selezionato **Password console globale**, inserisci la password che desideri utilizzare per tutti i nodi.
3. Se hai selezionato **Password console univoche**, inserisci una password univoca per uno o più nodi.
4. Selezionare **continua**.

Completa la modifica della password

1. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì** se si è pronti affinché StorageGRID inizi a modificare le password della console del nodo.



Non puoi annullare questo processo dopo l'avvio.

StorageGRID genera un nuovo pacchetto di ripristino contenente la nuova password.

2. Quando il nuovo pacchetto di ripristino è pronto, seleziona **Scarica nuovo pacchetto di ripristino** e salva il pacchetto di ripristino.
3. Aprire il `.zip` file.
4. Verificare che sia possibile accedere al contenuto, incluso il `Passwords.txt` file, che contiene le nuove password della console del nodo.
5. Copia il nuovo file del pacchetto di ripristino(`.zip`) in due luoghi sicuri, protetti e separati.



Non sovrascrivere il vecchio pacchetto di ripristino.

È necessario proteggere il file di ripristino, poiché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

6. Seleziona la casella di controllo per indicare che hai scaricato il nuovo pacchetto di ripristino e ne hai verificato il contenuto.

7. Selezionare **continua**.

StorageGRID aggiorna la password per ciascun nodo.

Se si verifica un errore durante il processo di aggiornamento, la barra di avanzamento 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**.

8. Se l'aggiornamento della password non è riuscito per uno o più nodi:

- a. Esaminare i messaggi di errore elencati nella tabella.
- b. Risolvere i problemi.
- c. Selezionare **Riprova**.



Il nuovo tentativo modifica solo le password della console dei nodi sui nodi che non sono riusciti durante i precedenti tentativi di modifica della password.

9. Quando la barra di avanzamento indica che non ci sono aggiornamenti rimanenti, selezionare **Fine**.

10. Dopo aver modificato le password della console del nodo per tutti i nodi, eliminare il [primo pacchetto di ripristino scaricato](#).

Modificare le password di accesso SSH per i nodi di amministrazione di StorageGRID

La modifica delle password di accesso SSH per i nodi Admin aggiorna anche i set univoci di chiavi SSH interne per ogni nodo nella griglia. Il nodo amministrativo primario utilizza queste chiavi SSH per accedere ai nodi utilizzando un'autenticazione protetta e senza password.

Utilizzare una chiave SSH per accedere a un nodo come `admin` o all'utente `root` su una connessione VM o console fisica.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

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. Questi non vengono modificati da questa procedura.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Controllo accessi > Password griglia**.
2. In **Cambia chiavi SSH**, selezionare **effettua 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.

Fasi

1. Inserire la passphrase di provisioning per la griglia.
2. Selezionare **Download recovery package** (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, selezionare **Sì** se si è pronti a cambiare le chiavi di accesso SSH.



Non puoi annullare questo processo dopo l'avvio.

Modificare 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.

Fasi

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. Aprire il .zip file.
 - b. Verificare che sia possibile accedere al contenuto, 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 pacchetto di ripristino.

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

4. Attendere l'aggiornamento delle chiavi su ciascun nodo, operazione che potrebbe richiedere alcuni minuti.

Se le chiavi vengono modificate per tutti i nodi, viene visualizzato un banner di successo verde.

Se si verifica un errore durante il processo di aggiornamento, un messaggio di intestazione elenca il numero di nodi che non sono riusciti a modificare le chiavi. Il sistema ritenta automaticamente il processo su qualsiasi nodo che non ha modificato la chiave. 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. Selezionare **Riprova**.

Il nuovo tentativo modifica solo le chiavi di accesso SSH sui nodi che hanno avuto esito negativo durante i precedenti tentativi di modifica della chiave.

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.

Usa la federazione delle identità in StorageGRID

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari.

Configurare la federazione delle identità per Grid Manager

È possibile configurare la federazione delle identità in Grid Manager se si desidera che i gruppi di amministratori e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai ["autorizzazioni di accesso specifiche"](#).
- Stai utilizzando Active Directory, Microsoft Entra ID, 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 intende 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 ["requisiti e considerazioni per il single sign-on"](#).
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità utilizza TLS 1.2 o 1.3. Vedere ["Crittografia supportata per le connessioni TLS in uscita"](#).

A proposito di questa attività

È possibile configurare un'origine identità per Grid Manager se si desidera importare gruppi da un altro sistema, ad esempio Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server. È possibile importare i seguenti tipi di gruppi:

- Gruppi di amministratori. Gli utenti dei gruppi di amministrazione possono accedere a Grid Manager ed eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per tenant che non utilizzano la propria origine di identità. Gli utenti dei gruppi di tenant possono accedere al tenant manager ed eseguire le attività in base alle autorizzazioni assegnate al gruppo nel tenant manager. Per ulteriori informazioni, vedere ["Creare un account tenant"](#) e ["Utilizzare un account tenant"](#)

Inserire la configurazione

Fasi

1. Selezionare **Configurazione > Controllo accessi > Federazione identità**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
 - **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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `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, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
 - **Nome host:** Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
 - **Port (porta):** Porta utilizzata per la connessione al server LDAP.



La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

- **Username:** Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName` O `uid`
- `objectGUID`, `entryUUID` O `nsuniqueid`
- `cn`
- `memberOf` O `isMemberOf`
- **Active Directory:** `objectSid`, `primaryGroupID`, `userAccountControl` E `userPrincipalName`
- **ID di ingresso:** `accountEnabled` E `userPrincipalName`

- **Password:** La password associata al nome utente.



Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

- **DN base gruppo:** Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (`DC=storagegrid,DC=example,DC=com`) possono essere utilizzati come gruppi federati.



I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

- **User base DN:** Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

- **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (ID AD e Entra):** `[USERNAME]@example.com`
- **Modello di nome di accesso di livello inferiore (ID AD e Entra):** `example\[USERNAME]`
- **Modello di nome distinto:** `CN=[USERNAME],CN=Users,DC=example,DC=com`

Includi **[NOME UTENTE]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.

- **Usa STARTTLS:** 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 Microsoft Entra ID.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Microsoft Entra ID.
- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.



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 si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo:** Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

Fasi

1. Selezionare **Test di connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
 - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
 - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.

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 connessione riuscito". Selezionare **Salva** per salvare la configurazione.
- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.



L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione 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.

A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.

- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non 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 lo stato Single Sign-On (SSO) è **Abilitato** o **Modalità sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere ["Disattiva single sign-on"](#).

Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

Linee guida per la configurazione di un server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.



Per le origini identità che non sono Active Directory o Microsoft Entra ID, 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.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, vedere le istruzioni per la manutenzione dell'appartenenza al gruppo inverso nella ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#).

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Vedere le informazioni sulla manutenzione dell'appartenenza al gruppo inverso nella ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#).

Informazioni correlate

["Porte utilizzate per le comunicazioni esterne"](#)

Gestisci i gruppi di amministratori in StorageGRID

È possibile creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Gli utenti devono appartenere a un gruppo per poter accedere al sistema StorageGRID.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

Creare un gruppo di amministratori

I gruppi di amministratori consentono di determinare quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nell'API Grid Management.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Controllo accessi > Gruppi amministratori**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

- Creare un gruppo locale se si desidera assegnare le autorizzazioni agli utenti locali.
- Creare un gruppo federated per importare gli utenti dall'origine dell'identità.

Gruppo locale

Fasi

1. Selezionare **Gruppo locale**.
2. Inserire un nome visualizzato per il gruppo, che sarà possibile aggiornare in seguito secondo necessità. Ad esempio, "Maintenance Users" (manutenzione utenti) o "ILM Administrators" (amministratori ILM).
3. Immettere un nome univoco per il gruppo, che non è possibile aggiornare in seguito.
4. Selezionare **continua**.

Gruppo federated

Fasi

1. Selezionare **Federated group**.
2. Immettere il nome del gruppo che si desidera importare, esattamente come appare nell'origine identità configurata.
 - Per Active Directory e Microsoft Entra ID, utilizzare sAMAccountName.
 - Per OpenLDAP, utilizzare il CN (Common Name).
 - Per un altro LDAP, utilizzare il nome univoco appropriato per il server LDAP.
3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Fasi

1. Per la modalità **Access**, selezionare se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API Grid Management o se possono visualizzare solo impostazioni e funzionalità.
 - **Read-write** (valore predefinito): Gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle autorizzazioni di gestione.
 - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management. Gli utenti locali di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Selezionare uno o più **"autorizzazioni del gruppo di amministrazione"**.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti al gruppo non potranno accedere a StorageGRID.

3. Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo e fine**.

Aggiunta di utenti (solo gruppi locali)

Fasi

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.

Se non sono ancora stati creati utenti locali, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere questo gruppo all'utente nella pagina utenti. Per ulteriori informazioni, vedere **"Gestire gli utenti"**.

2. Selezionare **Crea gruppo e fine**.

Visualizzare e modificare i gruppi di amministratori

È possibile visualizzare i dettagli dei gruppi esistenti, modificare un gruppo o duplicare un gruppo.

- Per visualizzare le informazioni di base per tutti i gruppi, consultare la tabella nella pagina gruppi.
- Per visualizzare tutti i dettagli di un gruppo specifico o per modificarlo, utilizzare il menu **azioni** o la pagina dei dettagli.

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli del gruppo	a. Selezionare la casella di controllo del gruppo. b. Selezionare azioni > Visualizza dettagli gruppo .	Selezionare il nome del gruppo nella tabella.

Attività	Menu delle azioni	Pagina dei dettagli
Modifica nome visualizzato (solo gruppi locali)	a. Selezionare la casella di controllo del gruppo. b. Selezionare azioni > Modifica nome gruppo . c. Inserire il nuovo nome. d. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome del gruppo per visualizzare i dettagli. b. Seleziona l'icona di modifica  . c. Inserire il nuovo nome. d. Selezionare Save Changes (Salva modifiche).
Modificare la modalità di accesso o le autorizzazioni	a. Selezionare la casella di controllo del gruppo. b. Selezionare azioni > Visualizza dettagli gruppo . c. In alternativa, modificare la modalità di accesso del gruppo. d. In alternativa, selezionare o deselezionare " autorizzazioni del gruppo di amministrazione ". e. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome del gruppo per visualizzare i dettagli. b. In alternativa, modificare la modalità di accesso del gruppo. c. In alternativa, selezionare o deselezionare " autorizzazioni del gruppo di amministrazione ". d. Selezionare Save Changes (Salva modifiche).

Duplicare un gruppo

Fasi

1. Selezionare la casella di controllo del gruppo.
2. Selezionare **azioni > Duplica gruppo**.
3. Completare la procedura guidata Duplica gruppo.

Eliminare un gruppo

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni associate al gruppo. L'eliminazione di un gruppo di amministratori rimuove gli utenti dal gruppo, ma non li elimina.

Fasi

1. Dalla pagina Groups (gruppi), selezionare la casella di controllo per ciascun gruppo che si desidera rimuovere.
2. Selezionare **azioni > Elimina gruppo**.
3. Selezionare **Elimina gruppi**.

Autorizzazioni del gruppo amministratore in StorageGRID

Quando si creano gruppi di utenti admin, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare

quali attività possono essere eseguite dall'utente.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti a tale gruppo non potranno accedere a Grid Manager o all'API Grid Management.

Per impostazione predefinita, qualsiasi utente appartenente a un gruppo che dispone di almeno un'autorizzazione può eseguire le seguenti attività:

- Accedi a Grid Manager
- Visualizza la dashboard
- Visualizzare le pagine dei nodi
- Visualizzare gli avvisi correnti e risolti
- Modifica della propria password (solo utenti locali)
- Visualizzare alcune informazioni fornite nelle pagine Configurazione e manutenzione

Interazione tra permessi e modalità di accesso

Per tutte le autorizzazioni, l'impostazione **modalità di accesso** del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità. Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Le sezioni seguenti descrivono le autorizzazioni che è possibile assegnare durante la creazione o la modifica di un gruppo amministrativo. Qualsiasi funzionalità non esplicitamente menzionata richiede l'autorizzazione **Root access**.

Accesso root

Questa autorizzazione consente di accedere a tutte le funzioni di amministrazione della griglia.

Modificare la password root del tenant

Questa autorizzazione consente di accedere all'opzione **Modifica password root** nella pagina tenant, consentendo di controllare chi può modificare la password per l'utente root locale del tenant. Questa autorizzazione viene utilizzata anche per la migrazione delle chiavi S3 quando è attivata la funzione di importazione delle chiavi S3. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Modifica password root**.



Per consentire l'accesso alla pagina dei tenant, che contiene l'opzione **Modifica password root**, assegnare anche l'autorizzazione **account tenant**.

ILM

Questa autorizzazione consente di accedere alle seguenti opzioni del menu **ILM**:

- Regole
- Policy
- Tag policy
- Pool di storage
- Gradi di storage

- Regioni
- Ricerca dei metadati degli oggetti



Per gestire i livelli di archiviazione, gli utenti devono disporre dell'autorizzazione **Altra configurazione della griglia**.

Manutenzione

Gli utenti devono disporre dell'autorizzazione Maintenance per utilizzare queste opzioni:

- **Configurazione > Controllo accessi**
 - Password di rete
- **Configurazione > Rete**
 - Nomi di dominio degli endpoint S3
- **Manutenzione > Attività**
 - Decommissionare
 - Espansione
 - Controllo dell'esistenza dell'oggetto
 - Recovery (recupero)
- **Manutenzione > Sistema**
 - Pacchetto di recovery
 - Aggiornamento del software
- **Supporto > Strumenti**
 - Registri

Gli utenti che non dispongono dell'autorizzazione Maintenance possono visualizzare, ma non modificare, le seguenti pagine:

- **Manutenzione > Rete**
 - Server DNS
 - Grid Network
 - Server NTP
- **Manutenzione > Sistema**
 - Licenza
- **Configurazione > Rete**
 - Nomi di dominio degli endpoint S3
- **Configurazione > Sicurezza**
 - Certificati
- **Configurazione > Monitoraggio**
 - Server syslog e audit

Gestire gli avvisi

Questa autorizzazione consente di accedere alle opzioni per la gestione degli avvisi. Gli utenti devono disporre di questa autorizzazione per gestire silenzi, notifiche di avviso e regole di avviso.

Query sulle metriche

Questa autorizzazione consente di accedere a:

- Pagina **Supporto > Strumenti > Metriche**
- Query di metriche Prometheus personalizzate utilizzando la sezione **metriche** dell'API Grid Management
- Schede dashboard di Grid Manager che contengono metriche

Ricerca dei metadati degli oggetti

Questa autorizzazione consente di accedere alla pagina **ILM > Object metadata lookup**.

Altra configurazione della griglia

Questa autorizzazione fornisce l'accesso alle seguenti opzioni aggiuntive di configurazione della griglia:

- **ILM**
 - Gradi di storage
- **Configurazione > Sistema**
- **Assistenza > Altro**
 - Priorità I/O
 - Servizi dei nodi
 - Watermark di storage



Il costo del collegamento richiede l'accesso come root.

Amministratore dell'appliance di storage

Questa autorizzazione fornisce:

- Accesso al System Manager di e-Series SANtricity sulle appliance di storage tramite il Grid Manager.
- La possibilità di eseguire attività di troubleshooting e manutenzione nella scheda Manage drives (Gestione dischi) per le appliance che supportano queste operazioni.

Account tenant

Questa autorizzazione consente di:

- Accedere alla pagina tenant, in cui è possibile creare, modificare e rimuovere gli account tenant
- Visualizzare le policy di classificazione del traffico esistenti
- Visualizza le schede dashboard di Grid Manager che contengono i dettagli del tenant

Gestisci gli utenti in StorageGRID

È possibile visualizzare utenti locali e federati. È inoltre possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzioni di Grid Manager possono accedere questi utenti.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Creare un utente locale

È possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi locali. Le autorizzazioni del gruppo controllano a quali funzioni dell'API Grid Manager e Grid Management l'utente può accedere.

È possibile creare solo utenti locali. Utilizzare l'origine dell'identità esterna per gestire utenti e gruppi federati.

Grid Manager include un utente locale predefinito, denominato "root". Non puoi rimuovere l'utente root.



Se è attivato il Single Sign-on (SSO), gli utenti locali non possono accedere a StorageGRID.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Controllo accessi > Utenti amministratori**.
2. Selezionare **Crea utente**.

Immettere le credenziali dell'utente

Fasi

1. Immettere il nome completo dell'utente, un nome utente univoco e una password.
2. Se si desidera, selezionare **Sì** se l'utente non deve avere accesso all'API Grid Manager o Grid Management.
3. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Facoltativamente, assegnare l'utente a uno o più gruppi per determinare le autorizzazioni dell'utente.

Se non sono ancora stati creati gruppi, è possibile salvare l'utente senza selezionare i gruppi. È possibile aggiungere questo utente a un gruppo nella pagina gruppi.

Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Per ulteriori informazioni, vedere ["Gestire i gruppi di amministratori"](#).

2. Selezionare **Crea utente** e selezionare **fine**.

Visualizzare e modificare gli utenti locali

È possibile visualizzare i dettagli degli utenti locali e federati esistenti. È possibile modificare un utente locale

per modificare il nome completo, la password o l'appartenenza al gruppo dell'utente. È inoltre possibile impedire temporaneamente a un utente di accedere a Grid Manager e all'API Grid Management.

È possibile modificare solo gli utenti locali. Utilizzare l'origine dell'identità esterna per gestire gli utenti federati.

- Per visualizzare le informazioni di base per tutti gli utenti locali e federati, consultare la tabella nella pagina utenti.
- Per visualizzare tutti i dettagli di un utente specifico, modificare un utente locale o modificare la password di un utente locale, utilizzare il menu **azioni** o la pagina dei dettagli.

Tutte le modifiche vengono applicate alla successiva disconnessione dell'utente e all'accesso a Grid Manager.



Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Change password** (Modifica password) nel banner Grid Manager.

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli dell'utente	- Selezionare la casella di controllo dell'utente. - Selezionare azioni > Visualizza dettagli utente.	Selezionare il nome dell'utente nella tabella.
Modifica nome completo (solo utenti locali)	- Selezionare la casella di controllo dell'utente. - Selezionare azioni > Modifica nome completo. - Inserire il nuovo nome. - Selezionare Save Changes (Salva modifiche).	- Selezionare il nome dell'utente per visualizzare i dettagli. - Seleziona l'icona di modifica . - Inserire il nuovo nome. - Selezionare Save Changes (Salva modifiche).
Negare o consentire l'accesso a StorageGRID	- Selezionare la casella di controllo dell'utente. - Selezionare azioni > Visualizza dettagli utente. - Selezionare la scheda Access (accesso). - Selezionare Sì per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare No per consentire all'utente di accedere. - Selezionare Save Changes (Salva modifiche).	- Selezionare il nome dell'utente per visualizzare i dettagli. - Selezionare la scheda Access (accesso). - Selezionare Sì per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare No per consentire all'utente di accedere. - Selezionare Save Changes (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modifica della password (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare azioni > Visualizza dettagli utente . c. Selezionare la scheda Password. d. Inserire una nuova password. e. Selezionare Cambia password .	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Password. c. Inserire una nuova password. d. Selezionare Cambia password .
Modifica dei gruppi (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare azioni > Visualizza dettagli utente . c. Selezionare la scheda gruppi. d. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. e. Selezionare Edit groups (Modifica gruppi) per selezionare diversi gruppi. f. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda gruppi. c. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. d. Selezionare Edit groups (Modifica gruppi) per selezionare diversi gruppi. e. Selezionare Save Changes (Salva modifiche).

Importa utenti federati

È possibile importare uno o più utenti federati, fino a un massimo di 100 utenti, direttamente nella pagina Utenti.

Fasi

1. Selezionare **Configurazione > Controllo accessi > Utenti amministratori**.
2. Seleziona **Importa utenti federati**.
3. Inserisci l'UUID o il nome utente di uno o più utenti federati.

Per voci multiple, aggiungere ogni UUID o nome utente su una nuova riga.

4. Selezionare **Importa**.

Se l'importazione nel campo Utenti non riesce per uno o più utenti, procedere come segue:

- a. Espandi **Utenti non importati** e seleziona **Copia utenti**.
- b. Riprovare l'importazione selezionando **Precedente** e incollando gli utenti copiati nella finestra di dialogo **Importa utenti federati**.

Dopo aver chiuso la finestra di dialogo **Importa utenti federati**, le informazioni sugli utenti federati vengono visualizzate nella pagina Utenti per gli utenti importati correttamente.

Duplicare un utente

È possibile duplicare un utente esistente per creare un nuovo utente con le stesse autorizzazioni.

Fasi

1. Selezionare la casella di controllo dell'utente.
2. Selezionare **azioni > utente duplicato**.
3. Completare la procedura guidata Duplica utente.

Eliminare un utente

È possibile eliminare un utente locale per rimuoverlo definitivamente dal sistema.



Impossibile eliminare l'utente root.

Fasi

1. Nella pagina utenti, selezionare la casella di controllo per ciascun utente che si desidera rimuovere.
2. Selezionare **azioni > Elimina utente**.
3. Selezionare **Delete user** (Elimina utente).

Utilizzo di SSO (Single Sign-on)

Scopri l'SSO di StorageGRID

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.

Il sistema StorageGRID supporta il single sign-on (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0) o OpenID Connect.

Prima di attivare SSO (Single Sign-on), esaminare in che modo i processi di accesso e disconnessione di StorageGRID vengono influenzati quando SSO è attivato.

Effettuare l'accesso quando SSO è attivato

Quando SSO è attivato e si accede a StorageGRID, si viene reindirizzati alla pagina SSO dell'organizzazione per convalidare le credenziali.

Fasi

1. Immettere il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione StorageGRID in un browser Web.

Viene visualizzata la pagina di accesso a StorageGRID.

- Se è la prima volta che accedi all'URL su questo browser, ti verrà richiesto un ID account.
- 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.



La pagina di accesso a 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`). Al contrario, l'utente viene immediatamente reindirizzato alla pagina di accesso SSO dell'organizzazione, in cui è possibile [Accedi con le tue credenziali SSO](#).

2. Indicare se si desidera accedere a Grid Manager o al tenant Manager:

- Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, inserire **0** come ID account o selezionare **Grid Manager** se compare nell'elenco degli account recenti.
- Per accedere al tenant Manager, inserire l'ID account tenant di 20 cifre o selezionare un tenant in base al nome, se visualizzato nell'elenco degli account recenti.

3. Selezionare **Accedi**

StorageGRID reindirizza l'utente alla pagina di accesso SSO della propria organizzazione. Ad esempio:

4. Accedi con le tue credenziali SSO.

Se le credenziali SSO sono corrette:

- a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
- b. StorageGRID convalida la risposta di autenticazione.
- c. Se la risposta è valida e l'utente appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID, l'utente ha effettuato l'accesso a Gestione griglia o a Gestione tenant, a seconda dell'account selezionato.



Se l'account del servizio non è accessibile, è comunque possibile effettuare l'accesso, purché si sia un utente esistente che appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID.

5. Se si dispone di autorizzazioni adeguate, è possibile accedere ad altri nodi di amministrazione o a Grid Manager o Tenant Manager.

Non è necessario immettere nuovamente le credenziali SSO.

Disconnettersi quando SSO è attivato

Quando SSO è abilitato per StorageGRID, ciò che accade quando si effettua la disconnessione dipende da ciò che si effettua l'accesso e da dove si effettua la disconnessione.

Fasi

1. Individuare il collegamento **Disconnetti** nell'angolo in alto a destra dell'interfaccia utente.
2. Selezionare **Disconnetti**.

Viene visualizzata la pagina di accesso a StorageGRID. Il menu a discesa **Recent Accounts** (account recenti) viene aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere a queste interfacce utente più rapidamente in futuro.



La tabella riassume ciò che accade quando si effettua la disconnessione se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti separatamente da tutte le sessioni del browser.

Se hai effettuato l'accesso a...	E ti disconnetterai da...	Sei disconnesso da...
Grid Manager su uno o più nodi di amministrazione	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi di amministrazione Nota: se si utilizza l'ID Entra per SSO, potrebbero essere necessari alcuni minuti per uscire da tutti i nodi amministrativi.
Tenant Manager su uno o più nodi di amministrazione	Tenant Manager su qualsiasi nodo di amministrazione	Tenant Manager su tutti i nodi di amministrazione
Sia Grid Manager che tenant Manager	Grid Manager	Solo Grid Manager. Per disconnettersi da SSO, devi anche disconnetterti da Tenant Manager.

Requisiti e considerazioni per StorageGRID SSO

Prima di abilitare il single sign-on (SSO) per un sistema StorageGRID, esaminare i requisiti e le considerazioni.

Requisiti del provider di identità

StorageGRID supporta diversi provider di identità (IdP) SSO.

OIDC

I seguenti SSO IdPs sono supportati per OpenID Connect (OIDC):

- Active Directory Federation Service (ad FS)
- ID di accesso Microsoft
- Keycloak
- PingFederate
- Okta

SAML

I seguenti SSO IdPs sono supportati per Security Assertion Markup Language 2.0 (SAML 2.0):

- Active Directory Federation Service (ad FS)
- ID di accesso Microsoft
- PingFederate

È necessario configurare la federazione delle identità per il sistema StorageGRID prima di poter configurare un provider di identità SSO. Il tipo di servizio LDAP utilizzato per i controlli di federazione delle identità che consentono di implementare il tipo di SSO.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory	• Active Directory • Keycloak • Okta • Entra ID • PingFederate
Entra ID	Entra ID

Requisiti AD FS

È possibile utilizzare una delle seguenti versioni di ad FS:

- Windows Server 2022 ad FS
- Windows Server 2019 ad FS
- Windows Server 2016 ad FS



Windows Server 2016 deve utilizzare il ["Aggiornamento KB3201845"](#) o una versione successiva.

Requisiti aggiuntivi

- Transport Layer Security (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Considerazioni per Entra ID

Se si utilizza Entra ID come tipo di SSO e gli utenti hanno nomi principali 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 dei certificati 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 (Entra ID) 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 lo avete già ["ha configurato un certificato personalizzato per l'interfaccia di gestione"](#) fatto, dovrete farlo ora. Quando si installa un certificato server personalizzato, viene utilizzato per tutti i nodi di amministrazione e può essere utilizzato in tutti i trust, le applicazioni aziendali o le connessioni SP di StorageGRID.



Si sconsiglia di utilizzare il certificato server predefinito di un nodo di amministrazione in una connessione SP, un'applicazione aziendale o un trust di parte attiva. Se il nodo si guasta e viene ripristinato, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della parte che si basa, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo amministrativo accedendo alla shell dei comandi del nodo e andando alla `/var/local/mgmt-api` directory. Un certificato server personalizzato è denominato `custom-server.crt`. Il certificato server predefinito del nodo è denominato `server.crt`.

Requisiti delle porte

Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443). Vedere ["Controllare l'accesso al firewall esterno"](#).

Conferma che gli utenti federati possano eseguire Sign in a StorageGRID

Prima di attivare il Single Sign-on (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per qualsiasi account tenant esistente.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- La federazione delle identità è già stata configurata.

Fasi

1. Se esistono account tenant, verificare che nessuno dei tenant utilizzi la propria origine di identità.



Quando si attiva SSO, un'origine identità configurata in Tenant Manager viene ignorata dall'origine identità configurata in Grid Manager. Gli utenti che appartengono all'origine dell'identità del tenant non potranno più accedere a meno che non dispongano di un account con l'origine dell'identità di Grid Manager.

- a. Accedi al tenant manager per ogni account tenant.
 - b. Selezionare **Gestione accessi > Federazione identità**.
 - c. Verificare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
 - d. In tal caso, verificare che i gruppi federati che potrebbero essere in uso per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.
2. Verificare che un utente federated possa accedere a Grid Manager:
 - a. Da Grid Manager, seleziona **Configurazione > Controllo accessi > Gruppi amministratori**.
 - b. Assicurarsi che almeno un gruppo federated sia stato importato dall'origine dell'identità di Active Directory e che sia stata assegnata l'autorizzazione di accesso root.
 - c. Disconnettersi.
 - d. Confermare che è possibile accedere nuovamente a Grid Manager come utente nel gruppo federated.

3. Se sono presenti account tenant, verificare che un utente federated che dispone dell'autorizzazione di accesso root possa effettuare l'accesso:

- a. Da Grid Manager, seleziona **Inquilini**.
- b. Selezionare l'account tenant e selezionare **azioni > Modifica**.
- c. Nella scheda Immetti dettagli, selezionare **continua**.
- d. Se la casella di controllo **Usa origine identità propria** è selezionata, deselezionare la casella e selezionare **Salva**.

Viene visualizzata la pagina del tenant.

- e. Selezionare l'account tenant, selezionare **Accedi** e accedere all'account tenant come utente root locale.
- f. Da Tenant Manager, seleziona **Gestione accessi > Gruppi**.
- g. Assicurarsi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di accesso root per questo tenant.
- h. Disconnettersi.
- i. Confermare che è possibile accedere nuovamente al tenant come utente nel gruppo federated.

Informazioni correlate

- ["Requisiti e considerazioni per il single sign-on"](#)
- ["Gestire i gruppi di amministratori"](#)
- ["Utilizzare un account tenant"](#)

Configura SSO con OIDC

Scopri come configurare l'SSO in StorageGRID usando OIDC

Configurare il single sign-on (SSO) in StorageGRID permette a StorageGRID (il service provider) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti.

Puoi configurare l'SSO in StorageGRID usando OpenID Connect (OIDC) o SAML. Segui questi passaggi high-level per configurare l'SSO in StorageGRID usando OIDC oppure scopri di più ["Configurare SSO usando SAML"](#).

1

Configura il provider di identità

In base al provider di identità SSO che vuoi utilizzare, puoi selezionare Active Directory o Entra ID come tipo di servizio LDAP per la federazione delle identità.

- Per Active Directory Federation Service (AD FS), puoi usare AD FS, Entra ID, Keycloak, Okta o PingFederate come provider di identità.
- Per Entra ID, puoi usare solo il provider di identità Entra ID.

Utilizza il software del provider di identità SSO per configurare OIDC per ciascun Admin Node nella tua griglia.

- Scopri ["creare un gruppo di applicazioni per ogni Admin Node"](#) Active Directory

- Scopri ["creare un'applicazione per ogni Admin Node"](#) in Entra ID
- Scopri ["creazione di un client per ogni Admin Node"](#) in Keycloak
- Scopri di più ["creare un'applicazione Okta per ogni Admin Node"](#)
- Scopri ["creare una service provider connection per ogni Admin Node"](#) in PingFederate

2

Configura SSO

Seleziona la procedura guidata Configura SSO per OIDC. Poi, configura l'SSO con il tuo provider di identità ed entra in modalità sandbox per configurare e testare l'SSO prima di abilitarlo per gli utenti di StorageGRID.

Scopri di più ["configurare l'SSO usando OIDC"](#)

3

Abilita SSO

Dopo aver verificato che puoi utilizzare l'SSO per accedere a ciascun Admin Node, abilita l'SSO per tutti gli utenti StorageGRID.

Scopri di più ["Abilitare l'SSO per gli utenti di StorageGRID"](#)

Crea gruppi di applicazioni in AD FS per OIDC in StorageGRID

Devi usare Active Directory Federation Services (AD FS) per creare un gruppo di applicazioni per ogni Admin Node per OpenID Connect (OIDC) nel tuo sistema.

Prima di iniziare

- Hai il fully qualified domain name (o l'indirizzo IP) e l'identificatore della relying party per ogni Admin Node nel tuo sistema.



Ogni Admin Node nel tuo sistema StorageGRID deve avere un gruppo di applicazioni. Questo garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node. Puoi creare un unico gruppo di applicazioni per tutti gli Admin Node (consigliato) oppure un gruppo di applicazioni diverso per ciascun Admin Node.

- Hai esperienza nella creazione di gruppi di applicazioni in AD FS o hai accesso alla documentazione di Microsoft AD FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.

A proposito di questa attività

Queste istruzioni si applicano a Windows Server 2022 AD FS. Se usi una versione diversa di AD FS, noterai lievi differenze nella procedura. Consulta la documentazione di Microsoft AD FS se hai domande.

Passaggio 1: Crea un gruppo di applicazioni

Puoi usare Windows PowerShell per creare rapidamente un gruppo di applicazioni.

Fasi

1. Da Gestione server Windows, selezionare **Strumenti > Gestione di ad FS**.
2. Seleziona **Gruppi di applicazioni > Aggiungi gruppo di applicazioni**

3. Per **Nome**, inserisci l'identificativo della relying party.
4. Nella sezione Modelli, seleziona **Applicazioni client-server > Applicazione server che accede a un'API web**.
5. Selezionare **Avanti**.
6. Segna il valore di **Client Identifier**.
7. Nella sezione **URI di reindirizzamento**, inserisci il FQDN (o l'indirizzo IP) callback e logged-out gli URI per il nodo di amministrazione:

- `https://<FQDN>/api/v4/oidc-callback` o `https://<IP_address>/api/v4/oidc-callback`
- `https://<FQDN>/api/v4/oidc-logged-out` o `https://<IP_address>/api/v4/oidc-logged-out`

Se usi un unico gruppo di applicazioni per tutti gli Admin Node, inserisci gli URI per ciascun Admin Node.
Se usi un gruppo di applicazioni diverso per ogni Admin Node, inserisci solo gli URI relativi al corrispondente Admin Node.

8. Selezionare **Aggiungi**.
9. Seleziona **Genera un segreto condiviso**, annota il valore per **Segreto**, quindi seleziona **Avanti**.
10. Inserisci l'identificativo del client per **Identificativo**.
11. Seleziona **Aggiungi**, poi seleziona **Avanti**.
12. Seleziona **Consenti a tutti**.
13. Verifica che l'applicazione server sia selezionata in **Applicazione client (chiamante)**.
14. Nella sezione **Ambiti consentiti**, verifica che siano selezionate solo le seguenti opzioni:
 - tutte le rivendicazioni
 - email
 - openid
 - profilo
15. Seleziona **Avanti > Avanti**.
16. Seleziona **Chiudi**.

Passaggio 2: Configura le regole di trasformazione dell'emissione

Configura le regole di trasformazione dell'emissione per ciascun gruppo di applicazioni.

Fasi

1. Nella pagina **Gestione AD FS**, fai clic con il pulsante destro del mouse sul gruppo di applicazioni, quindi seleziona **Proprietà**.
2. Seleziona l'API web creata in precedenza, quindi seleziona **Modifica**.
3. Seleziona **Regole di trasformazione dell'emissione > Aggiungi regola**
4. Sotto **Modello di regola di rivendicazione**, seleziona **Invia attributo LDAP come rivendicazioni**.
5. Selezionare **Avanti**.
6. Inserisci il nome di una regola di claim.

7. Seleziona **Active Directory** come archivio attributi.
8. Aggiungi le mappature degli attributi LDAP ai tipi di claim in uscita:
 - E-Mail Addresses - E-Mail Address
 - Token-Groups - Unqualified Names - Group
9. Selezionare **fine**.
10. Seleziona **Applica > OK > OK**.

Cosa c'è dopo

Dopo aver creato i gruppi di applicazioni, ["Configura SSO tramite OIDC"](#).

Crea applicazioni aziendali in Entra ID per OIDC in StorageGRID

Utilizza Entra ID per creare un'applicazione aziendale per ogni Admin Node per OpenID Connect (OIDC) nel tuo sistema.

Prima di iniziare

- Hai l'identificativo della relying party e il fully qualified domain name (FQDN) o l'indirizzo IP per ogni Admin Node nel tuo sistema.



Ogni nodo di amministrazione nel tuo sistema StorageGRID deve disporre di un'applicazione aziendale. Questo garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi nodo di amministrazione. Puoi creare un'unica applicazione aziendale per tutti i nodi di amministrazione (consigliato) oppure un'applicazione aziendale diversa per ciascun nodo di amministrazione.

- Hai esperienza nella creazione di applicazioni in Entra ID.
- Hai un account Entra ID con un abbonamento attivo.
- Nell'account Entra ID ricopri uno dei seguenti ruoli: Amministratore globale, Amministratore dell'applicazione cloud, Amministratore dell'applicazione o proprietario del servizio principale.

Passaggio 1: Accedi a Entra ID

Fasi

1. Accedere a ["Portale Azure"](#).
2. Seleziona ["ID di accesso Microsoft"](#).
3. Seleziona ["Registrazioni delle app"](#).

Passaggio 2: Registra una nuova applicazione

Registra una nuova applicazione aziendale per ogni Admin Node nel tuo sistema.

Fasi

1. Nel riquadro Applicazioni Entra ID Enterprise, seleziona **Registrazioni applicazioni > Nuova registrazione**.
2. Per **Nome**, inserisci l'identificativo della relying party.
3. In **Tipi di account supportati**, seleziona i tipi di account che possono usare l'applicazione o accedere all'API, ad esempio, **Solo tenant singolo - <tenant_name>**.

4. In **URI di reindirizzamento**, seleziona **Seleziona una piattaforma > Web**.
5. Inserisci l'URI di reindirizzamento fully qualified domain (o indirizzo IP) per il nodo Admin:
`https://<FQDN>/api/v4/oidc-callback` o `https://<IP_address>/api/v4/oidc-callback`
- Se usi un'unica applicazione aziendale per tutti i nodi di amministrazione, inserisci l'URI di ciascun nodo di amministrazione. Se usi un'applicazione aziendale diversa per ogni nodo di amministrazione, inserisci solo l'URI del nodo di amministrazione corrispondente.
6. Seleziona **Register**.
7. Nella pagina Panoramica della nuova registrazione dell'applicazione, annota l'**Application (client) ID** e il **Directory (tenant) ID**.

Passaggio 3: Configura un segreto client

Registra un client secret per ogni nuova applicazione.

Fasi

1. Nella pagina Panoramica della nuova registrazione dell'applicazione, seleziona **Gestisci > Certificati e segreti > Nuovo segreto client**.
2. Inserisci il client secret e imposta la data di scadenza desiderata.
3. Seleziona **Aggiungi** per creare il client secret.
4. Copia il **Value** segreto.



Il valore segreto non è visibile dopo che aggiorni o navighi dalla pagina del segreto del client.

Passaggio 4: Configura le autorizzazioni API

Configura le autorizzazioni API per ogni nuova applicazione.

Fasi

1. Nella pagina Panoramica della nuova registrazione dell'applicazione, seleziona **Gestisci > Autorizzazioni API > Aggiungi un'autorizzazione**.
2. Seleziona **Microsoft APIs > Microsoft Graph > Autorizzazioni delegate**.
3. Espandi **OpenId permissions**, poi seleziona **email**, **offline_access**, **openid** e **profile**.
4. Seleziona **Aggiungi autorizzazioni**.
5. Seleziona **Concedi il consenso amministrativo per <tenant>**, poi seleziona **Sì**.

Passaggio 5: Aggiungi l'URI di reindirizzamento per il logout

Aggiungi l'URI di reindirizzamento per il logout per ogni nuova applicazione.

Fasi

1. Nella pagina Panoramica della nuova registrazione dell'applicazione, seleziona **Gestisci > Autenticazione**.
2. Seleziona **Aggiungi URI di reindirizzamento > Web**.
3. Inserisci l'URI di reindirizzamento FQDN (o indirizzo IP) per l'Admin Node: `https://<FQDN>/api/v4/`

`oidc-logged-out` o `https://<IP_address>/api/v4/oidc-logged-out`

Se usi un unico gruppo di applicazioni per tutti gli Admin Node, inserisci l'URI per ciascun Admin Node. Se usi un gruppo di applicazioni diverso per ciascun Admin Node, inserisci solo l'URI per l'Admin Node corrispondente.

4. Seleziona **Configura**.

Cosa c'è dopo

Dopo aver creato le applicazioni aziendali, "[Configura SSO tramite OIDC](#)".

Crea client in Keycloak per OIDC in StorageGRID

Utilizza Keycloak per creare una connessione client per ogni Admin Node per OpenID Connect (OIDC) nel tuo sistema StorageGRID.

Prima di iniziare

- Hai esperienza nella creazione di client in Keycloak o hai accesso alla documentazione di Keycloak.
- Hai un account dedicato (Bind DN) per la consultazione della directory e le credenziali di accesso.
- Hai accesso come amministratore di Keycloak.

A proposito di questa attività

Ogni Admin Node nel tuo sistema StorageGRID deve avere una connessione client. Questo garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node. Puoi creare un'unica connessione client per tutti gli Admin Node (consigliato) oppure una connessione client diversa per ciascun Admin Node.

Utilizza le impostazioni predefinite, salvo diversa indicazione. In alcuni casi puoi utilizzare le impostazioni richieste dalla tua organizzazione.

Passaggio 1: Facoltativamente, crea un realm

Crea un realm Keycloak per configurare il provider LDAP e il client OIDC, oppure usa il realm predefinito di Keycloak.

Fasi

1. Seleziona **Create Realm**.
2. Inserisci un nome per il realm.
3. Seleziona **Enabled**.
4. Selezionare **Crea**.

Passaggio 2: Configura il provider LDAP

Configura il provider LDAP in modo che Keycloak si connetta al server LDAP Active Directory Federation Service (AD FS).

Fasi

1. Seleziona **Federazione utenti > Aggiungi provider LDAP**.
2. Nella scheda Impostazioni:
 - a. Inserisci i seguenti valori consigliati:

- Nome visualizzato nell'interfaccia utente: Inserisci un valore univoco.
- Fornitore: **Active Directory**
- URL di connessione: `ldap://<ldap_IP_address> o ldaps://<ldap_IP_address>`
- Pool di connessioni: **ON**
- Bind DN: Inserisci il tuo Bind DN
- Credenziali di associazione: Inserisci la password
- Modalità di modifica: **READ_ONLY**
- DN utente: Ad esempio, `CN=Users, DC=saml, DC=sgws`
- Attributo LDAP username: **sAMAccountName**
- Attributo LDAP RDN: **cn**
- Attributo LDAP UUID: **objectGUID**
- Classi di oggetti utente: `person, organizationalPerson, user`
- Filtro LDAP utente: `(sAMAccountName=*)`
- Ambito di ricerca: **Sottostruttura**
- Paginazione: **ON**
- Importa utenti: **ON**
- Sincronizzazione registrazioni: **ON**
- Rimuovi utenti non validi durante le ricerche: **ON**

b. Seleziona **Test connessione** e **Test autenticazione**.

Risolvi eventuali problemi che potrebbero presentarsi prima di continuare.

3. Selezionare **Salva**.

Passaggio 3: Configura la mappatura LDAP

Configura la mappatura LDAP per mappare AD come attributo in Keycloak.

Fasi

1. Vai a **User federation > LDAP**
2. Seleziona **Provider LDAP** che hai creato.
3. Nella scheda Mapper, seleziona **Aggiungi mapper > Crea nuovo mapper**.
4. Per Tipo di mapper, seleziona **user-attribute-ldap-mapper**.
5. Seleziona **Salva**, quindi inserisci le seguenti informazioni:
 - Attributo del modello utente: **userPrincipalName**
 - Attributo LDAP: **userPrincipalName**
 - Sola lettura: **ON**
 - Leggi sempre il valore da LDAP: **ON**
 - Obbligatorio in LDAP: **OFF**
 - Forza un valore predefinito: **ON**

- Attributo binario: **OFF**

6. Selezionare **Salva**.

Passaggio 4: Crea il client OIDC

Crea il client OIDC per il tuo sistema.

Fasi

1. Vai su **Clienti > Crea client**.
2. Per le impostazioni generali, inserisci le seguenti informazioni:
 - Nome: Inserisci un nome visualizzato per il client.
 - Tipo di client: **OIDC Connect**
 - ID cliente: Inserisci un valore univoco. Salva questo valore per utilizzarlo in seguito.
3. Selezionare **Avanti**.
4. Per la configurazione delle funzionalità, inserisci le seguenti informazioni:
 - Autenticazione client: **ATTIVA**
 - Flusso standard: **Abilita**
 - Concessioni di accesso diretto: **Enable**
 - Ruoli account di servizio: **Enable**
5. Selezionare **Avanti**.
6. Per le impostazioni di accesso, inserisci gli URI di reindirizzamento:



Se per l'interfaccia di gestione sono configurati uno o più endpoint del bilanciatore di carico, aggiungi gli URI di reindirizzamento per ciascuna porta. Per esempio:

`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` e
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

- URI di reindirizzamento validi: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback` e `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- URI di reindirizzamento post-logout validi:
`https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`
- Origini del web: `https://<Admin_IP_address_or_FQDN>`

7. Selezionare **Salva**.

Passaggio 5: Genera il client secret

Genera un segreto client per il client OIDC che hai creato.

Fasi

1. Vai su **Clienti**, poi seleziona il **client OIDC** che hai creato.
2. Nella scheda **Credenziali**, inserisci le seguenti informazioni:
 - authenticator client: **Client Id e Secret**
 - Segreto del client: **Genera o imposta un segreto del client**. Salva questo valore per utilizzarlo in seguito.

Passaggio 6: Definisci gli ambiti

Definisci gli ambiti in Keycloak.

Fasi

1. Vai su **Ambiti client** > **Crea ambito client**, quindi inserisci le seguenti informazioni:
 - Tipo: **Nessuno**
 - Protocollo: **OpenID Connect**
 - Visualizzazione nella schermata di consenso: **Abilitato**
 - Includi nei metadati del provider OpenID: **Abilitato**
2. Selezionare **Salva**.
3. Nella scheda Mapper, seleziona **Configura un nuovo mapper** > **Attributo utente**, quindi inserisci le seguenti informazioni:
 - Nome: Inserisci un valore univoco.
 - Attributo utente: **userPrincipalName**
 - Nome richiesta token: **upn**
 - Tipo JSON della claim: **String**
 - Aggiungi al token ID: **ON**
 - Aggiungi al token di accesso: **ON**
 - Aggiungi alle informazioni utente: **ON**
 - Aggiungi all'introspezione del token: **ON**
4. Selezionare **Salva**.
5. Vai su **Clienti** e seleziona il **client OIDC** che hai creato.
6. Seleziona **Ambiti client** > **Aggiungi ambito client**.
7. Seleziona l'ambito client che hai creato.
8. Selezionare **Aggiungi**.

Passaggio 7: Preparati a configurare SSO tramite OIDC

Salva le informazioni necessarie per configurare l'SSO con OIDC utilizzando Keycloak nel tuo sistema StorageGRID.

Fasi

1. Verifica di aver salvato il **ID client** e il **segreto client** dal client OIDC che hai creato.
2. Salva l'endpoint di rilevamento OpenID Connect per il realm. Questo è disponibile nell'endpoint di configurazione `well-known`:

```
https://<keycloak_host_ip/keycloak_host_name>/realms/<realm_name>/well-known/openid-configuration
```

Facoltativamente, puoi includere la porta di rete:

```
https://<keycloak_host_ip/keycloak_host_name>:<https_port>/realms/<realm_name>/well-known/openid-configuration
```

Cosa c'è dopo

Dopo aver creato i client OIDC, "[Configura SSO tramite OIDC](#)".

Crea un'applicazione Okta per OIDC in StorageGRID

Crea un'applicazione Okta per tutti i nodi di amministrazione per OpenID Connect (OIDC) nel tuo sistema StorageGRID.

Prima di iniziare

- Hai esperienza nella creazione di applicazioni Okta o hai accesso alla documentazione Okta.
- Hai accesso come amministratore Okta.

A proposito di questa attività

Un'applicazione Okta deve contenere URI di reindirizzamento per l'accesso e la disconnessione per tutti gli Admin Node. Gli URI di reindirizzamento garantiscono che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node. Puoi creare un'unica applicazione Okta per tutti gli Admin Node (consigliato) oppure un'applicazione diversa per ciascun Admin Node.

Utilizza le impostazioni predefinite, salvo diversa indicazione. In alcuni casi puoi utilizzare le impostazioni richieste dalla tua organizzazione.

Passaggio 1: Crea un'applicazione Okta

Crea un'applicazione Okta utilizzando l'interfaccia utente di Okta.

Fasi

1. In Okta, vai su **Applicazioni > Applicazioni**.
2. Seleziona **Crea integrazione app**, quindi inserisci le seguenti informazioni:
 - Metodo di accesso: **OIDC - OpenID Connect**
 - Tipo di applicazione: **Web Application**
3. Selezionare **Avanti**.
4. Inserisci un nome per l'applicazione nel campo Integrazione app.
5. Verifica che Authorization Code sia selezionato (impostazione predefinita) per i Core grants.
6. Aggiungi gli URI di reindirizzamento per l'accesso e la disconnessione per ciascun Admin Node:
 - URI di reindirizzamento all'accesso: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-callback`
 - URI di reindirizzamento per il logout: `https://<Admin_IP_address_or_FQDN>/api/v4/oidc-logged-out`



Se per l'interfaccia di gestione sono configurati uno o più endpoint del bilanciatore di carico, aggiungi gli URI di reindirizzamento per ciascuna porta. Per esempio:
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-callback` e
`https://<Admin_IP_address_or_FQDN>:<port>/api/v4/oidc-logged-out`

7. Seleziona **Salva**. Salva i valori dell'ID client e del client secret per utilizzarli in seguito.

Passaggio 2: Aggiungi un gruppo federato

Crea un gruppo o utilizza un gruppo esistente dal server Active Directory Federation Service (AD FS) per StorageGRID.

Fasi

1. In GRID Manager, seleziona **Configurazione > Gruppi di amministratori > Crea gruppo > Federa gruppo**.
2. Inserisci il nome del gruppo di server AD FS.
3. Seleziona **Lettura-scrittura** come modalità di accesso e **Accesso root** per i permessi.
4. Selezionare **Crea gruppo**.

Passaggio 3: Importa gruppi e utenti del server AD FS

Installa il client Okta Active Directory nel server AD FS. Poi importa i gruppi e gli utenti del server AD FS.

Fasi

1. In Okta, vai su **Directory > Integrazioni directory > Aggiungi directory > Aggiungi Active Directory**.
2. Seleziona **Configura Active Directory > Scarica agente**.
3. Segui subito la procedura di configurazione.



Se ritardi, la configurazione potrebbe bloccarsi e dovrai ricominciare da capo.

- a. Seleziona il dominio Active Directory.
 - b. Crea un account OktaService invece di collegare un utente esistente.
 - c. Seleziona le unità organizzative che contengono gli utenti e le unità organizzative che contengono i gruppi.
 - d. Seleziona il nome principale utente (UPN) che usa l'UPN di Active Directory come nome utente Okta.
Ad esempio: [user@domain.com](#)
4. Cerca l'applicazione **Okta AD Agent Management Utility**. Quindi, esegui l'applicazione e verifica che venga visualizzato il messaggio di stato `The agent is running`.



Il client Okta AD deve essere in esecuzione ogni volta che vuoi eseguire una sincronizzazione e un'importazione del server AD FS con Okta.

5. In Okta, vai su **Directory > Directory Integrations**.
6. Seleziona l'integrazione della directory che hai creato.
7. Seleziona **Importa > Importa ora**.
8. Seleziona l'utente che vuoi importare, poi seleziona **Conferma assegnazioni**.
9. Vai su **Directory > Persone** e conferma che l'utente sia stato importato correttamente.

Se lo stato dell'utente non è Attivo, seleziona **Attiva** e continua ad aggiornare la pagina finché l'utente non ha lo stato Attivo.

10. Vai su **Directory > Gruppi** e verifica che il gruppo per l'utente importato sia stato importato automaticamente.
11. Seleziona il gruppo e verifica che l'utente importato appartenga a questo gruppo.

Passaggio 4: Configura un claim

Configura un claim per includere i gruppi del server AD FS nel token di accesso. Quindi, verifica che il claim includa il gruppo importato per l'utente importato e l'applicazione Okta.

Fasi

1. In Okta, vai su **Directory > Gruppi**.
2. Seleziona il gruppo importato per l'utente importato.
3. Seleziona **Applications > Assign applications > Assign**.
4. Vai su **Sicurezza > API**.
5. Seleziona il server di autorizzazione **predefinito**.
6. Seleziona **Claims > Add Claim**. Quindi, crea un claim con le seguenti credenziali:
 - Nome: **groups**
 - Includi nel tipo di token: **ID Token - Always**
 - Tipo di valore: **Espressione**
 - Valore: **Groups.startsWith("active_directory","",100)**
 - Includi in: **Qualsiasi scope**
7. Vai su **Sicurezza > API**.
8. Seleziona il server di autorizzazione **predefinito**.
9. Seleziona la scheda **Anteprima token** e inserisci le seguenti credenziali per Request Properties:
 - Client OAuth/OIDC: **<application name>**
 - Tipo di concessione: **Codice di autorizzazione**
 - Utente: **Utente importato (indirizzo e-mail)**
 - Ambiti: **email, profilo, openid**
10. Selezionare **Esegui**.

Il gruppo importato appare nella scheda Anteprima id_token nel Payload.

Cosa c'è dopo

Dopo aver creato un'applicazione Okta, ["Configura SSO tramite OIDC"](#).

Crea connessioni service provider in PingFederate per OIDC in StorageGRID

Usa PingFederate per creare una connessione service provider (SP) per ciascun Admin Node per OpenID Connect (OIDC) nel tuo sistema.

Prima di iniziare

- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Si dispone di ["Guida di riferimento per l'amministratore"](#) per PingFederate Server. La documentazione di PingFederate fornisce istruzioni dettagliate e spiegazioni dettagliate.
- Tu hai il ["Autorizzazione amministratore"](#) per PingFederate Server.

A proposito di questa attività

Queste istruzioni riassumono come configurare il server PingFederate versione 12.1.10 come provider SSO

per StorageGRID. Se stai usando un'altra versione di PingFederate, potresti dover adattare queste istruzioni. Consulta la documentazione del server PingFederate per istruzioni dettagliate relative alla tua versione.

Utilizza le impostazioni predefinite, salvo diversa indicazione. In alcuni casi puoi utilizzare le impostazioni richieste dalla tua organizzazione, ad esempio le impostazioni per il metodo di autenticazione.

Passaggio 1: Crea l'archivio dati

Se non l'hai ancora fatto, crea un archivio dati per connettere PingFederate al LDAP server AD FS.

Fasi

1. Vai su **Sistema > Archivi dati e credenziali**.
2. Seleziona **Nuovo archivio dati**.
3. Per Tipo, seleziona **Directory (LDAP)**.
4. Selezionare **Avanti**.
5. In Configurazione LDAP:
 - Inserisci i valori per **Hostname**, **User DN** (username) e **Password**.
Utilizza i valori che hai usato quando ["configurazione della federazione delle identità"](#) in StorageGRID.
 - Per Active Directory, seleziona **Tipo LDAP**.

Passaggio 2: Crea il validatore delle credenziali della password

Se non l'hai ancora fatto, crea una convalida delle credenziali per la password.

Fasi

1. Seleziona **Password Credential Validators > Create New instance**.
2. Nella scheda Tipo, inserisci le seguenti informazioni:
 - a. NOME ISTANZA e ID ISTANZA: Puoi usare lo stesso valore per entrambi.
 - b. Tipo: Seleziona **LDAP Username Password Credential Validator**.
3. Selezionare **Avanti**.
4. Nella scheda Configurazione istanza, inserisci le seguenti informazioni:
 - LDAP DATASTORE: Seleziona il [archivio di dati](#) che hai creato.
 - RICERCA BASE: Inserisci le informazioni per il [Configurazione LDAP](#).
 - FILTRO DI RICERCA: Inserisci **sAMAccountName=\${username}**.
 - AMBITO DI RICERCA: Seleziona **Sottostruttura**.
5. Selezionare **Avanti**.
6. Nella scheda Contratto esteso, aggiungi i seguenti attributi: `memberOf`, `objectGUID`, `sAMAccountName`, `sn` e `userPrincipalName`
7. Seleziona **Avanti > Salva**.

Passaggio 3: Crea un'istanza dell'adattatore IdP

Se non l'hai ancora fatto, crea un'istanza dell'adattatore IdP (identity provider).



Ogni Admin Node nel tuo sistema StorageGRID deve disporre di una connessione IdP. Questo garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node. Puoi creare un'unica connessione IdP per tutti gli Admin Node (consigliato) oppure una connessione IdP diversa per ciascun Admin Node.

Fasi

1. Accedere a **Authentication > Integration > IdP Adapter**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda Tipo, inserisci le seguenti informazioni:
 - NOME ISTANZA e ID ISTANZA: Puoi usare lo stesso valore per entrambi.
 - TIPO: Seleziona **HTML Form IdP Adapter**.
4. Selezionare **Avanti**.
5. Nella scheda **Adattatore IdP**, seleziona **Aggiungi una nuova riga a 'Credential Validators'**.
6. Seleziona [validatore delle credenziali per la password](#) che hai creato.
7. Selezionare **Avanti**.
8. Nella scheda Contratto esteso, aggiungi gli attributi che hai mappato per il [validatore delle credenziali per la password](#).
9. Selezionare **Avanti**.
10. Nella scheda Attributi dell'adattatore, seleziona l'attributo **username** per Pseudonimo.
11. Seleziona **Avanti > Avanti**.
12. Rivedi il riepilogo e seleziona **Salva**.

Passaggio 4: Configura le impostazioni del server OAuth e del server di autorizzazione

Configura l'Authorization Server in modo che supporti i grant type accettati da StorageGRID.

Fasi

1. Vai su **Sistema > Impostazioni server di autorizzazione**.
2. Verifica che siano selezionate le seguenti opzioni per RIUTILIZZA LE CONCESSIONI DI ACCESSO PERSISTENTE ESISTENTI PER I TIPI DI CONCESSIONE:
 - IMPLICITO
 - CODICE DI AUTORIZZAZIONE
 - CREDENZIALI DELLA PASSWORD DEL PROPRIETARIO DELLA RISORSA



Se la tua azienda limita l'utilizzo delle RESOURCE OWNER PASSWORD CREDENTIALS, puoi utilizzare solo AUTHORIZATION CODE.

3. Per le impostazioni dei servizi Web amministrativi OAuth, seleziona [validatore delle credenziali per la password](#) che hai creato.

Passaggio 5: Definisci gli ambiti

Definisci gli ambiti in PingFederate.

Fasi

1. Vai su **Sistema > Impostazioni OAuth > Gestione ambito**.
2. Nella scheda Ambiti comuni, aggiungi i valori per **openid**, **email** e **profile**, se non sono già presenti.

Passaggio 6: Configura la mappatura dell'adattatore IdP

Configura la mappatura dell'adattatore IdP per associare gli attributi dell'IdP alle autorizzazioni persistenti rilasciate ai client, come i token di accesso o i token di aggiornamento.

Fasi

1. Vai su **Authentication > Policy Contract Grant Mapping**.
2. Seleziona **Mappatura delle concessioni dell'adattatore IdP**.
3. Dal menu a tendina SOURCE ADAPTER INSTANCE, seleziona la [Adattatore per moduli HTML](#) che hai creato.
4. Seleziona **Aggiungi mappatura > Contract Fulfillment**.
5. Nella sezione Origine, seleziona **Adapter** per USER_KEY e USER_NAME.
6. Nella sezione Valore, seleziona **sAMAccountName** per USER_KEY e **username** per USER_NAME.
7. Seleziona **Avanti > Avanti** per passare alla pagina di riepilogo.
8. Selezionare **Salva**.

Passaggio 7: Configura la mappatura delle credenziali del proprietario delle risorse

Configura la mappatura delle credenziali del proprietario delle risorse per assicurarti che le credenziali utente vengano convalidate correttamente durante l'autenticazione.

Fasi

1. Vai su **Authentication > Policy Contract Grant Mapping**.
2. Seleziona **Mappatura delle concessioni delle credenziali del proprietario della risorsa**.
3. Dal menu a tendina SOURCE PASSWORD VALIDATOR INSTANCE, seleziona l'[validatore delle credenziali per la password](#)istanza che hai creato.
4. Seleziona **Aggiungi mappatura > Contract Fulfillment**.
5. Aggiungi la mappatura per USER_KEY:
 - In Origine, seleziona **Password Credential Validator**.
 - Nella sezione Valore, seleziona **sAMAccountName**.
6. Seleziona **Avanti > Avanti** per passare alla pagina di riepilogo.
7. Selezionare **Salva**.

Passaggio 8: Crea o importa il certificato di firma

Se non lo si è già fatto, creare o importare il certificato di firma.

Fasi

1. Accedere a **sicurezza > chiavi e certificati di firma e decrittografia**.
2. Seleziona **Crea nuovo**, quindi inserisci le seguenti informazioni:
 - Nome comune (CN): deve essere il fully qualified domain name (FQDN) del server.
 - Organizzazione (Org): Inserisci il nome della tua organizzazione.

- Paese: Fornisci il codice paese di due lettere, ad esempio US per gli Stati Uniti.
- Algoritmo di chiave: Seleziona l'algoritmo di chiave appropriato, ad esempio **RSA**.
- Dimensione della chiave: impostata su **2048** bit.
- Algoritmo di firma: seleziona **RSA con SHA256** come algoritmo di firma per garantire operazioni crittografiche sicure.

Passaggio 9: Configura la gestione dei token di accesso

StorageGRID utilizza token di accesso per autenticare e autorizzare le richieste API in PingFederate.

Fasi

1. Vai su **Applicazioni > Gestione token di accesso**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda Tipo, inserisci le seguenti informazioni:
 - NOME ISTANZA e ID ISTANZA: Puoi usare lo stesso valore per entrambi.
 - Tipo: Verifica che il valore sia **JSON Web Tokens**.
4. Selezionare **Avanti**.
5. Nella scheda Configurazione istanza, inserisci le seguenti informazioni per i certificati:
 - ID CHIAVE: Inserisci un identificativo univoco per la chiave.
 - Certificato: Aggiungi il [certificato](#) che hai creato.
 - ALGORITMO JWS: Seleziona **RSA using SHA256**.
 - ID CHIAVE DEL CERTIFICATO DI FIRMA ATTIVO: Seleziona l'**ID CHIAVE** che hai creato in questo passaggio.
6. Seleziona **Avanti > Avanti**.
7. Nella scheda Contratto attributo token di accesso, seleziona **USER_KEY** per Nome attributo soggetto e **username** per Estendi il contratto.
8. Selezionare **Aggiungi**.
9. Seleziona **Avanti > Avanti > Avanti** per passare alla pagina di riepilogo.
10. Selezionare **Salva**.

Passaggio 10: Configura la mappatura del token di accesso

Configura la mappatura del token di accesso per utilizzare il token di accesso che hai creato.

Fasi

1. Vai su **Applicazioni > Access Token Mappings**.
2. Seleziona **Access Token Mappings**.
3. Seleziona **Aggiungi mappatura**.
4. Per il contesto, seleziona **Predefinito**.
5. Per Access Token Manager, seleziona il [token di accesso](#) che hai creato.
6. Seleziona **Avanti > Contract Fulfillment**:
7. Nella sezione Origine, seleziona **Persistent Grant** per il nome utente.

8. Nella sezione Valore, seleziona **USER_KEY** per il nome utente.
9. Seleziona **Avanti > Salva**.

Passaggio 11: Configura la policy OpenID Connect

Definisci le policy di OpenID Connect per l'accesso dei client agli attributi mappati secondo le specifiche OpenID.

Fasi

1. Vai su **Applicazioni > Client OAuth**.
2. Seleziona **OpenId Connect Policy Management > Add Policy**.
3. Nella scheda Gestisci criteri, inserisci le seguenti informazioni:
 - ID POLICY: Un identificativo univoco per la policy.
 - NOME DELLA POLICY: Un nome descrittivo per la policy.
 - GESTORE TOKEN DI ACCESSO: Seleziona il [token di accesso](#) che hai creato.
 - DURATA DEL TOKEN ID: Imposta la durata desiderata per il token ID, ad esempio 60 minuti o un'ora.
 - INCLUDI LE INFORMAZIONI UTENTE NEL TOKEN ID: Seleziona la casella per includere i dettagli utente nel token ID.
4. Selezionare **Avanti**.
5. Nella scheda Contratto attributi, rimuovi tutti gli attributi esistenti che non sono necessari per l'[archivio di dati](#) che hai creato. Mantieni solo gli attributi che desideri passare da Ping Authentication a StorageGRID.



Questo è un passaggio cruciale. Determina quali valori degli attributi sono inclusi nel token ID. StorageGRID eredita questi valori durante il processo di autenticazione.

6. Seleziona **Avanti > Avanti**.
7. Nella scheda Origine attributi e ricerca utente, seleziona **Aggiungi origine attributi**. Quindi inserisci le seguenti informazioni:
 - ID ORIGINE ATTRIBUTO e DESCRIZIONE ORIGINE ATTRIBUTO: Puoi usare lo stesso valore per entrambi.
 - ARCHIVIO DATI ATTIVO: Seleziona il [archivio di dati](#) che hai creato.
8. Selezionare **Avanti**.
9. Nella scheda LDAP Directory Search (Ricerca directory LDAP):
 - a. Inserire il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
 - b. Dal menu a tendina ROOT OBJECT CLASS, seleziona **objectClass**.
 - c. Dal menu a tendina ATTRIBUTO, aggiungi un attributo per ogni classe di oggetto che desideri mappare. Ad esempio:
 - InetOrgPerson: Aggiungi displayName, givenName o HomePhone.
 - utente: Aggiungi LocalID o userPrincipalName (upn).
 - in alto: Aggiungi memberOf o nome.
 - persona: Aggiungi sn.
10. Selezionare **Avanti**.

11. Nella scheda filtro LDAP, immettere **sAMAccountName={nome utente}**.

Devi personalizzare il filtro LDAP per assicurarti che StorageGRID recuperi gli attributi utente in base alla struttura specifica di Active Directory o LDAP della tua organizzazione. Consulta il tuo amministratore LDAP/AD per ottenere l'espressione di filtro appropriata per la tua configurazione.

12. Seleziona **Salva** e rivedi il riepilogo.

13. Nella scheda "Adempimento del contratto", inserisci le seguenti informazioni:

- Fonte: Seleziona la [archivio dati LDAP](#) che hai creato.
- Valore: Associa ciascun Attribute Contract al rispettivo valore.

14. Seleziona **Avanti > Avanti**.

15. Rivedi il riepilogo e seleziona **Salva**.

16. Vai su **Applicazioni > Client OAuth > Gestione delle policy di OpenID Connect**.

17. Verifica che la policy che hai creato sia impostata come policy predefinita.

Passaggio 12: Crea un client OAuth per il server OAuth

Crea un nuovo client OAuth per configurare le credenziali client necessarie e autorizzare le connessioni tra PingFederate e StorageGRID.

Fasi

1. Vai su **Applicazioni > Client OAuth**.

2. Seleziona **Aggiungi client**, quindi inserisci le seguenti informazioni:

- ID CLIENTE: Inserisci un valore univoco.
- AUTENTICAZIONE CLIENT: Seleziona **Client Secret**.
- CLIENT SECRET: Seleziona **CAMBIA SEGRETO > Genera segreto**.

Questo genera la chiave segreta per il client. Salva questa chiave per usarla più tardi.

- URI DI REINDIRIZZAMENTO: Fornisci gli URL di ritorno di StorageGRID nella sezione **URI di reindirizzamento**. Questi URL devono corrispondere agli URL configurati in StorageGRID per OAuth:
Ad esempio:

- `https://<Admin IP or Hostname>/api/v4/oidc-callback`

- `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`

- TIPI DI CONCESSIONE CONSENTITI: Seleziona le seguenti opzioni:

- **Codice di autorizzazione:** questo avvia il flusso OAuth.
- **Refresh Token:** Ottieni un nuovo token quando un token di accesso scade.
- **Credenziali del proprietario della risorsa:** Se hai bisogno di accedere direttamente alle credenziali utente per l'autenticazione.

- OPENID CONNECT: Seleziona **RSA utilizzando SHA-256** come algoritmo di firma del token ID.

- Modalità di logout: seleziona **OIDC Back-Channel**.

- URI di logout front-channel, URI di logout back-channel e URI di reindirizzamento post-logout: aggiungi l'URI di logout di StorageGRID: `https://<Admin IP or Hostname>/api/v4/oidc-logged-out`

3. Selezionare **Salva**.

Cosa c'è dopo

Dopo aver creato le connessioni SP, "[Configura SSO tramite OIDC](#)".

Configura SSO in StorageGRID usando OIDC

Segui la procedura guidata di configurazione di SSO per OpenID Connect (OIDC) e accedi alla modalità sandbox per configurare e testare il single sign-on (SSO) prima di abilitarlo per tutti gli utenti di StorageGRID. Dopo aver abilitato SSO, puoi tornare alla modalità sandbox quando necessario per modificare o testare nuovamente la configurazione.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[Autorizzazione di accesso root](#)".
- Hai configurato il client OIDC nel provider di identità SSO per il tuo sistema StorageGRID.
- Hai "[federazione di identità configurata](#)" per il tuo sistema StorageGRID.

Passaggio 1: Fornisci i dettagli del provider di identità

Accedi alla procedura guidata e compila i campi nella pagina "Fornisci i dettagli del provider di identità".

Fasi

1. Accedi alla procedura guidata per configurare le impostazioni SSO:

- a. Selezionare **Configurazione > Controllo accessi > Single sign-on**. Viene visualizzata la pagina Single Sign-On.



Se il pulsante Configura impostazioni SSO è disabilitato, conferma di aver configurato il provider di identità come origine dell'identità federata. Fare riferimento a "[Requisiti e considerazioni per il single sign-on](#)".

- b. Seleziona **Configura impostazioni SSO**. Viene visualizzata la pagina Fornisci dettagli provider di identità.

2. In **Protocollo**, seleziona **OIDC**.

3. Selezionare **tipo SSO** dall'elenco a discesa.

4. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.

- **Usa certificato CA del sistema operativo:** Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Usa certificato CA personalizzato:** Utilizza un certificato CA personalizzato per proteggere la connessione.

Se selezioni questa impostazione:

- i. Individuare la posizione del certificato CA.
- ii. Caricare il file del certificato CA.

- **Non utilizzare TLS:** Non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, eseguire immediatamente ["Riavviare il servizio Mgmt-api sui nodi Admin"](#) il test di un SSO corretto in Grid Manager.

5. Selezionare **Continua**. Viene visualizzata la pagina Fornisci l'identificativo della parte affidabile.

Passaggio 2: Inserisci le informazioni del cliente

Completa i campi nella fase "Inserisci le informazioni del cliente" della procedura guidata.

Fasi

1. Specifica l'identificativo della **relying party** per StorageGRID. Questo valore controlla il nome che usi per ogni configurazione OIDC.
 - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere SG o StorageGRID.
 - Se la tua griglia include più di un Admin Node, includi la stringa [HOSTNAME] nell'identificatore. Per esempio, SG-[HOSTNAME]. Includendo questa stringa, otterrai una tabella che mostra la configurazione OIDC per ogni Admin Node nella griglia, in base all'hostname del nodo.



Devi configurare OIDC per gli Admin Node nel tuo sistema StorageGRID. Questo garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node. Puoi usare la stessa configurazione OIDC per tutti gli Admin Node (consigliato) oppure impostare una configurazione OIDC diversa per ciascun Admin Node.

2. Inserisci l'**ID client**, il **client secret** e l'**URL dell'endpoint OpenID** per ogni identificatore della relying party.
3. Seleziona **Salva e accedi alla modalità sandbox**.

Passaggio 3: Test configurazione

Dopo essere entrato in modalità sandbox, puoi completare e testare la configurazione per il tipo di SSO selezionato.

La modalità sandbox semplifica la configurazione avanti e indietro e permette di testare tutte le impostazioni prima di abilitare SSO. StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, solo gli utenti federati e gli utenti locali possono accedere.

Fasi

1. Nella pagina Configura SSO, individua il collegamento nel passaggio Configurazione test della procedura guidata.

L'URL deriva dal valore immesso nel campo **Federation service name**.
2. Seleziona il link oppure copia e incolla l'URL in una nuova scheda per accedere alla pagina di accesso del tuo identity provider.
3. Inserisci il tuo nome utente e la tua password federati.
 - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un banner verde.

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
4. Segui i passaggi della procedura guidata per accedere alla pagina Test configurazione per ciascun Admin Node nella tua griglia.
 5. Ripeti i passaggi [2](#) e [3](#) per verificare la connessione SSO per ogni Admin Node.

Passaggio 4: Abilita single sign-on

Dopo aver verificato che puoi utilizzare il single sign-on per accedere a ciascun Admin Node, puoi abilitare il single sign-on per l'intero sistema StorageGRID.



Quando l'SSO è abilitato, tutti gli utenti devono utilizzare l'SSO per accedere a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Gli utenti locali non possono più accedere a StorageGRID. StorageGRID non fornisce uno script di autenticazione di esempio per tutti i provider SSO supportati.

Fasi

1. Nel passaggio Configurazione test della procedura guidata di configurazione SSO, seleziona **Abilita SSO**.
2. Rivedi il messaggio di avviso e seleziona **Abilita SSO**.

Ora è abilitato l'accesso singolo. Viene visualizzata la pagina Single Sign-On, che ora include i dettagli per l'SSO appena configurato.

3. Per modificare la configurazione, selezionare **Modifica**.
4. Per disabilitare single sign-on, seleziona **Disabilita**.



Se si utilizza il portale di Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere all'ID Entra, assicurarsi che l'utente del portale di Azure sia anche un utente StorageGRID autorizzato (un utente in un gruppo federato che è stato importato in StorageGRID) oppure disconnettersi dal portale di Azure prima di tentare di accedere a StorageGRID.

Configura SSO con SAML

Scopri come configurare l'SSO in StorageGRID usando SAML

Configurare il single sign-on (SSO) in StorageGRID permette a StorageGRID (il service provider) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti.

Puoi configurare l'SSO in StorageGRID utilizzando OpenID Connect (OIDC) o SAML. Segui questi passaggi high-level per configurare l'SSO in StorageGRID utilizzando SAML oppure scopri di più ["Configurare SSO usando OIDC"](#).



Configura SSO

Seleziona la procedura guidata Configura SSO per SAML. Poi configura SSO con il tuo identity provider ed entra in modalità sandbox.

Scopri di più ["configurare l'SSO usando SAML"](#)

2

Configura il provider di identità

In base al provider di identità SSO che vuoi utilizzare, puoi selezionare Active Directory o Entra ID come tipo di servizio LDAP per la federazione delle identità.

- Per Active Directory Federation Service (AD FS), puoi usare AD FS, Entra ID o il provider di identità PingFederate.
- Per Entra ID, puoi usare solo il provider di identità Entra ID.

Utilizza il software del provider di identità SSO per configurare SAML per ciascun Admin Node nella tua griglia.

- Scopri ["creare un gruppo di applicazioni per ogni Admin Node"](#) in Active Directory
- Scopri ["creare un'applicazione per ogni Admin Node"](#) in Entra ID
- Scopri ["creare una service provider connection per ogni Admin Node"](#) in PingFederate

3

Configurazione di test

Dopo aver configurato SAML per ciascun nodo amministratore, torna alla procedura guidata di configurazione SSO e testa la configurazione.

Scopri di più ["test della configurazione per SSO"](#)

4

Abilita SSO

Abilita l'SSO per tutti gli utenti di StorageGRID.

Scopri di più ["Abilitare l'SSO per gli utenti di StorageGRID"](#)

Configura SSO in StorageGRID usando SAML

Segui la procedura guidata di configurazione SSO per SAML ed entra in modalità sandbox per configurare e testare il single sign-on (SSO) prima di abilitarlo per tutti gli utenti StorageGRID. Dopo aver abilitato SSO, puoi tornare alla modalità sandbox quando necessario per modificare o ritestare la configurazione.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione 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 Entra ID, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory Federation Service (ad FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

A proposito di questa attività

Quando SSO è attivato e un utente tenta di accedere a un nodo amministratore, StorageGRID invia una richiesta di autenticazione al provider di identità SSO. A sua volta, il provider di identità SSO invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autenticazione ha avuto esito positivo. Per le richieste riuscite:

- La risposta di Active Directory o PingFederate include un UUID (Universally Unique Identifier) per l'utente.
- La risposta da Entra ID include un nome principale utente (UPN).

Per consentire a StorageGRID (il service provider) e al provider di identità SSO di comunicare in modo sicuro in merito alle richieste di autenticazione degli utenti, devi completare queste attività:

1. Configurare le impostazioni in StorageGRID.
2. Usa il software del provider di identità SSO per creare una relying party trust (AD FS), una Enterprise Application (Entra ID) o un Service Provider (PingFederate) per ciascun Admin Node.
3. 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.

Passaggio 1: Fornisci i dettagli del provider di identità

Accedi alla procedura guidata e compila i campi nella pagina "Fornisci i dettagli del provider di identità".

Fasi

1. Accedi alla procedura guidata:
 - a. Selezionare **Configurazione > Controllo accessi > Single sign-on**. Viene visualizzata la pagina Single Sign-On.



Se il pulsante Configura impostazioni SSO è disabilitato, conferma di aver configurato il provider di identità come origine dell'identità federata. Fare riferimento a ["Requisiti e considerazioni per il single sign-on"](#).

- b. Seleziona **Configura impostazioni SSO**. Viene visualizzata la pagina Fornisci dettagli provider di identità.
2. In **Protocollo**, seleziona **SAML**.
 3. Selezionare **tipo SSO** dall'elenco a discesa.
 4. Se hai selezionato Active Directory come tipo di SSO, immetti 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 Gestione server Windows. Selezionare **Tools > ad FS Management**. Dal menu Action (azione), selezionare **Edit Federation Service Properties** (Modifica proprietà servizio federazione). Il nome del servizio della federazione viene visualizzato nel secondo campo.

5. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.

- **Usa certificato CA del sistema operativo:** Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Usa certificato CA personalizzato:** Utilizza un certificato CA personalizzato per proteggere la connessione.

Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

- **Non utilizzare TLS:** Non utilizzare un certificato TLS per proteggere la connessione.



Se si modifica il certificato CA, eseguire immediatamente "[Riavviare il servizio Mgmt-api sui nodi Admin](#)" il test di un SSO corretto in Grid Manager.

6. Selezionare **Continua**. Viene visualizzata la pagina Fornisci l'identificativo della parte affidabile.

Passaggio 2: Fornisci trust della relying party, applicazioni aziendali o connessioni SP

Completa i campi nella Fase 2 della procedura guidata in base al tipo di SSO che hai selezionato.

Active Directory

Completa i campi nella fase **Fornisci l'identificativo della parte affidabile**.

Fasi

1. Specificare l'**identificatore della parte affidabile** per StorageGRID. Questo valore controlla il nome utilizzato per ogni trust della relying party in AD FS.
 - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere SG o StorageGRID.
 - Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG-[HOSTNAME] . L'inclusione di questa stringa genera una tabella che mostra l'identificatore della parte affidabile per ciascun nodo di amministrazione nella griglia, in base al nome host del nodo.



È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

2. Seleziona **Salva e accedi alla modalità sandbox**.

Entra ID

Completa i campi nella fase **Configura le applicazioni aziendali**.

Fasi

1. Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ciascuna applicazione aziendale in Entra ID.
 - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere SG o StorageGRID.
 - Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG-[HOSTNAME] . L'inclusione di questa stringa genera una tabella che mostra il nome di un'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



È necessario creare un'applicazione aziendale per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un'applicazione aziendale per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

2. Segui i passaggi in "[Crea applicazioni aziendali in Entra ID](#)" per creare un'applicazione aziendale per ciascun Admin Node elencato nella tabella.
3. Dall'ID Entra, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.
4. Dopo aver copiato e incollato un URL dei metadati di federazione per tutti i nodi amministrativi, seleziona **Salva e accedi alla modalità sandbox**.

PingFederate

Completa i campi nella fase **Fornisci SP connection ID**.

Fasi

1. Nella sezione Provider di servizi (SP), specificare **ID connessione SP** per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.
 - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere SG o StorageGRID.
 - Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG-[HOSTNAME] . L'inclusione di questa stringa genera 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 amministratore nel sistema StorageGRID. La disponibilità di una connessione SP per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

2. Specificare l'URL dei metadati della federazione per ciascun nodo amministratore nel campo **URL metadati federazione**.

Utilizzare il seguente formato:

```
https://<Federation Service  
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection  
ID>
```

3. Seleziona **Salva e accedi alla modalità sandbox**.

Passaggio 3: Configura i trust delle relying party, le applicazioni aziendali o le connessioni SP

Dopo aver salvato la configurazione ed essere entrati in modalità sandbox, è possibile completare e testare la configurazione per il tipo di SSO selezionato.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, solo gli utenti federati e gli utenti locali possono effettuare l'accesso.

Active Directory

Fasi

1. Accedere a 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 Configura SSO.

È necessario creare un trust per ciascun nodo di amministrazione mostrato nella tabella.

Per le istruzioni, vai su ["Creazione di trust di parti di base in ad FS"](#).

Entra ID

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
 - a. Accedere al nodo.
 - b. Selezionare **Configurazione > Controllo accessi > Single sign-on**.
 - c. Scaricare e salvare i metadati SAML per quel nodo.
3. Vai al portale di Azure.
4. Segui i passaggi in ["Crea applicazioni aziendali in Entra ID"](#) per caricare il file di metadati SAML per ciascun Admin Node nella corrispondente applicazione enterprise Entra ID.

PingFederate

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
 - a. Accedere al nodo.
 - b. Selezionare **Configurazione > Controllo accessi > Single sign-on**.
 - c. Scaricare e salvare i metadati SAML per quel nodo.
3. Accedere a PingFederate.
4. ["Creare una o più connessioni del provider di servizi \(SP\) per StorageGRID"](#). Usa l'ID di connessione SP per ciascun nodo Admin (mostrato nella tabella nella pagina Configura SSO) e i metadati SAML che hai scaricato per quel nodo Admin.

È necessario creare una connessione SP per ciascun nodo di amministrazione mostrato nella tabella.

Passaggio 4: Testa la configurazione

Prima di imporre l'uso dell'accesso singolo per l'intero sistema StorageGRID, verificare che l'accesso singolo e la disconnessione singola siano configurati correttamente per ciascun nodo di amministrazione.

Active Directory

Fasi

1. Nella pagina Configura SSO, individua il collegamento nel passaggio Configurazione test della procedura guidata.

L'URL deriva dal valore immesso nel campo **Federation service name**.

2. Selezionare il collegamento oppure copiare e incollare l'URL in un browser per accedere alla pagina di accesso del provider di identità.
3. Per confermare che è possibile utilizzare SSO per accedere a StorageGRID, selezionare **Accedi a uno dei seguenti siti**, selezionare l'identificativo della parte di base per il nodo di amministrazione principale e selezionare **Accedi**.
4. Immettere il nome utente e la password federated.
 - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.
 - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
5. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

Entra ID

Fasi

1. Vai alla pagina Single Sign-on nel portale Azure.
2. Selezionare **Test dell'applicazione**.
3. Immettere le credenziali di un utente federated.
 - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.
 - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
4. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

PingFederate

Fasi

1. Dalla pagina Configura SSO, seleziona il primo collegamento nel messaggio della modalità Sandbox.

Selezionare e verificare un collegamento alla volta.
2. Immettere le credenziali di un utente federated.
 - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.
 - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
3. Selezionare il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

Se viene visualizzato un messaggio Page Expired (pagina scaduta), selezionare il pulsante **Back** (Indietro) nel browser e inviare nuovamente le credenziali.

Passaggio 5: Abilita single sign-on

Dopo aver verificato che puoi utilizzare il single sign-on per accedere a ciascun Admin Node, puoi abilitare il single sign-on per l'intero sistema StorageGRID.



Quando SSO è attivato, tutti gli utenti devono utilizzare SSO per accedere a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Gli utenti locali non possono più accedere a StorageGRID.

Fasi

1. Nel passaggio Configurazione test della procedura guidata di configurazione SSO, seleziona **Abilita SSO**.
2. Rivedi il messaggio di avviso e seleziona **Abilita SSO**.

Ora è abilitato l'accesso singolo. Viene visualizzata la pagina Single Sign-On, che ora include i dettagli per l'SSO appena configurato.

3. Per modificare la configurazione, selezionare **Modifica**.
4. Per disabilitare l'accesso singolo, seleziona **Disabilita SSO**.



Se si utilizza il portale di Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere all'ID Entra, assicurarsi che l'utente del portale di Azure sia anche un utente StorageGRID autorizzato (un utente in un gruppo federato che è stato importato in StorageGRID) oppure disconnettersi dal portale di Azure prima di tentare di accedere a StorageGRID.

E ora?

Dopo aver configurato l'SSO tramite SAML, configura il provider di identità per gli Admin Nodes.

Se il tuo provider di identità è...	Devi...
Active Directory	"Crea un gruppo di applicazioni per ogni Admin Node"
Entra ID	"Crea un'applicazione per ogni Admin Node"
PingFederate	"Crea una connessione service provider per ogni Admin Node"

Crea trust di relying party in AD FS per SAML in StorageGRID

Devi usare Active Directory Federation Services (AD FS) per creare una relying party trust per ogni Admin Node per SAML nel tuo sistema. Puoi creare relying party trust usando i comandi PowerShell, importando i metadati SAML da StorageGRID o inserendo i dati manualmente.

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **ad FS** come tipo di SSO.

- Hai **"entrato in modalità sandbox"** in Grid Manager.
- 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 Configura SSO StorageGRID .



È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.
- Se si crea manualmente l'attendibilità del componente di base, si dispone del certificato personalizzato caricato per l'interfaccia di gestione di StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

A proposito di questa attività

Queste istruzioni si applicano a Windows Server 2016 ad FS. Se si utilizza una versione diversa di ad FS, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

Creare un trust di parte con Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust di parti.

Fasi

1. Dal menu Start di Windows, selezionare con il pulsante destro del mouse l'icona PowerShell e selezionare **Esegui come amministratore**.
2. Al prompt dei comandi di PowerShell, immettere il seguente comando:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Per *Admin_Node_Identifier*, immettere l'identificatore del gruppo di riferimento per il nodo di amministrazione, esattamente come viene visualizzato nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1.
- Per *Admin_Node_FQDN*, immettere il nome di dominio completo per lo stesso nodo amministrativo. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

3. Da Gestione server Windows, selezionare **Strumenti > Gestione di ad FS**.

Viene visualizzato lo strumento di gestione di ad FS.

4. Selezionare **ad FS > Trust di parte**.

Viene visualizzato l'elenco dei trust della parte che si basa.

5. Aggiungere un criterio di controllo degli accessi al trust della parte di base appena creato:
 - a. Individuare la fiducia della parte di base appena creata.

- b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit Access Control Policy** (Modifica policy di controllo degli accessi).
 - c. Selezionare un criterio di controllo degli accessi.
 - d. Selezionare **Applica e OK**
6. Aggiungere una policy di emissione delle richieste di rimborso al nuovo Trust della parte di base creato:
- a. Individuare la fiducia della parte di base appena creata.
 - b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
 - c. Selezionare **Aggiungi regola**.
 - d. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
 - e. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.
 - f. Per l'archivio attributi, selezionare **Active Directory**.
 - g. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
 - h. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
 - i. Selezionare **fine**, quindi **OK**.
7. Verificare che i metadati siano stati importati correttamente.
- a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
 - b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.
- Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.
8. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
9. Al termine, torna a StorageGRID e "[testare tutti i trust delle parti affidanti](#)" per verificare che siano configurati correttamente.

Creare un trust per la parte che si basa importando i metadati della federazione

È possibile importare i valori per ciascun trust di parte che si basa accedendo ai metadati SAML per ciascun nodo di amministrazione.

Fasi

1. In Gestione server Windows, selezionare **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, selezionare **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e selezionare **Avvia**.
4. Selezionare **Importa dati relativi alla parte che si basa pubblicati online o su una rete locale**.
5. In **Federation metadata address (nome host o URL)**, digitare la posizione dei metadati SAML per questo nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-metadata`

Per *Admin_Node_FQDN*, immettere il nome di dominio completo per lo stesso nodo amministrativo. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

6. Completare la procedura guidata Trust Party, salvare il trust della parte che si basa e chiudere la procedura guidata.



Quando si immette il nome visualizzato, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1.

7. Aggiungere una regola di richiesta di rimborso:
 - a. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
 - b. Selezionare **Aggiungi regola**:
 - c. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
 - d. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

- e. Per l'archivio attributi, selezionare **Active Directory**.
 - f. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
 - g. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
 - h. Selezionare **fine**, quindi **OK**.
8. Verificare che i metadati siano stati importati correttamente.
 - a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
 - b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.

9. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
10. Al termine, torna su StorageGRID e "[testare tutti i trust delle parti affidanti](#)" per confermare che siano configurati correttamente.

Creare manualmente un trust per la parte che si basa

Se si sceglie di non importare i dati per i trust della parte di base, è possibile inserire i valori manualmente.

Fasi

1. In Gestione server Windows, selezionare **Strumenti**, quindi selezionare **Gestione di ad FS**.

2. In azioni, selezionare **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e selezionare **Avvia**.
4. Selezionare **Inserire manualmente i dati relativi alla parte di base** e selezionare **Avanti**.
5. Completare la procedura guidata Trust Party:

- a. Immettere un nome visualizzato per questo nodo di amministrazione.

Per coerenza, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, SG-DC1-ADM1.

- b. Saltare il passaggio per configurare un certificato di crittografia token opzionale.
- c. Nella pagina Configure URL (Configura URL), selezionare la casella di controllo **Enable support for the SAML 2.0 WebSSO Protocol** (attiva supporto per il protocollo SAML WebSSO).
- d. Digitare l'URL dell'endpoint del servizio SAML per il nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-response`

Per *Admin_Node_FQDN*, immettere il nome di dominio completo per il nodo Admin. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

- e. Nella pagina Configure Identifier (Configura identificatori), specificare l'identificativo della parte di base per lo stesso nodo di amministrazione:

Admin_Node_Identifier

Per *Admin_Node_Identifier*, immettere l'identificatore del gruppo di riferimento per il nodo di amministrazione, esattamente come viene visualizzato nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1.

- f. Rivedere le impostazioni, salvare l'attendibilità della parte che si basa e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Edit Claim Issuance Policy (Modifica policy di emissione richieste di



Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).

6. Per avviare la procedura guidata Claim Rule, selezionare **Add Rule**:
 - a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
 - b. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.
 - c. Per l'archivio attributi, selezionare **Active Directory**.
 - d. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
 - e. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping

(mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.

f. Selezionare **fine**, quindi **OK**.

7. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.

8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):

a. Selezionare **Add SAML** (Aggiungi SAML).

b. Selezionare **Endpoint Type > SAML Logout**.

c. Selezionare **binding > Redirect**.

d. Nel campo **Trusted URL**, immettere l'URL utilizzato per la disconnessione singola (SLO) da questo nodo di amministrazione:

```
https://Admin_Node_FQDN/api/saml-logout
```

Per *Admin_Node_FQDN*, immettere il nome di dominio completo del nodo amministrativo. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per il trust della parte che si basa:

a. Aggiungere il certificato personalizzato:

- Se si dispone del certificato di gestione personalizzato caricato su StorageGRID, selezionare il certificato.
- Se non si dispone del certificato personalizzato, accedere al nodo Admin, andare nella directory del nodo `/var/local/mgmt-api Admin` e aggiungere il file del `custom-server.crt` certificato.



(`server.crt` Si sconsiglia l'utilizzo del certificato predefinito del nodo amministrativo).
Se il nodo Admin non riesce, il certificato predefinito viene rigenerato quando si ripristina il nodo ed è necessario aggiornare il trust della parte che si basa.

b. Selezionare **Applica e OK**.

Le proprietà della parte di base vengono salvate e chiuse.

10. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.

11. Al termine, torna su StorageGRID e "[testare tutti i trust delle parti affidanti](#)" per confermare che siano configurati correttamente.

Crea applicazioni aziendali in Entra ID per SAML in StorageGRID

Utilizza Entra ID per creare un'applicazione aziendale per ciascun Admin Node per SAML nel tuo sistema.

Prima di iniziare

- Hai iniziato a configurare l'accesso Single Sign-On per StorageGRID e hai selezionato **Entra ID** come tipo di SSO.
- Hai "[entrato in modalità sandbox](#)" in Grid Manager.

- 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 Configura SSO.



È necessario creare un'applicazione aziendale per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un'applicazione aziendale per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di applicazioni aziendali in Entra ID.
- Hai un account Entra ID con un abbonamento attivo.
- Nell'account Entra ID ricopri uno dei seguenti ruoli: Amministratore globale, Amministratore dell'applicazione cloud, Amministratore dell'applicazione o proprietario del servizio principale.

Passaggio 1: Accedi a Entra ID

Fasi

1. Accedere a ["Portale Azure"](#).
2. Vai a ["Entra ID"](#).
3. Selezionare ["Applicazioni aziendali"](#).

Passaggio 2: Crea applicazioni aziendali e salva la configurazione SSO di StorageGRID

Per salvare la configurazione SSO per Entra ID in StorageGRID, è necessario utilizzare Entra ID per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copia gli URL dei metadati della federazione dall'ID Entra e incollali nei campi **URL metadati della federazione** corrispondenti nella pagina Configura SSO.

Fasi

1. Ripetere i passaggi seguenti per ciascun nodo di amministrazione.
 - a. Nel riquadro Applicazioni aziendali Entra ID, selezionare **Nuova applicazione**.
 - b. Selezionare **Crea la tua applicazione**.
 - c. Per il nome, inserisci il **Nome dell'applicazione aziendale** che hai copiato dalla tabella dei dettagli del nodo di amministrazione nella pagina Configura SSO.
 - d. Lasciare selezionato il pulsante di opzione **integra qualsiasi altra applicazione che non trovi nella galleria (non-gallery)**.
 - e. Selezionare **Crea**.
 - f. Selezionare il collegamento **Get Started** nel campo **2. Impostare la casella Single Sign on** (accesso singolo) oppure selezionare il collegamento **Single Sign-on** (accesso singolo) nel margine sinistro.
 - g. Selezionare la casella **SAML**.
 - h. Copiare l'URL * dei metadati dell'App Federation, disponibile nella sezione **fase 3 certificato di firma SAML**.
 - i. Vai alla pagina Configura SSO e incolla l'URL nel campo **URL metadati federazione** che corrisponde al **Nome applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati della federazione per ciascun nodo di amministrazione e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, seleziona **Salva** nella pagina Configura SSO.

Passaggio 3: Scarica i metadati SAML per ogni Admin Node

Una volta salvata la configurazione SSO, è possibile scaricare un file di metadati SAML per ciascun nodo amministratore nel sistema StorageGRID.

Fasi

1. Ripetere questi passaggi per ciascun nodo di amministrazione.
 - a. Accedere a StorageGRID dal nodo di amministrazione.
 - b. Selezionare **Configurazione > Controllo accessi > Single sign-on**.
 - c. Selezionare il pulsante per scaricare i metadati SAML per il nodo di amministrazione.
 - d. Salva il file che caricherai in Entra ID.

Passaggio 4: Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ciascun nodo di amministrazione StorageGRID, eseguire i seguenti passaggi in Entra ID:

Fasi

1. Tornare al portale Azure.
2. Ripetere questi passaggi per ogni applicazione aziendale:



Potrebbe essere necessario aggiornare la pagina Enterprise Applications (applicazioni aziendali) per visualizzare le applicazioni aggiunte in precedenza nell'elenco.

- a. Accedere alla pagina Proprietà dell'applicazione aziendale.
 - b. Impostare **assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).
 - c. Vai alla pagina Single Sign-on.
 - d. Completare la configurazione SAML.
 - e. Selezionare il pulsante **carica file di metadati** e selezionare il file di metadati SAML scaricato per il nodo di amministrazione corrispondente.
 - f. Una volta caricato il file, selezionare **Salva**, quindi selezionare **X** per chiudere il riquadro. Viene visualizzata nuovamente la pagina Set up Single Sign-on with SAML (Configura Single Sign-on con SAML).
3. ["Testare ogni applicazione"](#).

Crea connessioni service provider in PingFederate per SAML in StorageGRID

Utilizza PingFederate per creare una connessione service provider (SP) per ciascun Admin Node per SAML nel tuo sistema. Per velocizzare il processo, importerai i metadati SAML da StorageGRID.

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **Ping Federate** come tipo di SSO.
- Hai ["entrato in modalità sandbox"](#) in Grid Manager.
- Hai l'*ID di connessione SP * per ogni nodo amministrativo nel tuo sistema. Puoi trovare questi valori nella

tabella dei dettagli dei nodi di amministrazione nella pagina Configura SSO.

- Sono stati scaricati i **metadati SAML** per ciascun nodo di amministrazione nel sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Si dispone di ["Guida di riferimento per l'amministratore"](#) per PingFederate Server. La documentazione di PingFederate fornisce istruzioni dettagliate e spiegazioni dettagliate.
- Tu hai il ["Autorizzazione amministratore"](#) per PingFederate Server.

A proposito di questa attività

Queste istruzioni riepilogano come configurare PingFederate Server versione 10.3 come provider SSO per StorageGRID. Se si utilizza un'altra versione di PingFederate, potrebbe essere necessario adattare queste istruzioni. Per istruzioni dettagliate sulla release, consultare la documentazione di PingFederate Server.

Completare i prerequisiti in PingFederate

Prima di poter creare le connessioni SP da utilizzare per StorageGRID, è necessario completare le attività dei prerequisiti in PingFederate. Quando si configurano le connessioni SP, verranno utilizzate le informazioni di questi prerequisiti.

Creare un archivio di dati

Se non lo si è già fatto, creare un archivio dati per connettere PingFederate al server LDAP di ad FS. Utilizzare i valori utilizzati ["configurazione della federazione delle identità"](#) in StorageGRID.

- **Tipo:** Directory (LDAP)
- **LDAP Type:** Active Directory
- **Binary Attribute Name** (Nome attributo binario): Inserire **objectGUID** nella scheda LDAP Binary Attributes (attributi binari LDAP) esattamente come mostrato.

Crea validatore credenziale password

Se non l'hai ancora fatto, crea una convalida delle credenziali per la password.

- **Type:** LDAP Username Password Credential Validator
- **Data store:** Selezionare il data store creato.
- **Base di ricerca:** Immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca:** SAMAccountName={nomeutente}
- **Scopo:** Sottostruttura

Crea istanza dell'adattatore IdP

Se non lo si è già fatto, creare un'istanza dell'adattatore IdP.

Fasi

1. Accedere a **Authentication > Integration > IdP Adapter**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda tipo, selezionare **HTML Form IdP Adapter**.
4. Nella scheda IdP Adapter, selezionare **Aggiungi una nuova riga a "Credential Validators"**.

5. Seleziona il [validatore delle credenziali per la password](#) che hai creato.
6. Nella scheda attributi adattatore, selezionare l'attributo **nome utente** per **pseudonimo**.
7. Selezionare **Salva**.

Creare o importare un certificato di firma

Se non lo si è già fatto, creare o importare il certificato di firma.

Fasi

1. Accedere a **sicurezza > chiavi e certificati di firma e decrittografia**.
2. Creare o importare il certificato di firma.

Creare una connessione SP in PingFederate

Quando si crea una connessione SP in PingFederate, si importano i metadati SAML scaricati da StorageGRID per il nodo di amministrazione. Il file di metadati contiene molti dei valori specifici necessari.



È necessario creare una connessione SP per ciascun nodo amministratore nel sistema StorageGRID, in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Seguire queste istruzioni per creare la prima connessione SP. Quindi, visitare il sito Web [Creare ulteriori connessioni SP](#) per creare eventuali connessioni aggiuntive.

Scegliere il tipo di connessione SP

Fasi

1. Accedere a **applicazioni > integrazione > connessioni SP**.
2. Selezionare **Crea connessione**.
3. Selezionare **non utilizzare un modello per questa connessione**.
4. Selezionare **browser SSO Profiles** (profili SSO browser) e **SAML 2.0** come protocollo.

Importare metadati SP

Fasi

1. Nella scheda Importa metadati, selezionare **file**.
2. Seleziona il file di metadati SAML scaricato dalla pagina Configura SSO per il nodo di amministrazione.
3. Esaminare il riepilogo dei metadati e le informazioni fornite nella scheda General Info (informazioni generali).

L'ID dell'entità del partner e il nome della connessione sono impostati sull'ID della connessione StorageGRID SP. (Ad esempio, 10.96.105.200-DC1-ADM1-105-200). L'URL di base è l'IP del nodo di amministrazione StorageGRID.

4. Selezionare **Avanti**.

Configurare IdP browser SSO

Fasi

1. Dalla scheda SSO del browser, selezionare **Configure browser SSO** (Configura SSO browser).

2. Nella scheda SAML profiles (profili SAML), selezionare le opzioni **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Assertion Lifetime (durata asserzione), non apportare modifiche.
5. Nella scheda Assertion Creation (creazione asserzione), selezionare **Configure Assertion Creation (Configura creazione asserzione)**.
 - a. Nella scheda Identity Mapping (mappatura identità), selezionare **Standard**.
 - b. Nella scheda Contratto attributo, utilizzare **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere il `urn:oid`, non utilizzato.

Istanza dell'adattatore di mappatura

Fasi

1. Nella scheda Authentication Source Mapping (mappatura origine autenticazione), selezionare **Map New Adapter Instance** (mappatura nuova istanza adattatore).
2. Nella scheda istanza scheda, selezionare il [istanza dell'adattatore](#) creato.
3. Nella scheda Mapping Method (metodo di mappatura), selezionare **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda origine attributo e Ricerca utente, selezionare **Aggiungi origine attributo**.
5. Nella scheda Archivio dati, fornire una descrizione e selezionare l'[archivio di dati](#) aggiunta.
6. Nella scheda LDAP Directory Search (Ricerca directory LDAP):
 - Inserire il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
 - Per l'ambito di ricerca, selezionare **sottostruttura**.
 - Per la classe di oggetti Root, cercare e aggiungere uno dei seguenti attributi: **ObjectGUID** o **userPrincipalName**.
7. Nella scheda LDAP Binary Attribute Encoding Types (tipi di codifica attributi binari LDAP), selezionare **Base64** come attributo **objectGUID**.
8. Nella scheda filtro LDAP, immettere **sAMAccountName={nome utente}**.
9. Nella scheda adempimento contratto attributo, selezionare **LDAP (attributo)** dall'elenco a discesa origine e selezionare **objectGUID** o **userPrincipalName** dall'elenco a discesa valore.
10. Esaminare e salvare l'origine dell'attributo.
11. Nella scheda origine attributo failsaved, selezionare **Interrompi transazione SSO**.
12. Esaminare il riepilogo e selezionare **fine**.
13. Selezionare **fine**.

Configurare le impostazioni del protocollo

Fasi

1. Nella scheda **connessione SP > SSO browser > Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL servizio clienti asserzione, accettare i valori predefiniti, importati dai metadati SAML di

StorageGRID (**POST** per l'associazione e `/api/saml-response` per l'URL dell'endpoint).

3. Nella scheda URL servizio SLO, accettare i valori predefiniti, importati dai metadati SAML di StorageGRID (**REDIRECT** per l'associazione e `/api/saml-logout` per l'URL dell'endpoint).
4. Nella scheda Allowable SAML Bindings (Binding SAML autorizzati), deselezionare **ARTEFATTO** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Firma Policy, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste Authn** e **Firma sempre asserzione**.
6. Nella scheda Encryption Policy (Criteri di crittografia), selezionare **None** (Nessuno).
7. Esaminare il riepilogo e selezionare **Done** (fine) per salvare le impostazioni del protocollo.
8. Esaminare il riepilogo e selezionare **fine** per salvare le impostazioni SSO del browser.

Configurare le credenziali

Fasi

1. Dalla scheda connessione SP, selezionare **credenziali**.
2. Dalla scheda credenziali, selezionare **Configura credenziali**.
3. Seleziona il [firma del certificato](#) che hai creato o importato.
4. Selezionare **Avanti** per accedere a **Gestisci impostazioni di verifica della firma**.
 - a. Nella scheda Trust Model (modello di attendibilità), selezionare **Unanchored** (non ancorato).
 - b. Nella scheda certificato di verifica della firma, esaminare le informazioni del certificato di firma importate dai metadati SAML di StorageGRID.
5. Esaminare le schermate di riepilogo e selezionare **Save** (Salva) per salvare la connessione SP.

Creare ulteriori connessioni SP

È possibile copiare la prima connessione SP per creare le connessioni SP necessarie per ciascun nodo di amministrazione nella griglia. Vengono caricati nuovi metadati per ogni copia.



Le connessioni SP per diversi nodi di amministrazione utilizzano impostazioni identiche, ad eccezione di ID entità del partner, URL di base, ID connessione, nome connessione, verifica firma, E SLO Response URL.

Fasi

1. Selezionare **Action > Copy** per creare una copia della connessione SP iniziale per ogni nodo Admin aggiuntivo.
2. Immettere l'ID connessione e il nome connessione per la copia, quindi selezionare **Salva**.
3. Scegliere il file di metadati corrispondente al nodo di amministrazione:
 - a. Selezionare **azione > Aggiorna con metadati**.
 - b. Selezionare **Scegli file** e caricare i metadati.
 - c. Selezionare **Avanti**.
 - d. Selezionare **Salva**.
4. Risolvere l'errore dovuto all'attributo inutilizzato:
 - a. Selezionare la nuova connessione.

- b. Selezionare **Configure browser SSO > Configure Assertion Creation > Attribute Contract**.
- c. Elimina la voce per **urn:oid**.
- d. Selezionare **Salva**.

Disabilita SSO in StorageGRID

È possibile disattivare SSO (Single Sign-on) se non si desidera più utilizzare questa funzionalità. È necessario disattivare il Single Sign-on prima di poter disattivare la federazione delle identità.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Fasi

1. Selezionare **Configurazione > Controllo accessi > Single sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo).

2. Seleziona **Disabilita**.

3. Selezionare **Sì**.

Viene visualizzato un messaggio di avviso che indica che gli utenti locali potranno accedere.

Al successivo accesso a StorageGRID, viene visualizzata la pagina di accesso a StorageGRID e sono necessari il nome utente e la password di un utente StorageGRID locale o federato.

Disabilitare e riabilitare temporaneamente il single sign-on (SSO) per un nodo Admin di StorageGRID

Se il sistema SSO (Single Sign-on) non funziona, potrebbe non essere possibile accedere a Grid Manager. In questo caso, è possibile disattivare e riabilitare temporaneamente SSO per un nodo di amministrazione. Per disattivare e riabilitare SSO, è necessario accedere alla shell dei comandi del nodo.

Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Si dispone del `Passwords.txt` file.
- Si conosce la password dell'utente root locale.

A proposito di questa attività

Dopo aver disattivato SSO per un nodo di amministrazione, è possibile accedere a Grid Manager come utente root locale. Per proteggere il sistema StorageGRID, è necessario utilizzare la shell dei comandi del nodo per riabilitare SSO sul nodo di amministrazione non appena si effettua la disconnessione.



La disattivazione di SSO per un nodo di amministrazione non influisce sulle impostazioni SSO per qualsiasi altro nodo di amministrazione nella griglia. La casella di controllo **Enable SSO** (attiva SSO) nella pagina Single Sign-on (accesso singolo) di Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute, a meno che non vengano aggiornate.

Fasi

1. Accedere a un nodo amministratore:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

2. A seconda della configurazione SSO, esegui uno dei seguenti comandi:

SAML

`disable-saml`

OIDC

`disable-oidc`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

3. Confermare che si desidera disattivare SSO.

Un messaggio indica che l'accesso singolo è disattivato sul nodo.

4. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.

Viene visualizzata la pagina di accesso di Grid Manager perché SSO è stato disattivato.

5. Accedere con il nome utente root e la password dell'utente root locale.
6. Se SSO è stato disattivato temporaneamente perché era necessario correggere la configurazione SSO:
 - a. Selezionare **Configurazione > Controllo accessi > Single sign-on**.
 - b. Modificare le impostazioni SSO non corrette o non aggiornate.
 - c. Selezionare **Salva**.

Selezionando **Save** (Salva) dalla pagina Single Sign-on (accesso singolo), l'SSO viene riattivato automaticamente per l'intera griglia.

7. Se l'SSO è stato disattivato temporaneamente perché era necessario accedere a Grid Manager per un altro motivo:
 - a. Eseguire qualsiasi attività o attività da eseguire.
 - b. Selezionare **Disconnetti** e chiudere Grid Manager.
 - c. Riabilitare SSO sul nodo di amministrazione. È possibile eseguire una delle seguenti operazioni:

- Eseguire il seguente comando: `enable-saml`

Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

Confermare che si desidera attivare SSO.

Un messaggio indica che il Single Sign-on è attivato sul nodo.

◦ Riavviare il nodo della griglia: `reboot`

8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.

9. Verificare che venga visualizzata la pagina di accesso a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

Usa la verifica multi-amministratore

Scopri la verifica multi-amministratore di StorageGRID

Come amministratore di StorageGRID, puoi utilizzare la verifica multi-amministratore (MAV) per assicurarti che alcune operazioni possano essere eseguite solo dopo l'approvazione degli amministratori designati. La MAV aiuta a prevenire modifiche accidentali o non autorizzate al tuo sistema StorageGRID.

MAV è disabilitato per impostazione predefinita.

Panoramica della configurazione MAV

Per configurare MAV, dovrai eseguire queste operazioni:

- Crea uno o più gruppi di amministratori. Gli amministratori MAV hanno potere di approvazione e di veto.
- Abilita la funzione di verifica multi-amministratore.
- Seleziona da un insieme di operazioni protette.

Devi avere i permessi di accesso Root per eseguire la configurazione iniziale e apportare modifiche in seguito.

Come vengono gestite le operazioni protette con MAV

Quando MAV è abilitato, il completamento di ogni operazione protetta richiede questi passaggi:

1. Quando un utente avvia l'operazione, viene generata una richiesta.
2. Prima che l'operazione possa essere eseguita, almeno un amministratore MAV deve approvare.
3. Quando viene approvata, l'operazione protetta da MAV viene eseguita automaticamente.

Configura la verifica multi-amministratore di StorageGRID

Configurare un sistema di verifica multi-amministratore (MAV) StorageGRID significa creare e gestire gruppi e utenti amministratori MAV, abilitare la funzione MAV e selezionare o configurare le operazioni protette.

Gli amministratori di MAV hanno potere di approvazione e di veto per le operazioni protette.

Prima di iniziare

- Si dispone di "[Autorizzazione di accesso root](#)".
- Hai effettuato l'accesso al Grid Manager dal nodo Admin principale.

Passaggio 1: Crea gruppi e utenti amministratori MAV

Puoi aggiungere amministratori esistenti a un gruppo MAV o creare nuovi amministratori.

Puoi configurare gli utenti di Active Directory (AD) come amministratori MAV. L'utente AD deve essere configurato come amministratore di StorageGRID.

Fasi

1. Per creare un gruppo di amministratori MAV, segui i passaggi per ["crea un gruppo locale o federato"](#).
2. Per le autorizzazioni di gruppo, seleziona **Accesso root** o **Richieste di verifica multi-amministratore**.
3. Aggiungi utenti locali o federati al gruppo oppure crea nuovi utenti locali e aggiungili al gruppo seguendo i passaggi per ["crea un utente locale"](#).

Passaggio 2: Abilita o disabilita MAV

Devi abilitare esplicitamente la verifica multi-amministratore (MAV). Se MAV è abilitata e decidi di disabilitarla quando ci sono richieste MAV in sospeso, una notifica indica che le richieste in sospeso verranno eliminate.

Fasi

1. Seleziona **Configurazione > Controllo accessi > Verifica multi-amministratore > Impostazioni MAV**.
2. Seleziona la casella di controllo **Abilita MAV** per abilitare la verifica multi-amministratore.
3. La sezione Gruppi di approvazione elenca i gruppi di amministratori MAV e gli approvatori.
4. Nella sezione Operazioni, seleziona le caselle di controllo per le operazioni che vuoi proteggere con MAV.
5. (Facoltativo) Se vuoi usare le notifiche email per avvisare gli amministratori MAV delle richieste di approvazione in sospeso:
 - a. Se non hai configurato un server di posta elettronica, segui i passaggi per ["configurare un server di posta elettronica"](#).
 - b. Inserisci l'indirizzo email del mittente.
 - c. Inserisci uno o più destinatari per le notifiche email.
6. Seleziona **Salva** per salvare le modifiche.



Se decidi di non configurare le notifiche email, gli amministratori MAV possono visualizzare la dashboard di Grid Manager o controllare la coda di approvazione per le richieste di approvazione in sospeso. Per controllare la coda di approvazione, seleziona **Altre richieste** nella pagina di verifica multi-amministratore.

Passaggio 3: Gestisci le operazioni protette

Dopo che hai abilitato la verifica multi-amministratore, puoi gestire le operazioni protette selezionando o deselezionando le caselle di controllo per le operazioni che vuoi proteggere con MAV.



Per StorageGRID 12.1, l'unica operazione protetta è l'attivazione della policy ILM. Devi selezionare la casella di controllo per l'attivazione della policy ILM se vuoi abilitare MAV.

Una richiesta MAV può avere uno dei seguenti stati:

- **In sospeso.** Richiesta avviata.

- **Scaduta.** La richiesta non è stata evasa entro 30 giorni. Oppure un utente con permessi di accesso Root ha disabilitato MAV, il che significa che tutte le richieste in sospeso sono scadute.
- **Ritirata.** Un utente ha ritirato la propria richiesta.
- **Approvato.** Un amministratore MAV ha approvato la richiesta in sospeso.
- **Rifiutata.** Un amministratore MAV ha respinto la richiesta in sospeso.

Risolvi i problemi delle notifiche email di MAV

Se gli amministratori MAV non ricevono notifiche via e-mail per le richieste in sospeso, segui questi passaggi per risolvere il problema.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

Fasi

1. Verificare le impostazioni.
 - a. Seleziona **Configuration > Monitoring > Email server**.
 - b. Verificare che le impostazioni del server e-mail (SMTP) siano corrette.
 - c. Verificare di aver specificato indirizzi e-mail validi per i destinatari.
2. Controllare il filtro antispam e assicurarsi che l'e-mail non sia stata inviata a una cartella di posta indesiderata.
3. Chiedi all'amministratore dell'email di confermare che le e-mail dell'indirizzo del mittente non vengono bloccate.
4. Raccogliere un file di log per l'Admin Node, quindi contattare il supporto tecnico.

Il supporto tecnico può utilizzare le informazioni contenute nei registri per determinare l'errore. Ad esempio, il file `prometheus.log` potrebbe visualizzare un errore durante la connessione al server specificato.

Vedi ["Raccogliere i file di log e i dati di sistema"](#).

Richiedi l'approvazione per le operazioni protette da MAV in StorageGRID

Come amministratore o utente di StorageGRID, quando avvii un'operazione protetta da MAV in StorageGRID, viene generata automaticamente una richiesta. Appare un messaggio che ti informa che l'operazione richiede l'approvazione.

Il sistema StorageGRID definisce quali operazioni sono protette da MAV. Quando avvii un'operazione protetta da MAV, la richiesta viene inviata agli amministratori MAV per l'approvazione.

Fasi

Il sistema StorageGRID ti informa che hai avviato un'operazione protetta da MAV.

1. Se necessario, esegui una delle seguenti attività:
 - a. Verifica lo stato della tua richiesta selezionando **Configurazione > Controllo accessi > Verifica multi-amministratore > Le mie richieste**.
 - **In sospeso.** Richiesta avviata.

- **Scaduta.** La richiesta non è stata evasa entro 30 giorni. Oppure un utente con permessi di accesso Root ha disabilitato MAV, il che significa che tutte le richieste in sospeso sono scadute.
 - **Ritirata.** Un utente ha ritirato la propria richiesta.
 - **Approvato.** Un amministratore MAV ha approvato la richiesta in sospeso.
 - **Rifiutata.** Un amministratore MAV ha respinto la richiesta in sospeso.
- b. Verifica le richieste in sospeso di altri utenti selezionando **Configurazione > Controllo accessi > Verifica multi-amministratore > Altre richieste**.
- c. Per annullare un'operazione, seleziona **Le mie richieste > la richiesta che desideri annullare > Ritira**.

Dopo che un amministratore MAV approva la richiesta, l'operazione viene eseguita automaticamente.

Se la tua richiesta viene rifiutata, l'operazione non viene eseguita e puoi inviare una nuova richiesta se necessario.

Gestisci le richieste di operazioni protette da MAV in StorageGRID

Come amministratore MAV, puoi gestire le richieste per operazioni protette da MAV in StorageGRID. Puoi visualizzare le tue richieste o quelle di altri utenti in sospeso, approvare o rifiutare le richieste e visualizzare la cronologia delle richieste passate.

Prima di iniziare

- Fai parte di un gruppo di amministratori MAV e hai il "[Autorizzazione di accesso root](#)".
- Hai effettuato l'accesso al Grid Manager dal nodo Admin principale.

Fasi

1. Se ricevi una notifica via e-mail relativa a una richiesta MAV, seleziona **Configurazione > Verifica multi-amministratore > Altre richieste**.

Inoltre, la dashboard di Grid Manager visualizza una notifica per le richieste MAV in sospeso.

2. Seleziona il pulsante di opzione per ogni richiesta che vuoi gestire.
3. Seleziona **Approva** o **Rifiuta** per approvare o rifiutare le richieste selezionate.
4. Per visualizzare la cronologia delle richieste precedenti, seleziona **Cronologia**.

USA la federazione di grid

Scopri la federazione di grid StorageGRID

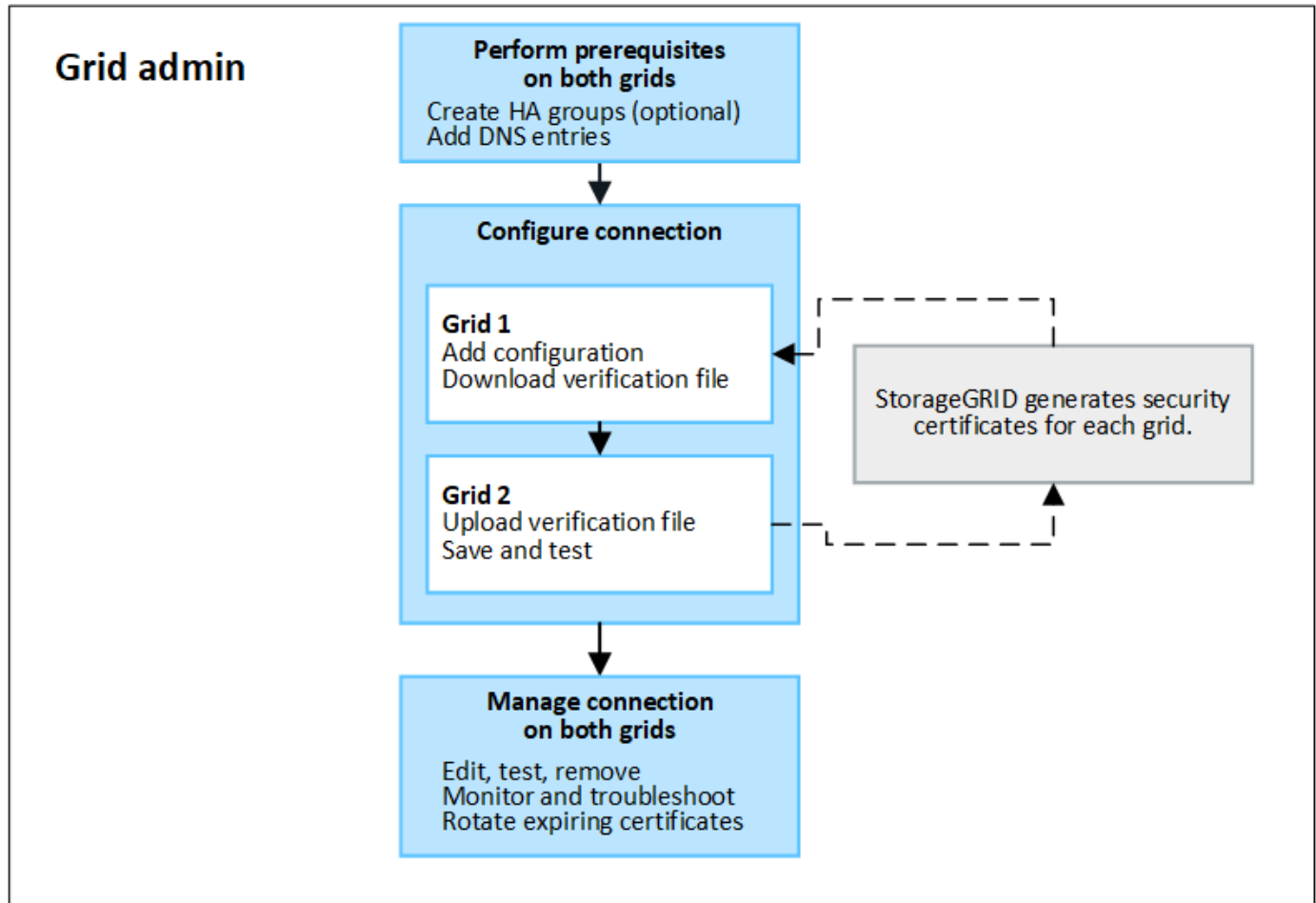
Puoi usare la federazione di griglia per sincronizzare i tenant e replicare i loro oggetti tra più sistemi StorageGRID per il ripristino di emergenza.

Che cos'è una connessione a federazione di griglie?

Una connessione a federazione di griglie è una connessione bidirezionale, affidabile e sicura tra i nodi amministratore e gateway in due sistemi StorageGRID.

Workflow per la federazione di grid

Il diagramma del flusso di lavoro riassume i passaggi per la configurazione di una connessione di federazione di grid tra due grid.



Considerazioni e requisiti per le connessioni a federazione di griglie

- Le griglie utilizzate per la federazione delle griglie devono eseguire versioni di StorageGRID identiche o con non più di una differenza di versione principale.

Per i dettagli sui requisiti di versione, fare riferimento a ["Note di rilascio"](#). È necessario accedere con il proprio account NetApp o crearne uno per accedere alle note di rilascio.

- Una griglia può avere una o più connessioni di federazione di griglia ad altre griglie. Ogni connessione a federazione di griglie è indipendente da qualsiasi altra connessione. Ad esempio, se la griglia 1 ha una connessione con la griglia 2 e una seconda connessione con la griglia 3, non esiste alcuna connessione implicita tra la griglia 2 e la griglia 3.
- Le connessioni a federazione di griglie sono bidirezionali. Una volta stabilita la connessione, è possibile monitorare e gestire la connessione da entrambe le griglie.
- Deve esistere almeno una connessione di federazione della griglia prima di poter utilizzare ["sincronizzazione account"](#) o ["replica cross-grid"](#).

Requisiti di rete e indirizzo IP

- Le connessioni a federazione di griglie possono avvenire su Grid Network, Admin Network o Client

Network.

- Una connessione a federazione di griglie collega una griglia a un'altra griglia. La configurazione per ogni griglia specifica un endpoint della federazione di griglia sull'altra griglia che consiste in nodi di amministrazione, nodi gateway o entrambi.
- La procedura consigliata consiste nel collegare **"Gruppi ad alta disponibilità (ha)"** i nodi Gateway e Admin su ciascuna rete. L'utilizzo di gruppi ha consente di garantire che le connessioni a federazione di griglie rimangano online se i nodi non sono più disponibili. Se l'interfaccia attiva in uno dei gruppi ha non riesce, la connessione può utilizzare un'interfaccia di backup.
- Si sconsiglia di creare una connessione a federazione di griglie che utilizzi l'indirizzo IP di un singolo nodo di amministrazione o di un nodo gateway. Se il nodo diventa non disponibile, anche la connessione a federazione di griglie non sarà disponibile.
- **"Replica cross-grid"** Of Objects richiede che i nodi storage di ciascun grid siano in grado di accedere ai nodi Admin e Gateway configurati nell'altro grid. Per ogni griglia, verificare che tutti i nodi di storage dispongano di un percorso a elevata larghezza di banda verso i nodi Admin o Gateway utilizzati per la connessione.

Utilizzare FQDN per bilanciare il carico della connessione

Per un ambiente di produzione, utilizzare FQDN (Fully Qualified Domain Name) per identificare ogni griglia della connessione. Quindi, creare le voci DNS appropriate, come indicato di seguito:

- L'FQDN per la griglia 1 è mappato a uno o più indirizzi IP virtuali (VIP) per i gruppi ha nella griglia 1 o all'indirizzo IP di uno o più nodi Admin o Gateway nella griglia 1.
- L'FQDN per la griglia 2 è mappato a uno o più indirizzi VIP per la griglia 2 o all'indirizzo IP di uno o più nodi Admin o Gateway nella griglia 2.

Quando si utilizzano più voci DNS, le richieste per utilizzare la connessione vengono bilanciate dal carico, come segue:

- Le voci DNS associate agli indirizzi VIP di più gruppi ha vengono bilanciate in base al carico tra i nodi attivi nei gruppi ha.
- Le voci DNS associate agli indirizzi IP di più nodi Admin o Gateway vengono bilanciate in base al carico tra i nodi mappati.

Requisiti delle porte

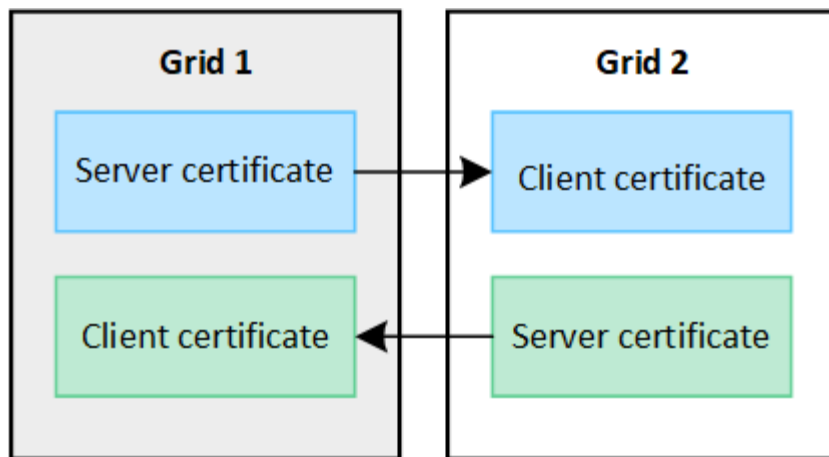
Quando si crea una connessione a federazione di griglie, è possibile specificare qualsiasi numero di porta inutilizzato compreso tra 23000 e 23999. Entrambe le griglie di questa connessione utilizzeranno la stessa porta.

È necessario assicurarsi che nessun nodo di una delle griglie utilizzi questa porta per altre connessioni.

Requisiti del certificato

Quando si configura una connessione a federazione di griglie, StorageGRID genera automaticamente quattro certificati SSL:

- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 1 alla griglia 2
- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 2 alla griglia 1



Per impostazione predefinita, i certificati sono validi per 730 giorni (2 anni). Quando questi certificati si avvicinano alla data di scadenza, l'avviso **scadenza del certificato federazione griglia** ricorda di ruotare i certificati, operazione che è possibile eseguire utilizzando Grid Manager.



Se i certificati a una delle due estremità della connessione scadono, la connessione non funziona più. La replica dei dati sarà in sospeso fino all'aggiornamento dei certificati.

Scopri di più

- ["Creare connessioni di federazione di griglie"](#)
- ["Gestire le connessioni a federazione di griglie"](#)
- ["Risolvere i problemi relativi agli errori di federazione della griglia"](#)

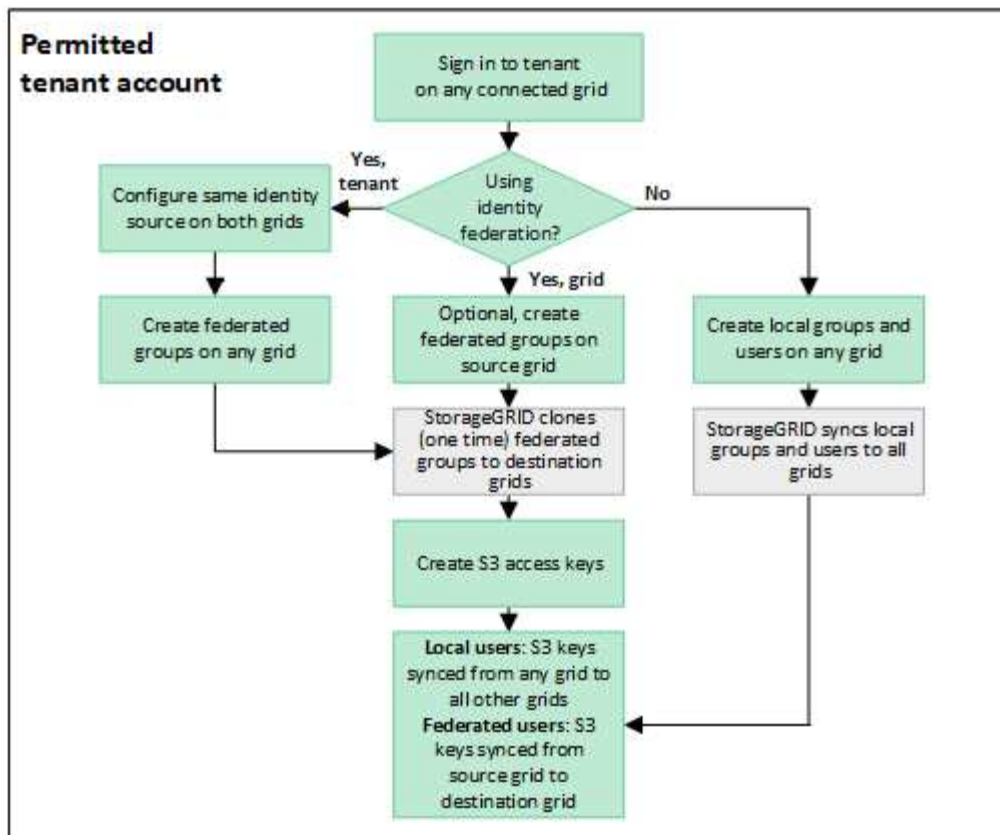
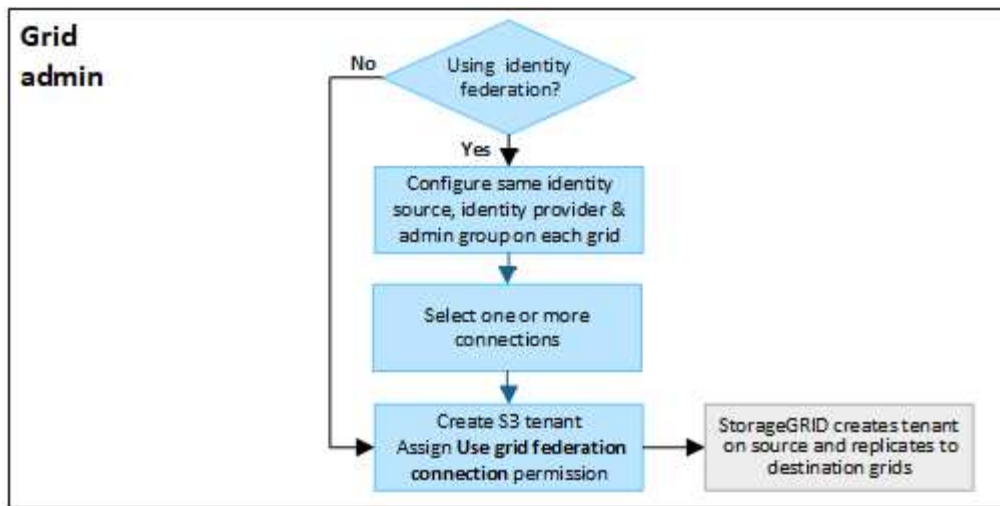
Scopri la sincronizzazione degli account in StorageGRID

La sincronizzazione dell'account è la replica automatica e continua di un tenant account, gruppi tenant, utenti tenant e, facoltativamente, delle chiavi di accesso S3 tra i sistemi StorageGRID in uno o più ["connessioni a federazione di griglie"](#).

La sincronizzazione dell'account è necessaria per ["replica cross-grid"](#). La sincronizzazione delle informazioni dell'account tra sistemi StorageGRID garantisce che gli utenti e i gruppi del tenant possano accedere ai bucket e agli oggetti corrispondenti su qualsiasi grid connessa.

Flusso di lavoro per la sincronizzazione dell'account

Il diagramma del flusso di lavoro mostra i passaggi che gli amministratori della griglia e i tenant autorizzati eseguiranno per configurare la sincronizzazione dell'account. Questi passaggi vengono eseguiti dopo il ["la connessione a federazione di griglie è configurata"](#).



Workflow di amministrazione della griglia

I passaggi eseguiti dagli amministratori di rete dipendono dal fatto che i sistemi StorageGRID ["connessione a federazione di griglie"](#) utilizzino il Single Sign-on (SSO) o la federazione delle identità.

Configura SSO per la sincronizzazione dell'account (facoltativo)

Se uno dei sistemi StorageGRID nella connessione a federazione di griglie utilizza SSO, entrambe le griglie devono utilizzare SSO. Prima di creare gli account tenant per la federazione di griglie, gli amministratori di griglie per le griglie di origine e di destinazione del tenant devono eseguire questi passaggi.

Fasi

1. Configurare la stessa origine di identità per entrambe le griglie. Vedere ["USA la federazione delle identità"](#).

2. Configurare lo stesso provider di identità SSO (IdP) per entrambe le griglie. Vedere ["Configurare il single sign-on"](#) .
3. ["Creare lo stesso gruppo di amministratori"](#) su entrambe le griglie importando lo stesso gruppo federated.

Quando si crea il tenant, si seleziona questo gruppo per disporre dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione.



Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non viene replicato nella destinazione.

Configura la federazione delle identità a livello di grid per la sincronizzazione degli 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 di griglie, gli amministratori di griglie per le griglie di origine e di destinazione del tenant devono eseguire questi passaggi.

Fasi

1. Configurare la stessa origine di identità per entrambe le griglie. Vedere ["USA la federazione delle identità"](#).
2. Facoltativamente, se un gruppo federated dispone dell'autorizzazione di accesso root iniziale per entrambi gli account tenant di origine e di destinazione, ["creare lo stesso gruppo di amministratori"](#) su entrambe le griglie importando lo stesso gruppo federated.



Se si assegna l'autorizzazione di accesso root a un gruppo federated che non esiste su entrambe le griglie, il tenant non viene replicato nella griglia di destinazione.

3. Se non si desidera che un gruppo federated disponga dell'autorizzazione di accesso root iniziale per entrambi gli account, specificare una password per l'utente root locale.

Creare un account tenant S3 consentito

Dopo la configurazione opzionale di SSO o federazione di identità, un amministratore di grid esegue questi passaggi per determinare quali tenant possono replicare gli oggetti bucket in altri sistemi StorageGRID.

Fasi

1. Determina quale griglia vuoi usare come griglia di origine del tenant per le operazioni di sincronizzazione degli account.

La griglia in cui viene creato il tenant è nota come *griglia di origine* del tenant. La griglia in cui viene replicato il tenant è nota come *griglia di destinazione* del tenant.

2. In tale griglia, creare un nuovo account tenant S3 o modificare un account esistente.
3. Assegnare l'autorizzazione **Usa connessione federazione griglia**.
4. Se l'account tenant gestirà i propri utenti federati, assegnare l'autorizzazione **use own Identity source**.

Se questa autorizzazione viene assegnata, sia il tenant di origine che il tenant di destinazione devono configurare la stessa origine di identità prima di creare gruppi federati. I gruppi federati aggiunti al tenant di origine non possono essere sincronizzati con il tenant di destinazione a meno che entrambe le griglie utilizzino la stessa origine di identità.

5. Selezionare una connessione a federazione di griglie specifica.

6. Salvare il tenant nuovo o modificato.

Quando viene salvato un nuovo tenant con l'autorizzazione **use grid Federation Connection**, StorageGRID crea automaticamente una replica del tenant sull'altro grid, come segue:

- Entrambi gli account tenant hanno lo stesso ID account, il nome, la quota di storage e le stesse autorizzazioni assegnate.
- Se selezioni un gruppo federato a cui assegnare i permessi di accesso root per il tenant, quel gruppo viene clonato nella destinazione tenant. Tuttavia, la replica continua non avviene per gruppi e utenti federati. Viene eseguita solo una clonazione una tantum.
- Se hai selezionato un utente locale con permessi di accesso root per il tenant, tale utente viene sincronizzato con il tenant di destinazione.

Per dettagli, consultare ["Gestire i tenant autorizzati per la federazione di grid"](#).

Flusso di lavoro account tenant consentito

Dopo che un tenant con l'autorizzazione **Usa connessione di federazione grid** è stato replicato nella grid di destinazione, gli account tenant autorizzati possono eseguire questi passaggi per sincronizzare gruppi tenant, utenti e chiavi di accesso S3.

Fasi

1. Accedi all'account tenant su qualsiasi grid connessa.
2. Se consentito, configura la federazione delle identità sia sull'account tenant di origine che su quello di destinazione.
3. Crea gruppi e utenti su qualsiasi grid connessa.

Quando vengono creati nuovi gruppi o utenti su un tenant, StorageGRID li sincronizza automaticamente con il tenant di destinazione.

4. Creare chiavi di accesso S3.
5. Facoltativamente, sincronizza le chiavi di accesso S3 dal tenant di origine al tenant di destinazione.

Per dettagli sul flusso di lavoro consentito per gli account tenant e per scoprire come vengono sincronizzati gruppi, utenti e chiavi di accesso S3, consulta ["Sincronizza gruppi di tenant e utenti"](#).

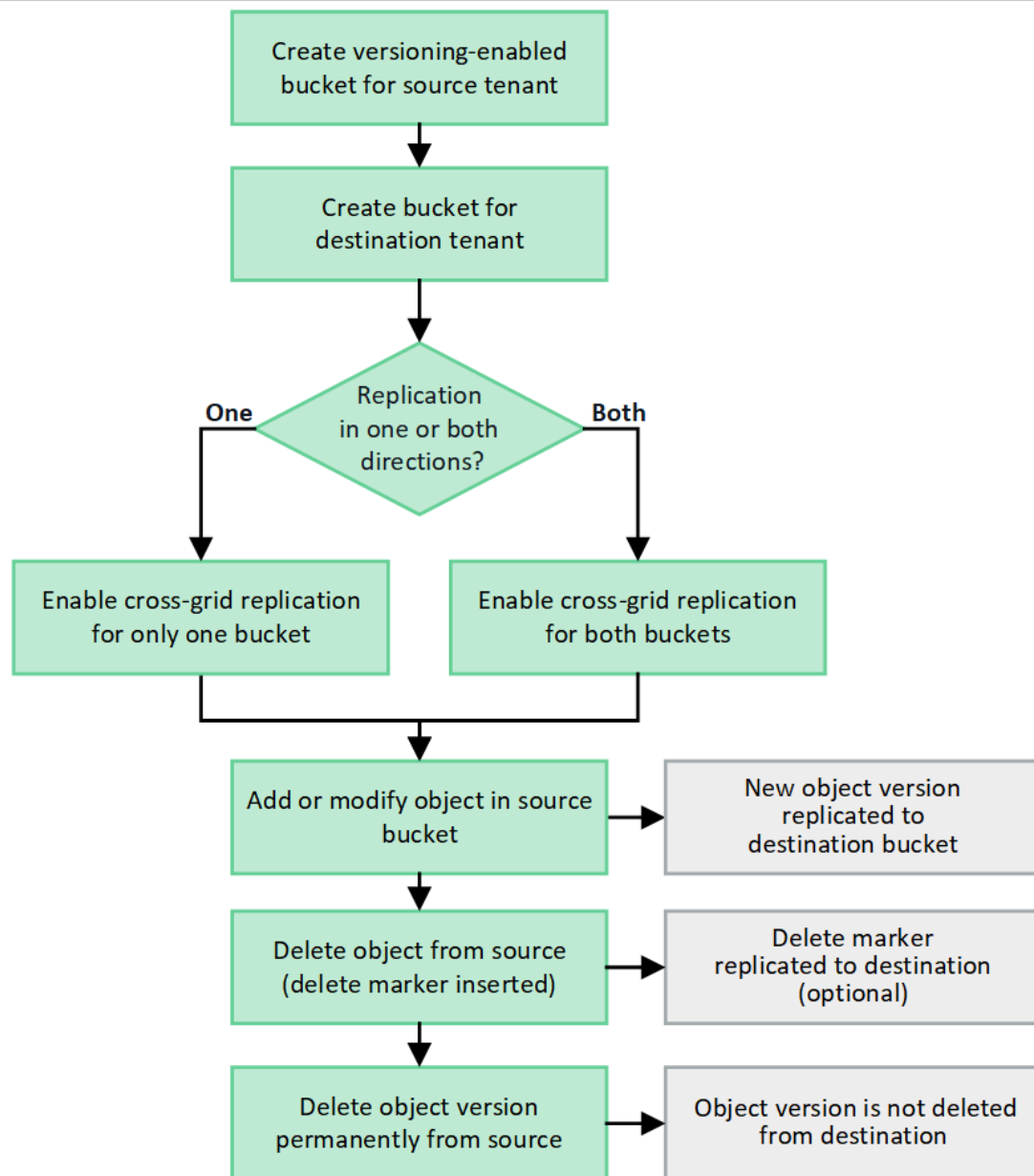
Scopri la replica cross-grid in StorageGRID

La replica cross-grid è la replica automatica di oggetti tra bucket S3 selezionati in due sistemi StorageGRID connessi in una ["connessione a federazione di griglie"](#). ["Sincronizzazione account"](#) è richiesta per la replica cross-grid.

Workflow per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi per configurare la replica tra griglie tra bucket su due griglie.

Tenant user



Requisiti per la replica cross-grid

Se un tenant account ha l'autorizzazione **Usa connessione di federazione griglia** per utilizzare uno o più ["connessioni a federazione di griglie"](#), un tenant con autorizzazione di accesso Root può creare bucket ("source" e "destination" bucket) nei corrispondenti tenant account su ogni griglia. Questi bucket:

- Possono avere nomi diversi l'uno dall'altro
- Può avere regioni diverse
- È necessario attivare la versione
- Devi avere una delle seguenti configurazioni di S3 Object Lock:
 - origine: **disabilitato**, destinazione: **disabilitato**
 - origine: **abilitata**, destinazione: **abilitata**
 - origine: **disabilitata**, destinazione: **abilitata**

Dopo aver creato entrambi i bucket, puoi configurare la replica tra griglie per uno o entrambi i bucket.

Scopri di più

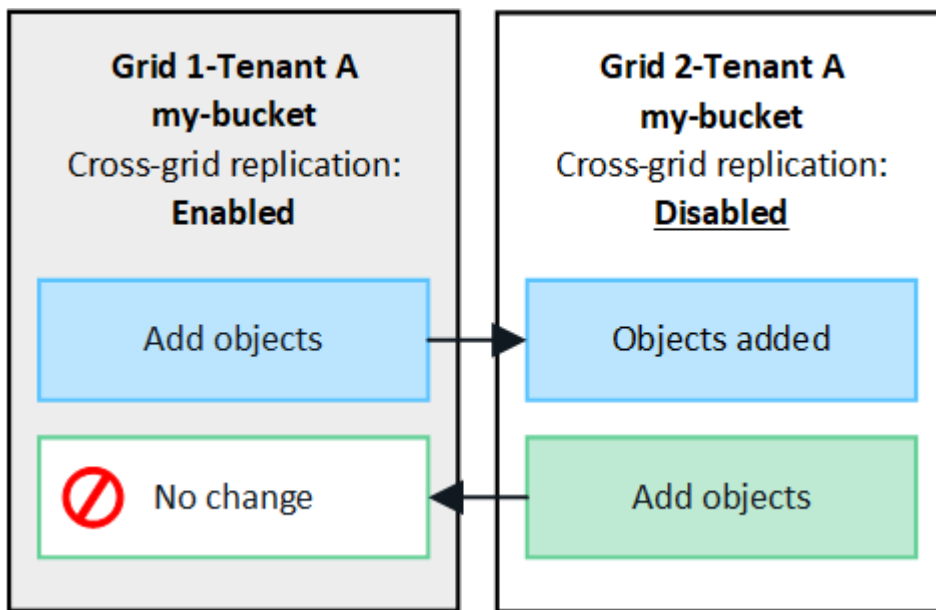
["Gestire la replica cross-grid"](#)

Come funziona la replica cross-grid

È possibile configurare la replica tra griglie in modo che avvenga in una direzione o in entrambe le direzioni.

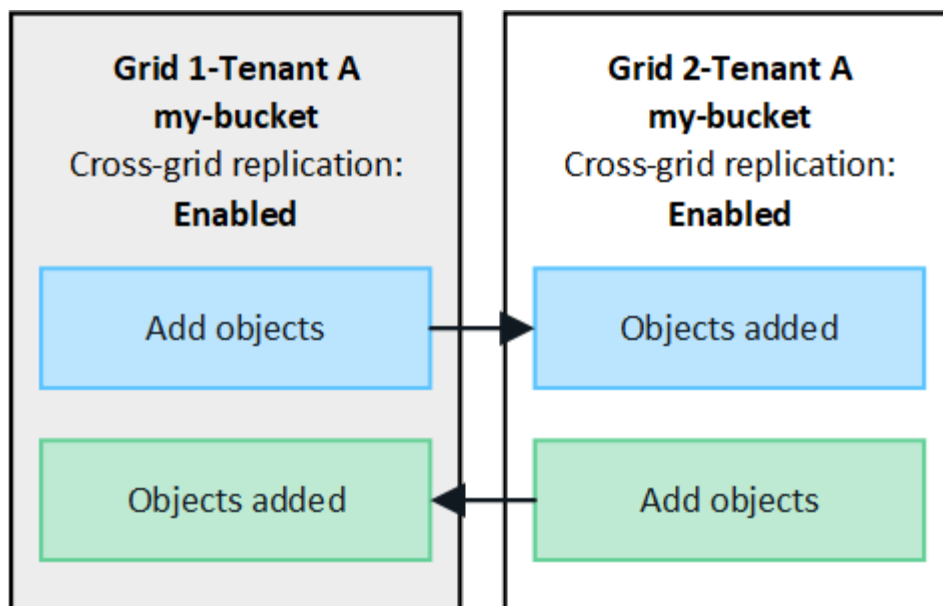
Replica in un'unica direzione

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.



Replica in entrambe le direzioni

Se si attiva la replica cross-grid per lo stesso bucket su entrambe le griglie, gli oggetti aggiunti a entrambi i bucket vengono replicati nell'altra griglia. Nella figura, la replica cross-grid è abilitata per `my-bucket` in entrambe le direzioni.



Cosa succede quando gli oggetti vengono acquisiti?

Quando un client S3 aggiunge un oggetto a un bucket con replica cross-grid attivata, si verifica quanto segue:

1. StorageGRID replica automaticamente l'oggetto dal bucket di origine al bucket di destinazione. Il tempo necessario per eseguire questa operazione di replica in background dipende da diversi fattori, tra cui il numero di altre operazioni di replica in sospeso.

Il client S3 può verificare lo stato di 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 ha uno dei seguenti valori:

Griglia	Stato della replica
Origine	• COMPLETATO: La replica è stata eseguita correttamente per tutte le connessioni di rete. • PENDING: L'oggetto non è stato replicato in almeno una connessione di rete. • 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 i criteri ILM attivi di ciascuna griglia per gestire gli oggetti, esattamente come per qualsiasi altro oggetto. Ad esempio, l'oggetto A sulla griglia 1 potrebbe essere memorizzato come due copie replicate e conservato per sempre, mentre la copia dell'oggetto A replicata sulla griglia 2 potrebbe essere memorizzata utilizzando la codifica di cancellazione 2+1 ed eliminata dopo tre anni.

Cosa succede quando gli oggetti vengono cancellati?

Come descritto in ["Eliminare il flusso di dati"](#), StorageGRID può eliminare un oggetto per uno dei seguenti motivi:

- Il client S3 invia una richiesta di eliminazione.
- Un utente di Tenant Manager seleziona l'"[Eliminare gli oggetti nel bucket](#)" opzione per rimuovere tutti gli oggetti da un bucket.
- Il bucket ha una configurazione del ciclo di vita che scade.
- L'ultimo periodo di tempo nella regola ILM per l'oggetto termina e non sono stati specificati ulteriori posizionamenti.

Quando StorageGRID elimina un oggetto a causa di un'operazione Delete Objects (Elimina oggetti) nel bucket, della scadenza del ciclo di vita del bucket o della scadenza del posizionamento ILM, l'oggetto replicato non viene mai cancellato dall'altra griglia in una connessione a federazione di griglie. Tuttavia, i marker di eliminazione aggiunti al bucket di origine da S3 client Delete possono essere replicati nel bucket di destinazione.

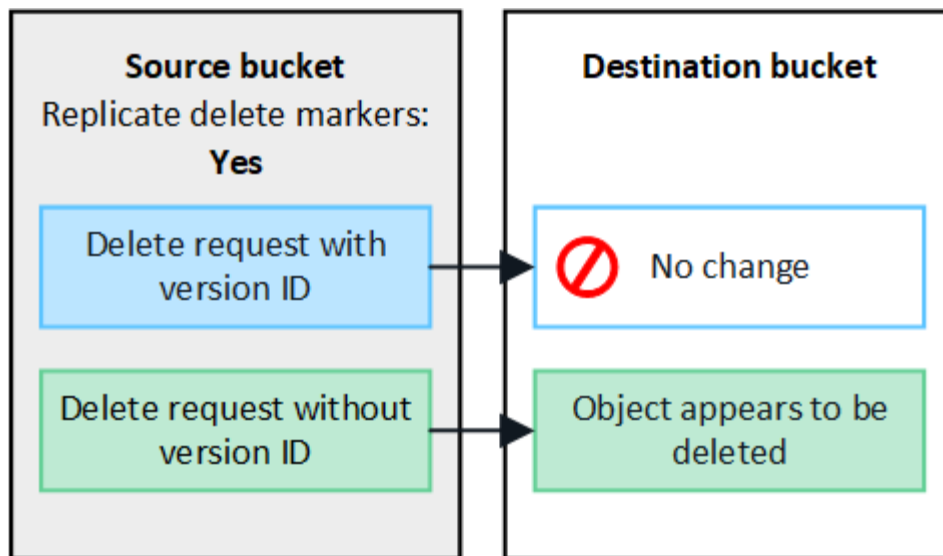
Per capire cosa accade quando un client S3 elimina oggetti da un bucket che ha la replica cross-grid attivata, rivedere come i client S3 eliminano oggetti dai bucket che hanno la versione attivata, come segue:

- Se un client S3 invia una richiesta di eliminazione che include un ID di versione, la versione dell'oggetto viene rimossa in modo permanente. Nessun marker di eliminazione aggiunto al bucket.
- Se un client S3 invia una richiesta di eliminazione che non include un ID 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 fallisce con 404 No Object Found
 - Una richiesta GetObject con un ID versione valido ha esito positivo e restituisce la versione dell'oggetto richiesta.

Quando un client S3 elimina un oggetto da un bucket con la replica cross-grid attivata, StorageGRID determina se replicare la richiesta di eliminazione nella destinazione, come segue:

- Se la richiesta di eliminazione include un ID 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 marker di eliminazione (impostazione predefinita), un marker di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione. In effetti, l'oggetto sembra essere cancellato su entrambe le griglie.
 - Se si sceglie di non replicare i 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 ["la replica cross-grid è stata attivata"](#). Le richieste di eliminazione per il bucket di origine che includono un ID versione non eliminano gli oggetti dal bucket di destinazione. Le richieste di eliminazione per il bucket di origine che non includono un ID versione sembrano eliminare gli oggetti nel bucket di destinazione.



Se si desidera mantenere sincronizzate le eliminazioni degli oggetti tra le griglie, creare corrispondenti ["Configurazioni del ciclo di vita S3"](#) per i bucket su entrambe le griglie.

Modalità di replica degli oggetti crittografati

Quando si utilizza la replica cross-grid per replicare oggetti tra griglie, è possibile crittografare singoli oggetti, utilizzare la crittografia bucket predefinita o configurare la crittografia a livello di griglia. È possibile aggiungere, modificare o rimuovere le impostazioni di crittografia predefinite del bucket o dell'intera griglia prima o dopo aver attivato la replica cross-grid per un bucket.

Per crittografare singoli oggetti, è possibile utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID) quando si aggiungono gli oggetti al bucket di origine. Utilizzare l'`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 il `SSEAlgorithm` parametro su `AES256`. La crittografia a livello di bucket si applica a tutti gli oggetti acquisiti senza l'`x-amz-server-side-encryption` intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

Per utilizzare la crittografia a livello di griglia, impostare l'opzione **Stored Object Encryption** su **AES-256**. La crittografia a livello di griglia si applica a tutti gli oggetti che non sono crittografati a livello di bucket o che sono acquisiti senza l'`x-amz-server-side-encryption` intestazione della richiesta. Vedere ["Configurare le opzioni di rete e degli oggetti"](#).



SSE non supporta AES-128. Se l'opzione **Crittografia degli oggetti archiviati** è abilitata per la griglia di origine utilizzando l'opzione **AES-128**, l'uso dell'algoritmo AES-128 non viene propagato all'oggetto replicato. Al contrario, l'oggetto replicato utilizza il bucket predefinito della destinazione o l'impostazione di crittografia a livello di griglia, se disponibile.

Quando si determina come crittografare gli oggetti di origine, StorageGRID applica le seguenti regole:

1. Utilizzare l'`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 di origine, a meno che tale oggetto non utilizzi la crittografia AES-128.
2. Se l'oggetto di origine non è crittografato o utilizza AES-128, utilizzare l'impostazione di crittografia predefinita del bucket di destinazione, se 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.

Replicazione cross-grid con S3 Object Lock

È possibile configurare la replica tra reti diverse tra bucket StorageGRID con S3 Object Lock abilitato nelle seguenti circostanze.

Quando S3 Object Lock sul bucket di origine è...	E S3 Object Lock sul bucket di destinazione è...
Abilitato	Abilitato
Disabili	Abilitato



Puoi abilitare il blocco degli oggetti S3 sui bucket esistenti, il che potrebbe portare a una configurazione errata in seguito.



Quando S3 Object Lock è abilitato sul bucket di origine, assicurati che sia abilitato anche sul bucket di destinazione. Se S3 Object Lock è disabilitato sul bucket di destinazione, si verifica un errore durante la replica. Consulta ["Avvisi ed errori di replica cross-grid"](#).

Quando S3 Object Lock sul bucket di origine è abilitato:

- Gli oggetti vengono bloccati con le impostazioni di conservazione nella destinazione in questo ordine:
 - a. Valori dell'intestazione di conservazione dell'oggetto sorgente per:


```
x-amz-object-lock-mode
```

```
x-amz-object-lock-retain-until-date
```
 - b. Se impostata, la conservazione predefinita del bucket di origine.
 - c. Se impostata, la conservazione predefinita del bucket di destinazione.

La conservazione predefinita del bucket di destinazione non sostituisce le impostazioni di conservazione replicate dall'oggetto di origine.

- È possibile impostare lo stato di conservazione legale per l'oggetto di destinazione utilizzando `x-amz-object-lock-legal-hold` durante il caricamento dell'oggetto.
- Si verifica un errore se il tenant o il bucket di destinazione non supporta le impostazioni di blocco degli oggetti S3 dell'oggetto di origine. Fare riferimento a ["Avvisi ed errori di replicazione tra griglie."](#)

Quando S3 Object Lock sul bucket di origine è disabilitato:

- È possibile configurare la conservazione predefinita sul bucket di destinazione per applicare le impostazioni di conservazione S3 Object Lock all'oggetto di destinazione.
- L'oggetto di destinazione non può impostare uno stato di conservazione legale.

PutObjectTagging e DeleteObjectTagging non sono supportati

Le richieste PutObjectTagging e DeleteObjectTagging non sono supportate per gli oggetti nei bucket in cui è abilitata la replica cross-grid.

Se un client S3 emette una richiesta PutObjectTagging o DeleteObjectTagging, 501 Not Implemented viene restituito. Il messaggio è `Put(Delete) ObjectTagging isn't available for buckets that have cross-grid replication configured.`

PutObjectRetention e PutObjectLegalHold non sono supportati

Le richieste PutObjectRetention e PutObjectLegalHold non sono completamente supportate per gli oggetti nei bucket in cui è abilitata la replica tra griglie.

Se un client S3 invia una richiesta PutObjectRetention o PutObjectLegalHold, le impostazioni dell'oggetto di origine vengono modificate, ma le modifiche non vengono applicate alla destinazione.

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 del segmento (Configurazione > Sistema > Opzioni di archiviazione)** della griglia di origine viene utilizzata su entrambe le griglie. Ad esempio, supponiamo che la dimensione massima del segmento per la griglia di origine sia 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. Viene 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 replica cross-grid e la replica CloudMirror in StorageGRID

Quando si inizia a utilizzare la federazione delle griglie, esaminare le somiglianze e le differenze tra ["replica cross-grid"](#) e ["Servizio di replica di StorageGRID CloudMirror"](#).



Non è possibile utilizzare CloudMirror su un bucket replicato tramite replica tra griglie e viceversa.

	Replica cross-grid	Servizio di replica di CloudMirror
Qual è lo scopo principale?	Un sistema StorageGRID funge da sistema di disaster recovery. Gli oggetti in un bucket possono essere replicati tra le griglie in una o entrambe le direzioni.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica 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 viene configurato?	1. Configurare una connessione a federazione di griglie tra due griglie. 2. Aggiungere nuovi account tenant, che vengono sincronizzati automaticamente con l'altra grid. 3. Aggiungere nuovi gruppi di tenant e utenti, che vengono anch'essi sincronizzati. 4. Creare bucket corrispondenti su ogni griglia e consentire la replica cross-grid in una o entrambe le direzioni.	1. Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. 2. Qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della sua configurazione?	• Un amministratore di grid configura la connessione e i tenant. • Gli utenti tenant configurano gruppi, utenti, chiavi e bucket.	In genere, un utente tenant.
Qual è la destinazione?	Un bucket S3 corrispondente e identico sull'altro sistema StorageGRID nella connessione a federazione di griglia.	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3). • Piattaforma Google Cloud (GCP)
È necessario il controllo della versione degli oggetti?	Sì, sia il bucket di origine che quello di destinazione devono avere attivato la versione degli oggetti.	No, la replica di CloudMirror supporta qualsiasi combinazione di bucket senza versioni e con versioni sia sull'origine che sulla destinazione.
Qual è la causa dello spostamento degli oggetti nella destinazione?	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket con replica cross-grid attivata.	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket configurato con un endpoint CloudMirror. Gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.

	Replica cross-grid	Servizio di replica di CloudMirror
Come vengono replicati gli oggetti?	La replica cross-grid crea oggetti con versione e replica l'ID della versione dal bucket di origine al bucket di destinazione. Ciò consente di mantenere l'ordine delle versioni in entrambe le griglie.	La replica di CloudMirror non richiede bucket abilitati per il controllo delle versioni, pertanto CloudMirror può eseguire l'ordine solo per una chiave all'interno di un sito. Non vi sono garanzie che l'ordine venga mantenuto per le richieste a un oggetto in un sito diverso.
Cosa succede se un oggetto non può essere replicato?	L'oggetto viene messo in coda per la replica, in base ai limiti di storage dei metadati.	L'oggetto viene messo in coda per la replica, in base ai limiti dei servizi della piattaforma (vedere "Consigli per l'utilizzo dei servizi della piattaforma").
I metadati di sistema dell'oggetto sono replicati?	Sì, quando un oggetto viene replicato nell'altra griglia, vengono replicati anche i relativi metadati di sistema. I metadati saranno identici su entrambe le griglie.	No, quando un oggetto viene replicato nel bucket esterno, i relativi metadati di sistema vengono aggiornati. I metadati variano in base al tempo di acquisizione e al comportamento dell'infrastruttura S3 indipendente.
Come vengono recuperati gli oggetti?	Le applicazioni possono recuperare o leggere gli oggetti effettuando una richiesta al bucket su una griglia.	Le applicazioni possono recuperare o leggere oggetti effettuando una richiesta a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.

	Replica cross-grid	Servizio di replica di CloudMirror
Cosa succede se un oggetto viene cancellato?	- Le richieste di eliminazione che includono un ID di versione non vengono mai replicate nella griglia di destinazione. - Le richieste di eliminazione che non includono un ID di versione aggiungono un contrassegno di eliminazione al bucket di origine, che può essere facoltativamente replicato nella griglia di destinazione. - Se la replica cross-grid è configurata per una sola direzione, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.	I risultati variano in base allo stato di versione dei bucket di origine e di destinazione (che non devono essere identici): - Se entrambi i bucket sono con versione, una richiesta di eliminazione aggiungerà un indicatore di eliminazione in entrambe le posizioni. - Se viene configurato solo il bucket di origine, una richiesta di eliminazione aggiungerà un indicatore di eliminazione all'origine, ma non alla destinazione. - Se nessuno dei bucket è dotato di versione, una richiesta di eliminazione elimina l'oggetto dall'origine ma non dalla destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.

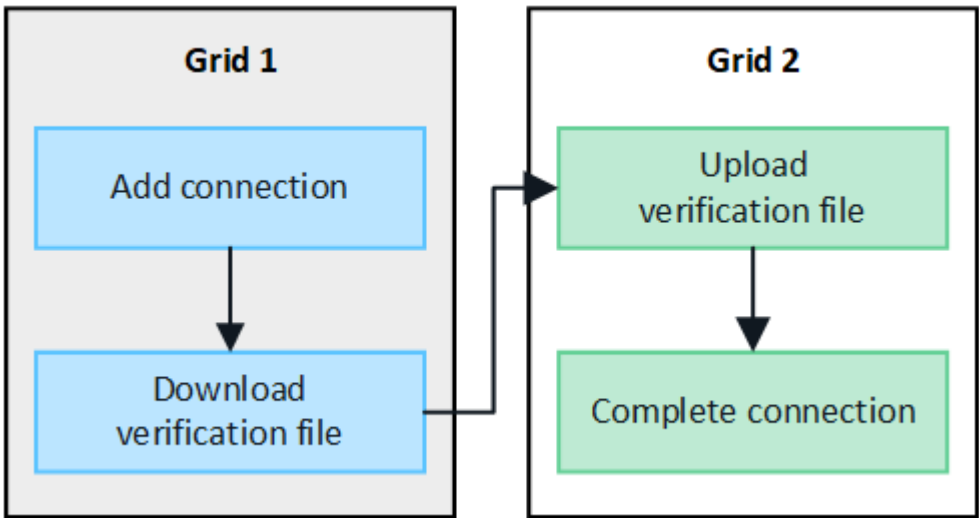
Creare connessioni di federazione della griglia StorageGRID

Puoi creare connessioni di federazione di griglia tra sistemi StorageGRID se vuoi sincronizzare i dettagli dei tenant e replicare i dati degli oggetti.

Come illustrato nella figura, la creazione di una connessione a federazione di griglie include operazioni su entrambe le griglie. La connessione viene aggiunta su una griglia e completata sull'altra. È possibile iniziare da una delle due griglie.



Facoltativamente, puoi ["automatizza la creazione, la modifica e la manutenzione delle connessioni di federazione della griglia"](#).



Prima di iniziare

- È stata esaminata la "[considerazioni e requisiti](#)" per la configurazione delle connessioni di federazione della griglia.
- Se si intende utilizzare FQDN (Fully Qualified Domain Name) per ogni griglia invece degli indirizzi IP o VIP, si conoscono i nomi da utilizzare e si conferma che il server DNS per ogni griglia dispone delle voci appropriate.
- Si sta utilizzando un "[browser web supportato](#)".
- Si dispone dell'autorizzazione di accesso root e della passphrase di provisioning per entrambe le griglie.

Aggiungi connessione

Eseguire questa procedura su uno dei due sistemi StorageGRID.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **Configurazione > Sistema > Federazione di griglia**.
3. Selezionare **Aggiungi connessione**.
4. Inserisci un nome di connessione, ovvero un nome univoco che ti aiuta a riconoscere questa connessione.
Ad esempio, Grid 1-Grid 2.
5. Se vuoi "[configurare uno spazio dei nomi globale](#)", seleziona **Abilita spazio dei nomi globale**.
6. Selezionare **continua**.
7. Inserisci i dettagli della griglia come segue:

Campo	Descrizione
FQDN o IP per questa griglia	Una delle seguenti opzioni: • L'FQDN della griglia a cui si è attualmente connessi • Indirizzo VIP di un gruppo ha su questa griglia • Indirizzo IP di un nodo Admin o di un nodo Gateway in questa griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia di destinazione.
Porta	La porta che si desidera utilizzare per questa connessione. È possibile immettere un numero di porta inutilizzato compreso tra 23000 e 23999. Entrambe le griglie di questa connessione utilizzeranno la stessa porta. È necessario assicurarsi che nessun nodo di una delle griglie utilizzi questa porta per altre connessioni.
Giorni di validità del certificato per questa griglia	Il numero di giorni in cui si desidera che i certificati di protezione per questa griglia nella connessione siano validi. Il valore predefinito è 730 giorni (2 anni), ma è possibile immettere un valore compreso tra 1 e 762 giorni. StorageGRID genera automaticamente certificati client e server per ogni griglia quando si salva la connessione.

Campo	Descrizione
Passphrase di provisioning per questa griglia	La passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
FQDN o IP per l'altra griglia	Una delle seguenti opzioni: • L'FQDN della griglia a cui si desidera connettersi • Indirizzo VIP di un gruppo ha sull'altra griglia • Indirizzo IP di un nodo Admin o di un nodo Gateway nell'altra griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla rete di origine.

1. Selezionare **Salva e continua**.
2. Per la fase Download verifica file, selezionare **Download verifica file**.

Una volta completata la connessione sull'altra griglia, non è più possibile scaricare il file di verifica da nessuna griglia.

3. Individuare il file scaricato (*connection-name.grid-federation*) e salvarlo in una posizione sicura.



Questo file contiene segreti (mascherati come *****) e altri dettagli sensibili e deve essere memorizzato e trasmesso in modo sicuro.

4. Selezionare **Close** (Chiudi) per tornare alla pagina Grid Federation (federazione griglia).
5. Verificare che sia visualizzata la nuova connessione e che il relativo **stato della connessione** sia in **attesa di connessione**.
6. Fornire il *connection-name.grid-federation* file all'amministratore della griglia per l'altra griglia.

Connessione completa

Eseguire questa procedura sul sistema StorageGRID a cui si sta effettuando la connessione (l'altra griglia).

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **Configurazione > Sistema > Federazione di griglia**.
3. Selezionare **carica file di verifica** per accedere alla pagina carica.
4. Selezionare **carica file di verifica**. Quindi, individuare e selezionare il file scaricato dalla prima griglia (*connection-name.grid-federation*).

Vengono visualizzati i dettagli della connessione.

5. Se si desidera, immettere un numero diverso di giorni validi per i certificati di sicurezza per questa griglia. Per impostazione predefinita, la voce **Certificate Valid Days** (giorni validi certificato) corrisponde al valore immesso nella prima griglia, ma ciascuna griglia può utilizzare date di scadenza diverse.

In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.



Se i certificati a una delle due estremità della connessione scadono, la connessione smette di funzionare e le repliche saranno in sospeso fino all'aggiornamento dei certificati.

6. Inserire la passphrase di provisioning per la griglia a cui si è attualmente connessi.

7. Selezionare **Save and test** (Salva e verifica).

I certificati vengono generati e la connessione viene testata. Se la connessione è valida, viene visualizzato un messaggio di esito positivo e la nuova connessione viene elencata nella pagina Grid Federation. Lo stato **Connection** sarà **Connected**.

Se viene visualizzato un messaggio di errore, risolvere eventuali problemi. Vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

8. Accedere alla pagina Grid Federation (federazione griglia) nella prima griglia e aggiornare il browser. Verificare che lo stato della connessione sia ora **connesso**.

9. Una volta stabilita la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Se si modifica questa connessione, viene creato un nuovo file di verifica. Il file originale non può essere riutilizzato.

Al termine

- Fare riferimento alle considerazioni relative a ["gestione dei tenant autorizzati"](#).
- ["Creare uno o più nuovi account tenant"](#), Assegnare l'autorizzazione **Use grid Federation Connection** e selezionare la nuova connessione.
- ["Gestire la connessione"](#) secondo necessità. È possibile modificare i valori di connessione, verificare una connessione, ruotare i certificati di connessione o rimuovere una connessione.
- ["Monitorare la connessione"](#) Come parte delle normali attività di monitoraggio StorageGRID.
- ["Risolvere i problemi di connessione"](#), compresa la risoluzione di eventuali avvisi ed errori relativi alla sincronizzazione degli account e alla replica cross-grid.

Automatizza le connessioni di federazione grid in StorageGRID

Dopo aver installato e configurato due o più sistemi StorageGRID con versione 12.1 o successiva, puoi automatizzare la creazione, la modifica e la manutenzione delle connessioni di federazione della griglia usando lo script Python `manage-grid-federation.py` e un file di configurazione JSON.

Prima di iniziare

- Tutte le griglie eseguono StorageGRID 12.1 o versioni successive.
- Se single sign-on (SSO) è abilitato su una qualsiasi griglia, lo hai disabilitato.
- Hai una macchina Linux con Python 3.6 o versioni successive installato.
- Conosci la posizione dei seguenti file nell'archivio di installazione:

Nome file	Descrizione
<code>manage-grid-federation.py</code>	Script Python utilizzato per automatizzare la gestione delle connessioni di federazione della grid

Nome file	Descrizione
manage-grid-federation.sample.json	File di configurazione di esempio da utilizzare con lo script

- Hai creato un `manage-grid-federation.json` file di configurazione. Per creare questo file, puoi modificare il file di configurazione di esempio `manage-grid-federation.sample.json`.



Conserva le password di amministrazione della griglia e le passphrase di provisioning dal `manage-grid-federation.json` file di configurazione in un luogo sicuro. Se le credenziali vengono omesse dal file, lo script le richiederà in modo interattivo. Dovresti anche conservare una copia di backup del file di configurazione modificato in un luogo sicuro.

Campi del file di configurazione

Il file di configurazione JSON è un array di oggetti. Ogni oggetto rappresenta una grid e supporta i seguenti campi:

Campo	Obbligatorio	Descrizione
hostname	Sì	Nome host o indirizzo IP del nodo Admin per la grid
nome_griglia	Sì	Nome visualizzato per la griglia (massimo 12 caratteri)
nome_utente	No	Nome utente admin della grid (richiesto in modalità interattiva se omesso)
password	No	Password di amministratore della griglia (richiesta interattivamente se omessa)
passphrase	No	Frase di accesso per il provisioning (richiesta in modo interattivo se omessa)
ca_bundle	No	Percorso per un bundle di certificati CA personalizzato per la verifica SSL
regione	No	Regione S3 predefinita desiderata per le connessioni allo spazio dei nomi globale
CNAME	No	CNAME desiderato per le connessioni allo spazio dei nomi globale
globalEndpoint	No	Endpoint desiderato dello spazio dei nomi globale



Se configuri uno qualsiasi dei campi dello spazio dei nomi globale (`region`, `CNAME`, `globalEndpoint`), devi fornire tutti e tre per ogni grid. Assicurati che le regioni e i CNAME siano unici tra le grid e che il valore `globalEndpoint` sia identico per tutte le grid.

A proposito di questa attività

Puoi usare lo `manage-grid-federation.py` script Python e il `manage-grid-federation.json` file di configurazione per automatizzare la gestione delle connessioni di federazione della griglia. Lo script esegue le seguenti operazioni:

- Autentichi a ciascuna griglia tramite l'API di gestione della griglia
- Verifica che tutte le griglie eseguano StorageGRID 12.1 o versioni successive

- Verifica che il single sign-on sia disabilitato su ogni grid
- Recupera le connessioni di federazione di grid esistenti e la configurazione S3
- Aggiorna le impostazioni della regione S3, del CNAME e dell'endpoint dello spazio dei nomi globale quando configurato
- Crea nuove connessioni di federazione di griglia per tutte le coppie di griglie non ancora connesse
- Modifica le connessioni esistenti quando cambiano i nomi visualizzati o le impostazioni dello spazio dei nomi globale
- Visualizza un riepilogo di tutte le connessioni e del loro stato



Puoi anche gestire le connessioni di federazione della griglia utilizzando l'interfaccia utente di Grid Manager o direttamente l'API di Grid Management.

Fasi

1. Accedere alla macchina Linux in uso per eseguire lo script Python.
2. Passa alla directory che contiene lo script.

Ad esempio:

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

dove **piattaforma** è debs, rpms, o vsphere.

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

Ad esempio:

```
./manage-grid-federation.py -i manage-grid-federation.json
```

Puoi usare le seguenti opzioni da riga di comando:

Opzione	Predefinito	Descrizione
<code>-i, --input-json-file</code>	<i>(obbligatorio)</i>	Percorso del file di configurazione JSON contenente l'elenco delle griglie
<code>-b, --base-port</code>	23001	Numero di porta iniziale per le nuove connessioni di federazione di griglia
<code>--no-verify-ssl</code>	Verifica SSL abilitata	Disabilita la verifica del certificato SSL per le connessioni da locale a grid

Modifica le connessioni esistenti

Se lo script rileva che le connessioni esistenti richiedono modifiche — ad esempio, perché i nomi visualizzati nella griglia sono cambiati o le impostazioni dello spazio dei nomi globale devono essere aggiornate — visualizzerà un riepilogo delle modifiche proposte e chiederà conferma prima di procedere.

Quando sono necessari aggiornamenti di configurazione S3 (`region`, `CNAME`, o `globalEndpoint` su griglie con namespace globale abilitato, lo script deve disabilitare temporaneamente il namespace globale per

applicare le modifiche. In questo caso, il messaggio di conferma ti avviserà dell'interruzione temporanea del routing:

```
*** Global Namespace Disable Required ***
Global Namespace must be disabled to update region/CNAME/globalEndpoint
settings.
Routing requests will not work until Global Namespace is re-enabled.
Grids requiring S3 updates: grid1.example.com, grid2.example.com
Proceed with these edits and the temporary routing outage? [y/N]:
```



Durante gli aggiornamenti di configurazione S3, mentre lo spazio dei nomi globale è temporaneamente disabilitato, le richieste di routing dello spazio dei nomi globale non funzionano. Pianifica questa operazione durante una finestra di manutenzione.

Al termine

Le connessioni della federazione della griglia vengono stabilite e configurate quando lo script visualizza un riepilogo di conferma simile al seguente:

```
===== Newly Established Connections =====
  • Grid-A and Grid-B – grid-a.example.com and grid-b.example.com on port
23001

Total new connections: 1

===== All Grid-Federation Connections =====
  Name                Source                Target                Port
Status      Global Namespace
-----
Grid-A and Grid-B grid-a.example.com    grid-b.example.com    23001    new
enabled

Total connections listed: 1

===== Grid S3 Configuration Summary =====
grid-a.example.com:
  Default Region: us-east-1
  CNAME: s3-a.example.com
  Global namespace endpoint: gn.example.com
grid-b.example.com:
  Default Region: us-west-1
  CNAME: s3-b.example.com
  Global namespace endpoint: gn.example.com
```


Stato di uscita

Codice	Descrizione
0	Script completato con successo
1	La convalida non è riuscita oppure una chiamata all'API della griglia ha restituito un errore (controlla l'output del log)



Se una qualsiasi connessione fallisce, lo script continua a elaborare le coppie rimanenti e segnala tutti i fallimenti nella sezione "Connessioni non riuscite" dell'output. Esamina i messaggi di errore e risolvi eventuali problemi prima di eseguire nuovamente lo script.

Scopri lo spazio dei nomi globale per la grid federation

Uno spazio dei nomi globale consente al tenant di accedere ai bucket su più sistemi StorageGRID. Quando lo spazio dei nomi globale è abilitato sulle connessioni di federazione della griglia, le richieste S3 CreateBucket e ListBuckets destinate all'endpoint dello spazio dei nomi globale possono essere inviate all'endpoint del bilanciatore di carico di qualsiasi griglia e vengono instradate automaticamente alla griglia corretta in base alla regione di firma nella richiesta.

Che cos'è uno spazio dei nomi globale?

Uno spazio dei nomi globale consente al tenant di accedere ai bucket su più sistemi StorageGRID. Quando lo spazio dei nomi globale è abilitato sulle connessioni di federazione della griglia, le richieste S3 CreateBucket e ListBuckets destinate all'endpoint dello spazio dei nomi globale possono essere inviate all'endpoint del bilanciatore di carico di qualsiasi griglia e vengono instradate automaticamente alla griglia corretta in base alla regione di firma nella richiesta.



Dovresti configurare un DNS resolver per eseguire la mappatura DNS degli URL dei bucket su una griglia specifica. Se necessario, consulta il tuo amministratore di rete per assicurarti che il DNS resolver sia configurato correttamente. Consulta ["Configura la risoluzione DNS"](#).

StorageGRID non impone nomi di bucket univoci tra le griglie nello spazio dei nomi globale, quindi bucket con lo stesso nome possono esistere su griglie diverse. La regione di firma nella richiesta viene utilizzata per determinare quale griglia possiede il bucket e deve ricevere la richiesta.

Ad esempio, se Grid A utilizza la regione `us-east-1` e Grid B utilizza la regione `us-west-1`, una richiesta CreateBucket inviata a qualsiasi grid con la regione `us-west-1` viene automaticamente instradata a Grid B.

Per ulteriori informazioni sulla federazione di griglie, consulta ["Che cos'è la federazione di griglie?"](#).

Esempio di spazio dei nomi globale

Griglia 1

- Regione predefinita: `region-1`
- CNAME predefinito: `s3.region-1.company.com`
- Endpoint globale: `s3.company.com`

Grid 2

- Regione predefinita: `region-2`
- CNAME predefinito: `s3.region-2.company.com`
- Endpoint globale: `s3.company.com`

Griglia 3

- Regione predefinita: `region-3`
- CNAME predefinito: `s3.region-3.company.com`
- Endpoint globale: `s3.company.com`

CreateBucket e ListBuckets operations

Se crei un bucket (bucket123 con regione di firma `region-2` e lo indirizzi all'endpoint globale `s3.company.com`, qualsiasi grid che riceve la richiesta creerà il bucket su Grid 2.

Operazioni specifiche per bucket e operazioni generali sugli oggetti

Dopo che un bucket è stato creato su una determinata griglia, il tuo resolver DNS risolverà l'URL del bucket nel CNAME del bucket e della griglia.

Nel [esempio sopra](#), il DNS resolver dovrebbe risolvere `bucket123.s3.company.com` in `bucket123.s3.grid3.company.com` (bucket e CNAME della grid). In altre parole, tutte le richieste vengono inviate direttamente a quella grid senza bisogno di routing aggiuntivo.

Esempio

`PutObject` to `bucket123.s3.company.com` risolve in `bucket123.s3.grid3.company.com`

Comportamento S3 con namespace globale

Dopo che lo spazio dei nomi globale è stato completamente configurato, si applica il seguente comportamento S3.

Applicazione della regione

Tutte le richieste S3 all'endpoint dello spazio dei nomi globale, eccetto "[CreateBucket](#)" e "[ListBucket](#)", richiedono che la regione di firma nell'intestazione di autenticazione V4 corrisponda alla regione predefinita della grid.

- Se la regione di firma non corrisponde, la richiesta viene rifiutata con il seguente errore:

```
An error occurred (AuthorizationHeaderMalformed) when calling the
<operation> operation: The authorization header is malformed; the region
'<signing-region>' is wrong; expecting '<grid-default-region>'
```

- L'applicazione delle restrizioni regionali si applica a tutti i bucket della griglia, inclusi quelli creati prima dell'abilitazione dello spazio dei nomi globale.
- L'applicazione delle restrizioni regionali si applica solo alle richieste di autenticazione V4. Le richieste anonime e V2 non sono soggette all'applicazione delle restrizioni regionali.

Routing CreateBucket

CreateBucket requests inviate all'endpoint dello spazio dei nomi globale (`s3.company.com` possono essere indirizzate all'endpoint del bilanciatore di carico di qualsiasi grid. La richiesta viene automaticamente instradata alla grid la cui regione predefinita corrisponde alla regione di firma nella richiesta.

Ad esempio:

- La griglia A ha regione predefinita `us-east-1` e la griglia B ha regione predefinita `us-west-1`.
- Un client invia una richiesta CreateBucket a `s3.company.com` con regione di firma `us-west-1`.
- Round-robin DNS indirizza la richiesta alla Grid A.
- Grid A instrada la richiesta a Grid B.
- Il bucket viene creato su Grid B.

Considerazioni aggiuntive per CreateBucket:

- L'LocationConstraint`elemento può essere impostato su una qualsiasi delle regioni predefinite o non predefinite della griglia. Questo influisce solo sulla policy ILM, non su quale griglia crea il bucket (a differenza del comportamento di AWS con `us-east-1`).
- La regione di firma nella richiesta determina quale grid crea il bucket (la regione di firma deve corrispondere alla regione predefinita della grid di destinazione).
- Le richieste V4 prefirmate sono supportate.
- Le richieste anonime e V2 non sono supportate per il routing dello spazio dei nomi globale.

Routing di ListBuckets

ListBuckets richieste inviate all'endpoint dello spazio dei nomi globale vengono instradate in modo simile alle richieste CreateBucket, utilizzando la regione di firma per determinare la griglia corretta.

Né le risposte di HEAD Bucket né quelle di ListBuckets includono la regione predefinita della griglia. La regione predefinita è implicita nella regione di firma, che viene imposta in modo da corrispondere alla regione predefinita della griglia.

Gestione degli account e delle chiavi di accesso

Gli account tenant e le chiavi di accesso S3 possono essere sincronizzati tra tutte le griglie usando ["sincronizzazione account"](#), ma lo spazio dei nomi globale funziona anche quando ogni griglia ha il proprio set separato di chiavi di accesso. Se usi chiavi di accesso separate, assicurati che il client S3 usi la chiave di accesso corretta quando invia richieste a ciascuna griglia.

E ora?

Ora sei pronto per ["configura lo spazio dei nomi globale"](#).

Configura uno spazio dei nomi globale per la federazione della griglia

Configura uno spazio dei nomi globale per consentire ai tenant di accedere ai bucket su più sistemi StorageGRID.

Per ulteriori informazioni sullo spazio dei nomi globale, consulta ["Scopri lo spazio dei nomi globale per la grid"](#)

federation".

Prima di iniziare

- Hai effettuato l'accesso al Grid Manager su ciascuna griglia utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per ogni griglia.
- Hai esaminato le "considerazioni e requisiti" per le connessioni di federazione della griglia.

Requisiti per la configurazione dello spazio dei nomi globale

- Tutte le griglie nello spazio dei nomi globale devono avere connessioni di federazione di griglia con lo spazio dei nomi globale abilitate tra ogni coppia di griglie.
- Il numero massimo di griglie che possono partecipare a un singolo namespace globale è 11 (la griglia locale e 10 griglie remote).



Il limite di 10 griglie è vincolato dal numero massimo totale di connessioni di federazione di griglia supportate da una distribuzione StorageGRID. Il limite totale di connessioni si applica a **tutte** le connessioni di federazione di griglia nella distribuzione, incluse quelle senza global namespace abilitato, quindi devi assicurarti che il global namespace completamente connesso e tutte le eventuali connessioni di federazione di griglia aggiuntive insieme non superino questo limite complessivo.

- I client S3 devono utilizzare l'autenticazione con firma versione 4 (SigV4). Le richieste anonime e con firma versione 2 non sono supportate per le operazioni di routing dello spazio dei nomi globale.
 - Le richieste firmate normali sono specificate come descritto a "Autenticazione delle richieste: utilizzo dell'intestazione Authorization (AWS Signature Version 4)".
 - Le richieste pre-firmate sono specificate come descritto in "Autenticazione delle richieste: utilizzo dei parametri di query (AWS Signature Version 4)".

Numero di connessioni richieste

In uno spazio dei nomi globale, ogni coppia di griglie deve essere connessa. Il numero di connessioni richieste dipende dal numero di griglie:

Numero di griglie	Numero di connessioni richieste
2	1
3	3
4	6
5	10
n	$n \times (n - 1) / 2$

Passaggio 1: Imposta una regione predefinita univoca per ogni griglia

Ogni griglia nello spazio dei nomi globale deve avere una regione predefinita univoca. La regione predefinita identifica la griglia che possiede un bucket.

CreateBucket e ListBuckets le richieste vengono instradate in base a questa regione e tutte le altre richieste devono corrispondere alla regione predefinita a cui vengono inviate.

Per ulteriori informazioni, consulta ["Configurare le regioni S3"](#).

Fasi

1. Su ciascuna griglia, ["imposta la regione predefinita su un valore univoco"](#). Ad esempio, imposta la Griglia A su `us-east-1` e la Griglia B su `us-west-1`.



Puoi comunque usare regioni non predefinite, impostate tramite l'elemento `LocationConstraint` in ["richieste CreateBucket"](#), per le policy ILM. Le regioni non predefinite non vengono validate per l'unicità tra le grid nello spazio dei nomi globale.

2. Ripeti l'operazione per ogni grid nello spazio dei nomi globale. Ogni grid deve avere una regione predefinita diversa.
3. Configura regioni aggiuntive secondo necessità.

Passaggio 2: Configura le impostazioni dello spazio dei nomi globale S3

Su ogni griglia nello spazio dei nomi globale, aggiungi due nomi di dominio degli endpoint S3:

- Un endpoint di namespace globale identico su tutte le griglie
- Un CNAME univoco per la grid

Configurerai il tuo DNS in modo che l'endpoint dello spazio dei nomi globale si risolva in una o più griglie e che gli endpoint CNAME univoci si risolvano nella griglia specifica.



Devi [configura la regione predefinita](#) prima di configurare le impostazioni dello spazio dei nomi globale S3. Quando abiliti le impostazioni dello spazio dei nomi globale, le richieste S3 falliranno se non specificano la regione corretta. Tutte le richieste S3 devono essere firmate con la regione predefinita della grid.

Fasi

1. In ogni griglia, seleziona **Configurazione > Rete > Nomi di dominio degli endpoint S3 > Nomi di dominio**.
2. Aggiungi un domain name endpoint dello spazio dei nomi globale che sia lo stesso su tutte le griglie. Ad esempio: `s3.example.com`.
3. Aggiungi un CNAME univoco per la griglia. Ad esempio, `s3.company.com`.
4. Selezionare **Salva**.
5. Seleziona **Impostazioni dello spazio dei nomi globale**.
 - a. Seleziona l'endpoint dello spazio dei nomi globale.
 - b. Seleziona il domain name univoco CNAME della grid.
6. Selezionare **Salva**.
7. Assicurati che i certificati server utilizzati dai client includano i nuovi nomi di dominio degli endpoint S3.
 - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza un proprio certificato, ["aggiornare il certificato associato all'endpoint"](#).
 - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il certificato API S3

globale o direttamente ai nodi di archiviazione, ["Aggiornare il certificato API S3 globale"](#).

8. Ripeti questi passaggi su ogni grid nello spazio dei nomi globale.

Per dettagli, consultare ["Configurare i nomi di dominio degli endpoint S3"](#).

Passaggio 3: Crea connessioni di federazione della griglia con spazio dei nomi globale abilitato

Dopo aver configurato i nomi di dominio degli endpoint S3 e le regioni predefinite su tutte le griglie, puoi creare connessioni di federazione di griglia con lo spazio dei nomi globale abilitato.

A proposito di questa attività

Quando crei una connessione di federazione grid e abiliti il global namespace, i campi global namespace endpoint, CNAME e default region vengono popolati automaticamente usando i valori che hai configurato nei passaggi precedenti. Il Grid Manager impedisce di abilitare il global namespace se questi campi non sono impostati correttamente.



Dopo che è stata creata una connessione di federazione di griglie con spazio dei nomi globale, l'endpoint dello spazio dei nomi globale, il CNAME e la regione predefinita per le griglie in quella connessione non possono essere modificati.

Fasi

1. Nella prima griglia, segui i passaggi descritti in ["Creare connessioni di federazione di griglie"](#).
2. Quando inserisci i dettagli di connessione, seleziona **Abilita spazio dei nomi globale**.

I campi per l'endpoint dello spazio dei nomi globale, il record CNAME e la regione predefinita vengono popolati automaticamente con i valori che hai configurato nei passaggi precedenti. Se uno qualsiasi dei valori è mancante o non valido, non puoi abilitare lo spazio dei nomi globale finché non risolvi i problemi.

3. Completa la connessione scaricando il file di verifica e caricandolo sull'altra griglia.
4. Ripeti i passaggi precedenti per ogni coppia di griglie nello spazio dei nomi globale.

Ad esempio, con 3 griglie, ti servono 3 connessioni (Grid A–Grid B, Grid A–Grid C, Grid B–Grid C). Con 4 griglie, ti servono 6 connessioni. Puoi avere un massimo di 10 griglie in un global namespace. Consulta [Numero di connessioni richieste](#).

Passaggio 4: Configura gli endpoint del bilanciatore di carico

["Configura un endpoint del bilanciatore di carico"](#) per ogni griglia nello spazio dei nomi globale. Usa la stessa porta per ciascuno di questi endpoint.



Assicurati di configurare gli endpoint del bilanciatore di carico prima di configurare la risoluzione DNS.

Passaggio 5: Configura la risoluzione DNS

StorageGRID non offre un DNS integrato per lo spazio dei nomi globale. Devi configurare la tua infrastruttura DNS esterna per instradare le richieste S3 al grid corretto.

Il tuo DNS resolver dovrebbe:

1. Risolvere l'endpoint dello spazio dei nomi globale (ad esempio, `s3.example.com`) sugli endpoint del bilanciatore di carico di una o più griglie, di solito utilizzando il DNS round-robin.

2. Risolvi il CNAME univoco di ogni griglia (ad esempio, `s3.grid-a.example.com`) negli endpoint del bilanciatore di carico per quella specifica griglia.
3. Per le richieste di bucket in stile virtual-hosted (ad esempio, `bucket.s3.example.com`), usa la policy di routing della tua organizzazione per mappare i nomi dei bucket al CNAME della griglia appropriata.

StorageGRID non fornisce un meccanismo basato su DNS per scoprire quale grid possiede un bucket. Se hai bisogno di un routing automatico basato sulla proprietà del bucket, usa il ["API di gestione del tenant"](#) per inviare richieste ListBucket che restituiscano gli UUID dei bucket. Mantieni una mappatura interna dagli UUID dei bucket alle grid. Il tuo DNS esterno dovrebbe usare quella mappatura invece di interrogare direttamente StorageGRID.

Informazioni correlate

- ["Che cos'è la federazione di griglie?"](#)
- ["Creare connessioni di federazione di griglie"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)
- ["Gestire le connessioni a federazione di griglie"](#)

Gestisci le connessioni di federazione della griglia StorageGRID

La gestione delle connessioni a federazione di griglie tra sistemi StorageGRID include la modifica dei dettagli di connessione, la rotazione dei certificati, la rimozione delle autorizzazioni del tenant e la rimozione delle connessioni inutilizzate.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager su una delle due griglie utilizzando un ["browser web supportato"](#).
- Si dispone del ["Autorizzazione di accesso root"](#) per la griglia a cui si è effettuato l'accesso.

Modifica una connessione a federazione di griglie

È possibile modificare una connessione a federazione di griglie effettuando l'accesso al nodo di amministrazione primario su una delle griglie della connessione. Una volta apportate le modifiche alla prima griglia, è necessario scaricare un nuovo file di verifica e caricarlo nell'altra griglia.



Durante la modifica della connessione, le richieste di sincronizzazione dell'account o di replica tra griglie continueranno a utilizzare le impostazioni di connessione esistenti. Devi modificare una connessione alla volta e caricare un file di verifica sulla griglia remota per ciascuna connessione. Le modifiche vengono applicate dopo che sono state caricate sulle griglie remote.

Avviare la modifica della connessione

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Seleziona **Nodi** e verifica che tutti gli altri nodi amministrativi nel tuo sistema siano online.



Quando si modifica una connessione a federazione di griglie, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi di amministrazione della prima griglia. Se il file non può essere salvato in tutti i nodi di amministrazione, viene visualizzato un messaggio di avviso quando si seleziona **Salva e test**.

3. Selezionare **Configurazione > Sistema > Federazione di griglia**.
4. Modificare i dettagli della connessione utilizzando il menu **azioni** della pagina Grid Federation o la pagina dei dettagli per una connessione specifica. Vedere "[Creare connessioni di federazione di griglie](#)" per informazioni su come accedere.

Menu delle azioni

- a. Selezionare il pulsante di opzione per la connessione.
- b. Selezionare **azioni > Modifica**.
- c. Inserire le nuove informazioni.

Pagina dei dettagli

- a. Selezionare un nome di connessione per visualizzarne i dettagli.
- b. Selezionare **Modifica**.
- c. Inserire le nuove informazioni.

5. Inserire la passphrase di provisioning per la griglia a cui si è connessi.
6. Selezionare **Salva e continua**.

I nuovi valori vengono salvati, ma non vengono applicati alla connessione fino a quando non si carica il nuovo file di verifica sull'altra griglia.

7. Selezionare **Scarica file di verifica**.

Per scaricare il file in un secondo momento, accedere alla pagina dei dettagli della connessione.

8. Individuare il file scaricato (*connection-name.grid-federation*) e salvarlo in una posizione sicura.



Il file di verifica contiene segreti e deve essere memorizzato e trasmesso in modo sicuro.

9. Selezionare **Close** (Chiudi) per tornare alla pagina Grid Federation (federazione griglia).
10. Verificare che lo stato della connessione sia **Pending EDIT** (Modifica in sospeso).



Se lo stato della connessione era diverso da **connesso** quando si inizia a modificare la connessione, non verrà modificato in **in attesa di modifica**.

11. Fornire il *connection-name.grid-federation* file all'amministratore della griglia per l'altra griglia.

Terminare la modifica della connessione

Terminare la modifica della connessione caricando il file di verifica sull'altra griglia.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **Configurazione > Sistema > Federazione di griglia**.
3. Selezionare **carica file di verifica** per accedere alla pagina di caricamento.
4. Selezionare **carica file di verifica**. Quindi, individuare e selezionare il file scaricato dalla prima griglia.
5. Inserire la passphrase di provisioning per la griglia a cui si è attualmente connessi.
6. Selezionare **Save and test** (Salva e verifica).

Se è possibile stabilire la connessione utilizzando i valori modificati, viene visualizzato un messaggio di esito positivo. In caso contrario, viene visualizzato un messaggio di errore. Esaminare il messaggio e risolvere eventuali problemi.

7. Chiudere la procedura guidata per tornare alla pagina Grid Federation.
8. Verificare che lo stato della connessione sia **connesso**.
9. Accedere alla pagina Grid Federation (federazione griglia) nella prima griglia e aggiornare il browser. Verificare che lo stato della connessione sia ora **connesso**.
10. Una volta stabilita la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Test di una connessione a federazione di griglie

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **Configurazione > Sistema > Federazione di griglia**.
3. Verificare la connessione utilizzando il menu **azioni** della pagina Grid Federation o la pagina dei dettagli per una connessione specifica.

Menu delle azioni

- a. Selezionare il pulsante di opzione per la connessione.
- b. Selezionare **azioni > Test**.

Pagina dei dettagli

- a. Selezionare un nome di connessione per visualizzarne i dettagli.
- b. Selezionare **Test di connessione**.

4. Controllare lo stato della connessione:

Stato della connessione	Descrizione
Connesso	Entrambe le griglie sono collegate e comunicano normalmente.
Errore	La connessione si trova in uno stato di errore. Ad esempio, un certificato è scaduto o un valore di configurazione non è più valido.

Stato della connessione	Descrizione
In attesa di modifica	La connessione su questa griglia è stata modificata, ma la connessione sta ancora utilizzando la configurazione esistente. Per completare la modifica, caricare il nuovo file di verifica nell'altra griglia.
In attesa di connessione	La connessione è stata configurata su questa griglia, ma la connessione non è stata completata sull'altra griglia. Scarica il file di verifica da questa griglia e caricalo nell'altra griglia.
Sconosciuto	La connessione si trova in uno stato sconosciuto, probabilmente a causa di un problema di rete o di un nodo offline.

- Se lo stato della connessione è **Error**, risolvere eventuali problemi. Quindi, selezionare di nuovo **Test di connessione** per confermare che il problema è stato risolto.

rotazione dei certificati di connessione

Ogni connessione a federazione di griglie utilizza quattro certificati SSL generati automaticamente per proteggere la connessione. Quando i due certificati per ogni griglia si avvicinano alla data di scadenza, l'avviso **scadenza del certificato federazione griglia** ricorda di ruotare i certificati.



Se i certificati a una delle due estremità della connessione scadono, la connessione smette di funzionare e le repliche saranno in sospenso fino all'aggiornamento dei certificati.

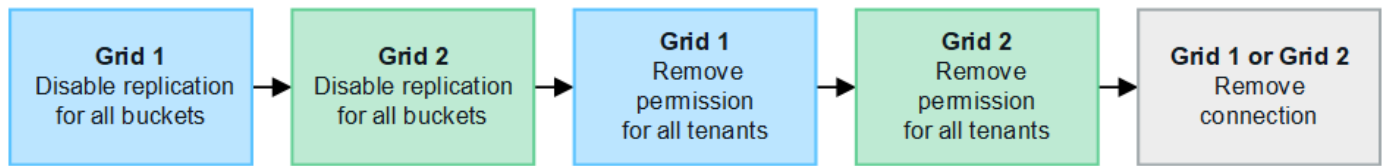
Fasi

- Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
- Selezionare **Configurazione > Sistema > Federazione di griglia**.
- Da una delle schede della pagina Grid Federation, selezionare il nome della connessione per visualizzarne i dettagli.
- Selezionare la scheda **certificati**.
- Selezionare **ruota certificati**.
- Specificare il numero di giorni in cui i nuovi certificati devono essere validi.
- Inserire la passphrase di provisioning per la griglia a cui si è connessi.
- Selezionare **ruota certificati**.
- Se necessario, ripetere questi passaggi sull'altra griglia della connessione.

In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

Rimuovi una connessione a federazione di griglie

È possibile rimuovere una connessione a federazione di griglia da una delle griglie della connessione. Come illustrato nella figura, è necessario eseguire i passaggi necessari su entrambe le griglie per confermare che la connessione non viene utilizzata da alcun tenant su nessuna griglia.



Prima di rimuovere una connessione, tenere presente quanto segue:

- La rimozione di una connessione non elimina gli elementi già copiati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti del tenant presenti in entrambe le griglie non vengono cancellati da nessuna griglia quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Quando si rimuove una connessione, la replica di tutti gli oggetti in sospeso (acquisiti ma non ancora replicati nell'altra griglia) avrà esito negativo in modo permanente.

Disattiva la replica per tutti i bucket del tenant

Fasi

1. Partendo da una griglia, accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **Configurazione > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **tenant consentiti**, determinare se la connessione viene utilizzata da qualsiasi tenant.
5. Se sono elencati dei locatari, istruire tutti i locatari a ["disattiva la replica cross-grid"](#) per tutti i loro bucket su entrambe le griglie nella connessione.



Non è possibile rimuovere l'autorizzazione **use grid Federation Connection** (Usa connessione federazione griglia) se alcuni bucket tenant hanno attivato la replica cross-grid. Ciascun account tenant deve disattivare la replica cross-grid per i bucket su entrambe le griglie.

Rimuovere i permessi per ciascun tenant

Una volta disattivata la replica cross-grid per tutti i bucket del tenant, rimuovere l'autorizzazione **Usa federazione grid** da tutti i tenant su entrambe le grid.

Fasi

1. Selezionare **Configurazione > Sistema > Federazione di griglia**.
2. Selezionare il nome della connessione per visualizzarne i dettagli.
3. Per ciascun tenant nella scheda **tenant consentiti**, rimuovere l'autorizzazione **Usa connessione federazione griglia** da ciascun tenant. Vedere ["Gestire i tenant autorizzati"](#).
4. Ripetere questi passaggi per i tenant consentiti sull'altra griglia.

Rimuovere la connessione

Fasi

1. Se nessun tenant su una griglia sta utilizzando la connessione, selezionare **Remove** (Rimuovi).
2. Controllare il messaggio di conferma e selezionare **Rimuovi**.
 - Se è possibile rimuovere la connessione, viene visualizzato un messaggio di conferma. La

connessione a federazione di griglie viene ora rimossa da entrambe le griglie.

- Se la connessione non può essere rimossa (ad esempio, è ancora in uso o si è verificato un errore di connessione), viene visualizzato un messaggio di errore. È possibile effettuare una delle seguenti operazioni:
 - Risolvere l'errore (consigliato). Vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).
 - Rimuovere la connessione con la forza. Vedere la sezione successiva.

Rimuovi una connessione a federazione di griglie con la forza

Se necessario, è possibile forzare la rimozione di una connessione che non ha lo stato **Connected**.

La rimozione forzata elimina solo la connessione dalla griglia locale. Per rimuovere completamente la connessione, eseguire le stesse operazioni su entrambe le griglie.

Fasi

1. Dalla finestra di dialogo di conferma, selezionare **Force remove** (forza rimozione).

Viene visualizzato un messaggio di successo. Questa connessione a federazione di griglie non può più essere utilizzata. Tuttavia, i bucket tenant potrebbero avere ancora la replica cross-grid attivata e alcune copie degli oggetti potrebbero essere già state replicate tra le griglie della connessione.

2. Dall'altra griglia della connessione, accedere a Grid Manager dal nodo di amministrazione primario.
3. Selezionare **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.

Gestisci i tenant autorizzati per la federazione di grid StorageGRID

Puoi consentire agli account tenant S3 di utilizzare una o più connessioni di federazione grid tra più sistemi StorageGRID. Quando ai tenant è consentito utilizzare una connessione, sono necessari passaggi specifici per modificare i dettagli del tenant o per rimuovere in modo permanente l'autorizzazione di un tenant all'utilizzo della connessione.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager su una delle due griglie utilizzando un ["browser web supportato"](#).
- Si dispone del ["Autorizzazione di accesso root"](#) per la griglia a cui si è effettuato l'accesso.
- Hai ["creazione di una connessione a federazione di griglie"](#) tra due griglie.
- Hai esaminato i flussi di lavoro per ["sincronizzazione account"](#) e ["replica cross-grid"](#).
- Come richiesto, hai già configurato il single sign-on (SSO) o la federazione delle identità per entrambe le griglie nella connessione. Vedi ["Scopri la sincronizzazione degli account per la federazione di griglie"](#).

Creare un tenant consentito

Se vuoi permettere a un tenant account nuovo o esistente di usare una connessione di federazione di griglia

per la sincronizzazione dell'account e la replica tra griglie, segui le istruzioni generali per ["Creare un nuovo tenant S3"](#) o ["modificare un account tenant"](#) e tieni presente quanto segue:

- È possibile creare il tenant da una griglia della connessione. La griglia in cui viene creato un tenant è la griglia di origine del *tenant*.
- Lo stato della connessione deve essere **connesso**.
- Quando il tenant viene creato o modificato per attivare l'autorizzazione **Usa connessione federazione griglia** e quindi salvato nella prima griglia, un tenant identico viene replicato automaticamente nell'altra griglia. La griglia in cui viene replicato il tenant è la griglia di destinazione del *tenant*.
- I tenant di entrambe le griglie avranno lo stesso ID account a 20 cifre, il nome, la descrizione, la quota e le autorizzazioni. In alternativa, è possibile utilizzare il campo **Description** per identificare il tenant di origine e il tenant di destinazione. Ad esempio, questa descrizione per un tenant creato sulla griglia 1 verrà visualizzata anche per il tenant replicato sulla griglia 2: "Questo tenant è stato creato sulla griglia 1".
- Per motivi di sicurezza, la password di un utente root locale non viene copiata nella griglia di destinazione.



Prima che un utente root locale possa accedere al tenant replicato nella griglia di destinazione, un amministratore della griglia per tale griglia deve ["modificare la password per l'utente root locale"](#).

- Una volta che il tenant nuovo o modificato è disponibile su entrambi i grid, gli utenti tenant possono eseguire queste operazioni:
 - Da qualsiasi griglia connessa, crea gruppi e utenti locali, che vengono sincronizzati automaticamente con tutte le altre griglie connesse. Vedi ["Sincronizza gruppi di tenant e utenti"](#).
 - Crea nuove chiavi di accesso S3 per gli utenti locali, che vengono sincronizzate automaticamente con le altre griglie connesse quando la sincronizzazione delle chiavi di accesso è abilitata per il tenant.



Le chiavi di accesso S3 per gli utenti federati vengono clonate una sola volta dalla sorgente alla destinazione quando vengono create. Se queste chiavi di accesso S3 vengono eliminate, queste modifiche non vengono sincronizzate con le altre griglie. Devi eliminare manualmente le chiavi di accesso S3 sulle altre griglie.

- Creare bucket identici su entrambe le griglie della connessione e abilitare la replica cross-grid in una direzione o in entrambe le direzioni. Vedere ["Gestire la replica cross-grid"](#).

Visualizzare un tenant consentito

È possibile visualizzare i dettagli di un tenant autorizzato a utilizzare una connessione a federazione di griglie.

Fasi

1. Selezionare **Inquilini**.
2. Dalla pagina tenant, selezionare il nome del tenant per visualizzare la pagina dei dettagli del tenant.
3. Seleziona facoltativamente la scheda **Federazione griglia** per ["monitorare le connessioni della grid federation"](#).

Modificare un tenant consentito

Se è necessario modificare un tenant con l'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per ["modifica di un account tenant"](#) e osservare quanto segue:

- Se un tenant ha l'autorizzazione **Usa la connessione di federazione di griglia**:

- Puoi modificare i dettagli del tenant da qualsiasi griglia nella connessione. Le modifiche alle impostazioni a livello di tenant (come nome, descrizione o quota), così come ai gruppi, agli utenti locali e alle chiavi di accesso S3 di proprietà degli utenti locali, vengono sincronizzate automaticamente con tutte le griglie connesse.
- Puoi modificare le **connessioni di federazione di griglia consentite** solo sulla griglia di origine.
- Puoi aggiungere una nuova connessione di federazione di griglia.



Non puoi deselezionare le connessioni esistenti. Per rimuovere una connessione, vai alla pagina dei dettagli del tenant, seleziona la scheda **Grid federation** e rimuovi l'autorizzazione.

- Se aggiungi una nuova connessione durante la modifica di un tenant, questo tenant verrà replicato nella griglia remota specificata da quella nuova connessione.

Eliminare un tenant consentito



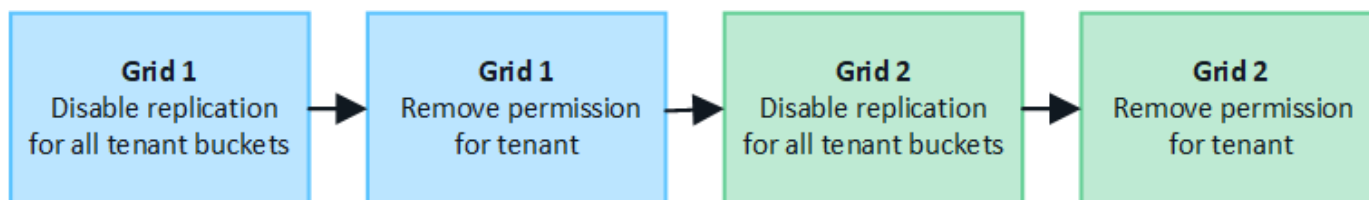
Se rimuovi il tenant originale dalla griglia di origine o il tenant sincronizzato dalla griglia di destinazione, il tenant viene rimosso da tutte le griglie, quindi l'account non può più essere utilizzato.

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 osservare quanto segue:

- Prima di poter rimuovere il tenant dalla griglia di origine, devi rimuovere tutti i bucket dell'account dalla griglia di origine.
- Prima di poter rimuovere il tenant sincronizzato dalla griglia di destinazione, devi rimuovere tutti i bucket dell'account sulla griglia di destinazione.
- Se rimuovi il tenant originale o quello sincronizzato, l'account non potrà più essere utilizzato per la replica tra griglie.
- Se rimuovi il tenant originale dalla griglia di origine o da qualsiasi griglia di destinazione, anche i gruppi di tenant, gli utenti e le chiavi che sono stati sincronizzati con le griglie di destinazione vengono rimossi.

Rimuovi l'autorizzazione Usa connessione federazione griglia

Per impedire a un tenant di utilizzare una connessione a federazione di griglie, è necessario rimuovere l'autorizzazione **Usa connessione a federazione di griglie**.



Prima di rimuovere l'autorizzazione di un tenant a utilizzare una connessione a federazione di griglie, tenere presente quanto segue:

- Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se uno dei bucket del tenant ha attivato la replica cross-grid. L'account tenant deve prima disattivare la replica cross-grid per tutti i bucket.
- La rimozione dell'autorizzazione **Usa connessione federazione griglia** non elimina gli elementi che sono

già stati replicati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti del tenant presenti in entrambe le griglie non vengono cancellati da nessuna griglia quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.

- Se si desidera riattivare questa autorizzazione con la stessa connessione di federazione della griglia, eliminare prima questo tenant sulla griglia di destinazione; in caso contrario, riabilitare questa autorizzazione causerà un errore.



Riattivando l'autorizzazione **Usa connessione di federazione griglia**, la griglia locale diventa la griglia di origine e viene avviata la sincronizzazione con la griglia remota specificata dalla connessione di federazione griglia selezionata. Se il tenant account esiste già sulla griglia remota, la sincronizzazione genererà un errore di conflitto.

Prima di iniziare

- Si sta utilizzando un ["browser web supportato"](#).
- Avete il ["Autorizzazione di accesso root"](#) per entrambe le griglie.

Disattiva la replica per i bucket tenant

Come primo passo, disattivare la replica cross-grid per tutti i bucket del tenant.

Fasi

1. Partendo da una griglia, accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **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 il locatario è presente nell'elenco, indicare a ["disattiva la replica cross-grid"](#) per tutti i bucket su entrambe le griglie della connessione.



Non è possibile rimuovere l'autorizzazione **use grid Federation Connection** (Usa connessione federazione griglia) se alcuni bucket tenant hanno attivato la replica cross-grid. Il tenant deve disattivare la replica cross-grid per i bucket su entrambe le griglie.

Rimuovere l'autorizzazione per il tenant

Una volta disattivata la replica cross-grid per i bucket tenant, è possibile rimuovere il permesso del tenant per utilizzare la connessione di federazione grid.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Rimuovere l'autorizzazione dalla pagina Grid Federation o dalla pagina tenant.

Pagina Grid Federation

- a. Selezionare **Configurazione > Sistema > Federazione di griglia**.
- b. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
- c. Nella scheda **tenant consentiti**, selezionare il pulsante di opzione corrispondente al tenant.
- d. Selezionare **Rimuovi permesso**.

Pagina tenant

- a. Selezionare **Inquilini**.
- b. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
- c. Nella scheda **Grid Federation**, selezionare il pulsante di opzione per la connessione.
- d. Selezionare **Rimuovi permesso**.

3. Esaminare gli avvisi nella finestra di dialogo di conferma e selezionare **Rimuovi**.

- Se l'autorizzazione può essere rimossa, viene visualizzata nuovamente la pagina dei dettagli e viene visualizzato un messaggio di conferma. Questo tenant non può più utilizzare la connessione a federazione di grid.
- Se in uno o più bucket tenant è ancora attivata la replica cross-grid, viene visualizzato un errore.

 **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

È possibile effettuare una delle seguenti operazioni:

- (Consigliato.) Accedere a Tenant Manager e disattivare la replica per ciascun bucket del tenant. Vedere ["Gestire la replica cross-grid"](#). Quindi, ripetere la procedura per rimuovere l'autorizzazione **Usa connessione alla rete**.
- Rimuovere l'autorizzazione forzatamente. Vedere la sezione successiva.

4. Passare all'altra griglia e ripetere questa procedura per rimuovere l'autorizzazione per lo stesso tenant sull'altra griglia.

Rimuovi l'autorizzazione in base alla forza

Se necessario, è possibile forzare la rimozione dell'autorizzazione di un tenant per utilizzare una connessione a federazione di griglia anche se i bucket tenant hanno la replica cross-grid attivata.

Prima di rimuovere l'autorizzazione di un locatario con la forza, prendere nota delle considerazioni generali per [rimozione dell'autorizzazione](#) e di queste considerazioni aggiuntive:

- Se si rimuove l'autorizzazione **Usa connessione federazione griglia** per forza, tutti gli oggetti che sono in attesa di replica nell'altra griglia (acquisiti ma non ancora replicati) continueranno a essere replicati. Per evitare che questi oggetti in-process raggiungano il bucket di destinazione, è necessario rimuovere anche

l'autorizzazione del tenant sull'altra griglia.

- Qualsiasi oggetto acquisito nel bucket di origine dopo la rimozione dell'autorizzazione **Usa connessione federazione griglia** non verrà mai replicato nel bucket di destinazione.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **Configurazione > Sistema > Federazione di griglia**.
3. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
4. Nella scheda **tenant consentiti**, selezionare il pulsante di opzione corrispondente al tenant.
5. Selezionare **Rimuovi permesso**.
6. Esaminare gli avvisi nella finestra di dialogo di conferma e selezionare **Force remove** (forza rimozione).

Viene visualizzato un messaggio di successo. Questo tenant non può più utilizzare la connessione a federazione di grid.

7. Se necessario, passare all'altra griglia e ripetere questa procedura per forzare la rimozione dell'autorizzazione per lo stesso account tenant sull'altra griglia. Ad esempio, è necessario ripetere questi passaggi sull'altra griglia per evitare che gli oggetti in-process raggiungano il bucket di destinazione.

Risoluzione dei problemi degli errori di federazione della griglia in StorageGRID

Potresti dover risolvere problemi relativi ad avvisi ed errori riguardanti le connessioni di federazione della griglia, la sincronizzazione degli account e la replica tra griglie.

Avvisi ed errori di connessione a Grid Federation

È possibile che si ricevano avvisi o si verifichino errori con le connessioni della federazione di griglie.

Dopo aver apportato qualsiasi modifica per risolvere un problema di connessione, verificare che lo stato della connessione torni a **connesso**. Per istruzioni, vedere ["Gestire le connessioni a federazione di griglie"](#).

Avviso di errore di connessione della federazione di griglie

Problema

È stato attivato l'avviso **errore di connessione federazione griglia**.

Dettagli

Questo avviso indica che la connessione a federazione di griglie tra le griglie non funziona.

Azioni consigliate

1. Esaminare le impostazioni della pagina Grid Federation per entrambe le griglie. Verificare che tutti i valori siano corretti. Vedere ["Gestire le connessioni a federazione di griglie"](#).
2. Esaminare i certificati utilizzati per la connessione. Assicurarsi che non ci siano avvisi per i certificati di federazione griglia scaduti e che i dettagli di ciascun certificato siano validi. Vedere le istruzioni per la rotazione dei certificati di connessione in ["Gestire le connessioni a federazione di griglie"](#).
3. Verificare che tutti i nodi Admin e Gateway in entrambe le griglie siano online e disponibili. Risolvere eventuali avvisi che potrebbero interessare questi nodi e riprovare.
4. Se è stato fornito un nome di dominio completo (FQDN) per la griglia locale o remota, verificare che il server DNS sia in linea e disponibile. Vedere ["Che cos'è la federazione di griglie?"](#) per i requisiti di rete,

indirizzo IP e DNS.

Scadenza dell'avviso del certificato di federazione griglia

Problema

È stato attivato l'avviso **scadenza del certificato federazione griglia**.

Dettagli

Questo avviso indica che uno o più certificati di federazione griglia stanno per scadere.

Azioni consigliate

Vedere le istruzioni per la rotazione dei certificati di connessione in ["Gestire le connessioni a federazione di griglie"](#).

Errore durante la modifica di una connessione a federazione di griglie

Problema

Quando si modifica una connessione a federazione di griglie, viene visualizzato il seguente messaggio di avviso quando si seleziona **Salva e test**: "Impossibile creare un file di configurazione candidato su uno o più nodi."

Dettagli

Quando si modifica una connessione a federazione di griglie, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi di amministrazione della prima griglia. Viene visualizzato un messaggio di avviso se il file non può essere salvato in tutti i nodi di amministrazione, ad esempio perché un nodo di amministrazione non è in linea.

Azioni consigliate

1. Dalla griglia che stai utilizzando per modificare la connessione, seleziona **Nodi**.
2. Verificare che tutti i nodi Admin per la griglia siano in linea.
3. Se alcuni nodi sono offline, ripristinarli online e provare a modificare nuovamente la connessione.

Errori di sincronizzazione dell'account

Impossibile accedere a un account tenant sincronizzato

Problema

Non puoi accedere a un account tenant sincronizzato. Il messaggio di errore nella pagina di accesso di Tenant Manager è "Le credenziali per questo account non erano valide. Riprova."

Dettagli

La password che imposti per l'utente root locale del tenant e per gli altri utenti locali viene sincronizzata automaticamente. Tuttavia, potresti dover cambiare la password per l'utente root locale del tenant sulla griglia di destinazione prima di poter accedere all'account del tenant su quella griglia.

Azioni consigliate

Prima che l'utente root possa accedere alla griglia di destinazione del tenant, è necessario che un amministratore della griglia ["modificare la password per l'utente root locale"](#) si trovi nella griglia di destinazione.

Tenant creato senza sincronizzazione

Problema

Vedi il messaggio "Tenant creato senza sincronizzazione" dopo aver creato un nuovo tenant con l'autorizzazione **Use grid federation connection**.

Dettagli

Questo problema può verificarsi se gli aggiornamenti allo stato della connessione vengono posticipati, causando l'elenco di una connessione non funzionante come **connessa**.

Azioni consigliate

1. Esaminare i motivi elencati nel messaggio di errore e risolvere eventuali problemi di rete o di altro tipo che potrebbero impedire il funzionamento della connessione. Vedere [Avvisi ed errori di connessione Grid Federation](#).
2. Seguire le istruzioni per testare una connessione di federazione della griglia in "[Gestire le connessioni a federazione di griglie](#)" per confermare che il problema è stato risolto.
3. Dalla griglia di origine del tenant, seleziona **Tenant**.
4. Individua il tenant account che non è stato sincronizzato.
5. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
6. Seleziona **Riprova la sincronizzazione**. Se l'errore è stato risolto, il tenant account verrà ora sincronizzato con l'altra grid.

Avvisi ed errori di replica cross-grid

Viene visualizzato l'ultimo errore per la connessione o il tenant

Problema

Quando "[visualizzazione di una connessione a federazione di griglie](#)" (o quando "[gestione dei tenant consentiti](#)" per una connessione) si nota un errore nella colonna **ultimo errore** nella pagina dei dettagli della connessione. Ad esempio:

Grid 1 - Grid 2

Local hostname (this grid):10.115.96.170

Port:23000

Remote hostname (other grid):10.115.96.175

Connection status: Connected

EditDownload fileTest connectionRemove

Permitted tenantsCertificates

Remove permissionClear errorSearch...

Displaying one result

Tenant name	Last error ?
 Tenant A	2025-03-13 15:54:59 PDT 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. (logID 13371653720226059496) 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 vengono 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 cancellato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il bucket di destinazione ha la versione sospesa.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più disponibile.
- L'oggetto di origine ha impostazioni di blocco degli oggetti S3 che non sono conformi alle impostazioni di conservazione a livello di tenant della griglia di destinazione.
- L'oggetto di origine ha impostazioni di blocco oggetto S3 e il blocco oggetto S3 è disabilitato sul bucket di destinazione.

Azioni consigliate

Se nella colonna **ultimo errore** viene visualizzato un messaggio di errore, attenersi alla seguente procedura:

1. Rivedere il testo del messaggio.
2. Eseguire tutte le azioni raccomandate.

Ad esempio, se il versioning è stato sospeso sul bucket di destinazione per la replica cross-grid, riattiva il versioning per quel bucket. Oppure, se S3 Object Lock è stato disabilitato sul bucket di destinazione per la replica cross-grid, abilita S3 Object Lock per quel bucket.

3. Selezionare la connessione o l'account tenant dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.



Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.



Dopo aver corretto l'errore, potrebbe essere visualizzato un nuovo **ultimo errore** se gli oggetti vengono acquisiti in un bucket diverso che presenta anche un errore.

7. Per determinare se alcuni oggetti non sono stati replicati a causa dell'errore bucket, vedere ["Identificare e riprovare le operazioni di replica non riuscite"](#).

Avviso di errore permanente della replica cross-grid

Problema

È stato attivato l'avviso **errore permanente replica cross-grid**.

Dettagli

Questo avviso indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un

motivo che richiede l'intervento dell'utente per la risoluzione. Questo avviso è generalmente causato da una modifica al bucket di origine o di destinazione.

Azioni consigliate

1. Accedere alla griglia in cui è stato attivato l'avviso.
2. Vai su **Configurazione > Sistema > Federazione di griglia** e individua il nome della connessione elencato nell'avviso.
3. Nella scheda Permitted tenant (tenant consentiti), esaminare la colonna **Last error** (ultimo errore) per determinare quali account tenant presentano errori.
4. Per ulteriori informazioni sugli errori, consultare le istruzioni nella sezione "[Monitorare le connessioni a federazione di griglie](#)" per esaminare le metriche di replica tra griglie.
5. Per ciascun account tenant interessato:
 - a. Consultare le istruzioni nella "[Monitorare l'attività del tenant](#)" per confermare che il tenant non ha superato la quota nella griglia di destinazione per la replica cross-grid.
 - b. Se necessario, aumentare la quota del tenant sulla griglia di destinazione per consentire il salvataggio di nuovi oggetti.
6. Per ogni tenant interessato, accedi a tenant Manager su entrambe le griglie, in modo da poter confrontare l'elenco dei bucket.
7. Per ogni bucket con replica cross-grid attivata, confermare quanto segue:
 - Esiste un bucket corrispondente per lo stesso tenant sull'altra griglia (deve utilizzare il nome esatto).
 - Entrambi i bucket hanno attivato la versione degli oggetti (la versione non può essere sospesa su nessuna griglia).
 - Nessuno dei due bucket si trova nello stato **Deleting Objects: Read-only**.
8. Per confermare che il problema è stato risolto, consultare le istruzioni in "[Monitorare le connessioni a federazione di griglie](#)" per esaminare le metriche di replica tra griglie oppure eseguire le seguenti operazioni:
 - a. Torna alla pagina Grid Federation.
 - b. Selezionare il tenant interessato e selezionare **Cancella errore** nella colonna **ultimo errore**.
 - c. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
 - d. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.



Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.



Una volta risolto, l'avviso potrebbe richiedere fino a un giorno.

- a. Accedere a "[Identificare e riprovare le operazioni di replica non riuscite](#)" per identificare gli oggetti o eliminare i marcatori che non sono stati replicati nell'altra griglia e riprovare la replica secondo necessità.

Avviso di risorsa di replica cross-grid non disponibile

Problema

È stato attivato l'avviso **risorsa di replica cross-grid non disponibile**.

Dettagli

Questo avviso indica che le richieste di replica cross-grid sono in sospeso perché una risorsa non è disponibile. Ad esempio, potrebbe essere presente un errore di rete.

Azioni consigliate

1. Monitorare l'avviso per verificare se il problema si risolve da solo.
2. Se il problema persiste, determinare se una griglia presenta un avviso di errore di connessione * federazione griglia per la stessa connessione o un avviso di errore di comunicazione * con nodo * per un nodo. Questo avviso potrebbe essere risolto quando si risolvono tali avvisi.
3. Per ulteriori informazioni sugli errori, consultare le istruzioni nella sezione ["Monitorare le connessioni a federazione di griglie"](#) per esaminare le metriche di replica tra griglie.
4. Se non riesci a risolvere l'avviso, contatta il supporto tecnico.

La replica cross-grid procederà normalmente dopo la risoluzione del problema.

Identificare e riprovare le operazioni di replica di StorageGRID non riuscite

Dopo aver risolto l'avviso **errore permanente replica cross-grid**, è necessario determinare se non è stato possibile replicare oggetti o marker di eliminazione nell'altra griglia. È quindi possibile recuperare questi oggetti o utilizzare l'API Grid Management per riprovare la replica.

L'avviso **errore permanente di replica cross-grid** indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per la risoluzione. Questo avviso è generalmente causato da una modifica al bucket di origine o di destinazione. Per ulteriori informazioni, vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

Determinare se non è stato possibile replicare oggetti

Per determinare se gli oggetti o i marcatori di eliminazione non sono stati replicati nell'altra griglia, è possibile cercare i messaggi nel registro di controllo ["CGRR \(Cross-Grid Replication Request\)"](#). Questo messaggio viene aggiunto al registro quando StorageGRID non riesce a replicare un oggetto, un oggetto multiparte o un indicatore di eliminazione nel bucket di destinazione.

È possibile utilizzare ["tool di verifica-spiegazione"](#) per convertire i risultati in un formato più facile da leggere.

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- Si dispone del `Passwords.txt` file.
- Si conosce l'indirizzo IP del nodo di amministrazione primario.

Fasi

1. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

2. Cercare i messaggi CGRR in audit.log e utilizzare lo strumento di spiegazione dell'audit per formattare i risultati.

Ad esempio, questo comando si greper per tutti i messaggi CGRR negli ultimi 30 minuti e utilizza lo strumento audit-exclaring.

```
# awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date {
print }' audit.log | grep CGRR | audit-explain
```

Il risultato del comando sarà simile a questo esempio, che contiene voci per sei messaggi CGRR. Nell'esempio, tutte le richieste di replica cross-grid hanno restituito un errore generale perché non è stato possibile replicare l'oggetto. I primi tre errori riguardano le operazioni "Replicate Object", mentre gli ultimi tre errori riguardano le operazioni "Replicate delete marker".

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Ciascuna voce contiene le seguenti informazioni:

Campo	Descrizione
Richiesta di replica CGRR Cross-Grid	Il nome della richiesta
tenant	ID account del tenant
connessione	L'ID della connessione a federazione di griglie

Campo	Descrizione
operazione	Il tipo di operazione di replica che si stava tentando di eseguire: • oggetto replicate • marker di eliminazione replicato • replica di un oggetto multiparte
bucket	Il nome del bucket
oggetto	Il nome dell'oggetto
versione	L'ID versione dell'oggetto
errore	Il tipo di errore. Se la replica cross-grid non riesce, l'errore è "General error" (errore generale).

Riprovare a eseguire repliche non riuscite

Dopo aver generato un elenco di oggetti e marker di eliminazione che non sono stati replicati nel bucket di destinazione e aver risolto i problemi sottostanti, è possibile riprovare la replica in due modi:

- Inserire ciascun oggetto nel bucket di origine.
- Utilizzare l'API privata Grid Management, come descritto.

Fasi

1. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
2. Selezionare **Vai alla documentazione API privata**.



Gli endpoint dell'API StorageGRID contrassegnati come "privati" sono soggetti a modifica senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Nella sezione **cross-grid-Replication-Advanced**, selezionare il seguente endpoint:

```
POST /private/cross-grid-replication-retry-failed
```

4. Selezionare **Provalo**.
5. Nella casella di testo **body**, sostituire la voce di esempio per **versionID** con un ID di versione di audit.log che corrisponde a una richiesta di replica cross-grid non riuscita.

Assicurarsi di conservare le virgolette doppie intorno alla stringa.

6. Selezionare **Esegui**.
7. Verificare che il codice di risposta del server sia **204**, a indicare che l'oggetto o il marker di eliminazione è stato contrassegnato come in sospeso per la replica cross-grid sull'altra griglia.



In sospeso indica che la richiesta di replica cross-grid è stata aggiunta alla coda interna per l'elaborazione.

Monitorare i tentativi di replica

È necessario monitorare le operazioni di ripetizione della replica per assicurarsi che vengano completate.



La replica di un oggetto o di un marker di eliminazione nell'altra griglia potrebbe richiedere diverse ore o più.

È possibile monitorare le operazioni di ripetizione in due modi:

- Utilizzare un S3 "[HeadObject \(oggetto intestazione\)](#)" o "[GetObject](#)" una richiesta. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• COMPLETATO: La replica è riuscita. • PENDING: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.

- Utilizzare l'API privata Grid Management, come descritto.

Fasi

1. Nella sezione **cross-grid-Replication-Advanced** della documentazione dell'API privata, selezionare il seguente endpoint:

```
GET /private/cross-grid-replication-object-status/{id}
```

2. Selezionare **Provalo**.
3. Nella sezione Parameter (parametro), immettere l'ID della versione utilizzato nella `cross-grid-replication-retry-failed` richiesta.
4. Selezionare **Esegui**.
5. Verificare che il codice di risposta del server sia **200**.
6. Esaminare lo stato della replica, che sarà uno dei seguenti:
 - **PENDING**: L'oggetto non è stato ancora replicato.
 - **COMPLETATO**: La replica è riuscita.
 - **FAILED**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Gestire la sicurezza

Gestisci la sicurezza in StorageGRID

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

Gestire la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Devi ["esaminare i metodi di crittografia disponibili"](#) determinare quali soddisfano i tuoi requisiti di protezione dei dati.

Gestire i certificati

È possibile ["configurare e gestire i certificati del server"](#) utilizzare per le connessioni HTTP o i certificati client utilizzati per autenticare un'identità client o utente sul server.

Configurare i server di gestione delle chiavi

Utilizzando un ["server di gestione delle chiavi"](#) possibile proteggere i dati StorageGRID anche se un'appliance viene rimossa dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.



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

Gestire le impostazioni del proxy

Se utilizzi servizi di piattaforma S3 o pool di cloud storage, puoi configurare un ["server proxy di archiviazione"](#) tra i nodi storage e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un ["admin proxy server \(server proxy amministratore\)"](#) tra i nodi Admin e il supporto tecnico.

Firewall di controllo

Per migliorare la protezione del sistema, è possibile controllare l'accesso ai nodi amministrativi di StorageGRID aprendo o chiudendo porte specifiche su ["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 l'implementazione.

Esaminare i metodi di crittografia StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. È necessario esaminare i metodi disponibili per determinare quali metodi soddisfano i requisiti di protezione dei dati.

La tabella fornisce un riepilogo generale dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Server di gestione delle chiavi (KMS) in Grid Manager	" configurare un server di gestione delle chiavi "Per il sito StorageGRID e " abilitare la crittografia dei nodi per l'appliance ". Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia a chiave (KEK). Questa chiave crittografa e decrta la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi appliance con Node Encryption attivato durante l'installazione. Tutti i dati dell'appliance sono protetti da perdite fisiche o rimozione dal data center. Nota: La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di archiviazione e le appliance di servizi.
Pagina crittografia unità nel programma di installazione dell'appliance StorageGRID	Se l'appliance contiene unità che supportano la crittografia hardware, è possibile impostare una passphrase dell'unità durante l'installazione. Quando si imposta una passphrase di unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non conoscano la passphrase. Prima di iniziare l'installazione, andare a Configure hardware > Drive Encryption per impostare una passphrase di unità che si applica a tutte le unità gestite da StorageGRID con crittografia automatica in un nodo.	Appliance che contengono dischi con crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. La crittografia dei dischi non si applica ai dischi gestiti da SANtricity. Se hai un'appliance storage con dischi a crittografia automatica e controller SANtricity, puoi abilitare la sicurezza dei dischi in SANtricity.
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione di protezione dell'unità è attivata per l'appliance StorageGRID, è possibile utilizzare " Gestore di sistema di SANtricity " per creare e gestire la chiave di protezione. La chiave è necessaria per accedere ai dati sui dischi protetti.	Appliance storage con dischi FDE (Full Disk Encryption) o dischi a crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non è utilizzabile con alcune appliance di storage o con alcuna appliance di servizi.
Crittografia degli oggetti memorizzati	L'opzione viene attivata " Crittografia degli oggetti memorizzati "in Grid Manager. Quando questa opzione è attivata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Nuovi dati oggetto S3 acquisiti. Gli oggetti memorizzati esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati.

Opzione di crittografia	Come funziona	Valido per
Crittografia bucket S3	Viene inviata una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati. "Operazioni sui bucket"
Crittografia a oggetti lato server (SSE) S3	Viene inviata una richiesta S3 per memorizzare un oggetto e includere l' `x-amz-server-side-encryption` intestazione della richiesta.	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. StorageGRID gestisce le chiavi. "Utilizzare la crittografia lato server"
Crittografia a oggetti S3 lato server con chiavi fornite dal cliente (SSE-C)	Viene inviata una richiesta S3 per memorizzare un oggetto e includere tre intestazioni di richiesta. • x-amz-server-side-encryption-customer-algorithm • x-amz-server-side-encryption-customer-key • x-amz-server-side-encryption-customer-key-MD5	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. Le chiavi vengono gestite al di fuori di StorageGRID. "Utilizzare la crittografia lato server"
Crittografia di un volume esterno o di un datastore	Se la piattaforma di implementazione lo supporta, si utilizza un metodo di crittografia esterno a StorageGRID per crittografare un intero volume o datastore.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o datastore sia crittografato. Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.

Opzione di crittografia	Come funziona	Valido per
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati degli oggetti e i metadati prima che vengano acquisiti in StorageGRID.	Solo dati a oggetti e metadati (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati. "Amazon Simple Storage Service - Guida utente: Protezione dei dati mediante crittografia lato client"

Utilizzare più metodi di crittografia

A seconda dei requisiti, è possibile utilizzare più metodi di crittografia alla volta. Ad esempio:

- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e utilizzare la funzionalità di sicurezza del disco in Gestione sistema di SANtricity per "crittografare due volte" i dati sui dischi con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare l'opzione di crittografia degli oggetti memorizzati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte degli oggetti richiede la crittografia, prendere in considerazione il controllo della crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo per le performance.

Informazioni correlate

["Scopri le opzioni di crittografia certificate FIPS"](#)

Gestire i certificati

Gestisci i certificati di sicurezza in StorageGRID

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

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

Quando un client si connette al server tramite HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client confronta 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 funziona come server per alcune connessioni (come l'endpoint del bilanciamento del carico) o come client per altre connessioni (come il servizio di replica di CloudMirror).

Certificato Grid CA predefinito

StorageGRID dispone di 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.

Utilizzare il certificato Grid CA per gli ambienti non di produzione. Per la produzione, utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Le connessioni non protette senza certificato sono supportate ma non consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati devono essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare la ["linee guida per la protezione avanzata del sistema per i certificati server"](#).
- StorageGRID supporta il raggruppamento di certificati da una CA in un singolo file (noto come bundle di certificati CA).



StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica di StorageGRID.

Accesso ai certificati di sicurezza

È possibile accedere alle informazioni su tutti i certificati StorageGRID in una singola posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

Fasi

1. Da Grid Manager, 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 certificati e per accedere alle impostazioni del certificato. È possibile accedere a una scheda se si dispone di ["autorizzazione appropriata"](#).
- **Globale:** Protegge l'accesso a StorageGRID da browser Web e client API esterni.
 - **Grid CA:** Protegge il traffico StorageGRID interno.
 - **Client:** Protegge le connessioni tra client esterni e il database StorageGRID Prometheus.
 - **Endpoints del bilanciamento del carico:** Protegge le connessioni tra i client S3 e il bilanciamento del carico StorageGRID.
 - **Tenant:** Protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi della piattaforma alle risorse di storage S3.
 - **Altro:** Protegge le connessioni StorageGRID che richiedono certificati specifici.

Ciascuna scheda viene descritta di seguito con collegamenti a dettagli aggiuntivi del certificato.

Globale

I certificati globali proteggono l'accesso StorageGRID dai browser Web e dai client API S3 esterni. Durante l'installazione, l'autorità di certificazione StorageGRID genera inizialmente due certificati globali. La procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- [Certificato dell'interfaccia di gestione](#): Protegge le connessioni del browser Web del client alle interfacce di gestione StorageGRID.
- [Certificato API S3](#): Protegge le connessioni API client ai nodi di archiviazione, ai nodi amministrativi e ai nodi gateway, che le applicazioni client S3 utilizzano per caricare e scaricare i dati oggetto.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Type**: Personalizzato o predefinito. + per una maggiore sicurezza della griglia, è necessario utilizzare sempre un certificato personalizzato.
- **Data di scadenza**: Se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

È possibile:

- Sostituire i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per una maggiore sicurezza della griglia:
 - ["Sostituire il certificato predefinito dell'interfaccia di gestione generata da StorageGRID"](#) Utilizzato per le connessioni di Grid Manager e Tenant Manager.
 - ["Sostituire il certificato API S3"](#) Utilizzato per connessioni endpoint nodo storage e bilanciamento del carico (opzionali).
- ["Ripristinare il certificato dell'interfaccia di gestione predefinita"](#).
- ["Ripristinare il certificato API S3 predefinito"](#).
- ["Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione"](#).
- Copiare o scaricare ["certificato dell'interfaccia di gestione"](#) o ["Certificato API S3"](#).

CA griglia

Il [Certificato Grid CA](#), generato dall'autorità di certificazione StorageGRID durante l'installazione di StorageGRID, protegge tutto il traffico StorageGRID interno.

Le informazioni sul certificato includono la data di scadenza del certificato e il contenuto del certificato.

È possibile ["Copia o scarica il certificato Grid CA"](#), ma non è possibile modificarlo.

Client

[Certificati client](#), Generato da un'autorità di certificazione esterna, proteggere le connessioni tra gli strumenti di monitoraggio esterni e il database di StorageGRID Prometheus.

La tabella dei certificati contiene una riga per ciascun certificato client configurato e indica se il certificato può essere utilizzato per l'accesso al database Prometheus, insieme alla data di scadenza

del certificato.

È possibile:

- ["Caricare o generare un nuovo certificato client."](#)
- Selezionare il nome di un certificato per visualizzare i dettagli del certificato in cui è possibile:
 - ["Modificare il nome del certificato client."](#)
 - ["Impostare l'autorizzazione di accesso Prometheus."](#)
 - ["Caricare e sostituire il certificato del client."](#)
 - ["Copiare o scaricare il certificato client."](#)
 - ["Rimuovere il certificato client."](#)
- Selezionare **azioni** per rapidamente ["modifica"](#), ["allega"](#) o ["rimuovere"](#) un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **azioni > Rimuovi**.

Endpoint del bilanciamento del carico

[Certificati endpoint per il bilanciamento del carico](#) Proteggere le connessioni tra i client S3 e il servizio di bilanciamento del carico StorageGRID su nodi gateway e nodi amministrativi.

La tabella degli endpoint del bilanciamento del carico contiene una riga per ogni endpoint del bilanciamento del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 globale o un certificato endpoint del bilanciamento del carico personalizzato. Viene visualizzata anche la data di scadenza di ciascun certificato.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

È possibile:

- ["Visualizzare un endpoint di bilanciamento del carico"](#), inclusi i dettagli del certificato.
- ["Specificare un certificato endpoint per il bilanciamento del carico per FabricPool."](#)
- ["Utilizzare il certificato API S3 globale"](#) invece di generare un nuovo certificato endpoint per il bilanciamento del carico.

Tenant

I locatari possono utilizzare [certificati del server di federazione delle identità](#) o [certificati endpoint del servizio di piattaforma](#) assicurare le loro connessioni con StorageGRID.

La tabella tenant ha una riga per ciascun tenant e indica se ciascun tenant dispone dell'autorizzazione per utilizzare la propria origine di identità o i propri servizi di piattaforma.

È possibile:

- ["Selezionare il nome di un tenant per accedere al tenant manager"](#)
- ["Selezionare un nome tenant per visualizzare i dettagli della federazione delle identità del tenant"](#)
- ["Selezionare un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"](#)
- ["Specificare un certificato endpoint del servizio di piattaforma durante la creazione dell'endpoint"](#)

Altro

StorageGRID utilizza altri certificati di sicurezza per scopi specifici. Questi certificati sono elencati in base al nome funzionale. Altri certificati di sicurezza includono:

- [Certificati Cloud Storage Pool](#)
- [Certificati di notifica degli avvisi via email](#)
- [Certificati server syslog esterni](#)
- [Certificati di connessione Grid Federation](#)
- [Certificati di federazione delle identità](#)
- [Certificati KMS \(Key Management Server\)](#)
- [Certificati Single Sign-on](#)

Le informazioni indicano il tipo di certificato utilizzato da una funzione e le relative date di scadenza del certificato server e client, a seconda dei casi. Selezionando il nome di una funzione si apre una scheda del browser in cui è possibile visualizzare e modificare i dettagli del certificato.



È possibile visualizzare e accedere alle informazioni relative ad altri certificati solo se si dispone di ["autorizzazione appropriata"](#).

È possibile:

- ["Specificare un certificato Cloud Storage Pool per S3, C2S S3 o Azure"](#)
- ["Specificare un certificato per le notifiche e-mail di avviso"](#)
- ["Utilizzare un certificato per un server syslog esterno"](#)
- ["Ruotare i certificati di connessione Grid Federation"](#)
- ["Visualizzare e modificare un certificato di federazione delle identità"](#)
- ["Caricare i certificati del server e del client del server di gestione delle chiavi \(KMS\)"](#)
- ["Specificare manualmente un certificato SSO per un trust della parte che si basa"](#)

Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti alle istruzioni di implementazione.

Certificato dell'interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management. È possibile utilizzare il certificato predefinito creato durante l'installazione o caricare un certificato personalizzato.	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 storage e agli endpoint del bilanciamento del carico (opzionale).	Configurazione > Sicurezza > Certificati , seleziona la scheda Globale , quindi seleziona Certificato API S3	"Configurare i certificati API S3"

Certificato Grid CA

Consultare la [Descrizione del certificato Grid CA predefinito](#).

Certificato del client di amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Client	Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni.	Configurazione > Sicurezza > Certificati e quindi selezionare la scheda Client	"Configurare i certificati client"

Certificato endpoint per il bilanciamento del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i client S3 e il servizio di bilanciamento del carico StorageGRID sui nodi gateway e i nodi amministrativi. È possibile caricare o generare un certificato di bilanciamento del carico quando si configura un endpoint di bilanciamento del carico. Le applicazioni client utilizzano il certificato di bilanciamento del carico durante la connessione a StorageGRID per salvare e recuperare i dati degli oggetti. È inoltre possibile utilizzare una versione personalizzata del certificato globale Certificato API S3 per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciamento del carico, non è necessario caricare o generare un certificato separato per ciascun endpoint del bilanciamento del carico. Nota: il certificato utilizzato per l'autenticazione del bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.	Configurazione > Rete > Endpoint del bilanciatore del carico	• "Configurare gli endpoint del bilanciamento del carico" • "Creare un endpoint di bilanciamento del carico per FabricPool"

Certificato endpoint Cloud Storage Pool

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un StorageGRID Cloud Storage Pool a una posizione di archiviazione esterna, come S3 Glacier o Microsoft Azure Blob Storage. È necessario un certificato diverso per ogni tipo di cloud provider.	ILM > Storage Pools	"Creare un pool di storage cloud"

Certificato di notifica degli avvisi via email

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi. • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione.	Avvisi > Configurazione e-mail	"Imposta le notifiche via email per gli avvisi"

Certificato server syslog esterno

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione TLS o RELP/TLS tra un server syslog esterno che registra gli eventi in StorageGRID. Nota: non è richiesto un certificato server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	Configurazione > Monitoraggio > Server di audit e syslog	"Utilizzare un server syslog esterno"

certificato di connessione Grid Federation

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra il sistema StorageGRID corrente e un'altra griglia in una connessione a federazione di griglie.	Configurazione > Sistema > Federazione di griglia	• "Creare connessioni di federazione di griglie" • "Ruotare i certificati di connessione"

Certificato di federazione delle identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, ad esempio Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente ai gruppi di amministrazione e agli utenti di essere gestiti da un sistema esterno.	Configurazione > Controllo accessi > Federazione identità	"USA la federazione delle identità"

Certificato del Key Management Server (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	Configurazione > Sicurezza > Server di gestione delle chiavi	" Aggiunta del server di gestione delle chiavi (KMS) "

Certificato endpoint dei servizi di piattaforma

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di storage S3.	Tenant Manager > STORAGE (S3) > endpoint dei servizi della piattaforma	" Creare endpoint di servizi di piattaforma " " Modifica dell'endpoint dei servizi della piattaforma "

Certificato SSO (Single Sign-on)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come ad FS (Active Directory Federation Services) e StorageGRID, utilizzati per le richieste SSO (Single Sign-on).	Configurazione > Controllo accessi > Single sign-on	" Configurare il single sign-on "

Esempi di certificati

Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

1. È possibile configurare un endpoint di bilanciamento del carico e caricare o generare un certificato server in StorageGRID.
2. Si configura una connessione client S3 all'endpoint del bilanciamento del carico e si carica lo stesso certificato sul client.
3. Quando il client desidera salvare o recuperare i dati, si connette all'endpoint del bilanciamento del carico utilizzando HTTPS.
4. StorageGRID risponde con il certificato del server, che contiene una chiave pubblica, e con una firma basata sulla chiave privata.

5. Il client confronta 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 KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

Tipi di certificati server supportati in StorageGRID

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (algoritmo di firma digitale a curva ellittica).



Il tipo di crittografia per il criterio di protezione deve corrispondere al tipo di certificato del server. Ad esempio, le crittografie RSA richiedono certificati RSA e le crittografie ECDSA richiedono certificati ECDSA. Vedere ["Gestire i certificati di sicurezza"](#). Se si configura un criterio di protezione personalizzato non compatibile con il certificato del server, è possibile ["ripristinare temporaneamente il criterio di protezione predefinito"](#).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere ["Sicurezza per S3 client"](#).

Configura i certificati dell'interfaccia di gestione in StorageGRID

È possibile sostituire il certificato dell'interfaccia di gestione predefinita con un singolo certificato personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza. È inoltre possibile ripristinare il certificato dell'interfaccia di gestione predefinita o generarne uno nuovo.

A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato dell'interfaccia di gestione personalizzata comune e dalla chiave privata corrispondente.

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione principale (CA)

utilizzata, gli utenti potrebbero dover installare il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e a Tenant Manager.



Per garantire che le operazioni non vengano interrotte da un certificato 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 invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Voi [ripristinare da un certificato dell'interfaccia di gestione personalizzata al certificato server predefinito](#).

Aggiungere un certificato di interfaccia di gestione personalizzata

Per aggiungere un certificato di interfaccia di gestione personalizzato, è possibile fornire un certificato personalizzato o generarne uno utilizzando Grid Manager.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

- a. Selezionare **carica certificato**.
- b. Caricare i file dei certificati del server richiesti:
 - **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
 - **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere di almeno 2048 bit.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
- c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
 - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.
- d. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

Generare un certificato

Generare i file dei certificati del server.



La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato dell'interfaccia di gestione personalizzata firmato da un'autorità di certificazione esterna.

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.

Campo	Descrizione
IP	Uno o più indirizzi IP da includere nel certificato.
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Dopo aver aggiunto un certificato dell'interfaccia di gestione personalizzata, la pagina del certificato dell'interfaccia di gestione visualizza informazioni dettagliate sul certificato per i certificati in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

Ripristinare il certificato dell'interfaccia di gestione predefinita

È possibile ripristinare l'utilizzo del certificato dell'interfaccia di gestione predefinita per Grid Manager e Tenant Manager Connections.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato predefinito dell'interfaccia di gestione viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione

Se è richiesta una convalida rigorosa del nome host, è possibile utilizzare uno script per generare il certificato dell'interfaccia di gestione.

Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Si dispone del `Passwords.txt` file.

A proposito di questa attività

La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato firmato da un'autorità di certificazione esterna.

Fasi

1. Ottenere il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati 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 Admin. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly `*` per rappresentare `admin1.ui.storagegrid.example.com` e `admin2.ui.storagegrid.example.com`.
- Impostare `--type` su `management` per configurare il certificato dell'interfaccia di gestione, utilizzato da Grid Manager e Tenant Manager.

- Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare l' `--days` argomento per sovrascrivere il periodo di validità predefinito.



Il periodo di validità di un certificato inizia quando `make-certificate` viene eseguito. È necessario assicurarsi che il client di gestione sia sincronizzato con la stessa origine temporale di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type  
management --days 720
```

L'output risultante contiene il certificato pubblico necessario al client API di gestione.

4. Selezionare e copiare il certificato.

Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`

6. Verificare che il certificato sia stato configurato:

- a. Accedere a Grid Manager.
- b. Selezionare **Configurazione > Sicurezza > Certificati**
- c. Nella scheda **Global**, selezionare **Management interface certificate**.

7. Configurare il client di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

Scaricare o copiare il certificato dell'interfaccia di gestione

È possibile salvare o copiare il contenuto del certificato dell'interfaccia di gestione per utilizzarlo altrove.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scaricare il file di certificato o il bundle CA

Scaricare il certificato o il file bundle CA .pem. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato o Scarica bundle CA**.

Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM or Copy CA bundle PEM**.

Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Configura i certificati API S3 in StorageGRID

È possibile sostituire o ripristinare il certificato del server utilizzato per le connessioni client S3 ai nodi di storage o agli endpoint di bilanciamento del carico. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Configurazione dei certificati API S3 e Swift"](#).

A proposito di questa attività

Per impostazione predefinita, ogni nodo di storage viene emesso un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Per tutti i nodi di storage viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare il nome host durante la connessione all'endpoint di storage. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di storage nella griglia.

Dopo aver completato la configurazione sul server, potrebbe essere necessario installare anche il certificato CA Grid nel client API S3 da utilizzare per accedere al sistema, a seconda dell'autorità di certificazione

principale (CA) in uso.



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.

Aggiungere un certificato API S3 personalizzato

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate:** Il file di certificato del server personalizzato (con codifica PEM).
- **Chiave privata del certificato:** Il file della chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere di almeno 2048 bit.

- **Bundle CA:** Un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione di emissione intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Selezionare i dettagli del certificato per visualizzare i metadati e PEM per ogni certificato API S3 personalizzato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Salva**.

Il certificato server personalizzato viene utilizzato per le nuove connessioni client S3 successive.

Generare un certificato

Generare i file dei certificati del server.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e PEM per il certificato API S3 personalizzato generato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.

Il certificato server personalizzato viene utilizzato per le nuove connessioni client S3 successive.

5. Selezionare una scheda per visualizzare i metadati per il certificato del server StorageGRID predefinito, un certificato CA firmato caricato o un certificato personalizzato generato.



Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 personalizzato, la pagina del certificato API S3 visualizza informazioni dettagliate sul certificato API S3 personalizzato in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

Ripristinare il certificato API S3 predefinito

È possibile ripristinare l'utilizzo del 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 di bilanciamento del carico.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare **Usa certificato predefinito**.

Quando si ripristina la versione predefinita del certificato API S3 globale, i file di certificato del server personalizzato configurati vengono eliminati e non possono essere recuperati dal sistema. Il certificato API S3 predefinito verrà utilizzato per le successive nuove connessioni client S3 ai nodi storage.

4. Selezionare **OK** per confermare l'avviso e ripristinare il certificato API S3 predefinito.

Se si dispone dell'autorizzazione di accesso root e il certificato API S3 personalizzato è stato utilizzato per le connessioni endpoint del bilanciamento del carico, viene visualizzato un elenco degli endpoint del bilanciamento del carico che non saranno più accessibili utilizzando il certificato API S3 predefinito.

Accedere a ["Configurare gli endpoint del bilanciamento del carico"](#) per modificare o rimuovere gli endpoint interessati.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Scaricare o copiare il certificato API S3

È possibile salvare o copiare il contenuto del certificato API S3 per utilizzarlo altrove.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati**.
2. Nella scheda **Globale**, selezionare **S3 certificato API**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scaricare il file di certificato o il bundle CA

Scaricare il certificato o il file bundle CA .pem. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato o Scarica bundle CA**.

Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

- ["UTILIZZARE L'API REST S3"](#)
- ["Configurare i nomi di dominio degli endpoint S3"](#)

Copia il certificato CA della griglia StorageGRID

StorageGRID utilizza un'autorità di certificazione interna (CA) per proteggere il traffico interno. Questo certificato non cambia se si caricano i propri certificati.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **CA griglia**.

2. Nella sezione **Certificate PEM**, scaricare o copiare il certificato.

Scaricare il file del certificato

Scaricare il file del certificato .pem.

- Selezionare **Scarica certificato**.
- Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copiare il testo del certificato per incollarlo altrove.

- Selezionare **Copy certificate PEM** (Copia certificato PEM).
- Incollare il certificato copiato in un editor di testo.
- Salvare il file di testo con l'estensione .pem.

Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disattivazione della convalida rigorosa del nome host, ad esempio i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciamento del carico.

Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

Quando si crea un endpoint di bilanciamento del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere ["Configurare StorageGRID per FabricPool"](#).

Fasi

- Facoltativamente, configurare un gruppo ad alta disponibilità (ha) da utilizzare per FabricPool.
- Creare un endpoint di bilanciamento del carico S3 da utilizzare per FabricPool.

Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA opzionale.

3. Collega StorageGRID come Tier cloud in ONTAP.

Specificare la porta endpoint del bilanciamento del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.



Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

Configura i certificati client in StorageGRID

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, fornendo un modo sicuro per i tool esterni di monitorare StorageGRID.

Se si desidera accedere a StorageGRID utilizzando uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client utilizzando Grid Manager e copiare le informazioni del certificato nello strumento esterno.

Vedere ["Gestire i certificati di sicurezza"](#) e ["Configurare certificati server personalizzati"](#).



Per garantire che le operazioni non vengano interrotte da un certificato 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 su nodi di appliance appositamente configurati, vedere le informazioni specifiche su ["Caricamento di un certificato del client KMS"](#).

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Per configurare un certificato client:
 - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
 - Se è stato configurato il certificato dell'interfaccia di gestione StorageGRID, si dispone della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
 - Per caricare il certificato, la chiave privata del certificato è disponibile sul computer locale.
 - La chiave privata deve essere stata salvata o registrata al momento della creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
 - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
 - Per caricare il proprio certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul computer locale.

Aggiungere certificati client

Per aggiungere il certificato client, attenersi a una delle seguenti procedure:

- [Certificato dell'interfaccia di gestione già configurato](#)
- [CERTIFICATO client emesso DALLA CA](#)
- [Certificato generato da Grid Manager](#)

Certificato dell'interfaccia di gestione già configurato

Utilizzare questa procedura per aggiungere un certificato client se un certificato dell'interfaccia di gestione è già configurato utilizzando una CA, un certificato client e una chiave privata forniti dal cliente.

Fasi

1. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
 - a. Selezionare **carica certificato**.
 - b. Selezionare **Sfoglia** e selezionare il file di certificato dell'interfaccia di gestione (.pem).
 - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
 - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
 - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

7. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

CERTIFICATO client emesso DALLA CA

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza un certificato client emesso dalla CA e una chiave privata.

Fasi

1. Eseguire i passaggi da a ["configurare un certificato dell'interfaccia di gestione"](#).
2. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per il certificato.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).

6. Selezionare **continua**.
7. Per il passo **Allega certificati**, caricare i file di certificato client, chiave privata e bundle CA:
 - a. Selezionare **carica certificato**.
 - b. Selezionare **Sfoglia** e selezionare 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 **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
 - c. Selezionare **Crea** per salvare il certificato in Grid Manager.

I nuovi certificati vengono visualizzati nella scheda Client.

8. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

Certificato generato da Grid Manager

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

Fasi

1. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, selezionare **genera certificato**.
7. Specificare le informazioni del certificato:
 - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
 - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
 - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

8. Selezionare **generate**.
9. selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e la posizione di download.

10. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e quindi seleziona la scheda **Globale**.
12. Selezionare **certificato interfaccia di gestione**.
13. Selezionare **Usa certificato personalizzato**.
14. Caricare i file `certificate.pem` e `private_key.pem` dal [dettagli del certificato del client](#) passaggio. Non è necessario caricare il bundle CA.
 - a. Selezionare **carica certificato**, quindi selezionare **continua**.
 - b. Caricare ciascun file di certificato (`.pem`).
 - c. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella pagina Management Interface certificate (certificato interfaccia di gestione).

15. [Configurare uno strumento di monitoraggio esterno](#), Come Grafana.

Configura uno strumento di monitoraggio esterno

Fasi

1. Configurare le seguenti impostazioni sullo strumento di monitoraggio esterno, ad esempio Grafana.
 - a. **Nome**: Immettere un nome per la connessione.

StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per verificare la connessione.

- b. **URL**: Immettere il nome di dominio o l'indirizzo IP per il nodo di amministrazione. Specificare HTTPS e la porta 9091.

Ad esempio: `https://admin-node.example.com:9091`

c. Abilitare **TLS Client Auth** e con **CA Certate**.

d. In TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL), copiare e incollare: +

- Il certificato CA dell'interfaccia di gestione a **CA Cert**
- Il certificato del client a **Client Cert**
- La chiave privata per **chiave client**

e. **ServerName**: Immettere il nome di dominio del nodo di amministrazione.

Il nome server deve corrispondere al nome di dominio così come appare nel certificato dell'interfaccia di gestione.

2. Salvare e verificare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo tool di monitoraggio esterno.

Per informazioni sulle metriche, vedere ["Istruzioni per il monitoraggio di StorageGRID"](#).

Modificare i certificati client

È possibile modificare un certificato client amministratore per modificarne il nome, abilitare o disabilitare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Modifica**, quindi selezionare **Modifica nome e permesso**

4. Immettere un nome per il certificato.

5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).

6. Selezionare **continua** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Allegare un nuovo certificato client

È possibile caricare un nuovo certificato una volta scaduto il certificato corrente.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.

Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Edit** (Modifica), quindi un'opzione di modifica.

Carica certificato

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **carica certificato**, quindi selezionare **continua**.
- b. Caricare il nome del certificato client (.pem).

Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- c. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il certificato aggiornato viene visualizzato nella scheda Client.

Generare un certificato

Generare il testo del certificato da incollare altrove.

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:

- **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
- **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
- **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.



Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

- c. Selezionare **generate**.
- d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.



Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del

certificato e incollarlo altrove.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

Specificare il nome del file della chiave privata e la posizione di download.

e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scaricare o copiare i certificati client

È possibile scaricare o copiare un certificato client da utilizzare altrove.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera copiare o scaricare.
3. Scaricare o copiare il certificato.

Scaricare il file del certificato

Scaricare il file del certificato `.pem`.

- a. Selezionare **Scarica certificato**.
- b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Copia certificato

Copiare il testo del certificato per incollarlo altrove.

- a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
- b. Incollare il certificato copiato in un editor di testo.
- c. Salvare il file di testo con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

Rimuovere i certificati client

Se non è più necessario un certificato client amministratore, è possibile rimuoverlo.

Fasi

1. Selezionare **Configurazione > Sicurezza > Certificati** e quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera rimuovere.
3. Selezionare **Delete** (Elimina), quindi confermare.



Per rimuovere fino a 10 certificati, selezionare ciascun certificato da rimuovere nella scheda Client, quindi selezionare **azioni > Elimina**.

Dopo la rimozione di un certificato, i client che hanno utilizzato il certificato devono specificare un nuovo certificato client per accedere al database StorageGRID Prometheus.

Configurare le impostazioni di sicurezza

Gestisci la policy TLS e SSH in StorageGRID

I criteri TLS e SSH determinano i protocolli e le crittografia utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

Il criterio di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderno (predefinito), a meno che il sistema non debba essere conforme ai criteri comuni o non sia necessario utilizzare altre crittografia.



Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le crittografia di questi criteri.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

Selezionare una policy di sicurezza

Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.

La scheda **TLS and SSH policies** (Criteri TLS e SSH) mostra i criteri disponibili. Il criterio attualmente attivo è contrassegnato da un segno di spunta verde sul riquadro del criterio.



2. Consulta le schede per conoscere le policy disponibili.

Compatibilità moderna (impostazione predefinita)

Utilizza il criterio predefinito se hai bisogno di una crittografia avanzata e non hai requisiti particolari. Questa policy è compatibile con la maggior parte dei client TLS e SSH.

Compatibilità con le versioni precedenti

Utilizzare il criterio di compatibilità Legacy se sono necessarie 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

Se hai bisogno della certificazione Common Criteria, utilizza la politica Common Criteria.

FIPS rigoroso

Utilizza la policy FIPS strict se hai bisogno della certificazione Common Criteria e devi usare il NetApp Cryptographic Security Module (NCSM) 3.1.2 o il modulo NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 per le connessioni client esterne agli endpoint del bilanciatore di carico, a Tenant Manager e a Grid Manager. Usare questa policy potrebbe ridurre le prestazioni.

NCSM 3.1.2 e il modulo NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1 vengono utilizzati nelle seguenti operazioni:

- NCSM
 - Connessioni TLS tra i seguenti servizi: ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw e cache-svc
 - Connessioni TLS tra i client e il servizio nginx-gw (endpoint del bilanciatore del carico)
 - Connessioni TLS tra i client e il servizio LDR
 - Crittografia del contenuto dell'oggetto per SSE-S3, SSE-C e impostazione di crittografia dell'oggetto archiviato
 - connessioni SSH

Per ulteriori informazioni, consulta il Programma di convalida degli algoritmi crittografici del NIST "[Certificato #A7816](#)".

- Modulo API di crittografia del kernel NetApp StorageGRID

Il modulo API NetApp StorageGRID Kernel Crypto è presente solo sulle piattaforme VM e appliance StorageGRID .

- Raccolta di entropia
- Crittografia dei nodi

Nota: Questo modulo non è stato sottoposto a certificazione.

Per ulteriori informazioni, consulta il Programma di convalida degli algoritmi crittografici del NIST "[Certificato di entropia n. E223](#)".

Nota: Dopo aver selezionato questa policy, "[eseguire un riavvio progressivo](#)" affinché tutti i nodi attivino l'NCSM. Utilizzare **Manutenzione > Riavvio progressivo** per avviare e monitorare i riavvii.

Personalizzato

Creare un criterio personalizzato se è necessario applicare le proprie crittografia.

Facoltativamente, se il tuo StorageGRID ha requisiti di crittografia FIPS 140, abilita la funzionalità della modalità FIPS per utilizzare NCSM 3.1.2 e il modulo NetApp StorageGRID Kernel Crypto API 6.12.63-1+ntap1:

- a. Imposta il `fipsMode` parametro a `true`.
- b. Quando richiesto, "eseguire un riavvio progressivo" affinché tutti i nodi attivino i moduli di crittografia. Utilizzare **Manutenzione > Riavvio progressivo** per avviare e monitorare i riavvii.
- c. Selezionare **Supporto > Diagnostica** per visualizzare le versioni attive del modulo FIPS.

3. Per visualizzare i dettagli relativi a crittografia, protocolli e algoritmi di ogni policy, selezionare **Visualizza dettagli**.
4. Per modificare la policy corrente, selezionare **Usa policy**.

Un segno di spunta verde viene visualizzato accanto a **policy corrente** nel riquadro del criterio.

Creare una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare le proprie crittografia.

Fasi

1. Dal riquadro del criterio più simile al criterio personalizzato che si desidera creare, selezionare **Visualizza dettagli**.
2. Selezionare **Copia negli Appunti**, quindi selezionare **Annulla**.



3. Dal riquadro **Custom policy**, selezionare **Configure and use** (Configura e utilizza).
4. Incollare il JSON copiato e apportare le modifiche necessarie.
5. Selezionare **Usa policy**.

Un segno di spunta verde viene visualizzato accanto a **Current policy** (policy corrente) nel riquadro Custom policy (policy personalizzate).

6. Facoltativamente, selezionare **Edit Configuration** (Modifica configurazione) per apportare ulteriori modifiche al nuovo criterio personalizzato.

Ripristinare temporaneamente il criterio di protezione predefinito

Se è stato configurato un criterio di protezione personalizzato, potrebbe non essere possibile accedere a Grid Manager se il criterio TLS configurato non è compatibile con ["certificato server configurato"](#).

È possibile ripristinare temporaneamente i criteri di protezione predefiniti.

Fasi

1. Accedere a un nodo amministratore:
 - a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Eseguire il seguente comando:

```
restore-default-cipher-configurations
```

3. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.
4. Per configurare nuovamente il criterio, procedere come [Selezionare una policy di sicurezza](#) segue.

Configurare la sicurezza di rete e degli oggetti di StorageGRID

È possibile configurare la protezione della rete e degli oggetti per crittografare gli oggetti archiviati, impedire determinate richieste S3 o consentire alle connessioni client ai nodi di archiviazione di utilizzare HTTP invece di HTTPS.

Crittografia degli oggetti memorizzati

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non vengono crittografati, ma è possibile scegliere di crittografare gli oggetti utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si attiva l'impostazione, tutti gli oggetti inseriti di recente vengono crittografati, ma non vengono apportate modifiche agli oggetti memorizzati esistenti. Se si disattiva la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti memorizzati si applica solo agli oggetti S3 che non sono stati crittografati mediante crittografia a livello di bucket o a livello di oggetto.

Per ulteriori informazioni sui metodi di crittografia StorageGRID, vedere ["Esaminare i metodi di crittografia StorageGRID"](#).

Impedire la modifica del client

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione **Impedisci modifica client**, le seguenti richieste vengono rifiutate.

API REST S3

- Richieste DeleteBucket
- Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3

Abilitare HTTP per le connessioni dei nodi di storage

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Utilizzare HTTP per le connessioni al nodo di archiviazione solo se i client S3 devono stabilire 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 (poiché è possibile ["configurare ciascun endpoint del bilanciamento del carico"](#) utilizzare HTTP o HTTPS).

Vedere ["Riepilogo: Indirizzi IP e porte per le connessioni client"](#) per informazioni sulle porte utilizzate dai client S3 durante la connessione ai nodi di archiviazione tramite HTTP o HTTPS.

Selezionare le opzioni

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone dell'autorizzazione di accesso root.

Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **rete e oggetti**.
3. Per la crittografia degli oggetti memorizzati, utilizzare l'impostazione **None** (predefinita) se non si desidera crittografare gli oggetti memorizzati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Se si desidera impedire ai client S3 di eseguire richieste specifiche, selezionare **Impedisci modifica client**.



Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

5. Se si desidera utilizzare connessioni HTTP, selezionare **Enable HTTP for Storage Node Connections** (attiva HTTP per connessioni nodo di storage) se i client si connettono direttamente ai nodi di storage.



Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

6. Selezionare **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia StorageGRID

Le impostazioni di protezione dell'interfaccia consentono di controllare se gli utenti sono disconnessi se sono inattivi per un periodo di tempo superiore a quello specificato e se

una traccia dello stack è inclusa nelle risposte di errore API.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

La pagina **Impostazioni di protezione** include le impostazioni **Timeout inattività browser** e **traccia stack API di gestione**.

Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. L'impostazione predefinita è 15 minuti.

Il timeout di inattività del browser è controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Quando l'autenticazione dell'utente scade, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disattivato o non è stato raggiunto il valore per il timeout del browser. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che SSO (Single Sign-on) sia abilitato per StorageGRID.

Se 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 ["Come funziona SSO"](#) .

Traccia stack API di gestione

Controlla se una traccia di stack viene restituita nelle risposte di errore delle API di Gestione griglia e di Gestione tenant.

Questa opzione è disattivata per impostazione predefinita, ma potrebbe essere necessario attivarla per un ambiente di test. In generale, è necessario lasciare disattivata la traccia dello stack negli ambienti di produzione per evitare di rivelare i dettagli del software interno quando si verificano errori API.

Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
 - a. Espandere la fisarmonica.
 - b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
 - c. Per disattivare questa funzione, deselezionare la casella di controllo.
 - d. Selezionare **Salva**.

La nuova impostazione non influisce sugli utenti che hanno effettuato l'accesso. Per rendere effettiva la nuova impostazione di timeout, gli utenti devono eseguire nuovamente l'accesso o aggiornare il browser.

4. Per modificare l'impostazione per la traccia stack API di gestione:
 - a. Espandere la fisarmonica.
 - b. Selezionare la casella di controllo per restituire una traccia di stack nelle risposte agli errori di API di Gestione griglia e di Gestione tenant.



Lasciare la traccia dello stack disattivata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

- c. Selezionare **Salva**.

Gestisci l'accesso SSH esterno in StorageGRID

Gestisci l'accesso SSH per il traffico in entrata nella griglia bloccando o consentendo l'accesso esterno. La gestione dell'accesso esterno SSH non ha alcun impatto sul traffico tra i nodi della griglia.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

Per migliorare la sicurezza del sistema, l'accesso SSH esterno è bloccato per impostazione predefinita. Se devi eseguire attività che richiedono l'accesso SSH in ingresso, come la risoluzione dei problemi, consenti temporaneamente l'accesso esterno. Una volta completata l'attività, blocca l'accesso esterno.

Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni di sicurezza**.
2. Selezionare la scheda **Blocca SSH**.
3. Utilizzare l'opzione **Blocca accesso SSH in ingresso** per gestire l'accesso SSH esterno:
 - a. Selezionare la casella di controllo per bloccare l'accesso (impostazione predefinita).
 - b. Deseleziona la casella di controllo per consentire l'accesso.



Richiede l'accesso sulla porta 22 tra il laptop di servizio e tutti gli altri nodi della griglia. Una volta completata l'attività di manutenzione, rimuovere l'accesso alla porta 22.

4. Selezionare **Salva**.

Configurare i server di gestione delle chiavi

Scopri i server di gestione delle chiavi in StorageGRID

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 alcuni server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportate, utilizzare ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi di qualsiasi appliance StorageGRID con l'impostazione **crittografia dei nodi** attivata durante l'installazione. L'utilizzo di server di gestione delle chiavi con questi nodi appliance consente di proteggere i dati anche in caso di rimozione di un'appliance dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.

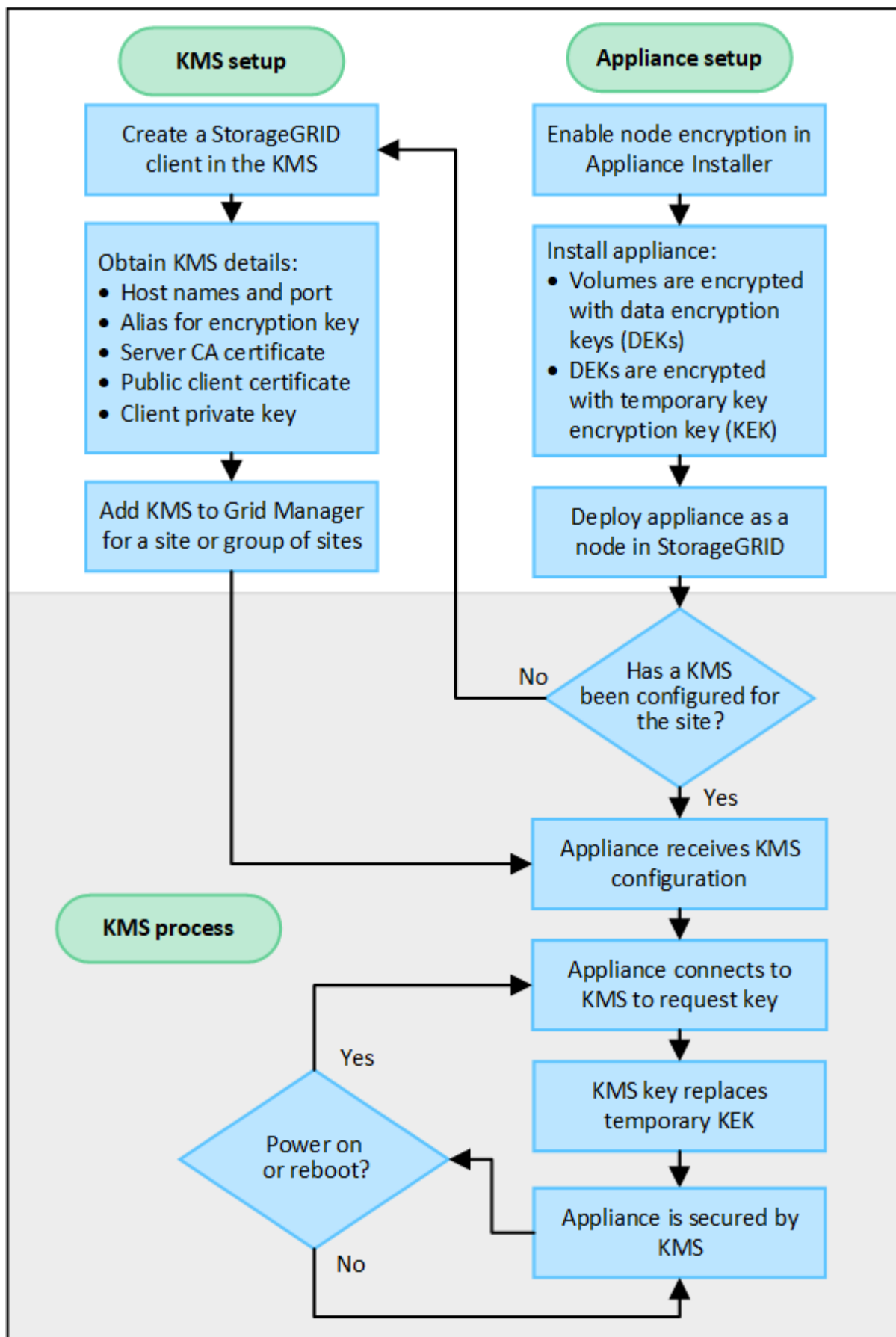


StorageGRID non crea o gestisce le chiavi esterne utilizzate per crittografare e decrittare i nodi dell'appliance. Se si intende utilizzare un server di gestione delle chiavi esterno per proteggere i dati StorageGRID, è necessario comprendere come configurare tale server e come gestire le chiavi di crittografia. L'esecuzione delle attività di gestione chiave non rientra nell'ambito di queste istruzioni. Per assistenza, consultare la documentazione relativa al server di gestione delle chiavi o contattare il supporto tecnico.

StorageGRID configurazione del server e dell'appliance di gestione delle chiavi

Prima di utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi appliance, è necessario completare due attività di configurazione: La configurazione di uno o più server KMS e l'abilitazione della crittografia dei nodi per i nodi appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi viene eseguito automaticamente.

Il diagramma di flusso mostra i passaggi di alto livello per l'utilizzo di un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.



Il diagramma di flusso mostra la configurazione di KMS e dell'appliance in parallelo; tuttavia, è possibile

configurare i server di gestione delle chiavi prima o dopo aver attivato la crittografia dei nodi per i nuovi nodi appliance, in base ai requisiti.

Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi include i seguenti passaggi di alto livello.

Fase	Fare riferimento a.
Accedere al software KMS e aggiungere un client per StorageGRID a ciascun cluster KMS o KMS.	"Configurare StorageGRID come client nel KMS"
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurare StorageGRID come client nel KMS"
Aggiungere il KMS al Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiunta di un server di gestione delle chiavi (KMS)"

Configurare l'apparecchio

La configurazione di un nodo appliance per l'utilizzo di KMS include i seguenti passaggi di alto livello.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID per attivare l'impostazione **crittografia del nodo** dell'appliance.



Non è possibile attivare l'impostazione **Node Encryption** dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non dispongono della crittografia dei nodi abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID. Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dei dati casuale (DEK), come segue:
 - I DEK vengono utilizzati per crittografare i dati su ciascun volume. Queste chiavi vengono generate utilizzando la crittografia del disco Linux Unified Key Setup (LUKS) nel sistema operativo dell'appliance e non possono essere modificate.
 - Ogni singolo DEK viene crittografato mediante una chiave di crittografia della chiave master (KEK). La chiave iniziale KEK è una chiave temporanea che crittografa i DEK fino a quando l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo appliance a StorageGRID.

Per ulteriori informazioni, vedere ["Abilitare la crittografia del nodo"](#).

Processo di crittografia per la gestione delle chiavi (si verifica automaticamente)

La crittografia per la gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance che ha attivato la crittografia dei nodi nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.

- Se un KMS è già stato configurato per il sito, l'appliance riceve la configurazione KMS.
 - Se non è ancora stato configurato un KMS per il sito, i dati dell'appliance continuano a essere crittografati dalla KEK temporanea fino a quando non si configura un KMS per il sito e l'appliance non riceve la configurazione KMS.
2. L'appliance utilizza la configurazione KMS per connettersi al KMS e richiedere una chiave di crittografia.
 3. Il KMS invia una chiave di crittografia all'appliance. La nuova chiave del KMS sostituisce la KEK temporanea e viene ora utilizzata per crittografare e decrittare i DEK per i volumi dell'appliance.



Tutti i dati che esistono prima che il nodo dell'appliance crittografato si connetta al KMS configurato vengono crittografati con una chiave temporanea. Tuttavia, i volumi dell'appliance non devono essere considerati protetti dalla rimozione dal data center fino a quando la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si ricollega al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a una perdita di alimentazione o a un riavvio.

Requisiti e considerazioni relativi al server di gestione delle chiavi StorageGRID

Prima di configurare un KMS (Key Management Server) esterno, è necessario comprendere le considerazioni e i requisiti.

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

["Key Management Interoperability Protocol Specification versione 1.4"](#)

Quali sono le considerazioni sulla rete?

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare attraverso la porta utilizzata per le comunicazioni KMIP (Key Management Interoperability Protocol). La porta KMIP predefinita è 5696.

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia del nodo disponga dell'accesso di rete al cluster KMS o KMS configurato per il sito.

Quali versioni di TLS sono supportate?

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID può supportare il protocollo TLS 1,2 o TLS 1,3 quando stabilisce connessioni KMIP a un cluster KMS o KMS, in base a ciò che il KMS supporta e a quale ["Policy TLS e SSH"](#) 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 appliance sono supportate?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nel grid con l'impostazione **crittografia nodo** attivata. Questa impostazione può essere attivata solo durante la fase di configurazione hardware dell'installazione dell'appliance mediante il

programma di installazione dell'appliance StorageGRID.



Non è possibile attivare la crittografia dei nodi dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia dei nodi abilitata.

È possibile utilizzare il KMS configurato per appliance StorageGRID e nodi appliance.

Non è possibile utilizzare il KMS configurato per i nodi software-based (non-appliance), inclusi i seguenti:

- Nodi implementati come macchine virtuali (VM)
- Nodi implementati all'interno di motori container su host Linux

I nodi implementati su queste altre piattaforme possono utilizzare la crittografia all'esterno di StorageGRID a livello di datastore o disco.

Quando è necessario configurare i server di gestione delle chiavi?

Per una nuova installazione, in genere è necessario configurare uno o più server di gestione delle chiavi in Grid Manager prima di creare tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti siano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo l'installazione dei nodi appliance.

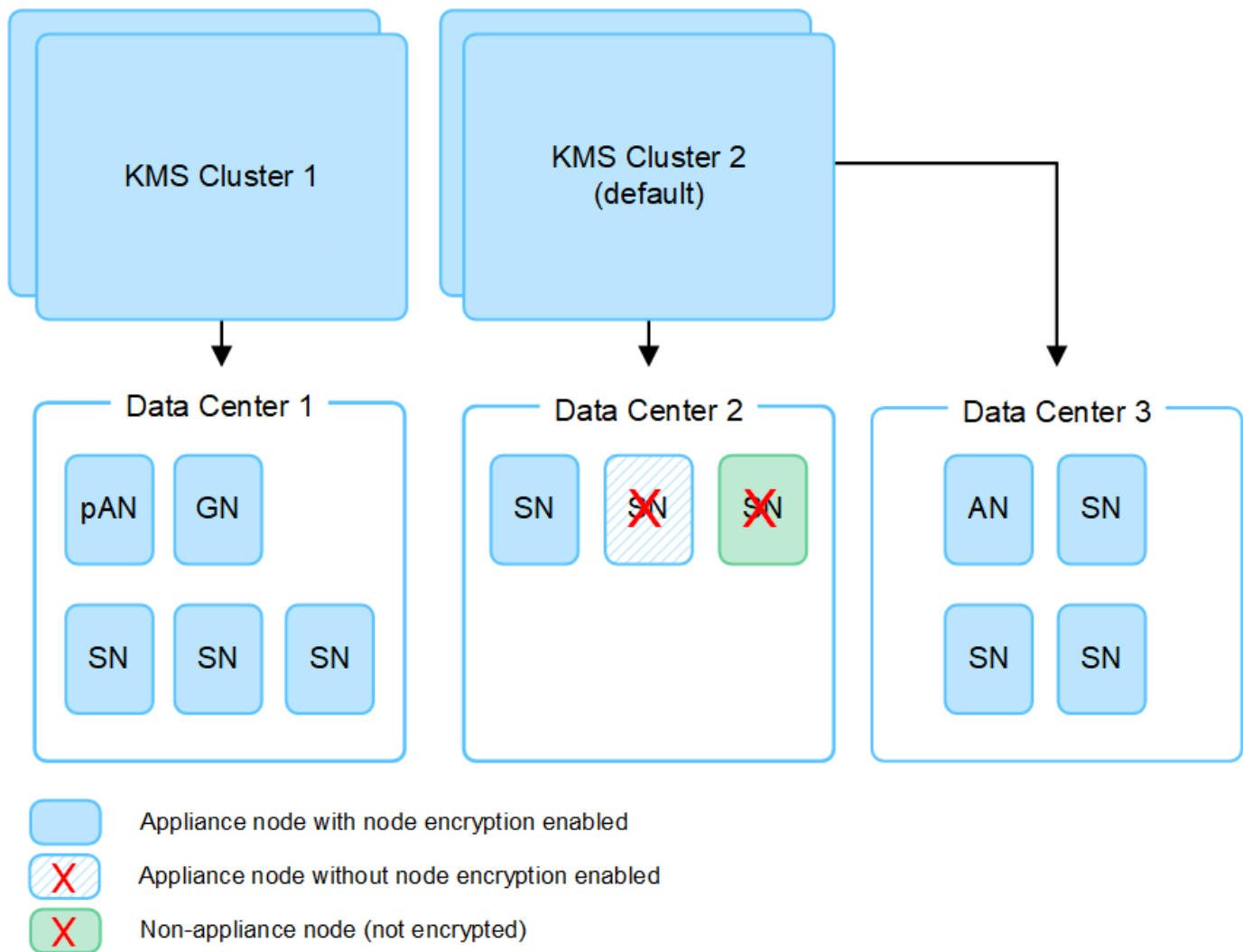
Quanti server di gestione delle chiavi sono necessari?

È possibile configurare uno o più server di gestione delle chiavi esterni per fornire chiavi di crittografia ai nodi dell'appliance nel sistema StorageGRID. Ogni KMS fornisce una singola chiave di crittografia ai nodi dell'appliance StorageGRID in un singolo sito o in un gruppo di siti.

StorageGRID supporta l'utilizzo di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono le impostazioni di configurazione e le chiavi di crittografia. Si consiglia di utilizzare i cluster KMS per la gestione delle chiavi perché migliora le funzionalità di failover di una configurazione ad alta disponibilità.

Si supponga, ad esempio, che il sistema StorageGRID disponga di tre siti per data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi appliance nel data center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi appliance in tutti gli altri siti. Quando si aggiunge il secondo cluster KMS, è possibile configurare un KMS predefinito per Data Center 2 e Data Center 3.

Tenere presente che non è possibile utilizzare un KMS per i nodi non appliance o per i nodi appliance che non hanno attivato l'impostazione **Node Encryption** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come Best practice per la sicurezza, è consigliabile utilizzare periodicamente ["ruotare la chiave di crittografia"](#) ogni KMS configurato.

Quando è disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi appliance crittografati nel sito o nei siti associati al KMS. La distribuzione deve avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografato non è in linea quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena verrà riavviato.
- Se la nuova versione della chiave non può essere utilizzata per crittografare i volumi dell'appliance per qualsiasi motivo, viene attivato l'avviso **rotazione chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potrebbe essere necessario contattare il supporto tecnico per ottenere assistenza nella risoluzione di questo avviso.

È possibile riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima decommissionare il nodo Grid per spostare i dati degli oggetti in un altro nodo. Quindi, è possibile utilizzare il programma di installazione dell'appliance StorageGRID per ["Cancellare la configurazione KMS"](#). La

cancellazione della configurazione KMS disattiva l'impostazione **crittografia nodo** e rimuove l'associazione tra il nodo appliance e la configurazione KMS per il sito StorageGRID.



Senza l'accesso alla chiave di crittografia KMS, i dati che rimangono sull'appliance non possono più essere utilizzati e bloccati in modo permanente.

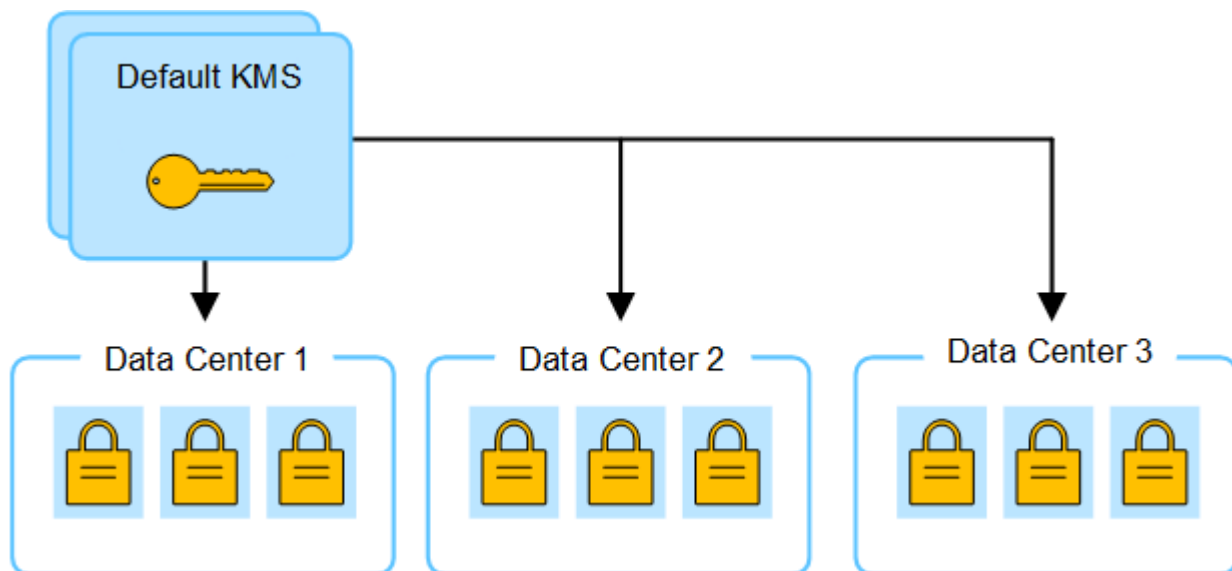
Considerazioni sulla modifica del KMS per un sito StorageGRID

Ciascun server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi appliance di un singolo sito o di un gruppo di siti. Se è necessario modificare il KMS utilizzato per un sito, potrebbe essere necessario copiare la chiave di crittografia da un KMS all'altro.

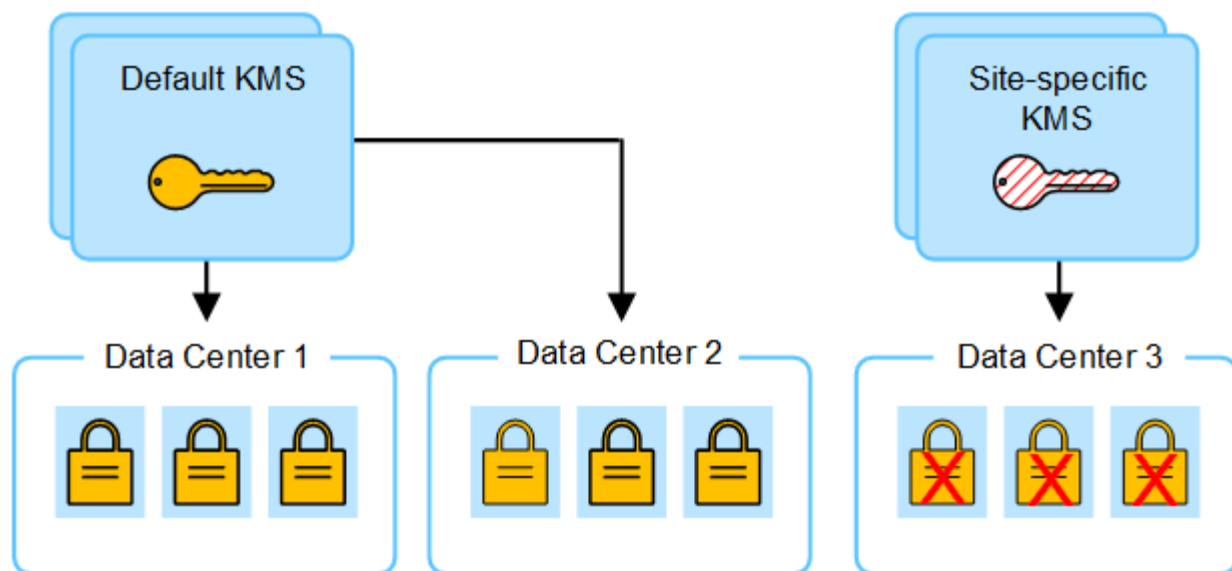
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittare i nodi crittografati dell'appliance nel sito.

Ad esempio:

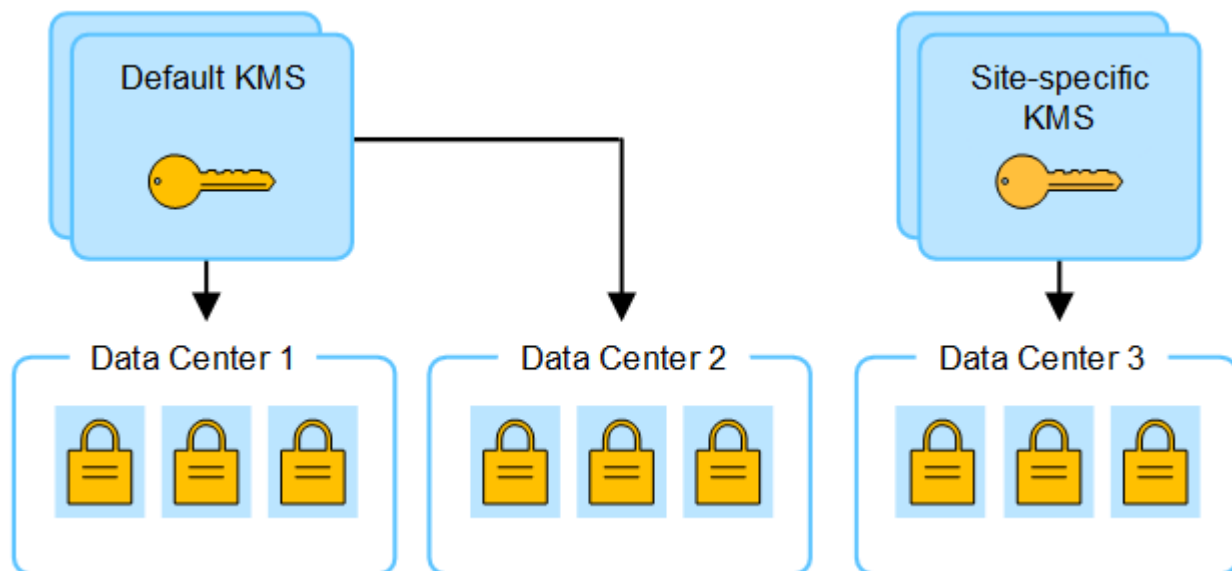
1. Inizialmente, viene configurato un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decrittare tali appliance.



3. Si decide di aggiungere un KMS specifico del sito per un sito (data center 3 nella figura). Tuttavia, poiché i nodi dell'appliance sono già crittografati, si verifica un errore di convalida quando si tenta di salvare la configurazione per il KMS specifico del sito. L'errore si verifica perché il KMS specifico del sito non dispone della chiave corretta per decrittare i nodi in quel sito.



4. Per risolvere il problema, copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Tecnicamente, si copia la chiave originale in una nuova chiave con lo stesso alias. La chiave originale diventa una versione precedente della nuova chiave). Il KMS specifico del sito dispone ora della chiave corretta per decrittografare i nodi appliance nel data center 3, in modo che possa essere salvato in StorageGRID.



Casi di utilizzo per la modifica del KMS utilizzato per un sito

La tabella riassume i passaggi necessari per i casi più comuni di modifica del KMS per un sito.

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
Si dispone di una o più voci KMS specifiche del sito e si desidera utilizzarne una come KMS predefinito.	Modificare il KMS specifico del sito. Nel campo Gestisci chiavi per, selezionare Siti non gestiti da un altro KMS (KMS predefinito). Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applica a tutti i siti che non dispongono di un KMS dedicato. "Modifica di un server di gestione delle chiavi (KMS)"
Si dispone di un KMS predefinito e si aggiunge un nuovo sito in un'espansione. Non si desidera utilizzare il KMS predefinito per il nuovo sito.	1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati con il KMS predefinito, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS. 2. Utilizzando Grid Manager, aggiungere il nuovo KMS e selezionare il sito. "Aggiunta di un server di gestione delle chiavi (KMS)"
Si desidera che il KMS di un sito utilizzi un server diverso.	1. Se i nodi dell'appliance nel sito sono già stati crittografati dal KMS esistente, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS esistente al nuovo KMS. 2. Utilizzando Grid Manager, modificare la configurazione KMS esistente e inserire il nuovo nome host o indirizzo IP. "Aggiunta di un server di gestione delle chiavi (KMS)"

Configurare StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ogni server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere KMS a StorageGRID.



Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportate, utilizzare ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Fasi

1. Dal software KMS, creare un client StorageGRID per ogni cluster KMS o KMS che si intende utilizzare.

Ogni KMS gestisce una singola chiave di crittografia per i nodi delle appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. creare una chiave utilizzando uno dei due metodi seguenti:
 - Utilizzare la pagina di gestione delle chiavi del prodotto KMS. Creare una chiave di crittografia AES per ogni cluster KMS o KMS.

La chiave di crittografia deve essere 2,048 bit o superiore e deve essere esportabile.

- Chiedere a StorageGRID di creare la chiave. Verrà richiesto quando si esegue il test e si salva dopo ["caricamento dei certificati client"](#).

3. Registrare le seguenti informazioni per ciascun cluster KMS o KMS.

Queste informazioni sono necessarie quando si aggiunge il KMS a StorageGRID:

- Nome host o indirizzo IP per ciascun server.
- Porta KMIP utilizzata dal KMS.
- Alias chiave per la chiave di crittografia nel KMS.

4. Per ogni cluster KMS o KMS, ottenere un certificato server firmato da un'autorità di certificazione (CA) o un bundle di certificati che contenga ciascuno dei file di certificato CA con codifica PEM, concatenati nell'ordine della catena di certificati.

Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

- Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.
- Il campo Subject alternative Name (SAN) in ciascun certificato del server deve includere il nome di dominio completo (FQDN) o l'indirizzo IP a cui StorageGRID si connetterà.



Quando si configura il KMS in StorageGRID, è necessario immettere gli stessi FQDN o indirizzi IP nel campo **Nome host**.

- Il certificato del server deve corrispondere al certificato utilizzato dall'interfaccia KMIP del KMS, che in genere utilizza la porta 5696.

5. Ottenere il certificato del client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato del client.

Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Aggiungi un server di gestione delle chiavi in StorageGRID

Utilizzare la procedura guidata del server di gestione delle chiavi StorageGRID per aggiungere ogni cluster KMS o KMS.

Prima di iniziare

- È stata esaminata la ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#).
- Si dispone di ["StorageGRID configurato come client nel KMS"](#), e si dispone delle informazioni necessarie per ogni cluster KMS o KMS.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

Se possibile, configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutte le appliance crittografate con nodo nella griglia verranno crittografate con il KMS predefinito. Se si desidera creare un KMS specifico del sito in un secondo momento, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Per ulteriori informazioni, vedere ["Considerazioni per la modifica del KMS per un sito"](#).

Fase 1: Dettagli DI KMS

Nella fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono forniti dettagli sul cluster KMS o KMS.

Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) con la scheda Configuration details (Dettagli di configurazione) selezionata.

2. Selezionare **Crea**.

Viene visualizzata la fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurati in tale KMS.

Campo	Descrizione
Nome KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. Nota: Se non è stata creata una chiave utilizzando il prodotto KMS, verrà richiesto di fare in modo che StorageGRID crei la chiave.
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è necessario configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. • Selezionare un sito se il KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Selezionare Siti non gestiti da un altro KMS (KMS predefinito) per configurare un KMS predefinito che si applicherà a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. Nota: Quando si salva la configurazione KMS, si verifica Un errore di convalida se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non si fornisce la versione corrente della chiave di crittografia originale al nuovo KMS.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.

Campo	Descrizione
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. Nota: il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

- Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
- Selezionare **continua**.

Fase 2: Caricare il certificato del server

Nella fase 2 (carica certificato server) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), viene caricato il certificato del server (o bundle di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Fasi

- Dal **passaggio 2 (carica certificato server)**, individuare la posizione del certificato server o del bundle di certificati salvato.
- Caricare il file del certificato.

Vengono visualizzati i metadati del certificato del server.



Se hai caricato un bundle di certificati, i metadati di ciascun certificato vengono visualizzati nella relativa scheda.

- Selezionare **continua**.

passaggio 3: Caricamento dei certificati client

Nella fase 3 (carica certificati client) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono caricati il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Fasi

- Dal **passaggio 3 (carica certificati client)**, individuare la posizione del certificato client.
- Caricare il file di certificato del client.

Vengono visualizzati i metadati del certificato client.

- Individuare la posizione della chiave privata per il certificato client.
- Caricare il file della chiave privata.
- Selezionare **Test e salvare**.

Se una chiave non esiste, viene richiesto di crearne una da StorageGRID.

Vengono verificate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata nel KMS, il nuovo server di gestione delle chiavi

viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.



Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Server gestione chiavi viene visualizzato come Sconosciuto. Per ottenere lo stato effettivo di ciascun certificato, StorageGRID potrebbe impiegare fino a 30 minuti. È necessario aggiornare il browser Web per visualizzare lo stato corrente.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test and Save** (verifica e salva), rivedere i dettagli del messaggio e selezionare **OK**.

Ad esempio, se un test di connessione non riesce, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

7. Se si desidera salvare la configurazione corrente senza verificare la connessione esterna, selezionare **Force Save** (forza salvataggio).



Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

8. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

La configurazione KMS viene salvata ma la connessione al KMS non viene verificata.

Gestire un key management server in StorageGRID

La gestione di un server di gestione delle chiavi (KMS) comporta la visualizzazione o la modifica dei dettagli, la gestione dei certificati, la visualizzazione dei nodi crittografati e la rimozione di un KMS quando non è più necessario.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazione di accesso richiesta"](#).

Visualizza i dettagli di KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, inclusi i dettagli delle chiavi e lo stato corrente dei certificati server e client.

Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina del server di gestione delle chiavi con le seguenti informazioni:

- La scheda Dettagli configurazione elenca tutti i server di gestione delle chiavi configurati.
- La scheda nodi crittografati elenca tutti i nodi con la crittografia dei nodi abilitata.

2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, selezionare il nome del KMS. Nella pagina dei dettagli del KMS sono elencate le seguenti informazioni:

Campo	Descrizione
Gestisce le chiavi per	Il sito StorageGRID associato al KMS. Questo campo visualizza il nome di un sito StorageGRID specifico o Siti non gestiti da un altro KMS (KMS predefinito).
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. Se è presente un cluster di due server di gestione delle chiavi, vengono elencati il nome di dominio completo o l'indirizzo IP di entrambi i server. Se in un cluster sono presenti più di due server di gestione delle chiavi, viene elencato il nome di dominio completo o l'indirizzo IP del primo KMS insieme al numero di server di gestione delle chiavi aggiuntivi nel cluster. Ad esempio: 10.10.10.10 and 10.10.10.11 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 della chiave	L'alias della chiave per il client StorageGRID nel KMS.
UID chiave	L'identificatore univoco dell'ultima versione della chiave.	Ultima modifica
La data e l'ora dell'ultima versione della chiave.	Certificato del server	Metadati
I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.	Certificato PEM	Il contenuto del file PEM (privacy Enhanced mail) per il certificato.
Certificato del client	Metadati	I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.

4. tutte le volte che richiesto dalle procedure di sicurezza dell'organizzazione, selezionare **Rotate key**, oppure utilizzare il software KMS, per creare una nuova versione della chiave.

Quando la rotazione della chiave ha esito positivo, i campi UID chiave e ultima modifica vengono aggiornati.

Se si ruota la chiave di crittografia utilizzando il software KMS, ruotarla dall'ultima versione utilizzata della chiave a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.



Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. StorageGRID richiede che tutte le versioni delle chiavi utilizzate in precedenza (così come quelle future) siano accessibili dal KMS con lo stesso alias della chiave. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

Gestire i certificati

Risolvere tempestivamente eventuali problemi relativi ai certificati server o client. Se possibile, sostituire i certificati prima che scadano.



Per mantenere l'accesso ai dati, è necessario risolvere al più presto eventuali problemi di certificato.

Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.
2. Nella tabella, esaminare il valore della scadenza del certificato per ogni KMS.
3. Se la scadenza del certificato per qualsiasi KMS è sconosciuta, attendere fino a 30 minuti, quindi aggiornare il browser Web.
4. Se la colonna scadenza certificato indica che un certificato è scaduto o è prossimo alla scadenza, selezionare il KMS per accedere alla pagina dei dettagli del KMS.
 - a. Selezionare **certificato server** e verificare il valore del campo "scade il".
 - b. Per sostituire il certificato, selezionare **Modifica certificato** per caricare un nuovo certificato.
 - c. Ripetere questi passaggi secondari e selezionare **Client certificate** invece di Server certificate (certificato server).
5. Quando vengono attivati gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS**, annotare la descrizione di ciascun avviso ed eseguire le azioni consigliate.

Per ottenere gli aggiornamenti alla scadenza del certificato, StorageGRID potrebbe richiedere fino a 30 minuti. Aggiornare il browser Web per visualizzare i valori correnti.



Se lo stato del certificato **Server è sconosciuto**, assicurarsi che il KMS consenta di ottenere un certificato server senza richiedere un certificato client.

Visualizzare i nodi crittografati

È possibile visualizzare informazioni sui nodi appliance nel sistema StorageGRID per i quali è stata attivata l'impostazione **crittografia nodo**.

Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi). La scheda Dettagli

configurazione mostra tutti i server di gestione delle chiavi configurati.

2. Nella parte superiore della pagina, selezionare la scheda **nodi crittografati**.

La scheda nodi crittografati elenca i nodi appliance nel sistema StorageGRID con l'impostazione **crittografia nodo** attivata.

3. Esaminare le informazioni contenute nella tabella per ciascun nodo appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo appliance.
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
Nome KMS	Il nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli di configurazione per aggiungere un KMS. "Aggiunta di un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un UID chiave completo, selezionare il testo. Un trattino (--) indica che l'UID della chiave non è noto, probabilmente a causa di un problema di connessione tra il nodo dell'appliance e il KMS.
Stato	Lo stato della connessione tra il KMS e il nodo dell'appliance. Se il nodo è connesso, l'indicatore data e ora viene aggiornato ogni 30 minuti. L'aggiornamento dello stato di connessione può richiedere alcuni minuti dopo le modifiche della configurazione KMS. Nota: aggiornare il browser Web per visualizzare i nuovi valori.

4. Se la colonna Status (Stato) indica un problema KMS, risolverlo immediatamente.

Durante le normali operazioni KMS, lo stato sarà **connesso a KMS**. Se un nodo viene disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (amministrativamente inattivo o Sconosciuto).

Gli altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

- Impossibile caricare la configurazione KMS
- Errore di connettività KMS
- Nome chiave di crittografia KMS non trovato
- Rotazione della chiave di crittografia KMS non riuscita
- La chiave KMS non è riuscita a decrittare un volume dell'appliance

- KMS non configurato

Eseguire le azioni consigliate per questi avvisi.



È necessario affrontare immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Modificare un KMS

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio, se un certificato sta per scadere.

Prima di iniziare

- Se si prevede di aggiornare il sito selezionato per un KMS, è stata esaminata la ["Considerazioni per la modifica del KMS per un sito"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera modificare e selezionare **azioni > Modifica**.

Puoi anche modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Edit** nella pagina dei dettagli del KMS.

3. Facoltativamente, aggiornare i dettagli nel **Passo 1 (dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. È sufficiente modificare il nome della chiave solo in rari casi. Ad esempio, è necessario modificare il nome della chiave se l'alias viene rinominato in KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.

Campo	Descrizione
Gestisce le chiavi per	Se si sta modificando un KMS specifico del sito e non si dispone già di un KMS predefinito, selezionare Sites Not Managed by another KMS (default KMS) (Siti non gestiti da un altro KMS (default KMS)*). Questa selezione converte un KMS specifico del sito nel KMS predefinito, che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti in un'espansione. Nota: se stai modificando un KMS specifico del sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. Nota: il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.

5. Selezionare **continua**.

Viene visualizzata la fase 2 (carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfoggia** e caricare il nuovo file.

7. Selezionare **continua**.

Viene visualizzata la fase 3 (carica certificati client) della procedura guidata Modifica un server di gestione delle chiavi.

8. Se è necessario sostituire il certificato client e la chiave privata del certificato client, selezionare **Browse** (Sfoggia) e caricare i nuovi file.

9. Selezionare **Test e salvare**.

Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi di appliance con crittografia a nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata nel KMS, il server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

10. Se viene visualizzato un messaggio di errore, esaminare i dettagli del messaggio e selezionare **OK**.

Ad esempio, se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non ha avuto esito positivo, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare

Imponi salvataggio.



Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

La configurazione KMS viene salvata.

12. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

La configurazione del KMS viene salvata, ma la connessione al KMS non viene verificata.

Rimozione di un server di gestione delle chiavi (KMS)

In alcuni casi, potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, è possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato.

Prima di iniziare

- È stata esaminata la ["considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato o se il sito non include nodi appliance con crittografia del nodo attivata.
- È possibile rimuovere il KMS predefinito se esiste già un KMS specifico del sito per ogni sito che ha nodi appliance con crittografia del nodo attivata.

Fasi

1. Selezionare **Configurazione > Sicurezza > Server di gestione delle chiavi**.

Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera rimuovere e selezionare **azioni > Rimuovi**.

Puoi anche rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Remove** dalla pagina dei dettagli del KMS.

3. Verificare che quanto segue sia vero:

- Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di un nodo appliance con crittografia del nodo attivata.
- Si sta rimuovendo il KMS predefinito, ma esiste già un KMS specifico del sito per ogni sito con crittografia del nodo.

4. Selezionare **Sì**.

La configurazione KMS viene rimossa.

Gestire le impostazioni del proxy

Configurare un proxy StorageGRID

Se si utilizzano servizi di piattaforma o Cloud Storage Pool, è possibile configurare un proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio dei messaggi dei servizi della piattaforma a endpoint esterni, ad esempio un endpoint su Internet.



Le impostazioni proxy di storage configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy di archiviazione.

Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni proxy**.
2. Nella scheda **archiviazione**, selezionare la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

Lasciare vuoto questo campo per utilizzare la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Selezionare **Salva**.

Dopo il salvataggio del proxy di storage, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di cloud storage.



Le modifiche del proxy possono richiedere fino a 10 minuti.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma da StorageGRID non vengano bloccati.
8. Se è necessario disattivare un proxy di archiviazione, deselezionare la casella di controllo e selezionare **Salva**.

Informazioni correlate

["Porte utilizzate per le comunicazioni esterne"](#)

Configura le impostazioni proxy amministrative in StorageGRID

Se si inviano pacchetti AutoSupport utilizzando HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi Admin e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedi ["Configurare AutoSupport"](#).

Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy amministratore.

Fasi

1. Selezionare **Configurazione > Sicurezza > Impostazioni proxy**.

Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, l'opzione Storage (archiviazione) è selezionata nel menu Tab (scheda).

2. Selezionare la scheda **Ammin**.
3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Facoltativamente, immettere un nome utente e una password per il server proxy.

Se il server proxy non richiede un nome utente o una password, lasciare vuoti questi campi.

7. Selezionare una delle seguenti opzioni:

- Se si desidera proteggere la connessione al proxy amministratore, selezionare **verifica certificato proxy**. Caricare un pacchetto CA per verificare l'autenticità dei certificati SSL presentati dal server proxy amministratore.



AutoSupport on Demand, e-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina dell'upgrade della StorageGRID non funzionano se viene verificato un certificato proxy.

Dopo aver caricato il pacchetto CA, vengono visualizzati i relativi metadati.

- Se non si desidera convalidare i certificati quando si comunica con il server proxy dell'amministratore, selezionare **non verificare il certificato proxy**.

8. Selezionare **Salva**.

Dopo aver salvato il proxy dell'amministratore, viene configurato il server proxy tra i nodi Admin e il supporto tecnico.



Le modifiche del proxy possono richiedere fino a 10 minuti.

9. Se è necessario disattivare il proxy amministratore, deselezionare la casella di controllo **Abilita proxy amministratore**, quindi selezionare **Salva**.

Firewall di controllo

Controlla l'accesso a StorageGRID tramite un firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

È possibile controllare l'accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, è possibile impedire ai tenant di connettersi a Grid Manager dal firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Se si desidera configurare il firewall interno StorageGRID, vedere ["Configurare il firewall interno"](#).

Porta	Descrizione	Se la porta è aperta...
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API. Nota: la porta 443 viene utilizzata anche per il traffico interno.
8443	Porta Grid Manager limitata sui nodi di amministrazione	• I browser Web e i client API di gestione possono accedere a Grid Manager e all'API di Grid Management utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a tenant Manager o all'API di gestione tenant. • Le richieste di contenuto interno verranno rifiutate.
9443	Porta limitata di Tenant Manager sui nodi di amministrazione	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione tenant utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API di Grid Management. • Le richieste di contenuto interno verranno rifiutate.



Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- ["Accedi a Grid Manager"](#)
- ["Creare un account tenant"](#)
- ["Comunicazioni esterne"](#)

Gestisci i controlli firewall interni in StorageGRID

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della rete consentendo di controllare l'accesso alla rete. Utilizzare il firewall per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per

l'implementazione della griglia specifica. Le modifiche apportate alla configurazione nella pagina di controllo Firewall vengono distribuite a ciascun nodo.

Utilizzare le tre schede della pagina di controllo Firewall per personalizzare l'accesso necessario per la griglia.

- **Privileged address list:** Utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o sottoreti nella notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Manage external access (Gestisci accesso esterno).
- **Gestisci accesso esterno:** Utilizzare questa scheda per chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network:** Utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

Le impostazioni di questa scheda sovrascrivono quelle della scheda Gestisci accesso esterno.

- Un nodo con una rete client non attendibile accetta solo le connessioni sulle porte endpoint del bilanciamento del carico configurate su quel nodo (endpoint globali, di interfaccia di nodo e di tipo di nodo).
- Le porte endpoint del bilanciamento del carico *sono le uniche porte aperte* sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Gestisci reti esterne.
- Se attendibili, tutte le porte aperte nella scheda Manage external access (Gestisci accesso esterno) sono accessibili, così come tutti gli endpoint del bilanciamento del carico aperti nella rete client.



Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso apportate in un'altra scheda. Verificare le impostazioni di tutte le schede per assicurarsi che la rete funzioni nel modo previsto.

Per configurare i controlli interni del firewall, vedere ["Configurare i controlli firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla protezione della rete, vedere ["Controllare l'accesso al firewall esterno"](#).

Elenco degli indirizzi privilegiati e schede di gestione degli accessi esterni

La scheda Privileged address list (elenco indirizzi privilegiati) consente di registrare uno o più indirizzi IP ai quali viene concesso l'accesso alle porte della griglia chiuse. La scheda Manage external access (Gestisci accesso esterno) consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non grid). Queste due schede spesso possono essere utilizzate insieme per personalizzare l'esatto accesso di rete necessario per la griglia.



Per impostazione predefinita, gli indirizzi IP privilegiati non dispongono dell'accesso alla porta della griglia interna.

Esempio 1: Utilizzare un host di collegamento per le attività di manutenzione

Si supponga di voler utilizzare un host jump (un host con protezione avanzata) per l'amministrazione di rete. È possibile utilizzare questi passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi privilegiati) per aggiungere l'indirizzo IP dell'host di collegamento.

2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.



Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, tutte le porte esterne sul nodo di amministrazione nella griglia verranno bloccate per tutti gli host, ad eccezione dell'host di collegamento. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Blocco delle porte sensibili

Supponiamo di voler bloccare porte sensibili e il servizio su quella porta. È possibile seguire i seguenti passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi con privilegi) per concedere l'accesso solo agli host che devono accedere al servizio.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.



Aggiungere l'indirizzo IP con privilegi prima di bloccare l'accesso a tutte le porte assegnate per accedere a Grid Manager e Tenant Manager (le porte preimpostate sono 443 e 8443). Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta sensibile e il servizio su quella porta saranno disponibili agli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host viene negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disattivazione dell'accesso ai servizi inutilizzati

A livello di rete, è possibile disattivare alcuni servizi che non si intende utilizzare. Ad esempio, per bloccare il traffico client HTTP S3, utilizzare l'interruttore nella scheda Gestisci accesso esterno per bloccare la porta 18084.

Scheda Untrusted Client Networks

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati esplicitamente.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *trusted*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni in entrata a ciascun nodo di rete su tutti ["porte esterne disponibili"](#).

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client di ciascun nodo è *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte esplicitamente configurate come endpoint del bilanciamento del carico. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#) e ["Configurare i controlli firewall"](#).

Esempio 1: Il nodo gateway accetta solo richieste HTTPS S3

Si supponga che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste

HTTPS S3. Eseguire le seguenti operazioni generali:

1. Dalla "[Endpoint del bilanciamento del carico](#)" pagina, configurare un endpoint di bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Dalla pagina di controllo Firewall, selezionare Untrusted (non attendibile) per specificare che la rete client sul nodo gateway non è attendibile.

Dopo aver salvato la configurazione, tutto il traffico in entrata sulla rete client del nodo gateway viene interrotto, ad eccezione delle richieste HTTPS S3 sulla porta 443 e delle richieste ICMP echo (ping).

Esempio 2: Storage Node invia richieste di servizi della piattaforma S3

Si supponga di voler attivare il traffico dei servizi della piattaforma S3 in uscita da un nodo di storage, ma di voler impedire qualsiasi connessione in entrata a tale nodo di storage sulla rete client. Eseguire questa fase generale:

- Dalla scheda Untrusted Client Networks (reti client non attendibili) della pagina di controllo Firewall, indicare che la rete client nel nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita verso destinazioni di servizi della piattaforma configurate.

Esempio 3: Limitazione dell'accesso a Grid Manager a una subnet

Si supponga di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Attenersi alla seguente procedura:

1. Collegare la rete client dei nodi di amministrazione alla subnet.
2. Utilizzare la scheda Untrusted Client Network (rete client non attendibile) per configurare la rete client come non attendibile.
3. Quando si crea un endpoint per il bilanciamento del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accede.
4. Selezionare **Sì** per la rete client non attendibile.
5. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni alla subnet).

Dopo aver salvato la configurazione, solo gli host della subnet specificata possono accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno di StorageGRID

È possibile configurare il firewall StorageGRID per controllare l'accesso di rete a porte specifiche sui nodi StorageGRID.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[autorizzazioni di accesso specifiche](#)".
- Sono state esaminate le informazioni in "[Gestire i controlli firewall](#)" e "[Linee guida per il networking](#)".
- Se si desidera che un nodo Admin o un nodo gateway accetti il traffico in entrata solo su endpoint configurati esplicitamente, sono stati definiti gli endpoint del bilanciamento del carico.



Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

A proposito di questa attività

StorageGRID include un firewall interno su ciascun nodo che consente di aprire o chiudere alcune porte sui nodi della griglia. È possibile utilizzare le schede di controllo Firewall per aprire o chiudere le porte aperte per impostazione predefinita in Grid Network, Admin Network e Client Network. È inoltre possibile creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia chiuse. Se si utilizza una rete client, è possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client ed è possibile configurare l'accesso a porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla griglia solo a quelle assolutamente necessarie migliora la sicurezza della griglia. Utilizzare le impostazioni di ciascuna delle tre schede di controllo del firewall per assicurarsi che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli del firewall, inclusi esempi, fai riferimento a ["Gestire i controlli firewall"](#).

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, consulta ["Controllare l'accesso al firewall esterno"](#).

Accedere ai controlli firewall

Fasi

1. Selezionare **Configurazione > Sicurezza > Controllo firewall**.

Le tre schede di questa pagina sono descritte in ["Gestire i controlli firewall"](#).

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate su una scheda non limitano le operazioni che è possibile eseguire sulle altre schede; tuttavia, le modifiche alla configurazione apportate su una scheda potrebbero modificare il comportamento delle porte configurate su altre schede.

Elenco di indirizzi con privilegi

La scheda elenco indirizzi privilegiati consente agli host di accedere alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni della scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla rete interna. Inoltre, gli endpoint del bilanciamento del carico e le porte aggiuntive aperte nella scheda Privileged address list (elenco indirizzi con privilegi) sono accessibili anche se bloccati nella scheda Manage external access (Gestisci accesso esterno).



Le impostazioni nella scheda Elenco indirizzi privilegiati possono sovrascrivere le impostazioni nella scheda Rete client non attendibile.

Fasi

1. Nella scheda Privileged address list (elenco indirizzi privilegiati), inserire l'indirizzo o la subnet IP che si desidera concedere l'accesso alle porte chiuse.

2. Facoltativamente, seleziona **Aggiungi un altro IP o una sottorete in notazione CIDR** per aggiungere altri client privilegiati.



Aggiungere il minor numero possibile di indirizzi all'elenco dei privilegi.

3. Facoltativamente, seleziona **Consenti agli indirizzi IP privilegiati di accedere alle porte interne di StorageGRID**. Fai riferimento a "[Porte interne StorageGRID](#)".



Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lasciarlo disattivato.

4. Selezionare **Salva**.

Gestire l'accesso esterno

Quando una porta viene chiusa nella scheda Manage external access (Gestisci accesso esterno), non è possibile accedervi da alcun indirizzo IP non Grid, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Per impostazione predefinita, è possibile chiudere solo le porte aperte e solo quelle chiuse.



Le impostazioni della scheda Manage external access (Gestisci accesso esterno) non possono sostituire quelle della scheda Untrusted Client Network (rete client non attendibile). Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda Manage external access (Gestisci accesso esterno). Le impostazioni della scheda Untrusted Client Network (rete client non attendibile) sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) della rete client.

Fasi

1. Selezionare **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non griglia) per i nodi della griglia.
2. Configurare le porte che si desidera aprire e chiudere utilizzando le seguenti opzioni:
 - Utilizzare il pulsante di commutazione accanto a ciascuna porta per aprire o chiudere la porta selezionata.
 - Selezionare **Open all displayed ports** (Apri tutte le porte visualizzate) per aprire tutte le porte elencate nella tabella.
 - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.



Se 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 sia stato aggiunto all'elenco degli indirizzi privilegiati.



Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi porta esterna immettendo un numero di porta. È possibile inserire un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che hanno la stringa "2" come parte del loro nome.

3. Selezionare **Salva**

Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate come endpoint del bilanciamento del carico e, facoltativamente, le porte aggiuntive selezionate in questa scheda. È inoltre possibile utilizzare questa scheda per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.



Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Le modifiche apportate alla configurazione nella scheda **Untrusted Client Network** (rete client non attendibile) sovrascrivono le impostazioni nella scheda **Manage external access** (Gestisci accesso esterno).

Fasi

1. Selezionare **Untrusted Client Network**.

2. Nella sezione Set New Node Default (Imposta nuovo nodo predefinito), specificare l'impostazione predefinita quando si aggiungono nuovi nodi alla griglia in una procedura di espansione.

- **Trusted** (impostazione predefinita): Quando un nodo viene aggiunto in un'espansione, la sua rete client viene considerata attendibile.
- **Untrusted**: Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile.

Se necessario, è possibile tornare a questa scheda per modificare l'impostazione di un nuovo nodo specifico.



Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.

3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del carico configurati esplicitamente o su porte selezionate aggiuntive:

- Selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Untrusted Client Network (rete client non attendibile).
- Selezionare **Trust on displayed nodes** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Untrusted Client Network (rete client non attendibile).
- Utilizzare l'interruttore accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

Ad esempio, è possibile selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi all'elenco Untrusted Client Network (rete client non attendibile), quindi utilizzare il pulsante di attivazione accanto a un singolo nodo per aggiungere tale singolo nodo all'elenco Trusted Client Network (rete client attendibile).



Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi nodo immettendo il nome del nodo. È possibile immettere un nome parziale. Ad esempio, se si immette un valore **GW**, vengono visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.

4. Selezionare **Salva**.

Le nuove impostazioni del firewall vengono applicate e rese effettive immediatamente. Le connessioni client esistenti potrebbero non funzionare se gli endpoint del load balancer non sono stati configurati.

Gestire i tenant

Account tenant in StorageGRID

Un account tenant consente di utilizzare l'API REST S3 (Simple Storage Service) per memorizzare e recuperare gli oggetti in un sistema StorageGRID.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Gestire i tenant"](#).

In qualità di amministratore di grid, è possibile creare e gestire gli account tenant utilizzati dai client S3 per memorizzare 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 memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, è possibile separare lo storage a oggetti del grid dai diversi reparti dell'organizzazione. In questo caso, è possibile creare account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.



Se si utilizza il protocollo client S3, è possibile utilizzare 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 bucket"](#) per maggiori informazioni.

- **Caso d'utilizzo del provider di servizi:** se si amministra un sistema StorageGRID come provider di servizi, è possibile separare lo storage a oggetti della griglia dalle diverse entità che affitteranno lo storage sulla griglia. In questo caso, è necessario creare account tenant per la società A, la società B, la società C e così via.

Per ulteriori informazioni, vedere ["Utilizzare un account tenant"](#).

Come si crea un account tenant?

Utilizzare il Grid Manager per creare un account tenant. Quando si crea un account tenant, si specificano le seguenti informazioni:

- Informazioni di base, tra cui nome del tenant, tipo di client (S3) e quota di archiviazione opzionale.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione a federazione di griglie.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione di identità o SSO (Single Sign-on).

Inoltre, è possibile attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

A cosa serve il tenant manager?

Dopo aver creato l'account tenant, gli utenti tenant possono accedere a tenant Manager per eseguire attività come le seguenti:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Usa la federazione di griglia per la sincronizzazione degli account e la replica tra griglie
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage



Mentre gli utenti del tenant S3 possono creare e gestire chiavi di accesso S3 e bucket con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Per ulteriori informazioni, vedere ["UTILIZZARE L'API REST S3"](#).

Crea un account tenant di StorageGRID

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 delle identità"](#) E ["single sign-on"](#) 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

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Accesso root o autorizzazione account tenant"](#).
- Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso root per l'account tenant a un gruppo federato, il gruppo federated è stato importato in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Vedere ["Gestire i gruppi di amministratori"](#).
- Se vuoi consentire a un tenant S3 di sincronizzare i dati dell'account e replicare gli oggetti del bucket in un'altra griglia utilizzando una connessione di federazione di griglia:
 - Si dispone di ["configurazione della connessione a federazione di griglie"](#).
 - Lo stato della connessione è **connesso**.
 - Si dispone dell'autorizzazione di accesso root.
 - Sono state esaminate le considerazioni relative a ["gestione dei tenant consentiti per la federazione di grid"](#).
 - Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager, lo stesso gruppo federated è stato importato in Grid Manager su entrambe le griglie.

Quando si crea il tenant, si seleziona questo gruppo per disporre dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione.



Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non viene replicato nella destinazione.

Accedere alla procedura guidata

Fasi

1. Selezionare **Inquilini**.
2. Selezionare **Crea**.

Inserire i dettagli

Fasi

1. Inserire i dettagli del tenant.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Quando viene creato, l'account tenant riceve un ID account univoco di 20 cifre.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant. Se si crea un tenant che utilizzerà una connessione a federazione di griglie, utilizzare questo campo per identificare il tenant di origine e il tenant di destinazione. Ad esempio, questa descrizione per un tenant creato sulla griglia 1 verrà visualizzata anche per il tenant replicato sulla griglia 2: "Questo tenant è stato creato sulla griglia 1".
Tipo di client	Deve essere S3 .
Quota di storage (opzionale)	Se si desidera che il tenant disponga di una quota di storage, un valore numerico per la quota e le unità.

2. Selezionare **continua**.

selezionare le autorizzazioni

Fasi

1. In alternativa, selezionare le autorizzazioni di base che si desidera assegnare al tenant.



Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, selezionare l'icona della guida per ciascuna autorizzazione.

Permesso	Se selezionato...
Consentire i servizi della piattaforma	Il tenant può utilizzare servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3" .

Permesso	Se selezionato...
Utilizza la propria origine 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 .
Consenti selezione S3	Il tenant può emettere richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant". Importante: Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.

2. In alternativa, selezionare le autorizzazioni avanzate che si desidera assegnare al tenant.

Permesso	Se selezionato...
Connessione federazione griglia	Il tenant può utilizzare le connessioni di federazione della griglia, che: - Fa sì che questo account tenant e tutti i gruppi tenant, utenti e chiavi di accesso S3 vengano sincronizzati tra questa griglia e le altre griglie nelle connessioni selezionate.  Se necessario per motivi di sicurezza o conformità, puoi deselezionare Abilita la sincronizzazione della chiave di accesso. - Consente a questo tenant di configurare la replica cross-grid tra i bucket corrispondenti su ogni grid. Vedere "Gestire i tenant consentiti per la federazione di grid".
Blocco oggetti S3	Consentire al tenant di utilizzare funzioni specifiche di blocco oggetti S3: Imposta periodo di conservazione massimo definisce per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Consenti la modalità di conformità impedisce agli utenti di sovrascrivere o eliminare le versioni degli oggetti protetti durante il periodo di conservazione.

3. Selezionare **continua**.

Definire l'accesso root e creare il tenant

Fasi

- Definire l'accesso root per l'account tenant, a seconda che il sistema StorageGRID utilizzi la federazione di identità, il single sign-on (SSO) o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

2. Selezionare **Crea tenant**.

Viene visualizzato un messaggio di successo e il nuovo tenant viene elencato nella pagina tenant. Per informazioni su come visualizzare i dettagli del tenant e monitorare l'attività del tenant, vedere "[Monitorare l'attività del tenant](#)".



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più in base a connettività di rete, stato dei nodi e operazioni Cassandra.

- Se hai selezionato l'autorizzazione **Usa connessione di federazione griglia** per il tenant, verifica che un tenant identico sia stato replicato sull'altra griglia nella connessione. I tenant su entrambe le griglie avranno lo stesso ID account a 20 cifre, nome, descrizione, quota e autorizzazioni.



Se visualizzi un messaggio di errore che indica che il tenant account è stato creato su questa grid ma non è stato sincronizzato con le altre grid, fai riferimento alle istruzioni in "[Risolvere i problemi relativi agli errori di federazione della griglia](#)".

Accesso al tenant (facoltativo)

Se necessario, è possibile accedere al nuovo tenant ora per completare la configurazione oppure accedere al tenant in un secondo momento. La procedura di accesso dipende dal fatto che si sia effettuato l'accesso a Grid Manager utilizzando la porta predefinita (443) o una porta con restrizioni. Vedere "[Controllare l'accesso al firewall esterno](#)".

Accedi subito

Se si utilizza...	Eseguire questa operazione...
Porta 443 e viene impostata una password per l'utente root locale	1. Selezionare Accedi come root. Al momento dell'accesso, vengono visualizzati i collegamenti per la configurazione di bucket, federazione di identità, gruppi e utenti. 2. Selezionare i collegamenti per configurare l'account tenant. Ciascun collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, vedere la "istruzioni per l'utilizzo degli account tenant".
Porta 443 e non è stata impostata una password per l'utente root locale	Selezionare Accedi e immettere le credenziali per un utente nel gruppo federated di accesso root.
Una porta con restrizioni	1. Selezionare fine 2. Selezionare limitato nella tabella tenant per ulteriori informazioni sull'accesso a questo account tenant. L'URL del tenant manager ha il seguente formato: <code>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/</code> ◦ <i>FQDN_or_Admin_Node_IP</i> È un nome di dominio completo o l'indirizzo IP di un nodo amministrativo ◦ <i>port</i> è la porta solo tenant ◦ <i>20-digit-account-id</i> È l'ID account univoco del tenant

Accedi più tardi

Se si utilizza...	Eseguire una di queste operazioni...
Porta 443	• Da Grid Manager, seleziona Tenant e seleziona * Sign in* a destra del nome del tenant. • Inserire l'URL del tenant in un browser Web: <code>https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/</code> ◦ <i>FQDN_or_Admin_Node_IP</i> È un nome di dominio completo o l'indirizzo IP di un nodo amministrativo ◦ <i>20-digit-account-id</i> È l'ID account univoco del tenant

Se si utilizza...	Eseguire una di queste operazioni...
Una porta con restrizioni	• Da Grid Manager, seleziona Inquilini e seleziona Limitato. • Inserire l'URL del tenant in un browser Web: <pre>https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id</pre> ◦ <i>FQDN_or_Admin_Node_IP</i> È un nome di dominio completo o l'indirizzo IP di un nodo amministrativo ◦ <i>port</i> è la porta limitata solo tenant ◦ <i>20-digit-account-id</i> È l'ID account univoco del tenant

Configurare il tenant

Segui le istruzioni in ["Utilizzare un account tenant"](#) per gestire gruppi di tenant e utenti, chiavi di accesso S3, bucket, servizi della piattaforma, sincronizzazione degli account e replica cross-grid.

Modificare un account tenant di StorageGRID

È possibile modificare un account tenant per modificare il nome visualizzato, la quota di storage o le autorizzazioni del tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Accesso root o autorizzazione account tenant"](#).



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più in base a connettività di rete, stato dei nodi e operazioni Cassandra.

Fasi

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](#)

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. Individuare l'account tenant che si desidera modificare.

Utilizzare la casella di ricerca per cercare un tenant in base al nome o all'ID del tenant.

3. Selezionare il tenant. È possibile effettuare una delle seguenti operazioni:

- Selezionare la casella di controllo del tenant e selezionare **azioni > Modifica**.
- Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **Modifica**.

4. Facoltativamente, modificare i valori per questi campi:

- **Nome**
- **Descrizione**
- **Quota di storage**

5. Selezionare **continua**.

6. Selezionare o deselezionare le autorizzazioni per l'account tenant.

- Se si disattiva **Platform Services** per un tenant che li sta già utilizzando, i servizi configurati per i bucket S3 smetteranno di funzionare. Non viene inviato alcun messaggio di errore al tenant. Ad esempio, se il tenant ha configurato la replica CloudMirror per un bucket S3, può comunque memorizzare oggetti nel bucket, ma le copie di tali oggetti non verranno più eseguite nel bucket S3 esterno configurato come endpoint. Vedere "[Gestire i servizi della piattaforma per gli account tenant S3](#)".
- Modificare l'impostazione di **Usa origine identità propria** 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:

- Disattivato e selezionato, il tenant ha già attivato la propria origine di identità. Un tenant deve disattivare l'origine dell'identità prima di poter utilizzare l'origine dell'identità configurata per Grid Manager.
- Disattivato e non selezionato, SSO è attivato per il sistema StorageGRID. Il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager.

- Selezionare o deselezionare l'autorizzazione **Allow S3 Select** (Consenti selezione S3) in base alle necessità. Vedere ["Manage S3 \(Gestisci S3\): Selezionare per gli account tenant"](#).
- Per rimuovere l'autorizzazione **Use grid Federation Connection**:
 - i. Seleziona la scheda Grid federation nella pagina dei dettagli del tenant.
 - ii. Seleziona la connessione che vuoi rimuovere.
 - iii. Selezionare **Rimuovi permesso**.
- Per aggiungere l'autorizzazione **Use grid Federation Connection**:
 - i. Selezionare la scheda **federazione griglia**.
 - ii. Selezionare la casella di controllo **Usa connessione federazione griglia**.
 - iii. Facoltativamente, selezionare **Clona utenti e gruppi locali esistenti** per clonarli nella griglia remota. Se si desidera, è possibile interrompere la clonazione in corso o riprovare a eseguire la clonazione se la clonazione di alcuni utenti o gruppi locali non è riuscita una volta completata l'ultima operazione di clonazione.



Se necessario per motivi di sicurezza o conformità, puoi deselezionare **Abilita la sincronizzazione della chiave di accesso**.

- Per impostare un periodo di conservazione massimo o consentire la modalità di conformità:



S3 blocco oggetti deve essere attivato sulla griglia prima di poter utilizzare queste impostazioni.

- i. Selezionare la scheda **blocco oggetti S3**.
- ii. Per **set Maximum Retention Period** (Imposta periodo di conservazione massimo), immettere un valore e selezionare il periodo di tempo dall'elenco a discesa.
- iii. Per **Consenti modalità di conformità**, selezionare la casella di controllo.

Modificare la password per l'utente root locale di un tenant StorageGRID

Potrebbe essere necessario modificare la password per l'utente root locale di un tenant se l'utente root è bloccato dall'account.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

Se il sistema StorageGRID è abilitato per il Single Sign-on (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire le attività dell'utente root, gli utenti devono appartenere a un gruppo federated che disponga dell'autorizzazione di accesso root per il tenant.

Fasi

1. Selezionare **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](#)

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	→ 📄

- Selezionare l'account tenant. È possibile effettuare una delle seguenti operazioni:
 - Selezionare la casella di controllo del tenant e selezionare **azioni > Modifica password root**.
 - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **azioni > Modifica password root**.
- Inserire la nuova password per l'account tenant.
- Selezionare **Salva**.

Eliminare un account tenant StorageGRID

È possibile eliminare un account tenant se si desidera rimuovere in modo permanente l'accesso del tenant al sistema.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Sono stati rimossi tutti i bucket S3 e gli oggetti associati all'account tenant.
- Se al tenant è consentito utilizzare le connessioni di grid federation, hai esaminato le considerazioni per ["Eliminazione di un tenant con l'autorizzazione di connessione Usa federazione griglia"](#). Le eliminazioni vengono sincronizzate, quindi se un tenant viene eliminato su una grid, verrà eliminato su tutte le grid selezionate.

Fasi

- Selezionare **Inquilini**.
- Individuare l'account tenant o gli account che si desidera eliminare.

Utilizzare la casella di ricerca per cercare un tenant in base al nome o all'ID del tenant.

- Per eliminare più tenant, selezionare le caselle di controllo e selezionare **azioni > Elimina**.
- Per eliminare un singolo tenant, effettuare una delle seguenti operazioni:

- Selezionare la casella di controllo e selezionare **azioni > Elimina**.
- Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **azioni > Elimina**.

5. Selezionare **Sì**.

Gestire i servizi della piattaforma

Scopri i servizi della piattaforma StorageGRID

I servizi della piattaforma includono la replica di 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 il grid in modo che i tenant possano accedere alle risorse esterne necessarie per l'utilizzo di questi servizi.

I servizi della piattaforma non sono supportati per ["secchi di rami"](#).

Replica di CloudMirror

Il servizio di replica di StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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

La replica di CloudMirror presenta alcune importanti analogie differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere ["Confronta la replica cross-grid e la replica CloudMirror"](#).

Notifiche

Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite sugli oggetti a un cluster Kafka esterno specificato, a un endpoint webhook o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.



Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantieni fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

Servizio di integrazione della ricerca

Il servizio di integrazione della ricerca viene utilizzato per inviare i metadati degli oggetti S3 a un indice Elasticsearch specificato, in cui è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.



Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono ai tenant la possibilità di utilizzare risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna alla distribuzione di StorageGRID, è necessario decidere se consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o modificano gli account tenant. È inoltre necessario configurare la rete in modo che i messaggi dei servizi della piattaforma generati dai tenant possano raggiungere le proprie destinazioni.

Consigli per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, tenere presenti i seguenti consigli:

- Se in un bucket S3 nel sistema StorageGRID sono attivate sia la versione che la replica CloudMirror, è necessario attivare anche la versione del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica di CloudMirror di generare versioni di oggetti simili sull'endpoint.
- Non utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica CloudMirror, le notifiche e l'integrazione della ricerca. La presenza di più di 100 tenant attivi può rallentare le performance del client S3.
- Le richieste a un endpoint che non possono essere completate verranno messe in coda per un massimo di 500,000 richieste. Questo limite è equamente condiviso tra i tenant attivi. I nuovi tenant possono superare temporaneamente questo limite di 500,000, in modo che i nuovi tenant non vengano penalizzati in modo ingiusto.

Informazioni correlate

- ["Gestire i servizi della piattaforma"](#)
- ["Configurare le impostazioni del proxy di storage"](#)
- ["Monitorare StorageGRID"](#)

Rete e porte per i servizi della piattaforma StorageGRID

Se si consente a un tenant S3 di utilizzare i servizi della piattaforma, è necessario configurare la rete per la griglia per garantire che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

È possibile abilitare i servizi della piattaforma per un account tenant S3 quando si crea o si aggiorna l'account tenant. Se i servizi della piattaforma sono attivati, il tenant può creare endpoint che fungono da destinazione per la replica CloudMirror, le notifiche di eventi o i messaggi di integrazione di ricerca dai bucket S3. Questi messaggi dei servizi della piattaforma vengono inviati dai nodi di storage che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Cluster Elasticsearch ospitato localmente
- Un'applicazione locale che supporta la ricezione di messaggi Amazon Simple Notification Service
- Un cluster Kafka ospitato localmente
- Un endpoint webhook esterno o ospitato localmente che supporta le richieste di notifica HTTP POST.

Questo endpoint può essere ospitato su vari server web, framework o strumenti di elaborazione dati come Fluentd.

- Un bucket S3 ospitato localmente sulla stessa o su un'altra istanza di StorageGRID
- Un endpoint esterno, ad esempio un endpoint su Amazon Web Services.

Per garantire che i messaggi dei servizi della piattaforma possano essere inviati, è necessario configurare la rete o le reti contenenti i nodi di storage ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi della piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati alle seguenti porte:

- **80**: Per gli URI endpoint che iniziano con http (la maggior parte degli endpoint)
- **443**: Per gli URI endpoint che iniziano con https (la maggior parte degli endpoint)
- **9092**: Per gli URI endpoint che iniziano con http o https (solo endpoint Kafka)

I tenant possono specificare una porta diversa quando creano o modificano un endpoint.



Se si utilizza un'implementazione StorageGRID come destinazione della replica di CloudMirror, i messaggi di replica potrebbero essere ricevuti su una porta diversa da 80 o 443. Assicurarsi che la porta utilizzata per S3 dall'implementazione StorageGRID di destinazione sia specificata nell'endpoint.

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

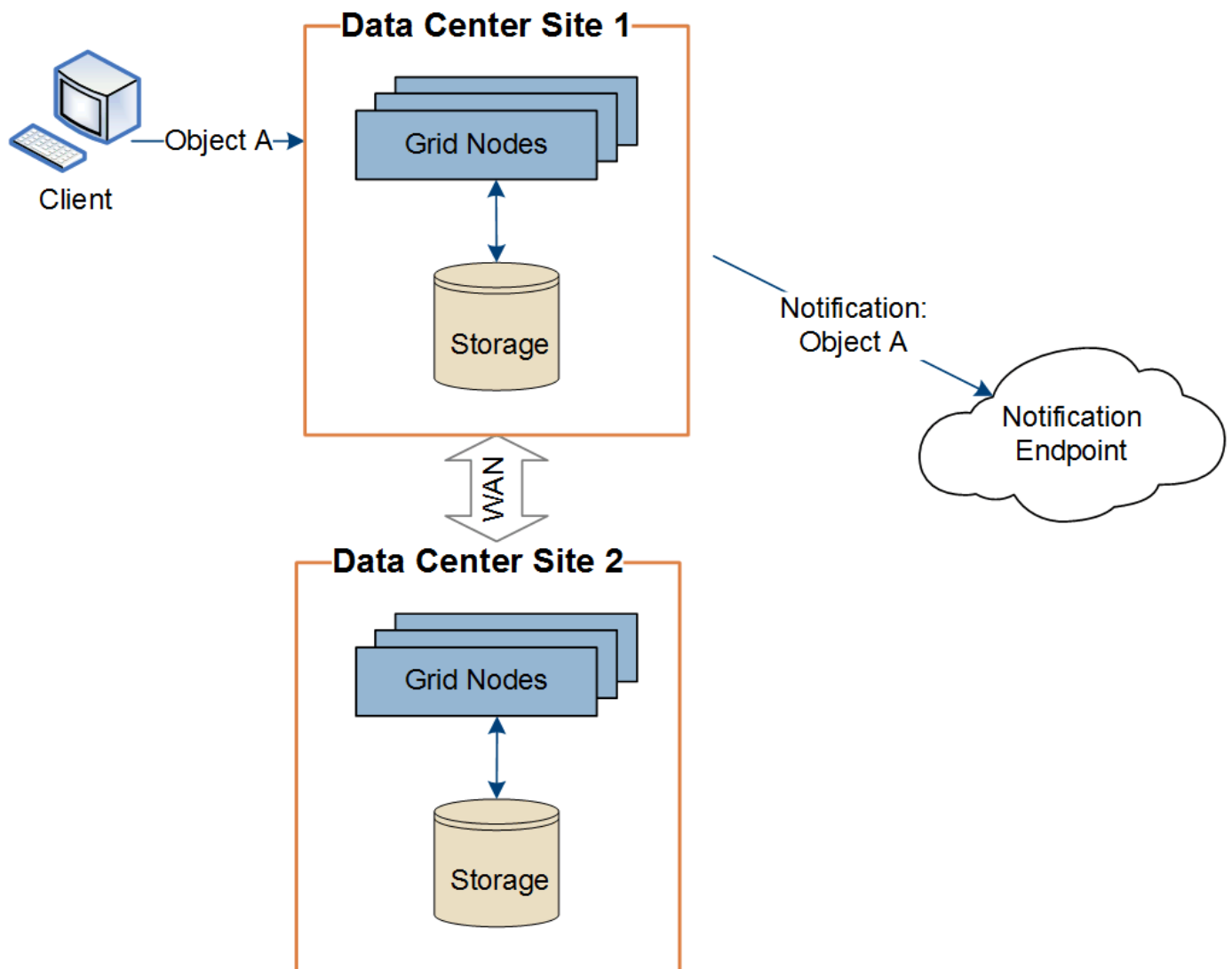
Informazioni correlate

- ["Utilizzare un account tenant"](#)
- ["Porte utilizzate per le comunicazioni esterne"](#)

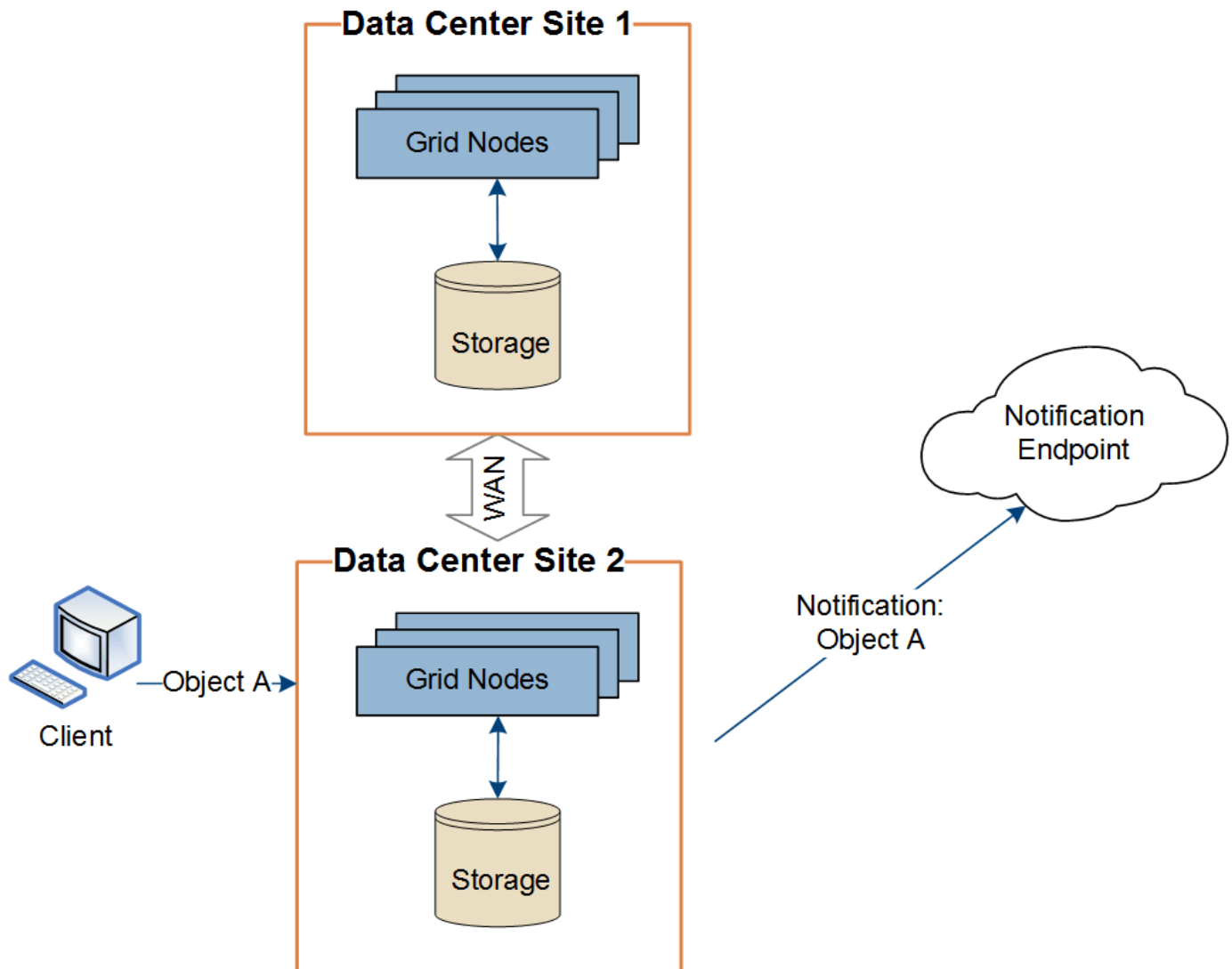
Consegna per sito dei messaggi dei servizi della piattaforma StorageGRID

Tutte le operazioni dei servizi della piattaforma vengono eseguite in base al sito.

Cioè, se un tenant utilizza un client per eseguire un'operazione S3 API Create su un oggetto connettendosi a un nodo gateway nel sito 1 del data center, la notifica relativa a tale azione viene attivata e inviata dal sito 1 del data center.



Se il client esegue successivamente un'operazione di eliminazione API S3 sullo stesso oggetto dal sito del data center 2, la notifica relativa all'azione di eliminazione viene attivata e inviata dal sito del data center 2.



Assicurarsi che la rete di ciascun sito sia configurata in modo che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risoluzione dei problemi dei servizi della piattaforma StorageGRID

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti tenant nel Tenant Manager. Tuttavia, se un tenant ha problemi a configurare o utilizzare i servizi della piattaforma, puoi usare il Grid Manager per aiutare a risolvere il problema.

Problemi con i nuovi endpoint

Prima che un tenant possa utilizzare i servizi della piattaforma, deve creare uno o più endpoint utilizzando il tenant Manager. Ciascun endpoint rappresenta una destinazione esterna per un servizio di piattaforma, come un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento del servizio di notifica semplice Amazon, un argomento di Kafka o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna che le credenziali necessarie per accedere a tale risorsa.

Quando un tenant crea un endpoint, il sistema StorageGRID convalida che l'endpoint esiste e che può essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Se la convalida degli endpoint non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida degli endpoint non è riuscita. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.



La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant.

Problemi con gli endpoint esistenti

Se si verifica un errore quando StorageGRID tenta di raggiungere un endpoint esistente, viene visualizzato un messaggio sul dashboard in Gestione tenant.



One or more endpoints have experienced an error and might not be functioning properly. Go to the [Endpoints](#) page to view the error details. The last error occurred 2 hours ago.

Gli utenti del tenant possono andare alla pagina Endpoint per vedere il messaggio di errore più recente per ciascun endpoint e per capire quanto tempo fa si è verificato l'errore. La colonna **Ultimo errore** mostra il messaggio di errore più recente per ciascun endpoint e indica quanto tempo fa si è verificato l'errore. Gli errori che includono l'icona  si sono verificati 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 della griglia o il supporto tecnico può utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se hai configurato un "[proxy di storage](#)" 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.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint negli ultimi 7 giorni, il dashboard di Tenant Manager visualizza un messaggio di avviso. È possibile accedere alla pagina Endpoint per ulteriori dettagli sull'errore.

Le operazioni del client non riescono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il malfunzionamento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non vengono eseguite correttamente se il servizio RSM (Replicated state Machine) interno viene arrestato o se sono presenti troppi messaggi dei servizi della piattaforma in coda per il recapito.

Per controllare lo stato dei servizi:

1. Selezionare **Nodi > sito > Nodo di archiviazione > Panoramica**.
2. Controllare gli avvisi attivi nella tabella Avvisi.
3. Risolvi tutti gli avvisi attivi. Se necessario, contattare l'assistenza tecnica.

Errori degli endpoint ripristinabili e non ripristinabili

Una volta creati gli endpoint, gli errori di richiesta del servizio della piattaforma possono verificarsi per diversi motivi. Alcuni errori possono essere ripristinati con l'intervento dell'utente. Ad esempio, potrebbero verificarsi errori ripristinabili per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o scadute.
- Il bucket di destinazione non esiste.
- Impossibile ricevere la notifica.

Se StorageGRID rileva un errore ripristinabile, la richiesta di servizio della piattaforma verrà rievitata fino a quando non avrà esito positivo.

Altri errori non sono recuperabili. Ad esempio, gli errori irrecuperabili potrebbero verificarsi per i seguenti motivi:

- L'endpoint è stato eliminato.
- Una destinazione endpoint webhook risponde a una richiesta di notifica con un `400 Bad Request` errore.

Se StorageGRID rileva un errore irreversibile dell'endpoint:

- In Grid Manager, vai a **supporto > Strumenti > metriche > Grafana > Platform Services Overview** per visualizzare i dettagli dell'errore.
- In Tenant Manager, accedere a **STORAGE (S3) > Platform Services Endpoint** per visualizzare i dettagli dell'errore.
- Verificare la `/var/local/log/bycast-err.log` presenza di errori correlati. I nodi di archiviazione che dispongono del servizio ADC contengono questo file di registro.

I messaggi dei servizi della piattaforma non possono essere inviati

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.

Verificare la presenza di avvisi correlati.

Performance più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione.

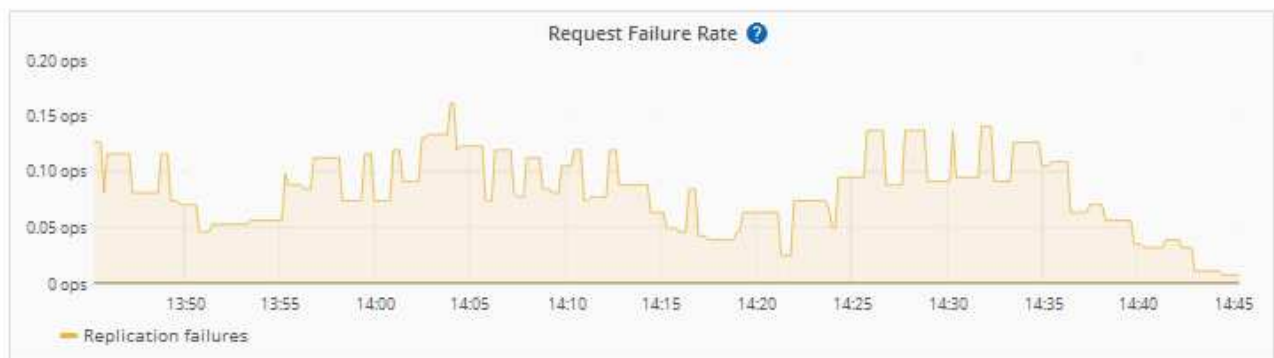
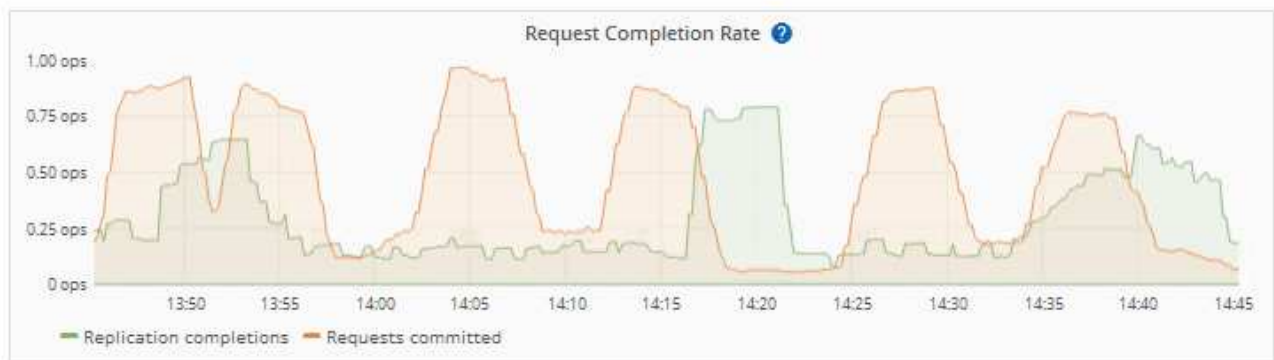
L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire.

È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma non vengono soddisfatte

Per visualizzare il tasso di errore della richiesta per i servizi della piattaforma:

1. Selezionare **Nodi**.
2. Selezionare **Site > Platform Services**.
3. Visualizza il grafico tasso di errore della richiesta.

[1 hour](#) [1 day](#) [1 week](#) [1 month](#) [Custom](#)

Avviso di servizi della piattaforma non disponibili

L'avviso **Platform Services unavailable** (servizi piattaforma non disponibili) indica che non è possibile eseguire operazioni di servizio della piattaforma in un sito perché sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM.

Il servizio RSM garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.

Per risolvere questo avviso, determinare quali nodi di storage del sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di storage che includono anche il servizio ADC). Quindi, assicurati che gran parte di questi nodi storage sia in esecuzione e disponibile.



Se più di un nodo di storage che contiene il servizio RSM si guasta in un sito, si perdono le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori linee guida per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni, vedere [Utilizzare un account tenant > risolvere i problemi relativi agli endpoint dei servizi della piattaforma](#).

Informazioni correlate

["Risolvere i problemi relativi al sistema StorageGRID"](#)

Gestisci S3 Select per account tenant in StorageGRID

È possibile consentire a determinati tenant S3 di utilizzare S3 Select per emettere richieste `SelectObjectContent` su singoli oggetti.

S3 Select offre un modo efficiente per cercare grandi quantità di dati senza dover implementare un database e le risorse associate per abilitare le ricerche. Inoltre, riduce i costi e la latenza del recupero dei dati.

Che cos'è S3 Select?

S3 Select consente ai client S3 di utilizzare le richieste `SelectObjectContent` per filtrare e recuperare solo i dati necessari da un oggetto. L'implementazione StorageGRID di S3 Select include un sottoinsieme di comandi e funzionalità S3 Select.

Considerazioni e requisiti per l'utilizzo di S3 Select

Requisiti di amministrazione della griglia

L'amministratore della griglia deve concedere ai tenant l'abilità S3 Select. Selezionare **Consenti S3 Seleziona** quando ["creazione di un tenant"](#) o ["modifica di un tenant"](#).

Requisiti di formato degli oggetti

L'oggetto che si desidera sottoporre a query deve essere in uno dei seguenti formati:

- **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
- **Parquet**. Requisiti aggiuntivi per gli oggetti in parquet:
 - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
 - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è di 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
 - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.

Requisiti degli endpoint

La richiesta `SelectObjectContent` deve essere inviata a ["Endpoint del bilanciamento del carico di StorageGRID"](#).

I nodi Admin e Gateway utilizzati dall'endpoint devono essere uno dei seguenti:

- Un nodo di appliance per i servizi
- Nodo software basato su VMware
- Nodo bare metal che esegue un kernel con cgroup v2 abilitato

Considerazioni generali

Le query non possono essere inviate direttamente ai nodi di storage.



Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.

Consultare la ["Istruzioni per l'utilizzo 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

Configura le connessioni client S3 a StorageGRID

In qualità di amministratore di rete, è possibile gestire le opzioni di configurazione che controllano il modo in cui le applicazioni client S3 si connettono al sistema StorageGRID per archiviare e recuperare i dati.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Configurare le connessioni client S3 e Swift"](#).

Attività di configurazione

1. Eseguire attività preliminari in StorageGRID, in base al modo in cui l'applicazione client si conatterà a StorageGRID.

Attività richieste

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 necessari all'applicazione per connettersi alla griglia. È possibile utilizzare l'installazione guidata S3 o configurare manualmente ogni entità StorageGRID. +

Utilizzare l'installazione guidata S3

Seguire i passaggi della procedura guidata di installazione S3.

Configurare manualmente

1. Creare un gruppo di alta disponibilità
2. Creare l'endpoint del bilanciamento del carico
3. Creare un account tenant
4. Creare bucket e chiavi di accesso
5. Configurare la regola e i criteri ILM

1. Utilizzare l'applicazione S3 per completare la connessione a StorageGRID. Creare voci DNS per associare gli indirizzi IP ai nomi di dominio che si intende utilizzare.

Se necessario, eseguire la configurazione di un'applicazione aggiuntiva.

2. Eseguire attività in corso nell'applicazione e in StorageGRID per gestire e monitorare lo storage a oggetti nel tempo.

Informazioni necessarie per collegare StorageGRID a un'applicazione client

Prima di poter collegare StorageGRID a un'applicazione client S3, è necessario eseguire le operazioni di configurazione in StorageGRID e ottenere un determinato valore.

Di quali valori ho bisogno?

La seguente tabella mostra i valori da configurare in StorageGRID e 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 bilanciamento del carico	Applicazione client
Certificato SSL	StorageGRID > endpoint del bilanciamento del carico	Applicazione client
Nome server (FQDN)	StorageGRID > endpoint del bilanciamento del carico	• Applicazione client • Voce DNS
ID chiave di accesso S3 e chiave di accesso segreta	StorageGRID > tenant e bucket	Applicazione client

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Nome bucket/container	StorageGRID > tenant e bucket	Applicazione client

Come si ottengono questi valori?

In base alle proprie esigenze, è possibile effettuare una delle seguenti operazioni per ottenere le informazioni necessarie:

- **Utilizzare il simbolo "Installazione guidata S3"**. L'installazione guidata S3 consente di configurare rapidamente i valori richiesti in StorageGRID e di creare uno o due file da utilizzare per la configurazione dell'applicazione S3. La procedura guidata guida l'utente attraverso i passaggi richiesti e aiuta a verificare che le impostazioni siano conformi alle Best practice di StorageGRID.



Se si sta configurando un'applicazione S3, si consiglia di utilizzare la procedura guidata di configurazione S3, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

- **Utilizzare il simbolo "Installazione guidata di FabricPool"**. Analogamente all'installazione guidata di S3, l'installazione guidata di FabricPool consente di configurare rapidamente i valori richiesti e di creare un file da utilizzare quando si configura un livello cloud FabricPool in ONTAP.



Se si prevede di utilizzare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool, si consiglia di utilizzare la procedura guidata di installazione di FabricPool, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

- **Configurare gli elementi manualmente.** Se si sta effettuando la connessione a un'applicazione S3 e si preferisce non utilizzare l'installazione guidata S3, è possibile ottenere i valori richiesti eseguendo la configurazione manualmente. Attenersi alla seguente procedura:
 - a. Configurare il gruppo di alta disponibilità (ha) che si desidera utilizzare per l'applicazione S3. Vedere ["Configurare i gruppi ad alta disponibilità"](#).
 - b. Creare l'endpoint di bilanciamento del carico che verrà utilizzato dall'applicazione S3. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#).
 - c. Creare l'account tenant che verrà utilizzato dall'applicazione S3. Vedere ["Creare un account tenant"](#).
 - d. Per un tenant S3, accedere all'account tenant e generare un ID della chiave di accesso e una chiave di accesso segreta per ogni utente che accede all'applicazione. Vedere ["Creare le proprie chiavi di accesso"](#).
 - e. Creare uno o più bucket S3 all'interno dell'account tenant. Per S3, vedere ["Creare un bucket S3"](#).
 - f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/container, creare una nuova regola ILM e attivare un nuovo criterio ILM per utilizzare tale regola. Vedere ["Creare una regola ILM"](#) e ["Creare un criterio ILM"](#).

Sicurezza per i client S3 in StorageGRID

Gli account tenant StorageGRID utilizzano applicazioni client S3 per salvare i dati degli oggetti in StorageGRID. È necessario esaminare le misure di protezione implementate per le applicazioni client.

Riepilogo

L'elenco seguente riassume il modo in cui viene implementata la protezione per l'API REST S3:

Sicurezza della connessione

TLS

Autenticazione del server

Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore

Autenticazione del client

S3 ID chiave di accesso account e chiave di accesso segreta

Autorizzazione del client

Proprietà dei bucket e tutte le policy di controllo degli accessi applicabili

In che modo StorageGRID fornisce la protezione per le applicazioni client

Le applicazioni client S3 possono connettersi al servizio di bilanciamento del carico su nodi gateway o nodi amministrativi o direttamente ai nodi storage.

- I client che si connettono al servizio Load Balancer possono utilizzare HTTPS o HTTP, in base alla modalità di ["configurare l'endpoint del bilanciamento del carico"](#).

HTTPS fornisce una comunicazione sicura e crittografata TLS ed è consigliato. È necessario allegare un certificato di protezione all'endpoint.

HTTP fornisce comunicazioni meno sicure e non crittografate e dovrebbe essere utilizzato solo per reti non di produzione o di test.

- I client che si connettono ai nodi di archiviazione possono anche utilizzare HTTPS o HTTP.

HTTPS è l'impostazione predefinita ed è consigliata.

HTTP fornisce comunicazioni meno sicure e non crittografate, ma può essere facoltativamente ["attivato"](#) utilizzato per reti non di produzione o di test.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire ["Intestazioni di autenticazione HTTP"](#) a StorageGRID per eseguire operazioni con le API REST.

Certificati di sicurezza e applicazioni client

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint del bilanciamento del carico. Ogni endpoint del bilanciamento del carico dispone di un proprio certificato—un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.

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

- Quando le applicazioni client si connettono direttamente a un nodo di storage, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia. Vedere ["Aggiungere un certificato API S3 personalizzato"](#).

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un 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 l'installazione guidata S3

Considerazioni e requisiti relativi alla procedura guidata di configurazione S3 di StorageGRID

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID come sistema di storage a oggetti per un'applicazione S3.

Quando utilizzare l'installazione guidata S3

L'installazione guidata S3 guida l'utente attraverso ogni fase della configurazione di StorageGRID per l'utilizzo con un'applicazione S3. Durante il completamento della procedura guidata, è possibile scaricare i file da utilizzare per immettere i valori nell'applicazione S3. Utilizzare la procedura guidata per configurare il sistema più rapidamente e per assicurarsi che le impostazioni siano conformi alle Best practice StorageGRID.

Se si dispone di ["Autorizzazione di accesso root"](#), è possibile completare l'installazione guidata di S3 quando si inizia a utilizzare il Gestore griglie StorageGRID oppure è possibile accedere e completare la procedura guidata in un secondo momento. A seconda dei requisiti, è possibile configurare manualmente alcuni o tutti gli elementi richiesti e utilizzare la procedura guidata per assemblare i valori richiesti da un'applicazione S3.

Prima di utilizzare la procedura guidata

Prima di utilizzare la procedura guidata, verificare di aver completato questi prerequisiti.

Ottenere gli indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ad alta disponibilità (ha), si conoscono i nodi a cui si conatterà l'applicazione S3 e la rete StorageGRID da utilizzare. Si conoscono anche i valori da inserire per la subnet CIDR, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si intende utilizzare una LAN virtuale per separare il traffico dall'applicazione S3, l'interfaccia VLAN è già stata configurata. Vedere ["Configurare le interfacce VLAN"](#).

Configurare la federazione di identità e SSO

Se 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 ["USA la federazione delle identità"](#) E ["Configurare il single sign-on"](#).

Ottenere e configurare i nomi di dominio

Si conosce il nome di dominio completo (FQDN) da utilizzare per StorageGRID. Le voci DNS (Domain Name Server) associano questo FQDN agli indirizzi IP virtuali (VIP) del gruppo ha creato utilizzando la procedura guidata.

Se intendi utilizzare richieste in stile virtual-hosted di S3, dovresti avere ["Nomi di dominio degli endpoint S3 configurati"](#). Si consiglia di utilizzare richieste in stile virtual-hosted.

Esaminare i requisiti del bilanciamento del carico e del certificato di sicurezza

Se si intende utilizzare il bilanciamento del carico StorageGRID, sono state esaminate le considerazioni generali sul bilanciamento del carico. Si dispone dei certificati da caricare o dei valori necessari per generare un certificato.

Se si intende utilizzare un endpoint esterno (di terze parti) per il bilanciamento del carico, si dispone del nome di dominio completo (FQDN), della porta e del certificato per il bilanciamento del carico.

Configurare le connessioni di federazione di griglie

Se vuoi consentire al tenant S3 di sincronizzare i dati dell'account e replicare gli oggetti del bucket in un'altra griglia utilizzando una connessione di federazione di griglia, conferma quanto segue prima di avviare il setup wizard:

- Si dispone di ["configurazione della connessione a federazione di griglie"](#).
- Lo stato della connessione è **connesso**.
- Si dispone dell'autorizzazione di accesso root.

Accedere e completare la setup wizard in StorageGRID

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID per l'utilizzo con un'applicazione S3. L'installazione guidata fornisce i valori necessari all'applicazione per accedere a un bucket StorageGRID e per salvare gli oggetti.

Prima di iniziare

- Si dispone di ["Autorizzazione di accesso root"](#).
- È stata esaminata la ["considerazioni e requisiti"](#) per l'utilizzo della procedura guidata.

Accedere alla procedura guidata

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Se il banner **FabricPool and S3 setup wizard** appare sulla dashboard, seleziona il collegamento nel banner. Se il banner non appare più, seleziona l'icona di aiuto  dalla barra dell'intestazione in Grid Manager e seleziona **FabricPool and S3 setup wizard**.
3. Nella sezione dell'applicazione S3 della pagina di installazione guidata di FabricPool e S3, selezionare **Configura ora**.

Fase 1 di 6: Configurare il gruppo ha

Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati S3. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni S3.

Per ulteriori informazioni su questa attività, vedere ["Gestire i gruppi ad alta disponibilità"](#).

Fasi

1. Se si prevede di utilizzare un bilanciamento del carico esterno, non è necessario creare un gruppo ha. Selezionare **Salta questo passaggio** e andare a [Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico](#).
2. Per utilizzare il bilanciamento del carico StorageGRID, è possibile creare un nuovo gruppo ha o utilizzare un gruppo ha esistente.

Creare un gruppo ha

- a. Per creare un nuovo gruppo ha, selezionare **Crea gruppo ha**.
- b. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

- c. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

- d. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

- e. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR e n. 8212; un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, 192.16.0.0/22.
Indirizzo IP del gateway (opzionale)	Se gli indirizzi IP S3 utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, inserire l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.

Campo	Descrizione
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

f. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine) per tornare all'installazione guidata S3.

g. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Utilizzare il gruppo ha esistente

a. Per utilizzare un gruppo ha esistente, selezionare il nome del gruppo ha dal menu **Select an ha group** (Seleziona un gruppo ha).

b. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

È possibile utilizzare il servizio bilanciamento del carico StorageGRID, disponibile su tutti i nodi gateway e di amministrazione, oppure connettersi a un bilanciamento del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciamento del carico StorageGRID.

Per ulteriori informazioni su questa attività, vedere ["Considerazioni per il bilanciamento del carico"](#).

Per utilizzare il servizio bilanciamento del carico di StorageGRID, selezionare la scheda **StorageGRID load balancer**, quindi creare o selezionare l'endpoint di bilanciamento del carico che si desidera utilizzare. Per utilizzare un bilanciamento del carico esterno, selezionare la scheda **bilanciamento del carico esterno** e fornire i dettagli sul sistema già configurato.

Creare l'endpoint

Fasi

1. Per creare un endpoint di bilanciamento del carico, selezionare **Crea endpoint**.
2. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin. Nota: non sono consentite le porte utilizzate da altri servizi di rete. Vedere "Porte interne StorageGRID".
Tipo di client	Deve essere S3 .
Protocollo di rete	Selezionare HTTPS. Nota: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

3. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Global (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

4. Per la fase di accesso del tenant, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

5. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per i dettagli su cosa immettere.
USA certificato StorageGRID S3	Utilizzare questa opzione solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Per ulteriori informazioni, vedere "Configurare i certificati API S3" .

6. Selezionare **fine** per tornare all'installazione guidata S3.

7. Selezionare **continua** per passare al punto tenant e bucket.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciamento del carico esistente

Fasi

1. Per utilizzare un endpoint esistente, selezionarne il nome dal campo **Select a load balancer endpoint**.

2. Selezionare **continua** per passare al punto tenant e bucket.

Utilizzare un bilanciamento del carico esterno

Fasi

1. Per utilizzare un bilanciamento del carico esterno, completare i seguenti campi.

Campo	Descrizione
FQDN	Il nome di dominio completo (FQDN) del bilanciamento del carico esterno.
Porta	Il numero di porta che l'applicazione S3 utilizzerà per connettersi al bilanciamento del carico esterno.
Certificato	Copiare il certificato del server per il bilanciamento del carico esterno e incollarlo in questo campo.

2. Selezionare **continua** per passare al punto tenant e bucket.

Fase 3 di 6: Creazione di tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per memorizzare e recuperare oggetti in StorageGRID. Ogni tenant dispone di utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità.

Un bucket è un container utilizzato per memorizzare 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 è necessario aggiungere bucket o impostare opzioni in un secondo momento, è possibile utilizzare Tenant Manager.

Per ulteriori informazioni su questa attività, vedere ["Creare un account tenant"](#) e ["Creare un bucket S3"](#).

Fasi

1. Immettere un nome per l'account tenant.

I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.

2. Definisci l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del tuo sistema StorageGRID ["federazione delle identità"](#), ["SSO \(Single Sign-on\)"](#), o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente da assegnare "Autorizzazione di accesso root" al tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.

Opzione	Eseguire questa operazione
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente da assegnare " Autorizzazione di accesso root " al tenant. Nessun utente locale può accedere.

- Se si desidera che la procedura guidata crei l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root, selezionare **Crea automaticamente la chiave di accesso S3 dell'utente root**.

Selezionare questa opzione se l'unico utente per il tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant, "[Utilizzare Tenant Manager](#)" per configurare chiavi e autorizzazioni.

- Se si desidera creare un bucket per questo tenant ora, selezionare **Crea bucket per questo tenant**.



Se S3 Object Lock è attivato per la griglia, il bucket creato in questa fase non ha S3 Object Lock abilitato. Se è necessario utilizzare un bucket blocco oggetti S3 per questa applicazione S3, non selezionare per creare un bucket ora. Utilizzare invece Tenant Manager in "[creare il bucket](#)" un secondo momento.

- Immettere il nome del bucket utilizzato dall'applicazione S3. Ad esempio, `s3-bucket`.

Non è possibile modificare il nome del bucket dopo averlo creato.

- Selezionare **Region** per questo bucket.

Utilizzare l'area predefinita (`us-east-1`) a meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base all'area del bucket.

- Selezionare **Crea e continua**.

fase 4 di 6: Download dei dati

Nella fase di download dei dati, è possibile scaricare uno o due file per salvare i dettagli di ciò che si è appena configurato.

Fasi

- Se è stato selezionato **Create root user S3 access key automatically** (Crea chiave di accesso S3 utente root automaticamente), eseguire una o entrambe le operazioni seguenti:
 - Selezionare **Scarica chiavi di accesso** per scaricare un `.csv` file contenente il nome dell'account del tenant, l'ID della chiave di accesso e la chiave di accesso segreta.
 - Seleziona 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 una posizione sicura.



Non chiudere questa pagina prima di aver copiato entrambi i tasti di accesso. I tasti non saranno disponibili dopo la chiusura di questa pagina. Assicurarsi di salvare queste informazioni in una posizione sicura perché possono essere utilizzate per ottenere dati dal sistema StorageGRID.

4. Se richiesto, selezionare la casella di controllo per confermare che le chiavi sono state scaricate o copiate.
5. Selezionare **continua** per passare alla regola ILM e al passaggio del criterio.

Fase 5 di 6: Esaminare la regola ILM e il criterio ILM per S3

Le regole ILM (Information Lifecycle Management) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID. Il criterio ILM incluso in StorageGRID crea due copie replicate di tutti gli oggetti. Questo criterio è attivo fino a quando non si attiva almeno un nuovo criterio.

Fasi

1. Esaminare le informazioni fornite nella pagina.
2. Se si desidera aggiungere istruzioni specifiche per gli oggetti appartenenti al nuovo tenant o bucket, creare una nuova regola e una nuova policy. Vedere ["Creare una regola ILM"](#) e ["Utilizzare i criteri ILM"](#).
3. Selezionare **ho esaminato questi passaggi e ho compreso cosa devo fare**.
4. Selezionare la casella di controllo per indicare che si comprende cosa fare in seguito.
5. Selezionare **continua** per accedere a **Riepilogo**.

Fase 6 di 6: Riepilogo

Fasi

1. Esaminare il riepilogo.
2. Prendere nota dei dettagli nei passaggi successivi, che descrivono la configurazione aggiuntiva che potrebbe essere necessaria prima di connettersi al client S3. Ad esempio, selezionando **Accedi come root** si passa a Tenant Manager, dove è possibile aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni del bucket.
3. Selezionare **fine**.
4. Configurare l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

Gestire i gruppi ha

Scopri i gruppi ad alta disponibilità di StorageGRID

I gruppi ad alta disponibilità (ha) forniscono connessioni dati ad alta disponibilità per client S3 e connessioni altamente disponibili al Grid Manager e al Tenant Manager.

È possibile raggruppare le interfacce di rete di più nodi Admin e Gateway in un gruppo ad alta disponibilità (ha). Se l'interfaccia attiva nel gruppo ha non riesce, un'interfaccia di backup può gestire il carico di lavoro.

Ciascun 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 client S3.
- I gruppi HA che includono solo nodi Admin forniscono connessioni altamente disponibili al Grid Manager e al Tenant Manager.
- Un gruppo ha che include solo appliance di servizi e nodi software basati su VMware può fornire connessioni altamente disponibili per ["S3 tenant che utilizzano S3 Select"](#). I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Come crei un gruppo ha?

1. Selezionare un'interfaccia di rete per uno o più nodi Admin o Gateway. È possibile utilizzare un'interfaccia Grid Network (eth0), un'interfaccia Client Network (eth2), un'interfaccia VLAN o un'interfaccia di accesso aggiunta al nodo.



Non è possibile aggiungere un'interfaccia a un gruppo ha se dispone di un indirizzo IP assegnato da DHCP.

2. Specificare un'interfaccia come principale. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.
3. È possibile determinare l'ordine di priorità per le interfacce di backup.
4. Al gruppo vengono assegnati da uno a 10 indirizzi IP virtuali (VIP). Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per istruzioni, vedere ["Configurare i gruppi ad alta disponibilità"](#).

Che cos'è l'interfaccia attiva?

Durante il normale funzionamento, tutti gli indirizzi VIP per il gruppo ha vengono aggiunti all'interfaccia primaria, che è la prima interfaccia nell'ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Cioè, durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Analogamente, durante il normale funzionamento, qualsiasi interfaccia a priorità inferiore per il gruppo ha agisce come interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi disponibile.

Visualizzare lo stato corrente del gruppo ha di un nodo

Per verificare se un nodo è assegnato a un gruppo HA e determinarne lo stato 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 corrisponde allo stato corrente del nodo nel gruppo ha:

- **Attivo:** Il gruppo ha è attualmente ospitato su questo nodo.
- **Backup:** Il gruppo ha non sta attualmente utilizzando questo nodo; si tratta di un'interfaccia di backup.
- **Arrestato:** Il gruppo ha non può essere ospitato su questo nodo perché il servizio ad alta disponibilità (keepalived) è stato arrestato manualmente.
- **Fault:** Il gruppo ha non può essere ospitato su questo nodo a causa di uno o più dei seguenti fattori:
 - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
 - L'interfaccia eth0 o VIP del nodo non è disponibile.
 - Il nodo non è attivo.

In questo esempio, il nodo di amministrazione primario è stato aggiunto a due gruppi ha. Questo nodo è attualmente l'interfaccia attiva per il gruppo di client di amministrazione e un'interfaccia di backup per il gruppo di client FabricPool.

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 non funziona?

L'interfaccia che attualmente ospita gli indirizzi VIP è l'interfaccia attiva. Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi VIP si spostano sulla prima interfaccia di backup disponibile nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia di backup disponibile e così via.

Il failover può essere attivato per uno dei seguenti motivi:

- Il nodo su cui è configurata l'interfaccia non funziona.
- Il nodo su cui è configurata l'interfaccia perde la connettività con tutti gli altri nodi per almeno 2 minuti.
- L'interfaccia attiva non funziona.
- Il servizio Load Balancer si arresta.
- Il servizio High Availability si interrompe.



Il failover potrebbe non essere attivato da guasti di rete esterni al nodo che ospita l'interfaccia attiva. Allo stesso modo, il failover non viene attivato dai servizi per Grid Manager o Tenant Manager.

Il processo di failover richiede in genere solo pochi secondi ed è abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

Quando il guasto viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati nell'interfaccia con priorità più alta disponibile.

Come i gruppi HA di StorageGRID garantiscono l'alta disponibilità

È possibile utilizzare gruppi ad alta disponibilità (ha) per fornire connessioni altamente disponibili a StorageGRID per i dati a oggetti e per l'utilizzo amministrativo.

- Un gruppo ha può fornire connessioni amministrative altamente disponibili al Grid Manager o al tenant Manager.
- Un gruppo ha può fornire connessioni dati ad alta disponibilità per S3 client.
- Un gruppo ha che contiene una sola interfaccia consente di fornire molti indirizzi VIP e di impostare esplicitamente gli indirizzi IPv6.

Un gruppo ha può fornire alta disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando si crea un gruppo ha, aggiungere interfacce dai tipi di nodi che forniscono i servizi richiesti.

- **Admin Node:** Include il servizio Load Balancer e abilita l'accesso al Grid Manager o al Tenant Manager.
- **Gateway Node:** Include il servizio Load Balancer.

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso a Grid Manager	• Nodo amministratore primario (primario) • Nodi amministrativi non primari Nota: l'Admin Node primario deve essere l'interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.
Accesso solo al tenant manager	• Nodi di amministrazione primari o non primari
Accesso client S3: servizio Load Balancer	• Nodi di amministrazione • Nodi gateway
S3 accesso client per "S3 Seleziona"	• Appliance di servizi • Nodi software basati su VMware Nota: I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Limitazioni dell'utilizzo di gruppi ha con Grid Manager o Tenant Manager

Se un servizio Grid Manager o Tenant Manager non funziona, il failover del gruppo ha non viene attivato.

Se hai effettuato l'accesso a Grid Manager o a Tenant Manager quando si verifica il failover, sei disconnesso e devi effettuare nuovamente l'accesso per riprendere l'attività.

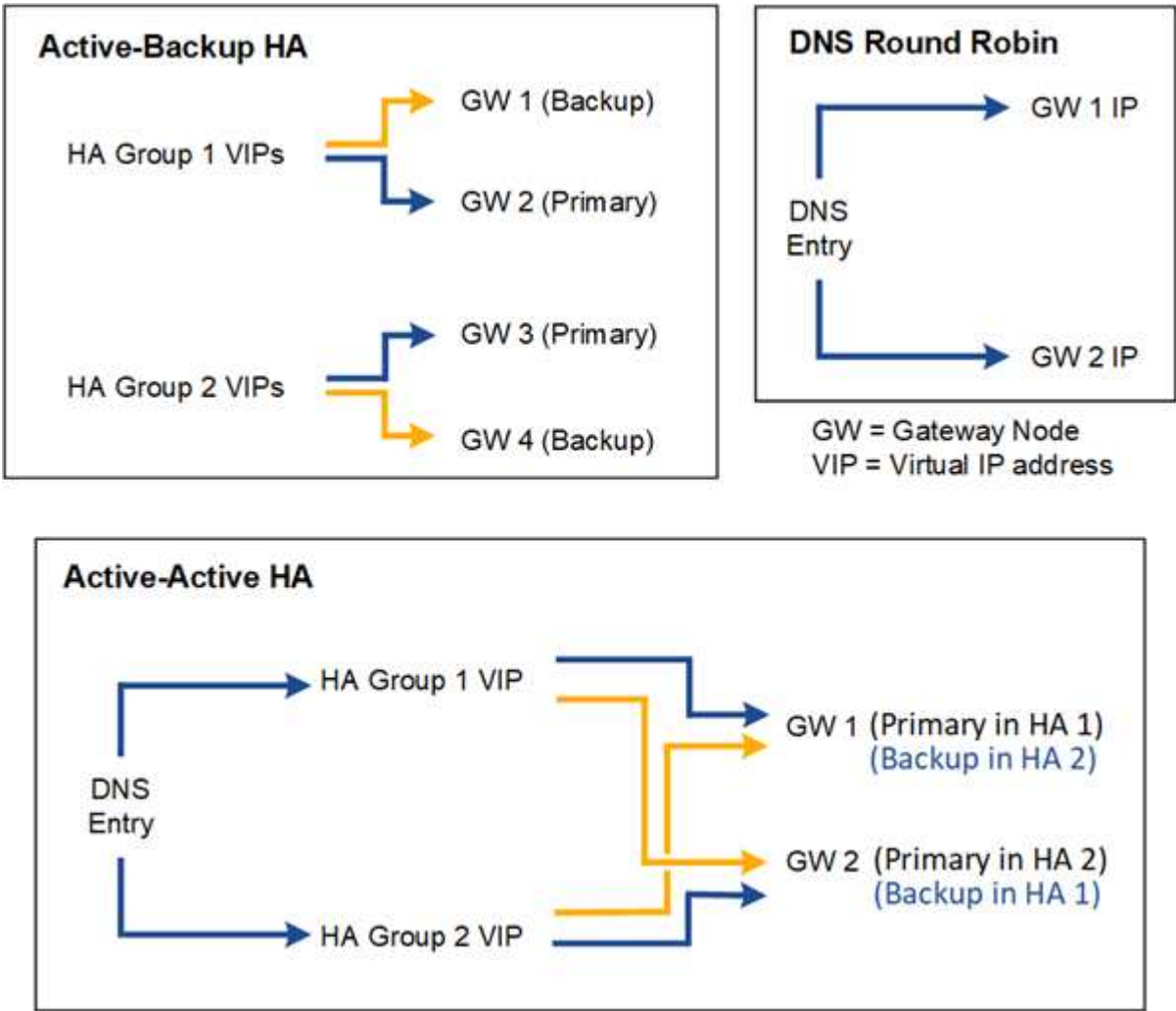
Non è possibile eseguire alcune procedure di manutenzione quando il nodo di amministrazione primario non è disponibile. Durante il failover, è possibile utilizzare Grid Manager per monitorare il sistema StorageGRID.

Opzioni di configurazione per i gruppi di alta disponibilità di StorageGRID

I seguenti diagrammi forniscono esempi di diverse modalità in cui è possibile configurare

i gruppi ad alta disponibilità (HA). Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia principale nel gruppo ha e il giallo indica l'interfaccia di backup nel gruppo ha.



La tabella riassume i vantaggi di ciascuna configurazione ha mostrata nel diagramma.

Configurazione	Vantaggi	Svantaggi
Ha Active-Backup	• Gestito da StorageGRID senza dipendenze esterne. • Failover rapido.	• Solo un nodo in un gruppo ha è attivo. Almeno un nodo per gruppo ha sarà inattivo.
DNS Round Robin	• Maggiore throughput aggregato. • Nessun host inattivo.	• Failover lento, che potrebbe dipendere dal comportamento del client. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Ha bisogno di un controllo dello stato di salute implementato dal cliente.

Configurazione	Vantaggi	Svantaggi
Ha Active-Active	• Il traffico viene distribuito tra più gruppi ha. • Throughput aggregato elevato che si adatta al numero di gruppi ha. • Failover rapido.	• Più complesso da configurare. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Ha bisogno di un controllo dello stato di salute implementato dal cliente.

Configura i gruppi ad alta disponibilità in StorageGRID

È possibile configurare i gruppi ad alta disponibilità (ha) per fornire l'accesso altamente disponibile ai servizi sui nodi Admin o Gateway.



Un sistema StorageGRID può avere un massimo di 255 gruppi HA.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- Se si intende utilizzare un'interfaccia VLAN in un gruppo ha, l'interfaccia VLAN è stata creata. Vedere ["Configurare le interfacce VLAN"](#).
- Se si intende utilizzare un'interfaccia di accesso per un nodo in un gruppo ha, l'interfaccia è stata creata:
 - **Linux (prima di installare il nodo):** ["Creare file di configurazione del nodo"](#)
 - **Linux (dopo aver installato il nodo):** ["Aggiungere interfacce trunk o di accesso a un nodo"](#)
 - **VMware (dopo l'installazione del nodo):** ["Aggiungere interfacce trunk o di accesso a un nodo"](#)



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Creare un gruppo ad alta disponibilità

Quando si crea un gruppo ad alta disponibilità, selezionare una o più interfacce e organizzarle in ordine di priorità. Quindi, assegnare uno o più indirizzi VIP al gruppo.

Un'interfaccia deve essere un nodo gateway o un nodo amministratore per essere incluso in un gruppo ha. Un gruppo ha può utilizzare solo un'interfaccia per un dato nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi ha.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Rete > Gruppi ad alta disponibilità**.
2. Selezionare **Crea**.

Inserire i dettagli del gruppo ha

Fasi

1. Fornire un nome univoco per il gruppo ha.
2. Facoltativamente, inserire una descrizione per il gruppo ha.
3. Selezionare **continua**.

Aggiungere interfacce al gruppo ha

Fasi

1. Selezionare una o più interfacce da aggiungere a questo gruppo ha.

Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

Add interfaces to the HA group

Select one or more interfaces for this HA group. You can select only one interface for each node.

Q
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

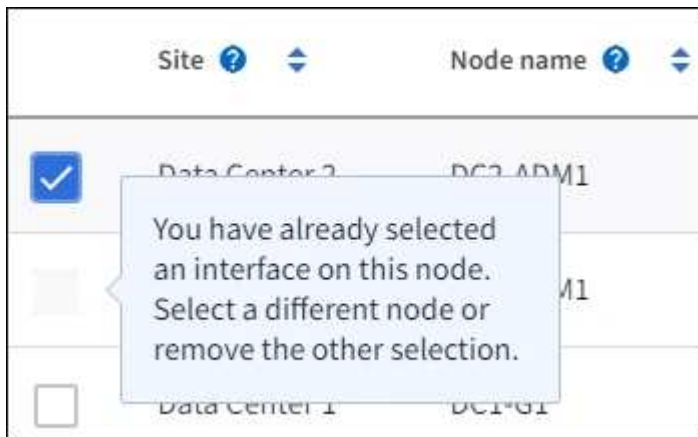


Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti per visualizzare la nuova interfaccia nella tabella.

Linee guida per la selezione delle interfacce

- Selezionare almeno un'interfaccia.
- È possibile selezionare una sola interfaccia per un nodo.
- Se il gruppo ha è per la protezione ha dei servizi Admin Node, che includono Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se il gruppo ha è per la protezione ha del traffico client S3, selezionare interfacce su nodi amministrativi, nodi gateway o entrambi.
- Se si selezionano interfacce su diversi tipi di nodi, viene visualizzata una nota informativa. Si ricorda che, in caso di failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo appena attivo. Ad esempio, un nodo gateway di backup non può fornire la protezione ha dei servizi del nodo amministratore. Analogamente, un nodo Admin di backup non può eseguire tutte le procedure di manutenzione che il nodo Admin primario può fornire.
- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. Il

suggerimento fornisce ulteriori informazioni.



- Non è possibile selezionare un'interfaccia se il relativo valore di sottorete o il gateway è in conflitto con un'altra interfaccia selezionata.
- Non è possibile selezionare un'interfaccia configurata se non dispone di un indirizzo IP statico.

2. Selezionare **continua**.

Determinare l'ordine di priorità

Se il gruppo ha include più di un'interfaccia, è possibile determinare quale sia l'interfaccia primaria e quali siano le interfacce di backup (failover). Se l'interfaccia principale non funziona, gli indirizzi VIP passano all'interfaccia con la priorità più alta disponibile. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia con la priorità più alta disponibile e così via.

Fasi

1. Trascinare le righe nella colonna **Ordine di priorità** per determinare l'interfaccia primaria e le interfacce di backup.

La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

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**.

Inserire gli indirizzi IP

Fasi

1. Nel campo **Subnet CIDR**, specificare la subnet VIP nella notazione CIDR: Un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32).

L'indirizzo di rete non deve avere bit host impostati. Ad esempio, 192.16.0.0/22.



Se si utilizza un prefisso a 32 bit, l'indirizzo di rete VIP funge anche da indirizzo del gateway e da indirizzo VIP.

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 S3 amministrativo o tenant accede a questi indirizzi VIP da una subnet diversa, immettere l'indirizzo IP **Gateway**. L'indirizzo del gateway deve trovarsi all'interno della subnet VIP.

Gli utenti client e admin utilizzeranno questo gateway per accedere agli indirizzi IP virtuali.

3. Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP e tutti saranno attivi contemporaneamente sull'interfaccia attiva.

Specificare almeno un indirizzo IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

4. Selezionare **Create ha group** (Crea gruppo ha) e selezionare **Finish** (fine).

Viene creato il gruppo ha ed è ora possibile utilizzare gli indirizzi IP virtuali configurati.

Passi successivi

Se si utilizza questo gruppo ha per il bilanciamento del carico, creare un endpoint per il bilanciamento del carico per determinare il protocollo di porta e di rete e per allegare eventuali certificati richiesti. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#).

Modificare un gruppo ad alta disponibilità

È possibile modificare un gruppo ad alta disponibilità (ha) per modificarne nome e descrizione, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o aggiornare indirizzi IP virtuali.

Ad esempio, potrebbe essere necessario modificare un gruppo ha se si desidera rimuovere il nodo associato a un'interfaccia selezionata in una procedura di decommissionamento del sito o del nodo.

Fasi

1. Selezionare **Configurazione > Rete > Gruppi ad alta disponibilità**.

La pagina High Availability groups (gruppi ad alta disponibilità) mostra tutti i gruppi ha esistenti.

2. Selezionare la casella di controllo del gruppo ha che si desidera modificare.
3. Eseguire una delle seguenti operazioni in base a quanto si desidera aggiornare:
 - Selezionare **azioni > Modifica indirizzo IP virtuale** per aggiungere o rimuovere indirizzi VIP.
 - Selezionare **azioni > Modifica gruppo ha** per aggiornare il nome o la descrizione del gruppo, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o rimuovere indirizzi VIP.
4. Se si seleziona **Modifica indirizzo IP virtuale**:
 - a. Aggiornare gli indirizzi IP virtuali per il gruppo ha.
 - b. Selezionare **Salva**.
 - c. Selezionare **fine**.
5. Se si seleziona **Edit ha group** (Modifica gruppo ha):
 - a. Facoltativamente, aggiornare il nome o la descrizione del gruppo.
 - b. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere o rimuovere interfacce.



Se il gruppo ha fornisce l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario

- c. Facoltativamente, trascinare le righe per modificare l'ordine di priorità dell'interfaccia primaria e delle interfacce di backup per questo gruppo ha.
- d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
- e. Selezionare **Salva**, quindi **fine**.

Rimuovere un gruppo ad alta disponibilità

È possibile rimuovere uno o più gruppi ad alta disponibilità (ha) alla volta.



Non è possibile rimuovere un gruppo ha se è associato a un endpoint di bilanciamento del carico. Per eliminare un gruppo ha, è necessario rimuoverlo da tutti gli endpoint del bilanciamento del carico che lo utilizzano.

Per evitare interruzioni dei client, aggiornare le applicazioni client S3 interessate prima di rimuovere un gruppo ha. Aggiornare ciascun client per la connessione utilizzando un altro indirizzo IP, ad esempio l'indirizzo IP virtuale di un gruppo ha diverso o l'indirizzo IP configurato per un'interfaccia durante l'installazione.

Fasi

1. Selezionare **Configurazione > Rete > Gruppi ad alta disponibilità**.
2. Esaminare la colonna **endpoint del bilanciamento del carico** per ciascun gruppo ha che si desidera rimuovere. Se sono elencati endpoint del bilanciamento del carico:
 - a. Vai a **Configurazione > Rete > Endpoint del bilanciamento del carico**.
 - b. Selezionare la casella di controllo per l'endpoint.
 - c. Selezionare **azioni > Modifica modalità di associazione endpoint**.
 - d. Aggiornare la modalità di binding per rimuovere il gruppo ha.
 - e. Selezionare **Save Changes** (Salva modifiche).
3. Se non sono elencati endpoint del bilanciamento del carico, selezionare la casella di controllo per ciascun gruppo ha che si desidera rimuovere.
4. Selezionare **azioni > Rimuovi gruppo ha**.
5. Esaminare il messaggio e selezionare **Delete ha group** (Elimina gruppo ha) per confermare la selezione.

Tutti i gruppi ha selezionati vengono rimossi. Nella pagina dei gruppi ad alta disponibilità viene visualizzato un banner verde di successo.

Gestire il bilanciamento del carico

Scopri il bilanciamento del carico di StorageGRID

Attraverso il bilanciamento del carico è possibile gestire i carichi di lavoro di acquisizione e recupero da client S3.

Cos'è il bilanciamento del carico?

Quando un'applicazione client salva o recupera i dati da un sistema StorageGRID, StorageGRID utilizza un sistema di bilanciamento del carico per gestire il carico di lavoro di acquisizione e recupero. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro tra più nodi di storage.

Il servizio bilanciamento del carico StorageGRID viene installato su tutti i nodi di amministrazione e su tutti i nodi gateway e fornisce il bilanciamento del carico di livello 7. Esegue la terminazione TLS (Transport Layer Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage.

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando si inoltra il traffico client ai nodi di storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU.



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 ["Utilizzare bilanciatori di carico di terze parti con StorageGRID"](#).

Quanti nodi per il bilanciamento del carico sono necessari?

Come Best practice generale, ogni sito del sistema StorageGRID deve includere due o più nodi nel servizio bilanciamento del carico. Ad esempio, un sito potrebbe includere due nodi gateway o sia un nodo amministratore che un nodo gateway. Assicurati che sia disponibile un'infrastruttura di rete, hardware o virtualizzazione adeguata per ogni nodo di bilanciamento del carico, sia che si utilizzino appliance per i servizi, nodi bare metal o nodi basati su macchine virtuali (VM).

Che cos'è un endpoint di bilanciamento del carico?

Un endpoint di bilanciamento del carico definisce la porta e il protocollo di rete (HTTPS o HTTP) che le richieste dell'applicazione client in entrata e in uscita utilizzeranno per accedere ai nodi che contengono il servizio Load Balancer. L'endpoint definisce anche il tipo di client (S3), la modalità di associazione e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint del bilanciatore del carico, utilizzare Grid Manager oppure completare la configurazione guidata di S3 e FabricPool :

- ["Configurare gli endpoint del bilanciamento del carico"](#)
- ["Utilizzare l'installazione guidata S3"](#)
- ["Utilizzare l'installazione guidata di FabricPool"](#)

Considerazioni sulla memorizzazione nella cache del bilanciatore del carico

La memorizzazione nella cache migliora significativamente le prestazioni quando un carico di lavoro opera su un sottoinsieme di dati e accede agli oggetti più volte. Inoltre, la memorizzazione nella cache fornisce l'accesso remoto all'archiviazione degli oggetti senza una distribuzione completa della griglia. La memorizzazione nella cache del bilanciatore del carico è disponibile solo per i nodi gateway.

Durante la creazione degli endpoint del bilanciatore del carico:

- Abilita la memorizzazione nella cache solo per i carichi di lavoro memorizzabili nella cache. I carichi di lavoro che accedono ai dati non memorizzati nella cache più spesso rispetto ai dati memorizzati nella cache avranno prestazioni peggiori rispetto a quelle che avrebbero se non fossero stati gestiti dalla cache. In alcuni casi, i carichi di lavoro con elevati tassi di sovrascrittura ed espulsione potrebbero anche superare la resistenza di scrittura dell'unità garantita.
- Si consiglia di valutare l'aggiunta di ulteriori endpoint o nodi per la memorizzazione nella cache di singoli carichi di lavoro che sono buoni candidati per la memorizzazione nella cache.
- Utilizzare endpoint distinti per carichi di lavoro memorizzabili nella cache e non memorizzabili nella cache. Questa separazione garantisce che i meccanismi di memorizzazione nella cache vengano applicati in modo appropriato e non interferiscano con l'elaborazione dei dati non memorizzabili nella cache.
- Valutare un potenziale carico di lavoro memorizzabile nella cache indirizzandolo all'endpoint abilitato alla cache. Monitorare e verificare il tasso di successo della cache per determinare l'idoneità del carico di lavoro per la memorizzazione nella cache. Questa valutazione aiuta a ottimizzare le prestazioni e a garantire un utilizzo efficiente delle risorse della cache.
- ["Esaminare i registri di audit"](#) per determinare se un carico di lavoro esistente sarebbe un buon candidato

per la memorizzazione nella cache. Per un dato periodo di tempo, determina quale percentuale di GET è destinata a oggetti univoci. Per essere idoneo alla memorizzazione nella cache, questo valore dovrebbe essere inferiore al 50%.

Esempi di carichi di lavoro che potrebbero essere buoni candidati per la memorizzazione nella cache

- Laghi di dati
- Calcolo ad alte prestazioni (HPC)
- Formazione AI/ML
- Reti di distribuzione dei contenuti (CDN)
- Gestione delle risorse multimediali
- Produzione video



- È possibile memorizzare nella cache più versioni dell'oggetto.
- Sono supportate le operazioni di lettura dell'intervallo.

Esempi di carichi di lavoro che non sono buoni candidati per la memorizzazione nella cache

- Piscina in tessuto
- Applicazioni di backup
- Livelli di archiviazione



Se un contenuto da servire tramite la cache richiede la crittografia a riposo, "[abilitare la crittografia del nodo o dell'unità](#)" sul nodo cache.

Tipi di oggetti e richieste che non verranno memorizzati nella cache

- IL `response-content-encoding` parametro di query
- IL `partNumber` parametro di query
- Intestazioni condizionali
 - `If-Match`
 - `If-Modified-Since`
 - `If-None-Match`
 - `If-Unmodified-Since`
- Richieste crittografate a riposo con uno dei seguenti metodi:
 - SSE (crittografia lato server con chiavi gestite StorageGRID)
 - SSE-C (crittografia lato server con chiavi fornite dal cliente)
 - Crittografia degli oggetti memorizzati

Tutte le richieste non memorizzate nella cache vengono inoltrate a un LDR upstream come se la cache non fosse abilitata.

Informazioni correlate

- "[Risoluzione dei problemi di memorizzazione nella cache del bilanciatore del carico](#)"

- Per ulteriori informazioni sulla memorizzazione nella cache del bilanciamento del carico, contattare l'assistenza tecnica.

Considerazioni per la porta

Per impostazione predefinita, la porta di un endpoint di bilanciamento del carico è 10433 per il primo endpoint creato, ma è possibile specificare qualsiasi porta esterna inutilizzata compresa tra 1 e 65535. Se si utilizza la porta 80 o 443, l'endpoint utilizzerà il servizio Load Balancer solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. Se si utilizza la stessa porta per più di un endpoint, è necessario specificare una modalità di binding diversa per ciascun endpoint.

Non sono consentite le porte utilizzate da altri servizi di rete. Vedere ["Porte interne StorageGRID"](#) .

Considerazioni sul protocollo di rete

Nella maggior parte dei casi, le connessioni tra le applicazioni client e StorageGRID devono utilizzare la crittografia TLS (Transport Layer Security). La connessione a StorageGRID senza crittografia TLS è supportata ma non consigliata, soprattutto negli ambienti di produzione. Quando si seleziona il protocollo di rete per l'endpoint del bilanciamento del carico StorageGRID, selezionare **HTTPS**.

Considerazioni per i certificati endpoint del bilanciamento del carico

Se si seleziona **HTTPS** come protocollo di rete per l'endpoint del bilanciamento del carico, è necessario fornire un certificato di sicurezza. È possibile utilizzare una di queste tre opzioni quando si crea l'endpoint del bilanciamento del carico:

- **Caricare un certificato firmato (consigliato).** Il certificato può essere firmato da un'autorità di certificazione pubblica o privata. L'utilizzo di un certificato del server CA pubblicamente attendibile per proteggere la connessione è la procedura consigliata. A differenza dei certificati generati, i certificati firmati da una CA possono essere ruotati senza interruzioni, in modo da evitare problemi di scadenza.

Prima di creare l'endpoint del bilanciamento del carico, è necessario ottenere i seguenti file:

- Il file di certificato del server personalizzato.
- Il file di chiave privata del certificato del server personalizzato.
- Facoltativamente, un bundle CA dei certificati di ciascuna autorità di certificazione di emissione intermedia.
- **Generare un certificato autofirmato.**
- **Utilizzare il certificato globale StorageGRID S3.** È necessario caricare o generare una versione personalizzata del certificato prima di poterla selezionare per l'endpoint del bilanciamento del carico. Vedere ["Configurare i certificati API S3"](#).

Di quali valori ho bisogno?

Per creare il certificato, è necessario conoscere tutti i nomi di dominio e gli indirizzi IP utilizzati dalle applicazioni client S3 per accedere all'endpoint.

La voce **Subject DN** (Distinguished Name) per il certificato deve includere il nome di dominio completo che l'applicazione client utilizzerà per StorageGRID. Ad esempio:

```
Subject DN:
/C=Country/ST=State/O=Company, Inc./CN=s3.storagegrid.example.com
```

Se necessario, il certificato può utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, *.storagegrid.example.com utilizza il carattere jolly * per rappresentare adm1.storagegrid.example.com e gn1.storagegrid.example.com.

Se vuoi utilizzare richieste in stile virtual-hosted di S3, il certificato deve includere anche una voce **Nome alternativo** per ciascuna "Nome di dominio dell'endpoint S3" che hai configurato, compresi eventuali nomi jolly. Ad esempio:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```



Se si utilizzano caratteri jolly per i nomi di dominio, vedere ["Linee guida per la protezione avanzata dei certificati server"](#).

È inoltre necessario definire una voce DNS per ciascun nome nel certificato di protezione.

Come si gestiscono i certificati in scadenza?



Se il certificato utilizzato per proteggere la connessione tra l'applicazione S3 e StorageGRID scade, l'applicazione potrebbe perdere temporaneamente l'accesso a StorageGRID.

Per evitare problemi di scadenza del certificato, attenersi alle seguenti Best practice:

- Monitorare attentamente tutti gli avvisi che avvisano di imminenti date di scadenza dei certificati, come ad esempio la scadenza del certificato endpoint del sistema di bilanciamento del carico* e la scadenza del certificato globale del server per gli avvisi API S3*.
- Mantenere sempre sincronizzate le versioni del certificato delle applicazioni StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.
- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e nell'applicazione S3 prima della scadenza del certificato esistente.

Considerazioni per la modalità di binding

La modalità di binding consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciamento del carico. Se un endpoint utilizza una modalità di binding, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente FQDN (Fully Qualified Domain Name). Le applicazioni client che utilizzano qualsiasi altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una delle seguenti modalità di binding:

- **Globale** (impostazione predefinita): Le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare questa impostazione a meno che non sia necessario limitare l'accessibilità di un endpoint.
- **IP virtuali dei gruppi ha.** Le applicazioni client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha.
- **Interfacce nodo.** I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate.
- **Tipo di nodo.** In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway.

Considerazioni sull'accesso al tenant

L'accesso tenant è una funzionalità di sicurezza opzionale che consente di controllare quali account tenant StorageGRID possono utilizzare un endpoint di bilanciamento del carico per accedere ai bucket. È possibile consentire a tutti i tenant di accedere a un endpoint (impostazione predefinita) oppure specificare un elenco dei tenant consentiti o bloccati per ciascun endpoint.

È possibile utilizzare questa funzionalità per fornire un migliore isolamento della sicurezza tra i tenant e i relativi endpoint. Ad esempio, è possibile utilizzare questa funzione per garantire che i materiali top-secret o altamente classificati di proprietà di un tenant rimangano completamente inaccessibili agli altri tenant.



Ai fini del controllo degli accessi, il tenant viene determinato dalle chiavi di accesso utilizzate nella richiesta del client; se non vengono fornite chiavi di accesso come parte della richiesta (ad esempio con accesso anonimo), il proprietario del bucket viene utilizzato per determinare il tenant.

Esempio di accesso al tenant

Per comprendere il funzionamento di questa funzionalità di sicurezza, si consideri il seguente esempio:

1. Sono stati creati due endpoint di bilanciamento del carico, come segue:
 - Endpoint **Public**: Utilizza la porta 10443 e consente l'accesso a tutti i tenant.
 - Endpoint **Top secret**: Utilizza la porta 10444 e consente l'accesso solo al tenant **Top secret**. Tutti gli altri tenant non possono accedere a questo endpoint.
2. Il `top-secret.pdf` è in un secchio di proprietà dell'inquilino **Top Secret**.

Per accedere a `top-secret.pdf`, un utente del locatario **Top Secret** può inviare una richiesta GET a `https://w.x.y.z:10444/top-secret.pdf`. Poiché a questo tenant è consentito utilizzare l'endpoint 10444, l'utente può accedere all'oggetto. Tuttavia, se un utente appartenente a un altro tenant invia la stessa richiesta allo stesso URL, riceve un messaggio di accesso immediato negato. L'accesso viene negato anche se le credenziali e la firma sono valide.

Disponibilità della CPU

Il servizio di bilanciamento del carico su ogni nodo amministrativo e nodo gateway funziona in modo indipendente quando inoltra traffico S3 ai nodi storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU. Le informazioni sul carico della CPU del nodo vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata più frequentemente. A tutti i nodi di storage viene assegnato un valore minimo di

peso di base, anche se un nodo riporta un utilizzo pari al 100% o non ne riporta l'utilizzo.

In alcuni casi, le informazioni sulla disponibilità della CPU sono limitate al sito in cui si trova il servizio Load Balancer.

Configurare gli endpoint del bilanciamento del carico StorageGRID

Gli endpoint di bilanciamento del carico determinano le porte e i protocolli di rete che i client S3 possono utilizzare quando si collegano al bilanciamento del carico StorageGRID sui nodi Gateway e Admin. È inoltre possibile utilizzare gli endpoint per accedere a Grid Manager, Tenant Manager o a entrambi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- È stata esaminata la ["considerazioni per il bilanciamento del carico"](#).
- Se in precedenza è stata rimappata una porta che si intende utilizzare per l'endpoint del bilanciamento del carico, si dispone di ["rimosso il remap della porta"](#).
- Hai creato tutti i gruppi ad alta disponibilità (ha) che intendi utilizzare. I gruppi HA sono consigliati, ma non richiesti. Vedere ["Gestire i gruppi ad alta disponibilità"](#).
- Se l'endpoint di bilanciamento del carico viene utilizzato da ["S3 tenant per S3 Select"](#), non deve utilizzare gli indirizzi IP o FQDN di alcun nodo bare-metal. Per gli endpoint del bilanciamento del carico utilizzati per S3 Select sono consentiti solo le appliance di servizi e i nodi software basati su VMware.
- Sono state configurate le interfacce VLAN che si intende utilizzare. Vedere ["Configurare le interfacce VLAN"](#).
- Se si crea un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

- Per caricare un certificato, è necessario disporre del certificato del server, della chiave privata del certificato e, facoltativamente, di un bundle CA.
- Per generare un certificato, sono necessari tutti i nomi di dominio e gli indirizzi IP utilizzati dai client S3 per accedere all'endpoint. Devi anche conoscere l'oggetto (Nome distinto).
- Se si desidera utilizzare il certificato API di StorageGRID S3 (che può essere utilizzato anche per le connessioni direttamente ai nodi di archiviazione), il certificato predefinito è già stato sostituito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere ["Configurare i certificati API S3"](#).

Creare un endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico del client S3 specifica una porta, un tipo di client (S3) e un protocollo di rete (HTTP o HTTPS). Gli endpoint del bilanciamento del carico dell'interfaccia di gestione specificano una porta, un tipo di interfaccia e una rete client non attendibile.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Rete > Endpoint del bilanciatore del carico**.
2. Per creare un endpoint per un client S3, selezionare la scheda **Client S3**.
3. Per creare un endpoint per l'accesso a Grid Manager, Tenant Manager o entrambi, selezionare la scheda **interfaccia di gestione**.
4. Selezionare **Crea**.

Inserire i dettagli dell'endpoint

Fasi

1. Selezionare le istruzioni appropriate per inserire i dettagli per il tipo di endpoint che si desidera creare.

Client S3

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata compresa tra 1 e 65535. Se si immette 80 o 8443, l'endpoint viene configurato solo sui nodi Gateway, a meno che non sia stata liberata la porta 8443. Quindi è possibile utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata su entrambi i nodi Gateway e Admin. Se stai configurando gli endpoint del bilanciatore di carico per un "spazio dei nomi globale", usa la stessa porta per ogni endpoint.
Tipo di client	Deve essere S3 .
Protocollo di rete	Il protocollo di rete che i client utilizzeranno per la connessione a questo endpoint. • Selezionare HTTPS per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Selezionare HTTP per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.
Abilita la memorizzazione nella cache	Abilita o disabilita "memorizzazione nella cache sui nodi gateway" per questo endpoint del bilanciatore del carico. Se si verificano problemi con la memorizzazione nella cache, fare riferimento a "Risoluzione dei problemi di memorizzazione nella cache del bilanciatore del carico".

Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.

Campo	Descrizione
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Gestore griglia, Gestore tenant o entrambi. • Gestore griglia: 8443 • Responsabile del tenant: 9443 • Sia Grid Manager che Tenant Manager: 443 Nota: È possibile utilizzare queste porte preimpostate o altre porte disponibili.
Tipo di interfaccia	Selezionare il pulsante di opzione per l'interfaccia StorageGRID a cui si accede utilizzando questo endpoint.
Rete client non attendibile	Selezionare Sì se l'endpoint deve essere accessibile alle reti client non attendibili. In caso contrario, selezionare No. Quando si seleziona Sì, la porta è aperta su tutte le reti client non attendibili. Nota: È possibile configurare una porta per essere aperta o chiusa a reti client non attendibili solo quando si crea l'endpoint di bilanciamento del carico.

1. Selezionare **continua**.

Selezionare una modalità di binding

Fasi

1. Selezionare una modalità di associazione per l'endpoint per controllare la modalità di accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Alcune modalità di associazione sono disponibili per gli endpoint client o per gli endpoint dell'interfaccia di gestione. Tutte le modalità per entrambi i tipi di endpoint sono elencate di seguito.

Modalità	Descrizione
Globale (impostazione predefinita per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Globale a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.

Modalità	Descrizione
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo (solo endpoint client)	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.
Tutti i nodi amministrativi (impostazione predefinita per gli endpoint dell'interfaccia di gestione)	I client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo amministrativo per accedere a questo endpoint.

Se più di un endpoint utilizza la stessa porta, StorageGRID utilizza questo ordine di priorità per decidere quale endpoint utilizzare: **IP virtuali dei gruppi ha** > **interfacce nodo** > **tipo di nodo** > **Globale**.

Se si stanno creando endpoint dell'interfaccia di gestione, sono consentiti solo i nodi Admin.

2. Se si seleziona **IP virtuali dei gruppi ha**, selezionare uno o più gruppi ha.

Se si stanno creando endpoint dell'interfaccia di gestione, selezionare VIP associati solo ai nodi Admin.

3. Se si seleziona **Node interfaces**, selezionare una o più interfacce di nodo per ciascun nodo Admin o nodo gateway che si desidera associare a questo endpoint.
4. Se si seleziona **Node type** (tipo nodo), selezionare Admin Node (nodi amministratore), che include sia l'Admin Node primario che qualsiasi Admin Node non primario, oppure Gateway Node (nodi gateway).

Controllo dell'accesso al tenant



Un endpoint dell'interfaccia di gestione può controllare l'accesso al tenant solo quando l'endpoint dispone di [Tipo di interfaccia di Tenant Manager](#).

Fasi

1. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. Selezionare questa opzione se non sono ancora stati creati account tenant. Dopo aver aggiunto account tenant, è possibile modificare l'endpoint del bilanciamento del carico per consentire o bloccare account specifici.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.

Campo	Descrizione
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Create** per aggiungere il nuovo endpoint del bilanciamento del carico. Quindi, andare a [Al termine](#). In caso contrario, selezionare **continua** per allegare il certificato.

Allega certificato

Fasi

1. Se si sta creando un endpoint **HTTPS**, selezionare il tipo di certificato di sicurezza che si desidera allegare all'endpoint.

Il certificato protegge le connessioni tra i client S3 e il servizio Load Balancer sui nodi Admin Node o Gateway.

- **Carica certificato.** Selezionare questa opzione se si dispone di certificati personalizzati da caricare.
- **Genera certificato.** Selezionare questa opzione se si dispone dei valori necessari per generare un certificato personalizzato.
- **Utilizzare il certificato StorageGRID S3.** Selezionare questa opzione se si desidera utilizzare il certificato API S3 globale, che può essere utilizzato anche per le connessioni direttamente ai nodi di archiviazione.

Non è possibile selezionare questa opzione a meno che non sia stato sostituito il certificato API S3 predefinito, firmato dalla CA griglia, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere ["Configurare i certificati API S3"](#).

- **Utilizza certificato interfaccia di gestione.** Selezionare questa opzione se si desidera utilizzare il certificato dell'interfaccia di gestione globale, che può essere utilizzato anche per le connessioni dirette ai nodi amministrativi.
2. Se non si utilizza il certificato StorageGRID S3, caricare o generare il certificato.

Carica certificato

- a. Selezionare **carica certificato**.
- b. Caricare i file dei certificati del server richiesti:
 - **Server certificate**: Il file di certificato del server personalizzato in codifica PEM.
 - **Chiave privata del certificato**: Il file della chiave privata del certificato del server personalizzato (.key).



Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere di almeno 2048 bit.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
- c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
 - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione .pem.

Ad esempio: storagegrid_certificate.pem

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.
- d. Selezionare **Crea**. + viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e l'endpoint.

Generare un certificato

- a. Selezionare **genera certificato**.
- b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.

Campo	Descrizione
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. Nota: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Crea**.

Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 o l'interfaccia di gestione e questo endpoint.

Al termine

Fasi

1. Se si utilizza un DNS, assicurarsi che il DNS includa un record per associare il nome di dominio completo (FQDN, Fully Qualified Domain Name) di StorageGRID a ciascun indirizzo IP utilizzato dai client per effettuare le connessioni.

L'indirizzo IP inserito nel record DNS dipende dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, i client si connetteranno agli indirizzi IP virtuali di quel gruppo ha.
- Se non si utilizza un gruppo ha, i client si connetteranno al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministratore.

È inoltre necessario assicurarsi che il record DNS faccia riferimento a tutti i nomi di dominio degli endpoint richiesti, inclusi i nomi con caratteri jolly.

2. Fornire ai client S3 le informazioni necessarie per connettersi all'endpoint:

- Numero di porta
- Nome di dominio completo o indirizzo IP
- Tutti i dettagli del certificato richiesti

Visualizzare e modificare gli endpoint del bilanciamento del carico

È possibile visualizzare i dettagli degli endpoint del bilanciamento del carico esistenti, inclusi i metadati del certificato per un endpoint protetto. È possibile modificare determinate impostazioni per un endpoint.

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, esaminare le tabelle nella pagina Endpoints del bilanciamento del carico.
- Per visualizzare tutti i dettagli relativi a un endpoint specifico, inclusi i metadati del certificato, selezionare il nome dell'endpoint nella tabella. Le informazioni visualizzate variano a seconda del tipo di endpoint e della sua configurazione.

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 Endpoints del bilanciamento del carico.



Se si perde l'accesso a Grid Manager durante la modifica della porta di un endpoint dell'interfaccia di gestione, aggiornare l'URL e la porta per riottenere l'accesso.



Dopo aver modificato un endpoint, potrebbe essere necessario attendere fino a 15 minuti per applicare le modifiche a tutti i nodi.

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni > Modifica nome endpoint. c. Inserire il nuovo nome. d. Selezionare Salva.	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Seleziona l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare Salva.
Modificare la porta dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni > Modifica porta endpoint c. Immettere un numero di porta valido. d. Selezionare Salva.	n/a
Modificare la modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni > Modifica modalità di associazione endpoint. c. Aggiornare la modalità di binding secondo necessità. d. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare Edit binding mode (Modifica modalità di associazione). c. Aggiornare la modalità di binding secondo necessità. d. Selezionare Save Changes (Salva modifiche).
Modificare il certificato dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni > Modifica certificato endpoint. c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato S3 globale, come richiesto. d. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda certificato. c. Selezionare Modifica certificato. d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato S3 globale, come richiesto. e. Selezionare Save Changes (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare l'accesso al tenant	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare azioni > Modifica accesso tenant . c. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. d. Selezionare Save Changes (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda accesso tenant . c. Selezionare Edit tenant access (Modifica accesso tenant). d. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. e. Selezionare Save Changes (Salva modifiche).

Rimuovere gli endpoint del bilanciamento del carico

È possibile rimuovere uno o più endpoint dal menu **azioni** oppure rimuovere un singolo endpoint dalla pagina dei dettagli.



Per evitare interruzioni dei client, aggiornare le applicazioni client S3 interessate prima di rimuovere un endpoint del bilanciamento del carico. Aggiornare ogni client per la connessione utilizzando una porta assegnata a un altro endpoint del bilanciamento del carico. Assicurarsi di aggiornare anche tutte le informazioni di certificato richieste.



Se si perde l'accesso a Grid Manager durante la rimozione di un endpoint dell'interfaccia di gestione, aggiornare l'URL.

- Per rimuovere uno o più endpoint:
 - Dalla pagina bilanciamento del carico, selezionare la casella di controllo per ciascun endpoint che si desidera rimuovere.
 - Selezionare **azioni > Rimuovi**.
 - Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
 - Dalla pagina bilanciamento del carico, selezionare il nome del punto finale.
 - Selezionare **Rimuovi** nella pagina dei dettagli.
 - Selezionare **OK**.

Configura i nomi di dominio degli endpoint S3 in StorageGRID

Per supportare le richieste in stile virtual-hosted S3, è necessario utilizzare Grid Manager per configurare l'elenco dei nomi di dominio degli endpoint S3 a cui si connettono i client S3.



L'utilizzo di un indirizzo IP per un nome di dominio endpoint non è supportato. Le versioni future impediranno questa configurazione.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Hai confermato che non è in corso un aggiornamento della griglia.



Non apportare modifiche alla configurazione del nome di dominio quando è in corso un aggiornamento della griglia.

A proposito di questa attività

Per consentire ai client di utilizzare i nomi di dominio degli endpoint S3, è necessario eseguire tutte le seguenti operazioni:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Verificare che la ["Certificato utilizzato dal client per le connessioni HTTPS a StorageGRID"](#) sia firmata per tutti i nomi di dominio richiesti dal client.

Ad esempio, se l'endpoint è `s3.company.com`, è necessario assicurarsi che il certificato utilizzato per le connessioni HTTPS includa l'`s3.company.com`endpoint` e il nome alternativo (SAN) dell'oggetto con caratteri jolly dell'endpoint: `*.s3.company.com`.

- Configurare il server DNS utilizzato dal client. Includere i record DNS per gli indirizzi IP utilizzati dai client per effettuare le connessioni e assicurarsi che i record riferiscano a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi i nomi con caratteri jolly.



I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo gateway, di un nodo amministratore o di un nodo di storage oppure connettendosi all'indirizzo IP virtuale di un gruppo ad alta disponibilità. È necessario comprendere il modo in cui le applicazioni client si connettono alla griglia in modo da includere gli indirizzi IP corretti nei record DNS.

I client che utilizzano connessioni HTTPS (consigliate) alla griglia possono utilizzare uno dei seguenti certificati:

- I client che si connettono a un endpoint di bilanciamento del carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciamento del carico può essere configurato per riconoscere diversi nomi di dominio degli endpoint S3.
- I client che si connettono a un endpoint del bilanciamento del carico o direttamente a un nodo di storage possono personalizzare il certificato API S3 globale in modo da includere tutti i nomi di dominio degli endpoint S3 richiesti.



Se non si aggiungono nomi di dominio degli endpoint S3 e l'elenco è vuoto, il supporto per le richieste in stile virtual-hosted S3 viene disattivato.

Aggiungere un nome di dominio dell'endpoint S3

Fasi

1. Selezionare **Configurazione > Rete > Nomi di dominio endpoint S3**.

2. Inserire il nome di dominio nel campo **Domain name 1**. Selezionare **Aggiungi un altro nome di dominio** per aggiungere altri nomi di dominio.
3. Selezionare **Salva**.
4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint S3 richiesti.
 - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza un proprio certificato, ["aggiornare il certificato associato all'endpoint"](#).
 - Se i client si connettono a un endpoint di bilanciamento 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 dei nomi di dominio degli endpoint possano essere risolte.

Risultato

Ora, quando i client utilizzano l'endpoint `bucket.s3.company.com`, il server DNS risolve l'endpoint corretto e il certificato autentica l'endpoint come previsto.

Rinominare un nome di dominio endpoint S3

Se si modifica un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

Fasi

1. Selezionare **Configurazione > Rete > Nomi di dominio endpoint S3**.
2. Selezionare il campo del nome di dominio che si desidera modificare e apportare le modifiche necessarie.
3. Selezionare **Salva**.
4. Selezionare **Sì** per confermare la modifica.

Eliminare un nome di dominio dell'endpoint S3

Se si rimuove un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

Fasi

1. Selezionare **Configurazione > Rete > Nomi di dominio endpoint S3**.
2. Seleziona l'icona di eliminazione  accanto al domain name.
3. Selezionare **Sì** per confermare l'eliminazione.

Informazioni correlate

- ["UTILIZZARE L'API REST S3"](#)
- ["Visualizzare gli indirizzi IP"](#)
- ["Configurare i gruppi ad alta disponibilità"](#)

Indirizzi IP e porte per le connessioni client StorageGRID

Per memorizzare o recuperare oggetti, le applicazioni client S3 si connettono al servizio Load Balancer, incluso in tutti i nodi Admin e Gateway, o al servizio Local Distribution Router (LDR), incluso in tutti i nodi Storage.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta del servizio su tale nodo. Facoltativamente, è possibile creare gruppi ad alta disponibilità (ha) di nodi di bilanciamento del carico per fornire connessioni ad alta disponibilità che utilizzano indirizzi IP virtuali (VIP). Se si desidera connettersi a StorageGRID utilizzando un nome di dominio completo (FQDN) invece di un indirizzo IP o VIP, è possibile configurare le voci DNS.

Questa tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Se sono già stati creati endpoint di bilanciamento del carico e gruppi ha (High Availability), vedere [Dove trovare gli indirizzi IP](#) per individuare questi valori in Grid Manager.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	Porta assegnata all'endpoint del bilanciamento del carico
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	Porta assegnata all'endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	Porta assegnata all'endpoint del bilanciamento del carico
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084

URL di esempio

Per connettere un'applicazione client all'endpoint Load Balancer di un gruppo ha di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

```
https://VIP-of-HA-group:LB-endpoint-port
```

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.5 e il numero di porta dell'endpoint del bilanciamento del carico è 10443, un'applicazione potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

```
https://192.0.2.5:10443
```

Dove trovare gli indirizzi IP

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Per trovare l'indirizzo IP di un nodo Grid:
 - a. Selezionare **Nodi**.
 - b. Selezionare il nodo Admin, il nodo gateway o il nodo di storage a cui si desidera connettersi.
 - c. Selezionare la scheda **Panoramica**.

- d. Nella sezione Node Information (informazioni sul nodo), annotare gli indirizzi IP del nodo.
- e. Selezionare **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature dell'interfaccia.

È possibile stabilire connessioni dalle applicazioni client a uno qualsiasi degli indirizzi IP presenti nell'elenco:

- **Eth0:** Grid Network
- **Eth1:** Admin Network (opzionale)
- **Eth2:** rete client (opzionale)



Se si sta visualizzando un nodo Admin o un nodo Gateway e si tratta del nodo attivo di un gruppo ad alta disponibilità, l'indirizzo IP virtuale del gruppo ha viene visualizzato su eth2.

3. Per trovare l'indirizzo IP virtuale di un gruppo ad alta disponibilità:
 - a. Selezionare **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 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, poiché tali porte sono riservate sui nodi Admin. Tutte le altre porte sono configurate sia sui nodi Gateway che sui nodi Admin.

- c. Selezionare il nome dell'endpoint dalla tabella.
- d. Verificare che il tipo **Client** (S3) corrisponda all'applicazione client che utilizzerà l'endpoint.

Gestire reti e connessioni

Configura le impostazioni di rete di StorageGRID

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

Configurare le interfacce VLAN

Puoi "[Creare interfacce LAN virtuale \(VLAN\)](#)" isolare e dividere il traffico per ragioni di sicurezza, flessibilità e prestazioni. Ogni interfaccia VLAN è associata a una o più interfacce principali sui nodi Admin e Gateway. È possibile utilizzare le interfacce VLAN nei gruppi ha e negli endpoint del bilanciamento del carico per separare il traffico client o amministrativo in base all'applicazione o al tenant.

Policy di classificazione del traffico

È possibile utilizzare "[policy di classificazione del traffico](#)" per identificare e gestire diversi tipi di traffico di rete, incluso il traffico correlato a bucket, tenant, subnet client o endpoint di bilanciamento del carico specifici. Queste policy possono essere utili per la limitazione e il monitoraggio del traffico.

Linee guida per le reti StorageGRID

È possibile utilizzare Grid Manager per configurare e gestire le reti e le connessioni StorageGRID.

Vedere ["Configurare connessioni client S3"](#) per informazioni su come connettere client S3.

Reti StorageGRID predefinite

Per impostazione predefinita, StorageGRID supporta tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per ulteriori informazioni sulla topologia di rete, vedere ["Linee guida per il networking"](#).

Grid Network

Obbligatorio. La rete griglia viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della rete, in tutti i siti e le subnet.

Admin Network (rete amministrativa)

Opzionale. La rete di amministrazione viene generalmente utilizzata per l'amministrazione e la manutenzione del sistema. Può essere utilizzato anche per l'accesso al protocollo client. La rete di amministrazione è in genere una rete privata e non deve essere instradabile tra i siti.

Rete client

Opzionale. La rete client è una rete aperta generalmente utilizzata per fornire l'accesso alle applicazioni client S3, in modo che la rete grid possa essere isolata e protetta. La rete client può comunicare con qualsiasi subnet raggiungibile tramite il gateway locale.

Linee guida

- Ogni nodo StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ogni rete a cui è assegnato.
- Un nodo Grid non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway, per rete, per nodo di rete, che deve trovarsi sulla stessa sottorete del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ciascun nodo, ogni rete viene mappata a una specifica interfaccia di rete.

Rete	Nome dell'interfaccia
Griglia	eth0
Admin (opzionale)	eth1
Client (opzionale)	eth2

- Se il nodo è collegato a un'appliance StorageGRID, vengono utilizzate porte specifiche per ciascuna rete. Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è attivato, 0.0.0.0/0 utilizza la

rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza Grid Network su eth0.

- La rete client non diventa operativa fino a quando il nodo grid non si è Unito alla griglia
- La rete amministrativa può essere configurata durante l'implementazione del nodo grid per consentire l'accesso all'interfaccia utente dell'installazione prima che la griglia sia completamente installata.

Interfacce opzionali

In alternativa, è possibile aggiungere interfacce aggiuntive a un nodo. Ad esempio, è possibile aggiungere un'interfaccia trunk a un nodo Admin o Gateway, in modo da ["Interfacce VLAN"](#) separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un ["Gruppo ad alta disponibilità \(ha\)"](#).

Per aggiungere trunk o interfacce di accesso, vedere quanto segue:

- **VMware (dopo l'installazione del nodo):** ["VMware: Aggiunta di interfacce di accesso o trunk a un nodo"](#)
 - **Linux (prima di installare il nodo):** ["Creare file di configurazione del nodo"](#)
 - **Linux (dopo aver installato il nodo):** ["Aggiungere interfacce trunk o di accesso a un nodo"](#)



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Visualizza gli indirizzi IP in StorageGRID

È possibile visualizzare l'indirizzo IP di ciascun nodo della griglia nel sistema StorageGRID. È quindi possibile utilizzare questo indirizzo IP per accedere al nodo Grid dalla riga di comando ed eseguire varie procedure di manutenzione.

Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

Per informazioni sulla modifica degli indirizzi IP, vedere ["Configurare gli indirizzi IP"](#).

Fasi

1. Selezionare **Nodi** > **nodo griglia** > **Panoramica**.
2. Selezionare **Mostra altri** a destra del titolo indirizzi IP.

Gli indirizzi IP per il 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.			

Configura le interfacce VLAN in StorageGRID

Crea interfacce LAN virtuali (VLAN) sui nodi di amministrazione e sui nodi gateway e utilizzale 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 per le interfacce VLAN

- Per creare un'interfaccia VLAN, immettere un ID VLAN e scegliere un'interfaccia principale su uno o più nodi.

- Un'interfaccia principale deve essere configurata come interfaccia di linea sullo switch.
- Un'interfaccia padre può essere Grid Network (eth0), Client Network (eth2) o un'interfaccia trunk aggiuntiva per la macchina virtuale o l'host bare-metal (ad esempio, ens256).
- Per ogni interfaccia VLAN, è possibile selezionare solo un'interfaccia principale per un nodo specifico. Ad esempio, non è possibile utilizzare l'interfaccia Grid Network e l'interfaccia Client Network sullo stesso nodo gateway dell'interfaccia principale per la stessa VLAN.
- Se l'interfaccia VLAN è per il traffico Admin Node, che include il traffico correlato a Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se l'interfaccia VLAN è per il traffico client S3, selezionare interfacce su nodi Admin o nodi Gateway.
- Per ulteriori informazioni sull'aggiunta di interfacce di linea, consultare quanto segue:
 - **VMware (dopo l'installazione del nodo):** ["VMware: Aggiunta di interfacce di accesso o trunk a un nodo"](#)
 - **Linux (prima di installare il nodo):** ["Creare file di configurazione del nodo"](#)
 - **Linux (dopo aver installato il nodo):** ["Aggiungere interfacce trunk o di accesso a un nodo"](#)



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Creare un'interfaccia VLAN

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- Un'interfaccia di linea è stata configurata nella rete e collegata al nodo VM o Linux. Si conosce il nome dell'interfaccia di linea.
- Si conosce l'ID della VLAN che si sta configurando.

A proposito di questa attività

L'amministratore di rete potrebbe aver configurato una o più interfacce di trunk e una o più VLAN per separare il traffico client o amministrativo che appartiene a diverse applicazioni o tenant. Ogni VLAN è identificata da un ID numerico o da un tag. Ad esempio, la rete potrebbe utilizzare la VLAN 100 per il traffico FabricPool e la VLAN 200 per un'applicazione di archiviazione.

È possibile utilizzare Grid Manager per creare interfacce VLAN che consentono ai client di accedere a StorageGRID su una VLAN specifica. Quando si creano interfacce VLAN, specificare l'ID VLAN e selezionare le interfacce principali (trunk) su uno o più nodi.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione > Rete > Interfacce VLAN**.
2. Selezionare **Crea**.

Inserire i dettagli delle interfacce VLAN

Fasi

1. Specificare l'ID della VLAN nella rete. È possibile immettere un valore compreso tra 1 e 4094.

Gli ID VLAN non devono essere univoci. Ad esempio, è possibile utilizzare l'ID VLAN 200 per il traffico amministrativo in un sito e lo stesso ID VLAN per il traffico client in un altro sito. È possibile creare interfacce VLAN separate con diversi set di interfacce padre in ogni sito. Tuttavia, due interfacce VLAN con lo stesso ID non possono condividere la stessa interfaccia su un nodo. Se si specifica un ID già utilizzato, viene visualizzato un messaggio.

2. Facoltativamente, inserire una breve descrizione per l'interfaccia VLAN.
3. Selezionare **continua**.

Scegliere le interfacce padre

La tabella elenca le interfacce disponibili per tutti i nodi Admin e Gateway in ogni sito della griglia. Le interfacce Admin Network (eth1) non possono essere utilizzate come interfacce padre e non vengono visualizzate.

Fasi

1. Selezionare una o più interfacce padre a cui collegare questa VLAN.

Ad esempio, è possibile collegare una VLAN all'interfaccia di rete client (eth2) per un nodo gateway e un nodo amministratore.

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**.

Confermare le impostazioni

Fasi

1. Esaminare la configurazione e apportare eventuali modifiche.
 - Se è necessario modificare l'ID o la descrizione della VLAN, selezionare **Enter VLAN details** (Inserisci dettagli VLAN) nella parte superiore della pagina.
 - Per modificare un'interfaccia padre, selezionare **Choose parent interfaces** (Scegli interfacce padre)

nella parte superiore della pagina oppure selezionare **Previous** (precedente).

- Se devi rimuovere un'interfaccia padre, seleziona l'icona del cestino .

2. Selezionare **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**).

Modificare un'interfaccia VLAN

Quando si modifica un'interfaccia VLAN, è possibile apportare i seguenti tipi di modifiche:

- Modificare l'ID o la descrizione della VLAN.
- Aggiungere o rimuovere interfacce padre.

Ad esempio, se si intende decommissionare il nodo associato, è possibile rimuovere un'interfaccia principale da un'interfaccia VLAN.

Tenere presente quanto segue:

- Non è possibile modificare un ID VLAN se l'interfaccia VLAN viene utilizzata in un gruppo ha.
- Non è possibile rimuovere un'interfaccia padre se tale interfaccia padre è utilizzata in un gruppo ha.

Ad esempio, si supponga che la VLAN 200 sia collegata alle interfacce padre sui nodi A e B. se un gruppo ha utilizza l'interfaccia VLAN 200 per il nodo A e l'interfaccia eth2 per il nodo B, è possibile rimuovere l'interfaccia padre non utilizzata per il nodo B, ma non è possibile rimuovere l'interfaccia padre utilizzata per il nodo A.

Fasi

1. Selezionare **Configurazione > Rete > Interfacce VLAN**.
2. Selezionare la casella di controllo dell'interfaccia VLAN che si desidera modificare. Quindi, selezionare **azioni > Modifica**.
3. Facoltativamente, aggiornare l'ID VLAN o la descrizione. Quindi, selezionare **continua**.

Non è possibile aggiornare un ID VLAN se la VLAN viene utilizzata in un gruppo ha.

4. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere interfacce padre o per rimuovere interfacce inutilizzate. Quindi, selezionare **continua**.
5. Esaminare la configurazione e apportare eventuali modifiche.
6. Selezionare **Salva**.

Rimuovere un'interfaccia VLAN

È possibile rimuovere una o più interfacce VLAN.

Non è possibile rimuovere un'interfaccia VLAN se è attualmente utilizzata in un gruppo ha. È necessario rimuovere l'interfaccia VLAN dal gruppo ha prima di poterla rimuovere.

Per evitare interruzioni del traffico client, è consigliabile eseguire una delle seguenti operazioni:

- Aggiungere una nuova interfaccia VLAN al gruppo ha prima di rimuovere questa interfaccia VLAN.

- Creare un nuovo gruppo ha che non utilizzi questa interfaccia VLAN.
- Se l'interfaccia VLAN che si desidera rimuovere è attualmente attiva, modificare il gruppo ha. Spostare l'interfaccia VLAN che si desidera rimuovere in fondo all'elenco delle priorità. Attendere che la comunicazione venga stabilita sulla nuova interfaccia principale, quindi rimuovere la vecchia interfaccia dal gruppo ha. Infine, eliminare l'interfaccia VLAN su quel nodo.

Fasi

1. Selezionare **Configurazione > Rete > Interfacce VLAN**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, selezionare **azioni > Elimina**.
3. Selezionare **Sì** per confermare la selezione.

Tutte le interfacce VLAN selezionate vengono rimosse. Nella pagina delle interfacce VLAN viene visualizzato un banner verde di successo.

Abilita StorageGRID CORS per un'interfaccia di gestione

In qualità di amministratore della griglia, puoi abilitare la condivisione delle risorse tra origini (CORS) per le richieste API di gestione a StorageGRID, se desideri che i dati in StorageGRID siano accessibili tramite API di gestione a un altro dominio.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- IL ["Autorizzazione di accesso root"](#) fornisce l'accesso a tutte le richieste di configurazione CORS.

A proposito di questa attività

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 voler creare una dashboard di monitoraggio per StorageGRID nel dominio `http://www.example.com`. Abilitando CORS in StorageGRID per `http://www.example.com` e "Grid Manager", il dominio StorageGRID risponde alle richieste dell'API di gestione della griglia da `http://www.example.com`.

Richieste API di gestione (mgmt-api) con `application/json` O `multipart/formdata` richieste di Content-Type sono supportati per CORS.

Fasi

1. In Grid Manager, vai su **CONFIGURAZIONE > Rete > Impostazioni CORS dell'interfaccia di gestione**.
2. Selezionare **Grid Manager**, **Tenant Manager** o entrambe le opzioni.
 - **Grid Manager**: abilita CORS per le richieste API di gestione della griglia tra domini.
 - **Tenant Manager**: abilita CORS per le richieste API di gestione tenant tra domini.
3. Inserisci l'URL dell'altro dominio nel campo **Domini**.

Selezionare **Aggiungi un altro dominio** se si desidera abilitare CORS in StorageGRID per più di un dominio.

4. Selezionare **Salva**.

Informazioni correlate

Gestire le policy di classificazione del traffico

Politiche di classificazione del traffico in StorageGRID

I criteri di classificazione del traffico consentono di identificare e monitorare diversi tipi di traffico di rete. Queste policy possono aiutarti a limitare il traffico e a monitorarle per migliorare le tue offerte di qualità del servizio.

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio bilanciamento del carico StorageGRID per i nodi gateway e i nodi di amministrazione. Per creare criteri di classificazione del traffico, è necessario aver già creato endpoint di bilanciamento del carico.

Regole corrispondenti

Ogni policy di classificazione del traffico contiene una o più regole corrispondenti per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Bucket
- Subnet
- Tenant
- Endpoint del bilanciamento del carico

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno del criterio in base agli obiettivi della regola. Qualsiasi traffico corrispondente a qualsiasi regola di un criterio viene gestito da tale criterio. Al contrario, è possibile impostare le regole in modo che corrispondano a tutto il traffico ad eccezione di un'entità specificata.

Limitazione del traffico

In alternativa, è possibile aggiungere i seguenti tipi di limite a un criterio:

- Larghezza di banda aggregata
- Larghezza di banda per richiesta
- Richieste simultanee
- Tasso di richiesta

I valori limite vengono applicati in base al bilanciamento del carico. Se il traffico viene distribuito simultaneamente tra più bilanciatori di carico, i tassi massimi totali sono un multiplo dei limiti di velocità specificati.



È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato.

Per i limiti di larghezza di banda aggregata o per singola richiesta, le richieste vengono elaborate in entrata o in uscita alla velocità che imposti. StorageGRID può imporre una sola velocità, quindi viene applicata la corrispondenza più specifica, in base al tipo di matcher. La larghezza di banda consumata dalla richiesta non viene conteggiata rispetto ad altre policy di corrispondenza meno specifiche che contengono policy di limite di

larghezza di banda aggregata. 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.

Nel Grid Manager, puoi visualizzare i grafici del traffico e verificare che le policy stiano applicando i limiti di traffico che ti aspetti.

Utilizzare i criteri di classificazione del traffico con gli SLA

È possibile utilizzare le policy di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare gli SLA (Service-Level Agreement) che forniscono specifiche per capacità, protezione dei dati e performance.

Nell'esempio riportato di seguito vengono illustrati tre livelli di uno SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi di performance di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Massime performance consentite	Costo
Oro	1 PB di storage consentito	3 copia regola ILM	25 richieste K/sec 5 GB/sec (40 Gbps) di larghezza di banda	€ al mese
Argento	250 TB di storage consentito	2 copia regola ILM	10 richieste K/sec 1,25 GB/sec (10 Gbps) di larghezza di banda	dollari al mese
Bronzo	100 TB di storage consentito	2 copia regola ILM	5 richieste K/sec 1 GB/sec (8 Gbps) di larghezza di banda	dollari al mese

Creare criteri di classificazione del traffico StorageGRID

È possibile creare policy di classificazione del traffico se si desidera monitorare e, facoltativamente, limitare il traffico di rete per bucket, bucket regex, CIDR, endpoint del bilanciamento del carico o tenant. Facoltativamente, è possibile impostare limiti per una policy in base alla larghezza di banda, al numero di richieste simultanee o alla velocità di richiesta.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- Sono stati creati endpoint di bilanciamento del carico che si desidera associare.

- Hai creato i tenant che desideri abbinare.

Fasi

1. Selezionare **Configurazione > Rete > Classificazione del traffico**.
2. Selezionare **Crea**.
3. Inserire un nome e una descrizione (opzionale) per la policy e selezionare **continua**.

Ad esempio, descrivi a cosa si applica questa policy di classificazione del traffico e a cosa limiterà.

4. Selezionare **Aggiungi regola** e specificare i seguenti dettagli per creare una o più regole corrispondenti per il criterio. I criteri creati devono avere almeno una regola corrispondente. Selezionare **continua**.

Campo	Descrizione
Tipo	Selezionare i tipi di traffico a cui si applica la regola corrispondente. I tipi di traffico sono bucket, bucket regex, CIDR, endpoint del bilanciamento del carico e tenant.
Valore corrispondente	Inserire il valore corrispondente al tipo selezionato. • Bucket: Immettere uno o più nomi di bucket. • Secchio regex: Immettere una o più espressioni regolari utilizzate per far corrispondere un insieme di nomi di bucket. L'espressione regolare non è ancorata. USA l'ancora ^ per trovare la corrispondenza all'inizio del nome del bucket e usa l'ancora per la corrispondenza alla fine del nome. La corrispondenza delle espressioni regolari supporta un sottoinsieme della sintassi PCRE (Perl Compatible Regular Expression). • CIDR: Inserire una o più subnet IPv4, nella notazione CIDR, che corrispondono alla subnet desiderata. • Endpoint del bilanciamento del carico: Selezionare il nome di un endpoint. Questi sono gli endpoint del bilanciamento del carico definiti in "Configurare gli endpoint del bilanciamento del carico". • Tenant: Il tenant matching utilizza l'ID della chiave di accesso. Se la richiesta non contiene un ID della chiave di accesso (ad esempio, l'accesso anonimo), viene utilizzata la proprietà del bucket a cui si accede per determinare il tenant.

Campo	Descrizione
Corrispondenza inversa	Se si desidera far corrispondere tutto il traffico di rete <i>tranne</i> coerente con il valore Type and Match appena definito, selezionare la casella di controllo Inverse Match (corrispondenza inversa). In caso contrario, lasciare deselezionata la casella di controllo. Ad esempio, se si desidera applicare questo criterio a tutti gli endpoint del bilanciamento del carico tranne uno, specificare l'endpoint del bilanciamento del carico da escludere e selezionare corrispondenza inversa. Per un criterio contenente più adattatori in cui almeno uno è un adattatore inverso, fare attenzione a non creare un criterio che corrisponda a tutte le richieste.

5. Facoltativamente, selezionare **Aggiungi un limite** e selezionare i seguenti dettagli per aggiungere uno o più limiti per controllare il traffico di rete associato a una regola.



StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

Campo	Descrizione
Tipo	Il tipo di limite che si desidera applicare al traffico di rete associato alla regola. Ad esempio, è possibile limitare la larghezza di banda o il tasso di richiesta. Nota: È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. Quando la larghezza di banda aggregata è in uso, la larghezza di banda per richiesta non è disponibile. Al contrario, quando viene utilizzata la larghezza di banda per richiesta, la larghezza di banda aggregata non è disponibile. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato. Per i limiti di larghezza di banda, StorageGRID applica la policy che meglio corrisponde al tipo di limite impostato. Ad esempio, se si dispone di una policy che limita il traffico in una sola direzione, il traffico nella direzione opposta sarà illimitato, anche se il traffico corrisponde a criteri aggiuntivi con limiti di larghezza di banda. StorageGRID implementa le corrispondenze "migliori" per i limiti di larghezza di banda nel seguente ordine: • Indirizzo IP esatto (/32 mask) • Nome esatto del bucket • Regex. Bucket • Tenant • Endpoint • Corrispondenze CIDR non esatte (non /32) • Corrispondenze inverse

Campo	Descrizione
Valido per	Se questo limite si applica alle richieste di lettura del client (GET o HEAD) o alle richieste di scrittura (PUT, POST o DELETE).
Valore	Il valore a cui il traffico di rete sarà limitato, in base all'unità selezionata. Ad esempio, immettere 10 e selezionare MiB/s per impedire che il traffico di rete associato a questa regola superi i 10 MiB/s. Nota: A seconda dell'impostazione delle unità, le unità disponibili saranno binarie (ad esempio, GiB) o decimali (ad esempio, GB). Per modificare l'impostazione delle unità, selezionare l'elenco a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare User Preferences (Preferenze utente).
Unità	L'unità che descrive il valore immesso.

Ad esempio, se si desidera creare un limite di larghezza di banda di 4 GB/s per un livello SLA, creare due limiti di larghezza di banda aggregati: GET/HEAD a 4 GB/s e PUT/POST/DELETE a 4 GB/s.

6. Selezionare **continua**.
7. Leggere e rivedere la policy di classificazione del traffico. Utilizzare il pulsante **precedente** per tornare indietro e apportare le modifiche necessarie. Quando si è soddisfatti della policy, selezionare **Salva e continua**.

Il traffico client S3 viene ora gestito in base alla politica di classificazione del traffico.

Al termine

["Visualizzare le metriche del traffico di rete"](#) per verificare che i criteri applichino i limiti di traffico previsti.

Modificare una policy di classificazione del traffico StorageGRID

È possibile modificare un criterio di classificazione del traffico per modificarne il nome o la descrizione oppure per creare, modificare o eliminare eventuali regole o limiti per il criterio.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Selezionare **Configurazione > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti vengono elencati in una tabella.

2. Modificare il criterio utilizzando il menu azioni o la pagina dei dettagli. Vedere ["creare policy di classificazione del traffico"](#) per informazioni su come accedere.

Menu delle azioni

- a. Selezionare la casella di controllo per la policy.
- b. Selezionare **azioni > Modifica**.

Pagina dei dettagli

- a. Selezionare il nome del criterio.
- b. Selezionare il pulsante **Edit** (Modifica) accanto al nome del criterio.

3. Per il passo inserire il nome del criterio, modificare facoltativamente il nome o la descrizione del criterio e selezionare **continua**.
4. Per il passo Add Matching rules (Aggiungi regole di corrispondenza), aggiungere una regola o modificare **Type** e **Match value** della regola esistente, quindi selezionare **Continue** (continua).
5. Per la fase Set Limits (Imposta limiti), aggiungere, modificare o eliminare un limite e selezionare **Continue** (continua).
6. Esaminare la policy aggiornata e selezionare **Salva e continua**.

Le modifiche apportate alla policy vengono salvate e il traffico di rete viene gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Eliminare una policy di classificazione del traffico StorageGRID

È possibile eliminare una policy di classificazione del traffico se non è più necessaria. Assicurarsi di eliminare la policy corretta perché non è possibile recuperare una policy quando viene eliminata.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Selezionare **Configurazione > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Criteri di classificazione del traffico con i criteri esistenti elencati in una tabella.

2. Eliminare il criterio utilizzando il menu azioni o la pagina dei dettagli.

Menu delle azioni

- a. Selezionare la casella di controllo per la policy.
- b. Selezionare **azioni > Rimuovi**.

Pagina dei dettagli della policy

- a. Selezionare il nome del criterio.
- b. Selezionare il pulsante **Remove** accanto al nome del criterio.

3. Selezionare **Sì** per confermare che si desidera eliminare il criterio.

La policy viene eliminata.

Visualizza le metriche del traffico di rete in StorageGRID

È possibile monitorare il traffico di rete visualizzando i grafici disponibili nella pagina **Criteri di classificazione del traffico**.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Accesso root o autorizzazione account tenant"](#).

A proposito di questa attività

Per qualsiasi criterio di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio di bilanciamento del carico per determinare se il criterio limita correttamente il traffico nella rete. I dati nei grafici possono aiutare a determinare se è necessario modificare la policy.

Anche se non vengono impostati limiti per una policy di classificazione del traffico, vengono raccolte le metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Fasi

1. Selezionare **Configurazione > Rete > Classificazione del traffico**.

Viene visualizzata la pagina **Criteri di classificazione del traffico** e i criteri esistenti vengono elencati nella tabella.

2. Selezionare il nome del criterio di classificazione del traffico per il quale si desidera visualizzare le metriche.

3. Selezionare la scheda **metriche**.

Vengono visualizzati i grafici dei criteri di classificazione del traffico. I grafici visualizzano le metriche solo per il traffico corrispondente al criterio selezionato.

I grafici riportati di seguito sono inclusi nella pagina.

- **Tasso di richiesta:** Questo grafico fornisce la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori di carico. I dati ricevuti includono intestazioni di richiesta per tutte le richieste e dimensioni dei dati del corpo per le risposte che hanno dati del corpo. Inviato include le intestazioni delle risposte per tutte le richieste e le dimensioni dei dati del corpo delle risposte per le richieste che includono i dati del corpo nella risposta.



Quando le richieste sono complete, questo grafico mostra solo l'utilizzo della larghezza di banda. Per le richieste di oggetti lenti o di grandi dimensioni, la larghezza di banda istantanea effettiva potrebbe differire dai valori riportati in questo grafico.

- **Tasso di risposta agli errori:** Questo grafico fornisce una velocità approssimativa alla quale le richieste corrispondenti a questa policy restituiscono errori (codice di stato HTTP ≥ 400) ai client.
- **Durata media della richiesta (non errore):** Questo grafico fornisce una durata media delle richieste riuscite corrispondenti a questa policy.
- **Utilizzo della larghezza di banda della policy:** Questo grafico fornisce la quantità di larghezza di banda

corrispondente a questa policy gestita da tutti i bilanciatori di carico. I dati ricevuti includono intestazioni di richiesta per tutte le richieste e dimensioni dei dati del corpo per le risposte che hanno dati del corpo. Inviato include le intestazioni delle risposte per tutte le richieste e le dimensioni dei dati del corpo delle risposte per le richieste che includono i dati del corpo nella risposta.

4. Posizionare il cursore su un grafico a linee per visualizzare una finestra a comparsa di valori su una parte specifica del grafico.
5. Selezionare **Grafana dashboard** sotto il titolo metriche per visualizzare tutti i grafici di una policy. Oltre ai quattro grafici della scheda **metriche**, è possibile visualizzare altri due grafici:
 - Write request rate by object size (tasso di richiesta di scrittura per dimensione oggetto): Tasso di richieste PUT/POST/DELETE corrispondenti a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le velocità mostrate nella vista con il passaggio del mouse sono troncate in conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
 - Read request rate by object size (tasso richiesta di lettura per dimensione oggetto): Il tasso per le richieste GET/HEAD corrispondenti a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le velocità mostrate nella vista con il passaggio del mouse sono troncate in conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
6. In alternativa, è possibile accedere ai grafici dal menu **Supporto**.
 - a. Selezionare **Supporto > Strumenti > Metriche**.
 - b. Selezionare **Traffic Classification Policy** dalla sezione **Grafana**.
 - c. Selezionare il criterio dal menu in alto a sinistra della pagina.
 - d. Posizionare il cursore su un grafico per visualizzare una finestra a comparsa che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante tale periodo di tempo.

Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID delle policy sono elencati nella pagina delle policy di classificazione del traffico.
7. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Algoritmi di cifratura supportati per le connessioni TLS in uscita in StorageGRID

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni TLS (Transport Layer Security) ai sistemi esterni utilizzati per la federazione di identità e i pool di storage cloud.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3 per le connessioni a sistemi esterni utilizzati per la federazione delle identità e i pool di storage cloud.

I cifrari TLS supportati per l'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, come versioni di protocollo, crittografia, algoritmi di scambio delle chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Se hai richieste specifiche su queste impostazioni, contatta il tuo rappresentante NetApp.

Vantaggi delle connessioni HTTP attive, inattive e simultanee in StorageGRID

La modalità di configurazione delle connessioni HTTP può influire sulle prestazioni del sistema StorageGRID. Le configurazioni variano a seconda che la connessione HTTP sia attiva o inattiva o che si dispongano di più connessioni simultanee.

È possibile identificare i vantaggi in termini di prestazioni per i seguenti tipi di connessioni HTTP:

- Connessioni HTTP inattive
- Connessioni HTTP attive
- Connessioni HTTP simultanee

I vantaggi di mantenere aperte le connessioni HTTP inattive

Mantenere aperte le connessioni HTTP quando le applicazioni client sono inattive per consentire transazioni successive. Mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP aperta e inattiva per più di 10 minuti.

Le connessioni HTTP aperte e inattive offrono i seguenti vantaggi:

- Latenza ridotta dal momento in cui il sistema StorageGRID stabilisce di eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

La latenza ridotta è il vantaggio principale, in particolare per il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dei dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con i trasferimenti eseguiti in precedenza
- Notifica istantanea di diverse classi di condizioni di errore che interrompono la connettività tra l'applicazione client e il sistema StorageGRID

Decidi per quanto tempo mantenere aperta una connessione inattiva bilanciando i vantaggi dell'avvio lento e l'allocazione delle risorse.

Vantaggi delle connessioni HTTP attive

Per le connessioni dirette ai nodi di storage, è necessario limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

La determinazione della durata massima per-cui una connessione deve essere mantenuta aperta è un compromesso tra i benefici della persistenza della connessione e l'allocazione ideale della connessione alle risorse di sistema interne.

Per le connessioni client ai nodi di storage, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID.

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 questo metodo annulla i preziosi vantaggi associati alle connessioni persistenti.

- Consente alle applicazioni client di indirizzare le transazioni HTTP ai servizi LDR che dispongono di spazio disponibile.
- Consente l'avvio delle procedure di manutenzione.

Alcune procedure di manutenzione vengono avviate solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, la limitazione della durata delle connessioni aperte può essere utile per consentire l'avvio tempestivo di alcune procedure di manutenzione. Se la durata delle connessioni client non è limitata, potrebbero essere necessari alcuni minuti per terminare automaticamente le connessioni attive.

Vantaggi delle connessioni HTTP simultanee

Tenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, aumentando così le performance. Il numero ottimale di connessioni parallele dipende da diversi fattori.

Le connessioni HTTP simultanee offrono i seguenti vantaggi:

- Latenza ridotta

Le transazioni possono iniziare immediatamente invece di attendere il completamento di altre transazioni.

- Maggiore throughput

Il sistema StorageGRID può eseguire transazioni parallele e aumentare il throughput delle transazioni aggregate.

Le applicazioni client devono stabilire più connessioni HTTP. Quando un'applicazione client deve eseguire una transazione, può selezionare e utilizzare immediatamente qualsiasi connessione stabilita che non sta elaborando una transazione.

Ogni topologia del sistema StorageGRID presenta una diversa velocità di picco per transazioni e connessioni simultanee. La capacità massima di elaborazione dipende dalle risorse di elaborazione, di rete, di archiviazione, dai collegamenti WAN e dal numero di server, servizi e applicazioni supportati dal sistema StorageGRID .

I sistemi StorageGRID spesso supportano più applicazioni client. Tenetelo presente quando determinate il numero massimo di connessioni simultanee. Se l'applicazione client è composta da più entità software, ciascuna delle quali stabilisce connessioni al sistema StorageGRID , 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 supportate dal sistema.
- Le applicazioni client che interagiscono con il sistema StorageGRID su una rete con larghezza di banda limitata potrebbero dover ridurre il grado di concorrenza per garantire che le singole transazioni vengano completate in un tempo ragionevole.
- Quando molte applicazioni client condividono il sistema StorageGRID, potrebbe essere necessario ridurre

il grado di concorrenza per evitare di superare i limiti del sistema.

Separazione dei pool di connessione HTTP per le operazioni di lettura e scrittura

È possibile utilizzare pool separati di connessioni HTTP per le operazioni di lettura e scrittura e controllare la quantità di un pool da utilizzare per ciascuno di essi. I pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi dominanti dal recupero (lettura) o dominanti dal negozio (scrittura). Con pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile regolare la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

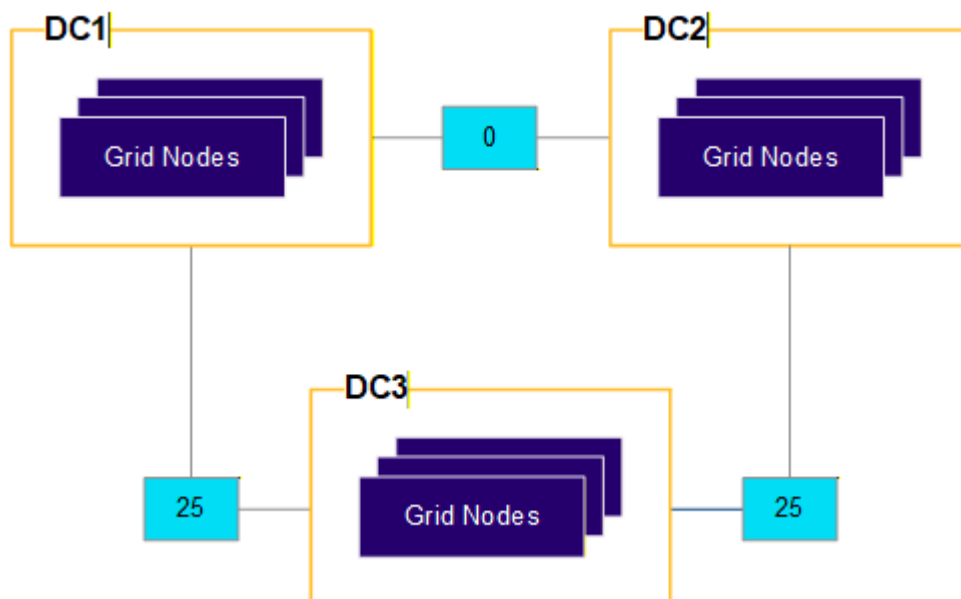
Gestisci i costi dei collegamenti in StorageGRID

I costi di collegamento consentono di assegnare la priorità al sito del data center che fornisce un servizio richiesto quando esistono due o più siti del data center. È possibile regolare i costi di collegamento in modo da riflettere la latenza tra i siti.

Quali sono i costi di collegamento?

- I costi di collegamento vengono utilizzati per assegnare la priorità alla copia oggetto utilizzata per soddisfare i recuperi di oggetti.
- I costi di collegamento vengono utilizzati dall'API di gestione del grid e dall'API di gestione del tenant per determinare i servizi StorageGRID interni da utilizzare.
- I costi di collegamento vengono utilizzati dal servizio Load Balancer sui nodi di amministrazione e sui nodi gateway per indirizzare le connessioni dei client. Consulta ["Considerazioni per il bilanciamento del carico"](#).

Il diagramma mostra una griglia a tre siti con costi di collegamento configurati tra i siti:



- Il servizio Load Balancer sui nodi Admin e Gateway distribuisce in modo uguale le connessioni client a tutti i nodi Storage nello stesso sito del data center e a qualsiasi sito del data center con un costo di collegamento pari a 0.

Nell'esempio, un nodo gateway nel sito 1 del data center (DC1) distribuisce in modo uguale le connessioni client ai nodi di storage in DC1 e ai nodi di storage in DC2. Un nodo gateway in DC3 invia le connessioni

client solo ai nodi di storage in DC3.

- Quando si recupera un oggetto che esiste come copie replicate multiple, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

Nell'esempio, se un'applicazione client in DC2 recupera un oggetto memorizzato sia in DC1 che in DC3, l'oggetto viene recuperato da DC1, poiché il costo di collegamento da DC1 a DC2 è 0, che è inferiore al costo di collegamento da DC3 a DC2 (25).

I costi di collegamento sono numeri relativi arbitrari senza unità di misura specifica. Ad esempio, un costo di collegamento di 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento di 25. La tabella mostra i costi di collegamento comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra siti fisici di data center	25 (impostazione predefinita)	Data center connessi tramite un collegamento WAN.
Tra i siti del data center logico nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus connessi da una LAN.

Aggiornare i costi dei collegamenti

È possibile aggiornare i costi di collegamento tra i siti del data center per riflettere la latenza tra i siti.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Seleziona **Supporto > Altro > Costo del collegamento**.
2. Per ogni sito elencato nella colonna Costo sito/link, inserisci un valore di costo da 0 a 100 per gli altri siti.

Non puoi modificare il costo del collegamento se l'origine è la stessa della destinazione.

3. Scarta o salva le modifiche:
 - Per annullare le modifiche, seleziona **Cancella modifiche**.
 - Per salvare le modifiche, seleziona **Salva**.

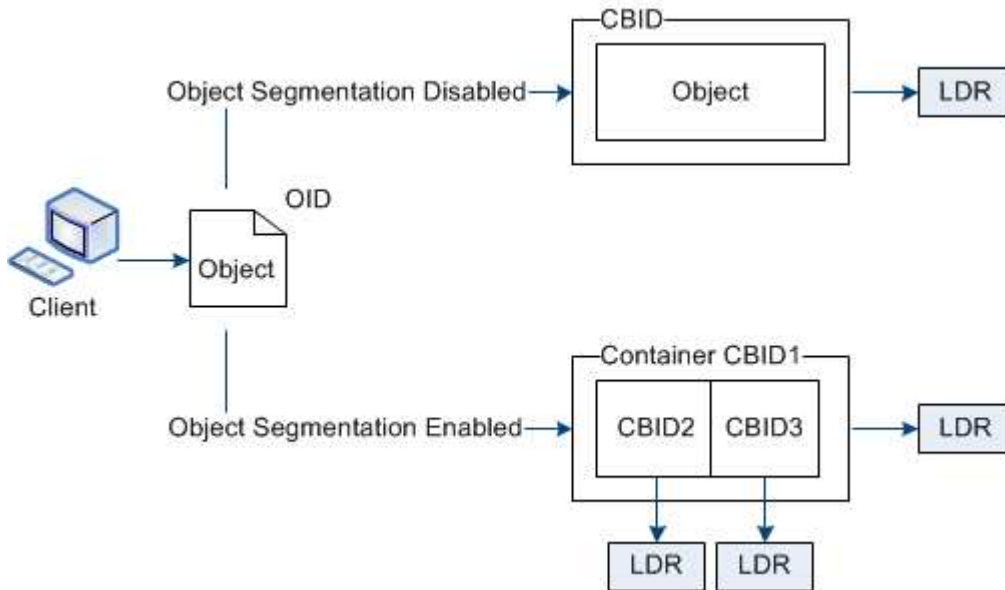
Gestire i nodi di storage

Utilizzare le opzioni di storage

Scopri la segmentazione degli oggetti in StorageGRID

La segmentazione degli oggetti è il processo di suddivisione di un oggetto in un insieme di oggetti di dimensioni fisse più piccole per ottimizzare l'utilizzo dello storage e delle risorse per oggetti di grandi dimensioni. Il caricamento multiparte S3 crea anche oggetti segmentati, con un oggetto che rappresenta ciascuna parte.

Quando un oggetto viene acquisito nel sistema StorageGRID, il servizio LDR suddivide l'oggetto in segmenti e crea un container di segmenti che elenca le informazioni di intestazione di tutti i segmenti come contenuto.



Al momento del recupero di un container di segmenti, il servizio LDR assembla l'oggetto originale dai suoi segmenti e lo restituisce al client.

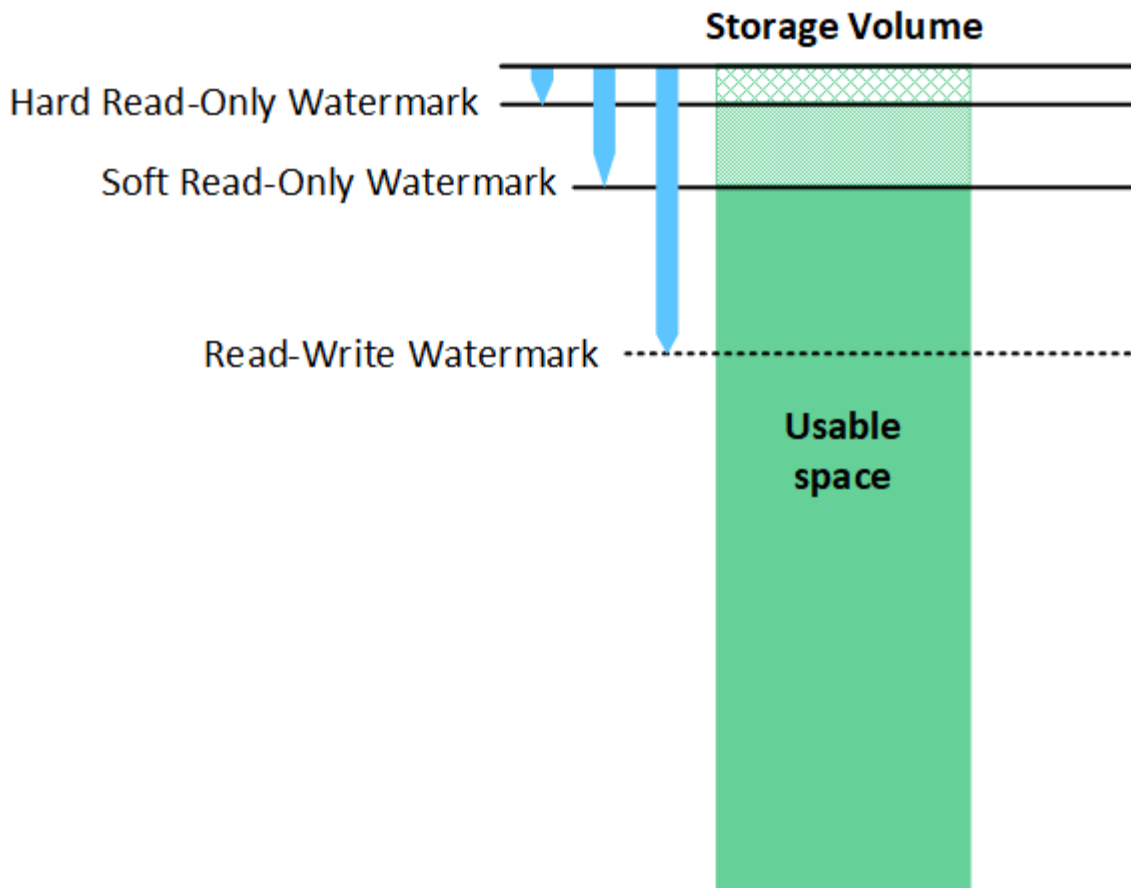
Il container e i segmenti non sono necessariamente memorizzati sullo stesso nodo di storage. Container e segmenti possono essere memorizzati in qualsiasi nodo di storage all'interno del pool di storage specificato nella regola ILM.

Ogni segmento viene trattato dal sistema StorageGRID in modo indipendente e contribuisce al conteggio di attributi come oggetti gestiti e oggetti memorizzati. Ad esempio, se un oggetto memorizzato nel sistema StorageGRID viene suddiviso in due segmenti, il valore degli oggetti gestiti aumenta di tre dopo il completamento dell'acquisizione, come segue:

segment container + segment 1 + segment 2 = three stored objects

Scopri le filigrane del volume di storage in StorageGRID

StorageGRID utilizza tre filigrane dei volumi di storage per garantire che i nodi di storage vengano trasferiti in modo sicuro in uno stato di sola lettura prima che lo spazio sia estremamente ridotto e per consentire ai nodi di storage che sono stati trasferiti in uno stato di sola lettura di tornare in lettura e scrittura.



Le filigrane dei volumi di storage si applicano solo allo spazio utilizzato per i dati degli oggetti replicati e codificati in cancellazione. Per informazioni sullo spazio riservato ai metadati degli oggetti sul volume 0, visitare il sito ["Gestire lo storage dei metadati degli oggetti"](#).

Che cos'è la filigrana morbida di sola lettura?

La filigrana di sola lettura morbida **volume di archiviazione** è la prima filigrana a indicare che lo spazio utilizzabile per i dati dell'oggetto di un nodo di archiviazione sta diventando completo.

Se ogni volume in un nodo di archiviazione ha meno spazio libero rispetto al watermark soft Read-only di quel volume, il nodo di archiviazione passa alla *modalità di sola lettura*. La modalità di sola lettura indica che il nodo di storage annuncia servizi di sola lettura al resto del sistema StorageGRID, ma soddisfa tutte le richieste di scrittura in sospeso.

Ad esempio, si supponga che ogni volume in un nodo di archiviazione abbia una filigrana di sola lettura morbida di 10 GB. Non appena ogni volume dispone di meno di 10 GB di spazio libero, il nodo di storage passa alla modalità di sola lettura.

Che cos'è la filigrana di sola lettura?

La filigrana di sola lettura rigida **volume di archiviazione** è la filigrana successiva per indicare che lo spazio utilizzabile di un nodo per i dati dell'oggetto sta diventando completo.

Se lo spazio libero su un volume è inferiore alla filigrana di sola lettura rigida di quel volume, la scrittura sul volume non riesce. Tuttavia, le scritture su altri volumi possono continuare fino a quando lo spazio libero su questi volumi non è inferiore alle filigrane di sola lettura.

Ad esempio, supponiamo che ogni volume in un nodo di archiviazione abbia un watermark di sola lettura fisso di 5 GB. Non appena ogni volume dispone di meno di 5 GB di spazio libero, Storage Node non accetta più richieste di scrittura.

La filigrana rigida di sola lettura è sempre inferiore alla filigrana morbida di sola lettura.

Che 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 diventare di nuovo in lettura/scrittura. Quando lo spazio libero su un qualsiasi volume di archiviazione in un nodo di archiviazione è maggiore del watermark di lettura-scrittura di quel volume, il nodo ritorna automaticamente allo stato di lettura-scrittura.

Ad esempio, supponiamo che il nodo di storage sia passato alla modalità di sola lettura. Si supponga inoltre che ogni volume abbia una filigrana di lettura/scrittura di 30 GB. Non appena lo spazio libero per qualsiasi volume aumenta fino a 30 GB, il nodo diventa di nuovo in lettura/scrittura.

La filigrana di sola lettura è sempre più grande della filigrana di sola lettura e della filigrana di sola lettura rigida.

Visualizzare le filigrane dei volumi di storage

È possibile visualizzare le impostazioni correnti del watermark e i valori ottimizzati per il sistema. Se non si utilizzano filigrane ottimizzate, è possibile determinare se è possibile o necessario regolare le impostazioni.

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

Consente di visualizzare le impostazioni correnti del watermark

È possibile visualizzare le impostazioni correnti del filigrana dello storage in Grid Manager.

Fasi

1. Selezionare **Supporto > Altro > Filigrane di archiviazione**.
2. Nella pagina Memorizzazione filigrane, controllare la casella di controllo utilizza valori ottimizzati.
 - Se la casella di controllo è selezionata, tutte e tre le filigrane sono ottimizzate per ogni volume di archiviazione su ogni nodo di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

Questa è l'impostazione predefinita e consigliata. Non aggiornare questi valori. Facoltativamente, è possibile [Visualizza filigrane di storage ottimizzate](#).

- Se la casella di controllo Usa valori ottimizzati non è selezionata, vengono utilizzate filigrane personalizzate (non ottimizzate). Si sconsiglia di utilizzare le impostazioni personalizzate della filigrana. Utilizzare le istruzioni di per ["Risoluzione dei problemi gli avvisi di override del watermark di sola lettura bassa"](#) determinare se è possibile o necessario regolare le impostazioni.

Quando si specificano le impostazioni personalizzate della filigrana, è necessario immettere valori superiori a 0.

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati calcolati per il watermark soft di sola lettura del volume di archiviazione. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

1. Selezionare **Supporto > Strumenti > Metriche**.
2. Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
3. Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato del watermark di sola lettura soft per tutti i volumi di archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per il watermark soft di sola lettura del volume di archiviazione, viene attivato l'avviso **low Read-only watermark override** per il nodo di archiviazione.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore massimo ottimizzato del watermark di sola lettura soft per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

Gestisci l'archiviazione dei metadati degli oggetti in StorageGRID

La capacità dei metadati degli oggetti di un sistema StorageGRID controlla il numero massimo di oggetti che possono essere memorizzati in tale sistema. Per garantire che il sistema StorageGRID disponga di spazio sufficiente per memorizzare nuovi oggetti, è necessario comprendere dove e come StorageGRID memorizza i metadati degli oggetti.

Che cos'è il metadata a oggetti?

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

Per un oggetto in StorageGRID, i metadati dell'oggetto includono i seguenti tipi di informazioni:

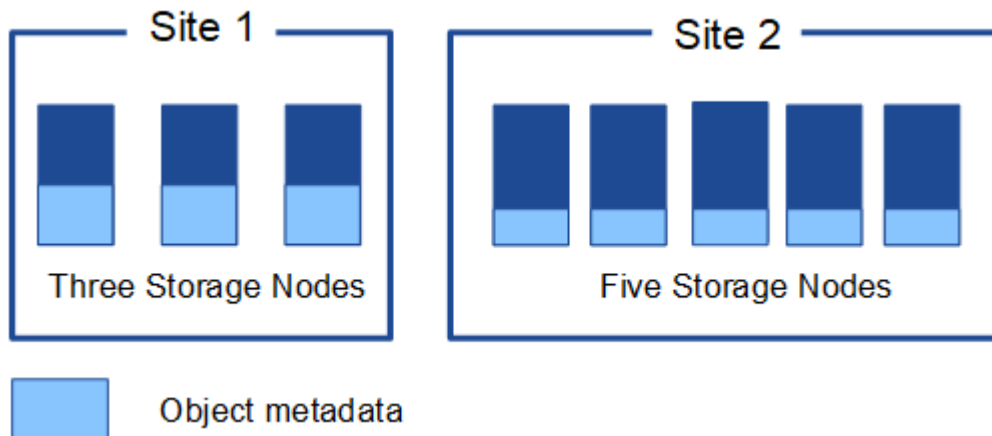
- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3, il nome o l'ID dell'account tenant, le dimensioni logiche dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.

- Per oggetti segmentati e multiparte, identificatori di segmenti e dimensioni dei dati.

Come vengono memorizzati i metadati degli oggetti?

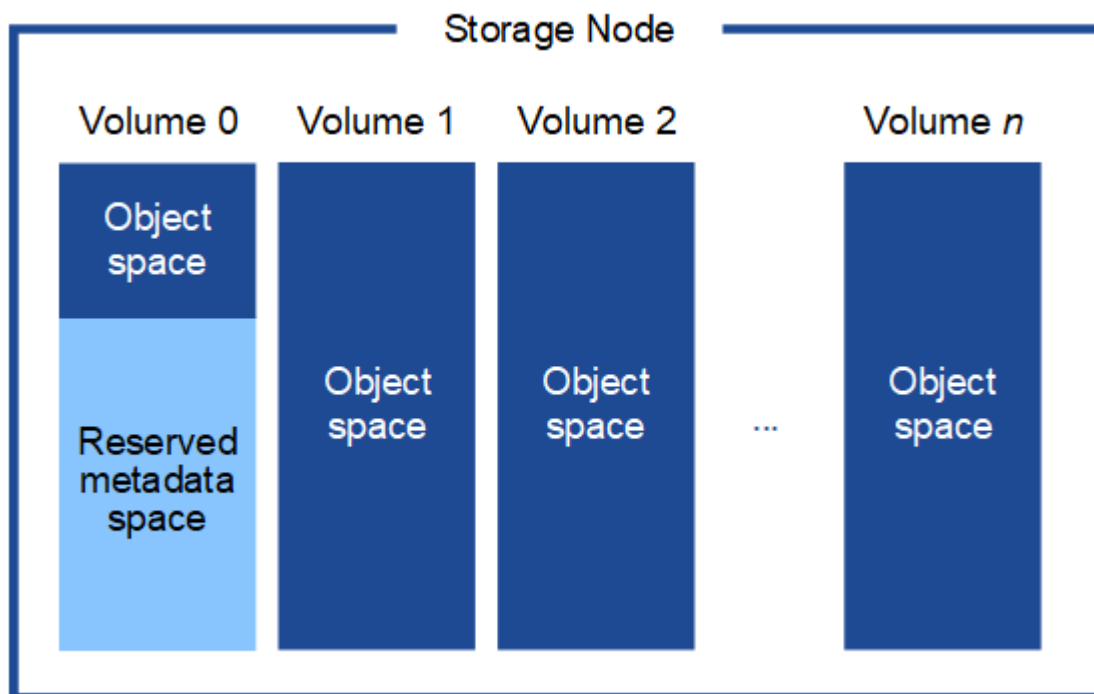
StorageGRID mantiene i metadati degli oggetti in un database Cassandra, che viene memorizzato indipendentemente dai dati degli oggetti. Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito.

Questa figura rappresenta i nodi di storage in due siti. Ogni sito ha la stessa quantità di metadati oggetto e i metadati di ciascun sito sono suddivisi tra tutti i nodi di storage di quel sito.



Dove sono memorizzati i metadati degli oggetti?

Questa figura rappresenta i volumi di storage per un singolo nodo di storage.



Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Utilizza lo spazio riservato per memorizzare i metadati degli oggetti e per eseguire le operazioni essenziali del database. Qualsiasi spazio rimanente sul volume di storage 0 e tutti gli altri volumi di storage nel nodo di storage vengono utilizzati esclusivamente per i dati a oggetti (copie replicate e frammenti

con codifica di cancellazione).

La quantità di spazio riservato ai metadati degli oggetti su un nodo di storage specifico dipende da diversi fattori, descritti di seguito.

Impostazione dello spazio riservato dei metadati

Lo *spazio riservato metadati* è un'impostazione a livello di sistema che rappresenta la quantità di spazio che sarà riservata ai metadati sul volume 0 di ogni nodo di archiviazione. Come mostrato nella tabella, il valore predefinito di questa impostazione si basa su:

- La versione software utilizzata al momento dell'installazione iniziale di StorageGRID.
- La quantità di RAM su ciascun nodo di storage.

Versione utilizzata per l'installazione iniziale di StorageGRID	Quantità di RAM sui nodi di storage	Impostazione predefinita spazio riservato metadati
12,1	128 GB o più su ciascun nodo di storage nella griglia	20 TB (20.000 GB)
	Meno di 128 GB su qualsiasi nodo di storage nel grid	3 TB (3.000 GB)
da 11,5 a 12,0	128 GB o più su ciascun nodo di storage nella griglia	8 TB (8.000 GB)
	Meno di 128 GB su qualsiasi nodo di storage nel grid	3 TB (3.000 GB)
da 11,1 a 11,4	128 GB o più su ciascun nodo di storage in un sito qualsiasi	4 TB (4.000 GB)
	Meno di 128 GB su qualsiasi nodo di storage in ogni sito	3 TB (3.000 GB)
11,0 o precedente	Qualsiasi importo	2 TB (2.000 GB)

Visualizza impostazione spazio riservato metadati

Per visualizzare l'impostazione dello spazio riservato ai metadati per il sistema StorageGRID, procedere come segue.

Fasi

1. Selezionare **Configurazione > Sistema > Impostazioni di archiviazione**.
2. Nella pagina Impostazioni archiviazione, espandere la sezione **spazio riservato metadati**.

Per StorageGRID 11,8 o versione successiva, il valore dello spazio riservato dei metadati deve essere almeno 100 GB e non più di 1 PB.

L'impostazione predefinita per una nuova installazione di StorageGRID 12.1 o superiore in cui ogni Storage

Node ha 128 GB o più di RAM è 20.000 GB (20 TB).

Spazio riservato effettivo per i metadati

A differenza dell'impostazione dello spazio riservato ai metadati a livello di sistema, per ogni nodo di archiviazione viene determinato lo *spazio riservato effettivo* per i metadati dell'oggetto. Per qualsiasi nodo di archiviazione, lo spazio riservato effettivo per i metadati dipende dalla dimensione del volume 0 per il nodo e dall'impostazione dello spazio riservato metadati a livello di sistema.

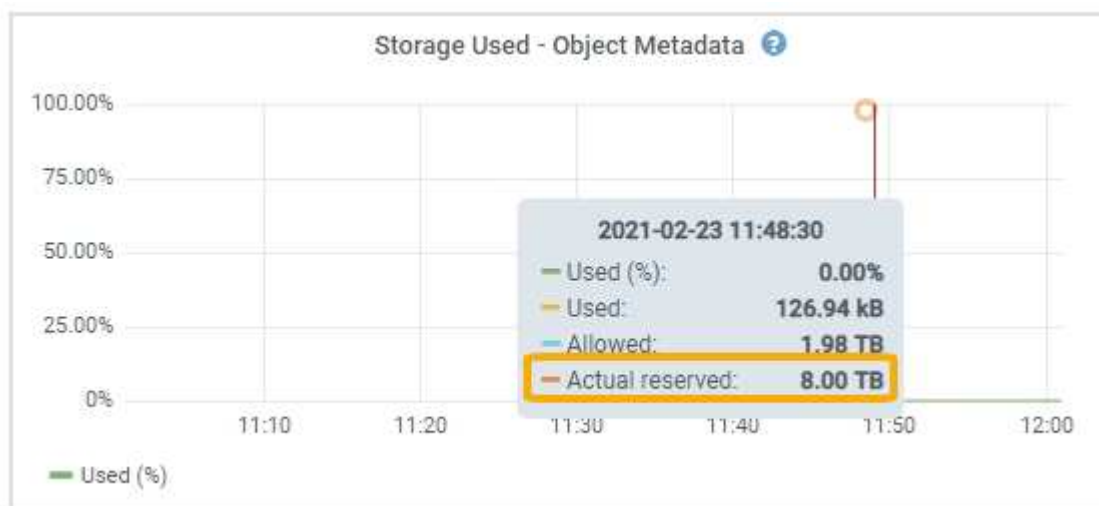
Dimensione del volume 0 per il nodo	Spazio riservato effettivo per i metadati
Meno di 500 GB (non in produzione)	10% del volume 0
500 GB o più + o + nodi di storage solo metadati	Il minore di questi valori: • Volume 0 • Impostazione dello spazio riservato dei metadati Nota: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.

Visualizzare lo spazio riservato effettivo per i metadati

Per visualizzare lo spazio riservato effettivo per i metadati su un nodo di storage specifico, procedere come segue.

Fasi

1. Da Grid Manager, seleziona **Nodi** > **Nodo di archiviazione**.
2. Selezionare la scheda **Storage**.
3. Posizionare il cursore sul grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto) e individuare il valore **Actual reserved** (riservato).



Nello screenshot, il valore effettivo riservato è 20 TB. Questo screenshot si riferisce a un grande Storage Node in una nuova installazione di StorageGRID 12.1. Il volume 0 è di almeno 20 TB, quindi utilizza l'impostazione predefinita dello spazio riservato per i metadati a livello di sistema.

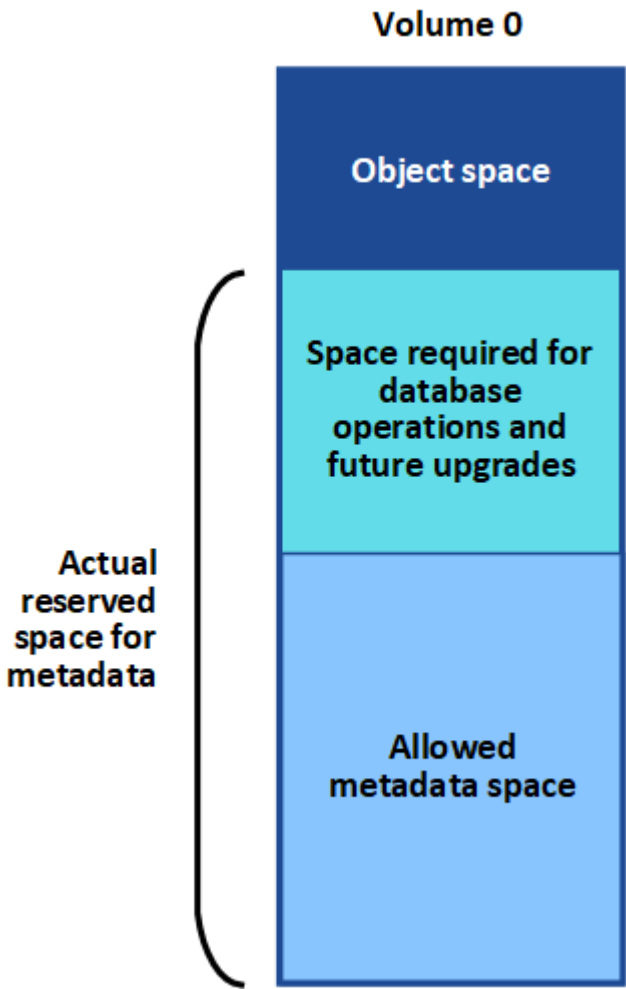
Esempio di spazio riservato effettivo per i metadati

Supponiamo che tu installi un nuovo sistema StorageGRID utilizzando la versione 12.1 o successiva. Per questo esempio, supponi che ogni Storage Node abbia più di 128 GB di RAM e che il volume 0 dello Storage Node 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo **spazio riservato ai metadati** a livello di sistema è impostato su 20 TB. (Questo è il valore predefinito per una nuova installazione di StorageGRID 12.1 o superiore se ogni Storage Node ha più di 128 GB di RAM.)
- Lo spazio **effettivamente riservato** per metadati per SN1 è 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione di **spazio riservato per metadati**.)

Spazio consentito di metadati

Lo spazio riservato effettivo di ciascun nodo di storage per i metadati viene suddiviso nello spazio disponibile per i metadati dell'oggetto (il *spazio consentito per i metadati*) e nello spazio necessario per le operazioni essenziali del database (come la compattazione e la riparazione) e per i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



La seguente tabella mostra come StorageGRID calcola lo spazio di metadati consentito* per diversi nodi di storage, in base alla quantità di memoria per il nodo e allo spazio riservato effettivo per i metadati.

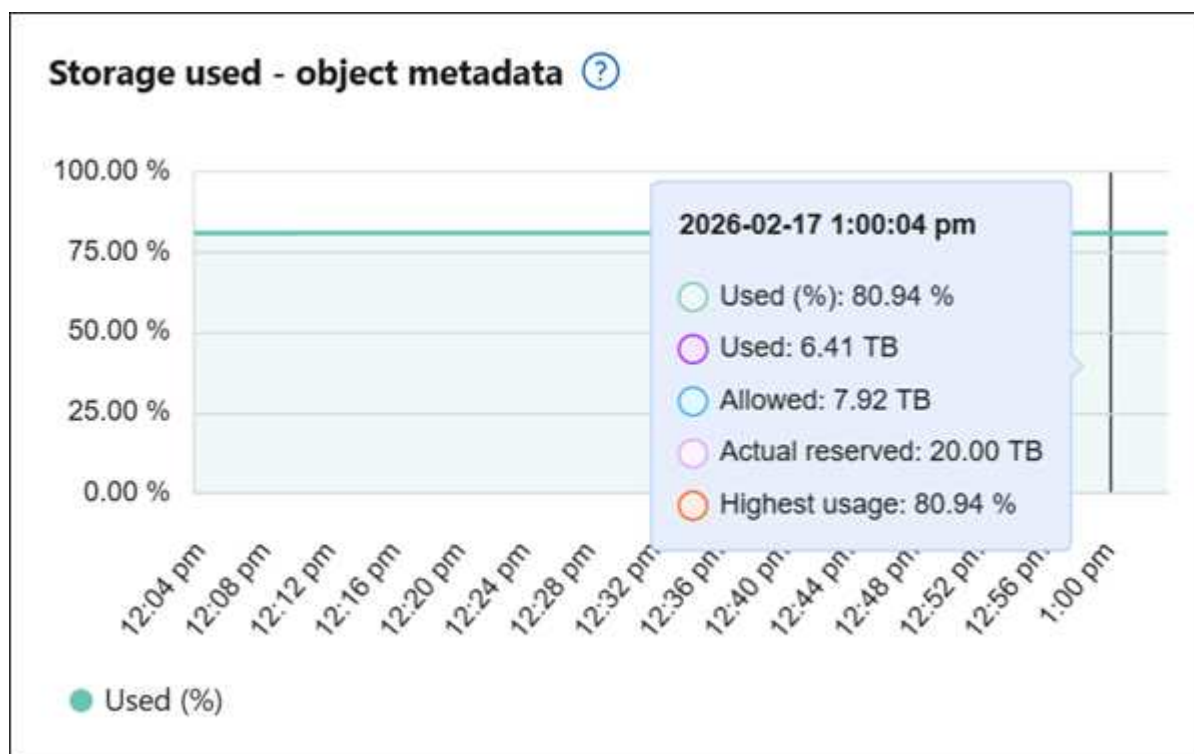
		Quantità di memoria sul nodo di storage	
	< 128 GB	>= 128 GB	Spazio riservato effettivo per i metadati
<= 4 TB	75% dello spazio riservato ai metadati, fino a un massimo di 1,32 TB	75% dello spazio riservato effettivo per i metadati, fino a un massimo di 1,98 TB	4 TB

Visualizzare lo spazio consentito per i metadati

Per visualizzare lo spazio di metadati consentito per un nodo di storage, procedere come segue.

Fasi

1. Da Grid Manager, seleziona **Nodi**.
2. Selezionare il nodo di storage.
3. Selezionare la scheda **Storage**.
4. Posizionare il cursore sul grafico dei metadati Storage used - Object e individuare il valore **Allowed**.



Nello screenshot, il valore **Allowed** è 7,92 TB, che è il valore massimo per un Storage Node il cui spazio riservato per i metadati è superiore a 4 TB.

Il valore **Allowed** corrisponde a questa metrica Prometheus:

Esempio di spazio consentito per i metadati

Supponiamo che tu installi un nuovo sistema StorageGRID utilizzando la versione 12.1 o successiva. Per questo esempio, supponi che ogni Storage Node abbia più di 128 GB di RAM e che il volume 0 dello Storage Node 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo **spazio riservato ai metadati** a livello di sistema è impostato su 20 TB. (Questo è il valore predefinito per una nuova installazione di StorageGRID 12.1 o superiore se ogni Storage Node ha più di 128 GB di RAM.)
- Lo spazio **effettivamente riservato** per metadati per SN1 è 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione di **spazio riservato per metadati**.)
- Lo spazio **consentito** per i metadati su SN1 è di 3,75 TB, in base al calcolo mostrato in [tabella per lo spazio consentito per i metadati](#): (spazio riservato per i metadati – 1 TB) × 75%, fino a un massimo di 7,92 TB.

In che modo i nodi di storage di diverse dimensioni influiscono sulla capacità degli oggetti

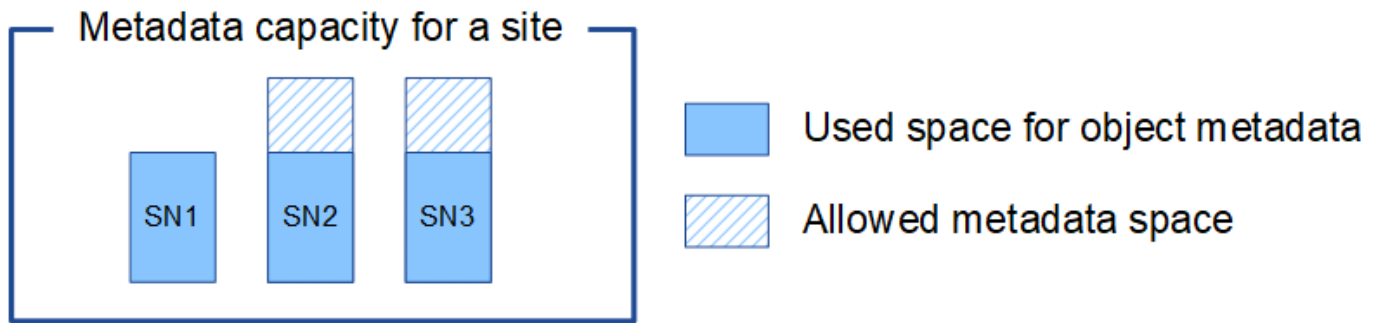
Come descritto in precedenza, StorageGRID distribuisce uniformemente i metadati degli oggetti nei nodi di storage di ciascun sito. Per questo motivo, se un sito contiene nodi di storage di dimensioni diverse, il nodo più piccolo del sito determina la capacità di metadati del sito.

Si consideri il seguente esempio:

- Si dispone di un grid a sito singolo contenente tre nodi di storage di dimensioni diverse.
- L'impostazione **spazio riservato metadati** è 4 TB.
- I nodi di storage hanno i seguenti valori per lo spazio riservato effettivo dei metadati e per lo spazio consentito dei metadati.

Nodo di storage	Dimensione del volume 0	Spazio riservato effettivo dei metadati	Spazio consentito di metadati
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Poiché i metadati degli oggetti sono distribuiti in modo uniforme tra i nodi di storage di un sito, ciascun nodo di questo esempio può contenere solo 1.32 TB di metadati. I 0.66 TB aggiuntivi di spazio consentito per i metadati SN2 e SN3 non possono essere utilizzati.



Analogamente, poiché StorageGRID gestisce tutti i metadati degli oggetti per un sistema StorageGRID in ogni sito, la capacità complessiva dei metadati di un sistema StorageGRID è determinata dalla capacità dei metadati degli oggetti del sito più piccolo.

Inoltre, poiché la capacità dei metadati degli oggetti controlla il numero massimo di oggetti, quando un nodo esaurisce la capacità dei metadati, la griglia è effettivamente piena.

Informazioni correlate

- Per informazioni su come monitorare la capacità dei metadati dell'oggetto per ogni nodo di storage, vedere le istruzioni di ["Monitoraggio di StorageGRID"](#).
- Per aumentare la capacità dei metadati degli oggetti per il tuo sistema, ["espandere una griglia"](#)aggiungendo nuovi nodi di storage.

Aumentare l'impostazione Metadata Reserved Space in StorageGRID

È possibile aumentare l'impostazione del sistema spazio riservato metadati se i nodi di archiviazione soddisfano requisiti specifici per la RAM e lo spazio disponibile.

Di cosa hai bisogno

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso root o altra autorizzazione di configurazione della griglia"](#).

A proposito di questa attività

Potrebbe essere possibile aumentare manualmente l'impostazione dello spazio riservato dei metadati a livello di sistema fino a 8 TB.

È possibile aumentare il valore dell'impostazione spazio riservato metadati a livello di sistema solo se entrambe le istruzioni sono vere:

- I nodi di storage di qualsiasi sito del sistema dispongono ciascuno di almeno 128 GB di RAM.
- I nodi di storage di qualsiasi sito del sistema dispongono ciascuno di spazio disponibile sufficiente sul volume di storage 0.

Se si aumenta questa impostazione, si riduce contemporaneamente lo spazio disponibile per lo storage a oggetti sul volume di storage 0 di tutti i nodi di storage. Per questo motivo, potrebbe essere preferibile impostare Metadata Reserved Space su un valore inferiore a 8 TB, in base ai requisiti previsti per i metadati degli oggetti.



In generale, è meglio utilizzare un valore più alto invece di un valore più basso. Se l'impostazione spazio riservato metadati è troppo grande, è possibile ridurla in un secondo momento. Al contrario, se si aumenta il valore in un secondo momento, il sistema potrebbe dover spostare i dati dell'oggetto per liberare spazio.

Per una spiegazione dettagliata del modo in cui l'impostazione spazio riservato metadati influisce sullo spazio consentito per l'archiviazione dei metadati dell'oggetto su un nodo di archiviazione specifico, vedere ["Gestire lo storage dei metadati degli oggetti"](#).

Fasi

1. Determinare l'impostazione corrente di Metadata Reserved Space.
 - a. Selezionare **Configurazione > Sistema > Impostazioni di archiviazione**.
 - b. Notare il valore di **Spazio riservato ai metadati**.
2. Assicurarsi di disporre di spazio disponibile sufficiente sul volume di storage 0 di ciascun nodo di storage per aumentare questo valore.
 - a. Selezionare **Nodi**.
 - b. Selezionare il primo nodo di storage nella griglia.
 - c. Selezionare la scheda Storage (archiviazione).
 - d. Nella sezione Volumes (volumi), individuare la voce **/var/local/rangedb/0**.
 - e. Verificare che il valore disponibile sia uguale o superiore alla differenza tra il nuovo valore che si desidera utilizzare e il valore corrente dello spazio riservato dei metadati.

Ad esempio, se l'impostazione spazio riservato metadati è attualmente di 4 TB e si desidera aumentarla a 6 TB, il valore disponibile deve essere pari o superiore a 2 TB.
 - f. Ripetere questi passaggi per tutti i nodi di storage.
 - Se uno o più nodi di storage non dispongono di spazio disponibile sufficiente, non è possibile aumentare il valore Metadata Reserved Space (spazio riservato metadati). Non continuare con questa procedura.
 - Se ogni nodo di storage dispone di spazio disponibile sufficiente sul volume 0, passare alla fase successiva.
3. Assicurarsi di disporre di almeno 128 GB di RAM su ciascun nodo di storage.
 - a. Selezionare **Nodi**.
 - b. Selezionare il primo nodo di storage nella griglia.
 - c. Selezionare la scheda **hardware**.
 - d. Posizionare il cursore del mouse sul grafico utilizzo memoria. Assicurarsi che la memoria totale sia di almeno 128 GB.
 - e. Ripetere questi passaggi per tutti i nodi di storage.
 - Se uno o più nodi di storage non dispongono di memoria totale sufficiente, non è possibile aumentare il valore Metadata Reserved Space (spazio riservato metadati). Non continuare con questa procedura.
 - Se ciascun nodo di storage dispone di almeno 128 GB di memoria totale, passare alla fase successiva.
4. Aggiornare l'impostazione Metadata Reserved Space (spazio riservato metadati).

- a. Selezionare **Configurazione > Sistema > Impostazioni di archiviazione**.
- b. Selezionare **Spazio riservato ai metadati**.
- c. Inserire il nuovo valore.

Ad esempio, per inserire 8 TB, che è il valore massimo supportato, inserire **8000000000000** (8, seguito da 12 zeri)

- d. Selezionare **Salva**.

Comprimi gli oggetti memorizzati in StorageGRID

È possibile attivare la compressione degli oggetti per ridurre le dimensioni degli oggetti memorizzati in StorageGRID, in modo che gli oggetti consumino meno spazio di storage.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

Per impostazione predefinita, la compressione degli oggetti è disattivata. Se si attiva la compressione, StorageGRID tenta di comprimere ogni oggetto durante il salvataggio, utilizzando la compressione senza perdita di dati.



Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

Prima di attivare la compressione degli oggetti, tenere presente quanto segue:

- Non selezionare **compress stored objects** a meno che non si sappia che i dati memorizzati sono comprimibili.
- Le applicazioni che salvano oggetti in StorageGRID potrebbero comprimere gli oggetti prima di salvarli. Se un'applicazione client ha già compresso un oggetto prima di salvarlo in StorageGRID, selezionando questa opzione non si ridurrà ulteriormente la dimensione di un oggetto.
- Non selezionare **compress stored objects** se si utilizza NetApp FabricPool con StorageGRID.
- Se si seleziona **compress stored objects**, le applicazioni client S3 devono evitare di eseguire operazioni GetObject che specificano un intervallo di byte da restituire. Queste operazioni di "lettura dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. Le operazioni GetObject che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client possono scadere.



Se è necessario comprimere gli oggetti e l'applicazione client deve utilizzare le letture dell'intervallo, aumentare il timeout di lettura per l'applicazione.

Fasi

1. Selezionare **Configurazione > Sistema > Impostazioni di archiviazione > Compressione oggetti**.
2. Selezionare la casella di controllo **Comprimi oggetti memorizzati**.

3. Selezionare **Salva**.

Gestisci nodi di storage completi in StorageGRID

Man mano che i nodi di storage raggiungono la capacità, è necessario espandere il sistema StorageGRID con l'aggiunta di nuovo storage. Sono disponibili tre opzioni: Aggiunta di volumi di storage, aggiunta di shelf di espansione dello storage e aggiunta di nodi di storage.

Aggiungere volumi di storage

Ciascun nodo di storage supporta un numero massimo di volumi di storage. Il valore massimo definito varia in base alla piattaforma. Se un nodo di storage contiene meno del numero massimo di volumi di storage, è possibile aggiungere volumi per aumentarne la capacità. Vedere le istruzioni per ["Espansione di un sistema StorageGRID"](#).

Aggiungere shelf di espansione dello storage

Alcuni nodi di storage delle appliance StorageGRID, come SG6060 o SG6160, sono in grado di supportare shelf di storage aggiuntivi. Se si dispone di appliance StorageGRID con funzionalità di espansione che non sono già state estese alla capacità massima, è possibile aggiungere shelf di storage per aumentare la capacità. Vedere le istruzioni per ["Espansione di un sistema StorageGRID"](#).

Aggiungere nodi storage

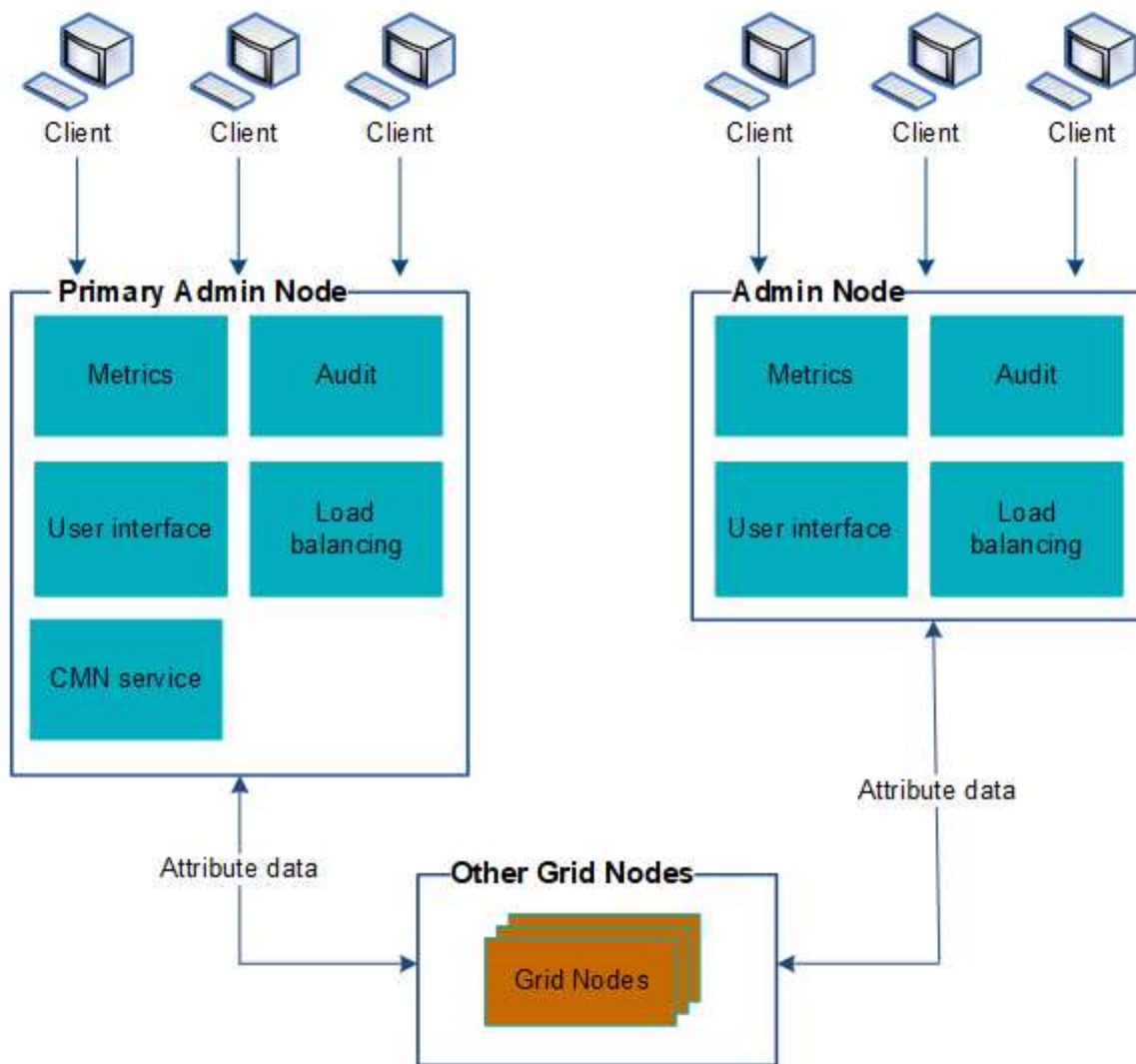
È possibile aumentare la capacità dello storage aggiungendo nodi di storage. Quando si aggiunge lo storage, è necessario prendere in considerazione le regole ILM attualmente attive e i requisiti di capacità. Vedere le istruzioni per ["Espansione di un sistema StorageGRID"](#).

Gestire i nodi di amministrazione

Utilizzare più nodi Admin in StorageGRID

Un sistema StorageGRID può includere più nodi di amministrazione per consentire di monitorare e configurare continuamente il sistema StorageGRID anche in caso di guasto di un nodo di amministrazione.

Se un nodo amministrativo non è disponibile, l'elaborazione degli attributi continua, gli avvisi vengono ancora attivati e le notifiche e-mail e i pacchetti AutoSupport vengono ancora inviati. Tuttavia, la disponibilità di più nodi amministrativi non fornisce protezione dal failover, ad eccezione delle notifiche e dei pacchetti AutoSupport.



Sono disponibili due opzioni per continuare a visualizzare e configurare il sistema StorageGRID in caso di errore di un nodo di amministrazione:

- I client Web possono riconnettersi a qualsiasi altro nodo Admin disponibile.
- Se un amministratore di sistema ha configurato un gruppo di nodi di amministrazione ad alta disponibilità, i client Web possono continuare ad accedere a Grid Manager o a Tenant Manager utilizzando l'indirizzo IP virtuale del gruppo ha. Vedere ["Gestire i gruppi ad alta disponibilità"](#).



Quando si utilizza un gruppo ha, l'accesso viene interrotto in caso di errore del nodo Admin attivo. Gli utenti devono effettuare nuovamente l'accesso dopo il failover dell'indirizzo IP virtuale del gruppo ha verso un altro nodo amministratore del gruppo.

Alcune attività di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario. In caso di guasto del nodo amministratore primario, è necessario ripristinarlo prima che il sistema StorageGRID funzioni nuovamente.

Identificare il nodo Admin primario in StorageGRID

Il nodo amministrativo primario fornisce più funzionalità rispetto ai nodi amministrativi non primari. Ad esempio, alcune procedure di manutenzione devono essere eseguite utilizzando il nodo amministrativo primario.

Per ulteriori informazioni sui nodi amministrativi, vedere ["Che cos'è un nodo amministrativo"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Fasi

1. Selezionare **Nodi**.
2. Immettere **primary** nella casella di ricerca.

Nei risultati della ricerca, identificare il nodo con "nodo amministrativo primario" visualizzato nella colonna tipo. Dovrebbe essere elencato un nodo amministrativo primario.

Gestire gli oggetti con ILM

Gestisci gli oggetti con ILM in StorageGRID

Le regole di gestione del ciclo di vita delle informazioni (ILM, Information Lifecycle Management) contenute in un criterio ILM indicano a StorageGRID come creare e distribuire copie dei dati degli oggetti e come gestirle nel tempo.

A proposito di queste istruzioni

La progettazione e l'implementazione di regole e politiche ILM richiedono un'attenta pianificazione. È necessario comprendere i requisiti operativi, la topologia del sistema StorageGRID, le esigenze di protezione degli oggetti e i tipi di storage disponibili. Quindi, è necessario determinare come si desidera copiare, distribuire e memorizzare diversi tipi di oggetti.

Seguire queste istruzioni per:

- Ulteriori informazioni su StorageGRID ILM, incluso ["Come ILM opera per tutta la vita di un oggetto"](#).
- Informazioni sulla configurazione di ["pool di storage"](#), ["Pool di cloud storage"](#) e ["Regole ILM"](#).
- Scopri come ["Creare, simulare e attivare un criterio ILM"](#) proteggere i dati degli oggetti in uno o più siti.
- Imparare come fare ["Gestire gli oggetti con S3 Object Lock"](#), che aiuta a garantire che gli oggetti in specifici bucket S3 non vengano eliminati o sovrascritti per un determinato periodo di tempo.

Scopri di più

Per ulteriori informazioni, consulta questi video:

[Panoramica delle regole ILM](#)

[Panoramica delle politiche ILM](#)

ILM e ciclo di vita degli oggetti

Come funziona ILM durante il ciclo di vita di un oggetto in StorageGRID

Comprendere come StorageGRID utilizza ILM per gestire gli oggetti in ogni fase della

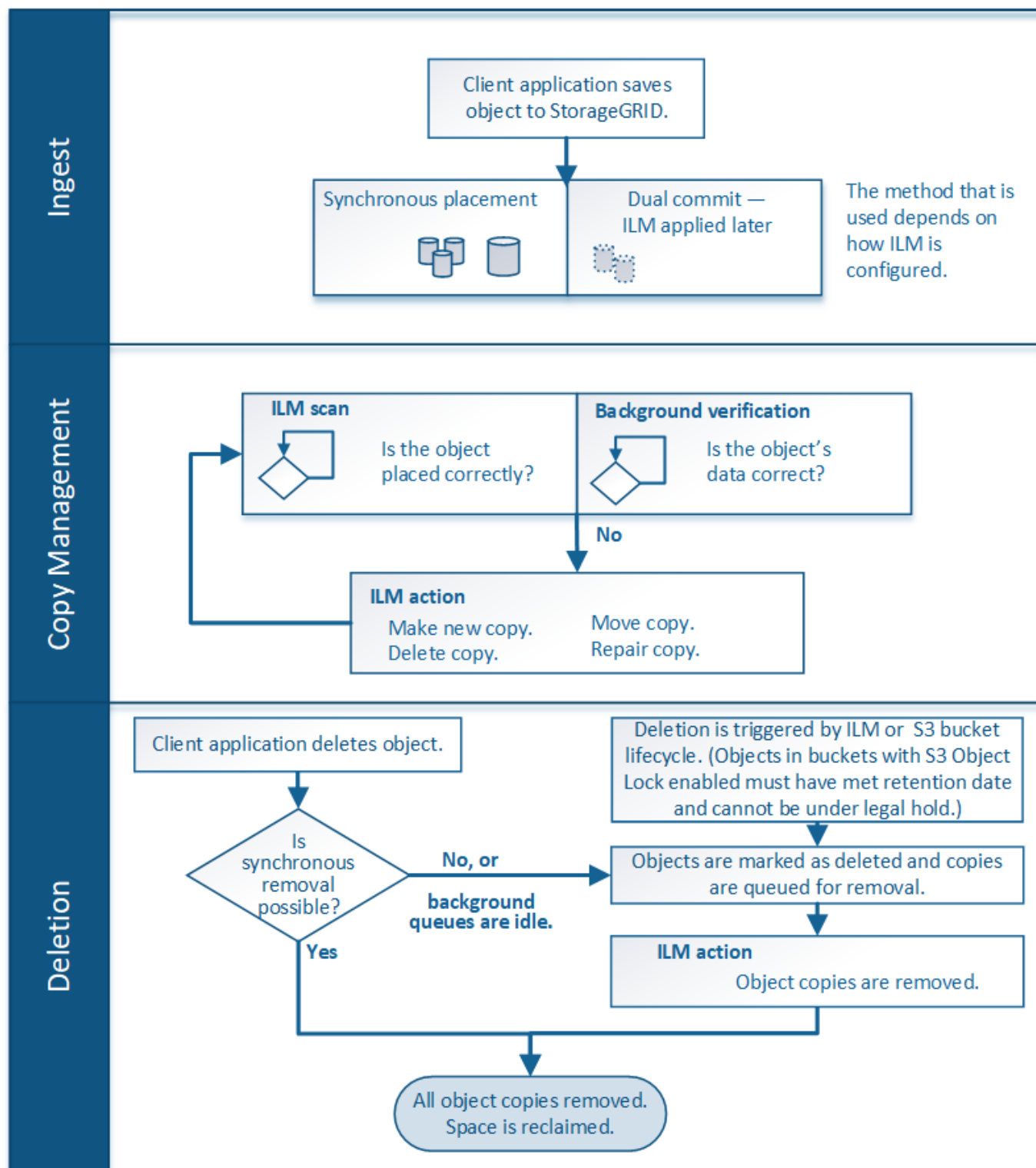
loro vita può aiutarti a progettare una policy più efficace.

- **Acquisizione:** L'acquisizione inizia quando un'applicazione client S3 stabilisce una connessione per salvare un oggetto nel sistema StorageGRID e viene completata quando StorageGRID restituisce un messaggio di acquisizione riuscita al client. I dati degli oggetti vengono protetti durante l'acquisizione applicando immediatamente le istruzioni ILM (posizionamento sincrono) o creando copie interinali e applicando ILM successivamente (doppio commit), a seconda di come sono stati specificati i requisiti ILM.
- **Gestione delle copie:** Dopo aver creato il numero e il tipo di copie degli oggetti specificati nelle istruzioni di posizionamento di ILM, StorageGRID gestisce le posizioni degli oggetti e protegge gli oggetti dalla perdita.
 - **Scansione e valutazione ILM:** StorageGRID esegue la scansione continua dell'elenco degli oggetti memorizzati nella griglia e verifica se le copie correnti soddisfano i requisiti ILM. Quando sono richiesti tipi, numeri o posizioni diversi di copie di oggetti, StorageGRID crea, elimina o sposta le copie in base alle necessità.
 - **Verifica dello sfondo:** StorageGRID esegue continuamente la verifica dello sfondo per verificare l'integrità dei dati dell'oggetto. Se viene rilevato un problema, StorageGRID crea automaticamente una nuova copia dell'oggetto o un frammento di oggetto erasure-coded sostitutivo in una posizione che soddisfa i requisiti ILM correnti. Vedere ["Verificare l'integrità dell'oggetto"](#).
- **Eliminazione oggetto:** La gestione di un oggetto termina quando tutte le copie vengono rimosse dal sistema StorageGRID. Gli oggetti possono essere rimossi in seguito a una richiesta di eliminazione da parte di un client o in seguito all'eliminazione da parte di ILM o all'eliminazione causata dalla scadenza di un ciclo di vita del bucket S3.



Gli oggetti in un bucket con S3 Object Lock abilitato non possono essere cancellati se sono in stato di conservazione legale o se è stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto.

Il diagramma riassume il funzionamento di ILM durante l'intero ciclo di vita di un oggetto.



Modalità di acquisizione degli oggetti

Opzioni di ingestione ILM in StorageGRID

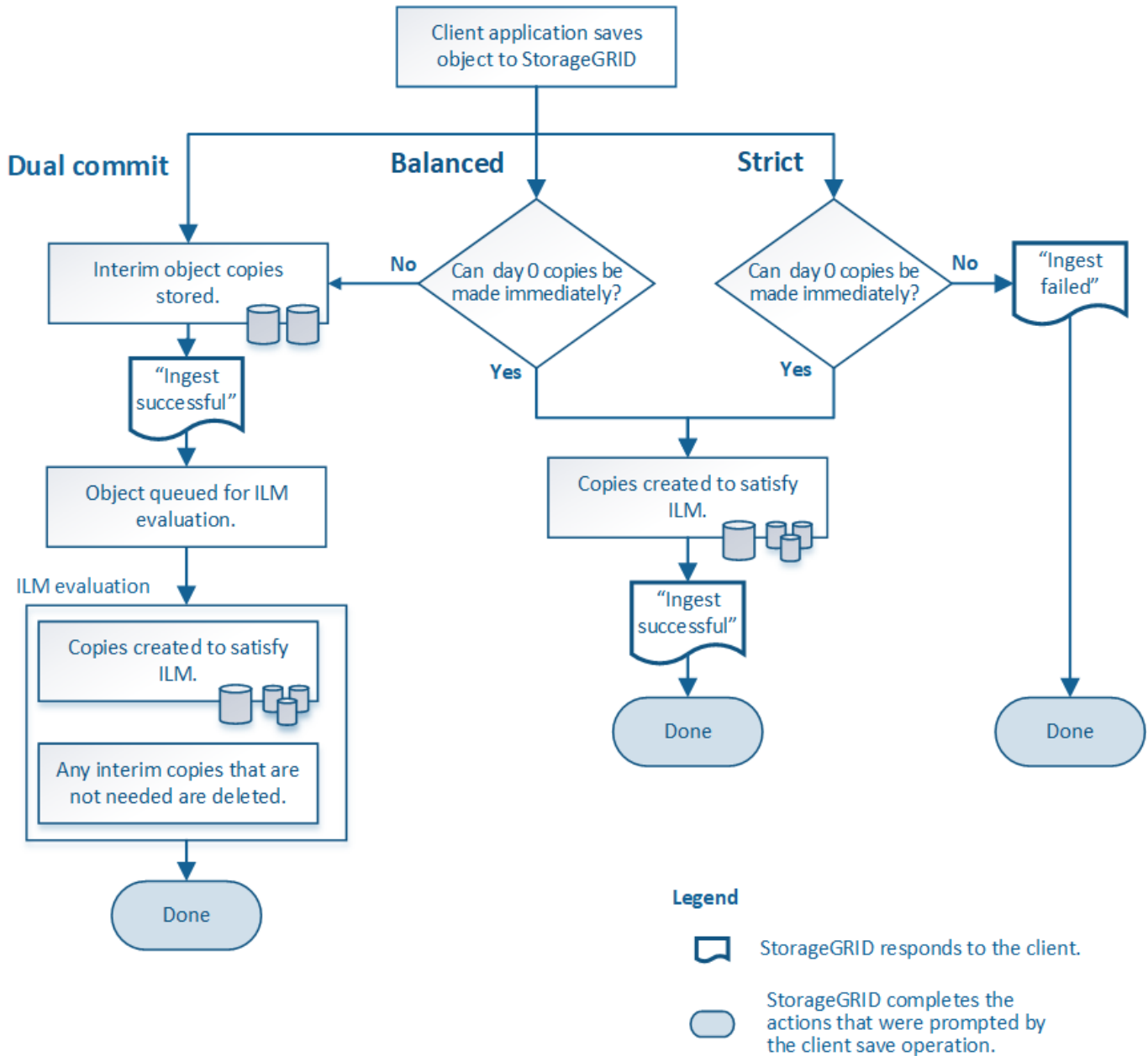
Quando si crea una regola ILM, si specifica una delle tre opzioni per la protezione degli oggetti in fase di acquisizione: Dual commit, strict o Balanced.

A seconda della scelta, StorageGRID esegue copie temporanee e mette in coda gli oggetti per la valutazione

ILM in un secondo momento, oppure utilizza il posizionamento sincrono e crea immediatamente copie per soddisfare i requisiti ILM.

Diagramma di flusso delle opzioni di acquisizione

Il diagramma di flusso mostra cosa accade quando gli oggetti vengono associati da una regola ILM che utilizza ciascuna delle tre opzioni di acquisizione.



Commit doppio

Quando si seleziona l'opzione Dual Commit, StorageGRID crea immediatamente copie temporanee degli oggetti su due diversi nodi storage e restituisce un messaggio "acquisizione riuscita" al client. L'oggetto viene messo in coda per la valutazione ILM e le copie che soddisfano le istruzioni di posizionamento della regola vengono eseguite in un secondo momento. Se il criterio ILM non può essere elaborato immediatamente dopo il dual commit, la protezione in caso di perdita del sito potrebbe richiedere del tempo.

Utilizzare l'opzione Dual Commit in uno dei seguenti casi:

- Stai utilizzando regole ILM multi-sito e la latenza di acquisizione client è la tua principale considerazione. Quando si utilizza il doppio commit, è necessario assicurarsi che la griglia possa eseguire il lavoro aggiuntivo di creazione e rimozione delle copie a doppio commit se non soddisfano ILM. In particolare:
 - Il carico sulla griglia deve essere sufficientemente basso da impedire un backlog ILM.
 - La griglia deve avere risorse hardware in eccesso (IOPS, CPU, memoria, larghezza di banda della rete e così via).
- Si stanno utilizzando regole ILM multi-sito e la connessione WAN tra i siti in genere ha una latenza elevata o una larghezza di banda limitata. In questo scenario, l'utilizzo dell'opzione di commit doppio può contribuire a prevenire i timeout del client. Prima di scegliere l'opzione Dual Commit, è necessario testare l'applicazione client con carichi di lavoro realistici.

Bilanciato (impostazione predefinita)

Quando si seleziona l'opzione Balanced (bilanciamento), StorageGRID utilizza anche il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie specificate nelle istruzioni di posizionamento della regola. In contrasto con l'opzione rigorosa, se StorageGRID non riesce immediatamente a fare tutte le copie, utilizza invece il doppio commit. Se la policy ILM utilizza posizionamenti su più siti e non è possibile ottenere una protezione immediata in caso di perdita del sito, viene attivato l'avviso **posizionamento ILM non raggiungibile**.

Utilizza l'opzione Balanced per ottenere la migliore combinazione di protezione dei dati, performance di grid e successo di acquisizione. Balanced (bilanciamento) è l'opzione predefinita nella creazione guidata regola ILM.

Rigoroso

Quando si seleziona l'opzione Strict, StorageGRID utilizza il posizionamento sincrono all'acquisizione e crea immediatamente tutte le copie degli oggetti specificate nelle istruzioni di posizionamento della regola. L'acquisizione non riesce se StorageGRID non riesce a creare tutte le copie, ad esempio perché una posizione di storage richiesta è temporaneamente non disponibile. Il client deve riprovare l'operazione.

Utilizzare l'opzione Strict se si dispone di un requisito operativo o normativo per memorizzare immediatamente gli oggetti solo nelle posizioni indicate nella regola ILM. Ad esempio, per soddisfare un requisito normativo, potrebbe essere necessario utilizzare l'opzione Strict e un filtro avanzato Location Constraint per garantire che gli oggetti non vengano mai memorizzati in determinati data center.

Vedere ["Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"](#).

Vantaggi, svantaggi e limitazioni delle opzioni di ingestione ILM in StorageGRID

Comprendere i vantaggi e gli svantaggi di ciascuna delle tre opzioni per la protezione dei dati in fase di acquisizione (Balanced, Strict o Dual Commit) può aiutare a decidere quale scegliere per una regola ILM.

Per una panoramica delle opzioni di acquisizione, vedere ["Opzioni di acquisizione"](#).

Vantaggi delle opzioni bilanciate e rigorose

Rispetto al doppio commit, che crea copie intermedie durante l'acquisizione, le due opzioni di posizionamento sincrono possono offrire i seguenti vantaggi:

- **Maggiore sicurezza dei dati:** I dati degli oggetti sono immediatamente protetti come specificato nelle istruzioni di posizionamento della regola ILM, che possono essere configurate per la protezione da un'ampia varietà di condizioni di guasto, incluso il guasto di più di una posizione di storage. Il doppio

commit può proteggere solo dalla perdita di una singola copia locale.

- **Operazione grid più efficiente:** Ogni oggetto viene elaborato una sola volta, man mano che viene acquisito. Poiché il sistema StorageGRID non deve tenere traccia o eliminare le copie temporanee, il carico di elaborazione è inferiore e lo spazio del database viene consumato meno.
- **(Balanced) Recommended (consigliato):** L'opzione Balanced (bilanciato) offre un'efficienza ILM ottimale. Si consiglia di utilizzare l'opzione Balanced (bilanciato), a meno che non sia richiesto un comportamento rigoroso di acquisizione o che la griglia soddisfi tutti i criteri per l'utilizzo di Dual Commit.
- **(Strict) certezze circa le posizioni degli oggetti:** L'opzione Strict garantisce che gli oggetti siano memorizzati immediatamente in base alle istruzioni di posizionamento nella regola ILM.

Svantaggi delle opzioni bilanciate e rigide

Rispetto al doppio commit, le opzioni bilanciate e rigide presentano alcuni svantaggi:

- **Ingest dei client più lunghi:** Le latenze di acquisizione dei client potrebbero essere più lunghe. Quando si utilizzano le opzioni bilanciate o rigorose, non viene restituito al client un messaggio di "acquisizione riuscita" finché non vengono creati e memorizzati tutti i frammenti con erasure coding o le copie replicate. Tuttavia, è molto probabile che i dati degli oggetti raggiungano il posizionamento finale molto più rapidamente.
- **(Strict) tassi più elevati di errore di acquisizione:** Con l'opzione Strict, l'acquisizione non riesce ogni volta che StorageGRID non è in grado di eseguire immediatamente tutte le copie specificate nella regola ILM. Se una posizione di storage richiesta è temporaneamente offline o se problemi di rete causano ritardi nella copia di oggetti tra siti, potrebbero verificarsi elevati tassi di errore di acquisizione.
- **(Strict) le posizioni di caricamento multiparte S3 potrebbero non essere quelle previste in alcune circostanze:** Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non funzioni. Tuttavia, con un caricamento S3 multiparte, ILM viene valutato per ogni parte dell'oggetto così come viene acquisito e per l'oggetto nel suo complesso al termine del caricamento multiparte. Nei seguenti casi, ciò potrebbe comportare posizionamenti diversi da quelli previsti:
 - **Se ILM cambia mentre è in corso un caricamento di più parti S3:** Poiché ogni parte viene posizionata in base alla regola attiva quando la parte viene inserita, alcune parti dell'oggetto potrebbero non soddisfare i requisiti ILM correnti al termine del caricamento di più parti. In questi casi, l'acquisizione dell'oggetto non ha esito negativo. Al contrario, qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.
 - **Quando le regole ILM filtrano sulla dimensione:** Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o superiori sono memorizzati in DC1 mentre tutti gli oggetti più piccoli sono memorizzati in DC2, ogni parte da 1 GB di un caricamento multiparte da 10 parti viene memorizzata in DC2. Quando ILM viene valutato per l'oggetto, tutte le parti dell'oggetto vengono spostate in DC1.
- **(Strict) Ingest non ha esito negativo quando i tag degli oggetti o i metadati vengono aggiornati e non è possibile eseguire le nuove posizioni richieste:** Con Strict, si prevede che gli oggetti vengano posizionati come descritto dalla regola ILM o che l'acquisizione non riesca. Tuttavia, quando si aggiornano metadati o tag per un oggetto già memorizzato nella griglia, l'oggetto non viene reinserito. Ciò significa che le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento non vengono apportate immediatamente. Le modifiche al posizionamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Se non è possibile apportare modifiche al posizionamento richieste (ad esempio, perché non è disponibile una nuova posizione richiesta), l'oggetto aggiornato mantiene la posizione corrente fino a quando non sono possibili modifiche al posizionamento.

Limitazioni al posizionamento degli oggetti con opzioni bilanciate e rigide

Le opzioni bilanciate o rigide non possono essere utilizzate per le regole ILM che hanno una delle seguenti istruzioni di posizionamento:

- Posizionamento in un pool di storage cloud al giorno 0.
- Posizionamenti in un Cloud Storage Pool quando la regola ha un tempo di creazione definito dall'utente come tempo di riferimento.

Queste restrizioni esistono perché StorageGRID non è in grado di eseguire copie in modo sincrono in un pool di archiviazione cloud e un tempo di creazione definito dall'utente potrebbe essere risolto al momento.

L'interazione tra regole ILM e coerenza per influire sulla protezione dei dati

Sia la regola ILM che la scelta della coerenza influiscono sulla protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, il comportamento di acquisizione selezionato per una regola ILM influisce sul posizionamento iniziale delle copie degli oggetti, mentre la coerenza utilizzata durante la memorizzazione di un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti. Poiché StorageGRID richiede l'accesso sia ai dati dell'oggetto che ai metadati per soddisfare le richieste del client, la selezione di livelli di protezione corrispondenti per il comportamento di coerenza e acquisizione può offrire una migliore protezione iniziale dei dati e risposte del sistema più prevedibili.

Di seguito viene riportato un breve riepilogo dei valori di coerenza disponibili in StorageGRID:

- **All:** Tutti i nodi ricevono immediatamente i metadati degli oggetti o la richiesta non riesce.
- **Strong-global:** garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti. Quando la semantica del quorum è configurata, si applicano i seguenti comportamenti:
 - Consente la tolleranza ai guasti del sito per le richieste dei client quando le griglie hanno tre o più siti. Le griglie a due siti non avranno tolleranza ai guasti del sito.
 - Le seguenti operazioni S3 non riusciranno se un sito è inattivo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Se necessario, puoi ["configurare la semantica del quorum StorageGRID per una coerenza globale forte"](#).

- **Strong-site:** I metadati degli oggetti vengono immediatamente distribuiti ad altri nodi del sito. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write:** Fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available:** Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono

raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.



Prima di selezionare un valore di coerenza, ["leggi la descrizione completa della coerenza"](#) .
Prima di modificare il valore predefinito, è necessario comprenderne i vantaggi e le limitazioni.

Esempio di interazione tra le regole di coerenza e ILM

Supponiamo di avere una griglia a tre siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM:** creare tre copie dell'oggetto, una nel sito locale e una in ciascun sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **Coerenza:** Strong-global (i metadati degli oggetti vengono distribuiti immediatamente su più siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue tutte e tre le copie dell'oggetto e distribuisce i metadati a più 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 nei siti remoti. L'oggetto è completamente recuperabile dagli altri siti.

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 nei siti remoti, 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. Contattare NetApp per assistenza.

Informazioni correlate

["Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"](#)

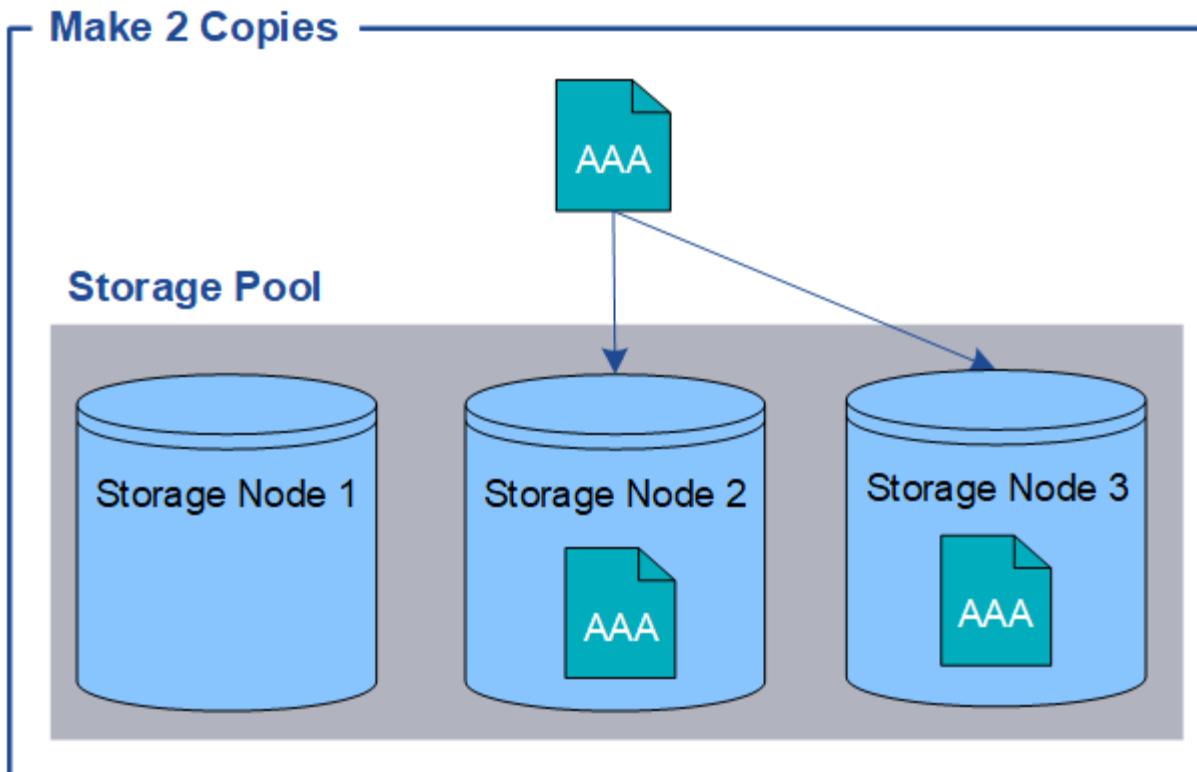
Modalità di archiviazione degli oggetti (replica o erasure coding)

Scopri la replica in StorageGRID

La replica è uno dei due metodi utilizzati da StorageGRID per archiviare i dati degli oggetti (l'erasure coding è l'altro metodo). 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 storage.

Quando si configura una regola ILM per la creazione di copie replicate, specificare il numero di copie da creare, la posizione delle copie e la durata della memorizzazione delle copie in ciascuna posizione.

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



Quando StorageGRID associa gli oggetti a questa regola, crea due copie dell'oggetto, collocando ciascuna copia su un nodo di storage diverso nel pool di storage. Le due copie possono essere collocate su due dei tre nodi di storage disponibili. In questo caso, la regola ha posizionato le copie degli oggetti sui nodi di storage 2 e 3. Poiché sono presenti due copie, l'oggetto può essere recuperato in caso di guasto di uno qualsiasi dei nodi del pool di storage.



StorageGRID può memorizzare solo una copia replicata di un oggetto su un dato nodo di storage. Se la griglia include tre nodi di storage e si crea una regola ILM di 4 copie, verranno eseguite solo tre copie, una copia per ciascun nodo di storage. Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Informazioni correlate

- ["Che cos'è l'erasure coding"](#)
- ["Che cos'è un pool di storage"](#)
- ["Abilita la protezione contro la perdita di sito utilizzando la replica e l'erasure coding"](#)

Rischi della replica a copia singola in StorageGRID

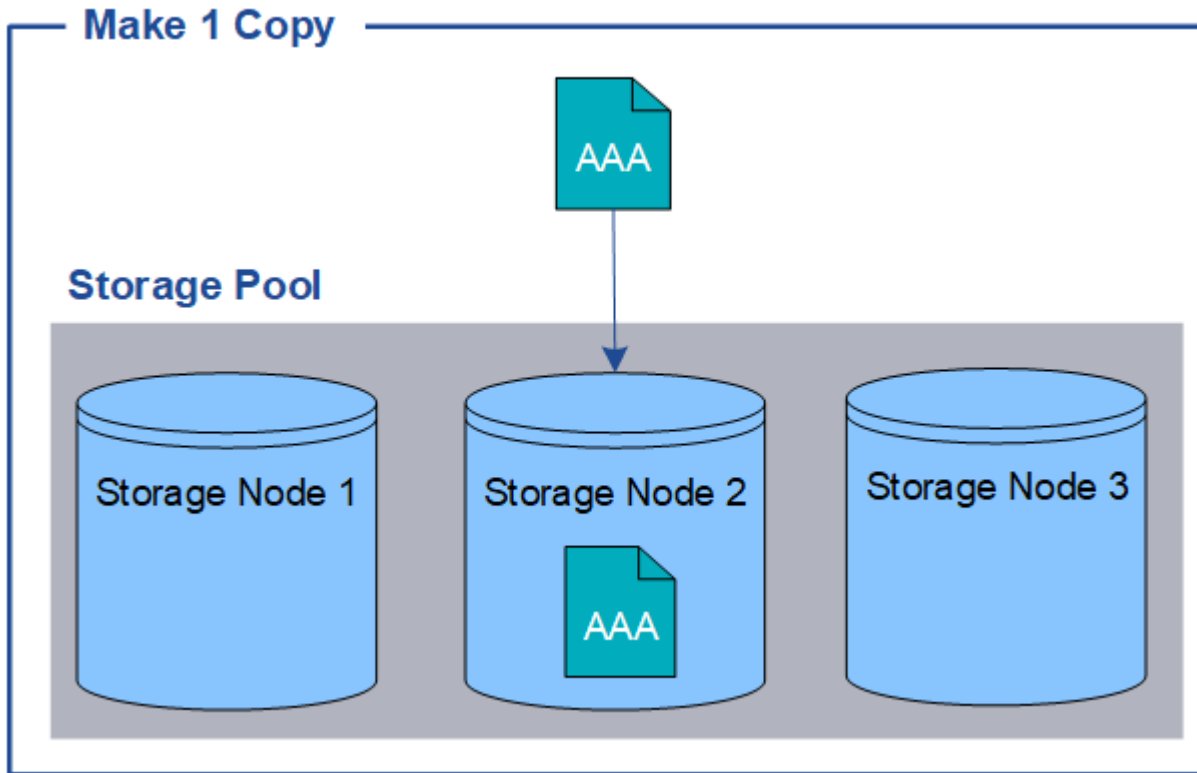
Quando si crea una regola ILM per creare copie replicate, è necessario specificare almeno due copie per un periodo di tempo qualsiasi nelle istruzioni di posizionamento.



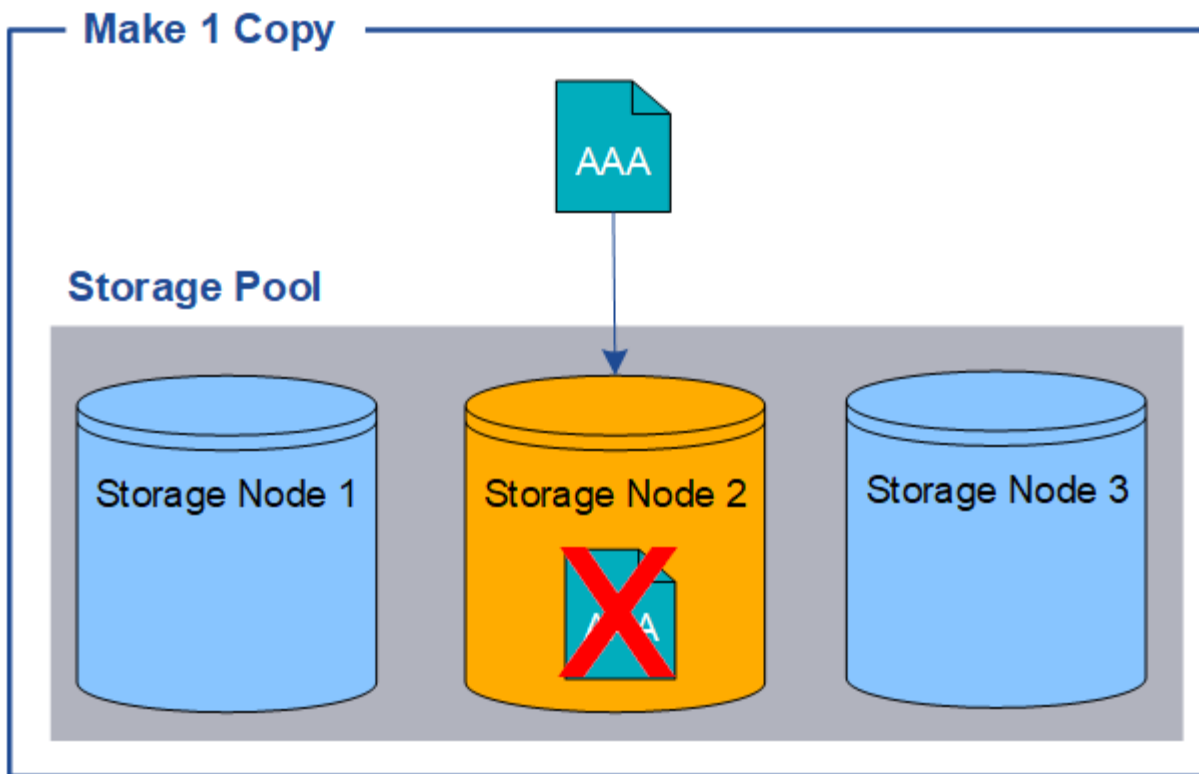
Non utilizzare una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Nell'esempio seguente, la regola Make 1 Copy ILM specifica che una copia replicata di un oggetto deve

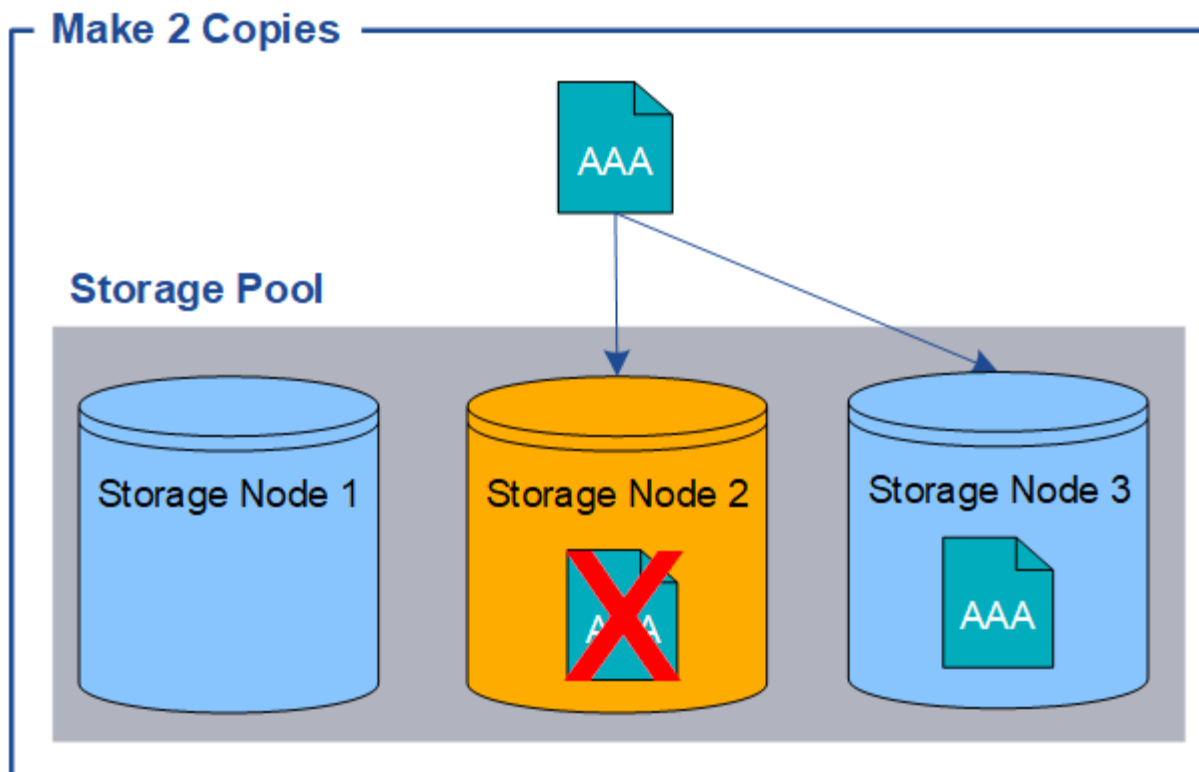
essere inserita in un pool di storage che contiene tre nodi di storage. Quando viene acquisito un oggetto che corrisponde a questa regola, StorageGRID inserisce una singola copia su un solo nodo di storage.



Quando una regola ILM crea una sola copia replicata di un oggetto, l'oggetto diventa inaccessibile quando il nodo di storage non è disponibile. In questo esempio, l'accesso all'oggetto AAA viene temporaneamente perso ogni volta che il nodo di storage 2 non è in linea, ad esempio durante un aggiornamento o un'altra procedura di manutenzione. In caso di guasto del nodo di storage 2, l'oggetto AAA andrà perso completamente.



Per evitare di perdere i dati degli oggetti, è necessario eseguire almeno due copie di tutti gli oggetti che si desidera proteggere con la replica. Se esistono due o più copie, è comunque possibile accedere all'oggetto se un nodo di storage si guasta o non è in linea.



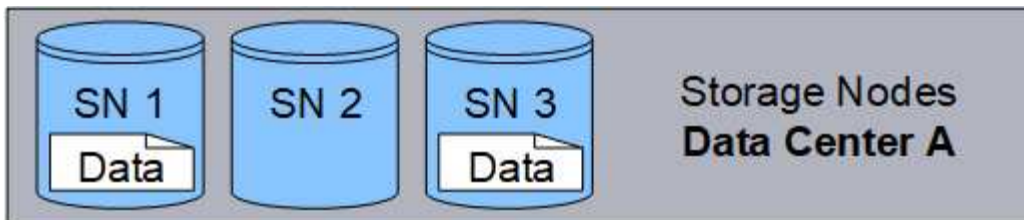
Scopri la codifica di cancellazione in StorageGRID

L'erasure coding è uno dei due metodi utilizzati da StorageGRID per memorizzare i dati degli oggetti (l'altro metodo è la replica). Quando gli oggetti corrispondono a una regola ILM che utilizza la codifica erasure, vengono suddivisi in frammenti di dati, vengono calcolati ulteriori frammenti di parità e ciascun frammento viene memorizzato in un nodo di storage diverso.

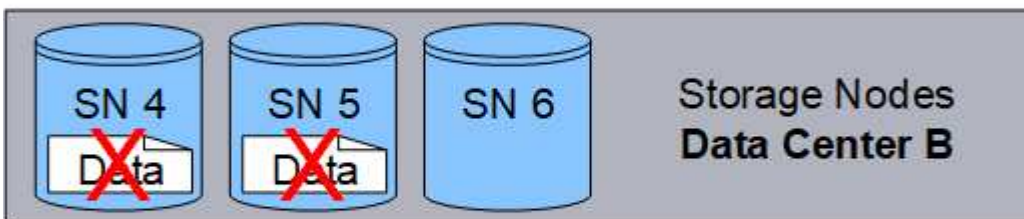
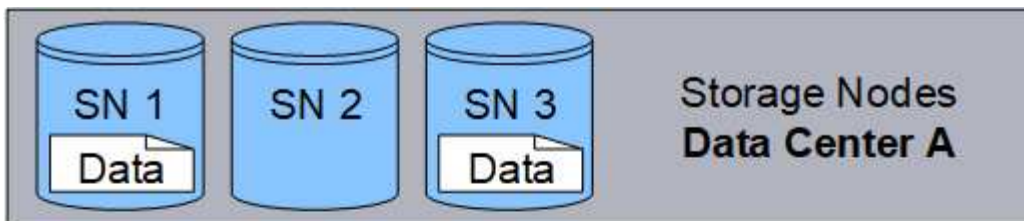
Quando si accede a un oggetto, questo viene riassembleato utilizzando i frammenti memorizzati. Se un dato o un frammento di parità viene corrotto o perso, l'algoritmo di erasure coding può ricreare quel frammento utilizzando un sottoinsieme dei dati rimanenti e dei frammenti di parità.

Quando crei regole ILM, StorageGRID crea profili di erasure coding in grado di supportarle. È possibile visualizzare un elenco di profili di erasure coding, ["rinominare un profilo con erasure coding"](#), o ["Disattivare un profilo di erasure coding se non è attualmente utilizzato in nessuna regola ILM"](#).

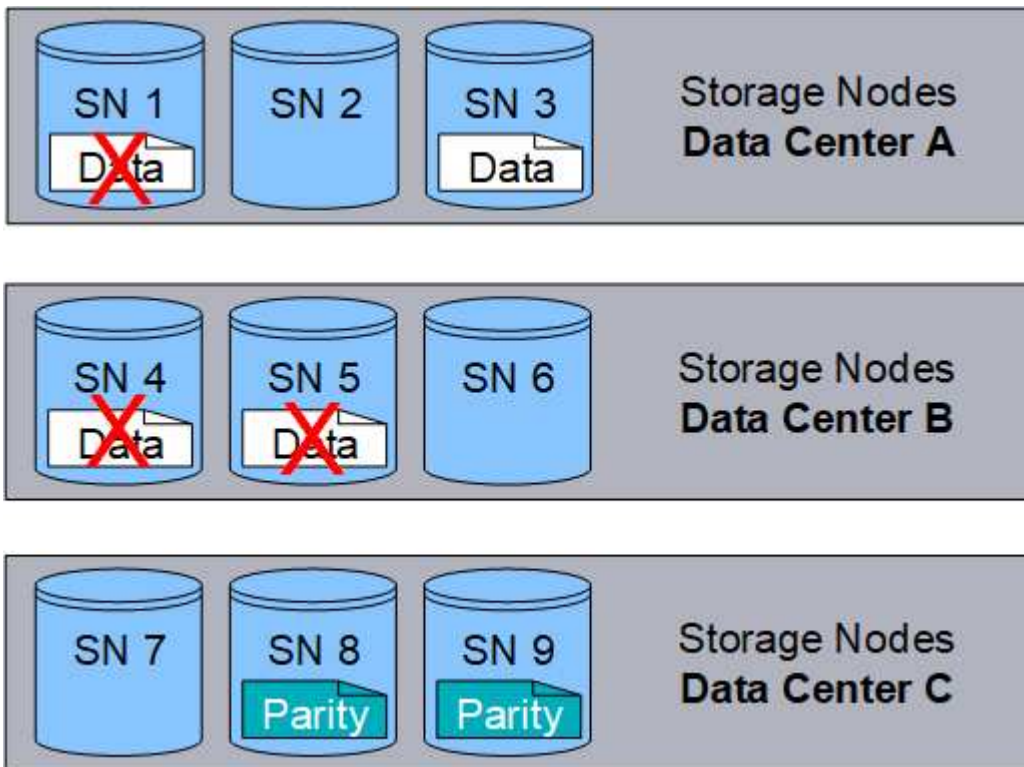
Nell'esempio seguente viene illustrato l'utilizzo di un algoritmo di erasure coding sui dati di un oggetto. In questo esempio, la regola ILM utilizza uno schema di erasure coding 4+2. Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati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



Lo schema di erasure coding 4+2 può essere configurato in vari modi. Ad esempio, è possibile configurare un pool di storage a sito singolo che contiene sei nodi di storage. Per "[protezione contro la perdita di sito](#)", è possibile utilizzare un pool di archiviazione contenente tre siti con tre nodi di archiviazione in ciascun sito. Un oggetto può essere recuperato finché quattro dei sei frammenti (dati o parità) rimangono disponibili. È possibile perdere fino a due frammenti senza perdita dei dati dell'oggetto. In caso di perdita di un intero sito, l'oggetto può comunque essere recuperato o riparato, purché tutti gli altri frammenti rimangano accessibili.



In caso di perdita di più di due nodi di storage, l'oggetto non può essere recuperato.



Informazioni correlate

- ["Cos'è la replica"](#)
- ["Che cos'è un pool di storage"](#)
- ["Cosa sono gli schemi di erasure coding"](#)
- ["Rinominare un profilo con erasure coding"](#)
- ["Disattivare un profilo di erasure coding"](#)

Scopri gli schemi di codifica di cancellazione in StorageGRID

Gli schemi di erasure coding controllano il numero di frammenti di dati e il numero di frammenti di parità creati per ciascun oggetto.

Quando si crea o modifica una regola ILM, si seleziona uno schema di erasure coding disponibile. StorageGRID crea automaticamente schemi di erasure coding in base al numero di nodi e siti storage che compongono il pool di storage che intendi utilizzare.

Protezione dei dati

Il sistema StorageGRID utilizza l'algoritmo di erasure coding Reed-Solomon. L'algoritmo suddivide un oggetto in k frammenti di dati e calcola m frammenti di parità.

I $k + m = n$ fragment sono distribuiti nei n nodi storage per garantire la protezione dei dati nel modo seguente:

- Per recuperare o riparare un oggetto, k sono necessari dei frammenti.
- Un oggetto può sopportare m frammenti persi o corrotti. Maggiore è il valore di m , maggiore è la tolleranza di errore.

La migliore data Protection è fornita dallo schema di erasure coding con la tolleranza ai guasti del nodo o del volume più elevata all'interno di un pool di storage.

Overhead dello storage

L'overhead di memorizzazione di uno schema di erasure coding viene calcolato dividendo il numero di frammenti di parità (m) per il numero di frammenti di dati (k). È possibile utilizzare l'overhead dello storage per calcolare la quantità di spazio su disco richiesta da ciascun oggetto con codifica di cancellazione:

$$\text{disk space} = \text{object size} + (\text{object size} * \text{storage overhead})$$

Ad esempio, se si memorizza un oggetto da 10 MB utilizzando lo schema 4+2 (con un overhead dello storage del 50%), l'oggetto consuma 15 MB di storage grid. Se si memorizza lo stesso oggetto da 10 MB utilizzando lo schema 6+2 (con un overhead dello storage del 33%), l'oggetto consuma circa 13.3 MB.

Seleziona lo schema di erasure coding con il valore totale più basso di $k+m$ quello che soddisfa le tue esigenze. Gli schemi di erasure coding con un numero inferiore di frammenti sono più efficienti dal punto di vista computazionale perché:

- Viene creato e distribuito (o recuperato) un numero inferiore di frammenti per oggetto
- Mostrano prestazioni migliori perché le dimensioni del frammento sono maggiori
- Possono richiedere un numero inferiore di nodi da aggiungere in un ["espansione quando è richiesto più storage"](#)

Linee guida per i pool di storage

Quando si seleziona il pool di storage da utilizzare per una regola che crea una copia con codice di cancellazione, utilizzare le seguenti linee guida per i pool di storage:

- Il pool di storage deve includere tre o più siti, o esattamente un sito.



Non è possibile utilizzare la codifica di cancellazione se il pool di storage include due siti.

- [Schemi di erasure coding per pool di storage contenenti tre o più siti](#)
- [Schemi di erasure coding per pool di storage a sito singolo](#)
- Non utilizzare un pool di archiviazione che includa il sito All Sites.
- Il pool di storage deve includere almeno nodi storage $k+m + 1$ in grado di memorizzare i dati degli oggetti.



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano dati e metadati di oggetti (nodo di archiviazione "combinato"), solo metadati di oggetti o solo dati di oggetti. Per ulteriori informazioni, fare riferimento a ["Tipi di nodi storage"](#).

Il numero minimo di nodi di archiviazione richiesto è $k+m$. Tuttavia, disporre di almeno un nodo di storage aggiuntivo può contribuire a prevenire gli errori di acquisizione o i backlog ILM se un nodo di storage richiesto non è temporaneamente disponibile.

Schemi di erasure coding per pool di storage contenenti tre o più siti

La seguente tabella descrive gli schemi di erasure coding attualmente supportati da StorageGRID per i pool di storage che includono tre o più siti. Tutti questi schemi offrono una protezione contro la perdita di sito. È

possibile perdere un sito e l'oggetto sarà ancora accessibile.

Per gli schemi di erasure coding che forniscono la protezione in caso di perdita di sito, il numero consigliato di nodi storage nel pool di storage supera $k+m+1$ poiché ciascun sito richiede un minimo di tre nodi storage.

Schema di erasure coding ($k+m$)	Numero minimo di siti implementati	Numero consigliato di nodi di storage in ogni sito	Numero totale consigliato di nodi di storage	Protezione contro le perdite di sito?	Overhead dello storage
4+2	3	3	9	Sì	50%
6+2	4	3	12	Sì	33%
8+2	5	3	15	Sì	25%
6+3	3	4	12	Sì	50%
9+3	4	4	16	Sì	33%
2+1	3	3	9	Sì	50%
4+1	5	3	15	Sì	25%
6+1	7	3	21	Sì	17%
7+5	3	5	15	Sì	71%



StorageGRID richiede un minimo di tre nodi di storage per sito. Per utilizzare lo schema 7+5, ogni sito richiede almeno quattro nodi di storage. Si consiglia di utilizzare cinque nodi di storage per sito.

Quando si seleziona uno schema di erasure coding che fornisce la protezione del sito, bilanciare l'importanza relativa dei seguenti fattori:

- **Numero di frammenti:** Le prestazioni e la flessibilità di espansione sono generalmente migliori quando il numero totale di frammenti è inferiore.
- **Fault tolerance:** La Fault tolerance è aumentata avendo più segmenti di parità (cioè, quando m ha un valore più alto).
- **Traffico di rete:** Quando si effettua il recupero da errori, utilizzando uno schema con più frammenti (cioè un totale più elevato per $k+m$) si crea più traffico di rete.
- **Overhead dello storage:** Gli schemi con overhead più elevato richiedono più spazio di storage per oggetto.

Ad esempio, quando si decide tra uno schema 4+2 e uno schema 6+3 (entrambi con un overhead dello storage del 50%), selezionare lo schema 6+3 se è richiesta una fault tolerance aggiuntiva. Selezionare lo schema 4+2 se le risorse di rete sono limitate. Se tutti gli altri fattori sono uguali, selezionare 4+2 perché il numero totale di frammenti è inferiore.



In caso di dubbi sul programma da utilizzare, selezionare 4+2 o 6+3 oppure contattare il supporto tecnico.

Schemi di erasure coding per pool di storage a sito singolo

Un pool di storage a sito singolo supporta tutti gli schemi di erasure coding definiti per tre o più siti, a condizione che il sito disponga di un numero sufficiente di nodi di storage.

Il numero minimo di nodi di archiviazione richiesto è $k+m$, ma si consiglia un pool di archiviazione con $k+m + 1$ nodi di archiviazione. Ad esempio, lo schema di erasure coding 2+1 richiede un pool di storage con almeno tre nodi di storage, ma si consiglia di utilizzare quattro nodi di storage.

Schema di erasure coding ($k+m$)	Numero minimo di nodi di storage	Numero consigliato di nodi di storage	Overhead dello storage
4+2	6	7	50%
6+2	8	9	33%
8+2	10	11	25%
6+3	9	10	50%
9+3	12	13	33%
2+1	3	4	50%
4+1	5	6	25%
6+1	7	8	17%
7+5	12	13	71%

Vantaggi, svantaggi e requisiti per l'erasure coding in StorageGRID

Prima di decidere se utilizzare la replica o la cancellazione del codice per proteggere i dati degli oggetti dalla perdita, è necessario comprendere i vantaggi, gli svantaggi e i requisiti per la cancellazione del codice.

Vantaggi dell'erasure coding

Rispetto alla replica, l'erasure coding offre maggiore affidabilità, disponibilità ed efficienza dello storage.

- **Affidabilità:** misurata in base al numero di guasti simultanei che possono essere sostenuti senza perdita di dati.
 - Replicazione: più copie identiche di oggetti vengono archiviate su nodi diversi e in più siti.
 - 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.

- **Disponibilità:** la capacità di ottenere 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 una disponibilità e un'affidabilità simili, gli oggetti con codice di cancellazione utilizzano meno spazio su disco rispetto agli oggetti replicati. 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 codifica in cancellazione viene calcolato come dimensione dell'oggetto più l'overhead dello storage. La percentuale di overhead dello storage è il numero di frammenti di parità diviso per il numero di frammenti di dati.

Svantaggi della codifica erasure

Rispetto alla replica, l'erasure coding presenta i seguenti svantaggi:

- È consigliato un maggior numero di siti e nodi di storage, a seconda dello schema di erasure coding. Al contrario, se si replicano i dati degli oggetti, è necessario un solo nodo di storage per ogni copia. Vedere ["Schemi di erasure coding per pool di storage contenenti tre o più siti"](#) e ["Schemi di erasure coding per pool di storage a sito singolo"](#).
- Aumento dei costi e della complessità delle espansioni dello storage. Per espandere un'implementazione che utilizza la replica, è necessario aggiungere capacità di storage in ogni posizione in cui vengono eseguite le copie a oggetti. Per espandere un'implementazione che utilizza il erasure coding, è necessario prendere in considerazione sia lo schema di erasure coding in uso sia la capacità dei nodi di storage esistenti. Ad esempio, se si attende che i nodi esistenti siano pieni al 100%, è necessario aggiungere almeno $k+m$ nodi storage, ma se si espandono quando i nodi esistenti sono pieni al 70%, è possibile aggiungere due nodi per sito e massimizzare la capacità dello storage utilizzabile. Per ulteriori informazioni, vedere ["Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione"](#).
- L'utilizzo di erasure coding in siti distribuiti geograficamente aumenta le latenze di recupero. I frammenti di oggetto per un oggetto sottoposto a erasure coding e distribuito tra i siti remoti richiedono più tempo per il recupero su connessioni WAN rispetto a un oggetto replicato e disponibile in locale (lo stesso sito a cui si connette il client).
- Quando si utilizza il erasure coding in siti distribuiti geograficamente, il traffico di rete WAN è più elevato per recuperi e riparazioni, in particolare per oggetti recuperati di frequente o per riparazioni di oggetti su connessioni di rete WAN.
- Quando si utilizza 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 il risultato di una 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 calcolo.

Quando utilizzare la codifica di cancellazione

Utilizzare la codifica di cancellazione per i seguenti requisiti:

- Oggetti di dimensioni superiori a 1 MB.



L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

- Storage a lungo termine o a freddo per contenuti recuperati raramente.
- Elevata disponibilità e affidabilità dei dati.
- Protezione contro guasti completi del sito e dei nodi.
- Efficienza dello storage.
- Implementazioni a singolo sito che richiedono una protezione dei dati efficiente con una sola copia codificata in cancellazione anziché più copie replicate.
- Implementazioni multi-sito in cui la latenza tra siti è inferiore a 100 ms.

Come StorageGRID determina la conservazione degli oggetti

StorageGRID offre agli amministratori di grid e ai singoli utenti tenant opzioni per specificare la durata della memorizzazione degli oggetti. In generale, tutte le istruzioni di conservazione fornite da un utente tenant hanno la precedenza sulle istruzioni di conservazione fornite dall'amministratore della griglia.

Come gli utenti tenant controllano la conservazione degli oggetti

Gli utenti tenant possono utilizzare questi metodi per controllare la durata della memorizzazione degli oggetti in StorageGRID:

- Se l'impostazione blocco oggetto S3 globale è attivata per la griglia, gli utenti tenant S3 possono creare bucket con blocco oggetto S3 abilitato e quindi selezionare un **periodo di conservazione predefinito** per ciascun bucket.
- Se l'impostazione globale S3 Object Lock è attivata per la griglia, gli utenti del tenant S3 possono creare bucket con S3 Object Lock abilitato e quindi utilizzare l'API REST S3 per specificare le impostazioni di conservazione fino alla data e conservazione legale per ciascuna versione dell'oggetto aggiunta a quel bucket.
 - Una versione dell'oggetto soggetta a blocco legale non può essere eliminata da alcun metodo.
 - Prima che venga raggiunta la data di conservazione di una versione a oggetti, tale versione non può essere eliminata da alcun metodo.
 - Gli oggetti nei bucket con blocco oggetti S3 abilitato vengono conservati da ILM "per sempre". Tuttavia, una volta raggiunta la data di conservazione, una versione dell'oggetto può essere eliminata da una richiesta del client o dalla scadenza del ciclo di vita del bucket. Vedere ["Gestire gli oggetti con S3 Object Lock"](#).
- Gli utenti del tenant S3 possono aggiungere una configurazione del ciclo di vita ai bucket che specifica un'azione di scadenza. Se esiste un ciclo di vita del bucket, StorageGRID memorizza un oggetto fino a quando non viene soddisfatta la data o il numero di giorni specificati nell'azione di scadenza, a meno che il client non elimini prima l'oggetto. Vedere ["Creare la configurazione del ciclo di vita S3"](#).
- Un client S3 può emettere una richiesta di eliminazione degli oggetti. StorageGRID assegna sempre la priorità alle richieste di eliminazione dei client sul ciclo di vita del bucket S3 o ILM quando si determina se eliminare o conservare un oggetto.

Come gli amministratori della griglia controllano la conservazione degli oggetti

Gli amministratori di grid possono utilizzare questi metodi per controllare la conservazione degli oggetti:

- Impostare un periodo di conservazione massimo per il blocco degli oggetti S3 per ogni tenant. Quindi, gli utenti tenant possono impostare un periodo di conservazione predefinito per ciascun bucket. Il periodo di conservazione massimo viene applicato anche a tutti gli oggetti appena acquisiti per quel bucket (Retain-until-date dell'oggetto).
- Creare le istruzioni di posizionamento ILM per controllare la durata di memorizzazione degli oggetti. Quando un oggetto viene associato da una regola ILM, StorageGRID memorizza tali oggetti fino allo scadere dell'ultimo periodo di tempo della regola ILM. Gli oggetti vengono conservati a tempo indeterminato se per le istruzioni di posizionamento viene specificato "per sempre".
- Indipendentemente da chi controlla la durata della conservazione degli oggetti, le impostazioni ILM determinano i tipi di copie degli oggetti (replicate o sottoposte a erasure coding) archiviati e la posizione delle copie (nodi storage o pool di cloud storage).

Come interagiscono il ciclo di vita del bucket S3 e ILM

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

Esempi di conservazione degli oggetti

Per comprendere meglio le interazioni tra blocco oggetti S3, impostazioni del ciclo di vita del bucket, richieste di eliminazione client e ILM, considerare gli esempi seguenti.

Esempio 1: Il ciclo di vita del bucket S3 mantiene gli oggetti più a lungo di ILM

ILM

Memorizzazione di due copie per 1 anno (365 giorni)

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Risultato

StorageGRID memorizza l'oggetto per 730 giorni. StorageGRID utilizza le impostazioni del ciclo di vita del bucket per determinare se eliminare o conservare un oggetto.



Se il ciclo di vita del bucket specifica che gli oggetti devono essere mantenuti più a lungo di quanto specificato da ILM, StorageGRID continua a utilizzare le istruzioni di posizionamento ILM per determinare il numero e il tipo di copie da memorizzare. In questo esempio, due copie dell'oggetto continueranno ad essere memorizzate in StorageGRID dai giorni 366 al 730.

Esempio 2: Il ciclo di vita del bucket S3 scade gli oggetti prima di ILM

ILM

Memorizzazione di due copie per 2 anni (730 giorni)

Ciclo di vita del bucket

Scadenza oggetti in 1 anno (365 giorni)

Risultato

StorageGRID elimina entrambe le copie dell'oggetto dopo il giorno 365.

Esempio 3: L'eliminazione del client sovrascrive il ciclo di vita del bucket e ILM

ILM

Memorizzazione di due copie sui nodi storage "per sempre"

Ciclo di vita del bucket

Scadenza degli oggetti in 2 anni (730 giorni)

Richiesta di eliminazione del client

Emesso il giorno 400

Risultato

StorageGRID elimina entrambe le copie dell'oggetto il giorno 400 in risposta alla richiesta di eliminazione del client.

Esempio 4: S3 Object Lock sovrascrive la richiesta di eliminazione del client

Blocco oggetti S3

Retain-until-date per una versione a oggetti è 2026-03-31. Non è in vigore una conservazione a fini giudiziari.

Regola ILM conforme

Memorizzazione di due copie sui nodi storage "per sempre"

Richiesta di eliminazione del client

Pubblicato il 2024-03-31

Risultato

StorageGRID non eliminerà la versione dell'oggetto perché la data di conservazione è ancora a 2 anni di distanza.

Come StorageGRID elimina gli oggetti

StorageGRID può eliminare gli oggetti in risposta diretta a una richiesta del client o automaticamente in conseguenza della scadenza di un ciclo di vita del bucket S3 o dei requisiti della policy ILM. La comprensione dei diversi modi in cui è possibile eliminare gli oggetti e del modo in cui StorageGRID gestisce le richieste di eliminazione può aiutare a gestire gli oggetti in modo più efficace.

StorageGRID può utilizzare uno dei due metodi per eliminare gli oggetti:

- Eliminazione sincrona: Quando StorageGRID riceve una richiesta di eliminazione del client, tutte le copie degli oggetti vengono rimosse immediatamente. Il client viene informato che l'eliminazione è stata eseguita correttamente dopo la rimozione delle copie.
- Gli oggetti vengono messi in coda per l'eliminazione: Quando StorageGRID riceve una richiesta di eliminazione, l'oggetto viene messo in coda per l'eliminazione e il client viene immediatamente informato dell'avvenuta eliminazione. Le copie degli oggetti vengono rimosse in seguito dall'elaborazione ILM in background.

Quando si eliminano gli oggetti, StorageGRID utilizza il metodo che ottimizza le performance di eliminazione, riduce al minimo i potenziali backlog di eliminazione e libera lo spazio più rapidamente.

La tabella riassume quando StorageGRID utilizza ciascun metodo.

Metodo di eliminazione	Se utilizzato
Gli oggetti vengono messi in coda per l'eliminazione	Quando una delle seguenti condizioni è vera: • L'eliminazione automatica degli oggetti è stata attivata da uno dei seguenti eventi: ◦ Viene raggiunta la data di scadenza o il numero di giorni nella configurazione del ciclo di vita di un bucket S3. ◦ È trascorso l'ultimo periodo di tempo specificato in una regola ILM. • Un client S3 richiede l'eliminazione e una o più di queste condizioni sono vere: ◦ Impossibile eliminare le copie entro 30 secondi perché, ad esempio, una posizione dell'oggetto non è temporaneamente disponibile. ◦ Le code di eliminazione in background sono inattive. Nota: gli oggetti in un bucket che ha attivato il blocco oggetti S3 non possono essere cancellati se sono in stato di conservazione legale o se è stato specificato un periodo di conservazione fino alla data, ma non ancora soddisfatto.
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 S3 client effettuano richieste di eliminazione, StorageGRID inizia aggiungendo oggetti alla coda di eliminazione. Passa quindi all'eliminazione sincrona. Assicurarsi che la coda di eliminazione in background disponga di oggetti da elaborare consente a StorageGRID di elaborare le eliminazioni in modo più efficiente, in particolare per i client con bassa concorrenza, evitando al contempo i backlog di eliminazione dei client.

Tempo necessario per eliminare gli oggetti

Il modo in cui StorageGRID elimina gli oggetti può influire sulle prestazioni del sistema:

- Quando StorageGRID esegue l'eliminazione sincrona, StorageGRID può impiegare fino a 30 secondi per restituire un risultato al client. Ciò significa che l'eliminazione può sembrare più lenta, anche se le copie vengono effettivamente rimosse più rapidamente di quanto non lo siano quando StorageGRID mette in coda gli oggetti per l'eliminazione.
- Se si sta monitorando attentamente le prestazioni di eliminazione durante un'eliminazione in blocco, è possibile notare che la velocità di eliminazione sembra essere lenta dopo l'eliminazione di un certo numero di oggetti. Questa modifica si verifica quando StorageGRID passa dall'accodamento di oggetti per l'eliminazione all'eliminazione sincrona. La riduzione apparente del tasso di eliminazione non significa che le copie degli oggetti vengano rimosse più lentamente. Al contrario, indica che, in media, lo spazio viene liberato più rapidamente.

Se si eliminano grandi quantità di oggetti e la priorità è liberare spazio rapidamente, considerare l'utilizzo di una richiesta client per eliminare gli oggetti piuttosto che eliminarli utilizzando ILM o altri metodi. In generale, lo spazio viene liberato più rapidamente quando l'eliminazione viene eseguita dai client perché StorageGRID può utilizzare l'eliminazione sincrona.

La quantità di tempo necessaria per liberare spazio dopo l'eliminazione di un oggetto dipende da diversi fattori:

- Se le copie degli oggetti vengono rimosse in modo sincrono o messe in coda per la rimozione in un secondo momento (per le richieste di eliminazione del client).
- Altri fattori, come il numero di oggetti nella griglia o la disponibilità di risorse della griglia quando le copie degli oggetti vengono messe in coda per la rimozione (sia per le eliminazioni dei client che per altri metodi).

Modalità di eliminazione degli oggetti con versione S3

Quando il controllo delle versioni è attivato per un bucket S3, StorageGRID segue il comportamento di Amazon S3 quando risponde alle richieste di eliminazione, sia che provengano da un client S3, dalla scadenza di un ciclo di vita del bucket S3 o dai requisiti della policy ILM.

Quando gli oggetti sono in versione, le richieste di eliminazione degli oggetti non eliminano la versione corrente dell'oggetto e non liberano spazio. Invece, una richiesta di eliminazione di un oggetto crea un marcatore di eliminazione di zero byte come versione corrente dell'oggetto, rendendo la versione precedente dell'oggetto "non corrente". Un marcatore di eliminazione di un oggetto diventa un marcatore di eliminazione di un oggetto scaduto quando è la versione corrente e non ci sono versioni non correnti.

Anche se l'oggetto non è stato rimosso, StorageGRID si comporta come se la versione corrente dell'oggetto non fosse più disponibile. Le richieste a quell'oggetto restituiscono 404 non trovato. Tuttavia, poiché i dati dell'oggetto non correnti non sono stati rimossi, le richieste che specificano una versione non corrente dell'oggetto possono avere successo.

Se un client elimina una versione di un oggetto con un ID versione da un ["secchio di rami"](#) StorageGRID nasconde l'esistenza della versione dell'oggetto ma non crea un marcatore di eliminazione nel bucket del ramo. Se un client elimina un oggetto senza un ID versione da un bucket di diramazione, StorageGRID crea un marcatore di eliminazione nel bucket di diramazione in base al comportamento S3 standard.

Per liberare spazio quando si eliminano gli oggetti con versione o per rimuovere i marcatori di eliminazione, utilizzare una delle seguenti opzioni:

- **S3 client request:** Specificare l'ID della versione dell'oggetto nella richiesta di ELIMINAZIONE DELL'oggetto S3 (`DELETE /object?versionId=ID`). Tenere presente che questa richiesta rimuove solo le copie degli oggetti per la versione specificata (le altre versioni occupano ancora spazio).
- **Ciclo di vita benna:** Utilizzare l' `NoncurrentVersionExpiration` azione nella configurazione del ciclo di vita benna. Quando viene raggiunto il numero di giorni non correnti specificato, StorageGRID rimuove in modo permanente tutte le copie delle versioni degli oggetti non correnti. Queste versioni degli oggetti non possono essere ripristinate.

L' `NewerNoncurrentVersions` azione nella configurazione del ciclo di vita del bucket specifica il numero di versioni non correnti mantenute in un bucket S3 versione. Se sono presenti più versioni non correnti di quelle `NewerNoncurrentVersions` specificate, StorageGRID rimuove le versioni precedenti una volta scaduto il valore `NoncurrentDays`. La `NewerNoncurrentVersions` soglia sovrascrive le regole del ciclo di vita fornite da ILM, il che significa che un oggetto non corrente con una versione compresa nella `NewerNoncurrentVersions` soglia viene mantenuto se ILM richiede la sua eliminazione.

Per rimuovere i marcatori di eliminazione degli oggetti scaduti, utilizzare l' `Expiration` azione con uno dei seguenti tag: `ExpiredObjectDeleteMarker`, `Days` o `Date`.

- **ILM: "Clonazione di una policy attiva"** E aggiungere due regole ILM alla nuova policy:
 - Prima regola: Utilizzare "ora non corrente" come ora di riferimento per far corrispondere le versioni non correnti dell'oggetto. In **"Fase 1 (immettere i dettagli) della procedura guidata Crea una regola ILM"**, selezionare **Si** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?"
 - Seconda regola: Utilizzare **Ingest Time** per corrispondere alla versione corrente. La regola "ora non corrente" deve essere visualizzata nel criterio sopra la regola **ora acquisizione**.

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 il creatore di eliminazione corrente è scaduto (non ci sono versioni non correnti).

- **Elimina oggetti nel bucket:** Utilizza il gestore tenant per **"elimina tutte le versioni degli oggetti"**, compresi i marcatori di eliminazione, da un bucket.

Quando un oggetto con versione viene eliminato, StorageGRID crea un marcatore di eliminazione a byte zero come versione corrente dell'oggetto. Tutti gli oggetti e i marcatori di eliminazione devono essere rimossi prima di poter eliminare un bucket in versione.

- I marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti possono essere rimossi solo tramite richieste client S3, ma non tramite ILM, regole del ciclo di vita bucket o Elimina oggetti nelle operazioni bucket.
- I marcatori di eliminazione da un bucket creato in StorageGRID 11,8 o versioni successive possono essere rimossi da ILM, regole del ciclo di vita bucket, Elimina oggetti nelle operazioni bucket o un'eliminazione client S3 esplicita.

Informazioni correlate

- ["UTILIZZARE L'API REST S3"](#)
- ["Esempio 4: Regole ILM e policy per gli oggetti con versione S3"](#)

Crea e assegna gradi di storage in StorageGRID

I gradi di storage identificano il tipo di storage utilizzato da un nodo di storage. È possibile creare gradi di storage se si desidera che le regole ILM posizionino determinati oggetti su determinati nodi di storage.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un **"browser web supportato"**.
- Si dispone di **"autorizzazioni di accesso specifiche"**.

A proposito di questa attività

Quando si installa StorageGRID per la prima volta, il livello di storage **predefinito** viene assegnato automaticamente a ogni nodo di storage del sistema. In base alle esigenze, è possibile definire gradazioni di storage personalizzate e assegnarle a diversi nodi di storage.

L'utilizzo di storage grades personalizzati consente di creare pool di storage ILM che contengono solo un tipo specifico di Storage Node. Ad esempio, è possibile che alcuni oggetti vengano memorizzati nei nodi di storage

più veloci, ad esempio le appliance di storage all-flash StorageGRID.



Ai nodi di archiviazione solo metadati non può essere assegnato un grado di archiviazione. Per ulteriori informazioni, fare riferimento a "[Tipi di nodi storage](#)".

Se il grado di archiviazione non è un problema (ad esempio, tutti i nodi di archiviazione sono identici), è possibile ignorare questa procedura e utilizzare la selezione **include tutti i gradi di archiviazione** per il grado di archiviazione quando si "[creare pool di storage](#)". L'utilizzo di questa selezione garantisce che il pool di storage includa ogni nodo di storage del sito, indipendentemente dal suo livello di storage.



Non creare più storage di quanto necessario. Ad esempio, non creare un livello di storage per ciascun nodo di storage. Assegnare invece ogni livello di storage a due o più nodi. I gradi di storage assegnati a un solo nodo possono causare backlog ILM se tale nodo non è più disponibile.

Fasi

1. Selezionare **ILM > Storage grades**.
2. Definire i livelli di storage personalizzati:
 - a. Per ogni livello di storage personalizzato che vuoi aggiungere, seleziona **Inserisci**  per aggiungere una riga.
 - b. Inserire 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 puoi eliminare i gradi di storage.

3. Assegnare nuovi gradi di storage ai nodi di storage:

a. Individua il nodo di archiviazione nell'elenco LDR e seleziona la relativa icona **Modifica** .

b. Selezionare il livello di storage appropriato dall'elenco.



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 storage a un nodo di storage specifico una sola volta. Un nodo di storage recuperato dal guasto mantiene il livello di storage assegnato in precedenza. Non modificare questa assegnazione dopo l'attivazione della policy ILM. Se l'assegnazione viene modificata, i dati vengono memorizzati in base al nuovo livello di storage.

- a. Selezionare **Applica modifiche**.

Utilizzare i pool di storage

Scopri i pool di storage in StorageGRID

Un pool di storage è un raggruppamento logico di nodi storage.

Quando si installa StorageGRID, viene creato automaticamente un pool di storage per sito. È possibile configurare ulteriori pool di storage in base alle esigenze di storage.



Durante l'installazione, è possibile configurare i nodi di archiviazione in modo che contengano dati e metadati di oggetti (nodo di archiviazione "combinato"), solo metadati di oggetti o solo dati di oggetti. I nodi di archiviazione solo metadati non possono essere utilizzati nei pool di archiviazione. Per ulteriori informazioni, fare riferimento a ["Tipi di nodi storage"](#).

I pool di storage hanno due attributi:

- **Storage grade:** Per i nodi di storage, le performance relative dello storage di backup.
- **Sito:** Il data center in cui vengono archiviati gli oggetti.

I pool di storage vengono utilizzati nelle regole ILM per determinare dove sono memorizzati i dati degli oggetti e il tipo di storage utilizzato. Quando si configurano le regole ILM per la replica, si selezionano uno o più pool di storage.

Linee guida per la configurazione del pool di storage in StorageGRID

Configurare e utilizzare i pool di storage per proteggersi dalla perdita di dati distribuendo i dati su più siti. Le copie replicate e le copie con codice di cancellazione richiedono diverse configurazioni del pool di storage.

Consulta ["Esempi di attivazione della protezione dalle perdite di sito mediante la replica e la cancellazione del codice"](#).

Linee guida per tutti i pool di storage

- Le configurazioni del pool di storage sono il più semplici possibile. Non creare più pool di storage del necessario.
- Creare pool di storage con il maggior numero possibile di nodi. Ogni pool di storage deve contenere due o più nodi. Un pool di storage con nodi insufficienti può causare backlog ILM se un nodo diventa non disponibile.
- Evitare di creare o utilizzare pool di storage che si sovrappongono (contenenti uno o più degli stessi nodi). Se i pool di storage si sovrappongono, è possibile che più di una copia dei dati dell'oggetto venga salvata sullo stesso nodo.
- In generale, non utilizzare il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) o il sito All Sites. Questi elementi vengono aggiornati automaticamente per includere i nuovi siti aggiunti in un'espansione, il che potrebbe non essere il comportamento desiderato.

Linee guida per i pool di storage utilizzati per le copie replicate

- Per la protezione contro la perdita del sito mediante ["replica"](#), specificare uno o più pool di archiviazione specifici del sito in ["Istruzioni di posizionamento per ogni regola ILM"](#).

Un pool di storage viene creato automaticamente per ogni sito durante l'installazione di StorageGRID.

L'utilizzo di un pool di storage per ciascun sito garantisce che le copie degli oggetti replicate vengano posizionate esattamente dove ci si aspetta (ad esempio, una copia di ogni oggetto in ogni sito per la protezione dalla perdita di sito).

- Se si aggiunge un sito in un'espansione, creare un nuovo pool di storage che contenga solo il nuovo sito. Quindi, ["Aggiornare le regole ILM"](#) per controllare quali oggetti vengono memorizzati nel nuovo sito.
- Se il numero di copie è inferiore al numero di pool di storage, il sistema distribuisce le copie per bilanciare l'utilizzo del disco tra i pool.
- Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. È necessario assicurarsi che i pool di storage selezionati non contengano gli stessi nodi di storage.

Linee guida per i pool di storage utilizzati per le copie erasure-coded

- Per la protezione delle perdite di sito mediante ["erasure coding"](#), creare pool di archiviazione composti da almeno tre siti. Se un pool di storage include solo due siti, non è possibile utilizzare tale pool di storage per la cancellazione del codice. Non sono disponibili schemi di erasure coding per un pool di storage con due siti.
- Il numero di nodi e siti di archiviazione contenuti nel pool di archiviazione determina quali ["schemi di erasure coding"](#) sono disponibili.
- Se possibile, un pool di storage deve includere un numero superiore al numero minimo di nodi di storage

richiesto per lo schema di erasure coding selezionato. Ad esempio, se si utilizza uno schema di erasure coding 6+3, è necessario disporre di almeno nove nodi di storage. Tuttavia, si consiglia di disporre di almeno un nodo di storage aggiuntivo per sito.

- Distribuire i nodi di storage tra i siti nel modo più uniforme possibile. Ad esempio, per supportare uno schema di erasure coding 6+3, configurare un pool di storage che includa almeno tre nodi di storage in tre siti.
- Se si hanno requisiti di throughput elevati, si sconsiglia di utilizzare un pool di storage che include più siti se la latenza di rete tra siti è superiore a 100 ms. Con l'aumentare della latenza, la velocità con cui StorageGRID può creare, posizionare e recuperare frammenti di oggetti diminuisce drasticamente a causa della diminuzione del throughput di rete TCP.

La diminuzione del throughput influisce sulle velocità massime raggiungibili di acquisizione e recupero degli oggetti (quando si seleziona Balanced o Strict come comportamento di acquisizione) o potrebbe causare ritardi nella coda ILM (quando si seleziona Dual commit come comportamento di acquisizione). Fai riferimento a "[Comportamento di acquisizione delle regole ILM](#)".



Se il grid include un solo sito, è impossibile utilizzare il pool di storage All Storage Nodes (StorageGRID 11,6 e versioni precedenti) o il sito All Sites in un profilo di erasure coding. Questo comportamento impedisce che il profilo diventi non valido se viene aggiunto un secondo sito.

Protezione dalla perdita del sito con pool di storage in StorageGRID

Se l'implementazione di StorageGRID include più di un sito, è possibile utilizzare la replica e la cancellazione del codice con pool di storage configurati in modo appropriato per abilitare la protezione dalla perdita di sito.

La replica e l'erasure coding richiedono diverse configurazioni del pool di storage:

- Per utilizzare la replica per la protezione dalla perdita di sito, utilizzare i pool di storage specifici del sito creati automaticamente durante l'installazione di StorageGRID. Quindi, creare regole ILM "[istruzioni per il posizionamento](#)" che specificano più pool di storage in modo da collocare una copia di ciascun oggetto in ogni sito.
- Per utilizzare l'erasure coding per la protezione in caso di perdita del sito, "[creare pool di storage composti da più siti](#)". Quindi, creare regole ILM che utilizzano un pool di storage costituito da più siti e qualsiasi schema di erasure coding disponibile.



Quando si configura la distribuzione StorageGRID per la protezione dalle perdite del sito, è necessario tenere conto anche degli effetti di "[opzioni di acquisizione](#)" E "[coerenza](#)".

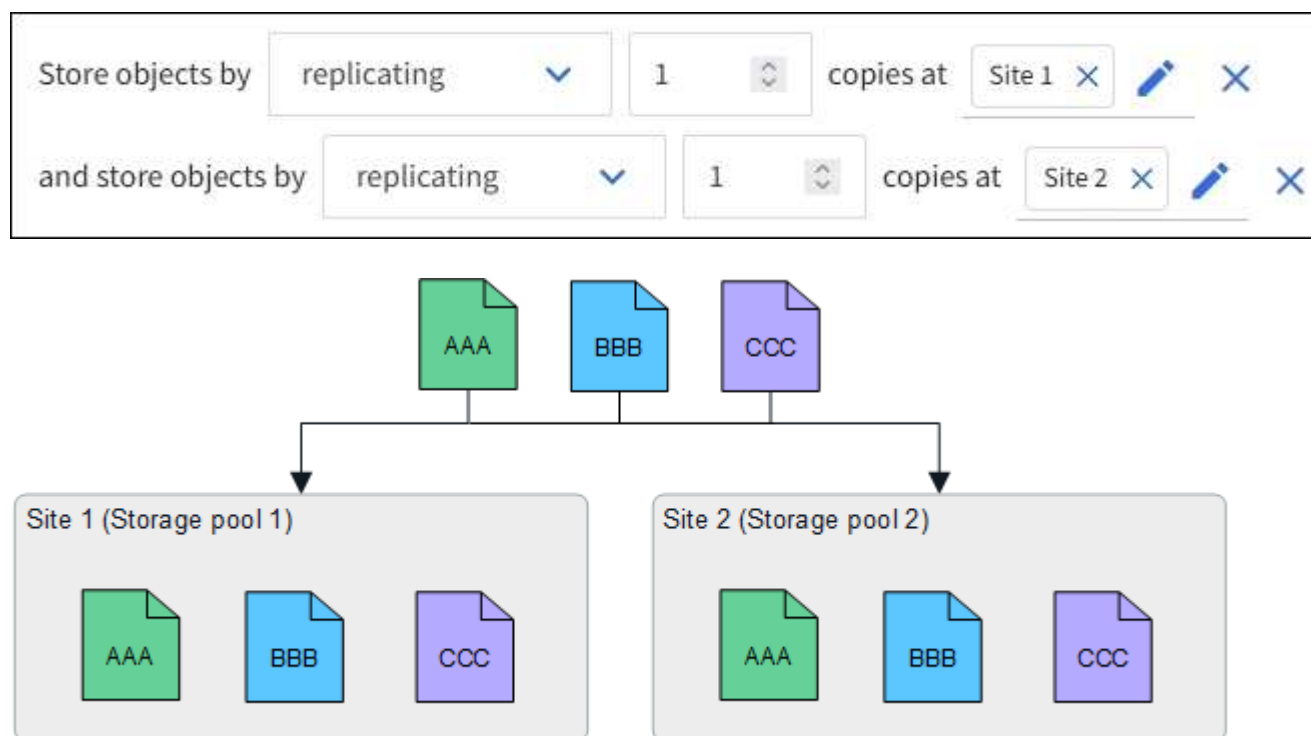
Esempio di replica

Per impostazione predefinita, viene creato un pool di storage per ciascun sito durante l'installazione di StorageGRID. La disponibilità di pool di storage costituiti da un solo sito consente di configurare le regole ILM che utilizzano la replica per la protezione dalla perdita di sito. In questo esempio:

- Il pool di archiviazione 1 contiene il sito 1
- Il pool di archiviazione 2 contiene il sito 2
- La regola ILM contiene due posizioni:
 - Memorizzare gli oggetti replicando 1 copia nel sito 1

- Memorizzare gli oggetti replicando 1 copia nel sito 2

Posizionamento delle regole ILM:



In caso di perdita di un sito, le copie degli oggetti sono disponibili nell'altro sito.

Esempio di erasure coding

La disponibilità di pool di storage costituiti da più di un sito per pool di storage consente di configurare le regole ILM che utilizzano la codifica di cancellazione per la protezione dalla perdita di sito. In questo esempio:

- Il pool di storage 1 contiene i siti da 1 a 3
- La regola ILM contiene un unico posizionamento: Memorizzare gli oggetti tramite erasure coding utilizzando uno schema EC 4+2 nello Storage Pool 1, che contiene tre siti

Posizionamento delle regole ILM:



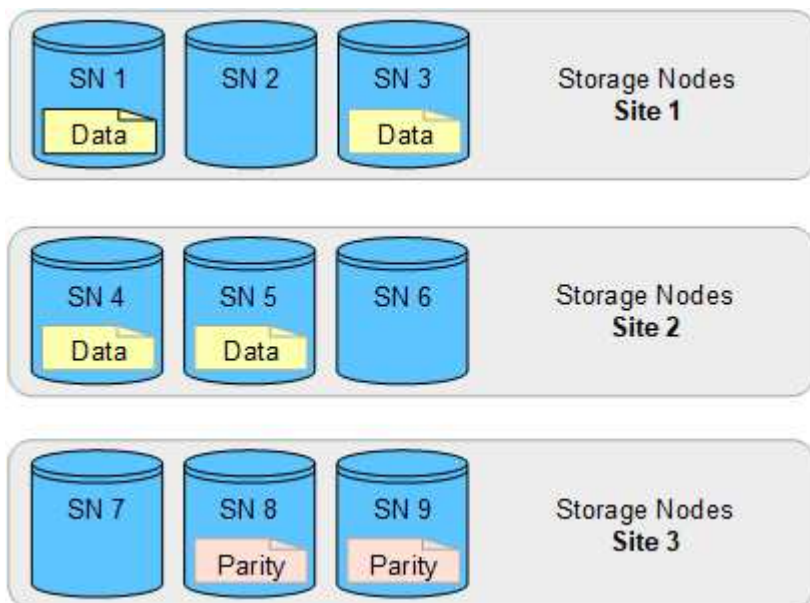
In questo esempio:

- La regola ILM utilizza uno schema di erasure coding 4+2.
- Ciascun oggetto viene suddiviso in quattro frammenti di dati uguali e due frammenti di parità vengono calcolati dai dati dell'oggetto.
- Ciascuno dei sei frammenti viene memorizzato su un nodo diverso in tre siti del data center per fornire protezione dei dati in caso di guasti al nodo o perdita del sito.

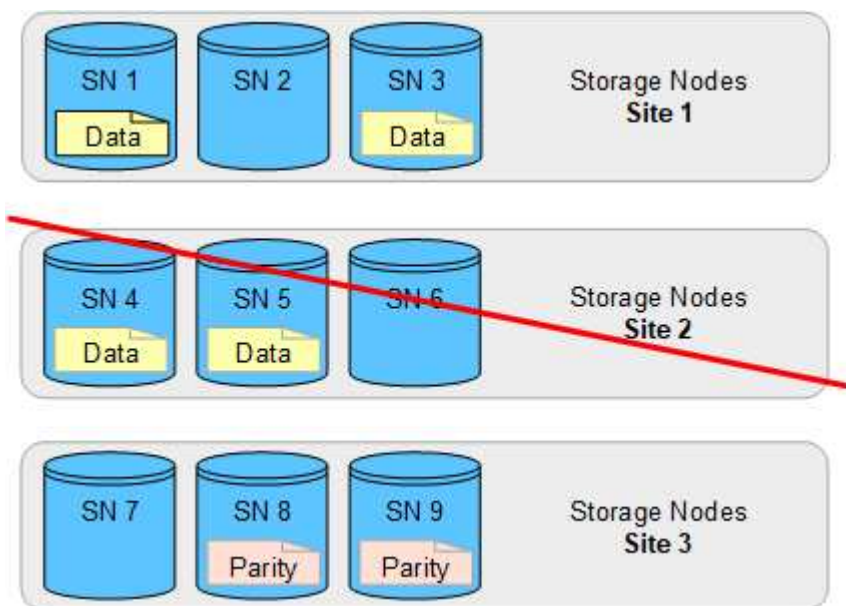


La codifica di cancellazione è consentita nei pool di storage contenenti un numero qualsiasi di siti, ad eccezione di due siti.

Regola ILM con schema di erasure coding 4+2:



In caso di perdita di un sito, è possibile recuperare i dati:



Crea un pool di storage in StorageGRID

Si creano pool di storage per determinare dove il sistema StorageGRID memorizza i dati a oggetti e il tipo di storage utilizzato. Ogni pool di storage include uno o più siti e uno o più tipi di storage.



Quando installi StorageGRID 12.0 o versioni successive su una nuova griglia, i pool di storage vengono creati automaticamente per ogni sito. Tuttavia, se inizialmente hai installato StorageGRID 11.6 o versioni precedenti, i pool di storage non vengono creati automaticamente per ogni sito.

Se si desidera creare pool di cloud storage per archiviare i dati degli oggetti al di fuori del sistema StorageGRID, vedere la ["Informazioni sull'utilizzo dei Cloud Storage Pools"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Hai esaminato le linee guida per la creazione di pool di storage.

A proposito di questa attività

I pool di storage determinano la posizione in cui vengono memorizzati i dati degli oggetti. Il numero di pool di storage necessari dipende dal numero di siti nella griglia e dal tipo di copie desiderato: Replicate o con codifica di cancellazione.

- Per la replica e l'erasure coding a sito singolo, creare un pool di storage per ciascun sito. Ad esempio, se si desidera memorizzare copie di oggetti replicate in tre siti, creare tre pool di storage.
- Per la cancellazione del codice in tre o più siti, creare un pool di storage che includa una voce per ciascun sito. Ad esempio, se si desidera erasure gli oggetti del codice in tre siti, creare un pool di storage.



Non includere il sito All Sites in un pool di storage che verrà utilizzato in un profilo di erasure coding. Invece, Aggiungi una voce separata al pool di storage per ogni sito che memorizzerà i dati sottoposti a erasure coding. Vedere [questo passo](#) per un esempio.

- Se si dispone di più storage di livello, non creare un pool di storage che includa diversi tipi di storage in un singolo sito. Consultare la ["Linee guida per la creazione di pool di storage"](#).

Fasi

1. Selezionare **ILM > Storage Pools**.

La scheda Storage Pools elenca tutti i pool di storage definiti.



Per le nuove installazioni di StorageGRID 11.6 o versioni precedenti, il pool di storage di tutti i nodi di storage viene aggiornato automaticamente ogni volta che si aggiungono nuovi siti del data center. Non utilizzare questo pool nelle regole ILM.

2. Per creare un nuovo pool di storage, selezionare **Crea**.
3. Immettere un nome univoco per il pool di storage. Utilizzare un nome che sia facile da identificare quando si configurano i profili di erasure coding e le regole ILM.
4. Dall'elenco a discesa **Sito**, selezionare un sito per questo pool di storage.

Quando si seleziona un sito, il numero di nodi di archiviazione nella tabella viene aggiornato automaticamente.

In generale, non utilizzare il sito All Sites in alcun pool di storage. Le regole ILM che utilizzano un pool di storage All Sites posizionano gli oggetti in qualsiasi sito disponibile, offrendo un minore controllo sul posizionamento degli oggetti. Inoltre, un pool di storage All Sites utilizza immediatamente i nodi di storage

in un nuovo sito, il che potrebbe non essere il comportamento previsto.

5. Dall'elenco a discesa **Storage grade**, selezionare il tipo di storage da utilizzare se una regola ILM utilizza questo pool di storage.

Il grado dello storage, *include tutti i gradi dello storage*, include tutti i nodi storage nel sito selezionato. Se sono stati creati altri gradi di storage per i nodi di storage nel grid, questi vengono elencati nell'elenco a discesa.

6. se si desidera utilizzare il pool di archiviazione in un profilo di erasure coding multisito, selezionare **Aggiungi più nodi** per aggiungere una voce per ciascun sito al pool di archiviazione.



Viene visualizzato un avviso se si aggiungono più voci con diversi gradi di storage per un sito.

Per rimuovere una voce, seleziona l'icona di eliminazione **X**.

7. Quando si è soddisfatti delle selezioni effettuate, selezionare **Save** (Salva).

Il nuovo pool di storage viene aggiunto all'elenco.

Visualizza i dettagli del pool di storage in StorageGRID

È possibile visualizzare i dettagli di un pool di storage per determinare dove viene utilizzato il pool di storage e per vedere quali nodi e gradi di storage sono inclusi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Fasi

1. Selezionare **ILM > Storage Pools**.

La tabella Storage Pools include le seguenti informazioni per ogni pool di storage che include i nodi di storage:

- **Name:** Il nome univoco del pool di storage.
- **Node count:** Numero di nodi nel pool di storage.
- **Utilizzo dello storage:** Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto su questo nodo. Questo valore non include i metadati degli oggetti.
- **Capacità totale:** Dimensione del pool di storage, che equivale alla quantità totale di spazio utilizzabile per i dati oggetto per tutti i nodi del pool di storage.
- **Utilizzo ILM:** Modalità di utilizzo del pool di storage. Un pool di storage potrebbe essere inutilizzato o potrebbe essere utilizzato in una o più regole ILM, profili di erasure coding o entrambe.

2. Per visualizzare i dettagli di un pool di archiviazione specifico, selezionarne il nome.

Viene visualizzata la pagina dei dettagli del pool di storage.

3. Visualizzare 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
- Storage grade
- Storage usage (utilizzo storage): La percentuale dello spazio utilizzabile totale per i dati degli oggetti utilizzati per il nodo di storage.



Lo stesso valore di utilizzo dello storage (%) viene visualizzato anche nel grafico Storage Used - Object Data per ciascun Storage Node (selezionare **Nodi > Storage Node > Storage**).

4. Visualizzare la scheda **utilizzo ILM** per determinare se il pool di storage è attualmente utilizzato in qualsiasi regola ILM o profilo di erasure coding.
5. Se si desidera, accedere alla pagina **ILM rules** per informazioni e gestione delle regole che utilizzano il pool di storage.

Consultare la ["Istruzioni per l'utilizzo delle regole ILM"](#).

Modifica un pool di storage in StorageGRID

È possibile modificare un pool di storage per modificarne il nome o per aggiornare siti e gradi di storage.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- È stata esaminata la ["linee guida per la creazione di pool di storage"](#).
- Se si intende modificare un pool di storage utilizzato da una regola nel criterio ILM attivo, si è preso in considerazione il modo in cui le modifiche influiranno sul posizionamento dei dati degli oggetti.

A proposito di questa attività

Se si aggiunge un nuovo livello di sito o storage a un pool di storage utilizzato nella policy ILM attiva, tenere presente che i nodi di storage nel nuovo livello di sito o storage non verranno utilizzati automaticamente. Per forzare StorageGRID a utilizzare un nuovo sito o storage grade, è necessario attivare un nuovo criterio ILM dopo aver salvato il pool di storage modificato.

Fasi

1. Selezionare **ILM > Storage Pools**.
2. Selezionare la casella di controllo del pool di storage che si desidera modificare.

Non è possibile modificare il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti).

3. Selezionare **Modifica**.
4. Se necessario, modificare il nome del pool di storage.
5. Se necessario, selezionare altri siti e livelli di storage.

Al cliente viene impedito di modificare il livello del sito o dello storage se il pool di storage viene utilizzato in un profilo di erasure coding e la modifica porterebbe all'invalidità dello schema di erasure coding. Ad

esempio, se un pool di storage utilizzato in un profilo di erasure coding include al momento un livello dello storage con un solo sito, è impossibile utilizzare un livello dello storage con due siti, perché la modifica renderebbe lo schema di erasure coding non valido.



L'aggiunta o la rimozione di siti da un pool di storage non sposterà i dati esistenti sottoposti a erasure coding. 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. Selezionare **Salva**.

Al termine

Se hai aggiunto un nuovo sito o un nuovo livello di storage a un pool di storage utilizzato nella policy ILM attiva, attiva una nuova policy ILM per forzare StorageGRID a utilizzare il nuovo sito o il nuovo livello di storage. Ad esempio, clona la tua policy ILM esistente e poi attiva il clone. Fai riferimento a ["Utilizzare le regole ILM e i criteri ILM"](#).

Rimuovere un pool di storage in StorageGRID

È possibile rimuovere un pool di storage che non viene utilizzato.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso richieste"](#).

Fasi

1. Selezionare **ILM > Storage Pools**.
2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il pool di storage.

Non puoi rimuovere un pool di storage se è utilizzato in una regola ILM o in un profilo di erasure coding. Se necessario, selezionare **nome pool di storage > utilizzo ILM** per determinare dove viene utilizzato il pool di storage.

3. Se il pool di storage che si desidera rimuovere non viene utilizzato, selezionare la casella di controllo.
4. Selezionare **Rimuovi**.
5. Selezionare **OK**.

Utilizza i Cloud Storage Pools

Scopri i Cloud Storage Pool in StorageGRID

Un pool di cloud storage ti permette di usare ILM per spostare i dati degli oggetti al di fuori del tuo sistema StorageGRID. Ad esempio, potresti voler spostare oggetti a cui accedi raramente verso cloud storage a costo inferiore, come Amazon S3 Glacier, S3 Glacier Deep Archive, Google Cloud o il livello di accesso Archive in Microsoft Azure Blob Storage. Oppure, potresti voler mantenere un backup cloud degli oggetti StorageGRID per migliorare il disaster recovery.

Dal punto di vista dell'ILM, un cloud storage pool è simile a un pool di storage. Per archiviare oggetti in entrambe le posizioni, selezioni il pool durante la creazione delle istruzioni di posizionamento per una regola

ILM. Tuttavia, mentre i pool di storage sono costituiti da Storage Nodes all'interno del sistema StorageGRID, un cloud storage pool è costituito da un bucket esterno (S3) o container (Azure Blob Storage).

La tabella confronta i pool di storage con i pool di storage cloud e mostra le analogie e le differenze di alto livello.

	Pool di storage	Pool di cloud storage
Come viene creato?	Utilizzando l'opzione ILM > Storage Pools in Grid Manager.	Utilizzando l'opzione ILM > Storage Pools > Cloud Storage Pools in Grid Manager. È necessario configurare il bucket o il container esterno prima di poter creare il Cloud Storage Pool.
Quanti pool è possibile creare?	Senza limiti.	Fino a 10.
Dove sono memorizzati gli oggetti?	Su uno o più nodi storage all'interno di StorageGRID.	In un bucket Amazon S3, in un container Azure Blob Storage o in Google Cloud esterno al sistema StorageGRID. Se il Cloud Storage Pool è un bucket Amazon S3: • È possibile configurare un ciclo di vita del bucket per la transizione di oggetti a storage a lungo termine e a basso costo, come Amazon S3 Glacier o S3 Glacier Deep Archive. Il sistema di storage esterno deve supportare la classe di storage Glacier e l'API S3 RestoreObject. • È possibile creare pool di storage cloud da utilizzare con AWS Commercial Cloud Services (C2S), che supporta l'AWS Secret Region. Se il pool di cloud storage è un container Azure Blob Storage, StorageGRID sposta l'oggetto al livello Archive. Nota: In generale, non configurare la gestione del ciclo di vita di Azure Blob Storage per il container utilizzato per un Cloud Storage Pool. RestoreObject operazioni sugli oggetti nel Cloud Storage Pool possono essere influenzate dal ciclo di vita configurato.
Cosa controlla il posizionamento degli oggetti?	Una regola ILM nei criteri ILM attivi.	Una regola ILM nei criteri ILM attivi.
Quale metodo di protezione dei dati viene utilizzato?	Replica o erasure coding.	Replica.

	Pool di storage	Pool di cloud storage
Quante copie di ciascun oggetto sono consentite?	Multiplo.	Una copia nel pool di storage cloud e, facoltativamente, una o più copie in StorageGRID. Nota: non è possibile memorizzare un oggetto in più di un Cloud Storage Pool alla volta.
Quali sono i vantaggi?	Gli oggetti sono rapidamente accessibili in qualsiasi momento.	Storage a basso costo. Nota: Non è possibile eseguire il tiering dei dati FabricPool nei pool di storage cloud.

Ciclo di vita di un oggetto pool di storage cloud in StorageGRID

Prima di implementare i Cloud Storage Pool, esaminare il ciclo di vita degli oggetti memorizzati in ciascun tipo di Cloud Storage Pool.

S3: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool S3.



"Glacier" si riferisce sia alla classe di storage Glacier che a quella Glacier Deep Archive, con una sola eccezione: La classe di storage Glacier Deep Archive non supporta il Tier di ripristino Expedited. È supportato solo il recupero in blocco o standard.



Google Cloud Platform (GCP) supporta il recupero di oggetti dallo storage a lungo termine senza richiedere un'operazione POST-ripristino.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato in S3 Cloud Storage Pool

- Quando l'oggetto viene associato a una regola ILM che utilizza un pool di storage cloud S3 come posizione di posizionamento, StorageGRID sposta l'oggetto nel bucket S3 esterno specificato dal pool di storage cloud.
- Quando l'oggetto è stato spostato nel Cloud Storage Pool S3, l'applicazione client può recuperarlo utilizzando una richiesta GetObject S3 da StorageGRID, a meno che l'oggetto non sia stato spostato nello storage Glacier.

3. Oggetto in transizione a Glacier (stato non recuperabile)

- Facoltativamente, l'oggetto può essere passato allo storage Glacier. Ad esempio, il bucket S3 esterno potrebbe utilizzare la configurazione del ciclo di vita per trasferire un oggetto allo storage Glacier immediatamente o dopo un certo numero di giorni.



Per trasferire oggetti, è necessario creare una configurazione del ciclo di vita per il bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

- Durante la transizione, l'applicazione client può utilizzare una richiesta S3 HeadObject per monitorare lo stato dell'oggetto.

4. Oggetto ripristinato dallo storage Glacier

Se un oggetto è stato spostato nello storage Glacier, l'applicazione client può emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile nel Cloud Storage Pool S3. La richiesta specifica il numero di giorni in cui la copia deve essere disponibile nel Cloud Storage Pool e il Tier di accesso ai dati da utilizzare per l'operazione di ripristino (accelerato, Standard o in blocco). Una volta raggiunta la data di scadenza della copia recuperabile, la copia viene automaticamente riportata in uno stato non recuperabile.



Se una o più copie dell'oggetto esistono anche sui nodi di storage all'interno di StorageGRID, non è necessario ripristinare l'oggetto da Glacier mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Azure: Ciclo di vita di un oggetto Cloud Storage Pool

Questa procedura descrive le fasi del ciclo di vita di un oggetto memorizzato in un Cloud Storage Pool di Azure.

1. Oggetto memorizzato in StorageGRID

Per avviare il ciclo di vita, un'applicazione client memorizza un oggetto in StorageGRID.

2. Oggetto spostato in Azure Cloud Storage Pool

Quando l'oggetto viene abbinato a una regola ILM che utilizza un Azure Cloud Storage Pool come posizione di collocazione, StorageGRID sposta l'oggetto nel container Azure Blob Storage esterno specificato dal Cloud Storage Pool.

3. Oggetto sottoposto a transizione al Tier di archiviazione (stato non recuperabile)

Subito dopo aver spostato l'oggetto nel pool di cloud storage di Azure, StorageGRID trasferisce automaticamente l'oggetto al livello Azure Blob Storage Archive.

4. Oggetto ripristinato dal Tier di archiviazione

Se un oggetto è stato spostato nel Tier Archive, l'applicazione client può emettere una richiesta S3 RestoreObject per ripristinare una copia recuperabile nell'Azure Cloud Storage Pool.

Quando StorageGRID riceve la RestoreObject, sposta temporaneamente l'oggetto nel livello Cool di Azure Blob Storage. Non appena viene raggiunta la data di scadenza nella richiesta RestoreObject, StorageGRID riporta l'oggetto al livello Archive.



Se una o più copie dell'oggetto sono presenti anche nei nodi di archiviazione all'interno di StorageGRID, non è necessario ripristinare l'oggetto dal livello di accesso di archiviazione mediante una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

5. Oggetto recuperato

Una volta ripristinato un oggetto in Azure Cloud Storage Pool, l'applicazione client può emettere una richiesta GetObject per recuperare l'oggetto ripristinato.

Informazioni correlate

["UTILIZZARE L'API REST S3"](#)

Casi d'uso del Cloud Storage Pool in StorageGRID

Utilizzando i Cloud Storage Pools, è possibile eseguire il backup o il tiering dei dati in una posizione esterna. Inoltre, puoi eseguire il backup o il Tier dei dati in più cloud.

Eseguire il backup dei dati StorageGRID in una posizione esterna

È possibile utilizzare un pool di storage cloud per eseguire il backup degli oggetti StorageGRID in una posizione esterna.

Se le copie in StorageGRID non sono accessibili, i dati dell'oggetto nel pool di storage cloud possono essere utilizzati per soddisfare le richieste dei client. Tuttavia, potrebbe essere necessario emettere la richiesta S3 RestoreObject per accedere alla copia dell'oggetto di backup nel Cloud Storage Pool.

I dati dell'oggetto in un pool di storage cloud possono essere utilizzati anche per recuperare i dati persi da StorageGRID a causa di un guasto di un volume di storage o di un nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.

Per implementare una soluzione di backup:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che memorizzi simultaneamente le copie degli oggetti sui nodi di storage (come copie replicate o codificate in cancellazione) e una singola copia degli oggetti nel Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Dati di Tier da StorageGRID a posizione esterna

È possibile utilizzare un pool di storage cloud per memorizzare oggetti all'esterno del sistema StorageGRID. Si supponga, ad esempio, di disporre di un elevato numero di oggetti da conservare, ma si prevede di accedervi raramente, se mai. È possibile utilizzare un pool di storage cloud per tierare gli oggetti in modo da ridurre il costo dello storage e liberare spazio in StorageGRID.

Per implementare una soluzione di tiering:

1. Creare un singolo pool di storage cloud.
2. Configurare una regola ILM che sposti gli oggetti utilizzati raramente dai nodi di storage al Cloud Storage Pool.
3. Aggiungere la regola al criterio ILM. Quindi, simulare e attivare la policy.

Mantenere più endpoint cloud

Puoi configurare più endpoint di Cloud Storage Pool se vuoi eseguire il tiering o il backup dei dati degli oggetti

su più cloud. I filtri nelle tue regole ILM ti permettono di specificare quali oggetti vengono archiviati in ciascun Cloud Storage Pool. Ad esempio, potresti voler archiviare gli oggetti di alcuni tenant o bucket in Amazon S3 Glacier e gli oggetti di altri tenant o bucket in Azure Blob Storage. Oppure, potresti voler spostare i dati tra Amazon S3 Glacier e Azure Blob Storage.



Quando si utilizzano endpoint multipli del Cloud Storage Pool, tenere presente che un oggetto può essere memorizzato in un solo Cloud Storage Pool alla volta.

Per implementare più endpoint cloud:

1. Crea fino a 10 pool di cloud storage.
2. Configurare le regole ILM in modo che memorizzino i dati dell'oggetto appropriati all'ora appropriata in ciascun Cloud Storage Pool. Ad esempio, memorizzare gli oggetti dal bucket A nel pool di cloud storage A e gli oggetti dal bucket B nel pool di cloud storage B. oppure gli oggetti nel pool di cloud storage A per un certo periodo di tempo, quindi spostarli nel pool di cloud storage B.
3. Aggiungere le regole alla policy ILM. Quindi, simulare e attivare la policy.

Requisiti e limiti del pool di storage cloud in StorageGRID

Se si prevede di utilizzare un pool di storage cloud per spostare oggetti fuori dal sistema StorageGRID, è necessario esaminare le considerazioni relative alla configurazione e all'utilizzo dei pool di storage cloud.

Considerazioni generali

- In generale, l'archiviazione cloud archivio, come Amazon S3 Glacier o Azure Blob Storage, è un'opzione economica per memorizzare dati a oggetti. Tuttavia, i costi per recuperare dati dall'archiviazione cloud archivio sono relativamente elevati. Per ottenere il costo complessivo più basso, devi considerare quando e con quale frequenza accederai agli oggetti nel Cloud Storage Pool. L'utilizzo di un Cloud Storage Pool è consigliato solo per contenuti a cui prevedi di accedere raramente.
- L'utilizzo dei pool di storage cloud con FabricPool non è supportato a causa della latenza aggiunta per recuperare un oggetto dalla destinazione del pool di storage cloud.
- Gli oggetti con blocco oggetti S3 abilitato non possono essere posizionati nei pool di storage cloud.
- 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:** Accesso anonimo
 - **Protocollo:** HTTP

Considerazioni sulle porte utilizzate per i pool di cloud storage

Per garantire che le regole ILM possano spostare oggetti da e verso il Cloud Storage Pool specificato, è necessario configurare la rete o le reti che contengono i nodi di storage del sistema. È necessario assicurarsi che le seguenti porte possano comunicare con il Cloud Storage Pool.

Per impostazione predefinita, i Cloud Storage Pool utilizzano le seguenti porte:

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

È possibile specificare una porta diversa quando si crea o si modifica un Cloud Storage Pool.

Se si utilizza un server proxy non trasparente, è necessario anche "[configurare un proxy di archiviazione](#)" consentire l'invio di messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Considerazioni sui costi

L'accesso allo storage nel cloud utilizzando un Cloud Storage Pool richiede la connettività di rete al cloud. Devi considerare il costo dell'infrastruttura di rete che utilizzerai per accedere al cloud e fornirlo in modo appropriato, in base alla quantità di dati che prevederai di spostare tra StorageGRID e il cloud utilizzando il pool di storage cloud.

Quando StorageGRID si connette all'endpoint esterno del pool di storage nel cloud, invia varie richieste per monitorare la connettività e garantire che possa eseguire le operazioni richieste. Anche se a queste richieste saranno associati costi aggiuntivi, il costo del monitoraggio di un pool di storage cloud dovrebbe essere solo una piccola frazione del costo complessivo di storage degli oggetti in S3 o Azure.

Se si devono spostare gli oggetti da un endpoint esterno del pool di cloud storage a StorageGRID, potrebbero verificarsi costi più significativi. Gli oggetti possono essere spostati di nuovo in StorageGRID in uno dei seguenti casi:

- L'unica copia dell'oggetto si trova in un pool di storage cloud e si decide di memorizzare l'oggetto in StorageGRID. In questo caso, le regole e i criteri ILM vengono riconfigurati. Quando si verifica la valutazione ILM, StorageGRID invia più richieste per recuperare l'oggetto dal pool di storage cloud. StorageGRID crea quindi localmente il numero specificato di copie replicate o codificate per la cancellazione. Una volta spostato di nuovo l'oggetto in StorageGRID, la copia nel pool di storage cloud viene eliminata.
- Gli oggetti vengono persi a causa di un guasto al nodo di storage. Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID ripristina temporaneamente l'oggetto e crea una nuova copia sul nodo di storage ripristinato.



Quando gli oggetti vengono spostati di nuovo in StorageGRID da un pool di storage cloud, StorageGRID invia più richieste all'endpoint del pool di storage cloud per ciascun oggetto. Prima di spostare un gran numero di oggetti, contattare il supporto tecnico per ottenere assistenza nella stima dei tempi e dei costi associati.

S3: Autorizzazioni richieste per il bucket Cloud Storage Pool

Le policy per il bucket S3 esterno utilizzato per un Cloud Storage Pool devono garantire a StorageGRID l'autorizzazione a 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 con controllo completo al bucket (`s3:*`); tuttavia, se ciò non è possibile, il criterio bucket deve concedere le seguenti autorizzazioni S3 a StorageGRID:

- `s3:AbortMultipartUpload`
- `s3:DeleteObject`
- `s3:GetObject`
- `s3:ListBucket`
- `s3:ListBucketMultipartUploads`
- `s3:ListMultipartUploadParts`

- s3:PutObject
- s3:RestoreObject

S3: Considerazioni sul ciclo di vita del bucket esterno

Lo spostamento degli oggetti tra StorageGRID e il bucket S3 esterno specificato nel pool di storage cloud è controllato dalle regole ILM e dalle policy ILM attive in StorageGRID. Al contrario, la transizione degli oggetti dal bucket S3 esterno specificato nel Cloud Storage Pool ad Amazon S3 Glacier o S3 Glacier Deep Archive (o a una soluzione di storage che implementa la classe di storage Glacier) è controllata dalla configurazione del ciclo di vita di tale bucket.

Per trasferire oggetti da Cloud Storage Pool, è necessario creare la configurazione del ciclo di vita appropriata nel bucket S3 esterno e utilizzare una soluzione storage che implementi la classe di storage Glacier e supporti l'API S3 RestoreObject.

Ad esempio, supponiamo che tutti gli oggetti spostati da StorageGRID al pool di storage cloud debbano essere trasferiti immediatamente allo storage Amazon S3 Glacier. Creare una configurazione del ciclo di vita sul bucket S3 esterno che specifica una singola azione (**transizione**) come segue:

```
<LifecycleConfiguration>
  <Rule>
    <ID>Transition Rule</ID>
    <Filter>
      <Prefix></Prefix>
    </Filter>
    <Status>Enabled</Status>
    <Transition>
      <Days>0</Days>
      <StorageClass>GLACIER</StorageClass>
    </Transition>
  </Rule>
</LifecycleConfiguration>
```

Questa regola trasferirebbe tutti gli oggetti bucket al Glacier Amazon S3 il giorno in cui sono stati creati (ovvero il giorno in cui sono stati spostati da StorageGRID al pool di storage cloud).



Quando si configura il ciclo di vita del bucket esterno, non utilizzare mai le azioni **Expiration** per definire quando gli oggetti scadono. Le azioni di scadenza fanno sì che il sistema di storage esterno elimini gli oggetti scaduti. Se in seguito si tenta di accedere a un oggetto scaduto da StorageGRID, l'oggetto eliminato non viene trovato.

Per trasferire oggetti in Cloud Storage Pool in S3 Glacier Deep Archive (invece di su 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 da S3 Glacier Deep Archive.

Azure: Considerazioni per il Tier di accesso

Quando si configura un account di storage Azure, è possibile impostare il Tier di accesso predefinito su Hot o Cool. Quando si crea un account storage da utilizzare con un Cloud Storage Pool, è necessario utilizzare l'hot

Tier come Tier predefinito. Anche se StorageGRID imposta immediatamente il Tier per l'archiviazione quando sposta gli oggetti nel pool di storage cloud, l'utilizzo dell'impostazione predefinita di Hot garantisce che non venga addebitata una tariffa per l'eliminazione anticipata degli oggetti rimossi dal Tier Cool prima del minimo di 30 giorni.

Azure: Gestione del ciclo di vita non supportata

Non usare la gestione del ciclo di vita di Azure Blob Storage per il container utilizzato con un Cloud Storage Pool. Le operazioni di ciclo di vita potrebbero interferire con le operazioni del Cloud Storage Pool.

Informazioni correlate

["Creare un pool di storage cloud"](#)

Pool di storage cloud e replica CloudMirror in StorageGRID

Quando si inizia a utilizzare i pool di storage cloud, potrebbe essere utile comprendere le analogie e le differenze tra i pool di storage cloud e il servizio di replica di StorageGRID CloudMirror.

	Pool di cloud storage	Servizio di replica di CloudMirror
Qual è lo scopo principale?	Agisce come destinazione di archiviazione. La copia dell'oggetto nel Cloud Storage Pool può essere l'unica copia dell'oggetto oppure può essere una copia aggiuntiva. Ovvero, invece di conservare due copie in loco, puoi conservarne una all'interno di StorageGRID e inviarne una copia al pool di storage cloud.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). Crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente.
Come viene configurato?	Definito allo stesso modo dei pool di storage, utilizzando Grid Manager o l'API Grid Management. Può essere selezionata come posizione di posizionamento in una regola ILM. Mentre un pool di storage è costituito da un gruppo di nodi di storage, un pool di storage cloud viene definito utilizzando un endpoint remoto S3 o Azure (indirizzo IP, credenziali e così via).	Un utente tenant " Configura la replica di CloudMirror " definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. Una volta configurato l'endpoint CloudMirror, qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.
Chi è responsabile della sua configurazione?	In genere, un amministratore di rete	In genere, un utente tenant
Qual è la destinazione?	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Tier Azure Blob Archive • Piattaforma Google Cloud (GCP)	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3) • Piattaforma Google Cloud (GCP)

	Pool di cloud storage	Servizio di replica di CloudMirror
Qual è la causa dello spostamento degli oggetti nella destinazione?	Una o più regole ILM nei criteri ILM attivi. Le regole ILM definiscono gli oggetti che StorageGRID sposta nel pool di storage cloud e quando gli oggetti vengono spostati.	L'atto di inserire un nuovo oggetto in un bucket di origine configurato con un endpoint CloudMirror. Gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono recuperati gli oggetti?	Le applicazioni devono effettuare richieste a StorageGRID per recuperare gli oggetti spostati in un pool di storage cloud. Se l'unica copia di un oggetto è stata trasferita allo storage di archiviazione, StorageGRID gestisce il processo di ripristino dell'oggetto in modo che possa essere recuperato.	Poiché la copia mirrorata nel bucket di destinazione è una copia indipendente, le applicazioni possono recuperare l'oggetto inviando richieste a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.
Puoi leggere direttamente dalla destinazione?	No. Gli oggetti spostati in un pool di cloud storage sono gestiti da StorageGRID. Le richieste di lettura devono essere indirizzate a StorageGRID (e StorageGRID sarà responsabile del recupero dal pool di storage cloud).	Sì, perché la copia mirrorata è una copia indipendente.
Cosa succede se un oggetto viene cancellato dall'origine?	L'oggetto viene anche eliminato dal Cloud Storage Pool.	L'azione di eliminazione non viene replicata. Un oggetto cancellato non esiste più nel bucket StorageGRID, ma continua ad esistere nel bucket di destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.
Come si accede agli oggetti dopo un disastro (sistema StorageGRID non operativo)?	I nodi StorageGRID guasti devono essere ripristinati. Durante questo processo, le copie degli oggetti replicati potrebbero essere ripristinate utilizzando le copie nel Cloud Storage Pool.	Le copie degli oggetti nella destinazione CloudMirror sono indipendenti da StorageGRID, pertanto è possibile accedervi direttamente prima del ripristino dei nodi StorageGRID.

Crea un pool di storage cloud in StorageGRID

Un pool di storage cloud specifica un singolo bucket Amazon S3 esterno o un altro cloud provider compatibile con S3 oppure un container Azure Blob Storage.

Quando crei un Cloud Storage Pool, specifichi il nome e la posizione del bucket o container esterno che

StorageGRID userà per archiviare gli oggetti, il tipo di cloud provider (Amazon S3/GCP o Azure Blob Storage) e le informazioni di cui StorageGRID ha bisogno per accedere al bucket o container esterno.

StorageGRID convalida il pool di storage cloud non appena viene salvato, quindi devi assicurarti che il bucket o il container specificato nel pool di storage cloud esista e sia raggiungibile.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso richieste"](#).
- È stata esaminata la ["Considerazioni per i Cloud Storage Pools"](#).
- Il bucket o contenitore esterno a cui fa riferimento il Cloud Storage Pool esiste già e si dispone di [informazioni sull'endpoint di servizio](#).
- Per accedere al secchio o al contenitore, è [informazioni sull'account per il tipo di autenticazione](#) possibile scegliere.

Fasi

1. Selezionare **ILM > Storage Pools > Cloud Storage Pools**.
2. Selezionare **Crea**, quindi immettere le seguenti informazioni:

Campo	Descrizione
Nome del pool di cloud storage	Un nome che descrive brevemente il Cloud Storage Pool e il suo scopo. Utilizzare un nome che sia facile da identificare quando si configurano le regole ILM.
Tipo di provider	Quale cloud provider utilizzerai per questo Cloud Storage Pool: • Amazon S3/GCP: Selezionare questa opzione per Amazon S3, Commercial Cloud Services (C2S) S3, Google Cloud Platform (GCP) o altri provider compatibili con S3. • Azure Blob Storage
Bucket o container	Il nome del bucket S3 esterno o del container Azure. Non puoi modificare questo valore dopo il salvataggio del Cloud Storage Pool.

3. in base alla selezione del tipo di provider, 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. Inserire il nome host. Esempio:

`s3-aws-region.amazonaws.com`

- c. Selezionare lo stile URL:

Opzione	Descrizione
Rilevamento automatico	Tentare di rilevare automaticamente lo stile URL da utilizzare, in base alle informazioni fornite. Ad esempio, se si specifica un indirizzo IP, StorageGRID utilizzerà un URL di tipo path. Selezionare questa opzione solo se non si conosce lo stile specifico da utilizzare.
Stile virtual-hosted	Utilizza un URL di tipo virtual-hosted per accedere al bucket. Gli URL in stile virtual-hosted includono il nome del bucket come parte del nome di dominio. Esempio: <code>https://bucket-name.s3.company.com/key-name</code>
Stile di percorso	Utilizzare un URL stile percorso per accedere al bucket. Gli URL stile percorso includono il nome del bucket alla fine Esempio: <code>https://s3.company.com/bucket-name/key-name</code> Nota: l'opzione URL stile percorso non è consigliata e sarà obsoleta in una release futura di StorageGRID.

- d. Se si desidera, inserire il numero della porta o utilizzare la porta predefinita: 443 per HTTPS o 80 per HTTP.

Azure Blob Storage

- a. Utilizzando uno dei seguenti formati, immettere l'URI per l'endpoint del servizio.

- `https://host:port`
- `http://host:port`

Esempio: `https://myaccount.blob.core.windows.net:443`

Se non si specifica una porta, per impostazione predefinita viene utilizzata la porta 443 per HTTPS e la porta 80 per HTTP.

4. selezionare **Continue**. Quindi, selezionare il tipo di autenticazione e immettere le informazioni richieste per l'endpoint del Cloud Storage Pool:

Tasto di accesso

Per Amazon S3/GCP o altro provider compatibile con S3

- a. **ID chiave di accesso:** Immettere l'ID della chiave di accesso per l'account proprietario del bucket esterno.
- b. **Chiave di accesso segreta:** Immettere la chiave di accesso segreta.

Ruoli IAM ovunque

Per AWS IAM Roles Anywhere service

StorageGRID utilizza AWS Security Token Service (STS) per generare dinamicamente un token di breve durata per accedere alle risorse AWS.

- a. **AWS IAM Roles Anywhere Region:** Selezionare la regione per il Cloud Storage Pool. Ad esempio, `us-east-1`.
- b. **Trust anchor URN:** Immettere l'URN dell'ancoraggio trust che convalida le richieste per le credenziali STS di breve durata. Può essere una CA principale o intermedia.
- c. **URN profilo:** Immettere l'URN del profilo IAM Roles Anywhere che elenca i ruoli che possono essere assunti da chiunque sia attendibile.
- d. **Role URN:** Inserire l'URN del ruolo IAM che può essere assunto da chiunque sia attendibile.
- e. **Durata sessione:** Immettere la durata delle credenziali di protezione temporanee e della sessione ruolo. Immettere almeno 15 minuti e non più di 12 ore.
- f. **Certificato CA del server** (opzionale): Uno o più certificati CA attendibili, in formato PEM, per la verifica del server IAM Roles Anywhere. Se omesso, il server non verrà verificato.
- g. **Certificato dell'entità finale:** La chiave pubblica, in formato PEM, del certificato X509 firmato dall'ancoraggio trust. 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 Commercial Cloud Services (C2S) S3

- a. **URL 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 all'account C2S.
- b. **Certificato CA del server:** Selezionare **Sfoglia** e caricare il certificato CA utilizzato da StorageGRID per verificare il CAP server. Il certificato deve essere codificato PEM ed emesso da un'autorità di certificazione pubblica competente (CA).
- c. **Certificato client:** Selezionare **Sfoglia** e caricare il certificato che StorageGRID utilizzerà per identificarsi nel CAP server. Il certificato client deve essere codificato PEM, rilasciato da un'autorità di certificazione pubblica (CA) appropriata e deve essere concesso l'accesso al conto C2S.
- d. **Chiave privata client:** Selezionare **Sfoglia** e caricare la chiave privata codificata PEM per il certificato client.
- e. Se la chiave privata del client è crittografata, immettere la passphrase per la decrittografia della chiave privata del client. In caso contrario, lasciare vuoto il campo **Password chiave privata client**.



Se il certificato client viene crittografato, utilizzare il formato tradizionale per la crittografia. Il formato crittografato PKCS n. 8 non è supportato.

Azure Blob Storage

Per l'archiviazione BLOB di Azure, solo chiave condivisa

- Nome account:** Immettere il nome dell'account di archiviazione proprietario del contenitore esterno
- Codice account:** Immettere la chiave segreta per l'account di archiviazione

È possibile utilizzare il portale Azure per trovare questi valori.

Anonimo

Non sono richieste informazioni aggiuntive.

5. Selezionare **continua**. Quindi scegliere il tipo di verifica del server che si desidera utilizzare:

Opzione	Descrizione
Utilizzare i certificati della CA principale nel sistema operativo del nodo di storage	Utilizzare i certificati Grid CA installati nel sistema operativo per proteggere le connessioni.
USA certificato CA personalizzato	Utilizzare un certificato CA personalizzato. Selezionare Sfoglia e caricare il certificato codificato PEM.
Non verificare il certificato	La selezione di questa opzione indica che le connessioni TLS al Cloud Storage Pool non sono sicure.

6. Selezionare **Salva**.

Quando si salva un pool di storage cloud, StorageGRID esegue le seguenti operazioni:

- Convalida l'esistenza del bucket o del container e dell'endpoint del servizio e la possibilità di raggiungerli utilizzando le credenziali specificate.
- Scrive un file marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere mai questo file, che è denominato `x-ntap-sgws-cloud-pool-uuid`.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida non è riuscita. Ad esempio, se si verifica un errore nel certificato o se il bucket o il container specificato non esiste già, potrebbe essere visualizzato un errore.

7. Se si verifica un errore, consultare la sezione ["Istruzioni per la risoluzione dei problemi dei Cloud Storage Pools"](#), risolvere eventuali problemi, quindi provare a salvare nuovamente il Cloud Storage Pool.

Informazioni correlate

["Porte utilizzate per le comunicazioni esterne"](#)

Visualizza i dettagli del pool di storage cloud in StorageGRID

Puoi visualizzare i dettagli di un Cloud Storage Pool per determinare dove viene utilizzato e per vedere quali nodi e gradi di storage sono inclusi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Fasi

1. Selezionare **ILM > Storage Pools > Cloud Storage Pools**.

La tabella Cloud Storage Pools include le seguenti informazioni per ogni Cloud Storage Pool che include i nodi di storage:

- **Nome:** Il nome univoco visualizzato del pool.
- **URI:** L'Uniform Resource Identifier del Cloud Storage Pool.
- **Tipo di provider:** Quale provider cloud viene utilizzato per questo pool di archiviazione cloud.
- **Container:** Il nome del bucket utilizzato per il pool di archiviazione cloud.
- **Utilizzo ILM:** Modalità di utilizzo del pool. Un Cloud Storage Pool potrebbe essere inutilizzato o potrebbe essere utilizzato in una o più regole ILM, profili di erasure coding o entrambe.
- **Ultimo errore:** L'ultimo errore rilevato durante un controllo dello stato di salute di questo pool di archiviazione cloud.

2. Per visualizzare i dettagli di un pool di cloud storage specifico, selezionarne il nome.

Viene visualizzata la pagina dei dettagli del pool.

3. Visualizzare la scheda **autenticazione** per informazioni sul tipo di autenticazione per questo Cloud Storage Pool e per modificare i dettagli di autenticazione.
4. Visualizzare la scheda **verifica server** per informazioni sui dettagli della verifica, modificare la verifica, scaricare un nuovo certificato o copiare il PEM del certificato.
5. Visualizzare la scheda **utilizzo ILM** per determinare se il Cloud Storage Pool è attualmente utilizzato in qualsiasi regola ILM o profilo di erasure coding.
6. In alternativa, andare alla pagina **regole ILM** ["informazioni e gestione di eventuali regole"](#) che utilizzano il Cloud Storage Pool.

Modifica un pool di storage cloud in StorageGRID

È possibile modificare un Cloud Storage Pool per modificarne il nome, l'endpoint del servizio o altri dettagli; tuttavia, non è possibile modificare il bucket S3 o il container Azure per un Cloud Storage Pool.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- È stata esaminata la ["Considerazioni per i Cloud Storage Pools"](#).

Fasi

1. Selezionare **ILM > Storage Pools > Cloud Storage Pools**.

La tabella Cloud Storage Pools elenca i Cloud Storage Pools esistenti.

2. Seleziona la casella di controllo per il Cloud Storage Pool che desideri modificare, quindi seleziona **azioni > Modifica**.

In alternativa, selezionare il nome del pool di archiviazione cloud, quindi selezionare **Modifica**.

3. Come richiesto, modificare il nome del Cloud Storage Pool, l'endpoint del servizio, le credenziali di autenticazione o il metodo di verifica del certificato.



Non puoi modificare il tipo di provider, il bucket S3 o il container Azure per un Cloud Storage Pool.

Se in precedenza è stato caricato un certificato server o client, è possibile espandere la fisarmonica **Dettagli certificato** per rivedere il certificato attualmente in uso.

4. Selezionare **Salva**.

Quando si salva un pool di storage cloud, StorageGRID convalida l'esistenza del bucket o del container e dell'endpoint del servizio e che è possibile raggiungerli utilizzando le credenziali specificate.

Se la convalida del Cloud Storage Pool non riesce, viene visualizzato un messaggio di errore. Ad esempio, se si verifica un errore del certificato, potrebbe essere visualizzato un errore.

Consultare le istruzioni per "[Risoluzione dei problemi relativi ai pool di storage cloud](#)", risolvere il problema, quindi riprovare a salvare il Cloud Storage Pool.

Rimuovere un Cloud Storage Pool in StorageGRID

È possibile rimuovere un Cloud Storage Pool se non utilizzato in una regola ILM e non contiene dati oggetto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[autorizzazioni di accesso richieste](#)".

Se necessario, utilizzare ILM per spostare i dati dell'oggetto

Se il Cloud Storage Pool che si desidera rimuovere contiene dati a oggetti, è necessario utilizzare ILM per spostare i dati in una posizione diversa. Ad esempio, è possibile spostare i dati su nodi di storage nel proprio grid o su un pool di storage cloud diverso.

Fasi

1. Selezionare **ILM > Storage Pools > Cloud Storage Pools**.

2. Esaminare la colonna relativa all'utilizzo di ILM nella tabella per determinare se è possibile rimuovere il Cloud Storage Pool.

Non puoi rimuovere un Cloud Storage Pool se viene utilizzato in una regola ILM o in un profilo di erasure coding.

3. Se si utilizza il Cloud Storage Pool, selezionare **cloud storage pool name > ILM usage**.
4. ["Clonare ogni regola ILM"](#) Che attualmente colloca gli oggetti nel pool di cloud storage da rimuovere.
5. Determinare dove si desidera spostare gli oggetti esistenti gestiti da ciascuna regola clonata.

È possibile utilizzare uno o più pool di storage o un pool di storage cloud diverso.

6. Modificare ciascuna regola clonata.

Per la fase 2 della creazione guidata regola ILM, selezionare la nuova posizione dal campo **copie at**.

7. ["Creare un nuovo criterio ILM"](#) e sostituire ciascuna delle vecchie regole con una regola clonata.
8. Attivare la nuova policy.
9. Attendere che ILM rimuova gli oggetti dal Cloud Storage Pool e li inseri nella nuova posizione.

Eliminare il pool di storage cloud

Quando il Cloud Storage Pool è vuoto e non viene utilizzato in alcuna regola ILM, è possibile eliminarlo.

Prima di iniziare

- Sono state rimosse tutte le regole ILM che potrebbero aver utilizzato il pool.
- Hai confermato che il bucket S3 o il container Azure non contiene oggetti.

Si verifica un errore se si tenta di rimuovere un Cloud Storage Pool se contiene oggetti. Vedere ["Risolvere i problemi dei pool di storage cloud"](#).



Quando crei un pool di storage cloud, StorageGRID scrive un file di marker nel bucket o nel container per identificarlo come pool di storage cloud. Non rimuovere questo file, che è denominato `x-ntap-sgws-cloud-pool-uuid`.

Fasi

1. Selezionare **ILM > Storage Pools > Cloud Storage Pools**.
2. Se la colonna ILM Usage (utilizzo ILM) indica che il Cloud Storage Pool non è in uso, selezionare la casella di controllo.
3. Selezionare **azioni > Rimuovi**.
4. Selezionare **OK**.

Risoluzione dei problemi dei pool di storage cloud in StorageGRID

Utilizzare questi passaggi per la risoluzione dei problemi per risolvere gli errori che potrebbero verificarsi durante la creazione, la modifica o l'eliminazione di un pool di storage cloud.

Determinare se si è verificato un errore

StorageGRID esegue un semplice controllo dello stato di salute di ogni pool di cloud storage leggendo l'oggetto noto `x-ntap-sgws-cloud-pool-uuid` per assicurarsi che il pool di cloud storage sia accessibile e funzioni correttamente. Quando StorageGRID rileva un errore nell'endpoint, esegue un controllo di integrità ogni minuto da ogni nodo di storage. Quando l'errore viene risolto, i controlli dello stato si interrompono. Se un controllo di integrità rileva un problema, viene visualizzato un messaggio nella colonna ultimo errore della

tabella Pool di archiviazione cloud nella pagina Pool di archiviazione.

La tabella mostra l'errore più recente rilevato per ciascun Cloud Storage Pool e indica quanto tempo fa si è verificato l'errore.

Inoltre, un avviso di **errore di connettività del Cloud Storage Pool** viene attivato se il controllo dello stato di salute rileva che uno o più nuovi errori del Cloud Storage Pool si sono verificati negli ultimi 5 minuti. Se si riceve una notifica via email per questo avviso, accedere alla pagina Storage Pools (selezionare **ILM > Storage Pools**), esaminare i messaggi di errore nella colonna Last error (ultimo errore) e consultare le linee guida per la risoluzione dei problemi riportate di seguito.

Controllare se un errore è stato risolto

Dopo aver risolto eventuali problemi sottostanti, è possibile determinare se l'errore è stato risolto. Dalla pagina Cloud Storage Pool, selezionare l'endpoint e selezionare **Clear error**. Un messaggio di conferma indica che StorageGRID ha eliminato l'errore per il pool di storage cloud.

Se il problema sottostante è stato risolto, il messaggio di errore non viene più visualizzato. Tuttavia, se il problema sottostante non è stato risolto (o se si verifica un errore diverso), il messaggio di errore viene visualizzato nella colonna Last error (ultimo errore) entro pochi minuti.

Errore: Controllo dello stato di salute non riuscito. Errore dall'endpoint

Potresti riscontrare questo errore in uno di questi casi:

- Quando abiliti S3 Object Lock con conservazione predefinita per il tuo bucket Amazon S3 dopo aver iniziato a usare 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 risolvere questo problema, segui i passaggi in "[Modifica di un pool di storage cloud](#)" senza apportare modifiche. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock sulla configurazione dell'endpoint del Cloud Storage Pool.

- Quando abiliti S3 Object Lock con conservazione predefinita per il tuo bucket S3 di StorageGRID dopo aver iniziato a usare questo bucket per un Cloud Storage Pool.

Per risolvere questo problema:

- Se usi HTTP: i cloud storage pool con S3 Object Lock abilitato non sono supportati. Modifica la connessione dell'endpoint per usare HTTPS.
- Se stai usando HTTPS: segui i passaggi in "[Modifica di un pool di storage cloud](#)" senza apportare modifiche. Questa azione attiva la convalida della configurazione del Cloud Storage Pool che rileva e aggiorna automaticamente il flag S3 Object Lock sulla configurazione dell'endpoint del Cloud Storage Pool.

Se hai altri problemi, contatta il supporto tecnico.

Errore: Questo Cloud Storage Pool contiene contenuti imprevisti

Questo errore potrebbe verificarsi quando si tenta di creare, modificare o eliminare un pool di storage cloud. Questo errore si verifica se il bucket o il contenitore include il x-ntap-sgws-cloud-pool-uuid file marcatore, ma quel file non ha il campo metadati con l'UUID previsto.

In genere, questo errore viene visualizzato solo se si crea un nuovo pool di storage cloud e un'altra istanza di

StorageGRID sta già utilizzando lo stesso pool di storage cloud.

Per risolvere il problema, provare a eseguire una delle seguenti operazioni:

- Se stai configurando un nuovo Cloud Storage Pool e il bucket contiene il `x-ntap-sgws-cloud-pool-uuid` file e le chiavi oggetto aggiuntive simili all'esempio seguente, crea un nuovo bucket e utilizza invece questo nuovo bucket.

Esempio di 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, eliminarlo.

Se questi passaggi non si applicano al proprio scenario, contattare 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 blocco oggetto S3 durante la configurazione di un nuovo Cloud Storage Pool. Vedere ["Considerazioni per i Cloud Storage Pools"](#).

Questo errore indica che un problema di connettività o di configurazione impedisce la scrittura di StorageGRID nel pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

- Se il messaggio di errore contiene `Get url: EOF`, controllare che l'endpoint del servizio utilizzato per il 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, autenticazione o protocollo non supportati, passare a una configurazione supportata con blocco oggetti S3 e provare a salvare nuovamente il nuovo Cloud Storage Pool.
- Per tutti gli altri messaggi di errore degli endpoint, provare una o più delle seguenti soluzioni:
 - Creare un container o bucket esterno con lo stesso nome immesso per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.
 - Correggere il nome del container o bucket specificato per il Cloud Storage Pool e provare a salvare di nuovo il nuovo Cloud Storage Pool.

Errore: Impossibile analizzare il certificato CA

Questo errore potrebbe verificarsi quando si tenta di creare o modificare un pool di storage cloud. L'errore si verifica se StorageGRID non ha potuto analizzare il certificato inserito durante la configurazione del pool di storage cloud.

Per correggere il problema, controllare il certificato CA fornito per eventuali problemi.

Errore: Impossibile trovare un pool di storage cloud con questo ID

Questo errore potrebbe verificarsi quando si tenta di modificare o eliminare un pool di storage cloud. Questo errore si verifica se l'endpoint restituisce una risposta 404, il che può significare una delle seguenti:

- Le credenziali utilizzate per il Cloud Storage Pool non dispongono dell'autorizzazione di lettura per il bucket.
- Il bucket utilizzato per il pool di cloud storage non include il `x-ntap-sgws-cloud-pool-uuid` file marker.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare che l'utente associato alla chiave di accesso configurata disponga delle autorizzazioni necessarie.
- Modificare il Cloud Storage Pool con le credenziali che dispongono delle autorizzazioni necessarie.
- Se le autorizzazioni sono corrette, contattare l'assistenza.

Errore: Impossibile controllare il contenuto del Cloud Storage Pool. Errore dall'endpoint

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore indica che un problema di connettività o configurazione impedisce a StorageGRID di leggere il contenuto del bucket del pool di storage cloud.

Per risolvere il problema, esaminare il messaggio di errore dall'endpoint.

Errore: Gli oggetti sono già stati posizionati in questo bucket

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Non è possibile eliminare un Cloud Storage Pool se contiene dati spostati da ILM, dati presenti nel bucket prima della configurazione del Cloud Storage Pool o dati inseriti nel bucket da un'altra origine dopo la creazione del Cloud Storage Pool.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Segui le istruzioni per riportare gli oggetti in StorageGRID in "ciclo di vita di un oggetto Cloud Storage Pool".
- Se si è certi che ILM non abbia inserito gli oggetti rimanenti nel Cloud Storage Pool, eliminarli manualmente dal bucket.



Non eliminare mai manualmente oggetti da un Cloud Storage Pool che potrebbe essere stato collocato in tale posizione da ILM. Se in un secondo momento si tenta di accedere a un oggetto eliminato manualmente da StorageGRID, l'oggetto eliminato non viene trovato.

Errore: Il proxy ha rilevato un errore esterno durante il tentativo di raggiungere il Cloud Storage Pool

È possibile che si verifichi questo errore se è stato configurato un proxy di storage non trasparente tra i nodi di storage e l'endpoint S3 esterno utilizzato per il Cloud Storage Pool. Questo errore si verifica se il server proxy esterno non riesce a raggiungere l'endpoint del Cloud Storage Pool. Ad esempio, il server DNS potrebbe non essere in grado di risolvere il nome host o potrebbe esserci un problema di rete esterno.

Provare una o più delle seguenti operazioni per risolvere il problema:

- Verificare le impostazioni del Cloud Storage Pool (**ILM > Storage Pools**).
- Controllare la configurazione di rete del server proxy di archiviazione.

Errore: Il certificato X,509 non è valido

Questo errore potrebbe verificarsi quando si tenta di eliminare un pool di storage cloud. Questo errore si verifica quando l'autenticazione richiede un certificato X,509 per garantire la convalida del Cloud Storage Pool esterno corretto e il pool esterno è vuoto prima di eliminare la configurazione del Cloud Storage Pool.

Per risolvere il problema, attenersi alla seguente procedura:

- Aggiornare il certificato configurato per l'autenticazione al Cloud Storage Pool.
- Assicurarsi che qualsiasi avviso di scadenza del certificato su questo Cloud Storage Pool sia stato risolto.

Informazioni correlate

["Ciclo di vita di un oggetto Cloud Storage Pool"](#)

Gestisci i profili di codifica di cancellazione in StorageGRID

È possibile visualizzare i dettagli di un profilo di erasure coding e rinominare un profilo, se necessario. È possibile disattivare un profilo di erasure coding se non è attualmente utilizzato in nessuna regola ILM.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso richieste"](#).

Visualizza i dettagli del profilo di erasure coding

È possibile visualizzare i dettagli di un profilo di erasure coding per determinarne lo stato, lo schema di erasure coding utilizzato e altre informazioni.

Fasi

1. Selezionare **Configurazione > Sistema > Codifica di cancellazione**.
2. Selezionare il profilo. Viene visualizzata la pagina dei dettagli del profilo.
3. In alternativa, è possibile visualizzare la scheda regole ILM per un elenco di regole ILM che utilizzano il profilo e i criteri ILM che utilizzano tali regole.
4. Facoltativamente, visualizzare la scheda nodi di archiviazione per i dettagli su ciascun nodo di archiviazione nel pool di archiviazione del profilo, ad esempio il sito in cui si trova e l'utilizzo dello storage.

Rinominare un profilo con erasure coding

Si consiglia di rinominare un profilo di erasure coding in modo da renderlo più ovvio.

Fasi

1. Selezionare **Configurazione > Sistema > Codifica di cancellazione**.
2. Selezionare il profilo che si desidera rinominare.
3. Selezionare **Rinomina**.

4. Immettere un nome univoco per il profilo di erasure coding.

Il nome del profilo di erasure coding viene aggiunto al nome del pool di storage nelle istruzioni di posizionamento di una regola ILM.



I nomi dei profili di erasure coding devono essere univoci. Si verifica un errore di convalida se si utilizza il nome di un profilo esistente, anche se tale profilo è stato disattivato.

5. Selezionare **Salva**.

Disattivare un profilo di erasure coding

È possibile disattivare un profilo di erasure coding se non si prevede più di utilizzarlo e se il profilo non è attualmente utilizzato in nessuna regola ILM.



Verificare che non siano in corso operazioni di riparazione dei dati sottoposte a erasure coding o procedure di decommissionamento. Viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di erasure coding mentre è in corso una di queste operazioni.

A proposito di questa attività

StorageGRID ti impedisce di disattivare un profilo di erasure coding se si verifica una delle seguenti condizioni:

- Il profilo di erasure coding è attualmente utilizzato in una regola ILM.
- Il profilo di erasure coding non viene più utilizzato in nessuna regola ILM, ma i dati degli oggetti e i frammenti di parità per il profilo esistono ancora.

Fasi

1. Selezionare **Configurazione > Sistema > Codifica di cancellazione**.
2. Nella scheda attivo, esaminare la colonna **Stato** per confermare che il profilo di erasure coding che si desidera disattivare non è utilizzato in nessuna regola ILM.

Non è possibile disattivare un profilo di erasure coding se è utilizzato in qualsiasi regola ILM. Nell'esempio, il profilo 2+1 Data Center 1 viene utilizzato in almeno una regola ILM.

☐	Profile name ?	Status ?	Storage pool ?	Erasure-coding scheme ?
☐	2+1 Data Center 1	Used in <u>5 rules</u>	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 ed esaminare il diagramma di conservazione per determinare se la regola utilizza il profilo di erasure coding che si desidera disattivare.
 - c. Se la regola ILM utilizza il profilo di erasure coding che si desidera disattivare, determinare se la regola è utilizzata in qualsiasi criterio ILM.
 - d. Completare i passaggi aggiuntivi nella tabella, in base alla posizione in cui viene utilizzato il profilo di erasure coding.

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
Mai utilizzato in nessuna regola ILM	Non sono necessari passaggi aggiuntivi. Continuare con questa procedura.	Nessuno
In una regola ILM che non è mai stata utilizzata in alcun criterio ILM	i. Modificare o eliminare tutte le regole ILM interessate. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. ii. Continuare con questa procedura.	"Utilizzare le regole ILM e i criteri ILM"
In una regola ILM che è attualmente in un criterio ILM attivo	i. Clonazione della policy. ii. Rimuovere la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungere una o più nuove regole ILM per garantire la protezione degli oggetti. iv. Salvare, simulare e attivare la nuova policy. v. Attendere che il nuovo criterio venga applicato e che gli oggetti esistenti vengano spostati in nuove posizioni in base alle nuove regole aggiunte. Nota: a seconda del numero di oggetti e delle dimensioni del sistema StorageGRID, potrebbero essere necessarie settimane o addirittura mesi per le operazioni ILM per spostare gli oggetti in nuove posizioni, in base alle nuove regole ILM. Mentre è possibile tentare di disattivare un profilo di erasure coding mentre è ancora associato ai dati, l'operazione di disattivazione non riesce. Se il profilo non è ancora pronto per la disattivazione, viene visualizzato un messaggio di errore. vi. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. vii. Continuare con questa procedura.	"Creare un criterio ILM" "Utilizzare le regole ILM e i criteri ILM"

Dove è stato utilizzato il profilo?	Ulteriori passaggi da eseguire prima di disattivare il profilo	Fare riferimento a queste istruzioni aggiuntive
In una regola ILM che è attualmente in un criterio ILM	i. Modificare il criterio. ii. Rimuovere la regola ILM che utilizza il profilo di erasure coding. iii. Aggiungere una o più nuove regole ILM per garantire la protezione di tutti gli oggetti. iv. Salvare il criterio. v. Modificare o eliminare la regola rimossa dal criterio. Se si modifica la regola, rimuovere tutti i posizionamenti che utilizzano il profilo di erasure coding. vi. Continuare con questa procedura.	"Creare un criterio ILM" "Utilizzare le regole ILM e i criteri ILM"

e. Aggiornare la pagina Erasure-Coding Profiles per assicurarsi che il profilo non venga utilizzato in una regola ILM.

4. Se il profilo non viene utilizzato in una regola ILM, selezionare il pulsante di opzione e selezionare **Disattiva**. Viene visualizzata la finestra di dialogo Disattiva profilo di erasure coding.



È possibile selezionare più profili da disattivare contemporaneamente, a condizione che ciascun profilo non venga utilizzato in alcuna regola.

5. Se sei sicuro di voler disattivare il profilo, seleziona **Disattiva**.

Risultati

- Se StorageGRID è in grado di disattivare il profilo di erasure coding, il suo stato è disattivato. Non è più possibile selezionare questo profilo per nessuna regola ILM. Non puoi riattivare un profilo disattivato.
- Se StorageGRID non è in grado di disattivare il profilo, viene visualizzato un messaggio di errore. Ad esempio, se i dati dell'oggetto sono ancora associati a questo profilo, viene visualizzato un messaggio di errore. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione.

Configurare le regioni S3 per StorageGRID

Le regole ILM possono filtrare gli oggetti in base alle regioni facoltative in cui vengono creati i bucket S3, consentendo di archiviare oggetti da regioni diverse in posizioni di archiviazione diverse.

Se si desidera utilizzare un'area del bucket S3 come filtro in una regola, è necessario innanzitutto creare le regioni che possono essere utilizzate dai bucket nel sistema.



Una volta creato il bucket, non è possibile modificare l'area di un bucket.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

Quando si crea un bucket S3, è possibile specificare che il bucket venga creato in un'area specifica. La specifica di una regione consente al bucket di essere geograficamente vicino ai propri utenti, in modo da ottimizzare la latenza, ridurre al minimo i costi e soddisfare i requisiti normativi.

Quando si crea una regola ILM, è possibile utilizzare la regione associata a un bucket S3 come filtro avanzato. Ad esempio, è possibile progettare una regola che si applica solo agli oggetti nei bucket S3 creati nell' `us-west-2` area. È quindi possibile specificare che le copie di tali oggetti vengano collocate sui nodi di storage in un sito del data center all'interno di tale regione per ottimizzare la latenza.

Durante la configurazione delle regioni, attenersi alle seguenti linee guida:

- Per impostazione predefinita, tutti i bucket sono considerati appartenenti alla `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 che non è stata definita in StorageGRID.
- Quando si crea il bucket S3, è necessario utilizzare il nome esatto della regione. I nomi delle regioni rilevano la distinzione tra maiuscole e minuscole. I caratteri validi sono numeri, lettere e trattini.



EU non è considerato un alias 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 utilizzata in una regola assegnata a qualsiasi criterio (attivo o inattivo).
- Se si utilizza un'area non valida come filtro avanzato in una regola ILM, non è possibile aggiungere tale regola a un criterio.

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 si elimina una regione dopo averla utilizzata per creare un bucket S3, sarà necessario aggiungerla nuovamente se si desidera utilizzare il filtro avanzato `Location Constraint` per trovare gli oggetti in tale bucket.

Fasi

1. Selezionare **ILM > regioni**.

Viene visualizzata la pagina Regioni.

2. Selezionare la scheda **Tutte le regioni** o **Regione predefinita**.

Tutte le regioni

Nella scheda **Tutte le regioni** sono elencate le regioni attualmente definite, inclusa la regione predefinita definita.



Non è possibile rimuovere o modificare la regione predefinita nella scheda **Tutte le regioni**. Utilizzare la scheda **Regione predefinita** per modificare la regione predefinita.

- a. Per aggiungere una regione, seleziona **Aggiungi un'altra regione**.
- b. Immettere il nome di una regione che si desidera utilizzare durante la creazione dei bucket S3.

Quando si crea il bucket S3 corrispondente, è necessario utilizzare il nome esatto della regione come elemento di richiesta LocationConstraint.

- c. Per rimuovere un'area non utilizzata, seleziona l'icona di eliminazione .

Se si tenta di rimuovere una regione attualmente utilizzata in qualsiasi criterio (attivo o inattivo), viene visualizzato un messaggio di errore.

- d. Una volta apportate le modifiche, selezionare **Salva**.

È ora possibile selezionare queste regioni dalla sezione Advanced filters (filtri avanzati) nel passaggio 1 della creazione guidata regola ILM. Vedere ["Utilizzare filtri avanzati nelle regole ILM"](#).

Regione predefinita

La scheda **Regione predefinita** visualizza la regione predefinita attualmente definita, che è possibile modificare.

- a. Per modificare la regione predefinita, selezionare il nome della regione dalle opzioni disponibili nell'elenco a discesa **Regione predefinita**.
- b. Selezionare **Salva**.

Creare una regola ILM

Scopri le regole ILM in StorageGRID

Per gestire gli oggetti, creare un set di regole ILM (Information Lifecycle Management) e organizzarle in un criterio ILM.

Ogni oggetto acquisito nel sistema viene valutato in base al criterio attivo. Quando una regola del criterio corrisponde ai metadati di un oggetto, le istruzioni della regola determinano le azioni eseguite da StorageGRID per copiare e memorizzare tale oggetto.



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

Elementi di una regola ILM

Una regola ILM ha tre elementi:

- **Filtering Criteria:** I filtri di base e avanzati di una regola definiscono a quali oggetti si applica la regola. Se un oggetto corrisponde a tutti i filtri, StorageGRID applica la regola e crea le copie dell'oggetto specificate nelle istruzioni di posizionamento della regola.
- **Istruzioni di posizionamento:** Le istruzioni di posizionamento di una regola definiscono il numero, il tipo e la posizione delle copie degli oggetti. Ciascuna regola può includere una sequenza di istruzioni di posizionamento per modificare il numero, il tipo e la posizione delle copie degli oggetti nel tempo. Quando scade il periodo di tempo per un posizionamento, le istruzioni nel posizionamento successivo vengono applicate automaticamente dalla valutazione ILM successiva.
- **Comportamento acquisizione:** Il comportamento di acquisizione di una regola consente di scegliere il modo in cui gli oggetti filtrati dalla regola sono 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 distinti e di grandi dimensioni. Questi filtri consentono di applicare una regola a specifici account tenant, bucket S3 specifici o entrambi.

I filtri di base offrono un metodo semplice per applicare regole diverse a un numero elevato di oggetti. Ad esempio, potrebbe essere necessario memorizzare i record finanziari della tua azienda per soddisfare i requisiti normativi, mentre potrebbe essere necessario memorizzare i dati del reparto di marketing per facilitare le operazioni quotidiane. Dopo aver creato account tenant separati per ciascun reparto o aver separato i dati dai diversi reparti in bucket S3 separati, è possibile creare facilmente una regola che si applica a tutti i record finanziari e una seconda regola che si applica a tutti i dati di marketing.

- I filtri avanzati offrono un controllo granulare. È possibile creare filtri per selezionare gli oggetti in base alle seguenti proprietà dell'oggetto:
 - Tempo di acquisizione
 - Ora dell'ultimo accesso
 - Nome completo o parziale dell'oggetto (Key)
 - Vincolo di posizione (solo S3)
 - Dimensione dell'oggetto
 - Metadati dell'utente
 - Tag Object (solo S3)

È possibile filtrare gli oggetti in base a criteri molto specifici. Ad esempio, gli oggetti memorizzati dal reparto di imaging di un ospedale potrebbero essere utilizzati frequentemente quando hanno meno di 30 giorni e poco tempo dopo, mentre gli oggetti che contengono informazioni sulle visite dei pazienti potrebbero dover essere copiati nel reparto di fatturazione della sede centrale della rete sanitaria. È possibile creare filtri che identifichino ciascun tipo di oggetto in base al nome dell'oggetto, alle dimensioni, ai tag di oggetto S3 o a qualsiasi altro criterio pertinente, quindi creare regole separate per memorizzare ciascun set di oggetti in modo appropriato.

È possibile combinare i filtri in base alle esigenze in una singola regola. Ad esempio, il reparto marketing potrebbe voler memorizzare file di immagini di grandi dimensioni in modo diverso dai record dei vendor, mentre il reparto risorse umane potrebbe dover memorizzare i record del personale in un'area geografica specifica e le informazioni sulle policy a livello centrale. In questo caso, è possibile creare regole che filtrino in base all'account tenant per separare i record da ciascun reparto, utilizzando i filtri in ciascuna regola per identificare il tipo specifico di oggetti a cui si applica la regola.

Istruzioni per il posizionamento delle regole ILM

Le istruzioni di posizionamento determinano dove, quando e come vengono memorizzati i dati degli oggetti. Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo.

Quando si creano le istruzioni per il posizionamento:

- Si inizia specificando l'ora di riferimento, che determina quando iniziano le istruzioni di posizionamento. Il tempo di riferimento potrebbe essere quando un oggetto viene acquisito, quando si accede a un oggetto, quando un oggetto con versione diventa non corrente o un tempo definito dall'utente.
- Quindi, specificare quando applicare il posizionamento rispetto al tempo di riferimento. Ad esempio, un posizionamento potrebbe iniziare il giorno 0 e continuare per 365 giorni, rispetto a quando l'oggetto è stato acquisito.
- Infine, specificare il tipo di copie (replica o erasure coding) e la posizione in cui sono memorizzate le copie. Ad esempio, è possibile memorizzare due copie replicate in due siti diversi.

Ciascuna regola può definire più posizioni per un singolo periodo di tempo e posizioni diverse per periodi di tempo diversi.

- Per posizionare oggetti in più posizioni durante un singolo periodo di tempo, selezionare **Aggiungi altro tipo o posizione** per aggiungere più di una riga per quel periodo di tempo.
- Per posizionare oggetti in posizioni diverse in periodi di tempo diversi, selezionare **Aggiungi un altro periodo di tempo** per aggiungere il periodo di tempo successivo. Quindi, specificare una o più righe entro il periodo di tempo.

L'esempio mostra due istruzioni di posizionamento nella pagina Definisci posizioni della creazione guidata regola ILM.

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 for 365 days

Store objects by replicating 2 copies at Data Center 1 , Data Center 2

and store objects by erasure coding using 6+3 EC scheme at all sites

1

Add other type or location

Time period 2
From Day 365 store forever

Store objects by replicating 2 copies at Data Center 3

2

Add other type or location

La prima istruzione di assegnazione 1 ha due righe per il primo anno:

- La prima riga crea due copie di oggetti replicate in due siti del data center.
- La seconda riga crea una copia con erasure coding pari a 6+3 usando tutti i siti del data center.

La seconda istruzione di collocazione 2 crea due copie dopo un anno e conserva tali copie per sempre.

Quando si definisce il set di istruzioni di posizionamento per una regola, è necessario assicurarsi che almeno un'istruzione di posizionamento inizi al giorno 0, che non vi siano intervalli tra i periodi di tempo definiti, e che l'istruzione finale di posizionamento continui per sempre o fino a quando non si richiede più alcuna copia oggetto.

Alla scadenza di ogni periodo di tempo previsto dalla regola, vengono applicate le istruzioni per il posizionamento dei contenuti per il periodo di tempo successivo. Vengono create nuove copie di oggetti e tutte le copie non necessarie vengono eliminate.

Comportamento di acquisizione delle regole ILM

Il comportamento di acquisizione controlla se le copie degli oggetti vengono posizionate immediatamente in base alle istruzioni della regola o se vengono eseguite copie temporanee e le istruzioni di posizionamento vengono applicate in un secondo momento. Per le regole ILM sono disponibili i seguenti comportamenti di acquisizione:

- **Balanced:** StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono eseguite copie temporanee e viene restituito il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.
- **Strict:** Tutte le copie specificate nella regola ILM devono essere eseguite prima che il client sia riuscito.
- **Doppio commit:** StorageGRID esegue immediatamente copie temporanee dell'oggetto e restituisce il successo al client. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Informazioni correlate

- ["Opzioni di acquisizione"](#)
- ["Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione"](#)
- ["L'interazione tra coerenza e regole ILM per influire sulla protezione dei dati"](#)

Esempio di regola ILM

Ad esempio, una regola ILM potrebbe specificare quanto segue:

- Si applicano solo agli oggetti appartenenti al tenant A.
- Eseguire due copie replicate di tali oggetti e memorizzare ciascuna copia in un sito diverso.
- Conserva le due copie "per sempre", il che significa che StorageGRID non le eliminerà automaticamente. Al contrario, StorageGRID conserverà questi oggetti fino a quando non saranno cancellati da una richiesta di eliminazione del client o dalla scadenza di un ciclo di vita del bucket.
- Utilizzare l'opzione bilanciato per il comportamento di acquisizione: L'istruzione di posizionamento a due siti viene applicata non appena il tenant A salva un oggetto in StorageGRID, a meno che non sia possibile eseguire immediatamente entrambe le copie richieste.

Ad esempio, se il sito 2 non è raggiungibile quando il tenant A salva un oggetto, StorageGRID eseguirà due copie intermedie sui nodi di storage nel sito 1. Non appena il sito 2 sarà disponibile, StorageGRID effettuerà la copia richiesta presso il sito.

Informazioni correlate

- ["Che cos'è un pool di storage"](#)
- ["Che cos'è un Cloud Storage Pool"](#)

Accedi alla procedura guidata Crea una regola ILM in StorageGRID

Le regole ILM consentono di gestire il posizionamento dei dati degli oggetti nel tempo. Per creare una regola ILM, utilizzare la procedura guidata Crea una regola ILM.



Se si desidera creare la regola ILM predefinita per un criterio, seguire invece l'["Istruzioni per la creazione di una regola ILM predefinita"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- Se si desidera specificare a quali account tenant si applica questa regola, si dispone dell'["Autorizzazione account tenant"](#) ID account per ciascun account.
- Se si desidera che la regola filtri gli oggetti sui metadati dell'ora dell'ultimo accesso, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati dal bucket S3.
- Hai configurato qualsiasi pool di storage cloud che intendi utilizzare. Vedere ["Creare un pool di storage cloud"](#).
- Si ha familiarità con ["opzioni di acquisizione"](#).
- Se è necessario creare una regola conforme da utilizzare con blocco oggetti S3, si ha familiarità con ["Requisiti per il blocco oggetti S3"](#).

- Facoltativamente, hai guardato il video:

[Panoramica delle regole ILM](#)

A proposito di questa attività

Quando si creano regole ILM:

- Prendere in considerazione la topologia e le configurazioni dello storage del sistema StorageGRID.
- Considerare i tipi di copie degli oggetti da creare (replicate o sottoposte a erasure coding) e il numero di copie di ciascun oggetto necessario.
- Determinare i tipi di metadati degli oggetti utilizzati nelle applicazioni che si connettono al sistema StorageGRID. Le regole ILM filtrano gli oggetti in base ai metadati.
- Considerare dove si desidera che le copie a oggetti vengano collocate nel tempo.
- Decidere quale opzione di acquisizione utilizzare (Balanced, Strict o Dual Commit).

Fasi

1. Selezionare **ILM > regole**.
2. Selezionare **Crea**. "[Fase 1 \(inserire i dettagli\)](#)" Viene visualizzata la procedura guidata Crea una regola ILM.

Inserisci dettagli e filtri per una regola ILM di StorageGRID

La fase **Enter details** della creazione guidata di una regola ILM consente di immettere un nome e una descrizione per la regola e di definire i filtri per la regola.

L'immissione di una descrizione e la definizione dei filtri per la regola sono facoltativi.

A proposito di questa attività

Quando si valuta un oggetto rispetto a "[Regola ILM](#)", StorageGRID confronta i metadati dell'oggetto con i filtri della regola. Se i metadati dell'oggetto corrispondono a tutti i filtri, StorageGRID utilizza la regola per posizionare l'oggetto. È possibile progettare una regola da applicare a tutti gli oggetti, oppure specificare filtri di base, come uno o più account tenant o nomi bucket, o filtri avanzati, come la dimensione dell'oggetto o i metadati dell'utente.

Fasi

1. Immettere un nome univoco per la regola nel campo **Nome**.
2. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.

È necessario descrivere lo scopo o la funzione della regola in modo da poterne riconoscere in un secondo momento.

3. Facoltativamente, selezionare uno o più account tenant S3 a cui si applica questa regola. Se questa regola è applicabile a tutti i tenant, lasciare vuoto questo campo.

Se non si dispone dell'autorizzazione di accesso root o dell'autorizzazione per gli account tenant, non è possibile selezionare i tenant dall'elenco. Immettere invece l'ID tenant o più ID come stringa delimitata da virgole.

4. Facoltativamente, specificare i bucket S3 a cui si applica questa regola.

Se si seleziona **Applica a tutti i bucket** (impostazione predefinita), la regola si applica a tutti i bucket S3.

5. Per i tenant S3, selezionare **Yes** (Sì) per applicare la regola solo alle versioni di oggetti precedenti nei bucket S3 che hanno attivato il controllo delle versioni.

Se si seleziona **Sì**, l'opzione "ora non corrente" verrà selezionata automaticamente per ora di riferimento in ["Passaggio 2 della creazione guidata di una regola ILM"](#).



L'ora non corrente si applica solo agli oggetti S3 nei bucket abilitati per il controllo delle versioni. Vedere ["Operazioni su benne, PutBucketVersioning"](#) e ["Gestire gli oggetti con S3 Object Lock"](#).

È possibile utilizzare questa opzione per ridurre l'impatto dello storage degli oggetti con versione filtrando le versioni degli oggetti non correnti. Vedere ["Esempio 4: Regole ILM e policy per gli oggetti con versione S3"](#).

6. In alternativa, selezionare **Aggiungi un filtro avanzato** per specificare filtri aggiuntivi.

Se non si configura il filtraggio avanzato, la regola si applica a tutti gli oggetti che corrispondono ai filtri di base. Per ulteriori informazioni sul filtraggio avanzato, vedere [Utilizzare filtri avanzati nelle regole ILM](#) e [Specificare più tipi di metadati e valori](#).

7. Selezionare **continua**. ["Fase 2 \(definizione delle posizioni\)"](#) Viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare filtri avanzati nelle regole ILM

Il filtraggio avanzato consente di creare regole ILM applicabili solo a oggetti specifici in base ai metadati. Quando si imposta il filtraggio avanzato per una regola, si seleziona il tipo di metadati che si desidera associare, si seleziona un operatore e si specifica un valore di metadati. Quando si valutano gli oggetti, la regola ILM viene applicata solo agli oggetti che hanno metadati corrispondenti al filtro avanzato.

La tabella mostra i tipi di metadati che è possibile specificare nei filtri avanzati, gli operatori che è possibile utilizzare per ogni tipo di metadati e i valori di metadati previsti.

Tipo di metadati	Operatori supportati	Valore dei metadati
Tempo di acquisizione	• è • non lo è • è prima • è acceso o prima • è dopo • sia acceso o dopo	Ora e data di acquisizione dell'oggetto. Nota: per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui la nuova policy verrà applicata per garantire che gli oggetti esistenti non vengano spostati inutilmente.

Tipo di metadati	Operatori supportati	Valore dei metadati
Chiave	• uguale a • non uguale • contiene • non contiene • inizia con • non inizia con • termina con • non finisce con	Tutto o parte di una chiave oggetto S3 univoca. Ad esempio, è possibile associare oggetti che terminano con <code>.txt</code> o iniziano con <code>test-object/</code>.
Ora dell'ultimo accesso	• è • non lo è • è prima • è acceso o prima • è dopo • sia acceso o dopo	Ora e data dell'ultimo recupero dell'oggetto (letto o visualizzato). Nota: se si prevede di utilizzare "usa l'ultimo tempo di accesso" un filtro avanzato, gli aggiornamenti dell'ora dell'ultimo accesso devono essere abilitati per il bucket S3.
Vincolo di posizione (solo S3)	• uguale a • non uguale	La regione in cui è stato creato un bucket S3. Utilizzare ILM > regioni per definire le regioni visualizzate. Nota: 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 S3".
Dimensione dell'oggetto	• uguale a • non uguale • inferiore a. • minore o uguale a. • maggiore di • maggiore o uguale a.	La dimensione dell'oggetto. L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

Tipo di metadati	Operatori supportati	Valore dei metadati
Metadati dell'utente	• contiene • termina con • uguale a • esiste • inizia con • non contiene • non finisce con • non uguale • non esiste • non inizia con	Coppia valore-chiave, dove Nome metadati utente è la chiave e valore metadati è il valore. Ad esempio, per filtrare gli oggetti che hanno metadati utente di <code>color=blue</code>, specificare <code>color</code> per Nome metadati utente, per l'operatore e <code>blue</code> per valore metadati <code>equals</code>. Nota: i nomi dei metadati utente non distinguono tra maiuscole e minuscole; i valori dei metadati utente distinguono tra maiuscole e minuscole.
Tag Object (solo S3)	• contiene • termina con • uguale a • esiste • inizia con • non contiene • non finisce con • non uguale • non esiste • non inizia con	Coppia key-value, dove nome tag oggetto è la chiave e valore tag oggetto è il valore. Ad esempio, per filtrare gli oggetti che hanno un tag di oggetto di <code>Image=True</code>, specificare <code>Image</code> per nome tag di oggetto, <code>equals</code> per l'operatore e <code>True</code> per valore tag di oggetto. Nota: i nomi dei tag degli oggetti e i valori dei tag degli oggetti fanno distinzione tra maiuscole e minuscole. È necessario inserire questi elementi esattamente come sono stati definiti per l'oggetto.

Specificare più tipi di metadati e valori

Quando si definisce il filtraggio avanzato, è possibile specificare più tipi di metadati e più valori di metadati. Ad esempio, se si desidera che una regola corrisponda a oggetti di dimensioni comprese tra 10 MB e 100 MB, selezionare il tipo di metadati **Object size** e specificare due valori di metadati.

- Il primo valore di metadati specifica oggetti superiori o uguali a 10 MB.
- Il secondo valore di metadati specifica gli oggetti inferiori o uguali a 100 MB.

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
▼

×

L'utilizzo di più voci consente di avere un controllo preciso su quali oggetti vengono associati. Nell'esempio seguente, la regola si applica agli oggetti che hanno il marchio A o il marchio B come valore dei metadati utente `camera_TYPE`. Tuttavia, la regola si applica solo agli oggetti Brand B di dimensioni inferiori a 10 MB.

Filter group 1 Objects with all of following metadata will be evaluated by this rule:

User metadata equals

[Add another advanced filter](#)

or **Filter group 2** Objects with all of following metadata will be evaluated by this rule:

User metadata equals

and Object size

[Add another advanced filter](#)

Definisci le istruzioni di posizionamento per una regola StorageGRID ILM

La fase **Definisci posizionamenti** della procedura guidata Crea regola ILM consente di definire le istruzioni di posizionamento che determinano la durata dell'archiviazione degli oggetti, il tipo di copie (replicate o sottoposte a erasure coding), la posizione di archiviazione e il numero di copie.



Le schermate mostrate sono esempi. I risultati possono variare a seconda della versione di StorageGRID in uso.

A proposito di questa attività

Una regola ILM può includere una o più istruzioni di posizionamento. Ogni istruzione di posizionamento si applica a un singolo periodo di tempo. Quando si utilizzano più istruzioni, i periodi di tempo devono essere contigui e almeno un'istruzione deve iniziare il giorno 0. Le istruzioni possono continuare per sempre o fino a quando non sono più necessarie copie di oggetti.

Ogni istruzione di posizionamento può avere più righe se si desidera creare diversi tipi di copie o utilizzare posizioni diverse durante tale periodo di tempo.

In questo esempio, la regola ILM memorizza una copia replicata nel sito 1 e una copia replicata nel sito 2 per il primo anno. Dopo un anno, viene creata una copia 2+1 con codice di cancellazione e salvata in un solo sito.

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

Fasi

1. Per **Reference Time** (tempo di riferimento), selezionare il tipo di tempo da utilizzare per il calcolo dell'ora di inizio di un'istruzione di posizionamento.

Opzione	Descrizione
Tempo di acquisizione	L'ora in cui l'oggetto è stato acquisito.
Ora dell'ultimo accesso	L'ora in cui l'oggetto è stato recuperato per l'ultima volta (letto o visualizzato). Per utilizzare questa opzione, è necessario attivare gli aggiornamenti dell'ora dell'ultimo accesso per il bucket S3. Fare riferimento alla "USA l'ultimo tempo di accesso nelle regole ILM".
Tempo di creazione definito dall'utente	Tempo specificato nei metadati definiti dall'utente.
Ora non corrente	L'opzione "ora non corrente" viene selezionata automaticamente se si seleziona Sì per la domanda "Applica questa regola solo alle versioni precedenti degli oggetti (nei bucket S3 con versione abilitata)?" in "Passaggio 1 della creazione guidata di una regola ILM" .

Se si desidera creare una regola *conforme*, è necessario selezionare **ora di acquisizione**. Fare riferimento alla ["Gestire gli oggetti con S3 Object Lock"](#).

2. Nella sezione **periodo di tempo e posizionamenti**, inserire un'ora di inizio e una durata per il primo periodo di tempo.

Ad esempio, è possibile specificare dove memorizzare gli oggetti per il primo anno (*dal giorno 0 memorizzare per 365 giorni*). Almeno un'istruzione deve iniziare al giorno 0.

3. Se si desidera creare copie replicate:

- a. Dall'elenco a discesa **Memorizza oggetti per**, selezionare **replica**.
- b. Selezionare il numero di copie che si desidera eseguire.

Se si modifica il numero di copie in 1, viene visualizzato un avviso. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Fare riferimento alla "[Perché non utilizzare la replica a copia singola](#)".

Per evitare il rischio, effettuare una o più delle seguenti operazioni:

- Aumentare il numero di copie per il periodo di tempo.
- Aggiungere copie ad altri pool di storage o a un pool di storage cloud.
- Selezionare **erasure coding** invece di **Replicating**.

È possibile ignorare questo avviso se questa regola crea già più copie per tutti i periodi di tempo.

- c. Nel campo **Copies at**, selezionare i pool di storage che si desidera aggiungere.

Se si specifica un solo pool di storage, tenere presente che StorageGRID può memorizzare solo una copia replicata di un oggetto su un nodo di storage specifico. Se la griglia include tre nodi di storage e si seleziona 4 come numero di copie, verranno eseguite solo tre copie e 8212 una copia per ciascun nodo di storage.

Viene attivato l'avviso **ILM placement unachievable** per indicare che la regola ILM non può essere applicata completamente.

Se si specificano più pool di storage, tenere presenti le seguenti regole:

- Il numero di copie non può essere superiore al numero di pool di storage.
- Se il numero di copie corrisponde al numero di pool di storage, viene memorizzata una copia dell'oggetto in ciascun pool di storage.
- Se il numero di copie è inferiore al numero di pool di storage, una copia viene memorizzata nel sito di acquisizione e il sistema distribuisce le copie rimanenti per mantenere bilanciato l'utilizzo del disco tra i pool, garantendo che nessun sito riceva più di una copia di un oggetto.
- Se i pool di storage si sovrappongono (contengono gli stessi nodi di storage), tutte le copie dell'oggetto potrebbero essere salvate in un solo sito. Per questo motivo, non specificare il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti) e un altro pool di storage.

4. Se si desidera creare una copia con codice di cancellazione:

- a. Dall'elenco a discesa **Memorizza oggetti per**, selezionare **erasure coding**.



L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

- b. Se non è stato aggiunto un filtro delle dimensioni dell'oggetto per un valore superiore a 200 KB, selezionare **precedente** per tornare al passaggio 1. Quindi, selezionare **Aggiungi un filtro avanzato** e impostare un filtro **dimensione oggetto** su qualsiasi valore maggiore di 200 KB.
- c. Selezionare il pool di storage che si desidera aggiungere e lo schema di erasure coding che si desidera utilizzare.

La posizione dello storage per una copia sottoposta a erasure coding include il nome dello schema di erasure coding, seguito dal nome del pool di storage.

Gli schemi di erasure coding disponibili sono limitati dal numero di nodi storage nel pool di storage selezionato. Accanto agli schemi che forniscono la ["migliore protezione o l'overhead dello storage più basso"](#), viene visualizzato un Recommended badge.

5. Facoltativamente:

- a. Selezionare **Aggiungi altro tipo o ubicazione** per creare copie aggiuntive in posizioni diverse.
- b. Selezionare **Add another time period** (Aggiungi un altro periodo di tempo) per aggiungere diversi periodi di tempo.



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 al termine del periodo di conservazione di ILM.

6. Se si desidera memorizzare oggetti in un pool di storage cloud:

- a. Nell'elenco a discesa **Memorizza oggetti per**, selezionare **replica**.
- b. Selezionare il campo **Copies at**, quindi selezionare un Cloud Storage Pool.

Quando si utilizzano i Cloud Storage Pool, tenere presenti le seguenti regole:

- Non puoi selezionare più di un Cloud Storage Pool in una singola istruzione di posizionamento. Allo stesso modo, non è possibile selezionare un Cloud Storage Pool e un pool di storage nelle stesse istruzioni di posizionamento.
- È possibile memorizzare solo una copia di un oggetto in un determinato pool di storage cloud. Se si imposta **copies** su 2 o più, viene visualizzato un messaggio di errore.
- Non è possibile memorizzare più copie di un oggetto contemporaneamente in nessun Cloud Storage Pool. Viene visualizzato un messaggio di errore se più posizioni che utilizzano un pool di storage cloud presentano date sovrapposte o se più righe nello stesso posizionamento utilizzano un pool di storage cloud.
- È possibile memorizzare un oggetto in un Cloud Storage Pool contemporaneamente all'archiviazione dell'oggetto come copie replicate o con erasure coding in StorageGRID. Tuttavia, è necessario includere più di una riga nelle istruzioni di posizionamento per il periodo di tempo, in modo da poter specificare il numero e il tipo di copie per ciascuna posizione.

7. Nel diagramma di conservazione, confermare le istruzioni per il posizionamento.

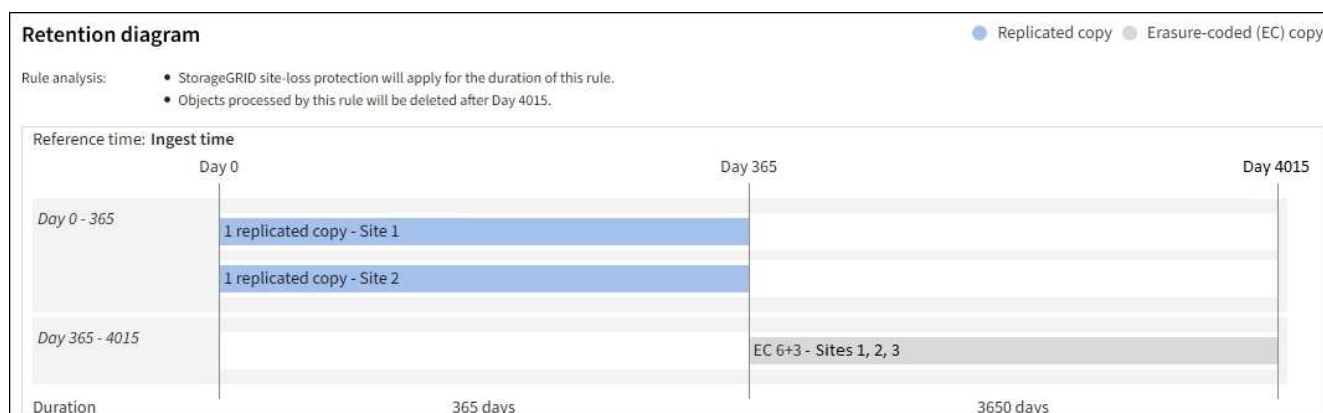
In questo esempio, la regola ILM memorizza una copia replicata nel sito 1 e una copia replicata nel sito 2 per il primo anno. Dopo un anno e per altri 10 anni, una copia con codice di cancellazione 6+3 verrà salvata in tre sedi. Dopo 11 anni totali, gli oggetti verranno cancellati da StorageGRID.

La sezione analisi delle regole del diagramma di conservazione riporta:

- La protezione contro la perdita di sito di StorageGRID verrà applicata per tutta la durata di questa regola.

- Gli oggetti elaborati da questa regola verranno cancellati dopo il giorno 4015.

Fare riferimento alla ["Abilita la protezione contro la perdita di sito."](#)



- Selezionare **continua**. ["Fase 3 \(selezionare il comportamento di acquisizione\)"](#) Viene visualizzata la procedura guidata Crea una regola ILM.

Utilizzare l'orario dell'ultimo accesso nelle regole ILM di StorageGRID

In una regola ILM, è possibile utilizzare l'ultimo tempo di accesso come ora di riferimento. Ad esempio, è possibile lasciare oggetti che sono stati visualizzati negli ultimi tre mesi sui nodi di storage locali, mentre si spostano oggetti che non sono stati visualizzati di recente in una posizione off-site. È inoltre possibile utilizzare l'ultimo tempo di accesso come filtro avanzato se si desidera che una regola ILM si applichi solo agli oggetti a cui è stato effettuato l'ultimo accesso in una data specifica.

A proposito di questa attività

Prima di utilizzare l'ultimo tempo di accesso in una regola ILM, esaminare le seguenti considerazioni:

- Quando si utilizza l'ultimo tempo di accesso come tempo di riferimento, tenere presente che la modifica dell'ultimo tempo di accesso per un oggetto non attiva una valutazione ILM immediata. Al contrario, le posizioni dell'oggetto vengono valutate e l'oggetto viene spostato come richiesto quando ILM in background valuta l'oggetto. Questa operazione potrebbe richiedere due settimane o più dopo l'accesso all'oggetto.

Tenere conto di questa latenza durante la creazione di regole ILM basate sull'ultimo tempo di accesso ed evitare posizionamenti che utilizzano brevi periodi di tempo (meno di un mese).

- Quando si utilizza l'ultima ora di accesso come filtro avanzato o come ora di riferimento, è necessario attivare gli ultimi aggiornamenti dell'ora di accesso per i bucket S3. È possibile utilizzare ["Manager tenant"](#) o ["API di gestione del tenant"](#).



Gli aggiornamenti dell'ora dell'ultimo accesso sono disabilitati per impostazione predefinita per i bucket S3.



Tenere presente che l'attivazione degli ultimi aggiornamenti del tempo di accesso può ridurre le performance, soprattutto nei sistemi con oggetti di piccole dimensioni. L'impatto delle performance si verifica perché StorageGRID deve aggiornare gli oggetti con nuovi timestamp ogni volta che gli oggetti vengono recuperati.

La tabella seguente riassume se l'ora dell'ultimo accesso viene aggiornata per tutti gli oggetti nel bucket per diversi tipi di richieste.

Tipo di richiesta	Se l'ora dell'ultimo accesso viene aggiornata quando gli ultimi aggiornamenti dell'ora di accesso sono disattivati	Se l'ora dell'ultimo accesso viene aggiornata quando sono attivati gli ultimi aggiornamenti dell'ora di accesso
Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Selezionare il comportamento di acquisizione per una regola StorageGRID ILM

La fase **Select ingest behavior** della procedura guidata Create ILM Rule consente di scegliere come proteggere gli oggetti filtrati da questa regola durante l'acquisizione.

A proposito di questa attività

StorageGRID può eseguire copie temporanee e mettere in coda gli oggetti per la valutazione ILM in un secondo momento, oppure può eseguire copie per soddisfare immediatamente le istruzioni di posizionamento della regola.

Fasi

1. Selezionare il ["comportamento di acquisizione"](#) da utilizzare.

Per ulteriori informazioni, vedere ["Vantaggi, svantaggi e limitazioni delle opzioni di acquisizione"](#).



Non è possibile utilizzare l'opzione bilanciato o rigoroso se la regola utilizza uno dei seguenti posizionamenti:

- Un pool di storage cloud al giorno 0
- Un Cloud Storage Pool quando la regola utilizza un tempo di creazione definito dall'utente come tempo di riferimento

Vedere ["Esempio 5: Regole e policy ILM per un comportamento rigoroso di acquisizione"](#).

2. Selezionare **Crea**.

Viene creata la regola ILM. La regola non diventa attiva fino a quando non viene aggiunta a e il criterio non ["Policy ILM"](#) viene attivato.

Per visualizzare i dettagli della regola, selezionare il nome della regola nella pagina delle regole ILM.

Crea una regola ILM predefinita in StorageGRID

Prima di creare un criterio ILM, è necessario creare una regola predefinita per inserire nel criterio gli oggetti non corrispondenti a un'altra regola. La regola predefinita non può utilizzare alcun filtro. Deve essere applicato a tutti i tenant, a tutti i bucket e a tutte le versioni degli oggetti.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

La regola predefinita è l'ultima regola da valutare in un criterio ILM, quindi non può utilizzare alcun filtro. Le istruzioni di posizionamento per la regola predefinita vengono applicate a tutti gli oggetti che non corrispondono a un'altra regola del criterio.

In questo criterio di esempio, la prima regola si applica solo agli oggetti appartenenti a test-tenant-1. La regola predefinita, ultima, si applica agli oggetti appartenenti a tutti gli altri account tenant.

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 si crea la regola predefinita, tenere presenti i seguenti requisiti:

- La regola predefinita viene posizionata automaticamente come ultima regola quando viene aggiunta a un criterio.
- La regola predefinita non può utilizzare filtri di base o avanzati.
- La regola predefinita deve essere applicata a tutte le versioni degli oggetti.

- La regola predefinita dovrebbe creare copie replicate.



Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono utilizzare un filtro avanzato per evitare che gli oggetti più piccoli vengano sottoposti a erasure coding.

- In generale, la regola predefinita deve conservare gli oggetti per sempre.
- Se si utilizza (o si prevede di abilitare) l'impostazione blocco oggetti S3 globale, la regola predefinita deve essere conforme.

Fasi

1. Selezionare **ILM > regole**.
2. Selezionare **Crea**.

Viene visualizzata la fase 1 (immettere i dettagli) della creazione guidata regola ILM.

3. Immettere un nome univoco per la regola nel campo **Nome regola**.
4. Se si desidera, inserire una breve descrizione per la regola nel campo **Descrizione**.
5. Lasciare vuoto il campo **account tenant**.

La regola predefinita deve essere applicata a tutti gli account tenant.

6. Lasciare la selezione a discesa Nome bucket come **si applica a tutti i bucket**.

La regola predefinita deve essere applicata a tutti i bucket S3.

7. Mantenere la risposta predefinita, **No**, per la domanda, "applicare questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?"
8. Non aggiungere filtri avanzati.

La regola predefinita non può specificare alcun filtro.

9. Selezionare **Avanti**.

Viene visualizzato il punto 2 (definizione delle posizioni).

10. Per Reference Time (ora di riferimento), selezionare un'opzione qualsiasi.

Se è stata mantenuta la risposta predefinita, **No**, per la domanda "applicare questa regola solo alle versioni precedenti degli oggetti?" L'ora non corrente non verrà inclusa nell'elenco a discesa. La regola predefinita deve applicare tutte le versioni degli oggetti.

11. Specificare le istruzioni di posizionamento per la regola predefinita.
 - La regola predefinita deve conservare gli oggetti per sempre. Quando si attiva un nuovo criterio, viene visualizzato un avviso se la regola predefinita non conserva gli oggetti per sempre. Devi confermare che questo è il comportamento che ti aspetti.
 - La regola predefinita dovrebbe creare copie replicate.



Non utilizzare una regola che crea copie con codice di cancellazione come regola predefinita per un criterio. Le regole di erasure coding devono includere il filtro avanzato **dimensione oggetto (MB) maggiore di 200 KB** per evitare che gli oggetti più piccoli vengano sottoposti a erasure coding.

- Se si utilizza (o si intende attivare) l'impostazione globale S3 Object Lock (blocco oggetto S3), la regola predefinita deve essere conforme:
 - Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
 - Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
 - Impossibile salvare le copie degli oggetti in un Cloud Storage Pool.
 - Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando l'ora di inizio come ora di riferimento.
 - Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

12. Consultare il diagramma di conservazione per confermare le istruzioni di posizionamento.

13. Selezionare **continua**.

Viene visualizzato il passaggio 3 (selezionare il comportamento di acquisizione).

14. Selezionare l'opzione di acquisizione da utilizzare e selezionare **Crea**.

Gestire le policy ILM

Scopri le policy ILM in StorageGRID

Un criterio ILM (Information Lifecycle Management) è un insieme ordinato di regole ILM che determina il modo in cui il sistema StorageGRID gestisce i dati degli oggetti nel tempo.



Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Policy ILM predefinita

Quando si installa StorageGRID e si aggiungono siti, viene creato automaticamente un criterio ILM predefinito, come segue:

- Se la griglia contiene un sito, il criterio predefinito contiene una regola predefinita che replica due copie di ciascun oggetto in quel sito.
- Se la griglia contiene più siti, la regola predefinita replica una copia di ciascun oggetto in ciascun sito.

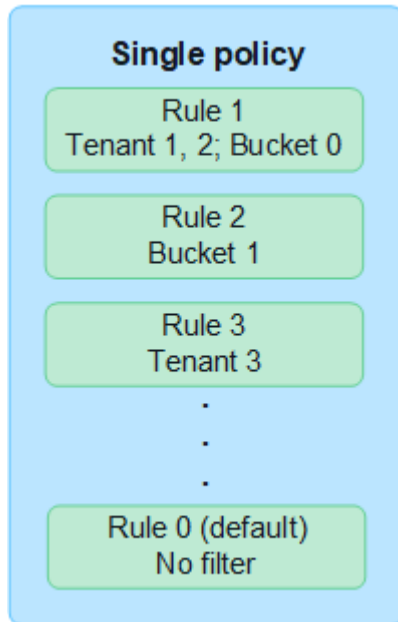
Se la policy predefinita non soddisfa i tuoi requisiti di archiviazione, puoi creare regole e policy personalizzate. Vedere ["Creare una regola ILM"](#) e ["Creare un criterio ILM"](#).

Una o più policy ILM attive?

È possibile disporre di uno o più criteri ILM attivi alla volta.

Un'unica policy

Se il grid usa un semplice schema di data Protection con poche regole specifiche del tenant e del bucket, utilizza una singola policy ILM attiva. Le regole ILM possono contenere filtri per gestire bucket o tenant diversi.



Quando si dispone di un solo criterio e i requisiti di un tenant cambiano, è necessario creare un nuovo criterio ILM o clonare il criterio esistente per applicare le modifiche, simulare e attivare quindi il nuovo criterio ILM. Le modifiche alla policy ILM possono comportare spostamenti degli oggetti che possono richiedere molti giorni e causare la latenza del sistema.

Policy multiple

Per offrire opzioni di qualità del servizio diverse ai tenant, è possibile disporre di più policy attive alla volta. Ogni policy può gestire tenant specifici, bucket S3 e oggetti. Quando si applicano o si modifica una policy per un insieme specifico di tenant o oggetti, le policy applicate agli altri tenant e oggetti non verranno influenzate.

Tag dei criteri ILM

Se desideri consentire ai tenant di alternare facilmente tra più policy di data Protection in base al bucket, utilizza policy ILM multiple con *tag policy ILM*. Ogni policy ILM viene assegnata a un tag, quindi i tenant etichettano un bucket per applicare la policy a quel bucket. È possibile impostare tag di policy ILM solo su bucket S3.

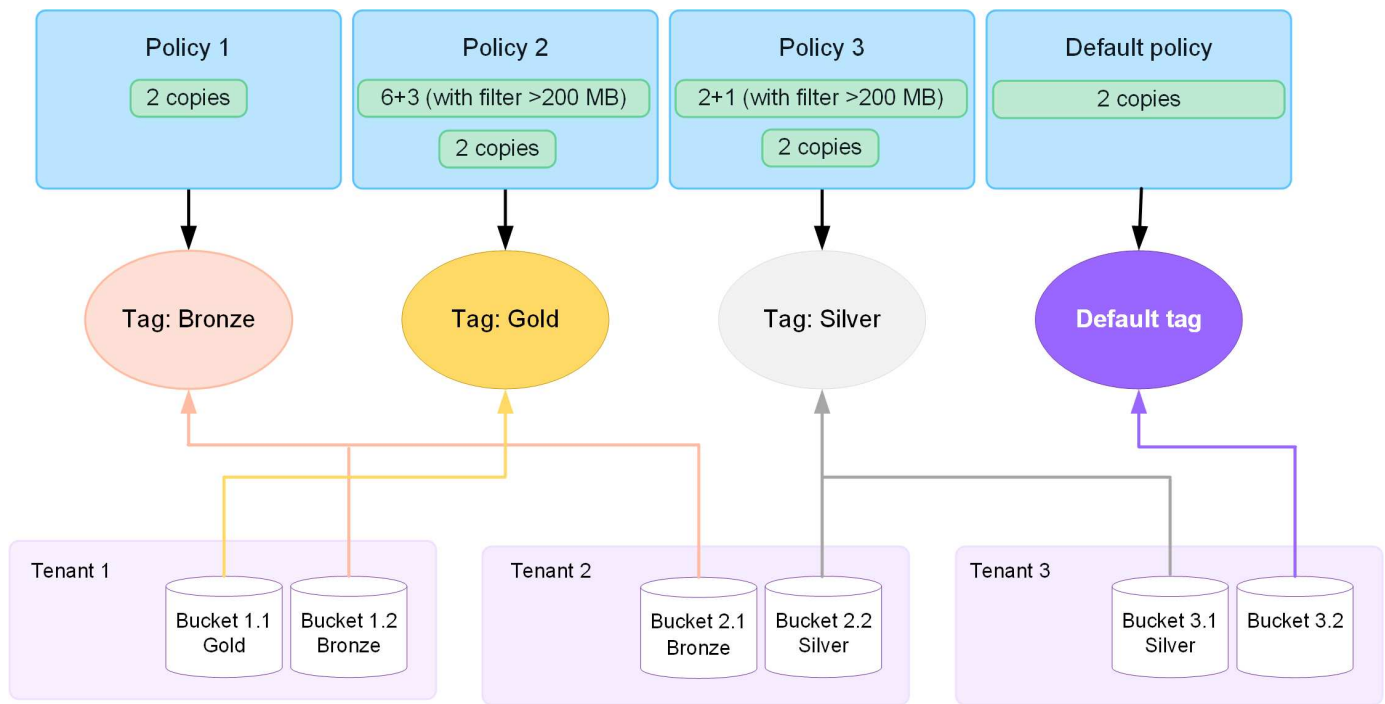
Ad esempio, potresti avere tre tag denominati Gold, Silver e Bronze. È possibile assegnare un criterio ILM a ciascun tag in base alla durata e alla posizione in cui tale criterio memorizza gli oggetti. I tenant possono scegliere la policy da utilizzare contrassegnando i propri bucket. Un bucket con tag Gold viene gestito dalla policy Gold e riceve il livello Gold di data Protection e performance.



Puoi [creare un massimo di 10 tag di policy](#) per la tua griglia.

Tag criterio ILM predefinito

Quando si installa StorageGRID, viene creato automaticamente un tag di criterio ILM predefinito. Ogni griglia deve avere un criterio attivo assegnato al tag predefinito. Il criterio predefinito si applica a tutti i bucket S3 non contrassegnati.



In che modo un criterio ILM valuta gli oggetti?

Una policy ILM attiva controlla il posizionamento, la durata e la protezione dei dati degli oggetti.

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

1. Se i filtri per la prima regola del criterio corrispondono a un oggetto, l'oggetto viene acquisito in base al comportamento di acquisizione di tale regola e memorizzato in base alle istruzioni di posizionamento di tale regola.
2. Se i filtri per la prima regola non corrispondono all'oggetto, l'oggetto viene valutato in base a ogni regola successiva nel criterio fino a quando non viene effettuata una corrispondenza.
3. Se nessuna regola corrisponde a un oggetto, vengono applicate le istruzioni di inserimento e posizionamento della regola predefinita nel criterio. La regola predefinita è l'ultima regola di un criterio. La regola predefinita deve essere applicata a tutti i tenant, a tutti i bucket S3 e a tutte le versioni degli oggetti e non può utilizzare alcun filtro avanzato.

Esempio di policy ILM

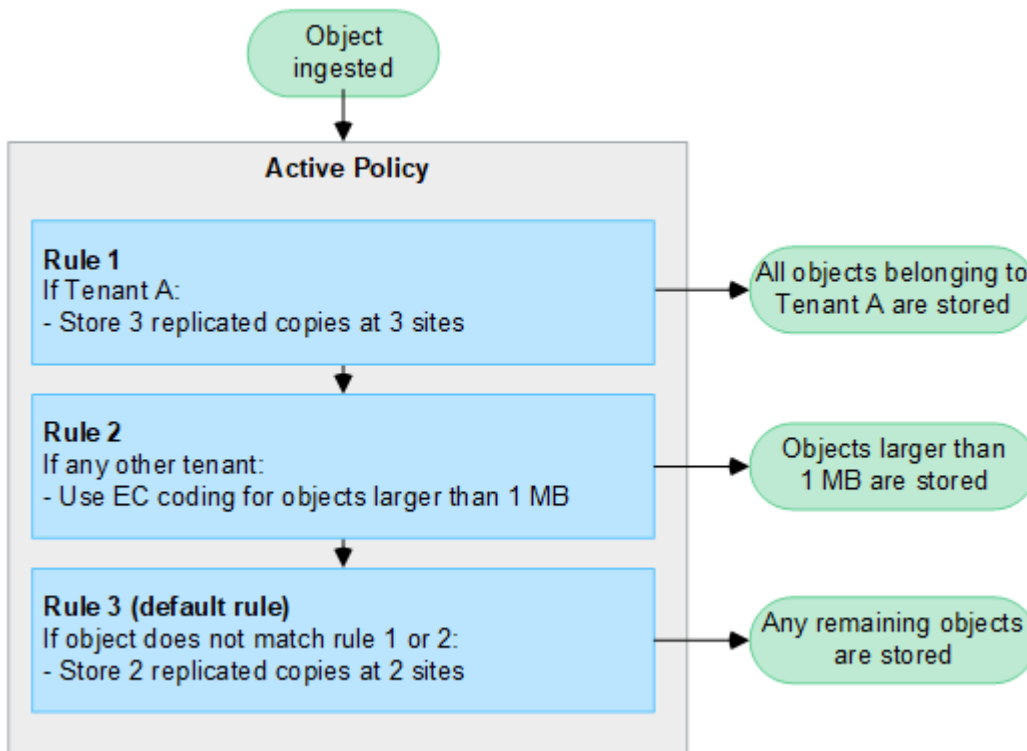
Ad esempio, un criterio ILM potrebbe contenere tre regole ILM che specificano quanto segue:

- **Regola 1: Copie replicate per il tenant A**
 - Abbina tutti gli oggetti appartenenti al tenant A.
 - Memorizzare questi oggetti come tre copie replicate in tre siti.
 - Gli oggetti appartenenti ad altri tenant non corrispondono alla regola 1, quindi vengono valutati in base alla regola 2.
- **Regola 2: Erasure coding per oggetti superiori a 1 MB**
 - Associare tutti gli oggetti degli altri tenant, ma solo se sono superiori a 1 MB. Questi oggetti più grandi vengono memorizzati utilizzando la codifica di cancellazione 6+3 in tre siti.
 - Non corrisponde a oggetti di dimensioni pari o inferiori a 1 MB, pertanto questi oggetti vengono valutati

in base alla regola 3.

- **Regola 3: 2 copie 2 data center** (impostazione predefinita)

- È l'ultima regola predefinita del criterio. Non utilizza filtri.
- Creare due copie replicate di tutti gli oggetti non corrispondenti alla regola 1 o alla regola 2 (oggetti non appartenenti al tenant A di dimensioni pari o inferiori a 1 MB).



Cosa sono i criteri attivi e inattivi?

Ogni sistema StorageGRID deve avere almeno una policy ILM attiva. Se si desidera disporre di più criteri ILM attivi, è necessario creare tag dei criteri ILM e assegnare un criterio a ciascun tag. I tenant applicano quindi i tag ai bucket S3. Il criterio predefinito viene applicato a tutti gli oggetti nei bucket che non hanno un tag di criterio assegnato.

Quando si crea per la prima volta un criterio ILM, selezionare una o più regole ILM e disporle in un ordine specifico. Dopo aver simulato il criterio per confermarne il comportamento, lo si attiva.

Quando si attiva un criterio ILM, StorageGRID utilizza tale criterio per gestire tutti gli oggetti, inclusi gli oggetti esistenti e gli oggetti appena acquisiti. Gli oggetti esistenti potrebbero essere spostati in nuove posizioni quando vengono implementate le regole ILM nel nuovo criterio.

Se si attivano più policy ILM alla volta e i tenant applicano tag ai bucket S3, gli oggetti in ogni bucket vengono gestiti in base alla policy assegnata al tag.

Un sistema StorageGRID tiene traccia della cronologia delle policy attivate o disattivate.

Considerazioni per la creazione di un criterio ILM

- Utilizzare solo il criterio fornito dal sistema, il criterio di base 2 copie, nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola Make 2 Copies in questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.



Il pool di storage All Storage Node viene creato automaticamente durante l'installazione di StorageGRID 11.6 e versioni precedenti. Se si esegue l'aggiornamento a una versione successiva di StorageGRID, il pool di tutti i nodi di storage continuerà a esistere. Se si installa StorageGRID 11.7 o versione successiva come nuova installazione, il pool di tutti i nodi di storage non viene creato.

- Durante la progettazione di un nuovo criterio, considerare tutti i diversi tipi di oggetti che potrebbero essere inseriti nella griglia. Assicurarsi che il criterio includa regole per la corrispondenza e posizionare questi oggetti secondo necessità.
- Mantenere la policy ILM il più semplice possibile. In questo modo si evitano situazioni potenzialmente pericolose in cui i dati degli oggetti non sono protetti come previsto quando nel tempo vengono apportate modifiche al sistema StorageGRID.
- Assicurarsi che le regole della policy siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio. Ad esempio, se la prima regola di un criterio corrisponde a un oggetto, tale oggetto non verrà valutato da altre regole.
- L'ultima regola in ogni policy ILM è la regola ILM predefinita, che non può utilizzare alcun filtro. Se un oggetto non è stato associato da un'altra regola, la regola predefinita controlla la posizione e il tempo di conservazione dell'oggetto.
- Prima di attivare un nuovo criterio, esaminare le modifiche apportate dal criterio al posizionamento degli oggetti esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Crea policy ILM in StorageGRID

Create una o più policy ILM per soddisfare i vostri requisiti di qualità del servizio.

La presenza di una policy ILM attiva ti consente di applicare le stesse regole ILM a tutti i tenant e bucket.

La disponibilità di più policy ILM attive ti consente di applicare le regole ILM appropriate a tenant e bucket specifici per soddisfare più requisiti di qualità del servizio.

Creare un criterio ILM

A proposito di questa attività

Prima di creare un criterio personalizzato, verificare che ["Policy ILM predefinita"](#) non soddisfi i requisiti di archiviazione.



Utilizzare solo i criteri forniti dal sistema, 2 Copies Policy (per le griglie a un sito) o 1 Copy per Site (per le griglie a più siti), nei sistemi di test. Per StorageGRID 11.6 e versioni precedenti, la regola predefinita in questo criterio utilizza il pool di storage All Storage Node, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.



Se ["L'impostazione Global S3 Object Lock \(blocco oggetti S3 globale\) è stata attivata"](#) devi assicurarti che la policy ILM sia conforme ai requisiti dei bucket che hanno S3 Object Lock abilitato. In questa sezione, segui le istruzioni che menzionano S3 Object Lock abilitato.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso richieste"](#).

- L'utente si "[Regole ILM create](#)" basa sull'attivazione di blocco oggetti S3.

Blocco oggetti S3 non abilitato

- Da "[Creazione delle regole ILM](#)" aggiungere al criterio. Se necessario, è possibile salvare un criterio, creare regole aggiuntive e quindi modificarlo per aggiungerne di nuove.
- Non sono presenti "[Creazione di una regola ILM predefinita](#)" filtri.

Blocco oggetti S3 attivato

- Il "[L'impostazione Global S3 Object Lock \(blocco oggetti S3 globale\) è già attivata](#)" per il sistema StorageGRID.
- Da "[Creazione delle regole ILM conformi e non conformi](#)" aggiungere al criterio. Se necessario, è possibile salvare un criterio, creare regole aggiuntive e quindi modificarlo per aggiungerne di nuove.
- Si dispone di "[Creazione di una regola ILM predefinita](#)" per il criterio che è conforme.

- Facoltativamente, hai guardato il video:

[Panoramica delle politiche ILM](#)

Vedere anche "[Utilizzare i criteri ILM](#)".

Fasi

1. Selezionare **ILM > Policy**.

Se l'impostazione blocco oggetti S3 globale è attivata, la pagina dei criteri ILM indica quali regole ILM sono conformi.

2. Stabilire come si desidera creare il criterio ILM.

Creare una nuova policy

- a. Selezionare **Crea policy**.

Clonazione della policy esistente

- a. Selezionare la casella di controllo relativa al criterio che si desidera iniziare, quindi selezionare **Clona**.

Modifica criterio esistente

- a. Se un criterio è inattivo, è possibile modificarlo. Selezionare la casella di controllo per il criterio inattivo che si desidera iniziare, quindi selezionare **Modifica**.

3. Nel campo **Nome criterio**, immettere un nome univoco per la policy.
4. Facoltativamente, nel campo **motivo della modifica**, immettere il motivo per cui si sta creando un nuovo criterio.
5. Per aggiungere regole al criterio, selezionare **Seleziona regole**. Selezionare il nome di una regola per visualizzare le relative impostazioni.

Se si sta clonando un criterio:

- Vengono selezionate le regole utilizzate dal criterio che si sta clonando.
- Se il criterio da clonare utilizza regole senza filtri che non erano la regola predefinita, viene richiesto di rimuovere tutte le regole tranne una di queste.
- Se la regola predefinita utilizza un filtro, viene richiesto di selezionare una nuova regola predefinita.
- Se la regola predefinita non è l'ultima, è possibile spostarla alla fine del nuovo criterio.

Blocco oggetti S3 non abilitato

- Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, selezionare **pagina regole ILM**.

La regola predefinita si applica a tutti gli oggetti che non corrispondono a un'altra regola del criterio. La regola predefinita non può utilizzare alcun filtro e viene sempre valutata per ultima.



Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se il sistema StorageGRID dispone di più siti, è possibile che due copie di un oggetto vengano posizionate sullo stesso sito.

Blocco oggetti S3 attivato

- Selezionare una regola predefinita per il criterio. Per creare una nuova regola predefinita, selezionare **pagina regole ILM**.

L'elenco delle regole contiene solo le regole che sono conformi e non utilizzano filtri.



Non utilizzare la regola di creazione di 2 copie come regola predefinita per un criterio. La regola Make 2 copies utilizza un singolo pool di storage, tutti i nodi di storage, che contiene tutti i siti. Se si utilizza questa regola, sullo stesso sito potrebbero essere collocate più copie di un oggetto.

- Se è necessaria una regola "predefinita" diversa per gli oggetti nei bucket S3 non conformi, selezionare **Includi una regola senza filtri per i bucket S3 non conformi** e selezionare una regola non conforme che non utilizza un filtro.

Ad esempio, è possibile utilizzare un Cloud Storage Pool per memorizzare oggetti in bucket che non hanno attivato il blocco oggetti S3.



È possibile selezionare solo una regola non conforme che non utilizza un filtro.

Vedere anche ["Esempio 7: Policy ILM conforme per il blocco oggetti S3"](#).

- Una volta selezionata la regola predefinita, selezionare **continua**.
- Per il passo altre regole, selezionare le altre regole che si desidera aggiungere al criterio. Queste regole utilizzano almeno un filtro (account tenant, nome bucket, filtro avanzato o tempo di riferimento non corrente). Quindi selezionare **Seleziona**.

La finestra Crea un criterio elenca ora le regole selezionate. La regola predefinita è alla fine, con le altre regole sopra di essa.

Se S3 Object Lock è attivato e è stata selezionata anche una regola "predefinita" non conforme, tale regola viene aggiunta come regola dalla seconda all'ultima nel criterio.



Viene visualizzato un avviso se una regola non mantiene gli oggetti per sempre. Quando si attiva questo criterio, è necessario confermare che si desidera che StorageGRID elimini gli oggetti quando sono trascorse le istruzioni di posizionamento per la regola predefinita (a meno che un ciclo di vita del bucket non mantenga gli oggetti per un periodo di tempo più lungo).

8. Trascinare le righe per le regole non predefinite per determinare l'ordine in cui verranno valutate queste regole.

Impossibile spostare la regola predefinita. Se S3 Object Lock è attivato, non è possibile spostare la regola "predefinita" non conforme se ne è stata selezionata una.



Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

9. Se necessario, selezionare **Select rules** (Seleziona regole) per aggiungere o rimuovere le regole.
10. Al termine, selezionare **Salva**.
11. Ripetere questa procedura per creare ulteriori criteri ILM.
12. [Simulare un criterio ILM](#). È necessario simulare sempre un criterio prima di attivarlo per assicurarsi che funzioni come previsto.

Simulare una policy

Simula una policy sugli oggetti di test prima di attivarla e applicarla ai dati di produzione.

Prima di iniziare

Si conosce il bucket S3/oggetto-chiave per ogni oggetto che si desidera testare.

Fasi

1. Utilizzando un client S3 o "[S3 Console](#)", acquisire gli oggetti necessari per testare ciascuna regola.
2. Nella pagina criteri ILM, selezionare la casella di controllo relativa al criterio, quindi selezionare **simula**.
3. Nel campo **oggetto**, immettere S3 bucket/object-key per un oggetto di test. Ad esempio, bucket-01/filename.png.
4. Se la versione S3 è attivata, è possibile immettere un ID versione per l'oggetto nel campo **ID versione**.
5. Selezionare **simulate**.
6. Nella sezione risultati di Simulation, verificare che ogni oggetto sia stato associato alla regola corretta.
7. Per determinare quale profilo di pool storage o erasure coding è in vigore, seleziona il nome della regola abbinata e vai alla pagina dei dettagli della regola.



Esaminare eventuali modifiche al posizionamento degli oggetti replicati e con erasure coding esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Risultati

Qualsiasi modifica alle regole della policy si rifletterà nei risultati della simulazione e mostrerà la nuova

corrispondenza e la corrispondenza precedente. La finestra Simula policy conserva gli oggetti che hai testato finché non selezioni **Cancella tutto** o l'icona di rimozione  per ciascun oggetto nell'elenco dei risultati della simulazione.

Informazioni correlate

["Esempi di simulazioni dei criteri ILM"](#)

Attivare un criterio

Quando si attiva un singolo nuovo criterio ILM, gli oggetti esistenti e gli oggetti appena acquisiti vengono gestiti da tale criterio. Quando si attivano più policy, i tag dei criteri ILM assegnati ai bucket determinano gli oggetti da gestire.

Prima di attivare un nuovo criterio:

1. Simulare il criterio per confermare che si comporta come previsto.
2. Esaminare eventuali modifiche al posizionamento degli oggetti replicati e con erasure coding esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.



Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile.

A proposito di questa attività

Quando si attiva un criterio ILM, il sistema distribuisce il nuovo criterio a tutti i nodi. Tuttavia, il nuovo criterio attivo potrebbe non essere effettivo fino a quando tutti i nodi della griglia non saranno disponibili per ricevere il nuovo criterio. In alcuni casi, il sistema attende l'implementazione di una nuova policy attiva per garantire che gli oggetti Grid non vengano rimossi accidentalmente. In particolare:

- Se si apportano modifiche ai criteri che **aumentano la ridondanza o la durata dei dati**, tali modifiche vengono implementate immediatamente. Ad esempio, se si attiva un nuovo criterio che include una regola di tre copie invece di una regola di due copie, tale criterio verrà implementato immediatamente perché aumenta la ridondanza dei dati.
- Se si apportano modifiche ai criteri che **potrebbero ridurre la ridondanza o la durata dei dati**, tali modifiche non verranno implementate finché non saranno disponibili tutti i nodi della griglia. Ad esempio, se si attiva un nuovo criterio che utilizza una regola di due copie invece di una regola di tre copie, il nuovo criterio viene visualizzato nella scheda criterio attivo, ma non avrà effetto fino a quando tutti i nodi non saranno online e disponibili.

Fasi

Seguire la procedura per attivare uno o più criteri:

Attivare un criterio

Se si dispone di un solo criterio attivo, procedere come segue. Se si dispone già di uno o più criteri attivi e si stanno attivando criteri aggiuntivi, seguire la procedura per l'attivazione di più criteri.

1. Quando si è pronti ad attivare un criterio, selezionare **ILM > Criteri**.

In alternativa, è possibile attivare un singolo criterio dalla pagina **ILM > Policy tags**.

2. Nella scheda Criteri, selezionare la casella di controllo relativa al criterio che si desidera attivare, quindi selezionare **attiva**.
3. Seguire la procedura appropriata:
 - Se viene visualizzato un messaggio di avviso che richiede di confermare l'attivazione del criterio, selezionare **OK**.
 - Se viene visualizzato un messaggio di avviso contenente i dettagli relativi al criterio:
 - i. Esaminare i dettagli per assicurarsi che i criteri gestiscano i dati come previsto.
 - ii. Se la regola predefinita memorizza gli oggetti per un numero limitato di giorni, esaminare il diagramma di conservazione e digitare il numero di giorni nella casella di testo.
 - iii. Se la regola predefinita memorizza gli oggetti per sempre, ma una o più altre regole hanno una conservazione limitata, digitare **yes** nella casella di testo.
 - iv. Selezionare **attiva criterio**.

Attivare più policy

Per attivare più policy, è necessario creare tag policy e assegnare una policy a ciascun tag. Puoi creare un massimo di 10 tag di policy per la tua griglia.



Quando vengono utilizzati più tag di policy, se i tenant riassegnano frequentemente i tag di policy ai bucket, le prestazioni della griglia potrebbero risentirne. Se hai tenant non attendibili, valuta la possibilità di utilizzare solo il tag di policy Default.

1. Selezionare **ILM > Policy tag**.
2. Selezionare **Crea**.
3. Nella finestra di dialogo Crea tag criterio, digitare un nome di tag e, facoltativamente, una descrizione per il tag.



I nomi e le descrizioni dei tag sono visibili ai locatari. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se il criterio assegnato eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni riservate in questi campi.

4. Selezionare **Crea tag**.
5. Nella tabella tag criteri ILM, utilizzare il menu a discesa per selezionare un criterio da assegnare al tag.
6. Se gli avvisi vengono visualizzati nella colonna limitazioni criteri, selezionare **Visualizza dettagli criteri** per rivedere il criterio.
7. Assicurarsi che ogni policy gestisca i dati come previsto.

8. Selezionare **attiva criteri assegnati**. In alternativa, selezionare **Cancella modifiche** per rimuovere l'assegnazione dei criteri.
9. Nella finestra di dialogo attiva criteri con nuovi tag, rivedere le descrizioni di come ciascun tag, criterio e regola gestirà gli oggetti. Apportare le modifiche necessarie per garantire che le policy gestiscano gli oggetti nel modo previsto.
10. Quando si è certi di voler attivare i criteri, digitare **yes** nella casella di testo, quindi selezionare **Activate policies** (attiva criteri).

Informazioni correlate

["Esempio 6: Modifica di un criterio ILM"](#)

Esempi di simulazioni di policy ILM in StorageGRID

Gli esempi di simulazioni dei criteri ILM forniscono linee guida per strutturare e modificare le simulazioni per l'ambiente in uso.

Esempio 1: Verifica delle regole durante la simulazione di un criterio ILM

In questo esempio viene descritto come verificare le regole durante la simulazione di un criterio.

In questo esempio, la **policy ILM di esempio** viene simulata rispetto agli oggetti acquisiti in due bucket. La policy include tre regole, come segue:

- La prima regola, **due copie, due anni per bucket-a**, si applica solo agli oggetti nel bucket-a.
- La seconda regola, **EC objects > 1 MB**, si applica a tutti i bucket, ma ai filtri sugli oggetti superiori a 1 MB.
- La terza regola, **due copie, due data center**, è la regola predefinita. Non include filtri e non utilizza il tempo di riferimento non corrente.

Dopo aver simulato il criterio, verificare che ogni oggetto sia stato associato alla regola corretta.

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
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 corrisponde correttamente alla prima regola, che filtra gli oggetti in bucket-a.
- bucket-b/test object greater than 1 MB.pdf è in bucket-b, quindi non corrisponde alla

prima regola. Al contrario, è stata associata correttamente dalla seconda regola, che filtra su oggetti superiori a 1 MB.

- `bucket-b/test object less than 1 MB.pdf` non corrisponde ai filtri nelle prime due regole, quindi viene posizionata in base alla regola predefinita, che non include filtri.

Esempio 2: Riordinare le regole durante la simulazione di un criterio ILM

Questo esempio mostra come è possibile riordinare le regole per modificare i risultati durante la simulazione di un criterio.

In questo esempio, viene simulata la policy **Demo**. Questo criterio, che ha lo scopo di trovare oggetti con metadati utente `series=x-men`, include tre regole, come segue:

- La prima regola, **PNGS**, filtra i nomi delle chiavi che terminano in `.png`.
- La seconda regola, **X-men**, si applica solo agli oggetti per il tenant A e ai filtri per `series=x-men` metadati utente.
- L'ultima regola, **due copie due data center**, è la regola predefinita, che corrisponde a tutti gli oggetti che non corrispondono alle prime due regole.

Fasi

1. Dopo aver aggiunto le regole e salvato il criterio, selezionare **simulate**.
2. Nel campo **Object**, immettere il bucket `S3/object-key` per un oggetto test e selezionare **simulate**.

Vengono visualizzati i risultati di Simulation, che mostrano che l'`Havok.png` oggetto è stato associato alla regola **PNGS**.

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` era destinato a testare la regola **X-men**.

3. Per risolvere il problema, riordinare le regole.
 - a. Selezionare **fine** per chiudere la finestra Simula policy ILM.
 - b. Selezionare **Edit** (Modifica) per modificare la policy.
 - c. Trascinare la regola **X-MEN** all'inizio dell'elenco.
 - d. Selezionare **Salva**.
4. Selezionare **simulate**.

Gli oggetti precedentemente testati vengono rivalutati in base alla policy aggiornata e vengono visualizzati i risultati della nuova simulazione. Nell'esempio, la colonna regola corrispondente mostra che l'`Havok.png` oggetto ora corrisponde alla regola dei metadati X-MEN, come previsto. La colonna di confronto precedente mostra che la regola PNG corrisponde all'oggetto nella simulazione precedente.

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 un criterio ILM

Questo esempio mostra come simulare una policy, correggere una regola nella policy e continuare la simulazione.

In questo esempio, viene simulata la policy **Demo**. Questo criterio consente di trovare oggetti che contengono `series=x-men` metadati dell'utente. Tuttavia, si sono verificati risultati imprevisti durante la simulazione di questo criterio rispetto all' `Beast.jpg` oggetto. Invece di corrispondere alla regola dei metadati X-MEN, l'oggetto corrisponde 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 test non corrisponde alla regola prevista nel criterio, è necessario esaminare ciascuna regola del criterio e correggere eventuali errori.

Fasi

1. Selezionare **fine** per chiudere la finestra di dialogo Simula policy. Nella pagina dei dettagli del criterio, selezionare **diagramma di conservazione**. Quindi, selezionare **Espandi tutto** o **Visualizza dettagli** per ogni regola in base alle necessità.
2. Esaminare l'account tenant della regola, il tempo di riferimento e i criteri di filtraggio.

Ad esempio, supponiamo che i metadati per la regola X-men siano stati immessi come "x-men01" invece di "x-men".

3. Per risolvere l'errore, correggere la regola come segue:
 - Se la regola fa parte del criterio, è possibile clonarla o rimuoverla dal criterio e modificarla.
 - Se la regola fa parte del criterio attivo, è necessario clonarla. Non è possibile modificare o rimuovere una regola dal criterio attivo.
4. Eseguire nuovamente la simulazione.

In questo esempio, la regola X-MEN corretta corrisponde ora all' `Beast.jpg` oggetto in base ai `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 in StorageGRID

È possibile visualizzare i dettagli dei tag dei criteri ILM, modificare un tag o rimuovere un tag.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso richieste"](#).

Visualizzare i dettagli dei tag dei criteri ILM

Per visualizzare i dettagli di un tag:

1. Selezionare **ILM > Policy tag**.
2. Selezionare il nome del criterio dalla tabella. Viene visualizzata la pagina dei dettagli del tag.
3. Nella pagina dei dettagli, visualizzare la cronologia precedente dei criteri assegnati.
4. Consente di visualizzare un criterio selezionandolo.

Modifica tag criterio ILM



I nomi e le descrizioni dei tag sono visibili ai locatari. Scegli valori che aiuteranno i tenant a prendere una decisione informata quando selezionano i tag dei criteri da assegnare ai loro bucket. Ad esempio, se il criterio assegnato eliminerà gli oggetti dopo un certo periodo di tempo, è possibile comunicarlo nella descrizione. Non includere informazioni riservate in questi campi.

Per modificare la descrizione di un tag esistente:

1. Selezionare **ILM > Policy tag**.
2. Seleziona la casella di controllo per il tag, quindi seleziona **Modifica**.

In alternativa, selezionare il nome del tag. Viene visualizzata la pagina dei dettagli del tag ed è possibile selezionare **Modifica** in quella pagina.

3. Modificare la descrizione del tag secondo necessità
4. Selezionare **Salva**.

Rimuovere il tag criterio ILM

Quando si rimuove un tag di criterio, a tutti i bucket a cui è assegnato tale tag verrà applicato il criterio predefinito.

Per rimuovere un'etichetta:

1. Selezionare **ILM > Policy tag**.
2. Selezionare la casella di controllo per il tag, quindi selezionare **Rimuovi**. Viene visualizzata una finestra di dialogo di conferma.

In alternativa, selezionare il nome del tag. Viene visualizzata la pagina dei dettagli del tag ed è possibile selezionare **Rimuovi** in quella pagina.

3. Selezionare **Sì** per eliminare il tag.

Informazioni correlate

["Scopri come creare tag di policy ILM"](#)

Verifica una policy ILM con la ricerca dei metadati degli oggetti in StorageGRID

Dopo aver attivato una policy ILM, acquisire gli oggetti di test rappresentativi nel sistema StorageGRID, quindi eseguire una ricerca nei metadati degli oggetti per confermare la creazione delle copie nella maniera prevista e il posizionamento nelle posizioni corrette.

Prima di iniziare

Hai un identificatore di oggetto, che può essere uno dei seguenti:

- **UUID**: 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**.

Fasi

1. Acquisire l'oggetto.
2. Selezionare **ILM > Object metadata lookup**.
3. Digitare l'identificativo dell'oggetto nel campo **Identifier**. È possibile immettere un UUID, CBID o un bucket/oggetto S3.
4. Facoltativamente, inserire un ID versione per l'oggetto (solo S3).
5. Selezionare **Cerca**.

Vengono visualizzati i risultati della ricerca dei metadati dell'oggetto. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, come ID oggetto (UUID), tipo di risultato (oggetto, marker di eliminazione, bucket S3) e dimensioni logiche dell'oggetto. Per ulteriori dettagli, fare riferimento alla schermata di esempio riportata di seguito.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.

- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
 - Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
 - Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
 - Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.
6. Verificare che l'oggetto sia memorizzato nella posizione o nelle posizioni corrette e che sia il tipo di copia corretto.

Se l'opzione Audit è attivata, è anche possibile monitorare il registro di audit per il messaggio ORLM Object Rules Met. Il messaggio di audit ORLM può fornire ulteriori informazioni sullo stato del processo di valutazione ILM, ma non può fornire informazioni sulla correttezza del posizionamento dei dati dell'oggetto o sulla completezza della policy ILM. È necessario valutarlo da soli. Per ulteriori informazioni, vedere ["Esaminare i registri di audit"](#).

Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.



La seguente schermata è un esempio. I risultati variano a seconda della versione di StorageGRID in uso.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAIS": "2",

```

Informazioni correlate

["UTILIZZARE L'API REST S3"](#)

Lavora con le policy ILM e le regole ILM in StorageGRID

In caso di cambiamento dei requisiti di storage, potrebbe essere necessario implementare criteri aggiuntivi o modificare le regole ILM associate a un criterio. È possibile visualizzare le metriche ILM per determinare le performance del sistema.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Visualizza i criteri ILM

Per visualizzare i criteri ILM attivi e inattivi e la cronologia di attivazione dei criteri:

1. Selezionare **ILM > Policy**.
2. Selezionare **Criteri** per visualizzare un elenco di criteri attivi e inattivi. La tabella elenca il nome di ciascun criterio, i tag a cui è assegnato il criterio e se il criterio è attivo o inattivo.
3. Selezionare **Cronologia attivazioni** per visualizzare un elenco delle date di inizio e di fine delle attivazioni per i criteri.
4. Selezionare il nome di un criterio per visualizzarne i dettagli.



Se si visualizzano i dettagli di un criterio il cui stato è modificato o eliminato, viene visualizzato un messaggio che spiega che si sta visualizzando la versione del criterio che era attiva per l'intervallo di tempo specificato e che è stata successivamente modificata o eliminata.

Modificare un criterio ILM

È possibile modificare solo un criterio inattivo. Se si desidera modificare un criterio attivo, disattivarlo o creare un clone e modificarlo.

Per modificare un criterio:

1. Selezionare **ILM > Policy**.
2. Selezionare la casella di controllo relativa al criterio che si desidera modificare, quindi selezionare **Modifica**.
3. Modificare il criterio seguendo le istruzioni riportate in "[Creare policy ILM](#)".
4. Simulare il criterio prima di riattivarlo.



Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Clonazione di una policy ILM

Per clonare un criterio ILM:

1. Selezionare **ILM > Policy**.
2. Selezionare la casella di controllo relativa al criterio da clonare, quindi selezionare **Clona**.
3. Creare un nuovo criterio a partire dal criterio clonato seguendo le istruzioni riportate in "[Creare policy ILM](#)".



Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Rimuovere un criterio ILM

È possibile rimuovere un criterio ILM solo se è inattivo. Per rimuovere un criterio:

1. Selezionare **ILM > Policy**.
2. Selezionare la casella di controllo relativa al criterio inattivo che si desidera rimuovere.
3. Selezionare **Rimuovi**.

Visualizza i dettagli della regola ILM

Per visualizzare i dettagli di una regola ILM, inclusi il diagramma di conservazione e le istruzioni di posizionamento della regola:

1. Selezionare **ILM > regole**.
2. Selezionare il nome della regola di cui si desidera visualizzare i dettagli. Esempio:

The screenshot shows the details for a rule named "2 copies 2 data centers". At the top, it lists properties: Compliant: No, Ingest behavior: Strict, and Reference time: Noncurrent time. Below these are buttons for Clone, Edit, and Remove. There are two tabs: "Rule detail" (active) and "Used in policies". Under "Rule detail", there's a section "Time period and placements" with two sub-tabs: "Retention diagram" (active) and "Placement instructions". The "Retention diagram" shows a timeline from "Day 0" to "Forever". It displays two retention periods: "2 replicated copies - Data Center 1" (blue bar) and "EC 2+1 - Data Center 1" (grey bar). Above the timeline, there's a legend for "Sort placements by" with options "Time period" (selected) and "Storage pool", and a legend for "Replicated copy" (blue dot) and "Erasure-coded (EC) copy" (grey dot). Below the timeline, a "Rule analysis" section states: "Objects processed by this rule will not be deleted by ILM." The timeline itself has a label "Day 0 - forever" on the left and "Duration" and "Forever" at the bottom.

Inoltre, è possibile utilizzare la pagina dei dettagli per clonare, modificare o rimuovere una regola. Non è possibile modificare o rimuovere una regola se utilizzata in alcun criterio.

Clonare una regola ILM

È possibile clonare una regola esistente se si desidera creare una nuova regola che utilizzi alcune delle impostazioni della regola esistente. Se è necessario modificare una regola utilizzata in qualsiasi criterio, è necessario clonare la regola e apportare le modifiche al clone. Una volta apportate le modifiche al clone, è possibile rimuovere la regola originale dal criterio e sostituirla con la versione modificata, se necessario.



Non è possibile clonare una regola ILM se è stata creata utilizzando StorageGRID versione 10.2 o precedente.

Fasi

1. Selezionare **ILM > regole**.
2. Selezionare la casella di controllo della regola da clonare, quindi selezionare **Clone**. In alternativa, selezionare il nome della regola, quindi selezionare **Clone** dalla pagina dei dettagli della regola.
3. Aggiornare la regola clonata seguendo i passaggi per [Modifica di una regola ILM](#) e ["Utilizzo di filtri avanzati"](#)

nelle regole ILM".

Quando si clonano una regola ILM, è necessario immettere un nuovo nome.

Modificare una regola ILM

Potrebbe essere necessario modificare una regola ILM per modificare un filtro o un'istruzione di posizionamento.

Non è possibile modificare una regola se utilizzata in qualsiasi criterio ILM. È possibile [clonare la regola](#) apportare tutte le modifiche necessarie alla copia clonata.



Un criterio ILM non configurato correttamente può causare una perdita di dati non ripristinabile. Prima di attivare un criterio ILM, esaminare attentamente il criterio ILM e le relative regole ILM, quindi simulare il criterio ILM. Verificare sempre che la policy ILM funzioni come previsto.

Fasi

1. Selezionare **ILM > regole**.
2. Verificare che la regola che si desidera modificare non sia utilizzata in alcun criterio ILM.
3. Se la regola che si desidera modificare non è in uso, selezionare la casella di controllo corrispondente e selezionare **azioni > Modifica**. In alternativa, selezionare il nome della regola, quindi selezionare **Modifica** nella pagina dei dettagli della regola.
4. Completare i passaggi della procedura guidata Modifica regola ILM. Se necessario, seguire i passi per ["Creazione di una regola ILM"](#) e ["Utilizzo di filtri avanzati nelle regole ILM"](#).

Quando si modifica una regola ILM, non è possibile modificarne il nome.

Rimuovere una regola ILM

Per mantenere gestibile l'elenco delle regole ILM correnti, rimuovi tutte le regole ILM che non sei in grado di utilizzare.

Fasi

Per rimuovere una regola ILM attualmente utilizzata in un criterio attivo:

1. Clonazione della policy.
2. Rimuovere la regola ILM dal clone dei criteri.
3. Salvare, simulare e attivare il nuovo criterio per assicurarsi che gli oggetti siano protetti come previsto.
4. Passare alla procedura per la rimozione di una regola ILM attualmente utilizzata in un criterio inattivo.

Per rimuovere una regola ILM attualmente utilizzata in un criterio inattivo:

1. Selezionare il criterio inattivo.
2. Rimuovere la regola ILM dal criterio o [rimuovere il criterio](#).
3. Passare alla procedura per la rimozione di una regola ILM non attualmente utilizzata.

Per rimuovere una regola ILM attualmente non utilizzata:

1. Selezionare **ILM > regole**.

2. Verificare che la regola che si desidera rimuovere non venga utilizzata in alcun criterio.
3. Se la regola che si desidera rimuovere non è in uso, selezionarla e scegliere **azioni > Rimuovi**. È possibile selezionare più regole e rimuoverle tutte contemporaneamente.
4. Selezionare **Sì** per confermare che si desidera rimuovere la regola ILM.

Visualizza metriche ILM

È possibile visualizzare le metriche per ILM, ad esempio il numero di oggetti nella coda e il tasso di valutazione. È possibile monitorare queste metriche per determinare le performance del sistema. Una grande coda o un tasso di valutazione potrebbe indicare che il sistema non è in grado di tenere il passo con la velocità di acquisizione, che il carico dalle applicazioni client è eccessivo o che esistono condizioni anomale.

Fasi

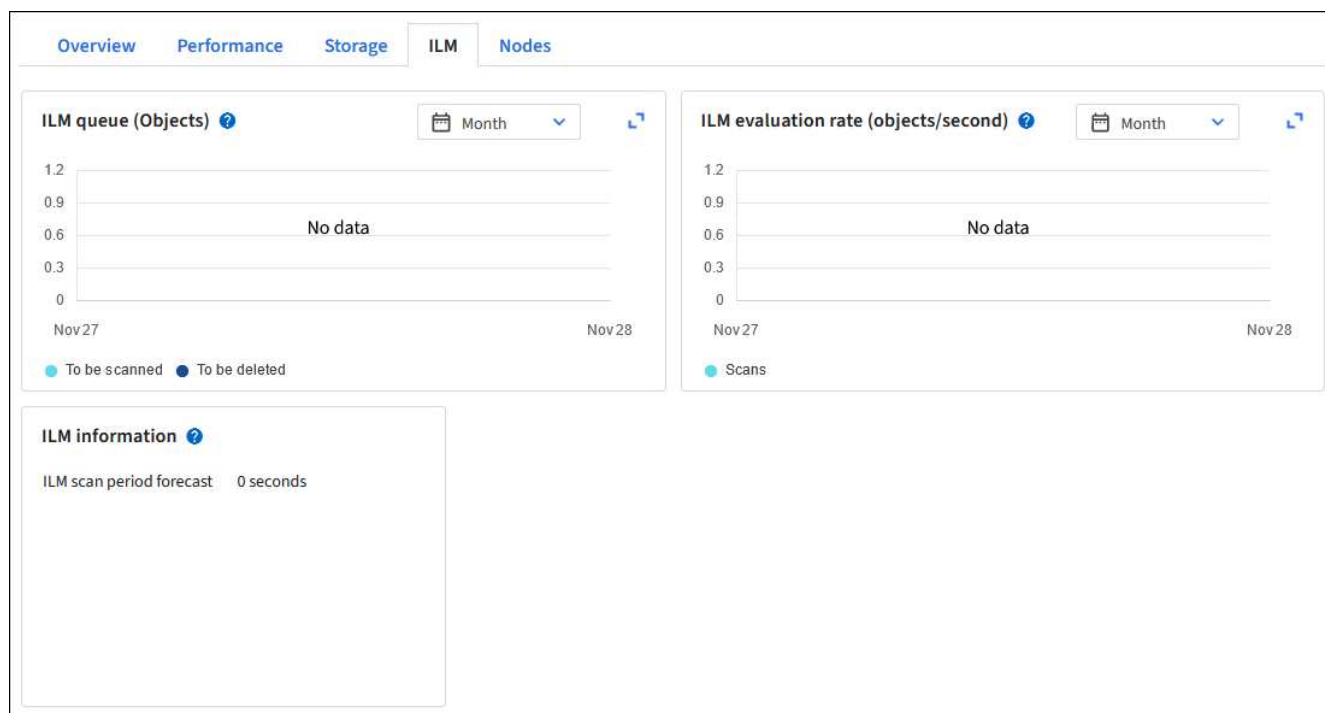
1. Selezionare **Dashboard > ILM**.



Poiché la dashboard può essere personalizzata, la scheda ILM potrebbe non essere disponibile.

2. Monitorare le metriche nella scheda ILM.

Puoi selezionare il punto interrogativo (?) per vedere una descrizione degli elementi nella scheda ILM.



USA blocco oggetti S3

Come S3 Object Lock protegge gli oggetti in StorageGRID

In qualità di amministratore di rete, è possibile attivare il blocco oggetti S3 per il sistema StorageGRID e implementare un criterio ILM conforme per garantire che gli oggetti in specifici bucket S3 non vengano cancellati o sovrascritti per un periodo di tempo

specificato.

Che cos'è il blocco oggetti S3?

La funzione blocco oggetti StorageGRID S3 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3).

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. Quando l'impostazione allow S3 Object Lock for existing buckets è abilitata, un account tenant S3 può abilitare S3 Object Lock per un bucket esistente. Se un bucket ha S3 Object Lock abilitato, il versioning del bucket è richiesto e viene abilitato automaticamente. Dopo che un account tenant S3 ha abilitato S3 Object Lock per un bucket nuovo o esistente, non può essere disabilitato.

Un bucket senza blocco oggetti S3 può avere solo oggetti senza impostazioni di conservazione specificate. Nessun oggetto acquisito avrà impostazioni di conservazione.

Un bucket con blocco oggetti S3 può avere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con blocco oggetto S3 e conservazione predefinita configurata può avere caricato oggetti con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, poiché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In effetti, 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 invariati.

Modalità di conservazione

La funzione blocco oggetti di StorageGRID S3 supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità equivalgono alle modalità di conservazione Amazon S3.

- In modalità compliance:
 - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
 - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare alcune impostazioni di conservazione.
 - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione:** Conformità o governance.
- **Mantieni-fino-data:** Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere cancellato.
- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono indipendenti dalla conservazione fino alla data odierna.



Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, fai riferimento a ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** Conformità o governance.
- **Default Retention Period** (periodo di conservazione predefinito): Per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di proprie impostazioni di conservazione. Gli oggetti bucket esistenti non vengono influenzati quando si aggiungono o si modificano queste impostazioni predefinite.

Fai riferimento a ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).

Confronto tra blocco oggetti S3 e conformità legacy

Il blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Poiché la funzione blocco oggetto S3 è conforme ai requisiti Amazon S3, depreca la funzione di conformità proprietaria di StorageGRID, che ora viene chiamata "conformità legacy".



L'impostazione globale di Compliance è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione S3 Object Lock viene abilitata automaticamente. Puoi continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket compliant esistenti; tuttavia, non puoi creare nuovi bucket compliant. Per dettagli, consulta ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#).

Se è stata utilizzata la funzionalità di conformità legacy in una versione precedente di StorageGRID, fare riferimento alla tabella seguente per informazioni sul confronto con la funzione blocco oggetti S3 di StorageGRID.

	Blocco oggetti S3	Compliance (legacy)
In che modo la funzionalità è abilitata a livello globale?	Da Grid Manager, seleziona Configurazione > Sistema > Blocco oggetto S3 .	Non più supportato.
In che modo è abilitata la funzione per un bucket?	Gli utenti devono attivare il blocco oggetti S3 quando creano un nuovo bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3.	Non più supportato.
La versione del bucket è supportata?	Sì. La versione del bucket è obbligatoria e viene attivata automaticamente quando il blocco oggetti S3 è attivato per il bucket.	No
Come viene impostata la conservazione degli oggetti?	Gli utenti possono impostare un periodo di conservazione fino alla data di scadenza per ciascuna versione dell'oggetto oppure impostare un periodo di conservazione predefinito per ciascun bucket.	Gli utenti devono impostare un periodo di conservazione per l'intero bucket. Il periodo di conservazione si applica a tutti gli oggetti nel bucket.
È possibile modificare il periodo di conservazione?	• In modalità compliance, è possibile aumentare il periodo di conservazione fino alla data di una versione a oggetti, ma non ridurlo mai. • In modalità governance, gli utenti con autorizzazioni speciali possono ridurre o persino rimuovere le impostazioni di conservazione di un oggetto.	Il periodo di conservazione di un bucket può essere aumentato ma non ridotto.
Dove viene controllata la conservazione legale?	Gli utenti possono porre un blocco legale o revocare un blocco legale per qualsiasi versione di oggetto nel bucket.	Un blocco legale viene posizionato sul bucket e influisce su tutti gli oggetti nel bucket.

	Blocco oggetti S3	Compliance (legacy)
Quando è possibile eliminare gli oggetti?	- In modalità compliance, è possibile eliminare una versione dell'oggetto dopo aver raggiunto la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale. - In modalità governance, gli utenti con autorizzazioni speciali possono eliminare un oggetto prima che venga raggiunta la data di conservazione, presupponendo che l'oggetto non sia sottoposto a conservazione legale.	È possibile eliminare un oggetto dopo la scadenza del periodo di conservazione, presupponendo che il bucket non sia sottoposto a conservazione legale. Gli oggetti possono essere cancellati automaticamente o manualmente.
La configurazione del ciclo di vita del bucket è supportata?	Sì	No

Flusso di lavoro S3 Object Lock in StorageGRID

In qualità di amministratore della griglia, è necessario coordinare strettamente gli utenti tenant per garantire che gli oggetti siano protetti in modo da soddisfare i requisiti di conservazione.



L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più in base a connettività di rete, stato dei nodi e operazioni Cassandra.

Gli elenchi seguenti per gli amministratori di grid e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzione blocco oggetti S3.

Amministratore di grid

- Attiva l'impostazione blocco oggetti S3 globale per l'intero sistema StorageGRID.
- Consenti agli utenti di abilitare S3 Object Lock per i bucket esistenti.
- Assicurarsi che i criteri ILM (Information Lifecycle Management) siano *conformi*, ovvero che soddisfino la ["Requisiti dei bucket con blocco oggetti S3 abilitato"](#).
- Se necessario, consentire a un tenant di utilizzare la modalità di conservazione Compliance. In caso contrario, è consentita solo la modalità Governance.
- In base alle necessità, imposta il periodo di conservazione massimo per un tenant.

Utente tenant

- Esaminare le considerazioni per bucket e oggetti con blocco oggetto S3.
- Se necessario, contatta un amministratore di grid per abilitare una delle seguenti impostazioni:
 - Blocco globale oggetto S3
 - Consenti l'attivazione del blocco oggetti S3 per i bucket esistenti

- Crea bucket con blocco oggetti S3 abilitato.
- Abilita il blocco degli oggetti S3 sui bucket esistenti.
- Facoltativamente, configurare le impostazioni di conservazione predefinite per un bucket:
 - Modalità di conservazione predefinita: Governance o conformità, se consentita dall'amministratore della griglia.
 - Periodo di conservazione predefinito: Deve essere minore o uguale al periodo di conservazione massimo impostato dall'amministratore di rete.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e impostare facoltativamente la conservazione specifica degli oggetti:
 - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore del grid.
 - Mantieni fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Informazioni correlate

Scopri di più ["Requisiti di S3 Object Lock"](#)

Requisiti di S3 Object Lock in StorageGRID

È necessario esaminare i requisiti per l'attivazione dell'impostazione globale di blocco oggetti S3, i requisiti per la creazione di regole ILM e criteri ILM conformi e le restrizioni applicate da StorageGRID ai bucket e agli oggetti che utilizzano il blocco oggetti S3.

Requisiti per l'utilizzo dell'impostazione globale S3 Object Lock

- È necessario attivare l'impostazione globale S3 Object Lock utilizzando Grid Manager o l'API Grid Management prima che qualsiasi tenant S3 possa creare un bucket con S3 Object Lock attivato.
- L'attivazione dell'impostazione globale S3 Object Lock consente a tutti gli account tenant S3 di creare bucket con S3 Object Lock attivato.
- Dopo aver attivato l'impostazione di blocco oggetti S3 globale, non è possibile disattivare l'impostazione.
- Non è possibile attivare il blocco oggetto S3 globale a meno che la regola predefinita in tutti i criteri ILM attivi non sia *conforme* (vale a dire, la regola predefinita deve essere conforme ai requisiti dei bucket con blocco oggetto S3 abilitato).
- Quando l'impostazione blocco oggetti S3 globale è attivata, non è possibile creare un nuovo criterio ILM o attivare un criterio ILM esistente a meno che la regola predefinita nel criterio non sia conforme. Una volta attivata l'impostazione globale S3 Object Lock, le pagine delle regole ILM e dei criteri ILM indicano quali regole ILM sono conformi.

Requisiti per abilitare S3 Object Lock sui bucket esistenti

Quando l'impostazione globale S3 Object Lock è abilitata, puoi facoltativamente consentire a tutti gli account tenant S3 o agli utenti S3 con le autorizzazioni di abilitare S3 Object Lock sui bucket esistenti. Quando un account tenant S3 o un utente S3 abilita S3 Object Lock su un bucket esistente, potrebbe causare una migrazione dei dati da un Cloud Storage Pool a StorageGRID, a seconda delle tue regole ILM.



Non puoi interrompere la migrazione dei dati non intenzionale dopo che è iniziata.

Requisiti per le regole ILM conformi

Se si desidera attivare l'impostazione blocco oggetto S3 globale, è necessario verificare che la regola predefinita in tutti i criteri ILM attivi sia conforme. Una regola conforme soddisfa i requisiti di entrambi i bucket con blocco oggetti S3 attivato e di tutti i bucket esistenti con conformità legacy attivata:

- Deve creare almeno due copie di oggetti replicate o una copia con codice di cancellazione.
- Queste copie devono esistere nei nodi di storage per l'intera durata di ciascuna riga nelle istruzioni di posizionamento.
- Impossibile salvare le copie degli oggetti in un Cloud Storage Pool.
- Almeno una riga delle istruzioni di posizionamento deve iniziare al giorno 0, utilizzando **Ingest Time** come ora di riferimento.
- Almeno una riga delle istruzioni di posizionamento deve essere "per sempre".

Requisiti per le policy ILM

Quando l'impostazione blocco oggetto S3 globale è attivata, i criteri ILM attivi e inattivi possono includere regole conformi e non conformi.

- La regola predefinita in un criterio ILM attivo o inattivo deve essere conforme.
- Le regole non conformi si applicano solo agli oggetti nei bucket che non hanno attivato il blocco oggetti S3 o che non hanno la funzionalità Compliance legacy attivata.
- Le regole conformi possono essere applicate agli oggetti in qualsiasi bucket; non è necessario attivare il blocco oggetti S3 o la conformità legacy per il bucket.

"Esempio di un criterio ILM conforme per il blocco degli oggetti S3"

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di

conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso le seguenti fasi:

1. Acquisizione oggetto

Quando una versione dell'oggetto viene aggiunta al bucket con S3 Object Lock attivato, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate le impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
- Se non sono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
- Se non sono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto che i metadati S3 definiti dall'utente.

2. Conservazione ed eliminazione degli oggetti

StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti delle copie degli oggetti e le posizioni dello storage sono determinati dalle regole di conformità nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla modalità di conservazione.

- Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Informazioni correlate

- ["Creare un bucket S3"](#)
- ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#)
- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Esempio 7: Policy ILM conforme per il blocco oggetti S3"](#)

Abilita il blocco degli oggetti S3 in StorageGRID

Se un account tenant S3 deve rispettare i requisiti normativi durante il salvataggio dei dati degli oggetti, è necessario attivare il blocco oggetti S3 per l'intero sistema StorageGRID. L'attivazione dell'impostazione globale S3 Object Lock consente a qualsiasi utente del tenant S3 di creare e gestire bucket e oggetti con S3 Object Lock.

Prima di iniziare

- Si dispone di ["Autorizzazione di accesso root"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai esaminato il flusso di lavoro S3 Object Lock e hai compreso le considerazioni.
- Hai confermato che la regola predefinita nella policy ILM attiva è conforme. Consulta ["Creare una regola ILM predefinita"](#) per i dettagli.

A proposito di questa attività

Un amministratore della griglia deve attivare l'impostazione globale S3 Object Lock per consentire agli utenti tenant di creare nuovi bucket con S3 Object Lock attivato. Una volta attivata, questa impostazione non può essere disattivata.

Dopo aver abilitato il blocco degli oggetti S3, un amministratore della griglia può anche consentire agli utenti del tenant di abilitare il blocco degli oggetti S3 su un bucket esistente. Dopo che un amministratore della griglia ha abilitato questa impostazione, può disabilitarla. Per ulteriori informazioni, consulta ["Requisiti di S3 Object Lock"](#).

Rivedere le impostazioni di conformità dei tenant esistenti dopo aver attivato l'impostazione blocco oggetto S3 globale. Quando si attiva questa impostazione, le impostazioni di blocco degli oggetti S3 per tenant dipendono dalla release di StorageGRID al momento della creazione del tenant.



L'impostazione globale di Compliance è obsoleta. Se hai abilitato questa impostazione utilizzando una versione precedente di StorageGRID, l'impostazione S3 Object Lock viene abilitata automaticamente. Puoi continuare a utilizzare StorageGRID per gestire le impostazioni dei bucket compliant esistenti; tuttavia, non puoi creare nuovi bucket compliant. Per dettagli, consulta ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#).

Fasi

1. Selezionare **Configurazione > Sistema > Blocco oggetto S3**.

Viene visualizzata la pagina S3 Object Lock Settings (Impostazioni blocco oggetti S3).

2. Seleziona **Abilita blocco oggetti S3** per abilitare il blocco oggetti S3 per l'intero sistema StorageGRID.
3. Facoltativamente, seleziona **Consenti l'attivazione del blocco degli oggetti S3 sui bucket esistenti**.



L'attivazione del blocco degli oggetti S3 su un bucket esistente potrebbe causare una migrazione dei dati da un cloud storage pool a StorageGRID, a seconda delle regole ILM. Non puoi interrompere questa migrazione una volta avviata. Per ulteriori informazioni, consulta ["Requisiti di S3 Object Lock"](#).

4. Selezionare **Applica**.

Viene visualizzata una finestra di dialogo di conferma che ricorda che non è possibile disattivare il blocco oggetti S3 dopo che è stato attivato.

5. Se si è certi di voler abilitare in modo permanente il blocco oggetti S3 per l'intero sistema, selezionare **OK**.

Quando si seleziona **OK**:

- Se la regola predefinita nel criterio ILM attivo è conforme, il blocco oggetti S3 è ora attivato per l'intera griglia e non può essere disattivato.
- Se la regola predefinita non è conforme, viene visualizzato un errore. Devi creare e attivare una nuova policy ILM che includa una regola conforme come regola predefinita. Seleziona **OK**. Poi, crea una nuova policy, simulala e attivala. Consulta ["Creare un criterio ILM"](#) per le istruzioni.

Risolvi gli errori di coerenza durante l'aggiornamento delle impostazioni di S3 Object Lock o di Compliance legacy in StorageGRID

Se un sito del data center o più nodi di storage in un sito non sono più disponibili, potrebbe essere necessario aiutare gli utenti del tenant S3 ad applicare le modifiche alla configurazione S3 Object Lock o legacy Compliance.

Gli utenti tenant che hanno bucket con S3 Object Lock (o Compliance legacy) abilitato possono modificare alcune impostazioni. Ad esempio, un utente tenant che utilizza il blocco oggetti S3 potrebbe dover mettere una versione dell'oggetto sotto il blocco legale.

Quando un utente tenant aggiorna le impostazioni di un bucket S3 o di una versione a oggetti, StorageGRID tenta di aggiornare immediatamente il bucket o i metadati dell'oggetto nella griglia. Se il sistema non è in grado di aggiornare i metadati perché un sito del data center o più nodi di storage non sono disponibili, viene visualizzato un errore:

```
503: Service Unavailable
Unable to update compliance settings because the settings can't be
consistently applied on enough storage services. Contact your grid
administrator for assistance.
```

Per risolvere questo errore, attenersi alla seguente procedura:

1. Tentare di rendere nuovamente disponibili tutti i nodi o i siti di storage il prima possibile.
2. Se non si riesce a rendere disponibile una quantità sufficiente di nodi di storage in ogni sito, contattare il supporto tecnico, che può aiutare a ripristinare i nodi e garantire che le modifiche vengano applicate in modo coerente in tutta la griglia.
3. Una volta risolto il problema sottostante, ricordare all'utente tenant di ripetere le modifiche alla configurazione.

Informazioni correlate

- ["Utilizzare un account tenant"](#)
- ["UTILIZZARE L'API REST S3"](#)
- ["Ripristino e manutenzione"](#)

Esempio di regole e policy ILM

Regole e policy ILM per la protezione e la conservazione di base degli oggetti in StorageGRID

È possibile utilizzare le seguenti regole e policy di esempio come punto di partenza per la definizione di un criterio ILM in modo da soddisfare i requisiti di protezione e conservazione degli oggetti.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 1: Copia dei dati degli oggetti in due siti

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due siti.

Definizione della regola	Valore di esempio
Pool di storage one-site	Due pool di storage, ciascuno contenente diversi siti, denominati Sito 1 e Sito 2.
Nome della regola	Due copie di due siti
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 al giorno per sempre, conservare una copia replicata nel sito 1 e una copia replicata nel sito 2.

La sezione analisi delle regole del diagramma di conservazione riporta:

- La protezione contro la perdita di sito di StorageGRID verrà applicata per tutta la durata di questa regola.
- Gli oggetti elaborati da questa regola non verranno eliminati da ILM.

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 erasure coding con abbinamento bucket

Questa regola ILM di esempio utilizza un profilo di erasure coding e un bucket S3 per determinare dove e per quanto tempo l'oggetto viene memorizzato.

Definizione della regola	Valore di esempio
Pool di storage con più siti	• Un pool di storage in tre siti (siti 1, 2, 3) • Utilizzare uno schema di erasure coding 6+3
Nome della regola	Record finanziari di S3 Bucket
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Per gli oggetti nel bucket S3 denominato Finance-records, creare una copia con erasure coding nel pool specificato dal profilo di erasure coding. Conserva questa copia per sempre.

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 ad esempio 1

In pratica, la maggior parte delle policy ILM è semplice, anche se il sistema StorageGRID consente di progettare policy ILM sofisticate e complesse.

Un tipico criterio ILM per un grid multi-sito potrebbe includere regole ILM come le seguenti:

- Al momento dell'acquisizione, è possibile memorizzare tutti gli oggetti appartenenti al bucket S3 citato `finance-records` in un pool storage contenente tre siti. Utilizzare la codifica di cancellazione 6+3.
- Se un oggetto non corrisponde alla prima regola ILM, utilizzare la regola ILM predefinita del criterio, due copie due data center, per memorizzare una copia di tale oggetto nel sito 1 e una copia nel sito 2.

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 i criteri ILM"](#)
- ["Creare policy ILM"](#)

Regole e policy ILM per il filtraggio delle dimensioni degli oggetti EC in StorageGRID

È possibile utilizzare le seguenti regole e policy di esempio come punti di partenza per definire un criterio ILM che filtra in base alle dimensioni dell'oggetto per soddisfare i requisiti EC consigliati.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 2: Utilizzare EC per oggetti superiori a 1 MB

In questo esempio, la cancellazione della regola ILM codifica gli oggetti superiori a 1 MB.



L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasures per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasures molto piccoli.

Definizione della regola	Valore di esempio
Nome della regola	Solo oggetti EC > 1 MB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB

Definizione della regola	Valore di esempio
Posizionamenti	Creare una copia 2+1 con codifica per la cancellazione utilizzando tre siti

Filter group 1
Objects with all of following metadata will be evaluated by this rule:

Object size
greater than
1
MB

ILM regola 2 per esempio 2: Due copie replicate

Questa regola ILM di esempio crea due copie replicate e non filtra in base alle dimensioni dell'oggetto. Questa regola è la regola predefinita per il criterio. Poiché la prima regola filtra tutti gli oggetti superiori a 1 MB, questa regola si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Nessuno
Posizionamenti	Dal giorno 0 al giorno per sempre, conservare una copia replicata nel sito 1 e una copia replicata nel sito 2.

Criterio ILM per esempio 2: Utilizzare EC per oggetti superiori a 1 MB

Questo esempio di policy ILM include due regole ILM:

- La prima regola di cancellazione codifica tutti gli oggetti superiori a 1 MB.
- La seconda regola ILM (predefinita) crea due copie replicate. Poiché gli oggetti superiori a 1 MB sono stati filtrati dalla regola 1, la regola 2 si applica solo agli oggetti di dimensioni pari o inferiori a 1 MB.

Regole e policy ILM per la protezione dei file immagine in StorageGRID

È possibile utilizzare le regole e i criteri di esempio seguenti per garantire che le immagini di dimensioni superiori a 1 MB siano sottoposte a erasure coding e che vengano create due copie di immagini di dimensioni inferiori.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

ILM regola 1 per esempio 3: Utilizzare EC per file di immagini superiori a 1 MB

Questa regola ILM di esempio utilizza il filtraggio avanzato per codificare tutti i file di immagine con dimensioni

superiori a 1 MB.



L'erasure coding è più adatto per oggetti superiori a 1 MB. Non utilizzare la codifica erasure per oggetti di dimensioni inferiori a 200 KB per evitare l'overhead di gestione di frammenti con codifica erasure molto piccoli.

Definizione della regola	Valore di esempio
Nome della regola	File immagine EC > 1 MB
Tempo di riferimento	Tempo di acquisizione
Filtro avanzato per la dimensione dell'oggetto	Dimensione dell'oggetto superiore a 1 MB
Filtri avanzati per Key	• Termina con .jpg • Termina con .png
Posizionamenti	Creare una copia 2+1 con codifica per la cancellazione 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 prima regola del criterio, l'istruzione di posizionamento della codifica di cancellazione si applica solo ai file .jpg e .png che sono superiori a 1 MB.

Regola ILM 2 per esempio 3: Creare 2 copie replicate per tutti i file di immagine rimanenti

Questa regola ILM di esempio utilizza un filtro avanzato per specificare che i file di immagine più piccoli devono essere replicati. Poiché la prima regola del criterio ha già trovato corrispondenza tra file di immagine superiori a 1 MB, questa regola si applica ai file di immagine di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Nome della regola	2 copie per i file immagine

656

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Filtri avanzati per Key	• Termina con .jpg • Termina con .png
Posizionamenti	Creare 2 copie replicate in due pool di storage

Policy ILM per esempio 3: Migliore protezione per i file di immagine

Questo esempio di policy ILM include tre regole:

- La prima regola di cancellazione codifica tutti i file di immagine superiori a 1 MB.
- La seconda regola consente di creare due copie dei file immagine rimanenti (ovvero, immagini di dimensioni pari o inferiori a 1 MB).
- La regola predefinita si applica a tutti gli oggetti rimanenti (ovvero a tutti i file non immagine).

Rule order	Rule name	Filters
1	  EC image files > 1 MB	Object size is greater than 1 MB
2	  2 copies for small images	Object size is less than or equal to 200 KB
Default	Default rule	—

Regole e policy ILM per le versioni non correnti degli oggetti S3 in StorageGRID

Se si dispone di un bucket S3 con versione abilitata, è possibile gestire le versioni non correnti degli oggetti includendo regole nel criterio ILM che utilizzano "tempo non corrente" come tempo di riferimento.



Se si specifica un tempo di conservazione limitato per gli oggetti, questi verranno eliminati in modo permanente una volta raggiunto il periodo di tempo. Assicurarsi di comprendere per quanto tempo gli oggetti verranno conservati.

Come illustrato in questo esempio, è possibile controllare la quantità di storage utilizzata dagli oggetti con versione utilizzando istruzioni di posizionamento diverse per le versioni degli oggetti non correnti.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.



Per eseguire la simulazione dei criteri ILM su una versione non corrente di un oggetto, è necessario conoscere l'UUID o il CBID della versione dell'oggetto. Per trovare UUID e CBID, utilizzare ["ricerca dei metadati degli oggetti"](#) mentre l'oggetto è ancora corrente.

ILM regola 1 per esempio 4: Salva tre copie per 10 anni

Questa regola ILM di esempio memorizza una copia di ciascun oggetto in tre siti per 10 anni.

Questa regola si applica a tutti gli oggetti, indipendentemente dal fatto che siano con versione.

Definizione della regola	Valore di esempio
Pool di storage	Tre pool di storage, ciascuno costituito da diversi data center, denominati Sito 1, Sito 2 e Sito 3.
Nome della regola	Tre copie dieci anni
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva tre copie replicate per 10 anni (3,652 giorni), una nel sito 1, una nel sito 2 e una nel sito 3. Alla fine dei 10 anni, eliminare tutte le copie dell'oggetto.

ILM regola 2 per esempio 4: Salva due copie di versioni non correnti per 2 anni

Questa regola ILM di esempio memorizza due copie delle versioni non correnti di un oggetto con versione S3 per 2 anni.

Poiché la regola ILM 1 si applica a tutte le versioni dell'oggetto, è necessario creare un'altra regola per filtrare le versioni non correnti.

Per creare una regola che utilizza "ora non corrente" come ora di riferimento, selezionare **Si** per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" Nel passaggio 1 (immettere i dettagli) della procedura guidata Crea una regola ILM. Quando si seleziona **Si**, viene automaticamente selezionata l'opzione *ora non corrente* per l'ora di riferimento e non è possibile selezionare un'ora di riferimento diversa.

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 memorizzate solo due copie delle versioni non correnti, che verranno memorizzate per due anni.

Definizione della regola	Valore di esempio
Pool di storage	Due pool di storage, ciascuno in diversi data center, sito 1 e sito 2.
Nome della regola	Versioni non correnti: Due copie per due anni
Tempo di riferimento	Ora non corrente Selezionato automaticamente quando si seleziona Sì per la domanda "Applica questa regola solo alle versioni di oggetti precedenti (nei bucket S3 con versione abilitata)?" Nella procedura guidata Crea una regola ILM.
Posizionamenti	Il giorno 0 relativo all'ora non corrente (ovvero, a partire dal giorno in cui la versione dell'oggetto diventa la versione non corrente), mantenere due copie replicate delle versioni dell'oggetto non correnti per 2 anni (730 giorni), una nel sito 1 e una nel sito 2. Alla fine di 2 anni, eliminare le versioni non aggiornate.

Policy ILM per esempio 4: Oggetti con versione S3

Se si desidera gestire le versioni precedenti di un oggetto in modo diverso dalla versione corrente, le regole che utilizzano l'ora non corrente come ora di riferimento devono essere visualizzate nel criterio ILM prima delle regole applicabili alla versione corrente dell'oggetto.

Un criterio ILM per gli oggetti con versione S3 potrebbe includere regole ILM come le seguenti:

- Mantenere le versioni precedenti (non aggiornate) di ciascun oggetto per 2 anni, a partire dal giorno in cui la versione è diventata non aggiornata.



Le regole "tempo non corrente" devono essere visualizzate nel criterio prima delle regole che si applicano alla versione dell'oggetto corrente. In caso contrario, le versioni degli oggetti non correnti non verranno mai abbinate alla regola "tempo non corrente".

- Al momento dell'acquisizione, creare tre copie replicate e memorizzare una copia in ciascuno dei tre siti. Conserva le copie della versione corrente dell'oggetto per 10 anni.

Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Qualsiasi versione dell'oggetto non corrente verrebbe associata dalla prima regola. Se una versione dell'oggetto non corrente ha più di 2 anni, viene eliminata in modo permanente da ILM (tutte le copie della versione non corrente vengono rimosse dalla griglia).
- La seconda regola corrisponde alla versione corrente dell'oggetto. Quando la versione corrente dell'oggetto è stata archiviata per 10 anni, il processo ILM aggiunge un marcatore di eliminazione come versione corrente dell'oggetto e rende la versione precedente "non corrente". La prossima volta che si verifica la valutazione ILM, questa versione non corrente corrisponde alla prima regola. Di conseguenza, la copia del sito 3 viene eliminata e le due copie del sito 1 e del sito 2 vengono memorizzate per altri 2 anni.

Informazioni correlate

["Modalità di eliminazione degli oggetti"](#)

Regole e policy ILM per il comportamento di acquisizione rigoroso in StorageGRID

È possibile utilizzare un filtro di posizione e il rigoroso comportamento di acquisizione in una regola per impedire che gli oggetti vengano salvati in una determinata posizione del data center.

In questo esempio, un tenant con sede a Parigi non desidera memorizzare alcuni oggetti al di fuori dell'UE a causa di problemi normativi. Altri oggetti, inclusi tutti gli oggetti di altri account tenant, possono essere memorizzati nel data center di Parigi o nel data center statunitense.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

- ["Opzioni di acquisizione"](#)
- ["Create ILM rule \(Crea regola ILM\): Selezionare il comportamento di acquisizione"](#)

ILM regola 1 per esempio 5: Ingest rigoroso per garantire il data center di Parigi

Questa regola ILM di esempio utilizza il comportamento rigoroso dell'acquisizione per garantire che gli oggetti salvati da un tenant basato su Parigi nei bucket S3 con la regione impostata su ue-West-3 (Parigi) non vengano mai memorizzati nel data center statunitense.

Questa regola si applica agli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi).

Definizione della regola	Valore di esempio
Account tenant	Tenant di Parigi
Filtro avanzato	Il vincolo di posizione equivale a eu-West-3
Pool di storage	Sito 1 (Parigi)
Nome della regola	Un ingest rigoroso per garantire il data center di Parigi
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre nel sito 1 (Parigi)
Comportamento di acquisizione	Rigoroso. Utilizza sempre le posizioni di questa regola per l'acquisizione. L'acquisizione non riesce se non è possibile memorizzare due copie dell'oggetto nel data center di Parigi.

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

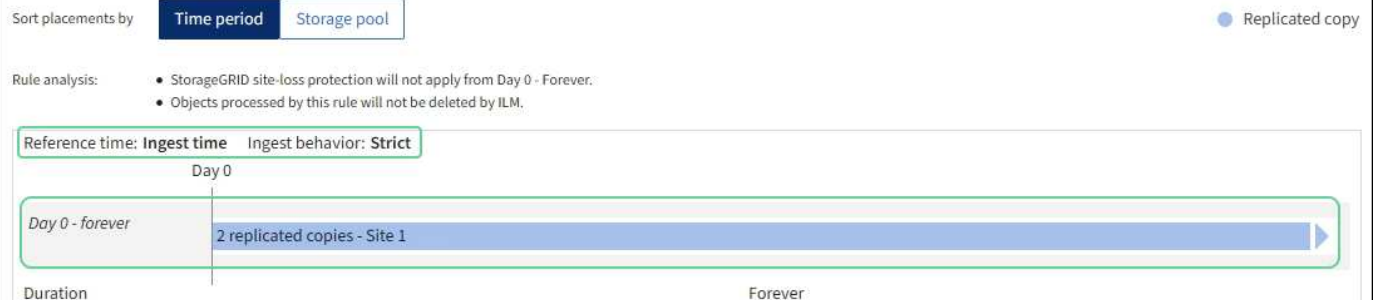
Clone Edit Remove

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



ILM regola 2 per esempio 5: Acquisizione bilanciata per altri oggetti

Questa regola ILM di esempio utilizza il comportamento di acquisizione bilanciata per fornire un'efficienza ILM ottimale per qualsiasi oggetto non associato alla prima regola. Verranno memorizzate due copie di tutti gli oggetti corrispondenti a questa regola: Una nel data center degli Stati Uniti e una nel data center di Parigi. Se la regola non può essere soddisfatta immediatamente, le copie temporanee vengono memorizzate in qualsiasi posizione disponibile.

Questa regola si applica agli oggetti che appartengono a qualsiasi tenant e a qualsiasi area.

Definizione della regola	Valore di esempio
Account tenant	Ignorare
Filtro avanzato	Non specificato
Pool di storage	Sito 1 (Parigi) e sito 2 (Stati Uniti)
Nome della regola	2 copie di 2 data center
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Il giorno 0, conserva due copie replicate per sempre in due data center

Definizione della regola	Valore di esempio
Comportamento di acquisizione	Bilanciato. Gli oggetti che corrispondono a questa regola vengono posizionati in base alle istruzioni di posizionamento della regola, se possibile. In caso contrario, le copie temporanee vengono eseguite in qualsiasi ubicazione disponibile.

Policy ILM per esempio 5: Combinazione di comportamenti di acquisizione

Il criterio ILM di esempio include due regole che hanno comportamenti di acquisizione diversi.

Un criterio ILM che utilizza due diversi comportamenti di acquisizione potrebbe includere regole ILM come le seguenti:

- Memorizzare gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 (Parigi) solo nel data center di Parigi. Non eseguire l'acquisizione se il data center di Parigi non è disponibile.
- Memorizzare tutti gli altri oggetti (inclusi quelli che appartengono al tenant di Parigi ma che hanno una regione bucket diversa) nel data center statunitense e nel data center di Parigi. Se le istruzioni di posizionamento non possono essere soddisfatte, eseguire copie temporanee in qualsiasi ubicazione disponibile.

Quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- Tutti gli oggetti che appartengono al tenant di Parigi e che hanno la regione del bucket S3 impostata su eu-West-3 vengono abbinati alla prima regola e memorizzati nel data center di Parigi. Poiché la prima regola utilizza un ingest rigoroso, questi oggetti non vengono mai memorizzati nel data center statunitense. Se i nodi di storage nel data center di Parigi non sono disponibili, l'acquisizione non riesce.
- Tutti gli altri oggetti sono abbinati dalla seconda regola, inclusi gli oggetti che appartengono al tenant di Parigi e che non hanno la regione del bucket S3 impostata su eu-West-3. Una copia di ciascun oggetto viene salvata in ciascun data center. Tuttavia, poiché la seconda regola utilizza l'acquisizione bilanciata, se un data center non è disponibile, vengono salvate due copie temporanee in qualsiasi posizione disponibile.

Come la modifica di una policy ILM influisce sulle prestazioni di StorageGRID

Se è necessario modificare la protezione dei dati o aggiungere nuovi siti, è possibile creare e attivare una nuova policy ILM.

Prima di modificare una policy, è necessario comprendere in che modo le modifiche apportate ai posizionamenti ILM possono influire temporaneamente sulle prestazioni generali di un sistema StorageGRID.

In questo esempio, è stato aggiunto un nuovo sito StorageGRID in un'espansione e occorre implementare una nuova policy ILM attiva per memorizzare i dati nel nuovo sito. Per implementare un nuovo criterio attivo, prima **"creare un criterio"**. Successivamente, è necessario **"simulare"** e quindi **"attivare"** la nuova policy.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

In che modo la modifica di un criterio ILM influisce sulle performance

Quando si attiva un nuovo criterio ILM, le prestazioni del sistema StorageGRID potrebbero risentirne

temporaneamente, soprattutto se le istruzioni di posizionamento nel nuovo criterio richiedono lo spostamento di molti oggetti esistenti in nuove posizioni.

Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Per garantire che un nuovo criterio ILM non influisca sul posizionamento degli oggetti replicati e con erasure coding esistenti, è possibile "Creare una regola ILM con un filtro per l'ora di acquisizione". Ad esempio, **Ingest Time è attivo o successivo a <date and time>**, in modo che la nuova regola si applichi solo agli oggetti acquisiti in data e ora specificate o successive.

I tipi di modifiche ai criteri ILM che possono influire temporaneamente sulle prestazioni di StorageGRID includono:

- Applicazione di un profilo di erasure coding diverso agli oggetti esistenti sottoposti a erasure coding.



StorageGRID considera ogni profilo di erasure coding come univoco e non riutilizza i frammenti di erasure coding quando viene utilizzato un nuovo profilo.

- Modifica del tipo di copie richieste per gli oggetti esistenti; ad esempio, conversione di una grande percentuale di oggetti replicati in oggetti con codifica per la cancellazione.
- Spostamento di copie di oggetti esistenti in una posizione completamente diversa; ad esempio, spostamento di un numero elevato di oggetti da o verso un Cloud Storage Pool o da o verso un sito remoto.

Policy ILM attiva ad esempio 6: Protezione dei dati in due siti

In questo esempio, la policy ILM attiva è stata inizialmente progettata per un sistema StorageGRID a due siti e utilizza due regole ILM.

Active policyPolicy 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 rulesRetention 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 da una codifica di cancellazione 2+1 in un singolo sito, mentre gli oggetti appartenenti a tutti gli altri tenant sono protetti in due siti utilizzando la replica

a 2 copie.

Regola 1: Erasure coding per un sito per il tenant A.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione one-site per il tenant A.
Account tenant	Tenant A.
Pool di storage	Sito 1
Posizionamenti	2+1 erasure coding in Site 1 dal giorno 0 a per sempre

Regola 2: Replica a due siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a due siti per altri tenant
Account tenant	Ignorare
Pool di storage	Sito 1 e sito 2
Posizionamenti	Due copie replicate dal giorno 0 a sempre: Una copia nel sito 1 e una nel sito 2.

Criterio ILM per esempio 6: Protezione dei dati in tre siti

In questo esempio, la policy ILM viene sostituita con una nuova policy per un sistema StorageGRID a tre siti.

Dopo aver eseguito un'espansione per aggiungere il nuovo sito, l'amministratore della griglia ha creato due nuovi pool di storage: Un pool di storage per il sito 3 e un pool di storage contenente tutti e tre i siti (non lo stesso del pool di storage predefinito di tutti i nodi di storage). Quindi, l'amministratore ha creato due nuove regole ILM e un nuovo criterio ILM, progettato per proteggere i dati in tutti e tre i siti.

Quando viene attivata questa nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti da una cancellazione 2+1 in tre siti, mentre gli oggetti appartenenti ad altri tenant (e gli oggetti più piccoli appartenenti al tenant A) saranno protetti in tre siti utilizzando la replica a 3 copie.

Regola 1: Erasure coding a tre siti per il tenant A.

Definizione della regola	Valore di esempio
Nome della regola	Codifica di cancellazione a tre siti per il tenant A.
Account tenant	Tenant A.
Pool di storage	Tutti e 3 i siti (inclusi Sito 1, Sito 2 e Sito 3)

Definizione della regola	Valore di esempio
Posizionamenti	2+1 erasure coding in tutti e 3 i siti dal giorno 0 a per sempre

Regola 2: Replica a tre siti per altri tenant

Definizione della regola	Valore di esempio
Nome della regola	Replica a tre siti per altri tenant
Account tenant	Ignorare
Pool di storage	Sito 1, sito 2 e sito 3
Posizionamenti	Tre copie replicate dal giorno 0 a sempre: Una copia presso il sito 1, una copia presso il sito 2 e una copia presso il sito 3.

Attivazione del criterio ILM ad esempio 6

Quando si attiva un nuovo criterio ILM, è possibile spostare gli oggetti esistenti in nuove posizioni o creare nuove copie degli oggetti per gli oggetti esistenti, in base alle istruzioni di posizionamento nelle regole nuove o aggiornate.



Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.



Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

Cosa succede quando cambiano le istruzioni di erasure coding

Nel criterio ILM attualmente attivo, per questo esempio, gli oggetti appartenenti al tenant A sono protetti utilizzando la codifica di cancellazione 2+1 nel sito 1. Nella nuova policy ILM, gli oggetti appartenenti al tenant A saranno protetti mediante erasure coding 2+1 nei siti 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- I nuovi oggetti acquisiti dal tenant A vengono suddivisi in due frammenti di dati e viene aggiunto un frammento di parità. Quindi, ciascuno dei tre frammenti viene memorizzato in un sito diverso.
- Gli oggetti esistenti appartenenti al tenant A vengono rivalutati durante il processo di scansione ILM in corso. Poiché le istruzioni di posizionamento dell'ILM utilizzano un nuovo profilo di erasure coding, vengono creati e distribuiti ai tre siti frammenti completamente nuovi e codificati tramite erasure coding.



I frammenti 2+1 esistenti nel sito 1 non vengono riutilizzati. StorageGRID considera ogni profilo di erasure coding come univoco e non riutilizza i frammenti di erasure coding quando viene utilizzato un nuovo profilo.

Cosa succede quando cambiano le istruzioni di replica

Nella policy ILM attualmente attiva per questo esempio, gli oggetti appartenenti ad altri tenant sono protetti utilizzando due copie replicate nei pool di storage dei siti 1 e 2. Nella nuova policy ILM, gli oggetti appartenenti ad altri tenant verranno protetti attraverso tre copie replicate nei pool di storage dei siti 1, 2 e 3.

Quando viene attivato il nuovo criterio ILM, si verificano le seguenti operazioni ILM:

- Quando un tenant diverso dal tenant A acquisisce un nuovo oggetto, StorageGRID crea tre copie e salva una copia in ogni sito.
- Gli oggetti esistenti appartenenti a questi altri tenant vengono rivalutati durante il processo di scansione ILM in corso. Poiché le copie degli oggetti esistenti nei siti 1 e 2 continuano a soddisfare i requisiti di replica della nuova regola ILM, StorageGRID deve creare solo una nuova copia dell'oggetto per il sito 3.

Impatto delle performance dell'attivazione di questa policy

Quando il criterio ILM in questo esempio è attivato, le prestazioni generali del sistema StorageGRID saranno temporaneamente influenzate. Per creare nuovi frammenti erasure-coded per gli oggetti esistenti del tenant A e nuove copie replicate nel sito 3 per gli oggetti esistenti degli altri tenant saranno necessari livelli di risorse grid superiori al normale.

Come conseguenza della modifica del criterio ILM, le richieste di lettura e scrittura del client potrebbero temporaneamente riscontrare latenze superiori al normale. Le latenze torneranno ai livelli normali dopo che le istruzioni di posizionamento sono state completamente implementate nella griglia.

Per evitare problemi di risorse quando si attiva un nuovo criterio ILM, è possibile utilizzare il filtro avanzato Ingest Time in qualsiasi regola che potrebbe modificare la posizione di un gran numero di oggetti esistenti. Impostare Ingest Time (tempo di acquisizione) su un valore maggiore o uguale al tempo approssimativo in cui la nuova policy verrà applicata per garantire che gli oggetti esistenti non vengano spostati inutilmente.



Contattare il supporto tecnico se è necessario rallentare o aumentare la velocità di elaborazione degli oggetti dopo una modifica della policy ILM.

Criterio ILM conforme per S3 Object Lock in StorageGRID

È possibile utilizzare il bucket S3, le regole ILM e il criterio ILM in questo esempio come punto di partenza quando si definisce un criterio ILM per soddisfare i requisiti di protezione e conservazione degli oggetti nei bucket con blocco oggetti S3 attivato.



Se hai utilizzato la funzionalità di conformità legacy nelle versioni precedenti di StorageGRID, puoi anche utilizzare questo esempio per gestire qualsiasi bucket esistente con la funzionalità di conformità legacy attivata.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita.

Informazioni correlate

- ["Gestire gli oggetti con S3 Object Lock"](#)
- ["Creare un criterio ILM"](#)

Esempio di bucket e oggetti per S3 Object Lock

In questo esempio, un account tenant S3 denominato Bank of ABC ha utilizzato il tenant Manager per creare un bucket con blocco oggetti S3 abilitato per memorizzare i record bancari critici.

Definizione del bucket	Valore di esempio
Nome account tenant	Banca di ABC
Nome bucket	banca-record
Area bucket	us-east-1 (impostazione predefinita)

Ogni versione oggetto e oggetto aggiunta al bucket di record bancari utilizzerà i seguenti valori per le `retain-until-date` impostazioni e `legal hold`.

Impostazione per ciascun oggetto	Valore di esempio
<code>retain-until-date</code>	"2030-12-30T23:59:59Z" (30 dicembre 2030) Ogni versione oggetto ha una propria <code>retain-until-date</code> impostazione. Questa impostazione può essere aumentata, ma non ridotta.
<code>legal hold</code>	"OFF" (non in vigore) È possibile mettere o revocare un blocco legale su qualsiasi versione oggetto in qualsiasi momento durante il periodo di conservazione. Se un oggetto è bloccato a fini giudiziari, l'oggetto non può essere eliminato anche se <code>retain-until-date</code> è stato raggiunto.

Regola ILM 1 per blocco oggetto S3 esempio: Profilo di erasure coding con abbinamento bucket

Questa regola ILM di esempio si applica solo all'account tenant S3 denominato Bank of ABC. Si abbina a qualsiasi oggetto nel `bank-records` bucket e quindi utilizza l'erasure coding per memorizzare l'oggetto sui nodi storage in tre siti di data center utilizzando un profilo di erasure coding 6+3. Questa regola soddisfa i requisiti dei bucket con blocco oggetti S3 attivato: Una copia viene conservata nei nodi di storage dal giorno 0 a per sempre, utilizzando l'ora di inizio come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Compliant Rule (regola conforme): Oggetti EC nel bucket dei record bancari - Bank of ABC

Definizione della regola	Valore di esempio
Account tenant	Banca di ABC
Nome bucket	bank-records
Filtro avanzato	Dimensione oggetto (MB) maggiore di 1 Nota: questo filtro garantisce che la codifica erasure non venga utilizzata per oggetti di dimensioni pari o inferiori a 1 MB.

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 memorizzare per sempre
Profilo di erasure coding	• Creare una copia con codifica di cancellazione sui nodi di storage in tre siti del data center • Utilizza uno schema di erasure coding 6+3

ILM regola 2 per S3 Object Lock esempio: Regola non conforme

Questa regola ILM di esempio memorizza inizialmente due copie di oggetti replicate sui nodi di storage. Dopo un anno, memorizza una copia su un Cloud Storage Pool per sempre. Poiché questa regola utilizza un Cloud Storage Pool, non è conforme e non si applica agli oggetti nei bucket con S3 Object Lock attivato.

Definizione della regola	Valore di esempio
Nome della regola	Regola non conforme: Utilizza il Cloud Storage Pool
Account tenant	Non specificato
Nome bucket	Non specificato, ma si applica solo ai bucket che non hanno S3 Object Lock (o la funzionalità Compliance legacy) abilitato.
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	• Il giorno 0, conserva due copie replicate sui nodi di storage nel data center 1 e nel data center 2 per 365 giorni • Dopo 1 anno, conserva per sempre una copia replicata in un Cloud Storage Pool

ILM regola 3 per S3 Object Lock esempio: Regola predefinita

Questa regola ILM di esempio copia i dati degli oggetti in pool di storage in due data center. Questa regola di conformità è stata progettata per essere la regola predefinita nel criterio ILM. Non include alcun filtro, non utilizza il tempo di riferimento non corrente e soddisfa i requisiti dei bucket con S3 Object Lock abilitato: Due copie di oggetti vengono conservate sui nodi di storage dal giorno 0 a per sempre, utilizzando Ingest come tempo di riferimento.

Definizione della regola	Valore di esempio
Nome della regola	Regola di conformità predefinita: Due copie di due data center
Account tenant	Non specificato
Nome bucket	Non specificato
Filtro avanzato	Non specificato

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Posizionamenti	Dal giorno 0 all'anno, conserva due copie replicate, una sui nodi di storage nel data center 1 e una sui nodi di storage nel data center 2.

Esempio di policy ILM conforme per S3 Object Lock

Per creare un criterio ILM che protegga efficacemente tutti gli oggetti del sistema, inclusi quelli nei bucket con S3 Object Lock attivato, è necessario selezionare le regole ILM che soddisfano i requisiti di storage per tutti gli oggetti. Quindi, è necessario simulare e attivare il criterio.

Aggiungere regole al criterio

In questo esempio, il criterio ILM include tre regole ILM, nel seguente ordine:

1. Regola conforme che utilizza la codifica erasure per proteggere oggetti superiori a 1 MB in un bucket specifico con blocco oggetti S3 attivato. Gli oggetti vengono memorizzati nei nodi di storage dal giorno 0 a sempre.
2. Una regola non conforme che crea due copie di oggetti replicate sui nodi di storage per un anno e sposta una copia di oggetto in un pool di storage cloud per sempre. Questa regola non si applica ai bucket con blocco oggetti S3 attivato perché utilizza un pool di storage cloud.
3. La regola di conformità predefinita che crea due copie di oggetti replicate sui nodi di storage dal giorno 0 a per sempre.

Simulare la policy

Dopo aver aggiunto regole al criterio, scelto una regola conforme predefinita e organizzato le altre regole, è necessario simulare il criterio testando gli oggetti dal bucket con blocco oggetti S3 attivato e da altri bucket. Ad esempio, quando si simula il criterio di esempio, si prevede che gli oggetti di test vengano valutati come segue:

- La prima regola corrisponde solo agli oggetti di test che sono superiori a 1 MB nei record di banco bucket per il tenant Bank of ABC.
- La seconda regola corrisponde a tutti gli oggetti in tutti i bucket non conformi per tutti gli altri account tenant.
- La regola predefinita corrisponde ai seguenti oggetti:
 - Oggetti di 1 MB o inferiori nei bucket bank-record per il tenant Bank of ABC.
 - Oggetti in qualsiasi altro bucket con S3 Object Lock attivato per tutti gli altri account tenant.

Attivare il criterio

Quando si è completamente soddisfatti del fatto che il nuovo criterio protegga i dati degli oggetti come previsto, è possibile attivarlo.

Come il ciclo di vita del bucket S3 e la policy ILM interagiscono in StorageGRID

A seconda della configurazione del ciclo di vita, gli oggetti seguono le impostazioni di conservazione del ciclo di vita del bucket S3 o di un criterio ILM.

Esempio di priorità del ciclo di vita dei bucket rispetto alla policy ILM

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"Days": 100},
"NoncurrentVersionExpiration": {"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 marker di eliminazione e "documenti/testo" diventa non corrente.
 - Dopo 5 giorni, un totale di 105 giorni dall'acquisizione, "documenti/testo" viene eliminato.
 - Dopo 95 giorni, per un totale di 200 giorni dall'acquisizione e 100 giorni dalla creazione del marker di eliminazione, il marker di eliminazione scaduto viene eliminato.
- Viene acquisito un oggetto denominato "video/filmato". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
 - Dopo 50 giorni viene creato un marker di eliminazione e "video/filmato" diventa non corrente.
 - Dopo 20 giorni, un totale di 70 giorni dall'acquisizione, "video/film" viene eliminato.
 - Dopo 30 giorni, per un totale di 100 giorni dall'acquisizione e 50 giorni dalla creazione del marker di eliminazione, il marker di eliminazione scaduto viene eliminato.

Esempio di ciclo di vita del bucket che mantiene implicitamente per sempre

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni

- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le X copie per 50 giorni

Ciclo di vita della benna

```
"Filter": {"Prefix": "docs/"}, "Expiration": {"ExpiredObjectDeleteMarker": true}
```

Risultato

- Viene acquisito un oggetto denominato "docs/text". Corrisponde al filtro del ciclo di vita del bucket del prefisso "docs/".

L'`Expiration`azione si applica solo ai marcatori di cancellazione scaduti, il che implica mantenere tutto il resto per sempre (a partire da "docs/").

I marcatori di eliminazione che iniziano con "docs/" vengono rimossi quando diventano scaduti.

- Viene acquisito un oggetto denominato "video/filmato". Non corrisponde al filtro e utilizza il criterio di conservazione ILM.
 - Dopo 50 giorni viene creato un marker di eliminazione e "video/filmato" diventa non corrente.
 - Dopo 20 giorni, un totale di 70 giorni dall'acquisizione, "video/film" viene eliminato.
 - Dopo 30 giorni, per un totale di 100 giorni dall'acquisizione e 50 giorni dalla creazione del marker di eliminazione, il marker di eliminazione scaduto viene eliminato.

Esempio di utilizzo del ciclo di vita bucket per duplicare ILM e ripulire i marcatori di eliminazione scaduti

Policy ILM

- Regola basata sul riferimento non corrente: Il giorno 0, tenere X copie per 20 giorni
- Regola basata sul riferimento al tempo di acquisizione (impostazione predefinita): Il giorno 0, conservare le copie X per sempre

Ciclo di vita della benna

```
"Filter": {}, "Expiration": {"ExpiredObjectDeleteMarker": true},  
"NoncurrentVersionExpiration": {"NoncurrentDays": 20}
```

Risultato

- Il criterio ILM viene duplicato nel ciclo di vita del bucket.
 - La regola per sempre della policy ILM è progettata per la rimozione manuale degli oggetti e la pulizia delle versioni non correnti dopo 20 giorni. Di conseguenza, la regola del tempo di acquisizione manterrà sempre i marcatori di eliminazione scaduti.
 - Il ciclo di vita del bucket duplica il comportamento del criterio ILM durante l'aggiunta di "ExpiredObjectDeleteMarker": true, che rimuove i marcatori di eliminazione una volta scaduti
- Un oggetto viene acquisito. Nessun filtro significa che il ciclo di vita del bucket si applica a tutti gli oggetti e sovrascrive le impostazioni di conservazione ILM.
 - 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 marker di eliminazione viene scaduto.
 - Poco dopo, il marker di eliminazione scaduto viene eliminato.

Hardening del sistema per StorageGRID

Scopri il rafforzamento del sistema per StorageGRID

La protezione avanzata del sistema è il processo che consente di eliminare il maggior numero possibile di rischi per la sicurezza da un sistema StorageGRID.

Durante l'installazione e la configurazione di StorageGRID, è possibile utilizzare queste linee guida per raggiungere gli obiettivi di protezione 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. Tali best practice devono includere la sicurezza fisica e ambientale che limiti l'accesso fisico e protegga il data center fisico e l'infrastruttura di supporto. È inoltre necessario fare riferimento a tutti gli standard normativi e alle raccomandazioni applicabili alla propria attività e area geografica.

StorageGRID segue la ["Policy di gestione delle vulnerabilità di NetApp"](#). Le vulnerabilità segnalate vengono verificate e risolte in base al processo di risposta agli incidenti di sicurezza del prodotto.

Per la protezione avanzata di un sistema StorageGRID, tenere presente quanto segue:

- **Quale delle tre reti StorageGRID** è stata implementata. Tutti i sistemi StorageGRID devono utilizzare la rete griglia, ma è possibile utilizzare anche la rete di amministrazione, la rete client o entrambi. Ogni rete ha considerazioni di sicurezza diverse.
- **Il tipo di piattaforme** utilizzato per i singoli nodi nel sistema StorageGRID. I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma dispone di un proprio set di Best practice per la protezione avanzata.
- **Quanto sono attendibili gli account tenant.** Se sei un provider di servizi con account tenant non attendibili, avrai problemi di sicurezza diversi rispetto all'utilizzo di tenant interni affidabili.
- **Quali sono i requisiti e le convenzioni di protezione** che la vostra organizzazione segue. Potrebbe essere necessario rispettare requisiti normativi o aziendali specifici.

Linee guida per il rafforzamento della sicurezza per gli aggiornamenti software StorageGRID

Per difenderti dagli attacchi, devi tenere aggiornato il tuo sistema StorageGRID e i servizi correlati.

Aggiornamenti al software StorageGRID

Se possibile, è necessario aggiornare il software StorageGRID alla versione principale più recente o alla versione principale precedente. Mantenere aggiornato StorageGRID aiuta a ridurre il tempo di attivazione delle vulnerabilità note e l'area complessiva della superficie di attacco. Inoltre, le versioni più recenti di StorageGRID contengono spesso funzionalità di protezione avanzata che non sono incluse nelle versioni precedenti.

Consultare ["Tool di matrice di interoperabilità NetApp"](#) (IMT) per determinare quale versione del software StorageGRID si deve utilizzare. Quando è necessaria una correzione rapida, NetApp assegna la priorità alla creazione di aggiornamenti per le release più recenti. Alcune patch potrebbero non essere compatibili con le release precedenti.

- Per scaricare le versioni più recenti di StorageGRID e le correzioni rapide, visitare il sito Web all'indirizzo ["Download NetApp: StorageGRID"](#).
- Per aggiornare il software StorageGRID, vedere ["Istruzioni per l'aggiornamento"](#).
- Per applicare una correzione rapida, vedere la ["Procedura di hotfix StorageGRID"](#).

Aggiornamenti a servizi esterni

I servizi esterni possono presentare vulnerabilità che influiscono indirettamente StorageGRID. 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 ["Tool di matrice di interoperabilità NetApp"](#).

Aggiornamenti agli hypervisor

Se i nodi StorageGRID sono in esecuzione su VMware o su un altro hypervisor, è necessario assicurarsi che il software e il firmware dell'hypervisor siano aggiornati.

Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp"](#).

Upgrade ai nodi Linux

Se i nodi StorageGRID utilizzano piattaforme host Linux, è necessario assicurarsi che gli aggiornamenti di sicurezza e del kernel siano applicati al sistema operativo host. Inoltre, è necessario applicare gli aggiornamenti del firmware all'hardware vulnerabile quando questi aggiornamenti diventano disponibili.

Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp"](#).

Linee guida per la protezione avanzata delle reti StorageGRID

Il sistema StorageGRID supporta fino a tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per informazioni dettagliate sulle reti StorageGRID, consultare ["Tipi di rete StorageGRID"](#).

Linee guida per Grid Network

È necessario configurare una rete griglia per tutto il traffico StorageGRID interno. Tutti i nodi Grid si trovano sulla rete Grid e devono essere in grado di comunicare con tutti gli altri nodi.

Durante la configurazione della rete Grid, attenersi alle seguenti linee guida:

- Assicurarsi che la rete sia protetta da client non attendibili, ad esempio quelli su Internet aperto.
- Se possibile, utilizzare Grid Network esclusivamente per il traffico interno. Sia la rete di amministrazione che la rete client presentano ulteriori restrizioni firewall che bloccano il traffico esterno verso i servizi interni. È supportato l'utilizzo di Grid Network per il traffico client esterno, ma questo tipo di utilizzo offre meno livelli di protezione.
- Se l'implementazione di StorageGRID si estende su più data center, utilizzare una rete privata virtuale (VPN) o equivalente sulla rete grid per fornire una protezione aggiuntiva per il traffico interno.
- Alcune procedure di manutenzione richiedono l'accesso Secure shell (SSH) sulla porta 22 tra il nodo di

amministrazione primario e tutti gli altri nodi della griglia. Utilizzare un firewall esterno per limitare l'accesso SSH ai client attendibili.

Linee guida per la rete amministrativa

La rete di amministrazione viene generalmente utilizzata per le attività amministrative (dipendenti attendibili che utilizzano Grid Manager o SSH) e per la comunicazione con altri servizi attendibili come LDAP, DNS, NTP o KMS (o server KMIP). Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete di amministrazione, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete di amministrazione. Consultare la ["elenco delle porte interne"](#).
- Se i client non attendibili possono accedere alla rete di amministrazione, bloccare l'accesso a StorageGRID sulla rete di amministrazione con un firewall esterno.

Linee guida per la rete client

La rete client viene generalmente utilizzata per i tenant e per le comunicazioni con servizi esterni, come il servizio di replica CloudMirror o un altro servizio della piattaforma. Tuttavia, StorageGRID non applica questo utilizzo internamente.

Se si utilizza la rete client, attenersi alle seguenti linee guida:

- Bloccare tutte le porte di traffico interne sulla rete client. Consultare la ["elenco delle porte interne"](#).
- Accettare il traffico client in entrata solo su endpoint configurati esplicitamente. Vedere le informazioni su ["gestione dei controlli firewall"](#).

Linee guida per la protezione avanzata dei nodi StorageGRID

I nodi StorageGRID possono essere implementati su macchine virtuali VMware, all'interno di un motore di container su host Linux o come appliance hardware dedicate. Ogni tipo di piattaforma e ogni tipo di nodo dispone di un proprio set di Best practice per la protezione avanzata.

Controlla l'accesso IPMI remoto a BMC

Puoi abilitare o disabilitare l'accesso IPMI remoto per tutti gli appliance che contengono un BMC. L'interfaccia IPMI remota consente l'accesso hardware di basso livello ai tuoi appliance StorageGRID a chiunque abbia un account BMC e una password. Se non ti serve l'accesso IPMI remoto al BMC, disattiva questa opzione.

- Per controllare l'accesso IPMI remoto al BMC in Grid Manager, vai su **Configuration > Security > Security settings > Appliances > Remote IPMI access**:
 - Deselezionare la casella di controllo **Abilita accesso IPMI remoto** per disattivare l'accesso IPMI al BMC.
 - Selezionare la casella di controllo **Abilita accesso IPMI remoto** per abilitare l'accesso IPMI al BMC.

Per ulteriori informazioni sull'indurimento BMC, vedere ["Controller di gestione del battiscopa Harden"](#) scheda informativa sulla sicurezza informatica dal ["Agenzia per la sicurezza nazionale \(NSA\)"](#) E ["Agenzia per la sicurezza informatica e delle infrastrutture \(CISA\)"](#).

Cambia la password BMC dell'appliance

Puoi cambiare la password BMC di un'appliance per limitare l'accesso e migliorare la sicurezza del sistema.

1. In Grid Manager vai su **Nodi > nodo griglia > Impostazioni BMC**.
2. Nella sezione Cambia password, inserisci una nuova password BMC di lunghezza compresa tra 8 e 16 caratteri nel campo **Nuova password** e poi inseriscila nuovamente nel campo **Conferma nuova password**.
3. Selezionare **Salva**.

Puoi anche cambiare la password BMC usando l'API `PUT /bmc-configuration/root-password`.

Controlla l'accesso alle porte USB esterne sugli appliance

Puoi abilitare le porte USB sugli appliance per consentire al supporto tecnico l'accesso per la diagnostica e la risoluzione dei problemi. Se non ti serve l'accesso alle porte USB, disabilita le porte per sicurezza. Le porte USB sono abilitate per impostazione predefinita dopo l'installazione iniziale o un upgrade.

- In Grid Manager, vai su **Configurazione > Sicurezza > Impostazioni di sicurezza > Apparecchiature > Accesso alla porta USB** per abilitare o disabilitare le porte USB:
 - Seleziona la casella di controllo **Abilita porte USB** e salva per abilitare le porte.

Se la casella di controllo USB era stata precedentemente deselezionata e salvata, seleziona la casella di controllo **Abilita porte USB** e salva per abilitare di nuovo le porte USB.
 - Deseleziona la casella **Abilita porte USB** e salva per disabilitare le porte.

Configurazione del firewall

Nell'ambito del processo di protezione avanzata del sistema, è necessario rivedere le configurazioni dei firewall esterni e modificarle in modo che il traffico venga accettato solo dagli indirizzi IP e dalle porte da cui è strettamente necessario.

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della rete consentendo di controllare l'accesso alla rete. È necessario ["gestire i controlli firewall interni"](#) impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per la distribuzione specifica della griglia. Le modifiche apportate alla configurazione nella pagina di controllo Firewall vengono distribuite a ciascun nodo.

In particolare, è possibile gestire queste aree:

- **Privileged addresses** (indirizzi con privilegi): È possibile consentire agli indirizzi IP o alle subnet selezionate di accedere alle porte chiuse dalle impostazioni nella scheda Manage external access (Gestisci accesso esterno).
- **Manage external access** (Gestisci accesso esterno): È possibile chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network**: È possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client e le porte aggiuntive che si desidera aprire quando è configurata una rete client non attendibile.

Sebbene questo firewall interno offra un ulteriore livello di protezione contro alcune minacce comuni, non elimina la necessità di un firewall esterno.

Per un elenco di tutte le porte interne ed esterne utilizzate da StorageGRID, vedere ["Porte interne"](#)

Disattivare i servizi inutilizzati

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 del software non attendibile. Non presupporre che le protezioni dell'hypervisor impediscano al malware di accedere ai dati protetti da StorageGRID se StorageGRID e il malware esistono sullo stesso hardware fisico. Ad esempio, gli attacchi Meltdown e Spectre sfruttano le vulnerabilità critiche dei processori moderni e consentono ai programmi di rubare dati in memoria sullo stesso computer.

Proteggere i nodi durante l'installazione

Non consentire agli utenti non attendibili di accedere ai nodi StorageGRID sulla rete durante l'installazione dei nodi. I nodi non sono completamente sicuri fino a quando non si sono Uniti alla griglia.

Limitare l'accesso fisico all'hardware

È necessario limitare l'accesso fisico ai nodi dell'appliance hardware StorageGRID , nonché agli host delle macchine virtuali VMware e agli host Linux che eseguono StorageGRID , solo agli amministratori autorizzati. Alcuni esempi di controlli di accesso fisico includono serrature, guardie, barriere fisiche e videosorveglianza.

I nodi degli appliance hardware sono progettati per essere installati e utilizzati solo da amministratori autorizzati. Non consentire agli amministratori non autorizzati di accedere ai nodi degli apparecchi hardware.

Linee guida per i nodi di amministrazione

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore.

Seguire queste linee guida per proteggere i nodi di amministrazione nel sistema StorageGRID:

- Proteggere tutti i nodi di amministrazione da client non attendibili, ad esempio quelli su Internet aperto. Assicurarsi che nessun client non attendibile possa accedere a qualsiasi nodo Admin sulla rete Grid, sulla rete amministrativa o sulla rete client.
- I gruppi StorageGRID controllano l'accesso alle funzioni di gestione griglia e di gestione tenant. Concedere a ciascun gruppo di utenti le autorizzazioni minime richieste per il proprio ruolo e utilizzare la modalità di accesso in sola lettura per impedire agli utenti di modificare la configurazione.
- Quando si utilizzano gli endpoint del bilanciamento del carico StorageGRID, utilizzare i nodi gateway invece dei nodi di amministrazione per il traffico client non attendibile.
- Se si dispone di tenant non attendibili, non consentire loro di accedere direttamente al tenant Manager o all'API di gestione tenant. I tenant non attendibili devono invece utilizzare un portale tenant o un sistema di gestione tenant esterno, che interagisce con l'API di gestione tenant.
- In alternativa, utilizzare un proxy amministratore per un maggiore controllo sulle comunicazioni AutoSupport dai nodi amministrativi al supporto NetApp. Vedere la procedura per ["creazione di un proxy amministratore"](#).

- Facoltativamente, utilizzare le porte limitate 8443 e 9443 per separare le comunicazioni di Grid Manager e Tenant Manager. Bloccare la porta condivisa 443 e limitare le richieste del tenant alla porta 9443 per una protezione aggiuntiva.
- Facoltativamente, utilizzare nodi di amministrazione separati per gli amministratori di grid e gli utenti del tenant.

Per ulteriori informazioni, vedere le istruzioni di ["Amministrazione di StorageGRID"](#).

Linee guida per i nodi di storage

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Seguire queste linee guida per proteggere i nodi di storage nel sistema StorageGRID.

- Non consentire ai client non attendibili di connettersi direttamente ai Storage Node. Usa un endpoint di bilanciamento del carico fornito da un Gateway Node o da un bilanciatore del carico di terze parti.
- Non abilitare i servizi in uscita per tenant non attendibili. Ad esempio, quando si crea l'account per un tenant non attendibile, non consentire al tenant di utilizzare la propria origine di identità e non consentire l'utilizzo dei servizi della piattaforma. Vedere la procedura per ["creazione di un account tenant"](#).
- Utilizzare un bilanciamento del carico di terze parti per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.
- In alternativa, puoi utilizzare un proxy storage per un maggiore controllo sui pool di cloud storage e sulle comunicazioni dei servizi della piattaforma dai nodi storage ai servizi esterni. Vedere la procedura per ["creazione di un proxy di archiviazione"](#).
- Facoltativamente, è possibile connettersi ai servizi esterni tramite la rete client. Quindi, seleziona **Configurazione > Sicurezza > Controllo firewall > Reti client non attendibili** e indica 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 opzionale per il bilanciamento del carico che le applicazioni client possono utilizzare per connettersi a StorageGRID. Attenersi alle seguenti linee guida per proteggere i nodi gateway nel sistema StorageGRID:

- Configurare e utilizzare gli endpoint del bilanciamento del carico. Vedere ["Considerazioni per il bilanciamento del carico"](#).
- Utilizzare un bilanciamento del carico di terze parti tra il client e il nodo gateway o i nodi di storage per il traffico client non attendibile. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi. Se si utilizza un bilanciamento del carico di terze parti, il traffico di rete può comunque essere configurato in modo opzionale per passare attraverso un endpoint interno di bilanciamento del carico o essere inviato direttamente ai nodi di storage.
- Se si utilizzano endpoint di bilanciamento del carico, è possibile fare in modo che i client si connettano tramite la rete client. Quindi, seleziona **Configurazione > Sicurezza > Controllo firewall > Reti client non attendibili** e indica 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 dell'appliance hardware

Le appliance hardware StorageGRID sono progettate appositamente per l'utilizzo in un sistema StorageGRID. Alcune appliance possono essere utilizzate come nodi di storage. Altri appliance possono essere utilizzati come nodi di amministrazione o nodi gateway. È possibile combinare nodi appliance con nodi basati su

software o implementare grid all-appliance completamente progettati.

Segui queste linee guida per proteggere i nodi dell'appliance hardware nel tuo sistema StorageGRID:

- Se l'appliance utilizza Gestione di sistema di SANtricity per la gestione del controller di storage, impedire ai client non attendibili di accedere a Gestione di sistema di SANtricity tramite la rete.
- Se l'appliance 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.

È possibile stabilire una VLAN per isolare le connessioni di rete BMC e limitare l'accesso a Internet BMC alle reti attendibili. Per ulteriori informazioni sull'applicazione della separazione VLAN, vedere ["Controller di gestione del battiscopa Harden"](#) scheda informativa sulla sicurezza informatica dal ["Agenzia per la sicurezza nazionale \(NSA\)"](#) E ["Agenzia per la sicurezza informatica e delle infrastrutture \(CISA\)"](#) .

Se non è disponibile una rete di gestione interna sicura e affidabile, lasciare la porta di gestione BMC scollegata o bloccata. Durante un caso di supporto, il supporto tecnico potrebbe richiedere un accesso temporaneo.

- Se l'appliance supporta la gestione remota dell'hardware del controller su Ethernet utilizzando lo standard IPMI (Intelligent Platform Management Interface), bloccare il traffico non attendibile sulla porta 623.

Puoi anche [disabilitare l'accesso IPMI remoto](#).



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 che contengono unità SED, FDE o NL-SAS FIPS gestite con SANtricity System Manager, ["Abilitare e configurare la protezione dell'unità SANtricity"](#).
- 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, utilizzare un server di gestione delle chiavi (KMS) per ["abilitare e configurare la crittografia del nodo software StorageGRID"](#) .

Informazioni correlate

["Scopri di più sulla sicurezza delle unità in SANtricity System Manager"](#)

Linee guida per l'hardening di TLS e SSH in StorageGRID

Dovresti controllare l'accesso SSH, sostituire i certificati TLS predefiniti e selezionare la policy di sicurezza appropriata per le connessioni TLS e SSH.

Linee guida per la protezione avanzata dei certificati

È necessario sostituire i certificati predefiniti creati durante l'installazione con certificati personalizzati.

Per molte organizzazioni, il certificato digitale autofirmato per l'accesso Web a StorageGRID non è conforme

alle policy di sicurezza delle informazioni. Nei sistemi di produzione, è necessario installare un certificato digitale con firma CA da utilizzare per l'autenticazione di StorageGRID.

In particolare, è necessario utilizzare certificati server personalizzati anziché i seguenti certificati predefiniti:

- **Certificato dell'interfaccia di gestione:** Utilizzato per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API.
- **Certificato API S3:** 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 oggetto.

Per ulteriori informazioni e istruzioni, vedere ["Gestire i certificati di sicurezza"](#).



StorageGRID gestisce separatamente i certificati utilizzati per gli endpoint del bilanciamento del carico. Per configurare i certificati di bilanciamento del carico, vedere ["Configurare gli endpoint del bilanciamento del carico"](#).

Quando si utilizzano certificati server personalizzati, attenersi alle seguenti linee guida:

- I certificati devono avere un *subjectAltName* che corrisponda alle voci DNS per StorageGRID. Per ulteriori informazioni, vedere la sezione 4,2.1,6, "Nome alternativo oggetto" in ["RFC 5280: Certificato PKIX e profilo CRL"](#).
- Se possibile, evitare l'utilizzo di certificati con caratteri jolly. Un'eccezione a questa linea guida è il certificato per un endpoint di stile host virtuale S3, che richiede l'utilizzo di un carattere jolly se i nomi dei bucket non sono noti in anticipo.
- Quando è necessario utilizzare i caratteri jolly nei certificati, è necessario adottare ulteriori misure per ridurre i rischi. Utilizzare un modello con caratteri jolly come `*.s3.example.com`, e non utilizzare il `s3.example.com` suffisso per altre applicazioni. Questo modello funziona anche con l'accesso S3 in stile percorso, ad esempio `dc1-s1.s3.example.com/mybucket`.
- Impostare i tempi di scadenza del certificato su brevi (ad esempio, 2 mesi) e utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò è particolarmente importante per i certificati con caratteri jolly.

Inoltre, i client devono utilizzare un rigoroso controllo del nome host quando comunicano con StorageGRID.

Linee guida per la protezione avanzata dei criteri TLS e SSH

È possibile selezionare un criterio di protezione per determinare quali protocolli e cifrature utilizzare per stabilire connessioni TLS sicure con applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

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 la politica Modern predefinita, a meno che il sistema non debba essere conforme ai Common Criteria, conforme a FIPS 140-2 o non sia necessario utilizzare altri cifrari.

Per ulteriori informazioni e istruzioni, vedere ["Gestire i criteri TLS e SSH"](#).

Gestisci l'accesso SSH esterno

Per migliorare la sicurezza del sistema, l'accesso SSH esterno è bloccato per impostazione predefinita. Abilitare l'accesso SSH solo quando è necessario eseguire attività che richiedono l'accesso SSH in ingresso, ad esempio la risoluzione dei problemi. Fare riferimento a ["Gestisci l'accesso SSH esterno"](#) per dettagli e

istruzioni.

Linee guida per il rafforzamento della sicurezza per log, password e messaggi di audit in StorageGRID

Oltre a seguire le linee guida per la protezione avanzata per reti e nodi StorageGRID, è necessario seguire le linee guida per la protezione avanzata per altre aree del sistema StorageGRID.

Password di installazione temporanea

Per proteggere il sistema StorageGRID durante l'installazione, impostare una password nella pagina della password del programma di installazione temporanea nell'interfaccia utente di installazione di StorageGRID o nell'API di installazione. Una volta impostata, questa password viene applicata a tutti i metodi di installazione di StorageGRID, inclusi l'interfaccia utente, l'API di installazione e `configure-storagegrid.py` lo script.

Per ulteriori informazioni, fare riferimento a:

- ["Installa StorageGRID sui nodi basati su software"](#)
- ["Installare l'appliance StorageGRID"](#)

Registri e messaggi di audit

Proteggere sempre i log StorageGRID e l'output dei messaggi di controllo in modo sicuro. I registri e i messaggi di audit di StorageGRID forniscono informazioni preziose dal punto di vista del supporto e della disponibilità del sistema. Inoltre, le informazioni e i dettagli contenuti nei registri StorageGRID e nell'output dei messaggi di audit sono generalmente di natura sensibile.

Configurare StorageGRID per inviare eventi di sicurezza a un server syslog esterno. Se si utilizza l'esportazione syslog, selezionare TLS e RELP/TLS per i protocolli di trasporto.

Per ulteriori informazioni sui registri StorageGRID, vedere la ["Riferimenti ai file di log"](#). Per ulteriori informazioni sui messaggi di controllo StorageGRID, vedere ["Messaggi di audit"](#).

NetApp AutoSupport

La funzione AutoSupport di StorageGRID consente di monitorare in modo proattivo lo stato del sistema e di inviare automaticamente i pacchetti al sito di supporto NetApp, al team di supporto interno dell'organizzazione o a un partner di supporto. Per impostazione predefinita, l'invio di pacchetti AutoSupport a NetApp è attivato quando StorageGRID viene configurato per la prima volta.

La funzione AutoSupport può essere disattivata. Tuttavia, NetApp consiglia di abilitare l'IT perché AutoSupport aiuta a velocizzare l'identificazione e la risoluzione dei problemi in caso di problemi nel sistema StorageGRID.

AutoSupport supporta HTTPS, HTTP e SMTP per i protocolli di trasporto. Data la natura sensibile dei pacchetti AutoSupport, NetApp consiglia vivamente di utilizzare HTTPS come protocollo di trasporto predefinito per l'invio di pacchetti AutoSupport a NetApp.

Condivisione delle risorse tra origini (CORS)

È possibile configurare la condivisione delle risorse cross-origin (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini. In generale, non abilitare il CORS a meno che non sia necessario. Se è richiesto un CORS, limitarlo alle origini attendibili.

Vedi i passaggi per ["configurazione di CORS per bucket e oggetti"](#).

Dispositivi di sicurezza esterni

Una soluzione di protezione avanzata completa deve affrontare i meccanismi di sicurezza esterni a StorageGRID. L'utilizzo di ulteriori dispositivi di infrastruttura per il filtraggio e la limitazione dell'accesso a StorageGRID è un metodo efficace per stabilire e mantenere una posizione di sicurezza rigorosa. Questi dispositivi di sicurezza esterni includono firewall, sistemi di prevenzione delle intrusioni (IPS) e altri dispositivi di sicurezza.

Per il traffico client non attendibile, si consiglia un bilanciamento del carico di terze parti. Il bilanciamento del carico di terze parti offre un maggiore controllo e ulteriori livelli di protezione dagli attacchi.

Mitigazione ransomware

Aiuta a proteggere i dati degli oggetti dagli attacchi ransomware seguendo i consigli descritti in ["Difesa ransomware con StorageGRID"](#).

StorageGRID con FabricPool

Flusso di lavoro di configurazione per l'utilizzo di StorageGRID con FabricPool

Se si utilizza il software NetApp ONTAP, è possibile utilizzare NetApp FabricPool per tierare i dati inattivi su un sistema di storage a oggetti NetApp StorageGRID.

Seguire queste istruzioni per:

- Scopri le considerazioni e le Best practice per la configurazione di StorageGRID per un carico di lavoro FabricPool.
- Scopri come configurare un sistema di storage a oggetti StorageGRID per l'utilizzo con FabricPool.
- Scopri come fornire i valori richiesti a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.

Guida rapida alla configurazione di StorageGRID per FabricPool

1

Pianificare la configurazione

- Decidere quale criterio di tiering dei volumi FabricPool utilizzare per eseguire il tiering dei dati ONTAP inattivi in StorageGRID.
- Pianificare e installare un sistema StorageGRID per soddisfare le esigenze di capacità e performance dello storage.
- Acquisire familiarità con il software di sistema StorageGRID, inclusi ["Grid Manager"](#) e ["Manager tenant"](#).
- Esaminare le procedure consigliate FabricPool per ["Gruppi HA"](#), ["bilanciamento del carico"](#), ["ILM"](#) e ["di più"](#).
- Consulta queste risorse aggiuntive, che forniscono dettagli sull'utilizzo e la configurazione di ONTAP e FabricPool:

["TR-4598: Best practice FabricPool in ONTAP"](#)

["Documentazione ONTAP per FabricPool"](#)

2

Eseguire le attività preliminari

Procurarsi il ["Informazioni necessarie per collegare StorageGRID come Tier cloud"](#), tra cui:

- Indirizzi IP
- Nomi di dominio
- Certificato SSL

Facoltativamente, configurare ["federazione delle identità"](#) E ["single sign-on"](#) .

3

Configurare le impostazioni StorageGRID

Utilizzare StorageGRID per ottenere i valori necessari a ONTAP per la connessione alla rete.

L'utilizzo di ["Installazione guidata di FabricPool"](#) è il metodo consigliato e più rapido per configurare tutti gli elementi, ma è anche possibile configurare ogni entità manualmente, se necessario.

4

Configure ONTAP and DNS (Configura DNS e DNS)

Utilizzare ONTAP per ["aggiungi un tier cloud"](#) utilizzare i valori StorageGRID. Quindi, ["Configurare le voci DNS"](#) associare gli indirizzi IP a qualsiasi nome di dominio che si intende utilizzare.

5

Monitoraggio e gestione

Quando il sistema è in funzione, eseguire le attività in corso in ONTAP e StorageGRID per gestire e monitorare il tiering dei dati FabricPool nel tempo.

Che cos'è FabricPool?

FabricPool è una soluzione di storage ibrido ONTAP che utilizza un aggregato flash dalle performance elevate come Tier delle performance e un archivio di oggetti come Tier del cloud. L'utilizzo di aggregati abilitati per FabricPool consente di ridurre i costi dello storage senza compromettere performance, efficienza o protezione.

FabricPool associa un Tier cloud (un archivio di oggetti esterno, come StorageGRID) a un Tier locale (un aggregato di storage ONTAP) per creare una raccolta composita di dischi. I volumi all'interno di FabricPool possono quindi sfruttare il tiering mantenendo i dati attivi (hot) sullo storage ad alte performance (il Tier locale) e inattivando (cold) i tiering nell'archivio di oggetti esterno (il Tier cloud).

Non sono necessarie modifiche architetturali e puoi continuare a gestire i dati e l'ambiente applicativo dal sistema di storage centrale ONTAP.

Che cos'è StorageGRID?

NetApp StorageGRID è un'architettura di storage che gestisce i dati come oggetti, rispetto ad altre architetture di storage come lo storage a blocchi o file. Gli oggetti vengono conservati all'interno di un singolo contenitore (ad esempio un bucket) e non vengono nidificati come file all'interno di una directory all'interno di altre directory. Sebbene lo storage a oggetti offra generalmente performance inferiori rispetto allo storage a blocchi o a file, è notevolmente più scalabile. I bucket StorageGRID possono contenere petabyte di dati e miliardi di oggetti.

Perché utilizzare StorageGRID come Tier cloud FabricPool?

FabricPool può eseguire il tiering dei dati ONTAP a diversi provider di storage a oggetti, tra cui StorageGRID. A differenza dei cloud pubblici che potrebbero impostare un numero massimo di IOPS (Input/Output Operations per Second) supportati a livello di bucket o container, le performance di StorageGRID sono scalabili in base al numero di nodi in un sistema. L'utilizzo di StorageGRID come livello cloud FabricPool ti consente di conservare i tuoi dati nel tuo cloud privato per ottenere le massime performance e il controllo completo sui tuoi dati.

Inoltre, non è necessaria una licenza FabricPool quando si utilizza StorageGRID come livello cloud.

Informazioni necessarie per collegare StorageGRID come livello cloud FabricPool

Prima di poter collegare StorageGRID come livello cloud per FabricPool, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere determinati valori da utilizzare in ONTAP.

Di quali valori ho bisogno?

La seguente tabella mostra i valori da configurare in StorageGRID e il modo in cui tali valori vengono utilizzati da ONTAP e dal server DNS.

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Indirizzi IP virtuali (VIP)	StorageGRID > Gruppo ha	Voce DNS
Porta	StorageGRID > endpoint del bilanciamento del carico	Gestore di sistema ONTAP > Aggiungi livello cloud
Certificato SSL	StorageGRID > endpoint del bilanciamento del carico	Gestore di sistema ONTAP > Aggiungi livello cloud
Nome server (FQDN)	StorageGRID > endpoint del bilanciamento del carico	Voce DNS
ID chiave di accesso e chiave di accesso segreta	StorageGRID > tenant e bucket	Gestore di sistema ONTAP > Aggiungi livello cloud
Nome bucket/container	StorageGRID > tenant e bucket	Gestore di sistema ONTAP > Aggiungi livello cloud

Come si ottengono questi valori?

In base alle proprie esigenze, è possibile effettuare una delle seguenti operazioni per ottenere le informazioni necessarie:

- Utilizzare il ["Installazione guidata di FabricPool"](#). L'installazione guidata di FabricPool consente di configurare rapidamente i valori richiesti in StorageGRID e di creare un file da utilizzare per configurare Gestione di sistema di ONTAP. La procedura guidata guida l'utente attraverso i passaggi richiesti e aiuta a verificare che le impostazioni siano conformi alle Best practice di StorageGRID e FabricPool.

- Configurare ogni elemento manualmente. Quindi, immettere i valori in Gestore di sistema di ONTAP o nell'interfaccia utente di ONTAP. Attenersi alla seguente procedura:
 - a. ["Configurare un gruppo ad alta disponibilità \(ha\) per FabricPool"](#).
 - b. ["Creare un endpoint di bilanciamento del carico per FabricPool"](#).
 - c. ["Creare un account tenant per FabricPool"](#).
 - d. Accedere all'account tenant e ["creare il bucket e le chiavi di accesso per l'utente root"](#).
 - e. Creare una regola ILM per i dati FabricPool e aggiungerla ai criteri ILM attivi. Vedere ["Configurare ILM per i dati FabricPool"](#).
 - f. Facoltativamente, ["Creare una policy di classificazione del traffico per FabricPool"](#).

Utilizzare l'installazione guidata di FabricPool

Scopri la StorageGRID FabricPool setup wizard

È possibile utilizzare la configurazione guidata di FabricPool per configurare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool. Una volta completata l'installazione guidata, è possibile immettere i dettagli richiesti in Gestione sistema di ONTAP.

Quando utilizzare l'installazione guidata di FabricPool

L'installazione guidata di FabricPool guida l'utente in ogni fase della configurazione di StorageGRID per l'utilizzo con FabricPool e configura automaticamente determinate entità, come ad esempio ILM e i criteri di classificazione del traffico. Durante il completamento della procedura guidata, è possibile scaricare un file da utilizzare per immettere i valori in Gestione sistema di ONTAP. Utilizzare la procedura guidata per configurare il sistema più rapidamente e per assicurarsi che le impostazioni siano conformi alle Best practice StorageGRID e FabricPool.

Se si dispone dell'autorizzazione di accesso root, è possibile completare l'installazione guidata di FabricPool quando si inizia a utilizzare Gestione griglia di StorageGRID oppure accedere e completare la procedura guidata in qualsiasi momento. A seconda dei requisiti, è possibile configurare manualmente alcuni o tutti gli elementi richiesti e quindi utilizzare la procedura guidata per assemblare i valori richiesti da ONTAP in un singolo file.



Utilizzare la procedura guidata di installazione di FabricPool, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

Prima di utilizzare la procedura guidata

Confermare di aver completato questi passaggi dei prerequisiti.

Esaminare le Best practice

- Si ha una comprensione generale di ["Informazioni necessarie per collegare StorageGRID come Tier cloud"](#).
- Hai esaminato le Best practice di FabricPool per:
 - ["Gruppi ad alta disponibilità \(ha\)"](#)
 - ["Bilanciamento del carico"](#)

- ["Regole e policy ILM"](#)

Ottenere gli indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ha, si sa a quali nodi ONTAP si conatterà e a quale rete StorageGRID verrà utilizzata. Si conoscono anche i valori da inserire per la subnet CIDR, l'indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si intende utilizzare una LAN virtuale per separare il traffico FabricPool, l'interfaccia VLAN è già stata configurata. Vedere ["Configurare le interfacce VLAN"](#).

Configurare la federazione di identità e SSO

Se 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 ["USA la federazione delle identità"](#) E ["Configurare il single sign-on"](#) .

Ottenere e configurare i nomi di dominio

- Si conosce il nome di dominio completo (FQDN) da utilizzare per StorageGRID. Le voci DNS (Domain Name Server) associano questo FQDN agli indirizzi IP virtuali (VIP) del gruppo ha creato utilizzando la procedura guidata. Vedere ["Configurare il server DNS"](#).
- Se prevedi di utilizzare richieste S3 in stile virtual-hosted, hai ["Nomi di dominio degli endpoint S3 configurati"](#). ONTAP utilizza URL in stile percorso per impostazione predefinita, ma è consigliato usare richieste in stile virtual-hosted.

Esaminare i requisiti del bilanciamento del carico e del certificato di sicurezza

Se si prevede di utilizzare il bilanciamento del carico StorageGRID, è stato esaminato il generale ["considerazioni per il bilanciamento del carico"](#). Si dispone dei certificati da caricare o dei valori necessari per generare un certificato.

Se si intende utilizzare un endpoint esterno (di terze parti) per il bilanciamento del carico, si dispone del nome di dominio completo (FQDN), della porta e del certificato per il bilanciamento del carico.

Confermare la configurazione del pool di storage ILM

Se inizialmente è stato installato StorageGRID 11,6 o versione precedente, è stato configurato il pool di archiviazione che verrà utilizzato. In generale, è necessario creare un pool di storage per ogni sito StorageGRID che verrà utilizzato per memorizzare i dati ONTAP.



Questo prerequisito non si applica se StorageGRID 11,7 o 11,8 è stato installato inizialmente. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente pool di storage per ogni sito.

Relazione tra ONTAP e il livello cloud StorageGRID

La procedura guidata FabricPool ti guida nel processo di creazione di un singolo Tier cloud StorageGRID che include un tenant StorageGRID, un set di chiavi di accesso e un bucket StorageGRID. Puoi associare questo livello cloud StorageGRID a uno o più livelli locali ONTAP.

L'aggiunta di un singolo Tier cloud a più Tier locali in un cluster è la Best practice generale. Tuttavia, a seconda dei requisiti, è possibile utilizzare più di un bucket o anche più tenant StorageGRID per i Tier locali in un singolo cluster. L'utilizzo di diversi bucket e tenant consente di isolare l'accesso ai dati e ai dati tra i Tier locali

di ONTAP, ma è piuttosto più complesso da configurare e gestire.

NetApp sconsiglia di collegare un singolo Tier cloud ai Tier locali in più cluster.



Per le procedure consigliate per l'utilizzo di StorageGRID con NetApp MetroCluster™ e mirror FabricPool, vedere ["TR-4598: Best practice FabricPool in ONTAP"](#).

Opzionale: Utilizzare un bucket diverso per ciascun Tier locale

Per utilizzare più di un bucket per i Tier locali in un cluster ONTAP, aggiungere più di un Tier cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo ha, endpoint di bilanciamento del carico, tenant e chiavi di accesso, ma utilizza un container diverso (bucket StorageGRID). Attenersi alla seguente procedura generale:

1. Da Gestione griglia di StorageGRID, completare la configurazione guidata di FabricPool per il primo livello cloud.
2. Da Gestore di sistema di ONTAP, Aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Da StorageGRID tenant manager, accedere al tenant creato dalla procedura guidata e creare un secondo bucket.
4. Completare nuovamente la procedura guidata FabricPool. Selezionare il gruppo ha esistente, l'endpoint del bilanciamento del carico e il tenant. Quindi, selezionare il nuovo bucket creato manualmente. Creare una nuova regola ILM per il nuovo bucket e attivare un criterio ILM per includere tale regola.
5. Da ONTAP, Aggiungi un secondo Tier cloud ma fornisci il nuovo nome del bucket.

Facoltativo: Utilizzare un tenant e un bucket diversi per ciascun Tier locale

Per utilizzare più di un tenant e diversi set di chiavi di accesso per i Tier locali in un cluster ONTAP, aggiungere più di un Tier cloud StorageGRID in ONTAP. Ogni livello cloud condivide lo stesso gruppo ha, endpoint di bilanciamento del carico, ma utilizza un tenant, chiavi di accesso e container (bucket StorageGRID) diversi. Attenersi alla seguente procedura generale:

1. Da Gestione griglia di StorageGRID, completare la configurazione guidata di FabricPool per il primo livello cloud.
2. Da Gestore di sistema di ONTAP, Aggiungi un livello cloud e utilizza il file scaricato da StorageGRID per fornire i valori richiesti.
3. Completare nuovamente la procedura guidata FabricPool. Selezionare il gruppo ha esistente e l'endpoint del bilanciamento del carico. Crea un nuovo tenant e bucket. Creare una nuova regola ILM per il nuovo bucket e attivare un criterio ILM per includere tale regola.
4. Da ONTAP, Aggiungi un secondo livello cloud ma fornisci la nuova chiave di accesso, la chiave segreta e il nome del bucket.

Accedi e completa il setup wizard di StorageGRID FabricPool

È possibile utilizzare la configurazione guidata di FabricPool per configurare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool.

Prima di iniziare

- È stata esaminata la ["considerazioni e requisiti"](#) per l'utilizzo della configurazione guidata di FabricPool.



Se si desidera configurare StorageGRID per l'utilizzo con qualsiasi altra applicazione client S3, visitare il sito "[Utilizzare l'installazione guidata S3](#)".

- Si dispone di "[Autorizzazione di accesso root](#)".

Accedere alla procedura guidata

È possibile completare l'installazione guidata di FabricPool quando si inizia a utilizzare Gestione griglia di StorageGRID oppure accedere e completare l'installazione guidata in qualsiasi momento.

Fasi

1. Accedere a Grid Manager utilizzando un "[browser web supportato](#)".
2. Se il banner **FabricPool and S3 setup wizard** appare sulla dashboard, seleziona il collegamento nel banner. Se il banner non appare più, seleziona l'icona di aiuto  dalla barra dell'installazione in Grid Manager e seleziona **FabricPool and S3 setup wizard**.
3. Nella sezione FabricPool della pagina di installazione guidata di FabricPool e S3, selezionare **Configura ora**.

Fase 1 di 9: Viene visualizzato il messaggio Configure ha group (Configura gruppo ha).

Fase 1 di 9: Configurare il gruppo ha

Un gruppo ad alta disponibilità (ha) è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati FabricPool. Un gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Per ulteriori informazioni su questa attività, vedere "[Gestire i gruppi ad alta disponibilità](#)" e "[Best practice per i gruppi ad alta disponibilità](#)".

Fasi

1. Se si prevede di utilizzare un bilanciamento del carico esterno, non è necessario creare un gruppo ha. Selezionare **Salta questo passaggio** e andare a [Fase 2 di 9: Configurare l'endpoint del bilanciamento del carico](#).
2. Per utilizzare il bilanciamento del carico StorageGRID, creare un nuovo gruppo ha o utilizzare un gruppo ha esistente.

Creare un gruppo ha

- a. Per creare un nuovo gruppo ha, selezionare **Crea gruppo ha**.
- b. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

- c. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

- d. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

- e. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR & 8212; un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, 192.16.0.0/22.
Indirizzo IP del gateway (opzionale)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.

Campo	Descrizione
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP e tutti saranno attivi contemporaneamente sull'interfaccia attiva. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

f. Selezionare **Crea gruppo ha**, quindi selezionare **fine** per tornare all'installazione guidata di FabricPool.

g. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Utilizzare il gruppo ha esistente

a. Per utilizzare un gruppo ha esistente, selezionare il nome del gruppo ha dall'elenco a discesa **Select an ha group** (Seleziona un gruppo ha).

b. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Fase 2 di 9: Configurare l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client, come FabricPool. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

È possibile utilizzare il servizio bilanciamento del carico StorageGRID, disponibile su tutti i nodi gateway e di amministrazione, oppure connettersi a un bilanciamento del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciamento del carico StorageGRID.

Per ulteriori informazioni su questa attività, vedere le sezioni generali "[considerazioni per il bilanciamento del carico](#)" e "[Best practice per il bilanciamento del carico per FabricPool](#)".

Fasi

1. Selezionare o creare un endpoint di bilanciamento del carico StorageGRID o utilizzare un bilanciamento del carico esterno.

Creare l'endpoint

- a. Selezionare **Crea endpoint**.
- b. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin. Nota: le porte utilizzate da altri servizi di rete non sono consentite. Consultare la "Riferimento porta di rete".
Tipo di client	Deve essere S3 .
Protocollo di rete	Selezionare HTTPS. Nota: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

- c. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Global (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

d. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. Allow all tenant è quasi sempre l'opzione appropriata per l'endpoint di bilanciamento del carico utilizzato per FabricPool. Selezionare questa opzione se si utilizza l'installazione guidata di FabricPool per un nuovo sistema StorageGRID e non sono stati ancora creati account tenant.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

e. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per i dettagli su cosa immettere.
USA certificato StorageGRID S3	Questa opzione è disponibile solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Per ulteriori informazioni, vedere "Configurare i certificati API S3" .

f. Selezionare **fine** per tornare all'installazione guidata di FabricPool.

g. Selezionare **continua** per passare al punto tenant e bucket.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciamento del carico esistente

- Selezionare il nome di un endpoint esistente dall'elenco a discesa **Select a load balancer endpoint**.
- Selezionare **continua** per passare al punto tenant e bucket.

Utilizzare un bilanciamento del carico esterno

- Completare i seguenti campi per il bilanciamento del carico esterno.

Campo	Descrizione
FQDN	Il nome di dominio completo (FQDN) del bilanciamento del carico esterno.
Porta	Il numero di porta che FabricPool utilizzerà per connettersi al bilanciamento del carico esterno.
Certificato	Copiare il certificato del server per il bilanciamento del carico esterno e incollarlo in questo campo.

- Selezionare **continua** per passare al punto tenant e bucket.

Fase 3 di 9: Tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per memorizzare e recuperare oggetti in StorageGRID. Ogni tenant dispone di utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità. È necessario creare un tenant StorageGRID prima di poter creare il bucket che FabricPool utilizzerà.

Un bucket è un container utilizzato per memorizzare gli oggetti e i metadati degli oggetti di un tenant. Anche se alcuni tenant potrebbero avere molti bucket, la procedura guidata consente di creare o selezionare solo un tenant e un bucket alla volta. Puoi utilizzare il tenant Manager in un secondo momento per aggiungere altri bucket necessari.

È possibile creare un nuovo tenant e bucket per l'utilizzo di FabricPool oppure selezionare un tenant e un bucket esistenti. Se si crea un nuovo tenant, il sistema crea automaticamente l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root del tenant.

Per ulteriori informazioni su questa attività, vedere ["Creare un account tenant per FabricPool"](#) e ["Creare un bucket S3 e ottenere una chiave di accesso"](#).

Fasi

Creare un nuovo tenant e bucket o selezionare un tenant esistente.

Nuovo tenant e bucket

1. Per creare un nuovo tenant e bucket, immettere un **Nome tenant**. Ad esempio, `FabricPool tenant`.
2. Definisci l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID ["federazione delle identità"](#) , ["SSO \(Single Sign-on\)"](#) , o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

3. Per **Nome bucket**, immettere il nome del bucket che verrà utilizzato da FabricPool per memorizzare i dati ONTAP. Ad esempio, `fabricpool-bucket`.



Non è possibile modificare il nome del bucket dopo averlo creato.

4. Selezionare **Region** per questo bucket.

Utilizzare l'area predefinita (`us-east-1`) a meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base all'area del bucket.

5. Selezionare **Create and continue** (Crea e continua) per creare il tenant e il bucket e passare alla fase di download dei dati

Selezionare tenant e bucket

L'account tenant esistente deve disporre di almeno un bucket che non ha attivato il controllo delle versioni. Non puoi selezionare un account tenant esistente se non esiste un bucket per quel tenant.

1. Selezionare il tenant esistente dall'elenco a discesa **Nome tenant**.
2. Selezionare il bucket esistente dall'elenco a discesa **Nome bucket**.

FabricPool non supporta il controllo delle versioni degli oggetti, pertanto i bucket con la versione attivata non vengono visualizzati.



Non selezionare un bucket con blocco oggetti S3 abilitato per l'utilizzo con FabricPool.

3. Selezionare **continua** per passare alla fase di download dei dati.

Fase 4 di 9: Download delle impostazioni ONTAP

Durante questa fase, è possibile scaricare un file da utilizzare per immettere i valori in Gestione di sistema di ONTAP.

Fasi

1. Facoltativamente, seleziona l'icona di copia () per copiare negli appunti sia l'ID della chiave di accesso che la chiave di accesso segreta.

Questi valori sono inclusi nel file di download, ma è possibile salvarli separatamente.

2. Selezionare **Scarica impostazioni ONTAP** per scaricare un file di testo contenente i valori immessi finora.

Il `ONTAP_FabricPool_settings_bucketname.txt` file include le informazioni necessarie per configurare StorageGRID come sistema di storage a oggetti per un Tier cloud FabricPool, tra cui:

- Dettagli sulla connessione del bilanciamento del carico, inclusi nome del server (FQDN), porta e certificato
- Nome bucket
- ID della chiave di accesso e chiave di accesso segreta per l'utente root dell'account tenant

3. Salvare le chiavi copiate e il file scaricato in una posizione sicura.



Non chiudere questa pagina fino a quando non sono stati copiati entrambi i tasti di accesso, scaricati le impostazioni ONTAP o entrambi. I tasti non saranno disponibili dopo la chiusura di questa pagina. Assicurarsi di salvare queste informazioni in una posizione sicura perché possono essere utilizzate per ottenere dati dal sistema StorageGRID.

4. Selezionare la casella di controllo per confermare di aver scaricato o copiato l'ID della chiave di accesso e la chiave di accesso segreta.
5. Selezionare **continua** per passare alla fase del pool di storage ILM.

Fase 5 di 9: Selezionare un pool di storage

Un pool di storage è un gruppo di nodi di storage. Quando si seleziona un pool di storage, si determinano i nodi che StorageGRID utilizzerà per memorizzare i dati a più livelli da ONTAP.

Per ulteriori informazioni su questo passaggio, vedere ["Creare un pool di storage"](#).

Fasi

1. Dall'elenco a discesa **Sito**, selezionare il sito StorageGRID che si desidera utilizzare per i dati a più livelli di ONTAP.
2. Dall'elenco a discesa **Storage pool**, selezionare il pool di storage per il sito.

Il pool di storage di un sito include tutti i nodi di storage di quel sito.

3. Selezionare **continua** per passare al passo della regola ILM.

Fase 6 di 9: Esaminare la regola ILM per FabricPool

Le regole ILM (Information Lifecycle Management) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID.

L'installazione guidata di FabricPool crea automaticamente la regola ILM consigliata per l'utilizzo di FabricPool. Questa regola si applica solo al bucket specificato. Utilizza la codifica di cancellazione 2+1 in un singolo sito per memorizzare i dati a più livelli da ONTAP.

Per ulteriori informazioni su questo passaggio, vedere ["Creare una regola ILM"](#) e ["Best practice per l'utilizzo di ILM con i dati FabricPool"](#).

Fasi

1. Esaminare i dettagli della regola.

Campo	Descrizione
Nome della regola	Generato automaticamente e non modificabile
Descrizione	Generato automaticamente e non modificabile
Filtro	Il nome del bucket Questa regola si applica solo agli oggetti salvati nel bucket specificato.
Tempo di riferimento	Tempo di acquisizione L'istruzione di posizionamento inizia quando gli oggetti vengono inizialmente salvati nel bucket.
Istruzioni per il posizionamento	USA erasure coding 2+1

2. Ordinare il diagramma di conservazione per **periodo di tempo** e **pool di storage** per confermare le istruzioni di posizionamento.
 - Il **periodo di tempo** per la regola è **giorno 0 - per sempre**. **Giorno 0** indica che la regola viene applicata quando i dati vengono sottoposti a tiering da ONTAP. **Per sempre** significa che ILM di StorageGRID non eliminerà i dati a più livelli da ONTAP.
 - Il **Storage pool** per la regola è il pool di storage selezionato. **EC 2+1** indica che i dati verranno memorizzati utilizzando la codifica di cancellazione 2+1. Ogni oggetto verrà salvato come due frammenti di dati e un frammento di parità. I tre frammenti per ciascun oggetto verranno salvati in diversi nodi di storage in un singolo sito.
3. Selezionare **Create and continue** (Crea e continua) per creare questa regola e passare al passaggio del criterio ILM.

Fase 7 di 9: Esaminare e attivare il criterio ILM

Una volta creata la regola ILM per l'utilizzo di FabricPool, la procedura guidata di installazione di FabricPool crea un criterio ILM. È necessario simulare e rivedere attentamente questo criterio prima di attivarlo.

Per ulteriori informazioni su questo passaggio, vedere ["Creare un criterio ILM"](#) e ["Best practice per l'utilizzo di ILM con i dati FabricPool"](#).



Quando si attiva un nuovo criterio ILM, StorageGRID utilizza tale criterio per gestire il posizionamento, la durata e la protezione dei dati di tutti gli oggetti nella griglia, inclusi gli oggetti esistenti e quelli appena acquisiti. In alcuni casi, l'attivazione di un nuovo criterio può causare lo spostamento degli oggetti esistenti in nuove posizioni.



Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

Fasi

1. Facoltativamente, aggiornare il nome * Policy* generato dal sistema. Per impostazione predefinita, il sistema aggiunge "+ FabricPool" al nome del criterio attivo o inattivo, ma è possibile fornire il proprio nome.
2. Esaminare l'elenco di regole nel criterio inattivo.
 - Se la griglia non dispone di un criterio ILM inattivo, la procedura guidata crea un criterio inattivo clonando il criterio attivo e aggiungendo la nuova regola all'inizio.
 - Se la griglia dispone già di un criterio ILM inattivo e tale criterio utilizza le stesse regole e lo stesso ordine del criterio ILM attivo, la procedura guidata aggiunge la nuova regola all'inizio del criterio inattivo.
 - Se il criterio inattivo contiene regole diverse o un ordine diverso da quello attivo, la procedura guidata crea un nuovo criterio inattivo clonando il criterio attivo e aggiungendo la nuova regola all'inizio.
3. Controllare l'ordine delle regole nel nuovo criterio inattivo.

Poiché la regola FabricPool è la prima regola, tutti gli oggetti nel bucket FabricPool vengono posizionati prima della valutazione delle altre regole del criterio. Gli oggetti in qualsiasi altro bucket vengono posizionati in base alle regole successive del criterio.

4. Consulta il diagramma di conservazione per scoprire come conservare i diversi oggetti.
 - a. Selezionare **Espandi tutto** per visualizzare un diagramma di conservazione per ciascuna regola nel criterio inattivo.
 - b. Selezionare **periodo di tempo** e **pool di storage** per rivedere il diagramma di conservazione. Confermare che le regole applicabili al bucket FabricPool o al tenant conservino gli oggetti **per sempre**.
5. Dopo aver esaminato il criterio inattivo, selezionare **attiva e continua** per attivare il criterio e passare alla fase di classificazione del traffico.



Gli errori in una policy ILM possono causare una perdita di dati irreparabile. Esaminare attentamente la policy prima di attivarla.

Fase 8 di 9: Creazione di criteri di classificazione del traffico

Come opzione, la configurazione guidata di FabricPool può creare una policy di classificazione del traffico che è possibile utilizzare per monitorare il carico di lavoro di FabricPool. La policy creata dal sistema utilizza una regola di corrispondenza per identificare tutto il traffico di rete correlato al bucket creato. Questo criterio monitora solo il traffico e non limita il traffico per FabricPool o altri client.

Per ulteriori informazioni su questo passaggio, vedere ["Creare una policy di classificazione del traffico per FabricPool"](#).

Fasi

1. Esaminare la policy.
2. Se si desidera creare questa policy di classificazione del traffico, selezionare **Crea e continua**.

Non appena FabricPool inizia a tiering dei dati su StorageGRID, puoi accedere alla pagina delle policy di classificazione del traffico per visualizzare le metriche del traffico di rete per questa policy. In seguito, è possibile aggiungere regole per limitare altri carichi di lavoro e garantire che il carico di lavoro FabricPool abbia la maggior parte della larghezza di banda.

3. In caso contrario, selezionare **Ignora questo passaggio**.

Fase 9 di 9: Riepilogo

Il riepilogo fornisce dettagli sugli elementi configurati, tra cui il nome del bilanciamento del carico, del tenant e del bucket, la policy di classificazione del traffico e la policy ILM attiva,

Fasi

1. Esaminare il riepilogo.
2. Selezionare **fine**.

Passi successivi

Dopo aver completato la procedura guidata FabricPool, eseguire questi passaggi aggiuntivi.

Fasi

1. Passare a ["Configurare Gestore di sistema di ONTAP"](#) per 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 le policy di tiering dei volumi.
2. Visitare il sito Web ["Configurare il server DNS"](#) e assicurarsi che il DNS includa un record per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID da utilizzare.
3. Visita il ["Altre Best practice per StorageGRID e FabricPool"](#) sito per scoprire le Best practice per i log di audit StorageGRID e altre opzioni di configurazione globale.

Configurare StorageGRID manualmente

Crea un gruppo ad alta disponibilità (HA) per FabricPool in StorageGRID

Quando si configura StorageGRID per l'utilizzo con FabricPool, è possibile creare facoltativamente uno o più gruppi ad alta disponibilità (ha). Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID. Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati FabricPool. Un gruppo ha utilizza indirizzi IP virtuali (VIP) per fornire un accesso altamente disponibile al servizio Load Balancer. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Per ulteriori informazioni su questa attività, vedere ["Gestire i gruppi ad alta disponibilità"](#). Per completare questa attività mediante la procedura guidata di installazione di FabricPool, andare a ["Accedere e completare l'installazione guidata di FabricPool"](#).

Prima di iniziare

- È stata esaminata la ["best practice per i gruppi ad alta disponibilità"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- Se si intende utilizzare una VLAN, è stata creata l'interfaccia VLAN. Vedere ["Configurare le interfacce VLAN"](#).

Fasi

1. Selezionare **Configurazione > Rete > Gruppi ad alta disponibilità**.
2. Selezionare **Crea**.
3. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

4. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

5. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

6. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR& 8212;un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, 192.16.0.0/22.

Campo	Descrizione
Indirizzo IP del gateway (opzionale)	Opzionale. Se gli indirizzi IP ONTAP utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, immettere l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

7. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine).

Crea un endpoint del bilanciatore del carico per FabricPool in StorageGRID

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client, come FabricPool. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

Quando si configura StorageGRID per l'utilizzo con FabricPool, è necessario configurare un endpoint di bilanciamento del carico e caricare o generare un certificato endpoint di bilanciamento del carico, utilizzato per proteggere la connessione tra ONTAP e StorageGRID.

Per completare questa attività mediante la procedura guidata di installazione di FabricPool, andare a ["Accedere e completare l'installazione guidata di FabricPool"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- Avete esaminato il generale ["considerazioni per il bilanciamento del carico"](#) e il ["Best practice per il bilanciamento del carico per FabricPool"](#).

Fasi

1. Selezionare **Configurazione > Rete > Endpoint del bilanciatore del carico**.
2. Selezionare **Crea**.
3. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.

Campo	Descrizione
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. Nota: le porte utilizzate da altri servizi di rete non sono consentite. Consultare la "Riferimento porta di rete". Fornirai questo numero a ONTAP quando Aggiungi StorageGRID come Tier cloud FabricPool.
Tipo di client	Selezionare S3 .
Protocollo di rete	Selezionare HTTPS. Nota: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

4. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione Global (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

5. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita)	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. Allow all tenant è quasi sempre l'opzione appropriata per l'endpoint di bilanciamento del carico utilizzato per FabricPool. Selezionare questa opzione se non sono ancora stati creati account tenant.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

6. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per i dettagli su cosa immettere.
USA certificato StorageGRID S3	Questa opzione è disponibile solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Per ulteriori informazioni, vedere "Configurare i certificati API S3" .

7. Selezionare **Crea**.



Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Crea un account tenant per FabricPool in StorageGRID

È necessario creare un account tenant in Grid Manager per l'utilizzo con FabricPool.

Gli account tenant consentono alle applicazioni client di memorizzare e recuperare oggetti su StorageGRID. Ogni account tenant dispone di un proprio ID account, gruppi e utenti autorizzati, bucket e oggetti.

Per ulteriori informazioni su questa attività, vedere ["Creare un account tenant"](#). Per completare questa attività mediante la procedura guidata di installazione di FabricPool, andare a ["Accedere e completare l'installazione guidata di FabricPool"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Fasi

1. Selezionare **Inquilini**.
2. Selezionare **Crea**.
3. Per la procedura di inserimento dei dettagli, immettere le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant.
Tipo di client	Deve essere S3 per FabricPool.
Quota di storage (opzionale)	Lasciare vuoto questo campo per FabricPool.

4. Per il passo Select permissions:

- a. Non selezionare **Allow platform Services** (Consenti servizi piattaforma).

I tenant FabricPool non devono in genere utilizzare servizi di piattaforma, come la replica di CloudMirror.

- b. Facoltativamente, selezionare **Usa origine identità propria**.

- c. Non selezionare **Allow S3 Select** (Consenti selezione S3).

I tenant FabricPool in genere non devono utilizzare S3 Select.

- d. Facoltativamente, seleziona **Usa connessione di federazione griglia** per consentire al tenant di utilizzare una ["connessione a federazione di griglie"](#) per la sincronizzazione degli account e la replica tra griglie. Quindi, seleziona la connessione di federazione 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 delle identità"](#), ["SSO \(Single Sign-on\)"](#), o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.

Opzione	Eseguire questa operazione
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

6. Selezionare **Crea tenant**.

Crea un bucket S3 e ottieni le chiavi di accesso per FabricPool in StorageGRID

Prima di utilizzare StorageGRID con un carico di lavoro FabricPool, è necessario creare un bucket S3 per i dati FabricPool. È inoltre necessario ottenere una chiave di accesso e una chiave di accesso segreta per l'account tenant che si utilizzerà per FabricPool.

Per ulteriori informazioni su questa attività, vedere ["Creare un bucket S3"](#) e ["Creare le proprie chiavi di accesso S3"](#). Per completare questa attività mediante la procedura guidata di installazione di FabricPool, andare a ["Accedere e completare l'installazione guidata di FabricPool"](#).

Prima di iniziare

- È stato creato un account tenant per l'utilizzo di FabricPool.
- Si dispone dell'accesso root all'account tenant.

Fasi

1. Accedi al tenant manager.

È possibile effettuare una delle seguenti operazioni:

- Dalla pagina account tenant in Grid Manager, selezionare il collegamento **Accedi** per il tenant e immettere le credenziali.
- Immettere l'URL dell'account tenant in un browser Web e le credenziali.

2. Creare un bucket S3 per i dati FabricPool.

È necessario creare un bucket unico per ogni cluster ONTAP che si intende utilizzare.

- Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
- Selezionare **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. Selezionare la regione per questo bucket.

Per impostazione predefinita, tutti i bucket vengono creati in `us-east-1` regione. Se la regione predefinita è configurata su una regione diversa da `us-east-1`, inizialmente viene selezionata quest'altra regione nel menu a discesa.

e. Selezionare **continua**.

f. Selezionare **Crea bucket**.



Non selezionare **attiva versione oggetto** per il bucket FabricPool. Allo stesso modo, non modificare un bucket FabricPool per utilizzare **available** o una coerenza non predefinita. La coerenza bucket consigliata per i bucket FabricPool è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket.

3. Creare una chiave di accesso e una chiave di accesso segreta.

- Selezionare **STORAGE (S3) > My access key**.
- Selezionare **Crea chiave**.
- Selezionare **Crea chiave di accesso**.
- Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.

Questi valori verranno immessi in ONTAP quando si configura StorageGRID come livello cloud FabricPool.



Se in futuro si generano una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID, inserire le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.

Configura StorageGRID ILM per i dati FabricPool

Puoi utilizzare questo semplice esempio di policy come punto di partenza per le tue regole e policy ILM.

In questo esempio si presuppone che si stiano progettando le regole ILM e una policy ILM per un sistema StorageGRID con quattro nodi di storage in un singolo data center a Denver, Colorado. I dati FabricPool in questo esempio utilizzano un bucket denominato `fabricpool-bucket`.



Le seguenti regole e policy ILM sono solo esempi. Esistono diversi modi per configurare le regole ILM. Prima di attivare un nuovo criterio, simularlo per verificare che funzioni come previsto per proteggere il contenuto dalla perdita. Per ulteriori informazioni, vedere ["Gestire gli oggetti con ILM"](#).



Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

Prima di iniziare

- È stata esaminata la ["Best practice per l'utilizzo di ILM con i dati FabricPool"](#).
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso a ILM o Root"](#).
- Se hai eseguito l'aggiornamento a StorageGRID 12.1 da una versione di StorageGRID precedente alla 11.7, hai configurato il pool di storage che utilizzerai. In generale, dovresti creare un pool di storage per

ogni sito StorageGRID che utilizzerai per archiviare i dati. (A partire dalla versione 11.7, i pool di storage vengono creati automaticamente per ogni sito.)



Questo prerequisito non si applica se StorageGRID 11,7 o 11,8 è stato installato inizialmente. Quando si installa inizialmente una di queste versioni, vengono creati automaticamente pool di storage per ogni sito.

Fasi

1. Creare una regola ILM applicabile solo ai dati in `fabricpool-bucket`. questa regola di esempio crea copie con erasure coding.

Definizione della regola	Valore di esempio
Nome della regola	2 + 1 erasure coding per i dati FabricPool
Nome bucket	<code>fabricpool-bucket</code> È anche possibile filtrare l'account tenant FabricPool.
Filtri avanzati	Dimensione dell'oggetto superiore a 0.2 MB. Nota: FabricPool scrive solo oggetti da 4 MB, ma è necessario aggiungere un filtro per le dimensioni degli oggetti perché questa regola utilizza la codifica di cancellazione.
Tempo di riferimento	Tempo di acquisizione
Periodo di tempo e collocamenti	Dal giorno 0 memorizzare per sempre Memorizzare gli oggetti cancellando il codice utilizzando lo schema 2+1 EC a Denver e conservarli in StorageGRID per sempre.  Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool.
Comportamento di acquisizione	Bilanciato

2. Creare una regola ILM predefinita che crei due copie replicate di qualsiasi oggetto non corrispondente alla prima regola. Non selezionare un filtro di base (account tenant o nome bucket) o filtri avanzati.

Definizione della regola	Valore di esempio
Nome della regola	Due copie replicate
Nome bucket	<i>nessuno</i>
Filtri avanzati	<i>nessuno</i>

Definizione della regola	Valore di esempio
Tempo di riferimento	Tempo di acquisizione
Periodo di tempo e collocamenti	Dal giorno 0 memorizzare per sempre Memorizzare gli oggetti replicando 2 copie a Denver.
Comportamento di acquisizione	Bilanciato

3. Creare un criterio ILM e selezionare le due regole. Poiché la regola di replica non utilizza alcun filtro, può essere l'ultima regola predefinita per il criterio.
4. Acquisire oggetti di test nella griglia.
5. Simulare il criterio con gli oggetti di test per verificare il comportamento.
6. Attivare il criterio.

Quando questo criterio è attivato, StorageGRID inserisce i dati degli oggetti come segue:

- I dati in tiering da FabricPool `fabricpool-bucket` saranno sottoposti a erasure coding attraverso lo schema di erasure coding 2+1. Due frammenti di dati e un frammento di parità verranno posizionati su tre diversi nodi di storage.
- Tutti gli oggetti in tutti gli altri bucket verranno replicati. Verranno create due copie e collocate su due diversi nodi di storage.
- Le copie verranno conservate in StorageGRID per sempre. ILM di StorageGRID non elimina questi oggetti.

Creare una politica di classificazione del traffico per FabricPool in StorageGRID

È possibile, in via opzionale, progettare una policy di classificazione del traffico StorageGRID per ottimizzare la qualità del servizio per il carico di lavoro FabricPool.

Per ulteriori informazioni su questa attività, vedere ["Gestire le policy di classificazione del traffico"](#). Per completare questa attività mediante la procedura guidata di installazione di FabricPool, andare a ["Accedere e completare l'installazione guidata di FabricPool"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

Le Best practice per la creazione di una policy di classificazione del traffico per FabricPool dipendono dal carico di lavoro, come segue:

- Se si prevede di suddividere i dati del carico di lavoro primario FabricPool in StorageGRID, assicurarsi che il carico di lavoro FabricPool abbia la maggior parte della larghezza di banda. È possibile creare una policy di classificazione del traffico per limitare tutti gli altri carichi di lavoro.



In generale, le operazioni di lettura FabricPool sono più importanti per le priorità rispetto alle operazioni di scrittura.

Ad esempio, se altri client S3 utilizzano questo sistema StorageGRID, è necessario creare un criterio di classificazione del traffico. È possibile limitare il traffico di rete per gli altri bucket, tenant, subnet IP o endpoint del bilanciamento del carico.

- In genere, non è consigliabile imporre limiti alla qualità del servizio a nessun carico di lavoro FabricPool; si consiglia di limitare solo gli altri carichi di lavoro.
- I limiti imposti agli altri carichi di lavoro devono tenere conto del comportamento di tali carichi di lavoro. I limiti imposti variano anche in base al dimensionamento e alle funzionalità del tuo grid e alla quantità di utilizzo prevista.

Fasi

1. Selezionare **Configurazione > Rete > Classificazione del traffico**.
2. Selezionare **Crea**.
3. Inserire un nome e una descrizione (opzionale) per la policy e selezionare **continua**.
4. Per il passo Add Matching rules (Aggiungi regole di corrispondenza), aggiungere almeno una regola.
 - a. Selezionare **Aggiungi regola**
 - b. Per tipo, selezionare **endpoint del bilanciamento del carico** e selezionare l'endpoint del bilanciamento del carico creato per FabricPool.

È inoltre possibile selezionare l'account o il bucket del tenant FabricPool.
 - c. Se si desidera che questo criterio di traffico limiti il traffico per gli altri endpoint, selezionare **corrispondenza inversa**.
5. Facoltativamente, aggiungere uno o più limiti per controllare il traffico di rete corrispondente alla regola.



StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

- a. Selezionare **Aggiungi un limite**.
 - b. Selezionare il tipo di traffico che si desidera limitare e il limite da applicare.
6. Selezionare **continua**.
 7. Leggere e rivedere la policy di classificazione del traffico. Utilizzare il pulsante **precedente** per tornare indietro e apportare le modifiche necessarie. Quando si è soddisfatti della policy, selezionare **Salva e continua**.

Dopo il completamento

["Visualizzare le metriche del traffico di rete"](#) per verificare che i criteri applichino i limiti di traffico previsti.

Configura ONTAP System Manager per aggiungere StorageGRID come livello cloud FabricPool

Dopo aver ottenuto le informazioni StorageGRID richieste, puoi accedere a ONTAP per aggiungere StorageGRID come livello cloud.

Prima di iniziare

- Una volta completata l'installazione guidata di FabricPool, il file è stato `ONTAP_FabricPool_settings_bucketname.txt` scaricato.

- Se StorageGRID è stato configurato manualmente, si dispone del nome di dominio completo (FQDN) utilizzato per StorageGRID o dell'indirizzo IP virtuale (VIP) per il gruppo StorageGRID ha, del numero di porta per l'endpoint del bilanciamento del carico, del certificato del bilanciamento del carico, L'ID della chiave di accesso e la chiave segreta per l'utente root dell'account tenant e il nome del bucket ONTAP utilizzato in tale tenant.

Accedere a Gestore di sistema di ONTAP

Queste istruzioni descrivono come utilizzare Gestione di sistema di ONTAP per aggiungere StorageGRID come livello cloud. È possibile completare la stessa configurazione utilizzando l'interfaccia utente di ONTAP. Per istruzioni, vedere ["Documentazione ONTAP per FabricPool"](#) .

Fasi

1. Accedere a Gestore di sistema per il cluster ONTAP che si desidera raggruppare in StorageGRID.
2. Accedere come amministratore del cluster.
3. Accedere a **STORAGE > Tier > Add Cloud Tier**.
4. Selezionare **StorageGRID** dall'elenco dei provider di archivi di oggetti.

Inserire i valori StorageGRID

Per ulteriori informazioni, vedere ["Documentazione ONTAP per FabricPool"](#) .

Fasi

1. Completare il modulo Add Cloud Tier (Aggiungi livello cloud) utilizzando il `ONTAP_FabricPool_settings_bucketname.txt` file o i valori ottenuti manualmente.

Campo	Descrizione
Nome	Immettere un nome univoco per questo livello cloud. È possibile accettare il valore predefinito.
Stile URL	Se "Nomi di dominio degli endpoint S3 configurati" selezioni Virtual-Hosted-Style URL. URL in formato percorso è l'impostazione predefinita per ONTAP, ma è consigliato utilizzare richieste in formato virtual-hosted-style per StorageGRID. Devi usare URL in formato percorso se fornisci un indirizzo IP invece di un domain name per il campo Server name (FQDN).

Campo	Descrizione
Nome server (FQDN)	Immettere il nome di dominio completo (FQDN) utilizzato per StorageGRID o l'indirizzo IP virtuale (VIP) per il gruppo StorageGRID ha. Ad esempio, <code>s3.storagegrid.company.com</code>. Tenere presente quanto segue: • L'indirizzo IP o il nome di dominio specificato deve corrispondere al certificato caricato o generato per l'endpoint del bilanciamento del carico di StorageGRID. • Se si fornisce un nome di dominio, il record DNS deve essere associato a ciascun indirizzo IP utilizzato per la connessione a StorageGRID. Vedere "Configurare il server DNS".
SSL	Enabled (attivato) (impostazione predefinita).
Certificato dell'archivio di oggetti	Incollare il PEM del certificato che si sta utilizzando per l'endpoint di bilanciamento del carico StorageGRID, inclusi: <pre>-----BEGIN CERTIFICATE----- E -----END CERTIFICATE-----.</pre> Nota: se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.
Porta	Inserire la porta utilizzata dall'endpoint del bilanciamento del carico StorageGRID. ONTAP utilizzerà questa porta quando si connette a StorageGRID. Ad esempio, 10433.
Chiave di accesso e chiave segreta	Immettere l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root dell'account tenant StorageGRID. Suggerimento: Se in futuro si generano una nuova chiave di accesso e una chiave di accesso segreta in StorageGRID, inserire le nuove chiavi in ONTAP prima di eliminare i vecchi valori da StorageGRID. In caso contrario, ONTAP potrebbe perdere temporaneamente l'accesso a StorageGRID.
Nome del container	Immettere il nome del bucket StorageGRID creato per l'utilizzo con questo Tier ONTAP.

2. Completare la configurazione finale di FabricPool in ONTAP.

- Collegare uno o più aggregati al livello cloud.
- Facoltativamente, creare una policy di tiering dei volumi.

Configura le voci del DNS server per StorageGRID con FabricPool

Dopo aver configurato i gruppi ad alta disponibilità, gli endpoint del bilanciamento del carico e i nomi di dominio degli endpoint S3, è necessario assicurarsi che il DNS includa

le voci necessarie per StorageGRID. È necessario includere una voce DNS per ciascun nome nel certificato di protezione e per ogni indirizzo IP che si potrebbe utilizzare.

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

Voci DNS per il nome del server StorageGRID

Aggiungere voci DNS per associare il nome del server StorageGRID (nome di dominio completo) a ciascun indirizzo IP StorageGRID che si intende utilizzare. Gli indirizzi IP immessi nel DNS dipendono dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, ONTAP si conatterà agli indirizzi IP virtuali di tale gruppo ha.
- Se non si utilizza un gruppo ha, ONTAP può connettersi al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore.
- Se il nome del server viene risolto in più indirizzi IP, ONTAP stabilisce le connessioni client con tutti gli indirizzi IP (fino a un massimo di 16 indirizzi IP). Gli indirizzi IP vengono raccolti con un metodo round-robin quando vengono stabilite le connessioni.

Voci DNS per richieste in stile virtual-hosted

Se hai definito ["Nomi di dominio degli endpoint S3"](#) e intendi utilizzare richieste in stile virtual-hosted, aggiungi le voci DNS per tutti i domain name degli endpoint S3 richiesti, inclusi eventuali nomi wildcard.

Best practice StorageGRID per FabricPool

Best practice per i gruppi HA (alta disponibilità) di StorageGRID con FabricPool

Prima di associare StorageGRID come livello cloud FabricPool, scopri i gruppi ad alta disponibilità (ha) di StorageGRID e consulta le Best practice per l'utilizzo dei gruppi ad alta disponibilità con FabricPool.

Che cos'è un gruppo ha?

Un gruppo ad alta disponibilità (ha) è un insieme di interfacce da più nodi gateway StorageGRID, nodi amministrativi o entrambi. Un gruppo ha aiuta a mantenere disponibili le connessioni dati dei client. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni FabricPool.

Ogni gruppo ha fornisce un accesso altamente disponibile ai servizi condivisi sui nodi associati. Ad esempio, un gruppo ha costituito da interfacce solo su nodi gateway o su entrambi i nodi Admin e Gateway fornisce un accesso altamente disponibile al servizio Load Balancer condiviso.

Per ulteriori informazioni sui gruppi ad alta disponibilità, vedere ["Gestire i gruppi ad alta disponibilità \(ha\)"](#).

Utilizzo di gruppi ha

Le Best practice per la creazione di un gruppo StorageGRID ha per FabricPool dipendono dal carico di lavoro.

- Se si prevede di utilizzare FabricPool con i dati del carico di lavoro primario, è necessario creare un gruppo ha che includa almeno due nodi di bilanciamento del carico per evitare l'interruzione del recupero dei dati.
- Se si prevede di utilizzare la policy di tiering del volume solo snapshot di FabricPool o Tier di performance locali non primari (ad esempio, ubicazioni per il disaster recovery o destinazioni NetApp SnapMirror®), è

possibile configurare un gruppo ha con un solo nodo.

Queste istruzioni descrivono la configurazione di un gruppo ha per Active-Backup ha (un nodo è attivo e un nodo è il backup). Tuttavia, potrebbe essere preferibile utilizzare DNS Round Robin o Active-Active ha. Per scoprire i vantaggi di queste altre configurazioni ha, vedere ["Opzioni di configurazione per i gruppi ha"](#).

Best practice per il bilanciamento del carico di StorageGRID con FabricPool

Prima di associare StorageGRID come livello cloud FabricPool, esaminare le Best practice per l'utilizzo dei bilanciatori di carico con FabricPool.

Per informazioni generali sul bilanciamento del carico StorageGRID e sul certificato di bilanciamento del carico, vedere ["Considerazioni per il bilanciamento del carico"](#).

Best practice per l'accesso del tenant all'endpoint del bilanciamento del carico utilizzato per FabricPool

È possibile controllare quali tenant possono utilizzare un endpoint specifico di bilanciamento del carico per accedere ai bucket. È possibile consentire tutti i tenant, consentire alcuni tenant o bloccare alcuni tenant. Quando si crea un endpoint di bilanciamento del carico per l'utilizzo di FabricPool, selezionare **Allow all tenant** (Consenti tutti i tenant). ONTAP crittografa i dati inseriti nei bucket StorageGRID, pertanto questo livello di sicurezza aggiuntivo non offre una sicurezza aggiuntiva minima.

Best practice per il certificato di sicurezza

Quando si crea un endpoint di bilanciamento del carico StorageGRID per l'utilizzo di FabricPool, si fornisce il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Nella maggior parte dei casi, la connessione tra ONTAP e StorageGRID deve utilizzare la crittografia TLS (Transport Layer Security). L'utilizzo di FabricPool senza crittografia TLS è supportato ma non consigliato. Quando si seleziona il protocollo di rete per l'endpoint del bilanciamento del carico StorageGRID, selezionare **HTTPS**. Quindi, fornire il certificato di sicurezza che consentirà a ONTAP di autenticarsi con StorageGRID.

Per ulteriori informazioni sul certificato server per un endpoint di bilanciamento del carico:

- ["Gestire i certificati di sicurezza"](#)
- ["Considerazioni per il bilanciamento del carico"](#)
- ["Linee guida per la protezione avanzata dei certificati server"](#)

Aggiungi certificato a ONTAP

Quando si aggiunge StorageGRID come livello cloud FabricPool, è necessario installare lo stesso certificato nel cluster ONTAP, inclusi i certificati root e gli eventuali certificati CA subordinati.

Gestire la scadenza del certificato



Se il certificato utilizzato per proteggere la connessione tra ONTAP e StorageGRID scade, FabricPool smetterà temporaneamente di funzionare e ONTAP perderà temporaneamente l'accesso ai dati a livello di StorageGRID.

Per evitare problemi di scadenza del certificato, attenersi alle seguenti Best practice:

- Monitorare attentamente tutti gli avvisi che avvisano di imminenti date di scadenza dei certificati, come ad esempio la scadenza del certificato endpoint del sistema di bilanciamento del carico* e la scadenza del

certificato globale del server per gli avvisi API S3*.

- Mantenere sempre sincronizzate le versioni StorageGRID e ONTAP del certificato. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato da ONTAP per il livello cloud.
- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile utilizzare l'API Grid Management per automatizzare la rotazione del certificato. Ciò consente di sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e in ONTAP prima della scadenza del certificato esistente. Se un certificato autofirmato è già scaduto, disattivare la convalida del certificato in ONTAP per evitare la perdita di accesso.

Vedere ["Knowledge base di NetApp: Come configurare un nuovo certificato server autofirmato StorageGRID su un'implementazione ONTAP FabricPool esistente"](#) per istruzioni.

Procedure consigliate per l'utilizzo di StorageGRID ILM con i dati FabricPool

Se si utilizza FabricPool per eseguire il tiering dei dati in StorageGRID, è necessario comprendere i requisiti per l'utilizzo di ILM (Information Lifecycle Management) di StorageGRID con i dati FabricPool.



FabricPool non conosce le regole o le policy ILM di StorageGRID. La perdita di dati può verificarsi se il criterio ILM di StorageGRID non è configurato correttamente. Per informazioni dettagliate, vedere ["Utilizzare le regole ILM per gestire gli oggetti"](#) e ["Creare policy ILM"](#).

Linee guida per l'utilizzo di ILM con FabricPool

Quando si utilizza l'installazione guidata di FabricPool, la procedura guidata crea automaticamente una nuova regola ILM per ogni bucket S3 creato e aggiunge tale regola a un criterio inattivo. Viene richiesto di attivare il criterio. La regola creata automaticamente segue le Best practice consigliate: Utilizza la codifica di cancellazione 2+1 in un singolo sito.

Se si sta configurando StorageGRID manualmente invece di utilizzare l'installazione guidata di FabricPool, consultare queste linee guida per assicurarsi che le regole ILM e i criteri ILM siano adatti ai dati FabricPool e ai requisiti di business. Potrebbe essere necessario creare nuove regole e aggiornare i criteri ILM attivi per soddisfare queste linee guida.

- Puoi utilizzare qualsiasi combinazione di regole di replica e erasure coding per proteggere i dati del livello cloud.

La Best practice consigliata consiste nell'utilizzare la codifica di cancellazione 2+1 all'interno di un sito per una protezione dei dati conveniente. L'erasure coding utilizza più CPU, ma offre una capacità di storage significativamente inferiore rispetto alla replica. Gli schemi 4+1 e 6+1 utilizzano una capacità inferiore rispetto allo schema 2+1. Tuttavia, gli schemi 4+1 e 6+1 sono meno flessibili se è necessario aggiungere nodi di storage durante l'espansione della griglia. Per ulteriori informazioni, vedere ["Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione"](#).

- Ogni regola applicata ai dati FabricPool deve utilizzare la codifica di cancellazione oppure creare almeno due copie replicate.



Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

- Se è necessario ["Rimuovere i dati FabricPool da StorageGRID"](#), utilizzare ONTAP per recuperare tutti i dati per il volume FabricPool e promuoverli al livello di prestazioni.



Per evitare la perdita di dati, non utilizzare una regola ILM che scadrà o eliminerà i dati del livello cloud di FabricPool. Impostare il periodo di conservazione in ogni regola ILM su **forever** per garantire che gli oggetti FabricPool non vengano cancellati da ILM StorageGRID.

- Non creare regole che spostino i dati del Tier cloud FabricPool dal bucket a un'altra posizione. Non è possibile utilizzare un pool di storage cloud per spostare i dati FabricPool in un altro archivio di oggetti.



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

- A partire da ONTAP 9.8, è possibile creare tag a oggetti per semplificare la classificazione e l'ordinamento dei dati a più livelli. Ad esempio, è possibile impostare i tag solo sui volumi FabricPool collegati a StorageGRID. Quindi, quando si creano le regole ILM in StorageGRID, è possibile utilizzare il filtro avanzato tag oggetto per selezionare e inserire questi dati.

Best practice per le impostazioni globali di StorageGRID con FabricPool

Quando si configura un sistema StorageGRID per l'utilizzo con FabricPool, potrebbe essere necessario modificare altre opzioni di StorageGRID. Prima di modificare un'impostazione globale, valutare in che modo la modifica influirà sulle altre applicazioni S3.

Destinazioni di log e messaggi di audit

I carichi di lavoro FabricPool spesso prevedono un elevato tasso di operazioni di lettura, che può generare un elevato volume di messaggi di audit.

- Se non è necessario un record delle operazioni di lettura del client per FabricPool o qualsiasi altra applicazione S3, è possibile andare facoltativamente su **Configurazione > Monitoraggio > Server di audit e syslog**. Modificare l'impostazione **Lecture client** su **Errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo. Vedere ["Configurare la gestione dei log e il server syslog esterno"](#) per i dettagli.
- Se si dispone di un grande grid, si utilizzano più tipi di applicazioni S3 o si desidera conservare tutti i dati di audit, configurare un server syslog esterno e salvare le informazioni di audit in remoto. L'utilizzo di un server esterno riduce al minimo l'impatto delle performance della registrazione dei messaggi di audit senza ridurre la completezza dei dati di audit. Per ulteriori informazioni, vedere ["Considerazioni sul server syslog esterno"](#).

Crittografia degli oggetti

Durante la configurazione di StorageGRID, è possibile attivare ["opzione globale per la crittografia degli oggetti memorizzati"](#) se è richiesta la crittografia dei dati per altri client StorageGRID. I dati a più livelli da FabricPool a

StorageGRID sono già crittografati, pertanto l'attivazione dell'impostazione StorageGRID non è necessaria. Le chiavi di crittografia lato client sono di proprietà di ONTAP.

Compressione degli oggetti

Durante la configurazione di StorageGRID, non attivare ["opzione globale per comprimere gli oggetti memorizzati"](#). I dati a più livelli da FabricPool a StorageGRID sono già compressi. L'utilizzo dell'opzione StorageGRID non riduce ulteriormente le dimensioni di un oggetto.

Blocco oggetti S3

Se l'impostazione globale S3 Object Lock è abilitata per il sistema StorageGRID, non abilitarla ["Blocco oggetti S3"](#) quando si creano bucket FabricPool. S3 Object Lock non è supportato per i bucket FabricPool.

Consistenza della benna

Per i bucket FabricPool, la coerenza del bucket consigliata è **Read-after-new-write**, che è la coerenza predefinita per un nuovo bucket. Non modificare i bucket FabricPool per utilizzare **available** o **strong-site**.

Tiering FabricPool

Se un nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verificare che il volume non disponga di un criterio di tiering FabricPool attivato. Ad esempio, se un nodo StorageGRID è in esecuzione su un host VMware, assicurarsi che il volume che esegue il backup del datastore per il nodo StorageGRID non abbia un criterio di tiering FabricPool attivato. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.



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

Rimuovere i dati FabricPool da StorageGRID

Se è necessario rimuovere i dati FabricPool attualmente memorizzati in StorageGRID, è necessario utilizzare ONTAP per recuperare tutti i dati del volume FabricPool e promuoverli al livello di performance.

Prima di iniziare

- Sono state esaminate le istruzioni e le considerazioni in ["Promuovi i dati al Tier di performance"](#).
- Si sta utilizzando ONTAP 9,8 o versione successiva.
- Si sta utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti StorageGRID per l'account tenant FabricPool che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#).

A proposito di questa attività

Queste istruzioni spiegano come trasferire i dati da StorageGRID a FabricPool. Eseguire questa procedura utilizzando ONTAP e Gestore tenant StorageGRID.

Fasi

1. Da ONTAP, immettere il `volume modify` comando.

Impostare `tiering-policy` su `none` per interrompere il nuovo tiering e impostare `cloud-retrieval-policy` su `promote` per restituire a StorageGRID tutti i dati precedentemente sottoposti a tiering.

Vedere ["Promuovi tutti i dati da un volume FabricPool al Tier di performance"](#).

2. Attendere il completamento dell'operazione.

È possibile utilizzare il `volume object-store` comando con `tiering` l'opzione a ["verifica lo stato della promozione del tier di performance"](#).

3. Una volta completata l'operazione di promozione, accedere al manager tenant StorageGRID per ottenere l'account tenant FabricPool.

4. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

5. Verificare che il bucket FabricPool sia vuoto.

6. Se la benna è vuota, ["eliminare il bucket"](#).

Al termine

Quando si elimina il bucket, il tiering da FabricPool a StorageGRID non può più continuare. Tuttavia, poiché il Tier locale è ancora collegato al Tier cloud di StorageGRID, Gestore di sistema di ONTAP restituirà messaggi di errore che indicano che il bucket non è accessibile.

Per evitare questi messaggi di errore, effettuare una delle seguenti operazioni:

- Utilizza il mirror FabricPool per collegare un altro livello cloud all'aggregato.
- Spostare i dati dall'aggregato FabricPool a un aggregato non FabricPool, quindi eliminare l'aggregato inutilizzato.

Per istruzioni, vedere la ["Documentazione ONTAP per FabricPool"](#) .

Utilizzare tenant e client StorageGRID

Utilizzare un account tenant

Utilizzare un account tenant StorageGRID

Un account tenant consente di utilizzare l'API REST S3 (Simple Storage Service) per memorizzare e recuperare gli oggetti in un sistema StorageGRID.

Che cos'è un account tenant?

Ogni account tenant ha i propri gruppi, utenti, bucket S3 e oggetti federati o locali.

Gli account tenant possono essere utilizzati per separare gli oggetti memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se il sistema StorageGRID viene utilizzato all'interno di un'azienda, lo storage a oggetti del grid potrebbe essere separato dai diversi reparti dell'organizzazione. Ad esempio, potrebbero essere presenti account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.



Se si utilizza il protocollo client S3, è 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 bucket](#)" per maggiori informazioni.

- **Caso d'utilizzo del provider di servizi:** se il sistema StorageGRID viene utilizzato da un provider di servizi, lo storage a oggetti della griglia potrebbe essere separato dalle diverse entità che affittano lo storage. Ad esempio, potrebbero essere presenti account tenant per la società A, la società B, la società C e così via.

Come creare un account tenant

Gli account tenant vengono creati da un "[Amministratore della griglia di StorageGRID che utilizza il gestore della griglia](#)". Quando si crea un account tenant, l'amministratore della griglia specifica quanto segue:

- Informazioni di base, tra cui nome del tenant, tipo di client (S3) e quota di archiviazione opzionale.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione a federazione di griglie.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione di identità o SSO (Single Sign-on).

Inoltre, gli amministratori della griglia possono attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

Configurare i tenant S3

Dopo un "[Viene creato l'account tenant S3](#)", è possibile accedere a Tenant Manager per eseguire attività quali:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Usa la federazione di griglia per la sincronizzazione degli account e la replica tra griglie
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage



Anche se è possibile creare e gestire bucket S3 con Tenant Manager, è necessario utilizzare un **"Client S3"** oppure **"S3 Console"** per acquisire e gestire gli oggetti.

Come effettuare l'accesso e disconnettersi

Sign in a StorageGRID Tenant Manager

È possibile accedere a Tenant Manager immettendo l'URL del tenant nella barra degli indirizzi di un **"browser web supportato"**.

Prima di iniziare

- Si dispone delle credenziali di accesso.
- Si dispone di un URL per accedere a Tenant Manager, fornito dall'amministratore della griglia. L'URL sarà simile a uno dei seguenti esempi:

```
https://FQDN_or_Admin_Node_IP/
```

```
https://FQDN_or_Admin_Node_IP:port/
```

```
https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id
```

```
https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id
```

L'URL include sempre un nome di dominio completo (FQDN), l'indirizzo IP di un nodo amministrativo o l'indirizzo IP virtuale di un gruppo ha di nodi amministrativi. Potrebbe anche includere un numero di porta, l'ID dell'account tenant a 20 cifre o entrambi.

- Se l'URL non include l'ID account a 20 cifre del tenant, si dispone di questo ID account.
- Si sta utilizzando un **"browser web supportato"**.
- I cookie sono attivati nel browser Web.
- L'utente appartiene a un gruppo di utenti che dispone di **"autorizzazioni di accesso specifiche"**.

Fasi

1. Avviare un **"browser web supportato"**.
2. Nella barra degli indirizzi del browser, immettere l'URL per accedere a Tenant Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser.

4. Accedi al tenant manager.

La schermata di accesso che viene visualizzata dipende dall'URL immesso e dalla configurazione di SSO (Single Sign-on) per StorageGRID.

Non si utilizza SSO

Se StorageGRID non utilizza SSO, viene visualizzata una delle seguenti schermate:

- Pagina di accesso a Grid Manager. Selezionare il collegamento **accesso tenant**.
- La pagina di accesso del Tenant Manager. Il campo **Account** potrebbe essere già compilato.
 - i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.
 - ii. Immettere il nome utente e la password.
 - iii. Selezionare **Accedi**.

Viene visualizzata la dashboard di Tenant Manager.

- iv. Se hai ricevuto una password iniziale da un altro utente, seleziona **Username > Change password** per proteggere il tuo account.

Utilizzo di SSO

Se StorageGRID utilizza SSO, viene visualizzata una delle seguenti schermate:

- La pagina SSO della tua organizzazione.

Immettere le credenziali SSO standard e selezionare **Accedi**.
- La pagina di accesso SSO di Tenant Manager.
 - i. Se l'ID account a 20 cifre del tenant non viene visualizzato, selezionare il nome dell'account tenant, se visualizzato nell'elenco degli account recenti, oppure inserire l'ID account.
 - ii. Selezionare **Accedi**.
 - iii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Viene visualizzata la dashboard di Tenant Manager.

Sign out di StorageGRID Tenant Manager

Una volta terminato il lavoro con il tenant manager, devi disconnetterti per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Individuare il menu a discesa Username (Nome utente) nell'angolo in alto a destra dell'interfaccia utente.
2. Selezionare il nome utente, quindi selezionare **Disconnetti**.

- Se SSO non è in uso:

Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso del tenant manager.



Se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.

- Se SSO è attivato:

Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. Il nome dell'account tenant a cui hai appena effettuato l'accesso viene elencato come predefinito nell'elenco a discesa **account recenti** e viene visualizzato l'ID account* del tenant.



Se SSO è attivato e si è anche connessi a Grid Manager, è necessario disconnettersi da Grid Manager per disconnettersi da SSO.

Dashboard Tenant Manager in StorageGRID

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 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.



La dimensione logica di tutti gli oggetti appartenenti a questo tenant include caricamenti multiparte incompleti e in corso. Le dimensioni non includono lo spazio fisico aggiuntivo utilizzato per le policy ILM. 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 è simile al seguente esempio:

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 tenant

Nella parte superiore della dashboard viene indicato il numero di bucket o container configurati, gruppi e utenti. Visualizza inoltre il numero di endpoint dei servizi di piattaforma, se configurati. Selezionare i collegamenti per visualizzare i dettagli.

A seconda delle "autorizzazioni di gestione tenant" opzioni configurate e del tipo di dispositivo in uso, il resto della dashboard visualizza diverse combinazioni di linee guida, utilizzo dello storage, informazioni sugli oggetti e dettagli del tenant.

Utilizzo dello storage e delle quote

Il pannello Storage Use (utilizzo storage) contiene le seguenti informazioni:

- La quantità di dati oggetto per il tenant.

Questo valore indica la quantità totale di dati dell'oggetto caricati e non rappresenta lo spazio utilizzato per memorizzare le copie di tali oggetti e dei relativi metadati.

- Se viene impostata una quota, la quantità totale di spazio disponibile per i dati dell'oggetto e la quantità e la percentuale di spazio rimanente. La quota limita la quantità di dati oggetto che è possibile acquisire.



L'utilizzo delle quote si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla la quota quando un tenant avvia il caricamento degli oggetti e rifiuta le nuove ricerche se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se la quota è stata superata. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino a quando l'utilizzo della quota non viene ricalcolato. I calcoli relativi all'utilizzo delle quote possono richiedere 10 minuti o più.

- Un grafico a barre che rappresenta le dimensioni relative dei bucket o dei container più grandi.

È possibile posizionare il cursore su uno dei segmenti del grafico per visualizzare lo spazio totale consumato da quel bucket o container.



- Per corrispondere al grafico a barre, un elenco dei bucket o container più grandi, inclusa la quantità totale di dati oggetto e il numero di oggetti per ciascun bucket o container.

Bucket name	Space used	Number of objects
 Bucket-02	944.7 GB	7,575
 Bucket-09	899.6 GB	589,677
 Bucket-15	889.6 GB	623,542
 Bucket-06	846.4 GB	648,619
 Bucket-07	730.8 GB	808,655
 Bucket-04	700.8 GB	420,493
 Bucket-11	663.5 GB	993,729
 Bucket-03	656.9 GB	379,329
 9 other buckets	2.3 TB	5,171,588

Se il tenant ha più di nove bucket o container, tutti gli altri bucket o container vengono combinati in una singola voce in fondo all'elenco.



Per modificare le unità per i valori di storage visualizzati in Tenant Manager, selezionare il menu a discesa User (utente) in alto a destra in Tenant Manager, quindi selezionare **User preferences** (Preferenze utente).

Avvisi sull'utilizzo delle quote

Se gli avvisi sull'utilizzo delle quote sono stati attivati in Grid Manager, questi avvisi vengono visualizzati in Tenant Manager quando la quota è bassa o superata, come segue:

- Se è stato utilizzato il 90% o più della quota di un tenant, viene attivato l'avviso **quota di utilizzo elevata del tenant**.

Chiedere all'amministratore di rete di aumentare la quota.

- Se si supera la quota, una notifica informa che non è possibile caricare nuovi oggetti.

utilizzo limite di capacità

Se hai impostato un limite di capacità per i tuoi bucket, la dashboard di Tenant Manager visualizza un elenco dei bucket principali per utilizzo limite di capacità.

Se non viene impostato alcun limite per una benna, la sua capacità è illimitata. Tuttavia, se l'account tenant dispone di una quota di storage totale e tale quota viene raggiunta, non sarà possibile acquisire più oggetti indipendentemente dal limite di capacità rimanente in un bucket.

Errori degli endpoint

Se hai utilizzato Grid Manager per configurare uno o più endpoint da utilizzare con i servizi della piattaforma, la dashboard di Tenant Manager visualizza un avviso se si sono verificati errori degli endpoint negli ultimi sette giorni.

 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 "errori degli endpoint dei servizi della piattaforma" visualizzare i dettagli su , selezionare **punti finali** per visualizzare la pagina punti finali.

API di gestione del tenant

Scopri l'API di gestione dei tenant di StorageGRID

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Tenant Management invece dell'interfaccia utente di Tenant Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

L'API di gestione dei tenant:

- Utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di interagire con l'API. L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.
- Usi "versione per supportare aggiornamenti senza interruzioni".

Per accedere alla documentazione Swagger per l'API di gestione tenant:

1. Accedi al tenant manager.
2. Nella parte superiore di Tenant Manager, selezionare l'icona della guida e selezionare **documentazione API**.

Operazioni API

L'API di gestione tenant organizza le operazioni API disponibili nelle seguenti sezioni:

- **Account:** Operazioni sull'account tenant corrente, incluso il recupero delle informazioni sull'utilizzo dello storage.
- **Auth:** Operazioni per l'autenticazione della sessione utente.

L'API di gestione tenant supporta lo schema di autenticazione del token del bearer. Per un accesso tenant, è necessario fornire un nome utente, una password e un ID account nel corpo JSON della richiesta di autenticazione (ovvero, POST /api/v3/authorize). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("autorizzazione: Token portante").

Per informazioni sul miglioramento della protezione dell'autenticazione, vedere ["Protezione contro la falsificazione di richieste cross-site"](#).



Se per il sistema StorageGRID è attivato il Single Sign-on (SSO), è necessario eseguire diversi passaggi per l'autenticazione. Consultare la ["Istruzioni per l'utilizzo dell'API Grid Management"](#).

- **Config:** Operazioni relative alla release del prodotto e alle versioni dell'API di gestione tenant. È possibile elencare la versione di release del prodotto e le principali versioni dell'API supportate da tale release.
- **contenitori:** operazioni sui bucket S3.
- **Disattivato-funzioni:** Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **Endpoint:** Operazioni per gestire un endpoint. Gli endpoint consentono a un bucket S3 di utilizzare un servizio esterno per la replica, le notifiche o l'integrazione della ricerca di StorageGRID CloudMirror.
- **Grid-Federation-Connections:** Operazioni su connessioni di federazione di grid e replica cross-grid.
- **Groups:** Operazioni per gestire gruppi tenant locali e recuperare gruppi tenant federati da un'origine di identità esterna.
- **Identity-source:** Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm:** Operazioni sulle impostazioni ILM (Information Lifecycle Management).
- **Regioni:** Operazioni per determinare quali regioni sono state configurate per il sistema StorageGRID.
- **s3:** Operazioni per gestire le chiavi di accesso S3 per gli utenti del tenant.
- **s3-configurations:** Operazioni per recuperare le configurazioni globali di S3.
- **s3-Object-lock:** Operazioni sulle impostazioni globali S3 Object Lock, utilizzate per supportare la conformità alle normative.
- **Utenti:** Operazioni per visualizzare e gestire gli utenti del tenant.

Dettagli dell'operazione

Quando si espandono le operazioni API, è possibile visualizzare l'azione HTTP, l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.

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>

Emettere richieste API



Tutte le operazioni API eseguite utilizzando la pagina Web documentazione API sono operazioni in tempo reale. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Selezionare l'azione HTTP per visualizzare i dettagli della richiesta.
2. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
3. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.

4. Selezionare **Provalo**.
5. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
6. Selezionare **Esegui**.
7. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Versionamento dell'API di gestione dei tenant di StorageGRID

L'API di gestione tenant utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.



È possibile configurare le versioni supportate. Per ulteriori informazioni, vedere la sezione **config** della documentazione Swagger API "[API di Grid Management](#)". È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare la GET `/versions` richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione API utilizzando un parametro di percorso (`/api/v4`) o un'intestazione (`Api-Version: 4`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Proteggi contro gli attacchi Cross-Site Request Forgery in StorageGRID

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare il `csrfToken` parametro su `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 true, un `GridCsrfToken` cookie viene impostato con un valore casuale per i login al Grid Manager e il `AccountCsrfToken` cookie viene impostato con un valore casuale per i login al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- L'`X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo codificato in forma: Un `csrfToken` parametro del corpo della richiesta codificato in forma.

Per configurare la protezione CSRF, utilizzare ["API di Grid Management"](#) o ["API di gestione del tenant"](#).



Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione "Content-Type: Application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare connessioni di federazione di griglie

Sincronizza gruppi di tenant e utenti in StorageGRID

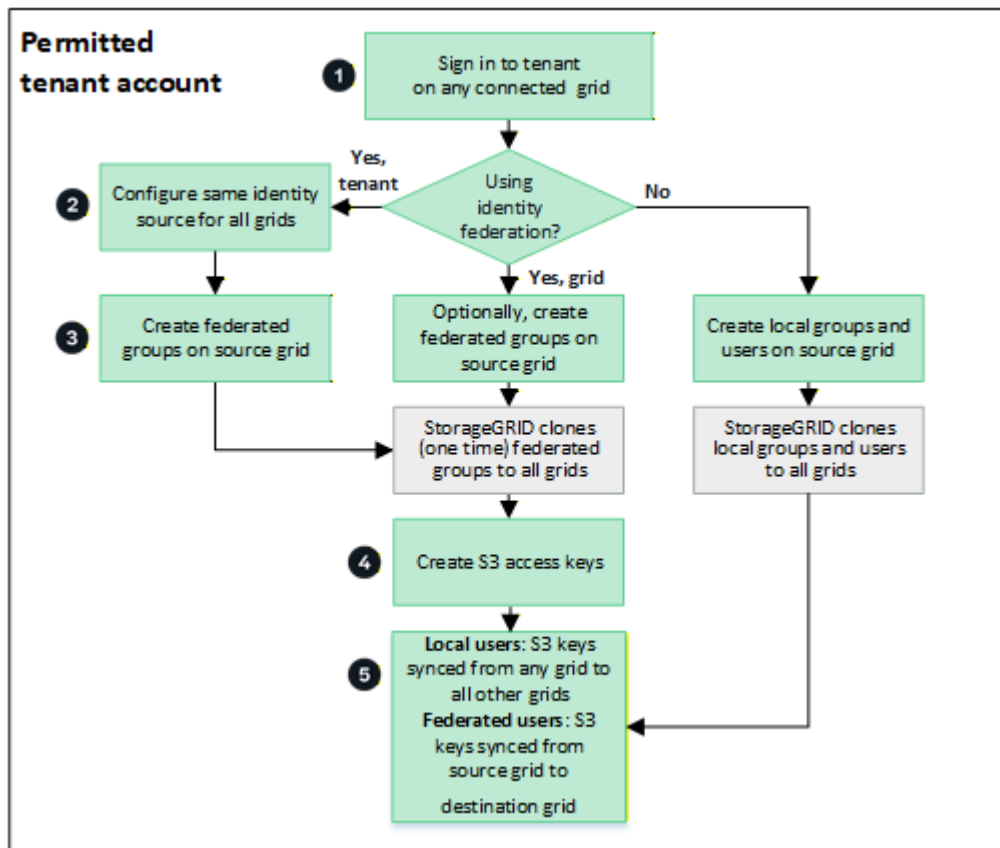
Se un tenant è stato creato o modificato per utilizzare connessioni di federazione grid, quel tenant viene replicato da un sistema StorageGRID (il tenant di origine) a tutti gli altri sistemi StorageGRID connessi (i tenant replica). Dopo che il tenant è stato replicato, i gruppi del tenant, gli utenti e le chiavi di accesso S3 vengono sincronizzati tra le griglie connesse.

Il sistema StorageGRID in cui il tenant viene originariamente creato è la *griglia sorgente* del tenant. Il tenant viene replicato su una o più *griglie di destinazione*. Gli account tenant su tutte le griglie connesse hanno lo stesso ID account, nome, descrizione, quota di storage, autorizzazioni assegnate e password dell'utente root. Per dettagli, consulta ["Scopri la sincronizzazione degli account per la federazione di griglie"](#) e ["Gestire i tenant autorizzati"](#).

La sincronizzazione delle informazioni dell'account del tenant è necessaria per ["replica cross-grid"](#) degli oggetti bucket. Avere gli stessi gruppi e utenti tenant su tutte le griglie garantisce che tu possa accedere ai bucket e agli oggetti corrispondenti su qualsiasi griglia connessa.

Flusso di lavoro del tenant per la sincronizzazione dell'account

Se il tuo tenant account dispone dell'autorizzazione **Use grid federation connection**, consulta il diagramma del flusso di lavoro per vedere quali passaggi eseguirai per sincronizzare gruppi, utenti e chiavi di accesso S3.



Questi sono i passaggi principali del flusso di lavoro:

1

Accedere al tenant

Accedi all'account tenant su qualsiasi grid connessa.

2

Facoltativamente, configurare la federazione delle identità

Se il tuo tenant account dispone dell'autorizzazione **Usa la tua origine di identità** per utilizzare gruppi e utenti federati, configura la stessa origine di identità (con le stesse impostazioni) per l'account tenant di origine e per uno o più account tenant di destinazione. I gruppi federati vengono clonati al momento della creazione e gli utenti federati vengono clonati quando viene creata una chiave. Affinché la clonazione avvenga, la stessa origine di identità deve essere configurata su tutte le grid. Per istruzioni, consulta ["USA la federazione delle identità"](#).

3

Creare gruppi e utenti

Puoi creare gruppi e utenti da qualsiasi grid connessa. Quando aggiungi un nuovo gruppo locale, StorageGRID lo sincronizza automaticamente con tutte le grid connesse. Anche le modifiche ai gruppi locali (modifica, eliminazione) vengono sincronizzate continuamente. I gruppi federati vengono clonati una sola volta al momento della creazione.

- Se la federazione delle identità è configurata per l'intero sistema StorageGRID o per l'account tenant, ["creare nuovi gruppi tenant"](#) importando gruppi federated dall'origine identità.
- Se non si utilizza la federazione delle identità, ["creare nuovi gruppi locali"](#) poi ["creare utenti locali"](#).

4

Creare S3 chiavi di accesso

Puoi ["creare le proprie chiavi di accesso"](#) o ["creare le chiavi di accesso di un altro utente"](#) su qualsiasi griglia per accedere ai bucket su tutte le griglie connesse.

5

Sincronizza le chiavi di accesso S3

Se devi accedere ai bucket con le stesse chiavi di accesso su tutte le griglie, crea le chiavi di accesso su una delle griglie. Per gli utenti locali, le chiavi di accesso vengono sincronizzate automaticamente per impostazione predefinita. Per gli utenti federati, devi creare le chiavi di accesso S3 sulla griglia di origine e selezionare **Abilita sincronizzazione chiavi di accesso** perché le chiavi vengano sincronizzate su tutte le griglie di destinazione.

Come vengono sincronizzati gruppi, utenti e chiavi di accesso S3?

Esamina questa sezione per capire come gruppi, utenti e chiavi di accesso S3 vengono sincronizzati tra le griglie connesse.

I gruppi locali vengono sincronizzati continuamente

Dopo che un account tenant è stato creato e replicato nella griglia di destinazione, StorageGRID sincronizza continuamente i gruppi locali su tutte le griglie connesse. Tutte le modifiche ai gruppi locali, incluse le operazioni di creazione, modifica ed eliminazione, effettuate su qualsiasi griglia vengono replicate automaticamente su tutte le altre griglie connesse.

Sia il gruppo originale che le sue copie sincronizzate hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e gli stessi criteri di gruppo S3. Per istruzioni, consulta ["Creare gruppi per il tenant S3"](#).

Gli utenti locali vengono sincronizzati continuamente

Quando crei un nuovo utente locale su una qualsiasi griglia connessa, StorageGRID sincronizza automaticamente quell'utente con tutte le altre griglie connesse. Anche le modifiche successive, incluse modifiche, eliminazioni e reimpostazioni della password, vengono sincronizzate continuamente. L'utente originale e le sue copie sincronizzate hanno lo stesso nome completo, nome utente e impostazione **Nega accesso**. Gli stessi utenti su ogni griglia appartengono anche agli stessi gruppi. Per istruzioni, consulta ["Gestire gli utenti"](#).

I gruppi federati vengono sincronizzati una sola volta durante la creazione

Supponendo che siano stati soddisfatti i requisiti per l'utilizzo della sincronizzazione dell'account con ["single sign-on"](#) e ["federazione delle identità"](#), i gruppi federati che crei (importi) per il tenant su una griglia vengono automaticamente sincronizzati con il tenant su tutte le altre griglie connesse.

Entrambi i gruppi hanno la stessa modalità di accesso, le stesse autorizzazioni di gruppo e gli stessi criteri di gruppo S3.

Una volta creati i gruppi federati per il tenant di origine e sincronizzati con altre griglie, gli utenti federati possono accedere al tenant su qualsiasi griglia connessa. Le modifiche successive ai gruppi federati non vengono sincronizzate automaticamente tra le griglie.

Le chiavi di accesso S3 possono essere sincronizzate automaticamente o manualmente

Per impostazione predefinita, StorageGRID sincronizza automaticamente le chiavi di accesso S3. Per motivi di sicurezza, puoi disabilitare la sincronizzazione automatica delle chiavi di accesso S3 per ciascun tenant e avere chiavi diverse per ogni tenant su ogni grid.

Per gestire le chiavi di accesso sulle griglie connesse, puoi fare una delle seguenti cose:

- Se non hai bisogno di usare le stesse chiavi per ogni grid, puoi disattivare la sincronizzazione automatica delle chiavi di accesso e ["creare le proprie chiavi di accesso"](#) o ["creare le chiavi di accesso di un altro utente"](#) su ogni grid.



Quando sincronizzi le chiavi di accesso S3 per un utente federato, sia l'utente che le chiavi di accesso S3 vengono sincronizzati con i tenant di destinazione.



Le chiavi di accesso S3 degli utenti locali vengono sincronizzate continuamente tra le griglie connesse, anche quando le chiavi vengono eliminate. Le chiavi di accesso S3 degli utenti federati vengono sincronizzate una sola volta al momento della creazione; le modifiche successive, incluse le eliminazioni, non vengono replicate. Puoi abilitare o disabilitare la sincronizzazione delle chiavi di accesso per ogni connessione tenant.

I gruppi e gli utenti aggiunti alla grid di destinazione vengono sincronizzati

Le modifiche apportate a qualsiasi griglia connessa, inclusa la creazione o l'importazione di gruppi e utenti locali, vengono sincronizzate automaticamente con tutte le altre griglie connesse.

I gruppi locali, gli utenti e le chiavi di accesso modificati o eliminati sono sincronizzati

Le modifiche apportate ai gruppi locali, agli utenti locali e alle chiavi di accesso S3 di proprietà degli utenti locali vengono sincronizzate continuamente su tutte le griglie connesse. Le operazioni sincronizzate includono modifiche, eliminazioni e reimpostazioni delle password.

Le modifiche apportate ai gruppi federati e alle chiavi di accesso S3 di proprietà degli utenti federati non vengono sincronizzate dopo la creazione iniziale.

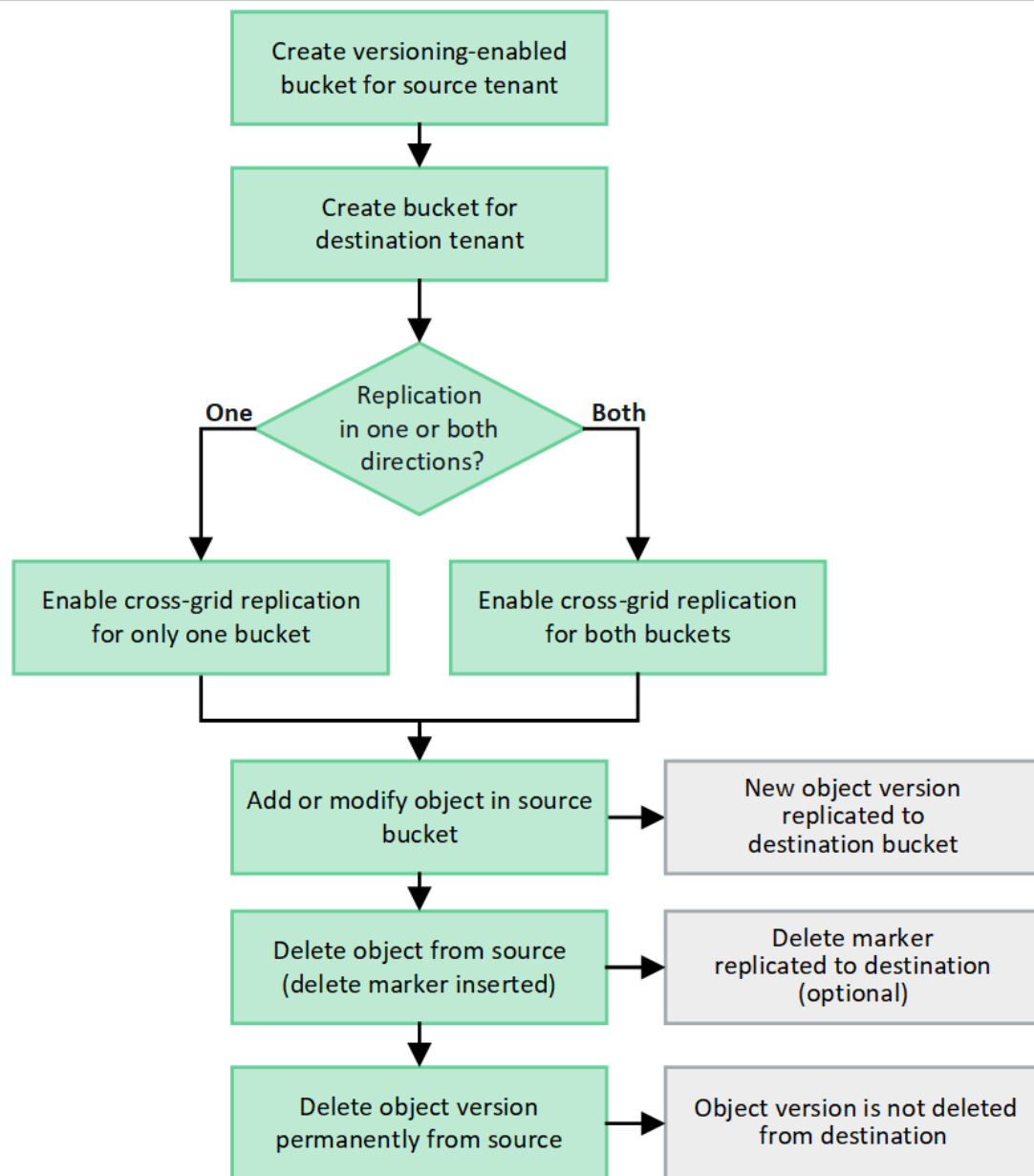
Gestisci la replica tra griglie in StorageGRID

Se all'account tenant è stata assegnata l'autorizzazione **Usa connessione federazione griglia** al momento della creazione, è possibile utilizzare la replica cross-grid per replicare automaticamente gli oggetti tra i bucket nella griglia di origine del tenant e i bucket nella griglia di destinazione del tenant. La replica cross-grid può avvenire in una o entrambe le direzioni.

Workflow per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi da eseguire per configurare la replica tra griglie tra bucket su due griglie. Questi passaggi sono descritti più dettagliatamente sotto il diagramma.

Tenant user



Configurare la replica cross-grid

Prima di poter utilizzare la replica tra griglie, è necessario accedere agli account tenant corrispondenti su ciascuna griglia e creare due bucket. 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. Fare riferimento a ["Che cos'è la replica cross-grid"](#).
- Stai usando un ["browser web supportato"](#).
- L'account tenant ha l'autorizzazione **Usa connessione federata di griglia** e su entrambe le griglie esistono account tenant identici. Fare riferimento a ["Gestire i tenant consentiti per la connessione a federazione di grid"](#).
- L'utente tenant con cui stai effettuando l'accesso esiste già su entrambe le griglie e appartiene a un gruppo di utenti che ha ["Autorizzazione di accesso root"](#).

- Se accedi alla griglia di destinazione del tenant come utente locale, l'utente root dell'account tenant ha impostato una password per il tuo account utente su quella griglia.

Crea due bucket

Come primo passo, accedi agli account tenant corrispondenti su ciascuna griglia e crea un bucket su ciascuna griglia.

Fasi

1. A partire da una delle due griglie della connessione a federazione di griglie, creare un nuovo bucket:
 - a. Accedere all'account tenant utilizzando le credenziali di un utente tenant presente in entrambe le griglie.

Se non 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 a ["Creare un bucket S3"](#).



I nomi dei bucket e le regioni possono essere diversi su ogni griglia.

- c. Nella scheda **Manage object settings** (Gestisci impostazioni oggetto), selezionare **Enable object versioning** (attiva versione oggetto).
 - d. Se S3 Object Lock è abilitato per il sistema StorageGRID , fare riferimento a ["Replicazione cross-grid con S3 Object Lock"](#) .
 - e. Selezionare **Crea bucket**.
 - f. Selezionare **fine**.
2. Ripetere questi passaggi per creare un bucket per lo stesso account tenant sull'altra griglia nella connessione di federazione della griglia.



Secondo necessità, ogni benna può utilizzare una regione diversa.

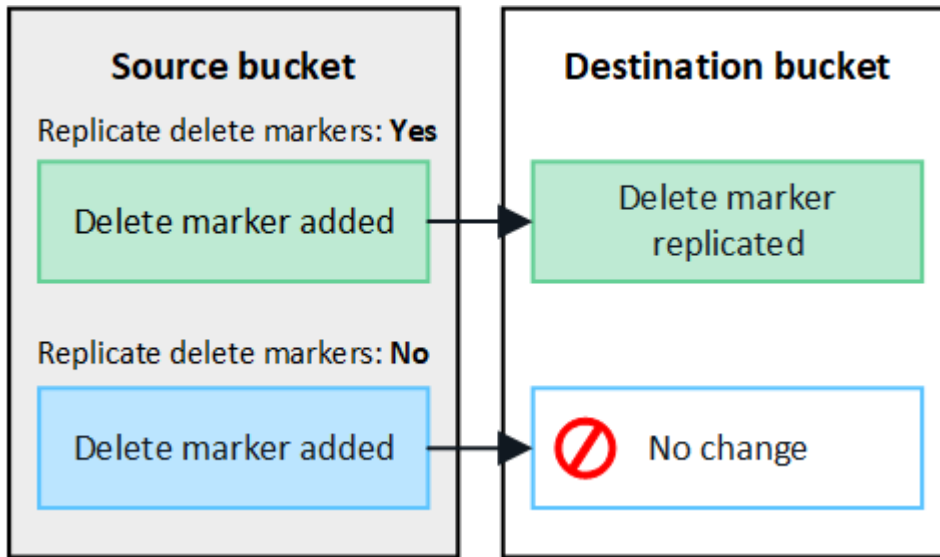
Abilitare la replica cross-grid

Fasi

1. A partire da una griglia di cui si desidera replicare gli oggetti, attivare ["replica cross-grid in un'unica direzione"](#):
 - a. Accedi all'account tenant per il bucket.
 - b. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
 - c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
 - d. Selezionare la scheda **Cross-grid Replication**.
 - e. Selezionare **Enable** (attiva) ed esaminare l'elenco dei requisiti.
 - f. Se tutti i requisiti sono stati soddisfatti, selezionare la connessione a federazione di griglia che si desidera utilizzare.
 - g. Facoltativamente, modificare l'impostazione di **Replicate delete markers** per determinare cosa accade nella griglia di destinazione se un client S3 invia una richiesta di eliminazione alla griglia di

origine che non include un ID di versione:

- **Sì** (impostazione predefinita): Un marcatore di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione.
- **No**: un marcatore di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione.



Se la richiesta di eliminazione include un ID 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.

Fare riferimento a ["Che cos'è la replica cross-grid"](#) per i dettagli.

- In alternativa, modificare l'impostazione della categoria di controllo **Cross-Grid Replication** per gestire il volume dei messaggi di controllo:
 - **Errore** (impostazione predefinita): Solo le richieste di replica cross-grid non riuscite sono incluse nell'output di controllo.
 - **Normale**: Sono incluse tutte le richieste di replica cross-grid, il che aumenta significativamente il volume dell'output di controllo.

- Selezionare **Enable (attiva) e test**.

Dopo qualche istante, verrà visualizzato un messaggio di conferma dell'operazione. Gli oggetti aggiunti a questo bucket vengono ora replicati automaticamente nell'altra griglia. **La replica tra griglie** è visualizzata come funzionalità abilitata nella pagina dei dettagli del bucket.

- Facoltativamente, passare al bucket corrispondente sull'altra griglia e ["abilitare la replica cross-grid in entrambe le direzioni"](#).

Test di replica tra griglie

Se la replica cross-grid è attivata per un bucket, potrebbe essere necessario verificare che la connessione e la replica cross-grid funzionino correttamente e che i bucket di origine e di destinazione soddisfino ancora tutti i requisiti (ad esempio, il controllo delle versioni è ancora attivato).

Prima di iniziare

- Stai usando un ["browser web supportato"](#) .
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Accedi all'account tenant per il bucket.
2. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
3. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
4. Selezionare la scheda **Cross-grid Replication**.
5. Selezionare **Test di connessione**.

Se la connessione è 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 i dettagli, fare riferimento a ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

6. Se la replica cross-grid è configurata per avvenire in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e selezionare **Test Connection** per verificare che la replica cross-grid funzioni nell'altra direzione.

Disattiva la replica cross-grid

Se non si desidera più copiare gli oggetti nell'altra griglia, è possibile interrompere in modo permanente la replica tra griglie.

Prima di disattivare la replica cross-grid, tenere presente quanto segue:

- La disattivazione della replica tra griglie non rimuove gli oggetti che sono già stati 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 cross-grid è stata attivata per ciascuno dei bucket (ovvero, se la replica si verifica in entrambe le direzioni), è possibile disattivare la replica cross-grid per uno o entrambi i bucket. Ad esempio, è possibile disattivare la replica degli oggetti da `my-bucket` sulla griglia 1 a `my-bucket` sulla griglia 2, continuando a replicare gli oggetti da `my-bucket` sulla griglia 2 a `my-bucket` sulla griglia 1.
- È necessario disabilitare la replica tra griglie prima di poter rimuovere l'autorizzazione di un tenant a utilizzare la connessione federata della griglia. Fare riferimento a ["Gestire i tenant autorizzati"](#) .

Prima di iniziare

- Stai usando un ["browser web supportato"](#) .
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Partendo dalla griglia di cui non si desidera più replicare gli oggetti, interrompere la replica cross-grid per il bucket:
 - a. Accedi all'account tenant per il bucket.
 - b. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

- c. Selezionare il nome del bucket dalla tabella per accedere alla pagina dei dettagli del bucket.
- d. Selezionare la scheda **Cross-grid Replication**.
- e. Selezionare **Disable Replication** (Disattiva replica).
- f. Se sei sicuro di voler disabilitare la replica tra griglie per questo bucket, digita **Sì** nella casella di testo e seleziona **Disabilita**.

Dopo alcuni istanti, viene visualizzato un messaggio di successo. I nuovi oggetti aggiunti a questo bucket non possono più essere replicati automaticamente nell'altra griglia. **La replica cross-grid** non viene più visualizzata come funzione abilitata nella pagina bucket.

2. Se la replica cross-grid è stata configurata per avvenire in entrambe le direzioni, passare al bucket corrispondente sull'altra griglia e interrompere la replica cross-grid nell'altra direzione.

Visualizza le connessioni di federazione della griglia in StorageGRID

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile visualizzare le connessioni consentite.

Prima di iniziare

- L'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**.
- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).

Fasi

1. Selezionare **STORAGE (S3) > Grid Federation Connections**.

Viene visualizzata la pagina Grid Federation Connection (connessione federazione griglia) che include una tabella che riepiloga le seguenti informazioni:

Colonna	Descrizione
Nome della connessione	Le connessioni della federazione di griglie che il tenant dispone dell'autorizzazione per l'utilizzo.
Bucket con replica cross-grid	Per ogni connessione a federazione di grid, i bucket tenant con replica cross-grid attivata. Gli oggetti aggiunti a questi bucket verranno replicati nell'altra griglia della connessione.
Ultimo errore	Per ogni connessione a federazione di griglie, si verifica l'errore più recente, se presente, quando i dati venivano replicati nell'altra griglia. Vedere Eliminare l'ultimo errore .

2. Facoltativamente, selezionare un nome bucket in ["visualizza i dettagli del bucket"](#).

Cancella l'ultimo errore

Nella colonna **ultimo errore** potrebbe essere visualizzato un errore per uno dei seguenti motivi:

- Versione dell'oggetto di origine non trovata.

- Bucket di origine non trovato.
- Il bucket di destinazione è stato cancellato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il bucket di destinazione ha la versione sospesa.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più disponibile.



In questa colonna viene visualizzato solo l'ultimo errore di replica tra griglie; gli errori precedenti che potrebbero essere stati rilevati non verranno visualizzati.

Fasi

1. Se nella colonna **ultimo errore** viene visualizzato un messaggio, visualizzare il testo del messaggio.

Ad esempio, questo errore indica che il bucket di destinazione per la replica cross-grid era in uno stato non valido, probabilmente perché il controllo delle versioni era stato sospeso o S3 Object Lock era attivato.

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 le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso nel bucket di destinazione per la replica cross-grid, riabilitare il controllo delle versioni per quel bucket.
3. Selezionare la connessione dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.



Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

7. Per determinare se alcuni oggetti non sono stati replicati a causa dell'errore bucket, vedere ["Identificare e riprovare le operazioni di replica non riuscite"](#).

Gestire gruppi e utenti

Usa la federazione delle identità in StorageGRID

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti tenant e consente agli utenti tenant di accedere all'account tenant utilizzando

credenziali familiari.

Configurare la federazione delle identità per Tenant Manager

È possibile configurare la federazione delle identità per Tenant Manager se si desidera che i gruppi e gli utenti dei tenant vengano gestiti in un altro sistema, ad esempio Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager tramite un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).
- Stai utilizzando Active Directory, Microsoft Entra ID, 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 intende utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere [Linee guida per la configurazione del server OpenLDAP](#).
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3. Vedere ["Crittografia supportata per le connessioni TLS in uscita"](#).

A proposito di questa attività

La possibilità di configurare un servizio di federazione delle identità per il tenant dipende dalla configurazione dell'account tenant. Il tenant potrebbe condividere il servizio di federazione delle identità configurato per Grid Manager. Se viene visualizzato questo messaggio quando si accede alla pagina Identity Federation, non è possibile configurare un'origine di identità federata separata per questo tenant.



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.

Inserire la configurazione

Quando si configura Identify Federation, vengono forniti i valori necessari a StorageGRID per connettersi a un servizio LDAP.

Fasi

1. Selezionare **Gestione accessi > Federazione identità**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.

LDAP service type

Select the type of LDAP service you want to configure.

Active Directory	Entra ID	OpenLDAP	Other

Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
- **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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `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 stai configurando Oracle Directory Server, inserisci `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, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
- **Nome host:** Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
 - **Port (porta):** Porta utilizzata per la connessione al server LDAP.



La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

- **Username:** Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName` o `uid`
- `objectGUID`, `entryUUID` o `nsuniqueid`

- `cn`
 - `memberOf o. isMemberOf`
 - **Active Directory:** `objectSid, primaryGroupID, userAccountControl E userPrincipalName`
 - **ID di ingresso:** `accountEnabled E userPrincipalName`
- **Password:** La password associata al nome utente.



Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

- **DN base gruppo:** Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (`DC=storagegrid,DC=example,DC=com`) possono essere utilizzati come gruppi federati.



I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

- **User base DN:** Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.



I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

- **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (ID AD e Entra):** `[USERNAME]@example.com`
- **Modello di nome di accesso di livello inferiore (ID AD e Entra):** `example\[USERNAME]`
- **Modello di nome distinto:** `CN=[USERNAME],CN=Users,DC=example,DC=com`

Includi **[NOME UTENTE]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.

- **Usa STARTTLS:** 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 Microsoft Entra ID.
- **Usa LDAPS:** l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Microsoft Entra ID.
- **Non utilizzare TLS:** il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.



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 si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo:** Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

Fasi

1. Selezionare **Test di connessione**.
2. Se non hai fornito un formato di nome utente di associazione:
 - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
 - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.

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

myusername

The username of a federated user.

Test password

Cancel Test Connection

- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.

- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.



L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione 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.

A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non 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 lo stato Single Sign-On (SSO) è **Abilitato** o **Modalità sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere ["Disattiva single sign-on"](#).

Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

Linee guida per la configurazione del server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.



Per le origini identità che non sono Active Directory o Microsoft Entra ID, 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.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, vedere le istruzioni per la manutenzione dell'appartenenza al gruppo inverso nella ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#).

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Vedere le informazioni sulla manutenzione dell'appartenenza al gruppo inverso nella ["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#).

Gestire i gruppi di tenant

Creare gruppi per un tenant S3 in StorageGRID

È possibile gestire le autorizzazioni per i gruppi di utenti S3 importando gruppi federati o creando gruppi locali.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).
- Se si prevede di importare un gruppo federated, si dispone di ["federazione di identità configurata"](#), e il gruppo Federated esiste già nell'origine identità configurata.
- Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni relative a ["sincronizzazione di gruppi di tenant e utenti"](#) e hai effettuato l'accesso alla grid di origine del tenant.

Accedere alla procedura guidata Crea gruppo

Come prima fase, accedere alla procedura guidata Crea gruppo.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

Fasi

1. Selezionare la scheda **Local group** (Gruppo locale) per creare un gruppo locale oppure la scheda **Federated group** (Gruppo federato) per importare un gruppo dall'origine dell'identità precedentemente configurata.

Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID, gli utenti appartenenti a gruppi locali non potranno accedere a Gestione tenant, anche se possono utilizzare le applicazioni client per gestire le risorse del tenant, in base alle autorizzazioni di gruppo.

2. Inserire il nome del gruppo.

- **Local group** (Gruppo locale): Immettere un nome visualizzato e un nome univoco. È possibile modificare il nome visualizzato in un secondo momento.



Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, si verificherà un errore di clonazione se lo stesso **nome univoco** esiste già per il tenant nella griglia di destinazione.

- **Federated group**: Immettere il nome univoco. Per Active Directory, il nome univoco è il nome associato all' `sAMAccountName` attributo. Per OpenLDAP, il nome univoco è il nome associato all' `uid` attributo.

3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Le autorizzazioni di gruppo controllano le attività che gli utenti possono eseguire nelle API di gestione tenant e tenant Manager.

Fasi

1. Per la modalità **Access**, selezionare una delle seguenti opzioni:
 - **Read-write** (valore predefinito): Gli utenti possono accedere a Tenant Manager e gestire la configurazione del tenant.
 - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API di gestione tenant Manager o tenant. Gli utenti locali di sola lettura possono modificare le proprie password.



Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

2. Selezionare una o più autorizzazioni per questo gruppo.

Vedere "[Permessi di gestione del tenant](#)".

3. Selezionare **continua**.

Impostare i criteri di gruppo S3

I criteri di gruppo determinano le autorizzazioni di accesso S3 che gli utenti avranno.

Fasi

1. Selezionare il criterio che si desidera utilizzare per questo gruppo.

Policy di gruppo	Descrizione
Nessun accesso S3	Predefinito. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
Accesso in sola lettura	Gli utenti di questo gruppo hanno accesso in sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
Accesso completo	Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
Riduzione del ransomware	Questo criterio di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti. Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.
Personalizzato	Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

- Se si seleziona **Custom**, inserire il criterio di gruppo. Ogni policy di gruppo ha un limite di dimensione di 5,120 byte. Immettere una stringa valida formattata con JSON.

Per informazioni dettagliate sui criteri di gruppo, incluse la sintassi del linguaggio e gli esempi, vedere ["Criteri di gruppo di esempio"](#).

- Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo e fine**.

Aggiunta di utenti (solo gruppi locali)

È possibile salvare il gruppo senza aggiungere utenti oppure aggiungere utenti locali già esistenti.

Fasi

- Facoltativamente, selezionare uno o più utenti locali per questo gruppo.
- Selezionare **Crea gruppo e fine**.

Il gruppo creato viene visualizzato nell'elenco dei gruppi.

Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo gruppo viene sincronizzato con la griglia di destinazione del tenant. **Riuscito** appare come stato di sincronizzazione nella sezione Panoramica della pagina dei dettagli del gruppo.

Autorizzazioni di gestione del tenant StorageGRID

Prima di creare un gruppo tenant, prendere in considerazione le autorizzazioni che si desidera assegnare a tale gruppo. Le autorizzazioni di gestione del tenant determinano le attività che gli utenti possono eseguire utilizzando il tenant Manager o l'API di gestione del tenant. Un utente può appartenere a uno o più gruppi. Le autorizzazioni sono cumulative se un utente appartiene a più gruppi.

Per accedere a tenant Manager o utilizzare l'API di gestione tenant, gli utenti devono appartenere a un gruppo che dispone di almeno un'autorizzazione. Tutti gli utenti che possono accedere possono eseguire le seguenti operazioni:

- Visualizza la dashboard
- Modificare la propria password (per gli utenti locali)

Per tutte le autorizzazioni, l'impostazione della modalità di accesso del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità.



Se un utente appartiene a più gruppi e un gruppo è impostato su sola lettura, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzioni selezionate.

È possibile assegnare le seguenti autorizzazioni a un gruppo.

Permesso	Descrizione	Dettagli
Accesso root	Fornisce l'accesso completo al tenant Manager e all'API di gestione del tenant.	
Gestisci le tue credenziali S3	Consente agli utenti di creare e rimuovere le proprie chiavi di accesso S3.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu STORAGE (S3) > My S3 access keys .
Visualizza tutti i bucket	Consente agli utenti di visualizzare tutti i bucket e le relative configurazioni.	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 bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.

Permesso	Descrizione	Dettagli
Gestire tutti i bucket	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.	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 bucket S3 o sui criteri di gruppo utilizzati dai client S3 o dalla console S3.
Gestire gli endpoint	Consente agli utenti di utilizzare il gestore tenant o l'API di gestione tenant per creare o modificare gli endpoint del servizio della piattaforma, che vengono utilizzati come destinazione per i servizi della piattaforma StorageGRID.	Gli utenti che non dispongono di questa autorizzazione non visualizzano l'opzione di menu Platform Services Endpoint .
Utilizzare la scheda Console S3	Se combinato con l'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket, consente agli utenti di visualizzare e gestire gli oggetti dalla scheda Console S3 nella pagina dei dettagli di un bucket.	

Gestisci i gruppi tenant di StorageGRID

Gestire i gruppi di tenant in base alle esigenze per visualizzare, modificare o duplicare un gruppo e altro ancora.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).

Visualizzare o modificare il gruppo

È possibile visualizzare e modificare le informazioni di base e i dettagli di ciascun gruppo.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Consultare le informazioni fornite nella pagina gruppi, che elenca le informazioni di base per tutti i gruppi locali e federati per questo account tenant.

Se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si stanno visualizzando i gruppi nella griglia di origine del tenant:

- Se alcuni gruppi non sono stati sincronizzati con il tenant sulla grid di destinazione, segui i passaggi per [riprova la sincronizzazione di gruppo](#).
3. Se si desidera modificare il nome del gruppo:
 - a. Selezionare la casella di controllo del gruppo.

- b. Selezionare **azioni > Modifica nome gruppo**.
 - c. Inserire il nuovo nome.
 - d. Selezionare **Salva modifiche**.
4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:
 - Selezionare il nome del gruppo.
 - Selezionare la casella di controllo relativa al gruppo e selezionare **azioni > Visualizza dettagli gruppo**.
5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun gruppo:
 - Nome visualizzato
 - Nome univoco
 - Tipo
 - Modalità di accesso
 - Permessi
 - Policy S3
 - Numero di utenti in questo gruppo
 - Ulteriori campi se l'account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** e si sta visualizzando il gruppo nella griglia di origine del tenant:
 - Stato della sincronizzazione, **Riuscita o Non riuscita**
 - Per i gruppi federati, un banner blu indica che se modifichi o elimini questo gruppo, le modifiche non verranno sincronizzate con l'altra griglia.
6. Modificare le impostazioni del gruppo secondo necessità. Fare riferimento a "[Creare gruppi per un tenant S3](#)" per i dettagli su cosa inserire.
 - a. Nella sezione Panoramica, modifica il nome visualizzato selezionando il nome o l'icona di modifica .
 - b. Nella scheda **permessi di gruppo**, aggiornare le autorizzazioni e selezionare **Salva modifiche**.
 - c. Nella scheda **Criteri di gruppo**, apportare le modifiche desiderate e selezionare **Salva modifiche**.

Facoltativamente, selezionare un criterio di gruppo S3 diverso o immettere la stringa JSON per un criterio personalizzato, a seconda delle necessità.
7. Per aggiungere uno o più utenti locali al gruppo:
 - a. Selezionare la scheda Users (utenti).

Manage users

You can add users to this group or remove users from this group.

Displaying one result

Username ⓘ	Full name ⓘ	Denied access ⓘ
User_02	User_02_Managers	No

- b. Selezionare **Aggiungi utenti**.
 - c. Selezionare gli utenti che si desidera aggiungere e selezionare **Aggiungi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

8. Per rimuovere utenti locali dal gruppo:

- a. Selezionare la scheda Users (utenti).
- b. Selezionare **Rimuovi utenti**.
- c. Selezionare gli utenti che si desidera rimuovere e selezionare **Rimuovi utenti**.

In alto a destra viene visualizzato il messaggio Success (operazione riuscita).

9. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Gruppo duplicato

È possibile duplicare un gruppo esistente per creare nuovi gruppi più rapidamente.



Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e duplichi un gruppo dalla griglia di origine del tenant, il gruppo duplicato verrà sincronizzato con la griglia di destinazione del tenant.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Selezionare la casella di controllo del gruppo che si desidera duplicare.
3. Selezionare **azioni > Duplica gruppo**.
4. Vedere ["Creare gruppi per un tenant S3"](#) per i dettagli su cosa inserire.
5. Selezionare **Crea gruppo**.

Riprova la sincronizzazione del gruppo

Se la sincronizzazione di un gruppo non riesce, nella colonna Stato di sincronizzazione del gruppo viene visualizzato "Non riuscito". Sopra la tabella viene visualizzato un banner per indicare che uno o più gruppi non sono riusciti a sincronizzarsi.

Fasi

Per riprovare la sincronizzazione:

1. Nel banner, seleziona **Riprova sync**. Questa operazione riprova la sincronizzazione per tutti i gruppi che non sono riusciti a sincronizzarsi.
2. Per riprovare a sincronizzare un singolo gruppo, seleziona il nome del gruppo. Nella pagina dei dettagli del gruppo, seleziona **Riprova sync**.
3. Visualizza lo stato dell'operazione di sincronizzazione dalla pagina dei dettagli di ogni gruppo che stai sincronizzando.

Se il nuovo tentativo ha esito positivo, nella colonna Stato di sincronizzazione per ciascun gruppo sincronizzato correttamente compare la dicitura "Riuscito" e il banner scompare.

Per ulteriori informazioni, vedi ["Sincronizza gruppi di tenant e utenti"](#).

Eliminare uno o più gruppi

È possibile eliminare uno o più gruppi. Gli utenti che appartengono solo a un gruppo cancellato non potranno più accedere al tenant manager o utilizzare l'account tenant.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Selezionare la casella di controllo per ciascun gruppo che si desidera eliminare.
3. Selezionare **azioni > Elimina gruppo** o **azioni > Elimina gruppi**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete group** (Elimina gruppo) o **Delete groups** (Elimina gruppi).

Imposta AssumeRole

Prima di iniziare

Per configurare AssumeRole devi essere un amministratore.

A proposito di questa attività

Per impostare AssumeRole, creare il gruppo di destinazione da assumere, se il gruppo non esiste già. Modificare i criteri S3 del gruppo per specificare le azioni consentite per l'assunzione di questo gruppo. Modificare i criteri di attendibilità S3 del gruppo per specificare gli utenti attendibili autorizzati ad assumere il ruolo del gruppo con l'API AssumeRole.

Credenziali di sicurezza temporanee create presupponendo che questo gruppo sia valido per una durata limitata. La sessione dura tra 15 minuti e 12 ore e la sessione predefinita è di 1 ora. Quando si rimuove l'utente dai criteri di attendibilità S3 del gruppo, l'utente non può più assumere questo gruppo.

Fasi

1. Selezionare **Gestione accessi > Gruppi**.
2. Selezionare il nome del gruppo.
3. Selezionare la scheda **Criterio di attendibilità S3**.
4. Aggiungi i tuoi criteri di attendibilità S3, incluso un elenco di utenti che possono eseguire AssumeRole.
5. Selezionare **Save Changes** (Salva modifiche).
6. Selezionare la scheda **Criteri di gruppo S3**.
7. Modificare il criterio S3 per specificare solo le azioni S3 richieste per gli utenti attendibili aggiunti nel criterio di attendibilità S3 di questo gruppo.
8. Selezionare **Save Changes** (Salva modifiche).

Esempio di una policy di trust AssumeRole S3

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "sts:AssumeRole",
      "Principal": {
        "AWS": [
          "urn:sgws:identity::1234567890:user/user1",
          "arn:aws:iam::1234567890:user/user2"
        ]
      }
    }
  ]
}
```

Il Principal:

- `"Principal": ""` corrisponde a tutti, comprese le richieste anonime (non firmate)
- `"Principal": { "AWS": "" }` corrisponde a qualsiasi identità o utente autenticato (non corrisponde alle richieste anonime)
- Si applica solo alle bucket policy
- Il principal è l'account/gli account/gli utenti a cui vengono concesse o negate le autorizzazioni

Una volta completata la configurazione, gli utenti elencati nei criteri di attendibilità S3 possono eseguire AssumeRole e ricevere le credenziali. Le autorizzazioni finali sono determinate dai criteri di gruppo, dai criteri del bucket e dai criteri di sessione. Per ulteriori informazioni, consultare ["Utilizzare le policy di accesso"](#).

Gestisci utenti tenant di StorageGRID

Puoi creare utenti locali e assegnarli a gruppi locali per determinare a quali funzionalità questi utenti possono accedere. Puoi anche importare utenti federati. Il Tenant Manager include un utente locale predefinito, chiamato *root*. Anche se puoi aggiungere e rimuovere utenti locali, non puoi rimuovere l'utente root.



Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID, gli utenti locali non potranno accedere al Tenant Manager o all'API di gestione del tenant, anche se possono usare le applicazioni client per accedere alle risorse del tenant, in base alle autorizzazioni di gruppo.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).
- Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia**, hai esaminato il flusso di lavoro e le considerazioni relative a ["sincronizzazione di gruppi di tenant e utenti"](#) e hai effettuato l'accesso alla grid di origine del tenant.

Crea un utente locale

È possibile creare un utente locale e assegnarlo a uno o più gruppi locali per controllarne le autorizzazioni di accesso.

Gli utenti S3 che non appartengono a nessun gruppo non dispongono di autorizzazioni di gestione o criteri di gruppo S3 applicati. Questi utenti potrebbero avere accesso al bucket S3 concesso tramite una policy bucket.

Accedere alla procedura guidata Crea utente

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Selezionare **Crea utente**.

Immettere le credenziali

Fasi

1. Per il passo **inserire le credenziali utente**, completare i seguenti campi.

Campo	Descrizione
Nome completo	Il nome completo dell'utente, ad esempio il nome e il cognome di una persona o il nome di un'applicazione.
Nome utente	Il nome utilizzato dall'utente per l'accesso. I nomi utente devono essere univoci e non possono essere modificati. Nota: Se l'account tenant dispone dell'autorizzazione Usa connessione federazione griglia , si verificherà un errore di clonazione se lo stesso Nome utente esiste già per il tenant nella griglia di destinazione.
Password e Conferma password	La password che l'utente utilizzerà inizialmente al momento dell'accesso.
Negare l'accesso	Selezionare Sì per impedire a questo utente di accedere all'account tenant, anche se potrebbe ancora appartenere a uno o più gruppi. Ad esempio, selezionare Sì per sospendere temporaneamente la possibilità di accesso dell'utente.

2. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Assegnare l'utente a uno o più gruppi locali per determinare quali attività possono eseguire.

L'assegnazione di un utente ai gruppi è facoltativa. Se preferisci, puoi selezionare gli utenti quando crei o modifichi i gruppi.

Gli utenti che non appartengono a nessun gruppo non disporranno di autorizzazioni di gestione. Le autorizzazioni sono cumulative. Gli utenti disporranno di tutte le autorizzazioni per tutti i gruppi a cui

appartengono. Vedere ["Permessi di gestione del tenant"](#).

2. Selezionare **Crea utente**.

Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e ti trovi sulla griglia di origine del tenant, il nuovo utente locale viene sincronizzato con la griglia di destinazione del tenant. **Riuscito** appare come **Stato di sincronizzazione** nella sezione Panoramica della pagina dei dettagli dell'utente.

3. Selezionare **fine** per tornare alla pagina utenti.

Visualizzare o modificare l'utente locale

Fasi

1. Selezionare **Gestione accessi > Utenti**.

2. Consultare le informazioni fornite nella pagina utenti, che elenca le informazioni di base per tutti gli utenti locali e federati per questo account tenant.

3. Se si desidera modificare il nome completo dell'utente:

- Selezionare la casella di controllo dell'utente.
- Selezionare **azioni > Modifica nome completo**.
- Inserire il nuovo nome.
- Selezionare **Salva modifiche**.

4. Se si desidera visualizzare ulteriori dettagli o apportare modifiche aggiuntive, effettuare una delle seguenti operazioni:

- Selezionare il nome utente.
- Selezionare la casella di controllo dell'utente e selezionare **azioni > Visualizza dettagli utente**.

5. Consultare la sezione Panoramica, che mostra le seguenti informazioni per ciascun utente:

- Nome completo
- Nome utente
- Tipo di utente
- Accesso negato
- Modalità di accesso
- Appartenenza al gruppo

6. Modificare le impostazioni utente in base alle esigenze. Vedere [Creare un utente locale](#) per i dettagli su cosa immettere.

- Nella sezione Panoramica, modifica il nome completo selezionando il nome o l'icona di modifica .

Impossibile modificare il nome utente.

- Nella scheda **Password**, modificare la password dell'utente e selezionare **Salva modifiche**.

- Nella scheda **accesso**, selezionare **No** per consentire all'utente di accedere o selezionare **Sì** per impedire all'utente di accedere. Quindi, selezionare **Salva modifiche**.

- Nella scheda **tasti di accesso**, selezionare **Crea tasto** e seguire le istruzioni per ["Creazione delle chiavi di accesso S3 di un altro utente"](#).

- Nella scheda **gruppi**, selezionare **Modifica gruppi** per aggiungere l'utente ai gruppi o rimuoverlo dai

gruppi. Quindi, selezionare **Save Changes** (Salva modifiche).

7. Confermare di aver selezionato **Save Changes** (Salva modifiche) per ciascuna sezione modificata.

Importa utenti federati

È possibile importare uno o più utenti federati, fino a un massimo di 100 utenti, direttamente nella pagina Utenti.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Seleziona **Importa utenti federati**.
3. Inserisci l'UUID o il nome utente di uno o più utenti federati.

Per voci multiple, aggiungere ogni UUID o nome utente su una nuova riga.

4. Selezionare **Importa**.

Se l'importazione nel campo Utenti non riesce per uno o più utenti, procedere come segue:

- a. Espandi **Utenti non importati** e seleziona **Copia utenti**.
- b. Riprovare l'importazione selezionando **Precedente** e incollando gli utenti copiati nella finestra di dialogo **Importa utenti federati**.

Dopo aver chiuso la finestra di dialogo **Importa utenti federati**, le informazioni sugli utenti federati vengono visualizzate nella pagina Utenti per gli utenti importati correttamente.

Utente locale duplicato

È possibile duplicare un utente locale per creare un nuovo utente più rapidamente.



Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione griglia** e duplichi un utente dalla griglia di origine del tenant, l'utente duplicato verrà sincronizzato con la griglia di destinazione del tenant.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Selezionare la casella di controllo dell'utente che si desidera duplicare.
3. Selezionare **azioni > utente duplicato**.
4. Vedere [Creare un utente locale](#) per i dettagli su cosa immettere.
5. Selezionare **Crea utente**.

Riprova la sincronizzazione utente

Se la sincronizzazione di un utente non riesce, nella colonna Stato di sincronizzazione per quell'utente viene visualizzato "Non riuscito". Sopra la tabella viene visualizzato un banner per indicare che uno o più utenti non sono riusciti a sincronizzarsi.

Fasi

Per riprovare la sincronizzazione:

1. Nel banner, seleziona **Riprova sync**. Questa operazione riprova la sincronizzazione per tutti gli utenti che non sono riusciti a sincronizzarsi.
2. Per riprovare a sincronizzare un singolo utente, seleziona il nome utente. Nella pagina dei dettagli dell'utente, seleziona **Riprova sync**.
3. Visualizza lo stato dell'operazione di sincronizzazione dalla pagina dei dettagli di ogni utente che stai sincronizzando.

Se il nuovo tentativo ha esito positivo, nella colonna Stato di sincronizzazione per ciascun utente sincronizzato correttamente compare la dicitura "Riuscito" e il banner scompare.

Per ulteriori informazioni, vedi ["Sincronizza gruppi di tenant e utenti"](#).

Eliminare uno o più utenti locali

È possibile eliminare in modo permanente uno o più utenti locali che non hanno più bisogno di accedere all'account tenant StorageGRID.



Se il tuo tenant account dispone dell'autorizzazione **Usa connessione di federazione grid** e elimini un utente locale, StorageGRID eliminerà l'utente corrispondente anche sulle altre griglie della connessione, a meno che tale utente non sia un utente federato su una griglia di destinazione. Devi usare l'origine di identità federata per eliminare gli utenti federati.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Selezionare la casella di controllo per ciascun utente che si desidera eliminare.
3. Selezionare **azioni > Elimina utente** o **azioni > Elimina utenti**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **Delete user** (Elimina utente) o **Delete users** (Elimina utenti).

Gestire le chiavi di accesso S3

Gestisci le chiavi di accesso S3 in StorageGRID

Ogni utente di un account tenant S3 deve disporre di una chiave di accesso per memorizzare e recuperare oggetti nel sistema StorageGRID. Una chiave di accesso è costituita da un ID della chiave di accesso e da una chiave di accesso segreta.

Le chiavi di accesso S3 possono essere gestite come segue:

- Gli utenti che dispongono dell'autorizzazione **Gestisci le tue credenziali S3** possono creare o rimuovere le proprie chiavi di accesso S3.
- Gli utenti che dispongono dell'autorizzazione **Root access** possono gestire le chiavi di accesso per l'account root S3 e tutti gli altri utenti. Le chiavi di accesso root forniscono l'accesso completo a tutti i bucket e gli oggetti per il tenant, a meno che non siano esplicitamente disabilitate da una policy bucket.

StorageGRID supporta l'autenticazione Firma versione 2 e Firma versione 4. L'accesso multiaccount non è consentito a meno che non sia esplicitamente abilitato da una policy bucket.

Crea le tue chiavi di accesso S3 in StorageGRID

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare le proprie chiavi di accesso S3. Per accedere ai bucket e agli oggetti, è necessario disporre di una chiave di accesso.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestisci le tue credenziali S3 o l'autorizzazione di accesso root"](#).

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 che consentono di creare e gestire i bucket per l'account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quante ne hai bisogno ed eliminare le chiavi che non stai utilizzando. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi in modo da limitare l'accesso a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre il rischio in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono rimosse automaticamente.
- Se il rischio di sicurezza nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare un periodo di scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.



È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3) > My access key**.

Viene visualizzata la pagina My access keys (i miei tasti di accesso) che elenca tutti i tasti di accesso esistenti.

2. Selezionare **Crea chiave**.

3. Effettuare una delle seguenti operazioni:

- Selezionare **non impostare una scadenza** per creare una chiave che non scadrà. (Impostazione predefinita)
- Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.



La data di scadenza può essere un massimo di cinque anni dalla data corrente. La scadenza può essere di almeno un minuto dall'ora corrente.

4. Selezionare **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), in cui sono elencati l'ID della chiave di accesso e la chiave di accesso segreta.

5. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.



Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni. Una volta chiusa la finestra di dialogo, non è possibile copiare o scaricare le chiavi.

6. Selezionare **fine**.

La nuova chiave è elencata nella pagina i miei tasti di accesso.

Visualizza le tue chiavi di accesso S3 in StorageGRID

Se si utilizza un locatario S3 e si dispone di ["autorizzazione appropriata"](#), è possibile visualizzare un elenco delle chiavi di accesso S3. È possibile ordinare l'elenco in base alla data di scadenza, in modo da determinare quali chiavi scadranno a breve. Se necessario, è possibile ["creare nuove chiavi"](#) o ["eliminare le chiavi"](#) che non si sta più utilizzando.



È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone delle credenziali Manage your own S3 ["permesso"](#) (Gestisci le proprie credenziali 3D).

Fasi

1. Selezionare **STORAGE (S3) > My access key**.
2. Dalla pagina My access keys (i miei tasti di accesso), ordinare le chiavi di accesso esistenti in base a **Expiration Time** (ora di scadenza) o **Access key ID** (ID chiave di accesso).
3. Se necessario, creare nuove chiavi o eliminare le chiavi che non si stanno più utilizzando.

Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, è possibile iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

Le chiavi scadute vengono rimosse automaticamente.

Elimina le tue chiavi di accesso S3 in StorageGRID

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le proprie chiavi di accesso S3. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestisci le tue autorizzazioni per le credenziali S3"](#).



È possibile accedere ai bucket S3 e agli oggetti appartenenti al tuo account utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per il tuo account in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **STORAGE (S3) > My access key**.
2. Nella pagina i miei tasti di accesso, selezionare la casella di controllo per ciascun tasto di accesso che si desidera rimuovere.
3. Selezionare **Delete key** (Elimina chiave).
4. Nella finestra di dialogo di conferma, selezionare **Elimina tasto**.

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina.

Crea le chiavi di accesso S3 di un altro utente in StorageGRID

Se si utilizza un tenant S3 e si dispone dell'autorizzazione appropriata, è possibile creare chiavi di accesso S3 per altri utenti, ad esempio applicazioni che richiedono l'accesso a bucket e oggetti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

È possibile creare una o più chiavi di accesso S3 per altri utenti in modo che possano creare e gestire i bucket per il proprio account tenant. Dopo aver creato una nuova chiave di accesso, aggiornare l'applicazione con il nuovo ID della chiave di accesso e la chiave di accesso segreta. Per motivi di sicurezza, non creare più chiavi di quelle richieste dall'utente ed eliminare le chiavi che non vengono utilizzate. Se si dispone di una sola chiave e sta per scadere, creare una nuova chiave prima della scadenza della vecchia, quindi eliminare quella vecchia.

Ogni chiave può avere un tempo di scadenza specifico o nessuna scadenza. Seguire queste linee guida per la scadenza:

- Impostare una scadenza per le chiavi per limitare l'accesso dell'utente a un determinato periodo di tempo. L'impostazione di un breve periodo di scadenza può contribuire a ridurre i rischi in caso di esposizione accidentale dell'ID della chiave di accesso e della chiave di accesso segreta. Le chiavi scadute vengono

rimosse automaticamente.

- Se il rischio di protezione nell'ambiente è basso e non è necessario creare periodicamente nuove chiavi, non è necessario impostare un tempo di scadenza per le chiavi. Se si decide in seguito di creare nuove chiavi, eliminare manualmente le vecchie chiavi.



È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.

Viene visualizzata la pagina User Detail (Dettagli utente).

3. Selezionare **Access keys**, quindi selezionare **Create key**.
4. Effettuare una delle seguenti operazioni:
 - Selezionare **non impostare un tempo di scadenza** per creare una chiave che non scade. (Impostazione predefinita)
 - Selezionare **Set an expiration time** (Imposta data di scadenza) e impostare la data e l'ora di scadenza.



La data di scadenza può essere un massimo di cinque anni dalla data corrente. La scadenza può essere di almeno un minuto dall'ora corrente.

5. Selezionare **Crea chiave di accesso**.

Viene visualizzata la finestra di dialogo Download access key (Scarica chiave di accesso), che elenca l'ID della chiave di accesso e la chiave di accesso segreta.

6. Copiare l'ID della chiave di accesso e la chiave di accesso segreta in una posizione sicura oppure selezionare **Download .csv** per salvare un foglio di calcolo contenente l'ID della chiave di accesso e la chiave di accesso segreta.



Non chiudere questa finestra di dialogo prima di aver copiato o scaricato queste informazioni. Una volta chiusa la finestra di dialogo, non è possibile copiare o scaricare le chiavi.

7. Selezionare **fine**.

La nuova chiave è elencata nella scheda Access Keys della pagina User Details (Dettagli utente).

Visualizza le chiavi di accesso S3 di un altro utente in StorageGRID

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile visualizzare le chiavi di accesso S3 di un altro utente. È possibile ordinare l'elenco in base all'ora di scadenza, in modo da determinare quali chiavi scadranno a breve. Se

necessario, è possibile creare nuove chiavi ed eliminare chiavi che non sono più in uso.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).



È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **Gestione accessi > Utenti**.
2. Nella pagina utenti, selezionare l'utente di cui si desidera visualizzare i tasti di accesso S3.
3. Nella pagina User details (Dettagli utente), selezionare **Access keys** (chiavi di accesso).
4. Ordinare le chiavi in base a **scadenza** o **ID chiave di accesso**.
5. Se necessario, creare nuove chiavi ed eliminare manualmente le chiavi che non sono più in uso.

Se si creano nuove chiavi prima della scadenza delle chiavi esistenti, l'utente può iniziare a utilizzare le nuove chiavi senza perdere temporaneamente l'accesso agli oggetti dell'account.

Le chiavi scadute vengono rimosse automaticamente.

Informazioni correlate

- ["Creare le chiavi di accesso S3 di un altro utente"](#)
- ["Eliminare le chiavi di accesso S3 di un altro utente"](#)

Elimina le chiavi di accesso S3 di un altro utente in StorageGRID

Se si utilizza un tenant S3 e si dispone delle autorizzazioni appropriate, è possibile eliminare le chiavi di accesso S3 di un altro utente. Una volta eliminata, una chiave di accesso non può più essere utilizzata per accedere agli oggetti e ai bucket dell'account tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).



È possibile accedere ai bucket S3 e agli oggetti appartenenti a un utente utilizzando l'ID della chiave di accesso e la chiave di accesso segreta visualizzati per tale utente in Tenant Manager. Per questo motivo, proteggere le chiavi di accesso come se si trattasse di una password. Ruotare regolarmente le chiavi di accesso, rimuovere eventuali chiavi inutilizzate dall'account e non condividerle mai con altri utenti.

Fasi

1. Selezionare **Gestione accessi > Utenti**.

2. Nella pagina utenti, selezionare l'utente di cui si desidera gestire le chiavi di accesso S3.
3. Nella pagina User details (Dettagli utente), selezionare **Access keys** (chiavi di accesso), quindi selezionare la casella di controllo per ogni chiave di accesso che si desidera eliminare.
4. Selezionare **azioni > Elimina tasto selezionato**.
5. Nella finestra di dialogo di conferma, selezionare **Elimina tasto**.

Viene visualizzato un messaggio di conferma nell'angolo superiore destro della pagina.

Gestire i bucket S3

Crea un bucket S3 di StorageGRID

È possibile utilizzare Tenant Manager per creare bucket S3 per i dati dell'oggetto.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone dell'accesso root o Gestisci tutti i bucket ["permesso"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.



Le autorizzazioni per impostare o modificare le proprietà di blocco degli oggetti S3 di bucket o oggetti possono essere concesse da ["policy bucket o policy di gruppo"](#).

- Se si prevede di attivare il blocco oggetti S3 per un bucket, un amministratore della griglia ha attivato l'impostazione globale di blocco oggetti S3 per il sistema StorageGRID e sono stati esaminati i requisiti per i bucket e gli oggetti blocco oggetti S3.
- Se più tenant avranno ciascuno fino a 5.000 bucket, ogni Storage Node nella griglia avrà un minimo di 64 GB di RAM.



Il sistema StorageGRID supporta un massimo di 20.000 bucket per ogni account tenant S3. Ogni grid può avere un massimo di 100.000 bucket, inclusi ["secchi di rami"](#). C'è anche un limite a ["profondità del bucket del branch"](#).

Accedere alla procedura guidata

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
2. Selezionare **Crea bucket**.

Inserire i dettagli

Fasi

1. Inserire i dettagli del bucket.

Campo	Descrizione
Nome bucket	Un nome per il bucket conforme alle seguenti regole: • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non deve contenere periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. Per ulteriori informazioni, consulta il "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket". Nota: Non è possibile modificare il nome del bucket dopo averlo creato.
Regione	La regione del bucket. L'amministratore 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. Se la regione predefinita è configurata su una regione diversa da <code>us-east-1</code>, questa altra regione viene inizialmente selezionata nel menu a discesa. Nota: Non è possibile modificare l'area dopo aver creato il bucket.

2. Selezionare **continua**.

Gestire le impostazioni

Fasi

1. Facoltativamente, attivare il controllo della versione degli oggetti per il bucket.

Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze.

È necessario abilitare il controllo delle versioni degli oggetti se:

- Il bucket verrà utilizzato per la replica tra griglie.
- Vuoi creare un ["secchio di rami"](#) da questo secchio.

2. Se l'impostazione globale S3 Object Lock (blocco oggetti S3) è attivata, attivare facoltativamente S3 Object Lock (blocco oggetti S3) per memorizzare gli oggetti utilizzando un modello WORM (Write-Once-Read-Many).

Attivare il blocco oggetti S3 per un bucket solo se è necessario mantenere gli oggetti per un periodo di tempo fisso, ad esempio per soddisfare determinati requisiti normativi. S3 Object Lock è un'impostazione permanente che consente di evitare l'eliminazione o la sovrascrittura degli oggetti per un periodo di tempo fisso o indefinito.



Una volta attivata l'impostazione S3 Object Lock per un bucket, non è possibile disattivarla. Chiunque disponga delle autorizzazioni corrette può aggiungere a questo bucket oggetti che non possono essere modificati. Potrebbe non essere possibile eliminare questi oggetti o il bucket stesso.

Se si attiva il blocco oggetti S3 per un bucket, il controllo della versione del bucket viene attivato automaticamente.

3. Se si seleziona **Enable S3 Object Lock** (attiva blocco oggetti S3), attivare facoltativamente **Default Retention** per questo bucket.



L'amministratore di rete deve concedere l'autorizzazione a ["Utilizzare funzioni specifiche di blocco oggetti S3"](#).

Quando l'opzione **Default Retention** (conservazione predefinita) è attivata, i nuovi oggetti aggiunti al bucket saranno automaticamente protetti dall'eliminazione o dalla sovrascrittura. L'impostazione **Default Retention** non si applica agli oggetti che hanno periodi di conservazione propri.

- a. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare una **modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	• Gli utenti con <code>s3:BypassGovernanceRetention</code> autorizzazione possono utilizzare l' <code>`x-amz-bypass-governance-retention: true`</code> intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. Nota: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.

- b. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare il **Default Retention Period** (periodo di conservazione predefinito) per il bucket.

Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

Un *massimo* periodo di conservazione, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore di rete crea il tenant. Quando si imposta un periodo di conservazione *default*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedere all'amministratore di rete di aumentare o diminuire il periodo di conservazione massimo.

4. Facoltativamente, seleziona **Abilita limite di capacità**, inserisci un valore e seleziona l'unità di capacità.

Il limite di capacità è la capacità massima disponibile per gli oggetti di questa benna. Questo valore rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).

Se non viene impostato alcun limite, la capacità di questa benna è illimitata. Per ulteriori informazioni, fare riferimento "[Utilizzo del limite di capacità](#)" a.

5. Facoltativamente, seleziona **Abilita limite conteggio oggetti**.

Il limite del conteggio degli oggetti è il numero massimo di oggetti che questo bucket può contenere. Questo valore rappresenta un importo logico (conteggio oggetti). Se non viene impostato alcun limite, il numero di oggetti è illimitato.

6. Selezionare **Crea bucket**.

Il bucket viene creato e aggiunto alla tabella nella pagina Bucket.

7. In alternativa, selezionare **Vai alla pagina dettagli bucket** per "[visualizza i dettagli del bucket](#)" ed eseguire una configurazione aggiuntiva.

Puoi anche "[creare bucket di rami](#)" secondo necessità.

Visualizza i dettagli del bucket S3 in StorageGRID

È possibile visualizzare i bucket nell'account tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "[browser web supportato](#)".
- L'utente appartiene a un gruppo di utenti che dispone di "[Autorizzazione accesso root](#), [Gestisci tutti i bucket](#) o [Visualizza tutti i bucket](#)". Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione nei criteri di gruppo o bucket.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

Viene visualizzata la pagina Bucket.

2. Rivedere la tabella di riepilogo per ciascun bucket.

In base alle esigenze, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco in avanti e indietro.



I valori Conteggio oggetti, spazio utilizzato e utilizzo visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi. Se nei bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

Nome

Il nome univoco del bucket, che non può essere modificato.

Funzionalità attivate

L'elenco delle funzioni attivate per il bucket.

Blocco oggetti S3

Se S3 Object Lock è attivato per il bucket.

Questa colonna viene visualizzata solo se S3 Object Lock (blocco oggetti S3) è attivato per la griglia. Questa colonna mostra anche informazioni relative a qualsiasi bucket compatibile legacy.

Regione

La regione del bucket, che non può essere modificata. Questa colonna è nascosta per impostazione predefinita.

Numero di oggetti

Il numero di oggetti in questo bucket. Se nel bucket è attivata la versione, le versioni degli oggetti non correnti vengono incluse in questo valore.

Quando gli oggetti vengono aggiunti o cancellati, questo valore potrebbe non essere aggiornato 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 in cancellazione o per i metadati degli oggetti.

L'aggiornamento di questo valore può richiedere fino a 10 minuti.

Utilizzo

La percentuale utilizzata del limite di capacità della benna, se impostato.

Il valore di utilizzo si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla il limite di capacità (se impostato) quando un tenant inizia a caricare gli oggetti e rifiuta le nuove acquisizioni 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, è possibile impedire temporaneamente a un tenant di caricare nuovi oggetti in questo bucket fino a quando l'utilizzo del limite di capacità non viene ricalcolato. I calcoli possono richiedere 10 minuti o più.

Questo valore indica le dimensioni logiche, non quelle fisiche necessarie per memorizzare gli oggetti e i relativi metadati.

Capacità

Se impostato, il limite di capacità per la benna.

Data di creazione

La data e l'ora di creazione del bucket. Questa colonna è nascosta per impostazione predefinita.

3. Per visualizzare i dettagli di un bucket specifico, selezionare il nome del bucket dalla tabella.
 - a. Visualizzare le informazioni di riepilogo nella parte superiore della pagina Web per confermare i dettagli per il bucket, come ad esempio il numero di aree e oggetti.

- b. Visualizza le barre di utilizzo del limite di capacità e del limite di utilizzo del numero di oggetti. 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, selezionare **Elimina oggetti nel bucket** e **Elimina bucket**.



Prestare particolare attenzione alle precauzioni visualizzate quando si seleziona ciascuna di queste opzioni. Per ulteriori informazioni, fare riferimento a:

- ["Elimina tutti gli oggetti in un bucket"](#)
- ["Eliminare un bucket"](#) (la benna deve essere vuota)

- d. Visualizzare o modificare le impostazioni del bucket in ciascuna delle schede, secondo necessità.
- **S3 Console:** Consente di visualizzare gli oggetti per il bucket. Per ulteriori informazioni, fare riferimento a ["Utilizzare la console S3"](#).
 - **Opzioni bucket:** Consente di visualizzare o modificare le impostazioni delle opzioni. Alcune impostazioni, come blocco oggetti S3, non possono essere modificate dopo la creazione del bucket.
 - ["Gestire la coerenza del bucket"](#)
 - ["Aggiornamenti dell'ora dell'ultimo accesso"](#)
 - ["Limite di capacità"](#)
 - ["Limite del conteggio degli oggetti"](#)
 - ["Versione degli oggetti"](#)
 - ["Blocco oggetti S3"](#)
 - ["Ritenzione bucket predefinita"](#)
 - ["Gestire la replica cross-grid"](#) (se consentito per il tenant)
 - **Platform Services:** ["Gestire i servizi della piattaforma"](#) (Se consentito per il locatario)
 - **Accesso bucket:** Consente di visualizzare o modificare le impostazioni delle opzioni. È necessario disporre di autorizzazioni di accesso specifiche.
 - Configurare ["CORS per bucket e oggetti"](#) in modo che il bucket e gli oggetti al suo interno siano accessibili alle applicazioni web in altri domini.
 - ["Controllo dell'accesso degli utenti"](#) Per un secchio S3 e oggetti in quel secchio.
 - **Rami:** visualizza l'elenco dei bucket di rami per il bucket. ["Crea un nuovo bucket di filiale o gestisci i bucket di filiale"](#).

Scopri i bucket di ramo di StorageGRID

Un bucket di diramazione fornisce l'accesso agli oggetti in un bucket così come esistevano in un determinato momento.

Si crea un bucket di diramazione da un bucket esistente. Dopo aver creato un bucket di diramazione, il bucket originale da cui è stato creato viene chiamato *bucket di base*. Inoltre, è possibile creare un bucket di diramazione da un altro bucket di diramazione.

Un bucket di diramazione fornisce l'accesso ai dati protetti, ma non funge da backup. Per continuare a proteggere i dati, utilizzare queste funzionalità sui bucket di base:

- ["Blocco oggetti S3"](#)
- ["Replica cross-grid"](#) per secchi di base
- ["Criteri dei bucket"](#) per i bucket con versione per ripulire le vecchie versioni degli oggetti

Si noti le seguenti caratteristiche dei bucket di diramazione:

- È possibile accedere agli oggetti nei bucket di diramazione utilizzando ["Console S3 per scaricare oggetti"](#).
- Quando i client accedono agli oggetti in un bucket di diramazione, il bucket di diramazione ["politiche di accesso"](#), anziché le policy del bucket di base, determinano se l'accesso è concesso o negato.
- Gli oggetti creati in un bucket di base vengono valutati in base a come ["Regole ILM"](#) applicare al secchio di base. Gli oggetti creati in un bucket di diramazione vengono valutati in base al modo in cui le regole ILM si applicano al bucket di diramazione.
- La replica tra griglie non è supportata per i bucket branch.
- I servizi della piattaforma non sono supportati per i bucket di filiale.

Esempi di utilizzo del bucket di diramazione

- È possibile utilizzare un branch bucket per rimuovere oggetti danneggiati creando un branch bucket da un punto nel tempo precedente al verificarsi del danneggiamento e quindi indirizzando le applicazioni al branch bucket anziché al bucket di base che contiene oggetti danneggiati.
- Stai salvando i dati in un bucket con versione. Si è verificata una vulnerabilità accidentale che ha causato l'ingestione di molti oggetti indesiderati dopo il tempo T . È possibile creare un bucket di diramazione per il valore temporale Prima, T , e reindirizzare le operazioni client a tale bucket di diramazione. Quindi, solo gli oggetti ingeriti prima del tempo precedente T vengono esposti ai client.
- Stai salvando dati in un bucket versionato. C'è stata una vulnerabilità accidentale che ha causato l'ingestione di molti oggetti indesiderati tra il tempo $T1$ e $T2$. Puoi creare un bucket di diramazione per i valori di tempo *Exclude*, $T1$ e $T2$, e reindirizzare le operazioni dei client a quel bucket di diramazione. Così, solo gli oggetti ingeriti prima di $T1$ e dopo $T2$ saranno esposti ai client.

Operazioni sugli oggetti nei bucket di diramazione

- Un'operazione PUT su un bucket di ramo crea un oggetto nel ramo.
- Un'operazione GET su un bucket di diramazione recupera un oggetto dal diramazione. Se l'oggetto non esiste nel bucket di diramazione, viene recuperato dal bucket di base.
- Le eliminazioni di oggetti dai bucket di diramazione avvengono come segue:

Operazione	Bersaglio	Risultato	Visibilità dell'oggetto nel bucket di base	Visibilità dell'oggetto nel bucket di diramazione
Elimina senza ID versione	Secchio di base	L'indicatore di eliminazione viene creato solo per il bucket di base	HEAD/GET restituisce L'oggetto non esiste, ma è ancora possibile accedere a versioni specifiche	HEAD/GET restituisce che l'oggetto esiste e che è ancora possibile accedere a versioni specifiche Il marcatore di eliminazione sarebbe stato creato dopo il bucket del ramo <code>beforeTime</code> .
Elimina con ID versione	Secchio di base	La versione specifica dell'oggetto viene eliminata sia per il bucket base che per quello branch	HEAD/GET restituisce La versione dell'oggetto non esiste	HEAD/GET restituisce La versione dell'oggetto non esiste
Elimina senza ID versione	Secchio per rami	Il marcatore di eliminazione viene creato solo per il bucket del ramo	HEAD/GET restituisce l'oggetto (l'oggetto bucket di base non è interessato)	HEAD/GET restituisce L'oggetto non esiste
Elimina con ID versione	Secchio per rami	La versione specifica dell'oggetto viene eliminata solo per il bucket di diramazione	HEAD/GET restituisce una versione specifica dell'oggetto (l'oggetto bucket di base non è interessato)	HEAD/GET restituisce La versione dell'oggetto non esiste

Fare riferimento anche a ["Modalità di eliminazione degli oggetti con versione S3"](#).

Gestisci i bucket di filiale di StorageGRID

Utilizzare Tenant Manager per creare e visualizzare i dettagli dei bucket delle filiali.

Prima di iniziare

- Hai effettuato l'accesso al Tenant Manager utilizzando un ["browser web supportato"](#).
- Appartieni a un gruppo di utenti che ha accesso Root o ["Gestisci autorizzazioni per tutti i bucket"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nei criteri di gruppo o di bucket.
- Il bucket di base da cui vuoi creare un ramo ha ["controllo delle versioni abilitato"](#).
- Sei il proprietario del secchio base.

A proposito di questa attività

Notare le seguenti informazioni per i bucket di diramazione:

Limite di profondità del bucket di branch

Un bucket di diramazione può contenere al massimo 20 bucket di base. Con l'aumentare della profondità del bucket di diramazione, la latenza può aumentare, soprattutto per le chiamate ListObjectVersions S3.

- Se crei un bucket di diramazione da un bucket di base che è un bucket normale (un bucket che è stato inizialmente creato come bucket di base), il nuovo bucket di diramazione ha un solo bucket di base.
- Se il bucket di base è a sua volta un bucket di diramazione, il nuovo bucket di diramazione eredita tutti i bucket di base di quest'ultimo. Specifichi direttamente un solo bucket di base; i bucket di base ereditati sono impliciti.
- Il numero totale di bucket di base (espliciti e impliciti) non può superare 20.

Ad esempio, supponi che il bucket **A** sia un bucket normale con la gestione delle versioni abilitata:

- Il bucket branch **B**, creato da **A**, ha un bucket di base: **A**.
- Il bucket di diramazione **C**, creato da **B**, ha due bucket di base: **B** (esplicito) e **A** (implicito).
- Il bucket di branch **D**, creato da **C**, ha tre bucket di base: **C** (esplicito), **B** (implicito) e **A** (implicito).
- Questo schema si ripete fino a una profondità massima di 20 bucket di base.

Autorizzazioni S3 Object Lock

Le autorizzazioni per impostare le proprietà di S3 Object Lock di bucket o oggetti possono essere concesse da ["policy bucket o policy di gruppo"](#).

Versionamento sospeso

Se si sospende il controllo delle versioni sul bucket di base, il contenuto del bucket di base non sarà più visibile nei relativi bucket rami.



Dopo aver configurato e creato un bucket di diramazione, non è possibile modificare la configurazione.

Crea bucket di diramazione

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
2. Seleziona il bucket da cui vuoi creare un ramo (il "bucket di base").
3. Nella pagina dei dettagli del bucket, seleziona **Rami > Crea bucket ramo**.

Il pulsante **Crea bucket di diramazione** è disabilitato se il bucket di base non ha il controllo delle versioni abilitato.

Inserire i dettagli

Fasi

1. Inserisci i dettagli per il bucket della filiale.

Campo	Descrizione
Nome del bucket di filiale	Un nome per il bucket di diramazione che rispetti queste regole: • Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). • Deve essere conforme al DNS. • Deve contenere almeno 3 e non più di 63 caratteri. • Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. • Non deve contenere periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. Per ulteriori informazioni, vedere "Documentazione di Amazon Web Services (AWS) sulle regole di denominazione del bucket". Nota: non è possibile modificare il nome dopo aver creato il bucket di diramazione.
Regione (non modificabile per i bucket di filiale)	Regione del bucket del ramo. La regione del bucket di diramazione deve corrispondere alla regione del bucket di base, pertanto questo campo è disabilitato per i bucket di diramazione.
Tipo di secchio per rami	• Lettura-scrittura: è possibile aggiungere o eliminare oggetti o versioni di oggetti nel bucket del ramo. • Sola lettura: non è possibile modificare gli oggetti nel bucket del ramo. Nota: è possibile impostare il tipo di bucket di diramazione su sola lettura solo se il bucket di diramazione è vuoto. Se il tipo per un bucket di branch esistente è impostato su lettura-scrittura e non hai scritto su di esso, puoi modificare il tipo in sola lettura.

2. Selezionare **continua**.

Filtro temporale

Scegli l'intervallo di tempo da cui includere le versioni degli oggetti dal bucket di base. Per qualsiasi filtro temporale, seleziona una data qualsiasi all'interno del seguente intervallo:

- Data minima: 1° gennaio 2010 (UTC)
- Data massima: cinque anni dalla data odierna (UTC)

Prima

Il bucket del ramo ti permette di accedere alle versioni degli oggetti create prima del tempo *Before*.

Dopo

Il bucket di ramo fornisce accesso alle versioni degli oggetti create dopo il tempo *After*.

Fra

Il bucket di ramo fornisce accesso alle versioni degli oggetti create tra gli orari *From* e *To*.

Escludi

Il bucket di branch non fornisce accesso alle versioni degli oggetti create tra i momenti *Exclude from* e *Exclude to*.

Gestisci le impostazioni dell'oggetto (facoltativo)

Le impostazioni degli oggetti per un bucket di diramazione non influiscono sulle versioni degli oggetti nel bucket di base.

Fasi

1. Se l'impostazione globale S3 Object Lock è abilitata, abilitare facoltativamente S3 Object Lock per il bucket branch. Per abilitare S3 Object Lock, il bucket di diramazione deve essere un bucket di lettura-scrittura.

Abilitare S3 Object Lock per un bucket di diramazione 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 al bucket del ramo oggetti che non possono essere modificati. Potresti non essere in grado di eliminare questi oggetti o il bucket di diramazione stesso.

2. Se hai selezionato **Abilita blocco oggetto S3**, abilita facoltativamente **Conservazione predefinita** per il bucket di diramazione.



L'amministratore di rete deve concedere l'autorizzazione a ["Utilizzare funzioni specifiche di blocco oggetti S3"](#).

Quando è abilitata la **Conservazione predefinita**, i nuovi oggetti aggiunti al bucket del ramo 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 l'opzione **Conservazione predefinita**, specificare una **Modalità di conservazione predefinita** per il bucket di filiale.

Modalità di conservazione predefinita	Descrizione
Governance	• Gli utenti con <code>s3:BypassGovernanceRetention</code> autorizzazione possono utilizzare l' <code>x-amz-bypass-governance-retention: true</code> intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Modalità di conservazione predefinita	Descrizione
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. Nota: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.

- b. Se è abilitata l'opzione **Conservazione predefinita**, specificare il **Periodo di conservazione predefinito** per il bucket di filiale.

Il **Periodo di conservazione predefinito** indica per quanto tempo i nuovi oggetti aggiunti al bucket di diramazione 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 *massimo* periodo di conservazione, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore di rete crea il tenant. Quando si imposta un periodo di conservazione *default*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario, chiedere all'amministratore di rete di aumentare o diminuire il periodo di conservazione massimo.

3. Facoltativamente, seleziona **Abilita limite di capacità**.

Il limite di capacità è la capacità massima disponibile per il bucket di diramazione. Questo valore rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione su disco).

Se non viene impostato alcun limite, la capacità del bucket di filiale è illimitata. Fare riferimento a ["Utilizzo del limite di capacità"](#) per maggiori informazioni.



Questa impostazione si applica solo agli oggetti inseriti direttamente nel bucket di diramazione e non agli oggetti visibili dal bucket di base attraverso il bucket di diramazione.

4. Facoltativamente, seleziona **Abilita limite conteggio oggetti**.

Il limite del conteggio degli oggetti è il numero massimo di oggetti che il bucket di diramazione può contenere. Questo valore rappresenta un importo logico (conteggio oggetti). Se non viene impostato alcun limite, il numero di oggetti è illimitato.



Questa impostazione si applica solo agli oggetti inseriti direttamente nel bucket di diramazione e non agli oggetti visibili dal bucket di base attraverso il bucket di diramazione.

5. Selezionare **Crea bucket**.

Il bucket di diramazione 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 di filiale"](#) ed eseguire configurazioni aggiuntive.

Nella pagina Dettagli bucket, alcune opzioni di configurazione relative alla modifica degli oggetti sono disabilitate per i bucket di sola lettura.

Applica un tag di policy ILM a un bucket StorageGRID

Scegli un tag di policy ILM da applicare a un bucket in base ai tuoi requisiti di storage a oggetti.

Il criterio ILM controlla la posizione di memorizzazione dei dati dell'oggetto e se vengono eliminati dopo un determinato periodo di tempo. L'amministratore di grid crea criteri ILM e li assegna ai tag dei criteri ILM quando si utilizzano più criteri attivi.



Evitare di riassegnare frequentemente il tag di un bucket. In caso contrario, potrebbero verificarsi problemi di prestazioni.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione accesso root, Gestisci tutti i bucket o Visualizza tutti i bucket"](#). Queste autorizzazioni hanno la precedenza sulle impostazioni di autorizzazione nei criteri di gruppo o bucket.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

Viene visualizzata la pagina Bucket. In base alle esigenze, è possibile ordinare le informazioni in base a qualsiasi colonna oppure scorrere l'elenco in avanti e indietro.

2. Selezionare il nome del bucket a cui si desidera assegnare un tag di criterio ILM.

È inoltre possibile modificare l'assegnazione dei tag dei criteri ILM per un bucket a cui è già stato assegnato un tag.



I valori Object Count (Conteggio oggetti) e Space used (spazio utilizzato) visualizzati sono stime. Queste stime sono influenzate dai tempi di acquisizione, dalla connettività di rete e dallo stato dei nodi. Se nel bucket è attivata la versione, le versioni degli oggetti eliminati vengono incluse nel conteggio degli oggetti.

3. Nella scheda Opzioni bucket, espandere il tag criterio ILM fisarmonica. Questa fisarmonica viene visualizzata solo se l'amministratore della griglia ha attivato l'uso di tag di criteri personalizzati.
4. Leggere la descrizione di ciascun tag di criterio per determinare quale tag applicare al bucket.



La modifica del tag di criterio ILM per un bucket attiva la rivalutazione ILM di tutti gli oggetti nel bucket. Se la nuova policy mantiene gli oggetti per un periodo di tempo limitato, gli oggetti meno recenti verranno eliminati.

5. Selezionare il pulsante di opzione per il tag che si desidera assegnare al bucket.
6. Selezionare **Save Changes** (Salva modifiche). Sul bucket viene impostata una nuova etichetta bucket S3 con la chiave NTAP-SG-ILM-BUCKET-TAG e il valore del tag criterio ILM.



Assicurarsi che le applicazioni S3 non sovrascrivano o eliminino accidentalmente la nuova etichetta del bucket. Se questo tag viene omesso quando si applica un nuovo TagSet al bucket, gli oggetti nel bucket torneranno a essere valutati in base al criterio ILM predefinito.



Impostare e modificare i tag dei criteri ILM utilizzando solo l'API di Tenant Manager o di Tenant Manager in cui il tag dei criteri ILM viene convalidato. Non modificare il `NTAP-SG-ILM-BUCKET-TAG` tag dei criteri ILM utilizzando l'API S3 `PutBucketTagging` o l'API S3 `DeleteBucketTagging`.



La modifica del tag della policy assegnato a un bucket ha un impatto temporaneo sulle performance, mentre gli oggetti vengono rivalutati utilizzando la nuova policy ILM.

Gestisci la policy dei bucket di StorageGRID

È possibile controllare l'accesso utente per un bucket S3 e gli oggetti in tale bucket.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Autorizzazione di accesso root"](#). Le autorizzazioni Visualizza tutti i bucket e Gestisci tutti i bucket consentono solo la visualizzazione.
- Hai verificato che il numero richiesto di nodi e siti storage è disponibile. Se due o più nodi di archiviazione non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

Fasi

1. Selezionare **bucket**, quindi selezionare il bucket che si desidera gestire.
2. Nella pagina dei dettagli del bucket, selezionare **accesso al bucket > criterio del bucket**.
3. Effettuare una delle seguenti operazioni:
 - Immettere un criterio bucket selezionando la casella di controllo **Abilita criterio**. Quindi immettere una stringa formattata JSON valida.

Ogni criterio bucket ha un limite di dimensioni di 20.480 byte.
 - Modificare un criterio esistente modificando la stringa.
 - Disattivare un criterio deselectando **attiva criterio**.

Per informazioni dettagliate sui criteri bucket, inclusi esempi e sintassi del linguaggio, vedere ["Esempio di policy bucket"](#).

Gestire la coerenza dei bucket di StorageGRID

I valori di coerenza possono essere utilizzati per specificare la disponibilità delle modifiche alle impostazioni del bucket e per fornire un equilibrio tra la disponibilità degli oggetti all'interno di un bucket e la coerenza di tali oggetti in diversi nodi e siti di archiviazione. È possibile modificare i valori di coerenza in modo che siano diversi dai valori predefiniti in modo che le applicazioni client possano soddisfare le proprie esigenze operative.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

Linee guida per la coerenza della benna

La coerenza del bucket viene utilizzata per determinare la coerenza delle applicazioni client che influiscono sugli oggetti all'interno del bucket S3. In generale, si dovrebbe usare la coerenza **Read-after-new-write** per i propri bucket.

modificare la coerenza del bucket

Se la coerenza **Read-after-new-write** non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza impostando la coerenza del bucket o utilizzando l'Consistency-Control`intestazione. La `Consistency-Control testata esclude la coerenza della benna.



Quando si modifica la consistenza di un bucket, solo gli oggetti che vengono acquisiti dopo la modifica sono garantiti per soddisfare l'impostazione modificata.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **.

4. Selezionare una coerenza per le operazioni eseguite sugli oggetti in questo bucket.

- **Tutti**: Offre il massimo livello di coerenza. Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
- **Strong-Global**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
- **Strong-Site**: Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write** (valore predefinito): Fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available**: Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

5. Selezionare **Save Changes** (Salva modifiche).

Cosa accade quando si modificano le impostazioni della benna

I bucket hanno impostazioni multiple che influiscono sul comportamento dei bucket e degli oggetti all'interno di tali bucket.

Per impostazione predefinita, le seguenti impostazioni del bucket utilizzano la coerenza **strong**. Se due o più nodi di archiviazione non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

- ["Eliminazione bucket vuoto in background"](#)
- ["Ora ultimo accesso"](#)
- ["Ciclo di vita del bucket"](#)
- ["Politica del bucket"](#)
- ["Etichettatura della benna"](#)
- ["Versione bucket"](#)
- ["Blocco oggetti S3"](#)
- ["Crittografia bucket"](#)



Il valore di coerenza per la versione bucket, blocco oggetto S3 e crittografia bucket non può essere impostato su un valore non fortemente coerente.

Le seguenti impostazioni della benna non utilizzano una forte coerenza e hanno una maggiore disponibilità per le modifiche. Le modifiche a queste impostazioni potrebbero richiedere del tempo prima di avere effetto.

- ["Configurazione dei servizi della piattaforma: Integrazione di notifica, replica o ricerca"](#)
- ["Configurare StorageGRID CORS per bucket e oggetti"](#)
- [Modificare la coerenza della benna](#)



Se la coerenza predefinita utilizzata durante la modifica delle impostazioni del bucket non soddisfa i requisiti dell'applicazione client, è possibile modificare la coerenza utilizzando l'Consistency-Control`intestazione per ["API REST S3"](#) o utilizzando le ``force` opzioni o `reducedConsistency` in ["API di gestione del tenant"](#).

Abilita o disabilita gli aggiornamenti dell'ora dell'ultimo accesso in StorageGRID

Quando gli amministratori della griglia creano le regole ILM (Information Lifecycle Management) per un sistema StorageGRID, possono facoltativamente specificare che l'ultimo tempo di accesso di un oggetto deve essere utilizzato per determinare se spostare l'oggetto in una posizione di storage diversa. Se si utilizza un tenant S3, è possibile sfruttare tali regole attivando gli ultimi aggiornamenti del tempo di accesso per gli oggetti in un bucket S3.

Queste istruzioni si applicano solo ai sistemi StorageGRID che includono almeno una regola ILM che utilizza l'opzione **ultimo tempo di accesso** come filtro avanzato o come tempo di riferimento. È possibile ignorare queste istruzioni se il sistema StorageGRID non include tale regola. Per ulteriori informazioni, vedere ["USA l'ultimo tempo di accesso nelle regole ILM"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

A proposito di questa attività

Ultimo tempo di accesso è una delle opzioni disponibili per l'istruzione di posizionamento **tempo di riferimento** per una regola ILM. L'impostazione del tempo di riferimento per una regola su ultimo tempo di accesso consente agli amministratori della griglia di specificare che gli oggetti devono essere posizionati in determinate posizioni di storage in base al momento dell'ultimo recupero (lettura o visualizzazione) di tali oggetti.

Ad esempio, per garantire che gli oggetti visualizzati di recente rimangano sullo storage più veloce, un amministratore della griglia può creare una regola ILM specificando quanto segue:

- Gli oggetti recuperati nell'ultimo mese devono rimanere sui nodi di storage locali.
- Gli oggetti che non sono stati recuperati nell'ultimo mese devono essere spostati in una posizione off-site.

Per impostazione predefinita, gli aggiornamenti dell'ultimo tempo di accesso sono disattivati. Se il sistema StorageGRID include una regola ILM che utilizza l'opzione **ultimo tempo di accesso** e si desidera che questa opzione venga applicata agli oggetti in questo bucket, è necessario abilitare gli aggiornamenti dell'ultimo tempo di accesso per i bucket S3 specificati in tale regola.



L'aggiornamento dell'ultimo tempo di accesso durante il recupero di un oggetto può ridurre le prestazioni di StorageGRID, in particolare per gli oggetti di piccole dimensioni.

Si verifica un impatto sulle performance con gli ultimi aggiornamenti dell'orario di accesso, perché StorageGRID deve eseguire questi passaggi aggiuntivi ogni volta che vengono recuperati gli oggetti:

- Aggiornare gli oggetti con nuovi timestamp
- Aggiungere gli oggetti alla coda ILM, in modo che possano essere rivalutati in base alle regole e ai criteri ILM correnti

La tabella riassume il comportamento applicato a tutti gli oggetti nel bucket quando l'ultimo tempo di accesso è disattivato o attivato.

Tipo di richiesta	Comportamento se l'ultimo tempo di accesso è disattivato (impostazione predefinita)		Comportamento se è attivata l'ultima ora di accesso	
	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?	Ultimo aggiornamento dell'orario di accesso?	Oggetto aggiunto alla coda di valutazione ILM?
Richiesta di recupero dei metadati di un oggetto quando viene emessa un'operazione HEAD	No	No	No	No

Richiesta di recuperare un oggetto, il relativo elenco di controllo degli accessi o i relativi metadati	No	No	Sì	Sì
Richiesta di aggiornamento dei metadati di un oggetto	Sì	Sì	Sì	Sì
Richiesta di elencare gli oggetti o le versioni degli oggetti	No	No	No	No
Richiesta di copia di un oggetto da un bucket all'altro	• No, per la copia di origine • Sì, per la copia di destinazione	• No, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione	• Sì, per la copia di origine • Sì, per la copia di destinazione
Richiesta di completare un caricamento multiparte	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato	Sì, per l'oggetto assemblato

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **ultimi aggiornamenti dell'ora di accesso**.
4. Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso.
5. Selezionare **Save Changes** (Salva modifiche).

Modifica la versione degli oggetti per un bucket S3 in StorageGRID

Se si utilizza un tenant S3, è possibile modificare lo stato di versione per i bucket S3.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un "[browser web supportato](#)".
- L'utente appartiene a un gruppo di utenti che dispone di "[Gestire tutti i bucket o le autorizzazioni di accesso root](#)". Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Hai verificato che il numero richiesto di nodi e siti storage è disponibile. Se due o più nodi di archiviazione

non sono disponibili all'interno di un sito o se un sito non è disponibile, le modifiche a queste impostazioni potrebbero non essere disponibili.

A proposito di questa attività

È possibile attivare o sospendere il controllo delle versioni degli oggetti per un bucket. Una volta attivata la versione per un bucket, non è possibile tornare allo stato senza versione. Tuttavia, è possibile sospendere il controllo delle versioni per il bucket.

- **Disabled (Disattivato):** La versione non è mai stata attivata
- **Enabled (attivato):** Il controllo delle versioni è attivato
- **Suspended (sospeso):** Il controllo delle versioni era stato precedentemente attivato e sospeso

Per ulteriori informazioni, vedere quanto segue:

- ["Versione degli oggetti"](#)
- ["Regole e criteri ILM per gli oggetti con versione S3 \(esempio 4\)"](#)
- ["Modalità di eliminazione degli oggetti"](#)

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **versione oggetto**.
4. Selezionare uno stato di versione per gli oggetti in questo bucket.

La versione degli oggetti deve rimanere abilitata per un bucket utilizzato per la replica cross-grid. Se S3 Object Lock (blocco oggetti S3) o legacy compliance (compliance legacy) è attivato, le opzioni **Object versioning** (versione oggetto) sono disattivate.

Opzione	Descrizione
Abilitare il controllo delle versioni	Abilitare la versione degli oggetti se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket. È quindi possibile recuperare le versioni precedenti di un oggetto in base alle esigenze. Gli oggetti già presenti nel bucket verranno sottoposti alla versione quando vengono modificati da un utente.
Sospendere il controllo delle versioni	Sospendere la versione degli oggetti se non si desidera più creare nuove versioni degli oggetti. È comunque possibile recuperare le versioni di oggetti esistenti.

5. Selezionare **Save Changes** (Salva modifiche).

Utilizza S3 Object Lock per conservare gli oggetti in StorageGRID

È possibile utilizzare il blocco oggetti S3 se i bucket e gli oggetti devono soddisfare i

requisiti normativi per la conservazione.



L'amministratore della griglia deve concedere l'autorizzazione per utilizzare funzioni specifiche di blocco oggetti S3.

Che cos'è il blocco oggetti S3?

La funzione blocco oggetti StorageGRID S3 è una soluzione di protezione degli oggetti equivalente a blocco oggetti S3 in Amazon Simple Storage Service (Amazon S3).

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. Quando l'impostazione allow S3 Object Lock for existing buckets è abilitata, un account tenant S3 può abilitare S3 Object Lock per un bucket esistente. Se un bucket ha S3 Object Lock abilitato, il versioning del bucket è richiesto e viene abilitato automaticamente. Dopo che un account tenant S3 ha abilitato S3 Object Lock per un bucket nuovo o esistente, non può essere disabilitato.

Un bucket senza blocco oggetti S3 può avere solo oggetti senza impostazioni di conservazione specificate. Nessun oggetto acquisito avrà impostazioni di conservazione.

Un bucket con blocco oggetti S3 può avere oggetti con e senza impostazioni di conservazione specificate dalle applicazioni client S3. Alcuni oggetti acquisiti avranno impostazioni di conservazione.

Un bucket con blocco oggetto S3 e conservazione predefinita configurata può avere caricato oggetti con impostazioni di conservazione specificate e nuovi oggetti senza impostazioni di conservazione. I nuovi oggetti utilizzano l'impostazione predefinita, poiché l'impostazione di conservazione non è stata configurata a livello di oggetto.

In effetti, 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 invariati.

Modalità di conservazione

La funzione blocco oggetti di StorageGRID S3 supporta due modalità di conservazione per applicare diversi livelli di protezione agli oggetti. Queste modalità equivalgono alle modalità di conservazione Amazon S3.

- In modalità compliance:
 - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
 - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità governance:
 - Gli utenti con autorizzazioni speciali possono utilizzare un'intestazione di bypass nelle richieste per modificare alcune impostazioni di conservazione.
 - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Impostazioni di conservazione per le versioni degli oggetti

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono utilizzare l'applicazione client S3 per specificare facoltativamente le seguenti impostazioni di conservazione per ogni oggetto aggiunto al bucket:

- **Modalità di conservazione:** Conformità o governance.
- **Mantieni-fino-data:** Se la data di conservazione di una versione dell'oggetto è futura, l'oggetto può essere recuperato, ma non può essere cancellato.
- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa. Le conservazioni legali sono indipendenti dalla conservazione fino alla data odierna.



Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Per i dettagli sulle impostazioni dell'oggetto, fai riferimento a ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

Impostazione di conservazione predefinita per i bucket

Se viene creato un bucket con S3 Object Lock attivato, gli utenti possono specificare le seguenti impostazioni predefinite per il bucket:

- **Modalità di conservazione predefinita:** Conformità o governance.
- **Default Retention Period** (periodo di conservazione predefinito): Per quanto tempo le nuove versioni degli oggetti aggiunte a questo bucket devono essere conservate, a partire dal giorno in cui vengono aggiunte.

Le impostazioni predefinite del bucket si applicano solo ai nuovi oggetti che non dispongono di proprie impostazioni di conservazione. Gli oggetti bucket esistenti non vengono influenzati quando si aggiungono o si modificano queste impostazioni predefinite.

Fai riferimento a ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).

S3 attività di blocco degli oggetti

Gli elenchi seguenti per gli amministratori di grid e gli utenti tenant contengono le attività di alto livello per l'utilizzo della funzione blocco oggetti S3.

Amministratore di grid

- Attiva l'impostazione blocco oggetti S3 globale per l'intero sistema StorageGRID.
- Consenti agli utenti di abilitare S3 Object Lock per i bucket esistenti.
- Assicurarsi che i criteri ILM (Information Lifecycle Management) siano *conformi*, ovvero che soddisfino la ["Requisiti dei bucket con blocco oggetti S3 abilitato"](#).
- Se necessario, consentire a un tenant di utilizzare la modalità di conservazione Compliance. In caso contrario, è consentita solo la modalità Governance.
- In base alle necessità, imposta il periodo di conservazione massimo per un tenant.

Utente tenant

- Esaminare le considerazioni per bucket e oggetti con blocco oggetto S3.
- Se necessario, contatta un amministratore di grid per abilitare una delle seguenti impostazioni:
 - Blocco globale oggetto S3
 - Consenti l'attivazione del blocco oggetti S3 per i bucket esistenti
- Crea bucket con blocco oggetti S3 abilitato.
- Abilita il blocco degli oggetti S3 sui bucket esistenti.
- Facoltativamente, configurare le impostazioni di conservazione predefinite per un bucket:
 - Modalità di conservazione predefinita: Governance o conformità, se consentita dall'amministratore della griglia.
 - Periodo di conservazione predefinito: Deve essere minore o uguale al periodo di conservazione massimo impostato dall'amministratore di rete.
- Utilizzare l'applicazione client S3 per aggiungere oggetti e impostare facoltativamente la conservazione specifica degli oggetti:
 - Modalità di conservazione. Governance o conformità, se consentito dall'amministratore del grid.
 - Mantieni fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia.

Requisiti per i bucket con S3 Object Lock attivato

- Se l'impostazione blocco oggetto S3 globale è attivata per il sistema StorageGRID, è possibile utilizzare Gestione tenant, API di gestione tenant o API REST S3 per creare bucket con blocco oggetto S3 attivato.
- Quando il blocco oggetti S3 è attivato per un bucket, StorageGRID attiva automaticamente il controllo delle versioni per quel bucket. Non puoi disattivare il blocco oggetti S3 o sospendere il controllo delle versioni per il bucket.
- Facoltativamente, è possibile specificare una modalità di conservazione e un periodo di conservazione predefiniti per ciascun bucket utilizzando Tenant Manager, l'API di gestione tenant o l'API REST S3. Le impostazioni di conservazione predefinite del bucket si applicano solo ai nuovi oggetti aggiunti al bucket che non dispongono di proprie impostazioni di conservazione. È possibile eseguire l'override di queste impostazioni predefinite specificando una modalità di conservazione e conservarla fino alla data per ogni versione dell'oggetto al momento del caricamento.
- La configurazione del ciclo di vita del bucket è supportata per i bucket con blocco oggetti S3 attivato.

Requisiti per gli oggetti nei bucket con S3 Object Lock attivato

- Per proteggere una versione dell'oggetto, è possibile specificare le impostazioni di conservazione predefinite per il bucket oppure le impostazioni di conservazione per ciascuna versione dell'oggetto. È possibile specificare le impostazioni di conservazione a livello di oggetto utilizzando l'applicazione client S3 o l'API REST S3.
- Le impostazioni di conservazione si applicano alle singole versioni di oggetti. Una versione a oggetti può avere un'impostazione di conservazione fino alla data e un'impostazione di conservazione legale, una ma non l'altra o nessuna delle due. La specifica di un'impostazione di conservazione fino a data o di conservazione legale per un oggetto protegge solo la versione specificata nella richiesta. È possibile creare nuove versioni dell'oggetto, mentre la versione precedente rimane bloccata.

Ciclo di vita degli oggetti nei bucket con S3 Object Lock attivato

Ogni oggetto salvato in un bucket con S3 Object Lock attivato passa attraverso le seguenti fasi:

1. Acquisizione oggetto

Quando una versione dell'oggetto viene aggiunta al bucket con S3 Object Lock attivato, le impostazioni di conservazione vengono applicate come segue:

- Se per l'oggetto sono specificate le impostazioni di conservazione, vengono applicate le impostazioni a livello di oggetto. Tutte le impostazioni predefinite del bucket vengono ignorate.
- Se non sono specificate impostazioni di conservazione per l'oggetto, vengono applicate le impostazioni predefinite del bucket, se presenti.
- Se non sono specificate impostazioni di conservazione per l'oggetto o il bucket, l'oggetto non è protetto da S3 Object Lock.

Se vengono applicate le impostazioni di conservazione, vengono protetti sia l'oggetto che i metadati S3 definiti dall'utente.

2. Conservazione ed eliminazione degli oggetti

StorageGRID memorizza più copie di ciascun oggetto protetto per il periodo di conservazione specificato. Il numero e il tipo esatti delle copie degli oggetti e le posizioni dello storage sono determinati dalle regole di conformità nelle policy ILM attive. La possibilità di eliminare un oggetto protetto prima che venga raggiunta la data di conservazione dipende dalla modalità di conservazione.

- Se un oggetto è sottoposto a un blocco legale, nessuno può eliminare l'oggetto, indipendentemente dalla modalità di conservazione.

Posso comunque gestire i bucket conformi alle versioni precedenti?

La funzione blocco oggetti S3 sostituisce la funzionalità di conformità disponibile nelle versioni precedenti di StorageGRID. Se sono stati creati bucket conformi utilizzando una versione precedente di StorageGRID, è possibile continuare a gestire le impostazioni di questi bucket; tuttavia, non è più possibile creare nuovi bucket conformi. Per istruzioni, vedere ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#).

Informazioni correlate

Scopri di più ["Requisiti di S3 Object Lock"](#)

Aggiorna la conservazione predefinita di S3 Object Lock in StorageGRID

Se al momento della creazione del bucket è stato attivato il blocco oggetti S3, è possibile modificare il bucket per modificare le impostazioni di conservazione predefinite. È possibile attivare (o disattivare) la conservazione predefinita e impostare una modalità di conservazione e un periodo di conservazione predefiniti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.

- Il blocco oggetti S3 è attivato globalmente per il sistema StorageGRID e il blocco oggetti S3 è stato attivato quando è stato creato il bucket. Vedere ["USA il blocco oggetti S3 per conservare gli oggetti"](#).

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.
2. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

3. Dalla scheda **Opzioni bucket**, selezionare la fisarmonica **S3 Object Lock**.
4. Facoltativamente, attivare o disattivare **Default Retention** per questo bucket.

Le modifiche apportate a questa impostazione non si applicano agli oggetti già presenti nel bucket o a qualsiasi oggetto che potrebbe avere periodi di conservazione propri.

5. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare una **modalità di conservazione predefinita** per il bucket.

Modalità di conservazione predefinita	Descrizione
Governance	• Gli utenti con <code>s3:BypassGovernanceRetention</code> autorizzazione possono utilizzare l' <code>`x-amz-bypass-governance-retention: true`</code> intestazione della richiesta per ignorare le impostazioni di conservazione. • Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione. • Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.
Conformità	• L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione. • La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita. • La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data. Nota: L'amministratore della griglia deve consentire l'utilizzo della modalità di conformità.

6. Se l'opzione **Default Retention** (conservazione predefinita) è attivata, specificare il **Default Retention Period** (periodo di conservazione predefinito) per il bucket.

Il **Default Retention Period** indica per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. Specificare un valore inferiore o uguale al periodo di conservazione massimo per il tenant, come impostato dall'amministratore della griglia.

Un *massimo* periodo di conservazione, che può essere un valore compreso tra 1 giorno e 100 anni, viene impostato quando l'amministratore di rete crea il tenant. Quando si imposta un periodo di conservazione *default*, non può superare il valore impostato per il periodo di conservazione massimo. Se necessario,

chiedere all'amministratore di rete di aumentare o diminuire il periodo di conservazione massimo.

7. Selezionare **Save Changes** (Salva modifiche).

Configura CORS per i bucket S3 in StorageGRID

È possibile configurare la condivisione delle risorse cross-origin (CORS) per un bucket S3 se si desidera che quel bucket e gli oggetti in quel bucket siano accessibili alle applicazioni web in altri domini.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- Per le richieste di configurazione GET CORS, l'utente appartiene a un gruppo di utenti che dispone di ["Gestisci tutti i bucket o Visualizza tutti i bucket"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- Per le richieste di configurazione PUT CORS, l'utente appartiene a un gruppo di utenti che dispone di ["Gestisci autorizzazioni per tutti i bucket"](#). Questa autorizzazione sovrascrive le impostazioni delle autorizzazioni nei criteri di gruppo o bucket.
- ["Autorizzazione di accesso root"](#) Fornisce l'accesso a tutte le richieste di configurazione CORS.

A proposito di questa attività

La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Ad esempio, si supponga di utilizzare un bucket S3 denominato `Images` per memorizzare la grafica. Configurando CORS per il `Images` bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito Web `http://www.example.com`.

Abilitare il CORS per un bucket

Fasi

1. Utilizzare un editor di testo per creare l'XML richiesto. Questo esempio mostra l'XML utilizzato per abilitare il CORS per un bucket S3. In particolare:
 - Consente a qualsiasi dominio di inviare richieste GET al bucket
 - Consente solo al `http://www.example.com` dominio di inviare richieste GET, POST ed ELIMINAZIONE
 - Sono consentite tutte le intestazioni delle richieste

```
<CORSConfiguration
  xmlns="http://s3.amazonaws.com/doc/2020-10-22/">
  <CORSRule>
    <AllowedOrigin>*</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
  <CORSRule>
    <AllowedOrigin>http://www.example.com</AllowedOrigin>
    <AllowedMethod>GET</AllowedMethod>
    <AllowedMethod>POST</AllowedMethod>
    <AllowedMethod>DELETE</AllowedMethod>
    <AllowedHeader>*</AllowedHeader>
  </CORSRule>
</CORSConfiguration>
```

Per ulteriori informazioni sull'XML di configurazione CORS, vedere ["Documentazione di Amazon Web Services \(AWS\): Guida utente di Amazon Simple Storage Service"](#).

2. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket dalla tabella.

Viene visualizzata la pagina dei dettagli del bucket.

4. Dalla scheda **bucket access**, selezionare la fisarmonica **Cross-Origin Resource Sharing (CORS)**.

5. Selezionare la casella di controllo **Enable CORS** (attiva CORS*).

6. Incollare l'XML di configurazione CORS nella casella di testo.

7. Selezionare **Save Changes** (Salva modifiche).

Modificare l'impostazione CORS

Fasi

1. Aggiornare l'XML di configurazione CORS nella casella di testo oppure selezionare **Clear** per ricominciare.

2. Selezionare **Save Changes** (Salva modifiche).

Disattiva l'impostazione CORS

Fasi

1. Deselezionare la casella di controllo **Enable CORS** (attiva CORS*).

2. Selezionare **Save Changes** (Salva modifiche).

Informazioni correlate

["Configurare StorageGRID CORS per un'interfaccia di gestione"](#)

Eliminare oggetti da un bucket S3 di StorageGRID

È possibile utilizzare Tenant Manager per eliminare gli oggetti in uno o più bucket.

Considerazioni e requisiti

Prima di eseguire questa procedura, tenere presente quanto segue:

- Quando si eliminano gli oggetti in un bucket, StorageGRID rimuove in modo permanente tutti gli oggetti e tutte le versioni degli oggetti in ogni bucket selezionato da tutti i nodi e siti nel sistema StorageGRID. StorageGRID rimuove anche i metadati degli oggetti correlati. Non sarà possibile recuperare queste informazioni.
- L'eliminazione di tutti gli oggetti in un bucket può richiedere minuti, giorni o persino settimane, in base al numero di oggetti, copie di oggetti e operazioni simultanee.
- Se un bucket ha **"Blocco oggetti S3 attivato"**, potrebbe rimanere nello stato **Deleting Objects: Read-only** per *years*.



Un bucket che utilizza il blocco oggetti S3 rimarrà nello stato **Deleting Objects: Read-only** (eliminazione oggetti: Sola lettura) fino a quando non viene raggiunta la data di conservazione per tutti gli oggetti e non vengono rimosse le conservazioni legali.

- Durante l'eliminazione degli oggetti, lo stato del bucket è **eliminazione degli oggetti: Sola lettura**. In questo stato, non è possibile aggiungere nuovi oggetti al bucket.
- Una volta cancellati tutti gli oggetti, il bucket rimane in stato di sola lettura. È possibile eseguire una delle seguenti operazioni:
 - Riportare il bucket in modalità di scrittura e riutilizzarlo per nuovi oggetti
 - Eliminare il bucket
 - Mantenere il bucket in modalità di sola lettura per riservare il proprio nome per un utilizzo futuro
- Se in un bucket è attivata la versione oggetto, è possibile rimuovere i marcatori di eliminazione creati in StorageGRID 11,8 o versioni successive utilizzando le operazioni Elimina oggetti nel bucket.
- Se in un bucket è attivata la versione oggetto, l'operazione di eliminazione degli oggetti non rimuoverà i marcatori di eliminazione creati in StorageGRID 11,7 o versioni precedenti. Vedere le informazioni sull'eliminazione di oggetti in un bucket in **"Modalità di eliminazione degli oggetti con versione S3"**.
- Se si utilizza **"replica cross-grid"**, tenere presente quanto segue:
 - L'utilizzo di questa opzione non elimina alcun oggetto dal bucket dell'altra griglia.
 - Se si seleziona questa opzione per il bucket di origine, l'avviso **errore replica cross-grid** verrà attivato se si aggiungono oggetti al bucket di destinazione sull'altra griglia. Se non è possibile garantire che nessuno aggiungerà oggetti al bucket sull'altra griglia, **"disattiva la replica cross-grid"** per quel bucket prima di eliminare tutti gli oggetti bucket.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un **"browser web supportato"**.
- L'utente appartiene a un gruppo di utenti che dispone di **"Autorizzazione di accesso root"**. Questa autorizzazione sovrascrive le impostazioni delle autorizzazioni nei criteri di gruppo o bucket.

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.

2. Utilizzare il menu **azioni** o la pagina dei dettagli per un bucket specifico.

Menu delle azioni

- Selezionare la casella di controllo per ciascun bucket da cui si desidera eliminare gli oggetti.
- Selezionare **azioni** > **Elimina oggetti nel bucket**.

Pagina dei dettagli

- Selezionare il nome di un bucket per visualizzarne i dettagli.
- Selezionare **Elimina oggetti nel bucket**.

3. Quando viene visualizzata la finestra di dialogo di conferma, rivedere i dettagli, inserire **Sì** e selezionare **OK**.

4. Attendere l'inizio dell'operazione di eliminazione.

Dopo alcuni minuti:

- Nella pagina dei dettagli del bucket viene visualizzato un banner di stato giallo. La barra di avanzamento indica la percentuale di oggetti eliminati.
- * (sola lettura)* viene visualizzato dopo il nome del bucket nella pagina dei dettagli del bucket.
- (eliminazione di oggetti: Sola lettura)** viene visualizzato accanto al nome del bucket nella pagina bucket.

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

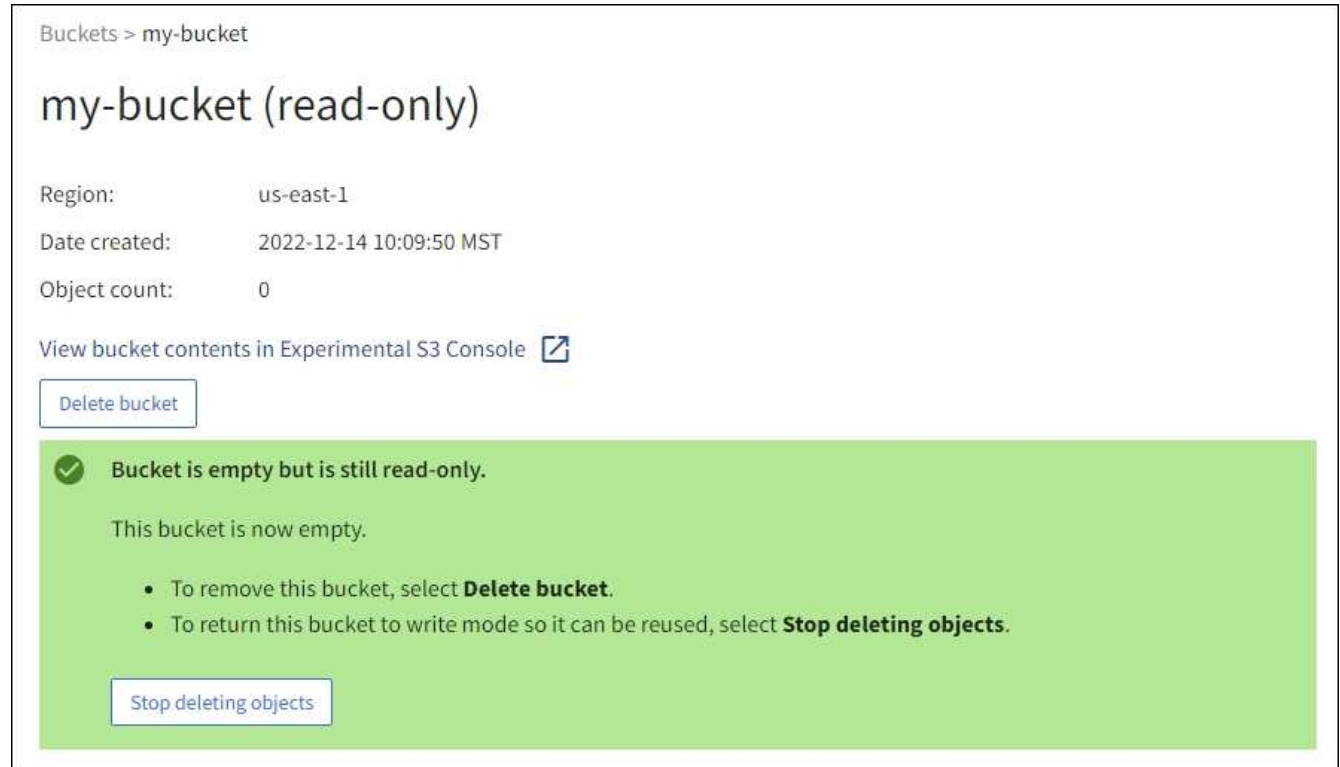
5. Quando l'operazione è in esecuzione, selezionare **Stop deleting objects** (Interrompi eliminazione oggetti) per interrompere il processo. Quindi, se si desidera, selezionare **Delete Objects in bucket** (Elimina oggetti

nel bucket) per riprendere il processo.

Quando si seleziona **Stop deleting objects**, il bucket torna alla modalità di scrittura; tuttavia, non è possibile accedere o ripristinare gli oggetti che sono stati cancellati.

6. Attendere il completamento dell'operazione.

Quando il bucket è vuoto, il banner di stato viene aggiornato, ma il bucket rimane di sola lettura.



7. Effettuare una delle seguenti operazioni:

- Uscire dalla pagina per mantenere il bucket in modalità di sola lettura. Ad esempio, è possibile mantenere un bucket vuoto in modalità di sola lettura per riservare il nome del bucket per un utilizzo futuro.
- Eliminare il bucket. È possibile selezionare **Delete bucket** (Elimina bucket) per eliminare un singolo bucket o tornare alla pagina Bucket e selezionare **Actions > Delete bucket** (azioni* > Delete bucket) per rimuovere più bucket.



Se non si riesce a eliminare un bucket con versione dopo l'eliminazione di tutti gli oggetti, i contrassegni di eliminazione potrebbero rimanere. Per eliminare il bucket, è necessario rimuovere tutti gli altri marker di eliminazione.

- Riportare il bucket in modalità di scrittura e, se si desidera, riutilizzarlo per nuovi oggetti. È possibile selezionare **Interrompi eliminazione oggetti** per un singolo bucket o tornare alla pagina bucket e selezionare **azione > Interrompi eliminazione oggetti** per più bucket.

Eliminare un bucket S3 di StorageGRID

È possibile utilizzare Tenant Manager per eliminare uno o più bucket S3 vuoti.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni delle autorizzazioni nelle policy di gruppo o bucket.
- I bucket che si desidera eliminare sono vuoti. Se i bucket che si desidera eliminare sono *non* vuoti, ["eliminare gli oggetti dal bucket"](#).

A proposito di questa attività

Queste istruzioni descrivono come eliminare un bucket S3 utilizzando il Tenant Manager. È inoltre possibile eliminare i bucket S3 utilizzando ["API di gestione del tenant"](#) o ["API REST S3"](#).

Non è possibile eliminare un bucket S3 se contiene oggetti, versioni di oggetti non correnti o contrassegni di eliminazione. Per informazioni sull'eliminazione degli oggetti con versione S3, vedere ["Modalità di eliminazione degli oggetti"](#).

Fasi

1. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

Viene visualizzata la pagina bucket che mostra tutti i bucket S3 esistenti.

2. Utilizzare il menu **azioni** o la pagina dei dettagli per un bucket specifico.

Menu delle azioni

- a. Selezionare la casella di controllo per ciascun bucket che si desidera eliminare.
- b. Selezionare **azioni > Elimina bucket**.

Pagina dei dettagli

- a. Selezionare il nome di un bucket per visualizzarne i dettagli.
- b. Selezionare **Delete bucket** (Elimina bucket).

3. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì**.

StorageGRID conferma che ogni bucket è vuoto e quindi elimina ogni bucket. Questa operazione potrebbe richiedere alcuni minuti.

Se un bucket non è vuoto, viene visualizzato un messaggio di errore. È necessario ["eliminare tutti gli oggetti ed eventuali marcatori di eliminazione nel bucket"](#) prima di poter eliminare il bucket.

Usa la console S3 in StorageGRID

È possibile utilizzare S3 Console per visualizzare e gestire gli oggetti in un bucket S3.

La console S3 consente di:

- Caricamento, download, ridenominazione, copia, spostamento, ed eliminare gli oggetti
- Visualizzare, ripristinare, scaricare ed eliminare le versioni degli oggetti
- Cercare gli oggetti in base al prefisso

- Gestire tag di oggetti
- Visualizzare i metadati degli oggetti
- Visualizzare, creare, rinominare, copiare, spostare, ed eliminare le cartelle

La console S3 offre un'esperienza utente migliorata per i casi più comuni. Non è progettato per sostituire le operazioni CLI o API in tutte le situazioni.



Se l'utilizzo di S3 Console comporta un'operazione troppo lunga (ad esempio, minuti o ore), considerare quanto segue:

- Riduzione del numero di oggetti selezionati
- Utilizzando metodi non grafici (API o CLI) per accedere ai dati

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- Se si desidera gestire gli oggetti, si appartiene a un gruppo di utenti che dispone dell'autorizzazione di accesso principale. In alternativa, si appartiene a un gruppo di utenti che dispone dell'autorizzazione Usa scheda Console S3 e dell'autorizzazione Visualizza tutti i bucket o Gestisci tutti i bucket. Vedere ["Permessi di gestione del tenant"](#).
- Per l'utente è stato configurato un criterio di gruppo o bucket S3. Vedere ["Utilizza policy di accesso a bucket e gruppi"](#).
- Conosci l'ID della chiave di accesso dell'utente e la chiave di accesso segreta. Facoltativamente, si dispone di un `.csv` file contenente queste informazioni. Consultare la ["istruzioni per la creazione delle chiavi di accesso"](#).

Fasi

1. Selezionare **Archiviazione > Bucket > nome bucket**.
2. Selezionare la scheda Console S3.
3. Incollare l'ID della chiave di accesso e la chiave di accesso segreta nei campi. Altrimenti, selezionare **Upload access keys** e selezionare il `.csv` file.
4. Selezionare **Accedi**.
5. Viene visualizzata la tavola degli oggetti bucket. È possibile gestire gli oggetti in base alle esigenze.

Ulteriori informazioni

- **Cerca per prefisso:** La funzione di ricerca del prefisso ricerca solo gli oggetti che iniziano con una parola specifica relativa alla cartella corrente. La ricerca non include oggetti che contengono la parola altrove. Questa regola si applica anche agli oggetti all'interno delle cartelle. Ad esempio, una ricerca `folder1/folder2/somefile-` restituisce gli oggetti all'interno della `folder1/folder2/` cartella e inizia con la parola `somefile-`.
- **Trascinare e rilasciare:** È possibile trascinare i file dal file manager del computer a S3 Console. Tuttavia, non è possibile caricare le cartelle.
- **Operazioni sulle cartelle:** Quando si sposta, copia o rinomina una cartella, tutti gli oggetti nella cartella vengono aggiornati uno alla volta, il che potrebbe richiedere del tempo.
- **Eliminazione permanente quando la versione bucket è disattivata:** Quando si sovrascrive o si elimina un oggetto in un bucket con la versione disattivata, l'operazione è permanente. Vedere ["Modificare la versione degli oggetti per un bucket"](#).

Gestire i servizi della piattaforma S3

Servizi della piattaforma S3

Scopri i servizi della piattaforma per StorageGRID

Prima di implementare i servizi della piattaforma, esaminare la panoramica e le considerazioni relative all'utilizzo di tali 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 di cloud ibrido consentendo di inviare notifiche di eventi e copie di oggetti S3 e metadati di oggetti a destinazioni esterne.

Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna all'implementazione di StorageGRID, i servizi della piattaforma offrono la potenza e la flessibilità derivanti dall'utilizzo di risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi per i dati.

È possibile configurare qualsiasi combinazione di servizi della piattaforma per un singolo bucket S3. Ad esempio, puoi configurare sia ["Servizio CloudMirror"](#) sia ["notifiche"](#) su un bucket S3 di StorageGRID così da poter replicare oggetti specifici su Amazon Simple Storage Service (S3), inviando allo stesso tempo una notifica relativa a ciascun oggetto a un'applicazione di monitoraggio di terze parti per aiutarti a tenere traccia delle spese AWS.



L'utilizzo dei servizi della piattaforma deve essere abilitato per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione del grid.

Modalità di configurazione dei servizi della piattaforma

I servizi della piattaforma comunicano con endpoint esterni configurati tramite ["Manager tenant"](#) o il ["API di gestione del tenant"](#). Ogni endpoint rappresenta una destinazione esterna, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon SNS, un endpoint webhook o un cluster Elasticsearch ospitato localmente, su AWS o altrove.

Dopo aver creato un endpoint esterno, è possibile attivare un servizio di piattaforma per un bucket aggiungendo la configurazione XML al bucket. La configurazione XML identifica gli oggetti su cui il bucket deve agire, l'azione che il bucket deve intraprendere e l'endpoint che il bucket deve utilizzare per il servizio.

È necessario aggiungere configurazioni XML separate per ogni servizio di piattaforma che si desidera configurare. Ad esempio:

- Se si desidera che tutti gli oggetti le cui chiavi iniziano con `/images` vengano replicati in un bucket Amazon S3, è necessario aggiungere una configurazione di replica al bucket di origine.
- Se si desidera anche inviare notifiche quando questi oggetti vengono memorizzati nel bucket, è necessario aggiungere una configurazione di notifica.
- Se si desidera indicizzare i metadati per questi oggetti, è necessario aggiungere la configurazione di notifica dei metadati utilizzata per implementare l'integrazione della ricerca.

Il formato per l'XML di configurazione è regolato dalle API REST S3 utilizzate per implementare i servizi della piattaforma StorageGRID:

Servizio di piattaforma	API REST S3	Fare riferimento a.
Replica di CloudMirror	• GetBucketReplication • PutBucketReplication	• "Replica di CloudMirror" • "Operazioni sui bucket"
Notifiche	• GetBucketNotificationConfiguration • PutBucketNotificationConfiguration	• "Notifiche" • "Operazioni sui bucket"
Integrazione della ricerca	• OTTENERE la configurazione della notifica dei metadati del bucket • INSERIRE la configurazione della notifica dei metadati del bucket	• "Integrazione della ricerca" • "Operazioni personalizzate di StorageGRID"

Considerazioni sull'utilizzo dei servizi della piattaforma

Considerazione	Dettagli
Monitoraggio degli endpoint di destinazione	È necessario monitorare la disponibilità di ciascun endpoint di destinazione. Se la connettività all'endpoint di destinazione viene persa per un periodo di tempo prolungato ed esiste un grande backlog di richieste, le richieste client aggiuntive (come LE richieste PUT) a StorageGRID non avranno esito positivo. È necessario riprovare queste richieste non riuscite quando l'endpoint diventa raggiungibile.
Rallentamento dell'endpoint di destinazione	Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione. L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire. È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Considerazione	Dettagli
Garanzie di ordinazione	StorageGRID garantisce l'ordine delle operazioni su un oggetto all'interno di un sito. Finché tutte le operazioni relative a un oggetto si trovano all'interno dello stesso sito, lo stato finale dell'oggetto (per la replica) sarà sempre uguale allo stato in StorageGRID. StorageGRID tenta al meglio di ordinare le richieste quando le operazioni vengono eseguite nei siti StorageGRID. Ad esempio, se si scrive inizialmente un oggetto nel sito A e successivamente si sovrascrive lo stesso oggetto nel sito B, l'oggetto finale replicato da CloudMirror nel bucket di destinazione non è garantito come l'oggetto più recente.
Eliminazioni di oggetti basate su ILM	Per far fronte al comportamento di eliminazione del CRR AWS e del servizio di notifica Amazon Simple, CloudMirror e le richieste di notifica degli eventi non vengono inviate quando un oggetto nel bucket di origine viene eliminato a causa delle regole ILM di StorageGRID. Ad esempio, se una regola ILM elimina un oggetto dopo 14 giorni, non viene inviata alcuna richiesta di notifica di CloudMirror o di evento. Al contrario, le richieste di integrazione della ricerca vengono inviate quando gli oggetti vengono eliminati a causa di ILM.
Utilizzo degli endpoint Kafka	L'autenticazione degli endpoint Kafka utilizza i seguenti tipi di autenticazione. Questi tipi sono diversi da quelli utilizzati per l'autenticazione di altri endpoint, come Amazon SNS, e richiedono credenziali per nome utente e password. • SASL/SEMPlice • SASL/SCRAM-SHA-256 • SASL/SCRAM-SHA-512 Nota: le impostazioni proxy di archiviazione configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Considerazioni sull'utilizzo del servizio di replica CloudMirror

Considerazione	Dettagli
Stato della replica	StorageGRID non supporta la <code>x-amz-replication-status</code> testata.
Dimensione dell'oggetto	La dimensione massima per gli oggetti che possono essere replicati in un bucket di destinazione dal servizio di replica CloudMirror è 5 TiB, che corrisponde alla dimensione massima dell'oggetto <i>supportata</i>. Nota: La dimensione massima <i>raccomandata</i> per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.

Considerazione	Dettagli
Versioni e ID della versione del bucket	Se il bucket S3 di origine in StorageGRID ha attivato la versione, è necessario attivare anche la versione per il bucket di destinazione. Quando usi il versioning, tieni presente che l'ordine delle versioni degli oggetti nel bucket di destinazione è approssimativo e non garantito dal servizio CloudMirror, a causa delle limitazioni del protocollo S3. Inoltre, i bucket di destinazione manterranno le proprie impostazioni e potrebbero non fornire il versioning. Nota: Gli ID della versione per il bucket di origine in StorageGRID non sono correlati agli ID della versione per il bucket di destinazione.
Tagging per le versioni degli oggetti	Il servizio CloudMirror non replica le richieste PutObjectTagging o DeleteObjectTagging che forniscono un ID di versione, a causa delle limitazioni del protocollo S3. Poiché gli ID di versione per l'origine e la destinazione non sono correlati, non esiste alcun modo per garantire che venga replicato un aggiornamento del tag a un ID di versione specifico. Al contrario, il servizio CloudMirror replica le richieste PutObjectTagging o DeleteObjectTagging che non specificano un ID di versione. Queste richieste aggiornano i tag per la chiave più recente (o la versione più recente se il bucket è in versione). Vengono replicati anche i normali ingest con tag (senza tagging degli aggiornamenti).
Caricamenti e valori multipart ETag	Quando si esegue il mirroring degli oggetti caricati utilizzando un caricamento multipart, il servizio CloudMirror non conserva le parti. Di conseguenza, il ETag valore per l'oggetto speculare sarà diverso dal 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 acquisire un oggetto nel bucket di origine per la replica CloudMirror e la richiesta include le intestazioni di richiesta SSE-C, l'operazione non riesce.
Bucket con blocco oggetti S3 attivato	Se il bucket S3 di origine in StorageGRID ha S3 Object Lock abilitato, dovresti abilitare S3 Object Lock anche per il bucket di destinazione con la conservazione predefinita configurata. La replica dei <i>dati oggetto</i> è supportata per i bucket di origine e di destinazione con S3 Object Lock abilitato. Tuttavia, i bucket di destinazione manterranno le proprie impostazioni per la conservazione degli oggetti e potrebbero non fornire la conformità o il versioning.

Scopri il servizio di replica CloudMirror di StorageGRID

È possibile abilitare la replica CloudMirror per un bucket S3 se si desidera che StorageGRID replichi oggetti specificati aggiunti al bucket in uno o più bucket di destinazione esterni.

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



CloudMirror replication è supportata solo se il bucket di origine ha S3 Object Lock abilitato e l'endpoint è un bucket S3 di Amazon o StorageGRID. Le impostazioni di Object Lock non vengono replicate nell'endpoint del bucket.

CloudMirror e ILM

La replica CloudMirror funziona indipendentemente dalle policy ILM attive del grid. Il servizio CloudMirror replica gli oggetti memorizzati nel bucket di origine e li consegna al bucket di destinazione il prima possibile. La consegna degli oggetti replicati viene attivata quando l'acquisizione degli oggetti ha esito positivo.

CloudMirror e replica cross-grid

La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Fare riferimento alla ["Confronta la replica cross-grid e la replica CloudMirror"](#).

Bucket Cloud Mirror e S3

La replica di CloudMirror è generalmente configurata per utilizzare un bucket S3 esterno come destinazione. Tuttavia, è anche possibile configurare la replica in modo che utilizzi un'altra implementazione StorageGRID o qualsiasi servizio compatibile con S3.

Bucket esistenti

Quando si attiva la replica CloudMirror per un bucket esistente, vengono replicati solo i nuovi oggetti aggiunti a tale bucket. Gli oggetti esistenti nel bucket non vengono replicati. Per forzare la replica degli oggetti esistenti, è possibile aggiornare i metadati dell'oggetto esistente eseguendo una copia dell'oggetto.



Se si utilizza la replica CloudMirror per copiare oggetti in una destinazione Amazon S3, tenere presente che Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione della richiesta PUT a 2 KB. Se un oggetto ha metadati definiti dall'utente superiori a 2 KB, tale oggetto non verrà replicato.

Bucket multipli di destinazione

Per replicare gli oggetti in un singolo bucket in più bucket di destinazione, specificare la destinazione per ogni regola nell'XML di configurazione della replica. Non è possibile replicare un oggetto in più bucket contemporaneamente.

Benne in versione o non in versione

È possibile configurare la replica di CloudMirror nei bucket con versione o senza versione. I bucket di destinazione possono essere aggiornati o non aggiornati. È possibile utilizzare qualsiasi combinazione di bucket con versione e senza versione. Ad esempio, è possibile specificare un bucket con versione come destinazione per un bucket di origine senza versione o viceversa. È inoltre possibile eseguire la replica tra bucket senza versione.

Eliminazione, loop di replica ed eventi

Comportamento di eliminazione

È uguale al 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 entrambi con versione, il marker di eliminazione viene replicato. Se il bucket di destinazione non è dotato di versione, l'eliminazione di un oggetto nel bucket di origine non replica il contrassegno di eliminazione nel bucket di destinazione o elimina l'oggetto di destinazione.

Protezione dai loop di replica

Quando gli oggetti vengono replicati nel bucket di destinazione, StorageGRID li contrassegna come "repliche". Un bucket StorageGRID di destinazione non replicerà gli oggetti contrassegnati come repliche, proteggendoti da loop di replica accidentali. Questo contrassegno di replica è interno a StorageGRID e non ti impedisce di sfruttare il CRR AWS quando utilizzi un bucket Amazon S3 come destinazione.



L'intestazione personalizzata utilizzata per contrassegnare una replica è `x-ntap-sg-replica`. Questo contrassegno impedisce un mirror a cascata. StorageGRID supporta un CloudMirror bidirezionale tra due griglie.

Eventi nel bucket di destinazione

L'unicità e l'ordinamento degli eventi nel bucket di destinazione non sono garantiti. Più di una copia identica di un oggetto di origine potrebbe essere consegnata alla destinazione in seguito alle operazioni eseguite per garantire il successo della consegna. In rari casi, quando lo stesso oggetto viene aggiornato simultaneamente da due o più siti StorageGRID diversi, l'ordine delle operazioni sul bucket di destinazione potrebbe non corrispondere all'ordine degli eventi sul bucket di origine.

Scopri le notifiche degli eventi di StorageGRID per i bucket S3

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, a un endpoint webhook o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.

Le notifiche degli eventi vengono create nel bucket di origine come specificato nella configurazione della notifica e vengono inviate alla destinazione. Se un evento associato a un oggetto ha esito positivo, viene creata una notifica relativa a tale evento e messa in coda per il recapito.

L'unicità e l'ordine delle notifiche non sono garantiti. È possibile che più di una notifica di un evento venga inviata alla destinazione a seguito delle operazioni eseguite per garantire il successo della consegna. Inoltre, poiché la consegna è asincrona, non è garantito che l'ordine temporale delle notifiche alla destinazione corrisponda all'ordine degli eventi nel bucket di origine, in particolare per le operazioni provenienti da diversi siti StorageGRID. È possibile utilizzare il `sequencer` campo nel messaggio dell'evento per determinare l'ordine degli eventi per un particolare oggetto, 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 evento:
 - S3:ObjectCreated:
 - s3:ObjectCreated:put
 - s3:ObjectCreated:Post
 - s3:ObjectCreated:Copy
 - s3:ObjectCreated:CompleteMultipartUpload
 - S3:ObjectRemoved:
 - s3:ObjectRemoved:Elimina
 - s3:ObjectRemoved>DeleteMarkerCreated
 - s3:ObjectRestore:Post

- Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ma non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nella tabella:

Nome della chiave	Valore StorageGRID
EventSource	sgws:s3
AwsRegion	<i>non incluso</i>
x-amz-id-2	<i>non incluso</i>
arn	urn:sgws:s3:::bucket_name

Scopri il servizio di integrazione della ricerca StorageGRID

È possibile attivare l'integrazione della ricerca per un bucket S3 se si desidera utilizzare un servizio di ricerca e analisi dei dati esterno per i metadati degli oggetti.

Il servizio di integrazione della ricerca è un servizio StorageGRID personalizzato che invia in modo automatico e asincrono i metadati degli oggetti S3 a un endpoint di destinazione ogni volta che un oggetto viene creato o eliminato o quando i relativi metadati o tag vengono aggiornati. Potrai quindi utilizzare sofisticati strumenti di ricerca, analisi dei dati, visualizzazione o apprendimento automatico forniti dal servizio di destinazione per cercare, analizzare e ottenere informazioni dai dati degli oggetti.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.

Sebbene l'integrazione di Elasticsearch possa essere configurata in un bucket con blocco oggetto S3 abilitato, i metadati S3 Object Lock (incluso lo stato Retain until Date e Legal Hold) degli oggetti non verranno inclusi nei metadati inviati a Elasticsearch.



Poiché il servizio di integrazione della ricerca fa sì che i metadati degli oggetti vengano inviati a una destinazione, il relativo XML di configurazione viene definito "*metadata* Notification Configuration XML". Questo XML di configurazione è diverso dal "XML di configurazione delle notifiche" utilizzato per attivare le notifiche *event*.

Integrazione di ricerca e bucket S3

È possibile attivare il servizio di integrazione della ricerca per qualsiasi bucket con versione o senza versione. L'integrazione della ricerca viene configurata associando XML di configurazione della notifica dei metadati al bucket che specifica gli oggetti su cui agire e la destinazione dei metadati dell'oggetto.

Le notifiche dei metadati vengono generate sotto forma di un documento JSON denominato con il nome del bucket, il nome dell'oggetto e l'ID 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 dell'utente.



Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Cerca notifiche

Le notifiche sui metadati vengono generate e messe in coda per essere inviate quando:

- Viene creato un oggetto.
- Un oggetto viene eliminato, anche quando gli oggetti vengono eliminati in seguito all'operazione della policy ILM della griglia.
- I tag o i metadati degli oggetti vengono aggiunti, aggiornati o cancellati. L'insieme completo di metadati e tag viene sempre inviato in seguito all'aggiornamento, non solo i valori modificati.

Dopo aver aggiunto XML per la configurazione delle notifiche dei metadati a un bucket, vengono inviate notifiche per i nuovi oggetti creati e per gli oggetti modificati aggiornando i dati, i metadati dell'utente o i tag. Tuttavia, non vengono inviate notifiche per oggetti già presenti nel bucket. Per garantire che i metadati degli oggetti per tutti gli oggetti nel bucket vengano inviati alla destinazione, eseguire una delle seguenti operazioni:

- Configurare il servizio di integrazione della ricerca subito dopo la creazione del bucket e prima di aggiungere oggetti.
- Eseguire un'azione su tutti gli oggetti già presenti nel bucket che attiverà l'invio di un messaggio di notifica dei metadati alla destinazione.

Servizio di integrazione della ricerca ed Elasticsearch

Il servizio di integrazione della ricerca di StorageGRID supporta un cluster Elasticsearch come destinazione. Come per gli altri servizi della piattaforma, la destinazione viene specificata nell'endpoint il cui URN viene utilizzato nel XML di configurazione per il servizio. Utilizzare "[Tool di matrice di interoperabilità NetApp](#)" per determinare le versioni supportate di Elasticsearch.

Gestire gli endpoint dei servizi della piattaforma

Configura gli endpoint dei servizi della piattaforma in StorageGRID

Prima di poter configurare un servizio di piattaforma per un bucket, è necessario configurare almeno un endpoint in modo che sia la destinazione del servizio di piattaforma.

L'accesso ai servizi della piattaforma viene attivato per tenant da un amministratore di StorageGRID. Per creare o utilizzare un endpoint di servizi di piattaforma, è necessario essere un utente tenant con autorizzazione di accesso Gestisci endpoint o root, in una griglia la cui rete è stata configurata per consentire ai nodi di storage di accedere alle risorse esterne degli endpoint. Per un singolo tenant, è possibile configurare un massimo di 500 endpoint di servizi della piattaforma. Per ulteriori informazioni, contattare l'amministratore di StorageGRID.

Che cos'è un endpoint di servizi di piattaforma?

Un endpoint dei servizi di piattaforma specifica le informazioni necessarie a StorageGRID per accedere alla destinazione esterna.

Ad esempio, se si desidera replicare gli oggetti da un bucket StorageGRID a un bucket Amazon S3, si crea un endpoint dei servizi della piattaforma che include le informazioni e le credenziali necessarie a StorageGRID per accedere al bucket di destinazione su Amazon.

Ogni tipo di servizio di piattaforma richiede un proprio endpoint, pertanto è necessario configurare almeno un endpoint per ogni servizio di piattaforma che si intende utilizzare. Dopo aver definito un endpoint di servizi di piattaforma, si utilizza l'URN dell'endpoint come destinazione nel XML di configurazione utilizzato per attivare il servizio.

È possibile utilizzare lo stesso endpoint della destinazione per più bucket di origine. Ad esempio, è possibile configurare diversi bucket di origine per inviare metadati di oggetto allo stesso endpoint di integrazione della ricerca, in modo da poter eseguire ricerche in più bucket. È inoltre possibile configurare un bucket di origine per utilizzare più endpoint come destinazione, che consente di eseguire operazioni quali l'invio di notifiche sulla creazione di oggetti a un argomento Amazon Simple Notification Service (Amazon SNS) e notifiche sull'eliminazione di oggetti a un secondo argomento Amazon SNS.

Endpoint per la replica di CloudMirror

StorageGRID supporta endpoint di replica che rappresentano i bucket S3. Questi bucket potrebbero essere ospitati su Amazon Web Services, sullo stesso o in un'implementazione remota di StorageGRID o su un altro servizio.

Endpoint per le notifiche

StorageGRID supporta endpoint Amazon SNS, Kafka e webhook. Gli endpoint Simple Queue Service (SQS) e AWS Lambda non sono supportati.

Endpoint per il servizio di integrazione della ricerca

StorageGRID supporta endpoint di integrazione della ricerca che rappresentano cluster Elasticsearch. Questi cluster di Elasticsearch possono trovarsi in un data center locale o in un cloud AWS o altrove.

L'endpoint di integrazione della ricerca si riferisce a un tipo e un indice Elasticsearch specifici. È necessario creare l'indice in Elasticsearch prima di creare l'endpoint in StorageGRID, altrimenti la creazione dell'endpoint non avrà esito positivo. Non è necessario creare il tipo prima di creare l'endpoint. StorageGRID crea il tipo, se necessario, quando invia i metadati dell'oggetto all'endpoint.

Informazioni correlate

["Amministrare StorageGRID"](#)

Specificare un URN per un endpoint dei servizi della piattaforma StorageGRID

Quando si crea un endpoint dei servizi della piattaforma, è necessario specificare un nome di risorsa (URN) univoco. Verrà utilizzato l'URN per fare riferimento all'endpoint quando si crea un XML di configurazione per il servizio di piattaforma. L'URN per ciascun endpoint deve essere univoco.

StorageGRID convalida gli endpoint dei servizi della piattaforma durante la loro creazione. Prima di creare un endpoint di servizi di piattaforma, verificare che la risorsa specificata nell'endpoint esista e che sia possibile

raggiungerla.

Elementi DI URNA

L'URN per un endpoint 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), utilizza `arn:aws`
- Se il servizio è ospitato localmente, utilizzare `urn:mysite`

Ad esempio, se si specifica l'URN per un endpoint CloudMirror ospitato su StorageGRID, l'URN potrebbe iniziare con `urn:sgws`.

L'elemento successivo dell'URN specifica il tipo di servizio della piattaforma, come segue:

Servizio	Tipo
Replica di CloudMirror	s3
Notifiche	sns, kafka , O webhook
Integrazione della ricerca	es

Ad esempio, per continuare a specificare l'URN per un endpoint CloudMirror ospitato su StorageGRID, aggiungere `s3` a `get urn:sgws:s3`.

Per la maggior parte degli endpoint, l'elemento finale dell'URN identifica la risorsa di destinazione specifica nell'URI di destinazione, ad esempio, `sns-topic-name` .

Per gli endpoint webhook, la risorsa di destinazione è l'URI di destinazione stesso.

Servizio	Risorsa specifica
Replica di CloudMirror	<code>bucket-name</code>
Notifiche	<code>sns-topic-name</code> o <code>kafka-topic-name</code> Nota: per gli endpoint webhook, l'elemento finale dell'URN può essere qualsiasi stringa, purché l'URN dell'endpoint sia univoco.
Integrazione della ricerca	<code>domain-name/index-name/type-name</code> Nota: se il cluster Elasticsearch è non configurato per creare gli indici automaticamente, è necessario creare l'indice manualmente prima di creare l'endpoint.

Urns per i servizi ospitati su AWS e GCP

Per le entità AWS e GCP, l'URN completo è un ARN AWS valido. Ad esempio:

- Replica di CloudMirror:

```
arn:aws:s3:::bucket-name
```

- Notifiche:

```
arn:aws:sns:region:account-id:topic-name
```

- Integrazione della ricerca:

```
arn:aws:es:region:account-id:domain/domain-name/index-name/type-name
```



Per un endpoint di integrazione della ricerca AWS, `domain-name` deve includere la stringa letterale `domain/`, come mostrato qui.

Urns per servizi in hosting locale

Quando si utilizzano servizi ospitati in locale invece di servizi cloud, è possibile specificare l'URN in qualsiasi modo che crei un URN valido e univoco, purché l'URN includa gli elementi richiesti nella terza e ultima posizione. È possibile lasciare vuoti gli elementi indicati da opzionale oppure specificarli in qualsiasi modo che consenta di identificare la risorsa e rendere l'URN unico. Ad esempio:

- Replica di CloudMirror:

```
urn:mysite:s3:::bucket-name
```

Per un endpoint CloudMirror ospitato su StorageGRID, è possibile specificare un URN valido che inizia con `urn:sgws:`

```
urn:sgws:s3:::bucket-name
```

- Notifiche:

Specificare un endpoint di Amazon Simple Notification Service:

```
urn:aws:sns:region:account-id:sns-topic-name
```

Specificare un endpoint Kafka:

```
urn::kafka:::kafka-topic-name
```



Facoltativamente, puoi includere `mysite` quando specifichi un endpoint Kafka:
`urn:mysite:kafka:::kafka-topic-name`

Specificare un endpoint webhook:

```
urn:mysite:webhook:::webhook-name
```

- Integrazione della ricerca:

```
urn:mysite:es:::domain-name/index-name/type-name
```



Per gli endpoint di integrazione della ricerca ospitati localmente, l'elemento può essere qualsiasi stringa, `domain-name` purché l'URN dell'endpoint sia univoco.

Creare un endpoint dei servizi della piattaforma StorageGRID

È necessario creare almeno un endpoint del tipo corretto prima di poter attivare un servizio di piattaforma.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire gli endpoint o l'autorizzazione di accesso root"](#).
- La risorsa a cui fa riferimento l'endpoint dei servizi della piattaforma è stata creata:
 - Replica di CloudMirror: Bucket S3
 - Notifica evento: argomento Amazon Simple Notification Service (Amazon SNS), argomento Kafka o endpoint webhook
 - Notifica di ricerca: indice Elasticsearch, se il cluster di destinazione non è configurato per creare automaticamente indici.
- Si dispone delle informazioni relative alla risorsa di destinazione:
 - Host e porta per l'Uniform Resource Identifier (URI)



Se si prevede di utilizzare un bucket ospitato su un sistema StorageGRID come endpoint per la replica di CloudMirror, contattare l'amministratore del grid per determinare i valori da inserire.

- Nome risorsa univoco (URN)

["Specificare URN per l'endpoint dei servizi della piattaforma"](#)

- Credenziali di autenticazione (se richieste):

Endpoint di integrazione della ricerca

Per gli endpoint di integrazione della ricerca, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
- HTTP di base: Nome utente e password

Endpoint di replica CloudMirror

Per gli endpoint di replica di CloudMirror, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key
- CAP (C2S Access Portal): URL con credenziali temporanee, certificati server e client, chiavi client e passphrase opzionale con chiave privata del client.

Endpoint Amazon SNS

Per gli endpoint Amazon SNS, è possibile utilizzare le seguenti credenziali:

- Access Key (chiave di accesso): Access key ID (ID chiave di accesso) e secret access key

Endpoint Kafka

Per gli endpoint Kafka, è possibile utilizzare le seguenti credenziali:

- SASL/PLAIN: Nome utente e password
- SASL/SCRAM-SHA-256: Nome utente e password
- SASL/SCRAM-SHA-512: Nome utente e password

- Certificato di sicurezza (se è richiesta la verifica del certificato)

- Se le funzioni di protezione di Elasticsearch sono attivate, si dispone del privilegio del cluster di monitoraggio per il test di connettività e del privilegio di scrittura dell'indice o di entrambi i privilegi di indice e di eliminazione per gli aggiornamenti dei documenti.

Fasi

1. Selezionare **STORAGE (S3) > Platform Services Endpoint**. Viene visualizzata la pagina Platform Services Endpoint.
2. Selezionare **Crea endpoint**.
3. Inserire un nome visualizzato per descrivere brevemente l'endpoint e il suo scopo.

Il tipo di servizio 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 URI HTTPS e porta 80 per URI HTTP (la maggior parte degli endpoint)
- Porta 9092 per URI HTTPS e HTTP (solo endpoint Kafka)

Ad esempio, l'URI per un bucket ospitato su StorageGRID potrebbe essere:

```
https://s3.example.com:10443
```

In questo esempio, `s3.example.com` rappresenta la voce DNS per l'IP virtuale (VIP) del gruppo ha (StorageGRID High Availability) e `10443` rappresenta la porta definita nell'endpoint del bilanciamento del carico.



Quando possibile, è necessario connettersi a un gruppo ha di nodi per il bilanciamento del carico per evitare un singolo punto di errore.

Analogamente, l'URI per un bucket ospitato su AWS potrebbe essere:

```
https://s3-aws-region.amazonaws.com
```



Se l'endpoint viene utilizzato per il servizio di replica CloudMirror, non includere il nome del bucket nell'URI. Il nome del bucket viene incluso nel campo **URN**.

5. Immettere il nome di risorsa (URN) univoco per l'endpoint.



Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

6. Selezionare **continua**.

7. Selezionare un valore per **tipo di autenticazione**.



Se si desidera l'autenticazione per gli endpoint webhook, configurare Mutual Transport Layer Security (mTLS) in [Fase 9](#).

Endpoint di integrazione della ricerca

Immettere o caricare le credenziali per un endpoint di integrazione della ricerca.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
HTTP di base	Utilizza un nome utente e una password per autenticare le connessioni alla destinazione.	• Nome utente • Password

Endpoint di replica CloudMirror

Immettere o caricare le credenziali per un endpoint di replica CloudMirror.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta
CAP (portale di accesso C2S)	Utilizza certificati e chiavi per autenticare le connessioni alla destinazione.	• URL temporaneo delle credenziali • Certificato CA del server (caricamento file PEM) • Certificato client (caricamento file PEM) • Chiave privata del client (caricamento file PEM, formato crittografato OpenSSL o formato chiave privata non crittografato) • Passphrase della chiave privata del client (opzionale)

Endpoint Amazon SNS

Immettere o caricare le credenziali per un endpoint Amazon SNS.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
Chiave di accesso	Utilizza credenziali di tipo AWS per autenticare le connessioni con la destinazione.	• ID chiave di accesso • Chiave di accesso segreta

Endpoint Kafka

Immettere o caricare le credenziali per un endpoint Kafka.

Le credenziali fornite devono disporre delle autorizzazioni di scrittura per la risorsa di destinazione.

Tipo di autenticazione	Descrizione	Credenziali
Anonimo	Fornisce l'accesso anonimo alla destinazione. Funziona solo per gli endpoint con protezione disattivata.	Nessuna autenticazione.
SASL/SEMPlice	Utilizza un nome utente e una password con testo normale per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-256	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-256 per autenticare le connessioni alla destinazione.	• Nome utente • Password
SASL/SCRAM-SHA-512	Utilizza un nome utente e una password utilizzando un protocollo di risposta alla verifica e l'hash SHA-512 per autenticare le connessioni alla destinazione.	• Nome utente • Password

Selezionare **Usa autenticazione con delega** se il nome utente e la password sono derivati da un token di delega ottenuto da un cluster Kafka.

8. Selezionare **continua**.

9. Selezionare un pulsante di opzione per **Verifica certificati** per scegliere come verificare la connessione TLS all'endpoint.

La maggior parte degli endpoint

Verificare la connessione TLS per l'integrazione della ricerca, la replica di CloudMirror, Amazon SNS o gli endpoint Kafka.

Tipo di verifica del certificato	Descrizione
TLS	Convalida il certificato del server per le connessioni TLS alla risorsa endpoint.
Disabili	La verifica del certificato è disabilitata. Questa opzione non è sicura.
USA certificato CA personalizzato	Il certificato CA personalizzato viene utilizzato per verificare l'identità del server durante la connessione all'endpoint.
Utilizzare il certificato CA del sistema operativo	Utilizzare il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni.

Endpoint Webhook e Kafka

Verifica la connessione TLS per gli endpoint webhook o Kafka.

Tipo di verifica del certificato	Descrizione
TLS	Convalida il certificato del server per le connessioni TLS alla risorsa endpoint.
mTLS	Convalida i certificati client e server per le connessioni TLS reciproche alla risorsa endpoint.
Disabili	La verifica del certificato è disabilitata. Questa opzione non è sicura.
USA certificato CA personalizzato	Il certificato CA personalizzato viene utilizzato per verificare l'identità del server durante la connessione all'endpoint.
Utilizzare il certificato CA del sistema operativo	Utilizzare il certificato Grid CA predefinito installato sul sistema operativo per proteggere le connessioni. Nota: Gli endpoint Webhook non hanno questa opzione.

Selezionando **mTLS**, queste opzioni diventano disponibili.

Tipo di verifica del certificato	Descrizione
Non verificare il certificato del server	Disabilita la verifica del certificato del server, il che significa che l'identità del server non viene verificata. Questa opzione non è sicura.

Tipo di verifica del certificato	Descrizione
Certificato del client	Il certificato client viene utilizzato per verificare l'identità del client durante la connessione all'endpoint.
Chiave privata del cliente	La chiave privata per il certificato client. Se crittografato, deve utilizzare il formato tradizionale PKCS #1 (il formato PKCS #8 non è supportato).
Frase segreta della chiave privata del cliente	La passphrase per decifrare la chiave privata del client. Se la chiave privata non è crittografata, lasciare vuoto questo campo.

10. Selezionare **Test e creare endpoint**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Torna ai dettagli dell'endpoint** e aggiornare le informazioni. Quindi, selezionare **Test e creare endpoint**.



La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant. Contattare l'amministratore di StorageGRID.

Dopo aver configurato un endpoint, è possibile utilizzare il relativo URN per configurare un servizio di piattaforma.

Informazioni correlate

- ["Specificare URN per l'endpoint dei servizi della piattaforma"](#)
- ["Configurare la replica di CloudMirror"](#)
- ["Configurare le notifiche degli eventi"](#)
- ["Configurare il servizio di integrazione della ricerca"](#)
- ["Porte utilizzate per le comunicazioni esterne"](#)

Verifica la connessione per un endpoint dei servizi della piattaforma StorageGRID

Se la connessione a un servizio della piattaforma è stata modificata, è possibile verificare la connessione per l'endpoint per verificare l'esistenza della risorsa di destinazione e che sia possibile raggiungerla utilizzando le credenziali specificate.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire gli endpoint o l'autorizzazione di accesso root"](#).

A proposito di questa attività

StorageGRID non convalida che le credenziali dispongano delle autorizzazioni corrette.

Fasi

1. Selezionare **STORAGE (S3) > Platform Services Endpoint**.

Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

2. Selezionare l'endpoint di cui si desidera verificare la connessione.

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Test di connessione**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene convalidata da un nodo in ogni sito.
- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Se è necessario modificare l'endpoint per correggere l'errore, selezionare **Configuration** (Configurazione) e aggiornare le informazioni. Quindi, selezionare **Test e salvare le modifiche**.

Modifica un endpoint dei servizi della piattaforma in StorageGRID

È possibile modificare la configurazione di un endpoint di servizi di piattaforma per modificarne il nome, l'URI o altri dettagli. Ad esempio, potrebbe essere necessario aggiornare le credenziali scadute o modificare l'URI in modo che punti a un indice Elasticsearch di backup per il failover. Non è possibile modificare l'URN per un endpoint di servizi di piattaforma.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire gli endpoint o l'autorizzazione di accesso root"](#).

Fasi

1. Selezionare **STORAGE (S3) > Platform Services Endpoint**.

Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

2. Selezionare l'endpoint che si desidera modificare.

Viene visualizzata la pagina dei dettagli dell'endpoint.

3. Selezionare **Configurazione**.

4. Se necessario, modificare la configurazione dell'endpoint.



Non è possibile modificare l'URN di un endpoint dopo la creazione dell'endpoint.

- Per modificare il nome visualizzato dell'endpoint, seleziona l'icona di modifica .
- Se necessario, modificare l'URI.
- Se necessario, modificare il tipo di autenticazione.
 - Per l'autenticazione della chiave di accesso, modificare la chiave in base alle necessità selezionando **Modifica chiave S3** e incollando un nuovo ID della chiave di accesso e una chiave di

accesso segreta. Se si desidera annullare le modifiche, selezionare **Ripristina modifica tasto S3**.

- Per l'autenticazione CAP (C2S Access Portal), modificare l'URL delle credenziali temporanee o la passphrase della chiave privata del client opzionale e caricare nuovi file di certificato e chiavi in base alle necessità.



La chiave privata del client deve essere in formato crittografato OpenSSL o non crittografato.

d. Se necessario, modificare il metodo di verifica dei certificati.

5. Selezionare **Test e salvare le modifiche**.

- Se è possibile raggiungere l'endpoint utilizzando le credenziali specificate, viene visualizzato un messaggio di esito positivo. La connessione all'endpoint viene verificata da un nodo in ogni sito.
- Se la convalida dell'endpoint non riesce, viene visualizzato un messaggio di errore. Modificare l'endpoint per correggere l'errore, quindi selezionare **Test e salvare le modifiche**.

Eliminare un endpoint dei servizi della piattaforma StorageGRID

È possibile eliminare un endpoint se non si desidera più utilizzare il servizio di piattaforma associato.

Prima di iniziare

- L'utente ha effettuato l'accesso al responsabile del tenant utilizzando un ["browser web supportato"](#).
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire gli endpoint o l'autorizzazione di accesso root"](#).

Fasi

1. Selezionare **STORAGE (S3) > Platform Services Endpoint**.

Viene visualizzata la pagina Platform Services Endpoint (endpoint dei servizi della piattaforma) che mostra l'elenco degli endpoint dei servizi della piattaforma già configurati.

2. Selezionare la casella di controllo per ciascun endpoint che si desidera eliminare.



Se elimini un endpoint di servizi di piattaforma in uso, il servizio di piattaforma associato verrà disattivato per tutti i bucket che utilizzano l'endpoint. Tutte le richieste non ancora completate verranno interrotte. Le nuove richieste continueranno a essere generate fino a quando non si modifica la configurazione del bucket per non fare più riferimento all'URN cancellato. StorageGRID segnalerà queste richieste come errori irrecuperabili.

3. Selezionare **azioni > Elimina endpoint**.

Viene visualizzato un messaggio di conferma.

4. Selezionare **Delete endpoint** (Elimina endpoint).

Risoluzione dei problemi relativi agli endpoint dei servizi della piattaforma StorageGRID

Se si verifica un errore quando StorageGRID tenta di comunicare con un endpoint dei servizi della piattaforma, viene visualizzato un messaggio sul dashboard. Nella pagina Platform Services Endpoint, la colonna Last error (ultimo errore) indica per quanto tempo

si è verificato l'errore. Se le autorizzazioni associate alle credenziali di un endpoint non sono corrette, non viene visualizzato alcun errore.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint dei servizi della piattaforma negli ultimi 7 giorni, la dashboard di Tenant Manager visualizza un messaggio di avviso. Per ulteriori informazioni sull'errore, visitare la pagina relativa agli endpoint dei servizi della piattaforma.

 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 visualizzato nella dashboard viene visualizzato anche nella parte superiore della pagina Platform Services Endpoint. Per visualizzare un messaggio di errore più dettagliato:

Fasi

1. Dall'elenco degli endpoint, selezionare l'endpoint che presenta l'errore.
2. Nella pagina dei dettagli dell'endpoint, seleziona **Connessione**. Questa scheda mostra solo l'errore più recente per un endpoint e indica quanto tempo fa si è verificato. Gli errori che includono l'icona X rossa  si sono verificati negli ultimi 7 giorni.

Controllare se l'errore è ancora aggiornato

Alcuni errori potrebbero continuare a essere visualizzati nella colonna **ultimo errore** anche dopo la risoluzione. Per verificare se un errore è corrente o per forzare la rimozione di un errore risolto dalla tabella:

Fasi

1. Selezionare l'endpoint.

Viene visualizzata la pagina dei dettagli dell'endpoint.

2. Selezionare **connessione > verifica connessione**.

Selezionando **verifica connessione**, StorageGRID convalida l'esistenza dell'endpoint dei servizi della piattaforma e può essere raggiunto con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Risolvi gli errori degli endpoint

È possibile utilizzare il messaggio **Last error** (ultimo errore) nella pagina dei dettagli dell'endpoint per determinare la causa dell'errore. Alcuni errori potrebbero richiedere la modifica dell'endpoint per risolvere il problema. Ad esempio, se StorageGRID non riesce ad accedere al bucket S3 di destinazione perché non dispone delle autorizzazioni di accesso corrette o la chiave di accesso è scaduta, può verificarsi un errore di CloudMirroring. Il messaggio è "è necessario aggiornare le credenziali dell'endpoint o l'accesso alla destinazione" e i dettagli sono "AccessDenied" o "InvalidAccessKeyId".

Se è necessario modificare l'endpoint per risolvere un errore, selezionando **verifica e salva modifiche** StorageGRID convalida l'endpoint aggiornato e conferma che è possibile raggiungerlo con le credenziali correnti. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Fasi

1. Selezionare l'endpoint.
2. Nella pagina dei dettagli dell'endpoint, selezionare **Configurazione**.
3. Modificare la configurazione dell'endpoint in base alle necessità.
4. Selezionare **connessione > verifica connessione**.

Credenziali endpoint con autorizzazioni insufficienti

Quando StorageGRID convalida un endpoint di servizi di piattaforma, conferma che le credenziali dell'endpoint possono essere utilizzate per contattare la risorsa di destinazione ed esegue un controllo delle autorizzazioni di base. Tuttavia, StorageGRID non convalida tutte le autorizzazioni richieste per determinate operazioni di servizi della piattaforma. Per questo motivo, se si riceve un errore quando si tenta di utilizzare un servizio di piattaforma (ad esempio "403 Proibito"), controllare le autorizzazioni associate alle credenziali dell'endpoint.

Informazioni correlate

- [Amministrare StorageGRID > risolvere i problemi relativi ai servizi della piattaforma](#)
- ["Creare endpoint di servizi di piattaforma"](#)
- ["Verifica della connessione per l'endpoint dei servizi della piattaforma"](#)
- ["Modifica dell'endpoint dei servizi della piattaforma"](#)

Configura la replica CloudMirror in StorageGRID

Per attivare la replica CloudMirror per un bucket, è necessario creare e applicare un XML di configurazione di replica bucket valido.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket per fungere da origine della replica.
- L'endpoint che si intende utilizzare come destinazione per la replica CloudMirror esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

La replica di CloudMirror copia gli oggetti da un bucket di origine a un bucket di destinazione specificato in un endpoint.

Per informazioni generali sulla replica bucket e su come configurarla, vedere ["Documentazione di Amazon Simple Storage Service \(S3\): Replica di oggetti"](#). Per informazioni sull'implementazione di GetBucketReplication, DeleteBucketReplication e PutBucketReplication da parte di StorageGRID, vedere ["Operazioni sui bucket"](#).



La replica di CloudMirror presenta importanti analogie e differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere ["Confronta la replica cross-grid e la replica CloudMirror"](#).

Durante la configurazione della replica di CloudMirror, osservare i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione di replica bucket valido, è necessario utilizzare l'URN di un endpoint bucket S3 per ogni destinazione.
- La replica è supportata solo per i bucket di origine o di destinazione con S3 Object Lock abilitato per i bucket Amazon S3 o StorageGRID S3. Le intestazioni di Object Lock non vengono replicate nell'oggetto di destinazione.
- Se si attiva la replica CloudMirror su un bucket che contiene oggetti, i nuovi oggetti aggiunti al bucket vengono replicati, ma gli oggetti esistenti nel bucket non vengono replicati. È necessario aggiornare gli oggetti esistenti per attivare la replica.
- Se abiliti S3 Object Lock sul bucket di destinazione dopo aver configurato la replica CloudMirror, potresti dover **"salva nuovamente l'endpoint"** per consentire la ripresa della replica.
- Se si specifica una classe di storage nell'XML di configurazione della replica, StorageGRID utilizza tale classe quando esegue operazioni sull'endpoint S3 di destinazione. L'endpoint di destinazione deve supportare anche la classe di storage specificata. Assicurarsi di seguire le raccomandazioni fornite dal vendor del sistema di destinazione.

Fasi

1. Abilita la replica per il bucket di origine:

- Utilizzare un editor di testo per creare l'XML di configurazione della replica richiesto per attivare la replica, come specificato nell'API di replica S3.
- Durante la configurazione dell'XML:
 - Tenere presente che StorageGRID supporta solo V1 della configurazione di replica. Ciò significa che StorageGRID non supporta l'utilizzo dell' `<Filter>` elemento per le regole e segue le convenzioni V1 per l'eliminazione delle versioni degli oggetti. Per ulteriori informazioni, consultare la documentazione di Amazon sulla configurazione della replica.
 - Utilizzare l'URN di un endpoint del bucket S3 come destinazione.
 - Se lo si desidera, aggiungere l' `<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, viene utilizzata la `STANDARD` classe di archiviazione.
 - `STANDARD_IA`: (Accesso standard - non frequente) Utilizza questa classe di storage per i dati a cui si accede meno frequentemente, ma che richiedono comunque un accesso rapido quando necessario.
 - `REDUCED_REDUNDANCY`: Utilizzare questa classe di archiviazione per i dati non critici e riproducibili che possono essere memorizzati con una ridondanza minore rispetto alla `STANDARD` classe di archiviazione.
 - Se si specifica un `Role` nell'XML di configurazione, `Role` questo verrà ignorato. Questo valore non viene utilizzato da StorageGRID.

```
<ReplicationConfiguration>
  <Role></Role>
  <Rule>
    <Status>Enabled</Status>
    <Prefix>2020</Prefix>
    <Destination>
      <Bucket>urn:sgws:s3:::2017-records</Bucket>
      <StorageClass>STANDARD</StorageClass>
    </Destination>
  </Rule>
</ReplicationConfiguration>
```

2. Selezionare **View bucket** (Visualizza bucket) dalla dashboard oppure selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Replication**.

5. Selezionare la casella di controllo **Enable Replication** (attiva replica).

6. Incollare il file XML di configurazione della replica nella casella di testo e selezionare **Save changes** (Salva modifiche).



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID utilizzando l'API di gestione griglia o di gestione griglia. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che la replica sia configurata correttamente:

- a. Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per la replica come specificato nella configurazione della replica.

Nell'esempio illustrato in precedenza, gli oggetti che corrispondono al prefisso "2020" vengono replicati.

- b. Verificare che l'oggetto sia stato replicato nel bucket di destinazione.

Per gli oggetti di piccole dimensioni, la replica avviene rapidamente.

Informazioni correlate

["Creare endpoint di servizi di piattaforma"](#)

Configura le notifiche degli eventi in StorageGRID

È possibile attivare le notifiche per un bucket creando un XML di configurazione delle notifiche e utilizzando Gestione tenant per applicare il file XML a un bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- Hai già creato un bucket per fungere da origine delle notifiche.
- L'endpoint che si intende utilizzare come destinazione per le notifiche degli eventi esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

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 Amazon SNS di destinazione, l'argomento Kafka o l'endpoint webhook specificato come URN di un endpoint.

Per informazioni generali sulle notifiche degli eventi e su come configurarle, fare riferimento alla ["Documentazione Amazon"](#). Per informazioni su come StorageGRID implementa l'API di configurazione delle notifiche bucket S3, fare riferimento alla ["Istruzioni per l'implementazione delle applicazioni client S3"](#).

Durante la configurazione delle notifiche degli eventi per un bucket, osservare i seguenti requisiti e caratteristiche:

- Quando si crea e si applica un XML di configurazione di notifica valido, è necessario utilizzare l'URN di un endpoint di notifica degli eventi per ciascuna destinazione.
- Sebbene la notifica degli eventi possa essere configurata in un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (incluso lo stato Mantieni fino alla data e conservazione legale) degli oggetti non verranno 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, all'argomento Kafka o all'endpoint webhook utilizzato come 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 della notifica.

Fasi

1. Abilita le notifiche per il bucket di origine:

- Utilizzare un editor di testo per creare l'XML di configurazione delle notifiche richiesto per attivare le notifiche degli eventi, come specificato nell'API di notifica S3.
- Quando si configura l'XML, utilizzare l'URN di un endpoint di notifica degli eventi come argomento di destinazione.

```

<NotificationConfiguration>
  <TopicConfiguration>
    <Id>Image-created</Id>
    <Filter>
      <S3Key>
        <FilterRule>
          <Name>prefix</Name>
          <Value>images/</Value>
        </FilterRule>
      </S3Key>
    </Filter>
    <Topic>arn:aws:sns:us-east-1:050340950352:sgws-topic</Topic>
    <Event>s3:ObjectCreated:*</Event>
  </TopicConfiguration>
</NotificationConfiguration>

```

2. In Tenant Manager, selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Event Notifications**.

5. Selezionare la casella di controllo **attiva notifiche eventi**.

6. Incollare l'XML di configurazione della notifica nella casella di testo e selezionare **Salva modifiche**.



I servizi della piattaforma devono essere abilitati per ciascun account tenant da un amministratore StorageGRID utilizzando l'API di gestione griglia o di gestione griglia. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che le notifiche degli eventi siano configurate correttamente:

- a. Eseguire un'azione su un oggetto nel bucket di origine che soddisfi i requisiti per l'attivazione di una notifica come configurato nel XML di configurazione.

Nell'esempio, viene inviata una notifica di evento ogni volta che viene creato un oggetto con il `images/` prefisso.

- b. Conferma che una notifica è stata recapitata all'argomento Amazon SNS di destinazione, all'argomento Kafka o all'endpoint webhook.

Ad esempio, se l'argomento di destinazione è ospitato su Amazon SNS, è possibile configurare il servizio in modo che invii un'e-mail al momento della consegna della notifica.

```

{
  "Records": [
    {
      "eventVersion": "2.0",
      "eventSource": "sgws:s3",
      "eventTime": "2017-08-08T23:52:38Z",
      "eventName": "ObjectCreated:Put",
      "userIdentity": {
        "principalId": "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"](#)

- ["Creare endpoint di servizi di piattaforma"](#)

Configura il servizio di integrazione della ricerca in StorageGRID

È possibile abilitare l'integrazione della ricerca per un bucket creando l'integrazione della ricerca XML e utilizzando Tenant Manager per applicare l'XML al bucket.

Prima di iniziare

- I servizi della piattaforma sono stati abilitati per l'account tenant da un amministratore di StorageGRID.
- È già stato creato un bucket S3 di cui si desidera indicizzare il contenuto.
- L'endpoint che si intende utilizzare come destinazione per il servizio di integrazione della ricerca esiste già e si dispone dell'URN.
- L'utente appartiene a un gruppo di utenti che dispone di ["Gestire tutti i bucket o le autorizzazioni di accesso root"](#). Queste autorizzazioni sovrascrivono le impostazioni di autorizzazione nelle policy di gruppo o bucket quando si configura il bucket utilizzando Tenant Manager.

A proposito di questa attività

Dopo aver configurato il servizio di integrazione della ricerca per un bucket di origine, la creazione di un oggetto o l'aggiornamento dei metadati o dei tag di un oggetto attiva l'invio dei metadati dell'oggetto all'endpoint di destinazione.

Se abiliti il servizio di integrazione della ricerca per un bucket che contiene già oggetti, le notifiche dei metadati non vengono inviate automaticamente per gli oggetti esistenti. Aggiornare questi oggetti esistenti per assicurarsi che i relativi metadati vengano aggiunti all'indice di ricerca della destinazione.

Fasi

1. Consentire l'integrazione della ricerca per un bucket:

- Utilizzare un editor di testo per creare l'XML di notifica dei metadati necessario per abilitare l'integrazione della ricerca.
- Quando si configura l'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, è possibile inviare metadati per gli oggetti con il prefisso `images` a una destinazione e metadati per gli oggetti con il prefisso `videos` a un'altra. Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate quando vengono inviate. 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 consentita.

Se necessario, fare riferimento alla [Esempi di XML di configurazione dei metadati](#).

```

<MetadataNotificationConfiguration>
  <Rule>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>/Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>

```

Elementi nella configurazione della notifica dei metadati XML:

Nome	Descrizione	Obbligatorio
MetadataNotificationConfiguration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì

Nome	Descrizione	Obbligatorio
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • <code>es</code> deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato <code>domain-name/myindex/mytype</code>. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. 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 dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'URN è incluso nell'elemento Destination.	Sì

2. In Tenant Manager, selezionare **STORAGE (S3) > Bucket**.

3. Selezionare il nome del bucket di origine.

Viene visualizzata la pagina dei dettagli del bucket.

4. Selezionare **Platform Services > Search Integration**

5. Selezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).

6. Incollare la configurazione di notifica dei metadati nella casella di testo e selezionare **Salva modifiche**.



I servizi della piattaforma devono essere attivati per ciascun account tenant da un amministratore StorageGRID utilizzando il gestore di griglia o l'API di gestione. Se si verifica un errore durante il salvataggio del file XML di configurazione, contattare l'amministratore di StorageGRID.

7. Verificare che il servizio di integrazione della ricerca sia configurato correttamente:

- Aggiungere un oggetto al bucket di origine che soddisfi i requisiti per l'attivazione di una notifica dei metadati come specificato nel file XML di configurazione.

Nell'esempio illustrato in precedenza, tutti gli oggetti aggiunti al bucket attivano una notifica dei metadati.

- Verificare che un documento JSON contenente i metadati e i tag dell'oggetto sia stato aggiunto all'indice di ricerca specificato nell'endpoint.

Al termine

Se necessario, è possibile disattivare l'integrazione della ricerca per un bucket utilizzando uno dei seguenti

metodi:

- Selezionare **STORAGE (S3) > Bucket** e deselezionare la casella di controllo **Enable search Integration** (attiva integrazione ricerca).
- Se si utilizza direttamente l'API S3, utilizzare una richiesta DI notifica DELETE Bucket metadata. Consultare le istruzioni per l'implementazione delle applicazioni client S3.

esempio: Configurazione di notifica dei metadati che si applica a tutti gli oggetti

In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:myes:es::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Esempio: Configurazione della notifica di metadati con due regole

In questo esempio, i metadati degli oggetti corrispondenti al prefisso `/images` vengono inviati a una destinazione, mentre i metadati degli oggetti corrispondenti al prefisso `/videos` vengono inviati a una seconda destinazione.

```

<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>

```

Formato di notifica dei metadati

Quando si attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. La `test` benna non è in versione, quindi l'etichetta `versionId` è vuota.

```
{
  "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 oggetto

versionID: Versione oggetto, per gli oggetti nei bucket in versione

region: Area bucket, ad esempio us-east-1

Metadati di sistema

size: Dimensione dell'oggetto (in byte) come visibile a un client HTTP

md5: Hash oggetto

Metadati dell'utente

metadata: Tutti i metadati utente per l'oggetto, come coppie chiave-valore

key:value

Tag

tags: Tutti i tag oggetto definiti per l'oggetto, come coppie chiave-valore

key:value

Come visualizzare i risultati in Elasticsearch

Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o

numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Attivare le mappature dinamiche dei campi nell'indice prima di configurare il servizio di integrazione della ricerca. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

UTILIZZARE L'API REST S3

Versioni e aggiornamenti supportati dall'API REST S3 di StorageGRID

StorageGRID supporta l'API S3 (Simple Storage Service), implementata come set di servizi Web REST (Representational state Transfer).

Il supporto per l'API REST S3 consente di connettere le applicazioni orientate ai servizi sviluppate per i servizi Web S3 con lo storage a oggetti on-premise che utilizza il sistema StorageGRID. Sono necessarie modifiche minime all'utilizzo corrente delle chiamate API REST S3 da parte di un'applicazione client.

Versioni supportate

StorageGRID supporta le seguenti versioni specifiche di STS, S3 e HTTP:

Elemento	Versione
Specifiche API STS AssumeRole	"Documentazione di Amazon Web Services (AWS): Riferimento API Amazon Assumerole" Per ulteriori informazioni su AssumeRole, fare riferimento a "Imposta AssumeRole" .
Specifica API S3	"Documentazione 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 la pipelining HTTP/1.1.

Aggiornamenti al supporto delle API REST S3

Rilasciare	Commenti
12.1.0	• If-Match L' `If-Match` intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l' `If-Match` intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented. • If-None-Match L' `If-None-Match` intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l' `If-None-Match` intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented. • Aggiunto il supporto per i valori di checksum precalcolati per le seguenti richieste e intestazioni supportate: ◦ CompleteMultipartUpload: x-amz-checksum-crc32, x-amz-checksum-crc32c, e x-amz-checksum-crc64nvme ◦ CreateMultipartUpload: CRC32, CRC32C, e CRC64NVME per x-amz-checksum-algorithm ◦ CopyObject: CRC32, CRC32C, CRC64NVME, e SHA256 per x-amz-checksum-algorithm ◦ PutObject: x-amz-checksum-crc32, x-amz-checksum-crc32c, e x-amz-checksum-crc64nvme ◦ UploadPart: x-amz-checksum-crc32, x-amz-checksum-crc32c, e x-amz-checksum-crc64nvme • Aggiunto il supporto per x-amz-checksum-type per CreateMultipartUpload e CompleteMultipartUpload. • Aggiunto il supporto per la `s3:x-amz-copy-source` chiave della condizione di policy. • Consenti di abilitare S3 Object Lock sui bucket esistenti.
12,0	• Aggiunto il supporto per la condivisione delle risorse tra origini (CORS) per un'interfaccia di gestione, che consente a un altro dominio di accedere ai dati in StorageGRID utilizzando le API di gestione. "Scopri di più" . • Aggiunto il supporto per STS AssumeRole e le policy di sessione. Vedi "un esempio di politica di sessione". Puoi configurare AssumeRole nei gruppi tenant.

Rilasciare	Commenti
11,9	• Aggiunto supporto per valori checksum SHA-256 pre-calcolati per le seguenti richieste e intestazioni supportate. È possibile utilizzare questa funzione per verificare l'integrità degli oggetti caricati: ◦ CompleteMultipartUpload: x-amz-checksum-sha256 ◦ CreateMultipartUpload: x-amz-checksum-algorithm ◦ GetObject: x-amz-checksum-mode ◦ HeadObject (scarto capo): x-amz-checksum-mode ◦ ListParts ◦ PutObject: x-amz-checksum-sha256 ◦ UploadPart: x-amz-checksum-sha256 • È stata aggiunta la possibilità per l'amministratore di grid di controllare le impostazioni di conservazione e conformità a livello di tenant. Queste impostazioni influiscono sulle impostazioni di blocco degli oggetti S3. ◦ Modalità di conservazione predefinita bucket e modalità di conservazione degli oggetti: Governance o conformità, se consentite dall'amministratore del grid. ◦ Periodo di conservazione predefinito del bucket e conservazione dell'oggetto fino alla data: Deve essere minore o uguale a quanto consentito dal periodo di conservazione massimo impostato dall'amministratore della griglia. • Supporto migliorato per la <code>aws-chunked</code> codifica del contenuto e i valori di streaming <code>x-amz-content-sha256</code>. 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 in modo che corrispondano ai nomi utilizzati in "Documentazione Amazon Web Services (AWS): Riferimento API Amazon Simple Storage Service" .
11,7	• Aggiunto "Riferimento rapido: Richieste API S3 supportate". • Aggiunto supporto per l'utilizzo della modalità DI GOVERNANCE con S3 Object Lock. • Aggiunto supporto per l'intestazione di risposta specifica di StorageGRID <code>x-ntap-sg-cgr-replication-status</code> per le richieste di oggetti GET e HEAD. Questa intestazione fornisce lo stato di replica di un oggetto per la replica cross-grid. • Le richieste SelectObjectContent ora supportano gli oggetti Parquet.

Rilasciare	Commenti
11,6	• Aggiunto il supporto per l'utilizzo del <code>partNumber</code> parametro di richiesta nelle richieste GET Object e HEAD Object. • Aggiunto supporto per una modalità di conservazione predefinita e un periodo di conservazione predefinito a livello di bucket per S3 Object Lock. • È stato aggiunto il supporto per <code>s3:object-lock-remaining-retention-days</code> la chiave della condizione della policy per impostare l'intervallo di periodi di conservazione consentiti per gli oggetti. • Modifica della dimensione massima <i>consigliata</i> per un'operazione di singolo oggetto PUT in 5 GiB (5,368,709,120 byte). Se si dispone di oggetti di dimensioni superiori a 5 GiB, utilizzare invece il caricamento multiparte.
11,5	• Aggiunto supporto per la gestione della crittografia bucket. • Aggiunto supporto per S3 Object Lock e richieste legacy di Compliance obsolete. • Aggiunto il supporto per l'utilizzo DELL'ELIMINAZIONE di più oggetti nei bucket con versione. • L' <code>Content-MD5</code> intestazione della richiesta è ora supportata correttamente.
11,4	• Aggiunto supporto per L'ELIMINAZIONE di tag bucket, L'AGGIUNTA DI tag bucket E L'AGGIUNTA di tag bucket. I tag di allocazione dei costi non sono supportati. • Per i bucket creati in StorageGRID 11.4, non è più necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. • Aggiunto il supporto per le notifiche bucket sul <code>s3:ObjectRestore:Post</code> tipo di evento. • I limiti di dimensione AWS per le parti multipart vengono ora applicati. Ogni parte di un caricamento multiparte deve essere compresa tra 5 MiB e 5 GiB. L'ultima parte può essere inferiore a 5 MiB. • Aggiunto supporto per TLS 1.3
11,3	• Aggiunto supporto per la crittografia lato server dei dati a oggetti con chiavi fornite dal cliente (SSE-C). • Aggiunto supporto per le operazioni di ELIMINAZIONE, RECUPERO e INSERIMENTO DEL ciclo di vita del bucket (solo azione scadenza) e per l' <code>x-amz-expiration</code> intestazione della risposta. • Aggiornamento DI PUT object, PUT object - Copy e Multipart Upload per descrivere l'impatto delle regole ILM che utilizzano il posizionamento sincrono durante l'acquisizione. • Le crittografia TLS 1.1 non sono più supportate.

Rilasciare	Commenti
11,2	Aggiunto supporto per il ripristino POST-oggetto da utilizzare con i Cloud Storage Pools. Aggiunto supporto per l'utilizzo della sintassi AWS per ARN, chiavi di condizione dei criteri e variabili dei criteri in policy di gruppo e bucket. Le policy di gruppo e bucket esistenti che utilizzano la sintassi StorageGRID continueranno a essere supportate. Nota: gli utilizzi di ARN/URN in altre configurazioni JSON/XML, inclusi quelli utilizzati nelle funzionalità personalizzate di StorageGRID, non sono cambiati.
11,1	Aggiunto supporto per la condivisione delle risorse tra origini (CORS), HTTP per connessioni client S3 ai nodi di rete e impostazioni di conformità sui bucket.
11,0	Supporto aggiunto per la configurazione dei servizi della piattaforma (replica CloudMirror, notifiche e integrazione della ricerca Elasticsearch) per i bucket. Inoltre, è stato aggiunto il supporto per i vincoli di posizione dei tag degli oggetti per i bucket e la coerenza disponibile.
10,4	Aggiunto supporto per le modifiche di scansione ILM alle versioni, agli aggiornamenti delle pagine dei nomi di dominio degli endpoint, alle condizioni e alle variabili nei criteri, agli esempi di policy e all'autorizzazione PutOverwriteObject.
10,3	Aggiunto supporto per il controllo delle versioni.
10,2	Aggiunto supporto per policy di accesso di gruppo e bucket e per copia multiparte (carica parte - Copia).
10,1	Aggiunto il supporto per il caricamento multipart, le richieste in stile virtual-hosted e l'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.

Richieste API S3 supportate in StorageGRID

In questa pagina viene riepilogato il modo in cui StorageGRID supporta le API di Amazon Simple Storage Service (S3).

Questa pagina include solo le operazioni S3 supportate da StorageGRID. Qualsiasi operazione S3 non elencata potrebbe restituire 501 Not Implemented o causare comportamenti imprevisti.



Per visualizzare la documentazione AWS relativa a ciascuna operazione, selezionare il collegamento nell'intestazione.

Parametri di query URI comuni e intestazioni di richiesta

Se non specificato, sono supportati i seguenti parametri di query URI comuni:

- `versionId` (come richiesto per le operazioni a oggetti)

Se non specificato, sono supportate le seguenti intestazioni di richiesta comuni:

- Authorization
- Connection
- Content-Length
- Content-MD5
- Content-Type
- Date
- Expect
- Host
- x-amz-date

Informazioni correlate

- ["Dettagli sull'implementazione dell'API REST S3"](#)
- ["Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"](#)

"AbortMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre a questo parametro di query URI aggiuntivo:

- uploadId

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni per caricamenti multiparte"](#)

"CompleteMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre a questo parametro di query URI aggiuntivo:

- uploadId
- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- x-amz-checksum-sha256
- x-amz-checksum-type
- x-amz-storage-class

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- ChecksumCRC32
- ChecksumCRC32C
- ChecksumCRC64NVME
- ChecksumSHA256
- CompleteMultipartUpload
- ETag
- Part
- PartNumber

Documentazione StorageGRID

["CompleteMultipartUpload"](#)

["Oggetto CopyObject"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- x-amz-checksum-algorithm
- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-metadata-directive
- x-amz-object-lock-legal-hold
- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-storage-class

- x-amz-tagging
- x-amz-tagging-directive
- x-amz-meta-<metadata-name>

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Oggetto CopyObject"](#)

"CreateBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- x-amz-bucket-object-lock-enabled

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"CreateMultipartUpload"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-algorithm
- x-amz-checksum-type
- x-amz-server-side-encryption
- x-amz-storage-class
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-tagging

- x-amz-object-lock-mode
- x-amz-object-lock-retain-until-date
- x-amz-object-lock-legal-hold
- x-amz-meta-`<metadata-name>`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["CreateMultipartUpload"](#)

["DeleteBucket"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Documentazione StorageGRID

["Operazioni sui bucket"](#)

["DeleteBucketCors"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

["DeleteBucketEncryption"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

["DeleteBucketLifecycle"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

"DeleteBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"DeleteObject (Elimina oggetto)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre all'intestazione della richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"DeleteObjects"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre all'intestazione della richiesta aggiuntiva:

- `x-amz-bypass-governance-retention`

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"DeleteObjectTagging"

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"GetBucketAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

"GetBucketLocation"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketNotificationConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetBucketVersioning"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"GetObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti 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

["GetObject"](#)

"GetObjectAcl"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"GetObjectLegalHold"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

"GetObjectLockConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"GetObjectRetention"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

"GetObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sugli oggetti"

"HeadBucket"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"HeadObject (oggetto intestazione)"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti 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 \(oggetto intestazione\)"](#)

["ListBucket"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Nessuno

Documentazione StorageGRID

[Operazioni sul servizio](#) > [ListBuckets](#)

["ListMultipartUploads"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- encoding-type
- key-marker
- max-uploads
- prefix
- upload-id-marker

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["ListMultipartUploads"](#)

["ListObjects \(oggetti elenco\)"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- delimiter
- encoding-type
- marker

- max-keys
- prefix

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"ListObjectsV2"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- continuation-token
- delimiter
- encoding-type
- fetch-owner
- max-keys
- prefix
- start-after

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"ListObjectVersions"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- delimiter
- encoding-type
- key-marker
- max-keys
- prefix
- version-id-marker

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"Operazioni sui bucket"

"ListParts"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri aggiuntivi:

- max-parts
- part-number-marker
- uploadId

Corpo della richiesta

Nessuno

Documentazione StorageGRID

"ListMultipartUploads"

"PutBucketCors"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketEncryption"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- ApplyServerSideEncryptionByDefault
- Rule
- ServerSideEncryptionConfiguration
- SSEAlgorithm

Documentazione StorageGRID

"Operazioni sui bucket"

"PutBucketLifecycleConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- And
- Days
- Expiration
- ExpiredObjectDeleteMarker
- Filter
- ID
- Key
- LifecycleConfiguration
- NewerNoncurrentVersions
- NoncurrentDays
- NoncurrentVersionExpiration
- Prefix
- Rule
- Status
- Tag
- Value

Documentazione StorageGRID

- ["Operazioni sui bucket"](#)
- ["Creare la configurazione del ciclo di vita S3"](#)

"PutBucketNotificationConfiguration"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

StorageGRID supporta questi tag XML del corpo della richiesta:

- Event
- Filter
- FilterRule
- Id

- Name
- NotificationConfiguration
- Prefix
- S3Key
- Suffix
- Topic
- TopicConfiguration
- Value

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"PutBucketPolicy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per i dettagli sui campi del corpo JSON supportati, vedere ["Utilizza policy di accesso a bucket e gruppi"](#) .

"PutBucketReplication"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Tag XML del corpo della richiesta

- Bucket
- Destination
- Prefix
- ReplicationConfiguration
- Rule
- Status
- StorageClass

Documentazione StorageGRID

["Operazioni sui bucket"](#)

"PutBucketTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al

momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sui bucket"](#)

["PutBucketVersioning"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Parametri del corpo della richiesta

StorageGRID supporta questi parametri del corpo della richiesta:

- VersioningConfiguration
- Status

Documentazione StorageGRID

["Operazioni sui bucket"](#)

["PutObject"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutte [parametri e intestazioni comuni](#) queste richieste, oltre alle seguenti intestazioni aggiuntive:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- 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

["PutObject"](#)

["PutObjectLegalHold"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["PutObjectLockConfiguration"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta la maggior parte delle [parametri e intestazioni comuni](#) opzioni per questa richiesta.

Corpo della richiesta

StorageGRID supporta la maggior parte dei parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione, con la seguente eccezione:

Non puoi usare PutObjectLockConfiguration per abilitare S3 Object Lock su un bucket esistente a meno che l'amministratore della griglia non ti abbia dato il permesso.

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

["PutObjectRetention"](#)

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre a questa intestazione aggiuntiva:

- x-amz-bypass-governance-retention

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

"PutObjectTagging"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

StorageGRID supporta tutti i parametri del corpo della richiesta definiti dall'API REST di Amazon S3 al momento dell'implementazione.

Documentazione StorageGRID

["Operazioni sugli oggetti"](#)

"RestoreObject"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per informazioni dettagliate sui campi corpo supportati, vedere ["RestoreObject"](#).

"SelectObjectContent"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta.

Corpo della richiesta

Per ulteriori informazioni sui body field supportati, vedere quanto segue:

- ["USA S3 Select"](#)
- ["SelectObjectContent"](#)

"UploadPart"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri di query URI aggiuntivi:

- `partNumber`
- `uploadId`

E queste intestazioni di richiesta aggiuntive:

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `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

["UploadPart"](#)

"UploadPartCopy"

Parametri di query URI e intestazioni di richiesta

StorageGRID supporta tutti [parametri e intestazioni comuni](#) per questa richiesta, oltre ai seguenti parametri di query URI aggiuntivi:

- partNumber
- uploadId

E queste intestazioni di richiesta aggiuntive:

- x-amz-copy-source
- x-amz-copy-source-if-match
- x-amz-copy-source-if-modified-since
- x-amz-copy-source-if-none-match
- x-amz-copy-source-if-unmodified-since
- x-amz-copy-source-range
- x-amz-server-side-encryption-customer-algorithm
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-copy-source-server-side-encryption-customer-algorithm
- x-amz-copy-source-server-side-encryption-customer-key
- x-amz-copy-source-server-side-encryption-customer-key-MD5

Corpo della richiesta

Nessuno

Documentazione StorageGRID

["UploadPartCopy"](#)

Testare la configurazione dell'API REST S3 di StorageGRID

Puoi utilizzare l'interfaccia a riga di comando (CLI AWS) di Amazon Web Services per verificare la tua connessione al sistema e verificare che sia possibile leggere e scrivere oggetti.

Prima di iniziare

- È stato scaricato e installato l'interfaccia CLI di AWS da ["aws.amazon.com/cli"](https://aws.amazon.com/cli/).
- In alternativa, si dispone di ["creato un endpoint del bilanciamento del carico"](#). In caso contrario, si conosce l'indirizzo IP del nodo di archiviazione a cui si desidera connettersi e il numero di porta da utilizzare. Vedere ["Indirizzi IP e porte per le connessioni client"](#).
- Si dispone di ["Creato un account tenant S3"](#).
- È stato effettuato l'accesso al tenant e ["ha creato una chiave di accesso"](#) a .

Per ulteriori informazioni su questi passi, vedere ["Configurare le connessioni client"](#).

Fasi

1. Configurare le impostazioni dell'interfaccia utente di AWS per utilizzare l'account creato nel sistema StorageGRID:
 - a. Accedere alla modalità di configurazione: `aws configure`
 - b. Inserire l'ID della chiave di accesso per l'account creato.
 - c. Inserire la chiave di accesso segreta per l'account creato.
 - d. Immettere la regione predefinita da utilizzare. Ad esempio, `us-east-1`.
 - e. Immettere il formato di output predefinito da utilizzare oppure premere **Invio** per selezionare JSON.
2. Creare un bucket.

In questo esempio si presuppone che sia stato configurato un endpoint del bilanciamento del carico per utilizzare l'indirizzo IP 10.96.101.17 e la porta 10443.

```
aws s3api --endpoint-url https://10.96.101.17:10443
--no-verify-ssl create-bucket --bucket testbucket
```

Se il bucket viene creato correttamente, viene restituita la posizione del bucket, come mostrato nell'esempio seguente:

```
"Location": "/testbucket"
```

3. Caricare un oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl
put-object --bucket testbucket --key s3.pdf --body C:\s3-
test\upload\s3.pdf
```

Se l'oggetto viene caricato correttamente, viene restituito un ETAG che rappresenta un hash dei dati dell'oggetto.

4. Elencare i contenuti del bucket per verificare che l'oggetto sia stato caricato.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
list-objects --bucket testbucket
```

5. Eliminare l'oggetto.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-object --bucket testbucket --key s3.pdf
```

6. Eliminare il bucket.

```
aws s3api --endpoint-url https://10.96.101.17:10443 --no-verify-ssl  
delete-bucket --bucket testbucket
```

Come StorageGRID implementa l'API REST S3

Come StorageGRID S3 REST API risolve le richieste client in conflitto

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite".

La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Come StorageGRID S3 REST API bilancia disponibilità e coerenza

La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la loro coerenza in diversi nodi e siti storage. È possibile modificare la coerenza come richiesto dall'applicazione.

Per impostazione predefinita, StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi GET 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.

Se si desidera eseguire operazioni a oggetti con una coerenza diversa, è possibile:

- Specificare una coerenza per [ogni secchio](#) .
- Specificare una coerenza per [Ogni operazione API](#).
- Modificare la coerenza predefinita a livello di griglia eseguendo una delle seguenti operazioni:
 - In Grid Manager, vai a **Configurazione > Sistema > Impostazioni di archiviazione > Coerenza predefinita del bucket**.
 - .



Una modifica alla coerenza a livello di griglia si applica solo ai bucket creati dopo la modifica dell'impostazione. Per determinare i dettagli di una modifica, vedere il registro di controllo situato in `/var/local/log` (cercare **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. La coerenza influisce sulla disponibilità degli oggetti per le richieste dei client.

È possibile impostare la coerenza per un bucket o un'operazione API su uno dei seguenti valori:

- **All:** Tutti i nodi ricevono immediatamente i metadati degli oggetti o la richiesta non riesce.
- **Strong-global:** garantisce la coerenza di lettura e scrittura per tutte le richieste dei client su tutti i siti. Quando la semantica del quorum è configurata, si applicano i seguenti comportamenti:
 - Consente la tolleranza ai guasti del sito per le richieste dei client quando le griglie hanno tre o più siti. Le griglie a due siti non avranno tolleranza ai guasti del sito.
 - Le seguenti operazioni S3 non riusciranno se un sito è inattivo:
 - DeleteBucketEncryption
 - PutBucketBranch
 - PutBucketEncryption
 - PutBucketVersioning
 - PutObjectLegalHold
 - PutObjectLockConfiguration
 - PutObjectRetention

Se necessario, puoi ["configurare la semantica del quorum StorageGRID per una coerenza globale forte"](#).

- **Strong-site:** I metadati degli oggetti vengono immediatamente distribuiti ad altri nodi del sito. Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
- **Read-after-new-write:** Fornisce coerenza lettura dopo scrittura per nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
- **Available:** Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Utilizzare la coerenza "Read-after-new-write" e "available"

Quando un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write", StorageGRID esegue la ricerca in più passaggi, come segue:

- Per prima cosa, cerca l'oggetto utilizzando una bassa coerenza.
- Se la ricerca non riesce, ripete la ricerca al valore di coerenza successivo finché non raggiunge una coerenza equivalente al comportamento per strong-Global.

Se un'operazione HEAD o GET utilizza la coerenza "Read-after-new-write" ma l'oggetto non esiste, la ricerca degli oggetti raggiungerà sempre una coerenza equivalente al comportamento per strong-Global. Poiché

questa coerenza richiede la disponibilità di più copie dei metadati degli oggetti in ogni sito, è possibile ricevere un elevato numero di errori del server interno 500 nel caso in cui due o più nodi storage nello stesso sito non fossero disponibili.

A meno che non si richiedano garanzie di coerenza simili a Amazon S3, è possibile evitare questi errori per le operazioni HEAD and GET impostando la coerenza su "disponibile". Quando un'operazione HEAD o GET utilizza la consistenza "disponibile", StorageGRID fornisce solo la consistenza finale. Non ritenta un'operazione non riuscita ad aumentare la coerenza, pertanto non richiede la disponibilità di più copie dei metadati degli oggetti.

specificare la coerenza per l'operazione API

Per impostare la coerenza per una singola operazione API, i valori di coerenza devono essere supportati per l'operazione ed è necessario specificare la coerenza nell'intestazione della richiesta. Nell'esempio riportato di seguito viene impostata la coerenza su "strong-Site" per un'operazione GetObject.

```
GET /bucket/object HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Consistency-Control: strong-site
```



È necessario utilizzare la stessa coerenza per entrambe le operazioni PutObject e GetObject.

Specifica la coerenza per il bucket

Per impostare la coerenza per il bucket, è possibile utilizzare la richiesta StorageGRID ["METTI la coerenza del bucket"](#). In alternativa, è possibile ["modificare la consistenza di un bucket"](#) rivolgersi al responsabile del tenant.

Quando si imposta la consistenza per un secchio, tenere presente quanto segue:

- L'impostazione della consistenza per un bucket determina la consistenza utilizzata per S3 operazioni eseguite sugli oggetti nel bucket o nella configurazione del bucket. Non influisce sulle operazioni sul bucket stesso.
- La coerenza per una singola operazione API sovrascrive la coerenza per il bucket.
- In generale, i bucket devono utilizzare la coerenza predefinita, "Read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare la coerenza per ogni richiesta API. Impostare la consistenza a livello del bucket solo come ultima risorsa.

Come interagiscono coerenza e regole ILM per influenzare la protezione dei dati

Sia la scelta della coerenza che la regola ILM influiscono sulla protezione degli oggetti. Queste impostazioni possono interagire.

Ad esempio, la coerenza utilizzata durante la memorizzazione di un oggetto influisce sul posizionamento iniziale dei metadati degli oggetti, mentre il comportamento di acquisizione selezionato per la regola ILM influisce sul posizionamento iniziale delle copie degli oggetti. Poiché StorageGRID richiede l'accesso sia ai metadati dell'oggetto che ai relativi dati per soddisfare le richieste del client, la selezione di livelli di protezione corrispondenti per il comportamento di coerenza e acquisizione può offrire una migliore protezione iniziale dei dati e risposte di sistema più prevedibili.

Per le regole ILM sono disponibili le seguenti "opzioni di acquisizione" opzioni:

Commit doppio

StorageGRID effettua immediatamente copie provvisorie dell'oggetto e restituisce il successo al cliente. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Rigoroso

Tutte le copie specificate nella regola ILM devono essere eseguite prima che l'operazione sia restituita al cliente.

Bilanciato

StorageGRID tenta di eseguire tutte le copie specificate nella regola ILM al momento dell'acquisizione; se ciò non è possibile, vengono create copie provvisorie e viene restituita al cliente l'avvenuta esecuzione. Le copie specificate nella regola ILM vengono eseguite quando possibile.

Esempio di interazione tra la regola coerenza e ILM

Supponiamo di avere una griglia a tre siti con la seguente regola ILM e la seguente coerenza:

- **Regola ILM:** creare tre copie dell'oggetto, una nel sito locale e una in ciascun sito remoto. Utilizzare un comportamento di acquisizione rigoroso.
- **Coerenza:** Strong-global (i metadati degli oggetti vengono distribuiti immediatamente su più siti).

Quando un client memorizza un oggetto nella griglia, StorageGRID esegue tutte e tre le copie dell'oggetto e distribuisce i metadati a più 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 nei siti remoti. L'oggetto è completamente recuperabile dagli altri siti.

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 nei siti remoti, 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. Contattare NetApp per assistenza.

Come StorageGRID utilizza il versioning degli oggetti

È possibile impostare lo stato di versione di un bucket se si desidera mantenere più versioni di ciascun oggetto. L'abilitazione della versione per un bucket può aiutare a proteggere dalla cancellazione accidentale di oggetti e consente di recuperare e ripristinare le versioni precedenti di un oggetto.

Il sistema StorageGRID implementa il controllo delle versioni con il supporto per la maggior parte delle funzionalità e con alcune limitazioni. StorageGRID supporta fino a 10,000 versioni di ciascun oggetto.

La versione degli oggetti può essere combinata con la gestione del ciclo di vita delle informazioni di StorageGRID (ILM) o con la configurazione del ciclo di vita del bucket S3. È necessario attivare esplicitamente il controllo delle versioni per ogni bucket. Quando la versione è abilitata per un bucket, a ogni oggetto aggiunto al bucket viene assegnato un ID di versione, che viene generato dal sistema StorageGRID.

L'utilizzo dell'autenticazione MFA (multi-factor Authentication) Delete non è supportato.



Il controllo delle versioni può essere attivato solo sui bucket creati con StorageGRID versione 10.3 o successiva.

ILM e versione

I criteri ILM vengono applicati a ogni versione di un oggetto. Un processo di scansione ILM esegue una scansione continua di tutti gli oggetti e li rivaluti in base al criterio ILM corrente. Qualsiasi modifica apportata ai criteri ILM viene applicata a tutti gli oggetti precedentemente acquisiti. Sono incluse le versioni precedentemente ingerite se è abilitato il controllo delle versioni. La scansione ILM applica le nuove modifiche ILM agli oggetti acquisiti in precedenza.

Per gli oggetti S3 nei bucket abilitati per le versioni, il supporto per le versioni consente di creare regole ILM che utilizzano "tempo non corrente" come ora di riferimento (selezionare **Sì** per la domanda "Applica questa regola solo alle versioni precedenti degli oggetti?" in "[Passaggio 1 della creazione guidata di una regola ILM](#)"). Quando un oggetto viene aggiornato, le sue versioni precedenti diventano non aggiornate. L'utilizzo di un filtro "tempo non corrente" consente di creare policy per ridurre l'impatto sullo storage delle versioni precedenti di oggetti.



Quando si carica una nuova versione di un oggetto utilizzando un'operazione di caricamento multiparte, l'ora non corrente per la versione originale dell'oggetto si riflette quando il caricamento multiparte è stato creato per la nuova versione, non quando il caricamento multiparte è stato completato. In casi limitati, il tempo non corrente per la versione originale potrebbe essere di ore o giorni prima del tempo per la versione corrente.

Informazioni correlate

- "[Modalità di eliminazione degli oggetti con versione S3](#)"
- "[Regole e criteri ILM per gli oggetti con versione S3 \(esempio 4\)](#)".

Usa l'API REST S3 per configurare StorageGRID S3 Object Lock

Se l'impostazione blocco oggetti S3 globale è attivata per il sistema StorageGRID, è possibile creare bucket con blocco oggetti S3 attivato. È possibile specificare la conservazione predefinita per ogni bucket o impostazioni di conservazione per ciascuna versione dell'oggetto.



StorageGRID non supporta l'header `x-amz-sdk-checksum-algorithm` nell'intestazione della richiesta.

Come attivare il blocco oggetti S3 per un bucket

Se l'impostazione globale di blocco oggetti S3 è attivata per il sistema StorageGRID, è possibile attivare il blocco oggetti S3 quando si crea ciascun bucket.

S3 Object Lock è un'impostazione permanente che può essere attivata solo quando si crea un bucket. Non puoi aggiungere o disattivare il blocco oggetti S3 dopo la creazione di un bucket.

Per abilitare il blocco degli oggetti S3 per un bucket, usa uno di questi metodi:

- Creare il bucket utilizzando il tenant Manager. Vedere "[Creare un bucket S3](#)".
- Creare il bucket utilizzando una richiesta CreateBucket con l'header `x-amz-bucket-object-lock-`

enabled`intestazione della richiesta. Vedere ["Operazioni sui bucket"](#).

- Gestisci le impostazioni del bucket dal Tenant Manager. Vedi ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).

S3 Object Lock richiede il controllo della versione del bucket, che viene attivato automaticamente quando viene creato il bucket. Non puoi sospendere il controllo delle versioni per il bucket. Vedere ["Versione degli oggetti"](#).

Impostazioni di conservazione predefinite per un bucket

Quando S3 Object Lock è attivato per un bucket, è possibile attivare la conservazione predefinita per il bucket e specificare una modalità di conservazione predefinita e un periodo di conservazione predefinito.

Modalità di conservazione predefinita

- In modalità COMPLIANCE:
 - L'oggetto non può essere eliminato fino a quando non viene raggiunta la data di conservazione.
 - La conservazione dell'oggetto fino alla data odierna può essere aumentata, ma non può essere diminuita.
 - La data di conservazione dell'oggetto non può essere rimossa fino al raggiungimento di tale data.
- In modalità GOVERNANCE:
 - Gli utenti con `s3:BypassGovernanceRetention` autorizzazione possono utilizzare l'`x-amz-bypass-governance-retention: true` intestazione della richiesta per ignorare le impostazioni di conservazione.
 - Questi utenti possono eliminare una versione dell'oggetto prima che venga raggiunta la data di conservazione.
 - Questi utenti possono aumentare, ridurre o rimuovere il mantenimento di un oggetto fino ad oggi.

Periodo di conservazione predefinito

Ogni bucket può avere un periodo di conservazione predefinito specificato in anni o giorni.

Come impostare la conservazione predefinita per un bucket

Per impostare la conservazione predefinita per un bucket, utilizzare uno dei seguenti metodi:

- Gestire le impostazioni del bucket da Tenant Manager. Vedere ["Creare un bucket S3"](#) e ["Aggiorna la conservazione predefinita del blocco oggetti S3"](#).
- Eseguire una richiesta `PutObjectLockConfiguration` per il bucket per specificare la modalità predefinita e il numero predefinito di giorni o anni.

PutObjectLockConfiguration

La richiesta `PutObjectLockConfiguration` consente di impostare e modificare la modalità di conservazione predefinita e il periodo di conservazione predefinito per un bucket con blocco oggetti S3 attivato. È inoltre possibile rimuovere le impostazioni di conservazione predefinite precedentemente configurate.

Quando nuove versioni degli oggetti vengono inserite 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 `retain-until-date` 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 di un oggetto, la retain-until-date della versione dell'oggetto rimane invariata e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito.

Per completare questa operazione, è necessario disporre dell'`s3:PutBucketObjectLockConfiguration` autorizzazione o essere account root.

Devi specificare una delle seguenti intestazioni della richiesta nella richiesta PutObjectLockConfiguration:

```
Content-MD5
x-amz-checksum-*
```



StorageGRID non convalida il contenuto dell'intestazione x-amz-checksum-* per questa operazione.

Esempio di richiesta

Questo esempio abilita S3 Object Lock per un bucket (se l'amministratore della griglia ha dato il permesso) e imposta la modalità di conservazione predefinita su COMPLIANCE e il periodo di conservazione predefinito su 6 anni.

```
PUT /bucket?object-lock HTTP/1.1
Accept-Encoding: identity
Content-Length: 308
Host: host
Content-MD5: request header
User-Agent: s3sign/1.0.0 requests/2.24.0 python/3.8.2
X-Amz-Date: date
X-Amz-Content-SHA256: authorization-string
Authorization: authorization-string

<ObjectLockConfiguration>
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Come determinare la conservazione predefinita per un bucket

Per determinare se S3 Object Lock è attivato per un bucket e per visualizzare la modalità di conservazione e il periodo di conservazione predefiniti, utilizzare uno dei seguenti metodi:

- Visualizza il bucket nel tenant manager. Vedere "[Visualizza i bucket S3](#)".
- Eseguire una richiesta GetObjectLockConfiguration.

GetObjectLockConfiguration

La richiesta GetObjectLockConfiguration consente di determinare se S3 Object Lock è attivato per un bucket e, se è attivato, verificare se sono presenti una modalità di conservazione predefinita e un periodo di conservazione configurato per il bucket.

Quando nuove versioni di oggetti vengono inserite nel bucket, viene applicata la modalità di conservazione predefinita se `x-amz-object-lock-mode` non è specificata. Il periodo di conservazione predefinito viene utilizzato per calcolare la `retain-until-date` se `x-amz-object-lock-retain-until-date` non è specificato.

Per completare questa operazione, è necessario disporre dell'`s3:GetBucketObjectLockConfiguration` autorizzazione o essere account root.

Esempio di richiesta

```
GET /bucket?object-lock HTTP/1.1
Host: host
Accept-Encoding: identity
User-Agent: aws-cli/1.18.106 Python/3.8.2 Linux/4.4.0-18362-Microsoft
botocore/1.17.29
x-amz-date: date
x-amz-content-sha256: authorization-string
Authorization: authorization-string
```

Esempio di risposta

```
HTTP/1.1 200 OK
x-amz-id-2:
iVmcB7OXXJRkRH1FiVq1151/T24gRfpwpuZrEG11Bb9ImOMAAe98oxSpXlknabA0LTvBYJpSIX
k=
x-amz-request-id: B34E94CACB2CEF6D
Date: Fri, 04 Sep 2020 22:47:09 GMT
Transfer-Encoding: chunked
Server: AmazonS3

<?xml version="1.0" encoding="UTF-8"?>
<ObjectLockConfiguration xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <ObjectLockEnabled>Enabled</ObjectLockEnabled>
  <Rule>
    <DefaultRetention>
      <Mode>COMPLIANCE</Mode>
      <Years>6</Years>
    </DefaultRetention>
  </Rule>
</ObjectLockConfiguration>
```

Come specificare le impostazioni di conservazione per un oggetto

Un bucket con S3 Object Lock abilitato può contenere una combinazione di oggetti con e senza le impostazioni di conservazione S3 Object Lock.

Le impostazioni di conservazione a livello di oggetto vengono specificate utilizzando l'API REST S3. Le impostazioni di conservazione per un oggetto sovrascrivono le impostazioni di conservazione predefinite per il bucket.

È possibile specificare le seguenti impostazioni per ciascun oggetto:

- **Modalità di conservazione:** CONFORMITÀ o GOVERNANCE.
- **Conserva-fino-data:** Una data che specifica per quanto tempo la versione dell'oggetto deve essere conservata da StorageGRID.
 - In modalità COMPLIANCE, se la data di conservazione è futura, l'oggetto può essere recuperato, ma non può essere modificato o cancellato. È possibile aumentare la data di conservazione fino alla data prevista, ma non è possibile ridurla o rimuoverla.
 - In modalità GOVERNANCE, gli utenti con autorizzazioni speciali possono ignorare l'impostazione di conservazione fino alla data odierna. Possono eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione. Possono anche aumentare, diminuire o addirittura rimuovere il mantenimento fino ad oggi.
- **Conservazione legale:** L'applicazione di un blocco legale a una versione oggetto blocca immediatamente tale oggetto. Ad esempio, potrebbe essere necessario sospendere legalmente un oggetto correlato a un'indagine o a una controversia legale. Una conservazione a fini giudiziari non ha una data di scadenza, ma rimane attiva fino a quando non viene esplicitamente rimossa.

L'impostazione di conservazione legale per un oggetto è indipendente dalla modalità di conservazione e dalla conservazione fino alla data. Se una versione dell'oggetto è sottoposta a blocco legale, nessuno può

eliminare tale versione.

Per specificare le impostazioni di blocco degli oggetti S3 quando si aggiunge una versione dell'oggetto a un bucket `"PutObject"`, eseguire una richiesta `"Oggetto CopyObject"` o `"CreateMultipartUpload"`.

È possibile utilizzare quanto segue:

- `x-amz-object-lock-mode`, Che può essere CONFORMITÀ o GOVERNANCE (distinzione tra maiuscole e minuscole).



Se si specifica `x-amz-object-lock-mode`, è necessario specificare anche `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 consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
 - La data di conservazione deve essere in futuro.
- `x-amz-object-lock-legal-hold`

Se la conservazione legale È ATTIVA (sensibile al maiuscolo/minuscolo), l'oggetto viene collocato sotto una conservazione legale. Se l'opzione `Legal Hold` è disattivata, non viene effettuata alcuna conservazione a fini giudiziari. Qualsiasi altro valore genera un errore 400 Bad Request (`InvalidArgument`).

Se si utilizza una di queste intestazioni di richiesta, tenere presente le seguenti restrizioni:

- Devi includere una delle seguenti intestazioni di richiesta se nella richiesta `PutObject` è presente una qualsiasi intestazione di richiesta `x-amz-object-lock-*`:

```
Content-MD5
x-amz-checksum-*
```

Queste intestazioni non sono necessarie per `CopyObject` o `CreateMultipartUpload`.

- Se il bucket non ha S3 Object Lock abilitato ed è presente un'intestazione di richiesta `x-amz-object-lock-*`, viene restituito un errore 400 Bad Request (`InvalidRequest`).
- La richiesta `PutObject` supporta l'uso di `x-amz-storage-class: REDUCED_REDUNDANCY` per abbinare il comportamento AWS. Tuttavia, quando un oggetto viene acquisito in un bucket con il blocco oggetti S3 attivato, `StorageGRID` eseguirà sempre un ingest a doppio commit.
- Una risposta successiva alla versione `GET` o `HeadObject` includerà le intestazioni `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, e `x-amz-object-lock-legal-hold`, se configurate e se il mittente della richiesta dispone delle autorizzazioni corrette `s3:Get*`.

È possibile utilizzare il `s3:object-lock-remaining-retention-days` tasto delle condizioni della policy per limitare i periodi di conservazione minimo e massimo consentiti per gli oggetti.

Come aggiornare le impostazioni di conservazione per un oggetto

Se è necessario aggiornare le impostazioni di conservazione o conservazione a fini giudiziari per una versione di oggetto esistente, è possibile eseguire le seguenti operazioni di sottosistema oggetto:

- `PutObjectLegalHold`

Se il nuovo valore di conservazione a fini giudiziari è **ATTIVO**, l'oggetto viene collocato sotto una conservazione a fini giudiziari. Se il valore di conservazione a fini giudiziari è **OFF**, la conservazione a fini giudiziari viene revocata.

- `PutObjectRetention`

- Il valore della modalità può essere **COMPLIANCE** o **GOVERNANCE** (distinzione tra maiuscole e minuscole).
- Il valore `Retain-until-date` deve essere nel formato `2020-08-10T21:46:00Z`. Sono consentiti i secondi frazionari, ma vengono conservate solo 3 cifre decimali (precisione in millisecondi). Non sono consentiti altri formati ISO 8601.
- Se una versione a oggetti ha un valore di conservazione esistente fino alla data odierna, è possibile aumentarlo. Il nuovo valore deve essere in futuro.

Devi specificare una delle seguenti intestazioni della richiesta:

```
Content-MD5
x-amz-checksum-*
```



StorageGRID non convalida il contenuto dell'intestazione `x-amz-checksum-*` per queste operazioni.

Come utilizzare LA modalità DI GOVERNANCE

Gli utenti che dispongono dell'`s3:BypassGovernanceRetention` autorizzazione possono ignorare le impostazioni di conservazione attive di un oggetto che utilizza la modalità di **GOVERNANCE**. Tutte le operazioni di **ELIMINAZIONE** o `PutObjectRetention` devono includere l'`x-amz-bypass-governance-retention:true` intestazione della richiesta. Questi utenti possono eseguire queste operazioni aggiuntive:

- Eseguire operazioni `DeleteObject` o `DeleteObjects` per eliminare una versione dell'oggetto prima che sia trascorso il periodo di conservazione.

Non è possibile eliminare gli oggetti che si trovano sotto un blocco legale. La sospensione legale deve essere disattivata.

L'`x-amz-bypass-governance-retention` intestazione non ha alcun effetto sugli oggetti senza S3 Object Lock.

- Eseguire le operazioni `PutObjectRetention` che modificano la modalità di una versione dell'oggetto dalla **GOVERNANCE** alla **CONFORMITÀ** prima che sia trascorso il periodo di conservazione dell'oggetto.

Non è mai consentito cambiare la modalità dalla **CONFORMITÀ** alla **GOVERNANCE**.

- Eseguire le operazioni `PutObjectRetention` per aumentare, ridurre o rimuovere il periodo di conservazione di una versione oggetto.

Informazioni correlate

- ["Gestire gli oggetti con S3 Object Lock"](#)
- ["USA il blocco oggetti S3 per conservare gli oggetti"](#)
- ["Guida dell'utente di Amazon Simple Storage Service: Blocco degli oggetti"](#)

Scopri la configurazione del ciclo di vita S3 per StorageGRID

È possibile creare una configurazione del ciclo di vita S3 per controllare quando oggetti specifici vengono cancellati 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 dettagli completi sulla creazione di configurazioni del ciclo di vita S3, vedi ["Guida utente di Amazon Simple Storage Service: Gestione del ciclo di vita degli oggetti"](#). Nota che StorageGRID supporta solo azioni di scadenza; non supporta azioni di transizione.

Che cos'è la configurazione del ciclo di vita

Una configurazione del ciclo di vita è un insieme di regole applicate agli oggetti in specifici bucket S3. Ogni regola specifica quali oggetti sono interessati e quando scadranno (in una data specifica o dopo un certo numero di giorni).

StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML:

- Scadenza: Consente di eliminare un oggetto quando viene raggiunta una data specificata o quando viene raggiunto un numero di giorni specificato, a partire dalla data di acquisizione dell'oggetto.
- NoncurrentVersionExpiration (NoncurrentExpiration versione): Consente di eliminare un oggetto quando viene raggiunto un numero di giorni specificato, a partire da quando l'oggetto è diventato non corrente.
- Filtro (prefisso, tag)
- Stato
- ID

Ciascun oggetto segue le impostazioni di conservazione di un ciclo di vita bucket S3 o di un criterio ILM. Quando viene configurato un ciclo di vita del bucket S3, le azioni di scadenza del ciclo di vita sovrascrivono il criterio ILM per gli oggetti corrispondenti al filtro del ciclo di vita del bucket. Gli oggetti che non corrispondono al filtro del ciclo di vita del bucket utilizzano le impostazioni di conservazione del criterio ILM. Se un oggetto corrisponde a un filtro del ciclo di vita bucket e non sono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione del criterio ILM non vengono utilizzate ed è implicito che le versioni degli oggetti vengano mantenute per sempre. Vedere ["Esempi di priorità per il ciclo di vita dei bucket S3 e la politica ILM"](#).

Di conseguenza, un oggetto potrebbe essere rimosso dalla griglia anche se le istruzioni di posizionamento in una regola ILM sono ancora applicabili all'oggetto. Oppure, un oggetto potrebbe essere conservato sulla griglia anche dopo che sono scadute le istruzioni di posizionamento ILM per l'oggetto. Per ulteriori informazioni, vedere ["Come ILM opera per tutta la vita di un oggetto"](#).



La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

StorageGRID supporta l'utilizzo delle seguenti operazioni bucket per gestire le configurazioni del ciclo di vita:

- DeleteBucketLifecycle
- GetBucketLifecycleConfiguration
- PutBucketLifecycleConfiguration

Creare la configurazione del ciclo di vita

Come primo passo nella creazione di una configurazione del ciclo di vita, è possibile creare un file JSON che includa una o più regole. Ad esempio, questo file JSON include tre regole, come segue:

1. La regola 1 si applica solo agli oggetti che corrispondono al prefisso `category1/` e che hanno un `key2` valore di `tag2`. Il `Expiration` parametro specifica che gli oggetti corrispondenti 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` parametro specifica che gli oggetti corrispondenti al filtro scadranno 100 giorni dopo l'acquisizione.



Le regole che specificano un numero di giorni sono relative al momento in cui l'oggetto è stato acquisito. Se la data corrente supera la data di acquisizione più il numero di giorni, alcuni oggetti potrebbero essere rimossi dal bucket non appena viene applicata la configurazione del ciclo di vita.

3. La regola 3 si applica solo agli oggetti che corrispondono al prefisso `category3/`. Il `Expiration` parametro specifica che tutte le versioni non correnti degli oggetti corrispondenti scadranno 50 giorni dopo che diventano 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, applicarlo a un bucket inviando una richiesta `PutBucketLifecycleConfiguration`.

Questa richiesta applica la configurazione del ciclo di vita nel file di esempio agli oggetti in un bucket denominato `testbucket`.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-bucket-lifecycle-configuration
--bucket testbucket --lifecycle-configuration file://bktjson.json
```

Per verificare che una configurazione del ciclo di vita sia stata applicata correttamente al bucket, eseguire una richiesta `GetBucketLifecycleConfiguration`. Ad esempio:

```
aws s3api --endpoint-url <StorageGRID endpoint> get-bucket-lifecycle-configuration
--bucket testbucket
```

Una risposta corretta elenca la configurazione del ciclo di vita appena applicata.

Verificare che la scadenza del ciclo di vita del bucket si applichi all'oggetto

È possibile determinare se una regola di scadenza nella configurazione del ciclo di vita si applica a un oggetto specifico quando si invia una richiesta `PutObject`, `HeadObject` o `GetObject`. Se si applica una regola, la risposta include un `Expiration` parametro che indica quando l'oggetto scade e quale regola di scadenza è stata abbinata.



Poiché il ciclo di vita del bucket sovrascrive ILM, `expiry-date` viene visualizzata la data effettiva in cui l'oggetto verrà eliminato. Per ulteriori informazioni, vedere ["Come viene determinata la conservazione degli oggetti"](#).

Ad esempio, questa richiesta `PutObject` è stata emessa il 22 giugno 2020 e inserisce un oggetto nel `testbucket` bucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> put-object
--bucket testbucket --key obj2test2 --body bktjson.json
```

La risposta corretta indica che l'oggetto scadrà tra 100 giorni (01 ottobre 2020) e che corrisponde alla regola 2 della configurazione del ciclo di vita.

```
{
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:49 GMT\\", rule-
id=\\"rule2\\",
  ETag: "\\"9762f8a803bc34f5340579d4446076f7\\""}
}
```

Ad esempio, questa richiesta HeadObject è stata utilizzata per ottenere metadati per lo stesso oggetto nel bucket testbucket.

```
aws s3api --endpoint-url <StorageGRID endpoint> head-object
--bucket testbucket --key obj2test2
```

La risposta di successo include i metadati dell'oggetto e indica che l'oggetto scadrà tra 100 giorni e che corrisponde alla regola 2.

```
{
  "AcceptRanges": "bytes",
  *Expiration: "expiry-date=\\"Thu, 01 Oct 2020 09:07:48 GMT\\", rule-
id=\\"rule2\\",
  "LastModified": "2020-06-23T09:07:48+00:00",
  "ContentLength": 921,
  "ETag": "\\"9762f8a803bc34f5340579d4446076f7\\""}
  "ContentType": "binary/octet-stream",
  "Metadata": {}
}
```



Per i bucket abilitati per la versione, l'`x-amz-expiration` intestazione della risposta si applica solo alle versioni correnti di oggetti.

Raccomandazioni per l'implementazione dell'API REST S3 con StorageGRID

Seguire questi consigli quando si implementa l'API REST S3 per l'utilizzo con StorageGRID.

Raccomandazioni per la gestione di 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 ricevere un numero elevato di errori del server interno 500 se due o più nodi di archiviazione nello stesso sito non sono disponibili o un sito remoto non è raggiungibile.

È possibile impostare la coerenza "disponibile" per ciascun bucket utilizzando la richiesta oppure specificare la coerenza nell'intestazione della ["METTI la coerenza del bucket"](#) richiesta per una singola operazione API.

Raccomandazioni per le chiavi a oggetti

Seguire questi consigli per i nomi delle chiavi degli oggetti, in base alla prima volta che il bucket è stato creato.

Bucket creati in StorageGRID 11.4 o versioni precedenti

- Non utilizzare valori casuali come primi quattro caratteri delle chiavi oggetto. Ciò è in contrasto con la precedente raccomandazione AWS per i prefissi principali. Utilizzare invece prefissi non casuali e non univoci, ad esempio `image`.
- Se si segue la precedente raccomandazione AWS per utilizzare caratteri casuali e univoci nei prefissi delle chiavi, inserire un prefisso tra le chiavi degli oggetti e il nome della directory. Ovvero, utilizzare questo formato:

```
mybucket/mydir/f8e3-image3132.jpg
```

Invece di questo formato:

```
mybucket/f8e3-image3132.jpg
```

Bucket creati in StorageGRID 11.4 o versioni successive

Non è necessario limitare i nomi delle chiavi degli oggetti per soddisfare le Best practice di performance. Nella maggior parte dei casi, è possibile utilizzare valori casuali per i primi quattro caratteri dei nomi delle chiavi degli oggetti.



Un'eccezione è rappresentata da un carico di lavoro S3 che rimuove continuamente tutti gli oggetti dopo un breve periodo di tempo. Per ridurre al minimo l'impatto delle performance per questo caso d'utilizzo, modificare una parte iniziale del nome della chiave ogni diverse migliaia di oggetti con qualcosa di simile alla data. Si supponga, ad esempio, che un client S3 scriva in genere 2,000 oggetti al secondo e che il criterio del ciclo di vita di ILM o bucket rimuova tutti gli oggetti dopo tre giorni. Per ridurre al minimo l'impatto sulle prestazioni, è possibile assegnare un nome alle chiavi utilizzando uno schema simile al seguente:

```
/mybucket/mydir/yyyymmddhhmmss-random_UUID.jpg
```

Raccomandazioni per "letture di gamma"

Se ["opzione globale per comprimere gli oggetti memorizzati"](#) è attivato, le applicazioni client S3 devono evitare di eseguire operazioni `GetObject` che specificano un intervallo di byte da restituire. Queste operazioni di "lettura dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. Le operazioni `GetObject` che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client possono scadere.



Se è necessario comprimere gli oggetti e l'applicazione client deve utilizzare le letture dell'intervallo, aumentare il timeout di lettura per l'applicazione.

Supporto per Amazon S3 REST API

Operazioni supportate e limitazioni dell'API REST S3 in StorageGRID

Il sistema StorageGRID implementa l'API del servizio di storage semplice (API versione

2006-03-01) con il supporto per la maggior parte delle operazioni e con alcune limitazioni. È necessario comprendere i dettagli dell'implementazione quando si integrano le applicazioni client API REST S3.

Il sistema StorageGRID supporta sia le richieste in stile virtual-hosted che quelle in stile path.

Gestione della data

L'implementazione StorageGRID dell'API REST S3 supporta solo formati di data HTTP validi.

Il sistema StorageGRID supporta solo i formati di data HTTP validi per tutte le intestazioni che accettano i valori di data. La parte temporale della data può essere specificata nel formato GMT (Greenwich Mean Time) o UTC (Universal Coordinated Time) senza offset del fuso orario (deve essere specificato ++1). Se si include l'`x-amz-date` intestazione nella richiesta, questo sovrascrive qualsiasi valore specificato nell'intestazione della richiesta Data. Quando si utilizza la versione 4 della firma AWS, l'`x-amz-date` 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 delle richieste comuni definite da ["Amazon Simple Storage Service API Reference: Intestazioni di richiesta comuni"](#), con un'eccezione.

Intestazione della richiesta	Implementazione
Autorizzazione	Supporto completo per firma AWS versione 2 Supporto per firma AWS versione 4, con le seguenti eccezioni: Quando si fornisce il valore checksum del payload effettivo in <code>x-amz-content-sha256</code>, il valore viene accettato senza convalida, come se il valore <code>UNSIGNED-PAYLOAD</code> fosse stato fornito per l'intestazione. Quando si fornisce un <code>x-amz-content-sha256</code> valore di intestazione che implica <code>aws-chunked</code> lo streaming (ad esempio, <code>STREAMING-AWS4-HMAC-SHA256-PAYLOAD</code>), le firme dei frammenti non vengono verificate in base ai dati dei frammenti.

Intestazioni di risposta comuni

Il sistema StorageGRID supporta tutte le intestazioni di risposta comuni definite dal *referimento API del servizio di storage semplice*, con un'eccezione.

Intestazione della risposta	Implementazione
<code>x-amz-id-2</code>	Non utilizzato

Come StorageGRID S3 REST API autentica le richieste

Il sistema StorageGRID supporta l'accesso anonimo e autenticato agli oggetti utilizzando l'API S3.

L'API S3 supporta Signature versione 2 e Signature versione 4 per l'autenticazione delle richieste API S3.

Le richieste autenticate devono essere firmate utilizzando l'ID della chiave di accesso e la chiave di accesso segreta.

Il sistema StorageGRID supporta due metodi di autenticazione: L'intestazione HTTP `Authorization` e i parametri di query.

Utilizzare l'intestazione autorizzazione HTTP

L'intestazione HTTP `Authorization` viene utilizzata da tutte le operazioni API S3, ad eccezione delle richieste anonime, laddove consentito dal criterio bucket. L' `Authorization` 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, che può essere utilizzata per concedere l'accesso temporaneo a risorse specifiche. Gli utenti con l'URL con prefisso non devono conoscere la chiave di accesso segreta per accedere alla risorsa, consentendo così l'accesso limitato a una risorsa da parte di terze parti.

Operazioni di servizio supportate in StorageGRID

Il sistema StorageGRID supporta le seguenti operazioni sul servizio.

Operazione	Implementazione
ListBucket (Precedentemente denominato GET Service)	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
OTTIENI l'utilizzo dello storage	La richiesta StorageGRID " OTTIENI l'utilizzo dello storage " indica la quantità totale di storage utilizzata da un account e per ogni bucket associato all'account. Si tratta di un'operazione sul servizio con un percorso di / e un parametro di query personalizzato (<code>?x-ntap-sg-usage</code>) aggiunto.
OPZIONI /	Le applicazioni client possono OPTIONS / inviare 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 storage è inattivo.

Operazioni del bucket S3 e dettagli di implementazione in StorageGRID

Il sistema StorageGRID supporta un massimo di 20.000 bucket per ogni account tenant S3.

Ogni griglia può avere un massimo di 100.000 secchi.

Se più tenant dispongono ciascuno di un massimo di 5.000 bucket, ogni Storage Node nella griglia deve avere un minimo di 64 GB di RAM.

Le restrizioni sui nomi dei bucket seguono le restrizioni standard della regione AWS US, ma dovresti limitarle ulteriormente alle convenzioni di denominazione DNS per supportare le richieste S3 in stile virtual-hosted.

Per ulteriori informazioni, consulta quanto segue:

- ["Guida 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"](#).

Puoi verificare se gli aggiornamenti all'ora dell'ultimo accesso sono abilitati o disabilitati per i singoli bucket. Consulta ["OTTIENI l'ultimo tempo di accesso a bucket"](#).

La seguente tabella descrive come StorageGRID implementa le operazioni del bucket API REST S3. Per eseguire una di queste operazioni, è necessario fornire le credenziali di accesso necessarie per l'account.

Operazione	Implementazione
CreateBucket	Crea un nuovo bucket. Creando il bucket, diventerai il proprietario del bucket. Nota: i bucket di directory S3 non sono supportati. • I nomi dei bucket devono rispettare le seguenti regole: ◦ Deve essere unico in ogni sistema StorageGRID (non solo univoco all'interno dell'account tenant). ◦ Deve essere conforme al DNS. ◦ Deve contenere almeno 3 e non più di 63 caratteri. ◦ Può essere una serie di una o più etichette, con etichette adiacenti separate da un punto. Ogni etichetta deve iniziare e terminare con una lettera minuscola o un numero e può utilizzare solo lettere minuscole, numeri e trattini. ◦ Non deve essere simile a un indirizzo IP formattato con testo. ◦ Non utilizzare i periodi nelle richieste di stile ospitate virtuali. I punti causano problemi con la verifica del certificato con caratteri jolly del server. • Per impostazione predefinita, i bucket vengono creati nella <code>us-east-1</code> regione; tuttavia, è possibile utilizzare l' <code>`LocationConstraint`</code> elemento di richiesta nel corpo della richiesta per specificare un'area diversa. Quando si utilizza l' <code>`LocationConstraint`</code> elemento, è necessario specificare il nome esatto di una regione definita utilizzando Grid Manager o l'API di gestione griglia. Contattare l'amministratore di sistema se non si conosce il nome della regione da utilizzare. Nota: Si verificherà un errore se la tua richiesta CreateBucket utilizza una regione che non è stata definita in StorageGRID. • Puoi includere l' <code>`x-amz-bucket-object-lock-enabled`</code> intestazione della richiesta per creare un bucket con S3 Object Lock abilitato. Consulta "Utilizzare l'API REST S3 per configurare il blocco oggetti S3". S3 Object Lock richiede il versioning del bucket, che viene abilitato automaticamente quando crei il bucket con S3 Object Lock abilitato. Puoi abilitare S3 Object Lock quando crei il bucket o in un secondo momento.
DeleteBucket	Elimina il bucket.
DeleteBucketCors	Elimina la configurazione CORS per il bucket.
DeleteBucketEncryption	Elimina la crittografia predefinita dal bucket. Gli oggetti crittografati esistenti rimangono crittografati, ma i nuovi oggetti aggiunti al bucket non vengono crittografati.

Operazione	Implementazione
DeleteBucketLifecycle	Elimina la configurazione del ciclo di vita dal bucket. Consulta "Creare la configurazione del ciclo di vita S3" .
DeleteBucketPolicy	Elimina il criterio allegato al bucket.
DeleteBucketReplication	Elimina la configurazione di replica collegata al bucket.
DeleteBucketTagging	Utilizza la <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, sarà presente un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag del bucket con un valore assegnato. Non inviare una richiesta <code>DeleteBucketTagging</code> se è presente un <code>NTAP-SG-ILM-BUCKET-TAG</code> tag del bucket. Invece, invia una richiesta <code>PutBucketTagging</code> con solo il <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> tag del bucket.
GetBucketAcl	Restituisce una risposta positiva e l'ID, il <code>DisplayName</code> e l'autorizzazione del proprietario del bucket, indicando che il proprietario ha accesso completo al bucket.
GetBucketCors	Restituisce la <code>cors</code> configurazione per la benna.
GetBucketEncryption	Restituisce la configurazione di crittografia predefinita per il bucket.
GetBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket GET)	Restituisce la configurazione del ciclo di vita per il bucket. Consulta "Creare la configurazione del ciclo di vita S3" .
GetBucketLocation	Restituisce la regione che hai impostato usando l' <code>LocationConstraint</code> elemento nella richiesta <code>CreateBucket</code> . Se la regione del bucket è <code>us-east-1</code> (predefinita), viene restituito un valore vuoto per <code>LocationConstraint</code> .
GetBucketNotificationConfiguration (Precedentemente denominata notifica bucket GET)	Restituisce la configurazione di notifica collegata al bucket.
GetBucketPolicy	Restituisce la policy allegata al bucket.

Operazione	Implementazione
GetBucketReplication	Restituisce la configurazione di replica collegata al bucket.
GetBucketTagging	Utilizza la <code>tagging</code> sottorisorsa per restituire tutti i tag per un bucket. Attenzione: se per questo bucket è impostato un tag di policy ILM diverso da quello predefinito, ci sarà un tag del bucket <code>NTAP-SG-ILM-BUCKET-TAG</code> con un valore assegnato. Non modificare o rimuovere questo tag.
GetBucketVersioning	Questa implementazione utilizza la <code>versioning</code> sottorisorsa per restituire lo stato di versione di un bucket. • <i>Blank</i>: La versione non è mai stata abilitata (bucket "Unversioned") • <i>Enabled</i> (attivato): Il controllo delle versioni è attivato • <i>Suspended</i> (sospeso): Il controllo delle versioni era stato precedentemente attivato e sospeso
GetObjectLockConfiguration	Restituisce la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito, se configurato. Consulta "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".
HeadBucket	Determina se esiste un bucket e si dispone dell'autorizzazione per accedervi. Questa operazione restituisce: • <code>x-ntap-sg-bucket-id</code>: UUID del bucket in formato UUID. • <code>x-ntap-sg-trace-id</code>: L'ID di traccia univoco della richiesta associata.

Operazione	Implementazione
ListObjects e ListObjectsV2 (Precedentemente denominato GET Bucket)	Restituisce alcuni o tutti gli oggetti (fino a 1.000) in un bucket. La classe di archiviazione per gli oggetti può avere due valori, anche se l'oggetto è stato acquisito con l' `REDUCED_REDUNDANCY` opzione della classe di archiviazione: • STANDARD, Che indica che l'oggetto è memorizzato in un pool di archiviazione costituito da nodi di archiviazione. • GLACIER, Che indica che l'oggetto è stato spostato nel bucket esterno specificato dal Cloud Storage Pool. Se il bucket contiene un numero elevato di chiavi eliminate con lo stesso prefisso, la risposta potrebbe includere alcune <code>CommonPrefixes</code> che non contengono chiavi. Per le richieste <code>HeadObject</code> e <code>ListObject</code>, <code>StorageGRID</code> restituisce i timestamp <code>LastModified</code> con una precisione diversa, mentre <code>AWS</code> restituisce i timestamp con la stessa precisione, come mostrato negli esempi seguenti: • <code>StorageGRID HeadObject</code>: "Ultima modifica": "2024-09-26T16:43:24+00:00" • <code>StorageGRID ListObject</code>: "Ultima modifica": "2024-09-26T16:43:24.931000+00:00" • <code>AWS HeadObject</code>: "Ultima modifica": "2023-10-17T00:19:54+00:00" • <code>AWS ListObject</code>: "Ultima modifica": "2023-10-17T00:19:54+00:00"
ListObjectVersions (Precedentemente denominate versioni oggetto GET Bucket)	Con l'accesso IN LETTURA IN un bucket, questa operazione con le <code>versions</code> risorse secondarie elenca i metadati di tutte le versioni di oggetti nel bucket.
PutBucketCors	Imposta la configurazione CORS per un bucket in modo che il bucket possa gestire le richieste cross-origin. La condivisione delle risorse tra origini (CORS) è un meccanismo di sicurezza che consente alle applicazioni Web client di un dominio di accedere alle risorse di un dominio diverso. Ad esempio, si supponga di utilizzare un bucket S3 denominato <code>images</code> per memorizzare la grafica. Impostando la configurazione CORS per il <code>images</code> bucket, è possibile consentire la visualizzazione delle immagini in quel bucket sul sito Web <code>http://www.example.com</code>.

Operazione	Implementazione
PutBucketEncryption	Consente di impostare lo stato di crittografia predefinito di un bucket esistente. Quando la crittografia a livello di bucket è attivata, tutti i nuovi oggetti aggiunti al bucket vengono crittografati. StorageGRID supporta la crittografia lato server con le chiavi gestite da StorageGRID. Quando si specifica la regola di configurazione della crittografia lato server, impostare il <code>SSEAlgorithm</code> parametro su <code>AES256</code> e non utilizzare il <code>KMSMasterKeyID</code> parametro. La configurazione della crittografia predefinita del bucket viene ignorata se la richiesta di caricamento dell'oggetto specifica già la crittografia (ovvero, se la richiesta include l' <code>`x-amz-server-side-encryption-*</code> intestazione della richiesta).
PutBucketLifecycleConfiguration (Precedentemente denominato ciclo di vita bucket PUT)	Crea una nuova configurazione del ciclo di vita per il bucket o sostituisce una configurazione del ciclo di vita esistente. StorageGRID supporta fino a 1,000 regole del ciclo di vita in una configurazione del ciclo di vita. Ogni regola può includere i seguenti elementi XML: • Scadenza (giorni, data, <code>ExpiredObjectDeleteMarker</code>) • <code>NoncurrentVersionExpiration</code> (<code>NewerNoncurrentVersions</code>, <code>NoncurrentDays</code>) • Filtro (prefisso, tag) • Stato • ID StorageGRID non supporta queste azioni: • <code>AbortIncompleteMultipartUpload</code> • Transizione Fai riferimento a "Creare la configurazione del ciclo di vita S3". Per capire come l'azione di <code>Expiration</code> nel ciclo di vita di un bucket interagisce con le istruzioni di posizionamento ILM, fai riferimento a "Come ILM opera per tutta la vita di un oggetto". Nota: La configurazione del ciclo di vita del bucket può essere utilizzata con bucket con blocco oggetti S3 attivato, ma la configurazione del ciclo di vita del bucket non è supportata per bucket conformi legacy.

Operazione	Implementazione
PutBucketNotificationConfiguration (Precedentemente denominata notifica bucket PUT)	Configura le notifiche per il bucket utilizzando l'XML di configurazione delle notifiche incluso nel corpo della richiesta. È necessario conoscere i seguenti dettagli di implementazione: - StorageGRID supporta argomenti Amazon Simple Notification Service (Amazon SNS), argomenti Kafka o endpoint webhook come destinazioni. Gli endpoint Simple Queue Service (SQS) o AWS Lambda non sono supportati. - La destinazione delle notifiche deve essere specificata come URN di un endpoint StorageGRID. Gli endpoint possono essere creati utilizzando il tenant Manager o l'API di gestione tenant. L'endpoint deve esistere perché la configurazione della notifica abbia esito positivo. Se l'endpoint non esiste, viene restituito un 400 Bad Request errore con il codice <code>InvalidArgument</code>. - Non è possibile configurare una notifica per i seguenti tipi di evento. Questi tipi di evento sono non supportati. <code>s3:ReducedRedundancyLostObject</code> <code>s3:ObjectRestore:Completed</code> - Le notifiche degli eventi inviate da StorageGRID utilizzano il formato JSON standard, ad eccezione del fatto che non includono alcune chiavi e utilizzano valori specifici per altre, come mostrato nell'elenco seguente: EventSource <code>sgws:s3</code> AwsRegion non incluso x-amz-id-2 non incluso arn <code>urn:sgws:s3:::bucket_name</code>
PutBucketPolicy	Imposta i criteri associati al bucket. Fai riferimento a "Utilizza policy di accesso a bucket e gruppi" .

Operazione	Implementazione
PutBucketReplication	Si configura "Replica di StorageGRID CloudMirror" per il bucket utilizzando l'XML di configurazione della replica fornito nel corpo della richiesta. Per la replica di CloudMirror, è necessario conoscere i seguenti dettagli di implementazione: • StorageGRID supporta solo la V1 della configurazione di replica. Questo significa che StorageGRID non supporta l'uso dell'elemento <code>Filter</code> per le regole e segue le convenzioni della V1 per l'eliminazione delle versioni degli oggetti. Per dettagli, consulta "Guida utente di Amazon Simple Storage Service: Configurazione della replica". • La replica del bucket può essere configurata su bucket con versione o senza versione. • È possibile specificare un bucket di destinazione diverso in ciascuna regola dell'XML di configurazione della replica. Un bucket di origine può replicare in più di un bucket di destinazione. • I bucket di destinazione devono essere specificati come URN degli endpoint StorageGRID come specificato in Tenant Manager o nell'API di gestione del tenant. Consulta "Configurare la replica di CloudMirror". L'endpoint deve esistere per il successo della configurazione della replica. Se l'endpoint non esiste, la richiesta non riesce come <code>400 Bad Request</code>. Il messaggio di errore indica: <code>Unable to save the replication policy. The specified endpoint URN does not exist: URN.</code> • 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 la <code>STANDARD</code> classe di archiviazione per impostazione predefinita. • Se si elimina un oggetto dal bucket di origine o si elimina lo stesso bucket di origine, il comportamento della replica tra regioni è il seguente: ◦ Se si elimina l'oggetto o il bucket prima che sia stato replicato, l'oggetto/bucket non viene replicato e non viene inviata alcuna notifica. ◦ Se elimini l'oggetto o il bucket dopo che è stato replicato, StorageGRID segue il comportamento standard di eliminazione di Amazon S3 per V1 della replica tra regioni.

Operazione	Implementazione
PutBucketTagging	Utilizza la <code>tagging</code> sottorisorsa per aggiungere o aggiornare una serie di tag per un bucket. Quando si aggiungono tag bucket, tenere presente le seguenti limitazioni: • StorageGRID e Amazon S3 supportano fino a 50 tag per ciascun bucket. • Le etichette associate a un bucket devono avere chiavi tag univoche. Una chiave tag può contenere fino a 128 caratteri Unicode. • I valori dei tag possono contenere fino a 256 caratteri Unicode. • Chiave e valori distinguono tra maiuscole e minuscole. Attenzione: se per questo bucket è impostato un tag di policy ILM non predefinito, ci sarà un tag <code>NTAP-SG-ILM-BUCKET-TAG</code> del bucket con un valore assegnato. Assicurati che il tag <code>NTAP-SG-ILM-BUCKET-TAG</code> del bucket sia incluso con il valore assegnato in tutte le richieste PutBucketTagging. Non modificare o rimuovere questo tag. Nota: Questa operazione sovrascriverà tutti i tag correnti già presenti nel bucket. Se qualsiasi tag esistente viene omissso dal set, tali tag verranno rimossi per il bucket.
PutBucketVersioning	Utilizza la <code>versioning</code> sottorisorsa per impostare lo stato di versione di un bucket esistente. È possibile impostare lo stato di versione con uno dei seguenti valori: • Enabled (attivato): Attiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono un ID di versione univoco. • Suspended (sospeso): Disattiva il controllo delle versioni degli oggetti nel bucket. Tutti gli oggetti aggiunti al bucket ricevono l'ID versione <code>null</code>.
PutObjectLockConfiguration	• Configura o rimuove la modalità di conservazione predefinita del bucket e il periodo di conservazione predefinito. • Se l'amministratore della griglia ha dato il permesso, abilita S3 Object Lock sui bucket esistenti. Se il periodo di conservazione predefinito viene modificato, la <code>retain-until-date</code> delle versioni degli oggetti esistenti rimane la stessa e non viene ricalcolata utilizzando il nuovo periodo di conservazione predefinito. Per informazioni dettagliate, consulta "Utilizzare l'API REST S3 per configurare il blocco oggetti S3".

Operazioni sugli oggetti

Come StorageGRID implementa le operazioni S3 REST API per gli oggetti

Questa sezione descrive come il sistema StorageGRID implementa le operazioni API REST S3 per gli oggetti.

Le seguenti condizioni si applicano a tutte le operazioni a oggetti:

- StorageGRID "valori di coerenza" sono supportati da tutte le operazioni sugli oggetti, ad eccezione delle seguenti:
 - GetObjectAcl
 - OPTIONS /
 - PutObjectLegalHold
 - PutObjectRetention
 - SelectObjectContent
- Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.
- Tutti gli oggetti in un bucket StorageGRID sono di proprietà del proprietario del bucket, inclusi gli oggetti creati da un utente anonimo o da un altro account.

Nella tabella seguente viene descritto il modo in cui StorageGRID implementa le operazioni degli oggetti API REST S3.

Operazione	Implementazione
DeleteObject (Elimina oggetto)	Durante l'elaborazione di una richiesta DeleteObject, StorageGRID tenta di rimuovere immediatamente tutte le copie dell'oggetto da tutte le posizioni memorizzate. Se l'esito è positivo, StorageGRID restituisce immediatamente una risposta al client. Se non è possibile rimuovere tutte le copie entro 30 secondi (ad esempio, perché una posizione è temporaneamente non disponibile), StorageGRID mette in coda le copie per la rimozione e indica che il client è riuscito. Restrizioni • L'autenticazione multifattore (MFA) e l'intestazione della risposta <code>x-amz-mfa</code> non sono supportate. • Le <code>If-Match</code> e <code>If-None-Match</code> intestazioni si comportano in modo diverso a seconda della configurazione di StorageGRID. Fornire queste intestazioni potrebbe restituire un messaggio di errore (501 Not Implemented). Se le <code>If-Match</code> o <code>If-None-Match</code> intestazioni vengono accettate ma non sono funzionanti, potrebbe essere attivato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented. L' <code>x-amz-bypass-governance-retention</code> intestazione non ha alcun effetto sugli oggetti senza S3 Object Lock. Versione Per rimuovere una versione specifica, il richiedente deve essere il proprietario del bucket e utilizzare la <code>versionId</code> sottorisorsa. L'utilizzo di questa sottorisorsa elimina in modo permanente la versione. Se il <code>versionId</code> corrisponde a un marcatore di eliminazione, l'intestazione della risposta <code>x-amz-delete-marker</code> viene riportata impostata su <code>true</code>. • Se un oggetto viene eliminato senza la <code>versionId</code> sottorisorsa in un bucket con il controllo delle versioni attivato, viene generato un indicatore di eliminazione. Il <code>versionId</code> marcatore per l'eliminazione viene restituito utilizzando l' <code>x-amz-version-id</code> intestazione della risposta e l' <code>x-amz-delete-marker</code> intestazione della risposta viene riportata impostata su <code>true</code>. • Se un oggetto viene eliminato senza la <code>versionId</code> sottorisorsa in un bucket con la versione sospesa, si ottiene l'eliminazione permanente di una versione 'null' già esistente o di un marcatore 'null' e la generazione di un nuovo marcatore 'null'. L' <code>x-amz-delete-marker</code> intestazione della risposta viene riportata impostata su <code>true</code>. Nota: In alcuni casi, per un oggetto potrebbero esistere più contrassegni di eliminazione. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.

Operazione	Implementazione
DeleteObjects (Precedentemente denominato ELIMINA più oggetti)	L'autenticazione multifattore (MFA) e l'intestazione della risposta <code>x-amz-mfa</code> non sono supportate. È possibile eliminare più oggetti nello stesso messaggio di richiesta. L' <code>x-amz-bypass-governance-retention</code> intestazione non ha alcun effetto sugli oggetti senza S3 Object Lock. Vedere "Utilizzare l'API REST S3 per configurare il blocco oggetti S3" per informazioni su come eliminare le versioni degli oggetti in modalità GOVERNANCE.
DeleteObjectTagging	Utilizza la <code>tagging</code> sottorisorsa per rimuovere tutti i tag da un oggetto. Versione Se il <code>versionId</code> parametro query non è specificato nella richiesta, l'operazione elimina tutti i tag dalla versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato <code>"MethodNotAllowed"</code> con l' <code>x-amz-delete-marker</code> intestazione della risposta impostata su <code>true</code>.
GetObject	"GetObject"
GetObjectAcl	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, indicando che il proprietario dispone dell'accesso completo all'oggetto.
GetObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
GetObjectTagging	Utilizza la <code>tagging</code> sottorisorsa per restituire tutti i tag per un oggetto. Versione Se il <code>versionId</code> parametro query non è specificato nella richiesta, l'operazione restituisce tutti i tag della versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato <code>"MethodNotAllowed"</code> con l' <code>x-amz-delete-marker</code> intestazione della risposta impostata su <code>true</code>.
HeadObject (oggetto intestazione)	"HeadObject (oggetto intestazione)"

Operazione	Implementazione
RestoreObject	"RestoreObject"
PutObject	"PutObject"
Oggetto CopyObject (Precedentemente denominato oggetto PUT - Copia)	"Oggetto CopyObject"
PutObjectLegalHold	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"
PutObjectRetention	"Utilizzare l'API REST S3 per configurare il blocco oggetti S3"

Operazione	Implementazione
PutObjectTagging	Utilizza la <code>tagging</code> sottorisorsa per aggiungere una serie di tag a un oggetto esistente. Limiti tag oggetto È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole. Aggiornamenti dei tag e comportamento di acquisizione Quando si utilizza PutObjectTagging per aggiornare i tag di un oggetto, StorageGRID non acquisisce nuovamente l'oggetto. Ciò significa che l'opzione per il comportamento di Ingest specificata nella regola ILM corrispondente non viene utilizzata. Le modifiche al posizionamento degli oggetti che vengono attivate dall'aggiornamento vengono apportate quando ILM viene rivalutato dai normali processi ILM in background. Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto. Risoluzione dei conflitti Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione. Versione Se il <code>versionId</code> parametro query non è specificato nella richiesta, l'operazione aggiunge tag alla versione più recente dell'oggetto in un bucket in versione. Se la versione corrente dell'oggetto è un marcatore di eliminazione, viene restituito lo stato "MethodNotAllowed" con l'<code>x-amz-delete-marker</code> intestazione della risposta impostata su <code>true</code>.
SelectObjectContent	"SelectObjectContent"

Operazioni Amazon S3 Select supportate in StorageGRID

StorageGRID supporta le seguenti condizioni, tipi di dati e operatori Amazon S3 Select per ["Comando SelectObjectContent"](#).



Gli elementi non elencati non sono supportati.

Per la sintassi, vedere ["SelectObjectContent"](#). Per ulteriori informazioni su S3 Select, vedere ["Documentazione AWS per S3 Select"](#).

Solo gli account tenant con S3 Select abilitato possono eseguire query SelectObjectContent. Consultare la ["Considerazioni e requisiti per l'utilizzo di S3 Select"](#).

Clausole

- SELEZIONARE l'elenco
- CLAUSOLA FROM
- Clausola WHERE
- Clausola di LIMITAZIONE

Tipi di dati

- bool
- intero
- stringa
- fluttuare
- decimale, numerico
- data e ora

Operatori

Operatori logici

- E.
- NO
- OPPURE

Operatori di confronto

- <
- >
- <=
- >=
- =
- =
- <>
- !=
- TRA
- POLL

Operatori di corrispondenza dei modelli

- MI PIACE
- _
- %

Operatori unitari

- È NULL
- NON È NULL

Operatori matematici

- +
- -
- *
- /
- %

StorageGRID segue la precedenza dell'operatore Amazon S3 Select.

Funzioni di aggregazione

- MEDIA()
- CONTEGGIO(*)
- MAX()
- MIN()
- SOMMA()

Funzioni condizionali

- CASO
- COALESCE
- NULLIF

Funzioni di conversione

- CAST (per il tipo di dati supportato)

Funzioni di data

- DATA_ADD
- DATA_DIFF
- ESTRARRE
- TO_STRING
- TO_TIMESTAMP

- UTCNOW

Funzioni di stringa

- CHAR_LENGTH, CHARACTER_LENGTH
- ABBASSARE
- SOTTOSTRINGA
- TAGLIARE
- SUPERIORE

Come StorageGRID utilizza la crittografia lato server

La crittografia lato server consente di proteggere i dati a oggetti inattivi. StorageGRID crittografa i dati durante la scrittura dell'oggetto e li decrta quando si accede all'oggetto.

Se si desidera utilizzare la crittografia lato server, è possibile scegliere una delle due opzioni che si escludono a vicenda, in base alla modalità di gestione delle chiavi di crittografia:

- **SSE (crittografia lato server con chiavi gestite da StorageGRID):** Quando si invia una richiesta S3 per memorizzare un oggetto, StorageGRID crittografa l'oggetto con una chiave univoca. Quando si invia una richiesta S3 per recuperare l'oggetto, StorageGRID utilizza la chiave memorizzata per decrittare l'oggetto.
- **SSE-C (crittografia lato server con chiavi fornite dal cliente):** Quando si invia una richiesta S3 per memorizzare un oggetto, viene fornita la propria chiave di crittografia. Quando si recupera un oggetto, si fornisce la stessa chiave di crittografia come parte della richiesta. Se le due chiavi di crittografia corrispondono, l'oggetto viene decrittografato e vengono restituiti i dati dell'oggetto.

Mentre StorageGRID gestisce tutte le operazioni di crittografia e decifratura degli oggetti, è necessario gestire le chiavi di crittografia fornite.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente.



Se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Utilizzare SSE

Per crittografare un oggetto con una chiave univoca gestita da StorageGRID, utilizzare la seguente intestazione di richiesta:

```
x-amz-server-side-encryption
```

L'intestazione della richiesta SSE è supportata dalle seguenti operazioni a oggetti:

- "PutObject"
- "Oggetto CopyObject"
- "CreateMultipartUpload"

Utilizzare SSE-C.

Per crittografare un oggetto con una chiave univoca gestita, vengono utilizzate tre intestazioni di richiesta:

Intestazione della richiesta	Descrizione
x-amz-server-side-encryption-customer-algorithm	Specificare l'algoritmo di crittografia. Il valore dell'intestazione deve essere AES256.
x-amz-server-side-encryption-customer-key	Specificare la chiave di crittografia che verrà utilizzata per crittografare o decrittare l'oggetto. Il valore della chiave deve essere 256 bit, con codifica base64.
x-amz-server-side-encryption-customer-key-MD5	Specificare il digest MD5 della chiave di crittografia in base a RFC 1321, utilizzato per garantire che la chiave di crittografia sia stata trasmessa senza errori. Il valore del digest MD5 deve essere a 128 bit con codifica base64.

Le intestazioni delle richieste SSE-C sono supportate dalle seguenti operazioni a oggetti:

- "GetObject"
- "HeadObject (oggetto intestazione)"
- "PutObject"
- "Oggetto CopyObject"
- "CreateMultipartUpload"
- "UploadPart"
- "UploadPartCopy"

Considerazioni sull'utilizzo della crittografia lato server con le chiavi fornite dal cliente (SSE-C)

Prima di utilizzare SSE-C, tenere presente quanto segue:

- È necessario utilizzare https.



StorageGRID rifiuta qualsiasi richiesta effettuata tramite http quando si utilizza SSE-C. per motivi di sicurezza, è necessario considerare qualsiasi chiave inviata accidentalmente utilizzando http come compromessa. Eliminare la chiave e ruotarla in base alle necessità.

- L'ETag nella risposta non è l'MD5 dei dati dell'oggetto.
- È necessario gestire il mapping delle chiavi di crittografia agli oggetti. StorageGRID non memorizza le chiavi di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia che fornisce per ciascun oggetto.
- Se il bucket è abilitato per la versione, ogni versione dell'oggetto deve disporre di una propria chiave di crittografia. L'utente è responsabile del rilevamento della chiave di crittografia utilizzata per ciascuna versione dell'oggetto.
- Poiché si gestiscono le chiavi di crittografia sul lato client, è necessario gestire anche eventuali protezioni aggiuntive, come la rotazione delle chiavi, sul lato client.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente.

- Se la replica cross-grid o CloudMirror è configurata per il bucket, non è possibile acquisire oggetti SSE-C. L'operazione di acquisizione non riesce.

Informazioni correlate

["Manuale dell'utente di Amazon S3: Utilizzo della crittografia lato server con chiavi fornite dal cliente \(SSE-C\)"](#)

Crea una copia di un oggetto in StorageGRID con la richiesta S3 CopyObject

È possibile utilizzare la richiesta CopyObject S3 per creare una copia di un oggetto già memorizzato in S3. Un'operazione CopyObject è la stessa dell'esecuzione di GetObject seguito da PutObject.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare ["caricamento multiparte"](#) invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11,7 o 11,8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

UTF-8 caratteri nei metadati dell'utente

Se una richiesta include valori UTF-8 (non escapati) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento di StorageGRID non è definito.

StorageGRID non analizza né interpreta i caratteri UTF-8 preceduti da escape inclusi nel nome o nel valore della chiave dei metadati definiti dall'utente. I caratteri UTF-8 preceduti da escape vengono trattati come caratteri ASCII:

- Le richieste hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 escapati.
- StorageGRID non restituisce l'`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-checksum-algorithm`: Specifica CRC32, CRC32C, CRC64NVME, o SHA256

Quando copi un oggetto, se l'oggetto sorgente ha un checksum o include `x-amz-checksum-algorithm`, l'oggetto copiato ha un checksum `FULL_OBJECT`.

Se l'oggetto sorgente ha un checksum ma la richiesta non include `x-amz-checksum-algorithm` o utilizza un valore di checksum non supportato, l'oggetto copiato avrà lo stesso tipo di checksum dell'oggetto sorgente. StorageGRID ignora valori `x-amz-checksum-algorithm` non validi o non supportati.

Se l'oggetto sorgente non ha un checksum e non include `x-amz-checksum-algorithm` oppure utilizza un valore di checksum non supportato, l'oggetto copiato non avrà un checksum.



Se una richiesta CopyObject non specifica un checksum e l'oggetto sorgente non ha un checksum, StorageGRID non calcola un checksum CRC-64/NVME predefinito per l'oggetto.

- `x-amz-copy-source`
- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente
- `x-amz-metadata-directive`: Il valore predefinito è `COPY`, che consente di copiare l'oggetto e i metadati associati.

È possibile specificare `REPLACE` se sovrascrivere i metadati esistenti durante la copia dell'oggetto o se aggiornare i metadati dell'oggetto.

- `x-amz-storage-class`
- `x-amz-tagging-directive`: Il valore predefinito è `COPY`, che consente di copiare l'oggetto e tutti i tag.

È possibile specificare `REPLACE` di sovrascrivere i tag esistenti durante la copia dell'oggetto o di aggiornare i tag.

- Intestazioni della richiesta di blocco oggetti S3:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

- Intestazioni di richiesta SSE:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`
- `x-amz-copy-source-server-side-encryption-customer-key`

- x-amz-copy-source-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption
- x-amz-server-side-encryption-customer-key-MD5
- x-amz-server-side-encryption-customer-key
- x-amz-server-side-encryption-customer-algorithm

Vedere [Intestazioni di richiesta per la crittografia lato server](#)

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- Cache-Control
- Content-Disposition
- Content-Encoding
- Content-Language
- Expires
- If-Match

L'`If-Match`intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l'`If-Match`intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented.

- If-None-Match

L'`If-None-Match`intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l'`If-None-Match`intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented.

- x-amz-website-redirect-location

Opzioni di classe storage

L'`x-amz-storage-class`intestazione della richiesta è supportata e influisce sul numero di copie degli oggetti create da StorageGRID se la regola ILM corrispondente utilizza il doppio commit o bilanciato "[opzione di acquisizione](#)".

- STANDARD

(Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- REDUCED_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit

doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l'`REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Utilizzo di `x-amz-copy-source` in CopyObject

Se il bucket e la chiave di origine, specificati nell'`x-amz-copy-source` intestazione, sono diversi dal bucket e dalla chiave di destinazione, una copia dei dati dell'oggetto di origine viene scritta nella destinazione.

Se l'origine e la destinazione corrispondono e l'`x-amz-metadata-directive` header è specificato come `REPLACE`, i metadati dell'oggetto vengono aggiornati con i valori dei metadati forniti nella richiesta. In questo caso, StorageGRID non re-ingestisce l'oggetto. Questo 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 si fornisce l'`x-amz-server-side-encryption` intestazione o l'`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. Eventuali modifiche al posizionamento degli oggetti attivate dall'aggiornamento vengono applicate quando ILM viene rivalutato dai normali processi ILM in background.

Ciò significa che se la regola ILM utilizza l'opzione Strict per il comportamento di acquisizione, non viene eseguita alcuna azione se non è possibile eseguire il posizionamento degli oggetti richiesto (ad esempio, perché non è disponibile una nuova posizione richiesta). L'oggetto aggiornato mantiene la posizione corrente fino a quando non è possibile il posizionamento richiesto.

Intestazioni di richiesta per la crittografia lato server

Se si utilizza ["usa 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 di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta CopyObject, in modo che l'oggetto possa essere decrittografato e quindi copiato:
 - `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
 - `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto sorgente.
- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca che si fornisce e si gestisce, includere le seguenti tre intestazioni:
 - `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
 - `x-amz-server-side-encryption-customer-key`: Specificare una nuova chiave di crittografia per l'oggetto di destinazione.

- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della nuova chiave di crittografia.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a ["utilizzo della crittografia lato server"](#).

- Se si desidera crittografare l'oggetto di destinazione (la copia) con una chiave univoca gestita da StorageGRID (SSE), includere questa intestazione nella richiesta CopyObject:

- `x-amz-server-side-encryption`



`server-side-encryption` Impossibile aggiornare il valore dell'oggetto. Eseguire invece una copia con un nuovo `server-side-encryption` valore utilizzando `x-amz-metadata-directive: REPLACE`.

Versione

Se il bucket di origine è in versione, è possibile utilizzare l'`x-amz-copy-source` intestazione per copiare la versione più recente di un oggetto. Per copiare una versione specifica di un oggetto, è necessario specificare esplicitamente la versione da copiare utilizzando la `versionId` sottorisorsa. Se il bucket di destinazione è in versione, la versione generata viene restituita nell'`x-amz-version-id` intestazione della risposta. Se la versione è sospesa per il bucket target, `x-amz-version-id` restituisce un valore "null".

Recupera un oggetto da un bucket in StorageGRID con la richiesta GetObject

È possibile utilizzare la richiesta GetObject S3 per recuperare un oggetto da un bucket S3.

Oggetti GetObject e multiparte

È possibile utilizzare il `partNumber` parametro di richiesta per recuperare una parte specifica di un oggetto multiparte o segmentato. L'`x-amz-mp-parts-count` elemento di risposta indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` su 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, l'`x-amz-mp-parts-count` elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. LE richieste di RECUPERO per un oggetto con caratteri UTF-8 di escape nei metadati definiti dall'utente non restituiscono l'`x-amz-missing-meta` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Accept-Encoding`

Quando un oggetto non ha un `Content-Encoding`, una richiesta GET con `Accept-Encoding: gzip` applica la compressione al volo alla risposta. Solo `gzip` influisce sulla codifica della risposta GET; `deflate`, `br` e `identity` non lo fanno. Per gli oggetti che hanno già una `Content-Encoding` memorizzata, StorageGRID restituisce la codifica memorizzata e non applica ulteriore compressione al volo in base a `Accept-Encoding`. StorageGRID non supporta operazioni di lettura di intervallo per richieste GET con `Accept-Encoding: gzip`.

- `x-amz-checksum-mode`: Specificare `ENABLED`

L'Range`intestazione non è supportata con `x-amz-checksum-mode` per `GetObject`. Quando si include Range nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Versione

Se non viene specificata una `versionId` sottorisorsa, 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 l' `x-amz-delete-marker` intestazione della risposta impostata su `true`.

Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre le intestazioni se l'oggetto è crittografato con una chiave univoca fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare `AES256`.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia dell'oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Comportamento degli oggetti `GetObject` per Cloud Storage Pool

Se un oggetto è stato memorizzato in ["Pool di cloud storage"](#), il comportamento di una richiesta `GetObject` dipende dallo stato dell'oggetto. Per ulteriori informazioni, vedere ["HeadObject \(oggetto intestazione\)"](#).



Se un oggetto viene memorizzato in un Cloud Storage Pool e sulla griglia esistono anche una o più copie dell'oggetto, le richieste `GetObject` tenteranno di recuperare i dati dalla griglia, prima di recuperarli da Cloud Storage Pool.

Stato dell'oggetto	Comportamento di GetObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK Viene recuperata una copia dell'oggetto.
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Viene recuperata una copia dell'oggetto.
Oggetto sottoposto a transizione in uno stato non recuperabile	403 Forbidden, InvalidObjectState Utilizzare una "RestoreObject" richiesta per ripristinare l'oggetto in uno stato recuperabile.
Oggetto in fase di ripristino da uno stato non recuperabile	403 Forbidden, InvalidObjectState Attendere il completamento della richiesta RestoreObject.
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Viene recuperata una copia dell'oggetto.

Oggetti multiparte o segmentati in un pool di storage cloud

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta GetObject potrebbe restituire erroneamente 200 OK quando alcune parti dell'oggetto sono già state trasferite a uno stato non recuperabile o quando alcune parti dell'oggetto non sono state ancora ripristinate.

In questi casi:

- La richiesta GetObject potrebbe restituire alcuni dati ma interrompersi a metà del trasferimento.
- Una richiesta GetObject successiva potrebbe restituire 403 Forbidden.

Replica GetObject e cross-grid

Se si utilizza ["federazione di grid"](#) ed ["replica cross-grid"](#) è attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• COMPLETATO: La replica è riuscita. • PENDING: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Griglia	Stato della replica
Destinazione	REPLICA: L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta la `x-amz-replication-status` testata.

Recupera metadati da un oggetto in StorageGRID con la richiesta S3 HeadObject

È possibile utilizzare la richiesta HeadObject S3 per recuperare i metadati da un oggetto senza restituire l'oggetto stesso. Se l'oggetto viene memorizzato in un Cloud Storage Pool, è possibile utilizzare HeadObject per determinare lo stato di transizione dell'oggetto.

Oggetti HeadObject e multiparte

È possibile utilizzare il `partNumber` parametro di richiesta per recuperare i metadati per una parte specifica di un oggetto multiparte o segmentato. L' `'x-amz-mp-parts-count'` elemento di risposta indica il numero di parti dell'oggetto.

È possibile impostare `partNumber` su 1 sia per gli oggetti segmentati/multiparte che per gli oggetti non segmentati/non multiparte; tuttavia, l' `'x-amz-mp-parts-count'` elemento di risposta viene restituito solo per gli oggetti segmentati o multiparte.

UTF-8 caratteri nei metadati dell'utente

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati nei metadati definiti dall'utente. Le richieste HEAD per un oggetto con caratteri UTF-8 di escape nei metadati definiti dall'utente non restituiscono l' `'x-amz-missing-meta'` intestazione se il nome o il valore della chiave include caratteri non stampabili.

Intestazione richiesta supportata

È supportata la seguente intestazione della richiesta:

- `x-amz-checksum-mode`

Il `partNumber` parametro e Range l'intestazione non sono supportati con `x-amz-checksum-mode` per HeadObject. Quando vengono inclusi nella richiesta con `x-amz-checksum-mode` abilitato, StorageGRID non restituisce un valore checksum nella risposta.

Intestazione della richiesta non supportata

La seguente intestazione di richiesta non è supportata e restituisce `XNotImplemented`:

- `x-amz-website-redirect-location`

Versione

Se non viene specificata una `versionId` sottorisorsa, 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 l' `x-amz-delete-marker` intestazione della risposta impostata su `'true'`.

Intestazioni delle richieste per la crittografia lato server con chiavi di crittografia fornite dal cliente (SSE-C)

Utilizzare tutte e tre queste intestazioni se l'oggetto è crittografato con una chiave univoca fornita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per l'oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia dell'oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Risposte HeadObject per gli oggetti Cloud Storage Pool

Se l'oggetto è memorizzato in ["Pool di cloud storage"](#), vengono restituite le seguenti intestazioni di risposta:

- `x-amz-storage-class`: GLACIER
- `x-amz-restore`

Le intestazioni delle risposte forniscono informazioni sullo stato di un oggetto quando viene spostato in un Cloud Storage Pool, facoltativamente trasferito in uno stato non recuperabile e ripristinato.

Stato dell'oggetto	Risposta a HeadObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto memorizzato in un pool di storage tradizionale o mediante erasure coding	200 OK (Non viene restituita alcuna intestazione di risposta speciale).
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK <code>x-amz-storage-class</code> : GLACIER <code>x-amz-restore</code> : <code>ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT"</code> Fino a quando l'oggetto non viene spostato in uno stato non recuperabile, il valore per viene impostato su un <code>expiry-date</code> tempo lontano in futuro. L'ora esatta della transizione non è controllata dal sistema StorageGRID.

Stato dell'oggetto	Risposta a HeadObject
L'oggetto è passato allo stato non recuperabile, ma almeno una copia esiste anche nella griglia	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="false", expiry-date="Sat, 23 July 20 2030 00:00:00 GMT" Il valore per expiry-date è impostato su un certo tempo lontano in futuro. Nota: Se la copia nella griglia non è disponibile (ad esempio, un nodo di archiviazione è inattivo), è necessario eseguire una "RestoreObject" richiesta di ripristino della copia dal pool di archiviazione cloud prima di poter recuperare correttamente l'oggetto.
L'oggetto è passato a uno stato non recuperabile e non esiste alcuna copia nella griglia	200 OK x-amz-storage-class: GLACIER
Oggetto in fase di ripristino da uno stato non recuperabile	200 OK x-amz-storage-class: GLACIER x-amz-restore: ongoing-request="true"
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" `expiry-date`Indica quando l'oggetto nel Cloud Storage Pool verrà riportato a uno stato non recuperabile.

Oggetti multiparte o segmentati nel Cloud Storage Pool

Se hai caricato un oggetto multiparte o se StorageGRID divide un oggetto di grandi dimensioni in segmenti, StorageGRID determina se l'oggetto è disponibile nel pool di storage cloud campionando un sottoinsieme delle parti o dei segmenti dell'oggetto. In alcuni casi, una richiesta HeadObject potrebbe restituire erroneamente `x-amz-restore: 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 state ancora ripristinate.

HeadObject e replica cross-grid

Se si utilizza ["federazione di grid"](#) ed ["replica cross-grid"](#) è attivato per un bucket, il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta HeadObject. La risposta include l'intestazione della risposta specifica di StorageGRID `x-ntap-sg-cgr-replication-status`, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• COMPLETATO: La replica è riuscita. • PENDING: L'oggetto non è stato ancora replicato. • ERRORE: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	REPLICA : L'oggetto è stato replicato dalla griglia di origine.



StorageGRID non supporta la `x-amz-replication-status` testata.

Aggiungi un oggetto a un bucket in StorageGRID con la richiesta S3 PutObject

È possibile utilizzare la richiesta S3 PutObject per aggiungere un oggetto a un bucket.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Dimensione dell'oggetto

La dimensione massima *raccomandata* per una singola operazione PutObject è di 5 GiB (5.368.709.120 byte). Se sono presenti oggetti di dimensioni superiori a 5 GiB, utilizzare ["caricamento multiparte"](#) invece.

La dimensione massima *supportata* per una singola operazione PutObject è 5 TiB (5.497.558.138.880 byte).



Se è stato eseguito l'aggiornamento da StorageGRID 11,6 o versioni precedenti, l'avviso S3 PUT object size too large verrà attivato se si tenta di caricare un oggetto che supera i 5 GiB. Se si dispone di una nuova installazione di StorageGRID 11,7 o 11,8, l'avviso non verrà attivato in questo caso. Tuttavia, per allinearsi allo standard AWS S3, le versioni future di StorageGRID non supporteranno il caricamento di oggetti di dimensioni superiori a 5 GiB.

Dimensione dei metadati dell'utente

Amazon S3 limita la dimensione dei metadati definiti dall'utente all'interno di ogni intestazione di richiesta PUT a 2 KB. StorageGRID limita i metadati dell'utente a 24 KiB. La dimensione dei metadati definiti dall'utente viene misurata prendendo la somma del numero di byte nella codifica UTF-8 di ogni chiave e valore.

UTF-8 caratteri nei metadati dell'utente

Se una richiesta include valori UTF-8 (non escapati) nel nome della chiave o nel valore dei metadati definiti dall'utente, il comportamento di StorageGRID non è definito.

StorageGRID non analizza o interpreta i caratteri UTF-8 escapati inclusi nel nome della chiave o nel valore dei metadati definiti dall'utente. I caratteri UTF-8 escapati vengono trattati come caratteri ASCII:

- Le richieste PutObject, CopyObject, GetObject e HeadObject hanno esito positivo se i metadati definiti dall'utente includono caratteri UTF-8 di escape.
- StorageGRID non restituisce l'`x-amz-missing-meta` intestazione se il valore interpretato del nome o del valore della chiave include caratteri non stampabili.

Limiti tag oggetto

È possibile aggiungere tag a nuovi oggetti durante il caricamento oppure aggiungerli a oggetti esistenti. StorageGRID e Amazon S3 supportano fino a 10 tag per ciascun oggetto. I tag associati a un oggetto devono avere chiavi tag univoche. Una chiave di tag può contenere fino a 128 caratteri Unicode e i valori di tag possono contenere fino a 256 caratteri Unicode. Chiave e valori distinguono tra maiuscole e minuscole.

Proprietà degli oggetti

In StorageGRID, tutti gli oggetti sono di proprietà dell'account del proprietario del bucket, inclusi gli oggetti creati da un account non proprietario o da un utente anonimo.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Cache-Control
- Content-Disposition
- Content-Encoding

Quando specifichi `aws-chunked` per Content-Encoding, StorageGRID non verifica i seguenti elementi:

- StorageGRID non verifica il `chunk-signature` rispetto ai dati dei chunk.
- StorageGRID non verifica il valore che fornisci per `x-amz-decoded-content-length` rispetto all'oggetto.
- Content-Language
- Content-Length
- Content-MD5
- Content-Type
- Expires
- Transfer-Encoding

La codifica di trasferimento a blocchi è supportata se `aws-chunked` si utilizza anche la firma del payload.

- Intestazioni della richiesta di checksum:

- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- x-amz-checksum-sha256



Se una richiesta PutObject non specifica un checksum, StorageGRID non calcola un checksum CRC-64/NVME predefinito per un oggetto.

- x-amz-meta-, seguito da una coppia nome-valore contenente metadati definiti dall'utente.

Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

```
x-amz-meta-name: value
```

Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano al momento della creazione dell'oggetto. Ad esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi dal 1 gennaio 1970.



Una regola ILM non può utilizzare sia un **tempo di creazione definito dall'utente** per il tempo di riferimento che l'opzione di acquisizione bilanciata o rigorosa. Quando viene creata la regola ILM viene restituito un errore.

- x-amz-tagging
- Intestazioni di richiesta blocco oggetti S3
 - x-amz-object-lock-mode
 - x-amz-object-lock-retain-until-date
 - x-amz-object-lock-legal-hold

Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la modalità di versione dell'oggetto e mantenere la data fino alla data. Vedere ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#).

- Intestazioni di richiesta SSE:
 - x-amz-server-side-encryption
 - x-amz-server-side-encryption-customer-key-MD5
 - x-amz-server-side-encryption-customer-key
 - x-amz-server-side-encryption-customer-algorithm

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- `If-Match`

L' `If-Match` intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l' `If-Match` intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented.

- `If-None-Match`

L' `If-None-Match` intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l' `If-None-Match` intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented.

- `x-amz-acl`
- `x-amz-checksum-md5`
- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`
- `x-amz-sdk-checksum-algorithm`
- `x-amz-trailer`
- `x-amz-website-redirect-location`

La `x-amz-website-redirect-location` testata ritorna `XNotImplemented`.

Opzioni di classe storage

L' `x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza l'opzione di acquisizione rigorosa, l' `x-amz-storage-class` intestazione non ha effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- `STANDARD` (Impostazione predefinita)

- **Doppio commit:** Se la regola ILM specifica l'opzione doppio commit per il comportamento di Ingest, non appena un oggetto viene acquisito, viene creata una seconda copia di tale oggetto e distribuita in un nodo di storage diverso (doppio commit). Quando viene valutato ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.
- **Balanced:** Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

Se StorageGRID è in grado di creare immediatamente tutte le copie dell'oggetto specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` intestazione non ha effetto.

- **REDUCED_REDUNDANCY**

- **Commit doppio:** Se la regola ILM specifica l'opzione commit doppio per il comportamento di Ingest, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (commit singolo).
- **Balanced:** Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L'`REDUCED\_REDUNDANCY` opzione viene utilizzata in modo ottimale quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso l'utilizzo di `REDUCED\_REDUNDANCY` elimina la creazione e la cancellazione non necessarie di una copia degli oggetti extra per ogni operazione di acquisizione.

L'uso dell'`REDUCED\_REDUNDANCY` opzione non è consigliato in altre circostanze. `REDUCED\_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.



Avere una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

La specifica `REDUCED_REDUNDANCY` influisce solo sul numero di copie create al momento della prima acquisizione di un oggetto. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l'`REDUCED\_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED\_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE:** Utilizzare la seguente intestazione se si desidera crittografare l'oggetto con una chiave univoca

gestita da StorageGRID.

- `x-amz-server-side-encryption`

Quando l'`x-amz-server-side-encryption`intestazione non è inclusa nella richiesta PutObject, l'intera griglia "[impostazione di crittografia degli oggetti archiviati](#)"viene omessa dalla risposta PutObject.

- **SSE-C:** Utilizzare tutte e tre queste intestazioni se si desidera crittografare l'oggetto con una chiave univoca che si fornisce e si gestisce.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.

- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.

- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a "[utilizzo della crittografia lato server](#)".



Se un oggetto viene crittografato con SSE o SSE-C, tutte le impostazioni di crittografia a livello di bucket o di griglia vengono ignorate.

Versione

Se la versione è abilitata per un bucket, viene generato automaticamente un univoco `versionId` per la versione dell'oggetto che viene memorizzato. Questo `versionId` viene anche restituito nella risposta utilizzando l'`x-amz-version-id`intestazione della risposta.

Se la versione è sospesa, la versione oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, verrà sovrascritta.

Calcoli della firma per l'intestazione autorizzazione

Quando si utilizza l'`Authorization`intestazione per autenticare le richieste, StorageGRID differisce da AWS nei seguenti modi:

- StorageGRID non richiede che `host` le intestazioni siano incluse in `CanonicalHeaders`.
- StorageGRID non richiede di `Content-Type` essere incluso in `CanonicalHeaders`.
- StorageGRID non richiede che `x-amz-*` le intestazioni siano incluse in `CanonicalHeaders`.



Come procedura consigliata generale, includere sempre queste intestazioni all'interno `CanonicalHeaders` per assicurarsi che siano verificate; tuttavia, se si escludono queste intestazioni, StorageGRID non restituisce un errore.

Per ulteriori informazioni, fare riferimento alla "[Calcoli della firma per l'intestazione dell'autorizzazione: Trasferimento del payload in un singolo chunk \(firma AWS versione 4\)](#)".

Informazioni correlate

- "[Gestire gli oggetti con ILM](#)"

- ["Riferimento API Amazon Simple Storage Service: PutObject"](#)

Ripristina un oggetto in StorageGRID con la richiesta S3 RestoreObject

È possibile utilizzare la richiesta S3 RestoreObject per ripristinare un oggetto memorizzato in un Cloud Storage Pool.

Tipo di richiesta supportato

StorageGRID supporta solo le richieste RestoreObject per ripristinare un oggetto. Non supporta il SELECT tipo di restauro. Selezionare Richieste restituite XNotImplemented.

Versione

Facoltativamente, specificare `versionId` per ripristinare una versione specifica di un oggetto in un bucket in versione. Se non si specifica `versionId`, viene ripristinata la versione più recente dell'oggetto

Comportamento di RestoreObject negli oggetti Cloud Storage Pool

Se un oggetto è stato memorizzato in una ["Pool di cloud storage"](#), una richiesta RestoreObject presenta il seguente comportamento, in base allo stato dell'oggetto. Per ulteriori informazioni, vedere ["HeadObject \(oggetto intestazione\)"](#).



Se un oggetto viene memorizzato in un Cloud Storage Pool ed esistono anche una o più copie dell'oggetto nella griglia, non è necessario ripristinarlo inviando una richiesta RestoreObject. La copia locale può essere recuperata direttamente, utilizzando una richiesta GetObject.

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto acquisito in StorageGRID ma non ancora valutato da ILM, o oggetto non presente in un pool di storage cloud	403 Forbidden, InvalidObjectState
Oggetto nel Cloud Storage Pool ma non ancora passato a uno stato non recuperabile	200 OK Non vengono apportate modifiche. Nota: Prima che un oggetto sia stato spostato in uno stato non recuperabile, non è possibile modificare il suo <code>expiry-date</code> .

Stato dell'oggetto	Comportamento di RestoreObject
Oggetto sottoposto a transizione in uno stato non recuperabile	202 Accepted Ripristina una copia recuperabile dell'oggetto in Cloud Storage Pool per il numero di giorni specificato nel corpo della richiesta. Al termine di questo periodo, l'oggetto viene riportato in uno stato non recuperabile. Facoltativamente, utilizzare l' <code>Tier</code> elemento di richiesta per determinare il tempo necessario per completare il processo di ripristino (<code>Expedited</code>, <code>Standard</code> o <code>Bulk</code>). Se non si specifica <code>Tier</code>, viene utilizzato il <code>Standard</code> livello. Importante: se un oggetto è stato migrato su S3 Glacier Deep Archive o se il Cloud Storage Pool utilizza Azure Blob Storage, non puoi ripristinarlo usando il <code>Expedited</code> livello. Viene restituito il seguente errore 403 Forbidden, InvalidTier: Retrieval option is not supported by this storage class.
Oggetto in fase di ripristino da uno stato non recuperabile	409 Conflict, RestoreAlreadyInProgress
Oggetto completamente ripristinato nel Cloud Storage Pool	200 OK Nota: se un oggetto è stato ripristinato ad uno stato recuperabile, è possibile modificarlo <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 relazione all'ora della richiesta.

Filtra i dati degli oggetti in StorageGRID con la richiesta S3 SelectObjectContent

È possibile utilizzare la richiesta S3 SelectObjectContent per filtrare il contenuto di un oggetto S3 in base a una semplice istruzione SQL.

Per ulteriori informazioni, vedere ["Riferimento API Amazon Simple Storage Service: SelectObjectContent"](#).

Prima di iniziare

- L'account tenant dispone dell'autorizzazione S3 Select.
- Si dispone dell' `s3:GetObject` autorizzazione per l'oggetto che si desidera sottoporre a query.
- L'oggetto che si desidera sottoporre a query deve essere in uno dei seguenti formati:
 - **CSV.** Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
 - **Parquet.** Requisiti aggiuntivi per gli oggetti in parquet:
 - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
 - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
 - La dimensione massima del gruppo di righe non compresso è di 512 MB.
 - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
 - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.

- L'espressione SQL ha una lunghezza massima di 256 KB.
- Qualsiasi record nell'input o nei risultati ha una lunghezza massima di 1 MiB.

Esempio di sintassi per le richieste CSV

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <CSV>
      <AllowQuotedRecordDelimiter>boolean</AllowQuotedRecordDelimiter>
      <Comments>#</Comments>
      <FieldDelimiter>\t</FieldDelimiter>
      <FileHeaderInfo>USE</FileHeaderInfo>
      <QuoteCharacter>'</QuoteCharacter>
      <QuoteEscapeCharacter>\\</QuoteEscapeCharacter>
      <RecordDelimiter>\n</RecordDelimiter>
    </CSV>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Esempio di sintassi della richiesta di parquet

```
POST /{Key+}?select&select-type=2 HTTP/1.1
Host: Bucket.s3.abc-company.com
x-amz-expected-bucket-owner: ExpectedBucketOwner
<?xml version="1.0" encoding="UTF-8"?>
<SelectObjectContentRequest xmlns=http://s3.amazonaws.com/doc/2006-03-01/>
  <Expression>string</Expression>
  <ExpressionType>string</ExpressionType>
  <RequestProgress>
    <Enabled>boolean</Enabled>
  </RequestProgress>
  <InputSerialization>
    <CompressionType>GZIP</CompressionType>
    <PARQUET>
    </PARQUET>
  </InputSerialization>
  <OutputSerialization>
    <CSV>
      <FieldDelimiter>string</FieldDelimiter>
      <QuoteCharacter>string</QuoteCharacter>
      <QuoteEscapeCharacter>string</QuoteEscapeCharacter>
      <QuoteFields>string</QuoteFields>
      <RecordDelimiter>string</RecordDelimiter>
    </CSV>
  </OutputSerialization>
  <ScanRange>
    <End>long</End>
    <Start>long</Start>
  </ScanRange>
</SelectObjectContentRequest>
```

Esempio di query SQL

Questa query ottiene il nome dello stato, 2010 popolazioni, 2015 popolazioni stimate e la percentuale di cambiamento rispetto ai dati del censimento degli Stati Uniti. I record nel file che non sono stati vengono ignorati.

```
SELECT STNAME, CENSUS2010POP, POPESTIMATE2015, CAST((POPESTIMATE2015 -
CENSUS2010POP) AS DECIMAL) / CENSUS2010POP * 100.0 FROM S3Object WHERE
NAME = STNAME
```

Le prime righe del file da interrogare, SUB-EST2020_ALL.csv, sono simili a quanto segue:

```
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`, sono simili a queste:

```
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, sono le seguenti:

```
Alabama,4779736,4854803,1.5705260708959658022953568983726297854
Alaska,710231,738430,3.9703983633493891424057806544631253775
Arizona,6392017,6832810,6.8959922978928247531256565807005832431
Arkansas,2915918,2979732,2.1884703204959810255295244928012378949
California,37253956,38904296,4.4299724839960620557988526104449148971
Colorado,5029196,5454328,8.4532796097030221132761578590295546246
```

Operazioni per caricamenti multiparte

Operazioni di caricamento multiparte supportate in StorageGRID

Questa sezione descrive come StorageGRID supporta le operazioni per gli upload di più parti.

Le seguenti condizioni e note si applicano a tutte le operazioni di caricamento multiparte:

- Non si devono superare i 1.000 caricamenti simultanei di più parti in un singolo bucket, poiché i risultati delle query ListMultipartUploads per quel bucket potrebbero restituire risultati incompleti.
- StorageGRID applica i limiti di dimensione AWS per le parti multipart. I client S3 devono seguire queste linee guida:
 - Ciascuna parte di un caricamento multiparte deve essere compresa tra 5 MiB (5,242,880 byte) e 5 GiB (5,368,709,120 byte).
 - L'ultima parte può essere inferiore a 5 MiB (5,242,880 byte).
 - In generale, le dimensioni delle parti devono essere il più grandi possibile. Ad esempio, utilizzare le dimensioni delle parti di 5 GiB per un oggetto 100 GiB. Poiché ogni parte è considerata un oggetto unico, l'utilizzo di parti di grandi dimensioni riduce l'overhead dei metadati StorageGRID.
 - Per gli oggetti di dimensioni inferiori a 5 GiB, prendere in considerazione l'utilizzo di un caricamento non multiparte.
- ILM viene valutato per ogni parte di un oggetto multiparte nel momento in cui viene acquisito e per l'oggetto nel suo insieme al completamento del caricamento multiparte, se la regola ILM utilizza il bilanciato o rigoroso ["opzione di acquisizione"](#). Devi essere consapevole di come questo influisca sul posizionamento di oggetti e parti:
 - Se ILM cambia mentre è in corso un caricamento multiparte S3, alcune parti dell'oggetto potrebbero

non soddisfare i requisiti ILM correnti al termine del caricamento multiparte. Qualsiasi parte non posizionata correttamente viene messa in coda per la rivalutazione ILM e spostata nella posizione corretta in un secondo momento.

- Quando si valuta ILM per una parte, StorageGRID filtra sulla dimensione della parte, non sulla dimensione dell'oggetto. Ciò significa che parti di un oggetto possono essere memorizzate in posizioni che non soddisfano i requisiti ILM per l'oggetto nel suo complesso. Ad esempio, se una regola specifica che tutti gli oggetti da 10 GB o più grandi sono memorizzati a DC1 GB mentre tutti gli oggetti più piccoli sono memorizzati a DC2 GB, ogni parte da 1 GB di un caricamento multiparte in 10 parti viene memorizzata a DC2 GB al momento dell'acquisizione. Tuttavia, quando ILM viene valutato per l'oggetto nel suo complesso, tutte le parti dell'oggetto vengono spostate in DC1.
- Tutte le operazioni di caricamento multiparte supportano StorageGRID ["valori di coerenza"](#) .
- Quando un oggetto viene acquisito utilizzando il caricamento multiparte, ["Soglia di segmentazione degli oggetti \(1 GiB\)"](#) non viene applicato.
- Se necessario, è possibile utilizzare ["crittografia lato server"](#) con caricamenti multiparte. Per utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID), è necessario includere l'`x-amz-server-side-encryption` intestazione della richiesta solo nella richiesta CreateMultipartUpload. Per utilizzare SSE-C (crittografia lato server con chiavi fornite dal cliente), specificare le stesse tre intestazioni di richiesta della chiave di crittografia nella richiesta CreateMultipartUpload e in ogni richiesta UploadPart successiva.
- Se un oggetto caricato in più parti è incluso in un ["secchio di rami"](#) dipende dall'ora in cui è stata avviata l'ingestione e dal filtro temporale per il bucket del ramo:
 - **Prima.** Se l'ingestione è stata avviata prima del timestamp *Before* del bucket del ramo, l'oggetto caricato in più parti viene incluso, indipendentemente da quando il caricamento viene completato.
 - **Dopo.** Se l'ingestione è stata avviata dopo il timestamp *After* del bucket del ramo, l'oggetto caricato in più parti viene incluso.
 - **Tra.** Se l'ingestione è stata avviata tra i timestamp *From* e *To* del bucket del ramo, l'oggetto caricato in più parti viene incluso, indipendentemente da quando il caricamento viene completato.
 - **Escludi.** Se l'ingestione è stata avviata prima dell'ora *Escludi da* del bucket del ramo o dopo l'ora *Escludi a*, l'oggetto caricato in più parti viene incluso.

Operazione	Implementazione
AbortMultipartUpload	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
CompleteMultipartUpload	Vedere "CompleteMultipartUpload"
CreateMultipartUpload (Precedentemente denominato Initiate Multipart Upload)	Vedere "CreateMultipartUpload"
ListMultipartUploads	Vedere "ListMultipartUploads"
ListParts	Implementato con tutti i comportamenti REST API di Amazon S3. Soggetto a modifiche senza preavviso.
UploadPart	Vedere "UploadPart"

Operazione	Implementazione
UploadPartCopy	Vedere "UploadPartCopy"

Come StorageGRID S3 REST API completa i caricamenti multiparte

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 il `partNumber` parametro di richiesta con CompleteMultipartUpload. Il parametro può iniziare con qualsiasi valore.

Risolvi i conflitti

Le richieste dei client in conflitto, come due client che scrivono sulla stessa chiave, vengono risolte in base alle "ultime vincite". La tempistica per la valutazione degli "ultimi successi" si basa sul momento in cui il sistema StorageGRID completa una data richiesta e non sul momento in cui i client S3 iniziano un'operazione.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Intestazioni della richiesta di checksum:

- `x-amz-checksum-crc32`
- `x-amz-checksum-crc32c`
- `x-amz-checksum-crc64nvme`
- `x-amz-checksum-sha256`
- `x-amz-checksum-type`



Se una richiesta CreateMultipartUpload non specifica un checksum, StorageGRID non calcola un checksum CRC-64/NVME predefinito per un oggetto.

- `x-amz-storage-class`

L' `'x-amz-storage-class'` intestazione influisce sul numero di copie di oggetti create da StorageGRID se la regola ILM corrispondente specifica ["Dual commit o opzione di acquisizione bilanciata"](#).

- STANDARD

(Impostazione predefinita) specifica un'operazione di ingest dual-commit quando la regola ILM utilizza l'opzione Dual commit o quando l'opzione Balanced (bilanciamento) torna alla creazione di copie interinali.

- REDUCED_REDUNDANCY

Specifica un'operazione di ingest a commit singolo quando la regola ILM utilizza l'opzione di commit doppio o quando l'opzione di bilanciamento ritorna alla creazione di copie interinali.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l'`REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.



Se un caricamento multiparte non viene completato entro 15 giorni, l'operazione viene contrassegnata come inattiva e tutti i dati associati vengono cancellati dal sistema.



Il ETag valore restituito non è una somma di MD5 dei dati, ma segue l'implementazione API Amazon S3 del ETag valore per gli oggetti multiparte.

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- If-Match

L'If-Match intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l'If-Match intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented.

- If-None-Match

L'If-None-Match intestazione si comporta in modo diverso a seconda della configurazione di StorageGRID. Fornire questa intestazione potrebbe restituire un messaggio di errore (501 Not Implemented). Se l'If-None-Match intestazione viene accettata ma non è funzionale, potrebbe essere visualizzato un avviso con istruzioni su come abilitare il comportamento di errore più restrittivo 501 Not Implemented.

- x-amz-checksum-md5
- x-amz-checksum-sha1
- x-amz-checksum-sha512
- x-amz-checksum-xxhash3
- x-amz-checksum-xxhash64
- x-amz-checksum-xxhash128

Versione

Questa operazione completa un caricamento multiparte. Se il controllo delle versioni è attivato per un bucket, la versione dell'oggetto viene creata al termine del caricamento multiparte.

Se la versione è abilitata per un bucket, viene generato automaticamente un univoco `versionId` per la versione dell'oggetto che viene memorizzato. Questo `versionId` viene anche restituito nella risposta utilizzando l' `x-amz-version-id` intestazione della risposta.

Se la versione è sospesa, la versione oggetto viene memorizzata con un valore nullo `versionId` e se esiste già una versione nulla, verrà sovrascritta.



Quando il controllo delle versioni è attivato per un bucket, il completamento di un caricamento multiparte crea sempre una nuova versione, anche se ci sono caricamenti multipli simultanei completati sulla stessa chiave a oggetti. Quando il controllo delle versioni non è abilitato per un bucket, è possibile avviare un caricamento multiparte e fare in modo che un altro caricamento multiparte venga avviato e completato prima sulla stessa chiave a oggetti. Nei bucket senza versione, il caricamento multiparte che completa l'ultimo ha la precedenza.

Replica, notifica o notifica dei metadati non riuscite

Se il bucket in cui si verifica il caricamento multiparte è configurato per un servizio di piattaforma, il caricamento multiparte riesce anche se l'azione di replica o notifica associata non riesce.

Un tenant può attivare la replica o la notifica non riuscita aggiornando i metadati o i tag dell'oggetto. Un tenant può reinviare i valori esistenti per evitare modifiche indesiderate.

Fare riferimento alla ["Risolvere i problemi relativi ai servizi della piattaforma"](#).

Intestazioni e opzioni delle richieste S3 CreateMultipartUpload in StorageGRID

L'operazione CreateMultipartUpload (precedentemente denominata Initiate Multipart Upload) avvia un caricamento multiparte per un oggetto e restituisce un ID di caricamento.

L'`x-amz-storage-class` intestazione della richiesta è supportata. Il valore inviato per `x-amz-storage-class` influisce sul modo in cui StorageGRID protegge i dati degli oggetti durante l'acquisizione e non sul numero di copie persistenti dell'oggetto memorizzate nel sistema StorageGRID (determinato da ILM).

Se la regola ILM corrispondente a un oggetto acquisito utilizza Strict ["opzione di acquisizione"](#), l'`x-amz-storage-class` intestazione non ha alcun effetto.

I seguenti valori possono essere utilizzati per `x-amz-storage-class`:

- **STANDARD** (Impostazione predefinita)
 - **Dual Commit:** Se la regola ILM specifica l'opzione di acquisizione Dual Commit, non appena un oggetto viene acquisito una seconda copia di tale oggetto viene creata e distribuita in un nodo di archiviazione diverso (dual commit). Quando viene valutato ILM, StorageGRID determina se queste copie intermedie iniziali soddisfano le istruzioni di posizionamento della regola. In caso contrario, potrebbe essere necessario creare nuove copie degli oggetti in posizioni diverse e eliminare le copie intermedie iniziali.
 - **Balanced:** Se la regola ILM specifica l'opzione Balanced (bilanciamento) e StorageGRID non può eseguire immediatamente tutte le copie specificate nella regola, StorageGRID esegue due copie intermedie su nodi di storage diversi.

Se StorageGRID è in grado di creare immediatamente tutte le copie dell'oggetto specificate nella regola ILM (posizionamento sincrono), l'`x-amz-storage-class` intestazione non ha effetto.

- **REDUCED_REDUNDANCY**
 - **Dual Commit:** Se la regola ILM specifica l'opzione Dual Commit, StorageGRID crea una singola copia provvisoria quando l'oggetto viene acquisito (Single Commit).

- **Balanced:** Se la regola ILM specifica l'opzione Balanced, StorageGRID crea una singola copia provvisoria solo se il sistema non è in grado di eseguire immediatamente tutte le copie specificate nella regola. Se StorageGRID è in grado di eseguire il posizionamento sincrono, questa intestazione non ha alcun effetto. L' `REDUCED_REDUNDANCY` opzione viene utilizzata in modo ottimale quando la regola ILM corrispondente all'oggetto crea una singola copia replicata. In questo caso l'utilizzo di `REDUCED_REDUNDANCY` elimina la creazione e la cancellazione non necessarie di una copia degli oggetti extra per ogni operazione di acquisizione.

L'uso dell' `REDUCED_REDUNDANCY` opzione non è consigliato in altre circostanze. `REDUCED_REDUNDANCY` aumenta il rischio di perdita di dati degli oggetti durante l'acquisizione. Ad esempio, è possibile che si verifichino perdite di dati se la singola copia viene inizialmente memorizzata su un nodo di storage che non riesce prima che si verifichi la valutazione ILM.



Avere una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

La specifica `REDUCED_REDUNDANCY` influisce solo sul numero di copie create al momento della prima acquisizione di un oggetto. Non influisce sul numero di copie dell'oggetto create quando l'oggetto viene valutato dalle policy ILM attive e non comporta l'archiviazione dei dati a livelli inferiori di ridondanza nel sistema StorageGRID.



Se si sta inserendo un oggetto in un bucket con S3 Object Lock attivato, l' `REDUCED_REDUNDANCY` opzione viene ignorata. Se si sta acquisendo un oggetto in un bucket di conformità legacy, `REDUCED_REDUNDANCY` l'opzione restituisce un errore. StorageGRID eseguirà sempre un ingest dual-commit per garantire che i requisiti di conformità siano soddisfatti.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `Content-Type`
- `x-amz-checksum-algorithm`: Specifica CRC32, CRC32C, CRC64NVME, o SHA256



Se la richiesta `CreateMultipartUpload` non specifica un checksum, StorageGRID non calcola un checksum CRC-64/NVME predefinito per un oggetto. StorageGRID ignora valori `x-amz-checksum-algorithm` non validi o non supportati.

- `x-amz-checksum-type`
- `x-amz-meta-`, seguito da una coppia nome-valore contenente metadati definiti dall'utente

Quando si specifica la coppia nome-valore per i metadati definiti dall'utente, utilizzare questo formato generale:

```
x-amz-meta-_name_: `value`
```

Se si desidera utilizzare l'opzione **tempo di creazione definito dall'utente** come tempo di riferimento per

una regola ILM, è necessario utilizzare `creation-time` come nome dei metadati che registrano al momento della creazione dell'oggetto. Ad esempio:

```
x-amz-meta-creation-time: 1443399726
```

Il valore per `creation-time` viene valutato in secondi dal 1 gennaio 1970.



L'aggiunta `creation-time` come metadati definiti dall'utente non è consentita se si aggiunge un oggetto a un bucket in cui è abilitata la conformità legacy. Viene restituito un errore.

- Intestazioni della richiesta di blocco oggetti S3:

- `x-amz-object-lock-mode`
- `x-amz-object-lock-retain-until-date`
- `x-amz-object-lock-legal-hold`

Se viene effettuata una richiesta senza queste intestazioni, le impostazioni di conservazione predefinite del bucket vengono utilizzate per calcolare la versione dell'oggetto che resta aggiornata.

["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)

- Intestazioni di richiesta SSE:

- `x-amz-server-side-encryption`
- `x-amz-server-side-encryption-customer-key-MD5`
- `x-amz-server-side-encryption-customer-key`
- `x-amz-server-side-encryption-customer-algorithm`

[Intestazioni di richiesta per la crittografia lato server](#)



Per informazioni sul modo in cui StorageGRID gestisce i caratteri UTF-8, vedere ["PutObject"](#).

Intestazioni di richiesta per la crittografia lato server

È possibile utilizzare le seguenti intestazioni di richiesta per crittografare un oggetto multiparte con crittografia lato server. Le opzioni SSE e SSE-C si escludono a vicenda.

- **SSE:** Utilizzare la seguente intestazione nella richiesta `CreateMultipartUpload` se si desidera crittografare l'oggetto con una chiave univoca gestita da StorageGRID. Non specificare questa intestazione in nessuna delle richieste `UploadPart`.
 - `x-amz-server-side-encryption`
- **SSE-C:** Utilizzare tutte e tre le intestazioni nella richiesta `CreateMultipartUpload` (e in ogni richiesta `UploadPart` successiva) se si desidera crittografare l'oggetto con una chiave univoca fornita e gestita dall'utente.

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la chiave di crittografia per il nuovo oggetto.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 della chiave di crittografia del nuovo oggetto.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni relative a ["utilizzo della crittografia lato server"](#).

Intestazioni di richiesta non supportate

La seguente intestazione della richiesta non è supportata:

- `x-amz-website-redirect-location`

La `x-amz-website-redirect-location` testata ritorna `XNotImplemented`.

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione `CompleteMultipartUpload`, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

Operazione S3 `ListMultipartUploads` e parametri supportati in StorageGRID

L'operazione `ListMultipartUploads` elenca i caricamenti multiparte in corso per un bucket.

Sono supportati i seguenti parametri di richiesta:

- `encoding-type`
- `key-marker`
- `max-uploads`
- `prefix`
- `upload-id-marker`
- `Host`
- `Date`
- `Authorization`

Versione

Il caricamento multiparte consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione `CompleteMultipartUpload`, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

L'operazione UploadPart carica una parte in un upload multiparte per un oggetto.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- Intestazioni della richiesta di checksum:

- x-amz-checksum-crc32
- x-amz-checksum-crc32c
- x-amz-checksum-crc64nvme
- x-amz-checksum-sha256

Se hai specificato un checksum CRC-32, CRC-32C, CRC-64/NVME o SHA-256 durante la richiesta CreateMultipartUpload, devi anche includere l'intestazione della richiesta di checksum in ogni richiesta UploadPart.



Se una richiesta CreateMultipartUpload non specifica un checksum, StorageGRID non calcola un checksum CRC-64/NVME predefinito per un oggetto.

- Content-Length
- Content-MD5

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta CreateMultipartUpload, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta UploadPart:

- x-amz-server-side-encryption-customer-algorithm: Specificare AES256.
- x-amz-server-side-encryption-customer-key: Specificare la stessa chiave di crittografia fornita nella richiesta CreateMultipartUpload.
- x-amz-server-side-encryption-customer-key-MD5: Specificare lo stesso digest MD5 fornito nella richiesta CreateMultipartUpload.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in "[Utilizzare la crittografia lato server](#)".

Intestazioni di richiesta non supportate

Le seguenti intestazioni di richiesta non sono supportate:

- x-amz-sdk-checksum-algorithm
- x-amz-trailer
- x-amz-checksum-md5

- `x-amz-checksum-sha1`
- `x-amz-checksum-sha512`
- `x-amz-checksum-xxhash3`
- `x-amz-checksum-xxhash64`
- `x-amz-checksum-xxhash128`

Versione

Il caricamento multipart consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione `CompleteMultipartUpload`, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

Carica una parte di un oggetto in StorageGRID con l'operazione S3 `UploadPartCopy`

L'operazione `UploadPartCopy` carica una parte di un oggetto copiando i dati da un oggetto esistente come origine dati.

L'operazione `UploadPartCopy` viene implementata con tutto il comportamento dell'API REST Amazon S3. Soggetto a modifiche senza preavviso.

Questa richiesta legge e scrive i dati dell'oggetto specificati in `x-amz-copy-source-range` sistema StorageGRID.

Intestazioni di richiesta supportate

Sono supportate le seguenti intestazioni di richiesta:

- `x-amz-copy-source-if-match`
- `x-amz-copy-source-if-none-match`
- `x-amz-copy-source-if-unmodified-since`
- `x-amz-copy-source-if-modified-since`

Intestazioni di richiesta per la crittografia lato server

Se è stata specificata la crittografia SSE-C per la richiesta `CreateMultipartUpload`, è necessario includere anche le seguenti intestazioni di richiesta in ogni richiesta `UploadPartCopy`:

- `x-amz-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-server-side-encryption-customer-key`: Specificare la stessa chiave di crittografia fornita nella richiesta `CreateMultipartUpload`.
- `x-amz-server-side-encryption-customer-key-MD5`: Specificare lo stesso digest MD5 fornito nella richiesta `CreateMultipartUpload`.

Se l'oggetto di origine viene crittografato utilizzando una chiave fornita dal cliente (SSE-C), è necessario includere le tre intestazioni seguenti nella richiesta `UploadPartCopy`, in modo che l'oggetto possa essere decrittografato e quindi copiato:

- `x-amz-copy-source-server-side-encryption-customer-algorithm`: Specificare AES256.
- `x-amz-copy-source-server-side-encryption-customer-key`: Specificare la chiave di crittografia fornita al momento della creazione dell'oggetto di origine.
- `x-amz-copy-source-server-side-encryption-customer-key-MD5`: Specificare il digest MD5 fornito al momento della creazione dell'oggetto sorgente.



Le chiavi di crittografia fornite non vengono mai memorizzate. Se si perde una chiave di crittografia, si perde l'oggetto corrispondente. Prima di utilizzare le chiavi fornite dal cliente per proteggere i dati degli oggetti, esaminare le considerazioni riportate in ["Utilizzare la crittografia lato server"](#).

Versione

Il caricamento multipart consiste in operazioni separate per l'avvio del caricamento, l'elenco dei caricamenti, il caricamento delle parti, l'assemblaggio delle parti caricate e il completamento del caricamento. Quando si esegue l'operazione `CompleteMultipartUpload`, gli oggetti vengono creati (e, se applicabile, vengono aggiornati).

Supporto per il checksum S3

StorageGRID rileva automaticamente se è stato specificato un checksum durante una richiesta `CreateMultipartUpload` e utilizza questo checksum nell'operazione `UploadPartCopy`. Non devi specificare un checksum in una richiesta `UploadPartCopy`. Se una richiesta `CreateMultipartUpload` non specifica un checksum, StorageGRID non calcola un checksum CRC-64/NVME predefinito per un oggetto. StorageGRID non include un checksum per la parte copiata quando `CreateMultipartUpload` non ha specificato un checksum.

Risposte di errore dell'API REST S3 di StorageGRID

Il sistema StorageGRID supporta tutte le risposte di errore standard dell'API REST S3 applicabili. Inoltre, l'implementazione di StorageGRID aggiunge diverse risposte personalizzate.

Codici di errore S3 API supportati

Nome	Stato HTTP
Accesso negato	403 proibita
BadDigest	400 richiesta errata
BucketAlreadyExists	409 conflitto
BucketNotEmpty	409 conflitto
IncompleteBody	400 richiesta errata
InternalError	500 errore interno del server

Nome	Stato HTTP
InvalidAccessKeyId	403 proibita
Documento invalidato	400 richiesta errata
InvalidBucketName	400 richiesta errata
InvalidBucketState	409 conflitto
InvalidDigest	400 richiesta errata
InvalidEncryptionAlgorithmError	400 richiesta errata
InvalidPart	400 richiesta errata
InvalidPartOrder	400 richiesta errata
InvalidRange	416 intervallo richiesto non riscontrabile
InvalidRequest	400 richiesta errata
InvalidStorageClass	400 richiesta errata
InvalidTag	400 richiesta errata
InvalidURI	400 richiesta errata
KeyTooLong	400 richiesta errata
MalformedXML	400 richiesta errata
MetadataTooLarge	400 richiesta errata
MethodNon consentito	405 metodo non consentito
MissingContentLength	411 lunghezza richiesta
MissingRequestBodyError	400 richiesta errata
MissingSecurityHeader	400 richiesta errata
NoSuchBucket	404 non trovato
NoSuchKey	404 non trovato

Nome	Stato HTTP
NoSuchUpload	404 non trovato
Non soddisfatto	501 non implementato
NoSuchBucketPolicy	404 non trovato
ObjectLockConfigurationNotFoundError	404 non trovato
PrecondizioneFailed	412 precondizione non riuscita
RequestTimeTooSkewed	403 proibita
ServiceUnavailable (Servizio non disponibile)	503 Servizio non disponibile
SignatureDoesNotMatch	403 proibita
TooManyBucket	400 richiesta errata
UserKeyMustBeSpecified	400 richiesta errata

Codici di errore personalizzati StorageGRID

Nome	Descrizione	Stato HTTP
XBucketLifecycleNotAllowed	La configurazione del ciclo di vita del bucket non è consentita in un bucket compatibile legacy	400 richiesta errata
XBucketPolicyParseException	Impossibile analizzare JSON policy bucket ricevuta.	400 richiesta errata
XComplianceConflict	Operazione negata a causa delle impostazioni di conformità legacy.	403 proibita
XComplianceRiduciRedundancyProibita	La ridondanza ridotta non è consentita nel bucket compatibile legacy	400 richiesta errata
XMaxBucketPolicyLengthExceed	La policy supera la lunghezza massima consentita della policy bucket.	400 richiesta errata
XMissingInternalRequestHeader	Manca un'intestazione di una richiesta interna.	400 richiesta errata
Conformità XNoSuchBucketCompliance	Nel bucket specificato non è attivata la compliance legacy.	404 non trovato

Nome	Descrizione	Stato HTTP
XNotAcceptable (XNotAccettabile)	La richiesta contiene una o più intestazioni di accettazione che non possono essere soddisfatte.	406 non accettabile
XNotImplemented	La richiesta fornita implica funzionalità non implementate.	501 non implementato

Operazioni personalizzate di StorageGRID

Operazioni personalizzate sui bucket supportate in 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
"COERENZA del bucket"	Restituisce la coerenza applicata a un determinato bucket.
"METTI la coerenza del bucket"	Imposta la coerenza applicata a un particolare bucket.
"OTTIENI l'ultimo tempo di accesso a bucket"	Restituisce se gli ultimi aggiornamenti dell'ora di accesso sono attivati o disattivati per un bucket specifico.
"TEMPO ULTIMO accesso bucket"	Consente di attivare o disattivare gli ultimi aggiornamenti dell'orario di accesso per un determinato bucket.
"ELIMINA la configurazione di notifica dei metadati del bucket"	Elimina l'XML di configurazione della notifica dei metadati associato a un bucket specifico.
"OTTIENI la configurazione della notifica dei metadati del bucket"	Restituisce l'XML di configurazione della notifica dei metadati associato a un bucket specifico.
"INSERIRE la configurazione della notifica dei metadati del bucket"	Configura il servizio di notifica dei metadati per un bucket.
"OTTIENI l'utilizzo dello storage"	Indica la quantità totale di spazio di archiviazione utilizzato da un account e per ciascun bucket associato all'account.
"Obsoleto: CreateBucket con impostazioni di conformità"	Obsoleto e non supportato: Non è più possibile creare nuovi bucket con Compliance abilitata.
"Obsoleto: OTTIENI la compliance del bucket"	Obsoleto ma supportato: Restituisce le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

Operazione	Descrizione
"Obsoleto: METTI la compliance del bucket"	Obsoleto ma supportato: Consente di modificare le impostazioni di conformità per un bucket compatibile esistente.

Recupera il livello di coerenza del bucket in StorageGRID con la richiesta GET Bucket consistency

La richiesta di coerenza GET Bucket consente di determinare la coerenza applicata a un determinato bucket.

La coerenza predefinita è impostata per garantire la lettura dopo scrittura per gli oggetti appena creati.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketConsistency o essere root dell'account.

Esempio di richiesta

```
GET /bucket?x-ntap-sg-consistency HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Nella risposta XML, <Consistency> restituirà uno dei seguenti valori:

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.
disponibile	Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Esempio di risposta

```
HTTP/1.1 200 OK
Date: Fri, 18 Sep 2020 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/11.5.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<Consistency xmlns="http://s3.storagegrid.com/doc/2015-02-01/">read-after-
new-write</Consistency>
```

Informazioni correlate

["Coerenza"](#)

Specificare i livelli di consistenza in StorageGRID con la richiesta PUT Bucket consistency

La richiesta di coerenza PUT bucket consente di specificare la coerenza da applicare alle operazioni eseguite su un bucket.

La coerenza predefinita è impostata per garantire la lettura dopo scrittura per gli oggetti appena creati.

Prima di iniziare

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketConsistency o essere root dell'account.

Richiesta

Il `x-ntap-sg-consistency` parametro deve contenere uno dei seguenti valori:

Coerenza	Descrizione
tutto	Tutti i nodi ricevono i dati immediatamente, altrimenti la richiesta non riesce.
forte-globale	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client in tutti i siti.
sito forte	Garantisce la coerenza di lettura dopo scrittura per tutte le richieste dei client all'interno di un sito.
read-after-new-write	(Impostazione predefinita) fornisce coerenza di lettura dopo scrittura per i nuovi oggetti ed eventuale coerenza per gli aggiornamenti degli oggetti. Offre alta disponibilità e garanzie di protezione dei dati. Consigliato per la maggior parte dei casi.

Coerenza	Descrizione
disponibile	Fornisce una coerenza finale sia per i nuovi oggetti che per gli aggiornamenti degli oggetti. Per i bucket S3, utilizzare solo se necessario (ad esempio, per un bucket che contiene valori di log che vengono raramente letti o per operazioni HEAD o GET su chiavi che non esistono). Non supportato per i bucket S3 FabricPool.

Nota: in generale, si dovrebbe usare la coerenza "Read-after-new-write". Se le richieste non funzionano correttamente, modificare il comportamento del client dell'applicazione, se possibile. In alternativa, configurare il client per specificare la coerenza per ogni richiesta API. Impostare la consistenza a livello del bucket solo come ultima risorsa.

Esempio di richiesta

```
PUT /bucket?x-ntap-sg-consistency=strong-global HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Informazioni correlate

["Coerenza"](#)

Recupera lo stato dell'ultimo accesso al bucket in StorageGRID con la richiesta GET Bucket last access time

La richiesta GET bucket last access time (OTTIENI bucket ultimo accesso) consente di determinare se gli ultimi aggiornamenti dell'orario di accesso sono attivati o disattivati per i singoli bucket.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketLastAccessTime o essere root dell'account.

Esempio di richiesta

```
GET /bucket?x-ntap-sg-lastaccesstime HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra che gli ultimi aggiornamenti dell'ora di accesso sono attivati per il bucket.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 01:02:18 GMT
Connection: CLOSE
Server: StorageGRID/10.3.0
x-amz-request-id: 12345
Content-Length: 127
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<LastAccessTime xmlns="http://s3.storagegrid.com/doc/2015-02-01/">enabled
</LastAccessTime>
```

Abilita e disabilita gli aggiornamenti dell'ora dell'ultimo accesso in StorageGRID con la richiesta PUT Bucket last access time

La richiesta PUT bucket Last access time consente di attivare o disattivare gli ultimi aggiornamenti del tempo di accesso per i singoli bucket. La disattivazione degli ultimi aggiornamenti dell'orario di accesso migliora le prestazioni ed è l'impostazione predefinita per tutti i bucket creati con la versione 10.3.0 o successiva.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketLastAccessTime per un bucket o essere root dell'account.



A partire dalla versione 10.3 di StorageGRID, gli aggiornamenti all'ultimo tempo di accesso sono disattivati per impostazione predefinita per tutti i nuovi bucket. Se si dispone di bucket creati utilizzando una versione precedente di StorageGRID e si desidera che corrispondano al nuovo comportamento predefinito, è necessario disattivare esplicitamente gli ultimi aggiornamenti del tempo di accesso per ciascuno di questi bucket precedenti. È possibile attivare o disattivare gli aggiornamenti per l'ora dell'ultimo accesso utilizzando la richiesta PUT Bucket last access time o dalla pagina dei dettagli di un bucket in Tenant Manager. Vedere ["Attiva o disattiva gli ultimi aggiornamenti dell'orario di accesso"](#).

Se gli ultimi aggiornamenti dell'ora di accesso sono disattivati per un bucket, alle operazioni sul bucket viene applicato il seguente comportamento:

- Le richieste GetObject, GetObjectAcl, GetObjectTagging e HeadObject non aggiornano l'ora dell'ultimo accesso. L'oggetto non viene aggiunto alle code per la valutazione ILM (Information Lifecycle Management).
- Le richieste CopyObject e PutObjectTagging che aggiornano solo i metadati aggiornano anche l'ora dell'ultimo accesso. L'oggetto viene aggiunto alle code per la valutazione ILM.
- Se gli aggiornamenti dell'ora dell'ultimo accesso sono disattivati per il bucket di origine, le richieste CopyObject non aggiornano l'ora dell'ultimo accesso per il bucket di origine. L'oggetto copiato non viene aggiunto alle code per la valutazione ILM del bucket di origine. Tuttavia, per la destinazione, le richieste CopyObject aggiornano sempre l'ora dell'ultimo accesso. La copia dell'oggetto viene aggiunta alle code per la valutazione ILM.
- CompleteMultipartUpload richiede l'aggiornamento dell'ora di ultimo accesso. L'oggetto completato viene aggiunto alle code per la valutazione ILM.

Richiedi esempi

In questo esempio viene attivato l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=enabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Questo esempio disattiva l'ultimo tempo di accesso per un bucket.

```
PUT /bucket?x-ntap-sg-lastaccesstime=disabled HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Disabilitare il servizio di integrazione della ricerca con la richiesta di configurazione della notifica dei metadati DELETE Bucket in StorageGRID

La richiesta di configurazione DELLA notifica dei metadati DEL bucket DELETE consente di disattivare il servizio di integrazione della ricerca per i singoli bucket eliminando il file XML di configurazione.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:DeleteBucketMetadataNotification per un bucket o essere root dell'account.

Esempio di richiesta

Questo esempio mostra la disattivazione del servizio di integrazione della ricerca per un bucket.

```
DELETE /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Configura l'integrazione della ricerca in StorageGRID con la richiesta di configurazione della notifica dei metadati del bucket GET

La richiesta DI configurazione DELLA notifica dei metadati GET Bucket consente di recuperare l'XML di configurazione utilizzato per configurare l'integrazione della ricerca per i singoli bucket.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:GetBucketMetadataNotification o essere root dell'account.

Esempio di richiesta

Questa richiesta recupera la configurazione di notifica dei metadati per il bucket denominato `bucket`.

```
GET /bucket?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Risposta

Il corpo della risposta include la configurazione della notifica dei metadati per il bucket. La configurazione della notifica dei metadati consente di determinare la configurazione del bucket per l'integrazione della ricerca. Ciò consente di determinare quali oggetti vengono indicizzati e a quali endpoint vengono inviati i metadati degli oggetti.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:_region:account-
ID_:domain/_mydomain/myindex/mytype_</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione in cui StorageGRID deve inviare i metadati degli oggetti. Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfi guration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì

Nome	Descrizione	Obbligatorio
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì

Nome	Descrizione	Obbligatorio
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • es deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato domain-name/myindex/mytype. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. Hanno la seguente forma: • arn:aws:es:_region:account-ID_:domain/mydomain/myindex/mytype • urn:mysite:es:::mydomain/myindex/mytype L'endpoint deve essere configurato prima dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'urn è incluso nell'elemento Destination.	Sì

Esempio di risposta

L'XML incluso tra i

```
<MetadataNotificationConfiguration></MetadataNotificationConfiguration>
```

tag mostra come è configurata l'integrazione con un endpoint di integrazione della ricerca per il bucket. In questo esempio, i metadati degli oggetti vengono inviati a un indice Elasticsearch denominato e a un tipo `2017 denominato ospitato in un dominio AWS records denominato current.

```
HTTP/1.1 200 OK
Date: Thu, 20 Jul 2017 18:24:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/11.0.0
x-amz-request-id: 3832973499
Content-Length: 264
Content-Type: application/xml

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix>2017</Prefix>
    <Destination>
      <Urn>arn:aws:es:us-east-
1:3333333:domain/records/current/2017</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

Informazioni correlate

["Utilizzare un account tenant"](#)

Abilita il servizio di integrazione della ricerca in StorageGRID con la richiesta di configurazione della notifica dei metadati del bucket PUT

La richiesta di configurazione DELLA notifica dei metadati PUT bucket consente di attivare il servizio di integrazione della ricerca per i singoli bucket. L'XML di configurazione della notifica dei metadati fornito nel corpo della richiesta specifica gli oggetti i cui metadati vengono inviati all'indice di ricerca di destinazione.

Per completare questa operazione, è necessario disporre dell'autorizzazione s3:PutBucketMetadataNotification per un bucket o essere account root.

Richiesta

La richiesta deve includere la configurazione della notifica dei metadati nel corpo della richiesta. Ogni configurazione di notifica dei metadati include una o più regole. Ogni regola specifica gli oggetti a cui si applica e la destinazione in cui StorageGRID deve inviare i metadati degli oggetti.

Gli oggetti possono essere filtrati in base al prefisso del nome dell'oggetto. Ad esempio, è possibile inviare metadati per gli oggetti con il prefisso `/images` a una destinazione e oggetti con il prefisso `/videos` a un'altra.

Le configurazioni con prefissi sovrapposti non sono valide e vengono rifiutate al momento dell'invio. Ad esempio, non è consentita una configurazione che includeva una regola per gli oggetti con il prefisso `test` e una seconda regola per gli oggetti con il prefisso `test2`.

Le destinazioni devono essere specificate utilizzando l'URN di un endpoint StorageGRID. L'endpoint deve esistere quando viene inoltrata la configurazione della notifica dei metadati o la richiesta non riesce come un 400 Bad Request. il messaggio di errore indica: Unable to save the metadata notification (search) policy. The specified endpoint URN does not exist: *URN*.

```
<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>rule-status</Status>
    <Prefix>key-prefix</Prefix>
    <Destination>
      <Urn>arn:aws:es:region:account-
ID:domain/mydomain/myindex/mytype</Urn>
    </Destination>
  </Rule>
  <Rule>
    <ID>Rule-2</ID>
    ...
  </Rule>
  ...
</MetadataNotificationConfiguration>
```

La tabella descrive gli elementi contenuti nel file XML di configurazione per la notifica dei metadati.

Nome	Descrizione	Obbligatorio
MetadataNotificationConfi guration	Tag container per le regole utilizzate per specificare gli oggetti e la destinazione per le notifiche dei metadati. Contiene uno o più elementi della regola.	Sì
Regola	Tag container per una regola che identifica gli oggetti i cui metadati devono essere aggiunti a un indice specificato. Le regole con prefissi sovrapposti vengono rifiutate. Incluso nell'elemento MetadataNotificationConfiguration.	Sì
ID	Identificatore univoco della regola. Incluso nell'elemento Rule.	No

Nome	Descrizione	Obbligatorio
Stato	Lo stato può essere "abilitato" o "Disabilitato". Non viene intrapresa alcuna azione per le regole disattivate. Incluso nell'elemento Rule.	Sì
Prefisso	Gli oggetti che corrispondono al prefisso vengono influenzati dalla regola e i relativi metadati vengono inviati alla destinazione specificata. Per far corrispondere tutti gli oggetti, specificare un prefisso vuoto. Incluso nell'elemento Rule.	Sì
Destinazione	Tag container per la destinazione di una regola. Incluso nell'elemento Rule.	Sì
Urna	URNA della destinazione in cui vengono inviati i metadati dell'oggetto. Deve essere l'URN di un endpoint StorageGRID con le seguenti proprietà: • <code>es</code> deve essere il terzo elemento. • L'URN deve terminare con l'indice e digitare dove sono memorizzati i metadati, nel formato <code>domain-name/myindex/mytype</code>. Gli endpoint vengono configurati utilizzando l'API tenant Manager o tenant Management. 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 dell'invio dell'XML di configurazione, altrimenti la configurazione non riesce e viene visualizzato un errore 404. L'urn è incluso nell'elemento Destination.	Sì

Richiedi esempi

Questo esempio mostra come abilitare l'integrazione della ricerca per un bucket. In questo esempio, i metadati degli oggetti per tutti gli oggetti vengono inviati alla stessa destinazione.

```
PUT /test1?x-ntap-sg-metadata-notification HTTP/1.1
Date: date
Authorization: authorization string
Host: host

<MetadataNotificationConfiguration>
  <Rule>
    <ID>Rule-1</ID>
    <Status>Enabled</Status>
    <Prefix></Prefix>
    <Destination>
      <Urn>urn:sgws:es:::sgws-notifications/test1/all</Urn>
    </Destination>
  </Rule>
</MetadataNotificationConfiguration>
```

In questo esempio, i metadati degli oggetti corrispondenti al prefisso `/images` vengono inviati a una destinazione, mentre i metadati degli oggetti corrispondenti al prefisso `/videos` vengono inviati 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 attiva il servizio di integrazione della ricerca per un bucket, viene generato un documento JSON e inviato all'endpoint di destinazione ogni volta che vengono aggiunti, aggiornati o cancellati metadati o tag dell'oggetto.

Questo esempio mostra un esempio di JSON che potrebbe essere generato quando un oggetto con la chiave `SGWS/Tagging.txt` viene creato in un bucket denominato `test`. La `test` benna non è in versione, quindi l'etichetta ``versionId`` è vuota.

```
{
  "bucket": "test",
  "key": "SGWS/Tagging.txt",
  "versionId": "",
  "accountId": "86928401983529626822",
  "size": 38,
  "md5": "3d6c7634a85436eee06d43415012855",
  "region": "us-east-1",
  "metadata": {
    "age": "25"
  },
  "tags": {
    "color": "yellow"
  }
}
```

Metadati degli oggetti inclusi nelle notifiche dei metadati

La tabella elenca tutti i campi inclusi nel documento JSON che viene inviato all'endpoint di destinazione quando è attivata l'integrazione della ricerca.

Il nome del documento include il nome del bucket, il nome dell'oggetto e l'ID della versione, se presente.

Tipo	Nome dell'elemento	Descrizione
Informazioni su bucket e oggetti	bucket	Nome del bucket
Informazioni su bucket e oggetti	chiave	Nome chiave oggetto
Informazioni su bucket e oggetti	ID versione	Versione oggetto, per gli oggetti nei bucket con versione
Informazioni su bucket e oggetti	regione	Ad esempio, la regione del bucket us-east-1
Metadati di sistema	dimensione	Dimensione dell'oggetto (in byte) come visibile a un client HTTP
Metadati di sistema	md5	Hash di oggetto
Metadati dell'utente	metadati <i>key:value</i>	Tutti i metadati dell'utente per l'oggetto, come coppie chiave-valore

Tipo	Nome dell'elemento	Descrizione
Tag	tag <i>key:value</i>	Tutti i tag di oggetto definiti per l'oggetto, come coppie chiave-valore



Per tag e metadati dell'utente, StorageGRID passa date e numeri a Elasticsearch come stringhe o come notifiche di eventi S3. Per configurare Elasticsearch in modo da interpretare queste stringhe come date o numeri, seguire le istruzioni di Elasticsearch per la mappatura dinamica dei campi e per i formati di mappatura dei dati. Prima di configurare il servizio di integrazione della ricerca, è necessario attivare le mappature dinamiche dei campi sull'indice. Una volta indicizzato un documento, non è possibile modificare i tipi di campo del documento nell'indice.

Informazioni correlate

["Utilizzare un account tenant"](#)

Recupera l'utilizzo dello storage dell'account e del bucket in StorageGRID con la richiesta GET Storage Usage

La richiesta GET Storage Usage indica la quantità totale di storage in uso da un account e per ciascun bucket associato all'account.

La quantità di spazio di archiviazione utilizzata da un account e dai relativi bucket può essere ottenuta da una richiesta ListBuckets modificata con il `x-ntap-sg-usage` parametro query. L'utilizzo dello storage bucket viene monitorato separatamente dalle richieste DI PUT ed ELIMINAZIONE elaborate dal sistema. Potrebbe verificarsi un ritardo prima che i valori di utilizzo corrispondano ai valori previsti in base all'elaborazione delle richieste, in particolare se il sistema è sottoposto a un carico pesante.

Per impostazione predefinita, StorageGRID tenta di recuperare le informazioni sull'utilizzo utilizzando una coerenza forte-globale. Se non è possibile ottenere una forte coerenza globale, StorageGRID tenta di recuperare le informazioni sull'utilizzo con una forte coerenza del sito.

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:ListAllMyBucket` o essere root dell'account.

Esempio di richiesta

```
GET /?x-ntap-sg-usage HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Questo esempio mostra un account con quattro oggetti e 12 byte di dati in due bucket. Ogni bucket contiene due oggetti e sei byte di dati.

```
HTTP/1.1 200 OK
Date: Sat, 29 Nov 2015 00:49:05 GMT
Connection: KEEP-ALIVE
Server: StorageGRID/10.2.0
x-amz-request-id: 727237123
Content-Length: 427
Content-Type: application/xml

<?xml version="1.0" encoding="UTF-8"?>
<UsageResult xmlns="http://s3.storagegrid.com/doc/2015-02-01">
<CalculationTime>2014-11-19T05:30:11.000000Z</CalculationTime>
<ObjectCount>4</ObjectCount>
<DataBytes>12</DataBytes>
<Buckets>
<Bucket>
<Name>bucket1</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
<Bucket>
<Name>bucket2</Name>
<ObjectCount>2</ObjectCount>
<DataBytes>6</DataBytes>
</Bucket>
</Buckets>
</UsageResult>
```

Versione

Ogni versione dell'oggetto memorizzata contribuirà ai `ObjectCount` valori e `DataBytes` nella risposta. I marcatori di eliminazione non vengono aggiunti al `ObjectCount` totale.

Informazioni correlate

["Coerenza"](#)

Richieste bucket obsolete per conformità legacy

Richieste di bucket deprecated per la Compliance StorageGRID legacy

Potrebbe essere necessario utilizzare l'API REST di StorageGRID S3 per gestire i bucket creati utilizzando la funzionalità di conformità legacy.

Funzionalità di compliance obsoleta

La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3.

Se in precedenza è stata attivata l'impostazione di conformità globale, l'impostazione di blocco oggetti S3 globale viene attivata in StorageGRID 11.6. Non è più possibile creare nuovi bucket con la conformità abilitata; tuttavia, se necessario, è possibile utilizzare l'API REST di StorageGRID S3 per gestire qualsiasi bucket compatibile esistente.

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Richieste di conformità obsolete:

- ["Deprecato - CONSENTE DI APPORTARE modifiche alla richiesta di conformità al bucket"](#)

L'elemento XML SGCompliance è obsoleto. In precedenza, era possibile includere questo elemento personalizzato StorageGRID nel corpo della richiesta XML opzionale di PUT bucket Requests per creare un bucket conforme.

- ["Obsoleto - CONFORMITÀ bucket"](#)

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.

- ["Deprecato - METTERE la compliance del bucket"](#)

La richiesta DI compliance PUT Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.

Elemento SGCompliance obsoleto in StorageGRID

L'elemento XML SGCompliance è obsoleto. In precedenza, è possibile includere questo elemento personalizzato StorageGRID nel corpo di richiesta XML opzionale delle richieste CreateBucket per creare un bucket conforme.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Non è più possibile creare nuovi bucket con Compliance abilitata. Se si tenta di utilizzare le modifiche della richiesta CreateBucket per la conformità per creare un nuovo bucket conforme, viene visualizzato il seguente messaggio di errore:

```
The Compliance feature is deprecated.  
Contact your StorageGRID administrator if you need to create new Compliant  
buckets.
```

Richiesta GET Bucket di conformità obsoleta in StorageGRID

La richiesta DI compliance GET Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per determinare le impostazioni di conformità attualmente in vigore per un bucket compatibile esistente.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:GetBucketCompliance` o essere root dell'account.

Esempio di richiesta

Questa richiesta di esempio consente di determinare le impostazioni di conformità per il bucket denominato `mybucket`.

```
GET /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization string
Host: host
```

Esempio di risposta

Nella risposta XML, `<SGCompliance>` elenca le impostazioni di conformità in vigore per il bucket. Questa risposta di esempio mostra le impostazioni di compliance per un bucket in cui ciascun oggetto verrà conservato per un anno (525,600 minuti), a partire da quando l'oggetto viene acquisito nella griglia. Attualmente non esiste un blocco legale in questo bucket. Ogni oggetto verrà automaticamente cancellato dopo un anno.


```

HTTP/1.1 200 OK
Date: date
Connection: connection
Server: StorageGRID/11.1.0
x-amz-request-id: request ID
Content-Length: length
Content-Type: application/xml

<SGCompliance>
  <RetentionPeriodMinutes>525600</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>

```

Nome	Descrizione
RetentionPeriodMinutes	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia.
LegalHold	• Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	• Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

Risposte agli errori

Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è 404 Not Found, con un codice di errore S3 di XNoSuchBucketCompliance.

Richiesta PUT Bucket compliance obsoleta in StorageGRID

La richiesta DI compliance PUT Bucket è obsoleta. Tuttavia, è possibile continuare a utilizzare questa richiesta per modificare le impostazioni di conformità per un bucket compatibile esistente. Ad esempio, è possibile mettere un bucket esistente in attesa legale o aumentarne il periodo di conservazione.



La funzionalità di conformità StorageGRID, disponibile nelle versioni precedenti di StorageGRID, è obsoleta ed è stata sostituita da blocco oggetti S3. Per ulteriori informazioni, vedere quanto segue:

- ["Utilizzare l'API REST S3 per configurare il blocco oggetti S3"](#)
- ["Knowledge base di NetApp: Come gestire i bucket conformi alle versioni precedenti in StorageGRID 11.5"](#)

Per completare questa operazione, è necessario disporre dell'autorizzazione `s3:PutBucketCompliance` o essere root dell'account.

È necessario specificare un valore per ogni campo delle impostazioni di compliance quando si invia una richiesta DI compliance PUT bucket.

Esempio di richiesta

Questa richiesta di esempio modifica le impostazioni di conformità per il bucket denominato `mybucket`. In questo esempio, gli oggetti in verranno conservati per due anni (1.051.200 minuti) invece di un anno, a partire dal momento in `mybucket` cui l'oggetto viene inserito nella griglia. Questo bucket non ha alcuna tenuta legale. Ogni oggetto verrà automaticamente cancellato dopo due anni.

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Date: date
Authorization: authorization name
Host: host
Content-Length: 152

<SGCompliance>
  <RetentionPeriodMinutes>1051200</RetentionPeriodMinutes>
  <LegalHold>false</LegalHold>
  <AutoDelete>true</AutoDelete>
</SGCompliance>
```

Nome	Descrizione
RetentionPeriodMinutes	La durata del periodo di conservazione per gli oggetti aggiunti a questo bucket, in minuti. Il periodo di conservazione inizia quando l'oggetto viene acquisito nella griglia. Importante quando si specifica un nuovo valore per <code>RetentionPeriodMinutes</code>, è necessario specificare un valore uguale o superiore al periodo di conservazione corrente del bucket. Una volta impostato il periodo di conservazione del bucket, non è possibile diminuire tale valore, ma solo aumentarlo.

Nome	Descrizione
LegalHold	• Vero: Questo bucket è attualmente sotto una stretta legale. Gli oggetti in questo bucket non possono essere cancellati fino a quando non viene revocata la conservazione a fini giudiziari, anche se il periodo di conservazione è scaduto. • Falso: Questo bucket non è attualmente sotto una stretta legale. Gli oggetti in questo bucket possono essere cancellati allo scadere del periodo di conservazione.
Eliminazione automatica	• Vero: Gli oggetti in questo bucket verranno cancellati automaticamente allo scadere del periodo di conservazione, a meno che il bucket non sia sottoposto a un blocco legale. • Falso: Gli oggetti in questo bucket non verranno cancellati automaticamente alla scadenza del periodo di conservazione. Se è necessario eliminarli, è necessario eliminarli manualmente.

Coerenza per le impostazioni di conformità

Quando aggiorni le impostazioni di compliance per un bucket S3 con una richiesta DI compliance PUT bucket, StorageGRID tenta di aggiornare i metadati del bucket nella griglia. Per impostazione predefinita, StorageGRID utilizza la coerenza **strong-Global** per garantire che tutti i siti dei data center e tutti i nodi di storage che contengono i metadati del bucket abbiano coerenza di lettura dopo scrittura per le impostazioni di conformità modificate.

Se StorageGRID non riesce a raggiungere la coerenza **strong-Global** perché un sito di data center o più nodi di archiviazione in un sito non sono disponibili, il codice di stato HTTP per la risposta è 503 `Service Unavailable`.

Se si riceve questa risposta, è necessario contattare l'amministratore del grid per assicurarsi che i servizi di storage richiesti siano resi disponibili il prima possibile. Se l'amministratore della griglia non è in grado di rendere disponibile una quantità sufficiente di nodi di archiviazione in ogni sito, il supporto tecnico potrebbe richiedere di riprovare la richiesta non riuscita forzando la coerenza **strong-Site**.



Non forzare mai la coerenza **strong-site** per la conformità del bucket PUT a meno che non sia stato richiesto dal supporto tecnico e a meno che non si capiscano le potenziali conseguenze dell'utilizzo di questo livello.

Quando la coerenza viene ridotta a **strong-Site**, StorageGRID garantisce che le impostazioni di conformità aggiornate abbiano coerenza di lettura dopo scrittura solo per le richieste client all'interno di un sito. Ciò significa che il sistema StorageGRID potrebbe disporre temporaneamente di più impostazioni incoerenti per questo bucket fino a quando non saranno disponibili tutti i siti e i nodi di storage. Le impostazioni incoerenti possono causare comportamenti imprevisti e indesiderati. Ad esempio, se si colloca un bucket in una conservazione legale e si forza una minore coerenza, le precedenti impostazioni di conformità del bucket (ovvero, blocco legale) potrebbero continuare a essere attive in alcuni data center. Di conseguenza, gli oggetti che si ritiene siano in stato di conservazione a fini giudiziari potrebbero essere eliminati allo scadere del periodo di conservazione, dall'utente o mediante eliminazione automatica, se attivata.

Per forzare l'uso della coerenza **strong-Site**, rimettere la richiesta di conformità PUT Bucket e includere l'`Consistency-Control` intestazione della richiesta HTTP, come segue:

```
PUT /mybucket/?x-ntap-sg-compliance HTTP/1.1
Consistency-Control: strong-site
```

Risposte agli errori

- Se il bucket non è stato creato per essere conforme, il codice di stato HTTP per la risposta è 404 Not Found.
- Se `RetentionPeriodMinutes` nella richiesta è inferiore al periodo di conservazione corrente del bucket, il codice di stato HTTP è 400 Bad Request.

Informazioni correlate

"[Deprecato: APPORTARE modifiche alla richiesta di conformità al bucket](#)"

Gestire le policy di accesso

Come StorageGRID utilizza le policy AWS per controllare l'accesso ai bucket e agli oggetti S3

StorageGRID utilizza il linguaggio delle policy di Amazon Web Services (AWS) per consentire ai tenant S3 di controllare l'accesso ai bucket e agli oggetti all'interno di tali bucket. Il sistema StorageGRID implementa un sottoinsieme del linguaggio dei criteri delle API REST S3. I criteri di accesso per l'API S3 sono scritti in JSON.

Panoramica dei criteri di accesso

StorageGRID supporta tre tipi di criteri di accesso:

- **Criteri bucket**, che sono gestiti utilizzando le operazioni API `GetBucketPolicy`, `PutBucketPolicy` e `DeleteBucketPolicy` S3 o l'API `Tenant Manager` o `Tenant Management`. Le policy del bucket sono collegate ai bucket, quindi sono configurate per controllare l'accesso degli utenti nell'account del proprietario del bucket o altri account al bucket e agli oggetti in esso contenuti. Una policy di bucket si applica a un solo bucket ed eventualmente a più gruppi.
- **Criteri di gruppo**, configurati utilizzando l'API di gestione `tenant Manager` o `tenant`. I criteri di gruppo sono associati a un gruppo dell'account, quindi sono configurati per consentire a tale gruppo di accedere a risorse specifiche di proprietà di tale account. Una policy di gruppo si applica a un solo gruppo e possibilmente a più bucket.
- **Criteri di sessione**, inclusi come parte della richiesta `AssumeRole`. I criteri di sessione si applicano solo alla sessione specificata, definendo ulteriormente le autorizzazioni di cui dispone l'utente, oltre a quelle concesse dai criteri di gruppo e di bucket.



Non vi è alcuna differenza di priorità tra i criteri di gruppo, bucket e sessione.

Le policy di gruppo e bucket di StorageGRID seguono una grammatica specifica definita da Amazon. All'interno di ogni policy è presente una serie di dichiarazioni di policy, ciascuna delle quali contiene i seguenti elementi:

- ID dichiarazione (Sid) (opzionale)
- Effetto
- Principal/NotPrincipal

- Risorsa/NotResource
- Azione/Notazione
- Condizione (opzionale)

Le istruzioni dei criteri vengono create utilizzando questa struttura per specificare le autorizzazioni: Grant <Effect> per consentire/negare a <Principal> di eseguire <Action> su <Resource> quando viene applicato <Condition>.

Ciascun elemento di policy viene utilizzato per una funzione specifica:

Elemento	Descrizione
SID	L'elemento Sid è opzionale. Il Sid deve essere utilizzato solo come descrizione per l'utente. Viene memorizzato ma non interpretato dal sistema StorageGRID.
Effetto	Utilizzare l'elemento Effect per stabilire se le operazioni specificate sono consentite o rifiutate. È necessario identificare le operazioni consentite (o negate) su bucket o oggetti utilizzando le parole chiave dell'elemento Action supportate.
Principal/NotPrincipal	È possibile consentire a utenti, gruppi e account di accedere a risorse specifiche ed eseguire azioni specifiche. Se nella richiesta non è inclusa alcuna firma S3, l'accesso anonimo è consentito specificando il carattere jolly (*) come principale. Per impostazione predefinita, solo l'account root ha accesso alle risorse di proprietà dell'account. Il Principal: • <code>"Principal": "*" </code> corrisponde a tutti, comprese le richieste anonime (non firmate) • <code>"Principal": { "AWS": "*" } </code> corrisponde a qualsiasi identità o utente autenticato (non corrisponde alle richieste anonime) • Si applica solo alle bucket policy • Il principal è l'account/gli account/gli utenti a cui vengono concesse o negate le autorizzazioni È sufficiente specificare l'elemento Principal in una policy bucket. Per i criteri di gruppo, il gruppo a cui è associato il criterio è l'elemento Principal implicito.
Risorsa/NotResource	L'elemento Resource identifica bucket e oggetti. Puoi consentire o negare le autorizzazioni per bucket e oggetti utilizzando il nome risorsa Amazon (ARN) per identificare la risorsa.

Elemento	Descrizione
Azione/Notazione	Gli elementi Action e Effect sono i due componenti delle autorizzazioni. Quando un gruppo richiede una risorsa, gli viene concesso o negato l'accesso alla risorsa. L'accesso viene negato a meno che non si assegnino specificamente autorizzazioni, ma è possibile utilizzare la funzione di negazione esplicita per ignorare un'autorizzazione concessa da un altro criterio.
Condizione	L'elemento Condition è opzionale. Le condizioni consentono di creare espressioni per determinare quando applicare un criterio.

Nell'elemento Action, è possibile utilizzare il carattere jolly (*) per specificare tutte le operazioni o un sottoinsieme di operazioni. Ad esempio, questa azione corrisponde a permessi come s3:GetObject, s3:PutObject e s3:DeleteObject.

```
s3:*Object
```

Nell'elemento Resource, è possibile utilizzare i caratteri jolly () e (?). **Mentre l'asterisco ()** corrisponde a 0 o più caratteri, il punto interrogativo (?) corrisponde a qualsiasi singolo carattere.

Nell'elemento Principal, i caratteri jolly non sono supportati, ad eccezione dell'impostazione dell'accesso anonimo, che concede l'autorizzazione a tutti. Ad esempio, impostare il carattere jolly (*) come valore Principal.

```
"Principal": ""
```

```
"Principal": {"AWS": ""}
```

Nell'esempio seguente, l'istruzione utilizza gli elementi Effect, Principal, Action e Resource. In questo esempio viene illustrata un'istruzione completa dei criteri bucket che utilizza l'effetto "Consenti" per assegnare ai Principals, al gruppo admin federated-group/admin e al gruppo Finance federated-group/finance, le autorizzazioni per eseguire l'azione s3:ListBucket sul bucket denominato mybucket e l'azione s3:GetObject su tutti gli oggetti all'interno di tale bucket.

```
{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": [
          "arn:aws:iam::27233906934684427525:federated-group/admin",
          "arn:aws:iam::27233906934684427525:federated-group/finance"
        ]
      },
      "Action": [
        "s3:ListBucket",
        "s3:GetObject"
      ],
      "Resource": [
        "arn:aws:s3:::mybucket",
        "arn:aws:s3:::mybucket/*"
      ]
    }
  ]
}
```

Il criterio bucket ha un limite di dimensione di 20,480 byte e il criterio di gruppo ha un limite di dimensione di 5,120 byte.

Coerenza delle policy

Per impostazione predefinita, gli aggiornamenti apportati ai criteri di gruppo sono coerenti. Quando un criterio di gruppo diventa coerente, le modifiche possono richiedere altri 15 minuti, a causa della memorizzazione nella cache dei criteri. Per impostazione predefinita, tutti gli aggiornamenti apportati ai criteri bucket sono fortemente coerenti.

Come richiesto, è possibile modificare le garanzie di coerenza per gli aggiornamenti delle policy bucket. Ad esempio, è possibile rendere disponibile una modifica a un criterio bucket in caso di fuori servizio di un sito.

In questo caso, è possibile impostare l'`Consistency-Control`intestazione nella richiesta PutBucketPolicy oppure utilizzare la richiesta di coerenza PUT Bucket. Quando un criterio bucket diventa coerente, le modifiche possono richiedere altri 8 secondi per diventare effettive, a causa del caching delle policy.



Se si imposta la coerenza su un valore diverso per risolvere una situazione temporanea, assicurarsi di riportare l'impostazione del livello del bucket al valore originale al termine dell'operazione. In caso contrario, tutte le richieste bucket future utilizzeranno l'impostazione modificata.

Che cos'è la politica di sessione?

Una policy di sessione è una policy di accesso che limita temporaneamente le autorizzazioni disponibili durante una sessione specifica, ad esempio quando un utente assume l'incarico di un gruppo. Una policy di sessione può consentire solo un sottoinsieme di autorizzazioni e non può concedere autorizzazioni aggiuntive.

Il gruppo stesso potrebbe avere permessi più ampi.

Utilizzare ARN nelle dichiarazioni delle policy

Nelle dichiarazioni delle policy, l'ARN viene utilizzato negli elementi Principal e Resource.

- Utilizzare questa sintassi per specificare la risorsa S3 ARN:

```
arn:aws:s3:::bucket-name
arn:aws:s3:::bucket-name/object_key
```

- Utilizzare questa sintassi per specificare l'ARN della risorsa di identità (utenti e gruppi):

```
arn:aws:iam::account_id:root
arn:aws:iam::account_id:user/user_name
arn:aws:iam::account_id:group/group_name
arn:aws:iam::account_id:federated-user/user_name
arn:aws:iam::account_id:federated-group/group_name
```

Altre considerazioni:

- È possibile utilizzare l'asterisco (*) come carattere jolly per far corrispondere zero o più caratteri all'interno della chiave oggetto.
- I caratteri internazionali, che puoi specificare nella chiave dell'oggetto, devono essere codificati usando JSON UTF-8 o le 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 un criterio

Nelle istruzioni policy, è possibile utilizzare l'elemento Resource per specificare il bucket o l'oggetto per cui le autorizzazioni sono consentite o negate.

- Ogni dichiarazione di policy richiede un elemento Resource. In un criterio, le risorse sono indicate dall'elemento Resource, o in alternativa, NotResource per esclusione.
- Specificare le risorse con un ARN di risorsa S3. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/*"
```

- È inoltre possibile utilizzare le variabili dei criteri all'interno della chiave a oggetti. Ad esempio:

```
"Resource": "arn:aws:s3:::mybucket/home/${aws:username}/*"
```


- Il valore della risorsa può specificare un bucket che non esiste ancora quando viene creato un criterio di gruppo.

Specificare le entità in un criterio

Utilizzare l'elemento Principal per identificare l'account utente, gruppo o tenant a cui è consentito/negato l'accesso alla risorsa dall'istruzione policy.

- Ogni dichiarazione di policy in una policy bucket deve includere un elemento Principal. Le dichiarazioni di policy in una policy di gruppo non necessitano dell'elemento Principal perché il gruppo è considerato il principale.
- In un criterio, i principal sono indicati dall'elemento "Principal" o in alternativa "NotPrincipal" per l'esclusione.
- Le identità basate sull'account devono essere specificate utilizzando un ID o un ARN:

```
"Principal": { "AWS": "account_id"}  
"Principal": { "AWS": "identity_arn" }
```

- In questo esempio viene utilizzato l'ID account tenant 27233906934684427525, che include l'account root e tutti gli utenti dell'account:

```
"Principal": { "AWS": "27233906934684427525" }
```

- È possibile specificare solo l'account root:

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:root" }
```

- È possibile specificare un utente federato specifico ("Alex"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
user/Alex" }
```

- È possibile specificare uno specifico gruppo federato ("Manager"):

```
"Principal": { "AWS": "arn:aws:iam::27233906934684427525:federated-  
group/Managers" }
```

- È possibile specificare un'entità anonima:

```
"Principal": "*" 
```

- Per evitare ambiguità, è possibile utilizzare l'UUID utente invece del nome utente:

```
arn:aws:iam::27233906934684427525:user-uuid/de305d54-75b4-431b-adb2-eb6b9e546013
```

Ad esempio, supponiamo che Alex abbandoni l'organizzazione e che il nome utente `Alex` venga eliminato. Se un nuovo Alex entra a far parte dell'organizzazione e viene assegnato lo stesso `Alex` nome utente, il nuovo utente potrebbe inavvertitamente ereditare le autorizzazioni concesse all'utente originale.

- Il valore principale può specificare un nome di gruppo/utente che non esiste ancora quando viene creata una policy del bucket.

Specificare le autorizzazioni in un criterio

In un criterio, l'elemento Action viene utilizzato per consentire/negare le autorizzazioni a una risorsa. È possibile specificare una serie di autorizzazioni in un criterio, indicate dall'elemento "Action" o, in alternativa, "NotAction" per l'esclusione. Ciascuno di questi elementi viene associato a specifiche operazioni REST API S3.

Le tabelle elencano le autorizzazioni applicabili ai bucket e le autorizzazioni applicabili agli oggetti.



Amazon S3 ora utilizza l'autorizzazione `S3:PutReplicationConfiguration` per entrambe le azioni `PutBucketReplication` e `DeleteBucketReplication`. StorageGRID utilizza autorizzazioni separate per ciascuna azione, che corrispondono alla specifica originale di Amazon S3.



Un'eliminazione viene eseguita quando si utilizza un put per sovrascrivere un valore esistente.

Autorizzazioni applicabili ai bucket

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:CreateBucket	CreateBucket	Sì. Nota: Utilizzare solo nei criteri di gruppo.
s3:Deletebucket	DeleteBucket	
s3>DeleteBucketMetadataNotification	ELIMINA la configurazione di notifica dei metadati del bucket	Sì
s3>DeleteBucketPolicy	DeleteBucketPolicy	
s3>DeleteReplicationConfiguration	DeleteBucketReplication	Sì, separare le autorizzazioni per PUT ed DELETE
s3:GetBucketAcl	GetBucketAcl	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:GetBucketCompliance	OTTIENI compliance bucket (obsoleta)	Sì
s3:GetBucketConsistency	COERENZA del bucket	Sì
s3:GetBucketCORS	GetBucketCors	
s3:GetEncryptionConfiguration	GetBucketEncryption	
s3:GetBucketLastAccessTime	OTTIENI l'ultimo tempo di accesso a bucket	Sì
s3:GetBucketLocation	GetBucketLocation	
s3:GetBucketMetadataNotification	OTTIENI la configurazione della notifica dei metadati del bucket	Sì
s3:GetBucketNotification	GetBucketNotificationConfiguration	
s3:GetBucketObjectLockConfiguration	GetObjectLockConfiguration	
s3:GetBucketPolicy	GetBucketPolicy	
s3:GetBucketTagging	GetBucketTagging	
s3:GetBucketVersioning	GetBucketVersioning	
s3:GetLifecycleConfiguration	GetBucketLifecycleConfiguration	
s3:GetReplicationConfiguration	GetBucketReplication	
s3:ListAllMyBucket	- ListBucket - OTTIENI l'utilizzo dello storage	Sì, per OTTIENI utilizzo storage. Nota: Utilizzare solo nei criteri di gruppo.
s3:ListBucket	- GetObject - HeadBucket - HeadObject (oggetto intestazione) - ListObjects (oggetti elenco)	
s3:ListBucketMultipartUploads	ListMultipartUploads	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:ListBucketVersions	SCARICA le versioni di bucket	
s3:PutBucketCompliance	METTERE la compliance del bucket (obsoleta)	Sì
s3:PutBucketConsistency	METTI la coerenza del bucket	Sì
s3:PutBucketCORS	- DeleteBucketCors† - PutBucketCors	
s3:PutEncryptionConfiguration	- DeleteBucketEncryption - PutBucketEncryption	
s3:PutBucketLastAccessTime	TEMPO ULTIMO accesso bucket	Sì
s3:PutBucketMetadataNotification	INSERIRE la configurazione della notifica dei metadati del bucket	Sì
s3:PutBucketNotification	PutBucketNotificationConfiguration	
s3:PutBucketObjectLockConfiguration	- CreateBucket con l' `x-amz-bucket-object-lock-enabled: true` intestazione della richiesta (richiede anche l'autorizzazione S3:CreateBucket) - PutObjectLockConfiguration	
s3:PutBucketPolicy	PutBucketPolicy	
s3:PutBucketTagging	- DeleteBucketTagging† - PutBucketTagging	
s3:PutBucketVersioning	PutBucketVersioning	
s3:PutLifecycleConfiguration	- DeleteBucketLifecycle† - PutBucketLifecycleConfiguration	
s3:PutReplicationConfiguration	PutBucketReplication	Sì, separare le autorizzazioni per PUT ed DELETE

Autorizzazioni applicabili agli oggetti

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:AbortMultipartUpload	AbortMultipartUpload	
s3:BypassGovernanceRetention	- DeleteObject (Elimina oggetto) - DeleteObjects - PutObjectRetention	
s3>DeleteObject	- DeleteObject (Elimina oggetto) - DeleteObjects	
s3>DeleteObjectTagging	DeleteObjectTagging	
s3>DeleteObjectVersionTagging	DeleteObjectTagging (una versione specifica dell'oggetto)	
s3>DeleteObjectVersion	DeleteObject (una versione specifica dell'oggetto)	
s3:GetObject	- GetObject - HeadObject (oggetto intestazione) - SelectObjectContent	
s3:GetObjectAcl	GetObjectAcl	
s3:GetObjectLegalHold	GetObjectLegalHold	
s3:GetObjectRetention	GetObjectRetention	
s3:GetObjectTagging	GetObjectTagging	
s3:GetObjectVersionTagging	GetObjectTagging (una versione specifica dell'oggetto)	
s3:GetObjectVersion	GetObject (una versione specifica dell'oggetto)	
s3:ListMultipartUploadParts	ListParts	

Permessi	OPERAZIONI REST API S3	Personalizzato per StorageGRID
s3:PutObject	• Oggetto CopyObject • CompleteMultipartUpload • CreateMultipartUpload • PutObject • UploadPart • UploadPartCopy	
s3:PutObjectLegalHold	PutObjectLegalHold	
s3:PutObjectRetention	PutObjectRetention	
s3:PutObjectTagging	PutObjectTagging	
s3:PutObjectVersionTagging	PutObjectTagging (una versione specifica dell'oggetto)	
s3:PutOverwriteObject	• CompleteMultipartUpload • Oggetto CopyObject • DeleteObjectTagging • PutObject • PutObjectTagging	Sì
s3:RestoreObject (Riavvia oggetto)	RestoreObject	

Utilizza il permesso PutOverwriteObject

l'autorizzazione s3:PutOverwriteObject è un'autorizzazione StorageGRID personalizzata che si applica alle operazioni che creano o aggiornano oggetti. L'impostazione di questa autorizzazione determina se il client può sovrascrivere i dati di un oggetto, i metadati definiti dall'utente o il tagging degli oggetti S3.

Le impostazioni possibili per questa autorizzazione includono:

- **Allow:** Il client può sovrascrivere un oggetto. Questa è l'impostazione predefinita.
- **Nega:** Il client non può sovrascrivere un oggetto. Se impostata su Nega, l'autorizzazione PutOverwriteObject funziona come segue:
 - Se un oggetto esistente viene trovato nello stesso percorso:
 - I dati dell'oggetto, i metadati definiti dall'utente o il tag S3 non possono essere sovrascritti.
 - Tutte le operazioni di acquisizione in corso vengono annullate e viene restituito un errore.
 - Se è attivata la versione S3, l'impostazione Nega impedisce alle operazioni PutObjectTagging o DeleteObjectTagging di modificare il TagSet per un oggetto e le relative versioni non correnti.
 - Se non viene trovato un oggetto esistente, questa autorizzazione non ha effetto.

- Quando questa autorizzazione non è presente, l'effetto è lo stesso come se fosse impostata l'opzione "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 sovrascrive l'impostazione dell'autorizzazione PutOverwriteObject.

Specificare le condizioni in un criterio

Le condizioni definiscono quando una policy sarà in vigore. Le condizioni sono costituite da operatori e coppie chiave-valore.

Le condizioni utilizzano coppie chiave-valore per la valutazione. Un elemento Condition può contenere più condizioni e ciascuna condizione può contenere più coppie chiave-valore. Il blocco Condition utilizza il seguente formato:

```
Condition: {
  condition_type: {
    condition_key: condition_values
```

Nell'esempio seguente, la condizione ipaddress utilizza la chiave SourceIp Condition.

```
"Condition": {
  "IpAddress": {
    "aws:SourceIp": "54.240.143.0/24"
    ...
  },
  ...
```

Operatori delle condizioni supportati

Gli operatori delle condizioni sono classificati come segue:

- Stringa
- Numerico
- Booleano
- Indirizzo IP
- Controllo nullo

Condizionare gli operatori	Descrizione
StringEquals	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole).

Condizionare gli operatori	Descrizione
StringNotEquals	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole).
StringEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (ignora maiuscole/minuscole).
StringNotEqualsIgnoreCase	Confronta una chiave con un valore stringa in base alla corrispondenza negata (ignora maiuscole/minuscole).
StringLike	Confronta una chiave con un valore stringa in base alla corrispondenza esatta (distinzione tra maiuscole e minuscole). Può includere caratteri jolly * e ?.
StringNotLike	Confronta una chiave con un valore stringa in base alla corrispondenza negata (distinzione tra maiuscole e minuscole). Può includere caratteri jolly * e ?.
Valori numerici Equals	Confronta una chiave con un valore numerico in base alla corrispondenza esatta.
NumericNotEquals	Confronta una chiave con un valore numerico in base alla corrispondenza negata.
NumericGreaterThan	Confronta un dato con un valore numerico basato sulla corrispondenza "maggiore di".
NumericGreaterThanEquals	Confronta una chiave con un valore numerico basato sulla corrispondenza "maggiore o uguale".
NumericLessThan	Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di".
NumericLessThanEquals	Confronta una chiave con un valore numerico basato sulla corrispondenza "minore di o uguale".
Bool	Confronta una chiave con un valore booleano basato sulla corrispondenza "true o false".
Indirizzo IP	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP.
NotIpAddress	Confronta una chiave con un indirizzo IP o un intervallo di indirizzi IP in base alla corrispondenza negata.
Null	Controlla se è presente una chiave di condizione nel contesto della richiesta corrente.

Condizionare gli operatori	Descrizione
Se esiste	Aggiunto a qualsiasi operatore di condizione, eccetto la condizione Null, per verificare l'assenza di quella chiave di condizione. Restituisce TRUE se la chiave di condizione non è presente.

Chiavi di condizione supportate

Tasti Condition	Azioni	Descrizione
aws: Sourcelp	Operatori IP	Corrisponde all'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 Admin e sui nodi Gateway, questo viene confrontato con l'indirizzo IP a monte del servizio Load Balancer. Nota: Se viene utilizzato un bilanciatore di carico di terze parti non trasparente, il confronto viene effettuato con l'indirizzo IP di tale bilanciatore di carico. Qualsiasi X-Forwarded-For intestazione viene ignorata perché non è possibile accertarne la validità.
aws:nome utente	Risorsa/identità	Corrisponde al nome utente del mittente da cui è stata inviata la richiesta. Può essere utilizzato per operazioni su bucket o oggetti.
s3:delimitatore	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Confronta con il parametro delimitatore specificato in una richiesta ListObjects o ListObjectVersions.

Tasti Condition	Azioni	Descrizione
S3:ExistingObjectTag/<tag-key>	s3:DeleteObjectTagging s3:DeleteObjectVersionTagging s3:GetObject s3:GetObjectAcl 3:GetObjectTagging s3:GetObjectVersion s3:GetObjectVersionAcl s3:GetObjectVersionTagging S3:PutObjectAcl s3:PutObjectTagging S3:PutObjectVersionAcl s3:PutObjectVersionTagging	Richiede che l'oggetto esistente abbia la chiave e il valore del tag specifici.
s3: tasti max	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Confronta con il parametro max-keys specificato in una richiesta ListObjects o ListObjectVersions.
s3:modalità-blocco-oggetto	s3:PutObject	Confronta con il <code>object-lock-mode</code> espanso dall'intestazione della richiesta nelle richieste PutObject, CopyObject e CreateMultipartUpload.
s3:modalità-blocco-oggetto	s3:PutObjectRetention	Confronta con il <code>object-lock-mode</code> espanso dal corpo XML nella richiesta PutObjectRetention.
s3:giorni-rimanenti-conservazione-blocco-oggetto	s3:PutObject	Viene confrontato con la data di scadenza specificata nell' <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 rientrino nell'intervallo consentito per le seguenti richieste: • PutObject • Oggetto CopyObject • CreateMultipartUpload

Tasti Condition	Azioni	Descrizione
s3:giorni-rimanti-conservazione-blocco-oggetto	s3:PutObjectRetention	Viene confrontato con la data di scadenza specificata nella richiesta PutObjectRetention per garantire che rientri nell'intervallo consentito.
s3:prefisso	s3:ListBucket e. s3:autorizzazioni ListBucketVersions	Si confronta con il parametro prefisso specificato in una richiesta ListObjects o ListObjectVersions, oppure con la chiave specificata per GetObject o HeadObject.
S3:RequestObjectTag/<tag-key>	s3:PutObject s3:PutObjectTagging s3:PutObjectVersionTagging	Richiede una chiave e un valore di tag specifici quando la richiesta dell'oggetto include il tagging.
s3:x-amz-copy-source	s3:PutObject	Confronta con x-amz-copy-source espanso dall'intestazione della richiesta nelle richieste PutObject e UploadPartCopy.
algoritmo-cliente-di-crittografia-lato-server-s3:x-amz	s3:PutObject	Confronta con il sse-customer-algorithm o al copy-source-sse-customer-algorithm espanso dall'intestazione della richiesta nelle richieste PutObject, CopyObject, CreateMultipartUpload, UploadPart, UploadPartCopy e CompleteMultipartUpload.

Specificare le variabili in un criterio

È possibile utilizzare le variabili nei criteri per popolare le informazioni sui criteri quando sono disponibili. È possibile utilizzare le variabili dei criteri nell' `Resource` elemento e nei confronti delle stringhe nell' `Condition` elemento.

In questo esempio, la variabile `${aws:username}` fa parte dell'elemento Resource:

```
"Resource": "arn:aws:s3:::bucket-name/home/${aws:username}/*"
```

In questo esempio, la variabile `${aws:username}` fa parte del valore di condizione nel blocco di condizione:

```
"Condition": {
  "StringLike": {
    "s3:prefix": "${aws:username}/*"
    ...
  },
  ...
}
```

Variabile	Descrizione
<code>\${aws:SourceIp}</code>	Utilizza la chiave SourceIp come variabile fornita.
<code>\${aws:username}</code>	Utilizza la chiave Username come variabile fornita.
<code>\${s3:prefix}</code>	Utilizza la chiave di prefisso specifica del servizio come variabile fornita.
<code>\${s3:max-keys}</code>	Utilizza la chiave max-keys specifica del servizio come variabile fornita.
<code>\${*}</code>	Carattere speciale. Utilizza il carattere come carattere * letterale.
<code>\${?}</code>	Carattere speciale. Utilizza il carattere come carattere letterale ?.
<code>\${\$}</code>	Carattere speciale. Utilizza il carattere come carattere letterale.

Creare policy che richiedono una gestione speciale

A volte un criterio può concedere autorizzazioni pericolose per la sicurezza o pericolose per operazioni continue, come il blocco dell'utente root dell'account. L'implementazione dell'API REST di StorageGRID S3 è meno restrittiva durante la convalida delle policy rispetto ad Amazon, ma altrettanto rigorosa durante la valutazione delle policy.

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Negare automaticamente le autorizzazioni all'account root	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Negare automaticamente le autorizzazioni all'utente/gruppo	Gruppo	Valido e applicato	Stesso
Consenti a un gruppo di account esterno qualsiasi autorizzazione	Bucket	Principal non valido	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio

Descrizione della policy	Tipo di policy	Comportamento di Amazon	Comportamento di StorageGRID
Consentire a un account root esterno o a un utente qualsiasi autorizzazione	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) quando consentito da un criterio	Stesso
Consenti a tutti i permessi per tutte le azioni	Bucket	Valido, ma le autorizzazioni per tutte le operazioni dei criteri del bucket S3 restituiscono un errore 405 Method Not Allowed (metodo non consentito) per l'account root esterno e gli utenti	Stesso
Negare a Everyone le autorizzazioni per tutte le azioni	Bucket	Valido e applicato, ma l'account utente root conserva l'autorizzazione per tutte le operazioni di policy del bucket S3	Stesso
Principal è un utente o un gruppo inesistente	Bucket	Principal non valido	Valido
La risorsa è un bucket S3 inesistente	Gruppo	Valido	Stesso
Principal è un gruppo locale	Bucket	Principal non valido	Valido
Il criterio concede a un account non proprietario (inclusi gli account anonimi) le autorizzazioni per l'inserimento degli oggetti.	Bucket	Valido. Gli oggetti sono di proprietà dell'account creatore e la policy del bucket non si applica. L'account creatore deve concedere le autorizzazioni di accesso per l'oggetto utilizzando gli ACL dell'oggetto.	Valido. Gli oggetti sono di proprietà dell'account proprietario del bucket. Si applica la policy bucket.

Protezione WORM (Write-Once-Read-Many)

È possibile creare bucket WORM (write-once-Read-many) per proteggere i dati, i metadati degli oggetti definiti dall'utente e il tagging degli oggetti S3. I bucket WORM vengono configurati in modo da consentire la creazione di nuovi oggetti e impedire la sovrascrittura o l'eliminazione del contenuto esistente. Utilizzare uno degli approcci descritti di seguito.

Per garantire che le sovrascritture vengano sempre negate, è possibile:

- Da Grid Manager, vai su **Configurazione > Sicurezza > Impostazioni di sicurezza > Rete e oggetti** e seleziona la casella di controllo **Impedisci modifiche client**.
- Applicare le seguenti regole e criteri S3:
 - Aggiungere un'operazione di NEGAZIONE PutOverwriteObject al criterio S3.
 - Aggiungere un'operazione di NEGAZIONE DeleteObject al criterio S3.
 - Aggiungere un'operazione PutObject ALLOW al criterio S3.



Impostare DeleteObject su DENY in una policy S3 non impedisce a ILM di eliminare gli oggetti quando esiste una regola come "zero copie dopo 30 giorni".



Anche quando tutte queste regole e policy vengono applicate, non si proteggono dalle scritture simultanee (vedi situazione A). Si proteggono dalle sovrascritture sequenziali completate (vedere situazione B).

Situazione A: Scritture simultanee (non protette)

```
/mybucket/important.doc
PUT#1 ---> OK
PUT#2 -----> OK
```

Situazione B: Sovrascritture sequenziali completate (con protezione)

```
/mybucket/important.doc
PUT#1 -----> PUT#2 ---X (denied)
```

Informazioni correlate

- ["Modalità di gestione degli oggetti da parte delle regole ILM di StorageGRID"](#)
- ["Esempio di policy bucket"](#)
- ["Criteri di gruppo di esempio"](#)
- ["Esempio di policy di sessione"](#)
- ["Gestire gli oggetti con ILM"](#)
- ["Utilizzare un account tenant"](#)

Esempio di policy di sessione dell'API REST S3 di StorageGRID

Utilizzare l'esempio seguente per creare una policy di sessione StorageGRID .

Esempio: impostare una policy di sessione che consenta il recupero degli oggetti

In questo esempio, al principale della sessione è consentito solo recuperare oggetti da bucket1. Tutte le altre azioni sono implicitamente negate, ad eccezione delle azioni specifiche di StorageGRID, come l'utilizzo dell'autorizzazione `"s3:PutOverwriteObject"`. La policy di sessione può essere fornita come file JSON durante la chiamata all'API AssumeRole.

```
{
  "Statement": [
    {
      "Action": "s3:GetObject",
      "Effect": "Allow",
      "Resource": "arn:aws:s3:::bucket1/*"
    }
  ]
}
```

Esempi di policy bucket S3 REST API di StorageGRID

Utilizza gli esempi di questa sezione per creare policy di accesso StorageGRID per i bucket.

I criteri del bucket specificano le autorizzazioni di accesso per il bucket a cui è associata la policy. È possibile configurare un criterio bucket utilizzando l'API S3 PutBucketPolicy tramite uno dei seguenti strumenti:

- ["Manager tenant"](#).
- AWS CLI utilizzando il seguente comando (vedere la ["Operazioni sui bucket"](#)):

```
> aws s3api put-bucket-policy --bucket examplebucket --policy
file://policy.json
```

In StorageGRID, il Principal:

- `"Principal": ""` corrisponde a tutti, comprese le richieste anonime (non firmate)
- `"Principal": { "AWS": "" }` corrisponde a qualsiasi identità o utente autenticato (non corrisponde alle richieste anonime)
- Si applica solo alle bucket policy
- Il principal è l'account/gli account/gli utenti a cui vengono concesse o negate le autorizzazioni

Esempio: Consentire a tutti l'accesso in sola lettura a un bucket

In questo esempio, a tutti, incluso anonimo, è consentito elencare gli oggetti nel bucket ed eseguire operazioni GetObject su tutti gli oggetti nel bucket. Tutte le altre operazioni verranno negate. Si noti che questo criterio potrebbe non essere particolarmente utile perché nessuno, ad eccezione dell'account root, dispone delle autorizzazioni di scrittura nel bucket.

```
{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadOnlyAccess",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:GetObject", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ]
    }
  ]
}
```

Esempio: Consentire a tutti gli utenti di un account l'accesso completo e a tutti gli utenti di un altro account l'accesso in sola lettura a un bucket

In questo esempio, a tutti gli utenti di un account specificato è consentito l'accesso completo a un bucket, mentre a tutti gli utenti di un altro account specificato è consentito solo elencare il bucket ed eseguire operazioni GetObject sugli oggetti nel bucket che iniziano con il `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. La policy bucket si applica a questi oggetti.


```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "95390887230002558202"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:GetObject",
      "Resource": "arn:aws:s3:::examplebucket/shared/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "31181711887329436680"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::examplebucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "shared/*"
        }
      }
    }
  ]
}

```

Esempio: Consentire a tutti l'accesso in sola lettura a un bucket e l'accesso completo per gruppo specificato

In questo esempio, a tutti gli utenti, incluso 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 possono accedere completamente.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/Marketing"
      },
      "Action": "s3:*",
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Allow",
      "Principal": "*",
      "Action": ["s3:ListBucket", "s3:GetObject"],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Esempio: Consentire a tutti l'accesso in lettura e scrittura a un bucket se il client si trova nell'intervallo IP

In questo esempio, Everyone, incluso l'anonimato, è autorizzato a elencare il bucket ed eseguire qualsiasi operazione oggetto su tutti gli oggetti nel bucket, a condizione che le richieste provengano da un intervallo IP specificato (da 54.240.143.0 a 54.240.143.255, eccetto 54.240.143.188). Tutte le altre operazioni verranno rifiutate e tutte le richieste al di fuori dell'intervallo IP verranno rifiutate.

```

{
  "Statement": [
    {
      "Sid": "AllowEveryoneReadWriteAccessIfInSourceIpRange",
      "Effect": "Allow",
      "Principal": "*",
      "Action": [ "s3:*Object", "s3:ListBucket" ],
      "Resource":
[ "arn:aws:s3:::examplebucket", "arn:aws:s3:::examplebucket/*" ],
      "Condition": {
        "IpAddress": { "aws:SourceIp": "54.240.143.0/24" },
        "NotIpAddress": { "aws:SourceIp": "54.240.143.188" }
      }
    }
  ]
}

```

Esempio: Consentire l'accesso completo a un bucket esclusivamente da un utente federato specificato

In questo esempio, all'utente federato Alex è consentito l'accesso completo al `examplebucket` bucket e ai relativi oggetti. A tutti gli altri utenti, tra cui 'root', vengono esplicitamente negate tutte le operazioni. Si noti tuttavia che a 'root' non vengono mai negate le autorizzazioni per `put/get/DeleteBucketPolicy`.

```

{
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    },
    {
      "Effect": "Deny",
      "NotPrincipal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-user/Alex"
      },
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::examplebucket",
        "arn:aws:s3:::examplebucket/*"
      ]
    }
  ]
}

```

Esempio: Autorizzazione PutOverwriteObject

In questo esempio, l'`Deny` effetto di PutOverwriteObject e DeleteObject garantisce che nessuno possa sovrascrivere o eliminare i dati dell'oggetto, i metadati definiti dall'utente e l'etichettatura degli oggetti S3.

```

{
  "Statement": [
    {
      "Effect": "Deny",
      "Principal": "*",
      "Action": [
        "s3:PutOverwriteObject",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
      ],
      "Resource": "arn:aws:s3:::wormbucket/*"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::wormbucket"
    },
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::95390887230002558202:federated-
group/SomeGroup"
      },
      "Action": "s3:*",
      "Resource": "arn:aws:s3:::wormbucket/*"
    }
  ]
}

```

Esempi di criteri di gruppo dell'API REST S3 di StorageGRID

Utilizzare gli esempi di questa sezione per creare criteri di accesso StorageGRID per i gruppi.

I criteri di gruppo specificano le autorizzazioni di accesso per il gruppo a cui è associato il criterio. Non vi è alcun Principal elemento nella politica perché è implicita. I criteri di gruppo vengono configurati utilizzando il tenant Manager o l'API.

Esempio: Impostare i criteri di gruppo utilizzando Tenant Manager

Quando si aggiunge o si modifica un gruppo in Tenant Manager, è possibile selezionare una policy di gruppo per determinare quali autorizzazioni di accesso S3 avranno i membri di questo gruppo. Vedere ["Creare gruppi per un tenant S3"](#).

- **Nessun accesso S3:** Opzione predefinita. Gli utenti di questo gruppo non hanno accesso alle risorse S3, a meno che l'accesso non sia concesso con una policy bucket. Se si seleziona questa opzione, solo l'utente root avrà accesso alle risorse S3 per impostazione predefinita.
- **Accesso di sola lettura:** Gli utenti di questo gruppo hanno accesso di sola lettura alle risorse S3. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo di sola lettura. Impossibile modificare questa stringa.
- **Accesso completo:** Gli utenti di questo gruppo hanno accesso completo alle risorse S3, inclusi i bucket. Quando si seleziona questa opzione, nella casella di testo viene visualizzata la stringa JSON per un criterio di gruppo ad accesso completo. Impossibile modificare questa stringa.
- **Ransomware Mitigation:** Questa policy di esempio si applica a tutti i bucket per questo tenant. Gli utenti di questo gruppo possono eseguire azioni comuni, ma non possono eliminare in modo permanente gli oggetti dai bucket che hanno attivato la versione degli oggetti.

Gli utenti di tenant Manager che dispongono dell'autorizzazione Gestisci tutti i bucket possono eseguire l'override di questa policy di gruppo. Limitare l'autorizzazione Manage All bucket (Gestisci tutti i bucket) agli utenti attendibili e utilizzare l'autenticazione multifattore (MFA), se disponibile.

- **Personalizzato:** Agli utenti del gruppo vengono concesse le autorizzazioni specificate nella casella di testo.

Esempio: Consentire l'accesso completo del gruppo a tutti i bucket

In questo esempio, a tutti i membri del gruppo è consentito l'accesso completo a tutti i bucket di proprietà dell'account tenant, a meno che non sia esplicitamente negato dalla policy bucket.

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

Esempio: Consentire l'accesso di gruppo in sola lettura a tutti i bucket

In questo esempio, tutti i membri del gruppo hanno accesso in sola lettura alle risorse S3, a meno che non sia esplicitamente negato dalla policy del bucket. Ad esempio, gli utenti di questo gruppo possono elencare gli oggetti e leggere i dati degli oggetti, i metadati e i tag.

```

{
  "Statement": [
    {
      "Sid": "AllowGroupReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:GetObjectVersionTagging"
      ],
      "Resource": "arn:aws:s3:::*"
    }
  ]
}

```

Esempio: Consenti ai membri del gruppo di accedere completamente solo alla loro "cartella" in un bucket

In questo esempio, i membri del gruppo possono solo elencare e accedere alla propria cartella specifica (prefisso chiave) nel bucket specificato. Tenere presente che le autorizzazioni di accesso da altre policy di gruppo e la policy del bucket devono essere prese in considerazione quando si determina la privacy di queste cartelle.

```

{
  "Statement": [
    {
      "Sid": "AllowListBucketOfASpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:ListBucket",
      "Resource": "arn:aws:s3:::department-bucket",
      "Condition": {
        "StringLike": {
          "s3:prefix": "${aws:username}/*"
        }
      }
    },
    {
      "Sid": "AllowUserSpecificActionsOnlyInTheSpecificUserPrefix",
      "Effect": "Allow",
      "Action": "s3:*Object",
      "Resource": "arn:aws:s3:::department-bucket/${aws:username}/*"
    }
  ]
}

```

Operazioni S3 tracciate nei log di controllo StorageGRID

I messaggi di audit vengono generati dai servizi StorageGRID e memorizzati in file di log di testo. È possibile rivedere i messaggi di audit specifici per S3 nel registro di audit per ottenere dettagli sulle operazioni di bucket e oggetti.

Operazioni bucket registrate nei registri di audit

- CreateBucket
- DeleteBucket
- DeleteBucketPolicy
- DeleteBucketTagging
- DeleteObjects
- GetBucketLifecycleConfiguration
- GetBucketPolicy
- GetBucketTagging
- HeadBucket
- ListObjects (oggetti elenco)
- ListObjectVersions
- METTI la compliance del bucket

- PutBucketLifecycleConfiguration
- PutBucketPolicy
- PutBucketTagging
- PutBucketVersioning

Operazioni a oggetti registrate nei registri di audit

- CompleteMultipartUpload
- Oggetto CopyObject
- DeleteObject (Elimina oggetto)
- GetObject
- HeadObject (oggetto intestazione)
- PutObject
- RestoreObject
- SelectObject (oggetto)
- UploadPart (quando una regola ILM utilizza un'acquisizione bilanciata o rigorosa)
- UploadPartCopy (quando una regola ILM utilizza l'acquisizione bilanciata o rigorosa)

Informazioni correlate

- ["Accedere al file di log di audit"](#)
- ["Messaggi di audit di scrittura del client"](#)
- ["Messaggi di audit in lettura del client"](#)

Utilizza Swift REST API (fine del ciclo di vita)

Supporto Swift REST API in StorageGRID

Il supporto per l'API Swift è terminato e verrà rimosso in una versione futura.



I dettagli Swift sono stati rimossi da questa versione del sito della documentazione. Vedere ["StorageGRID 11,8: Utilizza l'API REST Swift"](#).

Monitorare e risolvere i problemi di un sistema StorageGRID

Monitorare il sistema StorageGRID

USA AutoSupport

Scopri AutoSupport in StorageGRID

La funzione AutoSupport consente a StorageGRID di inviare pacchetti di stato e integrità al supporto tecnico NetApp.

Utilizzando AutoSupport è possibile risolvere i problemi più velocemente. Il supporto tecnico può monitorare le esigenze di archiviazione del tuo sistema e aiutarti a stabilire se è necessario aggiungere nuovi nodi o siti. Facoltativamente, AutoSupport può inviare i pacchi a un'ulteriore destinazione.

StorageGRID dispone di due tipi di AutoSupport:

- **StorageGRID AutoSupport** segnala problemi di software StorageGRID. Attivato per impostazione predefinita quando si installa StorageGRID per la prima volta. È possibile ["Modificare la configurazione AutoSupport predefinita"](#), se necessario.



Se StorageGRID AutoSupport non è abilitato, viene visualizzato un messaggio 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 disattivato.

- **Hardware appliance AutoSupport** segnala problemi relativi all'appliance StorageGRID. È necessario ["Configura AutoSupport hardware su ogni appliance"](#).

Che cos'è Digital Advisor?

Active IQ Digital Advisor (noto anche come Digital Advisor) è basato sul cloud e sfrutta l'analisi predittiva e la conoscenza della community dalla base installata di NetApp. Le sue valutazioni continue del rischio, gli avvisi predittivi, le indicazioni prescrittive e le azioni automatizzate ti aiutano a prevenire i problemi prima che si verifichino, portando a un miglioramento dello stato di salute del sistema e a una maggiore disponibilità del sistema.

Devi abilitare AutoSupport se vuoi usare le dashboard e le funzionalità di Digital Advisor sul sito di supporto NetApp.

["Documentazione di Digital Advisor"](#)

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 AutoSupport + tempo di generazione + dimensione compressa AutoSupport + dimensione decompressa AutoSupport + tempo totale di raccolta (ms)	File di cronologia AutoSupport.
AUTOSUPPORT.XML	Nodo + protocollo per contattare il supporto + URL di supporto per HTTP/HTTPS + Indirizzo di supporto + Stato ondemand AutoSupport + URL server ondemand AutoSupport + intervallo di polling ondemand AutoSupport	File di stato AutoSupport. Fornisce i dettagli del protocollo utilizzato, dell'URL e dell'indirizzo del supporto tecnico, dell'intervallo di polling e di OnDemand AutoSupport, se attivato o disattivato.
BUCKET.XML	ID 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 + tempo ultimo accesso abilitato + Policy abilitato + Configurazione criterio + Notifiche abilitate + Configurazione Cloud Mirror abilitato + Configurazione Cloud Mirror + Ricerca abilitata + Configurazione controllo bucket abilitato + Configurazione bucket con tag + Configurazione bucket	Fornisce dettagli di configurazione e statistiche a livello di bucket. Esempi di configurazioni bucket includono servizi di piattaforma, conformità e coerenza dei bucket.

Nome del file	Campi	Descrizione
GRID-CONFIGURATIONS.XML	ID attributo + Nome attributo + valore + Indice + ID tabella + Nome tabella	File di informazioni sulla configurazione a livello di griglia. Contiene informazioni sui certificati Grid, lo spazio riservato ai metadati, le impostazioni di configurazione a livello di griglia (conformità, blocco degli oggetti S3, compressione degli oggetti, avvisi, configurazione syslog e ILM), i dettagli del profilo di erasure coding, il nome DNS e "Nome NMS".
GRID-SPEC.XML	Specifiche della griglia, XML non elaborato	Utilizzato per la configurazione e la distribuzione di StorageGRID. Contiene le specifiche della griglia, l'IP del server NTP, l'IP del server DNS, la topologia di rete e i profili hardware dei nodi.
GRID-TASKS.XML	Nodo + percorso servizio + ID attributo + nome attributo + valore + indice + ID tabella + nome tabella	File di stato delle attività della griglia (procedure di manutenzione). Fornisce i dettagli delle attività attive, terminate, completate, non riuscite e in sospeso della griglia.
GRID.JSON	Griglia + Revisione + versione software + Descrizione + licenza + password + DNS + NTP + Siti + nodi	Informazioni sulla griglia.
ILM-CONFIGURATION.XML	ID attributo + Nome attributo + valore + Indice + ID tabella + Nome tabella	Elenco degli attributi per le configurazioni ILM.
ILM-STATUS.XML	Nodo + percorso servizio + ID attributo + nome attributo + valore + indice + ID tabella + nome tabella	File di informazioni sulle metriche ILM. Contiene le velocità di valutazione ILM per ogni nodo e le metriche a livello di grid.
ILM.XML	XML raw ILM	File di criteri ILM attivo. Contiene dettagli sulle policy ILM attive, come ID del pool di storage, comportamento di acquisizione, filtri, regole e descrizione.
LOG.TGZ	n/a	File di registro scaricabile. Contiene <code>bcast-err.log</code> e <code>servermanager.log</code> da ciascun nodo.

Nome del file	Campi	Descrizione
MANIFEST.XML	Ordine di raccolta + nome file contenuto AutoSupport per questi dati + Descrizione di questo elemento dati + numero di byte raccolti + tempo impiegato nella 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	Raggruppa le entità di servizio in " Albero NMS ". Fornisce dettagli sulla topologia della griglia. Il nodo può essere determinato in base ai servizi in esecuzione sul nodo.
OBJECTS-STATUS.XML	Nodo + percorso servizio + ID attributo + nome attributo + valore + indice + ID tabella + nome tabella	Stato dell'oggetto, inclusi lo stato della scansione in background, il trasferimento attivo, la velocità di trasferimento, i trasferimenti totali, la velocità di eliminazione, i frammenti corrotti, gli oggetti persi, gli oggetti mancanti, il tentativo di riparazione, la velocità di scansione, il periodo di scansione stimato e lo stato di completamento della riparazione.
SERVER-STATUS.XML	Nodo + percorso servizio + ID attributo + nome attributo + valore + indice + ID tabella + nome tabella	Configurazioni server Contiene questi dettagli per ogni nodo: Tipo di piattaforma, sistema operativo, memoria installata, memoria disponibile, connettività storage, numero di serie dello chassis dell'appliance di storage, numero di dischi guasti dello storage controller, temperatura dello chassis del controller di calcolo, hardware di calcolo, numero di serie del controller di calcolo, alimentatore, dimensioni dei dischi e tipo di disco.
SERVICE-STATUS.XML	Nodo + percorso 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 riparazione segmento, durata lavoro di riparazione, riavvii processo automatici e terminazione processo automatica.
STORAGE-GRADE.XML	ID grado storage + Nome grado storage + ID nodo storage + percorso del nodo storage	File di definizioni di livello di archiviazione per ogni nodo di archiviazione.

Nome del file	Campi	Descrizione
SUMMARY-ATTRIBUTES.XML	OID gruppo + percorso gruppo + ID attributo riepilogo + nome attributo riepilogo + valore + indice + ID tabella + nome tabella	Dati di stato del sistema di alto livello che riassumono le informazioni sull'utilizzo di StorageGRID. Fornisce dettagli quali nome della griglia, nomi dei siti, numero di nodi storage per grid e per sito, tipo di licenza, capacità e utilizzo della licenza, termini del supporto software e dettagli sulle operazioni di S3.
SYSTEM-ALERTS.XML	Nome + gravità + Nome nodo + Stato avviso + Nome sito + tempo di attivazione avviso + tempo di risoluzione avviso + ID regola + ID nodo + ID sito + tacitato + altre annotazioni + altre etichette	Avvisi di sistema correnti che indicano potenziali problemi nel sistema StorageGRID.
USERAGENTS.XML	Agente utente + numero di giorni + richieste HTTP totali + byte totali acquisiti + byte totali recuperati + richieste PUT + richieste GET + richieste DELETE + richieste HEAD + richieste POST + richieste OPZIONI + tempo medio richiesta (ms) + tempo medio richiesta PUT (ms) + tempo medio richiesta GET (ms) + tempo medio richiesta ELIMINAZIONE (ms) + tempo medio richiesta HEAD (ms) + tempo medio richiesta POST (ms) + tempo medio richiesta OPZIONI (ms)	Statistiche basate sugli agenti utente dell'applicazione. Ad esempio, il numero di operazioni PUT/GET/DELETE/HEAD per agente utente e la dimensione totale dei byte di ciascuna operazione.
X-HEADER-DATA	X-NetApp-asup-generated-on + X-NetApp-asup-hostname + X-NetApp-asup-os-version + X-NetApp-asup-serial-num + X-NetApp-asup-subject + X-NetApp-asup-system-id + X-NetApp-asup-model-name +	Dati di intestazione AutoSupport.

Configura AutoSupport in StorageGRID

La funzionalità AutoSupport consente al tuo sistema StorageGRID di inviare periodicamente, e in risposta a eventi specifici, messaggi sullo stato di salute e di funzionamento al supporto tecnico, permettendo così un monitoraggio e una risoluzione dei problemi proattivi. StorageGRID AutoSupport consente anche l'utilizzo di Digital

Advisor per raccomandazioni predittive.

Per impostazione predefinita, le funzionalità AutoSupport settimanali e basate su eventi sono abilitate per i sistemi StorageGRID basati su software quando installi per la prima volta StorageGRID. Tuttavia, devi [Configurare l'AutoSupport dell'hardware](#) su ciascun appliance. Se necessario, puoi modificare la configurazione AutoSupport.



Se vuoi modificare la configurazione di StorageGRID AutoSupport, apporta le modifiche solo sul nodo Admin primario.

Prima di iniziare

- Hai effettuato l'accesso al Grid Manager sul nodo Admin primario utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).
- Se userai HTTPS per inviare i pacchetti AutoSupport, hai fornito l'accesso a Internet outbound al nodo di amministrazione primario, direttamente o ["utilizzando un server proxy"](#) (le connessioni in entrata non sono necessarie).
- Se selezioni HTTP nella pagina AutoSupport di StorageGRID, devi ["configurato un server proxy"](#) inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiuteranno i pacchetti inviati tramite HTTP.
- Se utilizzerai SMTP come protocollo per i pacchetti AutoSupport, avrai ["hai configurato un server di posta elettronica"](#).

A proposito di questa attività

È possibile utilizzare qualsiasi combinazione delle seguenti opzioni per inviare i pacchetti AutoSupport al supporto tecnico:

- **Settimanale:** Invia automaticamente i pacchetti AutoSupport una volta alla settimana. Impostazione predefinita: Enabled (attivato).
- **Evento attivato:** Invia automaticamente pacchetti AutoSupport ogni ora o quando si verificano eventi di sistema significativi. Impostazione predefinita: Enabled (attivato).
- **Su richiesta:** Consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente i pacchetti AutoSupport, il che è utile quando stanno lavorando attivamente a un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disattivata.
- **Attivato dall'utente:** Inviare manualmente i pacchetti AutoSupport in qualsiasi momento.
- **Raccolta dei registri:** ["raccolgere manualmente i file di registro e i dati di sistema e inviare un pacchetto AutoSupport"](#) .

Configura AutoSupport

Per modificare la configurazione predefinita di installazione di AutoSupport o per configurare l'hardware AutoSupport su ciascun appliance StorageGRID:

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare il protocollo che si desidera utilizzare per inviare pacchetti AutoSupport.
 - **HTTPS:** Impostazione predefinita e consigliata per le nuove installazioni. Questo protocollo utilizza la porta 443. Se si desidera [Attivare la funzione AutoSupport on Demand](#), è necessario utilizzare HTTPS.
 - **HTTP:** Se selezioni HTTP, devi ["configurare un proxy server"](#) 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**: Utilizza questa opzione se vuoi che i pacchetti AutoSupport vengano inviati via e-mail. Devi prima ["configurare un server di posta elettronica"](#).

Il protocollo che imposti viene utilizzato per inviare tutti i pacchetti AutoSupport tranne AutoSupport on Demand, che richiede il protocollo HTTPS.

3. Se è stato selezionato **HTTPS**, selezionare se utilizzare un certificato di supporto NetApp (certificato TLS) per proteggere la connessione al server del supporto tecnico.
 - **Verify certificate** (verifica certificato*) (impostazione predefinita): Garantisce che la trasmissione dei pacchetti AutoSupport sia sicura. Il certificato di supporto NetApp è già installato con il software StorageGRID.
 - **Non verificare il certificato**: Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.
4. Se hai selezionato **SMTP**, usa il campo **Mittente** per inserire l'indirizzo del server di posta elettronica che hai configurato in precedenza.
5. Selezionare **Salva**. Tutti i pacchetti settimanali, attivati dall'utente e attivati da eventi vengono inviati utilizzando il protocollo selezionato.

Disattiva AutoSupport settimanale

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport all'assistenza tecnica una volta alla settimana.

Per determinare quando verrà inviato il pacchetto settimanale AutoSupport, andare alla scheda **AutoSupport > Results**. Nella sezione **AutoSupport settimanale**, osservare il valore per **ora pianificata successiva**.

È possibile disattivare l'invio automatico di pacchetti AutoSupport settimanali in qualsiasi momento.

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport* > Impostazioni**.
2. Deselezionare la casella di controllo **Enable Weekly AutoSupport** (Abilita aggiornamento settimanale).
3. Selezionare **Salva**.

Disattiva AutoSupport attivato dagli eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport all'assistenza tecnica ogni ora.

È possibile disattivare AutoSupport attivato da eventi in qualsiasi momento.

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport* > Impostazioni**.
2. Deselezionare la casella di controllo **attiva AutoSupport attivato da eventi**.
3. Selezionare **Salva**.

Attiva AutoSupport on Demand

AutoSupport on Demand può aiutare a risolvere i problemi sui quali il supporto tecnico sta lavorando

attivamente.

Per impostazione predefinita, AutoSupport on Demand è disattivato. L'attivazione di questa funzione consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente i pacchetti AutoSupport. Il supporto tecnico può anche impostare l'intervallo di tempo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può attivare o disattivare AutoSupport on Demand.

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare **HTTPS** per il protocollo.
3. Selezionare la casella di controllo **Enable Weekly AutoSupport** (Abilita aggiornamento settimanale).
4. Selezionare la casella di controllo **attiva AutoSupport su richiesta**.
5. Selezionare **Salva**.

AutoSupport on Demand è attivato e il supporto tecnico può inviare richieste AutoSupport on Demand a StorageGRID.

Disattiva i controlli per gli aggiornamenti software

Per impostazione predefinita, StorageGRID contatta NetApp per determinare se sono disponibili aggiornamenti software per il sistema. Se è disponibile una correzione rapida StorageGRID o una nuova versione, la nuova versione viene visualizzata nella pagina aggiornamento StorageGRID.

Se necessario, è possibile disattivare la verifica degli aggiornamenti software. Ad esempio, se il sistema non dispone di accesso WAN, disattivare il controllo per evitare errori di download.

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport* > Impostazioni**.
2. Deselezionare la casella di controllo **Controlla aggiornamenti software**.
3. Selezionare **Salva**.

Aggiungere una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, i pacchetti di stato e di integrità vengono inviati al supporto tecnico. È possibile specificare una destinazione aggiuntiva per tutti i pacchetti AutoSupport.

Per verificare o modificare il protocollo utilizzato per inviare i pacchetti AutoSupport, consulta le istruzioni per [configura AutoSupport](#).



Non è possibile utilizzare il protocollo SMTP per inviare pacchetti AutoSupport a una destinazione aggiuntiva.

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport* > Impostazioni**.
2. Selezionare **attiva destinazione AutoSupport aggiuntiva**.
3. Specificare quanto segue:

Nome host

Il nome host del server o l'indirizzo IP di un server di destinazione AutoSupport aggiuntivo.



È possibile inserire solo una destinazione aggiuntiva.

Porta

Porta utilizzata per connettersi a un server di destinazione AutoSupport aggiuntivo. L'impostazione predefinita è la porta 80 per HTTP o la porta 443 per HTTPS.

Convalida del certificato

Se viene utilizzato un certificato TLS per proteggere la connessione alla destinazione aggiuntiva.

- Selezionare **verifica certificato** per utilizzare la convalida del certificato.
- Selezionare **non verificare il certificato** per inviare i pacchetti AutoSupport senza la convalida del certificato.

Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

4. Se è stato selezionato **verifica certificato**, procedere come segue:

- a. Individuare la posizione del certificato CA.
- b. Caricare il file del certificato CA.

Vengono visualizzati i metadati del certificato CA.

5. Selezionare **Salva**.

Tutti i futuri pacchetti AutoSupport settimanali, attivati da eventi e attivati dall'utente verranno inviati alla destinazione aggiuntiva.

Configurazione di AutoSupport per le appliance

AutoSupport per appliance segnala problemi di hardware StorageGRID e StorageGRID AutoSupport segnala problemi di software StorageGRID, con una sola eccezione: Per SGF6112, StorageGRID AutoSupport segnala problemi di hardware e software. È necessario configurare AutoSupport su ogni appliance, ad eccezione di SGF6112, che non richiede configurazione aggiuntiva. AutoSupport viene implementato in maniera differente per le appliance di servizi e di storage.

Puoi utilizzare SANtricity per abilitare AutoSupport per ciascuna appliance di storage. È possibile configurare SANtricity AutoSupport durante la configurazione iniziale dell'appliance o dopo l'installazione di un'appliance:

- Per gli apparecchi SG6000 e SG5700, ["Configurare AutoSupport in Gestore di sistema di SANtricity"](#)

AutoSupport package dagli appliance E-Series possono essere inclusi in StorageGRID AutoSupport se configuri la consegna di AutoSupport tramite proxy in ["Gestore di sistema di SANtricity"](#).

StorageGRID AutoSupport non segnala problemi di hardware, ad esempio errori DIMM o HIC (host Interface Card). Tuttavia, alcuni guasti dei componenti potrebbero attivare ["avvisi hardware"](#). Per le appliance StorageGRID con un controller di gestione baseboard (BMC) è possibile configurare trap e-mail e SNMP per segnalare errori hardware:

- ["Impostare le notifiche e-mail per gli avvisi BMC"](#)

- ["Configurare le impostazioni SNMP per BMC"](#)

Informazioni correlate

- ["Porte utilizzate per le comunicazioni esterne"](#)
- ["Supporto NetApp"](#)

Avvia manualmente un pacchetto AutoSupport in StorageGRID

Per assistere il supporto tecnico nella risoluzione dei problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai l'autorizzazione di accesso Root o di altra configurazione della griglia.

Fasi

1. Selezionare **Supporto > Strumenti > * AutoSupport***.
2. Nella scheda **azioni**, selezionare **Invia AutoSupport** attivato dall'utente.

StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp . Se il tentativo ha esito positivo, i valori **Risultato più recente** e **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 .

3. Dopo 1 minuto, aggiorna la pagina AutoSupport nel tuo browser per accedere ai risultati più recenti.



Inoltre, puoi ["raccolgere file di registro e dati di sistema più estes"](#) e inviarli al sito di supporto NetApp .

Come StorageGRID gestisce gli errori dei pacchetti AutoSupport

Esamina l'elenco delle azioni che StorageGRID intraprende se un tentativo di invio di un pacchetto AutoSupport fallisce.

StorageGRID esegue azioni diverse a seconda del tipo di AutoSupport package. Puoi controllare lo stato dei pacchetti AutoSupport selezionando **Support > Tools > AutoSupport > Results**.

Quando il pacchetto AutoSupport non riesce a inviare, viene visualizzato "non riuscito" nella scheda **risultati** della pagina **AutoSupport**.



Se hai configurato un proxy server per inoltrare i pacchetti AutoSupport a NetApp, ["verificare che le impostazioni di configurazione del server proxy siano corrette"](#).

Errore settimanale del pacchetto AutoSupport

Se un pacchetto AutoSupport settimanale non viene inviato, il sistema StorageGRID esegue le seguenti operazioni:

1. Aggiorna l'attributo dei risultati più recenti in Riprova.
2. Tenta di inviare nuovamente il pacchetto AutoSupport 15 volte ogni quattro minuti per un'ora.

3. Dopo un'ora di errori di invio, aggiorna l'attributo dei risultati più recenti su non riuscito.
4. Tenta di inviare nuovamente un pacchetto AutoSupport all'ora pianificata successiva.
5. Mantiene la normale pianificazione AutoSupport se il pacchetto non riesce perché il servizio NMS non è disponibile e se un pacchetto viene inviato prima del termine di sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un pacchetto AutoSupport se non è stato inviato per sette giorni o più.

Errore del pacchetto AutoSupport attivato dall'utente o dagli eventi

Se un pacchetto AutoSupport attivato dall'utente o da un evento non riesce a inviare, il sistema StorageGRID esegue le seguenti operazioni:

1. Visualizza un messaggio di errore se l'errore è noto. Ad esempio, se un utente seleziona il protocollo SMTP senza fornire le 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 pacchetto.
3. Registra l'errore in `nms.log`.

Se si verifica un errore e il protocollo selezionato è SMTP, sulla 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.`

Informazioni su ["configurare le impostazioni del server di posta elettronica"](#).

Correggere un errore del pacchetto AutoSupport

Se si verifica un errore e il protocollo selezionato è SMTP, verifica che il server di posta elettronica del sistema StorageGRID sia configurato correttamente e che il tuo server di posta elettronica sia in esecuzione. Potrebbe apparire il seguente messaggio di errore nella pagina AutoSupport: i pacchetti AutoSupport non possono essere inviati tramite il protocollo SMTP a causa di impostazioni errate nella pagina E-mail Server.

Invio dei pacchetti e-Series AutoSupport tramite StorageGRID

Puoi inviare pacchetti AutoSupport di e-Series SANtricity System Manager al supporto tecnico tramite un nodo amministrativo StorageGRID piuttosto che la porta di gestione dell'appliance di storage.

Per ulteriori informazioni sull'utilizzo di AutoSupport con appliance e-Series, consulta ["AutoSupport hardware e-Series"](#).

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Tu hai il ["Autorizzazione di accesso root o amministratore dell'appliance di storage"](#).
- Hai configurato SANtricity AutoSupport:
 - Per gli apparecchi SG6000 e SG5700, ["Configurare AutoSupport in Gestore di sistema di SANtricity"](#)



È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

A proposito di questa attività

I pacchetti e-Series AutoSupport contengono dettagli sull'hardware di storage e sono più specifici degli altri pacchetti AutoSupport inviati dal sistema StorageGRID.

È possibile configurare un indirizzo speciale del server proxy in Gestione di sistema SANtricity per trasmettere pacchetti AutoSupport tramite un nodo amministrativo StorageGRID senza l'utilizzo della porta di gestione dell'appliance. I pacchetti AutoSupport trasmessi in questo modo vengono inviati da ["Nodo Admin mittente preferito"](#) e utilizzano quelli ["impostazioni proxy amministratore"](#) configurati in Gestore griglia.

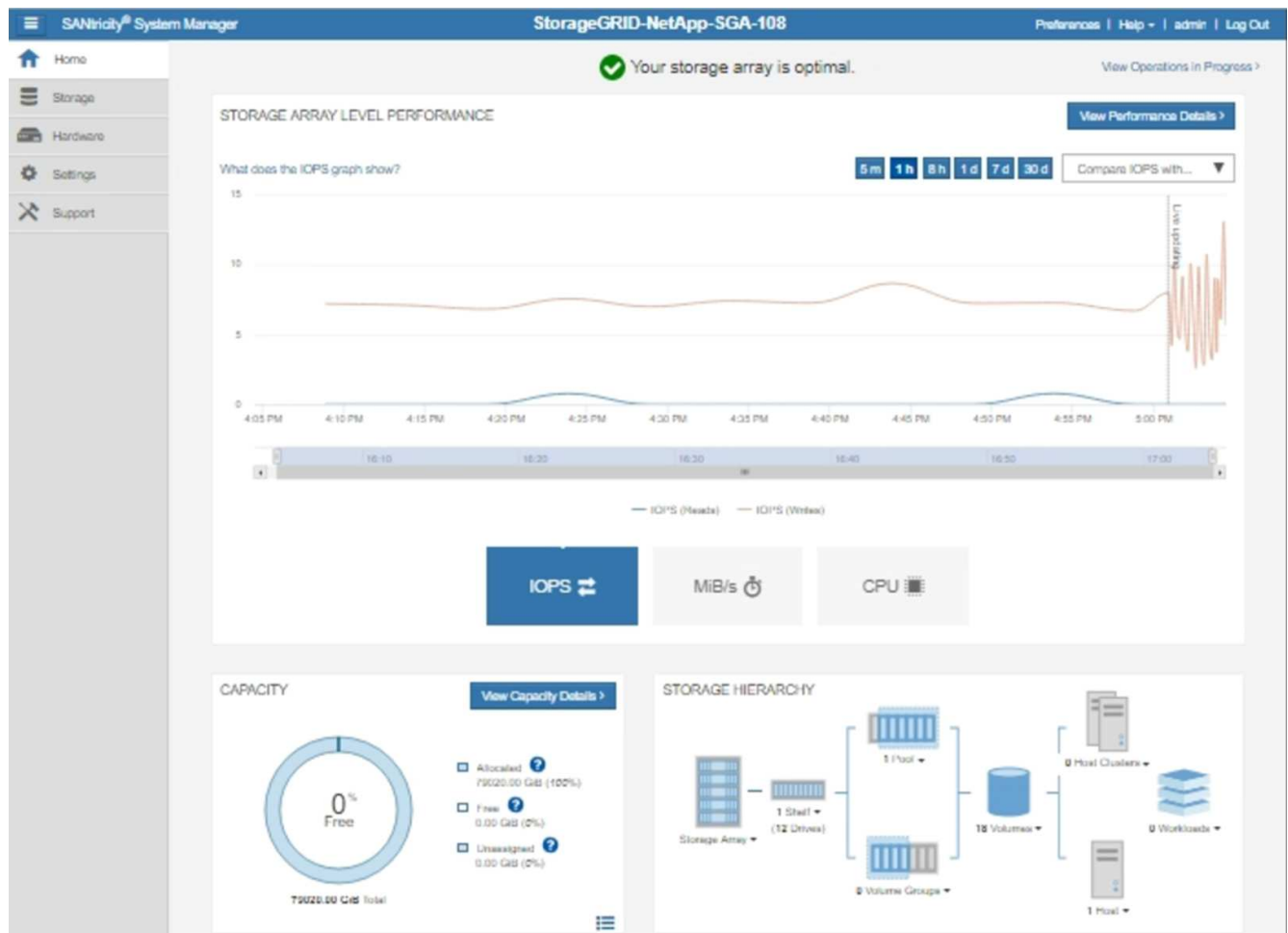


Questa procedura si applica solo alla configurazione di un server proxy StorageGRID per i pacchetti AutoSupport e-Series. Per ulteriori informazioni sulla configurazione di e-Series AutoSupport, consultare ["Documentazione NetApp e-Series e SANtricity"](#).

Fasi

1. Nel Grid Manager, seleziona **Nodi**.
2. Dall'elenco dei nodi a sinistra, selezionare il nodo dell'appliance di storage che si desidera configurare.
3. Selezionare **Gestore di sistema SANtricity**.

Viene visualizzata la home page di Gestore di sistema di SANtricity.



4. Selezionare **Supporto > Centro supporto > * AutoSupport***.

Viene visualizzata la pagina AutoSupport Operations.

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 erogazione AutoSupport**.

Viene visualizzata la pagina Configura metodo di erogazione AutoSupport.

Configure AutoSupport Delivery Method ✕

Select AutoSupport dispatch delivery method...

☒ HTTPS
☐ HTTP
☐ Email

HTTPS delivery settings Show destination address

Connect to support team...

☐ Directly ?
☒ via Proxy server ?

Host address ?

tunnel-host

Port number ?

10225

☐ My proxy server requires authentication
☐ via Proxy auto-configuration script (PAC) ?

Save
Test Configuration
Cancel

6. Selezionare **HTTPS** per il metodo di consegna.



Il certificato che abilita HTTPS è preinstallato.

7. Selezionare **via Proxy server**.

8. Immettere `tunnel-host` per l'indirizzo **host**.

`tunnel-host` È l'indirizzo speciale che consente di utilizzare un nodo amministrativo per inviare pacchetti AutoSupport e-Series.

9. Immettere `10225` per il **numero porta**.

`10225` È il numero di porta sul server proxy StorageGRID che riceve i pacchetti AutoSupport dal controller e-Series dell'appliance.

10. Selezionare **verifica configurazione** per verificare l'instradamento e la configurazione del server proxy AutoSupport.

Se corretto, viene visualizzato un messaggio in un banner verde: "La configurazione AutoSupport è stata verificata."

Se il test ha esito negativo, viene visualizzato un messaggio di errore su un banner rosso. Verificare le impostazioni DNS e la rete di StorageGRID, assicurarsi che l' "[Nodo Admin mittente preferito](#)" possa connettersi al sito di supporto NetApp ed eseguire nuovamente il test.

11. Selezionare **Salva**.

La configurazione viene salvata e viene visualizzato un messaggio di conferma: "Il metodo di consegna AutoSupport è stato configurato".

Monitorare un sistema StorageGRID

Monitorare regolarmente il sistema StorageGRID per assicurarsi che funzioni come previsto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[autorizzazioni di accesso specifiche](#)".



Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).

A proposito di questa attività

Queste istruzioni descrivono come:

- "[Visualizzare e gestire la dashboard](#)"
- "[Visualizzare la pagina nodi](#)"
- "[Monitorare regolarmente questi aspetti del sistema:](#)"
 - "[Stato del sistema](#)"
 - "[Capacità dello storage](#)"
 - "[Gestione del ciclo di vita delle informazioni](#)"
 - "[Risorse di rete e di sistema](#)"
 - "[Attività del tenant](#)"
 - "[Operazioni di bilanciamento del carico](#)"
 - "[Connessioni a federazione di griglie](#)"
- "Gestire gli avvisi"
- "[Visualizzare i file di registro](#)"
- "[Configurare la gestione dei log e il server syslog esterno](#)"
- "[Utilizzare un server syslog esterno](#)" per raccogliere le informazioni di controllo
- "[Utilizzare SNMP per il monitoraggio](#)"
- "[Modifica la priorità di I/O](#)" per modificare le priorità relative per le operazioni di I/O

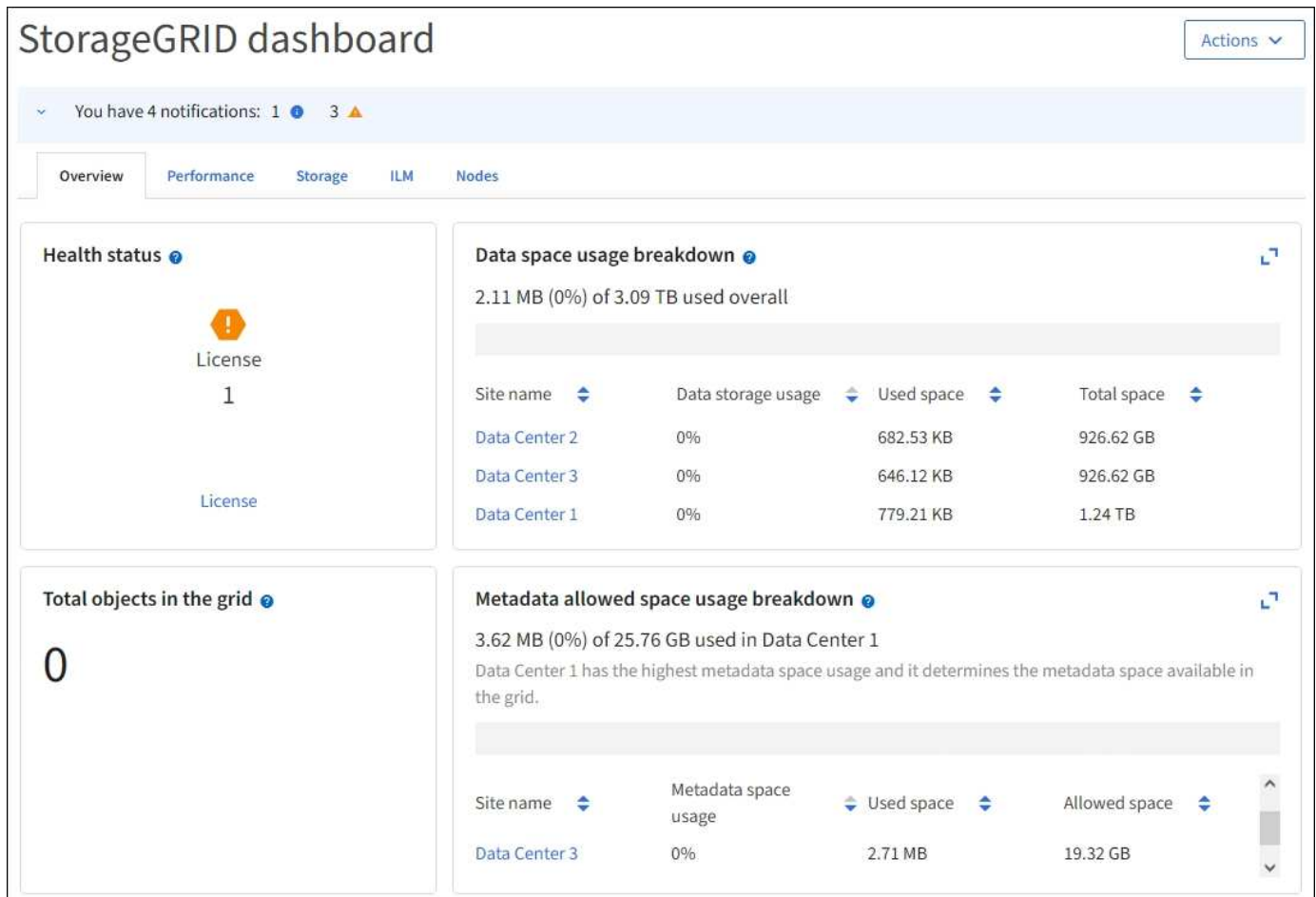
Visualizza e gestisci la dashboard in StorageGRID

È possibile utilizzare la dashboard per monitorare le attività del sistema in un colpo d'occhio. È possibile creare dashboard personalizzati per monitorare l'implementazione di StorageGRID.



Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).

Il dashboard potrebbe essere diverso a seconda della configurazione del sistema.



Visualizza la dashboard

La dashboard è costituita da schede che contengono informazioni specifiche sul sistema StorageGRID. Ciascuna scheda contiene le categorie di informazioni visualizzate sulle schede.

È possibile utilizzare la dashboard fornita con il sistema così com'è. Inoltre, è possibile creare dashboard personalizzati contenenti solo schede e schede rilevanti per il monitoraggio dell'implementazione di StorageGRID.

Le schede della dashboard fornite dal sistema contengono schede con i seguenti tipi di informazioni:

Scheda sulla dashboard fornita dal sistema	Contiene
Panoramica	Informazioni generali sulla griglia, ad esempio avvisi attivi, utilizzo dello spazio e oggetti totali nella griglia.
Performance	Utilizzo dello spazio, storage utilizzato nel tempo, S3 operazioni, durata della richiesta, tasso di errore.
Storage	Utilizzo delle quote dei tenant e dello spazio logico. Previsioni di utilizzo dello spazio per i dati e i metadati dell'utente.
ILM	Coda di gestione del ciclo di vita delle informazioni e tasso di valutazione.
Nodi	Utilizzo di CPU, dati e memoria per nodo. S3 operazioni per nodo. Distribuzione da nodo a sito.

Alcune schede possono essere ingrandite per una visualizzazione più agevole. Seleziona l'icona di ingrandimento  nell'angolo in alto a destra della scheda. Per chiudere una scheda ingrandita, seleziona l'icona di riduzione  oppure seleziona **Close**.

Gestire i dashboard

Se si dispone dell'accesso root (vedere "[Autorizzazioni del gruppo di amministrazione](#)"), è possibile eseguire le seguenti attività di gestione per i dashboard:

- Crea una dashboard personalizzata da zero. È possibile utilizzare dashboard personalizzati per controllare quali informazioni StorageGRID vengono visualizzate e come sono organizzate.
- Clonare una dashboard per creare dashboard personalizzati.
- Impostare una dashboard attiva per un utente. La dashboard attiva può essere la dashboard fornita dal sistema o una dashboard personalizzata.
- Impostare una dashboard predefinita, che è quella visualizzata da tutti gli utenti, a meno che non attivino la propria dashboard.
- Modificare il nome di una dashboard.
- Modificare una dashboard per aggiungere o rimuovere schede e schede. È possibile avere un minimo di 1 e un massimo di 20 schede.
- Rimuovere una dashboard.



Se si dispone di altre autorizzazioni oltre all'accesso root, è possibile impostare solo una dashboard attiva.

Per gestire i dashboard, selezionare **azioni > Gestisci dashboard**.



Configurare i dashboard

Per creare una nuova dashboard clonando la dashboard attiva, selezionare **azioni** > **Clona dashboard attiva**.

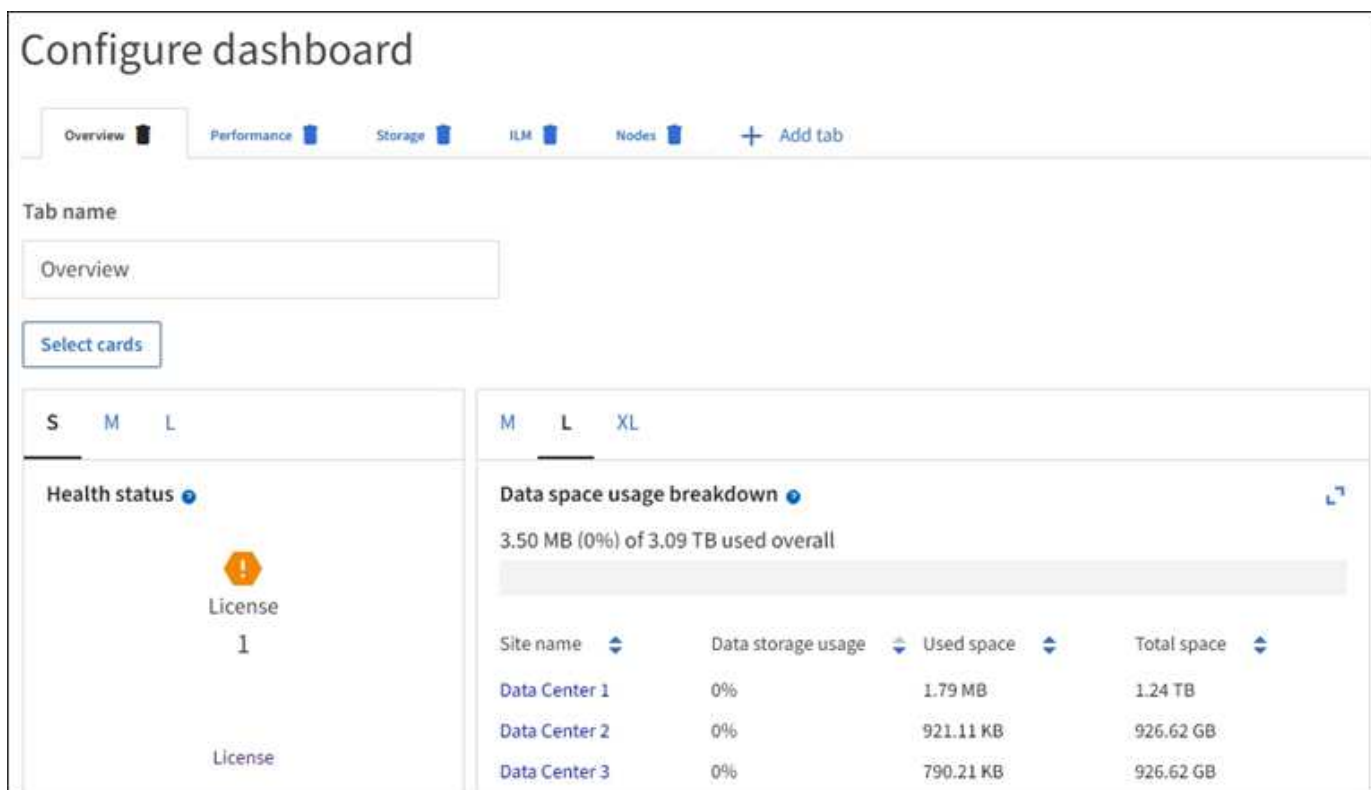
Per modificare o clonare una dashboard esistente, selezionare **azioni** > **Gestisci dashboard**.



La dashboard fornita dal sistema non può essere modificata o rimossa.

Durante la configurazione di una dashboard, è possibile:

- Aggiungere o rimuovere le schede
- Rinominare le schede e assegnarle nomi univoci
- Aggiungere, rimuovere o riorganizzare (trascinare) le schede per ciascuna scheda
- Selezionare le dimensioni delle singole schede selezionando **S**, **M**, **L** o **XL** nella parte superiore della scheda



Visualizzare la pagina nodi

Visualizza la pagina dei nodi StorageGRID

Quando hai bisogno di informazioni più dettagliate sul tuo sistema StorageGRID rispetto

a quelle fornite dalla dashboard, puoi utilizzare la pagina Nodes per visualizzare le metriche per l'intera griglia, ogni sito nella griglia e ogni nodo di un sito.

La tabella Nodes (nodi) elenca informazioni riepilogative per l'intera griglia, ciascun sito e ciascun nodo. Se un nodo è disconnesso o presenta un avviso attivo, viene visualizzata un'icona accanto al nome del nodo. Se il nodo è connesso e non sono presenti avvisi attivi, non viene visualizzata alcuna icona.



Quando un nodo non è connesso alla griglia, ad esempio durante l'aggiornamento o uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della griglia. Dopo che un nodo si ricollega alla griglia, attendere alcuni minuti per consentire la stabilizzazione dei valori.



Per modificare le unità per i valori di storage visualizzati in Grid Manager, selezionare il menu a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User preferences** (Preferenze utente).



Le schermate mostrate sono esempi. I risultati possono variare a seconda della versione di StorageGRID in uso.

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 di stato della connessione

Se un nodo viene disconnesso dalla griglia, accanto al nome del nodo viene visualizzata una delle seguenti icone.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per un motivo sconosciuto, un nodo viene disconnesso o i servizi sul nodo vengono inaspettatamente disattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista. Potrebbe essere attivato anche l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.	Richiede un'attenzione immediata. "Selezionare ciascun avviso" e seguire le azioni consigliate. Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo. Nota: Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).
	Non connesso - amministrazione non attiva Per un motivo previsto, il nodo non è connesso alla rete. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi. In base al problema sottostante, questi nodi tornano spesso online senza alcun intervento.	Determinare se eventuali avvisi influiscono su questo nodo. Se sono attivi uno o più avvisi, "Selezionare ciascun avviso" seguire le azioni consigliate.

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

Icone di avviso

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

 **Critico:** Si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Devi risolvere immediatamente il problema alla radice. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.

 **Grave:** Si è verificata una condizione anomala che sta influenzando le operazioni in corso o si sta avvicinando alla soglia per un avviso critico. Dovresti esaminare gli avvisi gravi e risolvere eventuali problemi sottostanti per assicurarti che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID.

 **Minore:** Il sistema funziona normalmente, ma è presente una condizione anomala che, se persiste, potrebbe compromettere la capacità del sistema di funzionare. Dovresti monitorare e risolvere gli avvisi minori che non si risolvono da soli per assicurarti che non causino un problema più serio.

Visualizza i dettagli di un sistema, sito o nodo

Per filtrare le informazioni visualizzate nella tabella Nodes (nodi), inserire una stringa di ricerca nel campo **Search** (Ricerca). È possibile eseguire una ricerca in base al nome del sistema, al nome visualizzato o al tipo (ad esempio, immettere **gat** per individuare rapidamente tutti i nodi gateway).

Per visualizzare le informazioni relative a griglia, sito o nodo:

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

Visualizza la scheda Panoramica di StorageGRID

La scheda Panoramica fornisce informazioni di base su ciascun nodo. Inoltre, vengono visualizzati tutti gli avvisi che attualmente influiscono sul nodo.

Viene visualizzata la scheda Overview (Panoramica) per tutti i nodi.

Informazioni sul nodo

La sezione Node Information (informazioni nodo) della scheda Overview (Panoramica) elenca le informazioni di base sul nodo.

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** (visualizzato solo se il nodo è stato rinominato): Il nome visualizzato corrente per il nodo. Utilizzare la ["Rinominare la griglia, i siti e i nodi"](#) procedura per aggiornare questo valore.
- **Nome sistema**: Il nome immesso per il nodo durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni StorageGRID interne e non possono essere modificati.
- **Tipo**: Il tipo di nodo — nodo amministrativo, nodo amministrativo primario, nodo di archiviazione o nodo gateway.
- **ID**: Identificatore univoco del nodo, chiamato anche UUID.
- **Stato connessione**: Uno dei tre stati. Viene visualizzata l'icona dello stato più grave.
 - **Sconosciuto** : Per un motivo sconosciuto, il nodo non è connesso alla grid oppure uno o più servizi sono inaspettatamente non disponibili. Ad esempio, la connessione di rete tra i nodi è stata persa, manca l'alimentazione o un servizio non è disponibile. Potrebbe anche essere attivato l'avviso **Unable to communicate with node**. Potrebbero essere attivi anche altri avvisi. Questa situazione richiede un intervento immediato.



Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).
 - **Inattivo per motivi amministrativi** : Il nodo non è connesso alla grid per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati arrestati correttamente, il nodo si sta riavviando oppure il software viene aggiornato. Potrebbero anche essere attivi uno o più avvisi.
 - **Connesso** : Il nodo è connesso alla griglia.
- **Storage utilizzato**: Solo per nodi di storage.
 - **Dati oggetto**: Percentuale dello spazio utilizzabile totale per i dati oggetto che è stato utilizzato nel nodo di storage.
 - **Metadati oggetto**: Percentuale dello spazio totale consentito per i metadati oggetto utilizzati nel nodo di storage.
- **Versione software**: La versione di StorageGRID installata sul nodo.
- **Gruppi ha**: Solo per nodi Admin Node e Gateway. Viene visualizzato se un'interfaccia di rete sul nodo è inclusa in un gruppo ad alta disponibilità e se tale interfaccia è l'interfaccia primaria.
- **Indirizzi IP**: Gli indirizzi IP del nodo. Seleziona **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 qualsiasi ["avvisi che attualmente interessano questo nodo e che non sono stati tacitati"](#). Selezionare il nome dell'avviso per visualizzare ulteriori dettagli e le azioni consigliate.

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.			

Gli avvisi sono inclusi anche per "stati di connessione del nodo".

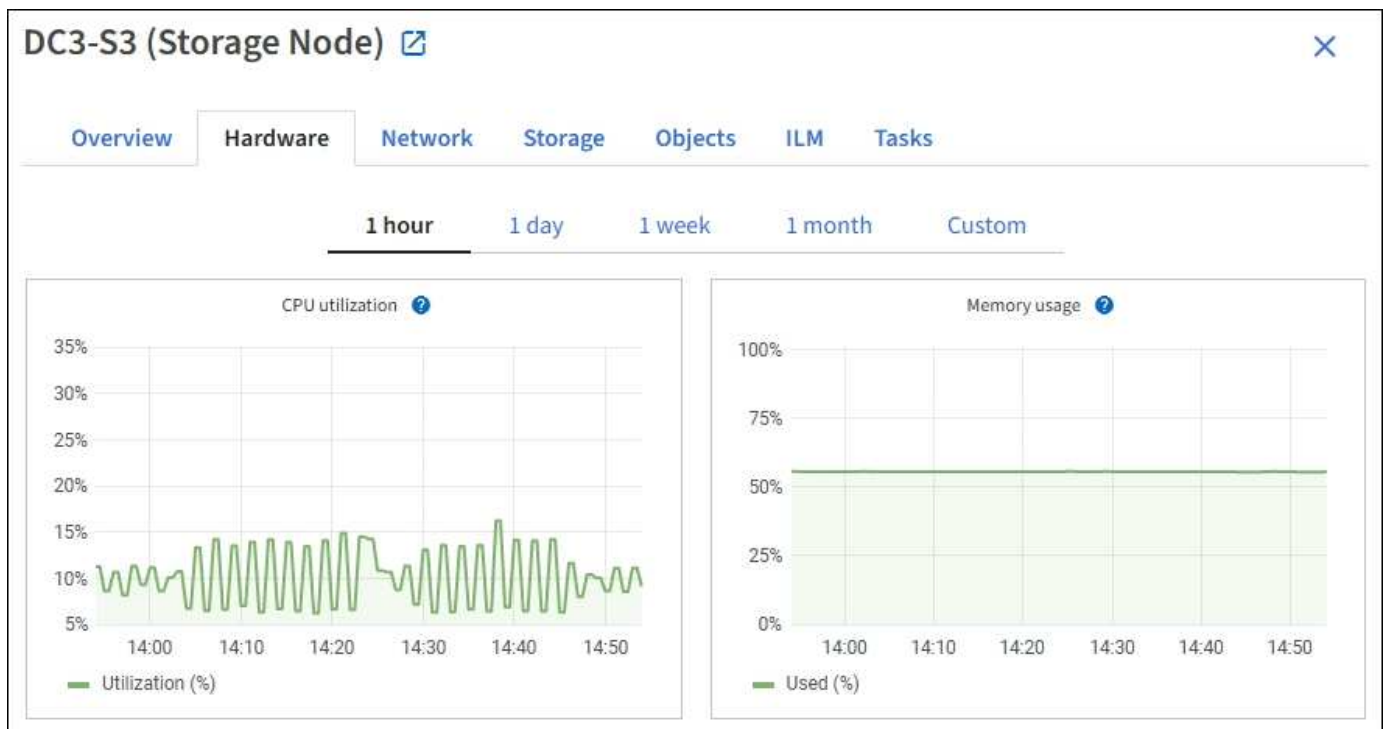
Visualizza la scheda Hardware di StorageGRID

La scheda hardware visualizza l'utilizzo della CPU e della memoria per ciascun nodo, oltre a informazioni aggiuntive sull'hardware delle appliance.



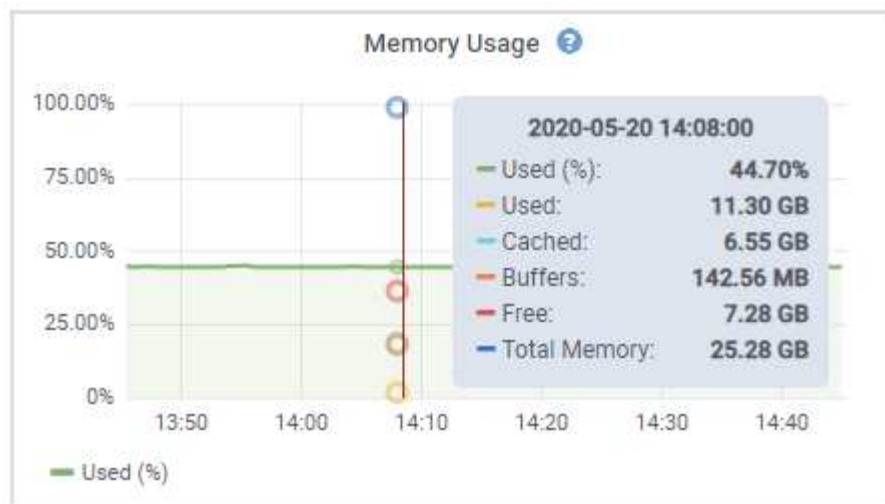
Grid Manager viene aggiornato con ogni versione e potrebbe non corrispondere alle schermate di esempio di questa pagina.

Viene visualizzata la scheda hardware per tutti i nodi.



Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per visualizzare i dettagli relativi all'utilizzo della CPU e della memoria, posizionare il cursore su ciascun grafico.



Se il nodo è un nodo appliance, questa scheda include anche una sezione con ulteriori informazioni sull'hardware dell'appliance.

Visualizza informazioni sui nodi di storage dell'appliance

La pagina Nodes (nodi) elenca le informazioni sullo stato di salute del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ciascun nodo di storage dell'appliance. È inoltre possibile visualizzare memoria, hardware di storage, versione del firmware del controller, risorse di rete, interfacce di rete, indirizzi di rete e ricevere e trasmettere dati.

Fasi

1. Dalla pagina Nodes (nodi), selezionare un nodo di storage dell'appliance.
2. Selezionare **Panoramica**.

La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

- **eth**: Rete griglia, rete amministrativa o rete client.
- **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte 1 GbE fisiche dell'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia di rete amministrativa StorageGRID (eth1). È possibile lasciare altre interfacce mtc disponibili per la connettività locale temporanea per un tecnico del data center.

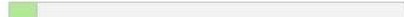
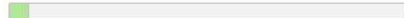
[Overview](#) [Hardware](#) [Network](#) [Storage](#) [Objects](#) [ILM](#) [Tasks](#)Node information [?](#)

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

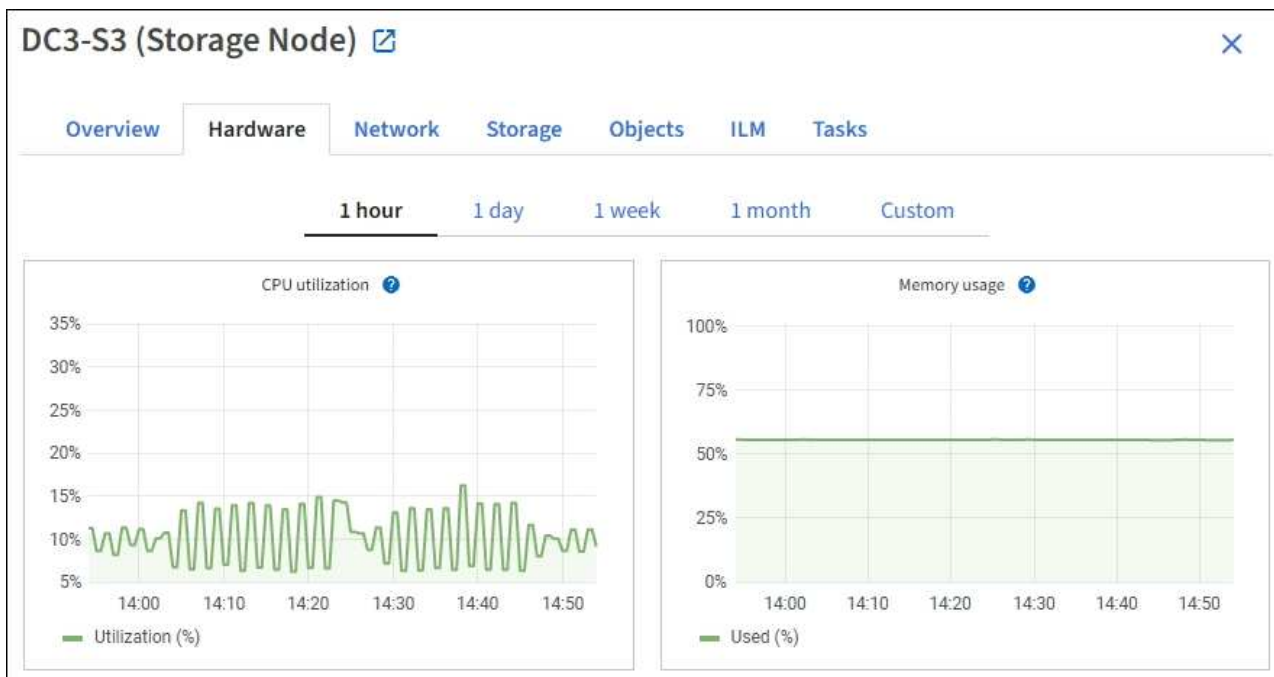
Alerts

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 gli avvisi attivi per il nodo.

3. Selezionare **hardware** per visualizzare ulteriori informazioni sull'appliance.

- Visualizza i grafici di utilizzo della CPU e della memoria per determinare le percentuali di utilizzo di CPU e memoria nel tempo. Per visualizzare un intervallo di tempo diverso, seleziona uno dei controlli sopra il grafico. Puoi visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. Puoi anche impostare un intervallo personalizzato, che ti permette di specificare intervalli di date e orari.



- b. Scorrere verso il basso per visualizzare la tabella dei componenti dell'appliance. Questa tabella contiene informazioni quali il nome del modello dell'appliance, i nomi dei controller, i numeri di serie e gli indirizzi IP e lo stato di ciascun componente.



Alcuni campi, ad esempio Compute controller BMC IP e Compute hardware, vengono visualizzati solo per le appliance dotate di tale funzionalità.

I componenti per gli shelf di storage e gli shelf di espansione, se sono parte dell'installazione, vengono visualizzati in una tabella separata sotto la tabella dell'appliance.

Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello di questo dispositivo StorageGRID mostrato in SANtricity OS.
Nome dello storage controller	Il nome dell'appliance StorageGRID visualizzato in SANtricity OS.
Storage controller A IP di gestione	Indirizzo IP per la porta di gestione 1 sul controller di storage A. si utilizza questo IP per accedere al sistema operativo SANtricity per risolvere i problemi di storage.
IP di gestione dello storage controller B.	Indirizzo IP per la porta di gestione 1 sullo storage controller B. si utilizza questo IP per accedere al sistema operativo SANtricity e risolvere i problemi di storage. Alcuni modelli di appliance non dispongono di un controller di storage B.
WWID dello storage controller	L'identificatore mondiale dello storage controller mostrato in SANtricity OS.

Nella tabella Appliance	Descrizione
Numero di serie dello chassis dell'appliance di storage	Il numero di serie dello chassis dell'appliance.
Versione del firmware del controller di storage	La versione del firmware del controller di storage per l'appliance.
Versione del sistema operativo SANtricity dello storage controller	Versione del sistema operativo SANtricity dello storage controller A.
Versione NVSRAM del controller di storage	Versione NVSRAM dello storage controller come indicato da System Manager di SANtricity. Per i modelli SG6060 e SG6160, se tra le due centraline è presente una mancata corrispondenza della versione NVSRAM, viene visualizzata la versione del controller A. Se la centralina A non è installata o funzionante, viene visualizzata la versione della centralina B.
Hardware per lo storage	Lo stato generale dell'hardware del controller dello storage. Se Gestore di sistema di SANtricity riporta lo stato di intervento richiesto per l'hardware di storage, anche il sistema StorageGRID riporta questo valore. Se lo stato è "richiede attenzione", controllare prima lo storage controller utilizzando il sistema operativo SANtricity. Quindi, assicurarsi che non esistano altri avvisi che si applicano al controller di elaborazione.
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Controller dello storage A	Lo stato dello storage controller A.
Controller dello storage B	Lo stato del controller di storage B. alcuni modelli di appliance non dispongono di un controller di storage B.
Alimentazione A del controller storage	Lo stato dell'alimentatore A per il controller dello storage.
Alimentazione controller storage B	Lo stato dell'alimentazione B del controller di storage.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).

Nella tabella Appliance	Descrizione
Dimensioni del disco per i dati di storage	Le dimensioni effettive di un'unità dati. Per il modello SG6160, vengono visualizzate anche le dimensioni dell'unità cache. Nota: Per i nodi con shelf di espansione, utilizzare Dimensioni del disco dati per ogni shelf invece. Le dimensioni effettive del disco potrebbero differire in base allo shelf.
Storage RAID mode (modalità RAID storage)	La modalità RAID configurata per l'appliance.
Connettività dello storage	Lo stato di connettività dello storage.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. Questo IP viene utilizzato per connettersi all'interfaccia BMC per monitorare e diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.
Hardware di calcolo	Lo stato dell'hardware del controller di calcolo. Questo campo non viene visualizzato per i modelli di appliance che non dispongono di hardware di calcolo e storage separati.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.
Alimentatore del controller di calcolo A	Stato dell'alimentatore A per il controller di calcolo.
Alimentatore del controller di calcolo B	Lo stato dell'alimentatore B per il controller di calcolo.

+

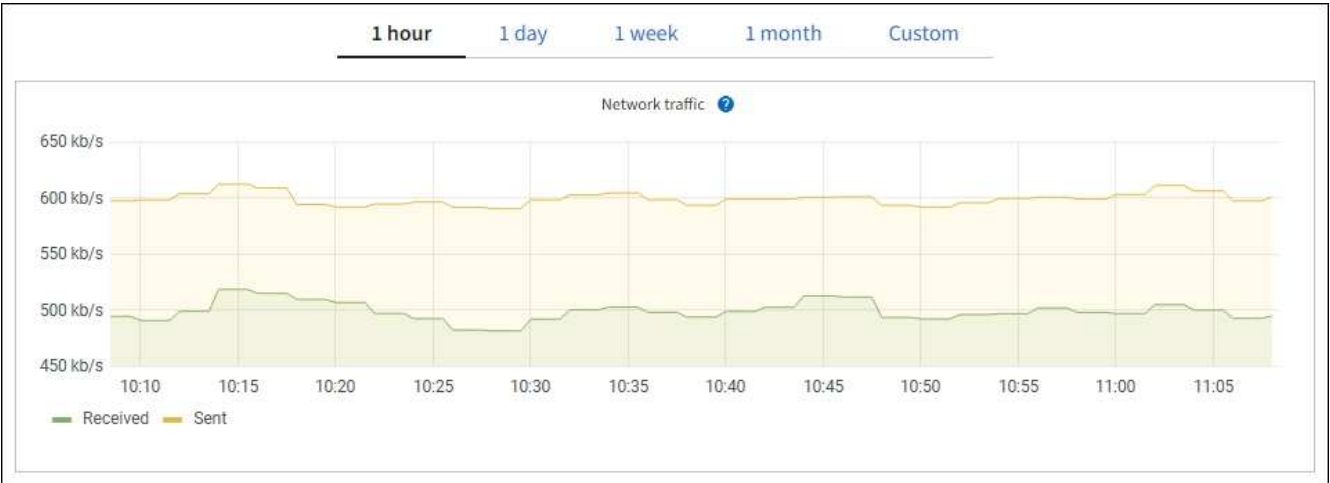
Nella tabella Storage shelf	Descrizione
Numero di serie dello shelf chassis	Il numero di serie dello chassis dello shelf di storage.
ID shelf	L'identificativo numerico dello shelf di storage. • 99: Shelf dello storage controller • 0: Primo shelf di espansione • 1: Secondo shelf di espansione Nota: gli scaffali di espansione si applicano solo ai modelli SG6060 e SG6160.
Stato dello shelf	Lo stato generale dello shelf di storage.
Stato IOM	Lo stato dei moduli di input/output (IOM) in qualsiasi shelf di espansione. N/D se non si tratta di uno shelf di espansione.
Stato dell'alimentatore	Lo stato generale degli alimentatori per lo shelf di storage.
Stato del cassetto	Lo stato dei cassette nello shelf di archiviazione. N/D se il ripiano non contiene cassette.
Stato della ventola	Lo stato generale delle ventole di raffreddamento nello shelf di storage.
Slot per dischi	Il numero totale di slot per dischi nello shelf di storage.
Dischi dati	Il numero di dischi nello shelf di storage utilizzati per lo storage dei dati.
dimensione del disco dati	La dimensione effettiva di un'unità dati nello shelf di storage.
Dischi cache	Il numero di dischi nello shelf di storage utilizzati come cache.
Dimensione dell'unità cache	La dimensione dell'unità cache più piccola nello shelf di storage. Normalmente, le unità cache sono tutte delle stesse dimensioni.
Stato della configurazione	Lo stato di configurazione dello shelf di storage.

a. Verificare che tutti gli stati siano "nominale".

Se uno stato non è "nominale", esaminare eventuali avvisi correnti. Puoi anche utilizzare Gestione di sistema di SANtricity per saperne di più su alcuni di questi valori hardware. Consultare le istruzioni per l'installazione e la manutenzione dell'apparecchio.

4. Selezionare **Network** per visualizzare le informazioni relative a ciascuna rete.

Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo.



a. Controlla 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

Usa la seguente tabella con i valori nella colonna **Velocità** della tabella Interfacce di rete per determinare se le porte di rete 10/25-GbE sull'appliance sono state configurate per utilizzare la modalità attivo/backup o la modalità LACP.



I valori mostrati nella tabella presuppongono che siano utilizzati tutti e quattro i collegamenti.

Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0,eth2)
Aggregato	LACP	25	100
Corretto	LACP	25	50
Corretto	Attivo/Backup	25	25
Aggregato	LACP	10	40
Corretto	LACP	10	20
Corretto	Attivo/Backup	10	10

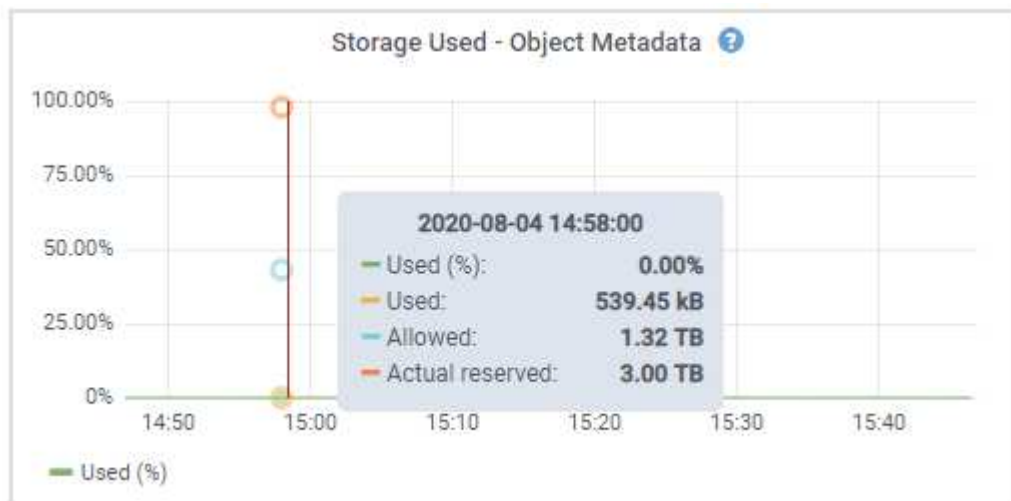
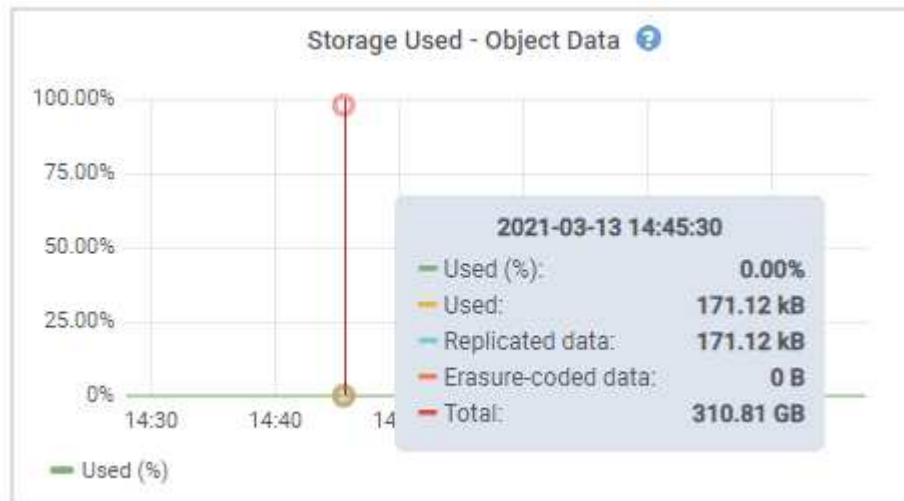
+

Consultare ["Configurare i collegamenti di rete"](#) per ulteriori informazioni sulla configurazione delle porte 10/25-GbE.

a. Controlla la sezione Comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.

5. Selezionare **Storage** per visualizzare i grafici che mostrano le percentuali di storage utilizzate nel tempo per i dati degli oggetti e i metadati degli oggetti, nonché informazioni su dischi, volumi e archivi di oggetti.



a. Scorrere verso il basso per visualizzare le quantità di storage disponibili per ciascun volume e archivio di oggetti.

Il nome internazionale di ciascun disco corrisponde all'identificativo mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà standard del volume in SANtricity OS (il software di gestione collegato al controller di storage dell'appliance).

Per semplificare l'interpretazione delle statistiche di lettura e scrittura dei dischi relative ai punti di montaggio del volume, la prima parte del nome visualizzato nella colonna **Name** della tabella Disk Devices (periferiche disco) (ovvero *sdc*, *sdd*, *sde* e così via) corrisponde al valore visualizzato nella colonna **Device** della tabella Volumes (volumi).

Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway

La pagina Nodes (nodi) elenca le informazioni sullo stato del servizio e tutte le risorse di calcolo, di dispositivo su disco e di rete per ogni appliance di servizi utilizzata come nodo di amministrazione o nodo gateway. È inoltre possibile visualizzare memoria, hardware di storage, risorse di rete, interfacce di rete, indirizzi di rete, e ricevere e trasmettere dati.

Fasi

1. Dalla pagina Nodes (nodi), selezionare un nodo Admin dell'appliance o un nodo Gateway dell'appliance.
2. Selezionare la scheda **Panoramica**.

La sezione Node information (informazioni nodo) della scheda Overview (Panoramica) visualizza informazioni riepilogative per il nodo, ad esempio il nome, il tipo, l'ID e lo stato di connessione del nodo. L'elenco degli indirizzi IP include il nome dell'interfaccia per ciascun indirizzo, come segue:

- **Adllb e adlli**: Visualizzato se si utilizza il bonding Active/backup per l'interfaccia di Admin Network
- **eth**: Rete griglia, rete amministrativa o rete client.
- **Hic**: Una delle porte fisiche 10, 25 o 100 GbE dell'appliance. Queste porte possono essere collegate tra loro e collegate alla rete griglia StorageGRID (eth0) e alla rete client (eth2).
- **mtc**: Una delle porte 1-GbE fisiche dell'appliance. Una o più interfacce mtc sono collegate per formare l'interfaccia Admin Network (eth1). È possibile lasciare altre interfacce mtc disponibili per la connettività locale temporanea per un tecnico del data center.

10-224-6-199-ADM1 (Primary Admin Node)

Overview
Hardware
Network
Storage
Load balancer
Tasks
SANtricity System Manager

Node information

Name:
10-224-6-199-ADM1

Type:
Primary Admin Node

ID:
6fdc1890-ca0a-4493-acdd-72ed317d95fb

Connection state:
Connected

Software version:
11.6.0 (build 20210928.1321.6687ee3)

IP addresses:

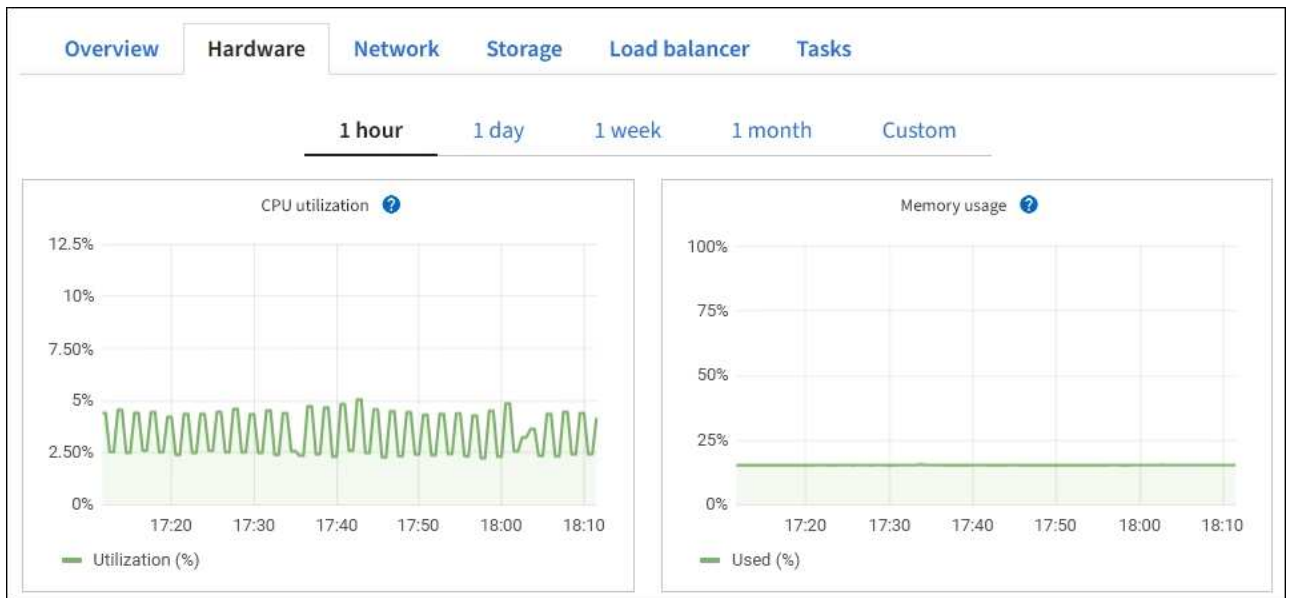
172.16.6.199 - eth0 (Grid Network)
10.224.6.199 - eth1 (Admin Network)
47.47.7.241 - eth2 (Client Network)

Hide additional 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 gli avvisi attivi per il nodo.

3. Seleziona la scheda **Hardware** per visualizzare ulteriori informazioni sull'appliance.
 - a. Visualizzare i grafici relativi all'utilizzo della CPU e della memoria per determinare le percentuali di utilizzo della CPU e della memoria nel tempo. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.



- b. Scorri verso il basso per visualizzare la tabella dei componenti dell'appliance. La tabella contiene informazioni quali il nome del modello, il numero di serie, la versione del firmware del controller e lo stato di ciascun componente.

Nella tabella Appliance	Descrizione
Modello di appliance	Il numero di modello dell'appliance StorageGRID.
Numero di dischi guasti del controller di storage	Il numero di dischi non ottimali.
Tipo di disco dati storage	Il tipo di dischi dell'appliance, ad esempio HDD (disco rigido) o SSD (disco a stato solido).
Dimensioni del disco per i dati di storage	Le dimensioni effettive di un'unità dati.
Storage RAID mode (modalità RAID storage)	La modalità RAID per l'appliance.
Alimentatore generale	Lo stato di tutti gli alimentatori dell'apparecchio.
IP BMC del controller di calcolo	L'indirizzo IP della porta BMC (Baseboard Management Controller) nel controller di calcolo. È possibile utilizzare questo IP per connettersi all'interfaccia BMC per monitorare e diagnosticare l'hardware dell'appliance. Questo campo non viene visualizzato per i modelli di appliance che non contengono un BMC.
Numero di serie del controller di calcolo	Il numero di serie del controller di calcolo.

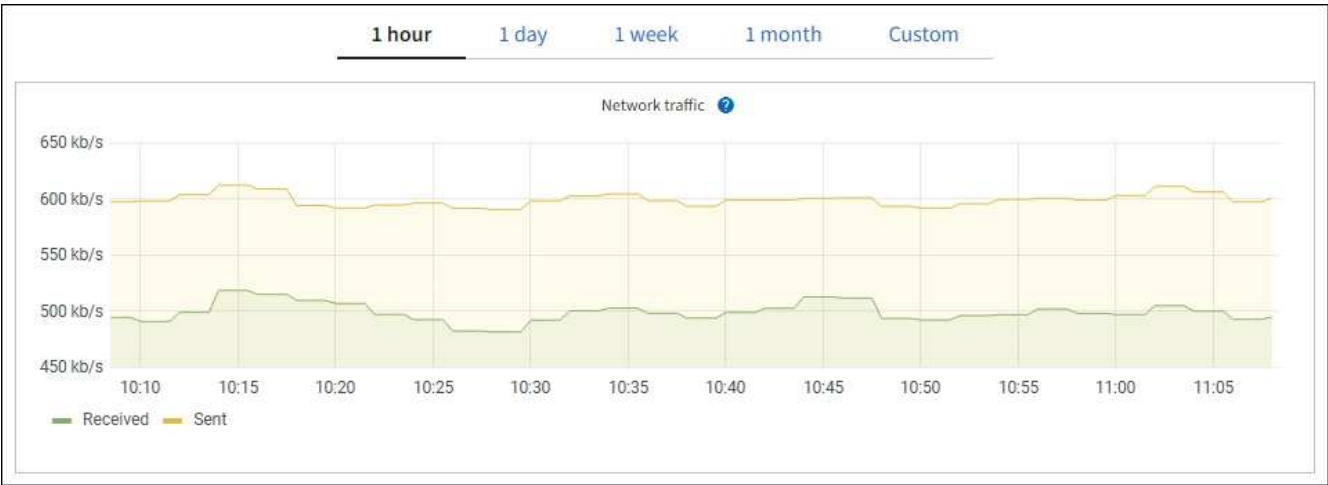
Nella tabella Appliance	Descrizione
Hardware di calcolo	Lo stato dell'hardware del controller di calcolo.
Temperatura della CPU del controller di calcolo	Lo stato della temperatura della CPU del controller di calcolo.
Temperatura dello chassis del controller di calcolo	Lo stato della temperatura del controller di calcolo.

c. Verificare che tutti gli stati siano "nominale".

Se uno stato non è "nominale", esaminare eventuali avvisi correnti.

4. Seleziona la scheda **Rete** per visualizzare le informazioni per ciascuna rete.

Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo.



a. Controlla la sezione Interfacce di rete.

Usa la seguente tabella con i valori nella colonna **Velocità** della tabella Interfacce di rete per determinare se le quattro porte di rete 40/100-GbE sull'appliance sono state configurate per utilizzare la modalità attivo/backup o la modalità LACP.

 I valori mostrati nella tabella presuppongono che siano utilizzati tutti e quattro i collegamenti.

Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0, eth2)
Aggregato	LACP	100	400
Corretto	LACP	100	200

Modalità link	Modalità bond	Velocità di collegamento HIC singola (hic1, hic2, hic3, hic4)	Velocità rete client/griglia prevista (eth0, eth2)
Corretto	Attivo/Backup	100	100
Aggregato	LACP	40	160
Corretto	LACP	40	80
Corretto	Attivo/Backup	40	40

a. Controlla la sezione Comunicazione di rete.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.

5. Seleziona la scheda **Archiviazione** per visualizzare le informazioni sui dispositivi disco e sui volumi sull'appliance di servizio.

Visualizza la scheda Rete di StorageGRID

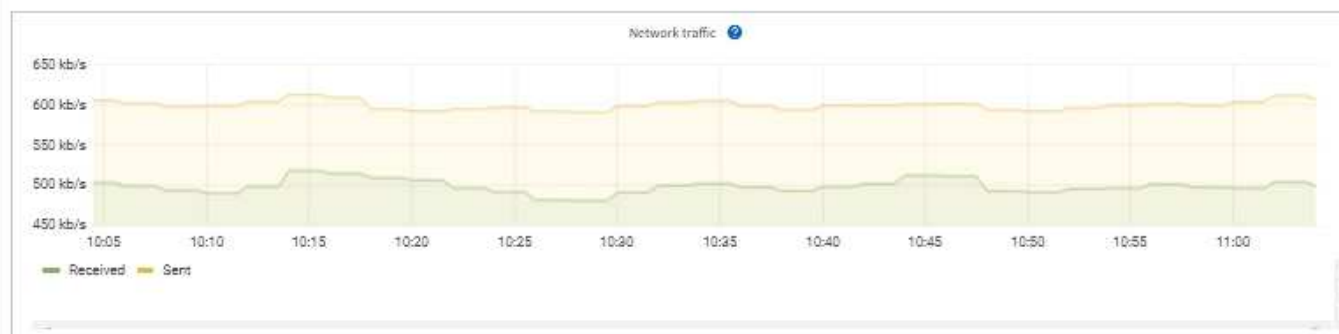
La scheda Network (rete) visualizza un grafico che mostra il traffico di rete ricevuto e inviato attraverso tutte le interfacce di rete del nodo, del sito o della griglia.

Viene visualizzata la scheda Network (rete) per tutti i nodi, ciascun sito e l'intera griglia.

Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.

Per i nodi, la tabella interfacce di rete fornisce informazioni sulle porte di rete fisiche di ciascun nodo. La tabella delle comunicazioni di rete fornisce dettagli sulle operazioni di ricezione e trasmissione di ciascun nodo e sui contatori di guasti segnalati dai driver.

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 di rete e le performance"](#)

Visualizza la scheda Storage della StorageGRID

La scheda Storage riepiloga la disponibilità dello storage e altre metriche di storage.

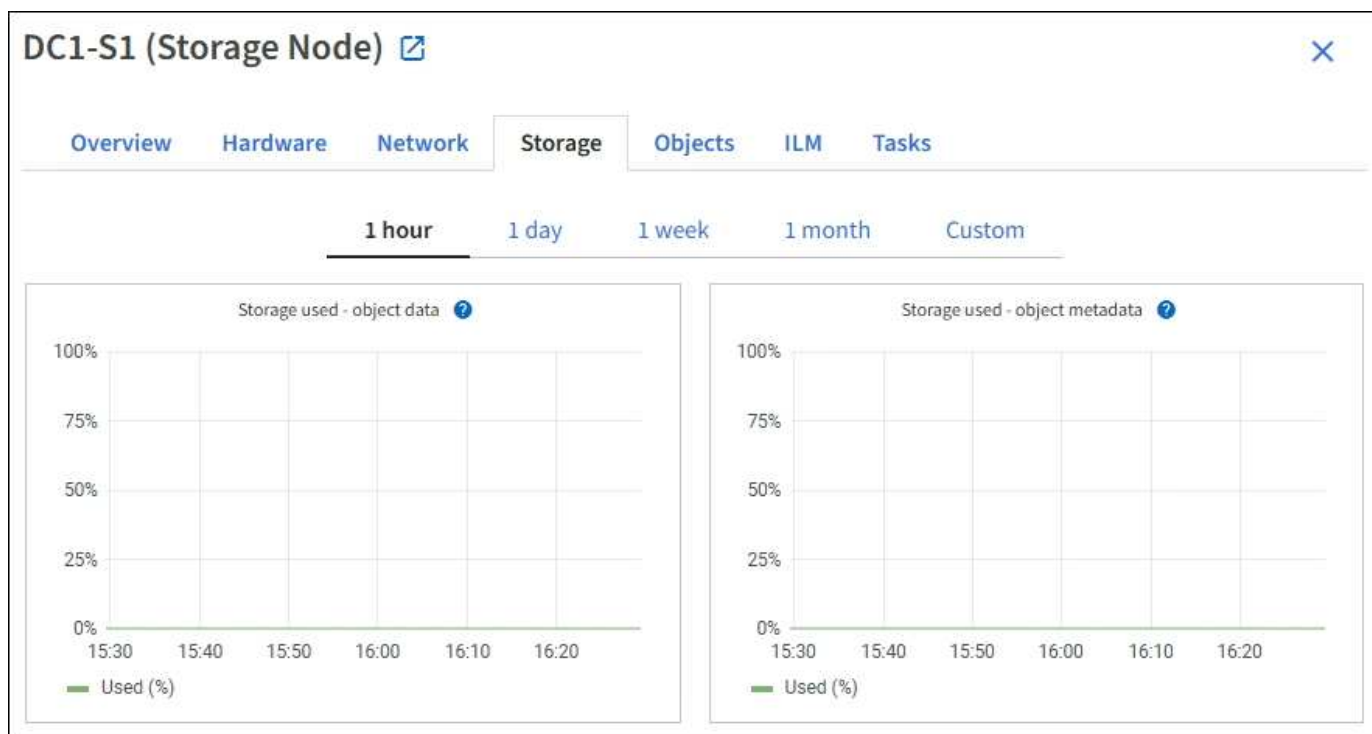
La scheda Archiviazione viene visualizzata per tutti i nodi, per ogni sito e per l'intera griglia. Questa scheda contiene le seguenti informazioni:

Grafici utilizzati per lo storage

Per i nodi di storage, ciascun sito e l'intero grid, la scheda Storage include grafici che mostrano la quantità di storage utilizzata dai dati degli oggetti e dai metadati degli oggetti nel tempo.



Quando un nodo non è connesso alla griglia, ad esempio durante l'aggiornamento o uno stato disconnesso, alcune metriche potrebbero non essere disponibili o essere escluse dai totali del sito e della griglia. Dopo che un nodo si ricollega alla griglia, attendere alcuni minuti per consentire la stabilizzazione dei valori.



Dischi, volumi e tabelle di archiviazione degli oggetti

Per tutti i nodi, la scheda Storage contiene i dettagli relativi ai dischi e ai volumi sul nodo. Per i nodi di storage, la tabella degli archivi di oggetti fornisce informazioni su ciascun volume di storage.

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	3 KB/s
cvloc(8:2,sda2)	N/A	0.67%	0 bytes/s	50 KB/s
sdc(8:16,sdb)	N/A	0.03%	0 bytes/s	4 KB/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.75 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	84.05 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	124.60 KB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

Informazioni correlate

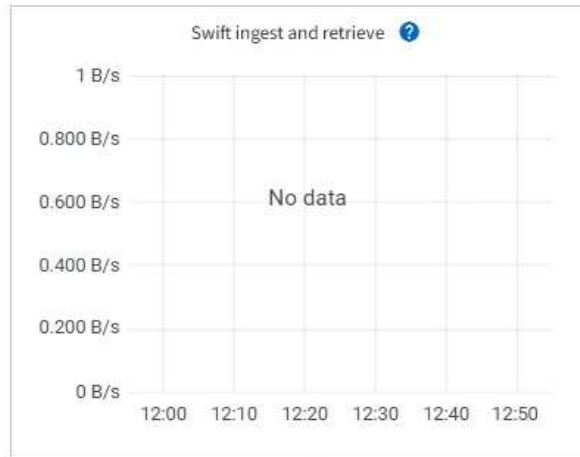
["Monitorare la capacità dello storage"](#)

Visualizza la scheda Oggetti di StorageGRID

La scheda oggetti fornisce informazioni su ["Tassi di acquisizione e recupero pari a S3 volte"](#).

Viene visualizzata la scheda oggetti per ciascun nodo di storage, ciascun sito e l'intera griglia. Per i nodi di storage, la scheda oggetti fornisce anche conteggi di oggetti e informazioni sulle query dei metadati e sulla verifica in background.

DC1-S1 (Storage Node) [🔗](#)

[Overview](#)[Hardware](#)[Network](#)[Storage](#)[Objects](#)[ILM](#)[Tasks](#)[1 hour](#)[1 day](#)[1 week](#)[1 month](#)[Custom](#)

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

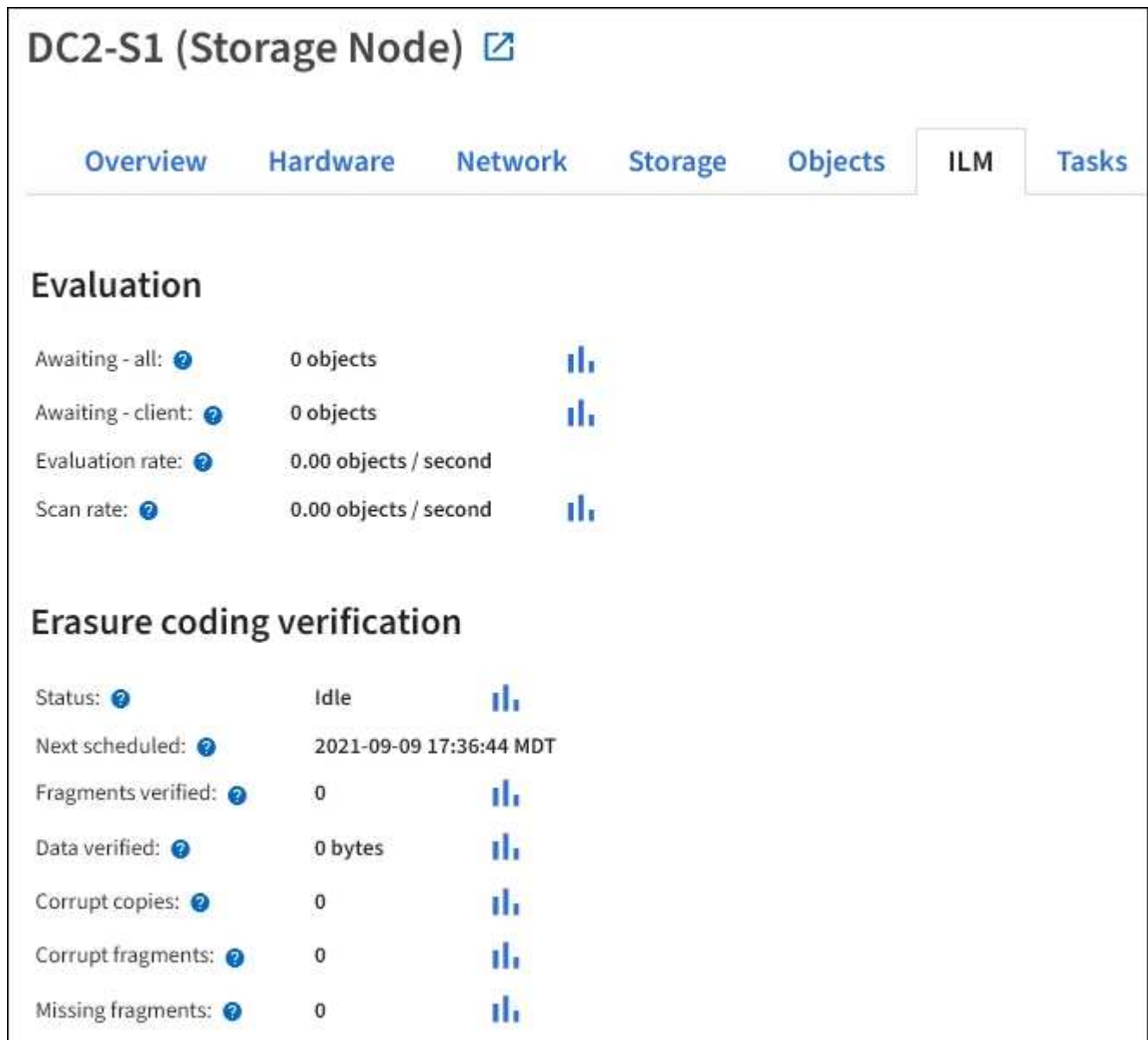
Quarantined objects: ? 0

Visualizza la scheda StorageGRID ILM

La scheda ILM fornisce informazioni sulle operazioni di Information Lifecycle management (ILM).

Viene visualizzata la scheda ILM per ciascun nodo di storage, ciascun sito e l'intera griglia. Per ogni sito e griglia, la scheda ILM mostra un grafico della coda ILM nel tempo. Per la griglia, questa scheda fornisce anche il tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

Per i nodi storage, la scheda ILM fornisce dettagli sulla valutazione ILM e sulla verifica in background per gli oggetti sottoposti a erasure coding.



Informazioni correlate

- ["Monitorare la gestione del ciclo di vita delle informazioni"](#)
- ["Amministrare StorageGRID"](#)

Utilizzare la scheda Attività di StorageGRID

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 nodi di archiviazione, è possibile impostare lo stato di archiviazione.

Per i requisiti e le istruzioni completi per ciascuna opzione di questa scheda, vedere quanto segue:

- ["Rinominare la griglia, i siti e i nodi"](#)
- ["Nodo di reboot grid"](#)
- ["Impostare l'apparecchio in modalità di manutenzione"](#)
- È possibile verificare o impostare lo stato di archiviazione di un nodo di archiviazione dopo aver aggiunto volumi SAN o collegati direttamente al nodo di archiviazione oppure dopo aver ripristinato un nodo di archiviazione. Tali istruzioni sono disponibili negli argomenti che descrivono tali attività.

Visualizza la scheda del bilanciamento del carico StorageGRID

La scheda bilanciamento del carico include i grafici delle performance e diagnostici relativi al funzionamento del servizio bilanciamento del carico.

Viene visualizzata la scheda Load Balancer (bilanciamento carico) per i nodi Admin e Gateway, per ciascun sito e per l'intera griglia. Per ogni sito, la scheda bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i nodi del sito. Per l'intera griglia, la scheda bilanciamento del carico fornisce un riepilogo aggregato delle statistiche per tutti i siti.

Se non viene eseguito alcun i/o attraverso il servizio di bilanciamento del carico o non è configurato alcun bilanciamento del carico, i grafici visualizzano "Nessun dato".



Richiesta di traffico

Questo grafico fornisce una media mobile di 3 minuti del throughput dei dati trasmessi tra gli endpoint del bilanciamento del carico e i client che eseguono le richieste, in bit al secondo.



Questo valore viene aggiornato al completamento di ogni richiesta. Di conseguenza, questo valore potrebbe differire dal throughput in tempo reale a bassi tassi di richiesta o per richieste di durata molto lunga. La scheda Network (rete) consente di ottenere una vista più realistica del comportamento corrente della rete.

Tasso di richiesta in entrata

Questo grafico fornisce una media mobile di 3 minuti del numero di nuove richieste al secondo, ripartita per tipo di richiesta (GET, PUT, HEAD e DELETE). Questo valore viene aggiornato quando le intestazioni di una nuova richiesta sono state convalidate.

Durata media della richiesta (non errore)

Questo grafico fornisce una media mobile di 3 minuti delle durate delle richieste, suddivisa per tipo di richiesta (GET, PUT, HEAD ed DELETE). Ogni durata della richiesta inizia quando un'intestazione di richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo di risposta completo viene restituito al client.

Tasso di risposta agli errori

Questo grafico fornisce una media mobile di 3 minuti del numero di risposte agli errori restituite ai client al secondo, ripartito per codice di risposta agli errori.

Informazioni correlate

- ["Monitorare le operazioni di bilanciamento del carico"](#)
- ["Amministrare StorageGRID"](#)

Visualizza la scheda Servizi della piattaforma StorageGRID

La scheda Platform Services (servizi piattaforma) fornisce informazioni sulle operazioni di servizio della piattaforma S3 in un sito.

Viene visualizzata la scheda Platform Services (servizi piattaforma) per ciascun sito. Questa scheda fornisce informazioni sui servizi della piattaforma S3, come la replica CloudMirror e il servizio di integrazione della ricerca. I grafici di questa scheda mostrano metriche come il numero di richieste in sospeso, la percentuale di completamento della richiesta e la percentuale di guasti della richiesta.

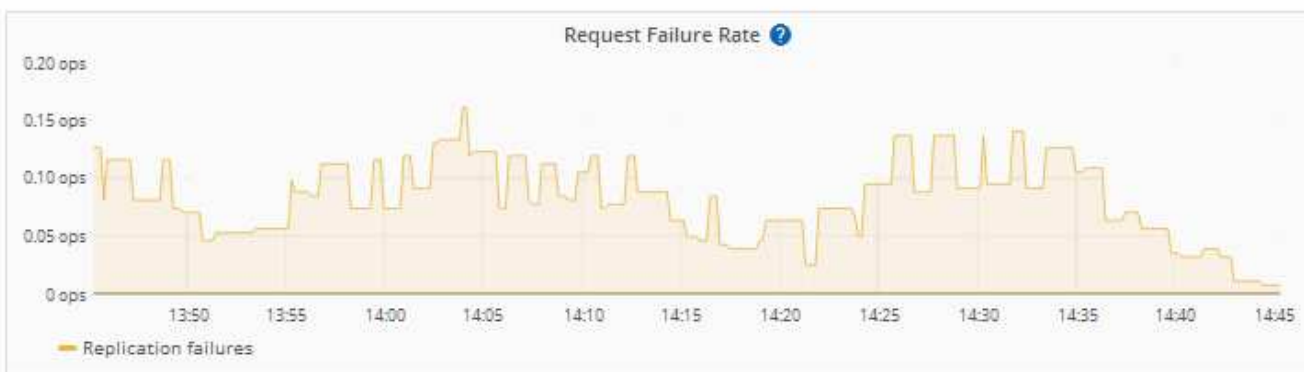
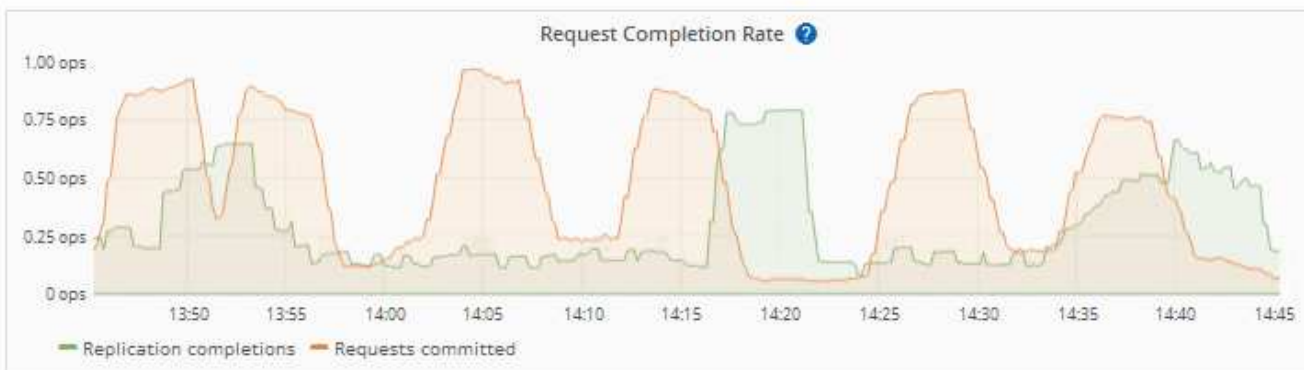
1 hour

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 di StorageGRID"](#).

Visualizza la scheda Gestisci unità di StorageGRID

La scheda Gestisci unità consente di accedere ai dettagli ed eseguire attività di risoluzione dei problemi e manutenzione sulle unità delle appliance che supportano questa funzionalità.

Utilizzando la scheda Gestisci unità, è possibile effettuare le seguenti operazioni:

- Visualizzare un layout delle unità di storage dei dati nell'appliance
- Visualizza una tabella in cui sono elencati ogni tipo, posizione, stato, versione del firmware e numero di serie del disco
- Eseguire le funzioni di risoluzione dei problemi e manutenzione su ciascuna unità

Per accedere alla scheda Gestisci unità, è necessario disporre di ["Autorizzazione di accesso root o amministratore dell'appliance di storage"](#).

Per informazioni sull'utilizzo della scheda Gestisci unità, vedere ["Utilizzare la scheda Gestisci unità"](#).

Visualizza la scheda SANtricity System Manager di StorageGRID

La scheda Gestore di sistema di SANtricity consente di accedere a Gestore di sistema di SANtricity senza dover configurare o collegare la porta di gestione dell'appliance di storage. È possibile utilizzare questa scheda per esaminare le informazioni ambientali e di diagnostica dell'hardware, nonché i problemi relativi ai dischi.



L'accesso a Gestione di sistema SANtricity da Gestione griglia è generalmente destinato solo al monitoraggio dell'hardware dell'appliance e alla configurazione di e-Series AutoSupport. Molte funzionalità e operazioni di Gestione sistema di SANtricity, come l'aggiornamento del firmware, non si applicano al monitoraggio dell'appliance StorageGRID. Per evitare problemi, seguire sempre le istruzioni per la manutenzione dell'hardware dell'apparecchio. Per aggiornare il firmware SANtricity, consultare la ["Procedure di configurazione della manutenzione"](#) relativa all'appliance di storage.



La scheda Gestore di sistema di SANtricity viene visualizzata solo per i nodi di appliance di storage che utilizzano hardware e-Series.

Utilizzando Gestione sistema di SANtricity, è possibile effettuare le seguenti operazioni:

- Visualizza i dati sulle performance come performance a livello di array di storage, latenza i/o, utilizzo della CPU del controller di storage e throughput.
- Controllare lo stato dei componenti hardware.
- Eseguire funzioni di supporto, tra cui la visualizzazione dei dati diagnostici e la configurazione di e-Series AutoSupport.



Per utilizzare SANtricity System Manager per configurare un proxy per E-Series AutoSupport, vedi ["Invio dei pacchetti e-Series AutoSupport tramite StorageGRID"](#).

Per accedere a Gestore di sistema di SANtricity tramite Gestione griglia, è necessario disporre di ["Autorizzazione di accesso root o amministratore dell'appliance di storage"](#).



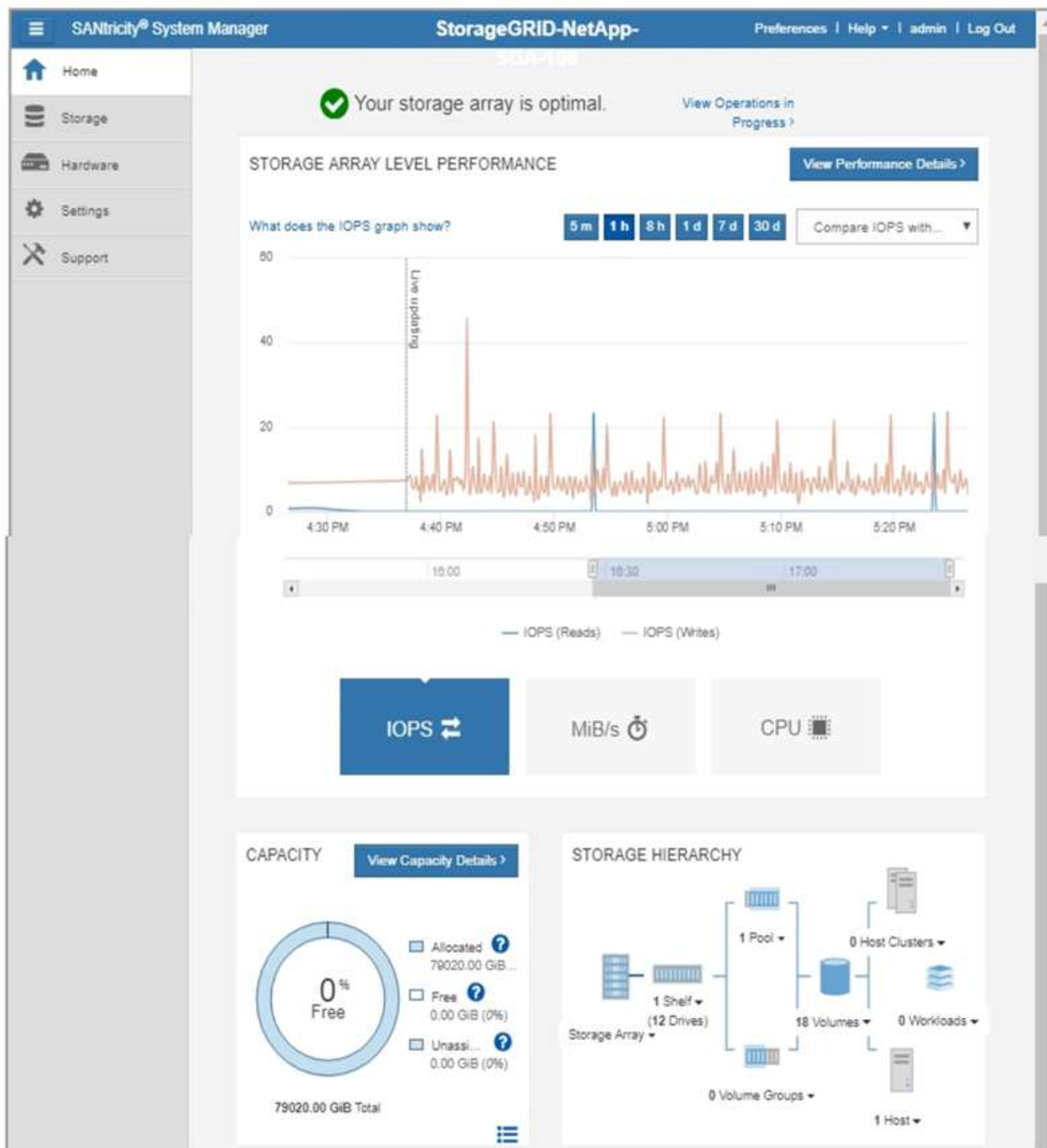
È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

La scheda visualizza la home page di Gestore di sistema di SANtricity.

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 Gestore di sistema di SANtricity per aprire Gestione di sistema di SANtricity in una nuova finestra del browser per una visualizzazione più semplice.

Per visualizzare i dettagli relativi all'utilizzo della capacità e delle prestazioni a livello di array di storage,

posizionare il cursore su ciascun grafico.

Per ulteriori informazioni sulla visualizzazione delle informazioni accessibili dalla scheda Gestore di sistema di SANtricity, vedere ["Documentazione di NetApp e-Series e SANtricity"](#).

Informazioni da monitorare regolarmente

Cosa e quando monitorare in StorageGRID

Anche se il sistema StorageGRID può continuare a funzionare quando si verificano errori o parti della griglia non sono disponibili, è necessario monitorare e risolvere potenziali problemi prima che influiscano sull'efficienza o sulla disponibilità della rete.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Informazioni sulle attività di monitoraggio

Un sistema occupato genera grandi quantità di informazioni. Il seguente elenco fornisce indicazioni sulle informazioni più importanti da monitorare costantemente.

Cosa monitorare	Frequenza
"Stato di salute del sistema"	Ogni giorno
Tasso a cui "Capacità di metadati e oggetti del nodo di storage" è consumato	Settimanale
"Operazioni di gestione del ciclo di vita delle informazioni"	Settimanale
"Risorse di rete e di sistema"	Settimanale
"Attività del tenant"	Settimanale
"S3 operazioni client"	Settimanale
"Operazioni di bilanciamento del carico"	Dopo la configurazione iniziale e dopo eventuali modifiche alla configurazione
"Connessioni a federazione di griglie"	Settimanale

Monitorare lo stato di salute del sistema in StorageGRID

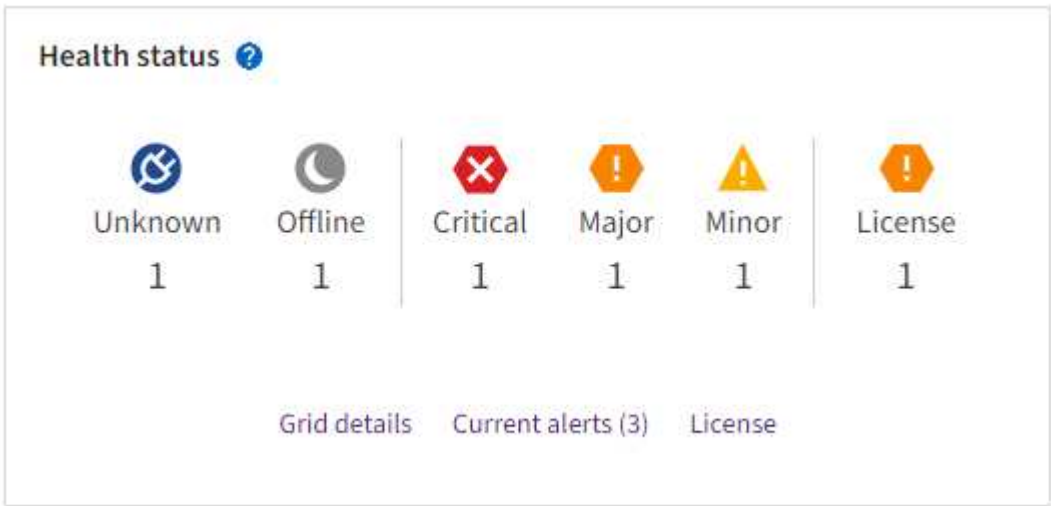
Monitorare quotidianamente lo stato di salute generale del sistema StorageGRID.

A proposito di questa attività

Il sistema StorageGRID può continuare a funzionare quando le parti della griglia non sono disponibili. I potenziali problemi indicati dagli avvisi non sono necessariamente problemi con le operazioni del sistema.

Esaminare i problemi riepilogati nella scheda di stato dello stato di salute del pannello di controllo di Grid Manager.

Per essere avvisati degli avvisi non appena vengono attivati, è possibile ["imposta le notifiche via email per gli avvisi"](#) o ["Configurare i trap SNMP"](#).



In caso di problemi, vengono visualizzati collegamenti che consentono di visualizzare ulteriori dettagli:

Collegamento	Viene visualizzato quando...
Dettagli della griglia	Tutti i nodi sono disconnessi (stato di connessione sconosciuto o amministrativamente inattivo).
Avvisi correnti (critici, maggiori, minori)	Gli avvisi sono attualmente attivo.
Avvisi risolti di recente	Avvisi attivati nella settimana precedente sono ora risolti.
Licenza	Si è verificato un problema con la licenza software per questo sistema StorageGRID. È possibile "aggiornare le informazioni sulla licenza in base alle necessità" .

Monitorare gli stati di connessione del nodo

Se uno o più nodi sono disconnessi dalla rete, potrebbero verificarsi problemi con le operazioni critiche di StorageGRID. Monitorare gli stati di connessione dei nodi e risolvere tempestivamente eventuali problemi.

Icona	Descrizione	Azione richiesta
	Non connesso - Sconosciuto Per un motivo sconosciuto, un nodo viene disconnesso o i servizi sul nodo vengono inaspettatamente disattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato o il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione dell'alimentazione o di un'interruzione imprevista. Potrebbe essere attivato anche l'avviso Impossibile comunicare con il nodo. Potrebbero essere attivi anche altri avvisi.	Richiede un'attenzione immediata. Selezionare ciascun avviso e seguire le azioni consigliate. Ad esempio, potrebbe essere necessario riavviare un servizio che ha arrestato o riavviato l'host per il nodo. Nota: Un nodo potrebbe apparire come sconosciuto durante le operazioni di shutdown gestite. In questi casi, è possibile ignorare lo stato Unknown (Sconosciuto).
	Non connesso - amministrazione non attiva Per un motivo previsto, il nodo non è connesso alla rete. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento. Potrebbero essere attivi anche uno o più avvisi. In base al problema sottostante, questi nodi tornano spesso online senza alcun intervento.	Determinare se eventuali avvisi influiscono su questo nodo. Se sono attivi uno o più avvisi, selezionare ciascun avviso e seguire le azioni consigliate.
	Connesso Il nodo è collegato alla rete.	Non è richiesta alcuna azione.

Visualizzare gli avvisi correnti e risolti

Current alerts (Avvisi correnti): Quando viene attivato un avviso, viene visualizzata un'icona di avviso sul dashboard. Nella pagina nodi viene visualizzata anche un'icona di avviso per il nodo. Se "[le notifiche e-mail di avviso sono configurate](#)", viene inviata anche una notifica e-mail, a meno che l'avviso non sia stato tacitato.

Avvisi risolti: È possibile cercare e visualizzare una cronologia degli avvisi risolti.

Facoltativamente, hai guardato il video:

[Panoramica degli avvisi](#)

La seguente tabella descrive le informazioni visualizzate in Grid Manager per gli avvisi correnti e risolti.

Intestazione di colonna	Descrizione
Nome o titolo	Il nome dell'avviso e la relativa descrizione.
Severità	La severità dell'avviso. Per gli avvisi correnti, se sono raggruppati più avvisi, la riga del titolo mostra il numero di istanze di tale avviso che si verificano a ogni livello di gravità.  Critico: Si è verificata una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Devi risolvere immediatamente il problema alla radice. Se il problema non viene risolto, potrebbero verificarsi interruzioni del servizio e perdita di dati.  Grave: Si è verificata una condizione anomala che sta influenzando le operazioni in corso o si sta avvicinando alla soglia per un avviso critico. Dovresti esaminare gli avvisi gravi e risolvere eventuali problemi sottostanti per assicurarti che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID.  Minore: Il sistema funziona normalmente, ma è presente una condizione anomala che, se persiste, potrebbe compromettere la capacità del sistema di funzionare. Dovresti monitorare e risolvere gli avvisi minori che non si risolvono da soli per assicurarti che non causino un problema più serio.
Tempo di attivazione	Current alerts (Avvisi correnti): La data e l'ora in cui l'avviso è stato attivato nell'ora locale e in UTC. Se vengono raggruppati più avvisi, la riga del titolo mostra l'ora dell'istanza più recente dell'avviso (<i>NEST</i>) e l'istanza più vecchia dell'avviso (<i>OLDEST</i>). Resolved alerts (Avvisi risolti): Quanto tempo fa è stato attivato l'avviso.
Sito/nodo	Il nome del sito e del nodo in cui si è verificato o si è verificato l'avviso.
Stato	Se l'avviso è attivo, tacitato o risolto. Se vengono raggruppati più avvisi e nell'elenco a discesa viene selezionato tutti gli avvisi , la riga del titolo mostra quante istanze di tale avviso sono attive e quante istanze sono state tacitate.
Tempo risolto (solo avvisi risolti)	Quanto tempo fa l'avviso è stato risolto.
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 che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso Low Object Data Storage includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata. Nota: se vengono raggruppati più avvisi correnti, i valori correnti non vengono visualizzati nella riga del titolo.

Intestazione di colonna	Descrizione
Valori attivati (solo avvisi risolti)	Il valore della metrica che ha causato l'attivazione dell'avviso. Per alcuni avvisi, vengono visualizzati valori aggiuntivi che consentono di comprendere e analizzare l'avviso. Ad esempio, i valori visualizzati per un avviso Low Object Data Storage includono la percentuale di spazio su disco utilizzato, la quantità totale di spazio su disco e la quantità di spazio su disco utilizzata.

Fasi

1. Selezionare il collegamento **Avvisi correnti** o **Avvisi risolti** per visualizzare un elenco di avvisi in tali categorie. È inoltre possibile visualizzare i dettagli di un avviso selezionando **nodi > nodo > Panoramica** e selezionando l'avviso dalla tabella Avvisi.

Per impostazione predefinita, gli avvisi correnti vengono visualizzati come segue:

- Vengono visualizzati per primi gli avvisi attivati più di recente.
- Più avvisi dello stesso tipo vengono visualizzati come gruppo.
- Gli avvisi che sono stati tacitati non vengono visualizzati.
- Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene visualizzato solo l'allarme più grave. Ovvero, se vengono raggiunte soglie di allarme per i livelli di severità minori, maggiori e critici, viene visualizzato solo l'avviso critico.

La pagina degli avvisi correnti viene aggiornata ogni due minuti.

2. Per espandere i gruppi di avvisi, seleziona la freccia in basso ▼. Per comprimere i singoli avvisi di un gruppo, seleziona la freccia in alto ▲ o il nome del gruppo.
3. Per visualizzare singoli avvisi invece di gruppi di avvisi, deselezionare la casella di controllo **Group alerts** (Avvisi di gruppo).
4. Per ordinare gli avvisi correnti o i gruppi di avvisi, seleziona le frecce su/giù ⬆️ nell'intestazione di ciascuna colonna.
 - Quando si seleziona **Group alerts** (Avvisi di gruppo), vengono ordinati sia i gruppi di avvisi che i singoli avvisi all'interno di ciascun gruppo. Ad esempio, è possibile ordinare gli avvisi in un gruppo in base all'ora * attivata per trovare l'istanza più recente di un avviso specifico.
 - Quando l'opzione **Group alerts** (Avvisi di gruppo) viene deselezionata, viene ordinato l'intero elenco di avvisi. Ad esempio, è possibile ordinare tutti gli avvisi in base a **nodo/sito** per visualizzare tutti gli avvisi relativi a un nodo specifico.
5. Per filtrare gli avvisi correnti in base allo stato (**tutti gli avvisi**, **attivi** o **silenziati**, utilizzare il menu a discesa nella parte superiore della tabella.

Vedere "[Tacitare le notifiche di avviso](#)".

6. Per ordinare gli avvisi risolti:
 - Selezionare un periodo di tempo dal menu a discesa **quando attivato**.
 - Selezionare una o più severità dal menu a discesa **severità**.
 - Selezionare una o più regole di avviso predefinite o personalizzate dal menu a discesa **regola di avviso** per filtrare gli avvisi risolti correlati a una regola di avviso specifica.
 - Selezionare uno o più nodi dal menu a discesa **nodo** per filtrare gli avvisi risolti relativi a un nodo specifico.

7. Per visualizzare i dettagli di un avviso specifico, selezionarlo. Una finestra di dialogo fornisce dettagli e azioni consigliate per l'avviso selezionato.
8. (Facoltativo) per un avviso specifico, selezionare **Silence this alert** (tacita questo avviso) per tacitare la regola che ha causato l'attivazione dell'avviso.

È necessario disporre di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#) per tacitare una regola di avviso.



Prestare attenzione quando si decide di tacitare una regola di avviso. Se una regola di avviso viene tacitata, è possibile che non si rilevi un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

9. Per visualizzare le condizioni correnti della regola di avviso:

- a. Dai dettagli dell'avviso, selezionare **View conditions** (Visualizza condizioni).

Viene visualizzata una finestra a comparsa che elenca l'espressione Prometheus per ogni severità definita.

- b. Per chiudere la finestra a comparsa, seleziona un punto qualsiasi al di fuori della finestra a comparsa.

10. Facoltativamente, selezionare **Edit rule** (Modifica regola) per modificare la regola di avviso che ha causato l'attivazione dell'avviso.

È necessario disporre di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#) per modificare una regola di avviso.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

11. Per chiudere i dettagli dell'avviso, selezionare **Chiudi**.

Monitora la capacità di archiviazione in StorageGRID

Monitorare lo spazio utilizzabile totale disponibile per garantire che il sistema StorageGRID non esaurisca lo spazio di storage per gli oggetti o per i metadati degli oggetti.

StorageGRID memorizza i dati degli oggetti e i metadati degli oggetti separatamente e riserva una quantità specifica di spazio per un database Cassandra distribuito che contiene metadati degli oggetti. Monitorare la quantità totale di spazio consumata per gli oggetti e per i metadati degli oggetti, nonché le tendenze della quantità di spazio consumata per ciascuno di essi. Ciò consente di pianificare in anticipo l'aggiunta di nodi ed evitare interruzioni del servizio.

È possibile ["visualizzare le informazioni sulla capacità dello storage"](#) per l'intero grid, per ogni sito e per ogni nodo di storage nel sistema StorageGRID.

Monitorare la capacità di storage per l'intero grid

Monitorare la capacità di storage complessiva del grid per garantire che rimanga spazio libero adeguato per i dati degli oggetti e i metadati degli oggetti. Comprendere come la capacità dello storage cambia nel tempo può aiutarti a pianificare l'aggiunta di nodi o volumi di storage prima che la capacità dello storage utilizzabile del grid venga consumata.

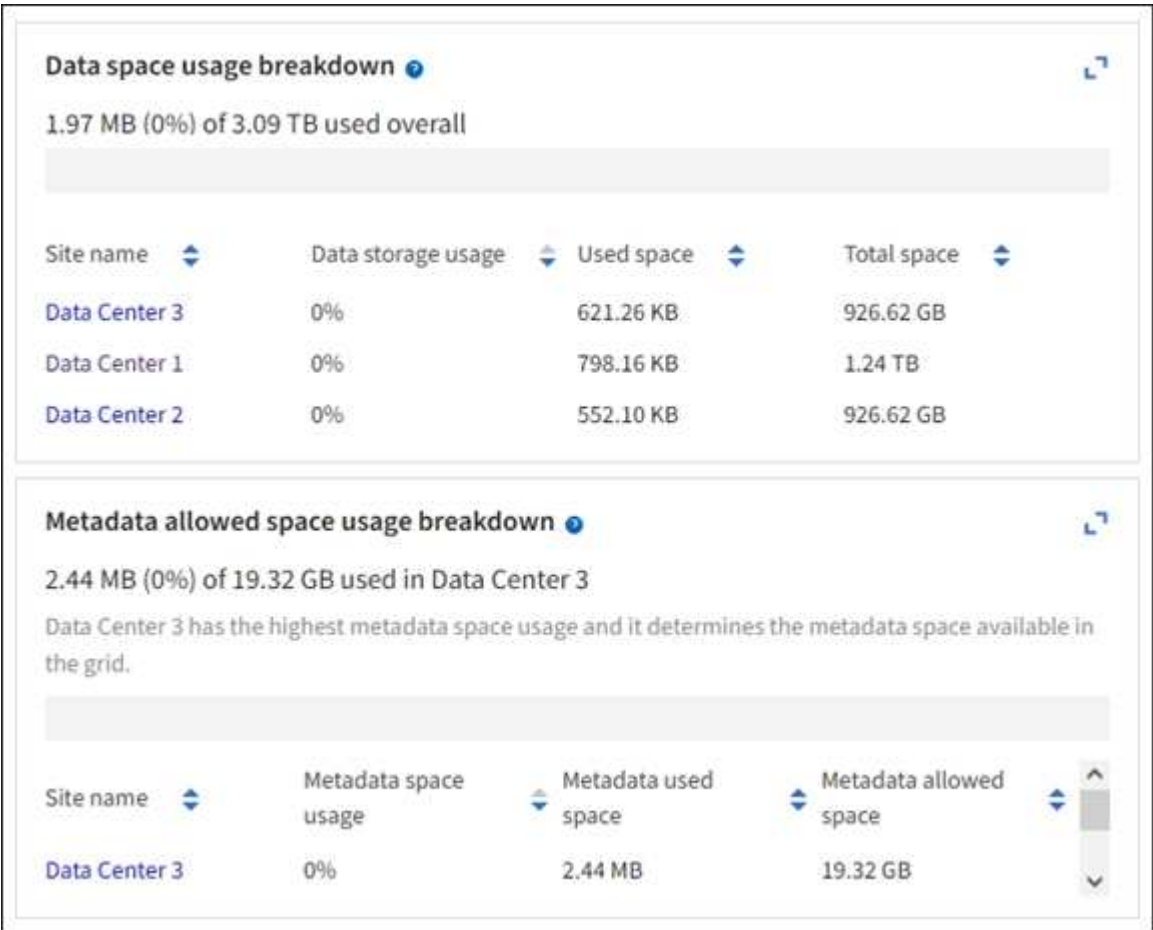
La dashboard di Grid Manager consente di valutare rapidamente la quantità di storage disponibile per l'intero grid e per ciascun data center. La pagina nodi fornisce valori più dettagliati per i dati degli oggetti e i metadati degli oggetti.

Fasi

- 1. Valutare la quantità di storage disponibile per l'intero grid e per ciascun data center.
 - a. Selezionare **Dashboard > Overview**.
 - b. Prendere nota dei valori riportati nelle schede di analisi dell'utilizzo dello spazio dati e delle schede di analisi dell'utilizzo dello spazio consentito dai metadati. Ciascuna scheda elenca una percentuale di utilizzo dello storage, la capacità dello spazio utilizzato e lo spazio totale disponibile o consentito dal sito.



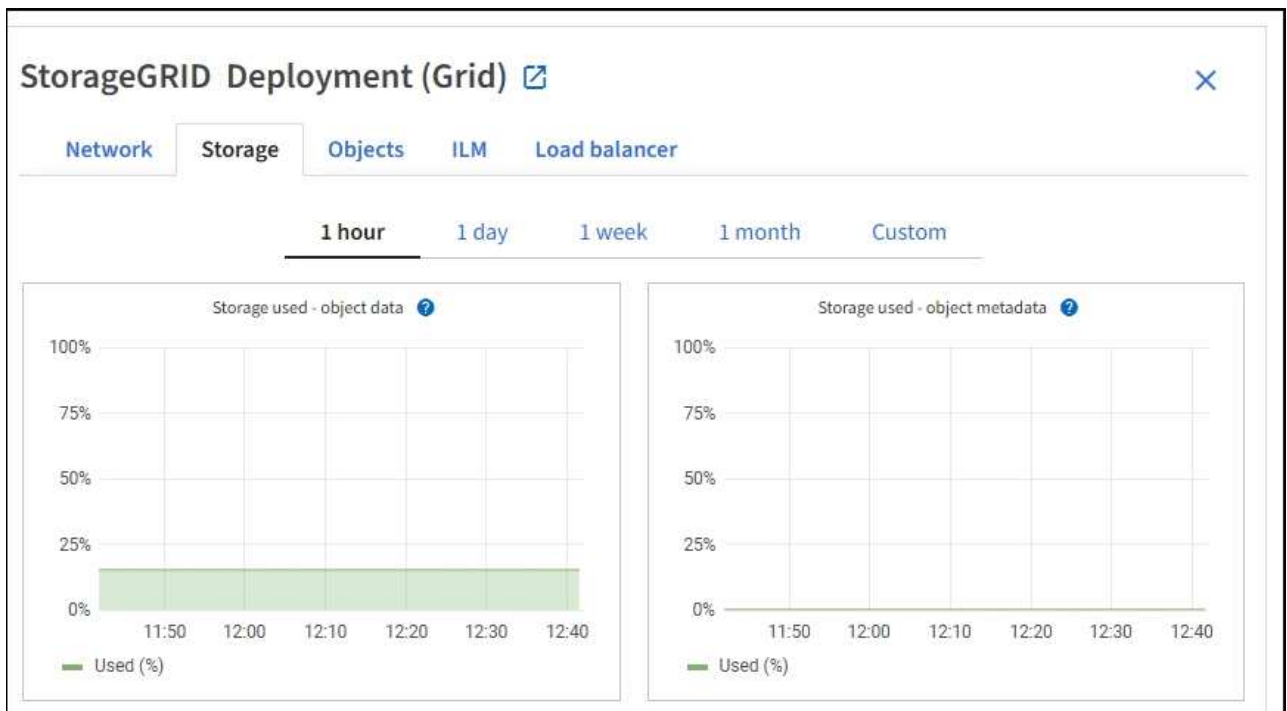
Il riepilogo non include i supporti di archiviazione.



- a. Annotare il grafico sulla scheda Storage over Time (archiviazione nel tempo). Utilizzare il menu a discesa Time Period (periodo di tempo) per determinare la velocità di utilizzo dello storage.



2. Utilizzare la pagina nodi per ulteriori dettagli sulla quantità di storage utilizzata e sulla quantità di storage disponibile nella griglia per i dati degli oggetti e i metadati degli oggetti.
 - a. Selezionare **Nodi**.
 - b. Selezionare **grid** > **Storage**.



- c. Posizionare il cursore sui grafici **Storage used - Object data** e **Storage used - Object metadata** per verificare la quantità di storage a oggetti e metadati a oggetti disponibile per l'intera griglia e la quantità di storage utilizzata nel tempo.



I valori totali di un sito o di un grid non includono nodi che non hanno riportato metriche per almeno cinque minuti, come i nodi offline.

3. Pianificare un'espansione per aggiungere nodi di storage o volumi di storage prima che la capacità di storage utilizzabile del grid venga consumata.

Quando si pianifica la tempistica di un'espansione, considerare quanto tempo sarà necessario per procurarsi e installare storage aggiuntivo.



Se la policy ILM utilizza la codifica erasure, è preferibile eseguire un'espansione quando i nodi di storage esistenti sono pieni al 70% circa per ridurre il numero di nodi da aggiungere.

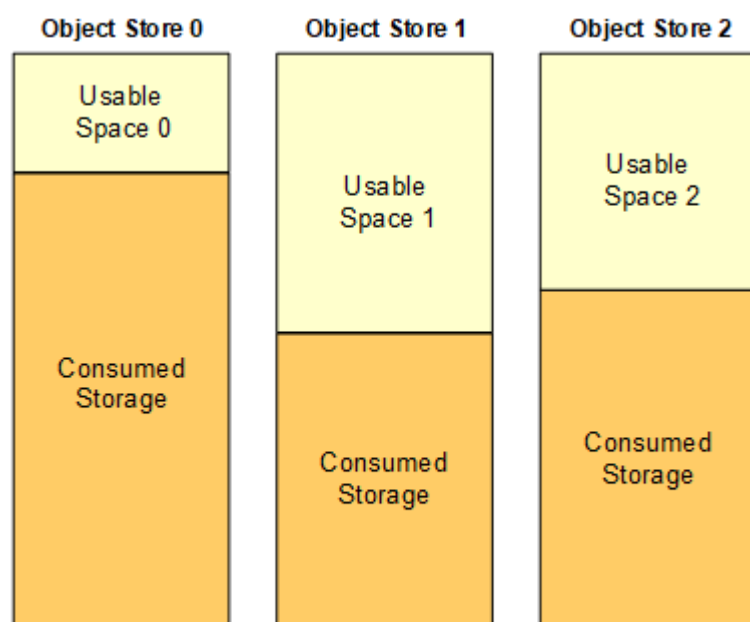
Per ulteriori informazioni sulla pianificazione di un'espansione di archiviazione, vedere ["Istruzioni per espandere StorageGRID"](#).

Monitorare la capacità di storage per ciascun nodo di storage

Monitorare lo spazio totale utilizzabile per ciascun nodo di storage per garantire che il nodo disponga di spazio sufficiente per i nuovi dati dell'oggetto.

A proposito di questa attività

Lo spazio utilizzabile è la quantità di spazio di storage disponibile per memorizzare gli oggetti. Lo spazio totale utilizzabile per un nodo di storage viene calcolato sommando lo spazio disponibile in tutti gli archivi di oggetti all'interno del nodo.



$$\text{Total Usable Space} = \text{Usable Space 0} + \text{Usable Space 1} + \text{Usable Space 2}$$

Fasi

1. Selezionare **Nodi > Nodo di archiviazione_ > Archiviazione**.

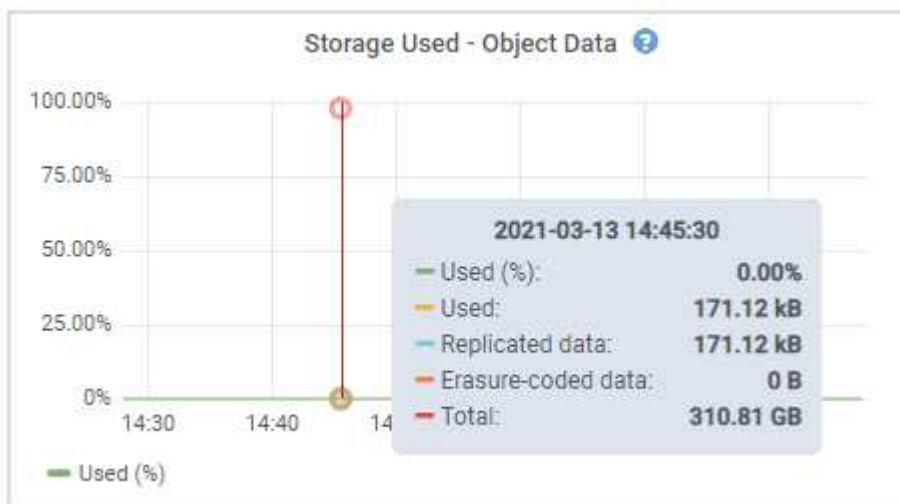
Vengono visualizzati i grafici e le tabelle del nodo.

2. Posizionare il cursore sul grafico Storage Used - Object data (Storage utilizzato - dati oggetto).

Vengono visualizzati i seguenti valori:

- **Used (%)**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto.
- **Used**: Quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
- **Dati replicati**: Stima della quantità di dati degli oggetti replicati su questo nodo, sito o griglia.
- **Erasure-coded data**: Stima della quantità di dati dell'oggetto con codifica di cancellazione su questo nodo, sito o griglia.

- **Total:** Quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è la `storagegrid_storage_utilization_data_bytes` metrica.



3. Esaminare i valori disponibili nelle tabelle volumi e archivi di oggetti, sotto i grafici.



Per visualizzare i grafici di questi valori, seleziona le icone dei grafici nelle colonne disponibili.

4. Monitorare i valori nel tempo per stimare il tasso di consumo dello spazio di storage utilizzabile.
5. Per mantenere le normali operazioni di sistema, aggiungere nodi di storage, aggiungere volumi di storage o archiviare i dati degli oggetti prima di consumare lo spazio utilizzabile.

Quando si pianifica la tempistica di un'espansione, considerare quanto tempo sarà necessario per procurarsi e installare storage aggiuntivo.



Se la policy ILM utilizza la codifica erasure, è preferibile eseguire un'espansione quando i nodi di storage esistenti sono pieni al 70% circa per ridurre il numero di nodi da aggiungere.

Per ulteriori informazioni sulla pianificazione di un'espansione di archiviazione, vedere ["Istruzioni per espandere StorageGRID"](#).

L'["Storage dei dati a oggetti basso"](#) avviso viene attivato quando rimane spazio insufficiente per l'archiviazione dei dati oggetto su un nodo di archiviazione.

Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage

Monitorare l'utilizzo dei metadati per ciascun nodo di storage per garantire che rimanga spazio sufficiente per le operazioni essenziali del database. È necessario aggiungere nuovi nodi di storage in ogni sito prima che i metadati dell'oggetto superino il 100% dello spazio consentito per i metadati.

A proposito di questa attività

StorageGRID conserva tre copie dei metadati degli oggetti in ogni sito per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita. Le tre copie vengono distribuite uniformemente su tutti i nodi di storage di ogni sito utilizzando lo spazio riservato ai metadati sul volume di storage 0 di ogni nodo di storage.

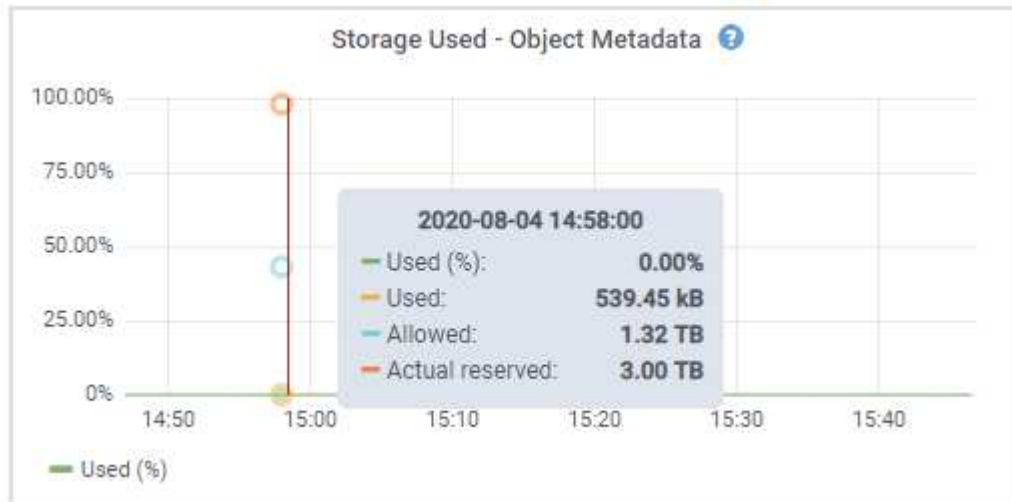
In alcuni casi, la capacità dei metadati degli oggetti della griglia potrebbe essere consumata più rapidamente

della capacità dello storage a oggetti. Ad esempio, se in genere si acquisiscono grandi quantità di oggetti di piccole dimensioni, potrebbe essere necessario aggiungere nodi di storage per aumentare la capacità dei metadati anche se rimane sufficiente capacità di storage a oggetti.

Alcuni dei fattori che possono aumentare l'utilizzo dei metadati includono la dimensione e la quantità di tag e metadati dell'utente, il numero totale di parti in un caricamento multiparte e la frequenza delle modifiche alle posizioni di storage ILM.

Fasi

1. Selezionare **Nodi > Nodo di archiviazione_ > Archiviazione**.
2. Posizionare il cursore sul grafico Storage Used - Object metadata (Storage utilizzato - metadati oggetto) per visualizzare i valori relativi a un orario specifico.



Utilizzato (%)

La percentuale dello spazio consentito per i metadati che è stato utilizzato su questo nodo di storage.

Metriche Prometheus: `storagegrid_storage_utilization_metadata_bytes` E.
`storagegrid_storage_utilization_metadata_allowed_bytes`

Utilizzato

I byte dello spazio di metadati consentito che sono stati utilizzati su questo nodo di storage.

Metrica Prometheus: `storagegrid_storage_utilization_metadata_bytes`

Consentito

Lo spazio consentito per i metadati dell'oggetto su questo nodo di storage. Per informazioni su come questo valore è determinato per ogni nodo di archiviazione, vedere la ["Descrizione completa dello spazio consentito per i metadati"](#).

Metrica Prometheus: `storagegrid_storage_utilization_metadata_allowed_bytes`

Riservato

Lo spazio effettivo riservato ai metadati su questo nodo di storage. Include lo spazio consentito e lo spazio richiesto per le operazioni essenziali dei metadati. Per informazioni su come viene calcolato questo valore per ciascun nodo di archiviazione, vedere la ["Descrizione completa dello spazio riservato effettivo per i metadati"](#).

La metrica Prometheus verrà aggiunta in una release futura.



I valori totali di un sito o di un grid non includono nodi che non hanno riportato metriche per almeno cinque minuti, come i nodi offline.

- Se il valore **utilizzato (%)** è pari o superiore al 70%, espandere il sistema StorageGRID aggiungendo nodi di storage a ciascun sito.



L'avviso **Low metadata storage** viene attivato quando il valore **used (%)** raggiunge determinate soglie. I risultati indesiderati possono verificarsi se i metadati dell'oggetto utilizzano più del 100% dello spazio consentito.

Quando si aggiungono nuovi nodi, il sistema ribilancia automaticamente i metadati degli oggetti in tutti i nodi di storage all'interno del sito. Consultare la ["Istruzioni per espandere un sistema StorageGRID"](#).

Monitorare le previsioni di utilizzo dello spazio

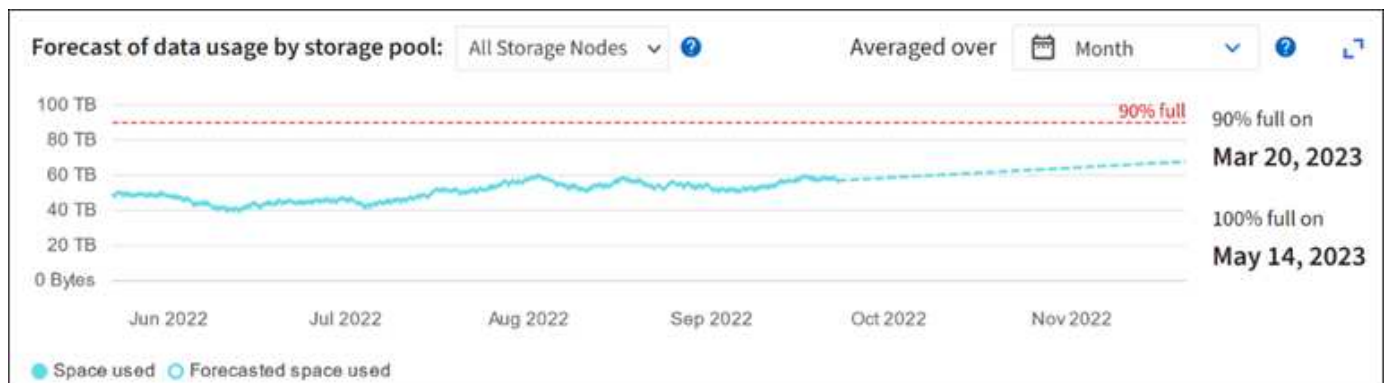
Monitorare le previsioni di utilizzo dello spazio per i dati utente e i metadati per stimare quando sarà necessario ["espandere una griglia"](#).

Se si nota che il tasso di consumo cambia nel tempo, selezionare un intervallo più breve dal menu a discesa **mediato su** per riflettere solo i modelli di acquisizione più recenti. Se si notano schemi stagionali, selezionare un intervallo più lungo.

Se si dispone di una nuova installazione StorageGRID, consentire l'accumulo di dati e metadati prima di valutare le previsioni di utilizzo dello spazio.

Fasi

- Nella dashboard, selezionare **Storage**.
- Visualizza le schede della dashboard, la previsione dell'utilizzo dei dati per pool di storage e la previsione dell'utilizzo dei metadati per sito.
- Utilizza questi valori per valutare quando sarà necessario aggiungere nuovi nodi di storage per lo storage di dati e metadati.



Monitorare la gestione del ciclo di vita delle informazioni in StorageGRID

Il sistema ILM (Information Lifecycle Management) fornisce la gestione dei dati per tutti gli oggetti memorizzati nella griglia. È necessario monitorare le operazioni ILM per capire se la griglia è in grado di gestire il carico corrente o se sono necessarie più risorse.

A proposito di questa attività

Il sistema StorageGRID gestisce gli oggetti applicando i criteri ILM attivi. I criteri ILM e le regole ILM associate determinano il numero di copie eseguite, il tipo di copie create, il luogo in cui vengono collocate e la durata di conservazione di ciascuna copia.

L'acquisizione di oggetti e altre attività correlate agli oggetti possono superare la velocità con cui StorageGRID può valutare ILM, causando la messa in coda degli oggetti le cui istruzioni di posizionamento ILM non possono essere soddisfatte quasi in tempo reale. È necessario controllare se StorageGRID è al passo con le azioni del client.

USA la scheda del pannello di controllo di Grid Manager

Fasi

Utilizzare la scheda ILM nella dashboard di Grid Manager per monitorare le operazioni ILM:

1. Accedi a Grid Manager.
2. Dal dashboard, selezionare la scheda ILM e annotare i valori sulla scheda coda ILM (oggetti) e sulla scheda velocità di valutazione ILM.

Sono previsti picchi temporanei nella scheda della coda ILM (oggetti) sul dashboard. Ma se la coda continua ad aumentare e non diminuisce mai, la griglia necessita di più risorse per funzionare in modo efficiente: Più nodi di storage o, se il criterio ILM colloca gli oggetti in posizioni remote, una maggiore larghezza di banda della rete.

Utilizzare la pagina Nodi

Fasi

Inoltre, esaminare le code ILM utilizzando la pagina **Nodi**:



I grafici nella pagina **Nodi** verranno sostituiti con le schede della dashboard corrispondenti in una futura versione StorageGRID .

1. Selezionare **Nodi**.
2. Selezionare **grid name > ILM**.
3. Posizionare il cursore sul grafico della coda ILM per visualizzare il valore dei seguenti attributi in un determinato momento:
 - **Oggetti accodati (da operazioni client)**: Il numero totale di oggetti in attesa di valutazione ILM a causa delle operazioni del client (ad esempio, acquisizione).
 - **Oggetti accodati (da tutte le operazioni)**: Il numero totale di oggetti in attesa di valutazione ILM.
 - **Scan rate (objects/sec)**: La velocità con cui gli oggetti nella griglia vengono sottoposti a scansione e messi in coda per ILM.
 - **Evaluation rate (objects/sec)**: La velocità corrente alla quale gli oggetti vengono valutati rispetto alla policy ILM nella griglia.



La sezione coda ILM è inclusa solo per la griglia. Queste informazioni non vengono visualizzate nella scheda ILM per un sito o un nodo di storage.

4. Nella sezione ILM Queue (coda ILM), esaminare i seguenti attributi.
 - **Periodo di scansione - stimato**: Il tempo stimato per completare una scansione ILM completa di tutti

gli oggetti.



Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti.

- **Riparazioni tentate:** Il numero totale di operazioni di riparazione degli oggetti per i dati replicati che sono stati tentati. Questo numero aumenta ogni volta che un nodo di storage tenta di riparare un oggetto ad alto rischio. Le riparazioni ILM ad alto rischio hanno la priorità se la rete diventa occupata.

La 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.

5. In alternativa, invia una query Prometheus per
`storagegrid_ilm_scan_period_estimated_minutes` E
`storagegrid_ilm_repairs_attempted`.

Monitora le risorse di rete e di sistema in StorageGRID

L'integrità e la larghezza di banda della rete tra nodi e siti, nonché l'utilizzo delle risorse da parte dei singoli nodi di rete, sono fondamentali per operazioni efficienti.

Monitorare le connessioni di rete e le performance

La connettività di rete e la larghezza di banda sono particolarmente importanti se il criterio ILM (Information Lifecycle Management) copia gli oggetti replicati tra siti o archivia oggetti con codifica di cancellazione utilizzando uno schema che fornisce la protezione dalla perdita di sito. Se la rete tra siti non è disponibile, la latenza di rete è troppo elevata o la larghezza di banda della rete è insufficiente, alcune regole ILM potrebbero non essere in grado di posizionare oggetti dove previsto. Questo può portare a errori di acquisizione (quando l'opzione di acquisizione rigorosa è selezionata per le regole ILM) o a scarse performance di acquisizione e backlog ILM.

Utilizza Grid Manager per monitorare la connettività e le performance di rete, in modo da poter risolvere tempestivamente qualsiasi problema.

Inoltre, è importante "[creazione di criteri di classificazione del traffico di rete](#)" monitorare il traffico relativo a tenant, bucket, subnet o endpoint del bilanciamento del carico specifici. È possibile impostare criteri di limitazione del traffico in base alle esigenze.

Fasi

1. Selezionare **Nodi**.

Viene visualizzata la pagina nodi. Ciascun nodo della griglia viene elencato in formato tabella.

DASHBOARD

ALERTS ✓

Current

Resolved

Silences

Rules

Email setup

NODES

TENANTS

ILM

CONFIGURATION

MAINTENANCE

SUPPORT

Nodes

View the list and status of sites and grid nodes.

Search...

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%

- Selezionare il nome della griglia, un sito del data center specifico o un nodo della griglia, quindi selezionare la scheda **Network**.

Il grafico del traffico di rete fornisce un riepilogo del traffico di rete complessivo per l'intera griglia, il sito del data center o il nodo.



- Se è stato selezionato un nodo della griglia, scorrere verso il basso per esaminare la sezione **Network Interfaces** 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

- Per i nodi della griglia, scorrere verso il basso per esaminare la sezione **Network Communication** della pagina.

Le tabelle di ricezione e trasmissione mostrano quanti byte e pacchetti sono stati ricevuti e inviati attraverso ciascuna rete, nonché altre metriche di ricezione e trasmissione.

3. Utilizza le metriche associate alle policy di classificazione del traffico per monitorare il traffico di rete.

a. Selezionare **Configurazione > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

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-7665bdc894b
Displaying 2 traffic classification policies.		

a. Per visualizzare i grafici che mostrano le metriche di rete associate a una policy, seleziona il pulsante di opzione a sinistra della policy e poi seleziona **Metriche**.

b. Esaminare i grafici per comprendere il traffico di rete associato alla policy.

Se un criterio di classificazione del traffico è progettato per limitare il traffico di rete, analizzare la frequenza con cui il traffico è limitato e decidere se il criterio continua a soddisfare le proprie esigenze. Di tanto in tanto, ["modificare ogni policy di classificazione del traffico in base alle esigenze"](#).

Informazioni correlate

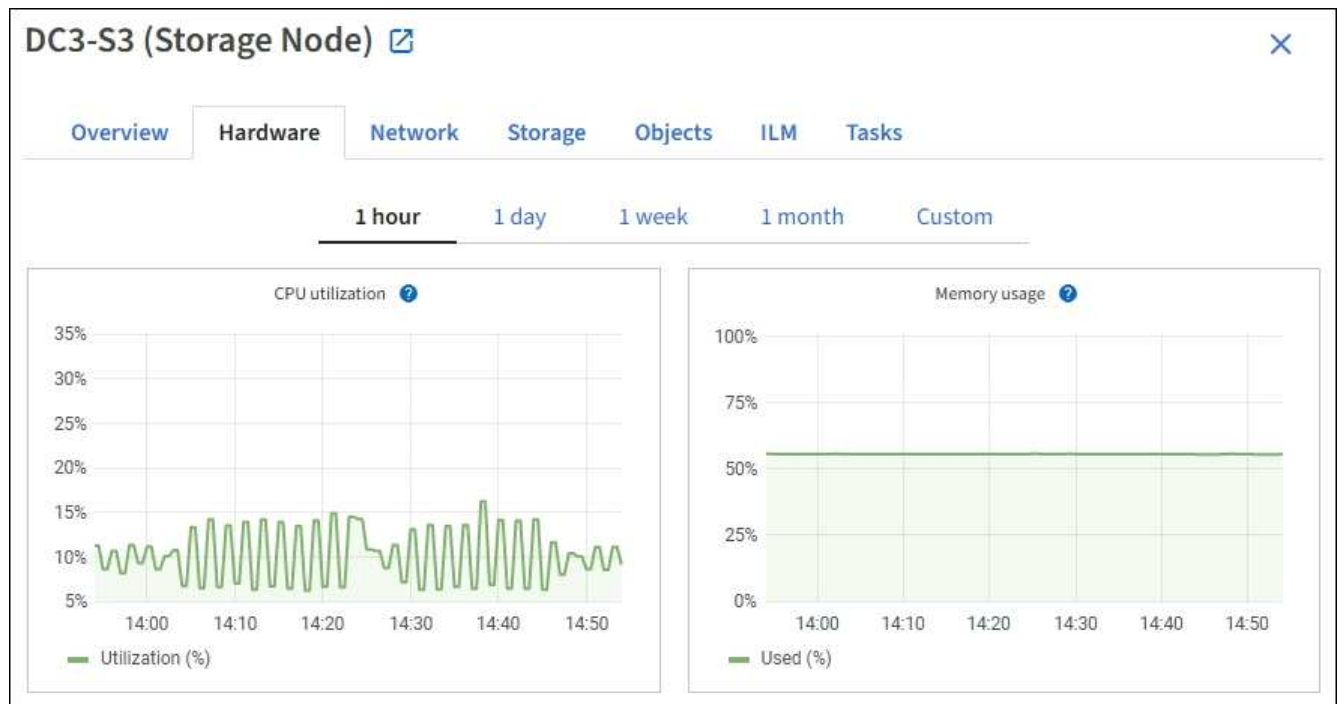
- ["Visualizzare la scheda rete"](#)
- ["Monitorare gli stati di connessione del nodo"](#)

Monitorare le risorse a livello di nodo

Monitorare i singoli nodi di griglia per verificare i livelli di utilizzo delle risorse. Se i nodi sono costantemente sovraccarichi, potrebbero essere necessari più nodi per operazioni efficienti.

Fasi

1. Dalla pagina **Nodi**, seleziona il nodo.
2. Selezionare la scheda **hardware** per visualizzare i grafici relativi all'utilizzo della CPU e della memoria.



3. Per visualizzare un intervallo di tempo diverso, selezionare uno dei comandi sopra il grafico o il grafico. È possibile visualizzare le informazioni disponibili per intervalli di 1 ora, 1 giorno, 1 settimana o 1 mese. È inoltre possibile impostare un intervallo personalizzato, che consente di specificare intervalli di data e ora.
4. Se il nodo è ospitato su un'appliance di storage o su un'appliance di servizi, scorrere verso il basso per visualizzare le tabelle dei componenti. Lo stato di tutti i componenti deve essere "nominale". Esaminare i componenti che presentano qualsiasi altro stato.

Informazioni correlate

- ["Visualizza informazioni sui nodi di storage dell'appliance"](#)
- ["Visualizza informazioni sui nodi di amministrazione dell'appliance e sui nodi gateway"](#)

Monitorare l'attività dei tenant in StorageGRID

Tutte le attività client S3 sono associate agli account tenant StorageGRID. È possibile utilizzare Grid Manager per monitorare l'utilizzo dello storage o il traffico di rete di tutti i tenant o di uno specifico tenant. È possibile utilizzare il registro di controllo o le dashboard Grafana per ottenere informazioni più dettagliate sull'utilizzo di StorageGRID da parte dei tenant.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Accesso root o autorizzazione account tenant"](#).

Visualizza tutti i tenant

La pagina tenant mostra le informazioni di base per tutti gli account tenant correnti.

Fasi

1. Selezionare **Inquilini**.

2. Esaminare le informazioni visualizzate nelle pagine del tenant.

Lo spazio logico utilizzato, l'utilizzo della quota, la quota e il numero di oggetti sono elencati per ogni tenant. Se una quota non è impostata per un tenant, i campi utilizzo quota e quota contengono un trattino (—).



La dimensione logica di tutti gli oggetti appartenenti a questo tenant include caricamenti multiparte incompleti e in corso. Le dimensioni non includono lo spazio fisico aggiuntivo utilizzato per le policy ILM. 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, effettua il Sign in a un tenant account selezionando il link di Sign in → nella colonna **Sign in/Copy URL**.
4. Facoltativamente, puoi copiare l'URL della pagina di Sign in di un tenant selezionando il link Copia URL 📄 nella colonna **Sign in/Copia URL**.
5. In alternativa, selezionare **Esporta in CSV** per visualizzare ed esportare un .csv file contenente i valori di utilizzo per tutti i tenant.

Viene richiesto di aprire o salvare il .csv file.

Il contenuto del .csv file è simile al seguente esempio:

Tenant ID	Display Name	Space Used (Bytes)	Quota utilization (%)	Quota (Bytes)	Object Count	Protocol
12659822378459233654	Tenant 01	2000000000	10	20000000000	100	S3
99658234112547853685	Tenant 02	85000000000	85	1100000000	500	S3
03521145586975586321	Tenant 03	60500000000	50	150000	10000	S3
44251365987569885632	Tenant 04	47500000000	95	1400000000	50000	S3
36521587546689565123	Tenant 05	50000000000	Infinity		500	S3

È possibile aprire il .csv file in un foglio di calcolo o utilizzarlo in automazione.

6. Se non sono presenti oggetti nell'elenco, selezionare **azioni > Elimina** per rimuovere uno o più tenant. Vedere "Elimina account tenant".

Non puoi rimuovere un account tenant se l'account include bucket o container.

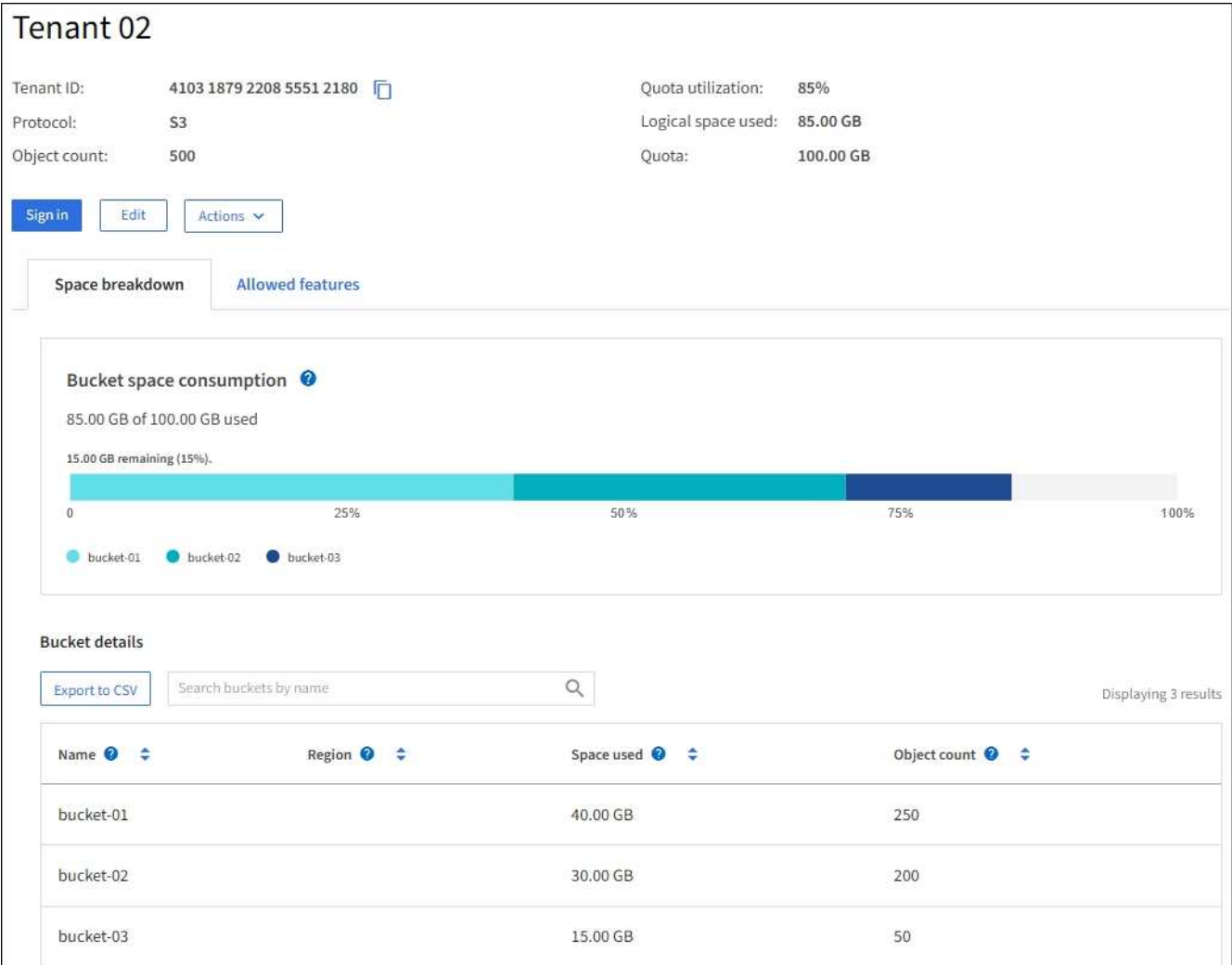
Visualizzare un tenant specifico

È possibile visualizzare i dettagli di un tenant specifico.

Fasi

- 1. Selezionare il nome del tenant dalla pagina tenant.

Viene visualizzata la pagina dei dettagli del tenant.



- 2. Esaminare la panoramica del tenant nella parte superiore della pagina.

Questa sezione della pagina dei dettagli fornisce informazioni di riepilogo per il tenant, tra cui il numero di oggetti del tenant, l'utilizzo della quota, lo spazio logico utilizzato e l'impostazione della quota.



La dimensione logica di tutti gli oggetti appartenenti a questo tenant include caricamenti multiparte incompleti e in corso. Le dimensioni non includono lo spazio fisico aggiuntivo utilizzato per le policy ILM. I valori dello spazio utilizzato sono stime. Tali stime sono influenzate dalla tempistica degli ingest, dalla connettività di rete e dallo stato del nodo.

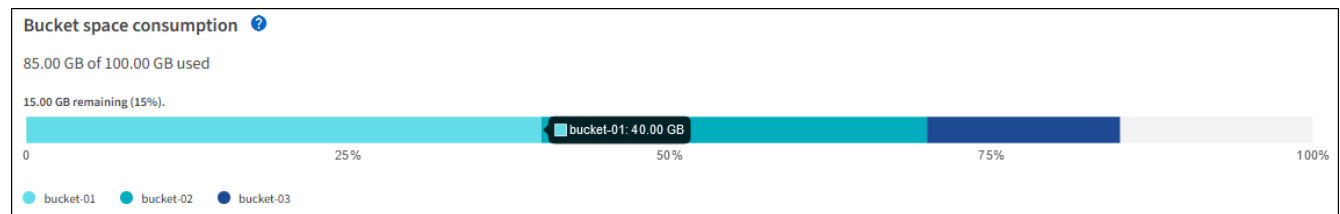
- 3. Dalla scheda **Space disruption** (suddivisione spazio), esaminare il grafico **Space Consumption**

(consumo spazio).

Questo grafico mostra il consumo di spazio totale 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 nel 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 container. Se il tenant ha superato la quota di storage di oltre l'1% e di almeno 1 GB, il grafico mostra la quota totale e la quantità in eccesso.

È possibile posizionare il cursore sul grafico a barre per visualizzare lo storage utilizzato da ciascun bucket o container. È possibile posizionare il cursore sul segmento di spazio libero per visualizzare la quantità di spazio rimanente.



L'utilizzo delle quote si basa su stime interne e in alcuni casi potrebbe essere superato. Ad esempio, StorageGRID controlla la quota quando un tenant avvia il caricamento degli oggetti e rifiuta le nuove ricerche se il tenant ha superato la quota. Tuttavia, StorageGRID non tiene conto delle dimensioni del caricamento corrente quando determina se la quota è stata superata. Se gli oggetti vengono eliminati, a un tenant potrebbe essere temporaneamente impedito di caricare nuovi oggetti fino a quando l'utilizzo della quota non viene ricalcolato. I calcoli relativi all'utilizzo delle quote possono richiedere 10 minuti o più.



L'utilizzo della quota di un tenant indica la quantità totale di dati oggetto caricati dal tenant su StorageGRID (dimensione logica). L'utilizzo della quota non rappresenta lo spazio utilizzato per memorizzare copie degli oggetti e dei relativi metadati (dimensioni fisiche).



È possibile attivare la regola di avviso **quota elevata utilizzo tenant** per determinare se i tenant consumano le proprie quote. Se attivato, questo avviso viene attivato quando un tenant utilizza il 90% della propria quota. Per istruzioni, vedere ["Modificare le regole degli avvisi"](#).

4. Dalla scheda **Space breakdown** (suddivisione spazio), rivedere i **Bucket details** (Dettagli bucket).

Questa tabella elenca i bucket S3 per il tenant. Lo spazio utilizzato è la quantità totale di dati dell'oggetto nel bucket o nel container. Questo valore non rappresenta lo spazio di storage richiesto per le copie ILM e i metadati degli oggetti.

5. Facoltativamente, selezionare **Export to CSV** (Esporta in CSV) per visualizzare ed esportare un file .csv contenente i valori di utilizzo per ciascun bucket o container.

Il contenuto di un singolo file del tenant S3 .csv è simile al seguente esempio:

Tenant ID	Bucket Name	Space Used (Bytes)	Number of Objects
64796966429038923647	bucket-01	88717711	14
64796966429038923647	bucket-02	21747507	11
64796966429038923647	bucket-03	15294070	3

È possibile aprire il .csv file in un foglio di calcolo o utilizzarlo in automazione.

- Se si desidera, selezionare la scheda **funzioni consentite** per visualizzare un elenco delle autorizzazioni e delle funzionalità attivate per il tenant. Vedere ["Modificare l'account tenant"](#) se è necessario modificare queste impostazioni.
- Se il tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **federazione griglia** per ulteriori informazioni sulla connessione.

Vedere ["Che cos'è la federazione di griglie?"](#) e ["Gestire i tenant consentiti per la federazione di grid"](#).

Visualizzare il traffico di rete

Se per un tenant sono in vigore criteri di classificazione del traffico, esaminare il traffico di rete per tale tenant.

Fasi

- Selezionare **Configurazione > Rete > Classificazione del traffico**.

Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.

- Esaminare l'elenco delle policy per identificare quelle applicabili a un tenant specifico.
- Per visualizzare le metriche associate a un criterio, selezionare il pulsante di opzione a sinistra del criterio e selezionare **metriche**.
- Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Per ulteriori informazioni, vedere ["Gestire le policy di classificazione del traffico"](#).

Utilizzare il registro di controllo

Facoltativamente, è possibile utilizzare il registro di audit per un monitoraggio più granulare delle attività di un tenant.

Ad esempio, è possibile monitorare i seguenti tipi di informazioni:

- Operazioni client specifiche, come PUT, GET o DELETE
- Dimensioni degli oggetti
- La regola ILM applicata agli oggetti
- L'IP di origine delle richieste del client

I registri di audit vengono scritti in file di testo che è possibile analizzare utilizzando lo strumento di analisi dei log scelto. Ciò consente di comprendere meglio le attività del cliente o di implementare sofisticati modelli di chargeback e fatturazione.

Per ulteriori informazioni, vedere ["Esaminare i registri di audit"](#).

Utilizza le metriche Prometheus

Facoltativamente, utilizza le metriche Prometheus per generare report sull'attività del tenant.

- In 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'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali.

- Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**. È possibile utilizzare le metriche nella sezione metriche dell'API Grid Management per creare regole di avviso e dashboard personalizzati per l'attività del tenant.

Per ulteriori informazioni, vedere ["Rivedere le metriche di supporto"](#).

Monitorare le operazioni del client S3 in StorageGRID

È possibile monitorare i tassi di acquisizione e recupero degli oggetti, nonché le metriche per i conteggi degli oggetti, le query e la verifica. È possibile visualizzare il numero di tentativi riusciti e non riusciti da parte delle applicazioni client di lettura, scrittura e modifica degli oggetti nel sistema StorageGRID.

Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

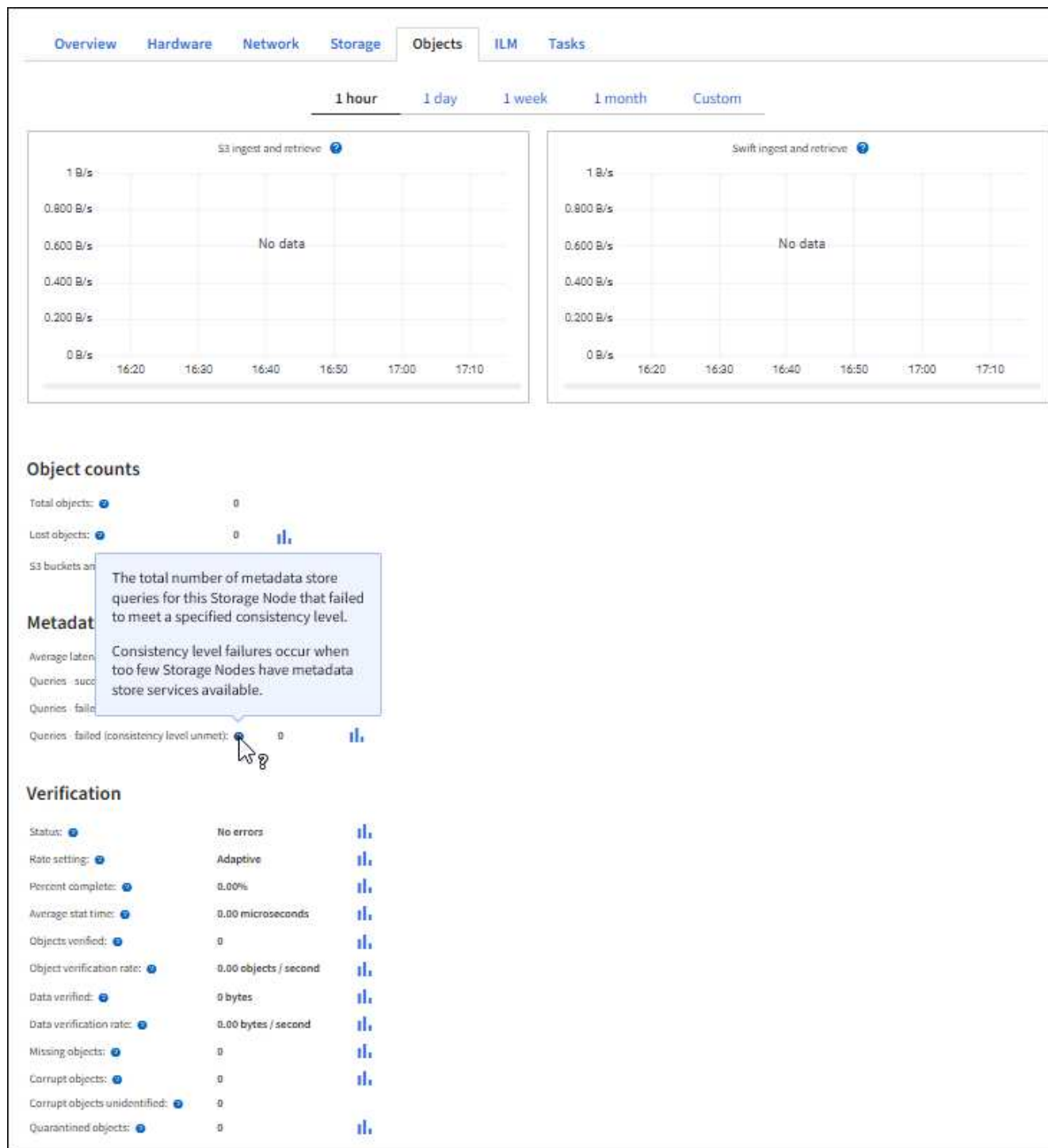
Fasi

1. Dalla dashboard, selezionare la scheda **prestazioni**.
2. Fare riferimento ai grafici S3, che riassumono 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), selezionare la scheda **oggetti**.

Il grafico mostra i tassi di acquisizione e recupero di S3 kb dell'intero sistema StorageGRID in byte al secondo e la quantità di dati acquisiti o recuperati. È possibile selezionare un intervallo di tempo o applicare un intervallo personalizzato.

5. Per visualizzare le informazioni relative a un determinato nodo di archiviazione, selezionare il nodo dall'elenco a sinistra e selezionare la scheda **oggetti**.

Il grafico mostra le velocità di acquisizione e recupero per il nodo. Questa scheda include inoltre metriche per il numero di oggetti, le query sui metadati e le operazioni di verifica.



Monitorare le operazioni di bilanciamento del carico in StorageGRID

Se si utilizza un bilanciamento del carico per gestire le connessioni client a StorageGRID, è necessario monitorare le operazioni di bilanciamento del carico dopo aver configurato il sistema inizialmente e dopo aver apportato modifiche alla configurazione o aver eseguito un'espansione.

A proposito di questa attività

È possibile utilizzare il servizio Load Balancer sui nodi Admin o Gateway o un bilanciamento del carico esterno di terze parti per distribuire le richieste dei client su più nodi di storage.

Dopo aver configurato il bilanciamento del carico, è necessario confermare che le operazioni di recupero e acquisizione degli oggetti vengono distribuite uniformemente tra i nodi di storage. Le richieste distribuite in modo uniforme garantiscono che StorageGRID rimanga reattivo alle richieste dei client sotto carico e possa contribuire a mantenere le performance dei client.

Se è stato configurato un gruppo ad alta disponibilità (ha) di nodi gateway o nodi di amministrazione in modalità Active-backup, solo un nodo del gruppo distribuisce attivamente le richieste dei client.

Per ulteriori informazioni, vedere ["Configurare connessioni client S3"](#).

Fasi

1. Se i client S3 si connettono utilizzando il servizio Load Balancer, controllare che i nodi Admin o Gateway distribuiscono attivamente il traffico come previsto:
 - a. Selezionare **Nodi**.
 - b. Selezionare un nodo gateway o un nodo amministratore.
 - c. Nella scheda **Overview**, verificare se un'interfaccia di nodo è in un gruppo ha e se l'interfaccia di nodo ha il ruolo di primario.

I nodi con il ruolo di primario e i nodi che non fanno parte di un gruppo ha devono distribuire attivamente le richieste ai client.

- d. Per ogni nodo che deve distribuire attivamente le richieste client, selezionare ["Scheda bilanciamento del carico"](#).

- e. Esaminare il grafico del traffico di richiesta del bilanciamento del carico dell'ultima settimana per assicurarsi che il nodo stia distribuendo attivamente le richieste.

I nodi di un gruppo ha con backup attivo potrebbero assumere di tanto in tanto il ruolo di backup. Durante questo periodo, i nodi non distribuiscono le richieste dei client.

- f. Esaminare il grafico del tasso di richiesta in entrata del bilanciamento del carico dell'ultima settimana per esaminare il throughput degli oggetti del nodo.
 - g. Ripetere questi passaggi per ogni nodo amministratore o nodo gateway nel sistema StorageGRID.
 - h. Facoltativamente, utilizzare le policy di classificazione del traffico per visualizzare un'analisi più dettagliata del traffico fornito dal servizio Load Balancer.

2. Verificare che queste richieste vengano distribuite uniformemente ai nodi di storage.

- a. Selezionare **Storage Node > LDR > HTTP**.
 - b. Esaminare il numero di **sessioni in entrata attualmente stabilite**.
 - c. Ripetere l'operazione per ogni nodo di storage nella griglia.

Il numero di sessioni deve essere approssimativamente uguale in tutti i nodi di storage.

Monitorare le connessioni della federazione della griglia StorageGRID

È possibile monitorare le informazioni di base su tutto ["connessioni a federazione di griglie"](#), le informazioni dettagliate su una connessione specifica o le metriche Prometheus sulle operazioni di replica cross-grid. È possibile monitorare una connessione da entrambe le griglie.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager su una delle due griglie utilizzando un ["browser web supportato"](#).
- Si dispone del ["Autorizzazione di accesso root"](#) per la griglia a cui si è effettuato l'accesso.

Visualizza tutte le connessioni

La pagina Grid Federation mostra informazioni di base su tutte le connessioni a federazione di griglie e su tutti gli account tenant autorizzati a utilizzare le connessioni a federazione di griglie.

Fasi

1. Selezionare **Configurazione > Sistema > Federazione di griglia**.

Viene visualizzata la pagina Grid Federation.

2. Per visualizzare le informazioni di base su tutte le connessioni in questa griglia, selezionare la scheda **connessioni**.

Da questa scheda è possibile:

- ["Creare una nuova connessione"](#).
- Selezionare una connessione esistente a ["modifica o verifica"](#).

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

[Add connection](#) [Upload verification file](#) [Actions](#) Search... Displaying 1 connection

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 di questa griglia che dispongono dell'autorizzazione **Usa connessione federazione griglia**, selezionare la scheda **tenant consentiti**.

Da questa scheda è possibile:

- ["Visualizza la pagina dei dettagli per ciascun tenant consentito"](#).
- Visualizzare la pagina dei dettagli per ciascuna connessione. Vedere [Visualizzare una connessione specifica](#).
- Selezionare un tenant consentito e ["rimuovere l'autorizzazione"](#).
- Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore, se presente. Vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

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 connessione a federazione di griglie specifica.

Fasi

1. Selezionare una delle schede dalla pagina Grid Federation, quindi selezionare il nome della connessione dalla tabella.

Dalla pagina dei dettagli per la connessione, è possibile:

- Consultare le informazioni di base sullo stato della connessione, inclusi i nomi host locali e remoti, la porta e lo stato della connessione.
- Selezionare una connessione a ["modifica, verifica o rimozione"](#).

2. Quando si visualizza una connessione specifica, selezionare la scheda **tenant consentiti** per visualizzare i dettagli relativi ai tenant consentiti per la connessione.

Da questa scheda è possibile:

- ["Visualizza la pagina dei dettagli per ciascun tenant consentito"](#).
- ["Rimuovere l'autorizzazione di un tenant"](#) per utilizzare la connessione.
- Verificare la presenza di errori di replica tra griglie e cancellare l'ultimo errore. Vedere ["Risolvere i problemi relativi agli errori di federazione della griglia"](#).

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](#) 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 è possibile:

- ["Ruotare i certificati di connessione"](#).
- Selezionare **Server** o **Client** per visualizzare o scaricare il certificato associato o copiare il PEM del certificato.

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

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-----
MIIGdTCBFB2gAwIBAgIIIMG43a6yhgowDQYJKoZIhvcNAQENBQAwZDZELMAKGAIUE
HBMCVVmxExeARBGNVBAgMCKNhbg1mb3JuaWxleXJAQBGNVBACMCVn1bm55dmf5ZTEU
AHTCCTFhCzEwMDk0MTIwOTY0ZABGAzBNVBASMEFLDEFjCBKGG9wdlR1L1I=

3. Per riprovare la replica degli oggetti che non sono stati replicati, vedere ["Identificare e riprovare le operazioni di replica non riuscite"](#).

Gestire gli avvisi

Gestisci gli avvisi in StorageGRID

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

Gli avvisi vengono attivati a livelli di severità specifici quando le condizioni delle regole di avviso vengono valutate come vere. Quando viene attivato un avviso, si verificano le seguenti azioni:

- Sul dashboard di Grid Manager viene visualizzata un'icona di severità degli avvisi e il numero di avvisi correnti viene incrementato.
- L'avviso viene visualizzato nella pagina di riepilogo **Nodi** e nella scheda **Nodi > nodo > Panoramica**.
- Viene inviata una notifica e-mail, presupponendo che sia stato configurato un server SMTP e che siano stati forniti indirizzi e-mail per i destinatari.
- Viene inviata una notifica SNMP (Simple Network Management Protocol), presupponendo che l'agente SNMP StorageGRID sia stato configurato.

È possibile creare avvisi personalizzati, modificare o disattivare gli avvisi e gestire le notifiche degli avvisi.

Per saperne di più:

- Rivedi i video:

[Panoramica degli avvisi](#)

[Avvisi personalizzati](#)

- Fare riferimento al ["Riferimenti agli avvisi"](#).

Visualizza le regole di avviso di StorageGRID

Le regole di avviso definiscono le condizioni che attivano ["avvisi specifici"](#). StorageGRID include una serie di regole di avviso predefinite, che è possibile utilizzare così com'è o modificare, oppure è possibile creare regole di avviso personalizzate.

È possibile visualizzare l'elenco di tutte le regole di avviso predefinite e personalizzate per scoprire quali condizioni attiveranno ciascun avviso e per verificare se gli avvisi sono disattivati.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).
- Facoltativamente, hai guardato il video:

[Panoramica degli avvisi](#)

Fasi

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 univoco e descrizione della regola di avviso. Vengono elencate per prime le regole di avviso personalizzate, seguite dalle regole di avviso predefinite. Il nome della regola di avviso è l'oggetto delle notifiche e-mail.

Intestazione di colonna	Descrizione
Condizioni	Le espressioni Prometheus che determinano quando viene attivato questo avviso. Un avviso può essere attivato in uno o più dei seguenti livelli di severità, ma non è richiesta alcuna condizione per ogni severità. • Critico : Esiste una condizione anomala che ha interrotto le normali operazioni di un nodo o servizio StorageGRID. Devi risolvere immediatamente il problema alla radice. 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 si sta avvicinando alla soglia per un avviso critico. Dovresti esaminare gli avvisi gravi e risolvere eventuali problemi sottostanti per assicurarti che la condizione anomala non interrompa il normale funzionamento di un nodo o servizio StorageGRID. • Minore : Il sistema funziona normalmente, ma è presente una condizione anomala che potrebbe influire sulla capacità del sistema di funzionare se persiste. Dovresti monitorare e risolvere gli avvisi minori che non si risolvono da soli per assicurarti che non causino un problema più serio.
Tipo	Il tipo di regola di avviso: • Default: Una regola di avviso fornita con il sistema. È possibile disattivare una regola di avviso predefinita o modificare le condizioni e la durata di una regola di avviso predefinita. Non è possibile rimuovere una regola di avviso predefinita. • Default*: Una regola di avviso predefinita che include una condizione o una durata modificate. Se necessario, è possibile ripristinare facilmente le impostazioni predefinite originali di una condizione modificata. • Personalizzato: Una regola di avviso creata dall'utente. È possibile disattivare, modificare e rimuovere regole di avviso personalizzate.
Stato	Se questa regola di avviso è attualmente attivata o disattivata. Le condizioni per le regole di avviso disabilitate non vengono valutate, quindi non vengono attivati avvisi.

Crea regole di avviso personalizzate in StorageGRID

È possibile creare regole di avviso personalizzate per definire le proprie condizioni di attivazione degli avvisi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).
- Si ha familiarità con ["Metriche Prometheus comunemente utilizzate"](#).

- Si comprende il "[Sintassi delle query Prometheus](#)".
- Facoltativamente, hai guardato il video:

[Avvisi personalizzati](#)

A proposito di questa attività

StorageGRID non convalida gli avvisi personalizzati. Se si decide di creare regole di avviso personalizzate, attenersi alle seguenti linee guida generali:

- Esaminare le condizioni per le regole di avviso predefinite e utilizzarle come esempi per le regole di avviso personalizzate.
- Se si definiscono più condizioni per una regola di avviso, utilizzare la stessa espressione per tutte le condizioni. Quindi, modificare il valore di soglia per ciascuna condizione.
- Controllare attentamente ogni condizione per verificare la presenza di errori di tipo e logici.
- Utilizzare solo le metriche elencate nell'API Grid Management.
- Quando si esegue il test di un'espressione utilizzando l'API Grid Management, tenere presente che una risposta "riuscita" potrebbe essere un corpo di risposta vuoto (nessun avviso attivato). Per verificare se l'avviso è effettivamente attivato, è possibile impostare temporaneamente una soglia su un valore che si prevede sia vero al momento.

Ad esempio, per testare l'espressione `node_memory_MemTotal_bytes < 24000000000`, eseguire prima `node_memory_MemTotal_bytes >= 0` e assicurarsi di ottenere i risultati previsti (tutti i nodi restituiscono un valore). Quindi, riportare l'operatore e la soglia ai valori previsti ed eseguire di nuovo. Nessun risultato indica che non sono presenti avvisi correnti per questa espressione.

- Non presumere che un avviso personalizzato funzioni a meno che non sia stata convalidata l'attivazione dell'avviso quando previsto.

Fasi

1. Selezionare **Avvisi > Regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare **Crea regola personalizzata**.

Viene visualizzata la finestra di dialogo Create Custom Rule (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 **Enabled** per determinare se questa regola di avviso è attualmente attivata.

Se una regola di avviso è disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.

4. Inserire le seguenti informazioni:

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.

Campo	Descrizione
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1,024 caratteri.

5. Nella sezione Condizioni, immettere un'espressione Prometheus per uno o più livelli di gravità dell'avviso.

Un'espressione di base è in genere della forma:

```
[metric] [operator] [value]
```

Le espressioni possono essere di qualsiasi lunghezza, ma vengono visualizzate su una singola riga dell'interfaccia utente. È richiesta almeno un'espressione.

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

```
node_memory_MemTotal_bytes < 24000000000
```

Per visualizzare le metriche disponibili e testare le espressioni Prometheus, seleziona l'icona di aiuto  e segui il collegamento alla sezione Metrics dell'API Grid Management.

6. Nel campo **durata**, immettere il periodo di tempo in cui una condizione deve rimanere in vigore continuamente prima che l'allarme venga attivato e selezionare un'unità di tempo.

Per attivare un avviso immediatamente quando una condizione diventa vera, immettere **0**. Aumentare questo valore per evitare che condizioni temporanee attivino avvisi.

L'impostazione predefinita è 5 minuti.

7. Selezionare **Salva**.

La finestra di dialogo si chiude e la nuova regola di avviso personalizzata viene visualizzata nella tabella regole di avviso.

Modifica le regole di avviso in StorageGRID

È possibile modificare una regola di avviso per modificare le condizioni di attivazione; per una regola di avviso personalizzata, è anche possibile aggiornare il nome della regola, la descrizione e le azioni consigliate.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

A proposito di questa attività

Quando si modifica una regola di avviso predefinita, è possibile modificare le condizioni per gli avvisi minori, maggiori e critici e la durata. Quando si modifica una regola di avviso personalizzata, è anche possibile modificare il nome, la descrizione e le azioni consigliate della regola.



Prestare attenzione quando si decide di modificare una regola di avviso. Se si modificano i valori di attivazione, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

Fasi

1. Selezionare **Avvisi > Regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione corrispondente alla regola di avviso che si desidera modificare.
3. Selezionare **Modifica regola**.

Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola). Questo esempio mostra una regola di avviso predefinita: I campi Nome univoco, Descrizione e azioni consigliate sono disattivati e non possono essere modificati.

Edit Rule - Low installed node memory

Enabled ☒

Unique Name

Low installed node memory

Description

The amount of installed memory on a node is low.

Recommended Actions (optional)

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

See the instructions for your platform:

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

Conditions ?

Minor

Major

node_memory_MemTotal_bytes < 24000000000

Critical

node_memory_MemTotal_bytes <= 12000000000

Enter the amount of time a condition must continuously remain in effect before an alert is triggered.

Duration

2

minutes

Cancel

Save

4. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

Se una regola di avviso è disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.



Se si disattiva la regola di avviso per un avviso corrente, è necessario attendere alcuni minuti affinché l'avviso non venga più visualizzato come avviso attivo.



In generale, la disattivazione di una regola di avviso predefinita non è consigliata. Se una regola di avviso è disattivata, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

5. Per le regole di avviso personalizzate, aggiornare le seguenti informazioni secondo necessità.



Non puoi modificare queste informazioni per le regole di avviso predefinite.

Campo	Descrizione
Nome univoco	Un nome univoco per questa regola. Il nome della regola di avviso viene visualizzato nella pagina Avvisi ed è anche l'oggetto delle notifiche e-mail. I nomi delle regole di avviso possono essere compresi tra 1 e 64 caratteri.
Descrizione	Una descrizione del problema che si verifica. La descrizione è il messaggio di avviso visualizzato nella pagina Avvisi e nelle notifiche e-mail. Le descrizioni delle regole di avviso possono essere comprese tra 1 e 128 caratteri.
Azioni consigliate	Facoltativamente, le azioni consigliate da intraprendere quando viene attivato questo avviso. Immettere le azioni consigliate come testo normale (senza codici di formattazione). Le azioni consigliate per le regole di avviso possono essere comprese tra 0 e 1,024 caratteri.

6. Nella sezione Condizioni, immettere o aggiornare l'espressione Prometheus per uno o più livelli di gravità dell'avviso.



Se si desidera ripristinare il valore originale di una condizione per una regola di avviso predefinita modificata, selezionare i tre punti a destra della condizione modificata.

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 fino a quando la condizione precedente non viene risolta. Al successivo soddisfacimento di una delle condizioni per la regola, l'avviso rifletterà i valori aggiornati.

Un'espressione di base è in genere della forma:

```
[metric] [operator] [value]
```

Le espressioni possono essere di qualsiasi lunghezza, ma vengono visualizzate su una singola riga dell'interfaccia utente. È richiesta almeno un'espressione.

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

```
node_memory_MemTotal_bytes < 24000000000
```

7. Nel campo **durata**, immettere il periodo di tempo in cui una condizione deve rimanere in vigore continuamente prima che l'allarme venga attivato, quindi selezionare l'unità di tempo.

Per attivare un avviso immediatamente quando una condizione diventa vera, immettere **0**. Aumentare questo valore per evitare che condizioni temporanee attivino avvisi.

L'impostazione predefinita è 5 minuti.

8. Selezionare **Salva**.

Se è stata modificata una regola di avviso predefinita, nella colonna tipo viene visualizzato **Default***. Se è stata disattivata una regola di avviso predefinita o personalizzata, nella colonna **Status** viene visualizzato **Disabled**.

Disabilita le regole di avviso in StorageGRID

È possibile modificare lo stato attivato/disattivato per una regola di avviso predefinita o personalizzata.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

A proposito di questa attività

Quando una regola di avviso viene disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.



In generale, la disattivazione di una regola di avviso predefinita non è consigliata. Se una regola di avviso è disattivata, potrebbe non essere rilevato un problema sottostante fino a quando non viene impedita l'esecuzione di un'operazione critica.

Fasi

1. Selezionare **Avvisi > Regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione corrispondente alla regola di avviso che si desidera attivare o disattivare.
3. Selezionare **Modifica regola**.

Viene visualizzata la finestra di dialogo Edit Rule (Modifica regola).

4. Selezionare o deselezionare la casella di controllo **Enabled** per determinare se questa regola di avviso è attualmente attivata.

Se una regola di avviso è disattivata, le sue espressioni non vengono valutate e non vengono attivati avvisi.



Se si disattiva la regola di avviso per un avviso corrente, è necessario attendere alcuni minuti affinché l'avviso non venga più visualizzato come avviso attivo.

5. Selezionare **Salva**.

Disabled viene visualizzato nella colonna **Status**.

Rimuovi le regole di avviso personalizzate in StorageGRID

È possibile rimuovere una regola di avviso personalizzata se non si desidera più utilizzarla.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

Fasi

1. Selezionare **Avvisi > Regole**.

Viene visualizzata la pagina regole di avviso.

2. Selezionare il pulsante di opzione per la regola di avviso personalizzata che si desidera rimuovere.

Non è possibile rimuovere una regola di avviso predefinita.

3. Selezionare **Rimuovi regola personalizzata**.

Viene visualizzata una finestra di dialogo di conferma.

4. Selezionare **OK** per rimuovere la regola di avviso.

Tutte le istanze attive dell'avviso verranno risolte entro 10 minuti.

Gestire le notifiche di avviso

Imposta le notifiche SNMP per gli avvisi StorageGRID

Se si desidera che StorageGRID invii notifiche SNMP quando si verificano avvisi, è necessario attivare l'agente SNMP StorageGRID e configurare una o più destinazioni trap.

È possibile utilizzare l'opzione **Configurazione > Monitoraggio > Agente SNMP** in 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 sulla configurazione dell'agente SNMP, vedere ["Utilizzare il monitoraggio SNMP"](#).

Dopo aver configurato l'agente SNMP StorageGRID, è possibile inviare due tipi di notifiche basate sugli eventi:

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

Le notifiche di trap e notifica vengono inviate quando viene attivato un avviso predefinito o personalizzato a qualsiasi livello di gravità. Per eliminare le notifiche SNMP per un avviso, è necessario configurare un silenzio per l'avviso. Vedere ["Tacitare le notifiche di avviso"](#).

Se la distribuzione di StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport e le trap SNMP e le informazioni. Se il nodo di amministrazione primario non è più disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere ["Che cos'è un nodo amministratore?"](#).

Configura le notifiche e-mail per gli avvisi di StorageGRID

Se si desidera che le notifiche e-mail vengano inviate quando si verificano avvisi, è necessario fornire informazioni sul server SMTP. È inoltre necessario immettere gli indirizzi e-mail per i destinatari delle notifiche di avviso.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).
- Hai ["hai configurato un server di posta elettronica"](#).

A proposito di questa attività

Se la distribuzione di StorageGRID include più nodi amministrativi, il nodo amministrativo primario è il mittente preferito per le notifiche di avviso, i pacchetti AutoSupport e le trap SNMP e le informazioni. Se il nodo di amministrazione primario non è più disponibile, le notifiche vengono inviate temporaneamente da altri nodi di amministrazione. Vedere ["Che cos'è un nodo amministratore?"](#).

Fasi

1. Seleziona **Avvisi > Email di avviso**.

Viene visualizzata la pagina delle notifiche e-mail.

2. Seleziona la casella di controllo **Abilita email per gli avvisi** per indicare che vuoi che vengano inviate email di notifica quando gli avvisi raggiungono le soglie configurate.
3. Nella sezione **Ricevi email in base alla gravità**, seleziona il pulsante di opzione che indica i tipi di avvisi per cui vuoi ricevere una notifica.

4. Nella sezione Mittente, specifica un indirizzo email valido da usare come indirizzo Da per le notifiche di avviso.

Ad esempio: storagegrid-alerts@example.com

- a. Nella sezione destinatari, immettere un indirizzo e-mail per ciascun elenco o persona che deve ricevere un'e-mail quando si verifica un avviso.

Seleziona **Aggiungi destinatario** per aggiungere destinatari.

5. Selezionare **Salva**.

Informazioni incluse nelle notifiche e-mail di avviso

Dopo che hai configurato il server di posta elettronica e abilitato la posta elettronica per gli avvisi, le notifiche email vengono inviate ai destinatari designati quando viene attivato un avviso, a meno che la regola di avviso non sia soppressa da un silenzio. Consulta ["Tacitare le notifiche di avviso"](#).

Le notifiche e-mail includono le seguenti informazioni:

NetApp StorageGRID

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

Didascalia	Descrizione
1	Il nome dell'avviso, seguito dal numero di istanze attive dell'avviso.

Didascalia	Descrizione
2	La descrizione dell'avviso.
3	Azioni consigliate per l'avviso.
4	Dettagli su ogni istanza attiva dell'avviso, inclusi il nodo e il sito interessati, la severità dell'avviso, l'ora UTC in cui è stata attivata la regola di avviso e il nome del servizio e del processo interessati.
5	Il nome host del nodo amministratore che ha inviato la notifica.

Modalità di raggruppamento degli avvisi

Per impedire l'invio di un numero eccessivo di notifiche e-mail quando vengono attivati gli avvisi, StorageGRID tenta di raggruppare più avvisi nella stessa notifica.

Fare riferimento alla tabella seguente per alcuni esempi di come StorageGRID raggruppa più avvisi nelle notifiche e-mail.

Comportamento	Esempio
Ogni notifica di avviso si applica solo agli avvisi con lo stesso nome. Se vengono attivati contemporaneamente due avvisi con nomi diversi, vengono inviate due notifiche e-mail.	- L'avviso A viene attivato su due nodi contemporaneamente. Viene inviata una sola notifica. - L'allarme A viene attivato sul nodo 1 e l'allarme B viene attivato contemporaneamente sul nodo 2. Vengono inviate due notifiche, una per ogni avviso.
Per un avviso specifico su un nodo specifico, se le soglie vengono raggiunte per più di una severità, viene inviata una notifica solo per l'avviso più grave.	Viene attivato l'allarme A e vengono raggiunte le soglie di allarme minore, maggiore e critico. Viene inviata una notifica per l'avviso critico.
La prima volta che viene attivato un avviso, StorageGRID attende 2 minuti prima di inviare una notifica. Se durante questo periodo vengono attivati altri avvisi con lo stesso nome, StorageGRID raggruppa tutti gli avvisi nella notifica iniziale.	- L'allarme A viene attivato sul nodo 1 alle 08:00. Non viene inviata alcuna notifica. - L'allarme A viene attivato sul nodo 2 alle 08:01. Non viene inviata alcuna notifica. - Alle 08:02, viene inviata una notifica per segnalare entrambe le istanze dell'avviso.
Se viene attivato un altro avviso con lo stesso nome, StorageGRID attende 10 minuti prima di inviare una nuova notifica. La nuova notifica riporta tutti gli avvisi attivi (gli avvisi correnti che non sono stati tacitati), anche se precedentemente segnalati.	- L'allarme A viene attivato sul nodo 1 alle 08:00. Viene inviata una notifica alle ore 08:02. - L'allarme A viene attivato sul nodo 2 alle 08:05. Una seconda notifica viene inviata alle 08:15 (10 minuti dopo). Vengono segnalati entrambi i nodi.

Comportamento	Esempio
Se sono presenti più avvisi correnti con lo stesso nome e uno di questi viene risolto, non viene inviata una nuova notifica se l'avviso si ripresenta sul nodo per il quale l'avviso è stato risolto.	1. 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 via email ogni 7 giorni fino a quando tutte le istanze dell'avviso non vengono risolte o la regola dell'avviso non viene tacitata.	1. L'allarme A viene attivato per il nodo 1 l'8 marzo. Viene inviata una notifica. 2. L'avviso A non viene risolto o tacitato. Ulteriori notifiche verranno inviate il 15 marzo, il 22 marzo, il 29 marzo e così via.

Risolvere i problemi relativi alle notifiche email di avviso

Segui questi passaggi per analizzare e risolvere il problema se viene attivato l'avviso di errore di notifica e-mail e non ricevi:

- Test delle notifiche del server di posta elettronica
- Email di avviso StorageGRID
- Email di verifica multi-amministratore (MAV)

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai l'autorizzazione ["Autorizzazione di accesso root"](#). Se hai l'autorizzazione Gestisci avvisi, puoi visualizzare, ma non modificare, la configurazione del server di posta elettronica.

Fasi

1. Verifica le impostazioni delle email di avviso.
 - a. Verificare di aver specificato indirizzi e-mail validi per i destinatari.
 - b. Seleziona **Configurazione > Server di posta elettronica** e verifica che le impostazioni del server di posta elettronica (SMTP) siano corrette.
2. Controllare il filtro antispam e assicurarsi che l'e-mail non sia stata inviata a una cartella di posta indesiderata.
3. Chiedi all'amministratore dell'email di confermare che le e-mail dell'indirizzo del mittente non vengono bloccate.
4. Verifica i seguenti elementi relativi al trasferimento della posta elettronica:
 - a. Monitoraggio dei log del server di posta elettronica: visualizza i log del server di posta elettronica utilizzato da StorageGRID (**Configuration > Email server**). Cerca errori di relay, errori di autenticazione e altri errori corrispondenti al momento in cui StorageGRID ha tentato di inviare un'email.

- b. Segnalazioni di mancata consegna (bounce-back): se le email non vengono ricevute e StorageGRID non segnala alcun errore, il problema potrebbe essere un bounce-back. Configurando l'indirizzo "mittente" con un indirizzo email valido, potrai vedere queste email di risposta ai bounce-back.
5. Raccogli i file di log dell'Admin Node che sta inviando le email. Esamina i file `/var/local/log/prometheus.log` e `/var/local/log/nms.log` per eventuali problemi evidenti che potresti riuscire a correggere. Se non riesci a risolvere il problema, contatta il supporto tecnico.

Il supporto tecnico può utilizzare le informazioni contenute nei registri per determinare l'errore. Ad esempio, il file `prometheus.log` potrebbe visualizzare un errore durante la connessione al server specificato.

Consulta ["Raccogliere i file di log e i dati di sistema"](#).

Silenza le notifiche di alert in StorageGRID

In alternativa, è possibile configurare le silenzi in modo da eliminare temporaneamente le notifiche di avviso.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Gestire gli avvisi o l'autorizzazione di accesso principale"](#).

A proposito di questa attività

È possibile disattivare le regole di avviso sull'intera griglia, su un singolo sito o su un singolo nodo e per una o più severità. Ogni silenzio elimina tutte le notifiche per una singola regola di avviso o per tutte le regole di avviso.

Se è stato attivato l'agente SNMP, le silenzi sopprimono anche i trap SNMP e informano.



Prestare attenzione quando si decide di tacitare una regola di avviso. Se si tacita un avviso, potrebbe non essere possibile rilevare un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica.

Fasi

1. Selezionare **Avvisi > Silenzi**.

Viene visualizzata la pagina Silences (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. Selezionare **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	

3. Selezionare o inserire le seguenti informazioni:

Campo	Descrizione
Regola di avviso	Il nome della regola di avviso che si desidera disattivare. È possibile selezionare qualsiasi regola di avviso predefinita o personalizzata, anche se la regola di avviso è disattivata. Nota: selezionare tutte le regole se si desidera disattivare tutte le regole di avviso utilizzando i criteri specificati in questa finestra di dialogo.
Descrizione	Facoltativamente, una descrizione del silenzio. Ad esempio, descrivi lo scopo di questo silenzio.
Durata	Per quanto tempo si desidera che questo silenzio rimanga attivo, in minuti, ore o giorni. Un silenzio può essere in vigore da 5 minuti a 1,825 giorni (5 anni). Nota: non disattivare una regola di avviso per un periodo di tempo prolungato. Se una regola di avviso viene tacitata, è possibile che non si rilevi un problema sottostante fino a quando non si impedisce il completamento di un'operazione critica. Tuttavia, potrebbe essere necessario utilizzare un silenzio esteso se un avviso viene attivato da una configurazione specifica e intenzionale, ad esempio per gli avvisi link down dell'appliance di servizi e link down dell'appliance di storage.
Severità	Quale severità o severità degli avvisi deve essere tacitata. Se l'avviso viene attivato in una delle severità selezionate, non viene inviata alcuna notifica.

Campo	Descrizione
Nodi	A quale nodo o nodi si desidera applicare questo silenzio. È possibile eliminare una regola di avviso o tutte le regole dell'intera griglia, di un singolo sito o di un singolo nodo. Se si seleziona l'intera griglia, il silenzio viene applicato a tutti i siti e a tutti i nodi. Se si seleziona un sito, il silenzio si applica solo ai nodi di quel sito. Nota: non è possibile selezionare più di un nodo o più siti per ogni silenzio. Se si desidera eliminare la stessa regola di avviso su più di un nodo o più siti contemporaneamente, è necessario creare silenzi aggiuntivi.

4. Selezionare **Salva**.

5. Se si desidera modificare o terminare un silenzio prima della scadenza, è possibile modificarlo o rimuoverlo.

Opzione	Descrizione
Modificare un silenzio	a. Selezionare Avvisi > Silenzi. b. Dalla tabella, selezionare il pulsante di opzione relativo al silenzio che si desidera modificare. c. Selezionare Modifica. d. Modificare la descrizione, il tempo rimanente, le severità selezionate o il nodo interessato. e. Selezionare Salva.
Eliminare un silenzio	a. Selezionare Avvisi > Silenzi. b. Dalla tabella, selezionare il pulsante di opzione per il silenzio che si desidera rimuovere. c. Selezionare Rimuovi. d. Selezionare OK per confermare che si desidera rimuovere questo silenzio. Nota: Le notifiche verranno inviate quando viene attivato questo avviso (a meno che non venga eliminato da un altro silenzio). Se questo avviso viene attivato, potrebbero essere necessari alcuni minuti per l'invio di notifiche e-mail o SNMP e per l'aggiornamento della pagina Avvisi.

Informazioni correlate

["Configurare l'agente SNMP"](#)

Avvisi in StorageGRID

Questo riferimento elenca gli avvisi predefiniti visualizzati in Grid Manager. Le azioni consigliate sono contenute nel messaggio di avviso ricevuto.

Se necessario, è possibile creare regole di avviso personalizzate per adattarsi al proprio approccio di gestione del sistema.

Alcuni avvisi predefiniti utilizzano "[Metriche Prometheus](#)".

Avvisi sull'appliance

Nome dell'avviso	Descrizione
Batteria dell'appliance scaduta	La batteria del controller di storage dell'appliance è scaduta.
Batteria dell'appliance guasta	La batteria del controller di storage dell'appliance si è guastata.
La capacità appresa della batteria dell'appliance non è sufficiente	La capacità appresa della batteria nel controller di storage dell'appliance non è sufficiente.
Batteria dell'apparecchio quasi scaduta	La batteria del controller di storage dell'appliance sta per scadere.
Batteria dell'apparecchio rimossa	La batteria nel controller di storage dell'appliance non è presente.
Batteria dell'apparecchio troppo calda	La batteria del controller di storage dell'apparecchio è surriscaldata.
Errore di comunicazione BMC dell'appliance	La comunicazione con il BMC (Baseboard Management Controller) è stata persa.
Rilevato guasto del dispositivo di avvio dell'apparecchio	È stato rilevato un problema con il dispositivo di avvio nell'apparecchio.
Periferica di backup della cache dell'appliance non riuscita	Si è verificato un errore in una periferica di backup della cache persistente.
Capacità insufficiente del dispositivo di backup della cache dell'appliance	La capacità della periferica di backup della cache è insufficiente.
Dispositivo di backup cache dell'appliance protetto da scrittura	Una periferica di backup della cache è protetta da scrittura.
Mancata corrispondenza delle dimensioni della memoria cache dell'appliance	I due controller dell'appliance hanno dimensioni della cache diverse.
Guasto della batteria CMOS dell'apparecchio	È stato rilevato un problema con la batteria CMOS nell'apparecchio.
Temperatura dello chassis del controller di calcolo dell'appliance troppo alta	La temperatura del controller di calcolo in un'appliance StorageGRID ha superato una soglia nominale.

Nome dell'avviso	Descrizione
Temperatura CPU del controller di calcolo dell'appliance troppo alta	La temperatura della CPU nel controller di calcolo di un'appliance StorageGRID ha superato una soglia nominale.
Il controller di calcolo dell'appliance richiede attenzione	È stato rilevato un guasto hardware nel controller di calcolo di un'appliance StorageGRID.
Si è verificato un problema nell'alimentatore A del controller di calcolo dell'appliance	L'alimentazione A nel controller di calcolo presenta un problema.
Si è verificato un problema nell'alimentatore B del controller di calcolo dell'appliance	L'alimentazione B nel controller di calcolo presenta un problema.
Il servizio di monitoraggio dell'hardware di calcolo dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage si è bloccato.
Unità DAS dell'appliance che supera il limite per i dati scritti al giorno	Una quantità eccessiva di dati viene scritta su un'unità ogni giorno, il che potrebbe invalidare la garanzia.
Rilevato guasto al disco DAS dell'appliance	È stato rilevato un problema con un disco DAS (Direct-Attached Storage) nell'appliance.
L'unità DAS dell'appliance si trova nello slot o nel nodo sbagliato	Un'unità di archiviazione collegata direttamente (DAS) si trova nello slot o nel nodo sbagliato
Spia localizzatore unità DAS dell'appliance accesa	La spia di posizionamento dell'unità per una o più unità DAS (Direct-Attached Storage) in un nodo di archiviazione dell'appliance è accesa.
Ricostruzione del disco DAS dell'appliance	È in corso la ricostruzione di un disco DAS (Direct-Attached Storage). Questo è previsto se è stato sostituito o rimosso/reinserito di recente.
Rilevato guasto alla ventola dell'appliance	È stato rilevato un problema relativo alla ventola dell'apparecchio.
Rilevato guasto nel Fibre Channel dell'appliance	È stato rilevato un problema di collegamento Fibre Channel tra lo storage controller dell'appliance e il controller di calcolo
Errore della porta HBA Fibre Channel dell'appliance	Una porta HBA Fibre Channel si sta guastando o si è guastata.
Unità flash cache dell'appliance non ottimali	I dischi utilizzati per la cache SSD non sono ottimali.

Nome dell'avviso	Descrizione
Interconnessione dell'appliance/contenitore della batteria rimosso	Il contenitore di interconnessione/batteria non è presente.
Porta LACP dell'appliance mancante	Una porta su un'appliance StorageGRID non partecipa al bond LACP.
Rilevato guasto alla scheda NIC dell'appliance	È stato rilevato un problema con una scheda di interfaccia di rete (NIC) nell'appliance.
Alimentatore generale dell'appliance degradato	La potenza di un'appliance StorageGRID è diversa dalla tensione di esercizio consigliata.
Aggiornamento software del sistema operativo SANtricity dell'appliance richiesto	La versione del software SANtricity è inferiore al minimo consigliato per questa versione di StorageGRID.
Rilevato guasto SFP dell'appliance	È stato rilevato un guasto SFP nel controller di calcolo di un'appliance StorageGRID.
Avviso critico SSD dell'appliance	Un'appliance SSD sta segnalando un avviso critico.
Guasto del controller dello storage dell'appliance A.	Si è verificato un errore nel controller storage A di un'appliance StorageGRID.
Guasto del controller storage dell'appliance B.	Il controller dello storage B in un'appliance StorageGRID si è guastato.
Guasto al disco del controller dello storage dell'appliance	Uno o più dischi di un'appliance StorageGRID si sono guastati o non sono ottimali.
Problema hardware del controller dello storage dell'appliance	Il software SANtricity segnala "richiede attenzione" per un componente di un'appliance StorageGRID.
Guasto all'alimentazione Del controller dello storage dell'appliance A.	L'alimentazione A di un'appliance StorageGRID non è conforme alla tensione di esercizio consigliata.
Guasto all'alimentazione B del controller storage dell'appliance	L'alimentazione B di un apparecchio StorageGRID non è conforme alla tensione di esercizio consigliata.
Il servizio di monitoraggio hardware dello storage dell'appliance si è bloccato	Il servizio che monitora lo stato dell'hardware dello storage si è bloccato.

Nome dell'avviso	Descrizione
Gli shelf di storage delle appliance sono degradati	Lo stato di uno dei componenti dello shelf di storage di un'appliance di storage è degradato.
Temperatura dell'apparecchio superata	La temperatura nominale o massima del controller di storage dell'appliance è stata superata.
Sensore di temperatura dell'apparecchio rimosso	È stato rimosso un sensore di temperatura.
Errore di avvio protetto UEFI dell'appliance	Un'appliance non è stata avviata in modo sicuro.
L'i/o del disco è molto lento	La lentezza dell'i/o del disco potrebbe influire sulle prestazioni della griglia.
Rilevato guasto alla ventola dell'appliance di storage	È stato rilevato un problema con un'unità ventola nel controller di storage di un'appliance.
La connettività dello storage dell'appliance di storage è degradata	Si è verificato un problema con una o più connessioni tra il controller di calcolo e il controller dello storage.
Dispositivo di storage inaccessibile	Impossibile accedere a un dispositivo di storage.

Avvisi di audit e syslog

Nome dell'avviso	Descrizione
I registri di controllo vengono aggiunti alla coda in-memory	Il nodo non può inviare i log al server syslog locale e la coda in-memory si sta riempiendo.
Errore di inoltro del server syslog esterno	Il nodo non può inoltrare i log al server syslog esterno.
Coda di audit di grandi dimensioni	La coda del disco per i messaggi di controllo è piena. Se questa condizione non viene risolta, le operazioni S3 potrebbero fallire.
I registri vengono aggiunti alla coda su disco	Il nodo non può inoltrare i log al server syslog esterno e la coda su disco si sta riempiendo.

Avvisi bucket

Nome dell'avviso	Descrizione
Il bucket FabricPool ha un'impostazione di coerenza del bucket non supportata	Un bucket FabricPool utilizza il livello di coerenza disponibile o di sito sicuro, che non è supportato.
Il bucket FabricPool ha un'impostazione di versione non supportata	In un bucket FabricPool è abilitata la versione o il blocco degli oggetti S3, che non sono supportati.
ListBucket controllo delle autorizzazioni per Get/Head object disabilitato	Il controllo dei permessi ListBucket per GetObject/HeadObject su chiavi inesistenti è disabilitato.

Avvisi Cassandra

Nome dell'avviso	Descrizione
Errore compattatore automatico Cassandra	Si è verificato un errore nel compattatore automatico Cassandra.
Metriche del compattatore automatico Cassandra non aggiornate	Le metriche che descrivono il compattatore automatico Cassandra non sono aggiornate.
Errore di comunicazione Cassandra	I nodi che eseguono il servizio Cassandra hanno problemi di comunicazione tra loro.
Le compaction di Cassandra sono sovraccaricate	Il processo di compattazione Cassandra è sovraccarico.
Errore di scrittura Cassandra oversize	Un processo StorageGRID interno ha inviato a Cassandra una richiesta di scrittura troppo grande.
Metriche di riparazione Cassandra non aggiornate	Le metriche che descrivono i lavori di riparazione Cassandra non sono aggiornate.
Il processo di riparazione di Cassandra è lento	Il progresso delle riparazioni del database Cassandra è lento.
Servizio di riparazione Cassandra non disponibile	Il servizio di riparazione Cassandra non è disponibile.
Tabella Cassandra corrotta	Cassandra ha rilevato un danneggiamento della tabella. Cassandra si riavvia automaticamente se rileva la corruzione della tabella.

Avvisi Cloud Storage Pool

Nome dell'avviso	Descrizione
Errore di connettività del pool di cloud storage	Il controllo dello stato di salute dei Cloud Storage Pools ha rilevato uno o più nuovi errori.
IAM Roles Anywhere End-Entity Certification Expiration	Il certificato IAM Roles Anywhere End-Entity sta per scadere.

Avvisi di replica cross-grid

Nome dell'avviso	Descrizione
Errore permanente della replica cross-grid	Si è verificato un errore di replica cross-grid che richiede l'intervento dell'utente per la risoluzione.
Risorse di replica cross-grid non disponibili	Le richieste di replica cross-grid sono in sospeso perché una risorsa non è disponibile.

Avvisi DHCP

Nome dell'avviso	Descrizione
Lease DHCP scaduto	Il lease DHCP su un'interfaccia di rete è scaduto.
Il lease DHCP sta per scadere	Il lease DHCP su un'interfaccia di rete sta per scadere.
Server DHCP non disponibile	Il server DHCP non è disponibile.

Avvisi di debug e traccia

Nome dell'avviso	Descrizione
Impatto delle performance di debug	Quando la modalità di debug è attivata, le prestazioni del sistema potrebbero risentirne negativamente.
Configurazione traccia attivata	Quando la configurazione di trace è attivata, le prestazioni del sistema potrebbero risentire negativamente.

Avvisi e-mail e AutoSupport

Nome dell'avviso	Descrizione
Impossibile inviare il messaggio AutoSupport	Impossibile inviare il messaggio AutoSupport più recente.

Nome dell'avviso	Descrizione
Errore di risoluzione del nome di dominio	Il nodo StorageGRID non è stato in grado di risolvere i nomi di dominio.
Errore di notifica e-mail	Impossibile inviare la notifica via email per un avviso.
Bucket di destinazione dell'archiviazione dei log non trovato	Manca il bucket di destinazione per l'archiviazione dei log, il che impedisce l'archiviazione dei log nel bucket di destinazione.
Errori di notifica SNMP	Errori durante l'invio di notifiche di notifica SNMP a una destinazione trap.
Accesso esterno SSH abilitato	L'accesso esterno SSH è abilitato da più di 24 ore.
Rilevato accesso SSH o console	Nelle ultime 24 ore, un utente ha effettuato l'accesso con la console Web o SSH.

Erasure coding (EC) alerts (Avvisi di codifica di cancellazione)

Nome dell'avviso	Descrizione
Servizio chunk con elevato numero di goroutine	Il servizio di suddivisione in blocchi presenta un numero insolitamente elevato di goroutine, il che potrebbe indicare un deadlock o una perdita di risorse.
Errore di ribilanciamento EC	La procedura di ribilanciamento EC non è riuscita o è stata interrotta.
Errore di riparazione EC	Un intervento di riparazione per i dati EC non è riuscito o è stato interrotto.
Riparazione EC in stallo	Un intervento di riparazione per i dati EC si è bloccato.
Errore di verifica dei frammenti sottoposti a erasure coding	I frammenti sottoposti a erasure coding non possono più essere verificati. I frammenti corrotti potrebbero non essere riparati.
Gruppi con codifica di cancellazione nello stato Needs Repair	Uno o più gruppi con codifica di cancellazione si trovano nello stato "Necessita di riparazione" quando non è in corso alcuna riparazione di dati con codifica di cancellazione.

Scadenza degli avvisi relativi ai certificati

Nome dell'avviso	Descrizione
Scadenza certificato CA proxy amministratore	Uno o più certificati nel pacchetto CA del server proxy amministratore stanno per scadere.

Nome dell'avviso	Descrizione
Scadenza del certificato client	Uno o più certificati client stanno per scadere.
Scadenza del certificato del server globale per S3	Il certificato del server globale per S3 sta per scadere.
Scadenza del certificato endpoint del bilanciamento del carico	Uno o più certificati endpoint per il bilanciamento del carico stanno per scadere.
Scadenza del certificato del server per l'interfaccia di gestione	Il certificato del server utilizzato per l'interfaccia di gestione sta per scadere.
Scadenza del certificato CA syslog esterno	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server syslog esterno sta per scadere.
Scadenza del certificato client syslog esterno	Il certificato client per un server syslog esterno sta per scadere.
Scadenza del certificato del server syslog esterno	Il certificato del server presentato dal server syslog esterno sta per scadere.

Avvisi Grid Network

Nome dell'avviso	Descrizione
Mancata corrispondenza MTU rete griglia	L'impostazione MTU per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia.

Avvisi di federazione delle griglie

Nome dell'avviso	Descrizione
Scadenza del certificato di federazione griglia	Uno o più certificati di federazione griglia stanno per scadere.
Errore di connessione alla federazione di griglie	La connessione a federazione di griglie tra la rete locale e remota non funziona.

Avvisi di utilizzo elevato o latenza elevata

Nome dell'avviso	Descrizione
Latenza elevata per le query sui metadati	Il tempo medio per le query dei metadati Cassandra è troppo lungo.

Avvisi di Identity Federation

Nome dell'avviso	Descrizione
Errore di sincronizzazione della federazione delle identità	Impossibile sincronizzare utenti e gruppi federati dall'origine dell'identità.
Errore di sincronizzazione della federazione delle identità per un tenant	Impossibile sincronizzare utenti e gruppi federati dall'origine dell'identità configurata da un tenant.

Avvisi ILM (Information Lifecycle Management)

Nome dell'avviso	Descrizione
Posizionamento ILM non raggiungibile	Non è possibile ottenere un'istruzione di posizionamento in una regola ILM per determinati oggetti.
Velocità di scansione ILM bassa	La velocità di scansione ILM è impostata su un valore inferiore a 100 oggetti/secondo.

Avvisi del server di gestione delle chiavi (KMS)

Nome dell'avviso	Descrizione
Scadenza del certificato CA KMS	Il certificato dell'autorità di certificazione (CA) utilizzato per firmare il certificato del server di gestione delle chiavi (KMS) sta per scadere.
Scadenza del certificato client KMS	Il certificato client per un server di gestione delle chiavi sta per scadere.
Impossibile caricare la configurazione KMS	La configurazione per il server di gestione delle chiavi esiste ma non è riuscita a caricarsi.
Errore di connettività KMS	Un nodo appliance non è riuscito a connettersi al server di gestione delle chiavi del proprio sito.
Nome chiave di crittografia KMS non trovato	Il server di gestione delle chiavi configurato non dispone di una chiave di crittografia corrispondente al nome fornito.
Rotazione della chiave di crittografia KMS non riuscita	Tutti i volumi dell'appliance sono stati decifrati correttamente, ma uno o più volumi non sono stati ruotati sulla chiave più recente.
KMS non configurato	Non esiste alcun server di gestione delle chiavi per questo sito.
La chiave KMS non è riuscita a decrittare un volume dell'appliance	Non è stato possibile decifrare uno o più volumi su un'appliance con crittografia del nodo abilitata con la chiave KMS corrente.

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 stato in grado di connettersi a uno o più server nel cluster del server di gestione delle chiavi per il sito.

Avvisi per il bilanciamento del carico

Nome dell'avviso	Descrizione
Collegamenti del bilanciatore di carico a richiesta zero elevati	Una percentuale elevata di connessioni agli endpoint del bilanciatore di carico disconnesse senza eseguire richieste.

Avvisi di offset dell'orologio locale

Nome dell'avviso	Descrizione
Grande offset temporale dell'orologio locale	L'offset tra l'orologio locale e l'ora NTP (Network Time Protocol) è troppo elevato.

Avvisi di memoria insufficiente o spazio insufficiente

Nome dell'avviso	Descrizione
Bassa capacità del disco di log di audit	Lo spazio disponibile per i registri di controllo è limitato. Se questa condizione non viene risolta, le operazioni S3 potrebbero fallire.
Memoria del nodo a bassa disponibilità	La quantità di RAM disponibile su un nodo è bassa.
Spazio libero ridotto per il pool di storage	Lo spazio disponibile per memorizzare i dati dell'oggetto nel nodo di storage è basso.
Memoria del nodo installata insufficiente	La quantità di memoria installata su un nodo è bassa.
Storage dei metadati basso	Lo spazio disponibile per memorizzare i metadati degli oggetti è basso.
Capacità disco di metriche ridotte	Lo spazio disponibile per il database delle metriche è basso.
Storage dei dati a oggetti basso	Lo spazio disponibile per memorizzare i dati degli oggetti è basso.
Override del watermark di sola lettura bassa	L'override del watermark di sola lettura soft del volume di archiviazione è inferiore al watermark ottimizzato minimo per un nodo di archiviazione.

Nome dell'avviso	Descrizione
Bassa capacità del disco root	Lo spazio disponibile sul disco root è insufficiente.
Bassa capacità dei dati di sistema	Lo spazio disponibile per /var/local è basso. Se questa condizione non viene risolta, le operazioni S3 potrebbero fallire.
Spazio libero nella directory tmp basso	Lo spazio disponibile nella directory /tmp è insufficiente.

Avvisi di rete di nodi o nodi

Nome dell'avviso	Descrizione
Quorum ADC non raggiunto	Il nodo di archiviazione con servizio ADC è offline. Le operazioni di espansione e dismissione sono bloccate finché non viene ripristinato il quorum ADC.
Utilizzo ricezione rete amministratore	L'utilizzo della ricezione nella rete amministrativa è elevato.
Uso della trasmissione della rete di amministrazione	L'utilizzo della trasmissione sulla rete amministrativa è elevato.
Errore di configurazione del firewall	Impossibile applicare la configurazione del firewall.
Endpoint dell'interfaccia di gestione in modalità fallback	Tutti gli endpoint dell'interfaccia di gestione ricadono troppo a lungo sulle porte predefinite.
Errore di connettività di rete del nodo	Si sono verificati errori durante il trasferimento dei dati tra nodi.
Errore frame ricezione rete nodo	Un'elevata percentuale di frame di rete ricevuti da un nodo presenta errori.
Nodo non sincronizzato con il server NTP	Il nodo non è sincronizzato con il server NTP (Network Time Protocol).
Nodo non bloccato con server NTP	Il nodo non è bloccato su un server NTP (Network Time Protocol).
Rete del nodo non appliance non in funzione	Uno o più dispositivi di rete sono disconnessi o non attivi.
Collegamento dell'appliance di servizi alla rete di amministrazione	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.

Nome dell'avviso	Descrizione
Collegamento dell'appliance di servizi alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.
Collegamento dell'appliance di servizi alla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 2	La porta di rete 2 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 3	La porta di rete 3 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di servizi disattivato sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage in Admin Network	L'interfaccia dell'appliance alla rete di amministrazione (eth1) è inattiva o disconnessa.
Collegamento dell'appliance di storage alla porta di rete dell'amministratore 1	La porta Admin Network 1 dell'appliance è inattiva o disconnessa.
Collegamento dell'appliance di storage alla rete client	L'interfaccia dell'appliance alla rete client (eth2) è inattiva o disconnessa.
Collegamento dell'appliance di storage inattivo sulla porta di rete 1	La porta di rete 1 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 2	La porta di rete 2 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 3	La porta di rete 3 sull'apparecchio è inattiva o scollegata.
Collegamento dell'appliance di storage inattivo sulla porta di rete 4	La porta di rete 4 sull'apparecchio è inattiva o scollegata.

Nome dell'avviso	Descrizione
Nodo di storage non nello stato di storage desiderato	Il servizio LDR su un nodo di archiviazione non può passare allo stato desiderato a causa di un errore interno o di un problema relativo al volume
Utilizzo della connessione TCP	Il numero di connessioni TCP su questo nodo si avvicina al numero massimo che è possibile tenere traccia.
Impossibile comunicare con il nodo	Uno o più servizi non rispondono o non è possibile raggiungere il nodo.
Riavvio del nodo imprevisto	Un nodo si è riavviato inaspettatamente nelle ultime 24 ore.

Avvisi a oggetti

Nome dell'avviso	Descrizione
Controllo dell'esistenza dell'oggetto non riuscito	Il processo di controllo dell'esistenza dell'oggetto non è riuscito.
Controllo dell'esistenza dell'oggetto bloccato	Il lavoro di verifica dell'esistenza dell'oggetto si è bloccato.
Oggetti potenzialmente persi	Uno o più oggetti potenzialmente persi dalla griglia.
Rilevati oggetti orfani	Sono stati rilevati oggetti orfani.
Dimensione della parte di upload multipart S3 troppo grande	Un client sta tentando un'operazione di caricamento in più parti che supera il limite di dimensione delle parti.
S3 HA POSTO la dimensione dell'oggetto troppo grande	Un client sta tentando di eseguire un'operazione PUT Object che supera i limiti di dimensione S3.
Richieste S3 che utilizzano intestazioni condizionali non supportate	Un client S3 sta utilizzando intestazioni condizionali non supportate (If-Match o If-None-Match) per determinate operazioni.
Richieste S3 che utilizzano la regione errata con namespace globale abilitato	Un client S3 sta utilizzando la regione di firma errata per accedere ai bucket di questa grid.
Rilevato oggetto corrotto non identificato	È stato trovato un file nello storage a oggetti replicato che non è stato possibile identificare come oggetto replicato.

Avvisi di danneggiamento degli oggetti

Nome dell'avviso	Descrizione
Mancata corrispondenza delle dimensioni dell'oggetto	Rilevata dimensione imprevista dell'oggetto durante la procedura di controllo dell'esistenza dell'oggetto.

Avvisi sui servizi della piattaforma

Nome dell'avviso	Descrizione
Richiesta di servizi piattaforma in sospeso capacità bassa	Il numero di richieste in sospeso di Platform Services si sta avvicinando alla capacità.
Servizi della piattaforma non disponibili	In un sito sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM.

Avvisi sul volume di storage

Nome dell'avviso	Descrizione
Il volume di storage richiede attenzione	Un volume di storage è offline e richiede attenzione.
Il volume di storage deve essere ripristinato	Un volume di storage è stato ripristinato e deve essere ripristinato.
Volume di storage offline	Un volume di archiviazione è stato offline per più di 5 minuti.
Tentativo di rimontaggio del volume di storage	Un volume di storage era offline e attivava un rimontaggio automatico. Ciò potrebbe indicare un problema dell'unità o errori del file system.
Ripristino volume non riuscito ad avviare la riparazione dei dati replicati	Impossibile avviare automaticamente la riparazione dei dati replicati per un volume riparato.

Avvisi dei servizi StorageGRID

Nome dell'avviso	Descrizione
servizio nginx con configurazione di backup	La configurazione del servizio nginx non è valida. È in uso la configurazione precedente.
servizio nginx-gw con configurazione di backup	La configurazione del servizio nginx-gw non è valida. È in uso la configurazione precedente.
Riavvio necessario per disattivare FIPS	La policy di sicurezza non richiede la modalità FIPS, ma sono in uso i moduli FIPS.

Nome dell'avviso	Descrizione
Riavvio necessario per attivare FIPS	La policy di sicurezza richiede la modalità FIPS, ma i moduli FIPS non sono in uso.
Servizio SSH con configurazione di backup	La configurazione del servizio SSH non è valida. È in uso la configurazione precedente.

Avvisi del tenant

Nome dell'avviso	Descrizione
Utilizzo elevato della quota del tenant	Viene utilizzata un'elevata percentuale di spazio di quota. Questa regola è disattivata per impostazione predefinita perché potrebbe causare un numero eccessivo di notifiche.

Metriche Prometheus comunemente utilizzate in StorageGRID

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.

È anche possibile [ottenere un elenco completo di tutte le metriche](#).

Per i dettagli sulla sintassi delle query di Prometheus, vedi "[Nozioni di base sulle interrogazioni](#)".

Quali sono le metriche Prometheus?

Le metriche Prometheus sono misurazioni di serie temporali. Il servizio Prometheus sui nodi di amministrazione raccoglie queste metriche dai servizi su tutti i nodi. Le metriche vengono memorizzate su ciascun nodo di amministrazione fino a quando lo spazio riservato ai dati Prometheus non è pieno. Quando il `/var/local/mysql_ibdata/` volume raggiunge la capacità, vengono eliminate per prime le metriche più vecchie.

Dove vengono utilizzate le metriche Prometheus?

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

- **Pagina nodi:** I grafici e i grafici nelle schede disponibili nella pagina nodi utilizzano lo strumento di visualizzazione Grafana per visualizzare le metriche delle serie temporali raccolte da Prometheus. Grafana visualizza i dati delle serie temporali in formato grafico e grafico, mentre Prometheus funge da origine dei dati back-end.



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



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

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

Elenco delle metriche più comuni

Il seguente elenco contiene le metriche Prometheus più comunemente utilizzate.



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

alertmanager_notifications_failed_total

Il numero totale di notifiche di avviso non riuscite.

node_filesystem_avail_bytes

La quantità di spazio del file system disponibile in byte per gli utenti non root.

Node_Memory_MemAvailable_Bytes

Campo delle informazioni sulla memoria MemAvailable_Bytes.

node_network_carrier

Valore portante di `/sys/class/net/iface`.

node_network_receive_errs_total

Statistica periferica di rete `receive_errs`.

node_network_transmit_errs_total

Statistica periferica di rete `transmit_errs`.

storagegrid_administively_down

Il nodo non è connesso alla rete per un motivo previsto. Ad esempio, il nodo o i servizi sul nodo sono stati normalmente spenti, il nodo è in fase di riavvio o il software è in fase di aggiornamento.

storagegrid_appliance_compute_controller_hardware_status

Lo stato dell'hardware del controller di calcolo in un'appliance.

storagegrid_appliance_failed_disks

Per lo storage controller di un'appliance, il numero di dischi non ottimali.

storagegrid_appliance_storage_controller_hardware_status

Lo stato generale dell'hardware dello storage controller in un'appliance.

storagegrid_content_bucket_and_containers

Numero totale di bucket S3 noti a questo nodo di archiviazione.

storagegrid_content_objects

Numero totale di oggetti dati S3 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.

storagegrid_content_objects_lost

Il numero totale di oggetti che il servizio rileva come mancanti dal sistema StorageGRID. È necessario intraprendere azioni per determinare la causa della perdita e se è possibile eseguire il ripristino.

["Risolvere i problemi relativi ai dati degli oggetti persi e mancanti"](#)

storagegrid_http_sessions_incoming_tented

Il numero totale di sessioni HTTP che sono state tentate per un nodo di storage.

storagegrid_http_sessions_incoming_currently_established

Il numero di sessioni HTTP attualmente attive (aperte) sul nodo di storage.

storagegrid_http_sessions_incoming_failed

Il numero totale di sessioni HTTP che non sono riuscite a completare correttamente, a causa di una richiesta HTTP non valida o di un errore durante l'elaborazione di un'operazione.

storagegrid_http_sessions_incoming_successful

Il numero totale di sessioni HTTP completate correttamente.

storagegrid_ilm_waiting_background_objects

Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalla scansione.

storagegrid_ilm_waiting_client_evaluation_objects_per_second

La velocità corrente alla quale gli oggetti vengono valutati in base al criterio ILM su questo nodo.

storagegrid_ilm_waiting_client_objects

Il numero totale di oggetti su questo nodo in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione).

storagegrid_ilm_waiting_total_objects

Il numero totale di oggetti in attesa di valutazione ILM.

storagegrid_ilm_scan_objects_per_second

La velocità con cui gli oggetti di proprietà di questo nodo vengono sottoposti a scansione e messi in coda per ILM.

storagegrid_ilm_scan_period_estimated_minutes

Il tempo stimato per completare una scansione ILM completa su questo nodo.

Nota: Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti di proprietà di questo nodo.

storagegrid_load_balancer_endpoint_cert_expiry_time

Il tempo di scadenza del certificato endpoint del bilanciamento del carico in secondi dall'epoca.

storagegrid_metadata_queries_average_latency_milliseconds

Il tempo medio richiesto per eseguire una query sull'archivio di metadati tramite questo servizio.

storagegrid_network_received_bytes

La quantità totale di dati ricevuti dall'installazione.

storagegrid_network_transmitted_bytes

La quantità totale di dati inviati dall'installazione.

storagegrid_node_cpu_utilization_percent

La percentuale di tempo CPU disponibile attualmente utilizzata da questo servizio. Indica la disponibilità del servizio. La quantità di tempo CPU disponibile dipende dal numero di CPU del server.

storagegrid_ntp_chouged_time_source_offset_milliseconds

Offset sistematico del tempo fornito da una fonte di tempo scelta. L'offset viene introdotto quando il ritardo per raggiungere un'origine temporale non è uguale al tempo richiesto per l'origine temporale per raggiungere il client NTP.

storagegrid_ntp_locked

Il nodo non è bloccato su un server NTP (Network Time Protocol).

storagegrid_s3_data_transfers_bytes_ingested

La quantità totale di dati acquisiti dai client S3 a questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_s3_data_transfers_bytes_retrieved

La quantità totale di dati recuperati dai client S3 da questo nodo di storage dall'ultima reimpostazione dell'attributo.

storagegrid_s3_operations_failed

Il numero totale di operazioni S3 non riuscite (codici di stato HTTP 4xx e 5xx), escluse quelle causate da un errore di autorizzazione S3.

storagegrid_s3_operations_successful

Il numero totale di operazioni S3 riuscite (codice di stato HTTP 2xx).

storagegrid_s3_operations_unauthorized

Il numero totale di operazioni S3 non riuscite che sono il risultato di un errore di autorizzazione.

storagegrid_servercertificate_management_interface_cert_expiry_days

Il numero di giorni prima della scadenza del certificato dell'interfaccia di gestione.

storagegrid_servercertificate_storage_api_endpoints_cert_expiry_days

Il numero di giorni prima della scadenza del certificato API dello storage a oggetti.

storagegrid_service_cpu_seconds

La quantità di tempo cumulativa in cui la CPU è stata utilizzata da questo servizio dopo l'installazione.

storagegrid_service_memory_usage_bytes

La quantità di memoria (RAM) attualmente utilizzata da questo servizio. Questo valore è identico a quello visualizzato dall'utility principale di Linux come RES.

storagegrid_service_network_received_bytes

La quantità totale di dati ricevuti dal servizio dopo l'installazione.

storagegrid_service_network_transmitted_bytes

La quantità totale di dati inviati da questo servizio.

storagegrid_service_reavvies

Il numero totale di riavvii del servizio.

storagegrid_service_runtime_seconds

Il tempo totale di esecuzione del servizio dopo l'installazione.

storagegrid_service_uptime_seconds

Il tempo totale di esecuzione del servizio dall'ultimo riavvio.

storagegrid_storage_state_current

Lo stato corrente dei servizi di storage. I valori degli attributi sono:

- 10 = non in linea
- 15 = manutenzione
- 20 = sola lettura
- 30 = Online

storagegrid_storage_status

Lo stato corrente dei servizi di storage. I valori degli attributi sono:

- 0 = Nessun errore

- 10 = in transizione
- 20 = spazio libero insufficiente
- 30 = Volume(i) non disponibile
- 40 = errore

storagegrid_storage_utilization_data_bytes

Una stima delle dimensioni totali dei dati di oggetti replicati e con erasure coding sul nodo storage.

storagegrid_storage_utilization_metadata_allowed_bytes

Lo spazio totale sul volume 0 di ciascun nodo di storage consentito per i metadati dell'oggetto. Questo valore è sempre inferiore allo spazio effettivo riservato ai metadati su un nodo, perché una parte dello spazio riservato è necessaria per le operazioni essenziali del database (come la compattazione e la riparazione) e i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati dell'oggetto controlla la capacità complessiva degli oggetti.

storagegrid_storage_utilization_metadata_bytes

La quantità di metadati oggetto sul volume di storage 0, in byte.

storagegrid_storage_utilization_total_space_bytes

La quantità totale di spazio di storage allocato a tutti gli archivi di oggetti.

storagegrid_storage_utilization_usable_space_bytes

La quantità totale di spazio di storage a oggetti rimanente. Calcolato sommando la quantità di spazio disponibile per tutti gli archivi di oggetti sul nodo di storage.

storagegrid_tenant_usage_data_bytes

La dimensione logica di tutti gli oggetti per il tenant.

storagegrid_tenant_usage_object_count

Il numero di oggetti per il tenant.

storagegrid_tenant_usage_quota_byte

La quantità massima di spazio logico disponibile per gli oggetti del tenant. Se non viene fornita una metrica di quota, è disponibile una quantità illimitata di spazio.

Ottieni un elenco di tutte le metriche

per ottenere l'elenco completo delle metriche, utilizza l'API Grid Management.

Fasi

1. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
2. Individuare le operazioni **metriche**.
3. Eseguire l'`GET /grid/metric-names` operazione.
4. Scarica i risultati.

Riferimenti ai file di log

File di log di StorageGRID

StorageGRID fornisce registri utilizzati per acquisire eventi, messaggi di diagnostica e condizioni di errore. Potrebbe essere richiesto di raccogliere i file di log e inoltrarli al supporto tecnico per agevolare la risoluzione dei problemi.

I log sono classificati come segue:

- ["Log del software StorageGRID"](#)
- ["Log di implementazione e manutenzione"](#)
- ["A proposito di bycast.log"](#)



I dettagli forniti per ciascun tipo di registro sono solo a scopo di riferimento. I registri sono destinati al troubleshooting avanzato da parte del supporto tecnico. Le tecniche avanzate che implicano la ricostruzione della cronologia dei problemi utilizzando i registri di controllo e i file di log dell'applicazione esulano dall'ambito di queste istruzioni.

Accedere ai registri

Per accedere ai registri, puoi ["raccogliere i file di log e i dati di sistema"](#) da uno o più nodi come un singolo archivio di file di registro. In alternativa, è possibile accedere ai singoli file di registro per ciascun nodo della griglia come segue:

Fasi

1. Immettere il seguente comando: `ssh admin@grid_node_IP`
2. Immettere la password elencata nel `Passwords.txt` file.
3. Immettere il seguente comando per passare alla directory principale: `su -`
4. Immettere la password elencata nel `Passwords.txt` file.

Esportare i log nel server syslog

L'esportazione dei registri al server syslog offre le seguenti funzionalità:

- Ricevi un elenco di tutte le richieste di Grid Manager e Tenant Manager, oltre alle richieste S3.
- Migliore visibilità delle richieste S3 che restituiscono errori, senza l'impatto sulle prestazioni causato dai metodi di registrazione degli audit.
- Accesso alle richieste del livello HTTP e ai codici di errore facili da analizzare.
- Migliore visibilità delle richieste bloccate dai classificatori del traffico nel bilanciamento del carico.

Per esportare i log, fare riferimento a ["Configurare la gestione dei log e il server syslog esterno"](#).

Categorie di file di log

L'archivio del file di log di StorageGRID contiene i log descritti per ciascuna categoria e i file aggiuntivi che contengono metriche e output dei comandi di debug.

Percorso di archiviazione	Descrizione
acct-tunnel.log	Registro per l'helper del tunnel account che funziona con il bilanciatore di carico.
audit	Messaggi di audit generati durante il normale funzionamento del sistema.
log-sistema-di-base	Informazioni di base sul sistema operativo, incluse le versioni delle immagini StorageGRID.
bundle	Informazioni sulla configurazione globale (bundle).
cache-svc	Memorizza i log del servizio nella cache (solo sui nodi gateway).
cassandra	Informazioni sul database Cassandra e registri di riparazione Reaper.
ce	Informazioni sui VCSs relative al nodo corrente e informazioni sul gruppo EC in base all'ID del profilo.
griglia	Log generali della griglia, inclusi debug (<code>broadcast.log</code>) e <code>servermanager</code> log.
grid.json	File di configurazione della griglia condiviso tra tutti i nodi. Inoltre, <code>node.json</code> è specifico per il nodo corrente.
hagroup	Metriche e registri dei gruppi ad alta disponibilità.
installare	<code>Gdu-server</code> e installare i registri.
internal-access.log	Registro interno del traffico proxy HTTP.
Arbitro lambda	Registri relativi alla richiesta del proxy S3 Select.
trapelato	Registri del servizio trapelato.
lumberjack.log	Messaggi di debug relativi alla raccolta dei log.
manage-audit.log	<code>`mgmt-api`</code> accedi ai registri di controllo.
Metriche	Log di servizio per Grafana, Jaeger, node exporter e Prometheus.
errore	Accesso Miscd e log degli errori.
mysql	La configurazione del database MariaDB e i relativi log.
netto	Log generati da script correlati alla rete e dal servizio Dynip.

Percorso di archiviazione	Descrizione
nginx	File e log di configurazione del bilanciamento del carico e della federazione di griglie. Include anche i log di traffico di Grid Manager e Tenant Manager.
nginx-gw	• <code>access.log</code>: Grid Manager e Tenant Manager richiedono messaggi di registrazione. ◦ Questi messaggi sono preceduti da <code>mgmt</code>: quando vengono esportati utilizzando syslog. ◦ 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 replica cross-grid in entrata. ◦ Questi messaggi sono preceduti da <code>cgr</code>: quando vengono esportati utilizzando syslog. ◦ 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 agli endpoint del bilanciatore del carico. ◦ Questi messaggi sono preceduti da <code>endpoint</code>: quando vengono esportati utilizzando syslog. ◦ 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>: Relativo al nuovo avviso di controllo DNS. • <code>stream-access.log</code>: sessioni proxy TCP/TLS stream (livello 4) per il blocco del flusso. Nota: Questo non è un registro delle richieste HTTP.
ntp	File di configurazione NTP e registri.
Oggetti orfani	Registri relativi agli oggetti orfani.
sistema operativo	File di stato nodo e griglia, inclusi i servizi <code>pid</code> .
altro	I file di registro in <code>/var/local/log</code> che non vengono raccolti in altre cartelle.
perf	Informazioni sulle prestazioni per CPU, rete e i/o del disco

Percorso di archiviazione	Descrizione
prometheus-data	Metriche Prometheus correnti, se la raccolta di log include i dati Prometheus.
provisioning	Log relativi al processo di provisioning della griglia.
zattera	Log dal cluster Raft utilizzato nei servizi della piattaforma.
revision_history.json	Cronologia delle revisioni.
routed-s3-access.log.gz	Registro degli accessi per il traffico di federazione della griglia instradato come S3 (URL di spazio dei nomi globale/federazione).
ssh	Registri relativi alla configurazione e al servizio SSH.
snmp	Configurazione dell'agente SNMP utilizzata per l'invio di notifiche SNMP.
socket-dati	Dati socket per il debug di rete.
system-bucket.log	update-system-bucket-configuration.log: Log del bucket di sistema.
system-commands.txt	Output dei comandi del container StorageGRID. Contiene informazioni di sistema, ad esempio le reti e l'utilizzo del disco.
pacchetto-ripristino-sincronizzazione	Correlato al mantenimento della coerenza del pacchetto di ripristino più recente su tutti i nodi di amministrazione e di archiviazione che ospitano il servizio ADC.
update-cipher-configurations.log	update-cors-configurations.log: Traccia i log relativi alle modifiche di TLS/cifratura e CORS.
update-leakd-configurations.log	Registro di configurazione del rilevamento degli orfani.

Log del software StorageGRID

È possibile utilizzare i registri di 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 `bycast.log` e `nms.log`, Vedere ["Configurare la gestione dei log"](#).

Log StorageGRID generali

Nome del file	Note	Trovato in
/var/local/log/bycast.log	Il file principale per la risoluzione dei problemi StorageGRID .	Tutti i nodi
/var/local/log/bycast-err.log	Contiene un sottoinsieme di <code>bycast.log</code> (messaggi con gravità ERROR e CRITICAL). Nel sistema vengono visualizzati anche i messaggi CRITICI .	Tutti i nodi
/var/local/core/	Contiene tutti i file core dump creati se il programma termina in modo anomalo. Le possibili cause includono errori di asserzione, violazioni o timeout di thread. Nota: Il file di <code>/var/local/core/kexec_cmd</code> solito esiste sui nodi dell'appliance e non indica un errore.	Tutti i nodi

Log relativi alla crittografia

Nome del file	Note	Trovato in
/var/local/log/ssh-config-generation.log	Contiene i log relativi alla generazione delle configurazioni SSH e al ricaricamento dei servizi SSH.	Tutti i nodi
/var/local/log/nginx/config-generation.log	Contiene i log relativi alla generazione di configurazioni nginx e al ricaricamento dei servizi nginx.	Tutti i nodi
/var/local/log/nginx-gw/config-generation.log	Contiene i log relativi alla generazione di configurazioni nginx-gw (e al ricaricamento dei servizi nginx-gw).	Nodi Admin e Gateway
/var/local/log/update-cipher-configurations.log	Contiene i registri relativi alla configurazione dei criteri TLS e SSH.	Tutti i nodi

Log della federazione di griglie

Nome del file	Note	Trovato in
/var/local/log/update_grid_federation_config.log	Contiene i log relativi alla generazione di configurazioni nginx e nginx-gw per le connessioni di federazione di griglie.	Tutti i nodi

Registri NMS

Nome del file	Note	Trovato in
/var/local/log/nms.log	• Acquisisce le notifiche da Grid Manager e Tenant Manager. • Acquisisce gli eventi correlati al funzionamento del servizio NMS. Ad esempio, notifiche e-mail e modifiche alla configurazione. • Contiene gli aggiornamenti del bundle XML risultanti dalle modifiche di configurazione apportate nel sistema. • Contiene messaggi di errore relativi al downsampling degli attributi eseguito una volta al giorno. • Contiene messaggi di errore del server Web Java, ad esempio errori di generazione pagina e errori HTTP Status 500. • Contiene i log relativi a AutoSupport.	Nodi di amministrazione
/var/local/log/nms.errlog	Contiene messaggi di errore relativi agli aggiornamenti del database MySQL. Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di amministrazione
/var/local/log/nms.requestlog	Contiene informazioni sulle connessioni in uscita dall'API di gestione ai servizi StorageGRID interni.	Nodi di amministrazione

Log di Server Manager

Nome del file	Note	Trovato in
/var/local/log/servermanager.log	File di log per l'applicazione Server Manager in esecuzione sul server.	Tutti i nodi
/var/local/log/GridstatBackend.errlog	File di log per l'applicazione backend della GUI di Server Manager.	Tutti i nodi
/var/local/log/gridstat.errlog	File di log per la GUI di Server Manager.	Tutti i nodi

Log dei servizi StorageGRID

Nome del file	Note	Trovato in
/var/local/log/acct.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/adc.errlog	Contiene il flusso standard di errore (stderr) dei servizi corrispondenti. Esiste un file di log per servizio. Questi file sono generalmente vuoti, a meno che non si verifichino problemi con il servizio.	Nodi di storage che eseguono il servizio ADC
/var/local/log/ams.errlog		Nodi di amministrazione
/var/local/log/cache-svc.log + /var/local/log/cache-svc.errlog	Memorizza i log del servizio di cache.	Nodi gateway
/var/local/log/cassandra/system.log	Informazioni per l'archivio di metadati (database Cassandra) che possono essere utilizzate se si verificano problemi durante l'aggiunta di nuovi nodi di storage o se l'attività di riparazione nodetool si blocca.	Nodi di storage
/var/local/log/cassandra-reaper.log	Informazioni per il servizio Cassandra Reaper, che esegue la riparazione dei dati nel database Cassandra.	Nodi di storage
/var/local/log/cassandra-reaper.errlog	Informazioni sugli errori per il servizio Cassandra Reaper.	Nodi di storage
/var/local/log/chunk.errlog		Nodi di storage
/var/local/log/cmn.errlog		Nodi di amministrazione
/var/local/log/cms.errlog	Questo file di log potrebbe essere presente sui sistemi che sono stati aggiornati da una versione precedente di StorageGRID. Contiene informazioni legacy.	Nodi di storage
/var/local/log/dds.errlog		Nodi di storage
/var/local/log/dmv.errlog		Nodi di storage

Nome del file	Note	Trovato in
/var/local/log/dynip*	Contiene i registri relativi al servizio di dinip, che monitora la griglia per rilevare le modifiche dell'IP dinamico e aggiorna la configurazione locale.	Tutti i nodi
/var/local/log/grafana.log	Log associato al servizio Grafana, utilizzato per la visualizzazione delle metriche in Grid Manager.	Nodi di amministrazione
/var/local/log/hagroups.log	Log associato ai gruppi ad alta disponibilità.	Nodi di amministrazione e nodi gateway
/var/local/log/hagroups_events.log	Tiene traccia delle modifiche di stato, come la transizione da BACKUP a MASTER o FAULT.	Nodi di amministrazione e nodi gateway
/var/local/log/idnt.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/jaeger.log	Log associato al servizio jaeger, utilizzato per la raccolta delle tracce.	Tutti i nodi
/var/local/log/kstn.errlog		Nodi di storage che eseguono il servizio ADC
/var/local/log/lambda*	Contiene i registri per il servizio S3 Select.	Nodi Admin e Gateway Solo alcuni nodi Admin e Gateway contengono questo log. Consultare la "S3 selezionare requisiti e limitazioni per i nodi Admin e Gateway" .
/var/local/log/ldr.errlog		Nodi di storage
/var/local/log/miscd/*.log	Contiene i log per il servizio MISCd (Information Service Control Daemon), che fornisce un'interfaccia per eseguire query e gestire servizi su altri nodi e per gestire le configurazioni ambientali sul nodo, ad esempio per eseguire query sullo stato dei servizi in esecuzione su altri nodi.	Tutti i nodi

Nome del file	Note	Trovato in
/var/local/log/nginx/*.log	Contiene i log per il servizio nginx, che funge da meccanismo di autenticazione e comunicazione sicura per diversi servizi grid (come Prometheus e Dynip) per poter comunicare con servizi su altri nodi tramite API HTTPS.	Tutti i nodi
/var/local/log/nginx-gw/*.log	Contiene i log generali relativi al servizio nginx-gw, inclusi i log degli errori e i log per le porte amministrative limitate sui nodi di amministrazione.	Nodi di amministrazione e nodi gateway
/var/local/log/nginx-gw/cgr-access.log.gz	Contiene log di accesso relativi al traffico di replica cross-grid.	Nodi di amministrazione, nodi gateway o entrambi, in base alla configurazione della federazione di griglie. Trovato solo nella griglia di destinazione per la replica cross-grid.
/var/local/log/nginx-gw/endpoint-access.log.gz	Contiene log di accesso per il servizio Load Balancer, che fornisce il bilanciamento del carico del traffico S3 dai client ai nodi storage.	Nodi di amministrazione e nodi gateway
/var/local/log/persistence*	Contiene i log per il servizio di persistenza, che gestisce i file sul disco root che devono persistere durante un riavvio.	Tutti i nodi
/var/local/log/prometheus.log	Per tutti i nodi, contiene il log del servizio dell'esportatore di nodi e il log del servizio di metriche dell'esportatore. Per i nodi di amministrazione, contiene anche i registri per i servizi Prometheus e Alert Manager.	Tutti i nodi
/var/local/log/raft.log	Contiene l'output della libreria utilizzata dal servizio RSM per il protocollo Raft.	Nodi storage con servizio RSM
/var/local/log/rms.errlog	Contiene i registri per il servizio RSM (Replicated state Machine Service), utilizzato per i servizi della piattaforma S3.	Nodi storage con servizio RSM
/var/local/log/ssm.errlog		Tutti i nodi

Nome del file	Note	Trovato in
/var/local/log/update-s3vs-domains.log	Contiene i registri relativi all'elaborazione degli aggiornamenti per la configurazione dei nomi di dominio host virtuali S3.vedere le istruzioni per l'implementazione delle applicazioni client S3.	Nodi Admin e Gateway
/var/local/log/update-snmp-firewall.*	Contiene i registri relativi alle porte firewall gestite per SNMP.	Tutti i nodi
/var/local/log/update-sysl.log	Contiene i registri relativi alle modifiche apportate alla configurazione syslog del sistema.	Tutti i nodi
/var/local/log/update-traffic-classes.log	Contiene i registri relativi alle modifiche apportate alla configurazione dei classificatori del traffico.	Nodi Admin e Gateway
/var/local/log/update-utcn.log	Contiene i registri relativi alla modalità di rete client non attendibile su questo nodo.	Tutti i nodi

Informazioni correlate

- ["A proposito di bycast.log"](#)
- ["UTILIZZARE L'API REST S3"](#)

Registri di distribuzione e manutenzione in StorageGRID

È possibile utilizzare i registri di implementazione e manutenzione per risolvere i problemi.

Nome del file	Note	Trovato in
/var/local/log/install.log	Creato durante l'installazione del software. Contiene un record degli eventi di installazione.	Tutti i nodi
/var/local/log/expansion-progress.log	Creato durante le operazioni di espansione. Contiene un record degli eventi di espansione.	Nodi di storage
/var/local/log/pa-move.log	Creato durante l'esecuzione <code>pa-move.sh</code> dello script.	Nodo amministratore primario
/var/local/log/pa-move-new_pa.log	Creato durante l'esecuzione <code>pa-move.sh</code> dello script.	Nodo amministratore primario

Nome del file	Note	Trovato in
/var/local/log/pa-move-old_pa.log	Creato durante l'esecuzione <code>pa-move.sh</code> dello script.	Nodo amministratore primario
/var/local/log/gdu-server.log	Creato dal servizio GDU. Contiene eventi correlati alle procedure di provisioning e manutenzione gestite dal nodo di amministrazione primario.	Nodi di amministrazione
/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

Scopri il file `broadcast.log` di StorageGRID

Il file `/var/local/log/broadcast.log` è il file di risoluzione dei problemi principale per il software StorageGRID. Esiste un `broadcast.log` file per ogni nodo della griglia. Il file contiene messaggi specifici del nodo della griglia.

Il file `/var/local/log/broadcast-err.log` è un sottoinsieme di `broadcast.log`. Contiene messaggi di errore di severità e CRITICI.

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 la gestione dei log e il server syslog esterno"](#).

Rotazione del file per `broadcast.log`

Quando il `broadcast.log` file raggiunge i 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 viene denominato `broadcast.log`. Quando il nuovo `broadcast.log` raggiunge i 1 GB, `broadcast.log.1` viene rinominato e compresso in diventa `broadcast.log.2.gz`, e `broadcast.log` viene rinominato `broadcast.log.1`.

Il limite di rotazione per `broadcast.log` è di 21 file. Quando viene creata la versione 22nd del `broadcast.log` file, il file più vecchio viene eliminato.

Il limite di rotazione per `broadcast-err.log` è di sette file.



Se un file di log è stato compresso, non è necessario decomprimerlo nella stessa posizione in cui è stato scritto. La decompressione del file nella stessa posizione può interferire con gli script di rotazione del log.

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 la gestione dei log e il server syslog esterno"](#).

Informazioni correlate

["Raccogliere i file di log e i dati di sistema"](#)

Messaggi nel bycast.log

I messaggi in `bycast.log` sono scritti dall'ADE (Asynchronous Distributed Environment). ADE è l'ambiente di runtime utilizzato dai servizi di ciascun nodo di rete.

Esempio di messaggio ADE:

```
May 15 14:07:11 um-sec-rg1-agn3 ADE: |12455685      0357819531
SVMR EVHR 2019-05-05T27T17:10:29.784677| ERROR 0906 SVMR: Health
check on volume 3 has failed with reason 'TOUT'
```

I messaggi ADE contengono le seguenti informazioni:

Segmento di messaggio	Valore nell'esempio
ID nodo	12455685
ID processo ADE	0357819531
Nome del modulo	SVMR
Identificatore del messaggio	EVHR
Ora di sistema UTC	2019-05-05T27T17:10:29.784677 (AAAA-MM-DDGH:MM:SS.UUUUUUUU)
Livello di severità	ERRORE
Numero di tracking interno	0906
Messaggio	SVMR: Controllo dello stato di salute sul volume 3 non riuscito con motivo 'TOUT'

Severità dei messaggi nel bycast.log

I messaggi in `bycast.log` sono livelli di gravità assegnati.

Ad esempio:

- **NOTA** — si è verificato un evento da registrare. La maggior parte dei messaggi di log è a questo livello.
- **ATTENZIONE** — si è verificata una condizione imprevista.
- **ERRORE** — si è verificato un errore grave che ha un impatto sulle operazioni.

- **CRITICO** — si è verificata una condizione anomala che ha interrotto le normali operazioni. È necessario risolvere immediatamente la condizione sottostante.

Codici di errore in `broadcast.log`

La maggior parte dei messaggi di errore in `broadcast.log` contiene 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 è riportato.

Codice di errore	Significato
SUC	Nessun errore
GERR	Sconosciuto
CANC	Annullato
ABRT	Interrotto
TOUT	Timeout
INVL	Non valido
NFND	Non trovato
VERS	Versione
CONF	Configurazione
NON RIUSCITO	Non riuscito
ICPL	Incompleto
FATTO	Fatto
SUNV	Servizio non disponibile

La tabella seguente elenca i codici di errore numerici in `broadcast.log`.

Numero di errore	Codice di errore	Significato
001	EPER	Operazione non consentita
002	ENOENT	Nessun file o directory di questo tipo

Numero di errore	Codice di errore	Significato
003	ESRCH	Nessun processo di questo tipo
004	EINTR	Chiamata di sistema interrotta
005	EIO	Errore i/O.
006	ENXIO	Nessun dispositivo o indirizzo di questo tipo
007	E2BIG	Elenco di argomenti troppo lungo
008	ENOEXEC	Errore di formato Exec
009	EBADF	Numero di file errato
010	ECHILD	Nessun processo figlio
011	EAGAIN	Riprovare
012	ENOMEM	Memoria esaurita
013	EACCES	Permesso negato
014	EFAULT	Indirizzo non valido
015	ENOTBLK	Dispositivo a blocchi richiesto
016	EBUSY	Periferica o risorsa occupata
017	EEXIST	Il file esiste
018	ESCLUDI	Collegamento tra dispositivi
019	ENODEV	Nessun dispositivo di questo tipo
020	ENOTDIR	Non una directory
021	EISDIR	È una directory
022	EINVAL	Argomento non valido
023	ENFILE	Overflow della tabella dei file

Numero di errore	Codice di errore	Significato
024	EMFILE	Troppi file aperti
025	ENOTTY	Non è una macchina da scrivere
026	ETXTBSY	File di testo occupato
027	EFBIG	File troppo grande
028	ENOSPC	Spazio non disponibile sul dispositivo
029	ESPIPE	Ricerca illegale
030	EROFS	File system di sola lettura
031	EMSINK	Troppi collegamenti
032	EPIPE	Tubo rotto
033	EDOM	Argomento matematico fuori dominio della funzione
034	ERANGE	Risultato matematico non rappresentabile
035	EDEADLK	Si verificherebbe un deadlock delle risorse
036	ENAMETOOLONG	Nome file troppo lungo
037	ENOLCK	Nessun blocco di record disponibile
038	ENOSYS	Funzione non implementata
039	ENOTEMPTY	Directory non vuota
040	ELOOP	Sono stati rilevati troppi collegamenti simbolici
041		
042	ENOMSG	Nessun messaggio del tipo desiderato
043	EIDRM	Identificatore rimosso
044	ECHRNG	Numero di canale fuori intervallo

Numero di errore	Codice di errore	Significato
045	EL2NSYNC	Livello 2 non sincronizzato
046	EL3HLT	Livello 3 arrestato
047	EL3RST	Ripristino 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 arrestato
052	EBADE	Scambio non valido
053	EBADR	Descrittore della richiesta non valido
054	ESCLUDI	Exchange pieno
055	ENOANO	Nessun anodo
056	EBADRQC	Codice di richiesta non valido
057	EBADSLT	Slot non valido
058		
059	EBFONT	Formato del file di font non valido
060	ENOSTR	Il dispositivo non è un flusso
061	ENODATA	Nessun dato disponibile
062	ETIME	Timer scaduto
063	ENOSR	Risorse out of Streams
064	ENONET	La macchina non è in rete
065	ENOPKG	Pacchetto non installato

Numero di errore	Codice di errore	Significato
066	EREMOTE	L'oggetto è remoto
067	ENOLINK	Il collegamento è stato separato
068	EADV	Errore di pubblicità
069	ESRMNT	Errore Srmount
070	ECOMM	Errore di comunicazione durante l'invio
071	PRONTO	Errore di protocollo
072	EMULTIHOP	Tentativo di multihop
073	EDOTDOT	Errore specifico RFS
074	EBADMSG	Non è un messaggio dati
075	Eoverflow	Valore troppo grande per il tipo di dati definito
076	ENOTUNIQ	Nome non univoco sulla rete
077	EBADFD	Descrittore del file in stato non valido
078	EREMCHG	Indirizzo remoto modificato
079	ELIBACC	Impossibile accedere a una libreria condivisa necessaria
080	ELIBBAD	Accesso a una libreria condivisa danneggiata
081	ELIBSCN	
082	ELIBMAX	Tentativo di collegamento in troppe librerie condivise
083	ELIBEXEC	Impossibile eseguire direttamente una libreria condivisa
084	EILSEQ	Sequenza di byte non valida
085	ERESTART	La chiamata di sistema interrotta deve essere riavviata

Numero di errore	Codice di errore	Significato
086	ESTRPIPE	Errore pipe flussi
087	EUSERS	Troppi utenti
088	ENOTSOCK	Funzionamento socket su non socket
089	EDESTADDRREQ	Indirizzo di destinazione obbligatorio
090	EMSGSIZE	Messaggio troppo lungo
091	EPROTOTYPE	Tipo di protocollo errato per il socket
092	ENOPROTOOPT	Protocollo non disponibile
093	EPROTONOSUPPORT	Protocollo non supportato
094	SESOCKTNOSUPPORT	Tipo di socket non supportato
095	EOPNOTSUPP	Operazione non supportata sull'endpoint di trasporto
096	EPFNOSUPPORT	Famiglia di protocolli non supportata
097	EAFNOSUPPORT	Famiglia di indirizzi non supportata dal protocollo
098	EADDRINUSE	Indirizzo già in uso
099	EADDRNOTAVAIL	Impossibile assegnare l'indirizzo richiesto
100	ENETDOWN	La rete non è disponibile
101	ENETUNREACH	La rete non è raggiungibile
102	ENETRESET	Connessione di rete interrotta a causa del ripristino
103	PRONTO	Il software ha causato l'interruzione della connessione
104	ECONNRESET	Connessione ripristinata da peer
105	ENOBUFS	Spazio buffer non disponibile
106	EISCONN	Endpoint di trasporto già connesso

Numero di errore	Codice di errore	Significato
107	ENOTCONN	Endpoint di trasporto non connesso
108	ESHUTDOWN	Impossibile inviare dopo l'arresto dell'endpoint di trasporto
109	ETOOMANYREFS	Troppi riferimenti: Impossibile unire
110	ETIMEDOUT	Timeout della connessione
111	ECONNREFUSED	Connessione rifiutata
112	EHOSTDOWN	Host non attivo
113	EHOSTUNREACH	Nessun percorso verso l'host
114	EALREADY	Operazione già in corso
115	EINPROGRESS	Operazione in corso
116		
117	EUCLEAN	La struttura deve essere pulita
118	ENOTNAM	Non è un file XENIX denominato
119	ENAVAIL	Nessun semaphore XENIX disponibile
120	EISNAM	È un file di tipo denominato
121	EREMOTEIO	Errore i/o remoto
122	EDQUOT	Quota superata
123	ENOMEDIUM	Nessun supporto trovato
124	EMPDIUMTYPE	Tipo di supporto errato
125	LED ECANCELED	Operazione annullata
126	ENOKEY	Chiave richiesta non disponibile
127	EKEYEXPIRED	Chiave scaduta

Numero di errore	Codice di errore	Significato
128	EKEYREVOKED	Chiave revocata
129	EKEYREJECTED	Chiave rifiutata dal servizio
130	EOWNERDEAD	Per i mutex più forti: Il proprietario è morto
131	ENOTRECOVERABLE	Per mutex affidabili: Stato non ripristinabile

Configurare la gestione dei log e il server syslog esterno

Server syslog esterni in StorageGRID

Un server syslog esterno è un server esterno a StorageGRID che può essere utilizzato per raccogliere informazioni di controllo del sistema in una singola posizione. L'utilizzo di un server syslog esterno consente di ridurre il traffico di rete sui nodi Admin e di gestire le informazioni in modo più efficiente. Per StorageGRID, il formato del pacchetto di messaggi syslog in uscita è conforme con RFC 3164.

I tipi di informazioni di controllo che è possibile inviare al server syslog esterno includono:

- Registri di audit contenenti i messaggi di audit generati durante il normale funzionamento del sistema
- Eventi correlati alla sicurezza, come accessi ed escalation a root
- Log delle applicazioni che potrebbero essere richiesti se è necessario aprire un caso di supporto per risolvere un problema riscontrato

Quando utilizzare un server syslog esterno

Un server syslog esterno è particolarmente utile se si dispone di un grid di grandi dimensioni, se si utilizzano più tipi di applicazioni S3 o se si desidera mantenere tutti i dati di revisione. L'invio di informazioni di audit a un server syslog esterno consente di:

- Raccogliere e gestire in modo più efficiente le informazioni di audit come messaggi di audit, registri delle applicazioni ed eventi di sicurezza.
- Riduci il traffico di rete sui nodi amministrativi, perché le informazioni di audit vengono trasferite direttamente dai vari nodi storage al server syslog esterno, senza dover passare attraverso un nodo amministrativo.



Quando i log vengono inviati a un server syslog esterno, i log singoli superiori a 8.192 byte vengono troncati alla fine del messaggio in conformità con le limitazioni comuni nelle implementazioni del server syslog esterno.



Per massimizzare le opzioni per il recupero completo dei dati in caso di guasto del server syslog esterno, (`localaudit.log` su ciascun nodo vengono mantenuti fino a 20 GB di registri locali dei record di controllo).

Come configurare un server syslog esterno

Per informazioni su come configurare un server syslog esterno, vedere ["Configurare la gestione dei log e il server syslog esterno"](#).

Se si intende configurare l'utilizzo del protocollo TLS o RELP/TLS, è necessario disporre dei seguenti certificati:

- **Certificati CA del server:** Uno o più certificati CA attendibili per la verifica del server syslog esterno nella codifica PEM. Se omesso, verrà utilizzato il certificato Grid CA predefinito.
- **Certificato client:** Certificato client per l'autenticazione al server syslog esterno nella codifica PEM.
- **Chiave privata client:** Chiave privata per il certificato client nella codifica PEM.



Se si utilizza un certificato client, è necessario utilizzare anche una chiave privata client. Se si fornisce una chiave privata crittografata, è necessario fornire anche la passphrase. L'utilizzo di una chiave privata crittografata non offre alcun vantaggio significativo in termini di sicurezza, in quanto è necessario memorizzare la chiave e la passphrase; per semplicità, si consiglia di utilizzare una chiave privata non crittografata, se disponibile.

Come valutare le dimensioni del server syslog esterno

Normalmente, il tuo grid è dimensionato per ottenere un throughput richiesto, definito in termini di operazioni S3 al secondo o byte al secondo. Ad esempio, potrebbe essere necessario che la griglia gestisca 1,000 operazioni S3 al secondo, o 2,000 MB al secondo, di acquisizione e recupero di oggetti. È necessario dimensionare il server syslog esterno in base ai requisiti dei dati del grid.

Questa sezione fornisce alcune formule euristiche che consentono di stimare la velocità e la dimensione media dei messaggi di log di vari tipi che il server syslog esterno deve gestire, espresse in termini di caratteristiche di performance note o desiderate della griglia (operazioni S3 al secondo).

Utilizzare le operazioni S3 al secondo nelle formule di stima

Se la griglia è stata dimensionata per un throughput espresso in byte al secondo, è necessario convertire questo dimensionamento in operazioni S3 al secondo per utilizzare le formule di stima. Per convertire il throughput della griglia, è necessario innanzitutto determinare la dimensione media degli oggetti, che è possibile utilizzare utilizzando le informazioni contenute nei registri di audit e nelle metriche esistenti (se presenti), oppure utilizzando la conoscenza delle applicazioni che utilizzeranno StorageGRID. Ad esempio, se la griglia è stata dimensionata per ottenere un throughput di 2,000 MB/secondo e la dimensione media dell'oggetto è di 2 MB, la griglia è stata dimensionata in modo da poter gestire 1,000 operazioni S3 al secondo (2,000 MB/2 MB).



Le formule per il dimensionamento del server syslog esterno nelle sezioni seguenti forniscono stime dei casi comuni (piuttosto che stime dei casi peggiori). A seconda della configurazione e del carico di lavoro, è possibile che venga visualizzata una velocità di messaggi syslog o un volume di dati syslog superiore o inferiore rispetto a quanto previsto dalle formule. Le formule devono essere utilizzate solo come linee guida.

Formule di stima per i log di audit

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule: Presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore):

```
Audit Log Rate = 2 x S3 Operations Rate
Audit Log Average Size = 800 bytes
```

Ad esempio, se la griglia è dimensionata per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 2,000 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di 1.6 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i registri di controllo, le variabili aggiuntive più importanti sono la percentuale di S3 operazioni che sono put (rispetto a GET) e la dimensione media, in byte, dei seguenti S3 campi (le abbreviazioni a 4 caratteri utilizzate nella tabella sono nomi di campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Utilizziamo P per rappresentare la percentuale di operazioni S3 che vengono messe, dove $0 \leq P \leq 1$ (quindi per un carico di lavoro PUT del 100%, $P = 1$ e per un carico DI lavoro GET del 100%, $P = 0$).

Utilizzare K per rappresentare la dimensione media della somma dei S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi il valore di K è 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei registri di controllo che il server syslog esterno dovrà gestire utilizzando le seguenti formule, presupponendo che i livelli di audit siano impostati sui valori predefiniti (tutte le categorie sono impostate su normale, ad eccezione di Storage, Che è impostato su Error):

```
Audit Log Rate = ((2 x P) + (1 - P)) x S3 Operations Rate
Audit Log Average Size = (570 + K) bytes
```

Ad esempio, se il tuo grid è dimensionato per 1,000 operazioni S3 al secondo, il tuo carico di lavoro è pari al 50% di put e i tuoi nomi account S3, nomi bucket, E i nomi degli oggetti hanno una media di 90 byte, il server

syslog esterno deve essere dimensionato per supportare 1,500 messaggi syslog al secondo e dovrebbe essere in grado di ricevere (e in genere memorizzare) i dati del registro di controllo a una velocità di circa 1 MB al secondo.

Formule di stima per livelli di audit non predefiniti

Le formule fornite per i registri di controllo presuppongono l'utilizzo delle impostazioni predefinite del livello di controllo (tutte le categorie sono impostate su normale, ad eccezione dello storage, che è impostato su errore). Non sono disponibili formule dettagliate per la stima del tasso e della dimensione media dei messaggi di audit per le impostazioni del livello di audit non predefinite. Tuttavia, la seguente tabella può essere utilizzata per effettuare una stima approssimativa del tasso; è possibile utilizzare la formula delle dimensioni medie fornita per i registri di controllo, ma è probabile che si verifichi una sovrastima perché i messaggi di controllo "extra" sono, in media, più piccoli dei messaggi di controllo predefiniti.

Condizione	Formula
Replica: Tutti i livelli di controllo sono impostati su Debug o Normal	Tasso del registro di controllo = 8 x S3 tasso di operazioni
Erasure coding (codifica erasure): I livelli di audit sono tutti impostati su Debug o Normal (normale)	Utilizzare la stessa formula utilizzata per le impostazioni predefinite

Formule di stima per gli eventi di sicurezza

Gli eventi di sicurezza non sono correlati con le operazioni S3 e in genere producono un volume trascurabile di log e dati. Per questi motivi, non vengono fornite formule di stima.

Formule di stima per i log delle applicazioni

Se non si dispone di informazioni sul carico di lavoro S3 diverse dal numero di operazioni S3 al secondo supportate dal grid, è possibile stimare il volume di log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule:

```
Application Log Rate = 3.3 x S3 Operations Rate
Application Log Average Size = 350 bytes
```

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il server syslog esterno deve essere dimensionato in modo da supportare 3,300 log delle applicazioni al secondo ed essere in grado di ricevere (e memorizzare) i dati del log delle applicazioni a una velocità di circa 1.2 MB al secondo.

Se conosci meglio il tuo carico di lavoro, puoi effettuare stime più accurate. Per i log delle applicazioni, le variabili aggiuntive più importanti sono la strategia di protezione dei dati (replica rispetto all'erasure coding), la percentuale di S3 operazioni messe (rispetto a GET/altro) e la dimensione media, in byte, dei seguenti S3 campi (le abbreviazioni di 4 caratteri utilizzate nella tabella sono i nomi dei campi del registro di controllo):

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.

Codice	Campo	Descrizione
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Tasto S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.

Stime di dimensionamento di esempio

In questa sezione vengono illustrati esempi di utilizzo delle formule di stima per le griglie con i seguenti metodi di protezione dei dati:

- Replica
- Erasure coding

Se si utilizza la replica per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove $0 \leq P \leq 1$ (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 S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K , è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

```
Application Log Rate = ((1.1 x P) + (2.5 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (220 + K)) + ((1 - P) x (240 + (0.2 x K))) Bytes
```

Ad esempio, se il grid è dimensionato per 1,000 operazioni S3 al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket e i nomi degli oggetti sono in media di 90 byte, il server syslog esterno deve essere dimensionato in modo da supportare 1800 log delle applicazioni al secondo, E riceverà (e in genere memorizzerà) i dati delle applicazioni a una velocità di 0.5 MB al secondo.

Se si utilizza l'erasure coding per la protezione dei dati

Sia P la percentuale di operazioni S3 che vengono messe, dove $0 \leq P \leq 1$ (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 S3 nomi di account, S3 bucket e S3 chiave. Supponiamo che il

nome dell'account S3 sia sempre my-s3-account (13 byte), che i bucket abbiano nomi a lunghezza fissa come /my/application/bucket-12345 (28 byte) e che gli oggetti abbiano chiavi a lunghezza fissa come 5733a5d7-f069-41ef-8fbd-13247494c69c (36 byte). Quindi K ha un valore di 90 (13+13+28+36).

Se è possibile determinare i valori per P e K, è possibile stimare il volume dei log delle applicazioni che il server syslog esterno dovrà gestire utilizzando le seguenti formule.

```
Application Log Rate = ((3.2 x P) + (1.3 x (1 - P))) x S3 Operations Rate
Application Log Average Size = (P x (240 + (0.4 x K))) + ((1 - P) x (185 + (0.9 x K))) Bytes
```

Ad esempio, se il grid è dimensionato per 1.000 S3 operazioni al secondo, il carico di lavoro è pari al 50% e i nomi degli account S3, i nomi dei bucket mentre i nomi degli oggetti hanno una media di 90 byte, il server syslog esterno dovrebbe essere dimensionato in modo da supportare 2.250 registri delle applicazioni al secondo e dovrebbe essere in grado di ricevere (e generalmente archiviare) dati delle applicazioni a una velocità di 0,6 MB al secondo.

Configura la gestione dei log in StorageGRID

Se necessario, configura i livelli di audit, le intestazioni del protocollo, la posizione dei messaggi e dei log di audit e la conservazione dei log.

Tutti i nodi StorageGRID generano messaggi di controllo e registri per monitorare l'attività e gli eventi del sistema. I messaggi e i registri di controllo sono strumenti essenziali per il monitoraggio e la risoluzione dei problemi.

Facoltativamente, puoi ["configurare un server syslog esterno"](#) per salvare le informazioni di audit in remoto. Puoi ridurre al minimo l'impatto sulle prestazioni della registrazione dei messaggi di audit senza ridurre la completezza dei dati di audit utilizzando un server esterno. Un syslog server esterno è particolarmente utile se hai una griglia di grandi dimensioni, usi diversi tipi di applicazioni S3 o vuoi conservare tutti i dati di audit.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Se si prevede di configurare un server syslog esterno, è necessario aver esaminato e seguito quanto segue. ["considerazioni sull'utilizzo di un server syslog esterno"](#).
- Se si intende configurare un server syslog esterno utilizzando il protocollo TLS o RELP/TLS, si dispone della CA del server e dei certificati client richiesti e della chiave privata del client.

Modificare i livelli dei messaggi di controllo

È possibile impostare un livello di audit diverso per ciascuna delle seguenti categorie di messaggi nel registro di audit:

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Sistema	Normale	"Messaggi di audit del sistema"

Categoria di audit	Impostazione predefinita	Ulteriori informazioni
Storage	Errore	"Messaggi di audit dello storage a oggetti"
Gestione	Normale	"Messaggio di audit della gestione"
Lecture del client	Normale	"Messaggi di audit in lettura del client"
Il client scrive	Normale	"Messaggi di audit di scrittura del client"
ILM	Normale	"Messaggi di controllo ILM"
Replica cross-grid	Errore	"CGRR: Richiesta di replica cross-grid"



Durante gli aggiornamenti, le configurazioni a livello di audit non saranno immediatamente effettive.

Fasi

1. Selezionare **Configurazione > Monitoraggio > Gestione log**.
2. Per ciascuna categoria di messaggi di audit, selezionare un livello di audit dall'elenco a discesa:

Livello di audit	Descrizione
Spento	Non vengono registrati messaggi di audit della categoria.
Errore	Vengono registrati solo 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 audit normale.

I messaggi inclusi per qualsiasi livello specifico includono quelli che verrebbero registrati ai livelli superiori. Ad esempio, il livello normale include tutti i messaggi di errore.



Se non hai bisogno di un registro dettagliato delle operazioni di lettura client per le tue applicazioni S3, puoi facoltativamente modificare l'impostazione **Lecture client** in **Errore** per ridurre il numero di messaggi di controllo registrati nel registro di controllo.

3. Selezionare **Salva**.

Definire le intestazioni delle richieste HTTP

Facoltativamente, è possibile definire qualsiasi intestazione di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client.

Fasi

1. Nella sezione **Audit Protocol headers**, definire le intestazioni di richiesta HTTP che si desidera includere nei messaggi di controllo di lettura e scrittura del client.

Utilizzare un asterisco (*) come carattere jolly per far corrispondere zero o più caratteri. Utilizzare la sequenza escape (\) per far corrispondere un asterisco letterale.

2. Selezionare **Add another header** (Aggiungi un'altra intestazione) per creare altre intestazioni, se necessario.

Quando StorageGRID rileva intestazioni HTTP in una richiesta, le include nel messaggio di audit nel campo HTRH.



Le intestazioni delle richieste del protocollo di controllo vengono registrate solo se il livello di controllo per **Lecture client** o **Scritture client** non è **Disattivato**.

3. Selezionare **Salva**

Configura la posizione del registro

Per impostazione predefinita, i messaggi di audit e i log vengono salvati sui nodi in cui vengono generati. StorageGRID ruota regolarmente e infine elimina i messaggi di audit e i log per evitare che consumino troppo spazio su disco. Per salvare i messaggi di audit e un sottoinsieme di log esternamente, [utilizzare un server syslog esterno](#).

Se si desidera salvare i file di registro internamente, scegliere un tenant e un bucket per l'archiviazione dei registri e abilitare l'archiviazione dei registri.

Usa un server syslog esterno

In alternativa, è possibile configurare un server syslog esterno per salvare registri di controllo, registri delle applicazioni e registri di eventi di sicurezza in una posizione esterna alla griglia.



Se non si desidera utilizzare un server syslog esterno, saltare questo passaggio e andare a [Seleziona la posizione del registro](#).



Se le opzioni di configurazione disponibili in questa procedura non sono sufficientemente flessibili da soddisfare i requisiti, è possibile applicare ulteriori opzioni di configurazione utilizzando gli `audit-destinations` endpoint, che si trovano nella sezione API privata di ["API di Grid Management"](#). Ad esempio, è possibile utilizzare l'API se si desidera utilizzare server syslog diversi per diversi gruppi di nodi.

Inserire le informazioni di syslog

Accedere alla procedura guidata Configura server syslog esterno e fornire le informazioni di cui StorageGRID ha bisogno per accedere al server syslog esterno.

Fasi

1. Dalla scheda Nodo locale e server esterno, seleziona **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 la fase **inserire le informazioni syslog** della procedura guidata, immettere un nome di dominio completo valido o un indirizzo IPv4 o IPv6 per il server syslog esterno nel campo **host**.
3. Inserire la porta di destinazione sul server syslog esterno (deve essere un numero intero compreso tra 1 e 65535). La porta predefinita è 514.
4. Selezionare il protocollo utilizzato per inviare le informazioni di audit al server syslog esterno.

Si consiglia di utilizzare **TLS** o **RELP/TLS**. Per utilizzare una di queste opzioni, è necessario caricare un certificato del server. L'utilizzo dei certificati consente di proteggere le connessioni tra la griglia e il server syslog esterno. Per ulteriori informazioni, vedere ["Gestire i certificati di sicurezza"](#).

Tutte le opzioni del protocollo richiedono il supporto e la configurazione del server syslog esterno. È necessario scegliere un'opzione compatibile con il server syslog esterno.



Il protocollo RELP (Reliable Event Logging Protocol) estende le funzionalità del protocollo syslog per fornire un'erogazione affidabile dei messaggi di evento. L'utilizzo di RELP può contribuire a prevenire la perdita di informazioni di controllo nel caso in cui il server syslog esterno debba essere riavviato.

5. Selezionare **continua**.
6. se si seleziona **TLS** o **RELP/TLS**, caricare i certificati CA del server, il certificato client e la chiave privata del client.
 - a. Selezionare **Sfoglia** per il certificato o la chiave che si desidera utilizzare.
 - b. Selezionare il certificato o il file della chiave.
 - c. Selezionare **Open** per caricare il file.

Accanto al nome del certificato o del file della chiave viene visualizzato un segno di spunta verde che indica che il caricamento è stato eseguito correttamente.

7. Selezionare **continua**.

Gestire il contenuto syslog

È possibile selezionare le informazioni da inviare al server syslog esterno.

Fasi

1. Per la fase **Gestisci contenuto syslog** della procedura guidata, selezionare ogni tipo di informazione di audit che si desidera inviare al server syslog esterno.
 - **Invia log di audit:** Invia eventi StorageGRID e attività di sistema
 - **Invia eventi di sicurezza:** Invia eventi di sicurezza, ad esempio quando un utente non autorizzato tenta di effettuare l'accesso o un utente accede come root
 - **Invia registri applicazione:** Consente di inviare messaggi ["File di log del software StorageGRID"](#) utili per la risoluzione dei problemi, tra cui:
 - `broadcast-err.log`
 - `broadcast.log`

- `jaeger.log`
- `nms.log` (Solo nodi amministrativi)
- `prometheus.log`
- `raft.log`
- `hagroups.log`

- **Invia log di accesso:** Invia log di accesso HTTP per le richieste esterne a Grid Manager, Tenant Manager, endpoint di bilanciamento del carico configurati e richieste di federazione griglia da sistemi remoti.

2. Utilizzare i menu a discesa per selezionare la gravità e la struttura (tipo di messaggio) per ciascuna categoria di informazioni di controllo che si desidera inviare.

L'impostazione dei valori di gravità e struttura consente di aggregare i registri in modo personalizzabile per semplificare l'analisi.

- a. Per **gravità**, selezionare **Passthrough** oppure selezionare un valore di gravità compreso tra 0 e 7.

Se selezioni un valore, StorageGRID applica il valore selezionato a tutti i messaggi di questo tipo. Perdi i dettagli sui diversi livelli di gravità se sovrascrivi la gravità con un valore fisso.

Severità	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di gravità di quando è stato registrato localmente sul nodo: • Per i registri di controllo, la gravità è "info". • Per gli eventi di sicurezza, i valori di gravità sono generati dalla distribuzione Linux sui nodi. • Per i registri delle applicazioni, i livelli di gravità variano tra "info" e "avviso", a seconda del problema. Ad esempio, aggiungendo un server NTP e configurando un gruppo ha si ottiene il valore "info", mentre arrestando intenzionalmente il servizio SSM o RSM si ottiene il valore "avviso". • Per i registri di accesso, la gravità è "info".
0	Emergenza: Il sistema non è utilizzabile
1	Attenzione: L'azione deve essere eseguita immediatamente
2	Critico: Condizioni critiche
3	Errore: Condizioni di errore
4	Avvertenza: Condizioni di avviso
5	Avviso: Condizione normale ma significativa

Severità	Descrizione
6	Informativo: Messaggi informativi
7	Debug: Messaggi a livello di debug

b. Per **Facility**, selezionare **Passthrough** o selezionare un valore di struttura compreso tra 0 e 23.

Se si seleziona un valore, questo verrà applicato a tutti i messaggi di questo tipo. Le informazioni sulle diverse strutture andranno perse se si sostituisce la struttura con un valore fisso.

Struttura	Descrizione
Passthrough	Ogni messaggio inviato al syslog esterno per avere lo stesso valore di struttura di quando è stato collegato localmente al nodo: • Per i registri di controllo, la struttura inviata al server syslog esterno è "local7". • Per gli eventi di sicurezza, i valori della struttura vengono generati dalla distribuzione linux sui nodi. • Per i registri delle applicazioni, i registri delle applicazioni inviati al server syslog esterno presentano i seguenti valori di struttura: ◦ <code>broadcast.log</code>: utente o daemon ◦ <code>broadcast-err.log</code>: utente, daemon, local3 o local4 ◦ <code>jaeger.log</code>: local2 ◦ <code>nms.log</code>: local3 ◦ <code>prometheus.log</code>: local4 ◦ <code>raft.log</code>: local5 ◦ <code>hagroups.log</code>: local6 • Per i registri di accesso, la struttura inviata al server syslog esterno è "local0".
0	kern (messaggi kernel)
1	utente (messaggi a livello utente)
2	mail
3	daemon (daemon di sistema)
4	auth (messaggi di sicurezza/autorizzazione)
5	syslog (messaggi generati internamente da syslogd)

Struttura	Descrizione
6	lpr (sottosistema di stampanti di linea)
7	news (sottosistema notizie di rete)
8	UUCP
9	cron (daemon di clock)
10	sicurezza (messaggi di sicurezza/autorizzazione)
11	FTP
12	NTP
13	logaudit (audit del log)
14	logalert (avviso di log)
15	clock (daemon di clock)
16	local0
17	local1
18	local2
19	local3
20	local4
21	local5
22	local6
23	local7

3. Selezionare **continua**.

Inviare messaggi di test

Prima di utilizzare un syslog server esterno, chiedi a tutti i nodi della tua grid di inviare messaggi di prova al syslog server esterno. Questi messaggi di prova ti aiutano a convalidare l'intera infrastruttura di raccolta dei log prima di iniziare a inviare dati al syslog server esterno.



Non utilizzare la configurazione del server syslog esterno fino a quando non si conferma che il server syslog esterno ha ricevuto un messaggio di test da ciascun nodo della griglia e che il messaggio è stato elaborato come previsto.

Fasi

1. Se non si desidera inviare messaggi di test perché si è certi che il server syslog esterno sia configurato correttamente e che sia in grado di ricevere informazioni di controllo da tutti i nodi della griglia, selezionare **Ignora e termina**.

Un banner verde indica che la configurazione è stata salvata.

2. In caso contrario, selezionare **Invia messaggi di prova** (scelta consigliata).

I risultati del test vengono visualizzati continuamente sulla pagina fino a quando non si interrompe il test. Mentre il test è in corso, i messaggi di controllo continuano a essere inviati alle destinazioni precedentemente configurate.

3. Se si verificano errori durante la configurazione del server syslog o in fase di esecuzione, correggerli e selezionare nuovamente **Invia messaggi di prova**.

Per informazioni sulla risoluzione di eventuali errori, consultare la sezione "[Risolvere i problemi di un server syslog esterno](#)".

4. Attendere che venga visualizzato un banner verde che indica che tutti i nodi hanno superato il test.
5. Controllare il server syslog per determinare se i messaggi di test vengono ricevuti ed elaborati come previsto.



Se si utilizza UDP, controllare l'intera infrastruttura di raccolta dei log. Il protocollo UDP non consente un rilevamento degli errori altrettanto rigoroso quanto gli altri protocolli.

6. Selezionare **Stop and Finish** (Interrompi e termina).

Viene nuovamente visualizzata la pagina **Audit and syslog server**. Un banner verde indica che la configurazione del server syslog è stata salvata.



Le informazioni di controllo StorageGRID non vengono inviate al server syslog esterno finché non si seleziona una destinazione che includa il server syslog esterno.

Seleziona la posizione del registro

È possibile specificare dove salvare i registri di controllo, i registri degli eventi di sicurezza, "[Registri delle applicazioni StorageGRID](#)" e vengono inviati i registri di accesso.

StorageGRID utilizza per impostazione predefinita le destinazioni di controllo dei nodi locali e memorizza le informazioni di controllo in `/var/local/log/localaudit.log`.



Quando si utilizza `/var/local/log/localaudit.log`, le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione. È possibile individuare il nodo con le voci più recenti utilizzando il `run-each-node --parallel "zgrep MGAU /var/local/log/localaudit.log | tail"` comando.

Alcune destinazioni sono disponibili solo se è stato configurato un server syslog esterno.

Fasi

1. Selezionare **Posizione registro > Nodo locale e server esterno**.
2. Per modificare la posizione del registro per i tipi di registro, selezionare un'opzione diversa.



Solo nodi locali e Server syslog esterno in genere offrono prestazioni migliori.

Opzione	Descrizione
Solo nodi locali (impostazione predefinita)	I messaggi di controllo, i registri degli eventi di 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. Per archiviare i registri per un periodo di tempo prolungato, utilizzare un tenant e un bucket per l'archiviazione dei registri.
Nodi amministrativi/nodi locali	I messaggi di controllo vengono inviati al registro di controllo sui nodi Admin, mentre i registri degli eventi di protezione e i registri delle applicazioni vengono memorizzati sui nodi che li hanno generati. Le informazioni di controllo sono memorizzate nei seguenti file: • Nodi amministrativi (primari e non primari): <code>/var/local/audit/export/audit.log</code> • Tutti i nodi: Il <code>/var/local/log/localaudit.log</code> file è in genere vuoto o mancante. Potrebbe contenere informazioni secondarie, ad esempio una copia aggiuntiva di alcuni messaggi.
Server syslog esterno	Le informazioni di 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
Nodi amministrativi 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 .

3. Selezionare **Salva**.

Viene visualizzato un messaggio di avviso.

4. Selezionare **OK** per confermare che si desidera modificare la destinazione per le informazioni di controllo.

I nuovi registri vengono inviati alle destinazioni selezionate. I registri esistenti rimangono nella posizione corrente.

Usa un secchio

I registri vengono ruotati periodicamente. Utilizzare un bucket S3 nella stessa griglia per archiviare i log per un periodo di tempo prolungato.

1. Seleziona **Posizione registro > Utilizza un bucket**.
2. Selezionare la casella di controllo **Abilita registri archivio**.
3. Se il tenant e il bucket elencati non sono quelli che desideri utilizzare, seleziona **Cambia tenant e bucket**, quindi seleziona **Crea tenant e bucket** oppure **Seleziona tenant e bucket**.

Crea tenant e bucket

- a. Inserisci un nuovo nome per l'inquilino.
- b. Inserisci e conferma una password per il nuovo tenant.
- c. Inserisci un nuovo nome per il bucket.
- d. Seleziona **Crea e abilita**.

Selezionare tenant e bucket

- a. Selezionare un nome di tenant dal menu a discesa.
- b. Selezionare un bucket dal menu a discesa.
- c. Selezionare **Seleziona e abilita**.

4. Selezionare **Salva**.

I log verranno archiviati nel tenant e nel bucket specificati. Il nome della chiave dell'oggetto per i registri è nel seguente formato:

```
system-logs/{node_hostname}/{absolute_path_to_log_file_on_node}--  
{last_modified_time}.gz
```

Ad esempio:

```
system-logs/DC1-SN1/var/local/log/localaudit.log--2025-05-12_13:41:44.gz
```

Gestisci la conservazione dei log

Puoi gestire per quanto tempo StorageGRID conserva i log creando una regola ILM o configurando una policy di ciclo di vita del bucket S3.

Regola ILM

Crea una regola ILM per il bucket e aggiungi questa regola alla policy ILM attiva.

Fasi

1. Selezionare **ILM > regole**.
2. Seleziona **Crea**. "**Fase 1 (inserire i dettagli)**" Viene visualizzata la finestra della procedura guidata "Crea una regola ILM":
 - a. Inserisci un nome univoco per la regola. Ad esempio: Regola ILM per i log archiviati.
 - b. Seleziona l'account tenant S3 per l'archiviazione dei log.
 - c. Specifica il bucket S3 per l'archiviazione dei log.
3. Continua su "**Fase 2 (definizione delle posizioni)**" e definisci il posizionamento per la regola dei log archiviati. Ad esempio, la regola ILM memorizza una copia replicata nel Sito 1 e una copia replicata nel Sito 2 per il primo anno. Dopo un anno, viene creata una copia con codifica di cancellazione 2+1 e salvata in un solo sito.
4. Dopo aver creato la regola, aggiungila a una policy ILM attiva.

ciclo di vita del bucket S3

Configura una policy del ciclo di vita su un bucket S3 per l'archiviazione dei log:

```
{
  "Rules": [
    {
      "ID": "Retain logs forever",
      "Filter": {},
      "Status": "Enabled",
      "Expiration": {}
    }
  ]
}
```

Quando configuri una policy di ciclo di vita S3 sul bucket S3 di archiviazione dei log, le azioni di scadenza del ciclo di vita sovrascrivono la policy ILM per gli oggetti che corrispondono al filtro di ciclo di vita del bucket. Gli oggetti che non corrispondono al filtro di ciclo di vita del bucket utilizzano le impostazioni di conservazione della policy ILM. Se un oggetto corrisponde a un filtro di ciclo di vita del bucket e non vengono specificate esplicitamente azioni di scadenza, le impostazioni di conservazione della policy ILM non vengono utilizzate e si intende che le versioni degli oggetti vengano conservate per sempre.

Configura il server di posta elettronica

Come amministratore di StorageGRID, devi configurare un server di posta elettronica per inviare notifiche dai sistemi di allerta e monitoraggio di StorageGRID che informano te, gli altri amministratori e il supporto tecnico sugli eventi e i problemi di sistema.

Le funzionalità di StorageGRID che utilizzano il server di posta elettronica per le notifiche includono avvisi, AutoSupport e la verifica multi-amministratore (MAV). Puoi usare lo stesso server di posta elettronica per tutte

le notifiche.

Prima di iniziare

- Si dispone di "[Autorizzazione di accesso root](#)".
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".

Fasi

1. Seleziona **Configuration > Monitoring > Email server**.

Viene visualizzata la pagina del server di posta elettronica.

2. Seleziona il menu a tendina, **Visualizza le funzionalità che potrebbero richiedere un server di posta elettronica**. Se vuoi vedere i dettagli e le informazioni necessarie per configurare le notifiche email per una funzionalità, seleziona **Visualizza**.

Verrai reindirizzato alla pagina di configurazione della funzionalità in Grid Manager. La pagina di configurazione di ciascuna funzionalità contiene una notifica che indica che hai bisogno di un server email per inviare notifiche email.

3. Per configurare un server di posta elettronica dalla pagina Server di posta elettronica:
 - a. Inserisci l'indirizzo IP o il FQDN del server email.
 - b. Seleziona il numero di porta utilizzato dal server di posta elettronica. Il valore predefinito è 25.
 - c. Per richiedere l'autenticazione, seleziona **Usa autenticazione** e inserisci nome utente e password.
 - d. Per richiedere la verifica dell'identità del server SMTP, seleziona **Usa Transport Layer Security (TLS)**. Poi:
 - i. Fornisci un pacchetto CA.
 - ii. Se il server di posta SMTP richiede ai mittenti di fornire certificati client per l'autenticazione, seleziona **Invia certificato client**. Poi fornisci il certificato client e la chiave privata.
 - e. Per verificare che le impostazioni della tua email siano corrette, invia un'email di prova inserendo mittente e destinatario. Seleziona **Invia**.

Viene visualizzato un messaggio di conferma che indica l'invio di un'e-mail di prova.

- f. Selezionare le caselle di posta in arrivo di tutti i destinatari e confermare che è stata ricevuta un'e-mail di prova.



Se l'e-mail non viene ricevuta entro pochi minuti o se viene attivato l'avviso **errore notifica e-mail**, controllare le impostazioni e riprovare.

- g. Accedi a qualsiasi altro nodo Admin e invia un'e-mail di prova per verificare la connettività da tutti i siti.



Quando si verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività. Ciò è in contrasto con il test dei pacchetti AutoSupport, in cui tutti i nodi amministrativi inviano l'e-mail di prova.

4. Selezionare **Salva**.

L'invio di un'email di prova non salva le impostazioni. Devi selezionare **Salva**.

Le impostazioni e-mail vengono salvate.

5. Vai alle pagine di configurazione delle funzionalità che utilizzano il server di posta elettronica e completa le impostazioni di notifica email.
- ["Avvisi"](#). Per gli avvisi, puoi anche ["configurare le notifiche SNMP"](#).
 - ["AutoSupport"](#). Puoi inviare i pacchetti AutoSupport tramite email, HTTPS o HTTP (HTTP non è consigliato).
 - ["Verifica multi-amministratore \(MAV\)"](#).

Utilizzare il monitoraggio SNMP

Utilizza il monitoraggio SNMP in StorageGRID

Se si desidera monitorare StorageGRID utilizzando il protocollo SNMP (Simple Network Management Protocol), è necessario configurare l'agente SNMP incluso in StorageGRID.

- ["Configurare l'agente SNMP"](#)
- ["Aggiornare l'agente SNMP"](#)

Funzionalità

Ogni nodo StorageGRID esegue un agente SNMP, o daemon, che fornisce un MIB. StorageGRID MIB contiene definizioni di tabella e di notifica per gli avvisi. Il MIB contiene anche informazioni sulla descrizione del sistema, come il numero di piattaforma e il numero di modello per ciascun nodo. Ogni nodo StorageGRID supporta anche un sottoinsieme di oggetti MIB-II.



Vedere ["Accedere ai file MIB"](#) se si desidera scaricare i file MIB sui nodi griglia.

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

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

Trappole

I trap sono notifiche inviate dall'agente SNMP che non richiedono un riconoscimento da parte del sistema di gestione. Le trap servono a notificare al sistema di gestione che si è verificato qualcosa all'interno di StorageGRID, ad esempio un avviso attivato.

I trap sono supportati in tutte e tre le versioni di SNMP.

Informa

Le informazioni sono simili alle trap, ma richiedono un riconoscimento da parte del sistema di gestione. Se l'agente SNMP non riceve una conferma entro un determinato periodo di tempo, invia nuovamente l'informazione fino a quando non viene ricevuta una conferma o non viene raggiunto il valore massimo di tentativi.

Le informazioni sono supportate in SNMPv2c e SNMPv3.

Le notifiche trap e inform vengono inviate nei seguenti casi:

- Viene attivato un avviso predefinito o personalizzato a qualsiasi livello di severità. Per eliminare le notifiche SNMP per un avviso, è necessario ["configurare un silenzio"](#) per tale avviso. Le notifiche di avviso vengono

inviare da ["Nodo Admin mittente preferito"](#).

Ogni avviso viene associato a uno dei tre tipi di trap in base al livello di gravità dell'avviso: ActiveMinorAlert, activeMajorAlert e activeCriticalAlert. Per un elenco degli avvisi che possono attivare questi trap, vedere la ["Riferimenti agli avvisi"](#).

Supporto della versione SNMP

La tabella fornisce un riepilogo generale dei contenuti supportati per ciascuna versione SNMP.

	SNMPv1	SNMPv2c	SNMPv3
Query (GET e GETNEXT)	Query MIB di sola lettura	Query MIB di sola lettura	Query MIB di sola lettura
Autenticazione e delle query	Stringa di comunità	Stringa di comunità	Utente del modello di sicurezza basato sull'utente (USM)
Notifiche (INTRAPPOLARE e INFORMARE)	Solo trap	Trap e informa	Trap e informa
Autenticazione e delle notifiche	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Community trap predefinita o stringa di comunità personalizzata per ciascuna destinazione trap	Utente USM per ciascuna destinazione trap

Limitazioni

- StorageGRID supporta l'accesso MIB di sola lettura. L'accesso in lettura/scrittura non è supportato.
- Tutti i nodi della griglia ricevono la stessa configurazione.
- SNMPv3: StorageGRID non supporta la modalità di supporto per il trasporto (TSM).
- SNMPv3: L'unico protocollo di autenticazione supportato è SHA (HMAC-SHA-96).
- SNMPv3: L'unico protocollo per la privacy supportato è AES.

Configura l'agente SNMP in StorageGRID

È possibile configurare l'agente SNMP StorageGRID in modo che utilizzi un sistema di gestione SNMP di terze parti per l'accesso MIB di sola lettura e le notifiche.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

L'agente SNMP di StorageGRID supporta SNMPv1, SNMPv2c e SNMPv3. È possibile configurare l'agente per una o più versioni. Per SNMPv3, è supportata solo l'autenticazione del modello di sicurezza utente (USM).

Tutti i nodi nella griglia utilizzano la stessa configurazione SNMP.

Specificare la configurazione di base

Come prima fase, attivare l'agente SNMP StorageGRID e fornire informazioni di base.

Fasi

1. Selezionare **Configurazione > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina SNMP Agent.

2. Per attivare l'agente SNMP su tutti i nodi della griglia, selezionare la casella di controllo **Enable SNMP** (attiva SNMP).
3. Inserire le seguenti informazioni nella sezione Configurazione di base.

Campo	Descrizione
Contatto per il sistema	Opzionale. Il contatto principale per il sistema StorageGRID, che viene restituito nei messaggi SNMP come sysContact. In genere, il contatto di sistema è un indirizzo e-mail. Questo valore si applica a tutti i nodi nel sistema StorageGRID. Il contatto di sistema può contenere al massimo 255 caratteri.
Ubicazione del sistema	Opzionale. La posizione del sistema StorageGRID, che viene restituita nei messaggi SNMP come sysLocation. La posizione del sistema può essere una qualsiasi informazione utile per identificare la posizione del sistema StorageGRID. Ad esempio, è possibile utilizzare l'indirizzo di una struttura. Questo valore si applica a tutti i nodi nel sistema StorageGRID. La posizione del sistema può contenere al massimo 255 caratteri.
Attivare le notifiche dell'agente SNMP	• Se selezionata, l'agente SNMP StorageGRID invia notifiche trap e inform. • Se questa opzione non è selezionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia alcuna notifica SNMP.
Abilita trap di autenticazione	Se selezionata, l'agente SNMP StorageGRID invia trap di autenticazione se riceve messaggi di protocollo autenticati in modo errato.

Immettere le stringhe di comunità

Se si utilizza SNMPv1 o SNMPv2c, completare la sezione Community Strings (stringhe comunità).

Quando il sistema di gestione interroga il MIB StorageGRID, invia una stringa di comunità. Se la stringa di comunità corrisponde a uno dei valori specificati, l'agente SNMP invia una risposta al sistema di gestione.

Fasi

1. Per **comunità di sola lettura**, è possibile immettere una stringa di comunità per consentire l'accesso MIB di sola lettura agli indirizzi di agenti IPv4 e IPv6.



Per garantire la sicurezza del sistema StorageGRID, non utilizzare "public" come stringa di comunità. Se questo campo viene lasciato vuoto, l'agente SNMP utilizza l'ID griglia del sistema StorageGRID come stringa di comunità.

Ogni stringa di community può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

2. Selezionare **Aggiungi un'altra stringa di comunità** per aggiungere altre stringhe.

Sono consentite fino a cinque stringhe.

creare destinazioni trap

Utilizzare la scheda destinazioni trap nella sezione altre configurazioni per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Fasi

1. Per il campo **Comunità trap predefinita**, è possibile immettere la stringa di comunità predefinita che si desidera utilizzare per le destinazioni trap SNMPv1 o SNMPv2.

Se necessario, è possibile fornire una stringa di comunità diversa ("personalizzata") quando si definisce una destinazione trap specifica.

La comunità trap predefinita può contenere al massimo 32 caratteri e non può contenere spazi vuoti.

2. Per aggiungere una destinazione trap, selezionare **Crea**.
3. Selezionare la versione SNMP che verrà utilizzata per la destinazione trap.
4. Completare il modulo Crea destinazione trap per la versione selezionata.

SNMPv1

Se si seleziona SNMPv1 come versione, completare questi campi.

Campo	Descrizione
Tipo	Deve essere trap per SNMPv1.
Host	Un indirizzo IPv4 o IPv6 o un nome di dominio completo (FQDN) per ricevere il trap.
Porta	Utilizzare 162, quale porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv2c

Se si seleziona SNMPv2c come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Stringa di comunità	Utilizzare la comunità trap predefinita, se specificata, oppure immettere una stringa di comunità personalizzata per questa destinazione trap. La stringa di community personalizzata può contenere un massimo di 32 caratteri e non può contenere spazi vuoti.

SNMPv3

Se si seleziona SNMPv3 come versione, completare questi campi.

Campo	Descrizione
Tipo	Se la destinazione verrà utilizzata per trap o informa.
Host	Un indirizzo IPv4 o IPv6 o FQDN per ricevere il trap.
Porta	Utilizzare 162, che è la porta standard per i trap SNMP a meno che non sia necessario utilizzare un altro valore.
Protocollo	Utilizzare UDP, che è il protocollo trap SNMP standard a meno che non sia necessario utilizzare TCP.
Utente USM	L'utente USM che verrà utilizzato per l'autenticazione. • Se si seleziona Trap, vengono visualizzati solo gli utenti USM senza ID motore autorevoli. • Se si seleziona inform, vengono visualizzati solo gli utenti USM con ID motore autorevoli. • Se non viene visualizzato alcun utente: i. Creare e salvare la destinazione trap. ii. Accedere a Creare utenti USM e creare l'utente. iii. Tornare alla scheda Destinazioni trap, selezionare la destinazione salvata dalla tabella e selezionare Modifica. iv. Selezionare l'utente.

5. Selezionare **Crea**.

La destinazione trap viene creata e aggiunta alla tabella.

Creare gli indirizzi degli agenti

Facoltativamente, utilizzare la scheda indirizzi agente nella sezione altre configurazioni per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

Se non si configura un indirizzo dell'agente, l'indirizzo di ascolto predefinito è la porta UDP 161 su tutte le reti StorageGRID.

Fasi

1. Selezionare **Crea**.
2. Inserire le seguenti informazioni.

Campo	Descrizione
Protocollo Internet	Se questo indirizzo utilizzerà IPv4 o IPv6. Per impostazione predefinita, SNMP utilizza IPv4.

Campo	Descrizione
Protocollo di trasporto	Se questo indirizzo utilizza UDP o TCP. Per impostazione predefinita, SNMP utilizza UDP.
Rete StorageGRID	La rete StorageGRID su cui l'agente ascolta. • Grid, Admin e Client Networks (reti Grid, Admin e Client): L'agente SNMP è in attesa di query su tutte e tre le reti. • Grid Network • Admin Network (rete amministrativa) • Rete client Nota: Se si utilizza la rete client per i dati non protetti e si crea un indirizzo agente per la rete client, tenere presente che anche il traffico SNMP non sarà sicuro.
Porta	Facoltativamente, il numero di porta su cui l'agente SNMP deve essere in attesa. La porta UDP predefinita per un agente SNMP è 161, ma è possibile immettere qualsiasi numero di porta inutilizzato. Nota: Quando si salva l'agente SNMP, StorageGRID apre automaticamente le porte degli indirizzi dell'agente sul firewall interno. È necessario assicurarsi che tutti i firewall esterni consentano l'accesso a queste porte.

3. Selezionare **Crea**.

L'indirizzo dell'agente viene creato e aggiunto alla tabella.

creare utenti USM

Se si utilizza SNMPv3, utilizzare la scheda utenti USM nella sezione altre configurazioni per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.



Per le destinazioni SNMPv3 *trap*, si consiglia di creare un utente USM per ciascun nodo di amministrazione. Se ogni nodo amministrativo non ha un utente USM, il sistema di gestione potrebbe smettere di ricevere notifiche se il nodo amministrativo primario non funziona.



SNMPv3 *inform* le destinazioni devono avere utenti con ID motore. SNMPv3 la destinazione *trap* non può avere utenti con ID motore.

Questi passaggi non si applicano solo se si utilizza SNMPv1 o SNMPv2c.

Fasi

1. Selezionare **Crea**.

2. Inserire le seguenti informazioni.

Campo	Descrizione
Nome utente	Un nome univoco per questo utente USM. I nomi utente possono avere un massimo di 32 caratteri e non possono contenere spazi vuoti. Il nome utente non può essere modificato dopo la creazione dell'utente.
Accesso MIB di sola lettura	Se selezionata, l'opzione consente all'utente di accedere in sola lettura al MIB.
ID motore autorevole	Se l'utente verrà utilizzato in una destinazione inform, l>ID motore autorevole per questo utente. Inserire da 10 a 64 caratteri esadecimali (da 5 a 32 byte) senza spazi. Questo valore è necessario per gli utenti USM che verranno selezionati nelle destinazioni trap per gli informa. Questo valore non è consentito per gli utenti USM che verranno selezionati nelle destinazioni trap per trap. Nota: Questo campo non viene visualizzato se si seleziona accesso MIB di sola lettura perché gli utenti USM che hanno accesso MIB di sola lettura non possono avere ID motore.
Livello di sicurezza	Il livello di sicurezza per l'utente USM: • Authprim: Questo utente comunica con autenticazione e privacy (crittografia). È necessario specificare un protocollo di autenticazione e una password, nonché un protocollo e una password per la privacy. • AuthNoPriv: Questo utente comunica con autenticazione e senza privacy (senza crittografia). Specificare un protocollo di autenticazione e una password.
Protocollo di autenticazione	Impostare sempre su SHA, che è l'unico protocollo supportato (HMAC-SHA-96).
Password	La password che l'utente utilizzerà per l'autenticazione.
Protocollo di privacy	Visualizzato solo se si seleziona authviv e si imposta sempre su AES, che è l'unico protocollo di privacy supportato.
Password	Visualizzato solo se è stato selezionato authviv. La password che l'utente utilizzerà per la privacy.

3. Selezionare **Crea**.

L'utente USM viene creato e aggiunto alla tabella.

4. Una volta completata la configurazione dell'agente SNMP, selezionare **Salva**.

La nuova configurazione dell'agente SNMP diventa attiva.

Informazioni correlate

["Porte utilizzate per le comunicazioni esterne"](#)

Aggiorna l'agente SNMP di StorageGRID

È possibile disattivare le notifiche SNMP, aggiornare le stringhe di comunità o aggiungere o rimuovere indirizzi di agenti, utenti USM e destinazioni trap.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

Per informazioni dettagliate su ciascun campo nella pagina dell'agente SNMP, vedere ["Configurare l'agente SNMP"](#). È necessario selezionare **Salva** nella parte inferiore della pagina per confermare le modifiche apportate in ciascuna scheda.

Fasi

1. Selezionare **Configurazione > Monitoraggio > Agente SNMP**.

Viene visualizzata la pagina SNMP Agent.

2. Per disattivare l'agente SNMP su tutti i nodi della griglia, deselegionare la casella di controllo **attiva SNMP** e selezionare **Salva**.

Se si riattiva l'agente SNMP, tutte le impostazioni di configurazione SNMP precedenti vengono mantenute.

3. Se si desidera, aggiornare le informazioni nella sezione Configurazione di base:

- a. Se necessario, aggiornare **System contact** e **System location**.
- b. In alternativa, selezionare o deselegionare la casella di controllo **attiva notifiche agente SNMP** per controllare se l'agente SNMP StorageGRID invia notifiche trap e inform.

Quando questa casella di controllo è deselegionata, l'agente SNMP supporta l'accesso MIB di sola lettura, ma non invia notifiche SNMP.

- c. Facoltativamente, selezionare o deselegionare la casella di controllo **Abilita trap di autenticazione** per controllare se l'agente SNMP di StorageGRID invia trap di autenticazione quando riceve messaggi di protocollo autenticati in modo errato.
4. Se si utilizza SNMPv1 o SNMPv2c, è possibile aggiornare o aggiungere una comunità **di sola lettura** nella sezione Community Strings (stringhe comunità).
 5. Per aggiornare le destinazioni trap, selezionare la scheda destinazioni trap nella sezione altre configurazioni.

Utilizzare questa scheda per definire una o più destinazioni per le notifiche trap StorageGRID o inform. Quando si attiva l'agente SNMP e si seleziona **Salva**, StorageGRID invia notifiche a ciascuna destinazione definita quando vengono attivati gli avvisi. Vengono inoltre inviate notifiche standard per le entità MIB-II supportate (ad esempio ifdown e coldstart).

Per informazioni dettagliate su cosa immettere, vedere ["Creare destinazioni trap"](#).

- Facoltativamente, aggiornare o rimuovere la comunità trap predefinita.

Se si rimuove la comunità trap predefinita, è necessario innanzitutto verificare che tutte le destinazioni trap esistenti utilizzino una stringa di comunità personalizzata.

- Per aggiungere una destinazione trap, selezionare **Crea**.
- Per modificare una destinazione trap, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere una destinazione trap, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

6. Per aggiornare gli indirizzi degli agenti, selezionare la scheda indirizzi agente nella sezione altre configurazioni.

Utilizzare questa scheda per specificare uno o più "indirizzi in ascolto". Si tratta degli indirizzi StorageGRID su cui l'agente SNMP può ricevere query.

Per informazioni dettagliate su cosa immettere, vedere ["Creare gli indirizzi degli agenti"](#).

- Per aggiungere un indirizzo agente, selezionare **Crea**.
- Per modificare l'indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Modifica**.
- Per rimuovere un indirizzo di un agente, selezionare il pulsante di opzione e selezionare **Rimuovi**.
- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

7. Per aggiornare gli utenti USM, selezionare la scheda utenti USM nella sezione altre configurazioni.

Utilizzare questa scheda per definire gli utenti USM autorizzati a interrogare il MIB o a ricevere trap e informazioni.

Per informazioni dettagliate su cosa immettere, vedere ["Creare utenti USM"](#).

- Per aggiungere un utente USM, selezionare **Crea**.
- Per modificare un utente USM, selezionare il pulsante di opzione e selezionare **Modifica**.

Il nome utente di un utente USM esistente non può essere modificato. Se è necessario modificare un nome utente, rimuovere l'utente e crearne uno nuovo.



Se si aggiunge o si rimuove l'ID motore autorevole di un utente e tale utente è attualmente selezionato per una destinazione, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

- Per rimuovere un utente USM, selezionare il pulsante di opzione e selezionare **Rimuovi**.



Se l'utente rimosso è attualmente selezionato per una destinazione trap, è necessario modificare o rimuovere la destinazione. In caso contrario, si verifica un errore di convalida quando si salva la configurazione dell'agente SNMP.

- Per confermare le modifiche, seleziona **Salva** nella parte inferiore della pagina.

8. Una volta aggiornata la configurazione dell'agente SNMP, selezionare **Salva**.

Accedere ai file MIB di StorageGRID

I file MIB contengono definizioni e informazioni sulle proprietà delle risorse e dei servizi gestiti per i nodi della griglia. È possibile accedere ai file MIB che definiscono gli oggetti e le notifiche per StorageGRID. Questi file possono essere utili per il monitoraggio della griglia.

Per ulteriori informazioni sui file SNMP e MIB, vedere ["Utilizzare il monitoraggio SNMP"](#).

Accedere ai file MIB

Per accedere ai file MIB, procedere come segue.

Fasi

1. Selezionare **Configurazione > Monitoraggio > Agente SNMP**.
2. Nella pagina dell'agente SNMP, selezionare il file che si desidera scaricare:
 - **NETAPP-STORAGEGRID-MIB.txt**: Definisce la tabella degli avvisi e le notifiche (trap) accessibili su tutti i nodi di amministrazione.
 - **ES-NETAPP-06-MIB.mib**: Definisce gli oggetti e le notifiche per le appliance basate su e-Series.
 - **MIB_1_10.zip**: Definisce gli oggetti e le notifiche per le appliance con un'interfaccia BMC.



È inoltre possibile accedere ai file MIB nella seguente posizione su qualsiasi nodo StorageGRID: `/usr/share/snmp/mibs`

3. Per estrarre gli OID StorageGRID dal file MIB:
 - a. Ottenere l'OID della directory principale del MIB StorageGRID:

```
root@user-adm1:~ # snmptranslate -On -IR storagegrid
```

Risultato: `.1.3.6.1.4.1.789.28669` (28669 È sempre l'OID per StorageGRID)

- b. Grep per l'OID StorageGRID nell'intero albero (usando `paste` per unire le linee):

```
root@user-adm1:~ # snmptranslate -Tso | paste -d " " - - | grep 28669
```



Il `snmptranslate` comando ha molte opzioni che sono utili per esplorare il MIB. Questo comando è disponibile su qualsiasi nodo StorageGRID.

Contenuto del file MIB

Tutti gli oggetti si trovano sotto l'OID StorageGRID.

Nome dell'oggetto	ID oggetto (OID)	Descrizione
		Il modulo MIB per le entità NetApp StorageGRID.

Oggetti MIB

Nome dell'oggetto	ID oggetto (OID)	Tipo	Accesso	modulo MIB	Descrizione
ActiveAlertCount		Integer32	Sola lettura	NETAPP-STORAGEGRID-MIB	Il numero di avvisi attivi in activeAlertTable.
ActiveAlertTable		Sequenza di ActiveAlertEntry	Non accessibile	NETAPP-STORAGEGRID-MIB	Tabella degli avvisi attivi in StorageGRID.
activeAlertEntry		Sequenza	Non accessibile	NETAPP-STORAGEGRID-MIB	Un singolo avviso StorageGRID , indicizzato in base all'ID avviso.
ActiveAlertId		Stringa di ottetti	Sola lettura	NETAPP-STORAGEGRID-MIB	L'ID dell'avviso. Unico solo nel set corrente di avvisi attivi.
ActiveAlertName		Stringa di ottetti	Sola lettura	NETAPP-STORAGEGRID-MIB	Il nome dell'avviso.
ActiveAlertInstance		Stringa di ottetti	Sola lettura	NETAPP-STORAGEGRID-MIB	Il nome dell'entità che ha generato l'avviso, in genere il nome del nodo.
ActiveAlertSeverity		Stringa di ottetti	Sola lettura	NETAPP-STORAGEGRID-MIB	La severità dell'avviso.
ActiveAlertStartTime		Data e ora	Sola lettura	NETAPP-STORAGEGRID-MIB	Ora in cui è stato attivato l'avviso.

Raccogliere dati StorageGRID aggiuntivi

Monitorare le prestazioni PUT e GET in StorageGRID

È possibile monitorare le performance di alcune operazioni, come ad esempio l'archiviazione e il recupero di oggetti, per identificare le modifiche che potrebbero richiedere ulteriori analisi.

A proposito di questa attività

Per monitorare le prestazioni, è possibile eseguire comandi S3 direttamente da una workstation o utilizzando l'applicazione S3tester open-source. L'utilizzo di questi metodi consente di valutare le performance indipendentemente da fattori esterni a StorageGRID, come problemi con un'applicazione client o problemi con una rete esterna.

Quando si eseguono i test delle operazioni PUT e GET, attenersi alle seguenti linee guida:

- Utilizzare dimensioni degli oggetti paragonabili agli oggetti che di solito si acquisiscono nella griglia.
- Eseguire operazioni su siti locali e remoti.

I messaggi in **"log di audit"** 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 audit SGET. È anche possibile trovare l'attributo TIME nei messaggi di controllo per le seguenti operazioni S3: DELETE, GET, HEAD, Metadata Updated, POST, PUT

Durante l'analisi dei risultati, esaminare il tempo medio richiesto per soddisfare una richiesta e il throughput complessivo che è possibile ottenere. Ripetere regolarmente gli stessi test e registrare i risultati, in modo da poter identificare i trend che potrebbero richiedere un'indagine.

- È possibile ["Scarica S3tester da github"](#).

Monitorare le operazioni di verifica degli oggetti in StorageGRID

Il sistema StorageGRID è in grado di verificare l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti danneggiati e mancanti.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).

A proposito di questa attività

Due ["processi di verifica"](#) lavorano insieme per garantire l'integrità dei dati:

- **La verifica in background** viene eseguita automaticamente, controllando continuamente la correttezza dei dati dell'oggetto.

La verifica in background verifica automaticamente e continuamente tutti i nodi di storage per determinare se sono presenti copie corrotte dei dati degli oggetti replicati e codificati in cancellazione. In caso di problemi, il sistema StorageGRID tenta automaticamente di sostituire i dati dell'oggetto corrotto da copie memorizzate in un'altra parte del sistema. La verifica in background non viene eseguita sugli oggetti in un Cloud Storage Pool.



L'avviso **rilevato oggetto corrotto non identificato** viene attivato se il sistema rileva un oggetto corrotto che non può essere corretto automaticamente.

- **Il controllo dell'esistenza di oggetti** può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) dei dati dell'oggetto.

Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti consente di verificare l'integrità dei dispositivi di storage, in particolare se un recente problema hardware potrebbe aver influenzato l'integrità dei dati.

È necessario esaminare regolarmente i risultati delle verifiche in background e dei controlli sull'esistenza degli oggetti. Esaminare immediatamente eventuali istanze di dati degli oggetti corrotti o mancanti per determinare la causa principale.

Fasi

1. Esaminare i risultati delle verifiche in background:

a. Selezionare **Nodi > Nodo di archiviazione_ > Oggetti**.

b. Verificare i risultati della verifica:

- Per controllare la verifica dei dati degli oggetti replicati, esaminare 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 controllare la verifica dei frammenti con codifica di cancellazione, selezionare **Storage Node > ILM** e controllare gli attributi nella sezione Erasure coding verification.

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 di aiuto.

2. Esaminare i risultati dei job di controllo dell'esistenza di oggetti:

- Selezionare **Manutenzione > Controllo esistenza oggetto > Cronologia lavori**.
- Esaminare la colonna Copie di oggetti mancanti rilevate. Se un processo ha causato la perdita di 100 o più copie di oggetti ed è stato attivato l'avviso **Oggetti potenzialmente 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

☐	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 <u>7 more</u>	0

Esaminare i messaggi di audit di StorageGRID

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

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

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

Ogni nodo amministrativo memorizza i messaggi di audit in file di testo. La condivisione dell'audit contiene il file attivo (audit.log) e i registri di audit compressi dei giorni precedenti. Ogni nodo della griglia memorizza anche una copia delle informazioni di audit generate sul nodo.

È possibile accedere ai file di log di controllo direttamente dalla riga di comando del nodo amministrativo.

StorageGRID può inviare informazioni di audit per impostazione predefinita, oppure è possibile modificare la destinazione:

- Il valore predefinito di StorageGRID per le destinazioni di audit dei nodi locali.
- Le voci del registro di controllo di Grid Manager e Tenant Manager potrebbero essere inviate a un nodo di archiviazione.
- In alternativa, è possibile modificare la destinazione dei registri di controllo e inviare le informazioni di controllo a un server syslog esterno. I registri locali dei record di controllo continuano a essere generati e memorizzati quando viene configurato un server syslog esterno.
- ["Scopri come configurare la gestione dei log"](#).

Per informazioni dettagliate sul file di log di audit, sul formato dei messaggi di audit, sui tipi di messaggi di audit e sugli strumenti disponibili per analizzare i messaggi di audit, vedere ["Esaminare i registri di audit"](#).

Raccogli i file di registro StorageGRID e i dati di sistema

È possibile recuperare i file di registro e i dati di sistema StorageGRID, inclusi i dati di configurazione, e inviarli al supporto tecnico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su qualsiasi nodo di amministrazione utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

Utilizzare Grid Manager per raccogliere ["file di log"](#), dati di sistema e dati di configurazione da qualsiasi nodo della griglia per il periodo di tempo selezionato. I dati vengono raccolti e archiviati in un .tar.gz file che potrai poi scaricare sul tuo computer locale o inviare al supporto tecnico.

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 la gestione dei log e il server syslog esterno"](#).

Se il nodo di amministrazione utilizzato per avviare la raccolta dei log va offline durante la raccolta, StorageGRID non conserva i risultati. Devi riavviare il nodo e riavviare la raccolta dei log al termine del riavvio.

Fasi

1. Selezionare **Supporto > Strumenti > Raccolta registri**. Viene visualizzata una tabella di nodi.
2. Selezionare i nodi della griglia per i quali si desidera raccogliere i file di log.

È possibile ordinare in base al nome del nodo, al sito e al tipo di nodo. Le colonne Tipo di sito e Tipo di nodo contengono filtri per la selezione in base a singoli siti e tipi di nodo.

3. Selezionare **continua**.

4. Selezionare l'intervallo di data e ora 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 memorizzato su un nodo o troppo grande per essere raccolto da un nodo di amministrazione per il download. Se si verifica uno dei due scenari, riavviare la raccolta dei registri con un set di dati più piccolo.

5. Selezionare i tipi di log che si desidera raccogliere.

- **Registri delle applicazioni:** registri specifici delle applicazioni che il supporto tecnico utilizza più frequentemente per la risoluzione dei problemi. I log raccolti sono un sottoinsieme dei log 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.

6. Facoltativamente, utilizzare la casella di testo **Note** per immettere note sui file di registro che si stanno raccogliendo.

È possibile utilizzare queste note per fornire informazioni di supporto tecnico sul problema che ha richiesto di raccogliere i file di log. Le note vengono aggiunte a un file denominato `info.txt`, insieme ad altre informazioni sulla raccolta di file di registro. Il `info.txt` file viene salvato nel pacchetto di archiviazione del file di registro.

7. Seleziona **Raccogli registri**.

È possibile utilizzare la pagina Raccolta log per monitorare l'avanzamento della raccolta dei file di log per ciascun nodo della griglia.

Se viene visualizzato un messaggio di errore relativo alle dimensioni del registro, provare a raccogliere i registri per un periodo di tempo più breve o per un numero inferiore di nodi.

8. Se la raccolta dei log fallisce:

- Se viene visualizzato il messaggio "Raccolta log non riuscita", è possibile riprovare la raccolta log o terminare la sessione senza riprovare.
- Se viene visualizzato il messaggio "Raccolta log parzialmente fallita", è possibile riprovare la raccolta log, terminare la sessione, scaricare il file di log parziale o inviarlo ad AutoSupport.



Puoi lasciare vuoto il campo della passphrase di provisioning per un tentativo standard oppure inserire la passphrase per riprovare tramite SSH.

9. Una volta completata la raccolta dei file di registro:

- Seleziona **Scarica** per scaricare il `.tar.gz` file.
- Seleziona **Invia ad AutoSupport** per inviare il `.tar.gz` inviare il file al supporto tecnico.

IL `.tar.gz` Il file contiene tutti i file di registro di tutti i nodi della griglia in cui la raccolta dei registri è avvenuta correttamente. Il combinato `.tar.gz` il file contiene un archivio di file di registro per ogni nodo della griglia.

L'oggetto del pacchetto AutoSupport è `USER_TRIGGERED_SUPPORT_BUNDLE`.

10. Selezionare **fine**.



IL `.tar.gz` il file viene eliminato quando selezioni **Fine**. Assicurati di scaricare o inviare prima il file.

Esaminare le metriche di StorageGRID

Durante la risoluzione di un problema, puoi lavorare con il supporto tecnico per rivedere metriche e grafici dettagliati per il tuo sistema StorageGRID.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

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



Gli strumenti disponibili nella pagina metriche sono destinati all'utilizzo da parte del supporto tecnico. Alcune funzioni e voci di menu di questi strumenti sono intenzionalmente non funzionali e sono soggette a modifiche. Vedere l'elenco di ["Metriche Prometheus comunemente utilizzate"](#).

Fasi

1. Come indicato dal supporto tecnico, seleziona **Supporto > Strumenti > Metriche**.

Di seguito è riportato un esempio della pagina Metrics (metriche):

Metrics

Access charts and metrics to help troubleshoot issues.

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

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 interface using the link below. You must be signed in to the Grid Manager.

<https://> 

Grafana is open-source software for metrics visualization. The Grafana interface provides pre-constructed dashboards that contain graphs of important metric values. Access the Grafana dashboards using the links below. You must be signed in to the Grid Manager.

ADE	Cloud Storage Pool Overview	Platform Services Processing
Account Service Overview	Decommission	Replicated Read Path Overview
Alertmanager	Erasure Coding - ADE	S3 - Node
Appliance Hardware Status	Erasure Coding - Overview	S3 Control
Audit Overview	Grid	S3 Overview
Bucket Cache	ILM	S3 Select
Cache Service	Identity Service Overview	Site
Cassandra Cluster Overview	Ingests	Support
Cassandra Network Overview	Node	SSD - Warranty
Cassandra Node Overview	Node (Internal Use)	Traces
Cassandra Table Cleanup	Object Chunk Leak Overview	Traffic Classification Policy
Chunk - Operations Overview	Object Serialization Mapping	Usage Processing
Chunk - Filesystem Latency Overview	OSL - AsyncIO	Virtual Memory (vmstat)
Chunk - Filesystem Latency Details	Platform Services Commits	
Cross Grid Replication	Platform Services Overview	

2. Per interrogare i valori correnti delle metriche StorageGRID e per visualizzare i grafici dei valori nel tempo, seleziona il collegamento nella sezione Prometheus.

Viene visualizzata l'interfaccia Prometheus. È possibile utilizzare questa interfaccia per eseguire query sulle metriche StorageGRID disponibili e per rappresentare graficamente le metriche StorageGRID nel tempo.



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

3. Per accedere a dashboard predefinite contenenti grafici delle metriche StorageGRID nel tempo, seleziona i collegamenti nella sezione Grafana.

Viene visualizzata l'interfaccia Grafana per il collegamento selezionato.



Modifica la priorità di I/O in StorageGRID

La priorità di input/output (I/O) consente di modificare le priorità relative per le operazioni di I/O sulla griglia.

Per impostazione predefinita, al traffico I/O PUT e GET del client viene assegnata la priorità più alta rispetto alle attività in background, come l'eliminazione dei dati con codice di cancellazione (EC) e la riparazione degli EC. Aumentando la priorità dell'eliminazione dei dati codificati in modo errato (EC) e delle attività di riparazione EC, è possibile completare queste attività più rapidamente. L'efficacia delle modifiche alla priorità di I/O è influenzata dalla frequenza delle richieste dei client, dalle fluttuazioni del traffico di rete e da altre attività di rete in corso.

Prima di iniziare

- Esaminare la pagina di priorità I/O per determinare quali opzioni potrebbero avere un impatto sulla rete.
- Valutare se il traffico client in corso può gestire in sicurezza tempi di attesa più lunghi o timeout dei client.
- Siate pronti a monitorare l'effetto del cambiamento di priorità e ad apportare le modifiche necessarie. Queste modifiche vengono implementate rapidamente, ma potrebbero volerci ore prima che i loro effetti

diventino visibili.

Fasi

1. Selezionare **Supporto > Priorità I/O**.
2. (Facoltativo) Modificare la priorità di eliminazione e riparazione EC, per le operazioni in background che eliminano i dati EC, rispetto ai valori predefiniti.



Utilizzare la priorità di eliminazione e riparazione EC bassa predefinita per le griglie che dispongono di nodi basati su RAID.

3. Selezionare **Salva**.
4. Monitorare il **"metrica"** per valutare l'effetto dei cambiamenti di priorità.

Esegui la diagnostica in StorageGRID

Durante la risoluzione di un problema, è possibile collaborare con il supporto tecnico per eseguire la diagnostica sul sistema StorageGRID e rivedere i risultati.

- ["Rivedere le metriche di supporto"](#)
- ["Metriche Prometheus comunemente utilizzate"](#)

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

La pagina Diagnostics (Diagnostica) esegue una serie di controlli diagnostici sullo stato corrente della griglia. Ogni controllo diagnostico può avere uno dei tre stati seguenti:

-  **Normale:** Tutti i valori rientrano nell'intervallo normale.
-  **Attenzione:** uno o più valori sono al di fuori dell'intervallo normale.
-  **Attenzione:** uno o più valori sono significativamente al di fuori dell'intervallo normale.

Gli stati di diagnostica sono indipendenti dagli avvisi correnti e potrebbero non indicare problemi operativi con la griglia. Ad esempio, un controllo diagnostico potrebbe mostrare lo stato di attenzione anche se non è stato attivato alcun allarme.

Fasi

1. Selezionare **Supporto > Strumenti > Diagnostica**.

Viene visualizzata la pagina Diagnostics (Diagnostica) che elenca i risultati di ciascun controllo diagnostico. I risultati vengono ordinati in base alla gravità (attenzione, attenzione e quindi normale). All'interno di ciascuna severità, i risultati sono ordinati in ordine alfabetico.

In questo esempio, una diagnosi ha lo stato Attenzione e tre diagnosi hanno lo stato Normale.

Diagnostics

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

 
Caution Attention
0 1

Run Diagnostics

 Node uptime

 Alert silences

 Appliance hardware component temperatures

 Cassandra automatic restarts

2. Per saperne di più su una diagnosi specifica, seleziona quella riga.

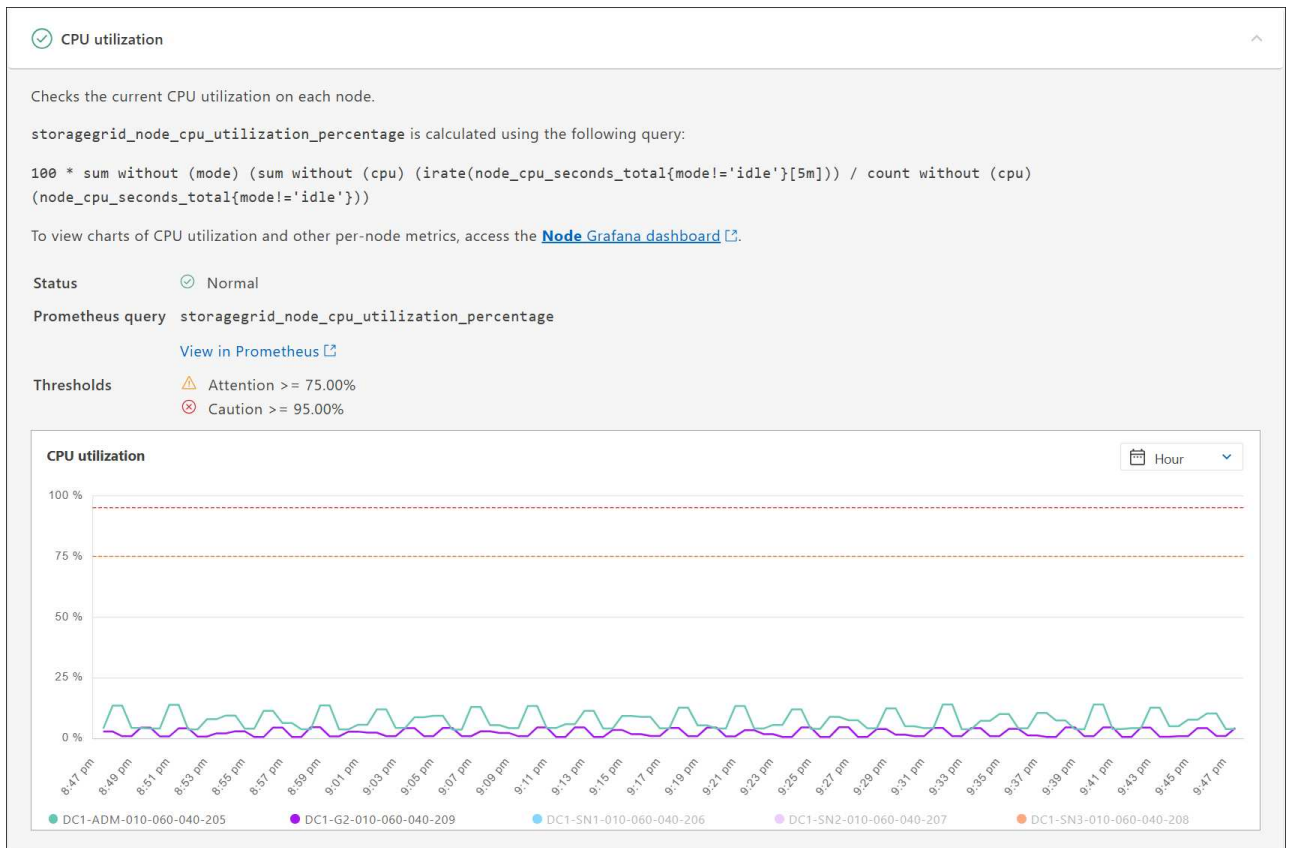
Vengono visualizzati i dettagli relativi alla diagnostica e ai risultati correnti. Sono elencati i seguenti dettagli:

- **Status** (Stato): Lo stato corrente di questa diagnostica: Normal (normale), Attention (attenzione) o Caution (attenzione).
- **Query Prometheus**: Se utilizzata per la diagnostica, l'espressione Prometheus utilizzata per generare i valori di stato. (Un'espressione Prometheus non viene utilizzata per tutte le diagnostiche).
- **Soglie**: Se disponibili per la diagnostica, le soglie definite dal sistema per ogni stato di diagnostica anomalo. (I valori di soglia non vengono utilizzati per tutte le diagnostiche).



Non puoi modificare queste soglie.

- **Valori di stato**: un grafico e una tabella (la tabella non è mostrata nello screenshot) che mostrano 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.



3. **Facoltativo:** per visualizzare i grafici Grafana correlati a questa diagnostica, seleziona **Dashboard Grafana**.

Questo collegamento non viene visualizzato per tutte le diagnostiche.

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. **Opzionale:** Per visualizzare un grafico dell'espressione di Prometheus nel tempo, seleziona **Visualizza in Prometheus**.

Viene visualizzato un grafico Prometheus dell'espressione utilizzata nella diagnostica.

☐ 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

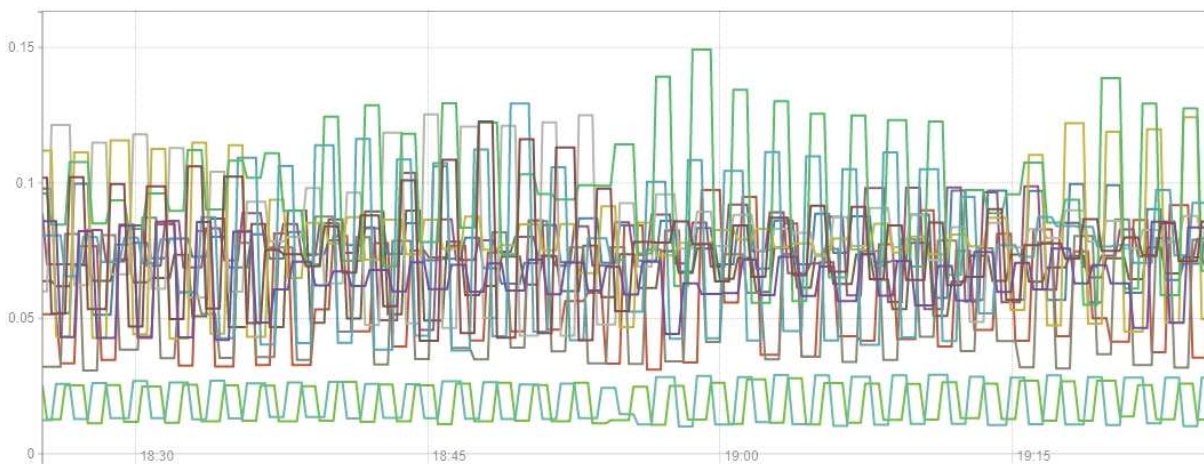
- insert metric at cursor - ▾

Graph Console

- 1h +

◀ Until ▶

Res. (s)

☐ stacked

- ✓ {instance="DC3-S3"}
- ✓ {instance="DC3-S2"}
- ✓ {instance="DC3-S1"}
- ✓ {instance="DC2-S3"}
- ✓ {instance="DC2-S2"}
- ✓ {instance="DC2-S1"}
- ✓ {instance="DC2-ADM1"}
- ✓ {instance="DC1-S3"}
- ✓ {instance="DC1-S2"}
- ✓ {instance="DC1-S1"}
- ✓ {instance="DC1-G1"}
- ✓ {instance="DC1-ARC1"}
- ✓ {instance="DC1-ADM1"}

[Remove Graph](#)[Add Graph](#)

Crea applicazioni di monitoraggio personalizzate per StorageGRID

Puoi creare dashboard e applicazioni di monitoraggio personalizzate utilizzando le metriche StorageGRID disponibili nell'API di gestione del grid.

Se si desidera monitorare le metriche non visualizzate in una pagina esistente di Grid Manager o se si desidera creare dashboard personalizzati per StorageGRID, è possibile utilizzare l'API di gestione griglia per eseguire query sulle metriche StorageGRID.

Puoi anche accedere direttamente alle metriche Prometheus con uno strumento di monitoraggio esterno, come Grafana. L'utilizzo di uno strumento esterno richiede il caricamento o la generazione di un certificato client amministrativo per consentire a StorageGRID di autenticare lo strumento per la sicurezza. Consultare la [Istruzioni per l'amministrazione di StorageGRID](#).

Per visualizzare le operazioni API delle metriche, incluso l'elenco completo delle metriche disponibili, vai su Grid Manager. Dalla parte superiore della pagina, seleziona l'icona di aiuto e seleziona **API documentation > metrics**.

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 dall'ambito di questa documentazione.

Risolvere i problemi relativi al sistema StorageGRID

Risolvere i problemi di un sistema StorageGRID

Se si riscontrano problemi durante l'utilizzo di un sistema StorageGRID, consultare i suggerimenti e le linee guida di questa sezione per ottenere assistenza nella determinazione e nella risoluzione del problema.

Spesso è possibile risolvere i problemi da soli; tuttavia, potrebbe essere necessario eseguire l'escalation di alcuni problemi al supporto tecnico.

definire il problema

Il primo passo per risolvere un problema è definire il problema in modo chiaro.

Questa tabella fornisce esempi dei tipi di informazioni che è possibile raccogliere per definire un problema:

Domanda	Esempio di risposta
Cosa fa o non fa il sistema StorageGRID? Quali sono i suoi sintomi?	Le applicazioni client segnalano che non è possibile acquisire oggetti in StorageGRID.
Quando è iniziato il problema?	L'acquisizione di oggetti è stata negata per la prima volta alle 14:50 dell'8 gennaio 2020.
Come hai notato il problema per la prima volta?	Notificato dall'applicazione client. Ha ricevuto anche notifiche email di avviso.
Il problema si verifica in modo coerente o solo a volte?	Il problema è in corso.

Domanda	Esempio di risposta
Se il problema si verifica regolarmente, quali passaggi lo causano	Il problema si verifica ogni volta che un client tenta di acquisire un oggetto.
Se il problema si verifica in modo intermittente, quando si verifica? Registrare i tempi di ciascun incidente di cui si è a conoscenza.	Il problema non è intermittente.
Hai già visto questo problema? Con quale frequenza avete avuto questo problema in passato?	Questa è la prima volta che vedo questo problema.

Valutare i rischi e l'impatto sul sistema

Una volta definito il problema, valutarne il rischio e l'impatto sul sistema StorageGRID. Ad esempio, la presenza di avvisi critici non significa necessariamente che il sistema non stia fornendo servizi di base.

Questa tabella riassume l'impatto del problema di esempio sulle operazioni del sistema:

Domanda	Esempio di risposta
Il sistema StorageGRID è in grado di acquisire contenuti?	No
Le applicazioni client possono recuperare il contenuto?	Alcuni oggetti possono essere recuperati e altri no.
I dati sono a rischio?	No
La capacità di condurre il business è gravemente compromessa?	Sì, perché le applicazioni client non possono memorizzare oggetti nel sistema StorageGRID e i dati non possono essere recuperati in modo coerente.

Raccogliere i dati

Dopo aver definito il problema e averne valutato il rischio e l'impatto, raccogliere i dati per l'analisi. Il tipo di dati più utili da raccogliere dipende dalla natura del problema.

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Creare una tempistica delle modifiche recenti	Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.	• Creare una tempistica delle modifiche recenti

Tipo di dati da raccogliere	Perché raccogliere questi dati	Istruzioni
Rivedere gli avvisi	Gli avvisi possono aiutare a determinare rapidamente la causa principale di un problema fornendo indizi importanti sui problemi sottostanti che potrebbero causarlo. Esaminare l'elenco degli avvisi correnti per verificare se StorageGRID ha identificato la causa principale di un problema. Rivedi gli avvisi attivati in passato per ulteriori informazioni.	• "Visualizzare gli avvisi correnti e risolti"
Stabilire le linee di base	Raccogliere informazioni sui livelli normali dei vari valori operativi. Questi valori di riferimento, e le deviazioni da queste linee di base, possono fornire indizi preziosi.	• Stabilire le linee di base
Eseguire test di acquisizione e recupero	Per risolvere i problemi di performance con acquisizione e recupero, utilizzare una workstation per memorizzare e recuperare gli oggetti. Confrontare i risultati con quelli osservati durante l'utilizzo dell'applicazione client.	• "Monitorare L'EFFICIENZA e OTTENERE le performance"
Esaminare i messaggi di audit	Esaminare i messaggi di audit per seguire in dettaglio le operazioni di StorageGRID. I dettagli nei messaggi di audit possono essere utili per la risoluzione di molti tipi di problemi, inclusi quelli relativi alle performance.	• "Esaminare i messaggi di audit"
Controllare le posizioni degli oggetti e l'integrità dello storage	In caso di problemi di storage, verificare che gli oggetti siano posizionati nel punto previsto. Verificare l'integrità dei dati dell'oggetto su un nodo di storage.	• "Monitorare le operazioni di verifica degli oggetti" • "Confermare le posizioni dei dati degli oggetti" • "Verificare l'integrità dell'oggetto"
Raccogliere i dati per il supporto tecnico	Il supporto tecnico potrebbe richiedere di raccogliere dati o rivedere informazioni specifiche per risolvere i problemi.	• "Raccogliere i file di log e i dati di sistema" • "Attivare manualmente un pacchetto AutoSupport" • "Rivedere le metriche di supporto"

Crea una timeline di modifiche recenti

Quando si verifica un problema, è necessario prendere in considerazione le modifiche apportate di recente e il momento in cui si sono verificate tali modifiche.

- Le modifiche al sistema StorageGRID, alla sua configurazione o al suo ambiente possono causare nuovi comportamenti.
- Una tempistica delle modifiche può aiutarti a identificare quali modifiche potrebbero essere responsabili di un problema e in che modo ciascuna modifica potrebbe avere influenzato il suo sviluppo.

Creare una tabella di modifiche recenti al sistema che includa informazioni su quando si è verificata ogni modifica e su eventuali dettagli rilevanti relativi alla modifica, ad esempio informazioni su ciò che è accaduto durante l'esecuzione della modifica:

Tempo di cambiamento	Tipo di cambiamento	Dettagli
Ad esempio: • Quando è stato avviato il ripristino del nodo? • Quando è stato completato l'aggiornamento del software? • Hai interrotto il processo?	Che cosa è successo? Cosa hai fatto?	Documentare i dettagli relativi alla modifica. Ad esempio: • Dettagli delle modifiche di rete. • Quale hotfix è stato installato. • Come sono cambiati i carichi di lavoro dei client. Assicurarsi di notare se più di una modifica si è verificata contemporaneamente. Ad esempio, questa modifica è stata apportata mentre era in corso un aggiornamento?

Esempi di modifiche recenti significative

Ecco alcuni esempi di modifiche potenzialmente significative:

- Il sistema StorageGRID è stato recentemente installato, ampliato o ripristinato?
- Il sistema è stato aggiornato di recente? È stata applicata una correzione rapida?
- L'hardware è stato riparato o modificato di recente?
- La policy ILM è stata aggiornata?
- Il carico di lavoro del client è cambiato?
- L'applicazione client o il suo comportamento sono cambiati?
- Hai modificato i bilanciatori di carico o aggiunto o rimosso un gruppo ad alta disponibilità di nodi di amministrazione o nodi gateway?
- Sono state avviate attività che potrebbero richiedere molto tempo? Alcuni esempi sono:
 - Ripristino di un nodo di storage guasto
 - Disattivazione del nodo di storage
- Sono state apportate modifiche all'autenticazione dell'utente, ad esempio l'aggiunta di un tenant o la modifica della configurazione LDAP?
- La migrazione dei dati è in corso?
- I servizi della piattaforma sono stati abilitati o modificati di recente?

- La compliance è stata abilitata di recente?
- I pool di storage cloud sono stati aggiunti o rimossi?
- Sono state apportate modifiche alla compressione o alla crittografia dello storage?
- Sono state apportate modifiche all'infrastruttura di rete? Ad esempio, VLAN, router o DNS.
- Sono state apportate modifiche alle origini NTP?
- Sono state apportate modifiche alle interfacce Grid, Admin o Client Network?
- Sono state apportate altre modifiche al sistema StorageGRID o al suo ambiente?

Stabilire le linee di base

È possibile stabilire linee di base per il sistema registrando i livelli normali di diversi valori operativi. In futuro, è possibile confrontare i valori correnti con queste linee di base per rilevare e risolvere i valori anomali.

Proprietà	Valore	Come ottenere
Consumo medio di storage	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Data (Storage utilizzato - dati oggetto), individuare un periodo in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare la quantità di storage consumata ogni giorno. È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Consumo medio di metadati	GB consumati al giorno Percentuale consumata al giorno	Accedere a Grid Manager. Nella pagina Nodes (nodi), selezionare l'intera griglia o un sito e passare alla scheda Storage (archiviazione). Nel grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto), individuare un punto in cui la riga è abbastanza stabile. Posiziona il cursore sul grafico per stimare la quantità di storage dei metadati consumata ogni giorno. È possibile raccogliere queste informazioni per l'intero sistema o per un data center specifico.
Tasso di operazioni S3	Operazioni/secondo	Nella dashboard di Grid Manager, seleziona Prestazioni > Operazioni S3 per nodi di archiviazione . 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 di acquisizione e recupero S3.

Proprietà	Valore	Come ottenere
Tasso di valutazione ILM	Oggetti/secondo	Dalla pagina nodi, selezionare grid > ILM . Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare un valore di riferimento per Evaluation rate per il sistema.
Velocità di scansione ILM	Oggetti/secondo	Selezionare Nodi > grid > ILM . Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare un valore di riferimento per velocità di scansione per il sistema.
Oggetti accodati dalle operazioni del client	Oggetti/secondo	Selezionare Nodi > grid > ILM . Nel grafico ILM Queue, individuare un punto in cui la riga è abbastanza stabile. Posizionare il cursore sul grafico per stimare un valore di riferimento per oggetti accodati (da operazioni client) per il sistema.
Latenza media delle query	Millisecondi	Selezionare Nodi > Nodo di archiviazione_ > Oggetti . Nella tabella Query, visualizza il valore per Latenza media.

Analizzare i dati

Utilizzare le informazioni raccolte per determinare la causa del problema e le potenziali soluzioni.

-analisi dipende dal problema, ma in generale:

- Individuare i punti di guasto e i colli di bottiglia utilizzando gli avvisi.
- Ricostruire la cronologia dei problemi utilizzando la cronologia e i grafici degli avvisi.
- Utilizzare i grafici per individuare le anomalie e confrontare la situazione del problema con il normale funzionamento.

Lista di controllo per le informazioni di escalation

Se non riesci a risolvere il problema da solo, contatta il supporto tecnico. Prima di contattare il supporto tecnico, raccogliere le informazioni elencate nella seguente tabella per facilitare la risoluzione del problema.

	Elemento	Note
	Dichiarazione del problema	Quali sono i sintomi del problema? Quando è iniziato il problema? Si verifica in modo coerente o intermittente? In caso di intermittenza, quali sono le volte in cui si è verificato il problema? Definire il problema
	Valutazione dell'impatto	Qual è la gravità del problema? Qual è l'impatto sull'applicazione client? • Il client si è connesso correttamente in precedenza? • Il client è in grado di acquisire, recuperare ed eliminare i dati?
	ID sistema StorageGRID	Selezionare Manutenzione > Sistema > Licenza . L'ID del sistema StorageGRID viene visualizzato come parte della licenza corrente.
	Versione del software	Nella parte superiore di Gestione griglia, selezionare l'icona della guida e selezionare About (informazioni su) per visualizzare la versione di StorageGRID.
	Personalizzazione	Riepilogare la configurazione del sistema StorageGRID. Ad esempio, elencare quanto segue: • Il grid utilizza la compressione dello storage, la crittografia dello storage o la conformità? • ILM produce oggetti replicati o sottoposti a erasure coding? ILM garantisce la ridondanza del sito? Le regole ILM utilizzano i comportamenti di ingest bilanciato, rigoroso o doppio commit?
	File di log e dati di sistema	Raccogli file di registro e dati di sistema per il tuo sistema. Selezionare Supporto > Strumenti > Raccolta registri . È possibile raccogliere i log per l'intera griglia o per i 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 installati in un sito includono il servizio ADC.
	Informazioni di riferimento	Raccogliere informazioni di riferimento relative alle operazioni di acquisizione, alle operazioni di recupero e al consumo dello storage. Stabilire le linee di base

✓	Elemento	Note
	Tempistiche delle modifiche recenti	Creare una timeline che riepiloga le modifiche recenti apportate al sistema o al suo ambiente. Creare una tempistica delle modifiche recenti
	Cronologia degli sforzi per diagnosticare il problema	Se sono state adottate misure per diagnosticare o risolvere il problema da soli, assicurarsi di registrare i passaggi e il risultato.

Risolvere i problemi relativi a oggetti e storage

Conferma le posizioni dei dati degli oggetti in StorageGRID

A seconda del problema, potrebbe essere necessario scegliere ["confermare la posizione in cui vengono memorizzati i dati dell'oggetto"](#). Ad esempio, è possibile verificare che il criterio ILM funzioni come previsto e che i dati degli oggetti vengano memorizzati dove previsto.

Prima di iniziare

- È necessario disporre di un identificatore di oggetto, che può essere uno dei seguenti:
 - **UUID**: Identificativo universalmente univoco dell'oggetto. Inserire il UUID in tutte le lettere maiuscole.
 - **CBID**: Identificatore univoco dell'oggetto all'interno di StorageGRID . È possibile ottenere il CBID di un oggetto dal log di audit. Inserire il CBID in tutte le lettere maiuscole.
 - **S3 bucket e oggetto chiave**: Quando un oggetto viene acquisito tramite ["Interfaccia S3"](#), l'applicazione client utilizza una combinazione di chiavi bucket e oggetto per memorizzare e identificare l'oggetto.

Fasi

1. Selezionare **ILM > Object metadata lookup**.
2. Digitare l'identificativo dell'oggetto nel campo **Identifier**.

È possibile immettere un UUID, un CBID o un bucket/chiave oggetto S3.

3. Se si desidera cercare una versione specifica dell'oggetto, inserire l'ID versione (facoltativo).

Object Metadata Lookup

Enter the identifier for any object stored in the grid to view its metadata.

Identifier

Version ID (optional)

Look Up

4. Selezionare **Cerca**.

"risultati della ricerca dei metadati degli oggetti"Viene visualizzato. In questa pagina sono elencati i seguenti tipi di informazioni:

- Metadati di sistema, tra cui l'ID oggetto (UUID), l'ID versione (facoltativo), il nome dell'oggetto, il nome del contenitore, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora della prima creazione dell'oggetto e la data e l'ora dell'ultima modifica dell'oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.
- Per oggetti segmentati e multiparte, un elenco di segmenti di oggetti che include identificatori di segmenti e dimensioni dei dati. Per gli oggetti con più di 100 segmenti, vengono visualizzati solo i primi 100 segmenti.
- Tutti i metadati degli oggetti nel formato di storage interno non elaborato. Questi metadati raw includono metadati interni del sistema che non sono garantiti per la persistenza dalla release alla release.

Nell'esempio seguente vengono illustrati i risultati della ricerca dei metadati degli oggetti per un oggetto di test S3 memorizzato come due copie replicate.

System Metadata

Object ID	A12E96FF-B13F-4905-9E9E-45373F6E7DA8
Name	testobject
Container	source
Account	t-1582139188
Size	5.24 MB
Creation Time	2020-02-19 12:15:59 PST
Modified Time	2020-02-19 12:15:59 PST

Replicated Copies

Node	Disk Path
99-97	/var/local/rangedb/2/p/06/0B/00nM8H\$ TFbnQQ} CV2E
99-99	/var/local/rangedb/1/p/12/0A/00nM8H\$ TFboW28 CXG%

Raw Metadata

```
{
  "TYPE": "CTNT",
  "CHND": "A12E96FF-B13F-4905-9E9E-45373F6E7DA8",
  "NAME": "testobject",
  "CBID": "0x8823DE7EC7C10416",
  "PHND": "FEA0AE51-534A-11EA-9FCD-31FF00C36D56",
  "PPTH": "source",
  "META": {
    "BASE": {
      "PAHS": "2",

```

Scopri i guasti dell'archivio di oggetti per i volumi di storage in StorageGRID

Lo storage sottostante su un nodo di storage è diviso in archivi di oggetti. Gli archivi di oggetti sono anche noti come volumi di storage.

È possibile visualizzare le informazioni sull'archivio oggetti per ciascun nodo di archiviazione. Selezionare **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

A seconda della natura del guasto, i guasti relativi a un volume di memorizzazione potrebbero essere riportati in ["avvisi relativi al volume di storage"](#). In caso di guasto di un volume di storage, è necessario riparare il volume di storage guasto per ripristinare la funzionalità completa del nodo di storage il prima possibile. Se necessario, è possibile accedere alla scheda **Configurazione** e ["Posizionare il nodo di storage in uno stato di sola-lettura"](#) in modo che il sistema StorageGRID possa utilizzarlo per il recupero dei dati mentre si prepara per un ripristino completo del server.

Verificare l'integrità dei dati degli oggetti in StorageGRID

Il sistema StorageGRID verifica l'integrità dei dati degli oggetti sui nodi di storage, verificando la presenza di oggetti corrotti e mancanti.

Esistono due processi di verifica: Verifica in background e verifica dell'esistenza degli oggetti (in precedenza chiamata verifica in primo piano). Lavorano insieme per garantire l'integrità dei dati. La verifica in background viene eseguita automaticamente e verifica continuamente la correttezza dei dati dell'oggetto. Il controllo dell'esistenza degli oggetti può essere attivato da un utente per verificare più rapidamente l'esistenza (anche se non la correttezza) degli oggetti.

Che cos'è la verifica in background?

Il processo di verifica in background verifica automaticamente e continuamente la presenza di copie corrotte dei dati degli oggetti nei nodi di storage e tenta automaticamente di risolvere eventuali problemi rilevati.

La verifica in background verifica l'integrità degli oggetti replicati e degli oggetti con codifica in cancellazione, come segue:

- **Oggetti replicati:** Se il processo di verifica in background trova un oggetto replicato corrotto, la copia corrotta viene rimossa dalla sua posizione e messa in quarantena in un altro punto del nodo di storage. Quindi, viene generata e posizionata una nuova copia non danneggiata per soddisfare le policy ILM attive. La nuova copia potrebbe non essere inserita nel nodo di storage utilizzato per la copia originale.



I dati degli oggetti corrotti vengono messi in quarantena invece che cancellati dal sistema, in modo che sia ancora possibile accedervi. Per ulteriori informazioni sull'accesso ai dati degli oggetti in quarantena, contattare il supporto tecnico.

- **Oggetti con codifica di cancellazione:** Se il processo di verifica in background rileva che un frammento di un oggetto con codifica di cancellazione è corrotto, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage, utilizzando i dati rimanenti e i frammenti di parità. Se il frammento danneggiato non può essere ricostruito, viene eseguito un tentativo di recuperare un'altra copia dell'oggetto. Se il recupero ha esito positivo, viene eseguita una valutazione ILM per creare una copia sostitutiva dell'oggetto con codice di cancellazione.

Il processo di verifica in background controlla solo gli oggetti sui nodi di storage. Non controlla gli oggetti in un Cloud Storage Pool. Gli oggetti devono avere più di quattro giorni di età per poter essere qualificati per la verifica in background.

La verifica in background viene eseguita a una velocità continua che non interferisce con le normali attività del sistema. Impossibile interrompere la verifica in background. Tuttavia, se si sospetta un problema, è possibile aumentare il tasso di verifica in background per verificare più rapidamente il contenuto di un nodo di storage.

Avvisi relativi alla verifica in background

Se il sistema rileva un oggetto corrotto che non è in grado di correggere automaticamente (perché il

danneggiamento impedisce l'identificazione dell'oggetto), viene attivato l'avviso **rilevato oggetto corrotto non identificato**.

Se la verifica in background non riesce a sostituire un oggetto danneggiato perché non riesce a individuarne un'altra copia, viene attivato l'avviso **Oggetti potenzialmente persi**.

Che cos'è il controllo dell'esistenza di un oggetto?

Il controllo dell'esistenza degli oggetti verifica se tutte le copie replicate previste degli oggetti e i frammenti con codifica di cancellazione sono presenti in un nodo di storage. Il controllo dell'esistenza degli oggetti non verifica i dati degli oggetti stessi (la verifica in background lo fa), ma fornisce un modo per verificare l'integrità dei dispositivi di storage, soprattutto se un recente problema hardware potrebbe avere influenzato l'integrità dei dati.

A differenza della verifica in background, che si verifica automaticamente, è necessario avviare manualmente un lavoro di verifica dell'esistenza di un oggetto.

Il controllo dell'esistenza degli oggetti legge i metadati di ogni oggetto memorizzato in StorageGRID e verifica l'esistenza di copie di oggetti replicate e frammenti di oggetti codificati per la cancellazione. I dati mancanti vengono gestiti come segue:

- **Copie replicate:** Se manca una copia dei dati degli oggetti replicati, StorageGRID tenta automaticamente di sostituire la copia da una copia memorizzata altrove nel sistema. Il nodo di storage esegue una copia esistente attraverso una valutazione ILM, che determina che il criterio ILM corrente non è più soddisfatto per questo oggetto perché manca un'altra copia. Viene generata e posizionata una nuova copia per soddisfare i criteri ILM attivi del sistema. Questa nuova copia potrebbe non essere posizionata nella stessa posizione in cui è stata memorizzata la copia mancante.
- **Frammenti con codifica di cancellazione:** Se manca un frammento di un oggetto con codifica di cancellazione, StorageGRID tenta automaticamente di ricostruire il frammento mancante sullo stesso nodo di storage utilizzando i frammenti rimanenti. Se il frammento mancante non può essere ricostruito (perché sono stati persi troppi frammenti), ILM tenta di trovare un'altra copia dell'oggetto, che può utilizzare per generare un nuovo frammento con codifica di cancellazione.

Eseguire il controllo dell'esistenza dell'oggetto

Viene creato ed eseguito un job di controllo dell'esistenza di un oggetto alla volta. Quando si crea un lavoro, selezionare i nodi di storage e i volumi che si desidera verificare. È inoltre possibile selezionare la coerenza per il lavoro.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso 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.
- Si è verificato che le seguenti procedure siano **non** in esecuzione sui nodi che si desidera controllare:
 - Espansione della griglia per aggiungere un nodo di storage
 - Decommissionare il nodo di storage
 - Ripristino di un volume di storage guasto
 - Ripristino di un nodo di storage con un disco di sistema guasto

- Ribilanciamento EC
- Clone del nodo dell'appliance

Il controllo dell'esistenza degli oggetti non fornisce informazioni utili durante l'esecuzione di queste procedure.

A proposito di questa attività

Il completamento di un processo di verifica dell'esistenza di un oggetto può richiedere giorni o settimane, in base al numero di oggetti nella griglia, ai volumi e ai nodi di storage selezionati e alla coerenza selezionata. È possibile eseguire un solo processo alla volta, ma è possibile selezionare più nodi e volumi di storage contemporaneamente.

Fasi

1. Selezionare **Manutenzione > Attività > Controllo esistenza oggetto**.
2. Selezionare **Crea job**. Viene visualizzata la procedura guidata Crea un processo di verifica dell'esistenza di un oggetto.
3. Selezionare i nodi contenenti i volumi che si desidera verificare. Per selezionare tutti i nodi online, selezionare la casella di controllo **Node name** (Nome nodo) nell'intestazione della colonna.

È possibile eseguire la ricerca in base al nome del nodo o al sito.

Non è possibile selezionare nodi che non sono connessi alla griglia.

4. Selezionare **continua**.
5. Selezionare uno o più volumi per ciascun nodo dell'elenco. È possibile cercare i volumi utilizzando il numero del volume di storage o il nome del nodo.

Per selezionare tutti i volumi per ciascun nodo selezionato, selezionare la casella di controllo **Storage volume** nell'intestazione della colonna.

6. Selezionare **continua**.
7. Selezionare la coerenza per il lavoro.

La coerenza determina il numero di copie dei metadati degli oggetti utilizzate per il controllo dell'esistenza dell'oggetto.

- **Strong-site**: Due copie di metadati in un singolo sito.
- **Strong-Global**: Due copie di metadati in ogni sito.
- **Tutti** (impostazione predefinita): Tutte e tre le copie dei metadati di ciascun sito.

Per ulteriori informazioni sulla coerenza, vedere le descrizioni nella procedura guidata.

8. Selezionare **continua**.
9. Controllare e verificare le selezioni. È possibile selezionare **Previous** (precedente) per passare a una fase precedente della procedura guidata e aggiornare le selezioni.

Viene generato un job di controllo dell'esistenza di un oggetto che viene eseguito fino a quando non si verifica una delle seguenti condizioni:

- Il lavoro viene completato.
- Il processo viene sospeso o annullato. È possibile riprendere un lavoro che è stato messo in pausa, ma non è possibile riprendere un lavoro che è stato annullato.

- Il lavoro si blocca. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto bloccato**. Seguire le azioni correttive specificate per l'avviso.
- Il lavoro non riesce. Viene attivato l'avviso **controllo dell'esistenza dell'oggetto non riuscito**. Seguire le azioni correttive specificate per l'avviso.
- Viene visualizzato il messaggio "Servizio non disponibile" o "errore interno del server". Dopo un minuto, aggiornare la pagina per continuare a monitorare il lavoro.



Se necessario, è possibile allontanarsi dalla pagina di controllo dell'esistenza dell'oggetto e tornare indietro per continuare a monitorare il lavoro.

10. Durante l'esecuzione del processo, visualizzare la scheda **lavoro attivo** e annotare il valore di copie oggetto mancanti rilevate.

Questo valore rappresenta il numero totale di copie mancanti di oggetti replicati e di oggetti con codifica di cancellazione con uno o più frammenti mancanti.

Se il numero di copie di oggetti mancanti rilevate è maggiore di 100, potrebbe esserci un problema con l'archiviazione del nodo di archiviazione.

11. Una volta completato il lavoro, eseguire eventuali azioni aggiuntive richieste:

- Se le copie oggetto mancanti rilevate sono pari a zero, non sono stati rilevati problemi. Non è richiesta alcuna azione.
- Se il valore Copie di oggetti mancanti rilevate è maggiore di zero e non è stato attivato l'avviso **Oggetti potenzialmente 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 potenzialmente persi**, l'integrità dei dati potrebbe essere compromessa. Contattare l'assistenza tecnica.
- È possibile esaminare le copie di oggetti potenzialmente perse utilizzando grep per estrarre i messaggi di controllo LLST: `grep LLST audit_file_name`.

Questa procedura è simile a quella per "[investigare oggetti potenzialmente persi](#)", sebbene per le copie degli oggetti si cerchi LLST invece di OLST.

12. Se è stata selezionata la coerenza globale forte o strong-Site per il lavoro, attendere circa tre settimane per la coerenza dei metadati, quindi rieseguire nuovamente il lavoro sugli stessi volumi.

Quando StorageGRID ha avuto il tempo di ottenere la coerenza dei metadati per i nodi e i volumi inclusi nel processo, la riesecuzione del processo potrebbe eliminare le copie degli oggetti mancanti segnalate erroneamente o causare il controllo di altre copie degli oggetti in caso di mancata esecuzione.

a. Selezionare **Manutenzione > Controllo esistenza oggetto > Cronologia lavori**.

b. Determinare quali lavori sono pronti per essere rieseguiti:

- i. Esaminare la colonna **ora di fine** per determinare quali lavori sono stati eseguiti più di tre settimane fa.
- ii. Per questi lavori, eseguire la scansione della colonna di controllo della coerenza per individuare la presenza di un sito forte o globale forte.

c. Selezionare la casella di controllo per ciascun processo che si desidera rieseguire, quindi selezionare **Rerun**.

- d. Nella procedura guidata Riesegui lavori, esaminare i nodi e i volumi selezionati e la coerenza.
- e. Quando si è pronti per rieseguire i lavori, selezionare **Rerun**.

Viene visualizzata la scheda lavoro attivo. Tutti i lavori selezionati vengono rieseguiti come un unico lavoro con una consistenza di sito sicuro. Un campo **lavori correlati** nella sezione Dettagli elenca gli ID lavoro per i lavori originali.

Risolvi l'avviso S3 PUT object size too large in StorageGRID

L'avviso S3 PUT object size too large viene attivato se un tenant tenta un'operazione PutObject non multipart che supera il limite di dimensione S3 di 5 GiB.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

Determinare quali tenant utilizzano oggetti di dimensioni superiori a 5 GiB, in modo da poterli notificare.

Fasi

1. Vai a **Configurazione > Monitoraggio > Server di audit e syslog**.
2. Se le scritture del client sono normali, accedere al registro di controllo:

- a. Invio `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

- e. Passare alla directory in cui si trovano i registri di controllo.

La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	<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> file è in genere vuoto o mancante in questa modalità.
Server syslog esterno	<code>/var/local/log/localaudit.log</code>

In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log O. /var/local/audit/export/`

Per saperne di più, fare riferimento a ["Seleziona la posizione del registro"](#).

f. Identificare i tenant che utilizzano oggetti di dimensioni superiori a 5 GiB.

- i. Invio `zgrep SPUT * | egrep "CSIZ\ (UI64\): ([5-9] | [1-9] [0-9]+) [0-9] {9}"`
- ii. Per ciascun messaggio di controllo nei risultati, esaminare il `S3AI` campo per determinare l'ID account tenant. Utilizzare gli altri campi del messaggio per determinare l'indirizzo IP utilizzato dal client, dal bucket e dall'oggetto:

Codice	Descrizione
SAIP	IP di origine
S3AI	ID tenant
S3BK	Bucket
S3KY	Oggetto
CSIZ	Dimensione (byte)

Esempio di risultati del registro di controllo

```
audit.log:2023-01-05T18:47:05.525999
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1672943621106262][TIME(UI64):80431733
3][SAIP(IPAD):"10.96.99.127"][S3AI(CSTR):"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 del client non sono normali, utilizzare l'ID tenant dell'avviso per identificare il tenant:

- a. Vai su **Supporto > Strumenti > Raccolta registri**. Raccogliere i registri delle applicazioni per il nodo di archiviazione nell'avviso. Specificare 15 minuti prima e dopo l'avviso. Fare riferimento a ["Raccogliere i file di log e i dati di sistema"](#).
- b. Estrarre il file e andare a `bycast.log`:

```
/GID<grid_id>_<time_stamp>/<site_node>/<time_stamp>/grid/bycast.log
```

- c. Cercare nel registro `method=PUT` e identificare il client nel `clientIP` campo.

Esempio di bycast.log


```
Jan 5 18:33:41 BHAVNAJ-DC1-S1-2-65 ADE: |12220829 1870864574 S3RQ %CEA
2023-01-05T18:33:41.208790| NOTICE 1404 af23cb66b7e3efa5 S3RQ:
EVENT_PROCESS_CREATE - connection=1672943621106262 method=PUT
name=</test/4MiB-0> auth=<V4> clientIP=<10.96.99.127>
```

4. Informare i locatari che la dimensione massima di PutObject è di 5 GiB e di utilizzare caricamenti multiparte per oggetti superiori a 5 GiB.
5. Ignorare l'avviso per una settimana se l'applicazione è stata modificata.

Risolvere i problemi relativi ai dati degli oggetti persi e mancanti

Scopri i dati degli oggetti persi e mancanti in StorageGRID

Gli oggetti possono essere recuperati per diversi motivi, tra cui le richieste di lettura da un'applicazione client, le verifiche in background dei dati degli oggetti replicati, le rivalutazioni ILM e il ripristino dei dati degli oggetti durante il ripristino di un nodo di storage.

Il sistema StorageGRID utilizza le informazioni sulla posizione 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 potenzialmente persi**, come segue:

- Per le copie replicate, se non è possibile recuperare un'altra copia, l'oggetto viene considerato perso e viene attivato l'avviso.
- Per le copie con erasure coding, se non è possibile recuperare una copia dalla posizione prevista, l'attributo copie danneggiate rilevate (ECOR) viene incrementato di uno prima di tentare di recuperare una copia da un'altra posizione. Se non viene trovata alcuna altra copia, viene attivato l'avviso.

È necessario esaminare immediatamente tutti gli avvisi di **Oggetti potenzialmente 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 su oggetti potenzialmente persi"](#). Gli avvisi di oggetti smarriti potrebbero essere attivati erroneamente per precauzione.

Nel caso in cui i dati degli oggetti senza copie vengano persi, non esiste alcuna soluzione di recupero. Tuttavia, è necessario ["azzerare il contatore degli oggetti potenzialmente persi"](#) per evitare che oggetti smarriti noti mascherino nuovi oggetti smarriti.

Risolvi l'avviso degli oggetti potenzialmente persi in StorageGRID

Quando viene attivato l'avviso **Oggetti potenzialmente persi**, è necessario indagare immediatamente. Raccogliere informazioni sugli oggetti interessati e contattare l'assistenza tecnica.

Prima di iniziare

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

- Si dispone di "[autorizzazioni di accesso specifiche](#)".
- È necessario disporre del `Passwords.txt` file.

A proposito di questa attività

L'avviso **Oggetti potenzialmente persi** indica che, secondo le informazioni disponibili in StorageGRID, non sono presenti copie di un oggetto nella griglia. I dati potrebbero essere andati persi definitivamente.

Esaminare immediatamente gli avvisi di oggetti smarriti. Potrebbe essere necessario intervenire per evitare ulteriori perdite di dati. In alcuni casi, potrebbe essere possibile ripristinare un oggetto perso se si esegue un'azione rapida.



Se vengono segnalati più di 10 oggetti smarriti, contattare l'assistenza tecnica. Non seguire questa procedura da solo.

Fasi

1. Selezionare **Nodi**.
2. Selezionare **Storage Node > Objects**.
3. Esaminare il numero di oggetti persi visualizzato nella tabella dei conteggi degli oggetti.

Questo numero indica il numero totale di oggetti che il nodo della griglia rileva come mancanti dall'intero sistema StorageGRID. Il valore è la somma dei contatori Lost Objects del componente Data Store all'interno dei servizi LDR e DDS.

4. Da un nodo di amministrazione, "[accedere al registro di controllo](#)" per determinare l'identificatore univoco (UUID) dell'oggetto che ha attivato l'avviso **Oggetti potenzialmente persi**:
 - a. Accedere al nodo Grid:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file. Quando si è collegati come root, il prompt cambia da `$` a `#`.
 - b. Passare alla directory in cui si trovano i registri di controllo.

La directory del registro di controllo e i nodi applicabili dipendono dalle impostazioni della destinazione di controllo.

Opzione	Destinazione
Nodi locali (impostazione predefinita)	<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> file è in genere vuoto o mancante in questa modalità.

Opzione	Destinazione
Server syslog esterno	/var/local/log/localaudit.log

In base alle impostazioni della destinazione di controllo, immettere: `cd /var/local/log O. /var/local/audit/export/`

Per saperne di più, fare riferimento a ["Seleziona la posizione del registro"](#).

- c. Utilizzare `grep` per estrarre i messaggi di audit OLST (Object Lost). Immettere: `grep OLST audit_file_name`
- d. Annotare il valore UUID incluso nel messaggio.

```
Admin: # grep OLST audit.log
2020-02-12T19:18:54.780426
[AUDT:[CBID(UI64):0x38186FE53E3C49A5][UUID(CSTR):"926026C4-00A4-449B-AC72-BCCA72DD1311"]
[PATH(CSTR):"source/cats"][NOID(UI32):12288733][VOLI(UI64):3222345986
][RSLT(FC32):NONE][AVER(UI32):10]
[ATIM(UI64):1581535134780426][ATYP(FC32):OLST][ANID(UI32):12448208][A
MID(FC32):ILMX][ATID(UI64):7729403978647354233]]
```

5. Cercare i metadati per l'oggetto perso utilizzando l'UUID:

- a. Selezionare **ILM > Object metadata lookup**.
- b. Immettere l'UUID e selezionare **Cerca**.
- c. Esaminare le posizioni nei metadati e intraprendere l'azione appropriata:

Metadati	Conclusione
<object_identifier> oggetto non trovato	Se l'oggetto non viene trovato, viene restituito il messaggio "ERROR": "". Se l'oggetto non viene trovato, azzerare il contatore degli oggetti potenzialmente persi per cancellare l'avviso. La mancanza di un oggetto indica che l'oggetto è stato eliminato intenzionalmente.
Posizioni > 0	Se nell'output sono elencate delle posizioni, l'avviso Oggetti potenzialmente persi potrebbe essere un falso positivo. Verificare che gli oggetti esistano. Utilizzare l'ID nodo e il percorso del file elencati nell'output per confermare che il file a oggetti si trova nella posizione indicata. Se gli oggetti esistono, azzerare il contatore degli oggetti potenzialmente persi per cancellare l'avviso.

Metadati	Conclusione
Posizioni = 0	Se nell'output non sono elencate posizioni, l'oggetto potrebbe essere mancante. Contattare l'assistenza tecnica. Il supporto tecnico potrebbe chiederti di verificare se è in corso una procedura di ripristino dello storage. Consulta: • "Ripristinare i dati dell'oggetto nel volume di storage per l'appliance" • "Ripristinare i dati degli oggetti nel volume di storage in cui il disco di sistema è intatto" • "Ripristinare i dati dell'oggetto nel volume di storage (errore del disco di sistema)"

6. Dopo aver risolto i problemi relativi agli oggetti persi, reimposta il contatore Oggetti potenzialmente persi per assicurarti che gli avvisi non siano falsi positivi:
 - a. Selezionare **Nodi**.
 - b. Selezionare **Nodo di archiviazione > Attività**.
 - c. Nella sezione Reimposta contatore oggetti potenzialmente persi, seleziona **Reimposta**.

Risolvi l'avviso di archiviazione dati oggetto insufficiente in StorageGRID

L'avviso **Low Object Data Storage** monitora lo spazio disponibile per memorizzare i dati degli oggetti su ciascun nodo di storage.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

L'avviso **archiviazione dati oggetto bassa** viene attivato quando la quantità totale di dati oggetto replicati e con erasure coding su un nodo di archiviazione soddisfa una delle condizioni configurate nella regola di avviso.

Per impostazione predefinita, viene attivato un avviso importante quando questa condizione viene valutata come true:

```
(storagegrid_storage_utilization_data_bytes /
(storagegrid_storage_utilization_data_bytes +
storagegrid_storage_utilization_usable_space_bytes)) >=0.90
```

In questa condizione:

- `storagegrid_storage_utilization_data_bytes` È una stima delle dimensioni totali dei dati di oggetti replicati e con erasure coding per un nodo storage.
- `storagegrid_storage_utilization_usable_space_bytes` È la quantità totale di spazio di archiviazione dell'oggetto rimanente per un nodo di archiviazione.

Se viene attivato un avviso **Low Object Data Storage** maggiore o minore, è necessario eseguire una procedura di espansione il prima possibile.

Fasi

1. Selezionare **Avvisi > Correnti**.

Viene visualizzata la pagina Avvisi.

2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low Object Data Storage**, se necessario, e selezionare l'avviso che si desidera visualizzare.



Selezionare l'avviso, non l'intestazione di un gruppo di avvisi.

3. Esaminare i dettagli nella finestra di dialogo e prendere nota di quanto segue:

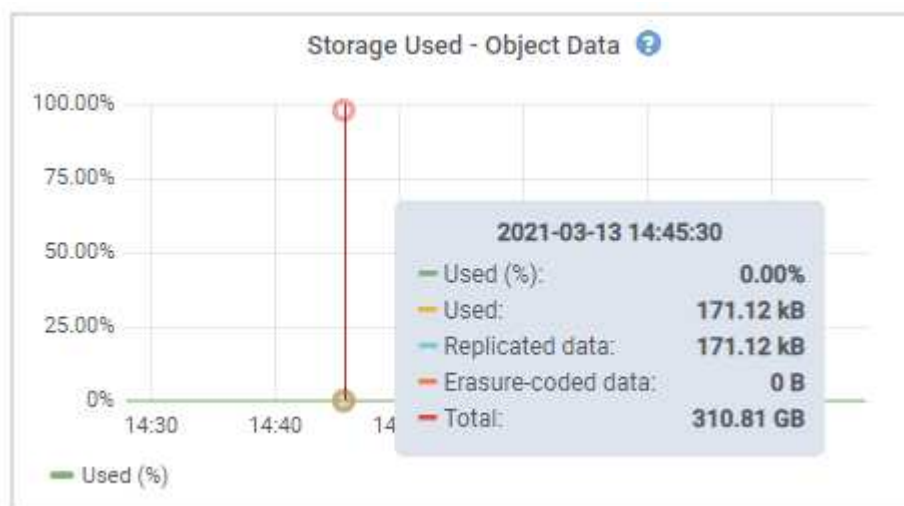
- Tempo di attivazione
- Il nome del sito e del nodo
- I valori correnti delle metriche per questo avviso

4. Selezionare **Nodi > Nodo o sito di archiviazione_ > Archiviazione**.

5. Posizionare il cursore sul grafico Storage Used - Object Data (Storage utilizzato - dati oggetto).

Vengono visualizzati i seguenti valori:

- **Used (%)**: Percentuale dello spazio utilizzabile totale utilizzato per i dati dell'oggetto.
- **Used**: Quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
- **Dati replicati**: Stima della quantità di dati degli oggetti replicati su questo nodo, sito o griglia.
- **Erase-coded data**: Stima della quantità di dati dell'oggetto con codifica di cancellazione su questo nodo, sito o griglia.
- **Total**: Quantità totale di spazio utilizzabile su questo nodo, sito o griglia. Il valore utilizzato è la `storagegrid_storage_utilization_data_bytes` metrica.



6. Selezionare i controlli dell'ora sopra il grafico per visualizzare l'utilizzo dello storage in diversi periodi di tempo.

L'utilizzo dello storage nel tempo può aiutarti a capire la quantità di storage utilizzata prima e dopo

l'attivazione dell'avviso e può aiutarti a stimare il tempo necessario per lo spazio rimanente del nodo.

7. Il più presto possibile, ["aggiungere capacità di storage"](#) alla vostra griglia.

È possibile aggiungere volumi di storage (LUN) ai nodi di storage esistenti oppure aggiungere nuovi nodi di storage.



Per ulteriori informazioni, vedere ["Gestire nodi storage completi"](#).

Risolvi l'override della filigrana in StorageGRID

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, potrebbe essere necessario risolvere l'avviso **bassa sostituzione filigrana di sola lettura**. Se possibile, aggiornare il sistema per iniziare a utilizzare i valori ottimizzati.

Nelle release precedenti, le tre ["filigrane dei volumi di storage"](#) erano impostazioni globali — gli stessi valori applicati a ogni volume di storage su ogni nodo di storage. A partire da StorageGRID 11.6, il software può ottimizzare queste filigrane per ogni volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Quando si esegue l'aggiornamento a StorageGRID 11.6 o versioni successive, le filigrane ottimizzate di sola lettura e di lettura/scrittura vengono applicate automaticamente a tutti i volumi di storage, a meno che non si verifichino le seguenti condizioni:

- Il sistema è vicino alla capacità e non è in grado di accettare nuovi dati se sono state applicate filigrane ottimizzate. In questo caso, StorageGRID non modificherà le impostazioni della filigrana.
- In precedenza, le filigrane dei volumi di storage sono state impostate su un valore personalizzato. StorageGRID non sovrascrive le impostazioni personalizzate del watermark con valori ottimizzati. Tuttavia, StorageGRID potrebbe attivare l'avviso di sovrascrittura filigrana di sola lettura * bassa se il valore personalizzato per la filigrana di sola lettura soft del volume di archiviazione è troppo piccolo.

Comprendere l'avviso

Se si utilizzano valori personalizzati per le filigrane dei volumi di storage, l'avviso **Low Read-only watermark override** potrebbe essere attivato per uno o più nodi di storage.

Ogni istanza dell'avviso indica che il valore personalizzato del watermark di sola lettura soft 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 del nodo di storage potrebbe essere molto basso prima di poter passare in sicurezza allo stato di sola lettura. Alcuni volumi di storage potrebbero diventare inaccessibili (automaticamente smontati) quando il nodo raggiunge la capacità.

Ad esempio, si supponga di aver precedentemente impostato il watermark soft di sola lettura del volume di archiviazione su 5 GB. Supponiamo ora che StorageGRID abbia calcolato i seguenti valori ottimizzati per i quattro volumi di storage nel nodo di storage A:

Volume 0	12 GB
Volume 1	12 GB
Volume 2	11 GB

Volume 3	15 GB

L'avviso **Low Read-only watermark override** viene attivato per il nodo di storage A perché il watermark personalizzato (5 GB) è inferiore al valore minimo ottimizzato per tutti i volumi in quel nodo (11 GB). Se si continua a utilizzare l'impostazione personalizzata, lo spazio del nodo potrebbe essere estremamente ridotto prima di poter passare in sicurezza allo stato di sola lettura.

Risolvere l'avviso

Seguire questa procedura se sono stati attivati uno o più avvisi **Low Read-only watermark override**. È inoltre possibile utilizzare queste istruzioni se si utilizzano impostazioni personalizzate per la filigrana e si desidera iniziare a utilizzare impostazioni ottimizzate anche se non sono stati attivati avvisi.

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root"](#).

A proposito di questa attività

È possibile risolvere l'avviso **deroga filigrana di sola lettura bassa** aggiornando le impostazioni di filigrana personalizzate con le nuove sostituzioni della filigrana. Tuttavia, se uno o più nodi di storage sono quasi pieni o si hanno requisiti ILM speciali, è necessario prima visualizzare le filigrane di storage ottimizzate e determinare se è sicuro utilizzarle.

Valutare l'utilizzo dei dati a oggetti per l'intero grid

Fasi

1. Selezionare **Nodi**.
2. Per ogni sito nella griglia, espandere l'elenco dei nodi.
3. Esaminare i valori percentuali mostrati nella colonna **dati oggetto utilizzati** per ciascun nodo di storage in ogni sito.

Nodes

View the list and status of sites and grid nodes.

Search... 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 la procedura appropriata:

- Se nessuno dei nodi di storage è quasi pieno (ad esempio, tutti i valori **dati oggetto utilizzati** sono inferiori al 80%), è possibile iniziare a utilizzare le impostazioni di override. Andare a [Utilizzare filigrane ottimizzate](#).
- Se le regole ILM utilizzano un comportamento di acquisizione rigoroso o se i pool di storage specifici sono quasi completi, eseguire i passaggi in [Visualizza filigrane di storage ottimizzate](#) e [Determinare se è possibile utilizzare filigrane ottimizzate](#).

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati calcolati per il watermark soft di sola lettura del volume di archiviazione. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

Fasi

- Selezionare **Supporto > Strumenti > Metriche**.
- Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
- Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore minimo ottimizzato del watermark di sola lettura soft per tutti i volumi di

archiviazione su ciascun nodo di archiviazione. Se questo valore è maggiore dell'impostazione personalizzata per il watermark soft di sola lettura del volume di archiviazione, viene attivato l'avviso **low Read-only watermark override** per il nodo di archiviazione.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

```
storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
```

L'ultima colonna mostra il valore massimo ottimizzato del watermark di sola lettura soft per tutti i volumi di archiviazione su ciascun nodo di archiviazione.

5. Nota sul valore massimo ottimizzato per ciascun nodo di storage.

[[determina-filigrane ottimizzate]]determinare se è possibile utilizzare filigrane ottimizzate

Fasi

1. Selezionare **Nodi**.
2. Ripetere questi passaggi per ogni nodo di storage online:
 - a. Selezionare **Storage Node > Storage**.
 - b. Scorri verso il basso fino alla tabella degli archivi degli oggetti.
 - c. Confrontare il valore **Available** per ciascun archivio di oggetti (volume) con il watermark ottimizzato massimo annotato per quel nodo di storage.
3. Se almeno un volume su ogni nodo di archiviazione online ha più spazio disponibile rispetto alla filigrana ottimizzata massima per quel nodo, andare a [Utilizzare filigrane ottimizzate](#) per iniziare a utilizzare le filigrane ottimizzate.

In caso contrario, espandere la griglia il prima possibile. ["aggiungere volumi di storage"](#)A un nodo esistente o ["Aggiungere nuovi nodi di storage"](#). Quindi, passare a [Utilizzare filigrane ottimizzate](#) per aggiornare le impostazioni della filigrana.

4. Se è necessario continuare a utilizzare i valori personalizzati per le filigrane del volume di archiviazione ["silenzio"](#)o ["disattiva"](#) l'avviso **Ignora filigrana di sola lettura bassa**.



Gli stessi valori di watermark personalizzati vengono applicati a ogni volume di storage su ogni nodo di storage. L'utilizzo di valori inferiori a quelli consigliati per le filigrane dei volumi di storage potrebbe causare l'inaccessibilità di alcuni volumi di storage (automaticamente smontati) quando il nodo raggiunge la capacità.

utilizza filigrane ottimizzate

Fasi

1. Vai a **Supporto > Altro > Filigrane di archiviazione**.
2. Selezionare la casella di controllo **Usa valori ottimizzati**.
3. Selezionare **Salva**.

Le impostazioni ottimizzate del watermark del volume di storage sono ora attive per ciascun volume di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

Risolvere i problemi relativi ai metadati in StorageGRID

Se si verificano problemi relativi ai metadati, gli avvisi ti informeranno sull'origine dei problemi e sulle azioni consigliate da intraprendere. In particolare, è necessario aggiungere nuovi nodi di archiviazione se viene attivato l'avviso archiviazione metadati bassa.

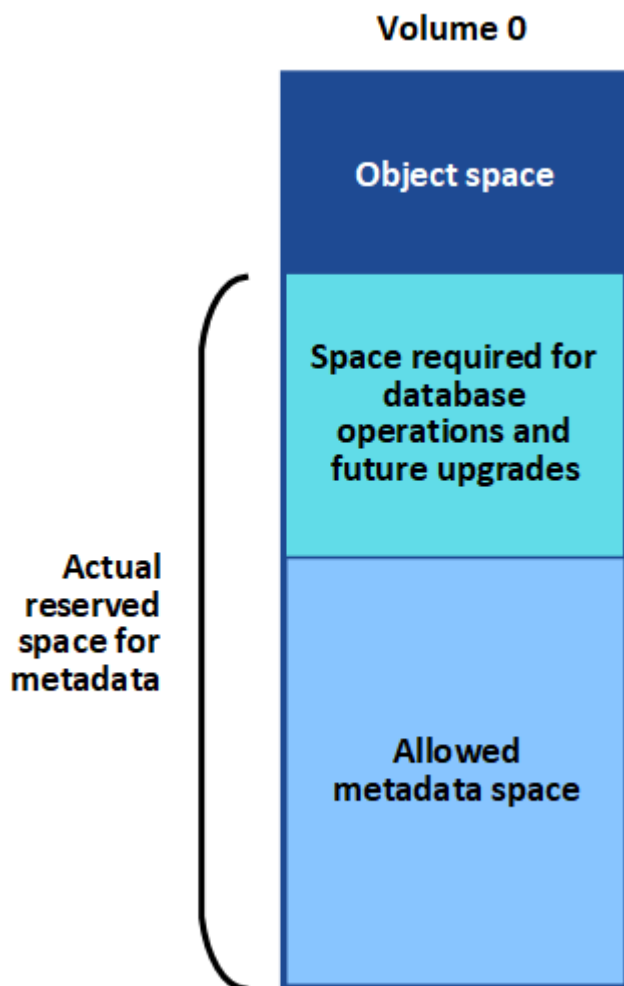
Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

Seguire le azioni consigliate per ogni avviso relativo ai metadati attivato. Se viene attivato l'avviso **Low metadata storage**, è necessario aggiungere nuovi nodi di storage.

StorageGRID riserva una certa quantità di spazio sul volume 0 di ciascun nodo di storage per i metadati dell'oggetto. Questo spazio, noto come *spazio riservato effettivo*, è suddiviso nello spazio consentito per i metadati dell'oggetto (lo spazio dei metadati consentito) e nello spazio richiesto per le operazioni essenziali del database, come la compattazione e la riparazione. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



Se i metadati degli oggetti consumano più del 100% dello spazio consentito per i metadati, le operazioni del database non possono essere eseguite in modo efficiente e si verificano errori.

Puoi ["Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage"](#) aiutarti ad anticipare gli errori e correggerli prima che si verifichino.

StorageGRID utilizza la seguente metrica Prometheus per misurare la quantità di spazio consentito per i metadati:

```
storagegrid_storage_utilization_metadata_bytes/storagegrid_storage_utilization_metadata_allowed_bytes
```

Quando l'espressione Prometheus raggiunge determinate soglie, viene attivato l'avviso **Low metadata storage**.

- **Minore:** I metadati degli oggetti utilizzano almeno il 70% dello spazio consentito per i metadati. È necessario aggiungere nuovi nodi di storage il prima possibile.
- **Major:** I metadati degli oggetti utilizzano almeno il 90% dello spazio consentito per i metadati. È necessario aggiungere immediatamente nuovi nodi di storage.



Quando i metadati dell'oggetto utilizzano almeno il 90% dello spazio consentito per i metadati, viene visualizzato un avviso sul dashboard. Se viene visualizzato questo avviso, è necessario aggiungere immediatamente nuovi nodi di storage. Non è mai necessario consentire ai metadati degli oggetti di utilizzare più del 100% dello spazio consentito.

- **Critico:** I metadati degli oggetti utilizzano almeno il 100% dello spazio consentito e stanno iniziando a consumare lo spazio necessario per le operazioni essenziali del database. È necessario interrompere l'acquisizione di nuovi oggetti e aggiungere immediatamente nuovi nodi di storage.



Se la dimensione del volume 0 è inferiore all'opzione di storage Metadata Reserved Space (ad esempio, in un ambiente non in produzione), il calcolo dell'avviso **Low metadata storage** potrebbe essere impreciso.

Fasi

1. Selezionare **Avvisi > Correnti**.
2. Dalla tabella degli avvisi, espandere il gruppo di avvisi **Low metadata storage**, se necessario, e selezionare l'avviso specifico che si desidera visualizzare.
3. Esaminare i dettagli nella finestra di dialogo degli avvisi.
4. Se è stato attivato un avviso importante o critico **Low metadata storage**, eseguire un'espansione per aggiungere immediatamente i nodi di storage.



Poiché StorageGRID conserva copie complete di tutti i metadati degli oggetti in ogni sito, la capacità dei metadati dell'intera griglia è limitata dalla capacità dei metadati del sito più piccolo. Se è necessario aggiungere capacità di metadati a un sito, è necessario utilizzare anche ["espandere qualsiasi altro sito"](#) lo stesso numero di nodi di archiviazione.

Dopo aver eseguito l'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi, aumentando così la capacità complessiva dei metadati della griglia. Non è richiesta alcuna azione da parte dell'utente. L'avviso **Low metadata storage** viene cancellato.

Risolvere gli errori dei certificati in StorageGRID

Se si verifica un problema di sicurezza o certificato quando si tenta di connettersi a StorageGRID utilizzando un browser Web, un client S3 o uno strumento di monitoraggio esterno, è necessario controllare il certificato.

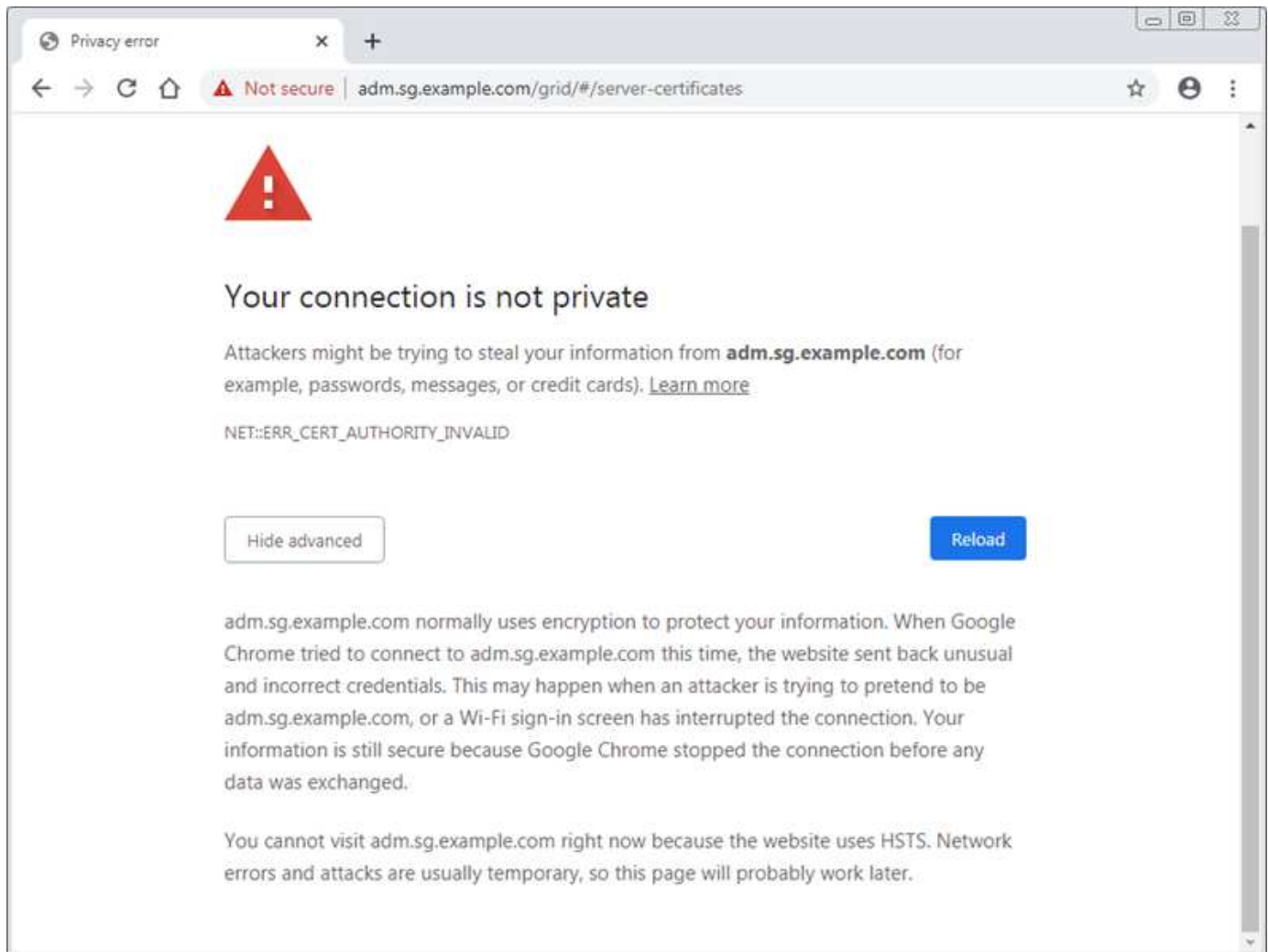
A proposito di questa attività

Gli errori dei certificati possono causare problemi quando si tenta di connettersi a StorageGRID utilizzando Gestione griglia, API di gestione griglia, Gestore tenant o API di gestione tenant. Gli errori dei certificati 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 invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Viene ripristinato da un certificato dell'interfaccia di gestione personalizzata al certificato del server predefinito.

L'esempio seguente mostra un errore di certificato quando il certificato dell'interfaccia di gestione personalizzata è scaduto:



Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere.

Quando si utilizzano certificati client per l'integrazione esterna di Prometheus, gli errori dei certificati possono essere causati dal certificato dell'interfaccia di gestione di StorageGRID o dai certificati client. L'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando un certificato client sta per scadere.

Fasi

Se hai ricevuto una notifica di avviso relativa a un certificato scaduto, accedi ai dettagli del certificato: . Selezionare **Configurazione > Sicurezza > Certificati** e quindi ["selezionare la scheda del certificato appropriata"](#) .

1. Controllare 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, caricare o generare un nuovo certificato.
 - Per un certificato server, vedere la procedura per ["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#).
 - Per un certificato client, vedere la procedura per ["configurazione di un certificato client"](#).
3. In caso di errori del certificato del server, provare una o entrambe le seguenti opzioni:
 - Assicurarsi che il campo Subject alternative Name (SAN) del certificato sia compilato e che LA SAN corrisponda all'indirizzo IP o al nome host del nodo a cui si sta effettuando la connessione.
 - Se si sta tentando di connettersi a StorageGRID utilizzando un nome di dominio:
 - i. Inserire l'indirizzo IP del nodo di amministrazione invece del nome di dominio per evitare l'errore di connessione e accedere a Grid Manager.
 - ii. Da Grid Manager, seleziona **Configurazione > Sicurezza > Certificati** e poi ["selezionare la scheda del certificato appropriata"](#) per installare un nuovo certificato personalizzato o continuare con il certificato predefinito.
 - iii. Nelle istruzioni per l'amministrazione di StorageGRID, vedere la procedura per ["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#).

Risolvi i problemi relativi al nodo di amministrazione e all'interfaccia utente in StorageGRID

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi ai nodi amministrativi e all'interfaccia utente di StorageGRID.

Errori di accesso al nodo amministrativo

Se si verifica un errore durante l'accesso a un nodo amministrativo StorageGRID, il sistema potrebbe presentare un problema relativo a ["networking"](#) o ["hardware"](#), a ["Servizi del nodo di amministrazione"](#) o a ["Problema con il database Cassandra"](#) nodi di archiviazione connessi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone del `Passwords.txt` file.
- Si dispone di ["autorizzazioni di accesso specifiche"](#).

A proposito di questa attività

Utilizzare queste linee guida per la risoluzione dei problemi se viene visualizzato uno dei seguenti messaggi di errore quando si tenta di accedere a un nodo amministratore:

- Your credentials for this account were invalid. Please try again.
- Waiting for services to start...
- Internal server error. The server encountered an error and could not complete your request. Please try again. If the problem persists, contact Technical Support.
- Unable to communicate with server. Reloading page...

Fasi

1. Attendere 10 minuti e riprovare a effettuare l'accesso.

Se l'errore non viene risolto automaticamente, passare alla fase successiva.

2. Se il sistema StorageGRID dispone di più di un nodo amministrativo, provare ad accedere al 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 si dispone di un solo nodo di amministrazione o non si riesce ancora ad accedere, passare alla fase successiva.

3. Determinare se l'hardware del nodo non è in linea.

4. Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID, consulta la procedura per configurare l'SSO usando "[OIDC](#)" o "[SAML](#)".

Potrebbe essere necessario disattivare temporaneamente e riattivare SSO per un singolo nodo di amministrazione per risolvere eventuali problemi.

5. Determinare se l'account in uso appartiene a un utente federato.

Se l'account utente federated non funziona, provare ad accedere a Grid Manager come utente locale, ad esempio root.

- Se l'utente locale può effettuare l'accesso:
 - i. Rivedere gli avvisi.
 - ii. Selezionare **Configurazione > Controllo accessi > Federazione identità**.
 - iii. Seleziona **Verifica connessione** per convalidare le impostazioni di connessione per il LDAP server.
 - iv. Se il test non riesce, risolvere eventuali errori di configurazione.
- Se l'utente locale non riesce ad accedere e si è certi che le credenziali siano corrette, passare alla fase successiva.

6. Utilizzare Secure Shell (SSH) per accedere al nodo di amministrazione:

- a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

7. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo 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. Verificare che il servizio nginx-gw sia in esecuzione # `service nginx-gw status`

9. utilizzare Lumberjack per raccogliere i registri: # `/usr/local/sbin/lumberjack.rb`

Se l'autenticazione non è riuscita in passato, è possibile utilizzare le opzioni di script `--start` e `--end` Lumberjack per specificare l'intervallo di tempo appropriato. Utilizzare `lumberjack -h` per i dettagli su queste opzioni.

L'output sul terminale indica dove è stato copiato l'archivio di log.

10. Rivedi i seguenti log:

- `/var/local/log/bycast.log`
- `/var/local/log/bycast-err.log`
- `/var/local/log/nms.log`
- `**/*commands.txt`

11. Se non si riesce a identificare alcun problema con il nodo di amministrazione, eseguire uno dei seguenti comandi per determinare gli indirizzi IP dei tre nodi di storage che eseguono il servizio ADC presso la propria sede. In genere, si tratta dei primi tre nodi di storage installati nel sito.

```
# cat /etc/hosts
```

```
# gpt-list-services adc
```

I nodi di amministrazione utilizzano il servizio ADC durante il processo di autenticazione.

12. Dal nodo Admin, utilizzare ssh per accedere a ciascuno dei nodi di archiviazione ADC, utilizzando gli indirizzi IP identificati.

13. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo griglia: `storagegrid-status`

Assicurarsi che i servizi `idnt`, `acct`, `nginx` e `cassandra` siano tutti in esecuzione.

14. Ripetere i passaggi [Utilizzare Lumberjack per raccogliere i registri](#) e [Esaminare i registri](#) per rivedere i registri sui nodi di archiviazione.

15. Se non si riesce a risolvere il problema, contattare il supporto tecnico.

Fornire al supporto tecnico i registri raccolti. Vedere anche ["Riferimenti ai file di log"](#).

Problemi dell'interfaccia utente

L'interfaccia utente di Grid Manager o Tenant Manager potrebbe non rispondere come previsto dopo l'aggiornamento del software StorageGRID.

Fasi

1. Assicurarsi di utilizzare un ["browser web supportato"](#).
2. Cancellare la cache del browser Web.

La cancellazione della cache rimuove le risorse obsolete utilizzate dalla versione precedente del software StorageGRID e consente all'interfaccia utente di funzionare nuovamente correttamente. Per istruzioni, consultare la documentazione del browser Web.

Risolvi i problemi di rete, hardware e piattaforma in StorageGRID

È possibile eseguire diverse attività per determinare l'origine dei problemi relativi a

problemi di rete, hardware e piattaforma StorageGRID.

[[422-unprocessable-entity-errors]]

== Errori "422: Entità non elaborabile"

L'errore 422: Unprocessable Entity può verificarsi per diversi motivi. Controllare il messaggio di errore per determinare la causa del problema.

Se viene visualizzato uno dei messaggi di errore elencati, eseguire l'azione consigliata.

Messaggio di errore	Causa principale e azione correttiva
<pre>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</pre>	Questo messaggio potrebbe essere visualizzato se si seleziona l'opzione non utilizzare TLS per Transport Layer Security (TLS) durante la configurazione della federazione delle identità utilizzando Windows Active Directory (ad). L'utilizzo dell'opzione non utilizzare TLS non è supportato per l'utilizzo con i server ad che applicano la firma LDAP. Selezionare l'opzione Use STARTTLS (Usa STARTTLS*) o l'opzione Use LDAPS (Usa LDAPS* per TLS).

Messaggio di errore	Causa principale e azione correttiva
<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 TLS (Transport Layer Security) da StorageGRID a un sistema esterno utilizzato per identificare la federazione o i pool di storage cloud. Controllare le cifre offerte dal sistema esterno. Il sistema deve utilizzare una delle "Crittografia supportata da StorageGRID" per le connessioni TLS in uscita, come illustrato nelle istruzioni per l'amministrazione di StorageGRID.

Avviso di mancata corrispondenza MTU della rete griglia

L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato quando l'impostazione Maximum Transmission Unit (MTU) per l'interfaccia Grid Network (eth0) differisce significativamente tra i nodi della griglia.

A proposito di questa attività

Le differenze nelle impostazioni MTU potrebbero indicare che alcune, ma non tutte, reti eth0 sono configurate per i frame jumbo. Una mancata corrispondenza delle dimensioni MTU superiore a 1000 potrebbe causare problemi di performance di rete.

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, ["consentire temporaneamente l'accesso"](#).
2. Elencare le impostazioni MTU per eth0 su tutti i nodi.
 - Utilizzare la query fornita in Grid Manager.
 - Passare alla *primary Admin Node IP address/metrics/graph* query seguente e immetterla: `node_network_mtu_bytes{device="eth0"}`
3. ["Modificare le impostazioni MTU"](#) Se necessario, per garantire che siano uguali per l'interfaccia di rete della griglia (eth0) su tutti i nodi.
 - Per i nodi basati su Linux e VMware, utilizzare il seguente comando: `/usr/sbin/change-ip.py [-h] [-n node] mtu network [network...]`

Esempio: `change-ip.py -n node 1500 grid admin`

Nota: Nei nodi basati su Linux, se il valore MTU desiderato per la rete nel contenitore supera il valore già configurato sull'interfaccia host, è necessario configurare l'interfaccia host in modo che abbia il

valore MTU desiderato, quindi utilizzare lo script per modificare il valore MTU `change-ip.py` della rete nel contenitore.

Utilizzare i seguenti argomenti per modificare la MTU su nodi basati su Linux o VMware.

Argomenti di posizione	Descrizione
<code>mtu</code>	MTU da impostare. Deve essere compreso tra 1280 e 9216.
<code>network</code>	Le reti a cui applicare la MTU. Includere uno o più dei seguenti tipi di rete: • griglia • amministratore • client

+

Argomenti facoltativi	Descrizione
<code>-h, - help</code>	Visualizzare il messaggio della guida e uscire.
<code>-n node, --node node</code>	Il nodo. L'impostazione predefinita è il nodo locale.

4. Se hai consentito l'accesso SSH esterno, **"bloccare l'accesso"** quando hai terminato il compito.

Avviso errore frame di ricezione rete nodo

Gli avvisi **errore frame di ricezione rete nodo** possono essere causati da problemi di connettività tra StorageGRID e l'hardware di rete. Questo avviso viene cancellato da solo dopo aver risolto il problema sottostante.

A proposito di questa attività

Gli avvisi **errore frame di ricezione rete nodo** possono essere causati dai seguenti problemi con l'hardware di rete che si connette a StorageGRID:

- La funzione FEC (Forward Error Correction) è obbligatoria e non in uso
- Mancata corrispondenza tra porta dello switch e MTU della scheda NIC
- Elevati tassi di errore di collegamento
- Buffer di anello NIC scaduto

Fasi

1. Seguire la procedura di risoluzione dei problemi per tutte le cause potenziali di questo avviso, data la configurazione della rete in uso.
2. A seconda della causa dell'errore, attenersi alla seguente procedura:

Mancata corrispondenza FEC



Questi passaggi sono applicabili solo agli avvisi **Node network reception frame error** causati dalla mancata corrispondenza FEC sulle apparecchiature StorageGRID.

- a. Controllare lo stato FEC della porta dello switch collegato all'appliance StorageGRID.
- b. Controllare l'integrità fisica dei cavi che collegano l'apparecchio allo switch.
- c. Se si desidera modificare le impostazioni FEC per tentare di risolvere l'avviso, verificare innanzitutto che il dispositivo sia configurato per la modalità **Auto** nella pagina di configurazione del collegamento del programma di installazione del dispositivo StorageGRID (consultare le istruzioni per il dispositivo in uso:
 - "SG6160"
 - "SGF6112"
 - "SG6000"
 - "SG5800"
 - "SG5700"
 - "SG110 e SG1100"
 - "SG100 e SG1000"
- d. Modificare le impostazioni FEC sulle porte dello switch. Le porte dell'appliance StorageGRID regoleranno le impostazioni FEC in modo che corrispondano, se possibile.

Non è possibile configurare le impostazioni FEC sulle appliance StorageGRID. Le appliance tentano invece di rilevare e duplicare le impostazioni FEC sulle porte dello switch a cui sono collegate. Se i collegamenti sono forzati a velocità di rete 25-GbE o 100-GbE, lo switch e la NIC potrebbero non riuscire a negoziare un'impostazione FEC comune. Senza un'impostazione FEC comune, la rete torna alla modalità "no-FEC". Quando la funzione FEC non è attivata, le connessioni sono più soggette a errori causati da disturbi elettrici.



Le appliance StorageGRID supportano Firecode (FC) e Reed Solomon (RS) FEC, oltre che FEC.

Mancata corrispondenza tra porta dello switch e MTU della scheda NIC

Se l'avviso è causato da una porta dello switch e da una mancata corrispondenza della MTU della NIC, verificare che la dimensione MTU configurata sul nodo corrisponda all'impostazione MTU per la porta dello switch.

La dimensione MTU configurata sul nodo potrebbe essere inferiore all'impostazione sulla porta dello switch a cui è connesso il nodo. Se un nodo StorageGRID riceve un frame Ethernet più grande della sua MTU, cosa possibile con questa configurazione, potrebbe essere segnalato l'avviso **Node network reception frame error**. Se si ritiene che questo sia quanto accade, modificare la MTU della porta dello switch in modo che corrisponda alla MTU dell'interfaccia di rete StorageGRID oppure modificare la MTU dell'interfaccia di rete StorageGRID in modo che corrisponda alla porta dello switch, in base agli obiettivi o ai requisiti della MTU end-to-end.



Per ottenere le migliori performance di rete, tutti i nodi devono essere configurati con valori MTU simili sulle interfacce Grid Network. L'avviso **Grid Network MTU mismatch** (mancata corrispondenza MTU rete griglia) viene attivato se si verifica una differenza significativa nelle impostazioni MTU per Grid Network su singoli nodi. I valori MTU non devono essere uguali per tutti i tipi di rete. Per ulteriori informazioni, vedere [Risolvere i problemi relativi all'avviso di mancata corrispondenza MTU della rete griglia](#).



Vedere anche "[Modificare l'impostazione MTU](#)".

Elevati tassi di errore di collegamento

- Attivare FEC, se non è già attivato.
- Verificare che il cablaggio di rete sia di buona qualità e non sia danneggiato o collegato in modo errato.
- Se i cavi non sembrano essere il problema, contattare il supporto tecnico.



In un ambiente con elevati livelli di rumore elettrico, potrebbero verificarsi errori elevati.

Buffer di anello NIC scaduto

Se l'errore è un buffer di anello della scheda di rete in eccesso, contattare il supporto tecnico.

Il buffer circolare può essere sovraccarico quando il sistema StorageGRID è sovraccarico e non è in grado di elaborare gli eventi di rete in modo tempestivo.

- Monitorare il problema e contattare l'assistenza tecnica se l'avviso non risolve il problema.

Errori di sincronizzazione dell'ora

Potrebbero verificarsi problemi con la sincronizzazione dell'ora nella griglia.

Se si verificano problemi di sincronizzazione dell'ora, verificare di aver specificato almeno quattro origini NTP esterne, ciascuna con uno strato 3 o un riferimento migliore, e che tutte le origini NTP esterne funzionino normalmente e siano accessibili dai nodi StorageGRID.



["Specifica dell'origine NTP esterna"](#) Per un'installazione StorageGRID a livello di produzione, non utilizzare il servizio Windows Time (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Time sulle versioni precedenti di Windows non è sufficientemente accurato e non è supportato da Microsoft per l'utilizzo in ambienti ad alta precisione, come StorageGRID.

Linux: Problemi di connettività di rete

Potrebbero verificarsi problemi di connettività di rete per i nodi StorageGRID ospitati su host Linux.

Clonazione indirizzo MAC

In alcuni casi, i problemi di rete possono essere risolti utilizzando la clonazione dell'indirizzo MAC. Se si utilizzano host virtuali, impostare il valore della chiave di clonazione dell'indirizzo MAC per ciascuna 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. Vedi le istruzioni per [creare file di configurazione del nodo](#).



Crea interfacce di rete virtuali separate da usare per il sistema operativo host Linux. Usare le stesse interfacce di rete per il sistema operativo host Linux e il container StorageGRID potrebbe rendere il sistema operativo host irraggiungibile.

Per maggiori informazioni, consultare le istruzioni per ["abilitazione della clonazione MAC"](#).

Linux: Lo stato del nodo è "orfano"

Un nodo Linux in uno stato orfano di solito indica che il servizio StorageGRID o il daemon del nodo StorageGRID che controlla il contenitore del nodo sono morti inaspettatamente.

A proposito di questa attività

Se un nodo Linux segnala che si trova in uno stato orfano, è necessario:

- Controllare i registri per verificare la presenza di errori e messaggi.
- Tentare di riavviare il nodo.
- Se necessario, utilizzare i comandi del motore dei container per arrestare il contenitore di nodi esistente.
- Riavviare il nodo.

Fasi

1. Controllare i log sia per il daemon di servizio che per il nodo orfano per verificare la presenza di errori evidenti o messaggi relativi all'uscita imprevista.
2. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
3. Tentare di riavviare il nodo eseguendo il seguente comando: `$ sudo storagegrid node start node-name`

```
$ sudo storagegrid node start DC1-S1-172-16-1-172
```

Se il nodo è orfano, la risposta è

```
Not starting ORPHANED node DC1-S1-172-16-1-172
```

4. Da Linux, arrestare il motore dei container e qualsiasi processo di controllo del nodo storagegrid. Ad esempio: `sudo docker stop --time secondscontainer-name`

Per `seconds`, immettere il numero di secondi che si desidera attendere per l'arresto del contenitore (in genere 15 minuti o meno). Ad esempio:

```
sudo docker stop --time 900 storagegrid-DC1-S1-172-16-1-172
```

5. Riavviare il nodo: `storagegrid node start node-name`

```
storagegrid node start DC1-S1-172-16-1-172
```

Linux: Risoluzione dei problemi relativi al supporto IPv6

Potrebbe essere necessario abilitare il supporto IPv6 nel kernel se sono stati installati nodi StorageGRID su host Linux e si nota che gli indirizzi IPv6 non sono stati assegnati ai contenitori di nodi come previsto.

A proposito di questa attività

Per visualizzare l'indirizzo IPv6 assegnato a un nodo 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 questa procedura per abilitare il supporto IPv6 nel kernel.

Fasi

1. Accedere all'host come root o utilizzando un account con autorizzazione sudo.
2. Eseguire il seguente comando: `sysctl net.ipv6.conf.all.disable_ipv6`

```
root@SG:~ # sysctl net.ipv6.conf.all.disable_ipv6
```

Il risultato deve essere 0.

```
net.ipv6.conf.all.disable_ipv6 = 0
```



Se il risultato non è 0, consultare la documentazione del sistema operativo per modificare `sysctl` le impostazioni. Quindi, modificare il valore su 0 prima di continuare.

3. Inserisci il 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 deve essere 1.

```
net.ipv6.conf.all.disable_ipv6 = 1
```



Se il risultato non è 1, questa procedura non si applica. Contattare il supporto tecnico.

5. Uscire dal contenitore: `exit`

```
root@DC1-S1:~ # exit
```

6. Come root, modificare il seguente file: `/var/lib/storagegrid/settings/sysctl.d/net.conf`.

```
sudo vi /var/lib/storagegrid/settings/sysctl.d/net.conf
```

7. Individuare le due righe seguenti e rimuovere i tag di commento. Quindi, salvare e chiudere il file.

```
net.ipv6.conf.all.disable_ipv6 = 0
```

```
net.ipv6.conf.default.disable_ipv6 = 0
```

8. Eseguire questi comandi per riavviare il container StorageGRID:

```
storagegrid node stop node-name
```

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

Risoluzione dei problemi dei messaggi di errore del server syslog esterno per StorageGRID

La tabella seguente descrive i messaggi di errore che potrebbero essere correlati a un server syslog esterno ed elenca le azioni correttive.

Questi errori vengono visualizzati dalla procedura guidata Configura server syslog esterno se si verificano problemi durante l'invio di messaggi di prova per convalidare la corretta configurazione del server syslog esterno.

Problemi in fase di esecuzione potrebbero essere segnalati dal "[Errore di inoltro del server syslog esterno](#)" allerta. Se ricevi questo avviso, segui le istruzioni contenute nell'avviso per inviare nuovamente i messaggi di prova e ottenere messaggi di errore dettagliati.

Per ulteriori informazioni sull'invio di informazioni di audit a un server syslog esterno, consultare:

- "[Considerazioni sull'utilizzo di un server syslog esterno](#)"
- "[Configurare la gestione dei log e il server syslog esterno](#)"

Messaggio di errore	Descrizione e azioni consigliate
Impossibile risolvere il nome host	Impossibile risolvere l'FQDN immesso per il server syslog in un indirizzo IP. 1. Controllare il nome host immesso. Se è stato immesso un indirizzo IP, assicurarsi che sia un indirizzo IP valido con la notazione W.X.Y.Z ("decimale separato da punti"). 2. Verificare che i server DNS siano configurati correttamente. 3. Verificare che ciascun nodo possa accedere agli indirizzi IP del server DNS.
Connessione rifiutata	Una connessione TCP o TLS al server syslog è stata rifiutata. Sulla porta TCP o TLS dell'host potrebbe non essere presente alcun servizio o un firewall potrebbe bloccare l'accesso. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Verificare che l'host del servizio syslog stia eseguendo un daemon syslog in attesa sulla porta specificata. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi all'IP e alla porta del server syslog.
Rete non raggiungibile	Il server syslog non si trova su una subnet collegata direttamente. Un router ha restituito un messaggio di errore ICMP per indicare che non è stato possibile inoltrare i messaggi di test dai nodi elencati al server syslog. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per instradare il traffico al server syslog attraverso l'interfaccia di rete e il gateway previsti (Grid, Admin o Client).
Host non raggiungibile	Il server syslog si trova su una subnet collegata direttamente (subnet utilizzata dai nodi elencati per gli indirizzi IP Grid, Admin o Client). I nodi hanno tentato di inviare messaggi di test, ma non hanno ricevuto risposte alle richieste ARP per l'indirizzo MAC del server syslog. 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Verificare che l'host che esegue il servizio syslog sia attivo.

Messaggio di errore	Descrizione e azioni consigliate
Timeout della connessione	È stato eseguito un tentativo di connessione TCP/TLS, ma non è stata ricevuta alcuna risposta dal server syslog per molto tempo. Potrebbe esserci un errore di configurazione del routing o un firewall potrebbe interrompere il traffico senza inviare alcuna risposta (una configurazione comune). 1. Verificare di aver immesso l'FQDN o l'indirizzo IP corretto per il server syslog. 2. Per ciascun nodo elencato, selezionare Grid Network Subnet List (elenco subnet rete griglia), Admin Networks Subnet Lists (elenchi subnet reti amministrative) e Client Network Gateway (Gateway di rete client). Verificare che siano configurati per indirizzare il traffico al server syslog utilizzando l'interfaccia di rete e il gateway (Grid, Admin o Client) su cui si prevede di raggiungere il server syslog. 3. Verificare che un firewall non blocchi l'accesso alle connessioni TCP/TLS dai nodi elencati all'IP e alla porta del server syslog.
Connessione chiusa dal partner	Una connessione TCP al server syslog è stata stabilita correttamente, ma in seguito è stata chiusa. I motivi potrebbero includere: • Il server syslog potrebbe essere stato riavviato o riavviato. • Il nodo e il server syslog potrebbero avere impostazioni TCP/TLS diverse. • Un firewall intermedio potrebbe chiudere le connessioni TCP inattive. • Un server non syslog in ascolto sulla porta del server syslog potrebbe aver chiuso la connessione. Per risolvere questo problema: 1. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 2. Se si utilizza il protocollo TLS, verificare che anche il server syslog utilizzi il protocollo TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. 3. Verificare che un firewall intermedio non sia configurato per chiudere le connessioni TCP inattive.
Errore certificato TLS	Il certificato del server ricevuto dal server syslog non era compatibile con il bundle di certificati CA e con il certificato client forniti. 1. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server sul server syslog. 2. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Inoltro sospeso	I record syslog non vengono più inoltrati al server syslog e StorageGRID non è in grado di rilevare il motivo. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale.

Messaggio di errore	Descrizione e azioni consigliate
Sessione TLS terminata	Il server syslog ha terminato la sessione TLS e StorageGRID non è in grado di rilevare il motivo. 1. Esaminare i log di debug forniti con questo errore per cercare di determinare la causa principale. 2. Verificare di aver immesso l'FQDN o l'indirizzo IP, la porta e il protocollo corretti per il server syslog. 3. Se si utilizza il protocollo TLS, verificare che anche il server syslog utilizzi il protocollo TLS. Se si utilizza il protocollo TCP, verificare che anche il server syslog utilizzi il protocollo TCP. 4. Verificare che il bundle di certificati CA e il certificato client (se presente) siano compatibili con il certificato server dal server syslog. 5. Verificare che le identità nel certificato del server dal server syslog includano i valori IP o FQDN previsti.
Query dei risultati non riuscita	Il nodo di amministrazione utilizzato per la configurazione e il test del server syslog non è in grado di richiedere i risultati del test dai nodi elencati. Uno o più nodi potrebbero non essere attivi. 1. Seguire le procedure standard per la risoluzione dei problemi per assicurarsi che i nodi siano online e che tutti i servizi previsti siano in esecuzione. 2. Riavviare il servizio miscd sui nodi elencati.

Scopri i problemi di memorizzazione nella cache del bilanciatore del carico in StorageGRID

Scopri i possibili problemi con la memorizzazione nella cache del bilanciatore del carico e come risolverli.

Determina se una richiesta è stata un hit della cache

- L'intestazione X-Cache viene impostata nella risposta alle richieste gestite dal servizio cache. Codici possibili:
 - HIT: L'oggetto è stato servito dalla cache
 - PARTIAL-HIT: Il bucket/chiave aveva un record nella cache, ma non tutto l'intervallo richiesto poteva essere servito dalla cache
 - STALE: Il bucket/chiave aveva un record nella cache, ma l'oggetto è stato aggiornato dall'ultima volta che è stato servito dalla cache.
 - MISS: L'oggetto non era nella cache
- IL `nginx-gw/endpoint-access.log.gz` il record per la richiesta include "unix:/run/cache-svc/cache-svc.sock" per le richieste gestite dalla cache.
- IL `cache-svc/cache-svc.log` segnala un messaggio del tipo "Richiesta 320390: completata con successo (cache hit)" o "Richiesta 320375: completata con successo (cache miss)." Trova il percorso richiesto cercando altri record con la stessa stringa "Request <number>".

Basso tasso di hit della cache

- Potrebbero verificarsi bassi tassi di hit della cache quando viene aggiunto un nuovo carico di lavoro o quando cambia il set di lavoro a cui accede un carico di lavoro. In queste situazioni, si prevede che il tasso di successo aumenterà nel tempo.
- Se più carichi di lavoro utilizzano la memorizzazione nella cache, valutare l'aggiunta di criteri di classificazione del traffico per isolare parti dei carichi di lavoro gestiti dalla cache. Le metriche relative al tasso di successo della cache sono disponibili in base ai criteri di classificazione del traffico. Se alcuni carichi di lavoro non riscontrano buoni tassi di successo nella cache, si consiglia di spostare tali carichi di lavoro su altri endpoint che non hanno la memorizzazione nella cache abilitata.
- Valutare la frequenza di espulsione della cache. Se la cache è troppo piccola per contenere il working set, si verificheranno alti tassi di espulsione e ciò potrebbe contribuire a ridurre i tassi di successo.
- Con FPVR potrebbero essere disponibili opzioni per migliorare i tassi di successo di determinati carichi di lavoro.

Bassa prestazione

- Valutare il tasso di successo della cache. Bassi tassi di hit della cache possono comportare scarse prestazioni complessive.
- Valutare la frequenza di espulsione della cache. Durante l'espulsione, alcune risorse di archiviazione vengono utilizzate per rimuovere oggetti esistenti dal disco. Se il processo di espulsione non tiene il passo con l'accesso di nuovi oggetti, il sistema potrebbe raggiungere le soglie di hard watermark e iniziare a bypassare la cache.
- Verificare i limiti di rete utilizzando le diagnosi "Utilizzo ricezione interfacce di rete" e "Utilizzo trasmissione interfacce di rete".

Esaminare i registri di audit

Messaggi e registri di controllo

Queste istruzioni contengono informazioni sulla struttura e sul contenuto dei messaggi di audit e dei registri di audit di StorageGRID. È possibile utilizzare queste informazioni per leggere e analizzare il registro di controllo dell'attività del sistema.

Queste istruzioni sono destinate agli amministratori responsabili della produzione di report sull'attività e sull'utilizzo del sistema che richiedono l'analisi dei messaggi di audit del sistema StorageGRID.

Per utilizzare il file di log di testo, è necessario disporre dell'accesso alla condivisione di audit configurata nel nodo di amministrazione.

Per informazioni sulla configurazione dei livelli dei messaggi di controllo e sull'utilizzo di un server syslog esterno, vedere ["Configurare la gestione dei log e il server syslog esterno"](#).

Come i messaggi di controllo si spostano attraverso il sistema StorageGRID nel file di log audit.log per la conservazione

Tutti i servizi StorageGRID generano messaggi di audit durante il normale funzionamento del sistema. È necessario comprendere in che modo questi messaggi di controllo passano dal sistema StorageGRID al `audit.log` file.

I seguenti flussi di lavoro per i messaggi di controllo e la conservazione dei messaggi di controllo sono applicabili solo se StorageGRID è configurato per **Nodi amministrativi/nodi locali** o **Nodo amministrativo e server syslog esterno**. Se StorageGRID è configurato per "Solo nodi locali" (predefinito) o "Server syslog esterno", i messaggi di controllo vengono salvati localmente su ciascun nodo nel `/var/local/log/localaudit.log` file e non può essere elaborato dai nodi di amministrazione o dai nodi di archiviazione.

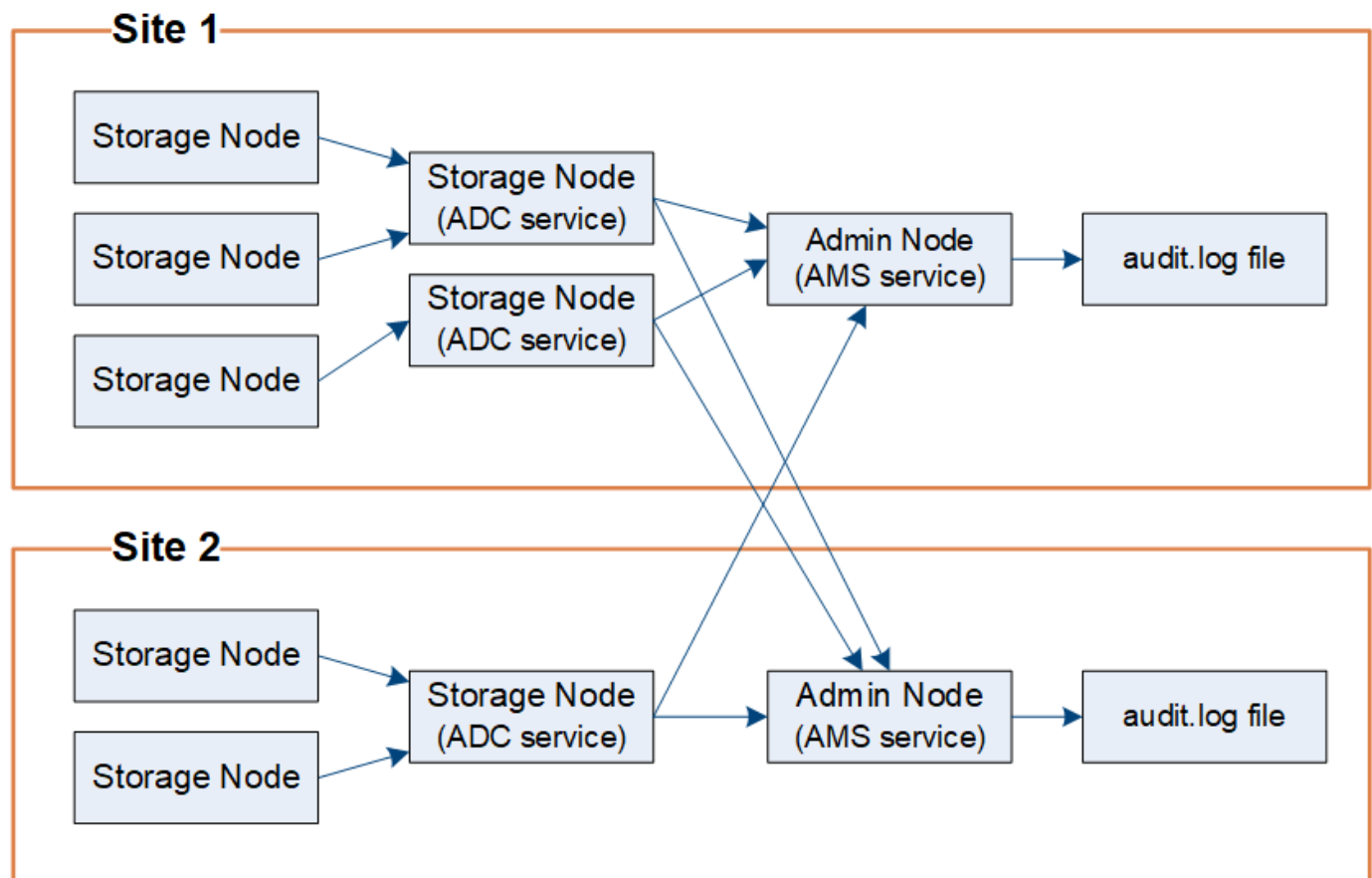
Controllare il flusso dei messaggi

I messaggi di controllo vengono elaborati dai nodi amministrativi quando StorageGRID è configurato per **nodi amministrativi/nodi locali** o **nodo amministrativo e server syslog esterno** e dai nodi di archiviazione che dispongono di un servizio di controller di dominio amministrativo (ADC).

Come mostrato nel diagramma di flusso dei messaggi di audit, ciascun nodo StorageGRID invia i propri messaggi di audit a uno dei servizi ADC nel sito del data center. Il servizio ADC viene attivato automaticamente per i primi tre nodi di storage installati in ogni sito.

A sua volta, ogni servizio ADC agisce come un relay e invia la propria raccolta di messaggi di audit a ogni nodo amministrativo nel sistema StorageGRID, che fornisce a ciascun nodo amministrativo un record completo dell'attività del sistema.

Ogni nodo amministrativo memorizza i messaggi di controllo in file di registro di testo; il file di registro attivo è denominato `audit.log`.

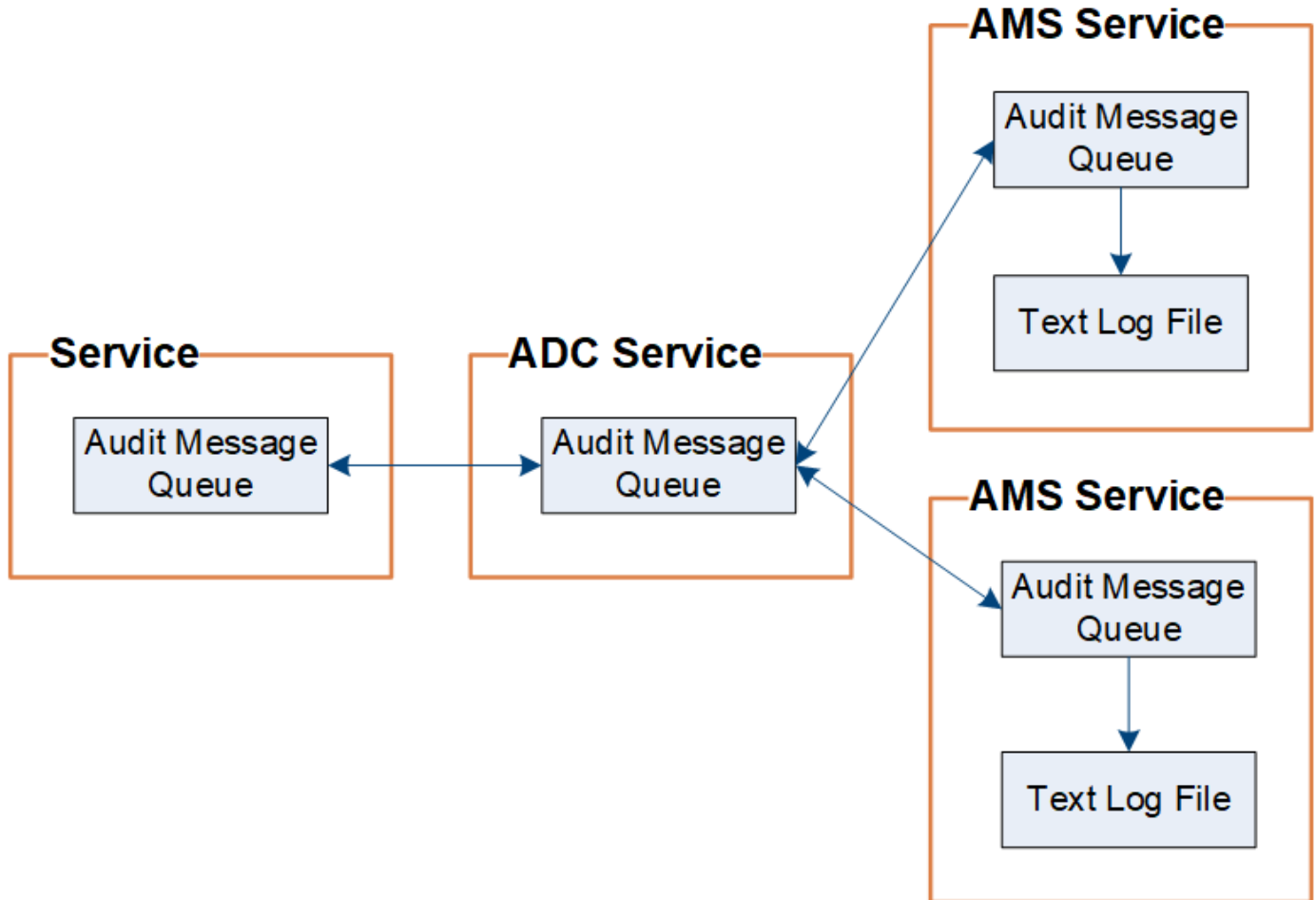


Controllare la conservazione dei messaggi

StorageGRID utilizza un processo di copia e cancellazione per garantire che non vengano persi messaggi di

controllo prima di poter essere scritti nel registro di controllo.

Quando un nodo genera o inoltra un messaggio di 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/audit/export` 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 danno priorità all'elaborazione del loro arretrato e diventano temporaneamente non disponibili per nuovi messaggi.

In particolare, potrebbero verificarsi i seguenti comportamenti:

- Se il `/var/local/audit/export` Quando la directory utilizzata da un nodo di amministrazione diventa piena, il nodo di amministrazione viene contrassegnato come non disponibile per nuovi messaggi di controllo finché la directory non è 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 viene contrassegnato come non disponibile per i messaggi di controllo finché la directory non è 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 vi sono nodi di archiviazione disponibili con il servizio ADC, i nodi di archiviazione memorizzano i messaggi di controllo localmente nel `/var/local/log/localaudit.log` file.

- Se il `/var/local/` directory utilizzata da un nodo di archiviazione diventa piena all'85%, il nodo inizia a rifiutare le richieste del client S3 con `503 Service Unavailable`.

I seguenti tipi di problemi possono causare un aumento delle code dei messaggi di audit:

- Interruzione di un nodo amministrativo o di un nodo di storage con il servizio ADC. Se uno dei nodi del sistema non è attivo, i nodi rimanenti potrebbero diventare backlogged.
- Tasso di attività sostenuta che supera la capacità di audit del sistema.
- Lo `/var/local/` spazio su un nodo di archiviazione ADC si riempie per motivi non correlati ai messaggi di controllo. In questo caso, il nodo smette di accettare nuovi messaggi di audit e assegna la priorità al backlog corrente, che può causare backlog su altri nodi.

Avviso di coda di audit estesa e allarme di messaggi di audit in coda (AMQS)

Per facilitare il monitoraggio delle dimensioni delle code dei messaggi di controllo nel tempo, l'avviso **Large audit queue** e l'allarme AMQS legacy vengono attivati quando il numero di messaggi in una coda Storage Node o Admin Node raggiunge determinate soglie.

Se viene attivato l'avviso **Large audit queue** o l'allarme AMQS legacy, iniziare controllando il carico sul sistema. Se si è verificato un numero significativo di transazioni recenti, l'avviso e l'allarme devono essere risolti nel tempo e possono essere ignorati.

Se l'avviso o l'allarme persiste e aumenta di 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 la gestione dei log e il server syslog esterno"](#).

Messaggi duplicati

Il sistema StorageGRID adotta un approccio conservativo in caso di guasto di rete o nodo. Per questo motivo, nel registro di controllo potrebbero essere presenti messaggi duplicati.

Accedi ai file di log di audit dalla riga di comando del nodo Admin di StorageGRID

La condivisione di controllo contiene il file attivo `audit.log` ed eventuali file di registro di controllo compressi. È possibile accedere ai file di log di controllo direttamente dalla riga di comando del nodo amministrativo.

IL `audit.log` il file rimane vuoto a meno che non si configuri StorageGRID per **Nodi amministrativi/nodi locali** o **Nodo amministrativo e server syslog esterno**. Per ulteriori informazioni, fare riferimento a ["Seleziona la posizione del registro"](#).

Prima di iniziare

- Si dispone di ["autorizzazioni di accesso specifiche"](#).
- È necessario disporre del `Passwords.txt` file.

- È necessario conoscere l'indirizzo IP di un nodo amministratore.

Fasi

1. Accedere a un nodo amministratore:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Accedere alla directory contenente i file di log di controllo:

```
cd /var/local/audit/export/
```

3. Visualizzare il file di log di audit corrente o salvato, secondo necessità.

Scopri la rotazione dei file di log di audit in StorageGRID

Se StorageGRID è configurato per **Nodi amministrativi/nodi locali** o **Nodo amministrativo e server syslog esterno**, i file dei registri di controllo vengono salvati nel nodo amministrativo `/var/local/audit/export/` 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. Fare riferimento a ["Configurare i messaggi di controllo e il server syslog esterno"](#).

Una volta al giorno, il file attivo `audit.log` viene salvato e viene avviato un nuovo `audit.log` file. Il nome del file salvato indica quando è stato salvato, nel formato `yyyy-mm-dd.txt`. Se in un solo giorno vengono creati più log di controllo, i nomi dei file utilizzano la data in cui il file è stato salvato, seguita da un numero, nel formato `yyyy-mm-dd.txt.n`. Ad esempio, `2018-04-15.txt` e `2018-04-15.txt.1` sono il primo e il secondo file di 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, lo spazio di archiviazione del nodo di amministrazione assegnato ai registri di controllo viene consumato. 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/audit/export/` elenco. I registri di controllo vengono eliminati in base alla data in cui sono stati creati. I registri più vecchi vengono eliminati per primi. È possibile monitorare le azioni dello script nel seguente file: `/var/local/log/manage-audit.log`.

Questo esempio mostra il file attivo `audit.log`, il file del giorno precedente (`2018-04-15.txt`) e il file compresso per il giorno precedente (`2018-04-14.txt.gz`).


```
audit.log
2018-04-15.txt
2018-04-14.txt.gz
```

Formato del file di log di audit

Scopri il formato dei file di log di audit in StorageGRID

I file di log di audit si trovano in ogni nodo di amministrazione e contengono una raccolta di singoli messaggi di audit.

Ogni messaggio di audit contiene quanto segue:

- Il tempo universale coordinato (UTC) dell'evento che ha attivato il messaggio di audit (ATIM) in formato ISO 8601, seguito da uno spazio:

YYYY-MM-DDTHH:MM:SS.UUUUUU, dove *UUUUUU* sono microsecondi.

- Il messaggio di verifica stesso, racchiuso tra parentesi quadre e che inizia con `AUDT`.

L'esempio seguente mostra tre messaggi di audit in un file di log di audit (interruzioni di riga aggiunte per la leggibilità). Questi messaggi sono stati generati quando un tenant ha creato un bucket S3 e aggiunto due oggetti a tale bucket.

2019-08-07T18:43:30.247711

```
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1565149504991681][TIME(UI64):73520][SAI
P(IPAD):"10.224.2.255"][S3AI(CSTR):"17530064241597054718"]
[SACC(CSTR):"s3tenant"][S3AK(CSTR):"SGKH9100SCkNB8M3MTWNt-
PhoTDwB9JOk7PtyLkQmA=="][SUSR(CSTR):"urn:sgws:identity::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][SA
IP(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][SA
IP(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 audit nei file di log di audit non sono facili da leggere o interpretare. È possibile utilizzare ["tool di verifica-spiegazione"](#) per ottenere riepiloghi semplificati dei messaggi di controllo nel registro di controllo. È possibile utilizzare ["tool audit-sum"](#) per riepilogare il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo impiegato da tali operazioni.

Utilizzare lo strumento audit-explain per tradurre i messaggi di audit di StorageGRID

È possibile utilizzare `audit-explain` lo strumento per convertire i messaggi di controllo nel registro di controllo in un formato di facile lettura.

Prima di iniziare

- Si dispone di "autorizzazioni di accesso specifiche".
- È necessario disporre del `Passwords.txt` file.
- È necessario conoscere l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

``audit-explain`` Lo strumento, disponibile sul nodo amministrativo principale, fornisce riepiloghi semplificati dei messaggi di controllo in un registro di controllo.



`audit-explain`` Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Le query di elaborazione ``audit-explain`` possono consumare una grande quantità di potenza della CPU, che potrebbe avere un impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico `audit-explain` dello strumento. Questi quattro "SPUT" messaggi di controllo sono stati generati quando il tenant S3 con ID account 92484777680322627870 utilizzava S3 richieste PUT per creare un bucket denominato "bucket1" e aggiungere tre oggetti a quel bucket.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

Lo `audit-explain` strumento può effettuare le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Elaborazione simultanea di più file. Ad esempio:

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/audit/export/*
```

- Accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o altri mezzi. Ad 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 eseguire `audit-explain` sulle parti, anziché sull'intero file.



``audit-explain`` Lo strumento non accetta file compressi come input di pipeline. Per elaborare i file compressi, fornire i nomi dei file come argomenti della riga di comando o utilizzare ``zcat`` lo strumento per decomprimere prima i file. Ad esempio:

```
zcat audit.log.gz | audit-explain
```

Utilizzare l' ``help (-h)`` opzione per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-explain -h
```

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

```
$ audit-explain /var/local/audit/export/audit.log
```

``audit-explain`` Lo strumento stampa interpretazioni leggibili di tutti i messaggi nel file o nei file specificati.



Per ridurre le lunghezze delle linee e agevolare la leggibilità, i timestamp non vengono visualizzati per impostazione predefinita. Se si desidera visualizzare i timestamp, utilizzare l' `(-t`` opzione timestamp).

Utilizzare lo strumento `audit-sum` per riepilogare i messaggi di audit di StorageGRID

È possibile utilizzare `audit-sum` lo strumento per contare i messaggi di controllo di scrittura, lettura, testa ed eliminazione e per visualizzare il tempo (o le dimensioni) minimo, massimo e medio per ogni tipo di operazione.

Prima di iniziare

- Si dispone di "autorizzazioni di accesso specifiche".
- Si dispone del `Passwords.txt` file.
- Si conosce l'indirizzo IP del nodo di amministrazione primario.

A proposito di questa attività

``audit-sum`` Lo strumento, disponibile nel nodo amministrativo principale, riepiloga il numero di operazioni di scrittura, lettura ed eliminazione registrate e il tempo necessario per tali operazioni.



`audit-sum`` Lo strumento è destinato principalmente all'uso da parte del supporto tecnico durante le operazioni di risoluzione dei problemi. Le query di elaborazione ``audit-sum`` possono consumare una grande quantità di potenza della CPU, che potrebbe avere un impatto sulle operazioni StorageGRID.

Questo esempio mostra l'output tipico `audit-sum` dello strumento. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

IL `audit-sum` Lo strumento fornisce conteggi e orari per i seguenti messaggi di controllo S3 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 precedenti StorageGRID . Ad esempio, ["StorageGRID 11.8 Utilizzo dello strumento di somma di controllo"](#) .

Codice	Descrizione	Fare riferimento a.
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Registra quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"

Codice	Descrizione	Fare riferimento a.
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket.	"SDEL: ELIMINAZIONE S3"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket.	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	"SHEA: TESTA S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket.	"SPUT: S3 PUT"

Lo `audit-sum` strumento può effettuare le seguenti operazioni:

- Elaborazione di registri di audit semplici o compressi. Ad esempio:

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Elaborazione simultanea di più file. Ad esempio:

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/audit/export/*
```

- Accettare l'input da una pipe, che consente di filtrare e pre-elaborare l'input utilizzando il `grep` comando o altri mezzi. Ad esempio:

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```



Questo strumento non accetta 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 o per raggruppare i riepiloghi dei messaggi in base al nome del bucket, al periodo di tempo o al tipo di destinazione. Per impostazione predefinita, i riepiloghi mostrano il tempo di funzionamento minimo, massimo e medio, ma è possibile utilizzare l' ``size (-s)`` opzione per esaminare le dimensioni dell'oggetto.

Utilizzare l' `'help (-h)'` opzione per visualizzare le opzioni disponibili. Ad esempio:

```
$ audit-sum -h
```

Fasi

1. Accedere al nodo di amministrazione principale:

- Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Se si desidera analizzare tutti i messaggi relativi alle operazioni di scrittura, lettura, testa ed eliminazione, attenersi alla seguente procedura:

- Immettere il seguente comando, dove `/var/local/audit/export/audit.log` rappresenta il nome e la posizione del file o dei file che si desidera analizzare:

```
$ audit-sum /var/local/audit/export/audit.log
```

Questo esempio mostra l'output tipico `audit-sum` dello strumento. Questo esempio mostra il tempo impiegato dalle operazioni del protocollo.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

In questo esempio, le operazioni SGET (S3 GET) sono le più lente in media a 1.13 secondi, ma le operazioni SGET e SPUT (S3 PUT) mostrano tempi lunghi nel caso peggiore di circa 1,770 secondi.

- Per visualizzare le operazioni di recupero 10 più lente, utilizzare il comando `grep` per selezionare solo i messaggi SGET e aggiungere l'opzione di output lungo (`-l`) per includere i percorsi oggetto:

```
grep SGET audit.log | audit-sum -l
```

I risultati includono il tipo (oggetto o bucket) e il percorso, che consentono di eseguire il `grep` del log di audit per altri messaggi relativi a questi oggetti specifici.

```

Total:          201906 operations
Slowest:        1740.290 sec
Average:        1.132 sec
Fastest:        0.010 sec
Slowest operations:
      time(usec)      source ip      type      size(B) path
      =====
      1740289662    10.96.101.125      object    5663711385
backup/r9010aQ8JB-1566861764-4519.iso
      1624414429    10.96.101.125      object    5375001556
backup/r9010aQ8JB-1566861764-6618.iso
      1533143793    10.96.101.125      object    5183661466
backup/r9010aQ8JB-1566861764-4518.iso
           70839    10.96.101.125      object         28338
bucket3/dat.1566861764-6619
           68487    10.96.101.125      object         27890
bucket3/dat.1566861764-6615
           67798    10.96.101.125      object         27671
bucket5/dat.1566861764-6617
           67027    10.96.101.125      object         27230
bucket5/dat.1566861764-4517
           60922    10.96.101.125      object         26118
bucket3/dat.1566861764-4520
           35588    10.96.101.125      object         11311
bucket3/dat.1566861764-6616
           23897    10.96.101.125      object         10692
bucket3/dat.1566861764-4516

```

+

Da questo esempio di output, è possibile notare che le tre richieste S3 GET più lente erano per oggetti di dimensioni pari a circa 5 GB, che sono molto più grandi degli altri oggetti. Le grandi dimensioni rappresentano i tempi di recupero lenti dei casi peggiori.

3. Per determinare le dimensioni degli oggetti inseriti e recuperati dalla griglia, utilizzare l'opzione dimensioni (-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 degli oggetti per SPUT è inferiore a 2.5 MB, ma la dimensione media per SGET è molto maggiore. Il numero di messaggi SPUT è molto superiore al numero di messaggi SGET, a indicare che la maggior parte degli oggetti non viene mai recuperata.

4. Se si desidera determinare se i recuperi sono stati lenti ieri:

- a. Immettere il comando nel registro di controllo appropriato e utilizzare l'opzione Group-by-Time (-gt), seguita 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. Sia i tempi massimi che quelli medi sono considerevolmente più alti durante questo intervallo di tempo e non aumentano gradualmente con l'aumentare del conteggio. Questi parametri suggeriscono che la capacità è stata superata, probabilmente nella rete o nella capacità della griglia di elaborare le richieste.

- b. Per determinare le dimensioni degli oggetti recuperati ogni ora ieri, aggiungere l'opzione size (-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 si sono verificati alcuni recuperi molto grandi quando il traffico di recupero complessivo era al massimo.

- c. Per ulteriori dettagli, utilizzare il ["tool di verifica-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 costituito da molte righe, aggiungere il `less` comando per visualizzare 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 per gli oggetti:

- a. Iniziare utilizzando l' ``-go`` opzione, che raggruppa i messaggi per le operazioni di oggetti e bucket separatamente:

```
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 hanno caratteristiche di performance diverse rispetto alle operazioni SPUT per gli oggetti.

- b. Per determinare quali bucket hanno le operazioni SPUT più lente, utilizzare `-gb` l'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.ldt002 0.361	1564563	0.011	51.569

- c. Per determinare quali bucket hanno la dimensione massima dell'oggetto SPUT, utilizzare sia le `-gb` opzioni e `-s`:

```
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.ltd002 0.352	1564563	0.000	999.972

Formato del messaggio di audit

Scopri la struttura dei messaggi di audit di StorageGRID

I messaggi di audit scambiati all'interno del sistema StorageGRID includono informazioni standard comuni a tutti i messaggi e contenuti specifici che descrivono l'evento o l'attività da segnalare.

Se le informazioni di riepilogo fornite dagli ["audit-spiegare"](#) strumenti e ["audit-sum"](#) non sono sufficienti, fare riferimento a questa sezione per comprendere il formato generale di tutti i messaggi di controllo.

Di seguito viene riportato un esempio di messaggio di audit che potrebbe essere visualizzato nel file di log dell'audit:

```
2014-07-17T03:50:47.484627
[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP(FC32):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):9445736326500603516]]
```

Ogni messaggio di audit 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 []
- Introdotta 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 di attributo, un tipo di dati e un valore che vengono riportati in questo formato:

```
[ATTR (type) :value] [ATTR (type) :value] ...  
[ATTR (type) :value] \n
```

Il numero di elementi di attributo nel messaggio dipende dal tipo di evento del messaggio. Gli elementi dell'attributo non sono elencati in un ordine specifico.

L'elenco seguente descrive gli elementi degli attributi:

- **ATTR** è un codice di quattro caratteri per l'attributo riportato. Esistono alcuni attributi comuni a tutti i messaggi di audit e ad altri specifici degli eventi.
- **type** È un identificatore di quattro caratteri del tipo di dati di programmazione del valore, come 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 nei messaggi di controllo StorageGRID

Per memorizzare le informazioni nei messaggi di audit vengono utilizzati diversi tipi di dati.

Tipo	Descrizione
UI32	Intero senza segno (32 bit); può memorizzare i numeri da 0 a 4,294,967,295.
UI64	Numero intero doppio senza segno (64 bit); può memorizzare i numeri da 0 a 18,446,744,073,709,551,615.
FC32	Costante di quattro caratteri; un valore intero senza segno a 32 bit rappresentato da quattro caratteri ASCII, ad esempio "ABCD".
IPAD	Utilizzato per gli indirizzi IP.
CSTR	Matrice a lunghezza variabile di caratteri UTF-8. È possibile eseguire l'escape dei caratteri con le seguenti convenzioni: • La barra rovesciata è • Il ritorno a capo è • Le virgolette doppie sono " . • L'avanzamento riga (nuova riga) è il n. • I caratteri possono essere sostituiti dai rispettivi equivalenti esadecimali (nel formato HH, dove HH è il valore esadecimale che rappresenta il carattere).

Dati specifici dell'evento nei messaggi di audit di StorageGRID

Ogni messaggio di audit nel registro di audit registra i dati specifici di un evento di sistema.

Dopo il contenitore di apertura [AUDT: che identifica il messaggio stesso, il successivo insieme di attributi fornisce informazioni sull'evento o sull'azione descritti 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\):"60025
621595611246499"\]
\[SACC\ (CSTR\):"account"\]\[S3AK\ (CSTR\):"SGKH4_Nc8SO1H6w3w0nCOFCGgk__E6dY
zKlumRsKJA=="\]
\[SUSR\ (CSTR\):"urn:sgws:identity:60025621595611246499:root"\]
\[SBAI\ (CSTR\):"60025621595611246499"\]\[SBAC\ (CSTR\):"account"\]\[S3BK\ (C
STR\):"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] [A
MID(FC32):S3RQ]
\[ATID(UI64):15552417629170647261\]
```

L'`ATYP`elemento (sottolineato nell'esempio) identifica l'evento che ha generato il messaggio. Questo messaggio di esempio include il "SHEA"codice del messaggio ([ATYP(FC32):SHEA]), che indica che è stato generato da una richiesta di S3 TESTINE riuscita.

Elementi comuni nei messaggi di audit di StorageGRID

Tutti i messaggi di audit contengono gli elementi comuni.

Codice	Tipo	Descrizione
IN MEZZO	FC32	Module ID (ID modulo): Identificatore di quattro caratteri dell'ID modulo che ha generato il messaggio. Indica il segmento di codice all'interno del quale è stato generato il messaggio di audit.
ANID	UI32	Node ID (ID nodo): L'ID del nodo della griglia assegnato al servizio che ha generato il messaggio. A ciascun servizio viene assegnato un identificatore univoco al momento della configurazione e dell'installazione del sistema StorageGRID. Impossibile modificare questo ID.
ASE	UI64	Audit Session Identifier (identificatore sessione di audit): Nelle release precedenti, questo elemento indica l'ora in cui il sistema di audit è stato inizializzato dopo l'avvio del servizio. Questo valore di tempo è stato misurato in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Nota: questo elemento è obsoleto e non compare più nei messaggi di audit.

Codice	Tipo	Descrizione
ASQN	UI64	Sequence Count (Conteggio sequenze): Nelle release precedenti, questo contatore è stato incrementato per ogni messaggio di audit generato sul nodo della griglia (ANID) e azzerato al riavvio del servizio. Nota: questo elemento è obsoleto e non compare più nei messaggi di audit.
ATID	UI64	Trace ID (ID traccia): Identificatore condiviso dalla serie di messaggi attivati da un singolo evento.
ATIM	UI64	Timestamp: L'ora in cui è stato generato l'evento che ha attivato il messaggio di audit, misurata in microsecondi dall'epoca del sistema operativo (00:00:00 UTC del 1° gennaio 1970). Si noti che la maggior parte degli strumenti disponibili per la conversione dell'indicatore data e ora in data e ora locali si basano su millisecondi. Potrebbe essere richiesto l'arrotondamento o il troncamento dell'indicatore data e ora registrato. L'ora leggibile dall'uomo che appare all'inizio del messaggio di controllo nel <code>audit.log</code> file è l'attributo ATIM in formato ISO 8601. La data e l'ora sono rappresentate come <code>YYYY-MMDDTHH:MM:SS.UUUUUU</code> , dove T è un carattere stringa letterale che indica l'inizio del segmento temporale della data. <code>UUUUUU</code> sono microsecondi.
ATYP	FC32	Event Type (tipo di evento): Identificatore di quattro caratteri dell'evento registrato. Questo regola il contenuto "payload" del messaggio: Gli attributi che sono inclusi.
MEDIA	UI32	Version (versione): La versione del messaggio di audit. Man mano che il software StorageGRID si evolve, le nuove versioni dei servizi potrebbero incorporare nuove funzionalità nei report di audit. Questo campo consente la compatibilità con le versioni precedenti del servizio AMS per l'elaborazione dei messaggi provenienti da versioni precedenti dei servizi.
RSLT	FC32	Risultato: Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

Formato ed esempi del messaggio di audit StorageGRID

È possibile trovare informazioni dettagliate in ciascun messaggio di audit. Tutti i messaggi di audit utilizzano lo stesso formato.

Di seguito è riportato un esempio di messaggio di controllo che potrebbe essere visualizzato 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 audit contiene informazioni sull'evento registrato, nonché informazioni sul messaggio di audit stesso.

Per identificare l'evento registrato dal messaggio di audit, cercare l'attributo ATYP (evidenziato di seguito):

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK(CSTR):"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 PUT S3 KB, che registra l'acquisizione di un oggetto in un bucket.

Il seguente messaggio di audit mostra anche il bucket a cui è associato l'oggetto:

```
2014-07-17T21:17:58.959669
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"bc644d
381a87d6cc216adcd963fb6f95dd25a38aa2cb8c9a358e8c5087a6af5f"] [
S3AK(CSTR):"UJXDKKQOXB7YARDS71Q2"] [S3BK\ (CSTR\): "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, prendere nota dell'indicatore orario UTC (Universal Coordinated Time) all'inizio del messaggio di audit. Questo valore è una versione leggibile dell'attributo ATIM del messaggio di audit stesso:

2014-07-17T21:17:58.959669

```
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):246979][S3AI(CSTR):"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, dall'inizio dell'epoca UNIX. Nell'esempio, il valore 1405631878959669 viene convertito in giovedì, 17-lug-2014 21:17:59:00 UTC.

Messaggi di audit e ciclo di vita degli oggetti

Quando i messaggi di audit vengono generati in StorageGRID

I messaggi di audit vengono generati ogni volta che un oggetto viene acquisito, recuperato o eliminato. È possibile identificare queste transazioni nel registro di controllo individuando i messaggi di controllo specifici di API S3.

I messaggi di audit sono collegati tramite identificatori specifici di ciascun protocollo.

Protocollo	Codice
Collegamento delle operazioni S3	S3BK (bucket), S3KY (chiave) o entrambi
Collegamento delle operazioni interne	CBID (identificatore interno dell'oggetto)

Tempistiche dei messaggi di audit

A causa di fattori come le differenze di tempo tra i nodi della griglia, le dimensioni degli oggetti e i ritardi di rete, l'ordine dei messaggi di controllo generati dai diversi servizi può variare rispetto a quello mostrato negli esempi di questa sezione.

Messaggi di audit per le transazioni di ingestione di oggetti in StorageGRID

Nell'audit log, puoi identificare le transazioni di acquisizione dei client individuando S3 messaggi di audit specifici di API.

Non tutti i messaggi di controllo generati durante una transazione di acquisizione sono elencati nella tabella seguente. Sono inclusi solo i messaggi necessari per tracciare la transazione di acquisizione.

S3: Acquisizione di messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SPUT	Transazione S3 PUT	Una transazione S3 PUT ingest è stata completata correttamente.	CBID, S3BK, S3KY	"SPUT: S3 PUT"
ORLM	Regole oggetto soddisfatte	Il criterio ILM è stato soddisfatto per questo oggetto.	CBID	"ORLM: Regole oggetto soddisfatte"

Esempio: Acquisizione di oggetti S3

La serie di messaggi di controllo riportata di seguito è un esempio dei messaggi di controllo generati e salvati nel registro di controllo quando un client S3 acquisisce un oggetto in un nodo di storage (servizio LDR).

In questo esempio, il criterio ILM attivo include la regola ILM Make 2 Copies.



Non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di acquisizione S3 (SPUT).

Questo esempio presuppone che sia stato precedentemente creato un bucket S3.

SPUT: S3 PUT

Il messaggio SPUT viene generato per indicare che è stata emessa una transazione S3 PUT per creare un oggetto in un bucket specifico.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):25771][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHya1RU_5cLflqajtaFmxJn946lAWRJfBF33gAOg=="][SUSR(CSTR):"urn:sgws:i
dentity::70899244468554783528:root"][SBAI(CSTR):"70899244468554783528"][SB
AC(CSTR):"test"][S3BK(CSTR):"example"][S3KY(CSTR):"testobject-0-
3"][CBID(UI64):0x8EF52DF8025E63A8][CSIZ(UI64):30720][AVER(UI32):10][ATIM
(UI64):150032627859669][ATYP(FC32):SPUT][ANID(UI32):12086324][AMID(FC32)
:S3RQ][ATID(UI64):14399932238768197038]]
```

ORLM: Regole oggetto soddisfatte

Il messaggio ORLM indica che il criterio ILM è stato soddisfatto per questo oggetto. Il messaggio include il CBID dell'oggetto e il nome della regola ILM applicata.

Per gli oggetti replicati, il campo LOCS include l'ID del nodo LDR e l'ID del volume delle posizioni degli oggetti.

2019-07-

```
17T21:18:31.230669[AUDT:[CBID(UI64):0x50C4F7AC2BC8EDF7][RULE(CSTR):"Make
2 Copies"]][STAT(FC32):DONE][CSIZ(UI64):0][UUID(CSTR):"0B344E18-98ED-4F22-
A6C8-A93ED68F8D3F"]][LOCS(CSTR):"CLDI 12828634 2148730112, CLDI 12745543
2147552014"]][RSLT(FC32):SUCS][AVER(UI32):10][ATYP(FC32):ORLM][ATIM(UI64)
:1563398230669][ATID(UI64):15494889725796157557][ANID(UI32):13100453][AMID
(FC32):BCMS]]
```

Per gli oggetti sottoposti a erasure coding, il campo LOCS include l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding

2019-02-23T01:52:54.647537

```
[AUDT:[CBID(UI64):0xFA8ABE5B5001F7E2][RULE(CSTR):"EC_2_plus_1"]][STAT(FC32)
:DONE][CSIZ(UI64):10000][UUID(CSTR):"E291E456-D11A-4701-8F51-
D2F7CC9AFECA"]][LOCS(CSTR):"CLEC 1 A471E45D-A400-47C7-86AC-
12E77F229831"]][RSLT(FC32):SUCS][AVER(UI32):10][ATIM(UI64):1550929974537]\[
ATYP(FC32):ORLM\][ANID(UI32):12355278][AMID(FC32):ILMX][ATID(UI64):41685
59046473725560]]
```

Il campo PATH include informazioni sul bucket S3 e sulla chiave.

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]]
```

Messaggi di audit per le transazioni di eliminazione degli oggetti in StorageGRID

È possibile identificare le transazioni di eliminazione degli oggetti nel registro di controllo individuando i messaggi di audit S3 specifici per API.

Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nelle tabelle seguenti. Sono inclusi solo i messaggi necessari per tracciare la transazione di eliminazione.

S3 eliminare i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SDEL	S3 Elimina	Richiesta di eliminazione dell'oggetto da un bucket.	CBID, S3KY	"SDEL: ELIMINAZIONE S3"

Esempio: Eliminazione di oggetti S3

Quando un client S3 elimina un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio di audit e salvato nel registro di audit.



Non tutti i messaggi di audit generati durante una transazione di eliminazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di eliminazione S3 (SDEL).

SDEL: S3 Elimina

L'eliminazione degli oggetti ha inizio quando il client invia una richiesta DeleteObject a un servizio LDR. Il messaggio contiene il bucket da cui eliminare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificare l'oggetto.

```
2017-07-
17T21:17:58.959669[AUDT:[RSLT(FC32):SUCS][TIME(UI64):14316][SAIP(IPAD):"10
.96.112.29"][S3AI(CSTR):"70899244468554783528"][SACC(CSTR):"test"][S3AK(CS
TR):"SGKHyaIRU_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]]
```

Messaggi di audit per le transazioni di recupero degli oggetti in StorageGRID

È possibile identificare le transazioni di recupero degli oggetti nel registro di controllo individuando i messaggi di audit S3 specifici per API.

Non tutti i messaggi di controllo generati durante una transazione di recupero sono elencati nella tabella seguente. Sono inclusi solo i messaggi necessari per tracciare la transazione di recupero.

Messaggi di controllo per il recupero S3

Codice	Nome	Descrizione	Traccia	Vedere
SGET	S3 GET	Richiesta di recupero di un oggetto da un bucket.	CBID, S3BK, S3KY	"SGET: S3 GET"

Esempio: Recupero di oggetti S3

Quando un client S3 recupera un oggetto da un nodo di storage (servizio LDR), viene generato un messaggio

di audit e salvato nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione di recupero S3 (SGET).

SGET: S3 GET

Il recupero degli oggetti ha inizio quando il client invia una richiesta GetObject a un servizio LDR. Il messaggio contiene il bucket da cui recuperare l'oggetto e la chiave S3 dell'oggetto, utilizzata per identificare l'oggetto.

```
2017-09-20T22:53:08.782605
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):47807][SAIP(IPAD):"10.96.112.26"][S3AI(
CSTR):"43979298178977966408"][SACC(CSTR):"s3-account-
a"][S3AK(CSTR):"SGKHt7GzEcu0yXhFhT_rL5mep4nJt1w75GBh-
O_FEW=="][SUSR(CSTR):"urn:sgws:identity::43979298178977966408:root"][SBAI(
CSTR):"43979298178977966408"][SBAC(CSTR):"s3-account-
a"]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02][CS
IZ(UI64):12][AVER(UI32):10][ATIM(UI64):1505947988782605]\[ATYP(FC32):SGE
T]\[ANID(UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):17742374343649889669]
]
```

Se la policy bucket lo consente, un client può recuperare in modo anonimo oggetti o recuperare oggetti da un bucket di proprietà di un account tenant diverso. Il messaggio di audit contiene informazioni sull'account tenant del proprietario del bucket, in modo da poter tenere traccia di queste richieste anonime e multiaccount.

Nel seguente messaggio di esempio, il client invia una richiesta GetObject per un oggetto memorizzato in un bucket che non possiede. I valori di SBAI e SBAC registrano l'ID e il nome dell'account tenant del bucket Owner, che differiscono dall'ID dell'account tenant e dal nome del client registrati in S3AI e SACC.

```
2017-09-20T22:53:15.876415
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):53244][SAIP(IPAD):"10.96.112.26"]\[S3AI
(CSTR):"17915054115450519830"]\[SACC(CSTR):"s3-account-
b"]\[S3AK(CSTR):"SGKHpoblWlP_kBkqSCbTi754Ls81BUog67I2L1SiUg=="][SUSR(CSTR)
:"urn:sgws:identity::17915054115450519830:root"]\[SBAI(CSTR):"4397929817
8977966408"]\[SBAC(CSTR):"s3-account-a"]\[S3BK(CSTR):"bucket-
anonymous"]\[S3KY(CSTR):"Hello.txt"]\[CBID(UI64):0x83D70C6F1F662B02][CSIZ(UI
64):12][AVER(UI32):10][ATIM(UI64):1505947995876415][ATYP(FC32):SGET][ANID(
UI32):12272050][AMID(FC32):S3RQ][ATID(UI64):6888780247515624902]]
```

Esempio: S3 selezionare su un oggetto

Quando un client S3 esegue una query S3 Select su un oggetto, i messaggi di audit vengono generati e salvati nel registro di audit.

Si noti che non tutti i messaggi di audit generati durante una transazione sono elencati nell'esempio seguente. Vengono elencati solo quelli relativi alla transazione S3 Select (SelectObjectContent).

Ogni query genera due messaggi di audit: Uno che esegue l'autorizzazione della richiesta S3 Select (il campo S3SR è impostato su "Select") e un'operazione GET standard successiva che recupera i dati dallo storage durante l'elaborazione.

```
2021-11-08T15:35:30.750038
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636385730715700][TIME(UI64):29173][SAI
P(IPAD):"192.168.7.44"][S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Ten
ant1636027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
entity::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBA
C(CSTR):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):0][S3SR(CSTR):"select"][AVER(UI32):10][ATIM(UI64
):1636385730750038][ATYP(FC32):SPOS][ANID(UI32):12601166][AMID(FC32):S3RQ]
[ATID(UI64):1363009709396895985]]
```

```
2021-11-08T15:35:32.604886
[AUDT:[RSLT(FC32):SUCS][CNID(UI64):1636383069486504][TIME(UI64):430690][SA
IP(IPAD):"192.168.7.44"][HTRH(CSTR):"{\"x-forwarded-
for\": \"unix:\"}"] [S3AI(CSTR):"63147909414576125820"][SACC(CSTR):"Tenant16
36027116"][S3AK(CSTR):"AUFD1XNVZ905F3TW7KSU"][SUSR(CSTR):"urn:sgws:identit
y::63147909414576125820:root"][SBAI(CSTR):"63147909414576125820"][SBAC(CST
R):"Tenant1636027116"][S3BK(CSTR):"619c0755-9e38-42e0-a614-
05064f74126d"][S3KY(CSTR):"SUB-
EST2020_ALL.csv"][CBID(UI64):0x0496F0408A721171][UUID(CSTR):"D64B1A4A-
9F01-4EE7-B133-
08842A099628"][CSIZ(UI64):10185581][MTME(UI64):1636380348695262][AVER(UI32
):10][ATIM(UI64):1636385732604886][ATYP(FC32):SGET][ANID(UI32):12733063][A
MID(FC32):S3RQ][ATID(UI64):16562288121152341130]]
```

Messaggi di controllo per gli aggiornamenti dei metadati degli oggetti S3 in StorageGRID

I messaggi di audit vengono generati quando un client S3 aggiorna i metadati di un oggetto.

I metadati S3 aggiornano i messaggi di audit

Codice	Nome	Descrizione	Traccia	Vedere
SUPD	Metadati S3 aggiornati	Generato quando un client S3 aggiorna i metadati di un oggetto acquisito.	CBID, S3KY, HTRH	"SUPD: Metadati S3 aggiornati"

Esempio: Aggiornamento dei metadati S3

L'esempio mostra una transazione riuscita per aggiornare i metadati di un oggetto S3 esistente.

SUPD: Aggiornamento dei metadati S3

Il client S3 effettua una richiesta (SUPD) per aggiornare i metadati specificati (`x-amz-meta-*`) per l'oggetto S3 (S3KY).

In questo esempio, le intestazioni della richiesta sono incluse nel campo HTRH perché è stato configurato come intestazione del protocollo di audit (**Configuration > Monitoring > Audit and syslog server**). Vedi ["Configurare la gestione dei log e il server syslog esterno"](#).

```
2017-07-11T21:54:03.157462
[AUDT:[RSLT(FC32):SUCS][TIME(UI64):17631][SAIP(IPAD):"10.96.100.254"]
[HTRH(CSTR):"{\"accept-encoding\": \"identity\", \"authorization\": \"AWS
LIUF17FGJARQHPY2E761:jul/hnZs/uNY+aVvV0lTSYhEGts=\",
\"content-length\": \"0\", \"date\": \"Tue, 11 Jul 2017 21:54:03
GMT\", \"host\": \"10.96.99.163:18082\",
\"user-agent\": \"aws-cli/1.9.20 Python/2.7.6 Linux/3.13.0-119-generic
botocore/1.3.20\",
\"x-amz-copy-source\": \"/testbkt1/testobj1\", \"x-amz-metadata-
directive\": \"REPLACE\", \"x-amz-meta-city\": \"Vancouver\"}"]
[S3AI(CSTR):"20956855414285633225"][SACC(CSTR):"acct1"][S3AK(CSTR):"SGKHyy
v9ZQqWRbJSQc5vI7mgioJwrdplShE02AUaww=="]
[SUSR(CSTR):"urn:sgws:identity::20956855414285633225:root"]
[SBAI(CSTR):"20956855414285633225"][SBAC(CSTR):"acct1"][S3BK(CSTR):"testbk
t1"]
[S3KY(CSTR):"testobj1"][CBID(UI64):0xCB1D5C213434DD48][CSIZ(UI64):10][AVER
(UI32):10]
[ATIM(UI64):1499810043157462][ATYP(FC32):SUPD][ANID(UI32):12258396][AMID(F
C32):S3RQ]
[ATID(UI64):8987436599021955788]]
```

Messaggi di audit

Scopri i tipi e i codici dei messaggi di audit in StorageGRID

Le descrizioni dettagliate dei messaggi di controllo restituiti dal sistema sono elencate nelle sezioni seguenti. Ciascun messaggio di audit viene elencato per primo in una tabella che raggruppa i messaggi correlati in base alla classe di attività rappresentata dal messaggio. Questi raggruppamenti sono utili sia per comprendere i tipi di attività sottoposte a audit che per selezionare il tipo di filtro dei messaggi di audit desiderato.

I messaggi di audit sono anche elencati in ordine alfabetico in base ai codici a quattro caratteri. Questo elenco alfabetico consente di trovare informazioni su messaggi specifici.

I codici a quattro caratteri utilizzati in questo capitolo sono i valori ATYP presenti nei messaggi di controllo,

come mostrato nel seguente messaggio di esempio:

```
2014-07-17T03:50:47.484627
\[AUDT:[RSLT(FC32):VRGN][AVER(UI32):10][ATIM(UI64):1405569047484627][ATYP\
(FC32\):SYSU][ANID(UI32):11627225][AMID(FC32):ARNI][ATID(UI64):94457363265
00603516]]
```

Per informazioni sull'impostazione dei livelli dei messaggi di controllo, sulla modifica delle destinazioni dei registri e sull'utilizzo di un server syslog esterno per le informazioni di controllo, vedere ["Configurare la gestione dei log e il server syslog esterno"](#)

Controllare le categorie dei messaggi

Messaggi di audit per gli eventi di sistema in StorageGRID

I messaggi di audit appartenenti alla categoria di audit del sistema vengono utilizzati per gli eventi correlati al sistema di audit stesso, agli stati dei nodi della griglia, all'attività delle attività a livello di sistema (attività della griglia) e alle operazioni di backup del servizio.

Codice	Titolo e descrizione del messaggio	Vedere
ECMC	Manca un frammento di dati con erasure coding: Indica che è stato rilevato un frammento di dati con erasure coding mancante.	"ECMC: Frammento di dati con codice di cancellazione mancante"
ECOC	Fragment di dati con erasure coding corrotto: Indica che è stato rilevato un frammento di dati sottoposto a erasure coding corrotto.	"ECOC: Frammento di dati con codice di cancellazione corrotto"
ETAF	Autenticazione di sicurezza non riuscita: Tentativo di connessione con Transport Layer Security (TLS) non riuscito.	"ETAF: Autenticazione di sicurezza non riuscita"
GNRG	Registrazione GNDS: Un servizio aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.	"GNRG: Registrazione GNDS"
NUR	Annullamento registrazione GNDS: Un servizio non si è registrato dal sistema StorageGRID.	"GNUR: Annullamento registrazione GNDS"
GTED	Grid Task Ended (attività griglia terminata): Il servizio CMN ha terminato l'elaborazione dell'attività Grid.	"GTED: Task Grid terminato"
GTST	Grid Task Started (attività griglia avviata): Il servizio CMN ha avviato l'elaborazione dell'attività Grid.	"GTST: Task Grid avviato"
GTSU	Grid Task Submitted (attività griglia inviata): È stata inviata un'attività Grid al servizio CMN.	"GTSU: Task Grid inviato"

Codice	Titolo e descrizione del messaggio	Vedere
LLST	Location Lost (posizione persa): Questo messaggio di audit viene generato quando una posizione viene persa.	"LLST: Località persa"
OLST	Object Lost (oggetti persi): Non è possibile individuare un oggetto richiesto all'interno del sistema StorageGRID.	"OLST: Il sistema ha rilevato un oggetto perso"
SADD	Security Audit Disable (Disattiva controllo protezione): La registrazione del messaggio di controllo è stata disattivata.	"SADD: Disattivazione dell'audit di sicurezza"
SADE	Security Audit Enable (attiva controllo di sicurezza): La registrazione del messaggio di controllo è stata ripristinata.	"SADE: Abilitazione controllo di sicurezza"
SVRF	Verifica archivio oggetti non riuscita: Un blocco di contenuto non ha superato i controlli di verifica.	"SVRF: Verifica archivio oggetti non riuscita"
SVRU	Object Store Verify Unknown (verifica archivio oggetti sconosciuto): Dati di oggetti imprevisti rilevati nell'archivio oggetti.	"SVRU: Verifica archivio oggetti sconosciuta"
SYSD	Node Stop (arresto nodo): È stato richiesto lo spegnimento.	"SYSD: Interruzione nodo"
SIST	Node stopping (interruzione nodo): Un servizio ha avviato un'interruzione senza interruzioni.	"SYST: Interruzione del nodo"
SISU	Node Start (Avvio nodo): Un servizio avviato; la natura dello shutdown precedente viene indicata nel messaggio.	"SYSU: Avvio nodo"

Messaggi di controllo per gli eventi di storage a oggetti in StorageGRID

I messaggi di audit appartenenti alla categoria di audit dello storage a oggetti vengono utilizzati per gli eventi correlati allo storage e alla gestione degli oggetti all'interno del sistema StorageGRID. Tra cui storage a oggetti e recuperi, trasferimenti da grid-node a grid-node e verifiche.



I codici di controllo vengono rimossi dal prodotto e dalla documentazione poiché le funzioni sono obsolete. Se si riscontra un codice di controllo non elencato qui, controllare le versioni precedenti di questo argomento per le versioni SG precedenti. Ad esempio, "[Messaggi di audit dello storage a oggetti StorageGRID 11,8](#)".

Codice	Descrizione	Vedere
BROR	Bucket Read Only Request (richiesta di sola lettura bucket): Un bucket è entrato o è uscito dalla modalità di sola lettura.	"BROR: Richiesta di sola lettura bucket"
CBSE	Object Send End (fine invio oggetto): L'entità di origine ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBSE: Fine invio oggetto"
CBRE	Object Receive End (fine ricezione oggetto): L'entità di destinazione ha completato un'operazione di trasferimento dei dati dal nodo griglia al nodo griglia.	"CBRE: Fine ricezione oggetto"
CGRR	Richiesta di replica cross-grid: StorageGRID ha tentato un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di grid.	"CGRR: Richiesta di replica cross-grid"
EBDL	Empty bucket Delete (Elimina bucket vuoto): Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuoto).	"EBDL: Eliminazione bucket vuoto"
EBKR	Empty bucket Request (richiesta bucket vuoto): Un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di oggetti).	"EBKR: Richiesta bucket vuoto"
SCMT	Commit dell'archivio oggetti: Un blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto.	"SCMT: Richiesta di commit dell'archivio di oggetti"
SREM	Rimozione archivio oggetti: Un blocco di contenuto è stato cancellato da un nodo griglia e non può più essere richiesto direttamente.	"SREM: Rimozione dell'archivio di oggetti"

Messaggi di audit per le operazioni di lettura del client in StorageGRID

I messaggi di controllo in lettura dei client vengono registrati quando un'applicazione client S3 richiede di recuperare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
S3SL	S3 Select request (richiesta S3 Select): Registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.	Client S3	"S3SL: Richiesta S3 Select"
SGET	S3 GET: Registra una transazione riuscita per recuperare un oggetto o elencare gli oggetti in un bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SGET: S3 GET"
SHEA	S3 HEAD: Registra una transazione riuscita per verificare l'esistenza di un oggetto o di un bucket.	Client S3	"SHEA: TESTA S3"

Messaggi di audit per le operazioni di scrittura del client in StorageGRID

I messaggi di controllo in scrittura del client vengono registrati quando un'applicazione client S3 richiede di creare o modificare un oggetto.

Codice	Descrizione	Utilizzato da	Vedere
OVWR	Object Overwrite: Registra una transazione per sovrascrivere un oggetto con un altro oggetto.	Client S3	"OVWR: Sovrascrittura degli oggetti"
SDEL	S3 DELETE (ELIMINA S3): Registra una transazione riuscita per eliminare un oggetto o un bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SDEL: ELIMINAZIONE S3"
SPOS	S3 POST: Registra una transazione riuscita per ripristinare un oggetto dallo storage AWS Glacier a un Cloud Storage Pool.	Client S3	"SPOS: POST S3"
SPUT	S3 PUT: Registra una transazione riuscita per creare un nuovo oggetto o bucket. Nota: se la transazione opera su una sottorisorsa, il messaggio di audit includerà il campo S3SR.	Client S3	"SPUT: S3 PUT"
SUPD	S3 Metadata Updated: Registra una transazione riuscita per aggiornare i metadati di un oggetto o bucket esistente.	Client S3	"SUPD: Metadati S3 aggiornati"

Messaggi di audit della gestione StorageGRID

La categoria Gestione registra le richieste degli utenti all'API di gestione.

Codice	Titolo e descrizione del messaggio	Vedere
MGAU	Messaggio di audit API di gestione: Un registro delle richieste degli utenti.	"MGAU: Messaggio di audit della gestione"

Messaggi di audit ILM di StorageGRID

I messaggi di audit appartenenti alla categoria di audit ILM vengono utilizzati per gli eventi relativi alle operazioni ILM (Information Lifecycle Management).

Codice	Titolo e descrizione del messaggio	Vedere
IDEL	ILM Initiated Delete (eliminazione avviata da ILM): Questo messaggio di controllo viene generato quando ILM avvia il processo di eliminazione di un oggetto.	"IDEL: Eliminazione avviata da ILM"
LKCU	Pulitura oggetto sovrascritto. Questo messaggio di audit viene generato quando un oggetto sovrascritto viene rimosso automaticamente per liberare spazio di storage.	"LKCU: Pulitura oggetto sovrascritta"
ORLM	Regole oggetto soddisfatte: Questo messaggio di audit viene generato quando i dati oggetto vengono memorizzati come specificato dalle regole ILM.	"ORLM: Regole oggetto soddisfatte"

Riferimento del messaggio di audit

Messaggio di audit BROR per le richieste di sola lettura del bucket in StorageGRID

Il servizio LDR genera questo messaggio di audit quando un bucket entra o esce dalla modalità di sola lettura. Ad esempio, un bucket entra in modalità di sola lettura mentre tutti gli oggetti vengono cancellati.

Codice	Campo	Descrizione
BKHD	UUID bucket	L'ID bucket.
BROV	Valore della richiesta di sola lettura del bucket	Se il bucket viene reso di sola lettura o se esce dallo stato di sola lettura (1 = sola lettura, 0 = non di sola lettura).
BROS	Motivo di sola lettura del bucket	Il motivo per cui il bucket viene reso di sola lettura o viene lasciato lo stato di sola lettura. Ad esempio, emptyBucket.

Codice	Campo	Descrizione
S3AI	ID account tenant S3	L'ID dell'account tenant che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Messaggio di audit CBRB per l'inizio della ricezione dell'oggetto in StorageGRID

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da

"Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

Messaggio di audit CBRE per la ricezione dell'oggetto in StorageGRID

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di destinazione.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.

Codice	Campo	Descrizione
RSLT	Risultato del trasferimento	Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati. CONL: Connessione persa durante il trasferimento CTMO: Timeout della connessione durante la creazione o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

Messaggio di audit CBSB per l'inizio dell'invio dell'oggetto in StorageGRID

Durante le normali operazioni di sistema, i blocchi di contenuto vengono continuamente trasferiti tra nodi diversi man mano che si accede, si replica e si mantengono i dati. Quando viene avviato il trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.

Codice	Campo	Descrizione
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.
CTSS	Avvia conteggio sequenza	Indica il primo numero di sequenze richiesto. Se l'operazione ha esito positivo, il trasferimento inizia dal conteggio di questa sequenza.
CTE	Conteggio sequenza finale previsto	Indica l'ultimo numero di sequenze richiesto. In caso di esito positivo, il trasferimento viene considerato completo al ricevimento di questo conteggio di sequenza.
RSLT	Transfer Start Status (Stato inizio trasferimento)	Stato al momento dell'avvio del trasferimento: SUCS: Trasferimento avviato correttamente.

Questo messaggio di audit indica che è stata avviata un'operazione di trasferimento dei dati da nodo a nodo su un singolo contenuto, come identificato dal relativo Content Block Identifier. L'operazione richiede dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "preveded End Sequence Count" (Conteggio sequenza finale previsto) I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e, se combinate con i messaggi di audit dello storage, per verificare il numero di repliche.

Messaggio di audit CBSE per la fine dell'invio dell'oggetto in StorageGRID

Al termine del trasferimento di un blocco di contenuto da un nodo all'altro, questo messaggio viene emesso dall'entità di origine.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco della sessione/connessione nodo-nodo.
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto trasferito.
CTDR	Direzione di trasferimento	Indica se il trasferimento CBID è stato avviato tramite push o pull: PUSH: L'operazione di trasferimento è stata richiesta dall'entità mittente. PULL: L'operazione di trasferimento è stata richiesta dall'entità ricevente.
CTSR	Entità di origine	L'ID nodo dell'origine (mittente) del trasferimento CBID.
CTD	Entità di destinazione	L'ID nodo della destinazione (destinatario) del trasferimento CBID.

Codice	Campo	Descrizione
CTSS	Avvia conteggio sequenza	Indica il numero di sequenze su cui è iniziato il trasferimento.
CTA	Conteggio sequenza finale effettivo	Indica che il conteggio dell'ultima sequenza è stato trasferito correttamente. Se il conteggio sequenza finale effettivo è uguale al conteggio sequenza iniziale e il risultato del trasferimento non ha avuto esito positivo, non è stato scambiato alcun dato.
RSLT	Risultato del trasferimento	Risultato dell'operazione di trasferimento (dal punto di vista dell'entità mittente): SUCS: Trasferimento completato correttamente; tutti i conteggi di sequenza richiesti sono stati inviati. CONL: Connessione persa durante il trasferimento CTMO: Timeout della connessione durante la creazione o il trasferimento UNRE: ID nodo di destinazione non raggiungibile CRPT: Trasferimento terminato a causa della ricezione di dati corrotti o non validi

Questo messaggio di audit indica che è stata completata un'operazione di trasferimento dei dati da nodo a nodo. Se il risultato del trasferimento ha avuto esito positivo, l'operazione ha trasferito i dati da "Start Sequence Count" (Conteggio sequenza iniziale) a "Actual End Sequence Count" (Conteggio sequenza finale effettivo). I nodi di invio e ricezione sono identificati dai rispettivi ID di nodo. Queste informazioni possono essere utilizzate per tenere traccia del flusso di dati del sistema e per individuare, tabulare e analizzare gli errori. Se combinato con i messaggi di audit dello storage, può essere utilizzato anche per verificare i conteggi delle repliche.

Messaggio di audit CGRR per le richieste di replica tra griglie in StorageGRID

Questo messaggio viene generato quando StorageGRID tenta di eseguire un'operazione di replica cross-grid per replicare gli oggetti tra bucket in una connessione a federazione di griglie.

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	La dimensione dell'oggetto in byte. L'attributo CSIZ è stato introdotto in StorageGRID 11,8. Di conseguenza, le richieste di replica cross-grid su un aggiornamento da StorageGRID 11,7 a 11,8 potrebbero presentare dimensioni totali degli oggetti imprecise.
S3AI	ID account tenant S3	L'ID dell'account tenant proprietario del bucket da cui l'oggetto viene replicato.

Codice	Campo	Descrizione
GFID	ID connessione federazione griglia	L'ID della connessione a federazione di griglie utilizzata per la replica cross-grid.
OPER	Funzionamento CGR	Il tipo di operazione di replica cross-grid che è stata tentata: • 0 = oggetto replicato • 1 = Replica oggetto multiparte • 2 = marcatore di eliminazione replicato
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.
VSID	ID versione	L'ID versione della versione specifica di un oggetto replicato.
RSLT	Codice risultato	Restituisce Successful (SUCS) o General error (GERR).

Messaggio di audit EBDL per le eliminazioni di oggetti bucket vuoti in StorageGRID

Lo scanner ILM ha eliminato un oggetto in un bucket che sta eliminando tutti gli oggetti (eseguendo un'operazione bucket vuota).

Codice	Campo	Descrizione
CSIZ	Dimensione oggetto	La dimensione dell'oggetto in byte.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
RSLT	Risultato dell'operazione di eliminazione	Il risultato di un evento, di un processo o di una transazione. Se non è rilevante per un messaggio, NON viene utilizzato NESSUNO invece di SUCS, in modo che il messaggio non venga accidentalmente filtrato.

Messaggio di audit EBKR per richieste di bucket vuoti in StorageGRID

Questo messaggio indica che un utente ha inviato una richiesta per attivare o disattivare il bucket vuoto (ovvero per eliminare oggetti bucket o per interrompere l'eliminazione di

oggetti).

Codice	Campo	Descrizione
BUID (BUID)	UUID bucket	L'ID bucket.
EBJS	Configurazione JSON bucket vuoto	Contiene il JSON che rappresenta la configurazione vuota corrente del bucket.
S3AI	ID account tenant S3	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Messaggio di audit ECMC per dati con codifica di cancellazione mancanti in StorageGRID

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati con codifica di cancellazione mancante.

Codice	Campo	Descrizione
VCMC	ID VCS	Il nome del VCS che contiene il blocco mancante.
MCID	ID chunk	L'identificatore del frammento con codifica di cancellazione mancante.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

Messaggio di audit ECOC per dati con codice di cancellazione corrotti in StorageGRID

Questo messaggio di audit indica che il sistema ha rilevato un frammento di dati corrotto con codifica di cancellazione.

Codice	Campo	Descrizione
VCCO	ID VCS	Il nome del VCS che contiene il blocco corrotto.
VLID	ID volume	Volume RangeDB contenente il frammento corrotto con codifica di cancellazione.
CCID	ID chunk	L'identificatore del frammento corrotto con codifica in cancellazione.

Codice	Campo	Descrizione
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non è pertinente per questo particolare messaggio. Viene utilizzato 'NONE' invece di 'SUCS' in modo che questo messaggio non venga filtrato.

Messaggio di audit ETAF per errori di autenticazione di sicurezza in StorageGRID

Questo messaggio viene generato quando un tentativo di connessione con Transport Layer Security (TLS) non riesce.

Codice	Campo	Descrizione
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP su cui l'autenticazione non è riuscita.
MALEDUCATO	Identità dell'utente	Identificatore dipendente dal servizio che rappresenta l'identità dell'utente remoto.
RSLT	Codice di motivazione	Il motivo del guasto: SCNI: Connessione sicura non riuscita. CERM: Certificato mancante. CERT: Certificato non valido. CERE: Certificato scaduto. CER: Certificato revocato. CSGN: Firma del certificato non valida. CSGU: Il firmatario del certificato non era noto. UCRM: Credenziali utente mancanti. UCRI: Credenziali utente non valide. UCRU: Le credenziali dell'utente non sono consentite. TOUT: Timeout dell'autenticazione.

Quando viene stabilita una connessione a un servizio sicuro che utilizza TLS, le credenziali dell'entità remota vengono verificate utilizzando il profilo TLS e la logica aggiuntiva integrata nel servizio. Se l'autenticazione non riesce a causa di certificati o credenziali non validi, imprevisti o non consentiti, viene registrato un messaggio di audit. Ciò consente di eseguire query per tentativi di accesso non autorizzati e altri problemi di connessione correlati alla sicurezza.

Il messaggio potrebbe derivare da un'entità remota con una configurazione errata o da tentativi di presentare credenziali non valide o non consentite al sistema. Questo messaggio di audit deve essere monitorato per

rilevare i tentativi di accesso non autorizzato al sistema.

Messaggio di audit GNRG per la registrazione GNDS in StorageGRID

Il servizio CMN genera questo messaggio di audit quando un servizio ha aggiornato o registrato informazioni su se stesso nel sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUC: Riuscito • SUNV: Servizio non disponibile • GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.
GNTTP	Tipo di dispositivo	Il tipo di dispositivo del nodo Grid (ad esempio, BLDR per un servizio LDR).
GNDV	Versione del modello del dispositivo	Stringa che identifica la versione del modello di dispositivo del nodo Grid nel bundle DMDL.
GNGP	Gruppo	Il gruppo a cui appartiene il nodo grid (nel contesto dei costi di collegamento e della classificazione delle query di servizio).
GNIA	Indirizzo IP	L'indirizzo IP del nodo della griglia.

Questo messaggio viene generato ogni volta che un nodo della griglia aggiorna la propria voce nel bundle dei nodi della griglia.

Messaggio di audit GNUR per l'annullamento della registrazione GNDS in StorageGRID

Il servizio CMN genera questo messaggio di audit quando un servizio ha informazioni non registrate su se stesso dal sistema StorageGRID.

Codice	Campo	Descrizione
RSLT	Risultato	Risultato della richiesta di aggiornamento: • SUC: Riuscito • SUNV: Servizio non disponibile • GERR: Altro guasto
GNID	ID nodo	L'ID nodo del servizio che ha avviato la richiesta di aggiornamento.

Messaggio di audit GTED per le attività di grid terminate in StorageGRID

Questo messaggio di audit indica che il servizio CMN ha terminato l'elaborazione dell'attività di griglia specificata e che l'attività è stata spostata nella tabella Cronologia. Se il risultato è SUCS, ABRT o ROLF, verrà visualizzato un messaggio di audit Grid Task Started (attività griglia avviata) corrispondente. Gli altri risultati indicano che l'elaborazione di questa attività della griglia non è mai stata avviata.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in modo univoco un'attività Grid generata e consente di gestire l'attività Grid nel suo ciclo di vita. Nota: l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
RSLT	Risultato	Risultato finale dello stato dell'attività Grid: • SUCS: L'attività Grid è stata completata correttamente. • ABRT: L'attività Grid è stata terminata senza un errore di rollback. • ROLF: L'attività Grid è stata terminata e non è stato possibile completare il processo di rollback. • CANC: L'attività della griglia è stata annullata dall'utente prima dell'avvio. • EXPR: L'attività Grid è scaduta prima dell'avvio. • IVLD: L'attività della griglia non era valida. • AUTH: L'attività della rete non è stata autorizzata. • DUPL: L'attività Grid è stata rifiutata come duplicata.

Messaggio di audit GTST per le attività di grid avviate in StorageGRID

Questo messaggio di audit indica che il servizio CMN ha avviato l'elaborazione dell'attività Grid specificata. Il messaggio di audit segue immediatamente il messaggio Grid Task Submitted per le attività Grid avviate dal servizio interno Grid Task Submission e selezionate per l'attivazione automatica. Per le attività della griglia inoltrate nella tabella Pending (in sospeso), questo messaggio viene generato quando l'utente avvia l'attività della griglia.

Codice	Campo	Descrizione
TSID	ID attività	Questo campo identifica in maniera univoca un'attività grid generata e consente di gestirne l'intero ciclo di vita. Nota: l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
RSLT	Risultato	Il risultato. Questo campo ha un solo valore: • SUCS: L'attività Grid è stata avviata correttamente.

Messaggio di audit GTSU per le attività di grid inviate in StorageGRID

Questo messaggio di audit indica che un'attività Grid è stata inviata al servizio CMN.

Codice	Campo	Descrizione
TSID	ID attività	Identifica in modo univoco un'attività grid generata e consente di gestarla per l'intero ciclo di vita. Nota: l'ID attività viene assegnato al momento in cui viene generata un'attività di griglia, non al momento in cui viene inviata. È possibile che un'attività di griglia venga inviata più volte e, in questo caso, il campo ID attività non è sufficiente per collegare in modo univoco i messaggi di audit inviati, avviati e terminati.
TTIP	Tipo di attività	Il tipo di attività della griglia.
VER	Versione attività	Un numero che indica la versione dell'attività Grid.
TDSC	Descrizione dell'attività	Una descrizione leggibile dell'attività Grid.
VAT	Valido dopo l'indicatore di data e ora	Il primo tempo (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui l'attività grid è valida.
VBTS	Valido prima dell'indicatore di data e ora	L'ultima ora (microsecondi UINT64 dal 1° gennaio 1970 - ora UNIX) in cui è valida l'attività grid.

Codice	Campo	Descrizione
TSRC	Origine	L'origine dell'attività: • TXTB: L'attività Grid è stata inviata tramite il sistema StorageGRID come blocco di testo firmato. • GRID: L'attività Grid è stata inviata tramite il Grid Task Submission Service interno.
ACTV	Tipo di attivazione	Il tipo di attivazione: • AUTO: L'attività della griglia è stata inviata per l'attivazione automatica. • PEND: L'attività Grid è stata inviata alla tabella in sospeso. Questa è l'unica possibilità per l'origine TXTB.
RSLT	Risultato	Risultato dell'invio: • SUCS: L'attività Grid è stata inviata correttamente. • ERRORE: L'attività è stata spostata direttamente nella tabella storica.

Messaggio di audit IDEL per le eliminazioni avviate da ILM in StorageGRID

Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto.

Il messaggio IDEL viene generato in una delle seguenti situazioni:

- **Per gli oggetti nei bucket S3 conformi:** Questo messaggio viene generato quando ILM avvia il processo di eliminazione automatica di un oggetto perché il relativo periodo di conservazione è scaduto (supponendo che l'impostazione di eliminazione automatica sia attivata e che la sospensione legale sia disattivata).
- **Per oggetti in bucket S3 non conformi.** Questo messaggio viene generato quando ILM avvia il processo di eliminazione di un oggetto poiché all'oggetto non sono attualmente applicate istruzioni di posizionamento nei criteri ILM attivi.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.
CMPA	Compliance: Eliminazione automatica	Solo per oggetti nei bucket S3 conformi. 0 (false) o 1 (true), che indica se un oggetto conforme deve essere cancellato automaticamente al termine del periodo di conservazione, a meno che il bucket non sia sottoposto a una conservazione legale.

Codice	Campo	Descrizione
CMPL	Compliance: Conservazione a fini legali	Solo per oggetti nei bucket S3 conformi. 0 (falso) o 1 (vero), che indica se il bucket è attualmente in stato di conservazione legale.
CMPR	Conformità: Periodo di conservazione	Solo per oggetti nei bucket S3 conformi. La durata del periodo di conservazione dell'oggetto in minuti.
CTME	Compliance: Tempo di acquisizione	Solo per oggetti nei bucket S3 conformi. Il tempo di acquisizione dell'oggetto. È possibile aggiungere il periodo di conservazione in minuti a questo valore per determinare quando l'oggetto può essere cancellato dal bucket.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato). CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto. CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Risultato dell'operazione ILM. SUCS: Operazione ILM riuscita.
REGOLA	Etichetta regole	- Se un oggetto in un bucket S3 conforme viene cancellato automaticamente perché il suo periodo di conservazione è scaduto, questo campo è vuoto. - Se l'oggetto viene eliminato perché non sono presenti ulteriori istruzioni di posizionamento attualmente applicabili all'oggetto, questo campo mostra l'etichetta leggibile dell'ultima regola ILM applicata all'oggetto.

Codice	Campo	Descrizione
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Messaggio di audit LKCU per la pulizia degli oggetti sovrascritti in StorageGRID

Questo messaggio viene generato quando StorageGRID rimuove un oggetto sovrascritto che in precedenza richiedeva la pulizia per liberare spazio di storage. Un oggetto viene sovrascritto quando un client S3 scrive un oggetto in un percorso già contenente un oggetto. Il processo di rimozione avviene automaticamente e in background.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LTP	Tipo di pulizia	<i>Solo per uso interno.</i>
LUID	UUID oggetto rimosso	L'identificativo dell'oggetto rimosso.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
UUID	Universally Unique Identifier	L'identificativo dell'oggetto ancora esistente. Questo valore è disponibile solo se l'oggetto non è stato eliminato.

Messaggio di audit LKDM per la pulizia degli oggetti trapezoidali in StorageGRID

Questo messaggio viene generato quando un frammento fuoriuscito è stato pulito o eliminato. Un blocco può far parte di un oggetto replicato o di un oggetto codificato per la cancellazione.

Codice	Campo	Descrizione
CLOC	Posizione del frammento	Il percorso del file del blocco fuoriuscito che è stato eliminato.
CTYP	Tipo di frammento	Tipo di pezzo: ec: Erasure-coded object chunk repl: Replicated object chunk
LTYP	Tipo di perdita	I cinque tipi di perdite che possono essere rilevate: object_leaked: Object doesn't exist in the grid location_leaked: Object exists in the grid, but found location doesn't belong to object mup_seg_leaked: Multipart upload was stopped or not completed, and the segment/part was left out segment_leaked: Parent UUID/CBID (associated container object) is valid but doesn't contain this segment no_parent: Container object is deleted, but object segment was left out and not deleted
CTIM	Crea il tempo	Ora in cui è stato creato il frammento fuoriuscito.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto a cui appartiene il blocco.
CBID	Identificatore del blocco di contenuto	CBID dell'oggetto a cui appartiene il blocco fuoriuscito.
CSIZ	Dimensione del contenuto	La dimensione del blocco in byte.

Messaggio di audit LLST per le posizioni di copia degli oggetti persi in StorageGRID

Questo messaggio viene generato ogni volta che non è possibile trovare una posizione per una copia dell'oggetto (replicata o con erasure coding).

Codice	Campo	Descrizione
CBIL	CBID	Il CBID interessato.

Codice	Campo	Descrizione
ECPR	Profilo di erasure coding	Per i dati degli oggetti con codifica erasure coding utilizzato.
LTYP	Tipo di ubicazione	CLDI (online): Per i dati degli oggetti replicati CLEC (Online): Per i dati degli oggetti con codifica erasure CLNL (Nearline): Per i dati degli oggetti replicati archiviati
NOID. (NOIDE	ID nodo di origine	L'ID del nodo in cui sono state perse le posizioni.
PCLD	Percorso dell'oggetto replicato	Il percorso completo alla posizione del disco dei dati dell'oggetto perso. Viene restituito solo quando LTYP ha un valore di CLDI (vale a dire, per gli oggetti replicati). Assume la forma <code>/var/local/rangedb/2/p/13/13/00oJs6X%{h{U}SeUFxE@</code>
RSLT	Risultato	SEMPRE NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
TSRC	Fonte di attivazione	UTENTE: Attivato dall'utente SYST: Attivato dal sistema
UUID	ID universalmente univoco	L'identificativo dell'oggetto interessato nel sistema StorageGRID.

Messaggio di audit MGAU per le richieste API di gestione in StorageGRID

La categoria Gestione registra le richieste degli utenti all'API di gestione. Ogni richiesta HTTP che non è 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 (come /api/v3-autorizza) e le richieste non valide agli URI API validi non vengono registrate.

Codice	Campo	Descrizione
MDIP	Indirizzo IP di destinazione	L'indirizzo IP del server (destinazione).
MDNA	Nome di dominio	Il nome del dominio host.
MPAT	PERCORSO di richiesta	Il percorso della richiesta.

Codice	Campo	Descrizione
MPQP	Parametri di query della richiesta	I parametri di query per la richiesta.
MRBD	Corpo della richiesta	Il contenuto dell'organismo di richiesta. Mentre il corpo della risposta viene registrato per impostazione predefinita, il corpo della richiesta viene registrato in alcuni casi quando il corpo della risposta è vuoto. Poiché le seguenti informazioni non sono disponibili nel corpo della risposta, vengono prese dal corpo della richiesta per i seguenti metodi POST: • Nome utente e ID account in POST authorize • Nuova configurazione delle subnet in POST /grid/grid-networks/update • Nuovi server NTP in POST /grid/ntp-servers/update • ID server decommissionati in POST /grid/servers/decommissionation Nota: le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).
MRMD	Metodo di richiesta	Il metodo di richiesta HTTP: • POST • IN PRIMO PIANO • ELIMINARE • PATCH
MRSC	Codice di risposta	Il codice di risposta.
MRSP	Corpo di risposta	Il contenuto della risposta (il corpo della risposta) viene registrato per impostazione predefinita. Nota: le informazioni sensibili vengono eliminate (ad esempio, una chiave di accesso S3) o mascherate con asterischi (ad esempio, una password).
MSIP	Indirizzo IP di origine	L'indirizzo IP (di origine) del client.
MUN	URN utente	L'URN (Uniform resource name) dell'utente che ha inviato la richiesta.
RSLT	Risultato	Restituisce Successful (SUCS) o l'errore segnalato dal backend.

Messaggio di audit OLST per oggetti persi rilevati dal sistema in StorageGRID

Questo messaggio viene generato quando il servizio DDS non riesce a individuare alcuna copia di un oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto perso.
NOID. (NOIDE	ID nodo	Se disponibile, l'ultima posizione nota diretta o near-line dell'oggetto perso. Se le informazioni sul volume non sono disponibili, è possibile avere solo l'ID nodo senza un ID volume.
PERCORSO	Bucket/chiave S3	Se disponibile, il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.
UUID	ID universalmente univoco	L'identificativo dell'oggetto perso nel sistema StorageGRID.
VOLO	ID volume	Se disponibile, l'ID del volume del nodo di archiviazione per l'ultima posizione nota dell'oggetto perso.

Messaggio di audit ORLM per le regole ILM soddisfatte in StorageGRID

Questo messaggio viene generato quando l'oggetto viene memorizzato e copiato correttamente come specificato dalle regole ILM.



Il messaggio ORLM non viene generato quando un oggetto viene memorizzato correttamente dalla regola predefinita Make 2 Copies se un'altra regola del criterio utilizza il filtro avanzato dimensione oggetto.

Codice	Campo	Descrizione
BUID (BUID)	Testata benna	Campo ID bucket. Utilizzato per operazioni interne. Viene visualizzato solo se STAT è PRGD.
CBID	Identificatore del blocco di contenuto	Il CBID dell'oggetto.

Codice	Campo	Descrizione
CSIZ	Dimensione del contenuto	La dimensione dell'oggetto in byte.
LOCS	Posizioni	La posizione di storage dei dati oggetto all'interno del sistema StorageGRID. Il valore per LOCS è "" se l'oggetto non ha posizioni (ad esempio, è stato cancellato). CLEC: Per gli oggetti sottoposti a erasure coding, l'ID del profilo di erasure coding e l'ID del gruppo di erasure coding applicati ai dati dell'oggetto. CLDI: Per gli oggetti replicati, l'ID del nodo LDR e l'ID del volume della posizione dell'oggetto. CLNL: ID nodo ARCO della posizione dell'oggetto se i dati dell'oggetto sono archiviati.
PERCORSO	Bucket/chiave S3	Il nome del bucket S3 e il nome della chiave S3.
RSLT	Risultato	Risultato dell'operazione ILM. SUCS: Operazione ILM riuscita.
REGOLA	Etichetta regole	Etichetta leggibile assegnata alla regola ILM applicata a questo oggetto.
SGC	UUID contenitore	UUID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo se l'oggetto è segmentato.
SGCB	CBID contenitore	CBID del contenitore per l'oggetto segmentato. Questo valore è disponibile solo per gli oggetti segmentati e multiparte.
URGENZA	Stato	Lo stato del funzionamento di ILM. FATTO: Operazioni ILM rispetto all'oggetto completate. DFER: L'oggetto è stato contrassegnato per la futura rivalutazione ILM. PRGD: L'oggetto è stato cancellato dal sistema StorageGRID. NLOC: I dati dell'oggetto non possono più essere trovati nel sistema StorageGRID. Questo stato potrebbe indicare che tutte le copie dei dati dell'oggetto sono mancanti o danneggiate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Il messaggio di audit ORLM può essere emesso più di una volta per un singolo oggetto. Ad esempio, viene emesso ogni volta che si verifica uno dei seguenti eventi:

- Le regole ILM per l'oggetto sono soddisfatte per sempre.
- Le regole ILM per l'oggetto sono soddisfatte per questa epoca.
- Le regole ILM hanno eliminato l'oggetto.
- Il processo di verifica in background rileva che una copia dei dati degli oggetti replicati è danneggiata. Il sistema StorageGRID esegue una valutazione ILM per sostituire l'oggetto corrotto.

Informazioni correlate

- ["Transazioni di acquisizione degli oggetti"](#)
- ["Transazioni di eliminazione degli oggetti"](#)

Messaggio di audit OVWR per sovrascritture di oggetti in StorageGRID

Questo messaggio viene generato quando un'operazione esterna (richiesta dal client) causa la sovrascrittura di un oggetto da parte di un altro oggetto.

Codice	Campo	Descrizione
CBID	Content Block Identifier (nuovo)	Il CBID per il nuovo oggetto.
CSIZ	Dimensione oggetto precedente	La dimensione, in byte, dell'oggetto da sovrascrivere.
OCBD	Content Block Identifier (precedente)	Il CBID dell'oggetto precedente.
UUID	ID universally Unique (nuovo)	L'identificativo del nuovo oggetto all'interno del sistema StorageGRID.
ID OUID	ID universally Unique (precedente)	L'identificativo dell'oggetto precedente all'interno del sistema StorageGRID.
PERCORSO	Percorso oggetto S3	Il percorso dell'oggetto S3 utilizzato sia per l'oggetto precedente che per quello nuovo

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione Object Overwrite. Il risultato è sempre: SUC: Riuscito
SGRP	Sito (gruppo)	Se presente, l'oggetto sovrascritto è stato cancellato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto sovrascritto.

Messaggio di audit S3SL per le richieste S3 Select in StorageGRID

Questo messaggio registra un completamento dopo che una richiesta S3 Select è stata restituita al client. Il messaggio S3SL può includere messaggi di errore e dettagli del codice di errore. La richiesta potrebbe non essere riuscita.

Codice	Campo	Descrizione
BYSC	Byte sottoposti a scansione	Numero di byte sottoposti a scansione (ricevuti) dai nodi di storage. BYSC e BYPR potrebbero essere diversi se l'oggetto viene compresso. Se l'oggetto è compresso, BYSC avrebbe il conteggio dei byte compressi e BYPR i byte dopo la decompressione.
BYPR	Byte elaborati	Numero di byte elaborati. Indica quanti byte di "byte sottoposti a scansione" sono stati effettivamente elaborati o utilizzati da un lavoro S3 Select.
BYRT	Byte restituiti	Numero di byte restituiti al client da un lavoro S3 Select.
RPR	Record elaborati	Numero di record o righe ricevuti da un processo S3 Select dai nodi di storage.
RERT	Record restituiti	Numero di record o righe di un lavoro S3 Select restituito al client.
JOFI	Lavoro terminato	Indica se il lavoro S3 Select ha terminato o meno l'elaborazione. Se questo è falso, il lavoro non è stato completato e i campi di errore probabilmente contengono dei dati. Il client potrebbe aver ricevuto risultati parziali o non avere alcun risultato.
RID	ID richiesta	Identificatore della richiesta S3 Select.
ETM	Tempo di esecuzione	Il tempo, in secondi, impiegato per il completamento del processo S3 Select.
ERMG	Messaggio di errore	Messaggio di errore generato dal lavoro S3 Select.
EROSO	Tipo di errore	Tipo di errore generato dal lavoro S3 Select.

Codice	Campo	Descrizione
ERST	Errore StackTrace	Errore StackTrace generato dal lavoro S3 Select.
S3BK	Bucket S3	Il nome del bucket S3.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 per l'utente che ha inviato la richiesta.
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket.

Messaggio di audit SADD per la disattivazione dell'audit di sicurezza in StorageGRID

Questo messaggio indica che il servizio di origine (ID nodo) ha disattivato la registrazione dei messaggi di audit. StorageGRID non raccoglie né invia più messaggi di audit.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Metodo utilizzato per disattivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per disattivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione era stata precedentemente attivata, ma ora è stata disattivata. Questo viene generalmente utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato (SADE) e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

Messaggio di audit SADE per l'abilitazione dell'audit di sicurezza in StorageGRID

Questo messaggio indica che il servizio di origine (ID nodo) ha ripristinato la registrazione dei messaggi di audit. StorageGRID sta nuovamente raccogliendo e inviando i messaggi di audit.

Codice	Campo	Descrizione
AETM	Abilitare il metodo	Il metodo utilizzato per attivare l'audit.
AEUN	Nome utente	Il nome utente che ha eseguito il comando per attivare la registrazione dell'audit.
RSLT	Risultato	Questo campo ha il valore NESSUNO. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. NON viene utilizzato NESSUNO invece di SUCS, in modo che questo messaggio non venga filtrato.

Il messaggio indica che la registrazione è stata precedentemente disattivata (SADD), ma ora è stata ripristinata. In genere viene utilizzato solo durante l'acquisizione in blocco per migliorare le prestazioni del sistema. In seguito all'attività in blocco, il controllo viene ripristinato e la capacità di disattivare il controllo viene quindi bloccata in modo permanente.

Messaggio di controllo SCMT per i commit dell'archivio di oggetti in StorageGRID

Il contenuto della griglia non viene reso disponibile o riconosciuto come memorizzato fino a quando non viene assegnato (ovvero viene memorizzato in modo persistente). Il contenuto memorizzato in maniera persistente è stato completamente scritto su disco e ha superato i relativi controlli di integrità. Questo messaggio viene emesso quando un blocco di contenuto viene assegnato allo storage.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto impegnato nello storage permanente.
RSLT	Codice risultato	Stato al momento in cui l'oggetto è stato memorizzato sul disco: SUCS: Oggetto memorizzato correttamente.

Questo messaggio indica che un dato blocco di contenuto è stato completamente memorizzato e verificato e può essere richiesto. Può essere utilizzato per tenere traccia del flusso di dati all'interno del sistema.

Messaggio di audit SDEL per le transazioni S3 DELETE in StorageGRID

Quando un client S3 esegue una transazione DI ELIMINAZIONE, viene effettuata una richiesta per rimuovere l'oggetto o il bucket specificato o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
ASRS	URN della sessione di ruolo assunto	L'identificativo univoco della sessione del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
ASRU	URN del ruolo assunto	L'identificativo univoco del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto cancellato in byte. Le operazioni sui bucket non includono questo campo.
DMRK	Elimina ID versione marker	L'ID versione del marker di eliminazione creato quando si elimina un oggetto da un bucket con versione. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta di eliminazione della replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta di eliminazione della replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP). x-amz-bypass-governance-retention viene incluso automaticamente se è presente nella richiesta.
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione DI ELIMINAZIONE. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.

Codice	Campo	Descrizione
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SGRP	Sito (gruppo)	Se presente, l'oggetto è stato eliminato nel sito specificato, che non è il sito in cui è stato acquisito l'oggetto.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UDM	Identificatore univoco universale per un marcatore di cancellazione	L'identificatore di un marcatore di eliminazione. I messaggi del registro di controllo specificano UUDM o UUID, dove UUDM indica un marcatore di eliminazione creato come risultato di una richiesta di eliminazione dell'oggetto e UUID indica un oggetto.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto eliminato. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Messaggio di audit SGET per le transazioni S3 GET in StorageGRID

Quando un client S3 esegue una transazione GET, viene effettuata una richiesta per recuperare un oggetto o elencare gli oggetti in un bucket o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
ASRS	URN della sessione di ruolo assunto	L'identificativo univoco della sessione del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
ASRU	URN del ruolo assunto	L'identificativo univoco del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. <code>`X-Forwarded-For`</code> Viene incluso automaticamente se è presente nella richiesta e se il <code>`X-Forwarded-For`</code> valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).
LITY	ListObjectsV2	È stata richiesta una risposta <i>formato v2</i> . Per ulteriori informazioni, vedere " AWS ListObjectsV2 ". Solo per operazioni CON benna GET.
NCHD	Numero di bambini	Include tasti e prefissi comuni. Solo per operazioni CON benna GET.
RANG	Range Read (lettura intervallo)	Solo per operazioni di lettura dell'intervallo. Indica l'intervallo di byte letti da questa richiesta. Il valore dopo la barra (/) mostra la dimensione dell'intero oggetto.

Codice	Campo	Descrizione
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.

Codice	Campo	Descrizione
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
TRNC	Troncato o non troncato	Impostare su false se sono stati restituiti tutti i risultati. Impostare su true se sono disponibili ulteriori risultati da restituire. Solo per operazioni CON benna GET.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Messaggio di audit SHEA per le operazioni S3 HEAD in StorageGRID

Quando un client S3 emette un'operazione 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 l'operazione ha esito positivo.

Codice	Campo	Descrizione
ASRS	URN della sessione di ruolo assunto	L'identificativo univoco della sessione del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
ASRU	URN del ruolo assunto	L'identificativo univoco del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
CBID	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNID	Identificatore di connessione	Identificativo univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto controllato in byte. Le operazioni sui bucket non includono questo campo.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` 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: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Messaggio di audit SPOS per le transazioni S3 POST in StorageGRID

Quando un client S3 invia una richiesta di oggetto POST, questo messaggio viene inviato dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
ASRS	URN della sessione di ruolo assunto	L'identificativo univoco della sessione del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
ASRU	URN del ruolo assunto	L'identificativo univoco del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
CBID	Identificatore del blocco di contenuto	L'identificativo univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0.

Codice	Campo	Descrizione
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` 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: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile. Impostare su "SELECT" per un'operazione di selezione S3.

Codice	Campo	Descrizione
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L>ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	Ripristinare le informazioni.
SUSR	S3 User URN (richiesta mittente)	L>ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L>ID versione della versione specifica di un oggetto richiesto. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Messaggio di audit SPUT per le transazioni S3 PUT in StorageGRID

Quando un client S3 esegue una transazione PUT, viene effettuata una richiesta per creare un nuovo oggetto o bucket o per rimuovere una sottorisorsa bucket/oggetto. Questo messaggio viene emesso dal server se la transazione ha esito positivo.

Codice	Campo	Descrizione
ASRS	URN della sessione di ruolo assunto	L'identificativo univoco della sessione del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
ASRU	URN del ruolo assunto	L'identificativo univoco del ruolo assunto. Presente solo quando la richiesta S3 utilizza credenziali di sicurezza temporanee provenienti da una richiesta AssumeRole.
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CMPS	Impostazioni di compliance	Le impostazioni di conformità utilizzate durante la creazione del bucket, se presenti nella richiesta (troncate ai primi 1024 caratteri).
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
GFID	ID connessione Grid Federation	L'ID di connessione della connessione a federazione di griglie associato a una richiesta DI PUT di replica a griglia incrociata. Incluso solo nei registri di controllo nella griglia di destinazione.
GFSA	ID account di origine Grid Federation	L'ID account del tenant sulla griglia di origine per una richiesta DI PUT di replica cross-grid. Incluso solo nei registri di controllo nella griglia di destinazione.

Codice	Campo	Descrizione
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. `X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` 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 è presente nella richiesta.
LKEN	Blocco oggetto attivato	Valore dell'intestazione della richiesta <code>x-amz-bucket-object-lock-enabled</code> , se presente nella richiesta.
LKSX	Blocco oggetto Legal Hold	Valore dell'intestazione della richiesta <code>x-amz-object-lock-legal-hold</code> , se presente nella richiesta PutObject.
LKMD	Modalità di conservazione 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 entro 100 anni dalla data di acquisizione dell'oggetto.
MTME	Ora dell'ultima modifica	Data e ora di Unix, in microsecondi, che indica quando l'oggetto è stato modificato per l'ultima volta.
RSLT	Codice risultato	Risultato della transazione PUT. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.

Codice	Campo	Descrizione
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
S3SR	S3 Subresource	Il bucket o la sottorisorsa oggetto su cui viene eseguita, se applicabile.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SRCF	Configurazione delle sottorisorse	La nuova configurazione delle sottorisorse (troncata ai primi 1024 caratteri).
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
ULID	ID upload	Incluso solo nei messaggi SPUT per le operazioni CompleteMultipartUpload. Indica che tutte le parti sono state caricate e assemblate.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.

Codice	Campo	Descrizione
VSID	ID versione	L'ID versione di un nuovo oggetto creato in un bucket con versione. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.
VSST	Stato di versione	Il nuovo stato di versione di un bucket. Vengono utilizzati due stati: "Attivato" o "sospeso". Le operazioni sugli oggetti non includono questo campo.

Messaggio di controllo SREM per la rimozione dell'archivio di oggetti in StorageGRID

Questo messaggio viene inviato quando il contenuto viene rimosso dallo storage persistente e non è più accessibile tramite API regolari.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto cancellato dallo storage permanente.
RSLT	Codice risultato	Indica il risultato delle operazioni di rimozione del contenuto. L'unico valore definito è: SUC: Contenuto rimosso dallo storage persistente

Questo messaggio di audit indica che un dato blocco di contenuto è stato cancellato da un nodo e non può più essere richiesto direttamente. Il messaggio può essere utilizzato per tenere traccia del flusso di contenuti cancellati all'interno del sistema.

Messaggio di audit SUPD per gli aggiornamenti dei metadati S3 in StorageGRID

Questo messaggio viene generato dall'API S3 quando un client S3 aggiorna i metadati per un oggetto acquisito. Il messaggio viene emesso dal server se l'aggiornamento dei metadati ha esito positivo.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	L'identificatore univoco del blocco di contenuto richiesto. Se il CBID non è noto, questo campo viene impostato su 0. Le operazioni sui bucket non includono questo campo.
CNCH	Intestazione del controllo di coerenza	Il valore dell'intestazione della richiesta HTTP Consistency-Control, se presente nella richiesta, quando si aggiornano le impostazioni di conformità di un bucket.
CNID	Identificatore di connessione	Identificatore univoco del sistema per la connessione TCP/IP.

Codice	Campo	Descrizione
CSIZ	Dimensione contenuto	La dimensione dell'oggetto recuperato in byte. Le operazioni sui bucket non includono questo campo.
HTRH	Intestazione richiesta HTTP	Elenco dei nomi e dei valori delle intestazioni delle richieste HTTP registrati selezionati durante la configurazione. <pre>`X-Forwarded-For` Viene incluso automaticamente se è presente nella richiesta e se il `X-Forwarded-For` valore è diverso dall'indirizzo IP del mittente della richiesta (campo di controllo SAIP).</pre>
RSLT	Codice risultato	Risultato della transazione GET. Il risultato è sempre: SUC: Riuscito
S3AI	ID account tenant S3 (richiesta mittente)	L'ID account tenant dell'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3AK	ID chiave di accesso S3 (richiesta mittente)	L'ID della chiave di accesso S3 hash per l'utente che ha inviato la richiesta. Un valore vuoto indica l'accesso anonimo.
S3BK	Bucket S3	Il nome del bucket S3.
S3KY	Chiave S3	Il nome della chiave S3, senza il nome del bucket. Le operazioni sui bucket non includono questo campo.
SACC	Nome account tenant S3 (mittente della richiesta)	Il nome dell'account tenant per l'utente che ha inviato la richiesta. Vuoto per richieste anonime.
SAIP	Indirizzo IP (Request sender)	L'indirizzo IP dell'applicazione client che ha eseguito la richiesta.
SBAC	Nome account tenant S3 (proprietario bucket)	Il nome dell'account tenant per il proprietario del bucket. Utilizzato per identificare l'accesso anonimo o multiaccount.

Codice	Campo	Descrizione
SBAI	ID account tenant S3 (proprietario bucket)	L'ID account tenant del proprietario del bucket di destinazione. Utilizzato per identificare l'accesso anonimo o multiaccount.
SUSR	S3 User URN (richiesta mittente)	L'ID account tenant e il nome utente dell'utente che effettua la richiesta. L'utente può essere un utente locale o LDAP. Ad esempio: <code>urn:sgws:identity::03393893651506583485:root</code> Vuoto per richieste anonime.
ORA	Ora	Tempo totale di elaborazione della richiesta in microsecondi.
TLIP	Indirizzo IP del bilanciamento del carico attendibile	Se la richiesta è stata instradata da un bilanciamento del carico di livello 7 attendibile, l'indirizzo IP del bilanciamento del carico.
UUID	Universally Unique Identifier	L'identificatore dell'oggetto all'interno del sistema StorageGRID.
VSID	ID versione	L'ID versione della versione specifica di un oggetto i cui metadati sono stati aggiornati. Le operazioni su bucket e oggetti in bucket senza versione non includono questo campo.

Messaggio di controllo SVRF per errori di verifica dell'archivio di oggetti in StorageGRID

Questo messaggio viene emesso ogni volta che un blocco di contenuto non supera il processo di verifica. Ogni volta che i dati degli oggetti replicati vengono letti o scritti su disco, vengono eseguiti diversi controlli di verifica e integrità per garantire che i dati inviati all'utente richiedente siano identici ai dati originariamente acquisiti nel sistema. Se uno di questi controlli non riesce, il sistema mette automaticamente in quarantena i dati dell'oggetto replicato corrotto per impedirne il recupero.

Codice	Campo	Descrizione
CBID	Identificatore del blocco di contenuto	Identificatore univoco del blocco di contenuto che non ha superato la verifica.

Codice	Campo	Descrizione
RSLT	Codice risultato	Tipo di errore di verifica: CRCF: Controllo di ridondanza ciclico (CRC) non riuscito. HMAC: Controllo HMAC (hash-based message Authentication code) non riuscito. EHSR: Hash di contenuto crittografato inatteso. PHSR: Hash di contenuto originale inaspettato. SEQC: Sequenza di dati errata sul disco. PERR: Struttura del file di disco non valida. DERR: Errore del disco. FNAM: Nome file non valido.



Questo messaggio deve essere monitorato attentamente. Gli errori di verifica del contenuto possono indicare guasti hardware imminenti.

Per determinare quale operazione ha attivato il messaggio, vedere il valore del campo AMID (Module ID) (ID modulo). Ad esempio, un valore SVFY indica che il messaggio è stato generato dal modulo Storage Verifier, ovvero la verifica in background e STOR indica che il messaggio è stato attivato dal recupero del contenuto.

Messaggio di controllo SVRU per contenuto di archivio di oggetti sconosciuto in StorageGRID

Il componente Storage del servizio LDR esegue una scansione continua di tutte le copie dei dati degli oggetti replicati nell'archivio di oggetti. Questo messaggio viene visualizzato quando viene rilevata una copia sconosciuta o imprevista dei dati degli oggetti replicati nell'archivio di oggetti e spostata nella directory di quarantena.

Codice	Campo	Descrizione
FPTH	Percorso del file	Il percorso del file della copia imprevista dell'oggetto.
RSLT	Risultato	Questo campo ha il valore 'NESSUNO'. RSLT è un campo obbligatorio per i messaggi, ma non pertinente per questo messaggio. Viene utilizzato 'NONE' invece di 'SUCC' in modo che questo messaggio non venga filtrato.



Il messaggio di audit SVRU: Object Store Verify Unknown deve essere monitorato attentamente. Significa che sono state rilevate copie impreviste dei dati dell'oggetto nell'archivio di oggetti. Questa situazione deve essere esaminata immediatamente per determinare come sono state create queste copie, perché può indicare guasti hardware imminenti.

Messaggio di audit SYSD per arresti di nodi regolari in StorageGRID

Quando un servizio viene arrestato correttamente, viene generato questo messaggio per indicare che è stato richiesto lo shutdown. In genere, questo messaggio viene inviato solo dopo un riavvio successivo, in quanto la coda dei messaggi di controllo non viene cancellata prima dell'arresto. Se il servizio non è stato riavviato, cercare il messaggio SYST inviato all'inizio della sequenza di arresto.

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. L'RSLT di un SYSD non può indicare uno shutdown "anomalo", perché il messaggio viene generato solo dagli shutdown "puliti".

Messaggio di audit SYST per l'arresto del nodo in StorageGRID

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 sua sequenza di arresto. SYST può essere utilizzato per determinare se è stato richiesto l'arresto, prima che il servizio venga riavviato (a differenza di SYSD, che di solito viene inviato dopo il riavvio del servizio).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito.

Il messaggio non indica se il server host viene arrestato, ma solo il servizio di reporting. Il codice RSLT di un messaggio SYST non può indicare uno shutdown "dirty", perché il messaggio viene generato solo dagli shutdown "clean".

Messaggio di audit SYSU per il nodo avviato in StorageGRID

Quando un servizio viene riavviato, questo messaggio viene generato per indicare se l'arresto precedente era pulito (comandato) o disordinato (imprevisto).

Codice	Campo	Descrizione
RSLT	Pulizia dello spegnimento	La natura dello shutdown: SUCS: Il sistema è stato spento in modo pulito. DSDN: Il sistema non è stato spento correttamente. VRGN: Il sistema è stato avviato per la prima volta dopo l'installazione (o la reinstallazione) del server.

Il messaggio non indica se il server host è stato avviato, ma solo il servizio di reporting. Questo messaggio può essere utilizzato per:

- Rilevare la discontinuità nel registro di controllo.
- Determinare se un servizio si guasta durante il funzionamento (poiché la natura distribuita del sistema StorageGRID può mascherare questi guasti). Server Manager riavvia automaticamente un servizio guasto.

Espandi la capacità o le funzionalità del tuo sistema StorageGRID

Scopri come espandere il tuo sistema StorageGRID

Scopri come espandere il tuo sistema StorageGRID per aumentare la capacità o le funzionalità senza interrompere le operazioni. È possibile aggiungere volumi di archiviazione ai nodi di archiviazione esistenti, aggiungere nuovi nodi di griglia a un sito esistente o aggiungere un nuovo sito.

Prima di espandere 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 o espansione. Fare riferimento a ["Controllare i lavori di riparazione dei dati"](#).

Un'espansione StorageGRID consente di aggiungere:

- Volumi storage sui nodi storage
- Nuovi nodi di griglia in un sito esistente
- Un intero nuovo sito

Il motivo dell'espansione determina il numero di nuovi nodi di ciascun tipo da aggiungere e la posizione dei nuovi nodi. Ad esempio, se si esegue un'espansione per aumentare la capacità dello storage, aggiungere la capacità dei metadati o aggiungere ridondanza o nuove funzionalità, esistono diversi requisiti dei nodi.

Seguire la procedura per il tipo di espansione che si sta eseguendo:

Aggiungere nodi griglia

1. Seguire la procedura per ["aggiunta di nodi griglia a un sito esistente"](#).
2. ["Aggiornare le subnet"](#).
3. Implementare nodi griglia:
 - ["Appliance"](#)
 - ["VMware"](#)
 - ["Linux"](#)



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

1. ["Eseguire l'espansione"](#).
2. ["Configurare il sistema espanso"](#).

Aggiungere volumi di storage

Seguire la procedura per ["Aggiunta di volumi di storage ai nodi di storage"](#).

Aggiungi nuovo sito

1. Seguire la procedura per ["Aggiunta di un nuovo sito"](#).
2. ["Aggiornare le subnet"](#).
3. Implementare nodi griglia:
 - ["Appliance"](#)
 - ["VMware"](#)
 - ["Linux"](#)



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

1. ["Eseguire l'espansione"](#).
2. ["Configurare il sistema espanso"](#).

Pianificazione dell'espansione

Pianificazione dell'espansione per i dati replicati in StorageGRID

Se il criterio ILM (Information Lifecycle Management) per l'implementazione include una regola che crea copie replicate di oggetti, è necessario considerare la quantità di storage da aggiungere e la posizione in cui aggiungere i nuovi volumi di storage o i nuovi nodi di storage.

Per informazioni su dove aggiungere storage aggiuntivo, esaminare le regole ILM che creano copie replicate. Se le regole ILM creano due o più copie di oggetti, pianificare di aggiungere storage in ogni posizione in cui vengono eseguite le copie di oggetti. Come semplice esempio, se si dispone di una griglia a due siti e di una regola ILM che crea una copia dell'oggetto in ogni sito, è necessario ["aggiungere storage"](#) in ogni sito per

aumentare la capacità complessiva dell'oggetto della griglia. Per informazioni sulla replica degli oggetti, vedere ["Cos'è la replica"](#).

Per motivi di performance, dovresti cercare di mantenere la capacità dello storage e la potenza di calcolo bilanciati tra i siti. Pertanto, per questo esempio, è necessario aggiungere lo stesso numero di nodi di storage a ciascun sito o volumi di storage aggiuntivi in ciascun sito.

Se si dispone di una policy ILM più complessa che include regole che posizionano oggetti in posizioni diverse in base a criteri come il nome del bucket o regole che cambiano le posizioni degli oggetti nel tempo, l'analisi dei punti in cui è richiesto lo storage per l'espansione sarà simile, ma più complessa.

La creazione di grafici sulla velocità di consumo della capacità di storage complessiva può aiutare a comprendere la quantità di storage da aggiungere all'espansione e quando sarà necessario lo spazio di storage aggiuntivo. È possibile utilizzare Grid Manager per ["monitorare e tracciare la capacità di storage"](#).

Quando si pianifica la tempistica di un'espansione, bisogna tenere presente quanto tempo potrebbe essere necessario per procurarsi e installare ulteriore spazio di archiviazione. Per semplificare la pianificazione dell'espansione, valutare l'aggiunta di nodi di archiviazione quando i nodi di archiviazione esistenti raggiungono il 70% della capacità.

Pianificazione dell'espansione per i dati con codice di cancellazione (EC) in StorageGRID

Se il criterio ILM include una regola che crea copie con codifica di cancellazione, è necessario pianificare dove aggiungere nuovo storage e quando aggiungere nuovo storage. La quantità di storage aggiunta e la tempistica dell'aggiunta possono influire sulla capacità di storage utilizzabile del grid.

Il primo passo nella pianificazione di un'espansione dello storage consiste nell'esaminare le regole dei criteri ILM che creano oggetti con codifica in cancellazione. Poiché StorageGRID crea $k+m$ frammenti per ogni oggetto con codifica di cancellazione e memorizza ciascun frammento su un nodo di storage diverso, è necessario assicurarsi che almeno $k+m$ nodi di storage abbiano spazio per i nuovi dati con codifica di cancellazione dopo l'espansione. Se il profilo di erasure coding fornisce la protezione dalla perdita di sito, è necessario aggiungere storage a ciascun sito. Vedere ["Cosa sono gli schemi di erasure coding"](#) per informazioni sui profili di erasure coding.

Il numero di nodi da aggiungere dipende anche dal livello di riempimento dei nodi esistenti quando si esegue l'espansione.

Raccomandazioni generali per l'aggiunta di capacità di storage per gli oggetti con codifica di cancellazione

Se si desidera evitare calcoli dettagliati, è possibile aggiungere due nodi di storage per sito quando i nodi di storage esistenti raggiungono il 70% della capacità.

Questa raccomandazione generale fornisce risultati ragionevoli in un'ampia gamma di schemi di erasure coding sia per le griglie a sito singolo che per le griglie in cui la codifica erasure fornisce protezione dalle perdite di sito.

Per comprendere meglio i fattori che hanno portato a questa raccomandazione o per sviluppare un piano più preciso per il vostro sito, vedere ["Considerazioni per il ribilanciamento dei dati con codifica erasure"](#). Per un consiglio personalizzato ottimizzato per la tua situazione, contatta il tuo consulente NetApp Professional Services.

Scopri di più sul ribilanciamento EC dopo l'espansione in StorageGRID

Se si sta eseguendo un'espansione per aggiungere nodi storage e si utilizzano le regole ILM per cancellare i dati, potrebbe essere necessario eseguire la procedura di riequilibrio EC (erasure coding) se non è possibile aggiungere nodi storage sufficienti per lo schema di erasure coding in uso.

Dopo aver esaminato queste considerazioni, eseguire l'espansione, quindi passare a ["Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage"](#) per eseguire la procedura.

Cos'è il ribilanciamento EC?

Il ribilanciamento EC è una procedura StorageGRID che potrebbe essere necessaria dopo l'espansione di un nodo di storage. La procedura viene eseguita come script della riga di comando dal nodo di amministrazione primario. Quando si esegue la procedura di ribilanciamento EC, StorageGRID ridistribuisce i frammenti con codifica erasure tra i nodi di storage esistenti e quelli appena aggiunti in un sito.

Procedura di ribilanciamento CE:

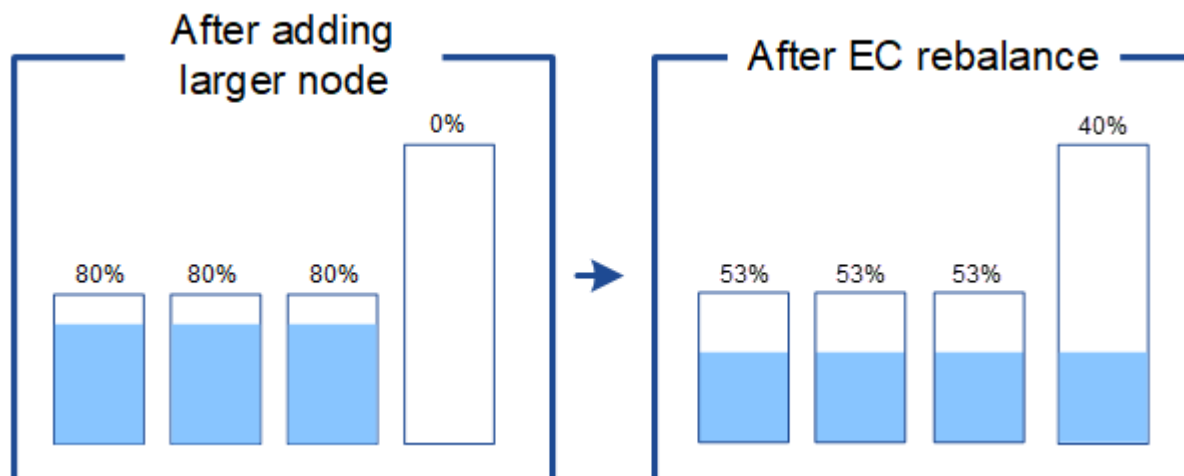
- Sposta solo i dati degli oggetti con codifica erasure. Non sposta i dati degli oggetti replicati.
- Ridistribuisce i dati all'interno di un sito. Non sposta i dati tra siti.
- Ridistribuisce i dati tra tutti i nodi di storage di un sito. Non ridistribuisce i dati all'interno dei volumi di storage.
- Tentativi di distribuire i byte di dati in modo che ogni nodo abbia lo stesso spazio utilizzabile. I nodi che contengono più dati replicati potrebbero memorizzare meno dati codificati con cancellazione dopo il completamento del ribilanciamento.
- Ridistribuisce lo spazio utilizzabile in modo uniforme tra i nodi di archiviazione senza considerare le capacità relative di ciascun nodo. I dati replicati sono inclusi nel calcolo.
- La procedura di ribilanciamento si considera completata se non è più possibile spostare dati codificati con cancellazione, anche se lo spazio utilizzabile non è ancora distribuito uniformemente.
- Non distribuirà i dati codificati per la cancellazione ai nodi di archiviazione che sono pieni per oltre l'80% o ai nodi di archiviazione che contengono solo metadati.
- Potrebbe diminuire le prestazioni delle operazioni ILM e delle operazioni client S3 quando viene eseguito—sono necessarie risorse aggiuntive per ridistribuire i frammenti di erasure coding.

Al termine della procedura di ribilanciamento EC:

- I dati con codifica erasure saranno stati spostati dai nodi di storage con meno spazio disponibile ai nodi di storage con più spazio disponibile.
- La protezione dei dati degli oggetti con codifica erasure rimane invariata.
- I valori utilizzati (%) potrebbero essere diversi tra i nodi di storage per due motivi:
 - Le copie replicate degli oggetti continueranno a consumare spazio sui nodi esistenti; la procedura di ribilanciamento EC non sposta i dati replicati.
 - I nodi con maggiore capacità potrebbero essere relativamente meno pieni rispetto ai nodi con minore capacità, anche se alla fine tutti i nodi avranno approssimativamente la stessa quantità di spazio utilizzabile.

Ad esempio, con uno schema di codifica di cancellazione 2+1, supponi che tre nodi da 200 TB siano

riempiti all'80% ($200 \times 0,8 = 160$ TB su ciascun nodo, ovvero 480 TB per il sito). Se aggiungi un nodo da 400 TB e esegui la procedura di ribilanciamento, tutti i nodi più vecchi avranno ora approssimativamente la stessa quantità di dati codificati con cancellazione (106,66 TB o 53% utilizzato). Il nuovo nodo avrà (160 TB di dati o 40% utilizzato). In questo caso, il Valore usato (%) per il nodo più grande sarà inferiore al Valore usato (%) per i nodi più piccoli. La procedura di ribilanciamento si completa prima che lo spazio utilizzabile sia bilanciato, poiché non è possibile spostare altri dati codificati con cancellazione senza violare i vincoli dello schema di codifica di cancellazione.



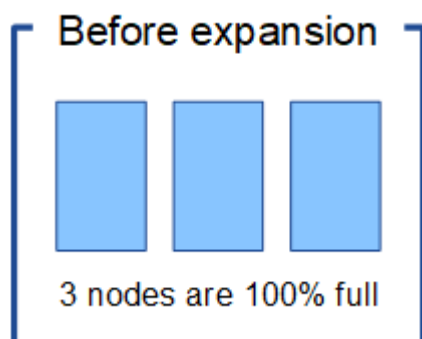
Quando ribilanciare i dati con codifica di cancellazione

La procedura di ribilanciamento EC ridistribuisce i dati codificati in modo da garantire che i nodi non diventino o rimangano pieni. La procedura aiuta a garantire che la codifica EC possa continuare sul sito.

Eseguire la procedura di ribilanciamento quando si verifica un errore preoccupante nella distribuzione dei dati su un sito e il sito memorizza principalmente dati EC (poiché i dati replicati non possono essere spostati tramite ribilanciamento).

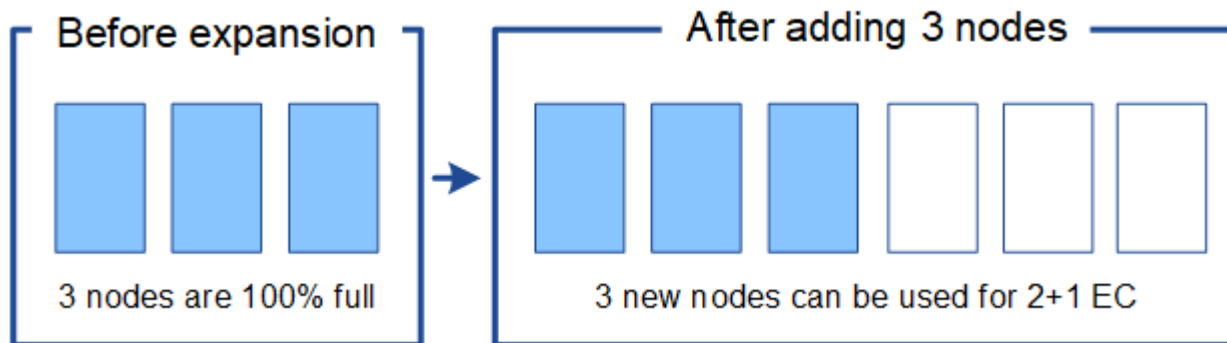
Considerare il seguente scenario:

- StorageGRID viene eseguito in un singolo sito, che contiene tre nodi di storage.
- Il criterio ILM utilizza una regola di erasure coding 2+1 per tutti gli oggetti più grandi di 1.0 MB e una regola di replica a 2 copie per gli oggetti più piccoli.
- Tutti i nodi di storage sono completamente pieni. L'avviso **Low Object Storage** è stato attivato al livello di gravità maggiore.



Il ribilanciamento non è necessario se aggiungi nodi a sufficienza

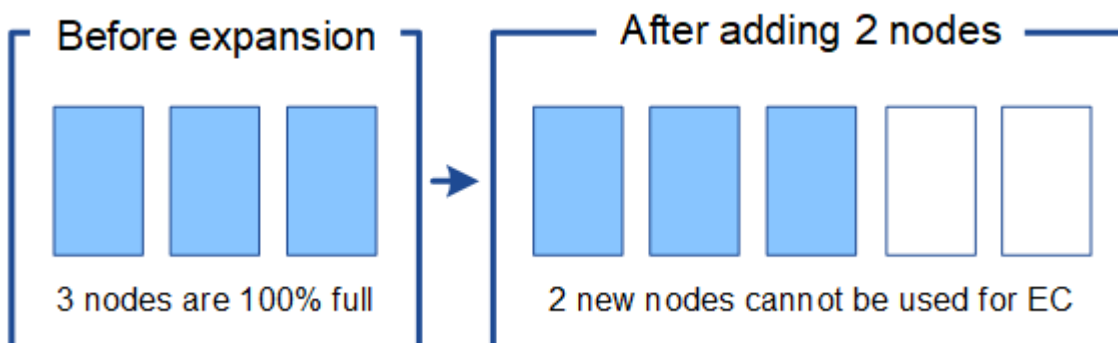
Per capire quando non è richiesto il ribilanciamento EC, supponiamo di aver aggiunto tre (o più) nuovi nodi di storage. In questo caso, non è necessario eseguire il ribilanciamento EC. I nodi di storage originali rimarranno pieni, ma i nuovi oggetti ora utilizzeranno i tre nuovi nodi per la codifica di cancellazione 2+1; i due frammenti di dati e un frammento di parità possono essere memorizzati su un nodo diverso.



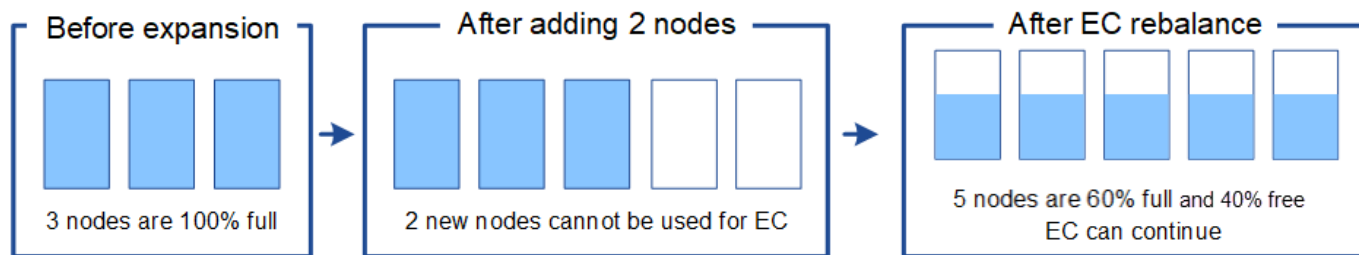
Anche se in questo caso è possibile eseguire la procedura di ribilanciamento EC, lo spostamento dei dati con codifica di cancellazione esistenti ridurrà temporaneamente le prestazioni della griglia, con un impatto sulle operazioni del client.

Il ribilanciamento è necessario se non è possibile aggiungere un numero sufficiente di nodi

Per capire quando è necessario ribilanciare EC, supponiamo di poter aggiungere solo due nodi storage, invece di tre. Poiché lo schema 2+1 richiede almeno tre nodi di storage per avere spazio disponibile, i nodi vuoti non possono essere utilizzati per i nuovi dati con codifica di cancellazione.



Per utilizzare i nuovi Storage Nodes, dovresti eseguire la procedura di ribilanciamento EC. Quando questa procedura viene eseguita, StorageGRID ridistribuisce i dati e i frammenti di parità codificati con cancellazione esistenti in modo che lo spazio utilizzabile sia distribuito uniformemente tra tutti i Storage Nodes del sito. In questo esempio, al termine della procedura di ribilanciamento EC, tutti e cinque i nodi sono ora pieni al 60% con il 40% di spazio utilizzabile e gli oggetti possono continuare a essere acquisiti nello schema di codifica con cancellazione 2+1 su tutti i Storage Nodes.



Raccomandazioni per il ribilanciamento CE

NetApp richiede il ribilanciamento EC se *tutte* le seguenti affermazioni sono vere:

- Si utilizza la codifica di cancellazione per i dati dell'oggetto.
- L'avviso **Low Object Storage** è stato attivato per uno o più nodi di storage in un sito, a indicare che i nodi sono pieni al 80% o più.
- Non è possibile aggiungere un numero sufficiente di nuovi nodi di storage per lo schema di erasure coding in uso. Vedere ["Aggiungere capacità di storage per gli oggetti con codifica per la cancellazione"](#).
- Durante l'esecuzione della procedura di ribilanciamento EC, i client S3 possono tollerare performance inferiori per le operazioni di scrittura e lettura.

Facoltativamente, è possibile eseguire la procedura di ribilanciamento EC se si preferisce che i nodi storage siano riempiti a livelli simili e i client S3 possono tollerare performance inferiori per le loro operazioni di scrittura e lettura mentre la procedura di riequilibrio EC è in esecuzione.

Come la procedura di ribilanciamento EC interagisce con altre attività di manutenzione

Non è possibile eseguire alcune procedure di manutenzione contemporaneamente all'esecuzione della procedura di ribilanciamento EC.

Procedura	Consentito durante la procedura di ribilanciamento EC?
Ulteriori procedure di ribilanciamento EC	No È possibile eseguire una sola procedura di ribilanciamento EC alla volta.
Procedura di decommissionamento Lavoro di riparazione dei dati EC	No • Non è possibile avviare una procedura di decommissionamento o una riparazione dei dati EC mentre è in esecuzione la procedura di ribilanciamento EC. • Non è possibile avviare la procedura di ribilanciamento EC mentre è in esecuzione una procedura di decommissionamento del nodo di storage o una riparazione dei dati EC.
Procedura di espansione	No Se è necessario aggiungere nuovi nodi di storage in un'espansione, eseguire la procedura di ribilanciamento EC dopo aver aggiunto tutti i nuovi nodi.

Procedura	Consentito durante la procedura di ribilanciamento EC?
Procedura di aggiornamento	No Se è necessario aggiornare il software StorageGRID, eseguire la procedura di aggiornamento prima o dopo l'esecuzione della procedura di ribilanciamento EC. Se necessario, è possibile terminare la procedura di ribilanciamento EC per eseguire un aggiornamento del software.
Procedura di clone del nodo dell'appliance	No Se è necessario clonare un nodo di storage dell'appliance, eseguire la procedura di ribilanciamento EC dopo aver aggiunto il nuovo nodo.
Procedura di hotfix	Sì. È possibile applicare una correzione rapida StorageGRID mentre è in esecuzione la procedura di ribilanciamento EC.
Altre procedure di manutenzione	No È necessario terminare la procedura di ribilanciamento EC prima di eseguire altre procedure di manutenzione.

Come la procedura di ribilanciamento EC interagisce con ILM

Durante l'esecuzione della procedura di ribilanciamento EC, evitare di apportare modifiche ILM che potrebbero modificare la posizione degli oggetti con codifica di cancellazione esistenti. Ad esempio, non iniziare a utilizzare una regola ILM con un profilo di erasure coding diverso. Se è necessario apportare tali modifiche ILM, interrompere la procedura di ribilanciamento EC.

Linee guida per l'espansione

Linee guida per l'aggiunta di capacità di oggetti in StorageGRID

È possibile espandere la capacità dello storage a oggetti del sistema StorageGRID aggiungendo volumi di storage ai nodi di storage esistenti o aggiungendo nuovi nodi di storage ai siti esistenti. È necessario aggiungere capacità di storage in modo che soddisfi i requisiti della policy ILM (Information Lifecycle Management).

Linee guida per l'aggiunta di volumi di storage

Prima di aggiungere volumi di storage ai nodi di storage esistenti, consultare le seguenti linee guida e limitazioni:

- È necessario esaminare le regole ILM correnti per determinare dove e quando ["aggiungere volumi di storage"](#) aumentare lo spazio di archiviazione disponibile per ["oggetti replicati"](#) o ["oggetti con codifica erasure"](#).
- Non è possibile aumentare la capacità dei metadati del sistema aggiungendo volumi di storage perché i metadati degli oggetti vengono memorizzati solo sul volume 0.

- Ogni nodo di storage basato su software può supportare un massimo di 48 volumi di storage. Se è necessario aggiungere capacità oltre tale limite, è necessario aggiungere nuovi nodi di storage.
- Puoi aggiungere uno o due shelf di espansione a ogni appliance SG6060. Ogni shelf di espansione aggiunge 16 volumi di storage. Con i due shelf di espansione installati, SG6060 supporta un totale di 48 volumi di storage.
- Puoi aggiungere uno o due shelf di espansione a ogni appliance SG6160. Ogni shelf di espansione aggiunge 60 volumi di storage. Con i due shelf di espansione installati, SG6160 supporta un totale di 180 volumi di storage.
- Non è possibile aggiungere volumi di storage ad altre appliance di storage.
- Non è possibile aumentare le dimensioni di un volume di storage esistente.
- Non è possibile aggiungere volumi di storage a un nodo di storage contemporaneamente all'aggiornamento del sistema, all'operazione di recovery o a un'altra espansione.

Dopo aver deciso di aggiungere volumi di storage e aver determinato i nodi di storage da espandere per soddisfare la policy ILM, seguire le istruzioni relative al tipo di nodo di storage:

- Per aggiungere uno o due shelf di espansione a un'appliance di archiviazione SG6060, visitare il sito ["Aggiungi shelf di espansione alla piattaforma SG6060 implementata"](#).
- Per aggiungere uno o due shelf di espansione a un'appliance di storage SG6160, passare al ["Aggiungi shelf di espansione alla piattaforma SG6160 implementata"](#)
- Per un nodo basato su software, seguire le istruzioni per ["Aggiunta di volumi di storage ai nodi di storage"](#).

Linee guida per l'aggiunta di nodi di storage

Prima di aggiungere nodi di storage ai siti esistenti, consultare le seguenti linee guida e limitazioni:

- È necessario esaminare le regole ILM correnti per determinare dove e quando aggiungere nodi di archiviazione per aumentare lo spazio di archiviazione disponibile per ["oggetti replicati"](#) o ["oggetti con codifica erasure"](#).
- Non aggiungere più di 10 nodi di storage in una singola procedura di espansione.
- È possibile aggiungere nodi di storage a più siti in una singola procedura di espansione.
- È possibile aggiungere nodi di storage e altri tipi di nodi in una singola procedura di espansione.
- Prima di avviare la procedura di espansione, è necessario confermare che tutte le operazioni di riparazione dei dati eseguite nell'ambito di un ripristino sono state completate. Vedere ["Controllare i lavori di riparazione dei dati"](#).
- Se è necessario rimuovere i nodi di storage prima o dopo l'esecuzione di un'espansione, non è necessario decommissionare più di 10 nodi di storage in una singola procedura Decommission Node.
- Aggiungere un numero sufficiente di nodi di archiviazione per mantenere le prestazioni di I/O dell'archiviazione sottostante. Le operazioni di scrittura verranno distribuite tra i nodi di archiviazione in base alla capacità di archiviazione disponibile. Se i nodi di archiviazione espansi dispongono di una capacità di archiviazione disponibile significativamente maggiore, tali nodi riceveranno un numero significativamente maggiore di scritture. In particolare, quando i nodi di archiviazione esistenti sono quasi pieni, le nuove scritture si baseranno solo sui nodi di archiviazione espansi. Le operazioni di lettura ed eliminazione saranno gestite in base al tuo carico di lavoro specifico.

Linee guida per il servizio ADC sui nodi di storage

Quando si configura l'espansione, è necessario scegliere se includere il servizio ADC (Administrative Domain

Controller) in ogni nuovo nodo di storage. Il servizio ADC tiene traccia della posizione e della disponibilità dei servizi grid.

- È possibile ["spostare il servizio ADC da un nodo di archiviazione a un altro sullo stesso sito"](#) Potrebbe
- Il sistema StorageGRID richiede che un ["Quorum dei servizi ADC"](#) sia sempre disponibile in ogni sito.
- Almeno tre nodi di storage in ogni sito devono includere il servizio ADC.
- Si sconsiglia di aggiungere il servizio ADC a ogni nodo di storage. L'inclusione di un numero eccessivo di servizi ADC può causare rallentamenti dovuti all'aumento della comunicazione tra i nodi.
- Un singolo grid non deve avere più di 48 nodi di storage con il servizio ADC. Ciò equivale a 16 siti con tre servizi ADC in ogni sito.
- In generale, quando si seleziona l'impostazione **Servizio ADC** per un nuovo nodo, 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 troppi pochi servizi ADC, selezionando **Sì** si garantisce che un nuovo servizio ADC sia disponibile prima che il vecchio servizio venga rimosso.

Linee guida per l'aggiunta di capacità di metadati in StorageGRID

Per garantire che sia disponibile spazio adeguato per i metadati degli oggetti, potrebbe essere necessario eseguire una procedura di espansione per aggiungere nuovi nodi di storage in ogni sito.

StorageGRID riserva spazio per i metadati degli oggetti sul volume 0 di ciascun nodo di storage. In ogni sito vengono conservate tre copie di tutti i metadati degli oggetti, distribuite uniformemente in tutti i nodi di storage.

È possibile utilizzare Grid Manager per monitorare la capacità dei metadati dei nodi di storage e stimare la velocità di utilizzo della capacità dei metadati. Inoltre, l'avviso **Low metadata storage** viene attivato per un nodo di storage quando lo spazio di metadati utilizzato raggiunge determinate soglie.

Si noti che la capacità dei metadati degli oggetti di una griglia potrebbe essere consumata più rapidamente rispetto alla capacità dello storage a oggetti, a seconda di come si utilizza la griglia. Ad esempio, se in genere si acquisiscono grandi quantità di oggetti di piccole dimensioni o si aggiungono grandi quantità di metadati o tag utente agli oggetti, potrebbe essere necessario aggiungere nodi di storage per aumentare la capacità dei metadati anche se rimane sufficiente capacità di storage a oggetti.

Per ulteriori informazioni, vedere quanto segue:

- ["Gestire lo storage dei metadati degli oggetti"](#)
- ["Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage"](#)

Linee guida per aumentare la capacità dei metadati

Prima di aggiungere nodi di storage per aumentare la capacità dei metadati, consultare le seguenti linee guida e limitazioni:

- Supponendo che sia disponibile una capacità di storage a oggetti sufficiente, avere più spazio disponibile per i metadati a oggetti aumenta il numero di oggetti che è possibile memorizzare nel sistema StorageGRID.
- È possibile aumentare la capacità dei metadati di un grid aggiungendo uno o più nodi di storage a ciascun sito.

- Lo spazio effettivo riservato ai metadati dell'oggetto su qualsiasi nodo di storage specifico dipende dall'opzione di storage Metadata Reserved Space (impostazione a livello di sistema), dalla quantità di RAM allocata al nodo e dalla dimensione del volume 0 del nodo.
- Non è possibile aumentare la capacità dei metadati aggiungendo volumi di storage ai nodi di storage esistenti, perché i metadati vengono memorizzati solo sul volume 0.
- Non è possibile aumentare la capacità dei metadati aggiungendo un nuovo sito.
- StorageGRID conserva tre copie di tutti i metadati degli oggetti in ogni sito. Per questo motivo, la capacità dei metadati del sistema è limitata dalla capacità dei metadati del sito più piccolo.
- Quando si aggiunge la capacità dei metadati, è necessario aggiungere lo stesso numero di nodi di storage a ciascun sito.

I nodi di storage solo per metadati hanno requisiti hardware specifici:

- Quando si utilizzano appliance StorageGRID, i nodi con soli 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 di solo metadati devono corrispondere alle risorse dei nodi di storage esistenti. Ad esempio:
 - Se il sito StorageGRID esistente utilizza appliance SG6000 o SG6100, i nodi basati solo sui metadati software devono soddisfare i seguenti requisiti minimi:
 - 128 GB DI RAM
 - CPU a 8 core
 - SSD da 8 TB o storage equivalente per il database Cassandra (rangedb/0)
 - Se il sito StorageGRID esistente utilizza nodi di archiviazione 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 almeno StorageGRID corrispondere ai nodi storage dei siti StorageGRID esistenti e alle nuove risorse del sito.

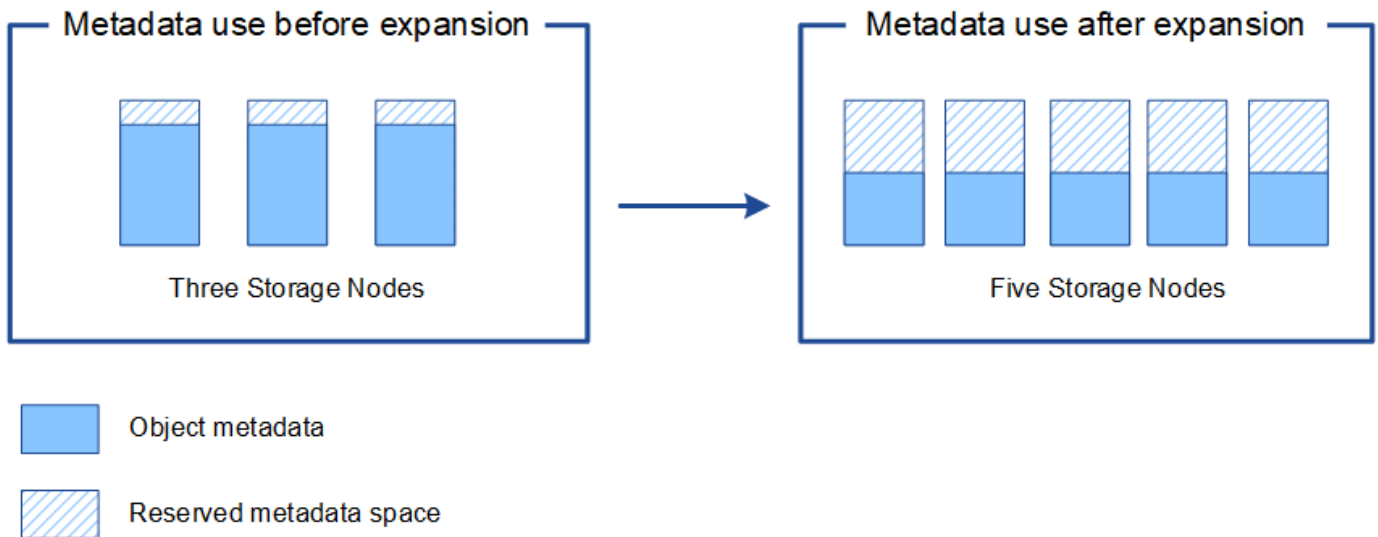
Consultare la ["Descrizione di Metadata Reserved Space"](#).

Come vengono ridistribuiti i metadati quando si aggiungono nodi di storage

Quando si aggiungono nodi di storage in un'espansione, StorageGRID ridistribuisce i metadati degli oggetti esistenti nei nuovi nodi di ciascun sito, aumentando così la capacità complessiva dei metadati del grid. Non è richiesta alcuna azione da parte dell'utente.

La figura seguente mostra come StorageGRID ridistribuisce i metadati degli oggetti quando si aggiungono nodi di storage in un'espansione. Il lato sinistro della figura rappresenta il volume 0 di tre nodi di storage prima di un'espansione. I metadati consumano una porzione relativamente grande dello spazio di metadati disponibile di ciascun nodo ed è stato attivato l'avviso **Low metadata storage**.

Il lato destro della figura mostra come vengono ridistribuiti i metadati esistenti dopo l'aggiunta di due nodi di storage al sito. La quantità di metadati su ciascun nodo è diminuita, l'avviso **Low metadata storage** non viene più attivato e lo spazio disponibile per i metadati è aumentato.



Linee guida per l'aggiunta di nodi di griglia in StorageGRID

È possibile aggiungere ridondanza o funzionalità aggiuntive a un sistema StorageGRID aggiungendo nuovi nodi grid ai siti esistenti.

Ad esempio, è possibile scegliere di aggiungere nodi gateway da utilizzare in un gruppo ad alta disponibilità (ha) oppure aggiungere un nodo amministratore in un sito remoto per consentire il monitoraggio utilizzando un nodo locale.

È possibile aggiungere uno o più dei seguenti tipi di nodi a uno o più siti esistenti in una singola operazione di espansione:

- Nodi amministrativi non primari
- Nodi di storage
- Nodi gateway

Durante la preparazione all'aggiunta di nodi di rete, tenere presente le seguenti limitazioni:

- Il nodo di amministrazione primario viene implementato durante l'installazione iniziale. Non è possibile aggiungere un nodo amministratore primario durante un'espansione.
- È possibile aggiungere nodi di storage e altri tipi di nodi nella stessa espansione.
- Quando si aggiungono nodi di storage, è necessario pianificare attentamente il numero e la posizione dei nuovi nodi. Vedere ["Linee guida per l'aggiunta della capacità degli oggetti"](#).
- Se l'opzione **Imposta nuovo nodo predefinito** è **Non attendibile** nella scheda Reti client non attendibili 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 l'impostazione di sicurezza per il nuovo nodo"](#) e ["configurare gli endpoint del bilanciamento del carico"](#).

Linee guida per l'aggiunta di un nuovo sito in StorageGRID

È possibile espandere il sistema StorageGRID aggiungendo un nuovo sito.

Linee guida per l'aggiunta di un sito

Prima di aggiungere un sito, esaminare i seguenti requisiti e limitazioni:

- È possibile aggiungere un solo sito per ciascuna operazione di espansione.
- Non è possibile aggiungere nodi grid a un sito esistente come parte della stessa espansione.
- Tutti i siti devono includere almeno tre Storage Node. Possono essere una qualsiasi combinazione di Storage Node combinati e Storage Node solo metadati. Se sono presenti più di tre Storage Node, possono essere una qualsiasi combinazione di Storage Node combinati, solo metadati e solo dati, purché siano disponibili tre servizi ADC. Per ulteriori informazioni, consulta ["Nodi di archiviazione richiesti per griglia e per sito"](#).
- Quando aggiungi un nuovo sito, il numero di oggetti che puoi archiviare non aumenta automaticamente. La capacità totale di oggetti di una grid dipende dalla quantità di storage disponibile, dalla policy ILM e dalla capacità dei metadati in ciascun sito.
- Quando si ridimensiona un nuovo sito, è necessario assicurarsi che includa una capacità di metadati sufficiente.

StorageGRID conserva una copia di tutti i metadati in ogni sito. Quando aggiungi un nuovo sito, assicurati che includa una capacità di metadati sufficiente sia per i metadati degli oggetti esistenti sia per la crescita futura.

Per ulteriori informazioni, consulta quanto segue:

- ["Gestire lo storage dei metadati degli oggetti"](#)
- ["Monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage"](#)
- È necessario considerare la larghezza di banda della rete disponibile tra i siti e il livello di latenza della rete. Gli aggiornamenti dei metadati vengono continuamente replicati tra i siti anche se tutti gli oggetti vengono memorizzati solo nel sito in cui vengono acquisiti.

Per evitare prestazioni scadenti dovute alla latenza:

- La codifica di cancellazione non è raccomandata tra siti con una latenza superiore a 100 ms.
- I siti nel tuo sistema StorageGRID non dovrebbero estendersi su ampie distanze geografiche, ad esempio su più continenti.
- Poiché il sistema StorageGRID rimane operativo durante l'espansione, è necessario rivedere le regole ILM prima di avviare la procedura di espansione. È necessario assicurarsi che le copie a oggetti non vengano memorizzate nel nuovo sito fino al completamento della procedura di espansione.

Ad esempio, prima di iniziare l'espansione, verifica se alcune regole utilizzano il pool di storage predefinito (All Storage Nodes). Se lo fanno, crea un nuovo pool di storage con i nodi di archiviazione esistenti e aggiorna le regole ILM per utilizzare il nuovo pool di storage. Altrimenti, gli oggetti vengono copiati nel nuovo sito non appena il primo nodo di quel sito diventa attivo.

Per ulteriori informazioni sulla modifica di una policy ILM durante l'aggiunta di un nuovo sito, consulta la ["Esempio di modifica di un criterio ILM"](#).

Preparati ad espandere il tuo sistema StorageGRID

Prima di eseguire un'operazione di espansione, raccogliere i materiali e installare e configurare eventuali nuovi hardware e reti.

Elemento	Note
Archivio di installazione di StorageGRID	Se si aggiungono nuovi nodi di griglia o un nuovo sito, è necessario scaricare ed estrarre l'archivio di installazione di StorageGRID. È necessario utilizzare la stessa versione attualmente in esecuzione sulla griglia. Per ulteriori informazioni, vedere le istruzioni di Download ed estrazione dei file di installazione di StorageGRID. Nota: non è necessario scaricare i file se si aggiungono nuovi volumi di storage ai nodi di storage esistenti o si installa una nuova appliance StorageGRID.
Laptop di assistenza	Il laptop di assistenza dispone di quanto segue: • Porta di rete • Client SSH (ad esempio, putty) • "Browser Web supportato"
Passwords.txt file	Contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando. Incluso nel pacchetto di recupero.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è contenuta nel Passwords.txt file.
Documentazione StorageGRID	• "Amministrare StorageGRID" • "Note di rilascio". È necessario accedere con il proprio account NetApp o crearne uno per accedere alle note di rilascio. • "Istruzioni per l'installazione della piattaforma"
Documentazione aggiornata per la piattaforma	Per le versioni supportate, vedere "Tool di matrice di interoperabilità (IMT)" .

Scaricare ed estrarre i file di installazione di StorageGRID

Prima di poter aggiungere nuovi nodi grid o un nuovo sito, è necessario scaricare l'archivio di installazione StorageGRID appropriato ed estrarre i file.

A proposito di questa attività

È necessario eseguire operazioni di espansione utilizzando la versione di StorageGRID attualmente in esecuzione sulla griglia.

Fasi

1. Andare a ["Download NetApp: StorageGRID"](#).
2. Selezionare la versione di StorageGRID attualmente in esecuzione nella griglia.

3. Accedi con il nome utente e la password del tuo account NetApp.
4. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
5. Nella colonna **Installa StorageGRID** della pagina di download, selezionare il .tgz file o .zip per la propria piattaforma.

La versione mostrata nel file di archivio dell'installazione deve corrispondere alla versione del software attualmente installato.

Utilizzare il .zip file se sul laptop di assistenza è in esecuzione Windows.

Piattaforma	Archivio di installazione
RHEL	StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .zip StorageGRID-Webscale- <i>version</i> -RPM- <i>uniqueID</i> .tgz
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 implementare una macchina virtuale che esegue una delle distribuzioni Linux supportate elencate sopra e seguire le istruzioni appropriate per Linux.

6. Scaricare ed estrarre il file di archivio.
7. Seguire la fase appropriata per la piattaforma per scegliere i file necessari, in base alla piattaforma, alla topologia della griglia pianificata e al modo in cui si espanderà il sistema StorageGRID.

I percorsi elencati nella fase per ciascuna piattaforma sono relativi alla directory di primo livello installata dal file di archivio.

8. Se si sta espandendo un sistema RHEL, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Pacchetto RPM per l'installazione delle immagini del nodo StorageGRID sui vostri host RHEL.

Percorso e nome del file	Descrizione
	Pacchetto RPM per l'installazione del servizio host StorageGRID sugli host RHEL.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Esempio di ruolo e playbook Ansible per la configurazione degli host RHEL per l'implementazione dei container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Uno script di supporto chiamato dallo script Python associato <code>storagegrid-ssoauth-azure.py</code> per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema Ubuntu o Debian, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	MD5 checksum 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.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.

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

1. Se si sta espandendo un sistema VMware, selezionare i file appropriati.

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file modello Open Virtualization Format (<code>.ovf</code>) e il file manifest) (<code>.mf</code> per la distribuzione del nodo amministrativo primario.
	Il file modello (<code>.ovf</code>) e il file manifesto) (<code>.mf</code> per la distribuzione di nodi Admin non primari.
	Il file modello (<code>.ovf</code>) e il file manifesto) (<code>.mf</code> per la distribuzione dei nodi Gateway.
	Il file modello (<code>.ovf</code>) e il file manifesto) (<code>.mf</code> per la distribuzione dei nodi di archiviazione basati su macchine virtuali.

Percorso e nome del file	Descrizione
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
	Un file di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> lo script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando è attivato il Single Sign-on (SSO). È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Uno script di supporto chiamato dallo script Python associato <code>storagegrid-ssoauth-azure.py</code> per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

1. Se si sta espandendo un sistema basato su appliance StorageGRID, selezionare i file appropriati.



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 in cui si esegue la procedura di ripristino.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini del nodo StorageGRID sulle appliance.
	MD5 checksum per il file /debs/storagegridwebscale-images-version-SHA.deb.

Verificare l'hardware e il collegamento in rete

Prima di iniziare l'espansione del sistema StorageGRID, verificare quanto segue:

- L'hardware necessario per supportare i nuovi nodi di rete o il nuovo sito è stato installato e configurato.
- Tutti i nuovi nodi dispongono di percorsi di comunicazione bidirezionali per tutti i nodi esistenti e nuovi (un requisito per la Grid Network). In particolare, verificare che le seguenti porte TCP siano aperte tra i nuovi nodi che si stanno aggiungendo nell'espansione e il nodo di amministrazione primario:
 - 1055
 - 7443
 - 8011
 - 10342

Vedere ["Comunicazioni interne al nodo di rete"](#).

- Il nodo di amministrazione primario può comunicare con tutti i server di espansione destinati a ospitare il sistema StorageGRID.
- Se uno dei nuovi nodi dispone di un indirizzo IP di rete su una subnet non utilizzata in precedenza, è già presente ["aggiunta della nuova subnet"](#)l'elenco delle subnet di rete griglia. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e avviare nuovamente la procedura.
- Non stai utilizzando la conversione degli indirizzi di rete (NAT) sulla rete di rete tra nodi di rete o tra siti StorageGRID. Quando si utilizzano indirizzi IPv4 privati per Grid Network, tali indirizzi devono essere direttamente instradabili da ogni nodo di griglia in ogni sito. L'utilizzo di NAT per il bridge della rete Grid attraverso un segmento di rete pubblica è supportato solo se si utilizza un'applicazione di tunneling trasparente per tutti i nodi della griglia, il che significa che i nodi della griglia non richiedono alcuna conoscenza degli indirizzi IP pubblici.

Questa restrizione NAT è specifica per i nodi di griglia e la rete di griglia. Se necessario, è possibile utilizzare NAT tra client esterni e nodi di rete, ad esempio per fornire un indirizzo IP pubblico per un nodo gateway.

Aggiunta di nodi o siti grid

Riepilogo del flusso di lavoro per l'aggiunta di nodi della griglia o nuovi siti a StorageGRID

Seguire questa procedura per aggiungere nodi di griglia a siti esistenti o per aggiungere un nuovo sito. È possibile eseguire un solo tipo di espansione alla volta.

Prima di iniziare

- Si dispone di ["Autorizzazione di accesso root o di manutenzione"](#).
- Tutti i nodi esistenti nel grid sono attivi e in esecuzione in tutti i siti.
- Tutte le precedenti procedure di espansione, aggiornamento, disattivazione o ripristino sono state completate.



Non è possibile avviare un'espansione mentre è in corso un'altra procedura di espansione, aggiornamento, ripristino o decommissionamento attivo. Tuttavia, se necessario, è possibile sospendere una procedura di decommissionamento per avviare un'espansione.

Fasi

1. ["Aggiorna le subnet per la rete Grid"](#).
2. ["Distribuisci i nuovi nodi della griglia"](#).
3. ["Eseguire l'espansione"](#).

Aggiungere o aggiornare le subnet alla rete Grid per l'espansione in StorageGRID

Quando si aggiungono nodi griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere sottoreti alla rete Grid.

StorageGRID mantiene un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete (eth0). Queste voci includono le subnet utilizzate per la rete griglia da ciascun sito nel sistema StorageGRID, nonché le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete griglia.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

A proposito di questa attività

Se uno dei nuovi nodi ha un indirizzo IP Grid Network su una subnet non utilizzata in precedenza, è necessario aggiungere la nuova subnet all'elenco Grid Network subnet prima di avviare l'espansione. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e avviare nuovamente la procedura.

Non utilizzare sottoreti che contengono i seguenti indirizzi IPv4 per la Grid Network, l'Admin Network o la Client Network di alcun nodo:

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



Ad esempio, non usare i seguenti intervalli di sottorete per la Grid Network, l'Admin Network o la Client Network di alcun nodo:

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

Fasi

1. Selezionare **Manutenzione > Rete > Rete di rete**.
2. Selezionare **Aggiungi un'altra subnet** per aggiungere una nuova subnet nella notazione CIDR.

Ad esempio, immettere 10.96.104.0/22.

3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.
 - b. Inserisci 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 in StorageGRID

I passaggi per l'implementazione di nuovi nodi grid in un'espansione sono gli stessi utilizzati al momento dell'installazione della griglia. Prima di eseguire l'espansione, è

necessario implementare tutti i nuovi nodi grid.

Quando si espande una griglia, i nodi aggiunti non devono corrispondere ai tipi di nodo esistenti. È possibile aggiungere nodi VMware, nodi Linux basati su container o nodi appliance.

VMware: Implementazione di nodi grid

È necessario implementare una macchina virtuale in VMware vSphere per ciascun nodo VMware che si desidera aggiungere all'espansione.

Fasi

1. ["Implementare il nuovo nodo come macchina virtuale"](#) e collegarlo a una o più reti StorageGRID .

Quando si implementa il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.

2. Dopo aver distribuito tutti i nuovi nodi VMware, ["eseguire la procedura di espansione"](#).

Linux: Implementazione di nodi grid

È possibile implementare nodi grid su nuovi host Linux o su host Linux esistenti. Se sono necessari altri host Linux per supportare i requisiti di CPU, RAM e storage dei nodi StorageGRID che si desidera aggiungere al grid, è necessario prepararli nello stesso modo in cui sono stati preparati gli host al momento dell'installazione. Quindi, i nodi di espansione vengono implementati nello stesso modo in cui vengono implementati i nodi di rete durante l'installazione.

Prima di iniziare

- Hai le istruzioni per installare StorageGRID per la tua versione di Linux e hai esaminato il ["requisiti hardware e di archiviazione"](#) .
- Se si prevede di implementare nuovi nodi grid su host esistenti, è stato confermato che gli host esistenti dispongono di CPU, RAM e capacità di storage sufficienti per i nodi aggiuntivi.
- Hai un piano per ridurre al minimo i domini di guasto. Ad esempio, non è necessario implementare tutti i nodi gateway su un singolo host fisico.



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

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

Fasi

1. Se si aggiungono nuovi host, accedere alle istruzioni di installazione per l'implementazione dei nodi StorageGRID.
2. Per implementare i nuovi host, seguire le istruzioni per la preparazione degli host.
3. Per creare file di configurazione del nodo e convalidare la configurazione StorageGRID, seguire le istruzioni per l'implementazione dei nodi Grid.
4. Se si aggiungono nodi a un nuovo host Linux, avviare il servizio host StorageGRID.
5. Se si aggiungono nodi a un host Linux esistente, avviare i nuovi nodi utilizzando l'interfaccia CLI del servizio host StorageGRID:
`sudo storagegrid node start [<node name>]`

Al termine

Dopo aver distribuito tutti i nuovi nodi della griglia, è possibile ["eseguire l'espansione"](#).

Appliance: Implementazione di storage, gateway o nodi di amministrazione non primari

Per installare il software StorageGRID su un nodo appliance, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance. In un'espansione, ogni appliance di storage funziona come un singolo nodo di storage e ogni appliance di servizi funziona come un singolo nodo di gateway o un nodo di amministrazione non primario. Qualsiasi appliance può connettersi a Grid Network, Admin Network e Client Network.

Prima di iniziare

- L'apparecchio è stato installato in un rack o in un cabinet, collegato alla rete e acceso.
- I passaggi sono stati completati ["Configurare l'hardware"](#).

La configurazione dell'hardware dell'appliance include i passaggi necessari per la configurazione delle connessioni StorageGRID (collegamenti di rete e indirizzi IP), nonché i passaggi facoltativi per abilitare la crittografia dei nodi, modificare la modalità RAID e rimappare le porte di rete.

- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete griglia nel nodo di amministrazione principale.
- Il firmware del programma di installazione dell'appliance StorageGRID sull'appliance sostitutiva è compatibile con la versione del software StorageGRID attualmente in esecuzione sulla griglia. Se le versioni non sono compatibili, è necessario aggiornare il firmware del programma di installazione dell'appliance StorageGRID.
- Si dispone di un laptop di assistenza con un ["browser web supportato"](#).
- Conosci uno degli indirizzi IP assegnati al controller di calcolo dell'appliance. È possibile utilizzare l'indirizzo IP per qualsiasi rete StorageGRID collegata.

A proposito di questa attività

Il processo di installazione di StorageGRID su un nodo appliance prevede le seguenti fasi:

- Specificare o confermare l'indirizzo IP del nodo Admin primario e il nome del nodo appliance.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.

Durante le attività di installazione dell'appliance, l'installazione viene interrotta. Per riprendere l'installazione, accedi a Grid Manager, approva tutti i nodi della griglia e completa il processo di installazione di StorageGRID.



Se è necessario implementare più nodi di appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando lo script di installazione `configure-sga.py` dell'appliance.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di elaborazione dell'appliance.

```
https://Controller_IP:8443
```

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Nella sezione connessione **Primary Admin Node**, determinare se è necessario specificare l'indirizzo IP per il nodo di amministrazione primario.

Se in precedenza sono stati installati altri nodi in questo data center, il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, supponendo che il nodo di amministrazione primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente sulla stessa sottorete.

3. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Immissione manuale dell'IP	a. Deselezionare la casella di controllo Enable Admin Node Discovery (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Selezionare Salva. d. Attendere che lo stato di connessione del nuovo indirizzo IP diventi pronto.
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo Enable Admin Node Discovery (attiva rilevamento nodo amministratore). b. Attendere che venga visualizzato l'elenco degli indirizzi IP rilevati. c. Selezionare il nodo di amministrazione principale per la griglia in cui verrà implementato il nodo di storage dell'appliance. d. Selezionare Salva. e. Attendere che lo stato di connessione del nuovo indirizzo IP diventi pronto.

4. Nel campo **Node name** (Nome nodo), immettere il nome che si desidera utilizzare per il nodo dell'appliance e selezionare **Save** (Salva).

Il nome del nodo viene assegnato al nodo dell'appliance nel sistema StorageGRID. Viene visualizzato nella pagina nodi (scheda Panoramica) di Grid Manager. Se necessario, è possibile modificare il nome quando si approva il nodo.

5. Nella sezione **Installazione**, verificare che lo stato corrente sia "Pronto per avviare l'installazione di *node name* nella griglia con nodo di amministrazione primario *admin_ip*" e che il pulsante **Avvia installazione** sia attivato.

Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

6. Dalla home page del programma di installazione dell'appliance StorageGRID, selezionare **Avvia installazione**.

Lo stato attuale cambia in "Installazione in corso" e viene visualizzata la pagina di installazione del monitor.

7. Se l'espansione include più nodi appliance, ripetere i passaggi precedenti per ogni appliance.



Se è necessario implementare più nodi storage dell'appliance contemporaneamente, è possibile automatizzare il processo di installazione utilizzando lo script di installazione dell'appliance `configure-sga.py`.

8. Se devi accedere manualmente alla pagina di installazione del monitor, seleziona **Installazione monitor** dalla barra dei menu.

La pagina di installazione di Monitor mostra lo stato di avanzamento dell'installazione.

La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.



Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta eseguendo nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "saltato".

9. Esaminare i progressi delle prime due fasi dell'installazione.

1. Configurare l'appliance

In questa fase, si verifica uno dei seguenti processi:

- Per un'appliance di storage, il programma di installazione si connette al controller dello storage, cancella qualsiasi configurazione esistente, comunica con SANtricity OS per configurare i volumi e configura le impostazioni dell'host.
- Per un'appliance di servizi, il programma di installazione cancella qualsiasi configurazione esistente dai dischi nel controller di calcolo e configura le impostazioni dell'host.

2. Installare il sistema operativo

In questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

10. Continuare a monitorare l'avanzamento dell'installazione fino a quando non viene visualizzato un messaggio nella finestra della console, che richiede di utilizzare Grid Manager per approvare il nodo.



Attendere che tutti i nodi aggiunti a questa espansione siano pronti per l'approvazione prima di passare al Grid Manager per approvare i nodi.

Eseguire un'espansione StorageGRID

Quando si esegue l'espansione, i nuovi nodi grid vengono aggiunti all'implementazione StorageGRID esistente.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone della passphrase di provisioning.
- Sono stati implementati tutti i nodi grid che vengono aggiunti in questa espansione.
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).

- Se si aggiungono nodi di storage, si conferma che tutte le operazioni di riparazione dei dati eseguite come parte di un ripristino sono state completate. Vedere ["Controllare i lavori di riparazione dei dati"](#).
- Se si aggiungono nodi di archiviazione e si desidera assegnare un grado di archiviazione personalizzato a tali nodi, si dispone già di ["creato il livello di storage personalizzato"](#). Si dispone anche dell'autorizzazione di accesso root o di entrambe le autorizzazioni Maintenance e ILM.
- Se si aggiunge un nuovo sito, sono state riviste e aggiornate le regole ILM. È necessario assicurarsi che le copie a oggetti non vengano memorizzate nel nuovo sito fino al completamento dell'espansione. Ad esempio, se una regola utilizza il pool di archiviazione predefinito (**tutti i nodi di archiviazione**), è necessario che ["creare un nuovo pool di storage"](#) contenga solo i nodi di archiviazione esistenti e ["Aggiornare le regole ILM"](#) il criterio ILM per utilizzare il nuovo pool di archiviazione. In caso contrario, gli oggetti verranno copiati nel nuovo sito non appena il primo nodo del sito diventa attivo.

A proposito di questa attività

L'esecuzione dell'espansione include le seguenti attività principali dell'utente:

1. Configurare l'espansione.
2. Avviare l'espansione.
3. Scarica un nuovo file del pacchetto di ripristino.
4. Monitorare le fasi e le fasi di espansione fino a quando tutti i nuovi nodi non vengono installati e configurati e tutti i servizi non vengono avviati.



Alcune fasi e fasi di espansione potrebbero richiedere molto tempo per essere eseguite su un grande grid. Ad esempio, lo streaming di Cassandra su un nuovo nodo di storage potrebbe richiedere solo pochi minuti se il database Cassandra è vuoto. Tuttavia, se il database Cassandra include una grande quantità di metadati degli oggetti, questa fase potrebbe richiedere diverse ore o più. Non riavviare i nodi di storage durante le fasi "espansione del cluster Cassandra" o "Avvio di Cassandra e dati in streaming".

Fasi

1. Seleziona **Manutenzione > Attività > Espansione griglia**.

Viene visualizzata la pagina di espansione della griglia. La sezione Nodi in sospenso elenca i nodi pronti per essere aggiunti.

2. Selezionare **Configure Expansion** (Configura espansione).

Viene visualizzata la finestra di dialogo Site Selection (selezione sito).

3. Selezionare il tipo di espansione che si desidera avviare:
 - Se si sta aggiungendo un nuovo sito, selezionare **nuovo** e immettere il nome del nuovo sito.
 - Se si aggiungono uno o più nodi a un sito esistente, selezionare **esistente**.

4. Selezionare **Salva**.

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

Se necessario, puoi posizionare il cursore su **Grid Network MAC Address** di un nodo per visualizzare i dettagli relativi a tale nodo.

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 manca un nodo, confermarne la corretta implementazione.

6. Dall'elenco dei nodi in sospeso, approvare i nodi che si desidera aggiungere a questa espansione.
 - a. Selezionare il pulsante di opzione accanto al primo nodo della griglia in sospeso che si desidera approvare.
 - b. Selezionare **approva**.

Viene visualizzato il modulo di configurazione del nodo della griglia.

- c. Se necessario, modificare le impostazioni generali:

Campo	Descrizione
Sito	Il nome del sito a cui verrà associato il nodo della griglia. Se si aggiungono più nodi, assicurarsi di selezionare il sito corretto per ciascun nodo. Se si aggiunge un nuovo sito, tutti i nodi vengono aggiunti al nuovo sito.
Nome	Il nome di sistema del nodo. I nomi di sistema sono richiesti per le operazioni StorageGRID interne e non possono essere modificati.
Tipo di storage (solo nodi storage)	• Dati e metadati ("combinati"): Nodo di archiviazione di metadati e dati oggetto • Solo dati: Nodo di storage contenente solo dati oggetto (nessun metadati) • Solo metadati: Nodo di storage contenente solo metadati (nessun dato oggetto)

Campo	Descrizione
Ruolo NTP	Il ruolo NTP (Network Time Protocol) del nodo Grid: • Selezionare automatico (impostazione predefinita) per assegnare automaticamente il ruolo NTP al nodo. Il ruolo primario verrà assegnato ai nodi di amministrazione, ai nodi di storage con servizi ADC, ai nodi gateway e a tutti i nodi grid che hanno indirizzi IP non statici. Il ruolo Client verrà assegnato a tutti gli altri nodi della griglia. • Selezionare Primary per assegnare manualmente il ruolo Primary NTP al nodo. Almeno due nodi in ogni sito devono avere il ruolo primario per fornire un accesso ridondante al sistema a fonti di tempistica esterne. • Selezionare Client per assegnare manualmente il ruolo NTP client al nodo.
Servizio ADC (nodi di storage 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. • 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, questa impostazione garantisce che un nuovo servizio ADC sia disponibile prima che il vecchio servizio venga rimosso. • Puoi "spostare il servizio ADC su un altro nodo di archiviazione nello stesso sito" per garantire che venga raggiunto il quorum di servizio ADC. • Selezionare automatico per consentire al sistema di determinare se questo nodo richiede il servizio ADC. Informazioni su "Quorum ADC".
Grado dello storage (nodi storage combinati o solo dati)	Utilizzare il livello di storage Default o selezionare il livello di storage personalizzato che si desidera assegnare al nuovo nodo. I livelli di storage vengono utilizzati dai pool di storage ILM, in modo che la selezione possa influire sugli oggetti da posizionare nel nodo di storage.

d. Se necessario, modificare le impostazioni per Grid Network, Admin Network e Client Network.

- **IPv4 Address (CIDR):** Indirizzo di rete CIDR per l'interfaccia di rete. Ad esempio:
172.16.10.100/24



Se si scopre che i nodi hanno indirizzi IP duplicati sulla rete Grid durante l'approvazione dei nodi, è necessario annullare l'espansione, ridistribuire le macchine virtuali o le appliance con un IP non duplicato e riavviare l'espansione.

- **Gateway:** Il gateway predefinito del nodo Grid. Ad esempio: 172.16.10.1
- **Subnet (CIDR):** Una o più sottoreti per la rete di amministrazione.

e. Selezionare **Salva**.

Il nodo della griglia approvata passa all'elenco dei nodi approvati.

- Per modificare le proprietà di un nodo della griglia approvato, selezionare il relativo pulsante di opzione e selezionare **Modifica**.
- Per spostare di nuovo un nodo della griglia approvato nell'elenco Pending Nodes (nodi in sospeso), selezionare il relativo pulsante di opzione e selezionare **Reset** (Ripristina).
- Per rimuovere in modo permanente un nodo di rete approvato, spegnere il nodo. Quindi, selezionare il pulsante di opzione corrispondente e selezionare **Rimuovi**.

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



Se possibile, è necessario approvare tutte le note della griglia in sospeso ed eseguire una singola espansione. Se si eseguono più piccole espansioni, sarà necessario più tempo.

7. Dopo aver approvato tutti i nodi della griglia, inserisci la **passphrase di provisioning** e seleziona **Espandi**.

Dopo alcuni minuti, questa pagina viene aggiornata per visualizzare lo stato della procedura di espansione. Quando sono in corso attività che influiscono sui singoli nodi della griglia, la sezione Grid Node Status (Stato nodo griglia) elenca lo stato corrente di ciascun nodo della griglia.



Durante la fase "Installazione dei nodi griglia" per una nuova appliance, il programma di installazione dell'appliance StorageGRID mostra il passaggio dall'installazione della fase 3 alla fase 4, completamento dell'installazione. Al termine della fase 4, il controller viene riavviato.



Un'espansione del sito include un'attività aggiuntiva per configurare Cassandra per il nuovo sito.

8. Non appena 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 del pacchetto di ripristino consente di ripristinare il sistema in caso di errore.

- Selezionare il collegamento per il download.
- Inserire la passphrase di provisioning e selezionare **Avvia download**.
- Al termine del download, aprire il .zip file e confermare che sia 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 storage a un sito esistente o si aggiunge un sito, monitorare le fasi di Cassandra, che si verificano quando i servizi vengono avviati sui nuovi nodi di griglia.



Non riavviare i nodi di storage durante le fasi di "espansione del cluster Cassandra" o "avvio di Cassandra e dati in streaming". Il completamento di queste fasi potrebbe richiedere molte ore per ogni nuovo nodo di storage, soprattutto se i nodi di storage esistenti contengono una grande quantità di metadati degli oggetti.

Aggiunta di nodi di storage

Se si aggiungono nodi di storage a un sito esistente, esaminare la percentuale indicata nel messaggio di stato "Avvio di Cassandra e streaming dei dati".

Questa percentuale stima il completamento dell'operazione di streaming Cassandra in base alla quantità totale di dati Cassandra disponibili e alla quantità già scritta nel nuovo nodo.

Aggiunta del sito

Se si aggiunge un nuovo sito, utilizzare `nodetool status` per monitorare l'avanzamento dello streaming Cassandra e per vedere quanti metadati sono stati copiati nel nuovo sito durante la fase "espansione del cluster Cassandra". Il carico totale di dati sul nuovo sito deve essere inferiore a circa il 20% del totale di un sito corrente.

10. Continuare a monitorare l'espansione fino al completamento di tutte le attività e alla ricomposizione del pulsante **Configure Expansion** (Configura espansione).

Al termine

A seconda dei tipi di nodi griglia aggiunti, eseguire ulteriori operazioni di integrazione e configurazione. Vedere ["Fasi di configurazione dopo l'espansione"](#).

Aggiungere volumi di storage

Aggiungi volumi di archiviazione al tuo sistema StorageGRID

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 storage, esaminare la ["linee guida per l'aggiunta della capacità degli oggetti"](#) per assicurarsi di sapere dove aggiungere volumi per soddisfare i requisiti del criterio ILM.



Queste istruzioni sono valide solo per i nodi storage basati su software. Consultare ["Aggiungi shelf di espansione alla piattaforma SG6060 implementata"](#) o ["Aggiungi shelf di espansione alla piattaforma SG6160 implementata"](#) per informazioni su come aggiungere volumi di storage a SG6060 o SG6160 installando shelf di espansione. Impossibile espandere altri nodi storage dell'appliance.

A proposito di questa attività

Lo storage sottostante di un nodo di storage è suddiviso in volumi di storage. I volumi di storage sono

dispositivi di storage basati su blocchi formattati dal sistema StorageGRID e montati per memorizzare oggetti. Ciascun nodo di storage può supportare fino a 48 volumi di storage, denominati *archivi di oggetti* in Grid Manager.



I metadati degli oggetti sono sempre memorizzati nell'archivio di oggetti 0.

Ogni archivio di oggetti viene montato su un volume che corrisponde al relativo ID. Ad esempio, l'archivio oggetti con un ID di 0000 corrisponde al `/var/local/rangedb/0` punto di montaggio.

Prima di aggiungere nuovi volumi di storage, utilizzare Grid Manager per visualizzare gli archivi di oggetti correnti per ciascun nodo di storage e i punti di montaggio corrispondenti. È possibile utilizzare queste informazioni quando si aggiungono volumi di storage.

Fasi

1. Selezionare **Nodi** > **sito** > **Nodo di archiviazione** > **Archiviazione**.
2. Scorrere verso il basso per visualizzare le quantità di storage disponibili per ciascun volume e archivio di oggetti.

Per i nodi di storage dell'appliance, il nome globale di ciascun disco corrisponde all'identificativo mondiale del volume (WWID) visualizzato quando si visualizzano le proprietà dei volumi standard in SANtricity OS (il software di gestione collegato al controller di storage dell'appliance).

Per semplificare l'interpretazione delle statistiche di lettura e scrittura dei dischi relative ai punti di montaggio del volume, la prima parte del nome visualizzato nella colonna **Name** della tabella Disk Devices (periferiche disco) (ovvero *sdc*, *sdd*, *sde* e così via) corrisponde al valore visualizzato nella colonna **Device** della tabella Volumes (volumi).

Disk devices

Name ? ⇅	World Wide Name ? ⇅	I/O load ? ⇅	Read rate ? ⇅	Write rate ? ⇅
sdc(8:16,sdb)	N/A	0.05%	0 bytes/s	4 KB/s
sde(8:48,sdd)	N/A	0.00%	0 bytes/s	82 bytes/s
sdf(8:64,sde)	N/A	0.00%	0 bytes/s	82 bytes/s
sdg(8:80,sdf)	N/A	0.00%	0 bytes/s	82 bytes/s
sdd(8:32,sdc)	N/A	0.00%	0 bytes/s	82 bytes/s
croot(8:1,sda1)	N/A	0.04%	0 bytes/s	4 KB/s
cvloc(8:2,sda2)	N/A	0.95%	0 bytes/s	52 KB/s

Volumes

Mount point ? ⇅	Device ? ⇅	Status ? ⇅	Size ? ⇅	Available ? ⇅	Write cache status ? ⇅
/	croot	Online	21.00 GB	14.73 GB 	Unknown
/var/local	cvloc	Online	85.86 GB	80.94 GB 	Unknown
/var/local/rangedb/0	sdc	Online	107.32 GB	107.17 GB 	Enabled
/var/local/rangedb/1	sdd	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/2	sde	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/3	sdf	Online	107.32 GB	107.18 GB 	Enabled
/var/local/rangedb/4	sdg	Online	107.32 GB	107.18 GB 	Enabled

Object stores

ID ? ⇅	Size ? ⇅	Available ? ⇅	Replicated data ? ⇅	EC data ? ⇅	Object data (%) ? ⇅	Health ? ⇅
0000	107.32 GB	96.44 GB 	1.55 MB 	0 bytes 	0.00%	No Errors
0001	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0002	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0003	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors
0004	107.32 GB	107.18 GB 	0 bytes 	0 bytes 	0.00%	No Errors

3. Seguire le istruzioni della piattaforma per aggiungere nuovi volumi di storage al nodo di storage.
 - ["VMware: Aggiunta di volumi di storage a Storage Node"](#)
 - ["Linux: Aggiunta di volumi direct-attached o SAN al nodo di storage"](#)

Aggiungere volumi di archiviazione ai nodi di archiviazione VMware in StorageGRID

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

- Hai accesso al ["istruzioni per l'installazione di StorageGRID per le distribuzioni VMware"](#).
- Si dispone del `Passwords.txt` file.
- Si dispone di ["autorizzazioni di accesso specifiche"](#).



Non tentare di aggiungere volumi di storage a un nodo di storage mentre è attiva una procedura di aggiornamento del software, di ripristino o un'altra procedura di espansione.

A proposito di questa attività

Il nodo di storage non è disponibile per un breve periodo di tempo quando si aggiungono volumi di storage. È necessario eseguire questa procedura su un nodo di storage alla volta per evitare impatti sui servizi grid rivolti al client.

Fasi

1. Se necessario, installare nuovo hardware per lo storage e creare nuovi datastore VMware.
2. Aggiungere uno o più dischi rigidi alla macchina virtuale per utilizzarli come storage (archivi di oggetti).
 - a. Aprire VMware vSphere Client.
 - b. Modificare le impostazioni della macchina virtuale per aggiungere uno o più dischi rigidi aggiuntivi.

I dischi rigidi sono in genere configurati come Virtual Machine Disk (VMDK). I VMDK sono più comunemente utilizzati e sono più facili da gestire, mentre i RDM potrebbero fornire performance migliori per i carichi di lavoro che utilizzano oggetti di dimensioni maggiori (ad esempio, superiori a 100 MB). Per ulteriori informazioni sull'aggiunta di dischi rigidi alle macchine virtuali, consultare la documentazione di VMware vSphere.

3. Riavviare la macchina virtuale utilizzando l'opzione **Restart Guest OS** nel client VMware vSphere o immettendo il seguente comando in una sessione ssh sulla macchina virtuale: `sudo reboot`



Non utilizzare **Power Off** o **Reset** per riavviare la macchina virtuale.

4. Configurare il nuovo storage per l'utilizzo da parte del nodo di storage:
 - a. Accedere al nodo Grid:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file. Quando si è collegati come root, il

prompt cambia da \$ a #.

- b. Configurare i nuovi volumi di storage:

```
sudo add_rangedbs.rb
```

Questo script trova i nuovi volumi di storage e richiede di formattarli.

- c. Immettere **y** per accettare la formattazione.
- d. Se uno dei volumi è stato precedentemente formattato, decidere se si desidera riformattarlo.
- Immettere **y** per riformattare.
 - Inserire **n** per saltare la riformattazione.

```
`setup_rangedbs.sh`Lo script viene eseguito automaticamente.
```

5. Verificare che i servizi vengano avviati correttamente:

- a. Visualizzare un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

- a. Attendere che tutti i servizi siano in esecuzione o verificati.
- b. Uscire dalla schermata di stato:

```
Ctrl+C
```

6. Verificare che il nodo di storage sia in linea:

- a. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
- b. Selezionare **Nodi > Nodo di archiviazione_ > Attività**.
- c. Se l'elenco a discesa **Stato di archiviazione** è impostato su Sola lettura o Offline, selezionare **Online**.
- d. Selezionare **Salva**.

7. Per visualizzare i nuovi archivi di oggetti, selezionare **Archiviazione**.

8. Visualizza i dettagli nella tabella **Volumi**.

Risultato

È possibile utilizzare la capacità estesa dei nodi di storage per salvare i dati degli oggetti.

Aggiungere volumi SAN o collegati direttamente ai nodi di archiviazione Linux in StorageGRID

Se un nodo di storage include meno di 48 volumi di storage, è possibile aumentarne la capacità aggiungendo nuovi dispositivi di storage a blocchi, rendendoli visibili agli host Linux e aggiungendo i nuovi mapping dei dispositivi a blocchi al file di configurazione StorageGRID utilizzato per il nodo di storage.

Prima di iniziare

- Hai accesso al ["istruzioni per l'installazione di StorageGRID"](#) per la tua piattaforma Linux.
- Si dispone del `Passwords.txt` file.
- Si dispone di ["autorizzazioni di accesso specifiche"](#).



Non tentare di aggiungere volumi di storage a un nodo di storage mentre è attiva una procedura di aggiornamento del software, di ripristino o un'altra procedura di espansione.

A proposito di questa attività

Il nodo di storage non è disponibile per un breve periodo di tempo quando si aggiungono volumi di storage. È necessario eseguire questa procedura su un nodo di storage alla volta per evitare impatti sui servizi grid rivolti al client.

Fasi

1. Installare il nuovo hardware di storage.

Per ulteriori informazioni, consultare la documentazione fornita dal fornitore dell'hardware.

2. Creare nuovi volumi di storage a blocchi delle dimensioni desiderate.

- Collegare le nuove unità e aggiornare la configurazione del controller RAID secondo necessità, oppure allocare le nuove LUN SAN sugli array di storage condivisi e consentire all'host Linux di accedervi.
- Utilizzare lo stesso schema di denominazione persistente utilizzato per i volumi di storage sul nodo di storage esistente.
- Se si utilizza la funzionalità di migrazione dei nodi StorageGRID, rendere visibili i nuovi volumi agli altri host Linux che sono destinazioni di migrazione per questo nodo di storage. Per ulteriori informazioni, consulta le istruzioni per l'installazione di StorageGRID per la tua piattaforma Linux.

3. Accedere all'host Linux che supporta il nodo di storage come root o con un account che dispone dell'autorizzazione sudo.

4. Verificare che i nuovi volumi di storage siano visibili sull'host Linux.

Potrebbe essere necessario eseguire una nuova scansione per le periferiche.

5. Eseguire il seguente comando per disattivare temporaneamente il nodo di storage:

```
sudo storagegrid node stop <node-name>
```

6. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo per il nodo di archiviazione, disponibile all'indirizzo `/etc/storagegrid/nodes/<node-name>.conf`.
7. Individuare la sezione del file di configurazione del nodo che contiene le mappature dei dispositivi di blocco dello storage a oggetti esistenti.

Nell'esempio, `BLOCK_DEVICE_RANGEDB_00` `BLOCK_DEVICE_RANGEDB_03` sono presenti le mappature dei dispositivi a blocchi di storage a 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 storage a oggetti corrispondenti ai volumi di storage a blocchi aggiunti per questo nodo di storage.

Assicurarsi di iniziare dal successivo `BLOCK_DEVICE_RANGEDB_nn`. Non lasciare un gap.

- In base all'esempio precedente, iniziare da `BLOCK_DEVICE_RANGEDB_04`.
- Nell'esempio seguente, al nodo sono stati aggiunti quattro nuovi volumi di storage 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 apportate al file di configurazione del nodo per il nodo di storage:

```
sudo storagegrid node validate <node-name>
```

Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

Se si osserva un errore simile a quanto segue, significa che il file di configurazione del nodo sta tentando di mappare il dispositivo a blocchi utilizzato da <node-name> per <PURPOSE> al dato <path-name> nel file system Linux, ma non esiste un file speciale del dispositivo a blocchi valido (o un softlink a un file speciale del 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
```

Verificare di aver immesso il corretto <path-name>.

10. Eseguire il seguente comando per riavviare il nodo con le nuove mappature del dispositivo a blocchi in posizione:

```
sudo storagegrid node start <node-name>
```

11. Accedere al nodo di archiviazione come amministratore utilizzando la password indicata nel `Passwords.txt` file.

12. Verificare che i servizi vengano avviati correttamente:

- a. Visualizzare un elenco dello stato di tutti i servizi sul server:

```
sudo storagegrid-status
```

Lo stato viene aggiornato automaticamente.

- b. Attendere che tutti i servizi siano in esecuzione o verificati.

- c. Uscire dalla schermata di stato:

```
Ctrl+C
```

13. Configurare il nuovo storage per l'utilizzo da parte del nodo di storage:

- a. Configurare i nuovi volumi di storage:

```
sudo add_rangedbs.rb
```

Questo script trova i nuovi volumi di storage e richiede di formattarli.

- b. Inserire **y** per formattare i volumi di storage.

- c. Se uno dei volumi è stato precedentemente formattato, decidere se si desidera riformattarlo.

- Immettere **y** per riformattare.
- Inserire **n** per saltare la riformattazione.

```
`setup_rangedbs.sh`Lo script viene eseguito automaticamente.
```

14. Verificare che lo stato di archiviazione del nodo di archiviazione sia online:

- a. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
- b. Selezionare **Nodi > Nodo di archiviazione_ > Attività**.
- c. Se l'elenco a discesa **Stato di archiviazione** è impostato su Sola lettura o Offline, selezionare **Online**.
- d. Selezionare **Salva**.

15. Per visualizzare i nuovi archivi di oggetti, selezionare **Archiviazione**.

16. Visualizza i dettagli nella tabella **Volumi**.

Risultato

È ora possibile utilizzare la capacità estesa dei nodi di storage per salvare i dati degli oggetti.

Configurare il sistema esteso

Configurare i nodi e i siti appena aggiunti in StorageGRID

Dopo aver completato un'espansione, è necessario eseguire ulteriori operazioni di integrazione e configurazione.

A proposito di questa attività

È necessario completare le attività di configurazione elencate di seguito per i nodi o i siti di griglia che si stanno aggiungendo all'espansione. Alcune attività potrebbero essere facoltative, a seconda delle opzioni selezionate durante l'installazione e l'amministrazione del sistema e di come si desidera configurare i nodi e i siti aggiunti durante l'espansione.

Fasi

1. Se è stato aggiunto un sito:
 - ["Creare un pool di storage"](#) Per il sito e ogni grado storage selezionato per i nuovi nodi storage.
 - Verificare che la policy ILM soddisfi i nuovi requisiti. Se sono necessarie modifiche alle regole, ["creare nuove regole"](#) e ["Aggiornare il criterio ILM"](#). Se le regole sono già corrette, ["attivare una nuova policy"](#) senza modifiche alle regole per garantire che StorageGRID utilizzi i nuovi nodi.
 - Verificare che i server NTP (Network Time Protocol) siano accessibili da tale sito. Vedere ["Gestire i server NTP"](#).



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

2. Se sono stati aggiunti uno o più nodi di storage a un sito esistente:
 - ["Visualizzare i dettagli del pool di storage"](#) Per confermare che ogni nodo aggiunto sia incluso nei pool di storage previsti e utilizzato nelle regole ILM previste.
 - Verificare che la policy ILM soddisfi i nuovi requisiti. Se sono necessarie modifiche alle regole, ["creare nuove regole"](#) e ["Aggiornare il criterio ILM"](#). Se le regole sono già corrette, ["attivare una nuova policy"](#) senza modifiche alle regole per garantire che StorageGRID utilizzi i nuovi nodi.
 - ["Verificare che il nodo di storage sia attivo"](#) e in grado di acquisire oggetti.
 - Se non è stato possibile aggiungere il numero consigliato di nodi di storage, ribilanciare i dati con

codifica di cancellazione. Vedere ["Ribilanciare i dati con codifica di cancellazione dopo l'aggiunta di nodi di storage"](#).

3. Se è stato aggiunto un nodo gateway:

- Se 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 i gruppi ad alta disponibilità"](#).

4. Se è stato aggiunto un nodo amministratore:

- a. Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID, crea una relying party trust per il nuovo Admin Node. Non puoi accedere al nodo finché non crei questa relying party trust. Consulta come configurare l'SSO usando ["OIDC"](#) o ["SAML"](#).
- 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 i gruppi ad alta disponibilità"](#).
- c. Facoltativamente, copiare il database Prometheus dal nodo di amministrazione primario al nodo di amministrazione di espansione se si desidera mantenere costanti le metriche storiche su ciascun nodo di amministrazione. Vedere ["Copia le metriche Prometheus"](#).
- d. Facoltativamente, copiare i registri di controllo esistenti dal nodo di amministrazione principale al nodo di amministrazione dell'espansione se si desidera mantenere coerenti le informazioni di registro cronologiche su ciascun nodo di amministrazione. Vedere ["Copia dei registri di audit"](#).

5. Per verificare se i nodi di espansione sono stati aggiunti con una rete client non attendibile o per modificare se la rete client di un nodo è 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 utilizzando un endpoint di bilanciamento del carico. Vedere ["Configurare gli endpoint del bilanciamento del carico"](#) e ["Gestire i controlli firewall"](#).

6. Configurare il DNS.

Se le impostazioni DNS sono state specificate separatamente per ciascun nodo della griglia, è necessario aggiungere impostazioni DNS personalizzate per nodo per i nuovi nodi. Vedere ["Modificare la configurazione DNS per un nodo griglia singolo"](#).

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

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

Verificare che i nodi di archiviazione siano attivi dopo un'espansione StorageGRID

Al termine di un'operazione di espansione che aggiunge nuovi nodi di storage, il sistema StorageGRID dovrebbe avviarsi automaticamente utilizzando i nuovi nodi di storage. È necessario utilizzare il sistema StorageGRID per verificare che il nuovo nodo di storage sia attivo.

Fasi

1. Accedere a Grid Manager utilizzando un "[browser web supportato](#)".
2. Selezionare **Nodi > Nodo di archiviazione di espansione_ > Archiviazione**.
3. Posizionare il cursore sul grafico **Storage Used - Object Data** (archiviazione utilizzata - dati oggetto) per visualizzare il valore di **Used**, che corrisponde alla quantità di spazio utilizzabile totale utilizzata per i dati dell'oggetto.
4. Verificare che il valore di **used** aumenti man mano che si sposta il cursore a destra sul grafico.

Copia le metriche di Prometheus nei nuovi nodi amministrativi in StorageGRID

Dopo aver aggiunto un nuovo nodo di amministrazione, è possibile copiare facoltativamente le metriche storiche gestite da Prometheus dal nodo di amministrazione primario al nuovo nodo di amministrazione. La copia delle metriche garantisce che le metriche storiche siano coerenti tra i nodi di amministrazione.

Prima di iniziare

- Il nuovo nodo di amministrazione è installato e in esecuzione.
- Si dispone del `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

Quando si aggiunge un nodo di amministrazione, il processo di installazione del software crea un nuovo database Prometheus. È possibile mantenere costanti le metriche storiche tra i nodi copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione di origine*) al nuovo nodo di amministrazione.



La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere 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. Accedere al nuovo nodo di amministrazione:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`

- iv. Immettere la password elencata nel `Passwords.txt` file.
- b. Arrestare il servizio Prometheus: `service prometheus stop`
- c. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `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 nuovo nodo amministrativo:
`/usr/local/prometheus/bin/prometheus-clone-db.sh Source_Admin_Node_IP`
- f. Quando richiesto, premere **Invio** per confermare che si desidera distruggere il nuovo database Prometheus nel nuovo nodo di amministrazione.

Il database Prometheus originale e i relativi dati storici vengono copiati nel nuovo nodo di amministrazione. Al termine dell'operazione di copia, lo script avvia il nuovo nodo di amministrazione. Viene visualizzato il seguente stato:

```
Database cloned, starting services
```

- a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Inserire:

```
ssh-add -D
```

- 4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.

```
service prometheus start
```

Copia i registri di controllo nei nuovi nodi di amministrazione in StorageGRID

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

- Sono state completate le fasi di espansione richieste per aggiungere un nodo di amministrazione.
- Si dispone del `Passwords.txt` file.

A proposito di questa attività

Per rendere disponibili i messaggi di audit storici su un nuovo nodo di amministrazione, è necessario copiare manualmente i file di log di audit da un nodo di amministrazione esistente al nodo di amministrazione dell'espansione.



Per impostazione predefinita, le informazioni di controllo vengono inviate a `localaudit` accedi a ciascun nodo. Per utilizzare questa procedura, è necessario aver configurato i nodi di amministrazione come destinazione di controllo come segue:

- Hai configurato **Nodi amministrativi/nodi locali** come destinazione del registro.
- Hai configurato **Admin Nodes e server syslog esterno** come destinazione del registro.

Fare riferimento a "[Configurare i messaggi di controllo e il server syslog esterno](#)" per i dettagli.

Fasi

1. Accedere al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@_primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per evitare che crei un nuovo file: `service ams stop`

3. Accedere alla directory di esportazione della verifica:

```
cd /var/local/audit/export/
```

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/audit/export/
```

6. Se viene richiesta la passphrase per `/root/.ssh/id_rsa`, immettere la password di accesso SSH per il nodo di amministrazione primario elencato nel `Passwords.txt` file.

7. Ripristinare il file originale `audit.log`:

```
mv new_name.txt audit.log
```

8. Avviare il servizio AMS:

```
service ams start
```

9. Disconnettersi dal server:

```
exit
```

10. Accedere al nodo di amministrazione dell'espansione:

- a. Immettere il seguente comando: `ssh admin@expansion_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

11. Aggiornare le impostazioni dell'utente e del gruppo per i file di log di controllo:

```
cd /var/local/audit/export/
```

```
chown ams-user:bycast *
```

12. Disconnettersi dal server:

```
exit
```

Ribilancia i dati codificati in modo da essere cancellati dopo aver aggiunto nodi al tuo sistema StorageGRID

Dopo aver aggiunto i nodi storage, è possibile utilizzare la procedura di ribilanciamento dell'erasure coding (EC) per ridistribuire i frammenti sottoposti a erasure coding tra i nodi storage nuovi ed esistenti.

Prima di iniziare

- Sono state completate le fasi di espansione per aggiungere i nuovi nodi di storage.
- È stata esaminata la ["considerazioni per il ribilanciamento dei dati con codifica erasure"](#).
- Si comprende che i dati degli oggetti replicati non verranno spostati da questa procedura e che la procedura di ribilanciamento EC non sposta i dati replicati. Tuttavia, quando si determina dove spostare i dati CE, si prendono in considerazione i dati replicati.
- Si dispone del `Passwords.txt` file.

Cosa succede quando viene eseguita questa procedura

Prima di iniziare la procedura, prendere nota di quanto segue:

- La procedura di ribilanciamento EC non si avvia se uno o più volumi sono offline (non montati) o se sono online (montati) ma in uno stato di errore.
- La procedura di ribilanciamento EC riserva temporaneamente una grande quantità di storage. Gli avvisi relativi allo storage potrebbero essere attivati, ma verranno risolti al termine del ribilanciamento. Se lo storage non è sufficiente per la prenotazione, la procedura di ribilanciamento EC non avrà esito positivo. Le riserve di storage vengono rilasciate al termine della procedura di ribilanciamento EC, indipendentemente dal fatto che la procedura abbia avuto esito negativo o positivo.
- Se un volume non è in linea mentre è in corso la procedura di riequilibrio EC, la procedura di riequilibrio terminerà. Tutti i frammenti di dati che sono stati già spostati rimarranno nelle nuove posizioni e i dati non andranno persi.

È possibile eseguire nuovamente la procedura dopo che tutti i volumi sono stati nuovamente online.

- Quando la procedura di riequilibrio EC è in esecuzione, le prestazioni delle operazioni ILM e delle operazioni client S3 potrebbero risentirne.



S3 le operazioni API per caricare oggetti (o parti di oggetti) potrebbero non riuscire durante la procedura di riequilibrio EC se sono necessarie più di 24 ore per il completamento. Le operazioni PUT di lunga durata non avranno esito positivo se la regola ILM applicabile utilizza un posizionamento bilanciato o rigoroso all'acquisizione. Viene segnalato il seguente errore: 500 Internal Server Error.

- **Condizioni di completamento del lavoro.** La procedura di riequilibrio CE è considerata completa quando si verifica una delle seguenti condizioni:
 - Impossibile spostare altri dati sottoposti a erasure coding.
 - I dati in tutti i nodi rientrano in una deviazione del 5% rispetto alla partizione di spazio utilizzabile target.
 - La procedura è in corso da 30 giorni.

Fasi

1. Rivedi i dettagli dello storage a oggetti corrente per il sito che intendi ribilanciare.
 - a. Selezionare **Nodi**.
 - b. Selezionare il primo nodo di storage nel sito.
 - c. Selezionare la scheda **Storage**.
 - d. Posizionare il cursore sul grafico Storage Used - Object Data (Storage utilizzato - dati oggetto) per visualizzare la quantità corrente di dati replicati e i dati con codifica di cancellazione sul nodo di storage.
 - e. Ripetere questa procedura per visualizzare gli altri nodi di storage del sito.
2. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

3. Avviare la procedura:

```
`rebalance-data start --site "site-name"
```

Per "*site-name*", specificare il primo sito in cui sono stati aggiunti nuovi nodi di archiviazione. Racchiudere *site-name* tra virgolette.

Viene avviata la procedura di ribilanciamento EC e viene restituito un ID lavoro.

4. Copiare l'ID lavoro.
5. monitorare lo stato della procedura di riequilibrio CE.
 - Per visualizzare lo stato di una singola procedura di ribilanciamento EC:

```
rebalance-data status --job-id job-id
```

Per *job-id*, specificare l'ID restituito all'avvio della procedura.

- Per visualizzare lo stato della procedura di ribilanciamento EC corrente e delle procedure precedentemente completate:

```
rebalance-data status
```



Per ottenere assistenza sul comando ribilanciamento-dati:

```
rebalance-data --help
```

6. Eseguire ulteriori operazioni in base allo stato restituito:

- Se *State* è, l'operazione di riequilibrio EC è *In progress* ancora in esecuzione. È necessario monitorare periodicamente la procedura fino al completamento.

Vai alla pagina [Nodi](#) per valutare la distribuzione dei dati tra i nodi di archiviazione nel sito.

Il processo di ribilanciamento EC si considera completato e si interromperà quando lo spazio utilizzabile in tutti i nodi rientrerà in una deviazione del 5% rispetto alla partizione di spazio utilizzabile target.

- Se *State* è *Success*, in alternativa, [esaminare lo storage a oggetti](#) per visualizzare i dettagli aggiornati del sito.

Lo spazio utilizzabile dovrebbe ora essere più bilanciato tra i Storage Node nel sito.

- Se *State* è *Failure*:

- Verificare che tutti i nodi di storage del sito siano connessi alla rete.
- Controllare e risolvere eventuali avvisi che potrebbero influire su questi nodi di storage.
- Riavviare la procedura di ribilanciamento EC:

```
rebalance-data start --job-id job-id
```

- [Visualizzare lo stato](#) della nuova procedura. Se *State* è ancora *Failure*, contattare il supporto tecnico.

7. Se la procedura di ribilanciamento EC genera un carico eccessivo (ad esempio, le operazioni di acquisizione sono interessate), sospendere la procedura.

```
rebalance-data pause --job-id job-id
```

8. Se è necessario terminare la procedura di ribilanciamento EC (ad esempio, in modo da poter eseguire un aggiornamento del software StorageGRID), immettere quanto segue:

```
rebalance-data terminate --job-id job-id
```



Quando si termina una procedura di riequilibrio EC, tutti i frammenti di dati che sono già stati spostati rimangono nelle nuove posizioni. I dati non vengono spostati di nuovo nella posizione originale.

9. Se si utilizza la codifica erasure in più siti, eseguire questa procedura per tutti gli altri siti interessati.

Risoluzione dei problemi di espansione in StorageGRID

Se si verificano errori durante il processo di espansione della griglia che non è possibile risolvere o se un'operazione della griglia non riesce, raccogliere i file di registro e contattare il supporto tecnico.

Prima di contattare il supporto tecnico, raccogliere i file di registro necessari per agevolare la risoluzione dei problemi.

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, ["consentire temporaneamente l'accesso"](#).
2. Connettersi al nodo di espansione che ha riscontrato errori:

a. Inserisci il seguente comando: `ssh -p 8022 admin@grid_node_IP`

La porta 8022 è la porta SSH del sistema operativo di base, mentre la porta 22 è la porta SSH del motore dei container che esegue StorageGRID.

b. Immettere la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt passa da `$` a `#`.

3. A seconda della fase di installazione raggiunta, recuperare uno dei seguenti log disponibili nel nodo grid:

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>
Linux	• <code>/var/log/storagegrid/daemon.log</code> • <code>/etc/storagegrid/nodes/<node-name>.conf</code> (per ogni nodo guasto) • <code>/var/log/storagegrid/nodes/<node-name>.log</code> (per ogni nodo guasto; potrebbe non esistere)

4. Se hai consentito l'accesso SSH esterno, ["bloccare l'accesso"](#) quando hai terminato il compito.

Gestire un sistema StorageGRID

Manutenzione della grid StorageGRID

Le attività di manutenzione della rete includono il decommissioning di un nodo o sito, la ridenominazione di una griglia, di un nodo o di un sito e la manutenzione delle reti. È inoltre possibile eseguire procedure host e middleware e procedure dei nodi di rete.



In queste istruzioni, "Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux® (RHEL), Ubuntu® o Debian®. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp"](#).

Prima di iniziare

- Hai una vasta conoscenza del sistema StorageGRID.
- Hai esaminato la topologia del sistema StorageGRID e hai compreso la configurazione della griglia.
- Si comprende che è necessario seguire tutte le istruzioni con precisione e prestare attenzione a tutte le avvertenze.
- Comprendete che le procedure di manutenzione non descritte non sono supportate o richiedono un intervento di assistenza.

Procedure di manutenzione per le appliance

Per le procedure hardware, vedere ["Istruzioni di manutenzione per l'apparecchio StorageGRID"](#).

Scarica il pacchetto di ripristino StorageGRID

Il file del pacchetto di ripristino consente di ripristinare il sistema StorageGRID in caso di errore.

Prima di iniziare

- Da qualsiasi nodo di amministrazione, accedi a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone della passphrase di provisioning.
- Si dispone di ["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.

Fasi

1. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.
2. Immettere la passphrase di provisioning e selezionare **Avvia download**.

Il download viene avviato immediatamente.

3. Al termine del download, aprire il .zip file e confermare che sia 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 .

Decommissiona i nodi o il sito

Decommissionare un nodo StorageGRID o un sito StorageGRID

È possibile eseguire una procedura di decommissionamento per rimuovere in modo permanente i nodi della griglia o un intero sito dal sistema StorageGRID.

Per rimuovere un nodo della griglia o un sito, eseguire una delle seguenti procedure di decommissionamento:

- Eseguire un ["decommissionare il nodo di rete"](#) per rimuovere uno o più nodi, che possono trovarsi in uno o più siti. I nodi rimossi possono essere online e connessi al sistema StorageGRID oppure offline e disconnessi.
- Eseguire un ["decommissionare il sito"](#) per rimuovere un sito. Se tutti i nodi sono connessi a StorageGRID, viene eseguita la **decommissionazione del sito connesso**. Se tutti i nodi sono disconnessi da StorageGRID, viene eseguita una **decommissionazione sito disconnessa**. Se il sito contiene una combinazione di nodi connessi e disconnessi, è necessario riportare tutti i nodi offline in linea.



Prima di eseguire un decommissionamento del sito disconnesso, contatta il tuo rappresentante NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site. Non tentare di decommissionare un sito disconnesso se si ritiene possibile ripristinare il sito o i dati degli oggetti dal sito.

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. Fare riferimento a ["Controllare i lavori di riparazione dei dati"](#) .

Decommissionamento dei nodi

Decommission del nodo grid StorageGRID

È possibile utilizzare la procedura di decommissionamento dei nodi per rimuovere uno o più nodi della griglia in uno o più siti. Impossibile decommissionare il nodo di amministrazione primario.

Quando decommissionare un nodo

Utilizzare la procedura di decommissionamento del nodo quando si verifica una delle seguenti condizioni:

- È stato aggiunto un nodo di archiviazione più grande in un'espansione e si desidera rimuovere uno o più nodi di archiviazione più piccoli, conservando al tempo stesso gli oggetti.



Se si desidera sostituire un vecchio apparecchio con un nuovo apparecchio, è consigliabile ["clonare il nodo appliance"](#) non aggiungere un nuovo apparecchio in un'espansione e quindi smantellare il vecchio apparecchio.

- Richiede meno storage totale.
- Non è più necessario un nodo gateway.
- Non è più necessario un nodo di amministrazione non primario.
- La griglia include un nodo disconnesso che non è possibile ripristinare o ripristinare online.
- La griglia include un nodo di archiviazione.

Come decommissionare un nodo

È possibile dismettere nodi di rete connessi o nodi di rete disconnessi.

Decommissiona i nodi connessi

In generale, è 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 **Disattiva nodi**).

Per istruzioni, vedere ["Decommissionare i nodi di rete connessi"](#).

Decommissiona i nodi disconnessi

In alcuni casi, potrebbe essere necessario smantellare un nodo di rete che non è attualmente connesso alla rete (uno il cui stato è sconosciuto o amministrativamente inattivo).

Per istruzioni, vedere ["Decommissionare nodi di rete disconnessi"](#).

Cosa considerare prima del decommissionamento di un nodo

Prima di eseguire una delle due procedure, esaminare le considerazioni relative a ciascun tipo di nodo:

- ["Considerazioni per il decommissionamento del nodo Admin o Gateway"](#)
- ["Considerazioni per la decommissionazione del nodo di storage"](#)

Considerazioni sulla decommission dei nodi Admin o Gateway di StorageGRID

Esaminare le considerazioni per lo smantellamento di un nodo amministrativo o di un nodo gateway.

Considerazioni sul nodo amministrativo

- Impossibile decommissionare il nodo di amministrazione primario.
- Non è possibile decommissionare un nodo amministrativo se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (ha). Rimuovere prima le interfacce di rete dal gruppo ha. Vedere le istruzioni per ["Gestione dei gruppi ha"](#).
- Se necessario, è possibile modificare in modo sicuro i criteri ILM durante il decommissioning di un nodo amministrativo.
- Se si decommissiona un nodo amministratore e si attiva l'accesso singolo (SSO) per il sistema StorageGRID, è necessario ricordare di rimuovere l'attendibilità della parte di base del nodo dai servizi di federazione di Active Directory (ad FS).
- Se si utilizza ["federazione di grid"](#), assicurarsi che l'indirizzo IP del nodo da smantellare non sia stato specificato per una connessione di federazione di rete.
- Quando si decommissiona un nodo di amministrazione disconnesso, i registri di controllo andranno persi

da quel nodo; tuttavia, questi registri dovrebbero esistere anche nel nodo di amministrazione primario.

Considerazioni per il nodo gateway

- Non è possibile decommissionare un nodo gateway se una delle sue interfacce di rete fa parte di un gruppo ad alta disponibilità (ha). Rimuovere prima le interfacce di rete dal gruppo ha. Vedere le istruzioni per ["Gestione dei gruppi ha"](#).
- Se necessario, è possibile modificare in modo sicuro i criteri ILM durante il decommissionamento di un nodo gateway.
- Se si utilizza ["federazione di grid"](#), assicurarsi che l'indirizzo IP del nodo da smantellare non sia stato specificato per una connessione di federazione di rete.
- È possibile decommissionare in modo sicuro un nodo gateway mentre è disconnesso.

Considerazioni sui nodi storage

Considerazioni sulla decommission dei nodi di archiviazione in StorageGRID

Prima del decommissioning di un nodo storage, prendi in considerazione la possibilità di clonare il nodo. Quindi, se si decide di decommissionare il nodo, controlla il modo in cui StorageGRID gestisce oggetti e metadati durante la procedura di decommissionamento.

Quando clonare un nodo invece di decommissionarlo

Se vuoi sostituire un nodo storage di un'appliance più vecchia con un'appliance più recente o più grande, prendi in considerazione la possibilità di clonare il nodo appliance invece di aggiungere una nuova appliance in un'espansione e poi dismettere la vecchia appliance.

Il cloning dei nodi dell'appliance consente di sostituire facilmente un nodo dell'appliance esistente con un'appliance compatibile nello stesso sito StorageGRID. Il processo di cloning trasferisce tutti i dati nella nuova appliance, mette in funzione la nuova appliance e lascia la vecchia appliance in uno stato preinstallato.

È possibile clonare un nodo appliance se è necessario:

- Sostituire un apparecchio che sta per esaurirsi.
- Aggiorna un nodo esistente per sfruttare la tecnologia di appliance migliorata.
- Aumenta la capacità dello storage grid senza modificare il numero di nodi di storage nel sistema StorageGRID.
- Migliorare l'efficienza dello storage, ad esempio cambiando la modalità RAID.

Per ulteriori informazioni, vedere ["Cloning del nodo dell'appliance"](#).

Considerazioni sui nodi di storage connessi

Esaminare le considerazioni per lo smantellamento di un nodo di storage connesso.

- Non è consigliabile decommissionare più di 10 nodi di storage in una singola procedura Decommission Node.
- Il sistema deve, in ogni momento, includere un numero sufficiente di Storage Node per soddisfare i requisiti operativi, inclusi il ["Quorum ADC"](#) e l'attivo ["Policy ILM"](#). Se una decommission dovesse portare il conteggio degli ADC di un sito al di sotto del quorum, StorageGRID sposta automaticamente il servizio ADC sui Storage Node non-ADC disponibili nello stesso sito, mantenendo il quorum ADC. Se il servizio

ADC non può essere spostato automaticamente, potresti doverlo ["aggiungi un nuovo nodo di archiviazione in un'operazione di espansione"](#) manualmente prima di poter decommissionare uno Storage Node esistente.

Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).

- Quando si rimuove un nodo di storage, grandi volumi di dati di oggetti vengono trasferiti sulla rete. Sebbene questi trasferimenti non debbano influenzare le normali operazioni del sistema, possono influire sulla quantità totale di larghezza di banda della rete consumata dal sistema StorageGRID.
- Le attività associate allo smantellamento del nodo di storage hanno una priorità inferiore rispetto alle attività associate alle normali operazioni di sistema. Ciò significa che lo smantellamento non interferisce con le normali operazioni del sistema StorageGRID e non deve essere pianificato per un periodo di inattività del sistema. Poiché lo smantellamento viene eseguito in background, è difficile stimare il tempo necessario per il completamento del processo. In generale, lo smantellamento termina più rapidamente quando il sistema non funziona correttamente o se viene rimosso un solo nodo di storage alla volta.
- La decommissionazione di un nodo di storage potrebbe richiedere giorni o settimane. Pianificare questa procedura di conseguenza. Sebbene il processo di decommissionamento sia progettato per non influire sulle operazioni del sistema, può limitare altre procedure. In generale, prima di rimuovere i nodi di rete, è necessario eseguire eventuali upgrade o espansioni del sistema pianificati.
- Se è necessario eseguire un'altra procedura di manutenzione durante la rimozione dei nodi di archiviazione, è possibile ["sospendere la procedura di decommissionamento"](#) riprenderla al termine dell'altra procedura.



Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background.

- Non è possibile eseguire operazioni di riparazione dei dati su nodi grid quando è in esecuzione un'attività di decommissionamento.
- Non apportare modifiche a un criterio ILM durante la chiusura di un nodo storage.
- Per rimuovere i dati in modo permanente e sicuro, è necessario cancellare le unità del nodo di archiviazione al termine della procedura di decommissionamento.

Considerazioni sui nodi storage disconnessi

Esaminare le considerazioni per il decommissionamento di un nodo di storage disconnesso.

- Non dismettere mai un nodo disconnesso a meno che non si sia certi che non possa essere messo in linea o ripristinato.



Non eseguire questa procedura se si ritiene che sia possibile ripristinare i dati dell'oggetto dal nodo. Contattare invece il supporto tecnico per determinare se è possibile eseguire il ripristino del nodo.

- Quando si decommissiona un nodo di storage disconnesso, StorageGRID utilizza i dati provenienti da altri nodi di storage per ricostruire i dati dell'oggetto e i metadati che si trovavano nel nodo disconnesso.
- La perdita di dati può verificarsi se si decommissiona più di un nodo di storage disconnesso. Il sistema potrebbe non essere in grado di ricostruire i dati se non sono disponibili un numero sufficiente di copie di

oggetti, frammenti con codifica di cancellazione o metadati di oggetti. Durante il decommissioning dei nodi storage in un grid con nodi solo metadati basati su software, il decommissioning di tutti i nodi configurati per memorizzare sia oggetti che metadati rimuove tutto lo storage a oggetti dal grid. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).



Se si dispone di più nodi di storage disconnessi che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

- Quando si decommissiona un nodo di storage disconnesso, StorageGRID avvia i lavori di riparazione dei dati al termine del processo di decommissionamento. Questi processi tentano di ricostruire i dati dell'oggetto e i metadati memorizzati nel nodo disconnesso.
- Quando si decommissiona un nodo di storage disconnesso, la procedura di decommissionamento viene completata in modo relativamente rapido. Tuttavia, i lavori di riparazione dei dati possono richiedere giorni o settimane e non vengono monitorati dalla procedura di decommissionamento. È necessario monitorare manualmente questi lavori e riavviarli secondo necessità. Vedere ["Controllare i lavori di riparazione dei dati"](#).
- Se si decommissiona un nodo di storage disconnesso che contiene l'unica copia di un oggetto, l'oggetto andrà perso. I processi di riparazione dei dati possono ricostruire e ripristinare gli oggetti solo se nei nodi di storage attualmente connessi sono presenti almeno una copia replicata o un numero sufficiente di frammenti con codifica di cancellazione.

Cos'è il quorum ADC di StorageGRID?

Il quorum ADC garantisce che un numero minimo di servizi Administrative Domain Controller (ADC) rimanga disponibile in ogni sito. StorageGRID sposta automaticamente il servizio ADC durante il decommission quando necessario.

Il servizio ADC, presente in alcuni nodi di archiviazione, mantiene le informazioni sulla topologia della griglia e fornisce servizi di configurazione alla griglia. Il sistema StorageGRID richiede un quorum di servizi ADC per essere sempre disponibile in ogni sito.

Non è possibile decommissionare un nodo di storage se la rimozione del nodo causerebbe il mancato rispetto del quorum di ADC. Per soddisfare il quorum ADC durante una disattivazione, è necessario che almeno tre nodi di archiviazione in ogni sito dispongano del servizio ADC. Se in un sito sono presenti più di tre nodi di archiviazione con il servizio ADC, la maggior parte di questi nodi deve rimanere disponibile dopo lo smantellamento: $((0.5 * \text{Storage Nodes with ADC}) + 1)$



Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).

Ad esempio, si supponga che un sito attualmente includa sei nodi di storage con servizi ADC e che si desideri smantellare tre nodi di storage. A causa del requisito di quorum di ADC, è necessario completare due procedure di decommissionamento, come indicato di seguito:

- Nella prima procedura di decommissionamento, è necessario assicurarsi che siano disponibili quattro nodi di archiviazione con servizi ADC: $((0.5 * 6) + 1)$. Ciò significa che all'inizio è possibile decommissionare solo due nodi di storage.
- 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: $((0.5 * 4) + 1)$.

Quando decommissioni un nodo di archiviazione che ospita il servizio ADC, StorageGRID sposta automaticamente il servizio ADC su un altro nodo di archiviazione nello stesso sito se la decommission portasse il numero di nodi ADC del sito al di sotto del quorum. Lo spostamento automatico richiede che tutti i nodi della grid siano connessi e che siano disponibili nodi di archiviazione non ADC nello stesso sito per ricevere il servizio. La procedura di decommission mantiene un minimo di tre nodi di archiviazione ADC per sito. Ad esempio, se decommissioni quattro o sei nodi ADC in un sito, dopo la procedura rimarranno tre nodi di archiviazione ADC, a condizione che siano presenti nodi non ADC disponibili nello stesso sito.

Se il servizio ADC non può essere spostato automaticamente, puoi ["spostare manualmente il servizio ADC"](#) su un altro Storage Node nello stesso sito oppure ["aggiungi un nuovo Storage Node in un'espansione"](#) e specificare che debba avere un servizio ADC. Poi puoi decommissionare lo Storage Node esistente senza influire sul quorum.

Esaminare la policy ILM di StorageGRID e la configurazione dello storage

Se si prevede di decommissionare un nodo di storage, è necessario rivedere la policy ILM del sistema StorageGRID prima di avviare il processo di decommissionamento.

Durante lo smantellamento, tutti i dati degli oggetti vengono migrati dal nodo di storage decommissionato ad altri nodi di storage.



La policy ILM di cui disponi *durante* la decommissionazione sarà quella utilizzata *dopo* la decommissionazione. È necessario assicurarsi che questa policy soddisfi i requisiti dei dati prima di iniziare la decommissionazione e dopo il completamento della decommissionazione.

È necessario rivedere le regole in ciascuna ["Criterio ILM attivo"](#) di esse per assicurarsi che il sistema StorageGRID continui a disporre di capacità sufficiente del tipo corretto e nelle posizioni corrette per consentire lo smantellamento di un nodo di archiviazione.

Considerare quanto segue:

- I servizi di valutazione ILM potranno copiare i dati degli oggetti in modo che le regole ILM siano soddisfatte?
- Cosa succede se un sito diventa temporaneamente non disponibile mentre è in corso la disattivazione? È possibile eseguire copie aggiuntive in una posizione alternativa?
- In che modo il processo di disattivazione influirà sulla distribuzione finale dei contenuti? Come descritto in ["Consolidare i nodi di storage"](#), è necessario ["Aggiungere nuovi nodi di storage"](#) prima di mettere fuori servizio quelli vecchi. Se si aggiunge un nodo di storage sostitutivo più grande dopo la disattivazione di un nodo di storage più piccolo, i vecchi nodi di storage potrebbero essere vicini alla capacità e il nuovo nodo di storage potrebbe non avere quasi alcun contenuto. La maggior parte delle operazioni di scrittura per i nuovi dati a oggetti verrebbe quindi indirizzata al nuovo nodo di storage, riducendo l'efficienza complessiva delle operazioni di sistema.
- Il sistema includerà sempre nodi storage sufficienti per soddisfare le policy ILM attive?



Un criterio ILM che non può essere soddisfatto porterà a backlog e avvisi e potrebbe arrestare il funzionamento del sistema StorageGRID.

Verificare che la topologia proposta risultante dal processo di disattivazione soddisfi la politica ILM valutando le aree elencate nella tabella.

Area da valutare	Che cosa considerare
Capacità disponibile	Ci sarà una capacità storage sufficiente per ospitare tutti i dati e oggetti archiviati nel sistema StorageGRID, incluse le copie permanenti dei dati e oggetti attualmente archiviati nel nodo storage da dismettere? Ci sarà capacità sufficiente per gestire la crescita prevista dei dati degli oggetti memorizzati per un ragionevole intervallo di tempo dopo il completamento del decommissionamento?
Ubicazione dello storage	Se nel sistema StorageGRID rimane una capacità sufficiente, la capacità è nelle posizioni giuste per soddisfare le regole di business del sistema StorageGRID?
Tipo di storage	Sarà disponibile uno storage sufficiente del tipo appropriato dopo il completamento dello smantellamento? Ad esempio, le regole ILM possono spostare i contenuti da un tipo di storage a un altro in base al tempo in cui i contenuti diventano obsoleti. In questo caso, è necessario assicurarsi che nella configurazione finale del sistema StorageGRID sia disponibile una quantità sufficiente di spazio di archiviazione del tipo appropriato.

Consolida i nodi di archiviazione StorageGRID

È possibile consolidare i nodi di storage per ridurre il numero di nodi di storage per un sito o un'implementazione, aumentando al contempo la capacità di storage.

Quando si consolidano i nodi di storage, si ["Espandere il sistema StorageGRID"](#) aggiungono nuovi nodi di storage con capacità maggiore e si disattivano i vecchi nodi di storage con capacità minore. Durante la procedura di decommissionamento, gli oggetti vengono migrati dai vecchi nodi di storage ai nuovi nodi di storage.



Se si consolidano appliance più vecchie e più piccole con nuovi modelli o appliance con capacità maggiore, prendere in considerazione ["clonare il nodo appliance"](#) (o utilizzare la clonazione dei nodi di appliance e la procedura di decommissionamento se non si esegue una sostituzione one-to-one).

Ad esempio, è possibile aggiungere due nuovi nodi di storage con capacità maggiore per sostituire tre nodi di storage meno recenti. Prima di tutto, utilizzare la procedura di espansione per aggiungere i due nuovi nodi di storage di dimensioni maggiori, quindi utilizzare la procedura di decommissionamento per rimuovere i tre nodi di storage di capacità inferiore.

Aggiungendo nuova capacità prima di rimuovere i nodi di storage esistenti, è possibile garantire una distribuzione più equilibrata dei dati nel sistema StorageGRID. Inoltre, si riduce la possibilità che un nodo di storage esistente venga spinto oltre il livello di filigrana dello storage.

Decommissionare più Storage Nodes di StorageGRID

Se è necessario rimuovere più di un nodo di storage, è possibile decommissionarli in sequenza o in parallelo.



Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).

- Se si decommissionano i nodi di storage in modo sequenziale, è necessario attendere che il primo nodo di storage completi la decommissionamento prima di iniziare a decommissionare il nodo di storage successivo.
- Se i nodi di storage vengono decommissionati in parallelo, i nodi di storage elaborano contemporaneamente le attività di decommissionamento per tutti i nodi di storage da decommissionare. Ciò può causare una situazione in cui tutte le copie permanenti di un file sono contrassegnate come "sola lettura", disattivando temporaneamente l'eliminazione nelle griglie in cui questa funzionalità è attivata.

Verifica i job di riparazione dei dati in StorageGRID

Prima di dismettere o espandere 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.

- Fare riferimento a ["Tipi di espansione"](#) per i dettagli su come espandere un nodo della griglia.
- Usa Grid Manager per monitorare i processi di ripristino in corso e visualizzare la cronologia dei ripristini. Consulta queste procedure:
 - ["Ripristinare i dati dell'oggetto nel volume di storage per l'appliance"](#)
 - ["Ripristinare i dati degli oggetti nel volume di storage in cui il disco di sistema è intatto"](#)
 - ["Ripristinare i dati dell'oggetto nel volume di storage \(errore del disco di sistema\)"](#)

Raccogliere il materiale necessario per il decommissionare del nodo StorageGRID

Prima di eseguire la decommissionazione di un nodo di rete, è necessario ottenere le seguenti informazioni.

Elemento	Note
Pacchetto di recupero .zip file	Devi "scarica il pacchetto di ripristino più recente" .zip file(<code>sgws-recovery-package-id-revision.zip</code>). È possibile utilizzare il file del pacchetto di ripristino per ripristinare il sistema in caso di errore.
Passwords.txt file	Questo file contiene le password necessarie per accedere ai nodi della griglia sulla riga di comando ed è incluso nel pacchetto di ripristino.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è contenuta nel Passwords.txt file.
Descrizione della topologia del sistema StorageGRID prima dello smantellamento	Se disponibile, procurarsi la documentazione che descrive la topologia corrente del sistema.

Accedi alla pagina Decommissiona nodi in StorageGRID

Quando si accede alla pagina nodi di disattivazione in Grid Manager, è possibile visualizzare a colpo d'occhio i nodi che possono essere disattivati.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).



Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).

Fasi

1. Selezionare **Manutenzione > Attività > Disattivazione**.
2. Selezionare **nodi di decommissionazione**.

Viene visualizzata la pagina nodi di decommissionazione. Da questa pagina è possibile:

- Determinare quali nodi di rete possono essere attualmente dismessi.
- Scopri lo stato di salute di tutti i nodi della griglia
- Ordinare l'elenco in ordine crescente o decrescente per **Nome**, **Sito**, **tipo** o **con ADC**.
- Inserisci i termini di ricerca per trovare rapidamente nodi specifici.

In questo esempio, un segno di spunta verde nella colonna Dismissione possibile indica che puoi decommissionare il nodo API Gateway e il nodo di Storage solo dati. Gli altri nodi non possono essere decommissionati per vari motivi. Ad esempio, il nodo Admin primario non può essere decommissionato perché la decommissione di questo tipo di nodo non è supportata. Il nodo di Storage solo metadati non può essere decommissionato perché il sito non soddisferebbe più i ["Quorum ADC"](#).

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-G1	Data Center 1	API Gateway Node	-		
DC1-S1	Data Center 1	Storage Node (Metadata-only)	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S2	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
DC1-S3	Data Center 1	Storage Node	Yes		No, site Data Center 1 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.
☐ DC1-S4	Data Center 1	Storage Node (Data-only)	No		
DC2-ADM1	Data Center 2	Admin Node	-		No, member of HA group(s): HAGroup. Before you can decommission this node, you must remove it from all HA groups.
DC2-S1	Data Center 2	Storage Node	Yes		No, site Data Center 2 needs at least 3 Storage Nodes with ADC services, or available non-ADC nodes to move ADC services to. ADC node decommission is not available if there are any offline nodes.

3. Esaminare la colonna **Dismissione possibile** per ciascun nodo che si desidera decommissionare.

Se è possibile disattivare un nodo della griglia, questa colonna include un segno di spunta verde e la colonna di sinistra contiene una casella di controllo. Se un nodo non può essere decommissionato, questa colonna descrive il problema. Se vi sono più motivi per cui un nodo non può essere dismesso, viene visualizzato il motivo più critico.

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, la disattivazione <i>node type</i> non è supportata.	Impossibile decommissionare il nodo di amministrazione primario.	Nessuno.
No, almeno un nodo della griglia è scollegato. Nota: questo messaggio viene visualizzato solo per i nodi della griglia connessi.	Non è possibile decommissionare un nodo di rete connesso se un nodo di rete è scollegato. La colonna Health include una di queste icone per i nodi della griglia disconnessi:  (grigio): Amministrativamente chiuso  (blu): Sconosciuto	È necessario riportare tutti i nodi disconnessi in linea o "decommissionare tutti i nodi disconnessi" prima di rimuovere un nodo connesso. Nota: Se la griglia contiene più nodi disconnessi, il software richiede di disattivarli tutti contemporaneamente, aumentando il rischio di risultati imprevisti.
No, uno o più nodi richiesti sono attualmente disconnessi e devono essere ripristinati. Nota: questo messaggio viene visualizzato solo per i nodi della griglia disconnessi.	Non è possibile decommissionare un nodo di rete disconnesso se anche uno o più nodi richiesti sono disconnessi (ad esempio, un nodo di storage necessario per il quorum ADC).	- Esaminare i messaggi Decommission possible per tutti i nodi disconnessi. - Determinare quali nodi non possono essere dismessi perché sono necessari. - Se lo stato di salute di un nodo richiesto è amministrativamente inattivo, riportare il nodo in linea. - Se l'integrità di un nodo richiesto è sconosciuta, eseguire una procedura di ripristino del nodo per ripristinare il nodo richiesto.
No, membro del gruppo HA: <i>nome gruppo</i> . Prima di poter dismettere questo nodo, è necessario rimuoverlo da tutti i gruppi HA.	Non è possibile decommissionare un nodo amministrativo o un nodo gateway se un'interfaccia di nodo appartiene a un gruppo ad alta disponibilità (ha).	Modificare il gruppo ha per rimuovere l'interfaccia del nodo o rimuovere l'intero gruppo ha. Vedere "Configurare i gruppi ad alta disponibilità" .

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, il sito <i>x</i> necessita di almeno 3 Storage Node con servizi ADC o di nodi non-ADC disponibili su cui spostare i servizi ADC. Il decommissionare del nodo ADC non è disponibile se uno qualsiasi dei nodi è offline.	Solo nodi di archiviazione (nodi di archiviazione combinati o solo metadati). Non puoi decommissionare un nodo di archiviazione se nel sito rimangono nodi insufficienti a supportare i requisiti di quorum ADC e il servizio ADC non può essere spostato automaticamente. Lo spostamento automatico richiede che siano online più di due nodi di archiviazione ADC nella grid e che siano disponibili nodi di archiviazione non ADC nello stesso sito.	Assicurati che siano soddisfatte le condizioni per lo spostamento automatico del servizio ADC (consulta "Quorum ADC"), oppure "spostare manualmente il servizio ADC" verso un altro Storage Node nello stesso sito. Puoi anche eseguire un'espansione aggiungendo un nuovo Storage Node al sito e specificando che deve avere un servizio ADC. Consulta "Riepilogo del flusso di lavoro per l'aggiunta di nodi griglia a StorageGRID".

Motivo possibile della decommissionazione	Descrizione	Procedura da seguire per risolvere il problema
No, uno o più profili di erasure coding necessitano di almeno n nodi di storage. Se il profilo non viene utilizzato in una regola ILM, è possibile disattivarlo.	Solo nodi di archiviazione. Non è possibile 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 erasure coding per l'erasure coding 4+2, devono rimanere almeno 6 nodi storage.	Per ogni profilo di erasure coding interessato, eseguire una delle seguenti operazioni, in base al modo in cui viene utilizzato il profilo: • Utilizzato nei criteri ILM attivi: Eseguire un'espansione. Aggiungere un numero sufficiente di nuovi nodi di storage per consentire la cancellazione del codice. Vedere le istruzioni per "espandere la tua griglia". • Utilizzato in una regola ILM ma non nei criteri ILM attivi: Modificare o eliminare la regola e quindi disattivare il profilo di erasure coding. • Non utilizzato in alcuna regola ILM: Disattivare il profilo di erasure coding. Nota: viene visualizzato un messaggio di errore se si tenta di disattivare un profilo di erasure coding e i dati dell'oggetto sono ancora associati al profilo. Potrebbe essere necessario attendere alcune settimane prima di provare di nuovo il processo di disattivazione. Ulteriori informazioni su "disattivazione di un profilo di erasure coding".
No, non è possibile smantellare un nodo di archiviazione a meno che il nodo non sia disconnesso.	Se un nodo archivio è ancora connesso, non è possibile rimuoverlo.	Nota: Il supporto per i nodi di archiviazione è stato rimosso. Se è necessario smantellare un nodo di archivio, vedere "Decommissionamento nodo griglia (sito doc StorageGRID 11,8)"

Decommissionare i nodi StorageGRID disconnessi

Potrebbe essere necessario decommissionare un nodo che non è attualmente connesso

alla rete (un nodo il cui stato di salute è sconosciuto o amministrativamente inattivo).

Prima di iniziare

- Comprendete le considerazioni per lo smantellamento ["Nodi Admin e Gateway"](#) e le considerazioni per lo smantellamento ["Nodi di storage"](#).
- Sono stati ottenuti tutti gli elementi prerequisites.
- Hai garantito che non siano attivi lavori di riparazione dei dati. Vedere ["Controllare i lavori di riparazione dei dati"](#).
- Hai confermato che il ripristino del nodo di storage non è in corso in nessun punto della griglia. In tal caso, è necessario attendere il completamento di qualsiasi ricostruzione Cassandra eseguita come parte del ripristino. È quindi possibile procedere con lo smantellamento.
- Si è assicurato che non verranno eseguite altre procedure di manutenzione mentre la procedura di decommissionamento del nodo è in esecuzione, a meno che la procedura di decommissionamento del nodo non sia in pausa.
- La colonna **Dismissione possibile** per il nodo o i nodi disconnessi che si desidera decommissionare include un segno di spunta verde.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

Puoi identificare i nodi disconnessi cercando l'icona blu "Sconosciuto"  o l'icona grigia "Amministrativamente non disponibile"  nella colonna **Integrità**.

Prima di disattivare qualsiasi nodo disconnesso, tenere presente quanto segue:

- Questa procedura è principalmente destinata alla rimozione di un singolo nodo disconnesso. Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.



La perdita di dati può verificarsi se si decommissiona più di un nodo di storage disconnesso alla volta. Vedere ["Considerazioni sui nodi storage disconnessi"](#).



Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).

- Se non è possibile rimuovere un nodo disconnesso (ad esempio, un nodo di storage necessario per il quorum ADC), non è possibile rimuovere nessun altro nodo disconnesso.

Fasi

1. A meno che non si stia smantellando un nodo di archiviazione (che deve essere disconnesso), tentare di riportare in linea tutti i nodi di griglia disconnessi o di ripristinarli.

Vedere ["Procedure di ripristino del nodo Grid"](#) per istruzioni.

2. Se non si riesce a ripristinare un nodo di rete disconnesso e si desidera decommissionarlo mentre è disconnesso, selezionare la casella di controllo corrispondente.



Se la griglia contiene più nodi disconnessi, il software richiede di decommissionarli tutti contemporaneamente, aumentando il potenziale di risultati imprevisti.



Prestare attenzione quando si sceglie di decommissionare più di un nodo di rete disconnesso alla volta, soprattutto se si selezionano più nodi di storage disconnessi. Se si dispone di più nodi di storage disconnessi che non è possibile ripristinare, contattare il supporto tecnico per determinare la procedura migliore.

3. Inserire la passphrase di provisioning.

Il pulsante **Avvia decommissionazione** è attivato.

4. Seleziona **Avvia decommissionare**.

Viene visualizzato un avviso che indica che è stato selezionato un nodo disconnesso e che i dati dell'oggetto andranno persi se il nodo dispone dell'unica copia di un oggetto.

5. Esamina l'elenco dei nodi e seleziona **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, seleziona il collegamento oppure vai su **Manutenzione > Sistema > Pacchetto di ripristino** per accedere alla pagina del 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 Decommissionare per assicurarsi che tutti i nodi selezionati siano dismessi correttamente.

I nodi di storage possono richiedere giorni o settimane per la decommissionazione. Una volta completate tutte le attività, viene visualizzato nuovamente l'elenco di selezione dei nodi con un messaggio di esito positivo. Se si decommissiona un nodo di storage disconnesso, un messaggio di informazioni indica che i lavori di riparazione sono stati avviati.

8. Dopo che i nodi si sono spenti automaticamente nell'ambito della procedura di decommissionamento, rimuovere eventuali macchine virtuali o altre risorse rimanenti associate al nodo decommissionato.



Non eseguire questo passaggio fino a quando i nodi non si sono spenti automaticamente.

9. Se stai decommissionando un Storage Node, monitora lo stato dei processi di riparazione dei **dati replicati** e dei **dati con codifica di cancellazione (EC)** che vengono avviati automaticamente durante il processo di decommissionamento.

Dati replicati

- Per determinare se le riparazioni sono state completate:
 - i. Selezionare **Nodi** > **Nodo di archiviazione in riparazione** > **ILM**.
 - ii. Esaminare gli attributi nella sezione Valutazione. Al termine delle riparazioni, l'attributo **in attesa - tutto** indica 0 oggetti.
- Per monitorare la riparazione in modo più dettagliato:
 - i. Selezionare **Nodi**.
 - ii. Selezionare **grid name** > **ILM**.
 - iii. Posiziona il cursore sul grafico della coda ILM per visualizzare il valore dell'attributo **Frequenza di scansione (oggetti/sec)**, che indica la velocità con cui gli oggetti nella griglia vengono scansati e messi in coda per ILM.
 - iv. Nella sezione Coda ILM, osserva i seguenti attributi:

- **Periodo di scansione - stimato:** Il tempo stimato per completare una scansione ILM completa di tutti gli oggetti.

Una scansione completa non garantisce che ILM sia stato applicato a tutti gli oggetti.

- **Riparazioni tentate:** numero totale di tentativi di operazioni di riparazione di oggetti per dati replicati considerati ad alto rischio. Gli oggetti ad alto rischio sono tutti gli oggetti di cui è rimasta una sola copia, sia che ciò sia specificato dalla policy ILM o sia dovuto alla perdita di copie. 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.

- v. In alternativa, invia una query Prometheus per
`storagegrid_ilm_scan_period_estimated_minutes E
storagegrid_ilm_repairs_attempted.`

Dati con erasure coding (EC)

Per monitorare la riparazione dei dati codificati per la cancellazione e riprovare le richieste che potrebbero non essere riuscite, seleziona **Supporto** > **Strumenti** > **Metriche** per visualizzare il tempo stimato di completamento e la % di completamento per il job corrente. Poi seleziona **EC Overview** nella sezione Grafana. Guarda le dashboard **Grid EC Job Estimated Time to Completion** e **Grid EC Job Percentage Completed**.

Al termine

Non appena i nodi disconnessi sono stati decommissionati e tutti i lavori di riparazione dei dati sono stati completati, è possibile decommissionare qualsiasi nodo di rete connesso secondo necessità.

Quindi, completare questi passaggi dopo aver completato la procedura di decommissionamento:

- Assicurarsi che i dischi del nodo della griglia decommissionata siano puliti. Utilizzare uno strumento o un

servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.

- Se un nodo dell'appliance è stato disattivato e i dati dell'appliance sono stati protetti mediante la crittografia del nodo, utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione del server di gestione delle chiavi (Cancella KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS. Per istruzioni, vedere ["Monitorare la crittografia dei nodi in modalità di manutenzione"](#).

Decommissionare i nodi StorageGRID collegati

È possibile decommissionare e rimuovere in modo permanente i nodi collegati alla rete.

Prima di iniziare

- Comprendete le considerazioni per lo smantellamento ["Nodi Admin e Gateway"](#) e le considerazioni per lo smantellamento ["Nodi di storage"](#).
- Hai raccolto tutti i materiali necessari.
- Hai garantito che non siano attivi lavori di riparazione dei dati.
- Hai confermato che il ripristino del nodo di storage non è in corso in nessun punto della griglia. In tal caso, attendere il completamento di qualsiasi ricostruzione Cassandra eseguita come parte del ripristino. È quindi possibile procedere con lo smantellamento.
- Si è assicurato che non verranno eseguite altre procedure di manutenzione mentre la procedura di decommissionamento del nodo è in esecuzione, a meno che la procedura di decommissionamento del nodo non sia in pausa.
- Si dispone della passphrase di provisioning.
- I nodi della griglia sono connessi.
- La colonna **Dismissione possibile** per il nodo o i nodi che si desidera decommissionare include un segno di spunta verde.



La decommissionazione non si avvia se uno o più volumi sono offline (non montati) o se sono online (montati) ma in uno stato di errore.



Se uno o più volumi vengono disconnessi mentre è in corso una decommissionazione, il processo di decommissionamento viene completato dopo che questi volumi sono tornati online.

- Tutti i nodi della griglia hanno uno stato di salute normale (verde) . Se visualizzi una di queste icone nella colonna **Salute**, devi provare a risolvere il problema:

Icona	Colore	Severità
	Giallo	Avviso
	Arancione chiaro	Minore
	Arancione scuro	Maggiore

Icona	Colore	Severità
	Rosso	Critico

- Se in precedenza è stato dismesso un nodo di storage disconnesso, tutti i lavori di riparazione dei dati sono stati completati correttamente. Vedere ["Controllare i lavori di riparazione dei dati"](#).



Non rimuovere la macchina virtuale o altre risorse di un nodo griglia fino a quando non viene richiesto in questa procedura.



Prestare attenzione quando si disattivano i nodi di storage in un grid che contiene nodi solo metadati basati su software. Se tutti i nodi configurati per l'archiviazione di *entrambi* oggetti e metadati vengono dismessi, la possibilità di archiviare oggetti viene rimossa dalla griglia. Per ulteriori informazioni sui nodi di storage solo per metadati, vedere ["Tipi di nodi storage"](#).

A proposito di questa attività

Quando un nodo viene smantellato, i suoi servizi vengono disattivati e il nodo si arresta automaticamente.

Fasi

1. Nella pagina nodi di decommissionazione, selezionare la casella di controllo per ciascun nodo della griglia che si desidera decommissionare.
2. Inserire la passphrase di provisioning.

Il pulsante **Avvia decommissionazione** è attivato.

3. Selezionare **Avvia demissione**.
4. Esaminare l'elenco dei nodi nella finestra di dialogo di conferma e selezionare **OK**.

Viene avviata la procedura di decommissionamento del nodo e viene visualizzato l'avanzamento per ciascun nodo.



Non scollegare un nodo di storage dopo l'avvio della procedura di decommissionamento. La modifica dello stato potrebbe causare la mancata copia di alcuni contenuti in altre posizioni.

5. Non appena il nuovo pacchetto di ripristino è disponibile, seleziona il collegamento al pacchetto di ripristino nel banner oppure seleziona **Manutenzione > Sistema > Pacchetto di ripristino** per accedere alla pagina del 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 di decommissionazione per assicurarsi che tutti i nodi selezionati vengano decommissionati correttamente.



I nodi di storage possono richiedere giorni o settimane per la decommissionazione.

Una volta completate tutte le attività, viene visualizzato nuovamente l'elenco di selezione dei nodi con un

messaggio di esito positivo.

Al termine

Completare questi passaggi dopo aver completato la procedura di decommissionamento del nodo:

1. Seguire la fase appropriata per la piattaforma. Ad esempio:
 - **Linux:** Potresti voler staccare i volumi ed eliminare i file di configurazione del nodo creati durante l'installazione. Vedere ["Installa StorageGRID sui nodi basati su software"](#).
 - **VMware:** Potrebbe essere necessario utilizzare l'opzione "Elimina da disco" di vCenter per eliminare la macchina virtuale. Potrebbe essere necessario eliminare anche i dischi dati indipendenti dalla macchina virtuale.
 - **Appliance StorageGRID:** Il nodo appliance torna automaticamente allo stato non distribuito, dove è possibile accedere al programma di installazione dell'appliance StorageGRID. È possibile spegnere l'apparecchio o aggiungerlo a un altro sistema StorageGRID.
2. Assicurarsi che i dischi del nodo della griglia decommissionata siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.
3. Se un nodo dell'appliance è stato disattivato e i dati dell'appliance sono stati protetti mediante la crittografia del nodo, utilizzare il programma di installazione dell'appliance StorageGRID per cancellare la configurazione del server di gestione delle chiavi (Cancella KMS). Se si desidera aggiungere l'appliance a un'altra griglia, è necessario cancellare la configurazione KMS. Per istruzioni, vedere ["Monitorare la crittografia dei nodi in modalità di manutenzione"](#).

Metti in pausa e riprendi il processo di decommission per i nodi di storage StorageGRID

Se è necessario eseguire una seconda procedura di manutenzione, è possibile sospendere la procedura di decommissionamento per un nodo di storage durante determinate fasi. Al termine dell'altra procedura, è possibile riprendere la decommissionamento.



Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).

Fasi

1. Selezionare **Manutenzione > Attività > Disattivazione**.

Viene visualizzata la pagina Decommission.

2. Selezionare **nodi di decommissionazione**.

Viene visualizzata la pagina nodi di decommissionazione. Quando la procedura di decommissionamento raggiunge una delle seguenti fasi, il pulsante **Pause** (Pausa) viene attivato.

- Valutazione di ILM

- Decommissionamento dei dati codificati a cancellazione

3. Selezionare **Pausa** per sospendere la procedura.

La fase corrente viene messa in pausa e il pulsante **Riprendi** viene attivato.

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 Q				
Name	Type	Progress	Stage	
DC1-S5	Storage Node		Evaluating ILM	
Pause Resume				

- Al termine dell'altra procedura di manutenzione, selezionare **Riprendi** per procedere con la decommissionazione.

Decommissionamento del sito

Considerazioni relative alla decommission del sito in StorageGRID

Prima di utilizzare la procedura di decommissionamento del sito per rimuovere un sito, è necessario esaminare le considerazioni.

Cosa accade quando si decommissiona un sito

Quando si decommissiona un sito, StorageGRID rimuove in modo permanente tutti i nodi del sito e del sito stesso dal sistema StorageGRID.

Una volta completata la procedura di decommissionamento del sito:

- Non è più possibile utilizzare StorageGRID per visualizzare o accedere al sito o a uno qualsiasi dei nodi del sito.
- Non puoi più utilizzare pool di storage o profili di erasure coding riferiti al sito. Quando StorageGRID disimpegna un sito, rimuove automaticamente questi pool di storage e disattiva questi profili di erasure coding.

Differenze tra le procedure di decommissionamento del sito connesso e disconnesso

È possibile utilizzare la procedura di decommissionamento del sito per rimuovere un sito in cui tutti i nodi sono connessi a StorageGRID (chiamata decommissionazione di un sito connesso) o per rimuovere un sito in cui tutti i nodi sono disconnessi da StorageGRID (chiamata decommissionazione di un sito disconnesso). Prima di iniziare, è necessario comprendere le differenze tra queste procedure.



Se un sito contiene un mix di nodi connessi (✓) e nodi disconnessi (☾ o ⚙), devi riportare online tutti i nodi offline.

- La decommissionazione di un sito connesso consente di rimuovere un sito operativo dal sistema StorageGRID. Ad esempio, è possibile eseguire la decommissionazione di un sito connesso per rimuovere un sito funzionante ma non più necessario.
- Quando StorageGRID rimuove un sito connesso, utilizza ILM per gestire i dati dell'oggetto nel sito. Prima di avviare la decommissionazione di un sito connesso, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM. I processi ILM per la migrazione dei dati degli oggetti e i processi interni per la rimozione di un sito possono essere eseguiti contemporaneamente, ma la procedura consigliata consiste nel consentire il completamento dei passaggi ILM prima di avviare la procedura di decommissionamento effettiva.
- La decommissionazione di un sito disconnesso consente di rimuovere un sito guasto dal sistema StorageGRID. Ad esempio, è possibile eseguire la decommissionazione di un sito disconnesso per rimuovere un sito distrutto da un incendio o un'inondazione.

Quando StorageGRID rimuove un sito disconnesso, considera tutti i nodi irripresinabili e non tenta di conservare i dati. Tuttavia, prima di avviare una decommissionazione disconnessa del sito, è necessario rimuovere il sito da tutte le regole ILM e attivare una nuova policy ILM.



Prima di eseguire una procedura di decommissionamento del sito disconnesso, è necessario contattare il rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site. Non tentare di decommissionare un sito disconnesso se si ritiene possibile ripristinare il sito o i dati degli oggetti dal sito.

Requisiti generali per la rimozione di un sito connesso o disconnesso

Prima di rimuovere un sito connesso o disconnesso, è necessario conoscere i seguenti requisiti:

- Non è possibile decommissionare un sito che include il nodo di amministrazione primario.
- Non è possibile decommissionare un sito se uno dei nodi dispone di un'interfaccia che appartiene a un gruppo ad alta disponibilità (ha). È necessario modificare il gruppo ha per rimuovere l'interfaccia del nodo o rimuovere l'intero gruppo ha.
- Non puoi decommissionare un sito se contiene una combinazione di nodi connessi (✓) e disconnessi (⚙ o ☾).
- Non puoi decommissionare un sito se un nodo di un altro sito è disconnesso (⚙ o ☾).
- Non è possibile avviare la procedura di decommissionamento del sito se è in corso un'operazione di riparazione del nodo ec. Vedere "[Controllare i lavori di riparazione dei dati](#)" per tenere traccia delle riparazioni dei dati sottoposti a erasure coding.
- Durante l'esecuzione della procedura di decommissionamento del sito:
 - Non è possibile creare regole ILM che si riferiscono al sito da smantellare. Inoltre, non è possibile modificare una regola ILM esistente per fare riferimento al sito.
 - Non è possibile eseguire altre procedure di manutenzione, ad esempio l'espansione o l'aggiornamento.



Se è necessario eseguire un'altra procedura di manutenzione durante lo smantellamento di un sito connesso, è possibile ["Sospendere la procedura durante la rimozione dei nodi di storage"](#). Il pulsante **Pause** (Pausa) viene attivato solo quando vengono raggiunte le fasi di decommissionamento dei dati con codifica di cancellazione o valutazione ILM; tuttavia, la valutazione ILM (migrazione dei dati) continuerà a essere eseguita in background. Una volta completata la seconda procedura di manutenzione, è possibile riprendere la decommissionamento.

- Se è necessario ripristinare un nodo dopo aver avviato la procedura di decommissionamento del sito, contattare il supporto.
- Non è possibile decommissionare più di un sito alla volta.
- Se il sito include uno o più nodi di amministrazione ed è abilitato il Single Sign-on (SSO) per il sistema StorageGRID, è necessario rimuovere tutti i trust delle parti che si basano sul sito dai servizi di federazione Active Directory (ad FS).

Requisiti per la gestione del ciclo di vita delle informazioni (ILM)

Durante la rimozione di un sito, è necessario aggiornare la configurazione ILM. La procedura guidata Decommission Site (Sito di rimozione) guida l'utente attraverso una serie di passaggi necessari per garantire quanto segue:

- Il sito non è oggetto di alcuna politica ILM. In tal caso, è necessario modificare i criteri o creare e attivare i criteri con nuove regole ILM.
- Nessuna regola ILM si riferisce al sito, anche se tali regole non sono utilizzate in alcuna politica. È necessario eliminare o modificare tutte le regole che fanno riferimento al sito.

Quando StorageGRID decompime il sito, disattiva automaticamente tutti i profili di erasure coding inutilizzati che fanno riferimento al sito ed elimina automaticamente eventuali pool di storage inutilizzati che fanno riferimento al sito. Se il pool di storage di tutti i nodi di storage esiste (StorageGRID 11.6 e versioni precedenti), viene rimosso perché utilizza tutti i siti.



Prima di rimuovere un sito, potrebbe essere necessario creare nuove regole ILM e attivare un nuovo criterio ILM. Queste istruzioni presuppongono una buona comprensione del funzionamento di ILM e la sua conoscenza della creazione di pool di storage, dei profili di erasure coding, delle regole ILM e della simulazione e attivazione di un criterio ILM. Vedere ["Gestire gli oggetti con ILM"](#).

Considerazioni per i dati dell'oggetto in un sito connesso

Se si sta eseguendo una decommissionazione del sito connesso, è necessario decidere cosa fare con i dati dell'oggetto esistenti nel sito quando si creano nuove regole ILM e un nuovo criterio ILM. È possibile eseguire una o entrambe le operazioni seguenti:

- Sposta i dati degli oggetti dal sito selezionato a uno o più altri siti della griglia.

Esempio per lo spostamento dei dati: Supponiamo di voler decommissionare un sito in Raleigh perché hai aggiunto un nuovo sito in Sunnyvale. In questo esempio, si desidera spostare tutti i dati dell'oggetto dal sito precedente al nuovo sito. Prima di aggiornare le regole ILM e i criteri ILM, è necessario esaminare la capacità in entrambi i siti. È necessario assicurarsi che il sito Sunnyvale disponga di capacità sufficiente per ospitare i dati dell'oggetto provenienti dal sito Raleigh e che la capacità di Sunnyvale rimanga adeguata per la crescita futura.



Per garantire la disponibilità di una capacità adeguata, potrebbe essere necessario ["espandere una griglia"](#) aggiungere volumi di archiviazione o nodi di archiviazione a un sito esistente o aggiungere un nuovo sito prima di eseguire questa procedura.

- Elimina le copie degli oggetti dal sito selezionato.

Esempio per l'eliminazione dei dati: Si supponga di utilizzare una regola ILM a 3 copie per replicare i dati degli oggetti su tre siti. Prima di smantellare un sito, è possibile creare una regola ILM equivalente a 2 copie per memorizzare i dati solo in due siti. Quando si attiva un nuovo criterio ILM che utilizza la regola 2-copy, StorageGRID elimina le copie dal terzo sito perché non soddisfano più i requisiti ILM. Tuttavia, i dati dell'oggetto rimangono protetti e la capacità dei due siti rimanenti rimane invariata.



Non creare mai una regola ILM a copia singola per consentire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.

Requisiti aggiuntivi per la decommissionazione di un sito connesso

Prima che StorageGRID possa rimuovere un sito connesso, è necessario assicurarsi che:

- Tutti i nodi nel tuo sistema StorageGRID devono avere uno stato di connessione **Connesso** (); tuttavia, i nodi possono avere avvisi attivi.



Se uno o più nodi sono disconnessi, è possibile completare i passaggi 1-4 della procedura guidata Smantella sito. Tuttavia, non è possibile completare la fase 5 della procedura guidata, che avvia il processo di decommissionamento, a meno che tutti i nodi non siano connessi.

- Se il sito che si intende rimuovere contiene un nodo gateway o un nodo amministrativo utilizzato per il bilanciamento del carico, potrebbe essere necessario ["espandere una griglia"](#) aggiungere un nuovo nodo equivalente in un altro sito. Assicurarsi che i client possano connettersi al nodo sostitutivo prima di avviare la procedura di decommissionamento del sito.
- Se il sito che si intende rimuovere contiene nodi gateway o nodi amministratore che si trovano in un gruppo ad alta disponibilità (ha), è possibile completare i passaggi 1-4 della procedura guidata Decommission Site. Tuttavia, non è possibile completare la fase 5 della procedura guidata, che avvia il processo di decommissionamento, fino a quando non si rimuovono questi nodi da tutti i gruppi ha. Se i client esistenti si connettono a un gruppo ha che include nodi dal sito, è necessario assicurarsi che possano continuare a connettersi a StorageGRID dopo la rimozione del sito.
- Se i client si connettono direttamente ai nodi di storage nel sito che si intende rimuovere, è necessario assicurarsi che possano connettersi ai nodi di storage in altri siti prima di avviare la procedura di decommissionamento del sito.
- È necessario fornire spazio sufficiente sugli altri siti per ospitare i dati degli oggetti che verranno spostati a causa di modifiche a qualsiasi policy ILM attiva. In alcuni casi, potrebbe essere necessario ["espandere una griglia"](#) aggiungere nodi di storage, volumi di storage o nuovi siti prima di poter completare la disattivazione di un sito connesso.
- Per completare la procedura di decommissionamento, è necessario attendere il tempo necessario. I processi ILM di StorageGRID potrebbero richiedere giorni, settimane o persino mesi per spostare o

eliminare i dati degli oggetti dal sito prima che il sito possa essere disattivato.



Lo spostamento o l'eliminazione dei dati degli oggetti da un sito potrebbe richiedere giorni, settimane o persino mesi, a seconda della quantità di dati nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

- Se possibile, completare i passaggi 1-4 della procedura guidata Decommission Site il prima possibile. La procedura di decommissionamento viene completata più rapidamente e con meno interruzioni e impatti sulle performance se si consente lo spostamento dei dati dal sito prima di avviare la procedura di decommissionamento effettiva (selezionando **Avvia decommissionamento** nella fase 5 della procedura guidata).

Requisiti aggiuntivi per la decommissionazione di un sito disconnesso

Prima che StorageGRID possa rimuovere un sito disconnesso, è necessario assicurarsi che:

- Hai contattato il tuo rappresentante commerciale NetApp. NetApp esaminerà i tuoi requisiti prima di attivare tutte le fasi della procedura guidata Decommission Site.



Non tentare di decommissionare un sito disconnesso se si ritiene che sia possibile ripristinare il sito o i dati degli oggetti dal sito. Vedere ["Come il supporto tecnico recupera un sito"](#).

- Tutti i nodi del sito devono avere uno stato di connessione di uno dei seguenti:
 - **Sconosciuto** (🔄): Per un motivo sconosciuto, un nodo è disconnesso o i servizi sul nodo sono inaspettatamente inattivi. Ad esempio, un servizio sul nodo potrebbe essere stato arrestato oppure il nodo potrebbe aver perso la connessione di rete a causa di un'interruzione di corrente o di un'interruzione imprevista.
 - **Amministrativamente non disponibile** (🌙): Il nodo non è connesso alla grid per un motivo previsto. 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 **Connected** (✅); tuttavia, questi altri nodi possono avere avvisi attivi.
- È necessario comprendere che non sarà più possibile utilizzare StorageGRID per visualizzare o recuperare i dati degli oggetti memorizzati nel sito. Quando StorageGRID esegue questa procedura, non tenta di conservare i dati del sito disconnesso.



Se le regole e i criteri ILM sono stati progettati per proteggere dalla perdita di un singolo sito, le copie degli oggetti rimangono nei siti rimanenti.

- È necessario comprendere che se il sito conteneva l'unica copia di un oggetto, l'oggetto viene perso e non può essere recuperato.

Considerazioni per la coerenza quando si rimuove un sito

La coerenza per un bucket S3 determina se StorageGRID replica completamente i metadati degli oggetti su tutti i nodi e i siti prima di informare il client del successo dell'acquisizione degli oggetti. La coerenza fornisce un equilibrio tra la disponibilità degli oggetti e la loro coerenza in diversi nodi e siti storage.

Quando StorageGRID rimuove un sito, deve assicurarsi che non vengano scritti dati sul sito da rimuovere. Di conseguenza, sovrascrive temporaneamente la consistenza per ciascun contenitore o bucket. Dopo aver

avviato il processo di decommissionamento del sito, StorageGRID utilizza temporaneamente una forte coerenza del sito per impedire che i metadati degli oggetti vengano scritti nel sito.

Come risultato di questa override temporanea, tenere presente che le operazioni di scrittura, aggiornamento ed eliminazione dei client che si verificano durante la decommissionazione di un sito possono avere esito negativo se più nodi diventano non disponibili negli altri siti.

Raccogliere il materiale necessario per il decommission del sito StorageGRID

Prima di decommissionare un sito, è necessario procurarsi i seguenti materiali.

Elemento	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 del pacchetto di ripristino 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.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è contenuta nel Passwords.txt file.
Descrizione della topologia del sistema StorageGRID prima dello smantellamento	Se disponibile, procurarsi la documentazione che descrive la topologia corrente del sistema.

Informazioni correlate

["Requisiti del browser Web"](#)

Seleziona un sito da decommissionare in StorageGRID

Per determinare se un sito può essere decommissionato, iniziare accedendo alla procedura guidata Decommissionare il sito.

Prima di iniziare

- Hai ottenuto tutti i materiali richiesti.
- Hai esaminato le considerazioni per la rimozione di un sito.
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di accesso root o autorizzazioni Maintenance e ILM"](#).

Fasi

1. Selezionare **Manutenzione > Attività > Disattivazione**.
2. Selezionare **Smantella sito**.

Viene visualizzata la fase 1 (Seleziona sito) della procedura guidata Smantella sito. Questo passaggio

include un elenco alfabetico dei siti nel sistema StorageGRID.

Decommission Site

1

Select Site

2

View Details

3

Revise ILM Policy

4

Remove ILM References

5

Resolve Node Conflicts

6

Monitor Decommission

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. Visualizzare i valori nella colonna **capacità di storage utilizzata** per determinare la quantità di storage attualmente utilizzata per i dati a oggetti in ogni sito.
- La capacità di storage utilizzata è una stima. Se i nodi sono offline, la capacità di storage utilizzata è l'ultimo valore noto per il sito.
- Per la decommissionazione di un sito connesso, questo valore rappresenta la quantità di dati dell'oggetto da spostare in altri siti o da eliminare da ILM prima di poter decommissionare il sito in modo sicuro.
 - Per la decommissionazione di un sito disconnesso, questo valore rappresenta la quantità di storage dei dati del sistema che diventa inaccessibile quando si decommissiona questo sito.



Se la policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, le copie dei dati dell'oggetto dovrebbero comunque esistere sui siti rimanenti.

4. Esaminare i motivi nella colonna **Smantella possibile** per determinare quali siti possono essere attualmente dismessi.



Se vi sono più motivi per cui un sito non può essere dismesso, viene visualizzato il motivo più critico.

Motivo possibile della decommissionazione	Descrizione	Passo successivo
Segno di spunta verde ()	È possibile decommissionare questo sito.	Andare a il passo successivo .

Motivo possibile della decommissionazione	Descrizione	Passo successivo
No. Questo sito contiene il nodo amministrativo primario.	Impossibile decommissionare un sito contenente il nodo di amministrazione primario.	Nessuno. Impossibile eseguire questa procedura.
No. Questo sito contiene uno o più nodi di archiviazione.	Impossibile decommissionare un sito contenente un nodo di archiviazione.	Nessuno. Impossibile eseguire questa procedura.
No. Tutti i nodi in questo sito sono disconnessi. Contatta il tuo rappresentante commerciale NetApp.	Non puoi eseguire il decommission di un sito connesso a meno che ogni nodo del sito sia connesso (✓).	Se si desidera eseguire una decommissionazione del sito disconnesso, è necessario contattare il rappresentante commerciale NetApp, che esaminerà i requisiti e attiverà il resto della procedura guidata Decommission Site. IMPORTANTE: Non scollegare mai i nodi online per poter rimuovere un sito. I dati andranno persi.

L'esempio mostra un sistema StorageGRID con tre siti. Il segno di spunta verde (✓) per i siti di Raleigh e Sunnyvale indica che puoi decommissionare quei siti. Tuttavia, non puoi decommissionare il sito di Vancouver perché contiene il nodo Admin primario.

1. Se è possibile decommissionare, selezionare il pulsante di opzione corrispondente al sito.

Il pulsante **Avanti** è attivato.

2. Selezionare **Avanti**.

Viene visualizzato il punto 2 (Visualizza dettagli).

Rivedere i dettagli del sito prima di decommissionare in StorageGRID

Dalla fase 2 (Visualizza dettagli) della procedura guidata Decommission Site, è possibile esaminare i nodi inclusi nel sito, verificare la quantità di spazio utilizzata su ciascun nodo di storage e valutare la quantità di spazio libero disponibile negli altri siti della griglia.

Prima di iniziare

Prima di decommissionare un sito, è necessario esaminare la quantità di dati oggetto presenti nel sito.

- Se si sta eseguendo una decommissionazione del sito connesso, è necessario comprendere la quantità di dati oggetto attualmente presenti nel sito prima di aggiornare ILM. In base alle capacità del sito e alle esigenze di protezione dei dati, è possibile creare nuove regole ILM per spostare i dati in altri siti o per eliminare i dati degli oggetti dal sito.

- Eseguire le espansioni dei nodi di storage necessarie prima di avviare la procedura di decommissionamento, se possibile.
- Se si esegue una decommissionazione disconnessa del sito, è necessario comprendere la quantità di dati oggetto che diventeranno inaccessibili in modo permanente quando si rimuove il sito.

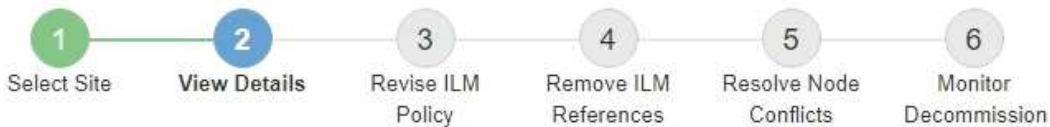


Se si sta eseguendo una decommissionazione disconnessa del sito, ILM non può spostare o eliminare i dati dell'oggetto. Tutti i dati che rimangono nel sito andranno persi. Tuttavia, se la policy ILM è stata progettata per proteggere dalla perdita di un singolo sito, le copie dei dati dell'oggetto rimangono nei siti rimanenti. Vedere ["Abilita la protezione contro la perdita di sito"](#).

Fasi

1. Dal passaggio 2 (Visualizza dettagli), esaminare eventuali avvisi relativi al sito selezionato per la rimozione.

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.

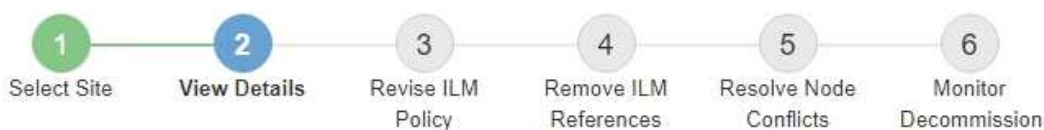
⚠ This site contains a mixture of connected and disconnected nodes. Before you can remove this site, you must bring all offline (blue or gray) nodes back online. Contact technical support if you need assistance.

Viene visualizzato un avviso nei seguenti casi:

- Il sito include un nodo gateway. Se i client S3 si stanno attualmente collegando a questo nodo, è necessario configurare un nodo equivalente in un altro sito. Assicurarsi che i client possano connettersi al nodo sostitutivo prima di continuare con la procedura di decommissionamento.
- Il sito contiene un mix di nodi connessi (✅) e nodi disconnessi (🌙 o 🔄). Prima di poter rimuovere questo sito, devi riportare online tutti i nodi offline.

2. Esaminare i dettagli del sito selezionato per la rimozione.

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 utilizzato totale, lo spazio libero e la capacità di tutti i nodi di storage nel sito.
 - Per la decommissionazione di un sito connesso, il valore **Used Space** rappresenta la quantità di dati oggetto che devono essere spostati in altri siti o cancellati con ILM.
 - Per la decommissionazione di un sito disconnesso, il valore **spazio utilizzato** indica la quantità di dati oggetto che diventeranno inaccessibili quando si rimuove il sito.
- Nomi, tipi e stati di connessione dei nodi:
 -  (Collegato)
 -  (Amministrativamente chiuso)
 -  (Sconosciuto)
- Dettagli su ciascun nodo:
 - Per ciascun nodo di storage, la quantità di spazio utilizzata per i dati dell'oggetto.

- Per i nodi Admin e Gateway, se il nodo è attualmente utilizzato in un gruppo ad alta disponibilità (ha). Non è possibile decommissionare un nodo Admin o un nodo Gateway utilizzato in un gruppo ha. Prima di iniziare la decommissionazione, modificare i gruppi ha per rimuovere tutti i nodi nel sito o rimuovere il gruppo ha se include solo i nodi da questo sito. Per istruzioni, vedere ["Gestire i gruppi ad alta disponibilità \(ha\)"](#).

3. Nella sezione Dettagli per altri siti della pagina, valuta lo spazio disponibile negli altri siti della griglia.

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 una decommissionazione del sito connesso e si prevede di utilizzare ILM per spostare i dati dell'oggetto dal sito selezionato (invece di eliminarli semplicemente), è necessario assicurarsi che gli altri siti abbiano una capacità sufficiente per ospitare i dati spostati e che rimanga una capacità adeguata per la crescita futura.



Viene visualizzato un avviso se lo spazio utilizzato * del sito che si desidera rimuovere è maggiore di **spazio libero totale per altri siti**. Per garantire che sia disponibile una capacità di storage adeguata dopo la rimozione del sito, potrebbe essere necessario eseguire un'espansione prima di eseguire questa procedura.

4. Selezionare **Avanti**.

Viene visualizzato il punto 3 (revisione policy ILM).

Rivedere le politiche ILM per il decommission di un sito in StorageGRID

Dal passaggio 3 (Rivedi criteri ILM) della procedura guidata Decommission Site, è possibile determinare se il sito è referenziato da qualsiasi criterio ILM.

Prima di iniziare

Avete una buona comprensione di come ["Gestire gli oggetti con ILM"](#). Hai familiarità con la creazione di pool di storage e regole ILM e con la simulazione e l'attivazione di una policy ILM.

A proposito di questa attività

StorageGRID non può decommissionare un sito se una regola ILM di qualsiasi policy (attiva o inattiva) fa riferimento a quel sito.

Se un criterio ILM fa riferimento al sito che si desidera decommissionare, è necessario rimuovere tali criteri o modificarli in modo che soddisfino i seguenti requisiti:

- Proteggere completamente tutti i dati degli oggetti.
- Non fare riferimento al sito che si sta smantellando.

- Non utilizzare pool di archiviazione che si riferiscono al sito o utilizzare l'opzione tutti i siti.
- Non utilizzare profili di erasure coding che fanno riferimento al sito.
- Non utilizzare la regola Crea 2 copie da StorageGRID 11,6 o da installazioni precedenti.



Non creare mai una regola ILM a copia singola per consentire la rimozione di un sito. Una regola ILM che crea una sola copia replicata per qualsiasi periodo di tempo mette i dati a rischio di perdita permanente. Se esiste una sola copia replicata di un oggetto, quest'ultimo viene perso in caso di errore o errore significativo di un nodo di storage. Inoltre, durante le procedure di manutenzione, ad esempio gli aggiornamenti, si perde temporaneamente l'accesso all'oggetto.



Se si esegue un *sito connesso decommissionamento*, è necessario considerare come StorageGRID deve gestire i dati dell'oggetto attualmente presenti nel sito che si desidera rimuovere. A seconda dei requisiti di data Protection, nuove regole possono spostare i dati degli oggetti esistenti in siti diversi o possono eliminare eventuali copie aggiuntive degli oggetti che non sono più necessarie.

Contatta il supporto tecnico se hai bisogno di assistenza nella progettazione di una nuova policy.

Fasi

1. Dalla fase 3 (revisione dei criteri ILM), determinare se i criteri ILM fanno riferimento al sito selezionato per la disattivazione.
2. Se non sono elencati criteri, selezionare **Avanti** per passare a "[Fase 4: Rimuovere i riferimenti ILM](#)".
3. Se sono elencati uno o più criteri ILM *Active*, clonare ogni criterio esistente o creare nuovi criteri che non fanno riferimento al sito da smantellare:

- a. Selezionare il collegamento per il criterio nella colonna Nome criterio.

La pagina dei dettagli del criterio ILM per il criterio viene visualizzata in una nuova scheda del browser. La pagina Decommission Site rimane aperta nella scheda Other (Altro).

- b. Attenersi alle seguenti linee guida e istruzioni, se necessario:

- Utilizzare le regole ILM:
 - "[Creare uno o più pool di storage](#)" che non si riferiscono al sito.
 - "[Modificare o sostituire le regole](#)" che fanno riferimento al sito.



Non selezionare la regola **Crea 2 copie** perché questa regola utilizza il pool di storage **tutti i nodi di storage**, che non è consentito.

- Utilizzare i criteri ILM:
 - "[Clonazione di una policy ILM esistente](#)" o "[Creare una nuova policy ILM](#)".
 - Assicurarsi che la regola predefinita e le altre regole non facciano riferimento al sito.



Verificare che le regole ILM siano nell'ordine corretto. Una volta attivato il criterio, gli oggetti nuovi ed esistenti vengono valutati dalle regole nell'ordine elencato, iniziando dall'inizio.

- c. Acquisire gli oggetti di test e simulare la policy per applicare le regole corrette.



Gli errori in un criterio ILM possono causare una perdita di dati irrecuperabile. Esaminare attentamente e simulare la policy prima di attivarla per confermare che funzionerà come previsto.



Quando si attiva un nuovo criterio ILM, StorageGRID lo utilizza per gestire tutti gli oggetti, inclusi quelli esistenti e quelli acquisiti di recente. Prima di attivare un nuovo criterio ILM, esaminare le eventuali modifiche apportate al posizionamento degli oggetti replicati e codificati in cancellazione esistenti. La modifica della posizione di un oggetto esistente potrebbe causare problemi di risorse temporanee quando i nuovi posizionamenti vengono valutati e implementati.

d. Attivare le nuove policy e assicurarsi che le vecchie policy siano ora inattive.

Se si desidera attivare più criteri, "[Seguire la procedura per creare i tag dei criteri ILM](#)".

Se si sta eseguendo una decommissionazione del sito connesso, StorageGRID inizia a rimuovere i dati dell'oggetto dal sito selezionato non appena si attiva il nuovo criterio ILM. Lo spostamento o l'eliminazione di tutte le copie degli oggetti potrebbe richiedere settimane. Sebbene sia possibile avviare in sicurezza la decommissionazione di un sito mentre i dati degli oggetti sono ancora presenti nel sito, la procedura di decommissionazione viene completata più rapidamente e con meno interruzioni e impatti sulle performance se si consente di spostare i dati dal sito prima di avviare la procedura di decommissionazione effettiva (Selezionando **Avvia decommissionazione** nella fase 5 della procedura guidata).

4. Per ciascun criterio *inattivo*, modificarlo o rimuoverlo selezionando prima il collegamento per ciascun criterio come descritto nei passaggi precedenti.
 - "[Modificare il criterio](#)" quindi non fa riferimento al sito da smantellare.
 - "[Rimuovere un criterio](#)".
5. Al termine delle modifiche alle regole e ai criteri ILM, non dovrebbero essere più elencati nel passaggio 3 (revisione dei criteri ILM). Selezionare **Avanti**.

Viene visualizzato il punto 4 (Rimuovi riferimenti ILM).

Rimuovi i riferimenti ILM a un sito in StorageGRID

Dal passaggio 4 (Rimuovi riferimenti ILM) della procedura guidata Decommission Site (Sito di decontaminazione), è necessario eliminare o modificare eventuali regole ILM non utilizzate che fanno riferimento al sito, anche se le regole non sono utilizzate in alcun criterio ILM.

Fasi

1. Determinare se eventuali regole ILM inutilizzate fanno riferimento al sito.

Se sono elencate regole ILM, tali regole fanno ancora riferimento al sito ma non vengono utilizzate in alcuna politica.



Quando StorageGRID decompime il sito, disattiva automaticamente tutti i profili di erasure coding inutilizzati che fanno riferimento al sito ed elimina automaticamente eventuali pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) viene rimosso perché utilizza il sito All Sites.

2. Modificare o eliminare ogni regola inutilizzata:

- Per modificare una regola, andare alla pagina ILM rules (regole ILM) e aggiornare tutti i posizionamenti che utilizzano un profilo di erasure coding o un pool di storage che fa riferimento al sito. Quindi, tornare al **Passo 4 (Rimozione dei riferimenti ILM)**.
- Per eliminare una regola, seleziona l'icona del cestino  e seleziona **OK**.



È necessario eliminare la regola **Make 2 copies** prima di poter decommissionare un sito.

3. Verificare che nessuna regola ILM non utilizzata faccia riferimento al sito e che il pulsante **Avanti** sia attivato.

4. Selezionare **Avanti**.



Tutti i pool storage rimanenti e i profili di erasure coding relativi al sito non saranno più validi quando il sito viene rimosso. Quando StorageGRID decompone il sito, disattiva automaticamente tutti i profili di erasure coding inutilizzati che fanno riferimento al sito ed elimina automaticamente eventuali pool di storage inutilizzati che fanno riferimento al sito. Il pool di storage All Storage Node (StorageGRID 11.6 e versioni precedenti) viene rimosso perché utilizza il sito All Sites.

Viene visualizzato il punto 5 (Risolvi conflitti di nodi).

Risolvere i conflitti tra i nodi e avviare la decommission in StorageGRID

Dalla fase 5 (Risolvi conflitti di nodi) della procedura guidata Smantella sito, è possibile determinare se i nodi nel sistema StorageGRID sono disconnessi o se i nodi nel sito selezionato appartengono a un gruppo ad alta disponibilità (ha). Una volta risolti i conflitti di nodo, avviare la procedura di decommissionamento da questa pagina.

Prima di iniziare

È necessario assicurarsi che tutti i nodi nel sistema StorageGRID siano nello stato corretto, come indicato di seguito:

- Tutti i nodi nel tuo sistema StorageGRID devono essere connessi (.



Se si sta eseguendo una decommissionazione del sito disconnesso, tutti i nodi del sito che si sta rimuovendo devono essere disconnessi e tutti i nodi di tutti gli altri siti devono essere connessi.



La decommissionazione non si avvia se uno o più volumi sono offline (non montati) o se sono online (montati) ma in uno stato di errore.



Se uno o più volumi vengono disconnessi mentre è in corso una decommissionazione, il processo di decommissionamento viene completato dopo che questi volumi sono tornati online.

- Nessun nodo del sito che si sta rimuovendo può avere un'interfaccia che appartiene a un gruppo ad alta disponibilità (ha).

A proposito di questa attività

Se un nodo è elencato per la fase 5 (Risolvi conflitti di nodi), è necessario correggere il problema prima di poter avviare la decommissionazione.

Prima di iniziare la procedura di decommissionamento del sito da questa pagina, fare riferimento alle seguenti considerazioni:

- Per completare la procedura di decommissionamento, è necessario attendere il tempo necessario.



Lo spostamento o l'eliminazione dei dati degli oggetti da un sito potrebbe richiedere giorni, settimane o persino mesi, a seconda della quantità di dati nel sito, del carico sul sistema, delle latenze di rete e della natura delle modifiche ILM richieste.

- Durante l'esecuzione della procedura di decommissionamento del sito:
 - Non è possibile creare regole ILM che si riferiscono al sito da smantellare. Inoltre, non è possibile modificare una regola ILM esistente per fare riferimento al sito.
 - Non è possibile eseguire altre procedure di manutenzione, ad esempio l'espansione o l'aggiornamento.



Se è necessario eseguire un'altra procedura di manutenzione durante la decommissionazione di un sito connesso, è possibile sospendere la procedura durante la rimozione dei nodi di storage. Il pulsante **Pause** viene attivato durante la fase "decommissionamento dei dati replicati ed Erasure-Coded Data" (disattivazione dei dati replicati ed Erasure-Coded Data).

- Se è necessario ripristinare un nodo dopo aver avviato la procedura di decommissionamento del sito, contattare il supporto.

Fasi

1. Esamina la sezione relativa ai nodi disconnessi del passaggio 5 (Risolvi i conflitti tra nodi) per determinare se uno qualsiasi dei nodi nel tuo sistema StorageGRID ha uno stato di connessione Unknown () o Administratively Down ()

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

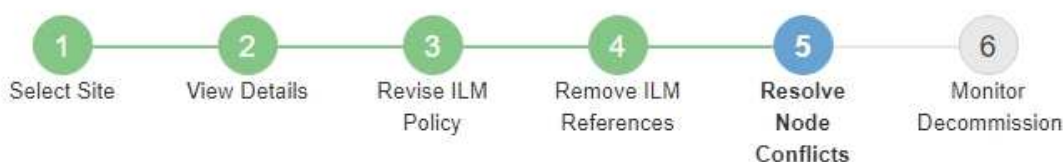
2. Se alcuni nodi sono disconnessi, riportarli in linea.

Consultare la "[Procedure dei nodi](#)". Se hai bisogno di assistenza, contatta il supporto tecnico.

3. Quando tutti i nodi disconnessi sono stati riportati online, consultare la sezione gruppi ha del passaggio 5 (Risolvi i conflitti dei nodi).

Questa tabella elenca tutti i nodi del sito selezionato che appartengono a un gruppo ad alta disponibilità (ha).

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 nell'elenco sono presenti nodi, eseguire una delle seguenti operazioni:

- Modificare ciascun gruppo ha interessato per rimuovere l'interfaccia del nodo.
- Rimuovere un gruppo ha che include solo i nodi da questo sito. Consultare le istruzioni per l'amministrazione di StorageGRID.

Se tutti i nodi sono connessi e nessun nodo del sito selezionato viene utilizzato in un gruppo HA, il campo **Provisioning passphrase** è abilitato.

5. Inserire la passphrase di provisioning.

Il pulsante **Avvia decommissionazione** viene attivato.

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 si è pronti per avviare la procedura di decommissionamento del sito, selezionare **Avvia decommissionazione**.

Un avviso elenca il sito e i nodi che verranno rimossi. Ti ricordiamo che potrebbero essere necessari giorni, settimane o mesi per rimuovere completamente il sito.

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. Esaminare l'avviso. Se si è pronti per iniziare, selezionare **OK**.

Quando viene generata la nuova configurazione della griglia, viene visualizzato un messaggio. Questo processo potrebbe richiedere del tempo, a seconda del tipo e del numero di nodi di rete decommissionati.

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 punto 6 (Monitor Decommission).



Il pulsante **precedente** rimane disattivato fino al completamento della decommissionazione.

Monitora l'avanzamento della decommission del sito in StorageGRID

Dalla fase 6 (Monitor Decommission) della procedura guidata della pagina Decommission Site (Smantella sito), è possibile monitorare l'avanzamento della procedura di rimozione del sito.

A proposito di questa attività

Quando StorageGRID rimuove un sito connesso, rimuove i nodi nel seguente ordine:

1. Nodi gateway
2. Nodi di amministrazione
3. Nodi di storage

Quando StorageGRID rimuove un sito disconnesso, rimuove i nodi nel seguente ordine:

1. Nodi gateway
2. Nodi di storage
3. Nodi di amministrazione

Ogni nodo gateway o nodo amministratore potrebbe richiedere solo pochi minuti o un'ora per la rimozione; tuttavia, i nodi storage potrebbero richiedere giorni o settimane.

Fasi

1. Non appena viene generato un nuovo pacchetto di ripristino, scaricare il file.

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. Scaricare il .zip file.

Vedi le istruzioni per "[scaricando il pacchetto di ripristino](#)".

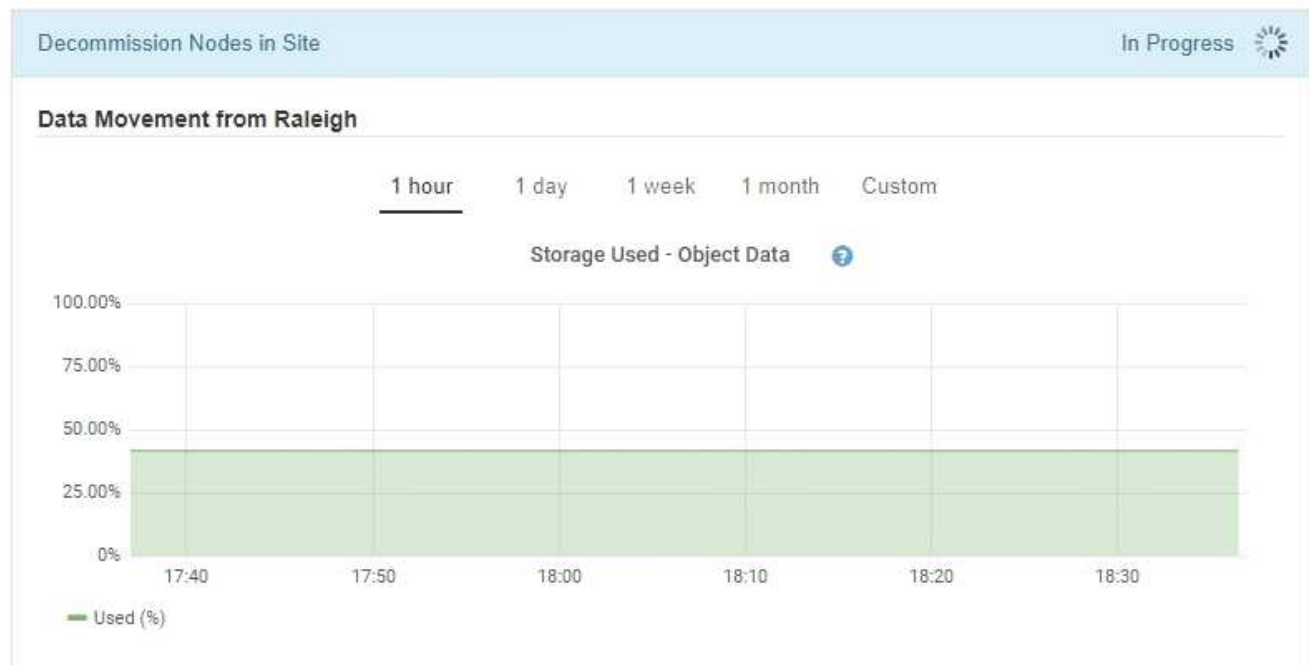


Il file del pacchetto di ripristino deve essere protetto perché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID.

2. Utilizzando il grafico spostamento dati, monitorare lo spostamento dei dati oggetto da questo sito ad altri siti.

Lo spostamento dei dati ha avuto inizio quando è stata attivata la nuova policy ILM nella fase 3 (revisione policy ILM). Lo spostamento dei dati avviene durante l'intera procedura di decommissionamento.

Decommission Site Progress



3. Nella sezione Node Progress della pagina, monitorare l'avanzamento della procedura di decommissionamento man mano che i nodi vengono rimossi.

Quando un nodo di storage viene rimosso, ciascun nodo passa attraverso una serie di fasi. Sebbene la maggior parte di queste fasi si verifichi rapidamente o anche in modo impercettibile, potrebbe essere necessario attendere giorni o addirittura settimane per il completamento di altre fasi, in base alla quantità di dati da spostare. Per gestire i dati con codifica di cancellazione e rivalutare ILM è necessario un tempo aggiuntivo.

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**



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 decommissionazione di un sito connesso, fare riferimento a questa tabella per comprendere le fasi di decommissionamento di un nodo di storage:

Fase	Durata stimata
In sospeso	Minuti o meno
Attendere i blocchi	Minuti
Preparare l'attività	Minuti o meno
Contrassegno LDR disattivato	Minuti
Decommissionamento dei dati replicati ed Erasure-Coded	Ore, giorni o settimane in base alla quantità di dati Nota: Se è necessario eseguire altre attività di manutenzione, è possibile sospendere la decommissionazione del sito in questa fase.
Stato impostato LDR	Minuti
Svuotare le code di audit	Da minuti a ore, in base al numero di messaggi e alla latenza di rete.
Completo	Minuti

Se si sta monitorando l'avanzamento di una decommissionazione di un sito disconnesso, fare riferimento a questa tabella per comprendere le fasi di decommissionamento di un nodo di storage:

Fase	Durata stimata
In sospeso	Minuti o meno
Attendere i blocchi	Minuti
Preparare l'attività	Minuti o meno
Disattiva servizi esterni	Minuti
Revoca del certificato	Minuti
Annulla registrazione nodo	Minuti
Livello di storage Annulla registrazione	Minuti
Rimozione del gruppo di storage	Minuti
Rimozione entità	Minuti

Fase	Durata stimata
Completo	Minuti

4. Una volta che tutti i nodi hanno raggiunto la fase completa, attendere il completamento delle restanti operazioni di decommissionamento del sito.
 - Durante la fase **Riparazione Cassandra**, StorageGRID effettua le riparazioni necessarie ai cluster Cassandra che rimangono nella vostra griglia. Queste riparazioni potrebbero richiedere diversi giorni o più, a seconda del numero di nodi di storage rimasti nel vostro grid.

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 storage**, vengono apportate le seguenti modifiche ILM:
 - Tutti i profili di erasure coding che fanno riferimento al sito sono disattivati.
 - Tutti i pool di storage che fanno riferimento al sito vengono eliminati.



Viene rimosso anche il pool di storage di tutti i nodi di storage (StorageGRID 11.6 e versioni precedenti) in quanto utilizza il sito All Sites.

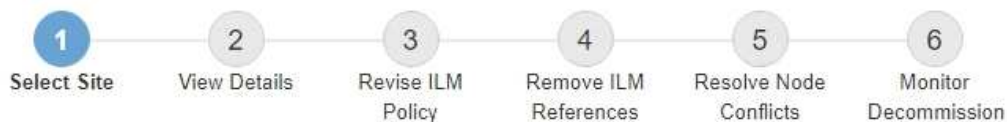
- Infine, durante la fase **Remove Configuration**, tutti i riferimenti rimanenti al sito e ai relativi nodi vengono rimossi dal resto della griglia.

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 decommissionamento, la pagina Decommission Site (Sito di decommissionamento) mostra un messaggio di esito positivo 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

Al termine

Completare queste attività dopo aver completato la procedura di decommissionamento del sito:

- Assicurarsi che i dischi di tutti i nodi di storage nel sito decommissionato siano puliti. Utilizzare uno strumento o un servizio di cancellazione dei dati disponibile in commercio per rimuovere in modo permanente e sicuro i dati dai dischi.
- Se il sito includeva uno o più nodi di amministrazione e l'SSO (Single Sign-on) è attivato per il sistema StorageGRID, rimuovere tutti i trust delle parti che si affidano al sito dai servizi di federazione di Active Directory (ad FS).
- Una volta spenti automaticamente i nodi durante la procedura di decommissionamento del sito connesso, rimuovere le macchine virtuali associate.

Rinominare la griglia, il sito o il nodo

Utilizzare la procedura di ridenominazione di StorageGRID

Se necessario, è possibile modificare i nomi visualizzati in Grid Manager per l'intera griglia, ciascun sito e ciascun nodo. È possibile aggiornare i nomi visualizzati in modo sicuro e in qualsiasi momento.

Qual è la procedura di ridenominazione?

Quando si installa inizialmente StorageGRID, specificare un nome per la griglia, ciascun sito e ciascun nodo. Questi nomi iniziali sono noti come *nomi di sistema* e sono i nomi inizialmente mostrati in StorageGRID.

I nomi di sistema sono richiesti per le operazioni StorageGRID interne e non possono essere modificati. Tuttavia, è possibile utilizzare la procedura di ridenominazione per definire nuovi *nomi di visualizzazione* per la griglia, ciascun sito e ciascun nodo. Questi nomi visualizzati vengono visualizzati in diverse posizioni StorageGRID invece dei nomi di sistema sottostanti (o in alcuni casi, oltre a questi).

Utilizzare la procedura di ridenominazione per correggere gli errori di battitura, implementare una convenzione di naming diversa o per indicare che un sito e tutti i suoi nodi sono stati ricollocati. A differenza dei nomi di sistema, i nomi visualizzati possono essere aggiornati quando richiesto e senza influire sulle operazioni StorageGRID.

Dove vengono visualizzati i nomi di sistema e di visualizzazione?

La seguente tabella riassume i nomi dei sistemi e dei display nell'interfaccia utente di StorageGRID e nei file StorageGRID.

Posizione	Nome del sistema	Nome visualizzato
Pagine di Grid Manager	Visualizzato a meno che l'elemento non venga rinominato	Se un elemento viene rinominato, viene visualizzato invece del nome del sistema in queste posizioni: • Dashboard • Pagina nodi • Pagine di configurazione per gruppi ad alta disponibilità, endpoint del bilanciamento del carico, interfacce VLAN, server di gestione delle chiavi, password grid, e il controllo del firewall • Avvisi • Definizioni del pool di storage • Pagina di ricerca dei metadati degli oggetti • Pagine relative alle procedure di manutenzione, tra cui upgrade, hotfix, upgrade del sistema operativo SANtricity, decommissionamento, espansione, ripristino e controllo dell'esistenza di oggetti • Pagine di supporto (registri e diagnostica) • Pagina Single Sign-on (accesso singolo), accanto al nome host del nodo di amministrazione nella tabella per i dettagli del nodo di amministrazione
Nodi > Scheda Panoramica per un nodo	Sempre mostrato	Visualizzato solo se l'elemento viene rinominato
API node-Health	Sempre restituito	Restituito solo se l'elemento viene rinominato

Posizione	Nome del sistema	Nome visualizzato
Prompt quando si utilizza SSH per accedere a un nodo	Visualizzato come nome principale a meno che l'elemento non sia stato rinominato: <pre>admin@SYSTEM-NAME: ~ \$</pre> Incluso tra parentesi quando l'elemento viene rinominato: <pre>admin@DISPLAY-NAME (SYSTEM-NAME): ~ \$</pre>	Visualizzato come nome principale quando l'elemento viene rinominato: <pre>admin@DISPLAY-NAME (SYSTEM-NAME): ~ \$</pre>
'Passwords.txt' file nel pacchetto di ripristino	Mostrato come Server Name	Mostrato come Display Name
/etc/hosts su tutti i nodi Ad esempio: <pre>10.96.99.128 SYSTEM-NAME 28989c59-a2c3-4d30-bb09-6879adf2437f DISPLAY-NAME localhost-grid # storagegrid-gen-host</pre>	Sempre mostrato nella seconda colonna	Quando l'elemento viene rinominato, visualizzato nella quarta colonna
topology-display-names.json, Incluso con i dati AutoSupport	Non incluso	Vuoto a meno che gli elementi non siano stati rinominati; in caso contrario, gli ID di griglia, sito e nodo vengono mappati sui rispettivi nomi visualizzati.

Requisiti per i nomi visualizzati

Prima di utilizzare questa procedura, esaminare i requisiti per i nomi visualizzati.

Visualizza i nomi dei nodi

I nomi visualizzati per i nodi devono seguire queste regole:

- Deve essere unico nel tuo sistema StorageGRID.
- Non può essere uguale al nome di sistema per qualsiasi altro elemento nel sistema StorageGRID.
- Deve contenere almeno 1 e non più di 32 caratteri.
- Può contenere numeri, trattini (-) e lettere maiuscole e minuscole.
- Può iniziare o terminare con una lettera o un numero, ma non può iniziare o terminare con un trattino.
- Non possono essere tutti i numeri.
- Sono insensibili alle maiuscole e alle minuscole. Ad esempio, DC1-ADM e dc1-adm sono considerati duplicati.

È possibile rinominare un nodo con un nome visualizzato precedentemente utilizzato da un nodo diverso, a condizione che la ridenominazione non comporti un nome visualizzato o un nome di sistema duplicati.

Visualizza i nomi della griglia e dei siti

I nomi visualizzati per la griglia e i siti seguono le stesse regole con le seguenti eccezioni:

- Può includere spazi.
- Può includere questi caratteri speciali: = - _ : , . @ !
- Può iniziare e terminare con i caratteri speciali, inclusi i trattini.
- Può essere composto da tutti i numeri o da caratteri speciali.

Best practice per i nomi visualizzati

Se si prevede di rinominare più elementi, documentare lo schema di denominazione generale prima di utilizzare questa procedura. Un sistema che garantisce nomi univoci, coerenti e facili da comprendere a colpo d'occhio.

È possibile utilizzare qualsiasi convenzione di naming che soddisfi i requisiti dell'organizzazione. Prendi in considerazione questi suggerimenti di base su cosa includere:

- **Site indicator:** Se si dispone di più siti, aggiungere un codice sito a ciascun nome di nodo.
- **Node type:** I nomi dei nodi indicano generalmente il tipo di nodo. È possibile utilizzare abbreviazioni come s, adm, e gw (nodo di archiviazione, nodo amministrativo e nodo gateway).
- **Node Number:** Se un sito contiene più di uno di un particolare tipo di nodo, aggiungere un numero univoco al nome di ciascun nodo.

Pensa due volte prima di aggiungere dettagli specifici ai nomi che potrebbero cambiare nel tempo. Ad esempio, non includere gli indirizzi IP nei nomi dei nodi perché è possibile modificarli. Allo stesso modo, le posizioni dei rack o i numeri dei modelli di appliance possono cambiare se si spostano le apparecchiature o si aggiorna l'hardware.

Esempi di nomi visualizzati

Si supponga che il sistema StorageGRID disponga di tre data center e di nodi di tipi diversi in ciascun data center. I nomi visualizzati potrebbero essere semplici come questi:

- **Griglia:** StorageGRID Deployment
- **Primo sito:** Data Center 1

- dc1-adm1
- dc1-s1
- dc1-s2
- dc1-s3
- dc1-gw1

- **Secondo sito:** Data Center 2

- dc2-adm2
- dc2-s1
- dc2-s2
- dc2-s3

- **Terzo sito:** Data Center 3

- dc3-s1
- dc3-s2
- dc3-s3

Aggiungi o aggiorna i nomi visualizzati di StorageGRID

È possibile utilizzare questa procedura per aggiungere o aggiornare i nomi di visualizzazione utilizzati per la griglia, i siti e i nodi. È possibile rinominare un singolo elemento, più elementi o anche tutti gli elementi contemporaneamente. La definizione o l'aggiornamento di un nome visualizzato non influisce in alcun modo sulle operazioni StorageGRID.

Prima di iniziare

- Da qualsiasi nodo di amministrazione, accedi a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Hai compreso i requisiti e le Best practice per i nomi visualizzati. Vedere ["Rinominare la griglia, i siti e i nodi"](#).

Come rinominare la griglia, i siti o i nodi

È possibile rinominare il sistema StorageGRID, uno o più siti o uno o più nodi.

È possibile utilizzare un nome visualizzato precedentemente utilizzato da un nodo diverso, purché il nome non sia un nome visualizzato o un nome di sistema duplicati.

Selezionare gli elementi da rinominare

Per iniziare, selezionare gli elementi che si desidera rinominare.

Fasi

1. Selezionare **Manutenzione > Attività > Rinomina griglia, siti e nodi**.

2. Per il passo **Select Names**, selezionare gli elementi che si desidera rinominare.

Elemento da modificare	Istruzioni
Nomi di tutto (o quasi tutto) nel sistema	a. Selezionare Seleziona tutto . b. Se si desidera, deselezionare gli elementi che non si desidera rinominare.
Nome della griglia	Selezionare la casella di controllo della griglia.
Nome di un sito e di alcuni o di tutti i suoi nodi	a. Selezionare la casella di controllo nell'intestazione della tabella per il sito. b. Facoltativamente, deselezionare i nodi che non si desidera rinominare.
Nome di un sito	Selezionare la casella di controllo del sito.
Nome di un nodo	Selezionare la casella di controllo del nodo.

3. Selezionare **continua**.

4. Esaminare la tabella, che include gli elementi selezionati.

- La colonna **Nome visualizzato** mostra il nome corrente di ciascun elemento. Se l'elemento non è mai stato rinominato, il nome visualizzato corrisponde al nome del sistema.
- La colonna **Nome sistema** mostra il nome immesso per ciascun elemento durante l'installazione. I nomi di sistema vengono utilizzati per le operazioni StorageGRID interne e non possono essere modificati. Ad esempio, il nome di sistema di un nodo potrebbe essere il nome host.
- La colonna **Type** indica il tipo di elemento: Grid, Site o il tipo di nodo specifico.

Proporre nuovi nomi

Per il passo **proporre nuovi nomi**, è possibile immettere un nome visualizzato per ciascun elemento singolarmente oppure rinominare gli elementi in blocco.

Rinominare gli elementi singolarmente

Seguire questa procedura per inserire un nome visualizzato per ciascun elemento che si desidera rinominare.

Fasi

1. Nel campo **Display name** (Nome visualizzato), immettere un nome visualizzato per ciascun elemento dell'elenco.

Vedere "[Rinominare la griglia, i siti e i nodi](#)" per conoscere i requisiti di denominazione.

2. Per rimuovere gli elementi che non vuoi rinominare, seleziona  nella colonna **Rimuovi dall'elenco**.

Se non si intende proporre un nuovo nome per un elemento, è necessario rimuoverlo dalla tabella.

3. Una volta proposti nuovi nomi per tutti gli elementi della tabella, selezionare **Rinomina**.

Viene visualizzato un messaggio di successo. I nuovi nomi visualizzati vengono ora utilizzati in Grid Manager.

Rinominare gli elementi in blocco

Utilizzare lo strumento di ridenominazione in blocco se i nomi degli elementi condividono una stringa comune che si desidera sostituire con una stringa diversa.

Fasi

1. Per il passo **proporre nuovi nomi**, selezionare **Usa lo strumento di ridenominazione in blocco**.

L'anteprima **Rename (Rinomina)** include tutti gli elementi visualizzati per il passo **Proponi nuovi nomi**. È possibile utilizzare l'anteprima per visualizzare l'aspetto dei nomi visualizzati dopo la sostituzione di una stringa condivisa.

2. Nel campo **existing string**, immettere la stringa condivisa che si desidera sostituire. Ad esempio, se la stringa che si desidera sostituire è `Data-Center-1`, immettere **Data-Center-1**.

Durante la digitazione, il testo viene evidenziato ovunque si trovi nei nomi a sinistra.

3. Seleziona  per rimuovere gli elementi che non vuoi rinominare con questo strumento.

Ad esempio, supponi di voler rinominare tutti i nodi che contengono la stringa `Data-Center-1`, ma non vuoi rinominare il sito `Data-Center-1` stesso. Seleziona  per rimuovere il sito dall'anteprima di rinomina.

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 **New string** (Nuova stringa), immettere la stringa sostitutiva che si desidera utilizzare. Ad esempio, inserire **DC1**.

Vedere "Rinominare la griglia, i siti e i nodi" per conoscere i requisiti di denominazione.

Quando si inserisce la stringa di sostituzione, i nomi a sinistra vengono aggiornati, in modo da verificare che i nuovi nomi siano corretti.

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.

- Una volta soddisfatti dei nomi visualizzati nell'anteprima, selezionare **Aggiungi nomi** per aggiungere i nomi alla tabella per il passo **proporre nuovi nomi**.
- Apporta le modifiche aggiuntive necessarie oppure seleziona ✕ per rimuovere gli elementi che non vuoi rinominare.
- Quando si è pronti a rinominare tutti gli elementi della tabella, selezionare **Rinomina**.

Viene visualizzato un messaggio di successo. I nuovi nomi visualizzati vengono ora utilizzati in Grid Manager.

Scarica il pacchetto di ripristino

Una volta terminata la ridenominazione degli elementi, scarica e salva un nuovo pacchetto di ripristino. I nuovi nomi visualizzati per gli elementi rinominati sono inclusi nel `Passwords.txt` file.

Fasi

- Inserire la passphrase di provisioning.
- Selezionare **Download recovery package** (Scarica pacchetto di ripristino).

Il download viene avviato immediatamente.

- Al termine del download, aprire il `Passwords.txt` file per visualizzare il nome del server per tutti i nodi e i nomi visualizzati per tutti i nodi rinominati.
- Copiare il `sgws-recovery-package-id-revision.zip` file in due posizioni sicure, sicure e separate.



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

5. Selezionare **fine** per tornare al primo passaggio.

Ripristare i nomi visualizzati ai nomi di sistema

È possibile ripristinare il nome di sistema originale di una griglia, di un sito o di un nodo rinominato. Quando si ripristina il nome di sistema di un elemento, le pagine di Grid Manager e altre posizioni StorageGRID non mostrano più un **Nome visualizzato** per quell'elemento. Viene visualizzato solo il nome di sistema dell'elemento.

Fasi

1. Selezionare **Manutenzione > Attività > Rinomina griglia, siti e nodi**.
2. Per il passo **Select Names**, selezionare gli elementi che si desidera ripristinare ai nomi di sistema.
3. Selezionare **continua**.
4. Per il passo **proporre nuovi nomi**, ripristinare i nomi visualizzati in nomi di sistema singolarmente o in blocco.

Ripristinare i nomi di sistema singolarmente

- a. Copia il nome di sistema originale di ciascun elemento e incollalo nel campo **Nome visualizzato**, oppure seleziona **X** per rimuovere gli elementi che non vuoi ripristinare.

Per ripristinare un nome visualizzato, il nome del sistema deve essere visualizzato nel campo **Nome visualizzato**, ma il nome non fa distinzione tra maiuscole e minuscole.

- b. Selezionare **Rinomina**.

Viene visualizzato un messaggio di successo. I nomi visualizzati per questi elementi non vengono più utilizzati.

Ripristinare i nomi di sistema in blocco

- a. Per il passo **proporre nuovi nomi**, selezionare **Usa lo strumento di ridenominazione in blocco**.
- b. Nel campo **existing string**, immettere la stringa del nome da sostituire.
- c. Nel campo **New string**, immettere la stringa del nome di sistema che si desidera utilizzare.
- d. Selezionare **Aggiungi nomi** per aggiungere i nomi alla tabella per il passo **proporre nuovi nomi**.
- e. Verifica che ogni voce nel campo **Nome visualizzato** corrisponda al nome nel campo **Nome di sistema**. Apporta le modifiche necessarie o seleziona **X** per rimuovere gli elementi che non vuoi ripristinare.

Per ripristinare un nome visualizzato, il nome del sistema deve essere visualizzato nel campo **Nome visualizzato**, ma il nome non fa distinzione tra maiuscole e minuscole.

- f. Selezionare **Rinomina**.

Viene visualizzato un messaggio di successo. I nomi visualizzati per questi elementi non vengono più utilizzati.

5. Scarica e salva un nuovo pacchetto di ripristino .

I nomi visualizzati per gli elementi ripristinati non sono più inclusi nel `Passwords.txt` file.

Procedure dei nodi

Procedure di manutenzione dei nodi StorageGRID

Potrebbe essere necessario eseguire procedure di manutenzione relative a specifici nodi di rete o servizi di nodi.

Sposta ADC

IL ["Servizio ADC"](#) si trova su alcuni nodi di archiviazione. In determinate circostanze di dismissione e conversione dei nodi, è necessario spostare il servizio ADC su un altro nodo di archiviazione nello stesso sito.

Convertire il nodo di archiviazione in un nodo solo dati

È possibile convertire i nodi di archiviazione che non contengono il servizio ADC in nodi di archiviazione solo dati.

Riavvio, spegnimento e alimentazione del nodo

Queste procedure vengono utilizzate per riavviare uno o più nodi, per arrestare e riavviare i nodi o per spegnere e riaccendere i nodi.

Rimappatura delle porte

È possibile utilizzare le procedure di rimappamento delle porte per rimuovere i rimappamenti delle porte da un nodo, ad esempio, se si desidera configurare un endpoint di bilanciamento del carico utilizzando una porta precedentemente rimappata.

Responsabile del server

Server Manager viene eseguito su ogni nodo grid per supervisionare l'avvio e l'arresto dei servizi e per garantire che i servizi si uniscano e abbandonino correttamente il sistema StorageGRID. Server Manager monitora inoltre i servizi su ogni nodo grid e tenta automaticamente di riavviare tutti i servizi che segnalano gli errori.

Per eseguire le procedure di Server Manager, in genere è necessario accedere alla riga di comando del nodo.



L'accesso a Server Manager deve essere effettuato solo se il supporto tecnico lo ha richiesto.

Spostare il servizio ADC in StorageGRID

È possibile spostare il servizio ADC su un altro nodo di archiviazione nello stesso sito.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Hai ["Autorizzazione di manutenzione o di accesso root"](#) .
- Il nodo sorgente contiene il servizio ADC.

- Il nodo di destinazione non contiene il servizio ADC.
- Il nodo di destinazione è un nodo contenente solo metadati o un nodo combinato (metadati e dati oggetto).
- Il nodo sorgente e il nodo di destinazione si trovano nello stesso sito.

A proposito di questa attività

Usa la procedura Sposta ADC per spostare manualmente il servizio ADC tra i nodi di storage. Ad esempio, potresti voler ridistribuire i servizi ADC tra i nodi o spostare il servizio ADC su un nodo con prestazioni superiori.

Questa procedura sposta i servizi ADC, IDNT, ACCT e RSM da un nodo di archiviazione a un altro nello stesso sito. I servizi RSM, IDNT e ACCT dipendono dal servizio ADC, pertanto vengono spostati automaticamente quando si sposta il servizio ADC.



- Non devi spostare manualmente il servizio ADC prima di ["conversione di un nodo di archiviazione in un nodo solo dati"](#) o decommissionare un Storage Node. Queste procedure spostano automaticamente il servizio ADC quando richiesto. Consulta ["Che cos'è il quorum dell'ADC?"](#) per i dettagli sui requisiti.
- StorageGRID sposta il servizio ADC sui nodi di storage più recenti che soddisfano i requisiti per l'hosting del servizio.

Fasi

1. Registrare gli ID dei nodi di origine e di destinazione.

Nell'API di gestione della griglia, l'ID del nodo sorgente è denominato `sourceNodeId`. L'ID del nodo di destinazione è denominato `targetNodeId`.

2. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
3. Selezionare **Vai alla documentazione API privata**.
4. Seleziona il `POST /private/move-adc/start` operazione. Fare riferimento a ["Emettere richieste API"](#) per maggiori informazioni.

Durante la procedura, i due nodi si riavvieranno in sequenza. Il nodo sorgente si riavvia per primo, seguito dal nodo di destinazione.

5. Puoi usare `GET /private/move-adc` per monitorare la procedura. Se si verificano errori, selezionare `POST /private/move-adc/retry` per riprovare la procedura.
6. ["Scarica un pacchetto di ripristino"](#) dopo aver completato questa procedura.

Convertire un nodo di storage StorageGRID in un nodo di soli dati

Per aumentare le prestazioni, è possibile convertire i nodi di archiviazione non ADC più lenti in nodi di archiviazione solo dati.

L'utilizzo di un nodo di storage esclusivamente per i dati può essere utile se i nodi di storage hanno caratteristiche di prestazioni diverse. Ad esempio, per aumentare potenzialmente le performance, potrebbero esserci nodi di storage su disco rotante a elevata capacità e solo dati accompagnati da nodi di storage dalle performance elevate e solo metadati.

Inoltre, è possibile ottenere una maggiore capacità di metadati rimuovendo i nodi con poca RAM da Cassandra, il che aumenta il limite di capacità di metadati per nodo. Fare riferimento a ["Gestire lo storage dei"](#)

[metadati degli oggetti](#)" .

Quando si convertono nodi solo dati, la griglia deve contenere almeno tre nodi di archiviazione combinati o solo metadati per sito.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Il nodo di archiviazione non è un nodo solo metadati o solo dati.
- Se il nodo di archiviazione contiene il servizio ADC, più di due nodi di archiviazione ADC sono online nella griglia e nodi di archiviazione non ADC sono disponibili nello stesso sito per ospitare il servizio ADC.
- C'è abbastanza spazio per i metadati su altri nodi del sito (o hai ["ha ampliato la tua griglia"](#)) per ospitare i metadati che verranno migrati dal nodo di archiviazione che si sta convertendo.



- Se i metadati che migrano verso altri nodi sullo stesso sito superano le dimensioni del ["spazio riservato ai metadati"](#) , la rete diventerà instabile.
- Dopo aver avviato la conversione, non sarà più possibile espandere la griglia.

A proposito di questa attività

Usa questa procedura per convertire uno o più nodi di archiviazione combinati in nodi solo dati. Se un nodo di archiviazione contiene il servizio ADC, il servizio viene automaticamente spostato su un altro nodo di archiviazione nello stesso sito durante la conversione.

Oltre a convertire il nodo di archiviazione, questa procedura dismette Cassandra dal nodo. Tutti i metadati verranno migrati verso nodi di archiviazione combinati o contenenti solo metadati. A seconda della quantità di metadati da migrare, il completamento di questa procedura potrebbe richiedere fino a diversi giorni per nodo.



In genere, è possibile convertire fino a 10 nodi alla volta se l'utilizzo dei metadati per nodo è inferiore a 1 TB. Se l'utilizzo dei metadati per nodo è superiore a 1 TB, convertire fino a 5 nodi per procedura.



StorageGRID sposta il servizio ADC sui nodi di storage più recenti che soddisfano i requisiti per l'hosting del servizio.

Fasi

1. Registrare gli ID dei nodi di archiviazione non ADC che si desidera convertire.
2. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
3. Selezionare **Vai alla documentazione API privata**.
4. Seleziona il POST `/private/convert-to-data-only-node/start` operazione. Fare riferimento a ["Emettere richieste API"](#) per maggiori informazioni.

Ogni nodo verrà riavviato durante la procedura.

5. Puoi usare GET `/private/convert-to-data-only-node` per monitorare la procedura. Se si verificano errori, selezionare POST `/private/convert-to-data-only-node/retry` per riprovare la procedura.
6. ["Scarica un pacchetto di ripristino"](#) dopo aver completato questa procedura.

Procedure di riavvio, spegnimento e alimentazione

Eseguire un riavvio progressivo di StorageGRID

È possibile eseguire un riavvio in sequenza per riavviare più nodi grid senza causare un'interruzione del servizio.

Prima di iniziare

- Si è effettuato l'accesso al Grid Manager sul nodo amministrativo primario e si sta utilizzando un ["browser web supportato"](#).



Per eseguire questa procedura, è necessario aver effettuato l'accesso al nodo amministrativo primario.

- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).

A proposito di questa attività

Utilizzare questa procedura se è necessario riavviare più nodi contemporaneamente. Ad esempio, è possibile utilizzare questa procedura dopo aver modificato la modalità FIPS per la griglia ["Criteri di sicurezza TLS e SSH"](#). Quando la modalità FIPS cambia, è necessario riavviare tutti i nodi per rendere effettiva la modifica.



Se è necessario riavviare un solo nodo, è possibile ["Riavviare il nodo dalla scheda Tasks \(attività\)"](#).

Quando StorageGRID riavvia i nodi della griglia, invia il `reboot` comando su ogni nodo, provocando l'arresto e il riavvio del nodo. Tutti i servizi vengono riavviati automaticamente.

- Il riavvio di un nodo VMware riavvia la macchina virtuale.
- Il riavvio di un nodo Linux riavvia il contenitore.
- Il riavvio di un nodo dell'appliance StorageGRID riavvia il controller di elaborazione.

La procedura di riavvio in sequenza può riavviare più nodi contemporaneamente, con le seguenti eccezioni:

- Due nodi dello stesso tipo non verranno riavviati contemporaneamente.
- I nodi gateway e i nodi amministrativi non verranno riavviati contemporaneamente.

Al contrario, questi nodi vengono riavviati in sequenza per garantire che i gruppi di ha, i dati degli oggetti e i servizi dei nodi critici rimangano sempre disponibili.

Quando si riavvia il nodo amministrativo primario, il browser perde temporaneamente l'accesso al Grid Manager, quindi non è più possibile monitorare la procedura. Per questo motivo, il nodo amministrativo primario viene riavviato per ultimo.

Eseguire un riavvio a rotazione

Selezionare i nodi che si desidera riavviare, rivedere le selezioni, avviare la procedura di riavvio e monitorare l'avanzamento.

Selezionare nodi

Come primo passo, accedere alla pagina di riavvio in sequenza e selezionare i nodi che si desidera riavviare.

Fasi

1. Selezionare **Manutenzione > Attività > Riavvio progressivo**.
2. Esaminare le icone di stato della connessione e di avviso nella colonna **Nome nodo**.



Non puoi riavviare un nodo se è disconnesso dalla grid. Le caselle di controllo sono disabilitate per i nodi con queste icone:  o .

3. Se in un nodo sono presenti avvisi attivi, esaminare l'elenco degli avvisi nella colonna **Riepilogo avvisi**.



Per visualizzare tutti gli avvisi correnti per un nodo, è anche possibile selezionare **Nodi > scheda Panoramica**.

4. Facoltativamente, eseguire le azioni consigliate per risolvere eventuali avvisi correnti.
5. Facoltativamente, se tutti i nodi sono connessi e si desidera riavviarli tutti, selezionare la casella di controllo nell'intestazione della tabella e selezionare **Seleziona tutto**. In caso contrario, selezionare ciascun nodo che si desidera riavviare.

È possibile utilizzare le opzioni di filtro della tabella per visualizzare i sottogruppi di nodi. Ad esempio, è possibile visualizzare e selezionare solo nodi di archiviazione o tutti i nodi di un determinato sito.

6. Selezionare **Rivedi selezione**.

Selezione di revisione

In questo passaggio, è possibile determinare il tempo necessario per la procedura di riavvio totale e confermare di aver selezionato i nodi corretti.

1. Nella pagina di selezione Revisione, esaminare il Riepilogo, che indica il numero di nodi che verranno riavviati e il tempo totale stimato per il riavvio di tutti i nodi.
2. Se si desidera, per rimuovere un nodo specifico dall'elenco di riavvio, selezionare **Rimuovi**.
3. In alternativa, per aggiungere altri nodi, selezionare **passaggio precedente**, selezionare i nodi aggiuntivi e selezionare **selezione revisione**.
4. Quando si è pronti ad avviare la procedura di riavvio in sequenza per tutti i nodi selezionati, selezionare **Reboot Node** (Riavvia nodi).
5. Se si è scelto di riavviare il nodo amministrativo primario, leggere il messaggio informativo e selezionare **Sì**.



Il nodo amministrativo primario sarà l'ultimo nodo da riavviare. Durante il riavvio di questo nodo, la connessione del browser andrà persa. Quando il nodo amministrativo primario è nuovamente disponibile, è necessario ricaricare la pagina di riavvio in sequenza.

Monitorare un riavvio continuo

Durante l'esecuzione della procedura di riavvio in sequenza, è possibile monitorarla dal nodo amministrativo principale.

Fasi

1. Esaminare lo stato di avanzamento generale dell'operazione, che include le seguenti informazioni:

- Numero di nodi riavviati
- Numero di nodi in corso di riavvio
- Numero di nodi che devono ancora essere riavviati

2. Esaminare la tabella per ciascun tipo di nodo.

Le tabelle forniscono una barra di avanzamento dell'operazione su ciascun nodo e mostrano la fase di riavvio per quel nodo, che può essere una delle seguenti:

- In attesa del riavvio
- Interruzione dei servizi
- Riavvio del sistema in corso
- Avvio dei servizi
- Riavvio completato

Interrompere la procedura di riavvio in sequenza

È possibile interrompere la procedura di riavvio in sequenza dal nodo amministrativo primario. Quando si arresta la procedura, qualsiasi nodo che abbia lo stato "arresto dei servizi", "riavvio del sistema" o "avvio dei servizi" completerà l'operazione di riavvio. Tuttavia, questi nodi non saranno più registrati come parte della procedura.

Fasi

1. Selezionare **Manutenzione > Attività > Riavvio progressivo**.
2. Dal passaggio **Monitor reboot** (riavvio monitor), selezionare **Stop reboot procedure** (Interrompi procedura di riavvio).

Riavvia il nodo StorageGRID dalla scheda Attività

È possibile riavviare un singolo nodo della griglia dalla scheda attività della pagina nodi.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Se si sta riavviando il nodo amministrativo primario o qualsiasi nodo di storage, sono state esaminate le seguenti considerazioni:
 - Quando si riavvia il nodo amministrativo primario, il browser perde temporaneamente l'accesso al Grid Manager.
 - Se si riavviano due o più nodi di archiviazione in un determinato sito, potrebbe non essere possibile accedere a determinati oggetti per la durata del riavvio. Questo problema può verificarsi se una regola ILM utilizza l'opzione di acquisizione **Dual Commit** (o una regola specifica **Balanced** e non è possibile creare immediatamente tutte le copie richieste). In questo caso, StorageGRID assegna gli oggetti appena acquisiti a due nodi storage nello stesso sito e valuta l'ILM in un secondo momento.
 - Per garantire l'accesso a tutti gli oggetti durante il riavvio di un nodo di storage, interrompere l'acquisizione di oggetti in un sito per circa un'ora prima di riavviare il nodo.

A proposito di questa attività

Quando StorageGRID riavvia un nodo grid, invia un comando sul nodo, `reboot` provocando l'arresto e il riavvio del nodo. Tutti i servizi vengono riavviati automaticamente.

- Il riavvio di un nodo VMware riavvia la macchina virtuale.
- Il riavvio di un nodo Linux riavvia il contenitore.
- Il riavvio di un nodo dell'appliance StorageGRID riavvia il controller di elaborazione.



Se è necessario riavviare più di un nodo, è possibile utilizzare "[procedura di riavvio in sequenza](#)".

Fasi

1. Selezionare **Nodi**.
2. Selezionare il nodo della griglia che si desidera riavviare.
3. Selezionare la scheda **Tasks**.
4. Selezionare **Reboot** (Riavvia).

Viene visualizzata una finestra di dialogo di conferma. Se si sta riavviando il nodo di amministrazione primario, la finestra di dialogo di conferma ricorda che la connessione del browser a Grid Manager viene temporaneamente persa quando i servizi vengono arrestati.

5. Inserire la passphrase di provisioning e selezionare **OK**.
6. Attendere il riavvio del nodo.

L'arresto dei servizi potrebbe richiedere del tempo.

Quando il nodo viene riavviato, viene visualizzata l'icona grigia (amministrativamente giù) per il nodo nella pagina nodi. Quando tutti i servizi sono stati riavviati e il nodo è collegato correttamente alla griglia, la pagina dei nodi dovrebbe visualizzare lo stato normale (nessuna icona a sinistra del nome del nodo), indicando che non sono attivi avvisi e che il nodo è connesso alla griglia.

Riavvia il nodo StorageGRID dalla shell dei comandi

Se è necessario monitorare più da vicino l'operazione di riavvio o se non si riesce ad accedere a Grid Manager, è possibile accedere al nodo Grid ed eseguire il comando di riavvio di Server Manager dalla shell dei comandi.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Facoltativamente, arrestare i servizi: `service servermanager stop`

L'interruzione dei servizi è un passaggio facoltativo, ma consigliato. L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto prima di riavviare il nodo nella fase successiva.

3. Riavviare il nodo della griglia: `reboot`
4. Disconnettersi dalla shell dei comandi: `exit`

Arrestare il nodo StorageGRID

È possibile chiudere un nodo Grid dalla shell dei comandi del nodo.

Prima di iniziare

- Si dispone del `Passwords.txt` file.

A proposito di questa attività

Prima di eseguire questa procedura, esaminare le seguenti considerazioni:

- In generale, non è necessario spegnere più di un nodo alla volta per evitare interruzioni.
- Non spegnere un nodo durante una procedura di manutenzione, a meno che non venga espressamente richiesto dalla documentazione o dal supporto tecnico.
- Il processo di shutdown si basa sulla posizione in cui è installato il nodo, come segue:
 - L'arresto di un nodo VMware arresta la macchina virtuale.
 - L'arresto di un nodo Linux arresta il container.
 - L'arresto di un nodo appliance StorageGRID arresta il controller di calcolo.
- Se si prevede di chiudere più di un nodo di storage in un sito, interrompere l'acquisizione di oggetti in quel sito per circa un'ora prima di spegnere i nodi.

Se una regola ILM utilizza l'opzione di acquisizione **doppio commit** (o se una regola utilizza l'opzione **bilanciato** e non è possibile creare immediatamente tutte le copie richieste), StorageGRID commuta immediatamente gli oggetti appena acquisiti su due nodi di storage sullo stesso sito e valuta ILM in un secondo momento. Se più di un nodo di storage in un sito viene arrestato, potrebbe non essere possibile accedere agli oggetti appena acquisiti per la durata della chiusura. Anche le operazioni di scrittura potrebbero non riuscire se nel sito rimangono disponibili troppi nodi di storage. Vedere ["Gestire gli oggetti con ILM"](#).

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare tutti i servizi: `service servermanager stop`

L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

3. Se il nodo è in esecuzione su una macchina virtuale VMware o si tratta di un nodo appliance, eseguire il comando shutdown: `shutdown -h now`

Eseguire questa operazione indipendentemente dal risultato del `service servermanager stop` comando.



Dopo aver inviato il `shutdown -h now` comando su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

Per l'appliance, questo comando spegne il controller, ma l'appliance è ancora accesa. Completare la fase successiva.

4. Se si sta spegnendo un nodo appliance, seguire la procedura relativa all'appliance.

SG6160

- a. Spegner il controller di storage SG6100-CN.
- b. Attendere lo spegnimento del LED di alimentazione blu sul controller di archiviazione SG6100-CN.

SGF6112

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6000

- a. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED di alimentazione blu si spenga.

SG5800

- a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
- c. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
- d. Spegner entrambi gli interruttori di alimentazione sul ripiano del controller e attendere lo spegnimento di tutti i LED sul ripiano del controller.

SG5700

- a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

SG100 o SG1000

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

Spegner un host StorageGRID

Prima di spegnere un host, è necessario interrompere i servizi su tutti i nodi della rete su tale host.

Fasi

1. Accedere al nodo Grid:

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare tutti i servizi in esecuzione sul nodo: `service servermanager stop`

L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

3. Ripetere i passaggi 1 e 2 per ciascun nodo dell'host.

4. Se si dispone di un host Linux:

- a. Accedere al sistema operativo host.
- b. Arrestare il nodo: `storagegrid node stop`
- c. Arrestare il sistema operativo host.

5. Se il nodo è in esecuzione su una macchina virtuale VMware o si tratta di un nodo appliance, eseguire il comando shutdown: `shutdown -h now`

Eseguire questa operazione indipendentemente dal risultato del `service servermanager stop` comando.



Dopo aver inviato il `shutdown -h now` comando su un nodo appliance, è necessario spegnere e riaccendere l'appliance per riavviare il nodo.

Per l'appliance, questo comando spegne il controller, ma l'appliance è ancora accesa. Completare la fase successiva.

6. Se si sta spegnendo un nodo appliance, seguire la procedura relativa all'appliance.

SG6160

- a. Spegner il controller di storage SG6100-CN.
- b. Attendere lo spegnimento del LED di alimentazione blu sul controller di archiviazione SG6100-CN.

SGF6112

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6000

- a. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED di alimentazione blu si spenga.

SG5800

- a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
- c. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
- d. Spegner entrambi gli interruttori di alimentazione sul ripiano del controller e attendere lo spegnimento di tutti i LED sul ripiano del controller.

SG5700

- a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

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

- ["Appliance di storage SGF6112 e SG6160"](#)
- ["SG6000 appliance di storage"](#)
- ["SG5700 appliance di storage"](#)
- ["SG5800 appliance di storage"](#)
- ["Appliance per i servizi SG110 e SG1100"](#)
- ["Appliance per i servizi SG100 e SG1000"](#)

Spegnere e riaccendere tutti i nodi StorageGRID

Potrebbe essere necessario spegnere l'intero sistema StorageGRID, ad esempio, se si sta spostando un data center. Questi passaggi forniscono una panoramica di alto livello della sequenza consigliata per l'esecuzione di uno shutdown e di un startup controllati.

Quando spegni tutti i nodi in un sito o in una griglia, non puoi accedere agli oggetti acquisiti finché i nodi di archiviazione sono offline.

Arrestare i servizi e chiudere i nodi di rete

Prima di spegnere un sistema StorageGRID, è necessario arrestare tutti i servizi in esecuzione su ciascun nodo di rete e quindi arrestare tutte le macchine virtuali VMware, i motori di container e le appliance StorageGRID.

A proposito di questa attività

Interrompi prima i servizi sui nodi di amministrazione e sui nodi gateway, poi interrompi i servizi sui nodi di archiviazione.

Questo approccio consente di utilizzare l'Admin Node primario per monitorare lo stato degli altri nodi della griglia il più a lungo possibile.



Se un singolo host include più di un nodo di griglia, non spegnere l'host fino a quando non sono stati arrestati tutti i nodi su tale host. Se l'host include il nodo di amministrazione primario, arrestare l'host per ultimo.



Se necessario, è possibile ["Migrare i nodi da un host Linux a un altro"](#) eseguire la manutenzione dell'host senza influire sulla funzionalità o sulla disponibilità della rete.

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, ["consentire temporaneamente l'accesso"](#).
2. Impedire a tutte le applicazioni client di accedere alla griglia.
3. Accedi a ciascun nodo gateway:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

4. Arresta tutti i servizi in esecuzione sul nodo: `service servermanager stop`

L'arresto dei servizi può richiedere fino a 15 minuti e potrebbe essere necessario accedere al sistema in remoto per monitorare il processo di arresto.

5. Ripetere i due passaggi precedenti per arrestare i servizi su tutti i nodi storage e su quelli non primari.

È possibile interrompere i servizi su questi nodi in qualsiasi ordine.



Se si invia 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.

6. Per il nodo amministrativo primario, ripetere i passaggi per [accesso al nodo](#) e [interruzione di tutti i servizi sul nodo](#).
7. Per i nodi in esecuzione su host Linux:
 - a. Accedere al sistema operativo host.
 - b. Arrestare il nodo: `storagegrid node stop`
 - c. Arrestare il sistema operativo host.
8. Per i nodi in esecuzione su macchine virtuali VMware e per i nodi di storage dell'appliance, eseguire il comando shutdown: `shutdown -h now`

Eseguire questa operazione indipendentemente dal risultato del `service servermanager stop` comando.

Per l'appliance, questo comando arresta il controller di calcolo, ma l'appliance è ancora accesa. Completare la fase successiva.

9. Se si dispone di nodi appliance, seguire la procedura relativa all'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 il controller di storage SG6100-CN.
- b. Attendere lo spegnimento del LED di alimentazione blu sul controller di archiviazione SG6100-CN.

SGF6112

- a. Spegner l'apparecchio.
- b. Attendere che il LED di alimentazione blu si spenga.

SG6000

- a. Attendere che il LED verde cache Active (cache attiva) sul retro dei controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED di alimentazione blu si spenga.

SG5800

- a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Dalla home page di Gestione sistema SANtricity, selezionare **Visualizza operazioni in corso**.
- c. Confermare che tutte le operazioni sono state completate prima di passare alla fase successiva.
- d. Spegner entrambi gli interruttori di alimentazione sul ripiano del controller e attendere lo spegnimento di tutti i LED sul ripiano del controller.

SG5700

- a. Attendere che il LED verde cache Active (cache attiva) sul retro del controller dello storage si spenga.

Questo LED si accende quando i dati memorizzati nella cache devono essere scritti sui dischi. Prima di spegnere il prodotto, attendere che il LED si spenga.

- b. Spegner l'apparecchio e attendere che il LED e il display a sette segmenti si interrompano.

10. Se necessario, disconnettersi dalla shell dei comandi: `exit`

La griglia StorageGRID è stata chiusa.

11. Se hai consentito l'accesso SSH esterno, ["bloccare l'accesso"](#) una volta terminato lo spegnimento dei nodi.

Avviare i nodi della griglia

Se possibile, accendere i nodi della rete in questo ordine:

- Prima di tutto, alimentare i nodi di amministrazione.
- Alimentare per ultimo i nodi gateway.



Se un host include più nodi di griglia, questi tornano online automaticamente quando accendi l'host.

Fasi

1. Accendere gli host per il nodo di amministrazione primario e tutti i nodi di amministrazione non primari.



Non puoi accedere ai nodi di amministrazione finché i nodi di archiviazione non vengono riavviati.

2. Accendere gli host di tutti i nodi di storage.

È possibile accendere questi nodi in qualsiasi ordine.

3. Accendere gli host per tutti i nodi gateway.
4. Accedi a Grid Manager.
5. Selezionare **Nodi** e monitorare lo stato dei nodi della griglia. Verificare che non vi siano icone di avviso accanto ai nomi dei nodi.

Informazioni correlate

- ["Appliance di storage SGF6112 e SG6160"](#)
- ["Appliance per i servizi SG110 e SG1100"](#)
- ["Appliance per i servizi SG100 e SG1000"](#)
- ["SG6000 appliance di storage"](#)
- ["SG5800 appliance di storage"](#)
- ["SG5700 appliance di storage"](#)

Procedure di rimappamento delle porte

Rimuovere le rimappature delle porte sugli apparecchi StorageGRID

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta che è già stata configurata come porta mappata di un remap di porta, è necessario prima rimuovere il remap di porta esistente, altrimenti l'endpoint non sarà efficace. È necessario eseguire uno script su ciascun nodo Admin e nodo gateway che dispone di porte remapped in conflitto per rimuovere tutti i remap delle porte del nodo.

A proposito di questa attività

Questa procedura rimuove tutti i rimap delle porte. Se hai bisogno di conservare alcuni rimaps, contatta il supporto tecnico.

Per informazioni sulla configurazione degli endpoint di bilanciamento del carico, vedere ["Configurazione degli endpoint del bilanciamento del carico"](#).



Se il remap della porta fornisce l'accesso al client, riconfigurare il client in modo che utilizzi una porta diversa come endpoint del bilanciamento del carico per evitare la perdita di servizio. In caso contrario, la rimozione del mapping delle porte causerà la perdita dell'accesso al client e dovrebbe essere pianificata in modo appropriato.



Questa procedura non funziona per un sistema StorageGRID implementato come container su host bare metal. Vedere le istruzioni per ["rimozione dei rimaps delle porte sugli host bare metal"](#).

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, ["consentire temporaneamente l'accesso"](#).
2. Accedere al nodo.
 - a. Immettere il seguente comando: `ssh -p 8022 admin@node_IP`

La porta 8022 è la porta SSH del sistema operativo di base, mentre la porta 22 è la porta SSH del motore dei container che esegue StorageGRID.
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

3. Eseguire lo script seguente: `remove-port-remap.sh`
4. Riavviare il nodo: `reboot`
5. Disconnettersi dalla shell dei comandi: `exit`
6. Ripetere questi passaggi su ogni nodo Admin e nodo gateway con porte remapped in conflitto.
7. Se hai consentito l'accesso SSH esterno, ["bloccare l'accesso"](#) una volta terminata la rimozione delle rimappature delle porte.

Informazioni correlate

- ["Porte utilizzate per le comunicazioni esterne"](#)

Rimuovere le rimappature delle porte di StorageGRID sugli host bare metal

Se si desidera configurare un endpoint per il servizio Load Balancer e si desidera utilizzare una porta che è già stata configurata come porta mappata di un remap di porta, è necessario prima rimuovere il remap di porta esistente, altrimenti l'endpoint non sarà efficace.

A proposito di questa attività

Se si esegue StorageGRID su host bare metal, seguire questa procedura invece della procedura generale per rimuovere i rimaps delle porte. È necessario modificare il file di configurazione del nodo per ogni nodo Admin e nodo gateway che ha porte remapped in conflitto per rimuovere tutti i remap delle porte del nodo e riavviare il nodo.



Questa procedura rimuove tutti i rimap delle porte. Se hai bisogno di conservare alcuni rimaps, contatta il supporto tecnico.

Per informazioni sulla configurazione degli endpoint del bilanciamento del carico, vedere le istruzioni per l'amministrazione di StorageGRID.



Questa procedura può causare una perdita temporanea del servizio quando i nodi vengono riavviati.

Fasi

1. Accedere all'host che supporta il nodo. Accedere come root o con un account che dispone dell'autorizzazione sudo.
2. Eseguire il seguente comando per disattivare temporaneamente il nodo: `sudo storagegrid node stop node-name`
3. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo per il nodo.

Il file di configurazione del nodo è disponibile all'indirizzo `/etc/storagegrid/nodes/node-name.conf`.

4. Individuare la sezione del file di configurazione del nodo che contiene i rimap delle porte.

Vedere le ultime due righe nell'esempio seguente.

```

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_ESL = 10.0.0.0/8, 172.19.0.0/16, 172.21.0.0/16
ADMIN_NETWORK_GATEWAY = 10.224.0.1
ADMIN_NETWORK_IP = 10.224.5.140
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_MTU = 1400
ADMIN_NETWORK_TARGET = eth1
ADMIN_NETWORK_TARGET_TYPE = DedicatedInterface
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 = DedicatedInterface
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 = DedicatedInterface
NODE_TYPE = VM_API_Gateway
PORT_REMAP = client/tcp/8082/443
PORT_REMAP_INBOUND = client/tcp/8082/443

```

5. Modificare LE voci PORT_REMAP e PORT_REMAP_INBOUND per rimuovere i rimap delle porte.

```

PORT_REMAP =
PORT_REMAP_INBOUND =

```

6. Esegui il seguente comando per validare le tue modifiche al file di configurazione del nodo per il nodo:
`sudo storagegrid node validate node-name`

Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

7. Eseguire il seguente comando per riavviare il nodo senza remaps delle porte: `sudo storagegrid node start node-name`
8. Accedere al nodo come amministratore utilizzando la password indicata nel `Passwords.txt` file.
9. Verificare che i servizi vengano avviati correttamente.
 - a. Visualizzare un elenco degli stati di tutti i servizi sul server: `sudo storagegrid-status`

Lo stato viene aggiornato automaticamente.

- b. Attendere che tutti i servizi abbiano lo stato di in esecuzione o verificato.
 - c. Uscire dalla schermata di stato: `Ctrl+C`
10. Ripetere questi passaggi su ogni nodo Admin e nodo gateway con porte remapped in conflitto.

Procedure di Server Manager

Visualizza lo stato e la versione di StorageGRID Server Manager

Per ciascun nodo Grid, è possibile visualizzare lo stato e la versione correnti di Server Manager in esecuzione su tale nodo Grid. È inoltre possibile ottenere lo stato corrente di tutti i servizi in esecuzione su quel nodo della griglia.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Visualizzare lo stato corrente di Server Manager in esecuzione sul nodo della griglia: **`service servermanager status`**

Viene riportato lo stato corrente di Server Manager in esecuzione sul nodo grid (in esecuzione o meno). Se lo stato di Server Manager è `running`, viene visualizzata l'ora di esecuzione dall'ultimo avvio. Ad esempio:

```
servermanager running for 1d, 13h, 0m, 30s
```

3. Visualizzare la versione corrente di Server Manager in esecuzione su un nodo griglia: **`service servermanager version`**

Viene visualizzata la versione corrente. Ad esempio:

```
11.1.0-20180425.1905.39c9493
```

4. Disconnettersi dalla shell dei comandi: **`exit`**

Visualizza lo stato attuale di tutti i servizi StorageGRID

È possibile visualizzare lo stato corrente di tutti i servizi in esecuzione su un nodo Grid in

qualsiasi momento.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Visualizzare lo stato di tutti i servizi in esecuzione sul nodo griglia: `storagegrid-status`

Ad esempio, l'output per il nodo di amministrazione primario mostra lo stato corrente dei servizi AMS, CMN e NMS in esecuzione. Questo output viene aggiornato immediatamente se lo stato di un servizio cambia.

```
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
attrDownSamp1         11.1.0     Running
attrDownSamp2         11.1.0     Running
node exporter          0.13.0+ds  Running
```

3. Tornare alla riga di comando, premere **Ctrl+C**.
4. Facoltativamente, visualizzare un report statico per tutti i servizi in esecuzione sul nodo griglia:
`/usr/local/servermanager/reader.rb`

Questo report include le stesse informazioni del report continuamente aggiornato, ma non viene aggiornato se lo stato di un servizio cambia.

5. Disconnettersi dalla shell dei comandi: `exit`

Avvia StorageGRID Server Manager e tutti i servizi

Potrebbe essere necessario avviare Server Manager, che avvia anche tutti i servizi sul nodo Grid.

Prima di iniziare

Si dispone del `Passwords.txt` file.

A proposito di questa attività

L'avvio di Server Manager su un nodo grid in cui è già in esecuzione comporta il riavvio di Server Manager e di tutti i servizi sul nodo grid.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.Quando si è collegati come root, il prompt cambia da `$` a `#`.
2. Avvio di Server Manager: `service servermanager start`
3. Disconnettersi dalla shell dei comandi: `exit`

Riavviare StorageGRID Server Manager e tutti i servizi

Potrebbe essere necessario riavviare Server Manager e tutti i servizi in esecuzione su un nodo della griglia.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.Quando si è collegati come root, il prompt cambia da `$` a `#`.
2. Riavviare Server Manager e tutti i servizi sul nodo griglia: `service servermanager restart`

Server Manager e tutti i servizi sul nodo grid vengono arrestati e quindi riavviati.



L'utilizzo del `restart` comando è identico all'utilizzo del `stop` comando seguito dal comando `start`.

3. Disconnettersi dalla shell dei comandi: `exit`

Arresta StorageGRID Server Manager e tutti i servizi

Server Manager è progettato per essere eseguito in qualsiasi momento, ma potrebbe essere necessario interrompere Server Manager e tutti i servizi in esecuzione su un nodo grid.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare Server Manager e tutti i servizi in esecuzione sul nodo griglia: `service servermanager stop`

Server Manager e tutti i servizi in esecuzione sul nodo grid vengono terminati senza problemi. L'arresto dei servizi può richiedere fino a 15 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Visualizza lo stato attuale di un servizio StorageGRID

È possibile visualizzare lo stato corrente di un servizio in esecuzione su un nodo della griglia in qualsiasi momento.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

2. Visualizzare lo stato corrente di un servizio in esecuzione su un nodo grid: `service servicename status`
lo stato corrente del servizio richiesto in esecuzione sul nodo grid viene segnalato (in esecuzione o meno).
Ad esempio:

```
cmn running for 1d, 14h, 21m, 2s
```

3. Disconnettersi dalla shell dei comandi: `exit`

Interrompi un servizio StorageGRID

Alcune procedure di manutenzione richiedono l'interruzione di un singolo servizio mantenendo in esecuzione altri servizi sul nodo grid. Interrompere i singoli servizi solo quando richiesto da una procedura di manutenzione.

Prima di iniziare

Si dispone del `Passwords.txt` file.

A proposito di questa attività

Quando si utilizza questa procedura per "arrestare amministrativamente" un servizio, Server Manager non riavvia automaticamente il servizio. È necessario avviare il servizio singolo manualmente o riavviare Server Manager.

Se è necessario arrestare il servizio LDR su un nodo di storage, tenere presente che potrebbe essere necessario un po' di tempo per arrestare il servizio in presenza di connessioni attive.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

2. Interruzione di un servizio individuale: `service servicename stop`

Ad esempio:

```
service ldr stop
```



L'interruzione dei servizi può richiedere fino a 11 minuti.

3. Disconnettersi dalla shell dei comandi: `exit`

Informazioni correlate

["Forzare l'interruzione del servizio"](#)

Forzare la terminazione di un servizio StorageGRID

Se è necessario arrestare immediatamente un servizio, è possibile utilizzare il `force-stop` comando .

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.Quando si è collegati come root, il prompt cambia da `$` a `#`.
2. Forzare manualmente l'interruzione del servizio: `service servicename force-stop`

Ad esempio:

```
service ldr force-stop
```

Il sistema attende 30 secondi prima di terminare il servizio.

3. Disconnettersi dalla shell dei comandi: `exit`

Avviare o riavviare un servizio StorageGRID

Potrebbe essere necessario avviare un servizio che è stato arrestato oppure arrestare e riavviare un servizio.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

2. Decidere quale comando emettere, in base al fatto che il servizio sia attualmente in esecuzione o interrotto.

- Se il servizio è attualmente interrotto, utilizzare il `start` comando per avviare il servizio manualmente:
`service servicename start`

Ad esempio:

```
service ldr start
```

- Se il servizio è attualmente in esecuzione, utilizzare il `restart` comando per arrestare e riavviare il servizio: `service servicename restart`

Ad esempio:

```
service ldr restart
```

+



L'utilizzo del `restart` comando è identico all'utilizzo del `stop` comando seguito dal comando `start`. È possibile risolvere il problema `restart` anche se il servizio è attualmente arrestato.

3. Disconnettersi dalla shell dei comandi: `exit`

Utilizzare un file DoNotStart di StorageGRID

Se si eseguono diverse procedure di manutenzione o configurazione sotto la direzione del supporto tecnico, potrebbe essere richiesto di utilizzare un file DoNotStart per impedire l'avvio dei servizi all'avvio o al riavvio di Server Manager.



Aggiungere o rimuovere un file DoNotStart solo se richiesto dal supporto tecnico.

Per impedire l'avvio di un servizio, inserire un file DoNotStart nella directory del servizio che si desidera impedire l'avvio. All'avvio, Server Manager cerca il file DoNotStart. Se il file è presente, non è possibile avviare il servizio (e i servizi da esso dipendenti). Quando il file DoNotStart viene rimosso, il servizio precedentemente interrotto viene avviato al successivo avvio o riavvio di Server Manager. I servizi non vengono avviati automaticamente quando il file DoNotStart viene rimosso.

Il modo più efficiente per impedire il riavvio di tutti i servizi consiste nell'impedire l'avvio del servizio NTP. Tutti i servizi dipendono dal servizio NTP e non possono essere eseguiti se il servizio NTP non è in esecuzione.

Aggiungere il file DoNotStart per il servizio

È possibile impedire l'avvio di un singolo servizio aggiungendo un file DoNotStart alla directory del servizio su un nodo Grid.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Aggiungere un file `DoNotStart`: `touch /etc/sv/service/DoNotStart`

dove `service` è il nome del servizio da impedire l'avvio. Ad esempio,

```
touch /etc/sv/ldr/DoNotStart
```

Viene creato un file `DoNotStart`. Non è necessario alcun contenuto di file.

Al riavvio di Server Manager o del nodo grid, Server Manager viene riavviato, ma il servizio non viene attivato.

3. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere il file `DoNotStart` per l'assistenza

Quando si rimuove un file `DoNotStart` che impedisce l'avvio di un servizio, è necessario avviarlo.

Prima di iniziare

Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo Grid:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Rimuovere il file `DoNotStart` dalla directory di servizio: `rm /etc/sv/service/DoNotStart`

dove `service` è il nome del servizio. Ad esempio,

```
rm /etc/sv/ldr/DoNotStart
```

3. Avviare il servizio: `service servicename start`
4. Disconnettersi dalla shell dei comandi: `exit`

Risoluzione dei problemi di Server Manager in StorageGRID

Se si verifica un problema durante l'utilizzo di Server Manager, controllare il file di log.

I messaggi di errore relativi a Server Manager vengono acquisiti nel file di registro di Server Manager, che si trova in: `/var/local/log/servermanager.log`

Controllare questo file per i messaggi di errore relativi agli errori. Se necessario, inoltrare il problema al supporto tecnico. Potrebbe essere richiesto di inoltrare i file di registro al supporto tecnico.

Servizio con stato di errore

Se si rileva che un servizio è entrato in uno stato di errore, tentare di riavviare il servizio.

Prima di iniziare

Si dispone del `Passwords.txt` file.

A proposito di questa attività

Server Manager monitora i servizi e riavvia quelli che si sono arrestati inaspettatamente. Se un servizio non riesce, Server Manager tenta di riavviarlo. Se si verificano tre tentativi non riusciti di avvio di un servizio entro cinque minuti, il servizio entra in uno stato di errore. Server Manager non tenta un altro riavvio.

Fasi

1. Accedere al nodo Grid:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Confermare lo stato di errore del servizio: `service servicename status`

Ad esempio:

```
service ldr status
```

Se il servizio è in stato di errore, viene visualizzato il seguente messaggio: `servicename in error state`. Ad esempio:

```
ldr in error state
```



Se lo stato del servizio è disabled, vedere le istruzioni di ["Rimozione di un file DoNotStart per un servizio"](#).

3. Tentare di rimuovere lo stato di errore riavviando il servizio: `service servicename restart`

Se il servizio non viene riavviato, contattare il supporto tecnico.

4. Disconnettersi dalla shell dei comandi: `exit`

Procedure di rete

Aggiorna le sottoreti per StorageGRID Grid Network

StorageGRID mantiene un elenco delle subnet di rete utilizzate per comunicare tra i nodi della griglia sulla rete (eth0). Queste voci includono le subnet utilizzate per la rete griglia da ciascun sito nel sistema StorageGRID, nonché le subnet utilizzate per NTP, DNS, LDAP o altri server esterni a cui si accede tramite il gateway della rete griglia. Quando si aggiungono nodi griglia o un nuovo sito in un'espansione, potrebbe essere necessario aggiornare o aggiungere sottoreti alla rete Grid.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi di rete, in notazione CIDR, delle subnet che si desidera configurare.

A proposito di questa attività

Se si sta eseguendo un'attività di espansione che include l'aggiunta di una nuova subnet, è necessario aggiungere una nuova subnet all'elenco delle subnet Grid Network prima di avviare la procedura di espansione. In caso contrario, sarà necessario annullare l'espansione, aggiungere la nuova subnet e riavviare l'espansione.

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

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



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

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

Aggiungere una subnet

Fasi

1. Selezionare **Manutenzione > Rete > Rete di rete**.
2. Selezionare **Aggiungi un'altra subnet** per aggiungere una nuova subnet nella notazione CIDR.

Ad esempio, immettere 10.96.104.0/22.

3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.
 - b. Inserisci 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.

Modificare una subnet

Fasi

1. Selezionare **Manutenzione > Rete > Rete di rete**.
2. Selezionare la subnet che si desidera modificare e apportare le modifiche necessarie.
3. Inserire la passphrase di provisioning e selezionare **Save** (Salva).
4. Selezionare **Sì** nella finestra di dialogo di conferma.
5. Attendi che le modifiche vengano applicate, quindi scarica un nuovo pacchetto di ripristino.
 - a. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.
 - b. Inserisci la **passphrase di provisioning**.

Eliminare una subnet

Fasi

1. Selezionare **Manutenzione > Rete > Rete di rete**.
2. Seleziona l'icona di eliminazione  accanto alla sottorete.
3. Inserire la passphrase di provisioning e selezionare **Save** (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. Inserisci la **passphrase di provisioning**.

Configurare gli indirizzi IP

Linee guida sugli indirizzi IP di StorageGRID

È possibile eseguire la configurazione di rete configurando gli indirizzi IP per i nodi della griglia utilizzando lo strumento Change IP (Modifica IP).

È necessario utilizzare lo strumento Change IP per apportare la maggior parte delle modifiche alla configurazione di rete impostata inizialmente durante l'implementazione della griglia. Le modifiche manuali che utilizzano i comandi e i file di rete Linux standard potrebbero non propagarsi a tutti i servizi StorageGRID e non persistere tra gli aggiornamenti, i riavvii o le procedure di ripristino dei nodi.



La procedura di modifica dell'IP può essere una procedura di interruzione. Alcune parti della griglia potrebbero non essere disponibili fino a quando non viene applicata la nuova configurazione.



Se si apportano modifiche solo all'elenco subnet di rete griglia, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Change IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si stanno eseguendo contemporaneamente modifiche al routing Grid Network e altre modifiche di rete.



Se si desidera modificare l'indirizzo IP della rete griglia per tutti i nodi della griglia, utilizzare ["procedura speciale per le modifiche a livello di griglia"](#).

Interfacce Ethernet

L'indirizzo IP assegnato a eth0 è sempre l'indirizzo IP Grid Network del nodo Grid. L'indirizzo IP assegnato a eth1 è sempre l'indirizzo IP Admin Network del nodo della griglia. L'indirizzo IP assegnato a eth2 è sempre l'indirizzo IP della rete client del nodo della griglia.

Si noti che su alcune piattaforme, come le appliance StorageGRID, eth0, eth1 ed eth2 potrebbero essere interfacce aggregate composte da bridge o legami subordinati di interfacce fisiche o VLAN. Su queste piattaforme, la scheda **SSM > Resources** potrebbe visualizzare l'indirizzo IP Grid, Admin e Client Network assegnato ad altre interfacce oltre a eth0, eth1 o eth2.

DHCP

È possibile configurare DHCP solo durante la fase di implementazione. Impossibile impostare DHCP durante la configurazione. Se si desidera modificare gli indirizzi IP, le subnet mask e i gateway predefiniti per un nodo griglia, è necessario utilizzare le procedure di modifica dell'indirizzo IP. Utilizzando lo strumento Change IP, gli indirizzi DHCP diventano statici.

Gruppi ad alta disponibilità (ha)

- Se un'interfaccia di rete client è contenuta in un gruppo ha, non è possibile modificare l'indirizzo IP di rete client per tale interfaccia con un indirizzo esterno alla subnet configurata per il gruppo ha.
- Non è possibile modificare l'indirizzo IP della rete client con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo ha configurato sull'interfaccia di rete client.
- Se un'interfaccia di rete Grid è contenuta in un gruppo ha, non è possibile modificare l'indirizzo IP della rete Grid per tale interfaccia con un indirizzo esterno alla subnet configurata per il gruppo ha.
- Non è possibile modificare l'indirizzo IP Grid Network con il valore di un indirizzo IP virtuale esistente assegnato a un gruppo ha configurato sull'interfaccia Grid Network.

Modificare la configurazione di rete del nodo in StorageGRID

Puoi modificare la configurazione di rete di uno o più nodi utilizzando lo strumento Cambia IP. Puoi modificare la configurazione della Grid Network oppure aggiungere, modificare o rimuovere le Admin o Client Network. Puoi anche modificare le impostazioni IP LAN per un nodo appliance BMC.

Prima di iniziare

Si dispone del `Passwords.txt` file.

A proposito di questa attività

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. Vedi StorageGRID ["istruzioni di installazione"](#) per il tuo sistema operativo Linux.

Appliance: sulle appliance StorageGRID, se il client o la rete amministrativa non sono stati configurati nel programma di installazione dell'appliance StorageGRID durante l'installazione iniziale, la rete non può essere aggiunta utilizzando solo il tool Cambia IP. Innanzitutto, è necessario ["impostare l'apparecchio in modalità di manutenzione"](#) configurare i collegamenti, riportare il dispositivo alla modalità operativa normale, quindi utilizzare lo strumento Modifica IP per modificare la configurazione di rete. Consultare la ["procedura per la configurazione dei collegamenti di rete"](#).

È possibile modificare l'indirizzo IP, la subnet mask, il gateway o il valore MTU per uno o più nodi su qualsiasi rete.

È inoltre possibile aggiungere o rimuovere un nodo da una rete client o da una rete amministrativa:

- È possibile aggiungere un nodo a una rete client o a una rete amministrativa aggiungendo un indirizzo IP/subnet mask su tale rete al nodo.
- È possibile rimuovere un nodo da una rete client o da una rete amministrativa eliminando l'indirizzo IP/subnet mask del nodo sulla rete.

I nodi non possono essere rimossi dalla Grid Network.



Non è consentito lo swap degli indirizzi IP. Se è necessario scambiare indirizzi IP tra nodi di rete, è necessario utilizzare un indirizzo IP intermedio temporaneo.



Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID e stai cambiando l'indirizzo IP di un Admin Node, tieni presente che qualsiasi relying party trust configurato utilizzando l'indirizzo IP dell'Admin Node (invece del suo fully qualified domain name, come consigliato) diventerà non valido. Non potrai più accedere al nodo. Subito dopo aver cambiato l'indirizzo IP, devi aggiornare o riconfigurare il relying party trust del nodo in Active Directory Federation Services (AD FS) con il nuovo indirizzo IP. Consulta le istruzioni per configurare l'SSO usando "OIDC" o "SAML".



Le modifiche apportate alla rete utilizzando lo strumento Cambia IP vengono propagate al firmware del programma di installazione delle appliance StorageGRID. In questo modo, se il software StorageGRID viene reinstallato su un'appliance o se un'appliance viene messa in modalità di manutenzione, la configurazione di rete sarà corretta.

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, ["consentire temporaneamente l'accesso"](#).
2. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

3. Avviare lo strumento Change IP inserendo il seguente comando: `change-ip`
4. Inserire la passphrase di provisioning quando richiesto.

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: █

```

5. Se si desidera, selezionare **1** per scegliere i nodi da aggiornare. Quindi selezionare una delle seguenti opzioni:

- **1:** Nodo singolo — selezionare per nome
- **2:** Nodo singolo — selezionare per sito, quindi per nome
- **3:** Nodo singolo — selezionare in base all'IP corrente
- **4:** Tutti i nodi di un sito
- **5:** Tutti i nodi della griglia

Nota: se si desidera aggiornare tutti i nodi, lasciare selezionato "tutti".

Una volta effettuata la selezione, viene visualizzato il menu principale, con il campo **Selected Nodes** (nodi selezionati) aggiornato per riflettere la scelta. Tutte le azioni successive vengono eseguite solo sui nodi visualizzati.

6. Nel menu principale, selezionare l'opzione **2** per modificare le informazioni relative a IP/mask, gateway e MTU per i nodi selezionati.

a. Selezionare la rete in cui si desidera apportare le modifiche:

- **1:** Rete di rete
- **2:** Rete amministrativa
- **3:** Rete client
- **4:** Tutte le reti

Dopo aver effettuato la selezione, il prompt mostra il nome del nodo, il nome della rete (Grid, Admin o Client), il tipo di dati (IP/mask, gateway o MTU) e il valore corrente.

Se si modificano l'indirizzo IP, la lunghezza del prefisso, il gateway o la MTU di un'interfaccia configurata con DHCP, l'interfaccia diventa statica. Quando si sceglie di modificare un'interfaccia configurata da DHCP, viene visualizzato un avviso per informare l'utente che l'interfaccia passerà a static (statica).

Le interfacce configurate come `fixed` non possono essere modificate.

- b. Per impostare un nuovo valore, immetterlo nel formato indicato per il valore corrente.
- c. Per lasciare invariato il valore corrente, premere **Invio**.

- d. Se il tipo di dati è `IP/mask`, è possibile eliminare la rete Admin o Client dal nodo immettendo `d` o `0,0,0,0/0`.
- e. Dopo aver modificato tutti i nodi che si desidera modificare, immettere `q` per tornare al menu principale.

Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

7. Per rivedere le modifiche, selezionare una delle seguenti opzioni:

- **5:** Mostra le modifiche nell'output isolato per mostrare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'output di esempio:

```

=====
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
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 mostrare aggiunte ed eliminazioni utilizzando la formattazione `strikehrough`. La corretta visualizzazione dipende dal client terminale che supporta le sequenze di escape VT100 necessarie.

8. Selezionare l'opzione **7** per convalidare tutte le modifiche.

Questa convalida garantisce che le regole per le reti Grid, Admin e Client, come ad esempio l'utilizzo di sottoreti sovrapposte, non vengano violate.

In questo esempio, la convalida ha restituito errori.

```

Validating new networking configuration... FAILED.

DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.
DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)

You must correct these errors before you can apply any changes.
Checking for Grid Network IP address swaps... PASSED.

Press Enter to continue

```

In questo esempio, la convalida è stata superata.

```

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

Press Enter to continue

```

9. Dopo il superamento della convalida, scegliere una delle seguenti opzioni:

- **8:** Salva le modifiche non applicate.

Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

- **10:** Applicare la nuova configurazione di rete.

10. Se è stata selezionata l'opzione **10**, scegliere una delle seguenti opzioni:

- **Apply:** Applica le modifiche immediatamente e riavvia automaticamente ogni nodo, se necessario.

Se la nuova configurazione di rete non richiede modifiche fisiche, selezionare **Apply** (Applica) per applicare le modifiche immediatamente. I nodi verranno riavviati automaticamente, se necessario. Verranno visualizzati i nodi che devono essere riavviati.

- **Fase:** Applicare le modifiche al successivo riavvio manuale dei nodi.

Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale per il funzionamento della nuova configurazione di rete, utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le necessarie modifiche fisiche di rete e riavviare i nodi interessati. Se si seleziona **Apply** (Applica) senza apportare prima queste modifiche alla rete, le modifiche non vengono eseguite correttamente.



Se si utilizza l'opzione **stage**, è necessario riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

- **CANCEL:** Non apportare modifiche alla rete in questo momento.

Se non si è a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, è possibile posticipare le modifiche per ridurre al minimo l'impatto sull'utente. Selezionando **CANCEL** si torna al menu principale e si conservano le modifiche in modo da poterle applicare in un secondo momento.

Quando si seleziona **Apply** o **Stage**, viene generato un nuovo file di configurazione di rete, viene eseguito il provisioning e i nodi vengono aggiornati con nuove informazioni di lavoro.

Durante il provisioning, l'output visualizza lo stato man mano che vengono applicati gli aggiornamenti.

Generating new grid networking description file...

Running provisioning...

Updating grid network configuration on Name

Dopo aver applicato o organizzato le modifiche, viene generato un nuovo pacchetto di ripristino come risultato della modifica alla configurazione della griglia.

11. Se si seleziona **fase**, seguire questi passaggi al termine del provisioning:

a. Apportare le modifiche di rete fisiche o virtuali richieste.

Modifiche fisiche alla rete: Apportare le modifiche fisiche necessarie alla rete, spegnendo il nodo in modo sicuro, se necessario.

Linux: Se si aggiunge il nodo a una rete di amministrazione o a una rete client per la prima volta, assicurarsi di aver aggiunto l'interfaccia come descritto in "[Linux: Aggiunta di interfacce al nodo esistente](#)".

a. Riavviare i nodi interessati.

12. Selezionare **0** per uscire dallo strumento Change IP una volta completate le modifiche.

13. Scarica un nuovo pacchetto di ripristino da Grid Manager.

a. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.

b. Inserire la passphrase di provisioning.

14. Se hai consentito l'accesso SSH esterno, "[bloccare l'accesso](#)" una volta terminata la modifica della configurazione della rete del nodo.

Modifica temporanea della velocità PDU LACP

Per eseguire operazioni di manutenzione sui componenti di rete installati nel dispositivo, ad esempio l'aggiornamento del firmware della scheda di rete, è possibile verificare che l'impostazione corrente della velocità PDU LACP soddisfi i requisiti di temporizzazione della comunicazione della scheda di rete. Se necessario, è possibile alternare in modo non persistente la velocità della PDU LACP tra veloce (attesa di 1 secondo) e lenta (attesa di 30 secondi).



Per apportare modifiche permanenti alla velocità PDU LACP, vedere "[Configurare i collegamenti di rete](#)".

Prima di iniziare

- Il nodo di amministrazione è installato e funzionante.
- Si dispone del `Passwords.txt` file.

Fasi

1. Accedere al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Per verificare l'impostazione corrente della velocità LACP PDU, immettere il seguente comando:

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh'
```

3. Per modificare temporaneamente la velocità PDU LACP, immettere il seguente comando:

```
run-each-node --parallel --port 8022 '/usr/sbin/set-lacp-rate.sh <speed>'
```

Dove `<speed>` È `fast` o `slow`.

Al successivo riavvio dell'appliance, la velocità PDU LACP tornerà all'impostazione precedente.

Modifica le impostazioni IP LAN del nodo BMC dell'appliance

Puoi modificare le impostazioni IP LAN per un nodo appliance BMC.

1. In Grid Manager vai su **Nodi > nodo griglia > Impostazioni BMC**.
2. Nella sezione delle impostazioni IP LAN, seleziona un tipo di assegnazione IP tra **Statico** o **DHCP**.
3. Inserisci l'indirizzo MAC, l'indirizzo IPv4 (CIDR) e il gateway predefinito per il BMC.
4. Selezionare **Salva**.

Puoi anche modificare o visualizzare le impostazioni IP LAN del BMC usando l' `PUT /bmc-configuration/root-password` o ``GET /bmc-configuration/root-password`` API.

Aggiungere o modificare gli elenchi di sottoreti sulla rete di amministrazione in StorageGRID

È possibile aggiungere, eliminare o modificare le subnet nell'elenco subnet di rete amministrativa di uno o più nodi.

Prima di iniziare

- Si dispone del `Passwords.txt` file.

È possibile aggiungere, eliminare o modificare le subnet in tutti i nodi dell'elenco subnet di rete amministrativa.

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

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



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

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

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, ["consentire temporaneamente l'accesso"](#).
2. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

3. Avviare lo strumento Change IP inserendo il seguente comando: `change-ip`
4. Inserire la passphrase di provisioning quando richiesto.

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: █

```

5. Facoltativamente, limitare le reti/nodi su cui vengono eseguite le operazioni. Scegliere una delle seguenti opzioni:
 - Selezionare i nodi da modificare scegliendo **1**, se si desidera filtrare su nodi specifici su cui eseguire l'operazione. Selezionare una delle seguenti opzioni:
 - **1**: Nodo singolo (selezionare per nome)
 - **2**: Nodo singolo (selezionare per sito, quindi per nome)
 - **3**: Nodo singolo (selezionato in base all'IP corrente)
 - **4**: Tutti i nodi di un sito
 - **5**: Tutti i nodi della griglia
 - **0**: Torna indietro
 - Consenti a "tutto" di rimanere selezionato. Una volta effettuata la selezione, viene visualizzata la schermata del menu principale. Il campo Selected Nodes (nodi selezionati) riflette la nuova selezione e ora tutte le operazioni selezionate verranno eseguite solo su questo elemento.
6. Nel menu principale, selezionare l'opzione per modificare le subnet per la rete amministrativa (opzione **3**).
7. Scegliere una delle seguenti opzioni:
 - Per aggiungere una subnet, immettere il seguente comando: `add CIDR`
 - Per eliminare una subnet, immettere il comando: `del CIDR`
 - Per impostare l'elenco delle subnet, immettere il seguente 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 digitazione richiesta utilizzando la "freccia su" per richiamare i valori digitati in precedenza al prompt di immissione corrente, quindi modificarli se necessario.

L'esempio riportato di seguito mostra l'aggiunta di subnet all'elenco subnet di rete amministrativa:

```

Editing: Admin Network Subnet List for node DK-10-224-5-20-G1

Press <enter> to use the list as shown
Use up arrow to recall a previously typed value, which you can then edit
Use 'add <CIDR> [, <CIDR>]' to add subnets <CIDR> [, <CIDR>] to the list
Use 'del <CIDR> [, <CIDR>]' to delete subnets <CIDR> [, <CIDR>] from the list
Use 'set <CIDR> [, <CIDR>]' to set the list to the given list
Use q to complete the editing session early and return to the previous menu

DK-10-224-5-20-G1
 10.0.0.0/8
 172.19.0.0/16
 172.21.0.0/16
 172.20.0.0/16

[add/del/set/quit <CIDR>, ...]: add 172.14.0.0/16, 172.15.0.0/16

```

8. Una volta pronti, inserire **q** per tornare alla schermata del menu principale. Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.



Se nel passaggio 3 è stata selezionata una delle modalità di selezione dei nodi "tutti", premere **Invio** (senza **q**) per passare al nodo successivo nell'elenco.

9. Scegliere una delle seguenti opzioni:

- Selezionare l'opzione **5** per visualizzare le modifiche nell'output isolato in modo da visualizzare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio riportato di seguito:

```

=====
Site: Data Center 1
=====
DC1-ADM1-105-154 Admin Subnets
                                add 172.17.0.0/16
                                del 172.16.0.0/16
                                [ 172.14.0.0/16 ]
                                [ 172.15.0.0/16 ]
                                [ 172.17.0.0/16 ]
                                [ 172.19.0.0/16 ]
                                [ 172.20.0.0/16 ]
                                [ 172.21.0.0/16 ]
Press Enter to continue

```

- Selezionare l'opzione **6** per visualizzare le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni). **Nota:** alcuni emulatori di terminali potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough.

Quando si tenta di modificare l'elenco delle subnet, viene visualizzato il seguente messaggio:

CAUTION: The Admin Network subnet list on the node might contain /32 subnets derived from automatically applied routes that aren't persistent. Host routes (/32 subnets) are applied automatically if the IP addresses provided for external services such as NTP or DNS aren't reachable using default StorageGRID routing, but are reachable using a different interface and gateway. Making and applying changes to the subnet list will make all automatically applied subnets persistent. If you don't want that to happen, delete the unwanted subnets before applying changes. If you know that all /32 subnets in the list were added intentionally, you can ignore this caution.

Se non sono state assegnate in modo specifico le subnet NTP e DNS dei server a una rete, StorageGRID crea automaticamente un percorso host (/32) per la connessione. Se, ad esempio, si preferisce un percorso /16 o /24 per la connessione in uscita a un server DNS o NTP, eliminare il percorso /32 creato automaticamente e aggiungere i percorsi desiderati. Se non si elimina la route host creata automaticamente, questa verrà persistente dopo l'applicazione di eventuali modifiche all'elenco delle subnet.



Sebbene sia possibile utilizzare questi percorsi host rilevati automaticamente, in generale è necessario configurare manualmente i percorsi DNS e NTP per garantire la connettività.

10. Selezionare l'opzione **7** per convalidare tutte le modifiche in fasi.

Questa convalida garantisce il rispetto delle regole per le reti Grid, Admin e Client, ad esempio l'utilizzo di sottoreti sovrapposte.

11. Se si desidera, selezionare l'opzione **8** per salvare tutte le modifiche in più fasi e tornare in seguito per continuare ad apportare le modifiche.

Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

12. Effettuare una delle seguenti operazioni:

- Selezionare l'opzione **9** se si desidera annullare tutte le modifiche senza salvare o applicare la nuova configurazione di rete.
- Selezionare l'opzione **10** se si desidera applicare le modifiche e fornire la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato quando vengono applicati gli aggiornamenti, come mostrato nell'output di esempio seguente:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

13. Scarica un nuovo pacchetto di ripristino da Grid Manager.

- a. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.

b. Inserire la passphrase di provisioning.

14. Se hai consentito l'accesso SSH esterno, "[bloccare l'accesso](#)" una volta terminato di aggiungere o modificare gli elenchi di subnet.

Aggiungi o modifica gli elenchi di subnet sulla Grid Network in StorageGRID

È possibile utilizzare lo strumento Change IP per aggiungere o modificare le subnet nella rete griglia.

Prima di iniziare

- Si dispone del `Passwords.txt` file.

È possibile aggiungere, eliminare o modificare le subnet nell'elenco subnet di rete griglia. Le modifiche influiscono sul routing su tutti i nodi della griglia.



Se si apportano modifiche solo all'elenco subnet di rete griglia, utilizzare Grid Manager per aggiungere o modificare la configurazione di rete. In caso contrario, utilizzare lo strumento Change IP se Grid Manager non è accessibile a causa di un problema di configurazione di rete o se si stanno eseguendo contemporaneamente modifiche al routing Grid Network e altre modifiche di rete.

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

- 192.168.130.101
- 192.168.130.121
- 192.168.131.101
- 192.168.131.121
- 192.168.130.102
- 192.168.130.122
- 192.168.131.102
- 192.168.131.122
- 198.51.100.2
- 198.51.100.4



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

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

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, "[consentire](#)

temporaneamente l'accesso" .

2. Accedere al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

3. Avviare lo strumento Change IP inserendo il seguente comando: `change-ip`

4. Inserire la passphrase di provisioning quando richiesto.

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: █
```

5. Nel menu principale, selezionare l'opzione per modificare le subnet per Grid Network (opzione 4).



Le modifiche apportate all'elenco di subnet di rete griglia sono a livello di griglia.

6. Scegliere una delle seguenti opzioni:

- Per aggiungere una subnet, immettere il seguente comando: `add CIDR`
- Per eliminare una subnet, immettere il comando: `del CIDR`
- Per impostare l'elenco delle subnet, immettere il seguente 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 digitazione richiesta utilizzando la "freccia su" per richiamare i valori digitati in precedenza al prompt di immissione corrente, quindi modificarli se necessario.

L'input di esempio riportato di seguito mostra l'impostazione delle subnet per l'elenco di subnet di rete

griglia:

```
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
```

7. Una volta pronti, inserire **q** per tornare alla schermata del menu principale. Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.
8. Scegliere una delle seguenti opzioni:
 - Selezionare l'opzione **5** per visualizzare le modifiche nell'output isolato in modo da visualizzare solo l'elemento modificato. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'esempio riportato di seguito:

```
=====
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 visualizzare le modifiche nell'output che visualizza la configurazione completa. Le modifiche sono evidenziate in verde (aggiunte) o in rosso (eliminazioni).



Alcune interfacce della riga di comando potrebbero mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough.

9. Selezionare l'opzione **7** per convalidare tutte le modifiche in fasi.

Questa convalida garantisce il rispetto delle regole per le reti Grid, Admin e Client, ad esempio l'utilizzo di sottoreti sovrapposte.

10. Se si desidera, selezionare l'opzione **8** per salvare tutte le modifiche in più fasi e tornare in seguito per continuare ad apportare le modifiche.

Questa opzione consente di uscire dallo strumento Change IP e di avviarlo di nuovo in un secondo momento, senza perdere alcuna modifica non applicata.

11. Effettuare una delle seguenti operazioni:

- Selezionare l'opzione **9** se si desidera annullare tutte le modifiche senza salvare o applicare la nuova configurazione di rete.
- Selezionare l'opzione **10** se si desidera applicare le modifiche e fornire la nuova configurazione di rete. Durante il provisioning, l'output visualizza lo stato quando vengono applicati gli aggiornamenti, come mostrato nell'output di esempio seguente:

```
Generating new grid networking description file...
```

```
Running provisioning...
```

```
Updating grid network configuration on Name
```

12. Se è stata selezionata l'opzione **10** quando si apportano modifiche alla rete griglia, selezionare una delle seguenti opzioni:

- **Apply**: Applica le modifiche immediatamente e riavvia automaticamente ogni nodo, se necessario.

Se la nuova configurazione di rete funziona contemporaneamente alla vecchia configurazione di rete senza modifiche esterne, è possibile utilizzare l'opzione **Apply** per una modifica della configurazione completamente automatica.

- **Fast**: Applicare le modifiche al successivo riavvio dei nodi.

Se è necessario apportare modifiche alla configurazione di rete fisica o virtuale per il funzionamento della nuova configurazione di rete, utilizzare l'opzione **stage**, arrestare i nodi interessati, apportare le necessarie modifiche fisiche di rete e riavviare i nodi interessati.



Se si utilizza l'opzione **stage**, riavviare il nodo il prima possibile dopo lo staging per ridurre al minimo le interruzioni.

- **CANCEL**: Non apportare modifiche alla rete in questo momento.

Se non si è a conoscenza del fatto che le modifiche proposte richiedono il riavvio dei nodi, è possibile posticipare le modifiche per ridurre al minimo l'impatto sull'utente. Selezionando **CANCEL** si torna al menu principale e si conservano le modifiche in modo da poterle applicare in un secondo momento.

Dopo aver applicato o organizzato le modifiche, viene generato un nuovo pacchetto di ripristino come risultato della modifica alla configurazione della griglia.

13. Se la configurazione viene interrotta a causa di errori, sono disponibili le seguenti opzioni:

- Per terminare la procedura di modifica dell'indirizzo IP e tornare al menu principale, immettere **a**.
- Per riprovare l'operazione non riuscita, immettere **r**.
- Per passare all'operazione successiva, immettere **c**.

L'operazione non riuscita può essere rieseguita in un secondo momento selezionando l'opzione **10** (Applica modifiche) dal menu principale. La procedura di modifica dell'IP non sarà completa fino a quando tutte le operazioni non saranno state completate correttamente.

- Se è stato necessario intervenire manualmente (ad esempio per riavviare un nodo) e si è certi che

l'azione che lo strumento ritiene non sia riuscita sia stata completata correttamente, immettere **f** per contrassegnarla come riuscita e passare all'operazione successiva.

14. Scarica un nuovo pacchetto di ripristino da Grid Manager.

- a. Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.
- b. Inserire la passphrase di provisioning.



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

15. Se hai consentito l'accesso SSH esterno, "[bloccare l'accesso](#)" una volta terminato di aggiungere o modificare gli elenchi di subnet.

Modifica gli indirizzi IP per tutti i nodi in una griglia StorageGRID

Se è necessario modificare l'indirizzo IP Grid Network per tutti i nodi della griglia, seguire questa procedura speciale. Non è possibile modificare l'IP Grid Network a livello di griglia utilizzando la procedura per modificare i singoli nodi.

Prima di iniziare

- Si dispone del `Passwords.txt` file.

Per garantire che la griglia venga avviata correttamente, è necessario apportare tutte le modifiche contemporaneamente.



Questa procedura si applica solo alla rete di rete. Non è possibile utilizzare questa procedura per modificare gli indirizzi IP nelle reti Admin o Client.

Se si desidera modificare gli indirizzi IP e il valore MTU per i nodi di un solo sito, seguire le "[Modificare la configurazione di rete del nodo](#)" istruzioni.

Fasi

1. Pianificare in anticipo le modifiche da apportare al di fuori dello strumento Change IP, ad esempio le modifiche a DNS o NTP, e le modifiche alla configurazione SSO (Single Sign-on), se utilizzata.



Se i server NTP esistenti non sono accessibili alla griglia dei nuovi indirizzi IP, aggiungere i nuovi server NTP prima di eseguire la procedura di modifica dell'indirizzo ip.



Se i server DNS esistenti non sono accessibili alla griglia dei nuovi indirizzi IP, aggiungere i nuovi server DNS prima di eseguire la procedura di modifica dell'indirizzo ip.



Se il single sign-on (SSO) è abilitato per il tuo sistema StorageGRID e qualsiasi relying party trust è stato configurato utilizzando gli indirizzi IP del nodo Admin (anziché i fully qualified domain name, come raccomandato), preparati ad aggiornare o riconfigurare questi relying party trust in Active Directory Federation Services (AD FS) immediatamente dopo aver cambiato gli indirizzi IP. Consulta la guida per configurare l'SSO usando "[OIDC](#)" o "[SAML](#)".



Se necessario, aggiungere la nuova subnet per i nuovi indirizzi IP.

2. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, "[consentire](#)

temporaneamente l'accesso" .

3. Accedere al nodo di amministrazione principale:

- a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

4. Avviare lo strumento Change IP inserendo il seguente comando: `change-ip`

5. Inserire la passphrase di provisioning quando richiesto.

Viene visualizzato il menu principale. Per impostazione predefinita, il `Selected nodes` 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: █
```

6. Nel menu principale, selezionare **2** per modificare le informazioni relative a IP/subnet mask, gateway e MTU per tutti i nodi.

- a. Selezionare **1** per apportare modifiche alla rete griglia.

Una volta effettuata la selezione, il prompt visualizza i nomi dei nodi, il nome della rete di griglia, il tipo di dati (IP/mask, Gateway o MTU), e valori correnti.

Se si modificano l'indirizzo IP, la lunghezza del prefisso, il gateway o la MTU di un'interfaccia configurata con DHCP, l'interfaccia diventa statica. Viene visualizzato un avviso prima di ogni interfaccia configurata da DHCP.

Le interfacce configurate come `fixed` non possono essere modificate.

- a. Per impostare un nuovo valore, immetterlo nel formato indicato per il valore corrente.
- b. Dopo aver modificato tutti i nodi che si desidera modificare, immettere **q** per tornare al menu principale.

Le modifiche vengono mantenute fino a quando non vengono cancellate o applicate.

7. Per rivedere le modifiche, selezionare una delle seguenti opzioni:

- **5**: Mostra le modifiche nell'output isolato per mostrare solo l'elemento modificato. Le modifiche sono

evidenziate in verde (aggiunte) o in rosso (eliminazioni), come mostrato nell'output di esempio:

```
=====  
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 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 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 mostrare aggiunte ed eliminazioni utilizzando la formattazione strikehrough. La corretta visualizzazione dipende dal client terminale che supporta le sequenze di escape VT100 necessarie.

8. Selezionare l'opzione **7** per convalidare tutte le modifiche.

Questa convalida garantisce che le regole per Grid Network, come ad esempio il non utilizzo di sottoreti sovrapposte, non vengano violate.

In questo esempio, la convalida ha restituito errori.

```
Validating new networking configuration... FAILED.  
  
DK-10-224-5-20-G1: The admin subnet 172.18.0.0/16 overlaps the 172.18.0.0/21 grid network.  
DK-10-224-5-22-S1: Duplicate Grid IP 172.16.5.18 (also in use by DK-10-224-5-21-ADM1)  
  
You must correct these errors before you can apply any changes.  
Checking for Grid Network IP address swaps... PASSED.  
  
Press Enter to continue
```

In questo esempio, la convalida è stata superata.

```
Validating new networking configuration... PASSED.  
Checking for Grid Network IP address swaps... PASSED.  
Press Enter to continue
```

9. Dopo il superamento della convalida, selezionare **10** per applicare la nuova configurazione di rete.

10. Selezionare **stage** per applicare le modifiche al successivo riavvio dei nodi.



Selezionare **stage**. Non eseguire un rolling restart, manualmente o selezionando **Apply** invece di **stage**; la griglia non si avvierà correttamente.

11. Una volta completate le modifiche, selezionare **0** per uscire dallo strumento Change IP.

12. Arrestare tutti i nodi contemporaneamente.



L'intera griglia deve essere chiusa, in modo che tutti i nodi siano spenti contemporaneamente.

13. Apportare le modifiche di rete fisiche o virtuali richieste.

14. Verificare che tutti i nodi della griglia non siano attivi.

15. Accendere tutti i nodi.

16. Dopo l'avvio della griglia:

- Se sono stati aggiunti nuovi server NTP, eliminare i valori dei server NTP precedenti.
- Se sono stati aggiunti nuovi server DNS, eliminare i valori dei server DNS precedenti.

17. Scarica il nuovo pacchetto di ripristino da Grid Manager.

- Selezionare **Manutenzione > Sistema > Pacchetto di ripristino**.
- Inserire la passphrase di provisioning.

18. Se hai consentito l'accesso SSH esterno, "**bloccare l'accesso**" quando hai finito di modificare gli indirizzi IP.

Informazioni correlate

- ["Aggiungere o modificare gli elenchi di subnet su Grid Network"](#)
- ["Chiudere il nodo della griglia"](#)

Aggiungere interfacce al nodo esistente

Aggiungi interfacce Admin o Client a un nodo Linux in StorageGRID

Seguire questa procedura per aggiungere un'interfaccia sulla rete di amministrazione o sulla rete client a un nodo Linux dopo l'installazione.

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, vedere ["Installa StorageGRID sui nodi basati su software"](#).

Questa procedura viene eseguita sul server Linux che ospita il nodo che richiede la nuova assegnazione di

rete, non all'interno del nodo. Questa procedura aggiunge l'interfaccia solo al nodo; si verifica un errore di convalida se si tenta di specificare altri parametri di rete.

Per fornire le informazioni di indirizzamento, è necessario utilizzare lo strumento Change IP (Modifica IP). Vedere "[Modificare la configurazione di rete del nodo](#)".

Fasi

1. Accedere al server Linux che ospita il nodo.
2. Modificare il file di configurazione del nodo: `/etc/storagegrid/nodes/node-name.conf`.



Non specificare altri parametri di rete, altrimenti si verificherà un errore di convalida.

- a. Aggiungere una voce per la nuova destinazione di rete. Ad esempio:

```
CLIENT_NETWORK_TARGET = bond0.3206
```

- b. Facoltativo: Aggiungere una voce per l'indirizzo MAC. Ad esempio:

```
CLIENT_NETWORK_MAC = aa:57:61:07:ea:5c
```

3. Eseguire il comando `node validate`:

```
sudo storagegrid node validate node-name
```

4. Risolvere tutti gli errori di convalida.

5. Eseguire il comando `node reload`:

```
sudo storagegrid node reload node-name
```

Aggiungi interfacce trunk o di accesso a un nodo Linux in StorageGRID

È possibile aggiungere trunk o interfacce di accesso supplementari a un nodo Linux dopo averlo installato. Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Prima di iniziare

- Hai accesso al "[istruzioni per l'installazione di StorageGRID](#)" sulla tua piattaforma Linux.
- Si dispone del `Passwords.txt` file.
- Si dispone di "[autorizzazioni di accesso specifiche](#)".



Non tentare di aggiungere interfacce a un nodo mentre è attiva una procedura di aggiornamento, ripristino o espansione del software.

A proposito di questa attività

Seguire questa procedura per aggiungere una o più interfacce aggiuntive a un nodo Linux dopo l'installazione del nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si

aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.

Il nodo non è disponibile per un breve periodo di tempo quando si aggiungono interfacce. Eseguire questa procedura su un nodo alla volta.

Fasi

1. Accedere al server Linux che ospita il nodo.
2. Utilizzando un editor di testo come vim o pico, modificare il file di configurazione del nodo:

```
/etc/storagegrid/nodes/node-name.conf
```

3. Aggiungere una voce al file per specificare il nome e, facoltativamente, la descrizione di ogni interfaccia aggiuntiva che si desidera aggiungere al nodo. USA questo formato.

```
INTERFACE_TARGET_#####=value
```

Per *#####*, specificare un numero univoco per ogni INTERFACE_TARGET voce che si sta aggiungendo.

Per *valore*, specificare il nome dell'interfaccia fisica sull'host bare-metal. Quindi, facoltativamente, aggiungere una virgola e fornire una descrizione dell'interfaccia, che viene visualizzata nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Ad esempio:

```
INTERFACE_TARGET_0001=ens256, Trunk
```



Non specificare altri parametri di rete, altrimenti si verificherà un errore di convalida.

4. Eseguire il seguente comando per convalidare le modifiche apportate al file di configurazione del nodo:

```
sudo storagegrid node validate node-name
```

Risolvere eventuali errori o avvisi prima di passare alla fase successiva.

5. Eseguire il seguente comando per aggiornare la configurazione del nodo:

```
sudo storagegrid node reload node-name
```

Al termine

- Se sono state aggiunte una o più interfacce di linea, andare a ["Configurare le interfacce VLAN"](#) per configurare una o più interfacce VLAN per ogni nuova interfaccia principale.
- Se sono state aggiunte una o più interfacce di accesso, passare al ["configurare i gruppi ad alta disponibilità"](#) per aggiungere le nuove interfacce direttamente ai gruppi di ha.

Aggiungi interfacce trunk o di accesso a un nodo VMware in StorageGRID

Una volta installato il nodo, è possibile aggiungere un trunk o un'interfaccia di accesso a un nodo VM. Le interfacce aggiunte vengono visualizzate nella pagina delle interfacce VLAN e nella pagina dei gruppi ha.

Prima di iniziare

- Hai accesso alle istruzioni per ["Installazione di StorageGRID sulla piattaforma VMware"](#) .
- Si dispone di macchine virtuali VMware con nodo di amministrazione e nodo di gateway.
- Si dispone di una subnet di rete che non viene utilizzata come rete, amministratore o rete client.
- Si dispone del `Passwords.txt` file.
- Si dispone di ["autorizzazioni di accesso specifiche"](#).



Non tentare di aggiungere interfacce a un nodo mentre è attiva una procedura di aggiornamento, ripristino o espansione del software.

A proposito di questa attività

Seguire questa procedura per aggiungere una o più interfacce aggiuntive a un nodo VMware dopo l'installazione del nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poter utilizzare le interfacce VLAN per separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in un gruppo ad alta disponibilità (ha).

Se si aggiunge un'interfaccia di linea, è necessario configurare un'interfaccia VLAN in StorageGRID. Se si aggiunge un'interfaccia di accesso, è possibile aggiungerla direttamente a un gruppo ha; non è necessario configurare un'interfaccia VLAN.

Il nodo potrebbe non essere disponibile per un breve periodo di tempo quando si aggiungono interfacce.

Fasi

1. In vCenter, aggiungere una nuova scheda di rete (tipo VMXNET3) a un nodo di amministrazione e a una macchina virtuale del nodo gateway. Selezionare le caselle di controllo **connesso** e **Connetti all'accensione**.

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. Utilizzare `ip link show` per confermare il rilevamento della nuova interfaccia di rete ens256.

```
ip link show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN mode
DEFAULT group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:4e:5b brd ff:ff:ff:ff:ff:ff
3: eth1: <BROADCAST,MULTICAST> mtu 1500 qdisc noop state DOWN mode
DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:fa:ce brd ff:ff:ff:ff:ff:ff
4: eth2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1400 qdisc mq state UP
mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:d6:87 brd ff:ff:ff:ff:ff:ff
5: ens256: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc mq master
ens256vrf state UP mode DEFAULT group default qlen 1000
    link/ether 00:50:56:a0:ea:88 brd ff:ff:ff:ff:ff:ff
```

Al termine

- Se sono state aggiunte una o più interfacce di linea, andare a ["Configurare le interfacce VLAN"](#) per configurare una o più interfacce VLAN per ogni nuova interfaccia principale.
- Se sono state aggiunte una o più interfacce di accesso, passare al ["configurare i gruppi ad alta disponibilità"](#) per aggiungere le nuove interfacce direttamente ai gruppi di ha.

Configurare i server DNS in StorageGRID

È possibile aggiungere, aggiornare e rimuovere i server DNS, in modo da poter utilizzare i nomi host FQDN (Fully Qualified Domain Name) anziché gli indirizzi IP.

Per utilizzare FQDN (Fully Qualified Domain Name) invece degli indirizzi IP quando si specificano i nomi host per le destinazioni esterne, specificare l'indirizzo IP di ciascun server DNS da utilizzare. Queste voci vengono utilizzate per AutoSupport, e-mail di avviso, notifiche SNMP, endpoint dei servizi della piattaforma, pool di storage cloud, e molto altro ancora.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone degli indirizzi IP dei server DNS da configurare.

A proposito di questa attività

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

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

Aggiungere un server DNS

Per aggiungere un server DNS, procedere come segue.

Fasi

1. Selezionare **Manutenzione > Rete > Server DNS**.
2. Selezionare **Aggiungi un altro server** per aggiungere un server DNS.
3. Selezionare **Salva**.

Modificare un server DNS

Per modificare un server DNS, procedere come segue.

Fasi

1. Selezionare **Manutenzione > Rete > Server DNS**.
2. Selezionare l'indirizzo IP del nome del server che si desidera modificare e apportare le modifiche necessarie.
3. Selezionare **Salva**.

Eliminare un server DNS

Per eliminare un indirizzo IP di un server DNS, procedere come segue.

Fasi

1. Selezionare **Manutenzione > Rete > Server DNS**.
2. Seleziona l'icona di eliminazione  accanto all'indirizzo IP.
3. Selezionare **Salva**.

Modificare la configurazione DNS per un singolo nodo StorageGRID

Invece di configurare il DNS a livello globale per l'intera implementazione, è possibile eseguire uno script per configurare il DNS in modo diverso per ciascun nodo della griglia.

In generale, 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.

Fasi

1. L'accesso SSH esterno è bloccato per impostazione predefinita. Se necessario, "[consentire temporaneamente l'accesso](#)".
2. Accedere al nodo di amministrazione principale:
 - a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da \$ a #.

- e. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `ssh-add`
- f. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
3. accedere al nodo da aggiornare con una configurazione DNS personalizzata: `ssh node_IP_address`
4. Eseguire lo script di installazione 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`]
```

5. Aggiungere l'indirizzo IPv4 di un server che fornisce il servizio dei nomi di dominio per la rete: `add <nameserver IP_address>`

6. Ripetere il `add nameserver` comando per aggiungere i server dei nomi.
7. Seguire le istruzioni richieste per altri comandi.
8. Salvare le modifiche e uscire dall'applicazione: `save`
9. chiudere la shell dei comandi sul server: `exit`
10. Per ciascun nodo della griglia, ripetere i passaggi da [accesso al nodo](#) a [chiudere la shell dei comandi](#).
11. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Immettere: `ssh-add -D`
12. Se hai consentito l'accesso SSH esterno, ["bloccare l'accesso"](#) una volta terminata la modifica della configurazione DNS.

Gestisci i server NTP in StorageGRID

È possibile aggiungere, aggiornare o rimuovere server NTP (Network Time Protocol) per garantire che i dati siano sincronizzati in modo accurato tra i nodi della griglia nel sistema StorageGRID.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Si dispone degli indirizzi IPv4 dei server NTP da configurare.

Utilizzo di NTP da parte di StorageGRID

Il sistema StorageGRID utilizza il protocollo NTP (Network Time Protocol) per sincronizzare l'ora tra tutti i nodi della griglia.

In ogni sito, ad almeno due nodi nel sistema StorageGRID viene assegnato il ruolo NTP primario. Si sincronizzano con un minimo consigliato di quattro e un massimo di sei sorgenti di tempo esterne e tra loro. Ogni nodo del sistema StorageGRID che non è un nodo NTP primario agisce come client NTP e si sincronizza con questi nodi NTP primari.

I server NTP esterni si connettono ai nodi ai quali sono stati precedentemente assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.

Linee guida del server NTP

Segui queste linee guida per proteggerti dai problemi di tempistica:

- I server NTP esterni si connettono ai nodi ai quali sono stati precedentemente assegnati ruoli NTP primari. Per questo motivo, si consiglia di specificare almeno due nodi con ruoli NTP primari.
- Assicurarsi che almeno due nodi di ciascun sito possano accedere ad almeno quattro origini NTP esterne. Se solo un nodo di un sito può raggiungere le origini NTP, si verificheranno problemi di tempistica se tale nodo non funziona. Inoltre, la designazione di due nodi per sito come origini NTP primarie garantisce tempi precisi se un sito viene isolato dal resto della rete.
- I server NTP esterni specificati devono utilizzare il protocollo NTP. È necessario specificare i riferimenti al server NTP di strato 3 o superiore per evitare problemi di deriva del tempo.



Quando specifichi l'origine NTP esterna per un'installazione di StorageGRID a livello di produzione, non usare il servizio Ora di Windows (W32Time) su una versione di Windows precedente a Windows Server 2016. Il servizio Ora sulle versioni precedenti di Windows non è sufficientemente preciso e non è supportato da Microsoft per l'uso in ambienti ad alta precisione, incluso StorageGRID. Per dettagli, vedi "[Limite di supporto per un tempo ad alta precisione](#)".

Configurare i server NTP

Per aggiungere, aggiornare o rimuovere i server NTP, procedere come segue.

Fasi

1. Selezionare **Manutenzione > Rete > Server NTP**.
2. Nella sezione Server, aggiungere, aggiornare o rimuovere le voci del server NTP, secondo necessità.

È necessario includere almeno quattro server NTP ed è possibile specificare fino a sei server.

3. Inserire la passphrase di provisioning per il sistema StorageGRID, quindi selezionare **Salva**.

La pagina viene disattivata fino al completamento degli aggiornamenti della configurazione.



Se tutti i server NTP non superano il test di connessione dopo aver salvato i nuovi server NTP, non procedere. Contattare il supporto tecnico.

Risolvere i problemi del server NTP

In caso di problemi con la stabilità o la disponibilità dei server NTP originariamente specificati durante l'installazione, è possibile aggiornare l'elenco delle origini NTP esterne utilizzate dal sistema StorageGRID aggiungendo server aggiuntivi o aggiornando o rimuovendo i server esistenti.

Ripristinare la connettività di rete per i nodi StorageGRID 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 rete possono causare nodi isolati.

A proposito di questa attività

L'isolamento del nodo è indicato da:

- Avvisi, come **Impossibile comunicare con il nodo (Avvisi > corrente)**
- Diagnostica relativa alla connettività (**Supporto > Strumenti > Diagnostica**)

Di seguito sono riportate alcune delle conseguenze derivanti dall'utilizzo di nodi isolati:

- Se sono isolati più nodi, potrebbe non essere possibile accedere a Grid Manager o accedervi.
- Se si isolano più nodi, i valori di utilizzo dello storage e di quota mostrati nella dashboard per il tenant Manager potrebbero essere obsoleti. I totali verranno aggiornati al ripristino della connettività di rete.

Per risolvere il problema di isolamento, eseguire un'utilità della riga di comando su ciascun nodo isolato o su un nodo di un gruppo (tutti i nodi di una subnet che non contiene il nodo di amministrazione primario) isolato

dalla griglia. L'utility fornisce ai nodi l'indirizzo IP di un nodo non isolato nella griglia, che consente al nodo isolato o al gruppo di nodi di contattare nuovamente l'intera griglia.



Se il sistema mDNS (Domain Name System) multicast è disattivato nelle reti, potrebbe essere necessario eseguire l'utilità della riga di comando su ogni nodo isolato.

Fasi

Questa procedura non si applica quando solo alcuni servizi sono offline o segnalano errori di comunicazione.

1. Accedere al nodo e verificare `/var/local/log/dynip.log` la presenza di messaggi di isolamento.

Ad esempio:

```
[2018-01-09T19:11:00.545] UpdateQueue - WARNING -- Possible isolation,
no contact with other nodes.
If this warning persists, manual action might be required.
```

Se si utilizza la console VMware, viene visualizzato un messaggio che indica che il nodo potrebbe essere isolato.

Nelle distribuzioni Linux, i messaggi di isolamento vengono visualizzati nei `/var/log/storagegrid/node/<nodename>.log` file.

2. Se i messaggi di isolamento sono ricorrenti e persistenti, eseguire il seguente comando:

```
add_node_ip.py <address>
```

Dove `<address>` è l'indirizzo IP di un nodo remoto connesso alla rete.

```
# /usr/sbin/add_node_ip.py 10.224.4.210

Retrieving local host information
Validating remote node at address 10.224.4.210
Sending node IP hint for 10.224.4.210 to local node
Local node found on remote node. Update complete.
```

3. Verificare quanto segue per ciascun nodo precedentemente isolato:

- I servizi del nodo sono stati avviati.
- Lo stato del servizio Dynamic IP è "in esecuzione" dopo l'esecuzione del `storagegrid-status` comando.
- Nella pagina nodi, il nodo non appare più disconnesso dal resto della griglia.



Se l'esecuzione del `add_node_ip.py` comando non risolve il problema, potrebbero esserci altri problemi di rete che devono essere risolti.

Procedure host e middleware

Migrare un nodo StorageGRID su un nuovo host Linux

È possibile migrare uno o più nodi StorageGRID da un host Linux (l' *host di origine*) a un altro host Linux (l' *host di destinazione*) per eseguire la manutenzione dell'host senza influire sulla funzionalità o sulla disponibilità del grid.

Ad esempio, è possibile migrare un nodo per eseguire l'applicazione di patch e il riavvio del sistema operativo.

Prima di iniziare

- Hai pianificato la distribuzione StorageGRID in modo da includere il supporto per la migrazione. Vedere ["Requisiti per la migrazione dei container di nodi"](#).
- L'host di destinazione è già pronto per l'uso con StorageGRID.
- Lo storage condiviso viene utilizzato per tutti i volumi di storage per nodo
- Le interfacce di rete hanno nomi coerenti tra gli host.



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

Sullo stesso host è possibile implementare altri tipi di nodi, come ad esempio i nodi Admin o Gateway. Tuttavia, se si dispone di più nodi dello stesso tipo (ad esempio due nodi gateway), non installare tutte le istanze sullo stesso host.

Esportare il nodo dall'host di origine

Come primo passo, chiudere il nodo grid ed esportarlo dall'host Linux di origine.

Eseguire i seguenti comandi sul *host di origine*.

Fasi

1. Ottenere lo stato di tutti i nodi attualmente in esecuzione sull'host di origine.

```
sudo storagegrid node status all
```

Output di esempio:

```
Name Config-State Run-State
DC1-ADM1 Configured Running
DC1-ARC1 Configured Running
DC1-GW1 Configured Running
DC1-S1 Configured Running
DC1-S2 Configured Running
DC1-S3 Configured Running
```

2. Identificare il nome del nodo che si desidera migrare e interromperlo se il relativo stato di esecuzione è in esecuzione.

```
sudo storagegrid node stop DC1-S3
```

Output di esempio:

```
Stopping node DC1-S3  
Waiting up to 630 seconds for node shutdown
```

3. Esportare il nodo dall'host di origine.

```
sudo storagegrid node export DC1-S3
```

Output di esempio:

```
Finished exporting node DC1-S3 to /dev/mapper/sgws-dc1-s3-var-local.  
Use 'storagegrid node import /dev/mapper/sgws-dc1-s3-var-local' if you  
want to import it again.
```

4. Prendere nota del `import` comando suggerito nell'output.

Questo comando verrà eseguito sull'host di destinazione nel passaggio successivo.

Nodo di importazione sull'host di destinazione

Dopo aver esportato il nodo dall'host di origine, importare e convalidare il nodo sull'host di destinazione. La convalida conferma che il nodo ha accesso agli stessi dispositivi di storage a blocchi e di interfaccia di rete dell'host di origine.

Eseguire i seguenti comandi sul *host di destinazione*.

Fasi

1. Importare il nodo sull'host di destinazione.

```
sudo storagegrid node import /dev/mapper/sgws-dc1-s3-var-local
```

Output di esempio:

```
Finished importing node DC1-S3 from /dev/mapper/sgws-dc1-s3-var-local.  
You should run 'storagegrid node validate DC1-S3'
```

2. Convalidare la configurazione del nodo sul nuovo host.

```
sudo storagegrid node validate DC1-S3
```

Output di esempio:

```
Confirming existence of node DC1-S3... PASSED
Checking configuration file /etc/storagegrid/nodes/DC1-S3.conf for node
DC1-S3... PASSED
Checking for duplication of unique values... PASSED
```

3. Se si verificano errori di convalida, risolverli prima di avviare il nodo migrato.

Per informazioni sulla risoluzione dei problemi, vedere StorageGRID ["istruzioni di installazione"](#) per il tuo sistema operativo Linux.

Avvia nodo migrato

Dopo aver validato il nodo migrato, avviarlo eseguendo un comando sul *host di destinazione*.

Fasi

1. Avviare il nodo sul nuovo host.

```
sudo storagegrid node start DC1-S3
```

2. Accedere a Grid Manager e verificare che lo stato del nodo sia verde senza alcun avviso.



Verificare che lo stato del nodo sia verde per garantire che il nodo migrato sia stato riavviato completamente e ricongiungesse alla griglia. Se lo stato non è verde, non migrare nodi aggiuntivi in modo da non avere più di un nodo fuori servizio.

3. Se non si riesce ad accedere a Grid Manager, attendere 10 minuti, quindi eseguire il seguente comando:

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

Verificare che il nodo migrato abbia uno stato di esecuzione in esecuzione.

Configura una macchina virtuale VMware per il riavvio automatico in StorageGRID

Se la macchina virtuale non si riavvia dopo il riavvio di VMware vSphere Hypervisor, potrebbe essere necessario configurare la macchina virtuale per il riavvio automatico.

Eseguire questa procedura se si nota che una macchina virtuale non si riavvia durante il ripristino di un nodo di griglia o l'esecuzione di un'altra procedura di manutenzione.

Fasi

1. Nell'albero di VMware vSphere Client, selezionare la macchina virtuale non avviata.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e selezionare **Power on** (accensione).
3. Configurare VMware vSphere Hypervisor per riavviare automaticamente la macchina virtuale in futuro.

Recovery o sostituzione dei nodi

Avvertenze e considerazioni per il ripristino dei nodi StorageGRID

In caso di guasto di un nodo della griglia, è necessario ripristinarlo il prima possibile. Prima di iniziare, è necessario esaminare tutti gli avvisi e le considerazioni per il ripristino del nodo.



StorageGRID è un sistema distribuito composto da più nodi che lavorano l'uno con l'altro. Non utilizzare le snapshot dei dischi per ripristinare i nodi della griglia. Fare invece riferimento alle procedure di ripristino e manutenzione per ciascun tipo di nodo.



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. Fare riferimento a ["Come il supporto tecnico recupera un sito"](#).

Di seguito sono riportati alcuni dei motivi per cui è stato eseguito il ripristino di un nodo Grid guasto il prima possibile:

- Un nodo Grid guasto può ridurre la ridondanza dei dati di sistema e dei dati a oggetti, lasciando l'utente vulnerabile al rischio di perdita permanente dei dati in caso di guasto di un altro nodo.
- Un nodo di grid guasto può influire sull'efficienza delle operazioni quotidiane.
- Un nodo Grid guasto può ridurre la capacità di monitorare le operazioni del sistema.
- Un nodo Grid guasto può causare un errore del server interno 500 se sono in vigore regole ILM rigide.
- Se un nodo di rete non viene recuperato tempestivamente, i tempi di ripristino potrebbero aumentare. Ad esempio, potrebbero svilupparsi code che devono essere cancellate prima del completamento del ripristino.

Seguire sempre la procedura di ripristino per il tipo specifico di nodo della griglia che si sta ripristinando. Le procedure di ripristino variano a seconda dei nodi amministrativi primari o non primari, dei nodi gateway, dei nodi appliance e dei nodi storage.

Condizioni preliminari per il ripristino dei nodi di rete

Quando si ripristinano i nodi della griglia, si presume che siano presenti tutte le seguenti condizioni:

- L'hardware fisico o virtuale guasto è stato sostituito e configurato.
- La versione del programma di installazione dell'appliance StorageGRID sul dispositivo sostitutivo corrisponde alla versione software del sistema StorageGRID, come descritto in ["Verificare e aggiornare la versione del programma di installazione dell'appliance StorageGRID"](#).
- Se stai ripristinando un nodo della griglia diverso dal nodo amministratore primario, deve esserci connettività tra il nodo della griglia che stai ripristinando e il nodo amministratore che gestisce la procedura di ripristino.
- 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 recovery del nodo in caso di guasto di un server che ospita più di un nodo griglia

Se un server che ospita più di un nodo della griglia si guasta, puoi ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server guasto ospita il nodo di amministrazione primario e non esistono nodi di amministrazione non primari, devi ripristinare prima il nodo di amministrazione primario.

Indirizzi IP per i nodi ripristinati

Non tentare di ripristinare un nodo utilizzando un indirizzo IP attualmente assegnato a un altro nodo. Quando si implementa il nuovo nodo, utilizzare l'indirizzo IP corrente del nodo guasto o un indirizzo IP inutilizzato.

Se si utilizza un nuovo indirizzo IP per implementare il nuovo nodo e ripristinarlo, il nuovo indirizzo IP continuerà a essere utilizzato per il nodo recuperato. Se si desidera ripristinare l'indirizzo IP originale, utilizzare lo strumento Cambia IP al termine del ripristino.

Raccogli il materiale necessario per il ripristino del nodo della griglia StorageGRID

Prima di eseguire le procedure di manutenzione, assicurarsi di disporre dei materiali necessari per ripristinare un nodo della griglia guasto.

Elemento	Note
Archivio di installazione di StorageGRID	Se è necessario ripristinare un nodo grid, è necessario farlo Scaricare i file di installazione di StorageGRID per la piattaforma. Nota: non è necessario scaricare i file se si stanno ripristinando volumi di storage guasti su un nodo di storage.
Laptop di assistenza	Il laptop di assistenza deve disporre di quanto segue: • Porta di rete • Client SSH (ad esempio, putty) • "Browser Web supportato"

Elemento	Note
Pacchetto di 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. Dopo aver effettuato l'accesso a un qualsiasi nodo di amministrazione, utilizzare Grid Manager per scaricare un pacchetto di ripristino. Selezionare Manutenzione > Sistema > Pacchetto di ripristino. Se non riesci ad accedere a Grid Manager, puoi trovare copie crittografate del pacchetto di ripristino 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.
Passphrase di provisioning	La passphrase viene creata e documentata al momento dell'installazione del sistema StorageGRID. La passphrase di provisioning non è contenuta nel Passwords.txt file.
Documentazione aggiornata per la piattaforma	Per la documentazione, visitare il sito Web del vendor della piattaforma. Per le versioni attualmente supportate della piattaforma, vedere "Tool di matrice di interoperabilità NetApp" .

Scaricare ed estrarre i file di installazione di StorageGRID

Scaricare il software ed estrarre i file, a meno che non si sia ["Ripristino dei volumi di storage guasti in un nodo di storage"](#).

È necessario utilizzare la versione di StorageGRID attualmente in esecuzione sulla griglia.

Fasi

1. Determinare la versione del software attualmente installata. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **About** (informazioni su).
2. Andare a ["Pagina dei download NetApp per StorageGRID"](#).
3. Selezionare la versione di StorageGRID attualmente in esecuzione nella griglia.

Le versioni software StorageGRID hanno questo formato: 11.x.y.

4. Accedi con il nome utente e la password del tuo account NetApp.
5. Leggere il Contratto di licenza con l'utente finale, selezionare la casella di controllo, quindi selezionare **Accept & Continue** (Accetta e continua).
6. Nella colonna **Installa StorageGRID** della pagina di download, selezionare il .tgz file o .zip per la propria piattaforma.

La versione mostrata nel file di archivio dell'installazione deve corrispondere alla versione del software attualmente installato.

Utilizzare il .zip file se si utilizza Windows.

Piattaforma	Archivio di installazione
RHEL	StorageGRID-Webscale-version-RPM-uniqueID.zip StorageGRID-Webscale-version-RPM-uniqueID.tgz
Ubuntu o Debian o appliance	StorageGRID-Webscale-version-DEB-uniqueID.zip StorageGRID-Webscale-version-DEB-uniqueID.tgz
VMware	StorageGRID-Webscale-version-VMware-uniqueID.zip StorageGRID-Webscale-version-VMware-uniqueID.tgz

7. Scaricare ed estrarre il file di archivio.
8. Passa alla sezione appropriata per la tua piattaforma per scegliere i file di cui hai bisogno, in base alla tua piattaforma e ai nodi della griglia che devi recuperare.

I percorsi elencati nella fase per ciascuna piattaforma sono relativi alla directory di primo livello installata dal file di archivio.

9. Se stai recuperando un ["nodo basato su software"](#) , seleziona i file appropriati:

RHEL

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

Percorso e nome del file	Descrizione
	Uno script di supporto chiamato dallo script Python associato <code>storagegrid-ssoauth-azure.py</code> per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

Ubuntu o Debian

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Un file di licenza NetApp non in produzione che è possibile utilizzare per le implementazioni di test e proof of concept.
	PACCHETTO DEB per l'installazione delle immagini dei nodi StorageGRID su host Ubuntu o Debian.
	MD5 checksum 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.
Tool di scripting per la distribuzione	Descrizione
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.

Percorso e nome del file	Descrizione
	Script Python di esempio che è possibile utilizzare per accedere all'API Grid Management quando è attivato il single sign-on. È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Esempio di manuale e ruolo Ansible per la configurazione di host Ubuntu o Debian per la distribuzione di container StorageGRID. È possibile personalizzare il ruolo o il manuale in base alle esigenze.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando SSO (Single Sign-on) è attivato utilizzando Active Directory o Ping Federate.
	Uno script di supporto chiamato dallo script Python associato <code>storagegrid-ssoauth-azure.py</code> per eseguire interazioni SSO con Azure.
	Schemi API per StorageGRID. Nota: Prima di eseguire un aggiornamento, è possibile utilizzare questi schemi per confermare che qualsiasi codice scritto per utilizzare le API di gestione StorageGRID sarà compatibile con la nuova release di StorageGRID se non si dispone di un ambiente StorageGRID non in produzione per il test di compatibilità degli aggiornamenti.

VMware

Percorso e nome del file	Descrizione
	Un file di testo che descrive tutti i file contenuti nel file di download di StorageGRID.
	Licenza gratuita che non fornisce alcun diritto di supporto per il prodotto.

Percorso e nome del file	Descrizione
	Il file del disco della macchina virtuale utilizzato come modello per la creazione di macchine virtuali con nodo grid.
	Il file modello Open Virtualization Format (.ovf) e il file manifest (.mf) per la distribuzione del nodo amministrativo primario.
	Il file modello (.ovf) e il file manifesto (.mf) per la distribuzione di nodi Admin non primari.
	Il file modello (.ovf) e il file manifesto (.mf) per la distribuzione dei nodi Gateway.
	Il file modello (.ovf) e il file manifesto (.mf) per la distribuzione dei nodi di archiviazione basati su macchine virtuali.
Tool di scripting per la distribuzione	Descrizione
	Uno script della shell Bash utilizzato per automatizzare l'implementazione dei nodi virtual grid.
	Un file di configurazione di esempio da utilizzare con <code>deploy-vsphere-ovftool.sh</code> lo script.
	Script Python utilizzato per automatizzare la configurazione di un sistema StorageGRID.
	Script Python utilizzato per automatizzare la configurazione delle appliance StorageGRID.
	Esempio di script Python che è possibile utilizzare per accedere all'API Grid Management quando è attivato il Single Sign-on (SSO). È anche possibile utilizzare questo script per l'integrazione federate Ping.
	Un file di configurazione di esempio da utilizzare con <code>configure-storagegrid.py</code> lo script.
	Un file di configurazione vuoto da utilizzare con <code>configure-storagegrid.py</code> lo script.

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

10. Se si sta ripristinando un sistema basato su appliance StorageGRID, selezionare i file appropriati.



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 in cui si esegue la procedura di ripristino.

Percorso e nome del file	Descrizione
	PACCHETTO DEB per l'installazione delle immagini del nodo StorageGRID sulle appliance.
	MD5 checksum per il file <code>/debs/storagegridwebscale-images-version-SHA.deb</code> .

Selezionare la procedura di ripristino del nodo StorageGRID

Seleziona la procedura di ripristino corretta per il tipo di nodo che ha avuto un guasto.

Nodo della griglia	Procedura di recovery
Nodo di storage	La procedura di ripristino dello Storage Node dipende dal tipo di errore. "Ripristino da guasti del nodo di storage"

Nodo della griglia	Procedura di recovery
Nodo Admin	La procedura Admin Node (nodo amministratore) dipende dalla necessità di ripristinare il nodo amministratore primario o un nodo amministratore non primario. "Ripristino da errori del nodo di amministrazione"
Nodo gateway	"Ripristino da guasti del nodo gateway"
Nodo di archiviazione	"Ripristino da guasti al nodo di archivio (sito di documentazione StorageGRID 11,8)"



Se un server che ospita più di un nodo della griglia si guasta, puoi ripristinare i nodi in qualsiasi ordine. Tuttavia, se il server guasto ospita il nodo di amministrazione primario e non esistono nodi di amministrazione non primari, devi ripristinare prima il nodo di amministrazione primario. Ripristinare prima il nodo di amministrazione primario impedisce che il ripristino degli altri nodi si blocchi mentre cercano di contattare il nodo di amministrazione primario. Se è disponibile un nodo di amministrazione non primario, puoi usarlo per ripristinare gli altri nodi, così quei ripristini possono procedere senza contattare il nodo di amministrazione primario.

Ripristino da guasti del nodo di storage

Ripristina dai guasti dei nodi di archiviazione StorageGRID

La procedura per il ripristino di un nodo di storage guasto dipende dal tipo di guasto e dal tipo di nodo di storage guasto.

Utilizzare questa tabella per selezionare la procedura di ripristino per un nodo di storage guasto.

Problema	Azione	Note
Si è verificato un errore in più di un nodo di storage.	Contattare il supporto tecnico.	Se si verifica un guasto a più di un nodo di archiviazione, il supporto tecnico deve intervenire per il ripristino al fine di prevenire incoerenze nel database Cassandra che potrebbero causare la perdita di dati. Potrebbe essere necessaria una procedura di ripristino del sito. Il supporto tecnico può stabilire quando è sicuro avviare il ripristino di un secondo Storage Node. Nota: Se più di un nodo di archiviazione che contiene il servizio ADC si guasta in un sito, tutte le richieste di servizio della piattaforma in sospeso per quel sito andranno perse.
Si è verificato un errore in più di un nodo di storage in un sito o in un intero sito.	Contattare il supporto tecnico. Potrebbe essere necessario eseguire una procedura di ripristino del sito.	Il supporto tecnico valuterà la tua situazione e svilupperà un piano di recovery. Vedere "Come il supporto tecnico recupera un sito" .
Si è verificato un errore in un nodo di storage dell'appliance.	"Ripristinare il nodo storage dell'appliance"	La procedura di ripristino per i nodi di storage dell'appliance è la stessa per tutti i guasti.
Uno o più volumi di storage sono guasti, ma il disco di sistema è intatto	"Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto"	Questa procedura viene utilizzata per i nodi di storage basati su software.
Il disco di sistema è guasto.	"Ripristino in caso di guasto al disco di sistema"	La procedura di sostituzione del nodo dipende dalla piattaforma di implementazione e dal fatto che anche i volumi di storage abbiano avuto un guasto.



Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Ripristinare il nodo storage dell'appliance

Avvisi per il ripristino dei nodi di archiviazione dell'appliance StorageGRID

La procedura per il ripristino di un nodo di storage dell'appliance StorageGRID guasto è la stessa, sia che si stia ripristinando dalla perdita del disco di sistema che dalla perdita dei soli volumi di storage.



Se più di un nodo di archiviazione è guasto (o è offline), contattare l'assistenza tecnica. Non eseguire la seguente procedura di ripristino. Potrebbe verificarsi una perdita di dati. Per ulteriori informazioni, fare riferimento a ["Come il supporto tecnico recupera un sito"](#).



Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.



Per le procedure di manutenzione dell'hardware, ad esempio le istruzioni per la sostituzione di un controller o la reinstallazione di SANtricity OS, consultare la ["Istruzioni di manutenzione per l'apparecchio di stoccaggio"](#).

Preparare il nodo di archiviazione dell'appliance StorageGRID per la reinstallazione

Quando si ripristina un nodo di storage dell'appliance, è necessario prima preparare l'appliance per la reinstallazione del software StorageGRID.

Fasi

1. Accedere al nodo di storage guasto:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Preparare il nodo di archiviazione dell'appliance per l'installazione del software StorageGRID.

```
sgareinstall
```

3. Quando viene richiesto di continuare, immettere: `y`

L'apparecchio si riavvia e la sessione SSH termina. In genere, il programma di installazione dell'appliance StorageGRID richiede circa 5 minuti, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.



Non tentare di accelerare il riavvio spegnendo e riaccendendo o ripristinando l'apparecchio. È possibile interrompere gli aggiornamenti automatici di BIOS, BMC o altri aggiornamenti del firmware.

Il nodo di storage dell'appliance StorageGRID viene ripristinato e i dati sul nodo di storage non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale devono rimanere intatti; tuttavia, si consiglia di confermarli al termine della procedura.

Dopo aver eseguito il `sgareinstall` comando, tutti gli account, le password e le chiavi SSH con provisioning StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avviare l'installazione dell'appliance StorageGRID

Per installare StorageGRID su un nodo di storage dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance.

Prima di iniziare

- L'appliance è stata installata in un rack, collegata alla rete e accesa.
- I collegamenti di rete e gli indirizzi IP sono stati configurati per l'appliance mediante il programma di installazione dell'appliance StorageGRID.
- Conosci l'indirizzo IP di uno dei seguenti Admin Node:
 - Il nodo Admin principale per la grid StorageGRID
 - Un nodo Admin non primario, se disponibile
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono state definite nell'elenco delle subnet della rete griglia nel nodo di amministrazione principale.
- Queste attività preliminari sono state completate seguendo le istruzioni di installazione dell'appliance di storage. Vedere ["Avvio rapido per l'installazione dell'hardware"](#).
- Si sta utilizzando un ["browser web supportato"](#).
- Conosci uno degli indirizzi IP assegnati al controller di calcolo nell'appliance. È possibile utilizzare l'indirizzo IP per Admin Network (porta di gestione 1 sul controller), Grid Network o Client Network.

A proposito di questa attività

Per installare StorageGRID su un nodo di storage dell'appliance:

- Specifichi l'indirizzo IP del nodo Admin primario. Se il nodo Admin primario non è disponibile, specifichi l'indirizzo IP del nodo Admin non primario, se disponibile. Confermi anche il nome host (nome di sistema) del nodo.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.



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.

- Durante il processo, l'installazione viene interrotta. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo di storage in sospeso come sostituzione del nodo guasto.
- Una volta configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Fasi

1. Aprire un browser e inserire uno degli indirizzi IP del controller di calcolo nell'appliance.

```
https://Controller_IP:8443
```

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Nella sezione Primary Admin Node Connection (connessione nodo amministratore primario), determinare se è necessario specificare l'indirizzo IP per il nodo amministratore primario.

Il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, presupponendo che il nodo amministratore primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa sottorete.

3. Se questo indirizzo IP non viene visualizzato o se è necessario modificarlo, specificare l'indirizzo:

Opzione	Fasi
Immissione manuale dell'IP	a. Deselezionare la casella di controllo Enable Admin Node Discovery (attiva rilevamento nodo amministratore). b. Inserire manualmente l'indirizzo IP. Nota: per l'installazione, immettere manualmente l'indirizzo IP del nodo di amministrazione che si desidera utilizzare per installare il nodo. Per il ripristino, utilizzare l'IP del nodo di amministrazione primario, se disponibile; in caso contrario, utilizzare l'IP di un nodo di amministrazione non primario. a. Selezionare Salva. b. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo Enable Admin Node Discovery (attiva rilevamento nodo amministratore). b. Dall'elenco degli indirizzi IP rilevati, seleziona il nodo di amministrazione per la griglia in cui verrà distribuito questo nodo di archiviazione dell'appliance. Nota: per il ripristino, utilizzare l'IP del nodo di amministrazione primario, se disponibile; in caso contrario, utilizzare l'IP di un nodo di amministrazione non primario. a. Selezionare Salva. b. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".

4. Nel campo **Nome nodo**, inserisci lo stesso hostname (nome di sistema) che hai usato per il nodo che stai recuperando e seleziona **Salva**.
5. Nella sezione Installazione, verifica che lo stato corrente sia "Pronto per avviare l'installazione di *node name* nella griglia con il nodo amministratore primario ``admin_ip``" e che il pulsante **Avvia installazione** sia abilitato.

Se il pulsante **Avvia installazione** non è attivato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Per istruzioni, consultare le istruzioni di manutenzione dell'apparecchio.

6. Dalla home page di StorageGRID Appliance Installer, seleziona **Avvia installazione**.

Lo stato attuale cambia in "Installazione in corso" e viene visualizzata la pagina di installazione del monitor.



Se devi accedere manualmente alla pagina di installazione del Monitor, seleziona **Installazione del Monitor** dalla barra dei menu. Vedi ["Installazione dell'appliance di monitoraggio"](#).

Monitorare l'installazione dell'appliance StorageGRID

Il programma di installazione dell'appliance StorageGRID indica lo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

Fasi

1. Per monitorare l'avanzamento dell'installazione, seleziona **Monitora installazione** dalla barra dei menu.

La pagina di installazione di Monitor mostra lo stato di avanzamento dell'installazione.

La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.



Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta eseguendo nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "saltato".

2. Esaminare i progressi delle prime due fasi dell'installazione.

- **1. Configurare lo storage**

Durante questa fase, il programma di installazione si connette al controller dello storage, cancella qualsiasi configurazione esistente, comunica con il sistema operativo SANtricity per configurare i volumi e configura le impostazioni dell'host.

- **2. Installare il sistema operativo**

In questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID nell'appliance.

3. Continuare a monitorare lo stato di avanzamento dell'installazione fino a quando la fase **Install StorageGRID** (Installazione guidata) non viene interrotta e sulla console integrata viene visualizzato un messaggio che richiede di approvare questo nodo nel nodo di amministrazione utilizzando Gestione griglia.
4. Andare a ["Selezionare Start Recovery \(Avvia ripristino\) per configurare il nodo di storage dell'appliance"](#).

Seleziona Avvia ripristino per configurare il nodo di archiviazione dell'appliance StorageGRID

Selezionare Start Recovery (Avvia ripristino) in Grid Manager (Gestione griglia) per configurare un nodo di storage dell'appliance come sostituzione del nodo guasto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).

- Si dispone della passphrase di provisioning.
- Hai implementato un nodo storage dell'appliance di recovery.
- Si dispone della data di inizio di qualsiasi intervento di riparazione per i dati codificati per la cancellazione.

Fasi

1. Dal Grid Manager, seleziona **Manutenzione > Attività > Ripristino nodo**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Inserisci la **passphrase di provisioning**.
4. Seleziona **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 Recovery Grid Node (nodo griglia di ripristino).
 - Se il nodo della griglia raggiunge la fase "In attesa di passaggi manuali", devi [rimontare e riformattare manualmente i volumi di storage dell'appliance](#).
 - Se il messaggio "In attesa di passaggi manuali" non viene visualizzato, significa che i volumi di archiviazione sono stati rimontati e riformattati automaticamente e puoi [ripristinare i dati degli oggetti nei volumi](#).



In qualsiasi momento durante il ripristino, puoi selezionare **Reset** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo rimarrà in uno stato indeterminato se resetti la procedura.

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo dell'appliance in uno stato preinstallato eseguendo `sgareinstall` sul nodo.

Rimontare e riformattare i volumi di archiviazione dell'appliance StorageGRID (procedura manuale)

Se la procedura automatica non riesce a rimontare i volumi di storage conservati e a riformattare i volumi di storage danneggiati, devi eseguire manualmente due script per

completare queste operazioni. Il primo script rimonta i volumi correttamente formattati come volumi di storage StorageGRID. Il secondo script riformatta eventuali volumi non montati, ricostruisce il database Cassandra, se necessario, e avvia i servizi.

Durante il ripristino di un nodo di archiviazione, se nel Grid Manager viene visualizzato il messaggio "In attesa di passaggi manuali", segui questi passaggi per rimontare e riformattare i volumi di archiviazione. Se non vedi questo messaggio, le operazioni di rimontaggio e riformattazione sono state completate automaticamente e puoi saltare *questa* procedura e ["ripristina i dati dell'oggetto"](#).

Prima di iniziare

- L'hardware è già stato sostituito per tutti i volumi di storage guasti che è necessario sostituire.

L'esecuzione `sn-remount-volumes` dello script può aiutare a identificare volumi di storage aggiuntivi guasti.

- 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. Non eseguire il `sn-recovery-postinstall.sh` sceneggiatura.

A proposito di questa attività

Per completare questa procedura, eseguire le seguenti attività di alto livello:

- Accedere al nodo di storage recuperato.
- Eseguire `sn-remount-volumes` lo script per rimontare volumi di storage formattati correttamente. Quando viene eseguito, lo script esegue le seguenti operazioni:
 - Consente di montare e rimuovere ciascun volume di storage per riprodurre il journal XFS.
 - Esegue un controllo di coerenza del file XFS.
 - Se il file system è coerente, determina se il volume di storage è un volume di storage StorageGRID formattato correttamente.
 - Se il volume di storage è formattato correttamente, esegue il remontaggio del volume di storage. Tutti i dati esistenti sul volume rimangono intatti.
- Esaminare l'output dello script e risolvere eventuali problemi.
- Eseguire `sn-recovery-postinstall.sh` lo script. Quando viene eseguito, lo script 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 guasti e ripristinare i metadati degli oggetti. Il riavvio del nodo di archiviazione prima del `sn-recovery-postinstall.sh` completamento causa errori per i servizi che tentano di avviarsi e causa l'uscita dei nodi di appliance StorageGRID dalla modalità di manutenzione.

- Riformatta tutti i volumi di storage che `sn-remount-volumes` non è stato possibile attivare o che non sono stati formattati correttamente.



Se un volume di storage viene riformattato, tutti i dati presenti in tale volume andranno persi. È necessario eseguire un'ulteriore procedura per ripristinare i dati degli oggetti da altre posizioni nella griglia, supponendo che le regole ILM siano state configurate per memorizzare più copie di un oggetto.

- Ricostruisce il database Cassandra sul nodo, se necessario.
- Avvia i servizi sul nodo di storage.

Fasi

1. Accedere al nodo di storage recuperato:

- Immettere il seguente comando: `ssh admin@grid_node_IP`
- Immettere la password elencata nel `Passwords.txt` file.
- Immettere il seguente comando per passare alla directory principale: `su -`
- Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Eseguire il primo script per rimontare eventuali volumi di storage correttamente formattati.



Se tutti i volumi di storage sono nuovi e devono essere formattati, o se tutti i volumi di storage sono guasti, è possibile saltare questa fase ed eseguire il secondo script per riformattare tutti i volumi di storage non montati.

- Eseguire lo script: `sn-remount-volumes`

Questo script potrebbe richiedere ore per essere eseguito su volumi di storage che contengono dati.

- Durante l'esecuzione dello script, esaminare l'output e rispondere alle 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 log contiene informazioni più dettagliate rispetto all'output della riga di comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully
```

===== Device /dev/sdc =====

Mount and unmount device /dev/sdc and checking file system consistency:

Error: File system consistency check retry failed on device /dev/sdc. You can see the diagnosis information in the /var/local/log/sn-remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-postinstall.sh, this volume and any data on this volume will be deleted. If you only had two copies of object data, you will temporarily have only a single copy.

StorageGRID 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 storage è stato rimontato correttamente e tre volumi di storage hanno avuto errori.

- `/dev/sdb` Ha superato il controllo di coerenza del file system XFS e aveva una struttura di volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi che vengono rimontati dallo script vengono conservati.
- `/dev/sdc` Controllo della coerenza del file system XFS non riuscito perché il volume di archiviazione era nuovo o danneggiato.
- `/dev/sdd` impossibile montare perché il disco non è stato inizializzato o il superblocco del disco è danneggiato. Quando lo script non riesce a montare un volume di storage, chiede se si desidera eseguire il controllo di coerenza del file system.
 - Se il volume di storage è collegato a un nuovo disco, rispondere **N** alla richiesta. Non è necessario controllare il file system su un nuovo disco.
 - Se il volume di storage è collegato a un disco esistente, rispondere **Y** alla richiesta. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I risultati vengono salvati nel `/var/local/log/sn-remount-volumes.log` file di registro.
- `/dev/sde` È stato superato il controllo di coerenza del file system XFS e la struttura del volume era valida; tuttavia, l'ID del nodo LDR nel `volID` file non corrispondeva all'ID per questo nodo di archiviazione (`configured LDR noid` visualizzato in alto). Questo messaggio indica che questo volume appartiene a un altro nodo di storage.

3. Esaminare l'output dello script e risolvere eventuali problemi.



Se un volume di storage non ha superato il controllo di coerenza del file system XFS o non è stato possibile montarlo, esaminare attentamente i messaggi di errore nell'output. È necessario comprendere le implicazioni dell'esecuzione `sn-recovery-postinstall.sh` dello script su questi volumi.

- a. Verificare che i risultati includano una voce per tutti i volumi previsti. Se alcuni volumi non sono elencati, eseguire nuovamente lo script.
- b. Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indichino che un volume di storage non appartiene a questo nodo di storage.

Nell'esempio, l'output per `/dev/sde` include il seguente messaggio di errore:

Error: This volume does not belong to this node. Fix the attached volume and re-run this script.



Se un volume di storage viene segnalato come appartenente a un altro nodo di storage, contattare il supporto tecnico. Se si esegue `sn-recovery-postinstall.sh` lo script, il volume di archiviazione verrà riformattato e ciò potrebbe causare la perdita di dati.

- c. Se non è stato possibile montare alcun dispositivo di storage, annotare il nome del dispositivo e riparare o sostituire il dispositivo.



È necessario riparare o sostituire i dispositivi di storage che non possono essere montati.

- d. Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire `sn-remount-volumes` nuovamente lo script per confermare che tutti i volumi di storage che è possibile rimontare siano stati rimontati.



Se un volume di storage non può essere montato o non è formattato correttamente e si passa alla fase successiva, il volume e i dati presenti nel volume verranno eliminati. Se si dispone di due copie di dati oggetto, si disporrà di una sola copia fino al completamento della procedura successiva (ripristino dei dati oggetto).



Non eseguire `sn-recovery-postinstall.sh` lo script se si ritiene che i dati rimanenti su un volume di storage guasto non possano essere ricostruiti da un'altra parte della griglia (ad esempio, se il criterio ILM utilizza una regola che crea una sola copia o se i volumi non sono riusciti su più nodi). Contattare invece il supporto tecnico per determinare come ripristinare i dati.

4. Eseguire `sn-recovery-postinstall.sh` lo script: `sn-recovery-postinstall.sh`

Questo script riformatta tutti i volumi di storage che non possono essere montati o che sono stati trovati per essere formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; avvia i servizi sul nodo di storage.

Tenere presente quanto segue:

- L'esecuzione dello script potrebbe richiedere ore.
- In generale, si consiglia di lasciare la sessione SSH da sola mentre lo script è in esecuzione.
- Non premere **Ctrl+C** mentre la sessione SSH è attiva.
- Lo script viene eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzarne l'avanzamento dalla pagina Recovery (Ripristino).
- Se Storage Node utilizza il servizio RSM, lo script potrebbe sembrare bloccato per 5 minuti quando i servizi del nodo vengono riavviati. Questo ritardo di 5 minuti è previsto ogni volta che il servizio RSM viene avviato per la prima volta.



Il servizio RSM è presente sui nodi di storage che includono il servizio ADC.



Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. Durante l'esecuzione dello script `sn-recovery-postinstall.sh`, monitorare la pagina di ripristino in Grid Manager.

La barra di avanzamento e la colonna fase nella pagina Ripristino forniscono uno stato di alto livello `sn-recovery-postinstall.sh` dello script.

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 che lo script `sn-recovery-postinstall.sh` ha avviato i servizi sul nodo, è possibile ripristinare i dati degli oggetti in qualsiasi volume di storage formattato dallo script.

Lo script chiede se vuoi usare il processo di ripristino del volume di Grid Manager per ripristinare i dati degli oggetti.

- Nella maggior parte dei casi, dovresti ["Ripristinare i dati degli oggetti utilizzando Grid Manager"](#). Rispondi `y` per utilizzare Grid Manager.
- In rari casi, ad esempio quando sai che il nodo sostitutivo ha meno volumi disponibili per lo storage a oggetti rispetto al nodo originale, contatta il supporto tecnico per ripristinare manualmente i dati degli oggetti. Se si verifica uno di questi casi, rispondi `n` e premi un tasto qualsiasi per tornare alla riga di comando.

Ripristinare i dati degli oggetti in un volume di archiviazione per un'appliance StorageGRID

Dopo il ripristino dei volumi di storage per il nodo di storage dell'appliance, è possibile ripristinare i dati degli oggetti replicati o codificati in cancellazione che sono stati persi in caso di guasto del nodo di storage.

Prima di iniziare

- Se la procedura automatica non è riuscita a rimontare i volumi di archiviazione conservati e a riformattare i volumi di archiviazione danneggiati, hai eseguito una di queste procedure:
 - ["Rimontare e riformattare i volumi di storage delle appliance \(procedura manuale\)"](#)

- ["Rimontare e riformattare i volumi di storage \(procedura manuale\)"](#)

- Hai verificato che il nodo di archiviazione su cui stai ripristinando gli oggetti ha uno stato di connessione **Connesso**  nella scheda **Nodi > Panoramica** del Grid Manager.
- Hai confermato quanto segue:
 - Non è in corso un'espansione della griglia per aggiungere un nodo di archiviazione Storage Node.
 - Un decommission di Storage Node non è in corso o non è fallito.
 - Il ripristino di un volume di archiviazione danneggiato non è in corso.
 - Il ripristino di un nodo di Storage con un'unità di sistema guasta non è in corso.
 - Non è in corso alcuna operazione di ribilanciamento EC.
 - La clonazione del nodo dell'appliance non è in corso.

A proposito di questa attività

Dopo che hai sostituito le unità e i volumi sono stati formattati, Grid Manager visualizza i volumi come candidati per il ripristino nella scheda **Manutenzione > Ripristino volumi > Nodi da ripristinare**.

Se possibile, ripristinare i dati degli oggetti utilizzando la pagina di ripristino del volume in Grid Manager. È possibile [attivare la modalità di ripristino automatico](#) avviare automaticamente il ripristino del volume quando i volumi sono pronti per essere ripristinati o [eseguire manualmente il ripristino del volume](#). Attenersi alle seguenti linee guida:

- Se i volumi sono elencati in **Manutenzione > Ripristino volumi > Nodi da ripristinare**, ripristinare i dati dell'oggetto come descritto nei passaggi seguenti. I volumi saranno elencati se:
 - Alcuni, ma non tutti, volumi di storage in un nodo sono guasti
 - Tutti i volumi di storage in un nodo sono guasti e vengono sostituiti con lo stesso numero di volumi o più volumi

La pagina di ripristino del volume in Grid Manager consente inoltre di [monitorare il processo di ripristino del volume](#) e [visualizzare la cronologia del ripristino](#).

Se il nodo di archiviazione ripristinato contiene meno volumi rispetto al nodo che sta sostituendo, contatta il supporto tecnico per assistenza.

È possibile ripristinare due tipi di dati oggetto:

- Gli oggetti dati replicati vengono ripristinati da altre posizioni, supponendo che le regole ILM della griglia siano state configurate per rendere disponibili le copie degli oggetti.
 - Se una regola ILM è stata configurata per memorizzare una sola copia replicata e tale copia si trovava su un volume di archiviazione che ha subito un errore, non potrai recuperare l'oggetto.
 - Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto.
- Gli oggetti dati con erasure coding (EC) vengono ripristinati ri assemblando i frammenti memorizzati. I frammenti corrotti o persi vengono ricreati dall'algoritmo di erasure coding dai dati rimanenti e dai frammenti di parità.

Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati sottoposti a erasure coding, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.



Il ripristino dei volumi dipende dalla disponibilità delle risorse in cui sono memorizzate le copie a oggetti. L'avanzamento del ripristino dei volumi non è lineare e potrebbe richiedere giorni o settimane.

attiva la modalità di ripristino automatico

Quando si attiva la modalità di ripristino automatico, il ripristino del volume si avvia automaticamente quando i volumi sono pronti per essere ripristinati.

Fasi

1. In Grid Manager 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 potrai avviare manualmente i processi di ripristino del volume su nessun nodo.
- I ripristini del volume inizieranno automaticamente solo quando non sono in corso altre procedure di manutenzione.
- È possibile monitorare lo stato del lavoro dalla pagina di monitoraggio dell'avanzamento.
- StorageGRID ritenta automaticamente il ripristino del volume che non si avvia.

4. Una volta compresi i risultati dell'attivazione della modalità di ripristino automatico, selezionare **Sì** nella finestra di dialogo di conferma.

È possibile disattivare la modalità di ripristino automatico in qualsiasi momento.

Ripristino manuale di un volume o nodo non riuscito

Per ripristinare un volume o un nodo guasto, procedere come segue.

Fasi

1. In Grid Manager vai su **Manutenzione > Ripristino volume**.
2. Selezionare la scheda **nodi da ripristinare**, quindi far scorrere l'interruttore per **modalità di ripristino automatico** sulla posizione disattivata.

Il numero sulla scheda indica il numero di nodi con volumi che richiedono il ripristino.

3. Espandere ciascun nodo per visualizzare i volumi in esso che richiedono il ripristino e il relativo stato.
4. Correggere eventuali problemi che impediscono il ripristino di ciascun volume. I problemi saranno indicati quando si seleziona **in attesa di passaggi manuali**, se viene visualizzato come stato del volume.
5. Selezionare un nodo da ripristinare in cui tutti i volumi indicano uno stato Pronto per il ripristino.

È possibile ripristinare i volumi solo per un nodo alla volta.

Ciascun volume nel nodo deve indicare che è pronto per il ripristino.

6. Selezionare **Avvia ripristino**.
7. Risolvere eventuali avvisi che potrebbero essere visualizzati o selezionare **Avvia comunque** per ignorare gli avvisi e avviare il ripristino.

I nodi vengono spostati dalla scheda **Nodes to restore** (nodi da ripristinare) alla scheda **Restoration Progress** (avanzamento ripristino) all'avvio del ripristino.

Se non è possibile avviare il ripristino di un volume, il nodo torna alla scheda **nodi da ripristinare**.

Visualizza l'avanzamento del ripristino

La scheda **Restoration Progress** (avanzamento ripristino) mostra lo stato del processo di ripristino del volume e le informazioni sui volumi di un nodo da ripristinare.

I tassi di riparazione dei dati per gli oggetti replicati e codificati per la cancellazione in tutti i volumi sono medie che riassumono tutti i restauri in corso. Viene inoltre indicata la % di oggetti in tali volumi che sono integri e non richiedono restauro.



Il ripristino dei dati replicati dipende dalla disponibilità delle risorse in cui sono memorizzate le copie replicate. L'avanzamento del ripristino dei dati replicati non è lineare e potrebbe richiedere giorni o settimane.

La sezione lavori di ripristino visualizza informazioni sui ripristini dei volumi avviati da Grid Manager.

- Il numero nell'intestazione della sezione lavori di ripristino indica il numero di volumi che vengono ripristinati o messi in coda per il ripristino.
- La tabella visualizza le informazioni relative a ciascun volume di un nodo da ripristinare e al relativo stato di avanzamento.
 - L'avanzamento per ciascun nodo visualizza la percentuale per ciascun lavoro.
 - Espandere la colonna Dettagli per visualizzare l'ora di inizio del ripristino e l'ID del processo.
- Se il ripristino di un volume non riesce:
 - La colonna Stato indica `failed (attempting retry)`, e verrà riavviata automaticamente.
 - Se più lavori di ripristino non hanno avuto esito positivo, il lavoro più recente verrà rielaborato automaticamente per primo.
 - L'avviso **guasto riparazione EC** viene attivato se i tentativi continuano a non riuscire. Per risolvere il problema, attenersi alla procedura riportata nell'avviso.

Visualizza la cronologia del ripristino

La scheda **Restoration history** (Cronologia ripristino) mostra informazioni su tutti i ripristini dei volumi completati correttamente.



Le dimensioni non sono applicabili agli oggetti replicati e vengono visualizzate solo per i ripristini che contengono oggetti di dati EC (erasure coding).

Verifica lo stato dello storage dopo il ripristino di un nodo di storage dell'appliance StorageGRID

Dopo aver ripristinato un nodo di storage dell'appliance, è necessario verificare che lo stato desiderato del nodo di storage dell'appliance sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che si riavvia il server del nodo di storage.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **Nodi > Nodo di archiviazione_ > Attività**.
2. Se l'elenco a discesa **Stato di archiviazione** è impostato su Sola lettura o Offline, selezionare **Online**.
3. Selezionare **Salva**.

Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto

Avvisi per il ripristino dei volumi di storage StorageGRID

Prima di ripristinare volumi di archiviazione non riusciti per un nodo di archiviazione, esaminare i seguenti avvisi.

I volumi di storage (o rangedb) in un nodo di storage sono identificati da un numero esadecimale, noto come ID del volume. Ad esempio, 0000 è il primo volume e 000F è il sedicesimo volume. Il primo archivio di oggetti (volume 0) su ciascun nodo di storage utilizza fino a 4 TB di spazio per i metadati degli oggetti e le operazioni del database Cassandra; qualsiasi spazio rimanente su tale volume viene utilizzato per i dati degli oggetti. Tutti gli altri volumi di storage vengono utilizzati esclusivamente per i dati a oggetti.

Il database Cassandra potrebbe essere ricostruito come parte della procedura di ripristino del volume se:

- Il volume 0 non funziona e viene recuperato.
- Il disco di sistema e uno o più volumi di storage si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di archiviazione. Se Cassandra è stata ricostruita di recente, i dati di Cassandra potrebbero non essere ancora coerenti in tutta la griglia. Se troppi nodi di archiviazione sono offline:

- Alcuni dati di Cassandra potrebbero non essere disponibili.
- Potrebbe verificarsi una perdita di dati.



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. Per ulteriori informazioni, fare riferimento a ["Come il supporto tecnico recupera un sito"](#).



Se le regole ILM sono configurate per archiviare una sola 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 grid"](#)

Identifica e smonta i volumi di storage non funzionanti in StorageGRID

Durante il ripristino di un nodo di storage con volumi di storage guasti, è necessario identificare e smontare i volumi guasti. È necessario verificare che solo i volumi di storage guasti vengano riformattati come parte della procedura di ripristino.

Prima di iniziare

L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).

A proposito di questa attività

È necessario ripristinare i volumi di storage guasti il prima possibile.

La prima fase del processo di ripristino consiste nel rilevare i volumi che sono stati scollegati, che devono essere disinstallati o che presentano errori di i/O. Se i volumi guasti sono ancora collegati ma hanno un file system corrotto in modo casuale, il sistema potrebbe non rilevare alcun danneggiamento nelle parti del disco non utilizzate o non allocate.



È necessario completare questa procedura prima di eseguire la procedura manuale per ripristinare i volumi, ad esempio aggiungere o ricollegare i dischi, arrestare il nodo, avviare il nodo o riavviare. In caso contrario, quando si esegue `reformat_storage_block_devices.rb` lo script, potrebbe verificarsi un errore del file system che causa il blocco o l'errore dello script.



Riparare l'hardware e collegare correttamente i dischi prima di eseguire il `reboot` comando.



Identificare con attenzione i volumi di storage guasti. Queste informazioni verranno utilizzate per verificare quali volumi devono essere riformattati. Dopo la riformattazione di un volume, i dati del volume non possono essere recuperati.

Per ripristinare 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 punto di montaggio, il nome del dispositivo e le dimensioni del volume vengono visualizzati in Grid Manager.

Fasi

1. Completare i seguenti passaggi per registrare i volumi di storage guasti e i relativi nomi dei dispositivi:
 - a. Selezionare **Nodi > sito > Nodo di archiviazione non riuscito > Archiviazione**.
 - b. Scorrere verso il basso per individuare la tabella Volumi e la tabella Archivi oggetti e registrare le seguenti informazioni per ciascun volume con stato Sconosciuto o Offline.
 - Dalla tabella Volumi, registrare il punto di montaggio, il dispositivo e la dimensione.
 - Dalla tabella degli archivi degli oggetti, registrare il `object_store_ID`.

``object_store_ID`` È l'ID del volume di archiviazione guasto. Ad esempio, specificare ``0`` nel comando un archivio oggetti con ID 0000.

2. Accedere al nodo di storage guasto:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

3. Eseguire il seguente script per smontare un volume di storage guasto:

```
sn-unmount-volume object_store_ID
```

4. Se richiesto, premere **y** per arrestare il servizio Cassandra a seconda del volume di storage 0.



Se il servizio Cassandra è già stato arrestato, non viene richiesto. Il servizio Cassandra viene arrestato solo per il volume 0.

```
root@Storage-180:~/var/local/tmp/storage~ # sn-unmount-volume 0
Services depending on storage volume 0 (cassandra) aren't down.
Services depending on storage volume 0 must be stopped before running
this script.
Stop services that require storage volume 0 [y/N]? y
Shutting down services that require storage volume 0.
Services requiring storage volume 0 stopped.
Unmounting /var/local/rangedb/0
/var/local/rangedb/0 is unmounted.
```

In pochi secondi, il volume viene smontato. Vengono visualizzati messaggi che indicano ogni fase del processo. Il messaggio finale indica che il volume è stato smontato.

5. Se la disinstallazione non riesce perché il volume è occupato, è possibile forzare la disinstallazione utilizzando l' `--use-umountof` opzione:



La forzatura di un'operazione di disinstallazione mediante l' `--use-umountof` opzione potrebbe causare il comportamento imprevisto o il blocco dei processi o dei servizi che utilizzano il volume.

```
root@Storage-180:~ # sn-unmount-volume --use-umountof
/var/local/rangedb/2
Unmounting /var/local/rangedb/2 using umountof
/var/local/rangedb/2 is unmounted.
Informing LDR service of changes to storage volumes
```

Recupera i volumi di storage danneggiati e ricostruisci il database Cassandra in StorageGRID

È necessario eseguire uno script che riformatta e rimontana lo storage su volumi di storage guasti e ricostruisce il database Cassandra sul nodo di storage, se il sistema lo ritiene necessario.

Prima di iniziare

- Si dispone del `Passwords.txt` file.
- I dischi di sistema sul server sono intatti.
- La causa del guasto è stata identificata e, se necessario, l'hardware di storage sostitutivo è già stato acquistato.
- Le dimensioni totali dello storage sostitutivo sono le stesse dell'originale.
- 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.**)
- Si dispone di ["analisi degli avvisi relativi al ripristino del volume di storage"](#).

Fasi

1. Se necessario, sostituire lo storage fisico o virtuale guasto associato ai volumi di storage guasti identificati e non montati in precedenza.

Non rimontare i volumi in questa fase. L'archiviazione viene rimontata e aggiunta a `/etc/fstab` in un passaggio successivo.

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. Accedere al nodo di storage guasto:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati 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 salvare il file.



Il commento di un volume non riuscito nel file `/etc/fstab` è sufficiente. Il volume deve essere eliminato da `fstab` poiché il processo di ripristino verifica che tutte le righe nel `fstab` file corrispondano ai file system montati.

5. Riformattare eventuali volumi di storage guasti e ricostruire il database Cassandra, se necessario.

Immettere: `reformat_storage_block_devices.rb`

- Quando il volume di storage 0 viene smontato, vengono visualizzati messaggi e messaggi che indicano che il servizio Cassandra è in fase di arresto.
- Se necessario, viene richiesto di ricostruire il database Cassandra.

- Esaminare gli avvisi. Se non sono applicabili, ricostruire il database Cassandra. Immettere: **Y**
- Se più di un nodo di archiviazione è offline. Inserisci: **n**

Lo script verrà chiuso senza ricostruire Cassandra. Contattare il supporto tecnico.

- Per ogni unità rangedb sul nodo di archiviazione, quando viene richiesto:, Immettere una delle seguenti risposte: Reformat the rangedb drive <name> (device <major number>:<minor number>)? [y/n]?

- **y** per riformattare un disco con errori. In questo modo, il volume di archiviazione viene riformattato e il volume di archiviazione riformattato viene aggiunto al `/etc/fstab` file.
- **n** se il disco non contiene errori e non si desidera riformattarlo.



Selezionando **n** si esce dallo script. Montare il disco (se si ritiene che i dati sul disco debbano essere conservati e il disco non è stato montato per errore) oppure rimuoverlo. Quindi, eseguire nuovamente il `reformat_storage_block_devices.rb` comando.



Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

Nell'output di esempio seguente, l'unità `/dev/sdf` deve essere riformattata e Cassandra non ha 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 b951bfcb-4804-41ad-b490-
805dfd8df16c
All devices processed
Running: /usr/local/ldr/setup_rangedb.sh 12368435
Cassandra does not need rebuilding.
Starting services.
Informing storage services of new volume

Reformatting done. Now do manual steps to
restore copies of data.
```

E ora?

Dopo che i volumi di archiviazione sono stati riformattati e rimontati e le operazioni Cassandra necessarie sono state completate, puoi ["Ripristinare i dati degli oggetti utilizzando Grid Manager"](#).

Ripristina i dati dell'oggetto nel volume di archiviazione StorageGRID dove l'unità di sistema è intatta

Dopo il ripristino di un volume di storage su un nodo di storage in cui il disco di sistema è intatto, è possibile ripristinare i dati degli oggetti replicati o codificati in cancellazione che sono stati persi in caso di guasto del volume di storage.

Prima di iniziare

- Se la procedura automatica non è riuscita a rimontare i volumi di archiviazione conservati e a riformattare i volumi di archiviazione danneggiati, hai eseguito una di queste procedure:
 - ["Rimontare e riformattare i volumi di storage delle appliance \(procedura manuale\)"](#)
 - ["Rimontare e riformattare i volumi di storage \(procedura manuale\)"](#)
- Hai verificato che il nodo di archiviazione su cui stai ripristinando gli oggetti ha uno stato di connessione **Connesso**  nella scheda **Nodi > Panoramica** del Grid Manager.
- Hai confermato quanto segue:
 - Non è in corso un'espansione della griglia per aggiungere un nodo di archiviazione Storage Node.
 - Un decommission di Storage Node non è in corso o non è fallito.
 - Il ripristino di un volume di archiviazione danneggiato non è in corso.
 - Il ripristino di un nodo di Storage con un'unità di sistema guasta non è in corso.
 - Non è in corso alcuna operazione di ribilanciamento EC.
 - La clonazione del nodo dell'appliance non è in corso.

A proposito di questa attività

Dopo che hai sostituito le unità e i volumi sono stati formattati, Grid Manager visualizza i volumi come candidati per il ripristino nella scheda **Manutenzione > Ripristino volumi > Nodi da ripristinare**.

Se possibile, ripristinare i dati degli oggetti utilizzando la pagina di ripristino del volume in Grid Manager. È possibile [attivare la modalità di ripristino automatico](#) avviare automaticamente il ripristino del volume quando i volumi sono pronti per essere ripristinati o [eseguire manualmente il ripristino del volume](#). Attenersi alle seguenti linee guida:

- Se i volumi sono elencati in **Manutenzione > Ripristino volumi > Nodi da ripristinare**, ripristinare i dati dell'oggetto come descritto nei passaggi seguenti. I volumi saranno elencati se:
 - Alcuni, ma non tutti, volumi di storage in un nodo sono guasti
 - Tutti i volumi di storage in un nodo sono guasti e vengono sostituiti con lo stesso numero di volumi o più volumi

La pagina di ripristino del volume in Grid Manager consente inoltre di [monitorare il processo di ripristino del volume](#) e [visualizzare la cronologia del ripristino](#).

Se il nodo di archiviazione ripristinato contiene meno volumi rispetto al nodo che sta sostituendo, contatta il supporto tecnico per assistenza.

È possibile ripristinare due tipi di dati oggetto:

- Gli oggetti dati replicati vengono ripristinati da altre posizioni, supponendo che le regole ILM della griglia siano state configurate per rendere disponibili le copie degli oggetti.

- Se una regola ILM è stata configurata per memorizzare una sola copia replicata e tale copia si trovava su un volume di archiviazione che ha subito un errore, non potrai recuperare l'oggetto.
- Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto.
- Gli oggetti dati con erasure coding (EC) vengono ripristinati ri assemblando i frammenti memorizzati. I frammenti corrotti o persi vengono ricreati dall'algoritmo di erasure coding dai dati rimanenti e dai frammenti di parità.

Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati sottoposti a erasure coding, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.



Il ripristino dei volumi dipende dalla disponibilità delle risorse in cui sono memorizzate le copie a oggetti. L'avanzamento del ripristino dei volumi non è lineare e potrebbe richiedere giorni o settimane.

attiva la modalità di ripristino automatico

Quando si attiva la modalità di ripristino automatico, il ripristino del volume si avvia automaticamente quando i volumi sono pronti per essere ripristinati.

Fasi

1. In Grid Manager 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 potrai avviare manualmente i processi di ripristino del volume su nessun nodo.
- I ripristini del volume inizieranno automaticamente solo quando non sono in corso altre procedure di manutenzione.
- È possibile monitorare lo stato del lavoro dalla pagina di monitoraggio dell'avanzamento.
- StorageGRID ritenta automaticamente il ripristino del volume che non si avvia.

4. Una volta compresi i risultati dell'attivazione della modalità di ripristino automatico, selezionare **Sì** nella finestra di dialogo di conferma.

È possibile disattivare la modalità di ripristino automatico in qualsiasi momento.

Ripristino manuale di un volume o nodo non riuscito

Per ripristinare un volume o un nodo guasto, procedere come segue.

Fasi

1. In Grid Manager vai su **Manutenzione > Ripristino volume**.
2. Selezionare la scheda **nodi da ripristinare**, quindi far scorrere l'interruttore per **modalità di ripristino automatico** sulla posizione disattivata.

Il numero sulla scheda indica il numero di nodi con volumi che richiedono il ripristino.

3. Espandere ciascun nodo per visualizzare i volumi in esso che richiedono il ripristino e il relativo stato.
4. Correggere eventuali problemi che impediscono il ripristino di ciascun volume. I problemi saranno indicati quando si seleziona **in attesa di passaggi manuali**, se viene visualizzato come stato del volume.
5. Selezionare un nodo da ripristinare in cui tutti i volumi indicano uno stato Pronto per il ripristino.

È possibile ripristinare i volumi solo per un nodo alla volta.

Ciascun volume nel nodo deve indicare che è pronto per il ripristino.

6. Selezionare **Avvia ripristino**.
7. Risolvere eventuali avvisi che potrebbero essere visualizzati o selezionare **Avvia comunque** per ignorare gli avvisi e avviare il ripristino.

I nodi vengono spostati dalla scheda **Nodes to restore** (nodi da ripristinare) alla scheda **Restoration Progress** (avanzamento ripristino) all'avvio del ripristino.

Se non è possibile avviare il ripristino di un volume, il nodo torna alla scheda **nodi da ripristinare**.

Visualizza l'avanzamento del ripristino

La scheda **Restoration Progress** (avanzamento ripristino) mostra lo stato del processo di ripristino del volume e le informazioni sui volumi di un nodo da ripristinare.

I tassi di riparazione dei dati per gli oggetti replicati e codificati per la cancellazione in tutti i volumi sono medie che riassumono tutti i restauri in corso. Viene inoltre indicata la % di oggetti in tali volumi che sono integri e non richiedono restauro.



Il ripristino dei dati replicati dipende dalla disponibilità delle risorse in cui sono memorizzate le copie replicate. L'avanzamento del ripristino dei dati replicati non è lineare e potrebbe richiedere giorni o settimane.

La sezione lavori di ripristino visualizza informazioni sui ripristini dei volumi avviati da Grid Manager.

- Il numero nell'intestazione della sezione lavori di ripristino indica il numero di volumi che vengono ripristinati o messi in coda per il ripristino.
- La tabella visualizza le informazioni relative a ciascun volume di un nodo da ripristinare e al relativo stato di avanzamento.
 - L'avanzamento per ciascun nodo visualizza la percentuale per ciascun lavoro.
 - Espandere la colonna Dettagli per visualizzare l'ora di inizio del ripristino e l'ID del processo.
- Se il ripristino di un volume non riesce:
 - La colonna Stato indica `failed (attempting retry)`, e verrà riavviata automaticamente.
 - Se più lavori di ripristino non hanno avuto esito positivo, il lavoro più recente verrà rielaborato automaticamente per primo.
 - L'avviso **guasto riparazione EC** viene attivato se i tentativi continuano a non riuscire. Per risolvere il problema, attenersi alla procedura riportata nell'avviso.

Visualizza la cronologia del ripristino

La scheda **Restoration history** (Cronologia ripristino) mostra informazioni su tutti i ripristini dei volumi completati correttamente.



Le dimensioni non sono applicabili agli oggetti replicati e vengono visualizzate solo per i ripristini che contengono oggetti di dati EC (erasure coding).

Verifica lo stato dello storage dopo il ripristino dei volumi di storage StorageGRID

Dopo il ripristino dei volumi di storage, è necessario verificare che lo stato desiderato del nodo di storage sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che si riavvia il server del nodo di storage.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **Nodi > Nodo di archiviazione_ > Attività**.
2. Se l'elenco a discesa **Stato di archiviazione** è impostato su Sola lettura o Offline, selezionare **Online**.
3. Selezionare **Salva**.

Ripristino in caso di guasto al disco di sistema

Avvisi per il ripristino dell'unità di sistema del nodo di storage StorageGRID

Prima di ripristinare un'unità di sistema guasta di un nodo di archiviazione, esaminare le avvertenze generali ["avvertenze e considerazioni per il ripristino del nodo grid"](#) e specifiche riportate di seguito.

I nodi di archiviazione dispongono di un database Cassandra che include metadati degli oggetti. Il database Cassandra potrebbe essere ricostruito se:

- Un volume di archiviazione si guasta e viene recuperato.
- Il disco di sistema e uno o più volumi di storage si guastano e vengono ripristinati.

Quando Cassandra viene ricostruita, il sistema utilizza le informazioni provenienti da altri nodi di archiviazione. Se Cassandra è stata ricostruita di recente, i dati di Cassandra potrebbero non essere ancora coerenti in tutta la griglia. Se troppi nodi di archiviazione sono offline:

- Alcuni dati di Cassandra potrebbero non essere disponibili.
- Potrebbe verificarsi una perdita di dati.



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. Per ulteriori informazioni, fare riferimento a ["Come il supporto tecnico recupera un sito"](#).



Se questo Storage Node è in modalità di manutenzione di sola lettura per consentire il recupero degli oggetti da parte di un altro Storage Node con volumi di storage guasti, ripristina i volumi sullo Storage Node con volumi di storage guasti prima di ripristinare questo Storage Node guasto. Vedi le istruzioni per ["ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto"](#).



Se le regole ILM sono configurate in modo da memorizzare una sola copia replicata e la copia esiste su un volume di storage che ha avuto esito negativo, non sarà possibile ripristinare l'oggetto.

Sostituire il nodo di storage StorageGRID

Se il disco di sistema presenta un guasto, è necessario sostituire il nodo di storage.

Selezionare la procedura di sostituzione del nodo per la piattaforma. I passaggi per sostituire un nodo sono gli stessi per tutti i tipi di nodi griglia.



Questa procedura si applica solo ai nodi di storage basati su software. È necessario seguire una procedura diversa da ["Ripristinare un nodo di storage dell'appliance"](#).

Linux: se non si è sicuri che il disco di sistema sia guasto, seguire le istruzioni per sostituire il nodo per determinare quali passaggi di ripristino sono necessari.

Piattaforma	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux" .

Seleziona Avvia ripristino per configurare il nodo di archiviazione StorageGRID

Dopo aver sostituito un nodo di storage, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.
- Si dispone della data di inizio di qualsiasi intervento di riparazione per i dati codificati per la cancellazione.

A proposito di questa attività

Se Storage Node è installato come container su un host Linux, eseguire questa operazione solo se si verifica una delle seguenti condizioni:

- È stato necessario utilizzare il `--force` flag per importare il nodo o è stato emesso `storagegrid node force-recovery node-name`
- Era necessario eseguire una reinstallazione completa del nodo oppure ripristinare `/var/local`.

Fasi

1. Accedi al nodo amministratore principale. Se il nodo amministratore principale non è disponibile, usa un nodo amministratore non primario, se presente.
2. Dal Grid Manager, seleziona **Manutenzione > Attività > Ripristino nodo**.
3. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

4. Inserisci la **passphrase di provisioning**.
5. Fai clic su **Avvia ripristino**.
6. Monitora l'avanzamento del ripristino selezionando **Manutenzione > Attività > Ripristino nodo** e visualizzando l'avanzamento del ripristino.
 - Se il nodo della griglia raggiunge la fase "In attesa di passaggi manuali", devi ["rimontare e riformattare manualmente i volumi di archiviazione"](#). Al termine dei passaggi manuali, procedi a ["ripristinare i dati degli oggetti nei volumi"](#).
 - Se il ripristino del nodo della griglia è passato dallo stato **In corso** allo stato **Ripristinato** senza passare attraverso la fase "In attesa di interventi manuali", non è richiesta alcuna ulteriore azione.



In qualsiasi momento durante il ripristino, puoi selezionare **Reset** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo rimarrà in uno stato indeterminato se resetti la procedura.

Se vuoi riprovare il ripristino dopo aver reimpostato la procedura, devi riportare il nodo dell'appliance a uno stato pre-installazione, come segue:

- **VMware:** Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux:** Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`

Rimontare e riformattare i volumi di storage StorageGRID (procedura manuale)

Se la procedura automatica non riesce a rimontare i volumi di storage conservati e a riformattare i volumi di storage danneggiati, devi eseguire manualmente due script per completare queste operazioni. Il primo script rimonta i volumi correttamente formattati come volumi di storage StorageGRID. Il secondo script riformatta eventuali volumi non montati, ricostruisce il database Cassandra, se necessario, e avvia i servizi.

Durante il ripristino di un nodo di archiviazione, se nel Grid Manager viene visualizzato il messaggio "In attesa di passaggi manuali", segui questi passaggi per rimontare e riformattare i volumi di archiviazione. Se non vedi questo messaggio, le operazioni di rimontaggio e riformattazione sono state completate automaticamente e puoi saltare *questa* procedura e ["ripristinare i dati dell'oggetto"](#).

Prima di iniziare

- L'hardware è già stato sostituito per tutti i volumi di storage guasti che è necessario sostituire.

L'esecuzione `sn-remount-volumes` dello script può aiutare a identificare volumi di storage aggiuntivi guasti.

- 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.**)
- Si dispone di "[Esamine le avvertenze relative al ripristino del disco di sistema Storage Node](#)".



Contattare l'assistenza tecnica se più di un nodo di archiviazione è offline. Non eseguire il `sn-recovery-postinstall.sh` sceneggiatura.

A proposito di questa attività

Per completare questa procedura, eseguire le seguenti attività di alto livello:

- Accedere al nodo di storage recuperato.
- Eseguire `sn-remount-volumes` lo script per rimontare volumi di storage formattati correttamente. Quando viene eseguito, lo script esegue le seguenti operazioni:
 - Consente di montare e rimuovere ciascun volume di storage per riprodurre il journal XFS.
 - Esegue un controllo di coerenza del file XFS.
 - Se il file system è coerente, determina se il volume di storage è un volume di storage StorageGRID formattato correttamente.
 - Se il volume di storage è formattato correttamente, esegue il remontaggio del volume di storage. Tutti i dati esistenti sul volume rimangono intatti.
- Esaminare l'output dello script e risolvere eventuali problemi.
- Eseguire `sn-recovery-postinstall.sh` lo script. Quando viene eseguito, lo script 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 guasti e ripristinare i metadati degli oggetti. Il riavvio del nodo di archiviazione prima del `sn-recovery-postinstall.sh` completamento causa errori per i servizi che tentano di avviarsi e causa l'uscita dei nodi di appliance StorageGRID dalla modalità di manutenzione. Vedere il passo per [script post-installazione](#).

- Riformatta tutti i volumi di storage che `sn-remount-volumes` non è stato possibile attivare o che non sono stati formattati correttamente.



Se un volume di storage viene riformattato, tutti i dati presenti in tale volume andranno persi. È necessario eseguire un'ulteriore procedura per ripristinare i dati degli oggetti da altre posizioni nella griglia, supponendo che le regole ILM siano state configurate per memorizzare più copie di un oggetto.

- Ricostruisce il database Cassandra sul nodo, se necessario.
- Avvia i servizi sul nodo di storage.

Fasi

1. Accedere al nodo di storage recuperato:

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Eseguire il primo script per rimontare eventuali volumi di storage correttamente formattati.



Se tutti i volumi di storage sono nuovi e devono essere formattati, o se tutti i volumi di storage sono guasti, è possibile saltare questa fase ed eseguire il secondo script per riformattare tutti i volumi di storage non montati.

- a. Eseguire lo script: `sn-remount-volumes`

Questo script potrebbe richiedere ore per essere eseguito su volumi di storage che contengono dati.

- b. Durante l'esecuzione dello script, esaminare l'output e rispondere alle richieste.



Se necessario, è possibile utilizzare il `tail -f` comando per monitorare il contenuto del file di registro dello script (`/var/local/log/sn-remount-volumes.log`). Il file di log contiene informazioni più dettagliate rispetto all'output della riga di comando.

```
root@SG:~ # sn-remount-volumes
The configured LDR noid is 12632740

===== Device /dev/sdb =====
Mount and unmount device /dev/sdb and checking file system
consistency:
The device is consistent.
Check rangedb structure on device /dev/sdb:
Mount device /dev/sdb to /tmp/sdb-654321 with rangedb mount options
This device has all rangedb directories.
Found LDR node id 12632740, volume number 0 in the volID file
Attempting to remount /dev/sdb
Device /dev/sdb remounted successfully

===== Device /dev/sdc =====
Mount and unmount device /dev/sdc and checking file system
consistency:
Error: File system consistency check retry failed on device /dev/sdc.
You can see the diagnosis information in the /var/local/log/sn-
remount-volumes.log.

This volume could be new or damaged. If you run sn-recovery-
postinstall.sh,
this volume and any data on this volume will be deleted. If you only
```

had two
copies of object data, you will temporarily have only a single copy.
StorageGRID 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 storage è stato rimontato correttamente e tre volumi di storage hanno avuto errori.

- /dev/sdb Ha superato il controllo di coerenza del file system XFS e aveva una struttura di volume valida, quindi è stato rimontato correttamente. I dati sui dispositivi che vengono rimontati dallo script vengono conservati.
- /dev/sdc Controllo della coerenza del file system XFS non riuscito perché il volume di archiviazione era nuovo o danneggiato.
- /dev/sdd impossibile montare perché il disco non è stato inizializzato o il superblocco del disco è danneggiato. Quando lo script non riesce a montare un volume di storage, chiede se si desidera eseguire il controllo di coerenza del file system.
 - Se il volume di storage è collegato a un nuovo disco, rispondere **N** alla richiesta. Non è necessario controllare il file system su un nuovo disco.
 - Se il volume di storage è collegato a un disco esistente, rispondere **Y** alla richiesta. È possibile utilizzare i risultati del controllo del file system per determinare l'origine del danneggiamento. I risultati vengono salvati nel /var/local/log/sn-remount-volumes.log file di registro.
- /dev/sde È stato superato il controllo di coerenza del file system XFS e la struttura del volume era valida; tuttavia, l'ID del nodo LDR nel file volID non corrispondeva all'ID di questo nodo di archiviazione (`configured LDR noid` visualizzato in alto). Questo messaggio indica che questo volume appartiene a un altro nodo di storage.

3. Esaminare l'output dello script e risolvere eventuali problemi.



Se un volume di storage non ha superato il controllo di coerenza del file system XFS o non è stato possibile montarlo, esaminare attentamente i messaggi di errore nell'output. È necessario comprendere le implicazioni dell'esecuzione `sn-recovery-postinstall.sh` dello script su questi volumi.

- a. Verificare che i risultati includano una voce per tutti i volumi previsti. Se alcuni volumi non sono elencati, eseguire nuovamente lo script.
- b. Esaminare i messaggi per tutti i dispositivi montati. Assicurarsi che non vi siano errori che indichino che un volume di storage non appartiene a questo nodo di storage.

Nell'esempio, l'output per `/dev/sde` include il seguente messaggio di errore:

```
Error: This volume does not belong to this node. Fix the attached
volume and re-run this script.
```



Se un volume di storage viene segnalato come appartenente a un altro nodo di storage, contattare il supporto tecnico. Se si esegue `sn-recovery-postinstall.sh` lo script, il volume di archiviazione verrà riformattato e ciò potrebbe causare la perdita di dati.

- c. Se non è stato possibile montare alcun dispositivo di storage, annotare il nome del dispositivo e riparare o sostituire il dispositivo.



È necessario riparare o sostituire i dispositivi di storage che non possono essere montati.

- d. Dopo aver riparato o sostituito tutti i dispositivi non montabili, eseguire `sn-remount-volumes` nuovamente lo script per confermare che tutti i volumi di storage che è possibile rimontare siano stati rimontati.



Se un volume di storage non può essere montato o non è formattato correttamente e si passa alla fase successiva, il volume e i dati presenti nel volume verranno eliminati. Se si dispone di due copie di dati oggetto, si disporrà di una sola copia fino al completamento della procedura successiva (ripristino dei dati oggetto).



Non eseguire `sn-recovery-postinstall.sh` lo script se si ritiene che i dati rimanenti su un volume di storage guasto non possano essere ricostruiti da un'altra parte della griglia (ad esempio, se il criterio ILM utilizza una regola che crea una sola copia o se i volumi non sono riusciti su più nodi). Contattare invece il supporto tecnico per determinare come ripristinare i dati.

4. Eseguire `sn-recovery-postinstall.sh` lo script: `sn-recovery-postinstall.sh`

Questo script riformatta tutti i volumi di storage che non possono essere montati o che sono stati trovati per essere formattati in modo non corretto; ricostruisce il database Cassandra sul nodo, se necessario; avvia i servizi sul nodo di storage.

Tenere presente quanto segue:

- L'esecuzione dello script potrebbe richiedere ore.
- In generale, si consiglia di lasciare la sessione SSH da sola mentre lo script è in esecuzione.
- Non premere **Ctrl+C** mentre la sessione SSH è attiva.
- Lo script viene eseguito in background se si verifica un'interruzione della rete e termina la sessione SSH, ma è possibile visualizzarne l'avanzamento dalla pagina Recovery (Ripristino).
- Se Storage Node utilizza il servizio RSM, lo script potrebbe sembrare bloccato per 5 minuti quando i servizi del nodo vengono riavviati. Questo ritardo di 5 minuti è previsto ogni volta che il servizio RSM viene avviato per la prima volta.



Il servizio RSM è presente sui nodi di storage che includono il servizio ADC.



Alcune procedure di ripristino StorageGRID utilizzano Reaper gestire le riparazioni Cassandra. Le riparazioni vengono eseguite automaticamente non appena vengono avviati i servizi correlati o richiesti. Si potrebbe notare un output di script che menziona "reaper" o "riparazione Cassandra". Se viene visualizzato un messaggio di errore che indica che la riparazione non è riuscita, eseguire il comando indicato nel messaggio di errore.

5. durante l'`sn-recovery-postinstall.sh`esecuzione dello script, monitorare la pagina Recovery in Grid Manager.

La barra di avanzamento e la colonna fase nella pagina Ripristino forniscono uno stato di alto livello `sn-recovery-postinstall.sh` dello script.

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 che `sn-recovery-postinstall.sh` lo script ha avviato i servizi sul nodo, è possibile ripristinare i dati degli oggetti in qualsiasi volume di storage formattato dallo script.

Lo script chiede se si desidera utilizzare il processo di ripristino del volume di Grid Manager.

- Nella maggior parte dei casi, dovresti ["Ripristinare i dati degli oggetti utilizzando Grid Manager"](#). Rispondi `y` per utilizzare Grid Manager.
- In rari casi, ad esempio quando sai che il nodo sostitutivo ha meno volumi disponibili per lo storage a oggetti rispetto al nodo originale, contatta il supporto tecnico per ripristinare manualmente i dati degli oggetti. Se si verifica uno di questi casi, rispondi `n` e premi un tasto qualsiasi per tornare alla riga di comando.

Ripristina i dati dell'oggetto sul volume di storage StorageGRID (guasto dell'unità di sistema)

Dopo il ripristino dei volumi di storage per un nodo di storage non appliance, è possibile ripristinare i dati degli oggetti replicati o codificati in cancellazione che sono stati persi in caso di guasto del nodo di storage.

Prima di iniziare

- Se la procedura automatica non è riuscita a rimontare i volumi di archiviazione conservati e a riformattare i volumi di archiviazione danneggiati, hai eseguito una di queste procedure:
 - ["Rimontare e riformattare i volumi di storage delle appliance \(procedura manuale\)"](#)
 - ["Rimontare e riformattare i volumi di storage \(procedura manuale\)"](#)

- Hai verificato che il nodo di archiviazione su cui stai ripristinando gli oggetti ha uno stato di connessione **Connesso**  nella scheda **Nodi > Panoramica** del Grid Manager.
- Hai confermato quanto segue:
 - Non è in corso un'espansione della griglia per aggiungere un nodo di archiviazione Storage Node.
 - Un decommission di Storage Node non è in corso o non è fallito.
 - Il ripristino di un volume di archiviazione danneggiato non è in corso.
 - Il ripristino di un nodo di Storage con un'unità di sistema guasta non è in corso.
 - Non è in corso alcuna operazione di ribilanciamento EC.
 - La clonazione del nodo dell'appliance non è in corso.

A proposito di questa attività

Dopo che hai sostituito le unità e i volumi sono stati formattati, Grid Manager visualizza i volumi come candidati per il ripristino nella scheda **Manutenzione > Ripristino volumi > Nodi da ripristinare**.

Se possibile, ripristinare i dati degli oggetti utilizzando la pagina di ripristino del volume in Grid Manager. È possibile [attivare la modalità di ripristino automatico](#) avviare automaticamente il ripristino del volume quando i volumi sono pronti per essere ripristinati o [eseguire manualmente il ripristino del volume](#). Attenersi alle seguenti linee guida:

- Se i volumi sono elencati in **Manutenzione > Ripristino volumi > Nodi da ripristinare**, ripristinare i dati dell'oggetto come descritto nei passaggi seguenti. I volumi saranno elencati se:
 - Alcuni, ma non tutti, volumi di storage in un nodo sono guasti
 - Tutti i volumi di storage in un nodo sono guasti e vengono sostituiti con lo stesso numero di volumi o più volumi

La pagina di ripristino del volume in Grid Manager consente inoltre di [monitorare il processo di ripristino del volume](#) e [visualizzare la cronologia del ripristino](#).

Se il nodo di archiviazione ripristinato contiene meno volumi rispetto al nodo che sta sostituendo, contatta il supporto tecnico per assistenza.

È possibile ripristinare due tipi di dati oggetto:

- Gli oggetti dati replicati vengono ripristinati da altre posizioni, supponendo che le regole ILM della griglia siano state configurate per rendere disponibili le copie degli oggetti.
 - Se una regola ILM è stata configurata per memorizzare una sola copia replicata e tale copia si trovava su un volume di archiviazione che ha subito un errore, non potrai recuperare l'oggetto.
 - Se l'unica copia rimanente di un oggetto si trova in un pool di storage cloud, StorageGRID deve inviare più richieste all'endpoint del pool di storage cloud per ripristinare i dati dell'oggetto.
- Gli oggetti dati con erasure coding (EC) vengono ripristinati ri assemblando i frammenti memorizzati. I frammenti corrotti o persi vengono ricreati dall'algoritmo di erasure coding dai dati rimanenti e dai frammenti di parità.

Le riparazioni dei dati con codifica erasure possono iniziare mentre alcuni nodi di storage sono offline. Tuttavia, se non è possibile tenere conto di tutti i dati sottoposti a erasure coding, la riparazione non può essere completata. La riparazione verrà completata dopo che tutti i nodi saranno disponibili.



Il ripristino dei volumi dipende dalla disponibilità delle risorse in cui sono memorizzate le copie a oggetti. L'avanzamento del ripristino dei volumi non è lineare e potrebbe richiedere giorni o settimane.

attiva la modalità di ripristino automatico

Quando si attiva la modalità di ripristino automatico, il ripristino del volume si avvia automaticamente quando i volumi sono pronti per essere ripristinati.

Fasi

1. In Grid Manager 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 potrai avviare manualmente i processi di ripristino del volume su nessun nodo.
- I ripristini del volume inizieranno automaticamente solo quando non sono in corso altre procedure di manutenzione.
- È possibile monitorare lo stato del lavoro dalla pagina di monitoraggio dell'avanzamento.
- StorageGRID ritenta automaticamente il ripristino del volume che non si avvia.

4. Una volta compresi i risultati dell'attivazione della modalità di ripristino automatico, selezionare **Sì** nella finestra di dialogo di conferma.

È possibile disattivare la modalità di ripristino automatico in qualsiasi momento.

Ripristino manuale di un volume o nodo non riuscito

Per ripristinare un volume o un nodo guasto, procedere come segue.

Fasi

1. In Grid Manager vai su **Manutenzione > Ripristino volume**.
2. Selezionare la scheda **nodi da ripristinare**, quindi far scorrere l'interruttore per **modalità di ripristino automatico** sulla posizione disattivata.

Il numero sulla scheda indica il numero di nodi con volumi che richiedono il ripristino.

3. Espandere ciascun nodo per visualizzare i volumi in esso che richiedono il ripristino e il relativo stato.
4. Correggere eventuali problemi che impediscono il ripristino di ciascun volume. I problemi saranno indicati quando si seleziona **in attesa di passaggi manuali**, se viene visualizzato come stato del volume.
5. Selezionare un nodo da ripristinare in cui tutti i volumi indicano uno stato Pronto per il ripristino.

È possibile ripristinare i volumi solo per un nodo alla volta.

Ciascun volume nel nodo deve indicare che è pronto per il ripristino.

6. Selezionare **Avvia ripristino**.
7. Risolvere eventuali avvisi che potrebbero essere visualizzati o selezionare **Avvia comunque** per ignorare gli avvisi e avviare il ripristino.

I nodi vengono spostati dalla scheda **Nodes to restore** (nodi da ripristinare) alla scheda **Restoration Progress** (avanzamento ripristino) all'avvio del ripristino.

Se non è possibile avviare il ripristino di un volume, il nodo torna alla scheda **nodi da ripristinare**.

Visualizza l'avanzamento del ripristino

La scheda **Restoration Progress** (avanzamento ripristino) mostra lo stato del processo di ripristino del volume e le informazioni sui volumi di un nodo da ripristinare.

I tassi di riparazione dei dati per gli oggetti replicati e codificati per la cancellazione in tutti i volumi sono medie che riassumono tutti i restauri in corso. Viene inoltre indicata la % di oggetti in tali volumi che sono integri e non richiedono restauro.



Il ripristino dei dati replicati dipende dalla disponibilità delle risorse in cui sono memorizzate le copie replicate. L'avanzamento del ripristino dei dati replicati non è lineare e potrebbe richiedere giorni o settimane.

La sezione lavori di ripristino visualizza informazioni sui ripristini dei volumi avviati da Grid Manager.

- Il numero nell'intestazione della sezione lavori di ripristino indica il numero di volumi che vengono ripristinati o messi in coda per il ripristino.
- La tabella visualizza le informazioni relative a ciascun volume di un nodo da ripristinare e al relativo stato di avanzamento.
 - L'avanzamento per ciascun nodo visualizza la percentuale per ciascun lavoro.
 - Espandere la colonna Dettagli per visualizzare l'ora di inizio del ripristino e l'ID del processo.
- Se il ripristino di un volume non riesce:
 - La colonna Stato indica `failed (attempting retry)`, e verrà riavviata automaticamente.
 - Se più lavori di ripristino non hanno avuto esito positivo, il lavoro più recente verrà rielaborato automaticamente per primo.
 - L'avviso **guasto riparazione EC** viene attivato se i tentativi continuano a non riuscire. Per risolvere il problema, attenersi alla procedura riportata nell'avviso.

Visualizza la cronologia del ripristino

La scheda **Restoration history** (Cronologia ripristino) mostra informazioni su tutti i ripristini dei volumi completati correttamente.



Le dimensioni non sono applicabili agli oggetti replicati e vengono visualizzate solo per i ripristini che contengono oggetti di dati EC (erasure coding).

Verifica lo stato dello storage dopo il ripristino di un'unità di sistema di un nodo di storage StorageGRID

Dopo aver ripristinato l'unità di sistema per un nodo di storage, è necessario verificare che lo stato desiderato del nodo di storage sia impostato su online e assicurarsi che lo stato sia online per impostazione predefinita ogni volta che il server del nodo di storage viene riavviato.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Il nodo di storage è stato ripristinato e il ripristino dei dati è stato completato.

Fasi

1. Selezionare **Nodi > Nodo di archiviazione_ > Attività**.
2. Se l'elenco a discesa **Stato di archiviazione** è impostato su Sola lettura o Offline, selezionare **Online**.
3. Selezionare **Salva**.

Ripristino da errori del nodo di amministrazione

Ripristino del nodo Admin primario o non primario in StorageGRID

Il processo di ripristino per un nodo di amministrazione dipende dal fatto che si tratti del nodo di amministrazione primario o di un nodo di amministrazione non primario.

I passaggi di alto livello per il ripristino di un nodo di amministrazione primario o non primario sono gli stessi, anche se i dettagli dei passaggi differiscono.

Seguire sempre la procedura di ripristino corretta per l'Admin Node che si sta ripristinando. Le procedure hanno lo stesso aspetto ad un livello elevato, ma differiscono nei dettagli.

Scelte

- ["Ripristina il nodo Admin primario utilizzando lo stesso nodo Admin primario"](#)
- ["Ripristina dai guasti del nodo di amministrazione primario utilizzando un nodo di amministrazione non primario"](#)
- ["Ripristino da guasti non primari del nodo di amministrazione"](#)

Riprendi dai guasti del nodo di amministrazione primario usando lo stesso nodo di amministrazione primario

Ripristina il nodo Admin primario di StorageGRID utilizzando lo stesso nodo Admin primario

È necessario completare un set specifico di attività per eseguire il ripristino da un guasto primario del nodo di amministrazione. Il nodo di amministrazione primario ospita il servizio CMN (Configuration Management Node) per la griglia.



Devi riparare o sostituire tempestivamente un nodo di amministrazione primario guasto, altrimenti potresti non riuscire a eseguire alcune procedure di manutenzione.

Seguire questi passaggi di alto livello per ripristinare un nodo amministrativo primario:

1. ["Copia i registri di controllo dal nodo di amministrazione primario non riuscito"](#)
2. ["Sostituire il nodo amministrativo primario"](#)
3. ["Configurare il nodo amministrativo primario sostitutivo"](#)
4. ["Determinare se esiste un requisito di hotfix per il nodo amministrativo primario recuperato"](#)
5. ["Ripristinare il registro di controllo sul nodo amministrativo primario recuperato"](#)

6. "Ripristinare il database del nodo amministrativo quando si ripristina un nodo amministrativo primario"
7. "Ripristinare le metriche Prometheus durante il ripristino di un nodo amministrativo primario"

Copia i log di controllo da un nodo Admin primario di StorageGRID non riuscito

Se è possibile copiare i registri di controllo dal nodo di amministrazione primario guasto, è necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione primario recuperato dopo che è attivo e in esecuzione.

A proposito di questa attività

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.



Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

Fasi

1. Se possibile, accedere al nodo di amministrazione primario non riuscito. In caso contrario, accedi a qualsiasi nodo di amministrazione disponibile.
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per evitare che crei un nuovo file di registro: `service ams stop`
3. Accedere alla directory di esportazione della verifica:

```
cd /var/local/audit/export
```

(O `cd /var/local/log` sui sistemi precedenti)

4. Rinominare il file di registro di origine con un nome di file numerato univoco.



- Se il file di registro è in `/var/local/audit/export` directory, il suo nome è `audit.log`.
- Se il file di registro è in `/var/local/log` directory, il suo nome è `localaudit.log`.

Ad esempio, rinominare il `localaudit.log` file a `2025-10-22.txt.1`.

```
ls -l
mv localaudit.log 2025-10-22.txt.1
```

5. Riavviare il servizio AMS: `service ams start`
6. Creare la directory per copiare tutti i file di log di controllo in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando richiesto, inserire la password per admin.

7. Copiare tutti i file di log di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando richiesto, inserire la password per admin.

8. Disconnettersi come root: `exit`

Sostituisci il nodo di amministrazione primario di StorageGRID utilizzando lo stesso nodo di amministrazione primario

Per ripristinare un nodo di amministrazione primario, è necessario prima sostituire l'hardware fisico o virtuale.

Per ripristinare un nodo di amministrazione primario, è necessario prima sostituire l'hardware fisico o virtuale.

- Puoi sostituire un nodo Admin primario guasto con un nodo Admin primario in esecuzione sulla stessa piattaforma.
- Puoi sostituire un nodo amministrativo primario in esecuzione su VMware o su un host Linux con un nodo amministrativo primario ospitato su un'appliance di servizi StorageGRID.
- Puoi sostituire un nodo Admin primario in esecuzione su un host VMware con un'appliance di servizi SG1000 o SG100.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino primario del nodo di amministrazione.

Piattaforma sostitutiva	Procedura
VMware	" Sostituisci un nodo VMware con un nodo di ripristino " " Sostituisci un nodo VMware con SG1000 o SG100 "
Linux	" Sostituire un nodo Linux "
Appliance di servizi	" Sostituire un'appliance di servizi "

Piattaforma sostitutiva	Procedura
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux" .

Configura un nodo Admin primario sostitutivo in StorageGRID

Il nodo sostitutivo deve essere configurato come nodo amministratore primario per il sistema StorageGRID.

Prima di iniziare

- Per i nodi di amministrazione primari ospitati su macchine virtuali, la macchina virtuale è stata implementata, attivata e inizializzata.
- Per i nodi di amministrazione primari ospitati su un'appliance di servizi, l'appliance è stata sostituita e il software è stato installato. Consultare la ["Istruzioni per l'installazione dell'apparecchio"](#).
- Hai l'ultimo backup del file del pacchetto di ripristino(`sgws-recovery-package-id-revision.zip`).
- Si dispone della passphrase di provisioning.

Fasi

1. Aprire il browser Web e accedere a `https://primary_admin_node_ip`.
2. Gestione di una password di installazione temporanea come necessario:
 - Se una password è già stata impostata utilizzando uno di questi metodi, immetterla per continuare.
 - Un utente imposta 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 all'indirizzo `/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, impostare una password per proteggere il programma di installazione di StorageGRID.
3. Seleziona **Ripristina un nodo amministratore primario non funzionante**.

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. Selezionare **Sfoglia**.
 - b. Individua il file del pacchetto di ripristino più recente per il tuo sistema StorageGRID e seleziona **Apri**.
5. Inserire la passphrase di provisioning.
6. Seleziona **Avvia ripristino**.

Viene avviato il processo di ripristino. Grid Manager potrebbe non essere disponibile per alcuni minuti all'avvio dei servizi richiesti. Al termine del ripristino, viene visualizzata la pagina di accesso.

7. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.



Per configurare una relying party trust, consulta la configurazione del single sign-on usando "OIDC" o "SAML". Per accedere al certificato server predefinito, accedi alla shell dei comandi dell'Admin Node. Vai alla directory `/var/local/mgmt-api` e seleziona il file `server.crt`.



Dopo il ripristino di un nodo amministrativo primario, ["determinare se è necessario applicare una correzione rapida"](#).

Determinare i requisiti di hotfix per il nodo amministratore primario in StorageGRID

Dopo il ripristino di un nodo amministrativo primario, determinare se è necessario

applicare una correzione rapida.

Prima di iniziare

Il ripristino del nodo amministrativo primario è stato completato.

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Selezionare **Nodi**.
3. Dall'elenco a sinistra, selezionare il nodo di amministrazione principale.
4. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
5. Selezionare qualsiasi altro nodo della griglia.
6. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
 - Se le versioni visualizzate nei campi **versione software** sono identiche, non è necessario applicare una correzione rapida.
 - Se le versioni visualizzate nei campi **versione software** sono diverse, è necessario ["applicare una correzione rapida"](#) aggiornare il nodo amministrativo primario recuperato alla stessa versione.

Ripristina il registro di controllo sul nodo amministratore primario di StorageGRID recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione primario guasto, è possibile copiarlo nel nodo di amministrazione primario che si sta ripristinando.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- I registri di controllo sono stati copiati in un'altra posizione dopo l'errore del nodo di amministrazione originale.

A proposito di questa attività

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se esiste un solo nodo Admin e non è possibile copiare il log di audit dal nodo guasto, il nodo Admin recuperato inizia a registrare gli eventi nel log di audit come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima possibile.

Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:



- È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
- È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.

Vedere ["Configurare la gestione dei log e il server syslog esterno"](#) per i dettagli.

Fasi

1. Accedere al nodo di amministrazione recuperato:

- a. Immettere il seguente comando: `ssh admin@recovery_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt passa da \$ a #.

2. Controlla quali file di controllo sono stati conservati: `cd /var/local/audit/export`

3. Copiare i file di log di controllo conservati nel nodo amministrativo recuperato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Quando richiesto, inserire la password per admin.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.

5. Aggiornare le impostazioni 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 di StorageGRID Admin Node durante il recupero del nodo amministratore primario

Se si desidera conservare le informazioni cronologiche sugli attributi e gli avvisi su un nodo amministrativo primario che non ha superato il test, è possibile ripristinare il database del nodo amministrativo. È possibile ripristinare questo database solo se il sistema StorageGRID include un altro nodo amministratore.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Si dispone del `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di errore di un nodo amministratore, le informazioni storiche memorizzate nel database del nodo amministratore andranno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Dati degli attributi storici, utilizzati nei grafici di stile legacy nella pagina dei nodi

Quando si ripristina un nodo amministratore, il processo di installazione del software crea un database Admin Node vuoto sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti successivamente.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le informazioni storiche copiando il database del nodo di amministrazione da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database del nodo di amministrazione.



La copia del database Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere 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 ripristinato:
 - a. Accedere al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file.
 - b. Arrestare il servizio MI: `service mi stop`
 - c. Arrestare il servizio api di gestione: `service mgmt-api stop`
 - d. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `ssh-add`
 - e. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
 - f. Quando richiesto, confermare che si desidera sovrascrivere il database MI nel nodo Admin recuperato.

Il database e i relativi dati storici vengono copiati nel nodo di amministrazione recuperato. Al termine

dell'operazione di copia, lo script avvia il nodo Admin recuperato.

g. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Immettere: `ssh-add -D`

5. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristina le metriche Prometheus quando recuperi il nodo Admin primario di StorageGRID

Facoltativamente, è possibile conservare le metriche storiche gestite da Prometheus su un nodo di amministrazione primario che ha avuto problemi. Le metriche Prometheus possono essere ripristinate solo se il sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Si dispone del `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le metriche storiche copiando il database Prometheus da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database Prometheus.



La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere 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 ripristinato:
 - a. Accedere al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`

- ii. Immettere la password elencata nel `Passwords.txt` file.
- iii. Immettere il seguente comando per passare alla directory principale: `su -`
- iv. Immettere la password elencata nel `Passwords.txt` file.
- b. Arrestare il servizio Prometheus: `service prometheus stop`
- c. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `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 distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

- a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Immettere: `ssh-add -D`
- 4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine. `service prometheus start`

Ripristina dai guasti del nodo di amministrazione primario utilizzando un nodo di amministrazione non primario

Ripristina dai guasti del nodo di amministrazione primario di StorageGRID utilizzando un nodo di amministrazione non primario

Devi completare una serie specifica di attività per ripristinare il sistema dopo un errore del nodo di amministrazione primario utilizzando un nodo di amministrazione non primario. Il nodo di amministrazione primario ospita il servizio Configuration Management Node (CMN) per la grid.

Segui questi high-level passaggi per ripristinare un nodo Admin primario usando un nodo Admin non primario:

1. ["Copia i registri di controllo dal nodo di amministrazione primario non riuscito"](#)
2. ["Sostituire nodo amministratore primario"](#)
3. ["Seleziona Avvia ripristino per configurare il nodo Admin primario"](#)
4. ["Determinare il requisito di hotfix per il nodo amministrativo primario"](#)
5. ["Ripristinare il log di audit sul nodo di amministrazione primario recuperato"](#)
6. ["Ripristinare le metriche Prometheus durante il ripristino del nodo di amministrazione primario"](#)

Copia i log di audit di StorageGRID da un nodo Admin primario guasto

Se è possibile copiare i registri di controllo dal nodo di amministrazione primario guasto, è necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema

della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione primario recuperato dopo che è attivo e in esecuzione.

A proposito di questa attività

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.



Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

Fasi

1. Se possibile, accedere al nodo di amministrazione primario non riuscito. In caso contrario, accedi a qualsiasi nodo di amministrazione disponibile.
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Inserisci il seguente comando per passare all'account utente root: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per evitare che crei un nuovo file di registro: `service ams stop`
3. Accedere alla directory di esportazione della verifica:

```
cd /var/local/audit/export
```

(O `cd /var/local/log` sui sistemi precedenti)

4. Rinominare il file di registro di origine con un nome di file numerato univoco.



- Se il file di registro è in `/var/local/audit/export` directory, il suo nome è `audit.log`.
- Se il file di registro è in `/var/local/log` directory, il suo nome è `localaudit.log`.

Ad esempio, rinominare il `localaudit.log` file a `2025-10-22.txt.1`.

```
ls -l
mv localaudit.log 2025-10-22.txt.1
```


5. Riavviare il servizio AMS: `service ams start`

6. Creare la directory per copiare tutti i file di log di controllo in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando richiesto, inserisci la password per l'account utente admin.

7. Copiare tutti i file di log di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando richiesto, inserisci la password per l'account utente admin.

8. Disconnettiti come utente root: `exit`.

Sostituisci il nodo Admin primario di StorageGRID usando un nodo Admin non primario

Per ripristinare un nodo di amministrazione primario, è necessario prima sostituire l'hardware fisico o virtuale.

- Puoi sostituire un nodo Admin primario guasto con un nodo Admin primario in esecuzione sulla stessa piattaforma.
- Puoi sostituire un nodo amministrativo primario in esecuzione su VMware o su un host Linux con un nodo amministrativo primario ospitato su un'appliance di servizi StorageGRID.
- Puoi sostituire un nodo Admin primario in esecuzione su un host VMware con un'appliance di servizi SG1000 o SG100.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino primario del nodo di amministrazione.

Piattaforma sostitutiva	Procedura
VMware	" Sostituisci un nodo VMware con un nodo di ripristino " "Sostituisci il nodo VMware con l'appliance di servizi SG1000 o SG100"
Linux	" Sostituire un nodo Linux "
Appliance di servizi	" Sostituire un'appliance di servizi "
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per " Sostituzione di un nodo Linux ".

Seleziona Avvia ripristino per configurare il nodo Admin primario

Dopo aver sostituito un nodo Admin primario, devi selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituto del nodo guasto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.

Fasi

1. Dal Grid Manager, seleziona **Manutenzione > Attività > Ripristino nodo**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Inserisci la **passphrase di provisioning**.
4. Seleziona **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 Recovery Grid Node (nodo griglia di ripristino).



Durante l'esecuzione della procedura di ripristino, puoi selezionare **Reset** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo rimarrà in uno stato indeterminato se resetti la procedura.

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware:** Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux:** Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`
- **Appliance:** Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo dell'appliance in uno stato preinstallato eseguendo `sgareinstall` sul nodo. Vedere ["Preparazione dell'appliance per la reinstallazione \(solo sostituzione della piattaforma\)"](#).

6. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.



Per configurare un trust della parte affidabile, vedere ["Configurare il single sign-on"](#) . 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.

Determina se è necessario un hotfix StorageGRID per il nodo Admin primario

Dopo aver ripristinato un nodo Admin primario, determina se devi applicare un hotfix.

Prima di iniziare

Il ripristino del nodo Admin primario è completo.

Fasi

1. Accedere a Grid Manager utilizzando un ["browser web supportato"](#).
2. Selezionare **Nodi**.
3. Dall'elenco a sinistra, selezionare il nodo di amministrazione principale.
4. Nella scheda Overview (Panoramica), annotare la versione visualizzata nel campo **Software Version** (versione software).
5. Selezionare qualsiasi altro nodo della griglia.
6. Nella scheda Panoramica, nota le versioni visualizzate nel campo **Versione software**.
 - Se le versioni visualizzate nei campi **versione software** sono identiche, non è necessario applicare una correzione rapida.
 - Se le versioni visualizzate nei campi **versione software** sono diverse, è necessario ["applicare una correzione rapida"](#)aggiornare il nodo amministrativo primario recuperato alla stessa versione.

Ripristina il registro di controllo di StorageGRID su un nodo amministrativo primario recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione primario guasto, è possibile copiarlo nel nodo di amministrazione primario che si sta ripristinando.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- I registri di controllo sono stati copiati in un'altra posizione dopo l'errore del nodo di amministrazione originale.

A proposito di questa attività

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è

possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se esiste un solo nodo Admin e non è possibile copiare il log di audit dal nodo guasto, il nodo Admin recuperato inizia a registrare gli eventi nel log di audit come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima possibile.

Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:



- È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
- È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.

Vedere ["Configurare la gestione dei log e il server syslog esterno"](#) per i dettagli.

Fasi

1. Accedere al nodo di amministrazione recuperato:

- a. Immettere il seguente comando: `ssh admin@recovery_Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt passa da `$` a `#`.

2. Controlla quali file di controllo sono stati conservati: `cd /var/local/audit/export`

3. Copiare i file di log di controllo conservati nel nodo amministrativo recuperato: `scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY* .`

Quando richiesto, inserire la password per admin.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.
5. Aggiornare le impostazioni utente e gruppo dei file di registro di controllo sul nodo di amministrazione recuperato: `chown ams-user:bycast *`
6. Disconnettersi come root: `exit`

Ripristina le metriche Prometheus quando recuperi un nodo amministratore primario StorageGRID

Facoltativamente, è possibile conservare le metriche storiche gestite da Prometheus su un nodo di amministrazione primario che ha avuto problemi. Le metriche Prometheus possono essere ripristinate solo se il sistema StorageGRID include un altro nodo di amministrazione.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Si dispone del `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione primario e il sistema StorageGRID dispone di un altro nodo di amministrazione, è possibile ripristinare le metriche storiche copiando il database Prometheus da un nodo di amministrazione non primario (il *nodo di amministrazione di origine*) al nodo di amministrazione primario recuperato. Se il sistema dispone solo di un nodo di amministrazione primario, non è possibile ripristinare il database Prometheus.



La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere 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 ripristinato:
 - a. Accedere al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file.
 - b. Arrestare il servizio Prometheus: `service prometheus stop`
 - c. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `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 distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi

- a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Immettere:`ssh-add -D`

4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine.`service prometheus start`

Ripristino da guasti non primari del nodo di amministrazione

Ripristina da guasti del nodo amministratore non primario di StorageGRID

È necessario completare le seguenti attività per eseguire il ripristino da un errore non primario del nodo di amministrazione. Un nodo amministratore ospita il servizio CMN (Configuration Management Node) ed è noto come nodo amministratore primario. Sebbene sia possibile avere più nodi di amministrazione, ogni sistema StorageGRID include un solo nodo di amministrazione primario. Tutti gli altri nodi Admin non sono nodi Admin primari.

Seguire questi passaggi di alto livello per ripristinare un nodo amministrativo non primario:

1. ["Copiare i registri di controllo dal nodo di amministrazione non primario non riuscito"](#)
2. ["Sostituire il nodo amministrativo non primario"](#)
3. ["Selezionare Avvia ripristino per configurare il nodo amministrativo non primario"](#)
4. ["Ripristinare il registro di controllo su un nodo amministrativo non primario recuperato"](#)
5. ["Ripristinare il database del nodo amministrativo quando si ripristina un nodo amministrativo non primario"](#)
6. ["Ripristinare le metriche Prometheus durante il ripristino di un nodo amministrativo non primario"](#)

Copia i log di controllo da un nodo Admin non primario di StorageGRID non riuscito

Se è possibile copiare i registri di controllo dal nodo di amministrazione non riuscito, è necessario conservarli per mantenere il record dell'attività e dell'utilizzo del sistema della griglia. È possibile ripristinare i registri di controllo conservati nel nodo di amministrazione non primario recuperato una volta attivato e in esecuzione.

Questa procedura copia i file di log di audit dal nodo di amministrazione non riuscito in una posizione temporanea su un nodo griglia separato. Questi registri di controllo conservati possono quindi essere copiati nel nodo di amministrazione sostitutivo. I registri di controllo non vengono copiati automaticamente nel nuovo nodo di amministrazione.

A seconda del tipo di errore, potrebbe non essere possibile copiare i registri di controllo da un nodo di amministrazione non riuscito. Se l'implementazione ha un solo nodo di amministrazione, il nodo di amministrazione recuperato avvia la registrazione degli eventi nel registro di controllo in un nuovo file vuoto e i dati precedentemente registrati vengono persi. Se l'implementazione include più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione.



Se i registri di controllo non sono ora accessibili sul nodo di amministrazione guasto, potrebbe essere possibile accedervi in un secondo momento, ad esempio dopo il ripristino dell'host.

1. Se possibile, accedere al nodo Admin non riuscito. In caso contrario, accedere al nodo di amministrazione primario o a un altro nodo di amministrazione, se disponibile.

- a. Immettere il seguente comando: `ssh admin@grid_node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.
- c. Immettere il seguente comando per passare alla directory principale: `su -`
- d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Arrestare il servizio AMS per evitare che crei un nuovo file di registro: `service ams stop`
3. Accedere alla directory di esportazione della verifica:

```
cd /var/local/audit/export/
```

4. Rinominare il file di origine `audit.log` con un nome di file numerato univoco. Ad esempio, rinominare il file `audit.log` in `2023-10-25.txt.1`.

```
ls -l
mv audit.log 2023-10-25.txt.1
```

5. Riavviare il servizio AMS: `service ams start`
6. Creare la directory per copiare tutti i file di log di controllo in una posizione temporanea su un nodo griglia separato: `ssh admin@grid_node_IP mkdir -p /var/local/tmp/saved-audit-logs`

Quando richiesto, inserire la password per admin.

7. Copiare tutti i file di log di controllo nella posizione temporanea: `scp -p * admin@grid_node_IP:/var/local/tmp/saved-audit-logs`

Quando richiesto, inserire la password per admin.

8. Disconnettersi come root: `exit`

Sostituisci il nodo Admin non primario di StorageGRID

Per ripristinare un nodo di amministrazione non primario, è necessario sostituire l'hardware fisico o virtuale.

È possibile sostituire un nodo di amministrazione non primario guasto con un nodo di amministrazione non primario in esecuzione sulla stessa piattaforma oppure sostituire un nodo di amministrazione non primario in esecuzione su VMware o su un host Linux con un nodo di amministrazione non primario in hosting su un'appliance di servizi.

Utilizzare la procedura corrispondente alla piattaforma sostitutiva selezionata per il nodo. Una volta completata

la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino del nodo Admin non primario.

Piattaforma sostitutiva	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
Appliance di servizi	"Sostituire un'appliance di servizi"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux" .

Seleziona **Avvia ripristino** per configurare il nodo Admin non primario di StorageGRID

Dopo aver sostituito un nodo Admin non primario, selezionare **Avvia ripristino** in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.

Fasi

1. Dal Grid Manager, seleziona **Manutenzione > Attività > Ripristino nodo**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Inserisci la **passphrase di provisioning**.
4. Seleziona **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 Recovery Grid Node (nodo griglia di ripristino).



Durante l'esecuzione della procedura di ripristino, puoi selezionare **Reset** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo rimarrà in uno stato indeterminato se resetti la procedura.

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware:** Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux:** Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`
- **Appliance:** Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo dell'appliance in uno stato preinstallato eseguendo `sgareinstall` sul nodo. Vedere "[Preparazione dell'appliance per la reinstallazione \(solo sostituzione della piattaforma\)](#)".

6. Se è attivato il Single Sign-on (SSO) per il sistema StorageGRID e il trust della parte di base per il nodo di amministrazione ripristinato è stato configurato per utilizzare il certificato dell'interfaccia di gestione predefinita, aggiornare (o eliminare e ricreare) il trust della parte di base del nodo in Active Directory Federation Services (ad FS). Utilizzare il nuovo certificato server predefinito generato durante il processo di ripristino del nodo di amministrazione.



Per configurare un trust della parte affidabile, vedere "[Configurare il single sign-on](#)". 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 amministrativo non primario di StorageGRID recuperato

Se è stato possibile conservare il registro di controllo dal nodo di amministrazione non primario non riuscito, in modo da conservare le informazioni del registro di controllo cronologico, è possibile copiarle nel nodo di amministrazione non primario che si sta

ripristinando.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- I registri di controllo sono stati copiati in un'altra posizione dopo l'errore del nodo di amministrazione originale.

A proposito di questa attività

In caso di errore di un nodo amministratore, i registri di controllo salvati in quel nodo amministratore potrebbero andare persi. Potrebbe essere possibile conservare i dati in caso di perdita copiando i registri di controllo dal nodo di amministrazione non riuscito e ripristinando questi registri di controllo nel nodo di amministrazione ripristinato. A seconda dell'errore, potrebbe non essere possibile copiare i registri di controllo dal nodo di amministrazione non riuscito. In tal caso, se l'implementazione ha più di un nodo di amministrazione, è possibile ripristinare i registri di controllo da un altro nodo di amministrazione, poiché i registri di controllo vengono replicati in tutti i nodi di amministrazione.

Se esiste un solo nodo Admin e non è possibile copiare il log di audit dal nodo guasto, il nodo Admin recuperato inizia a registrare gli eventi nel log di audit come se l'installazione fosse nuova.

Per ripristinare la funzionalità di registrazione, è necessario ripristinare un nodo amministratore il prima possibile.



Per impostazione predefinita, le informazioni di controllo vengono inviate al registro di controllo sui nodi di amministrazione. È possibile saltare questi passaggi se si verifica una delle seguenti condizioni:

- È stato configurato un server syslog esterno e i registri di controllo vengono inviati al server syslog invece che ai nodi di amministrazione.
- È stato specificato esplicitamente che i messaggi di audit devono essere salvati solo sui nodi locali che li hanno generati.

Vedere "[Configurare la gestione dei log e il server syslog esterno](#)" per i dettagli.

Fasi

1. Accedere al nodo di amministrazione recuperato:

a. Digitare il seguente comando:

```
ssh admin@recovery_Admin_Node_IP
```

b. Immettere la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Dopo aver effettuato l'accesso come root, il prompt passa da `$` a `#`.

2. Controllare quali file di audit sono stati conservati:

```
cd /var/local/log
```

3. Copiare i file di log di controllo conservati nel nodo di amministrazione recuperato:

```
scp admin@grid_node_IP:/var/local/tmp/saved-audit-logs/YYYY*
```

Quando richiesto, inserire la password per admin.

4. Per motivi di sicurezza, eliminare i registri di controllo dal nodo Grid guasto dopo aver verificato che siano stati copiati correttamente nel nodo Admin ripristinato.
5. Aggiornare le impostazioni di utente e gruppo dei file di log di controllo sul nodo di amministrazione recuperato:

```
chown ams-user:bycast *
```

6. Disconnettersi come root: `exit`

Ripristina il database di StorageGRID Admin Node durante il recupero di un nodo Admin non primario

Se si desidera conservare le informazioni cronologiche sugli attributi e gli avvisi su un nodo amministrativo non primario che non ha superato il test, è possibile ripristinare il database del nodo amministrativo dal nodo amministrativo primario.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Si dispone del `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di errore di un nodo amministratore, le informazioni storiche memorizzate nel database del nodo amministratore andranno perse. Questo database include le seguenti informazioni:

- Cronologia degli avvisi
- Dati storici sugli attributi, utilizzati nei grafici della pagina Nodes

Quando si ripristina un nodo amministratore, il processo di installazione del software crea un database Admin Node vuoto sul nodo recuperato. Tuttavia, il nuovo database include solo le informazioni relative ai server e ai servizi attualmente presenti nel sistema o aggiunti successivamente.

Se è stato ripristinato un nodo Admin non primario, è possibile ripristinare le informazioni storiche copiando il database del nodo Admin dal nodo Admin primario (il *nodo Admin di origine*) nel nodo recuperato.



La copia del database Admin Node potrebbe richiedere diverse ore. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.
2. Eseguire il seguente comando dal nodo di amministrazione di origine. Quindi, immettere la passphrase di

provisioning, se richiesto. `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 ripristinato:
 - a. Accedere al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file.
 - b. Arrestare il servizio MI: `service mi stop`
 - c. Arrestare il servizio api di gestione: `service mgmt-api stop`
 - d. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `ssh-add`
 - e. Immettere la password di accesso SSH elencata nel `Passwords.txt` file.
 - f. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Immettere: `ssh-add -D`
6. Riavviare i servizi sul nodo di amministrazione di origine: `service servermanager start`

Ripristina le metriche Prometheus quando recuperi il nodo Admin non primario di StorageGRID

In alternativa, è possibile conservare le metriche storiche gestite da Prometheus su un nodo amministrativo non primario che ha avuto problemi.

Prima di iniziare

- Il nodo Admin recuperato è installato e in esecuzione.
- Il sistema StorageGRID include almeno due nodi di amministrazione.
- Si dispone del `Passwords.txt` file.
- Si dispone della passphrase di provisioning.

A proposito di questa attività

In caso di guasto di un nodo di amministrazione, le metriche mantenute nel database Prometheus sul nodo di amministrazione andranno perse. Quando si ripristina l'Admin Node, il processo di installazione del software crea un nuovo database Prometheus. Una volta avviato il nodo di amministrazione recuperato, vengono registrate le metriche come se fosse stata eseguita una nuova installazione del sistema StorageGRID.

Se è stato ripristinato un nodo di amministrazione non primario, è possibile ripristinare le metriche storiche copiando il database Prometheus dal nodo di amministrazione primario (il *nodo di amministrazione di origine*) al nodo di amministrazione recuperato.



La copia del database Prometheus potrebbe richiedere un'ora o più. Alcune funzionalità di Grid Manager non saranno disponibili mentre i servizi vengono arrestati sul nodo di amministrazione di origine.

Fasi

1. Accedere al nodo di amministrazione di origine:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere 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 ripristinato:
 - a. Accedere al nodo di amministrazione recuperato:
 - i. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - ii. Immettere la password elencata nel `Passwords.txt` file.
 - iii. Immettere il seguente comando per passare alla directory principale: `su -`
 - iv. Immettere la password elencata nel `Passwords.txt` file.
 - b. Arrestare il servizio Prometheus: `service prometheus stop`
 - c. Aggiungere la chiave privata SSH all'agente SSH. Immettere: `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 distruggere il nuovo database Prometheus nel nodo di amministrazione recuperato.

Il database Prometheus originale e i relativi dati storici vengono copiati nel nodo Admin recuperato. Al termine dell'operazione di copia, lo script avvia il nodo Admin recuperato. Viene visualizzato il seguente stato:

Database clonato, avvio dei servizi
 - a. Se non si richiede più l'accesso senza password ad altri server, rimuovere la chiave privata dall'agente SSH. Immettere: `ssh-add -D`
4. Riavviare il servizio Prometheus sul nodo di amministrazione di origine. `service prometheus start`

Ripristino da guasti del nodo gateway

Sostituire il nodo gateway di StorageGRID

È possibile sostituire un nodo gateway guasto con un nodo gateway in esecuzione sullo stesso hardware fisico o virtuale oppure sostituire un nodo gateway in esecuzione su VMware o su un host Linux con un nodo gateway in hosting su un'appliance di servizi.

La procedura di sostituzione del nodo da seguire dipende dalla piattaforma utilizzata dal nodo sostitutivo. Una volta completata la procedura di sostituzione del nodo (adatta a tutti i tipi di nodo), questa procedura indirizzerà l'utente al passaggio successivo per il ripristino del nodo gateway.

Piattaforma sostitutiva	Procedura
VMware	"Sostituire un nodo VMware"
Linux	"Sostituire un nodo Linux"
Appliance di servizi	"Sostituire un'appliance di servizi"
OpenStack	I file e gli script dei dischi delle macchine virtuali forniti da NetApp per OpenStack non sono più supportati per le operazioni di recovery. Se è necessario ripristinare un nodo in esecuzione in un'implementazione OpenStack, scaricare i file per il sistema operativo Linux in uso. Quindi, seguire la procedura per "Sostituzione di un nodo Linux" .

Seleziona Avvia ripristino per configurare il nodo gateway di StorageGRID

Dopo aver sostituito un nodo gateway, selezionare Avvia ripristino in Grid Manager per configurare il nuovo nodo come sostituzione del nodo guasto.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["Autorizzazione di manutenzione o di accesso root"](#).
- Si dispone della passphrase di provisioning.
- Il nodo sostitutivo è stato implementato e configurato.

Fasi

1. Dal Grid Manager, seleziona **Manutenzione > Attività > Ripristino nodo**.
2. Selezionare il nodo della griglia che si desidera ripristinare nell'elenco Pending Nodes (nodi in sospeso).

I nodi vengono visualizzati nell'elenco dopo un errore, ma non è possibile selezionare un nodo fino a quando non è stato reinstallato e pronto per il ripristino.

3. Inserisci la **passphrase di provisioning**.
4. Seleziona **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 Recovery Grid Node (nodo griglia di ripristino).



Durante l'esecuzione della procedura di ripristino, puoi selezionare **Reset** per avviare un nuovo ripristino. Viene visualizzata una finestra di dialogo che indica che il nodo rimarrà in uno stato indeterminato se resetti la procedura.

Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo a uno stato preinstallato, come segue:

- **VMware:** Eliminare il nodo virtual grid implementato. Quindi, quando si è pronti per riavviare il ripristino, ridistribuire il nodo.
- **Linux:** Riavviare il nodo eseguendo questo comando sull'host Linux: `storagegrid node force-recovery node-name`
- **Appliance:** Se si desidera riprovare il ripristino dopo aver reimpostato la procedura, è necessario ripristinare il nodo dell'appliance in uno stato preinstallato eseguendo `sgareinstall` sul nodo. Vedere "[Preparazione dell'appliance per la reinstallazione \(solo sostituzione della piattaforma\)](#)".

Ripristino da errori del nodo di archiviazione

Ripristina dai guasti del nodo di archiviazione StorageGRID

Il supporto per i nodi archivio è stato rimosso.

Per informazioni sul ripristino dei nodi di archiviazione, vedere "[Ripristino da guasti al nodo di archivio \(sito di documentazione StorageGRID 11,8\)](#)".

Sostituire il nodo Linux

Sostituire un nodo Linux in StorageGRID

Se un guasto richiede l'implementazione di uno o più nuovi host fisici o virtuali o la reinstallazione di Linux su un host esistente, implementare e configurare l'host sostitutivo

prima di poter ripristinare il nodo grid. Questa procedura è una fase del processo di ripristino del nodo grid per tutti i tipi di nodi grid.

"Linux" si riferisce a una distribuzione Red Hat® Enterprise Linux® (RHEL), Ubuntu® o Debian®. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Questa procedura viene eseguita solo come un passaggio nel processo di ripristino di nodi di archiviazione basati su software, nodi amministrativi primari o non primari o nodi gateway. I passaggi sono identici indipendentemente dal tipo di nodo di griglia che si sta ripristinando.

Se su un host Linux fisico o virtuale sono ospitati più nodi della grid, puoi recuperarli in qualsiasi ordine. Tuttavia, se è presente il primary Admin Node, devi recuperarlo per primo per evitare di bloccare il recupero degli altri nodi della grid mentre tentano di contattare il primary Admin Node. Se non puoi recuperare prima il primary Admin Node e un non-primary Admin Node è disponibile, puoi usare un non-primary Admin Node per recuperare i nodi in qualsiasi ordine.

Distribuisci nuovi host Linux per StorageGRID

Con alcune eccezioni, è possibile preparare i nuovi host 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. Vedere ["Installare Linux"](#).



"Linux" si riferisce a una distribuzione RHEL, Ubuntu o Debian. Per un elenco delle versioni supportate, vedere ["Tool di matrice di interoperabilità NetApp \(IMT\)"](#).

Questa procedura include i passaggi per eseguire le seguenti attività:

1. Installare Linux.
2. Configurare la rete host.
3. Configurare lo storage host.
4. Installare il motore del container.
5. Installare il servizio host StorageGRID.



Interrompere dopo aver completato l'attività "Installa servizio host StorageGRID" nelle istruzioni di installazione. Non avviare l'attività "distribuzione dei nodi della griglia".

Durante l'esecuzione di questi passaggi, prendere nota delle seguenti importanti linee guida:

- Assicurarsi di utilizzare gli stessi nomi di interfaccia host utilizzati sull'host originale.
- Se si utilizza lo storage condiviso per supportare i nodi StorageGRID o si sono spostati alcuni o tutti i dischi o gli SSD dai nodi guasti ai nodi sostitutivi, è necessario ristabilire le stesse mappature dello storage presenti sull'host originale. Ad esempio, se sono stati utilizzati WWID e alias in `/etc/multipath.conf` come consigliato nelle istruzioni di installazione, assicurarsi di utilizzare le stesse coppie alias/WWID in `/etc/multipath.conf` sull'host sostitutivo.
- Se il nodo StorageGRID utilizza lo storage assegnato da un sistema NetApp ONTAP, verifica che il volume non disponga di una policy di tiering FabricPool abilitata. La disattivazione del tiering FabricPool per i volumi utilizzati con i nodi StorageGRID semplifica la risoluzione dei problemi e le operazioni di storage.



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

Ripristina i nodi StorageGRID sull'host

Per ripristinare un nodo Grid guasto in un nuovo host Linux, eseguire questa procedura per ripristinare il file di configurazione del nodo.

1. [Ripristinare e convalidare il nodo](#) ripristinando il file di configurazione del nodo. Per una nuova installazione, viene creato un file di configurazione del nodo per ciascun nodo della griglia da installare su un host. Quando si ripristina un nodo della griglia su un host sostitutivo, il file di configurazione del nodo viene ripristinato o sostituito per eventuali nodi della griglia guasti.
2. [Avviare il servizio host StorageGRID](#).
3. Secondo necessità, [ripristinare i nodi che non si avviano](#).

Se sono stati conservati volumi di storage a blocchi dall'host precedente, potrebbe essere necessario eseguire ulteriori procedure di ripristino. I comandi di questa sezione consentono di determinare quali procedure aggiuntive sono necessarie.

Ripristinare e validare i nodi della griglia

Se recuperi un nodo da un nodo Admin non primario, imposta ADMIN_IP sull'indirizzo IP della Grid Network del nodo Admin non primario, così il nodo recuperato si registra con il nodo Admin non primario invece che con il nodo Admin primario. Per visualizzare le regole per le chiavi della Admin Network, consulta ["Creare file di configurazione del nodo StorageGRID per le distribuzioni Linux"](#).

È necessario ripristinare i file di configurazione della griglia per eventuali nodi della griglia guasti, quindi validare i file di configurazione della griglia e risolvere eventuali errori.

A proposito di questa attività

È possibile importare qualsiasi nodo della griglia che dovrebbe essere presente sull'host, a condizione che il suo `/var/local` volume non sia stato perso a causa dell'errore dell'host precedente. Ad esempio, il `/var/local` volume potrebbe esistere ancora se si utilizza lo storage condiviso per i volumi di dati del sistema StorageGRID, come descritto nelle istruzioni di installazione di StorageGRID per il sistema operativo Linux in uso. L'importazione del nodo ripristina il file di configurazione del nodo sull'host.

Se non è possibile importare nodi mancanti, è necessario ricreare i file di configurazione della griglia.

È quindi necessario convalidare il file di configurazione della griglia e risolvere eventuali problemi di rete o storage che potrebbero verificarsi prima di riavviare StorageGRID. Quando si crea nuovamente il file di configurazione per un nodo, è necessario utilizzare lo stesso nome per il nodo sostitutivo utilizzato per il nodo che si sta ripristinando.

Vedi ["Istruzioni per l'installazione di Linux"](#) per maggiori informazioni sulla posizione del `/var/local` volume per un nodo.

Fasi

1. Nella riga di comando dell'host recuperato, elencare tutti i nodi StorageGRID attualmente configurati: `sudo storagegrid node list`

Se non sono configurati nodi di griglia, non verrà generato alcun output. Se alcuni nodi della griglia sono configurati, l'output deve essere nel seguente formato:

Name	Metadata-Volume
dc1-adm1	/dev/mapper/sgws-adm1-var-local
dc1-gw1	/dev/mapper/sgws-gw1-var-local
dc1-sn1	/dev/mapper/sgws-sn1-var-local
dc1-arc1	/dev/mapper/sgws-arc1-var-local

Se alcuni o tutti i nodi della griglia che devono essere configurati sull'host non sono elencati, è necessario ripristinare i nodi della griglia mancanti.

2. Per importare i nodi della griglia che hanno un /var/local volume:

- Esegui il seguente comando per ogni nodo da importare:`sudo storagegrid node import node-var-local-volume-path`

Il `storagegrid node import` comando ha esito positivo solo se il nodo di destinazione è stato chiuso in modo netto sull'host su cui è stato eseguito l'ultima volta. In caso contrario, si verificherà un errore simile al seguente:

```
This node (node-name) appears to be owned by another host (UUID host-uuid).
```

Use the `--force` flag if you are sure import is safe.

- Se viene visualizzato l'errore relativo al nodo di proprietà di un altro host, eseguire nuovamente il comando con l' `--force` indicatore per completare l'importazione:`sudo storagegrid --force node import node-var-local-volume-path`



Tutti i nodi importati con il `--force` flag richiederanno ulteriori operazioni di ripristino prima di poter rientrare nella griglia, come descritto in ["Cosa c'è di seguito: Se necessario, eseguire ulteriori passaggi di ripristino"](#).

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 ["Creare file di configurazione del nodo"](#).



Quando si crea nuovamente il file di configurazione per un nodo, è necessario utilizzare lo stesso nome per il nodo sostitutivo utilizzato per il nodo che si sta ripristinando. Per le implementazioni Linux, assicurarsi che il nome del file di configurazione contenga il nome del nodo. Se possibile, utilizzare le stesse interfacce di rete, le mappature dei dispositivi a blocchi e gli stessi indirizzi IP. Questa procedura riduce al minimo la quantità di dati che devono essere copiati nel nodo durante il ripristino, il che potrebbe rendere il ripristino molto più rapido (in alcuni casi, minuti piuttosto che settimane).



Se si utilizzano nuovi dispositivi a blocchi (dispositivi che il nodo StorageGRID non ha utilizzato in precedenza) come valori per una qualsiasi delle variabili di configurazione che iniziano con `BLOCK_DEVICE_` quando si crea nuovamente il file di configurazione per un nodo, seguire le linee guida riportate in [Correggere gli errori del dispositivo a blocchi mancanti](#).

4. Eseguire il seguente comando sull'host ripristinato per elencare tutti i nodi StorageGRID.

```
sudo storagegrid node list
```

5. Convalidare il file di configurazione del nodo per ogni nodo della griglia il cui nome è stato visualizzato nell'output dell'elenco dei nodi StorageGRID:

```
sudo storagegrid node validate node-name
```

Prima di avviare il servizio host StorageGRID, è necessario risolvere eventuali errori o avvisi. Le sezioni seguenti forniscono ulteriori dettagli sugli errori che potrebbero avere un significato speciale durante il ripristino.

Correggere gli errori di interfaccia di rete mancanti

Se la rete host non è configurata correttamente o un nome non è scritto correttamente, si verifica un errore quando StorageGRID controlla la mappatura specificata nel `/etc/storagegrid/nodes/node-name.conf` file.

Potrebbe essere visualizzato un errore o un avviso corrispondente a questo modello:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: GRID_NETWORK_TARGET = <host-interface-name>
      <node-name>: Interface <host-interface-name>' does not exist
```

L'errore potrebbe essere segnalato per Grid Network, Admin Network o Client Network. Questo errore indica che il `/etc/storagegrid/nodes/node-name.conf` file associa la rete StorageGRID indicata all'interfaccia host denominata *host-interface-name*, ma non esiste alcuna interfaccia con tale nome sull'host corrente.

Se viene visualizzato questo errore, verificare di aver completato la procedura descritta in ["Implementare nuovi host Linux"](#). Utilizzare gli stessi nomi per tutte le interfacce host utilizzati sull'host originale.

Se non è possibile assegnare un nome alle interfacce host in modo che corrispondano al file di configurazione del nodo, è possibile modificare il file di configurazione del nodo e modificare il valore DI `GRID_NETWORK_TARGET`, `ADMIN_NETWORK_TARGET` o `CLIENT_NETWORK_TARGET` in modo che corrisponda a un'interfaccia host esistente.

Assicurarsi che l'interfaccia host fornisca l'accesso alla porta di rete fisica o alla VLAN appropriata e che l'interfaccia non faccia riferimento direttamente a un dispositivo di collegamento o di bridge. È necessario configurare una VLAN (o un'altra interfaccia virtuale) sulla parte superiore del dispositivo bond sull'host oppure utilizzare una coppia di bridge e Virtual Ethernet (veth).

Correggere gli errori del dispositivo a blocchi mancanti

Il sistema verifica che ciascun nodo recuperato sia mappato a un file speciale valido per il dispositivo a blocchi o a un softlink valido a un file speciale per il dispositivo a blocchi. Se StorageGRID trova una mappatura non valida nel `/etc/storagegrid/nodes/node-name.conf` file, viene visualizzato un errore relativo al dispositivo di blocco mancante.

Se si verifica un errore corrispondente a questo modello:

```
Checking configuration file /etc/storagegrid/nodes/<node-name>.conf for
node <node-name>...
ERROR: <node-name>: BLOCK_DEVICE_PURPOSE = <path-name>
       <node-name>: <path-name> does not exist
```

Significa che `/etc/storagegrid/nodes/node-name.conf` associa il dispositivo a blocchi utilizzato da `node-name` PURPOSE al nome percorso specificato nel file system Linux, ma non c'è un file speciale del dispositivo a blocchi valido, o softlink a un file speciale del dispositivo a blocchi, in quella posizione.

Verificare di aver completato le operazioni descritte in ["Implementare nuovi host Linux"](#). Utilizzare gli stessi nomi persistenti dei dispositivi per tutti i dispositivi a blocchi utilizzati sull'host originale.

Se non è possibile ripristinare o ricreare il file speciale del dispositivo di blocco mancante, è possibile allocare un nuovo dispositivo di blocco con le dimensioni e la categoria di archiviazione appropriate e modificare il file di configurazione del nodo per modificare il valore di `BLOCK_DEVICE_PURPOSE` per puntare al nuovo file speciale del dispositivo di blocco.

Determina la dimensione e la categoria di archiviazione appropriate utilizzando le tabelle per il tuo sistema operativo Linux. Vedere ["Requisiti di storage e performance"](#).

Rivedere le raccomandazioni per ["configurazione dell'archiviazione host"](#) prima di procedere con la sostituzione del dispositivo a blocchi.



Se è necessario fornire un nuovo dispositivo di archiviazione a blocchi per qualsiasi variabile del file di configurazione che inizia con `BLOCK_DEVICE_` perché il dispositivo di blocco originale è stato perso con l'host guasto, assicurarsi che il nuovo dispositivo di blocco non sia formattato prima di tentare ulteriori procedure di ripristino. Il nuovo dispositivo a blocchi non verrà formattato se si utilizza lo storage condiviso e si è creato un nuovo volume. In caso di dubbi, eseguire il seguente comando per tutti i nuovi file speciali del dispositivo di storage a blocchi.



Eseguire il seguente comando solo per i nuovi dispositivi di storage a blocchi. Non eseguire questo comando se si ritiene che lo storage a blocchi contenga ancora dati validi per il nodo da ripristinare, in quanto i dati sul dispositivo andranno persi.

```
sudo dd if=/dev/zero of=/dev/mapper/my-block-device-name bs=1G count=1
```

Avviare il servizio host StorageGRID

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

Fasi

1. Eseguire i seguenti comandi su ciascun host:

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

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

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

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

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

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

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

Ripristinare i nodi che non si avviano normalmente

Se un nodo StorageGRID non si ricongiungerà normalmente alla griglia e non verrà visualizzato come ripristinabile, potrebbe essere danneggiato. È possibile forzare il nodo in modalità di ripristino.

Fasi

1. Verificare che la configurazione di rete del nodo sia corretta.

Il nodo potrebbe non essere riuscito a ricongiungersi alla griglia a causa di mappature dell'interfaccia di rete non corrette o di un gateway o indirizzo IP Grid Network non corretto.

2. Se la configurazione di rete è corretta, eseguire il `force-recovery` comando:

```
sudo storagegrid node force-recovery node-name
```

3. Eseguire le fasi di ripristino aggiuntive per il nodo. Vedere ["Cosa c'è di seguito: Se necessario, eseguire ulteriori passaggi di ripristino"](#).

Eseguire ulteriori passaggi di ripristino del nodo StorageGRID

A seconda delle azioni specifiche intraprese per eseguire i nodi StorageGRID sull'host sostitutivo, potrebbe essere necessario eseguire ulteriori operazioni di ripristino per ciascun nodo.

Il ripristino del nodo è completo se non è stato necessario intraprendere alcuna azione correttiva durante la sostituzione dell'host Linux o il ripristino del nodo Grid guasto nel nuovo host.

Azioni correttive e passi successivi

Durante la sostituzione del nodo, potrebbe essere necessario intraprendere una delle seguenti azioni correttive:

- È stato necessario utilizzare `--force` il flag per importare il nodo.
- Per qualsiasi `<PURPOSE>`, il valore della `BLOCK_DEVICE_<PURPOSE>` variabile del file di configurazione si riferisce a un dispositivo di blocco che non contiene gli stessi dati che ha fatto prima dell'errore dell'host.

- Hai emesso `storagegrid node force-recovery node-name` per il nodo.
- È stato aggiunto un nuovo dispositivo a blocchi.

Se è stata eseguita una di queste azioni correttive, è necessario eseguire ulteriori operazioni di ripristino.

Tipo di ripristino	Passo successivo
Nodo amministratore primario	• "Seleziona Avvia ripristino per configurare il nodo Admin primario" • "Recupera il nodo Admin primario usando un nodo Admin non primario"
Nodo amministrativo non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"
Nodo gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo di storage (basato su software): • Se è stato utilizzato <code>--force</code> il flag per importare il nodo o è stato emesso <code>storagegrid node force-recovery node-name</code> • Se è stata eseguita una reinstallazione completa del nodo o se è stato necessario ripristinare <code>/var/local</code>	"Selezionare Avvia ripristino per configurare il nodo di storage"
Nodo di storage (basato su software): • Se è stato aggiunto un nuovo dispositivo a blocchi. • Se, per qualsiasi <code><PURPOSE></code>, il valore della <code>BLOCK_DEVICE_<PURPOSE></code> variabile del file di configurazione si riferisce a un dispositivo a blocchi che non contiene gli stessi dati che ha fatto prima dell'errore dell'host.	"Ripristino in seguito a un errore del volume di storage in cui il disco di sistema è intatto"

Sostituisci un nodo VMware in StorageGRID con un nodo di ripristino

Quando si ripristina un nodo StorageGRID guasto ospitato su VMware, si rimuove il nodo guasto e si implementa un nodo di ripristino.

Prima di iniziare

Hai determinato che la macchina virtuale non può essere ripristinata e deve essere sostituita.

A proposito di questa attività

VMware vSphere Web Client viene utilizzato per rimuovere prima la macchina virtuale associata al nodo Grid guasto. Quindi, è possibile implementare una nuova macchina virtuale.

Questa procedura è solo una fase del processo di ripristino del nodo grid. La procedura di rimozione e implementazione del nodo è identica per tutti i nodi VMware, inclusi nodi amministrativi, nodi storage e nodi gateway.

Fasi

1. Accedere a VMware vSphere Web Client.
2. Passare alla macchina virtuale del nodo della griglia guasto.
3. Prendere nota di tutte le informazioni necessarie per implementare il nodo di ripristino.
 - a. Fare clic con il pulsante destro del mouse sulla macchina virtuale, selezionare la scheda **Edit Settings** (Modifica impostazioni) e annotare le impostazioni in uso.
 - b. Selezionare la scheda **vApp Options** per visualizzare e registrare le impostazioni di rete del nodo della griglia.
4. Se il nodo Grid guasto è un nodo Storage, determinare se uno dei dischi rigidi virtuali utilizzati per lo storage dei dati non è danneggiato e conservarlo per il ricollegamento al nodo Grid ripristinato.
5. Spegnerne la macchina virtuale.
6. Selezionare **azioni > tutte le azioni vCenter > Elimina dal disco** per eliminare la macchina virtuale.
7. Distribuisci una nuova macchina virtuale come nodo sostitutivo e collegala a una o più reti StorageGRID . Per le istruzioni vedere ["Implementazione di un nodo StorageGRID come macchina virtuale"](#) .

Quando si implementa il nodo, è possibile rimappare le porte del nodo o aumentare le impostazioni della CPU o della memoria.



Dopo aver implementato il nuovo nodo, è possibile aggiungere nuovi dischi virtuali in base ai requisiti di storage, ricollegare eventuali dischi rigidi virtuali conservati dal nodo Grid guasto precedentemente rimosso o da entrambi.

8. Completare la procedura di ripristino del nodo, in base al tipo di nodo che si sta ripristinando.

Tipo di nodo	Passare a.
Nodi di amministrazione	"Ripristino del nodo Admin primario o non primario in StorageGRID"
Nodo gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo di storage	"Selezionare Avvia ripristino per configurare il nodo di storage"

Sostituisci il nodo VMware in StorageGRID con SG1000 o SG100

Se il nodo di amministrazione primario è in esecuzione come nodo VMware, puoi sostituirlo con un'appliance di servizi SG1000 o SG100.



Dopo aver completato e verificato la sostituzione del nodo, devi eliminare il nodo VMware originale. Lasciare il vecchio nodo in funzione rischia una grave interruzione della grid se dovesse tornare online.

Prima di iniziare

- Hai determinato che la macchina virtuale non può essere ripristinata e deve essere sostituita.
- Hai verificato che non ci sono procedure di manutenzione della rete in corso.
- Hai confermato che la versione di StorageGRID Appliance Installer sull'appliance di servizio SG1000 o SG100 corrisponde alla versione del software del tuo sistema StorageGRID.
- Hai le seguenti informazioni sul nodo amministratore primario esistente:

Nome del nodo: Devi installare l'appliance dei servizi usando lo stesso nome del nodo del nodo di amministrazione primario esistente. Il nome del nodo è il nome host (nome del sistema).

Indirizzo IP: Puoi assegnare all'appliance di servizi lo stesso indirizzo IP del nodo Admin primario esistente (consigliato), oppure puoi scegliere un nuovo indirizzo IP non utilizzato su ciascuna rete.

- Si dispone della passphrase di provisioning.

Passaggio 1: Sostituisci il nodo VMware

Per prima cosa rimuovi il nodo Admin primario esistente nel Grid Manager. Poi installi l'appliance di servizi SG1000 o SG100 come nuovo nodo Admin primario usando StorageGRID Appliance Installer e recuperi il nodo. Se usi un nuovo indirizzo IP, puoi installare l'appliance di servizi prima di rimuovere il nodo Admin primario esistente.

Usa l'indirizzo IP esistente

Sostituisci il nodo amministratore primario utilizzando l'indirizzo IP del nodo amministratore primario esistente.

Fasi

1. Scarica il pacchetto di ripristino da Grid Manager:
 - a. Seleziona **Manutenzione > Recovery package**.
 - b. Inserisci la passphrase di provisioning e scarica il pacchetto.
2. Accedi al nodo amministratore primario esistente:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Passa all'utente root: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

3. ["Copia i log di controllo dal nodo amministratore primario esistente"](#).
4. Arresta Server Manager e tutti i servizi sul nodo della griglia:

```
shutdown -h now
```

Attendi fino a 15 minuti perché i servizi si fermino.

5. ["Installa l'appliance di servizi SG1000 o SG100"](#).
6. ["Distribuisci l'appliance di servizi SG1000 o SG100"](#).
7. Dopo aver selezionato **Avvia installazione**, attendi circa dieci minuti perché l'installazione raggiunga la fase **Carica il programma di installazione di StorageGRID**.

Dopo sei o sette minuti, il browser reindirizza per avviare il ripristino.

8. Verifica che l'orologio dell'apparecchio sia corretto.
 - a. Utilizza SSH per connetterti alla porta 8022:
 - i. Inserisci il comando: `ssh -p 8022 admin@grid_node_IP`.
 - ii. Passa all'utente root: `su -`
 - iii. Inserisci `netappl!`.
 - b. Verifica che l'orologio dell'appliance sia entro pochi minuti dall'UTC corrente. Se necessario, imposta la data e l'ora corrette:

```
date -s "DD Mon YYYY HH:MM:SS"
```

9. Torna al browser web e seleziona **Ripristina un nodo amministratore primario non funzionante**.

10. Carica il [pacchetto di ripristino che hai scaricato](#).
11. Inserisci la passphrase di provisioning e seleziona **Avvia ripristino**.

Viene visualizzata la barra di avanzamento del ripristino. Attendi dai sei ai dieci minuti perché il processo di ripristino si completi e i servizi si avviino.

12. Accedi a Grid Manager quando richiesto.

Usa il nuovo indirizzo IP

Sostituisci il nodo amministratore primario usando un nuovo indirizzo IP.

Fasi

1. ["Installa l'appliance di servizi SG1000 o SG100"](#).
2. Controlla che l'orologio del dispositivo sia corretto per evitare errori NTP durante il ripristino.
 - a. Utilizza SSH per connetterti alla porta 8022:
 - i. Inserisci il comando: `ssh -p 8022 admin@grid_node_IP`.
 - ii. Passa all'utente root: `su -`
 - iii. Inserisci `netapp1!`.
 - b. Verifica che l'orologio dell'appliance sia entro pochi minuti dall'ora corrente UTC (Tempo Coordinato Universale). Se necessario, imposta la data e l'ora corrette.

```
date -s "DD Mon YYYY HH:MM:SS"
```

3. Vai su **Carica software StorageGRID** nel programma di installazione dell'appliance StorageGRID e verifica che la versione del software precaricato sull'appliance corrisponda alla versione di StorageGRID in esecuzione sulla griglia. Se le versioni non corrispondono:
 - a. Scarica il pacchetto di installazione Debian corretto di StorageGRID da ["Sito di supporto NetApp"](#).
 - b. Seleziona **Rimuovi** per rimuovere il software di installazione.
 - c. Carica i file `storagegrid-webscale-images-<sg-version>.deb` e `storagegrid-webscale-images-<sgversion>.deb.md5`.
4. Nella scheda Home di StorageGRID Appliance Installer, seleziona **Primary Admin (with Load Balancer)** come tipo di nodo.
5. Inserisci il nome del nodo. Il nome del nodo deve corrispondere al nome del nodo Admin Node primario esistente.



Non selezionare **Avvia installazione**.

6. Verifica se la sottorete del nuovo indirizzo IP è nella rete di griglia. Se la nuova sottorete IP non è presente, aggiungila alla rete di griglia:
 - a. In Grid Manager, seleziona **Manutenzione > Rete Grid**.
 - b. Inserisci la passphrase di provisioning per aggiornare l'elenco delle sottoreti.
7. Scarica il pacchetto di ripristino da GRID Manager:
 - a. Seleziona **Manutenzione > Recovery package**.

b. Inserisci la passphrase di provisioning, quindi scarica il pacchetto.

8. Accedi al nodo amministratore primario esistente:

a. Immettere il seguente comando: `ssh admin@grid_node_IP`

b. Immettere la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla directory principale: `su -`

d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

9. ["Copia i log di controllo dal nodo amministratore primario esistente"](#).

10. Arresta Server Manager e tutti i servizi sul nodo della griglia:

```
service servermanager stop
```

Attendi fino a 15 minuti perché i servizi si fermino.

11. Nella scheda Home del programma di installazione dell'appliance StorageGRID:

a. Verifica le seguenti impostazioni:

- Il tipo di nodo è impostato su **Primary Admin (con Load Balancer)**
- Il nome del nodo corrisponde al nome del nodo Admin primario esistente

b. Annota il nuovo indirizzo IP.

12. Seleziona **Avvia installazione**.

Consenti circa 10 minuti perché l'installazione arrivi al passaggio **Load StorageGRID installer**.

Dopo sei o sette minuti, il browser reindirizza per avviare la procedura di ripristino.

13. Verifica che l'orologio dell'apparecchio sia corretto.

a. Utilizza SSH per connetterti alla porta 8022:

i. Inserisci il comando: `ssh -p 8022 admin@grid_node_IP`.

ii. Passa all'utente root: `su -`

iii. Inserisci `netapp1!`.

b. Verifica che l'orologio dell'appliance sia entro pochi minuti dall'UTC corrente. Se necessario, imposta la data e l'ora corrette:

```
date -s "DD Mon YYYY HH:MM:SS"
```

14. Torna al browser web, quindi seleziona **Ripristina un nodo Admin primario non funzionante**.

15. Carica il [pacchetto di ripristino che hai scaricato](#).

16. Inserisci la passphrase di provisioning e seleziona **Avvia ripristino**.

La pagina di ripristino del nodo Admin primario scompare e poi riappare. Se selezioni di nuovo **Avvia**

ripristino, 500: Internal Server Error appare perché il ripristino è stato avviato ma non può inviare l'aggiornamento al Grid Manager, che sta usando il nuovo indirizzo IP. Risolvi questo problema aggiornando l'indirizzo IP del nodo Admin primario nel file `/etc/hosts`:

a. Utilizza SSH per connetterti alla porta 8022:

i. Inserisci il comando: `ssh -p 8022 admin@grid_node_IP`.

ii. Passa all'utente root: `su -`

iii. Immettere la password elencata nel `Passwords.txt` file.

b. Accedi al registro:

```
tail /var/local/log/install.log
```

Dovresti visualizzare ripetutamente il seguente errore: `curl: (7) Failed to connect to <primary_Admin_Node_name> port9999: No route to host`

Questo è il comportamento previsto. StorageGRID sta tentando di inviare l'aggiornamento al nodo Admin primario utilizzando l'indirizzo IP del nodo Admin primario esistente.

c. Verifica che il container sia in esecuzione:

```
storagegrid node status
```

```
storagegrid node enter <primary_Admin_Node_name>
```

a. Nel `/etc/hosts` file all'interno del container, sostituisci l'indirizzo IP del nodo Admin primario esistente con il nuovo indirizzo IP.

b. Salva il file.

c. Torna al browser web. Dopo alcuni secondi, appare la barra di avanzamento del ripristino.

Concedi da sei a dieci minuti perché il processo di ripristino si completi e i servizi si avviino.

17. Accedi a Grid Manager quando richiesto.

18. Aggiorna il pacchetto di ripristino:

a. Accedere al nodo di amministrazione principale:

i. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`

ii. Passa all'utente root: `su -`

iii. Inserisci il seguente comando: `change-ip`

b. Seleziona l'opzione **3 – Modifica elenchi di sottoreti di rete amministrativa**, quindi aggiungi la nuova sottorete.

StorageGRID genera automaticamente un nuovo pacchetto di ripristino con il nuovo indirizzo IP del nodo Admin primario.

19. Scarica il pacchetto di ripristino più recente dal Grid Manager.

Passaggio 2: Completa il ripristino del nodo

Utilizza un nodo Admin non primario esistente come nodo Admin di origine per le procedure di ripristino (log di audit, database del nodo Admin e metriche Prometheus). Se la grid non ha un nodo Admin non primario, puoi usare il nodo VMware originale che viene sostituito, a patto che sia in esecuzione su un indirizzo IP diverso da quello del nodo Admin primario ripristinato.

Fasi

1. ["Ripristina il registro di controllo"](#).
2. ["Ripristina il database Admin Node"](#).
3. ["Ripristina metriche Prometheus"](#).
4. Verifica che il nuovo nodo Admin primario funzioni correttamente. Poi elimina subito il nodo VM o il container bare-metal originale.

Sostituire il nodo guasto con l'appliance di servizi

Sostituire il nodo StorageGRID guasto con l'appliance di servizi

È possibile utilizzare un'appliance di servizi per recuperare un nodo gateway guasto, un nodo di amministrazione non primario guasto o un nodo di amministrazione primario guasto ospitato su VMware, un host Linux o un'appliance di servizi. Questa procedura è una fase della procedura di ripristino del nodo di rete.

Prima di iniziare

- Hai determinato che è vera una delle seguenti situazioni:
 - Impossibile ripristinare la macchina virtuale che ospita il nodo.
 - L'host Linux fisico o virtuale per il nodo grid è guasto e deve essere sostituito.
 - L'appliance di servizi che ospita il nodo Grid deve essere sostituita.
- Hai confermato che la versione del programma di installazione dell'appliance StorageGRID sul dispositivo di servizi corrisponde alla versione software del tuo sistema StorageGRID. Vedere ["Verificare e aggiornare la versione del programma di installazione dell'appliance StorageGRID"](#).



Non installare un'appliance di servizi SG110 e SG1100 o un'appliance di servizi SG100 e SG1000 nello stesso sito. Potrebbero verificarsi performance imprevedibili.

A proposito di questa attività

È possibile utilizzare un'appliance per i servizi per ripristinare un nodo grid guasto nei seguenti casi:

- Il nodo guasto era ospitato su VMware o Linux (["cambiamento di piattaforma"](#))
- Il nodo guasto era ospitato su un'appliance di servizi (["sostituzione della piattaforma"](#))

Installare l'appliance di servizi StorageGRID (solo cambio di piattaforma)

Quando si ripristina un nodo Grid guasto ospitato su VMware o su un host Linux e si utilizza un'appliance di servizi per il nodo sostitutivo, è necessario prima installare il nuovo hardware dell'appliance utilizzando lo stesso nome di nodo (nome di sistema) del nodo guasto.

Prima di iniziare

Sono disponibili le seguenti informazioni sul nodo guasto:

- **Node name** (Nome nodo): È necessario installare l'appliance di servizi utilizzando lo stesso nome di nodo del nodo guasto. Il nome del nodo è il nome host (nome del sistema).
- **Indirizzi IP**: È possibile assegnare al dispositivo di servizi gli stessi indirizzi IP del nodo guasto, che è l'opzione preferita, oppure selezionare un nuovo indirizzo IP inutilizzato su ciascuna rete.

A proposito di questa attività

Eseguire questa procedura solo se si sta ripristinando un nodo guasto ospitato su VMware o Linux e lo si sta sostituendo con un nodo ospitato su un'appliance di servizi.

Fasi

1. Seguire le istruzioni per l'installazione di un nuovo dispositivo di servizi. Vedere ["Avvio rapido per l'installazione dell'hardware"](#).
2. Quando viene richiesto il nome di un nodo, utilizzare il nome del nodo guasto.

Preparare l'appliance StorageGRID per la reinstallazione (solo sostituzione della piattaforma)

Durante il ripristino di un nodo Grid ospitato su un'appliance di servizi, è necessario preparare l'appliance per la reinstallazione del software StorageGRID.

Eseguire questa procedura solo se si sta sostituendo un nodo guasto ospitato su un'appliance di servizi. Non seguire questi passaggi se il nodo guasto era originariamente ospitato su un host VMware o Linux.

Fasi

1. Accedere al nodo Grid guasto:
 - a. Immettere il seguente comando: `ssh admin@grid_node_IP`
 - b. Immettere la password elencata nel `Passwords.txt` file.
 - c. Immettere il seguente comando per passare alla directory principale: `su -`
 - d. Immettere la password elencata nel `Passwords.txt` file.

Quando si è collegati come root, il prompt cambia da `$` a `#`.

2. Preparare l'appliance per l'installazione del software StorageGRID. Immettere: `sgareinstall`
3. Quando viene richiesto di continuare, immettere: `y`

L'apparecchio si riavvia e la sessione SSH termina. In genere, il programma di installazione dell'appliance StorageGRID richiede circa 5 minuti, anche se in alcuni casi potrebbe essere necessario attendere fino a 30 minuti.

L'appliance di servizi viene reimpostata e i dati sul nodo Grid non sono più accessibili. Gli indirizzi IP configurati durante il processo di installazione originale devono rimanere intatti; tuttavia, si consiglia di confermarli al termine della procedura.

Dopo aver eseguito il `sgareinstall` comando, tutti gli account, le password e le chiavi SSH con provisioning StorageGRID vengono rimossi e vengono generate nuove chiavi host.

Avvia l'installazione del software StorageGRID su un'appliance di servizi

Per installare un nodo gateway o un nodo amministrativo su un'appliance di servizi, utilizzare il programma di installazione dell'appliance StorageGRID, incluso nell'appliance.

Prima di iniziare

- L'appliance viene installata in un rack, collegata alla rete e accesa.
- I collegamenti di rete e gli indirizzi IP vengono configurati per l'appliance mediante il programma di installazione dell'appliance StorageGRID.
- Se stai installando un Gateway Node o un Admin Node non primario, conosci l'indirizzo IP di uno dei seguenti Admin Node:
 - Il nodo Admin principale per la grid StorageGRID
 - Un nodo Admin non primario, se disponibile e se viene utilizzato per ripristinare il nodo
- Se stai ripristinando un nodo (incluso il nodo Admin primario) utilizzando un nodo Admin non primario, puoi specificare l'indirizzo IP di quel nodo Admin.
- Tutte le subnet della rete griglia elencate nella pagina di configurazione IP del programma di installazione dell'appliance StorageGRID sono definite nell'elenco delle subnet della rete griglia sul nodo di amministrazione primario.

Vedere ["Avvio rapido per l'installazione dell'hardware"](#).

- Si sta utilizzando un ["browser web supportato"](#).
- Uno degli indirizzi IP assegnati al dispositivo. È possibile utilizzare l'indirizzo IP per Admin Network, Grid Network o Client Network.
- Se si installa un nodo amministrativo primario, sono disponibili i file di installazione di Ubuntu o Debian per questa versione di StorageGRID.



Una versione recente del software StorageGRID viene precaricata sull'appliance di servizi durante la produzione. Se la versione precaricata del software corrisponde alla versione utilizzata nella distribuzione di StorageGRID, non sono necessari i file di installazione.

A proposito di questa attività

Per installare il software StorageGRID su un'appliance di servizi:

- Per un nodo Admin Node primario, devi specificare il nome del nodo e poi caricare i pacchetti software appropriati (se richiesto). Se stai ripristinando il nodo Admin Node primario e hai un Admin Node non primario nella tua grid, puoi scegliere se ripristinare il nodo usando un Admin Node non primario e specificando l'IP di quell'Admin Node oppure installare o ripristinare il nodo usando la configurazione attuale.
- Per un nodo Admin non primario o un nodo gateway, specificare o confermare l'indirizzo IP del nodo Admin primario e il nome del nodo.
- Avviare l'installazione e attendere la configurazione dei volumi e l'installazione del software.
- Durante il processo, l'installazione viene interrotta. Per riprendere l'installazione, è necessario accedere a Grid Manager e configurare il nodo in sospeso come sostituzione del nodo guasto.
- Una volta configurato il nodo, il processo di installazione dell'appliance viene completato e l'appliance viene riavviata.

Fasi

1. Aprire un browser e immettere uno degli indirizzi IP per il dispositivo di servizi.

`https://Controller_IP:8443`

Viene visualizzata la pagina iniziale del programma di installazione dell'appliance StorageGRID.

2. Per installare un nodo di amministrazione primario:
 - a. Nella sezione questo nodo, per **Node Type**, selezionare **Primary Admin**.
 - b. Nel campo **Nome nodo**, inserisci lo stesso nome utilizzato per il nodo che stai ripristinando e seleziona **Salva**.
 - c. Seleziona una delle due modalità disponibili nella sezione Modalità di installazione. Puoi scegliere tra il metodo Install a node or recover this node using current configuration oppure il metodo Recover this node using a non-primary Admin Node.

Metodo di configurazione corrente

Installa un nodo o ripristina questo nodo utilizzando la configurazione corrente.

- i. Nella sezione Installazione, verifica la versione del software indicata in Stato corrente. Se la versione del software pronta per l'installazione è corretta, salta direttamente a [Fase di installazione](#).
- ii. Se devi caricare una versione diversa del software, nel menu **Advanced** seleziona **Upload StorageGRID software**. Viene visualizzata la pagina Upload StorageGRID Software.
- iii. Seleziona **Sfoglia** per caricare il **pacchetto software** e il **file di checksum** per il software StorageGRID. I file vengono caricati automaticamente dopo che li hai selezionati.
- iv. Seleziona **Home** per tornare alla pagina iniziale di StorageGRID Appliance Installer.

Metodo del nodo Admin non primario

Ripristina questo nodo utilizzando un nodo Admin non primario.

- i. Nel campo IP del nodo amministratore non primario, inserisci l'indirizzo IP della rete grid del nodo amministratore non primario che vuoi usare per il ripristino e seleziona **Salva**.
- ii. Se la versione del software pronta per l'installazione è corretta, passare alla [Fase di installazione](#).

3. Per installare un nodo gateway o un nodo amministrativo non primario:
 - a. Nella sezione questo nodo, per **Node Type**, selezionare **Gateway** o **non-Primary Admin**, a seconda del tipo di nodo che si sta ripristinando.
 - b. Nel campo **Nome nodo**, inserisci lo stesso nome utilizzato per il nodo che stai ripristinando e seleziona **Salva**.
 - c. Nella sezione Primary Admin Node Connection (connessione nodo amministratore primario), determinare se è necessario specificare l'indirizzo IP per il nodo amministratore primario.

Il programma di installazione dell'appliance StorageGRID è in grado di rilevare automaticamente questo indirizzo IP, presupponendo che il nodo amministratore primario o almeno un altro nodo della griglia con ADMIN_IP configurato sia presente nella stessa sottorete.

d. Se questo indirizzo IP non viene visualizzato o è necessario modificarlo, specificare l'indirizzo:

Opzione	Descrizione
Immissione manuale dell'IP	a. Deselezionare la casella di controllo Enable Admin Node Discovery (attiva rilevamento nodo amministratore). b. Inserire l'indirizzo IP manualmente. c. Selezionare Salva. d. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".
Rilevamento automatico di tutti i nodi amministrativi primari connessi	a. Selezionare la casella di controllo Enable Admin Node Discovery (attiva rilevamento nodo amministratore). b. Dall'elenco degli indirizzi IP rilevati, selezionare il nodo di amministrazione principale per la griglia in cui verrà implementata l'appliance di servizi. c. Selezionare Salva. d. Attendere che lo stato della connessione del nuovo indirizzo IP diventi "pronto".

4. nella sezione Installation (Installazione), verificare che lo stato corrente sia Ready to start installation of node name (Pronto per avviare l'installazione del nome del nodo) e che il pulsante **Start Installation** (Avvia installazione) sia attivato.

Se il pulsante **Avvia installazione** non è abilitato, potrebbe essere necessario modificare la configurazione di rete o le impostazioni della porta. Fare riferimento alle istruzioni di manutenzione dell'apparecchio.

5. Dalla home page di StorageGRID Appliance Installer, seleziona **Avvia installazione**.

Lo stato attuale cambia in "Installazione in corso" e viene visualizzata la pagina di installazione del monitor.



Se devi accedere manualmente alla pagina di installazione del Monitor, seleziona **Monitor installation** dalla barra dei menu.

Monitorare l'installazione degli appliance di servizi StorageGRID

Il programma di installazione dell'appliance StorageGRID indica lo stato fino al completamento dell'installazione. Una volta completata l'installazione del software, l'appliance viene riavviata.

Fasi

1. Per monitorare l'avanzamento dell'installazione, seleziona **Monitora installazione** dalla barra dei menu.

La pagina di installazione di Monitor mostra lo stato di avanzamento dell'installazione.

La barra di stato blu indica l'attività attualmente in corso. Le barre di stato verdi indicano le attività completate correttamente.



Il programma di installazione garantisce che le attività completate in un'installazione precedente non vengano rieseguite. Se si sta eseguendo nuovamente un'installazione, tutte le attività che non devono essere rieseguite vengono visualizzate con una barra di stato verde e lo stato "saltato".

2. Esaminare i progressi delle prime due fasi dell'installazione.

◦ **1. Configurare lo storage**

Durante questa fase, il programma di installazione cancella qualsiasi configurazione esistente dai dischi e configura le impostazioni dell'host.

◦ **2. Installare il sistema operativo**

Durante questa fase, il programma di installazione copia l'immagine del sistema operativo di base per StorageGRID dal nodo di amministrazione primario all'appliance o installa il sistema operativo di base dal pacchetto di installazione per il nodo di amministrazione primario.

3. Continuare a monitorare l'avanzamento dell'installazione fino a quando non si verifica una delle seguenti condizioni:

- Per i nodi gateway dell'appliance o i nodi di amministrazione dell'appliance non primaria, la fase **Install StorageGRID** (Installazione del nodo) viene sospesa e sulla console integrata viene visualizzato un messaggio che richiede di approvare questo nodo nel nodo di amministrazione utilizzando Gestione griglia.
- Per i nodi di amministrazione primari dell'appliance, viene visualizzata una quinta fase (carica programma di installazione StorageGRID). Se la quinta fase è in corso per più di 10 minuti, aggiornare la pagina manualmente.

4. Passare alla fase successiva del processo di ripristino per il tipo di nodo Grid dell'appliance che si sta ripristinando.

Tipo di ripristino	Riferimento
Nodo gateway	"Selezionare Avvia ripristino per configurare il nodo gateway"
Nodo amministrativo non primario	"Selezionare Avvia ripristino per configurare il nodo di amministrazione non primario"
Nodo amministratore primario	"Configurare il nodo amministrativo primario sostitutivo"

Come il supporto tecnico ripristina un sito StorageGRID

In caso di guasto di un intero sito StorageGRID o in caso di guasto di più nodi di storage, è necessario contattare il supporto tecnico. Il supporto tecnico valuterà la tua situazione, svilupperà un piano di recovery e ripristinerà i nodi o il sito guasti in modo da soddisfare gli obiettivi di business, ottimizzare i tempi di recovery e prevenire inutili perdite di dati.



Il ripristino del sito può essere eseguito solo dal supporto tecnico.

I sistemi StorageGRID sono resilienti a una vasta gamma di guasti e puoi eseguire molte procedure di

ripristino e manutenzione autonomamente. Tuttavia, è difficile creare una procedura di ripristino del sito semplice e generalizzata, in quanto i passaggi dettagliati dipendono da fattori specifici della situazione. Ad esempio:

- **I tuoi obiettivi di business:** Dopo la perdita completa di un sito StorageGRID, dovresti valutare come soddisfare al meglio i tuoi obiettivi di business. Ad esempio, si desidera ricostruire il sito smarrito sul posto? Sostituire il sito StorageGRID perso in una nuova posizione? La situazione di ogni cliente è diversa e il tuo piano di recovery deve essere progettato per soddisfare le tue priorità.
- **Natura esatta del guasto:** Prima di iniziare un ripristino del sito, stabilire se i nodi del sito guasto sono intatti o se i nodi di storage contengono oggetti ripristinabili. Se si ricostruiscono nodi o volumi di storage che contengono dati validi, potrebbe verificarsi una perdita di dati non necessaria.
- **Criteri ILM attivi:** Il numero, il tipo e la posizione delle copie degli oggetti nella griglia sono controllati dai criteri ILM attivi. Le specifiche dei criteri ILM possono influire sulla quantità di dati ripristinabili e sulle tecniche specifiche necessarie per il ripristino.



Se un sito contiene l'unica copia di un oggetto e il sito viene perso, l'oggetto viene perso.

- **Coerenza bucket (o contenitore):** La coerenza applicata a un bucket (o contenitore) influisce sul fatto che StorageGRID replica completamente i metadati degli oggetti in tutti i nodi e siti prima di informare il client del successo dell'acquisizione degli oggetti. Se il valore di coerenza consente un'eventuale coerenza, alcuni metadati degli oggetti potrebbero essere andati persi nel guasto del sito. Ciò può influire sulla quantità di dati ripristinabili e potenzialmente sui dettagli della procedura di ripristino.
- **Cronologia delle modifiche recenti:** I dettagli della procedura di ripristino possono essere influenzati dall'eventuale presenza di procedure di manutenzione in corso al momento dell'errore o dall'eventuale modifica recente delle policy ILM. Prima di iniziare un ripristino del sito, il supporto tecnico deve valutare la cronologia recente del tuo grid e la sua situazione attuale.



Il ripristino del sito può essere eseguito solo dal supporto tecnico.

Di seguito viene fornita una panoramica generale del processo utilizzato dal supporto tecnico per il ripristino di un sito guasto:

1. Assistenza tecnica:
 - a. Effettua una valutazione dettagliata del guasto.
 - b. Collaborerà per esaminare gli obiettivi aziendali.
 - c. Sviluppa un piano di ripristino personalizzato in base alla situazione.
2. Se il nodo amministrativo primario è guasto, il supporto tecnico lo ripristina.
3. Il supporto tecnico recupera tutti i nodi di storage, seguendo questa descrizione:
 - a. Sostituire l'hardware o le macchine virtuali del nodo di storage secondo necessità.
 - b. Ripristinare i metadati dell'oggetto nel sito guasto.
 - c. Ripristinare i dati dell'oggetto nei nodi di storage ripristinati.



La perdita di dati si verifica se vengono utilizzate le procedure di ripristino per un singolo nodo di storage guasto.



In caso di guasto di un intero sito, il supporto tecnico utilizza comandi specializzati per ripristinare correttamente gli oggetti e i metadati degli oggetti.

4. Il supporto tecnico recupera altri nodi guasti.

Una volta ripristinati i metadati degli oggetti e i dati, il supporto tecnico utilizza procedure standard per recuperare nodi Gateway non riusciti o nodi amministrativi non primari.

Informazioni correlate

["Decommissionare il sito"](#)

Soluzioni e risorse StorageGRID

Vai a "[Soluzioni e risorse 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 l'accesso a dichiarazioni di copyright, marchi, 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 dei marchi NetApp sono marchi di NetApp, Inc. Altri nomi di società e prodotti potrebbero essere marchi dei rispettivi proprietari.

["https://www.netapp.com/company/legal/trademarks/"](https://www.netapp.com/company/legal/trademarks/)

Brevetti

Un elenco aggiornato dei brevetti di proprietà di NetApp è disponibile all'indirizzo:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Direttiva sulla privacy

["https://www.netapp.com/company/legal/privacy-policy/"](https://www.netapp.com/company/legal/privacy-policy/)

licenza API

La presente documentazione non concede alcuna licenza o altri diritti alla StorageGRID S3 REST API. Qualsiasi utilizzo o accesso alla StorageGRID S3 REST API richiede ed è soggetto a un contratto di licenza separato con NetApp.

Open source

I file di avviso forniscono informazioni sul copyright e sulle licenze di terze parti utilizzate nel software NetApp.

https://library.netapp.com/ecm/ecm_download_file/ECMLP3351268

https://library.netapp.com/ecm/ecm_download_file/ECMLP3373066

Informazioni sul copyright

Copyright © 2026 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.