Amministrare StorageGRID

StorageGRID

NetApp
November 04, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-118/admin/index.html on November 04, 2025. Always check docs.netapp.com for the latest.

Sommario

Amministrare StorageGRID . . . 1
Administer StorageGRID: Panoramica . . . 1
A proposito di queste istruzioni . . . 1
Prima di iniziare . . . 1
Inizia subito con Grid Manager . . . 1
Requisiti del browser Web . . . 1
Accedi a Grid Manager . . . 2
Disconnettersi da Grid Manager . . . 8
Modificare la password . . . 8
Visualizzare le informazioni sulla licenza StorageGRID . . . 9
Aggiornare le informazioni sulla licenza StorageGRID . . . 10
Utilizzare l'API . . . 10
Controllo dell'accesso a StorageGRID . . . 32
Control StorageGRID access: Panoramica . . . 32
Modificare la passphrase di provisioning . . . 33
Modificare le password della console dei nodi . . . 34
USA la federazione delle identità . . . 36
Gestire i gruppi di amministratori . . . 41
Autorizzazioni del gruppo di amministrazione . . . 44
Gestire gli utenti . . . 48
Utilizzo di SSO (Single Sign-on) . . . 51
USA la federazione di grid . . . 79
Che cos'è la federazione di griglie? . . . 79
Che cos'è il clone dell'account? . . . 82
Che cos'è la replica cross-grid? . . . 85
Confronta la replica cross-grid e la replica CloudMirror . . . 91
Creare connessioni di federazione di griglie . . . 93
Gestire le connessioni a federazione di griglie . . . 96
Gestire i tenant consentiti per la federazione di grid . . . 101
Risolvere i problemi relativi agli errori di federazione della griglia . . . 107
Identificare e riprovare le operazioni di replica non riuscite . . . 112
Gestire la sicurezza . . . 116
Gestione della sicurezza: Panoramica . . . 116
Esaminare i metodi di crittografia StorageGRID . . . 117
Gestire i certificati . . . 120
Configurare le impostazioni di sicurezza . . . 153
Configurare i server di gestione delle chiavi . . . 158
Gestire le impostazioni del proxy . . . 176
Firewall di controllo . . . 178
Gestire i tenant . . . 186
Gestire i tenant: Panoramica . . . 186
Creare un account tenant . . . 187
Modificare l'account tenant . . . 192

Modificare la password per l'utente root locale del tenant . . . 194
Elimina account tenant . . . 195
Gestire i servizi della piattaforma . . . 195
Manage S3 (Gestisci S3): Selezionare per gli account tenant . . . 204
Configurare le connessioni client . . . 205
Configurazione delle connessioni client S3 e Swift: Panoramica . . . 205
Sicurezza per client S3 o Swift . . . 208
Utilizzare l'installazione guidata S3 . . . 210
Gestire i gruppi ha . . . 220
Gestire il bilanciamento del carico . . . 231
Configurare i nomi di dominio degli endpoint S3 . . . 245
Riepilogo: Indirizzi IP e porte per le connessioni client . . . 247
Gestire reti e connessioni . . . 249
Configurazione delle impostazioni di rete: Panoramica . . . 249
Linee guida per le reti StorageGRID . . . 250
Visualizzare gli indirizzi IP . . . 251
Configurare le interfacce VLAN . . . 252
Gestire le policy di classificazione del traffico . . . 256
Crittografia supportata per le connessioni TLS in uscita . . . 263
Vantaggi delle connessioni HTTP attive, inattive e simultanee . . . 264
Gestire i costi di collegamento . . . 266
USA AutoSupport . . . 268
Use AutoSupport: Panoramica . . . 268
Configurare AutoSupport . . . 274
Attivare manualmente un pacchetto AutoSupport . . . 279
Risolvere i problemi relativi ai pacchetti AutoSupport . . . 279
Invio dei pacchetti e-Series AutoSupport tramite StorageGRID . . . 280
Gestire i nodi di storage . . . 284
Gestione dei nodi di storage: Panoramica . . . 284
Utilizzare le opzioni di storage . . . 284
Gestire lo storage dei metadati degli oggetti . . . 288
Aumentare l'impostazione spazio riservato metadati . . . 295
Compressione degli oggetti memorizzati . . . 297
Impostazioni di configurazione del nodo di storage . . . 298
Gestire nodi storage completi . . . 303
Gestire i nodi di amministrazione . . . 303
Utilizzare più nodi di amministrazione . . . 303
Identificare il nodo di amministrazione principale . . . 305
Visualizzare lo stato delle notifiche e le code . . . 305
Modalità di visualizzazione degli allarmi riconosciuti da Admin Node (sistema legacy) . . . 306
Configurare l'accesso al client di audit . . . 306
Gestire i nodi di archiviazione . . . 312
Archiviazione nel cloud tramite l'API S3 . . . 312
Archiviazione su nastro tramite middleware TSM . . . 319
Configurare le impostazioni di recupero del nodo di archiviazione . . . 325

Configurare la replica del nodo di archiviazione . . . 326
Impostare gli allarmi personalizzati per il nodo di archiviazione . . . 327
Integrare Tivoli Storage Manager . . . 327
Migrare i dati in StorageGRID . . . 334
Confermare la capacità del sistema StorageGRID . . . 334
Determinare il criterio ILM per i dati migrati . . . 334
Valutare l'impatto della migrazione sulle operazioni . . . 335
Pianificare e monitorare la migrazione dei dati . . . 335

Amministrare StorageGRID

Administer StorageGRID: Panoramica

Seguire queste istruzioni per configurare e amministrare un sistema StorageGRID.

A proposito di queste istruzioni

Le attività principali per la configurazione e l'amministrazione di StorageGRID consentono di:

- Utilizzare il Grid Manager per impostare gruppi e utenti
- Creare account tenant per consentire alle applicazioni client S3 e Swift di memorizzare e recuperare oggetti
- Configurare e gestire le reti StorageGRID
- Configurare AutoSupport
- Gestire le impostazioni dei nodi

Prima di iniziare

- Hai una conoscenza generale del sistema StorageGRID.
- Hai una conoscenza abbastanza dettagliata delle shell dei comandi Linux, delle reti e della configurazione e configurazione dell'hardware del server.

Inizia subito con Grid Manager

Requisiti del browser Web

È necessario utilizzare un browser Web supportato.

Browser Web	Versione minima supportata
Google Chrome	119
Microsoft Edge	119
Mozilla Firefox	119

Impostare la larghezza consigliata per la finestra del browser.

Larghezza del browser	Pixel
Minimo	1024
Ottimale	1280

Accedi a Grid Manager

Per accedere alla pagina di accesso di Grid Manager, immettere il nome di dominio completo (FQDN) o l'indirizzo IP di un nodo amministratore nella barra degli indirizzi di un browser Web supportato.

Panoramica

Ogni sistema StorageGRID include un nodo di amministrazione primario e un numero qualsiasi di nodi di amministrazione non primari. Per gestire il sistema StorageGRID, è possibile accedere a Grid Manager da qualsiasi nodo amministrativo. Tuttavia, i nodi Admin non sono esattamente gli stessi:

- Le conferme di allarme (sistema legacy) eseguite su un nodo di amministrazione non vengono copiate in altri nodi di amministrazione. Per questo motivo, le informazioni visualizzate per gli allarmi potrebbero non apparire identiche su ciascun nodo di amministrazione.
- Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

Connettersi al gruppo ha

Se i nodi di amministrazione sono inclusi in un gruppo ad alta disponibilità (ha), la connessione viene eseguita utilizzando l'indirizzo IP virtuale del gruppo ha o un nome di dominio completo che viene mappato all'indirizzo IP virtuale. Il nodo di amministrazione primario deve essere selezionato come interfaccia principale del gruppo, in modo che quando si accede a Grid Manager, si accede al nodo di amministrazione primario, a meno che il nodo di amministrazione primario non sia disponibile. Vedere "Gestire i gruppi ad alta disponibilità".

Utilizzare SSO

Le fasi di accesso sono leggermente diverse se "È stato configurato Single Sign-on (SSO)".

Accedi a Grid Manager sul primo nodo di amministrazione

Prima di iniziare

- Si dispone delle credenziali di accesso.
- Si sta utilizzando un "browser web supportato".
- I cookie sono attivati nel browser Web.
- L'utente appartiene a un gruppo di utenti che dispone di almeno un'autorizzazione.
- Hai l'URL per Grid Manager:

  `https://FQDN_or_Admin_Node_IP/`

  È possibile utilizzare il nome di dominio completo, l'indirizzo IP di un nodo amministrativo o l'indirizzo IP virtuale di un gruppo ha di nodi amministrativi.

  Per accedere a Grid Manager su una porta diversa da quella predefinita per HTTPS (443), includere il numero di porta nell'URL:

  `https://FQDN_or_Admin_Node_IP:port/`

  > SSO non è disponibile sulla porta di Restricted Grid Manager. È necessario utilizzare la porta 443.

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per Grid Manager.
3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser. Vedere "Gestire i certificati di sicurezza".
4. Accedi a Grid Manager.

   La schermata di accesso visualizzata dipende dalla configurazione di SSO (Single Sign-on) per StorageGRID.

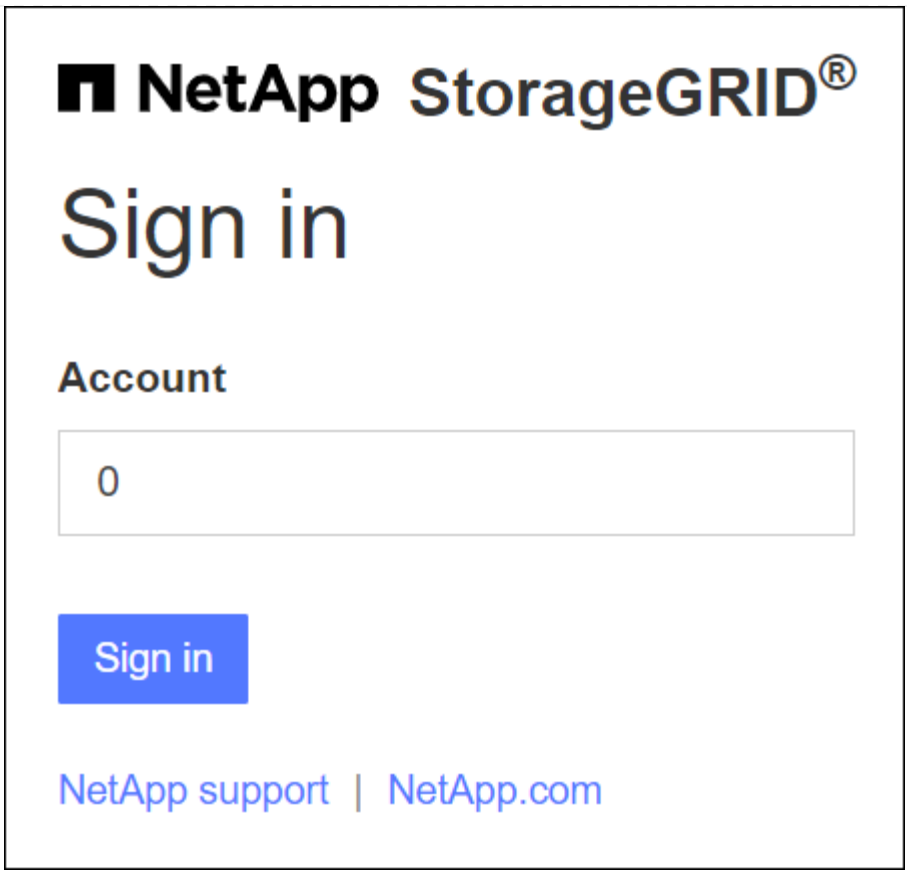
Non si utilizza SSO

a. Immettere il nome utente e la password per Grid Manager.

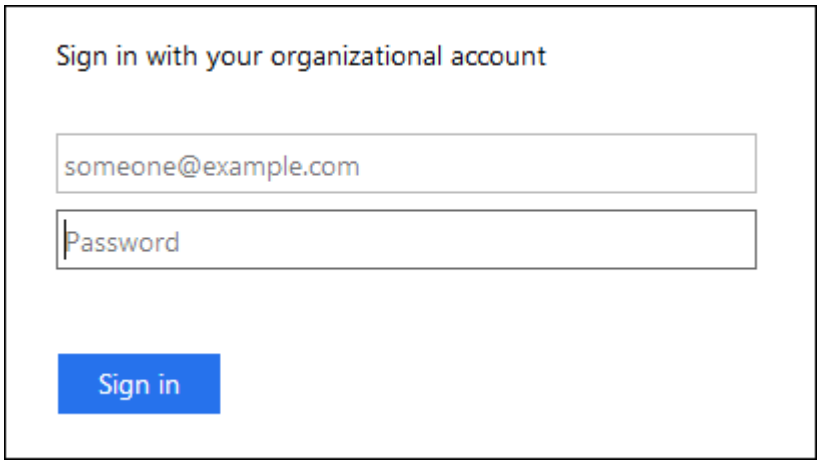
b. Selezionare **Accedi**.

Utilizzo di SSO

- Se StorageGRID utilizza SSO ed è la prima volta che si accede all'URL dal browser:
  i. Selezionare **Accedi**. È possibile lasciare lo 0 nel campo account.



ii. Immettere le credenziali SSO standard nella pagina di accesso SSO dell'organizzazione. Ad esempio:



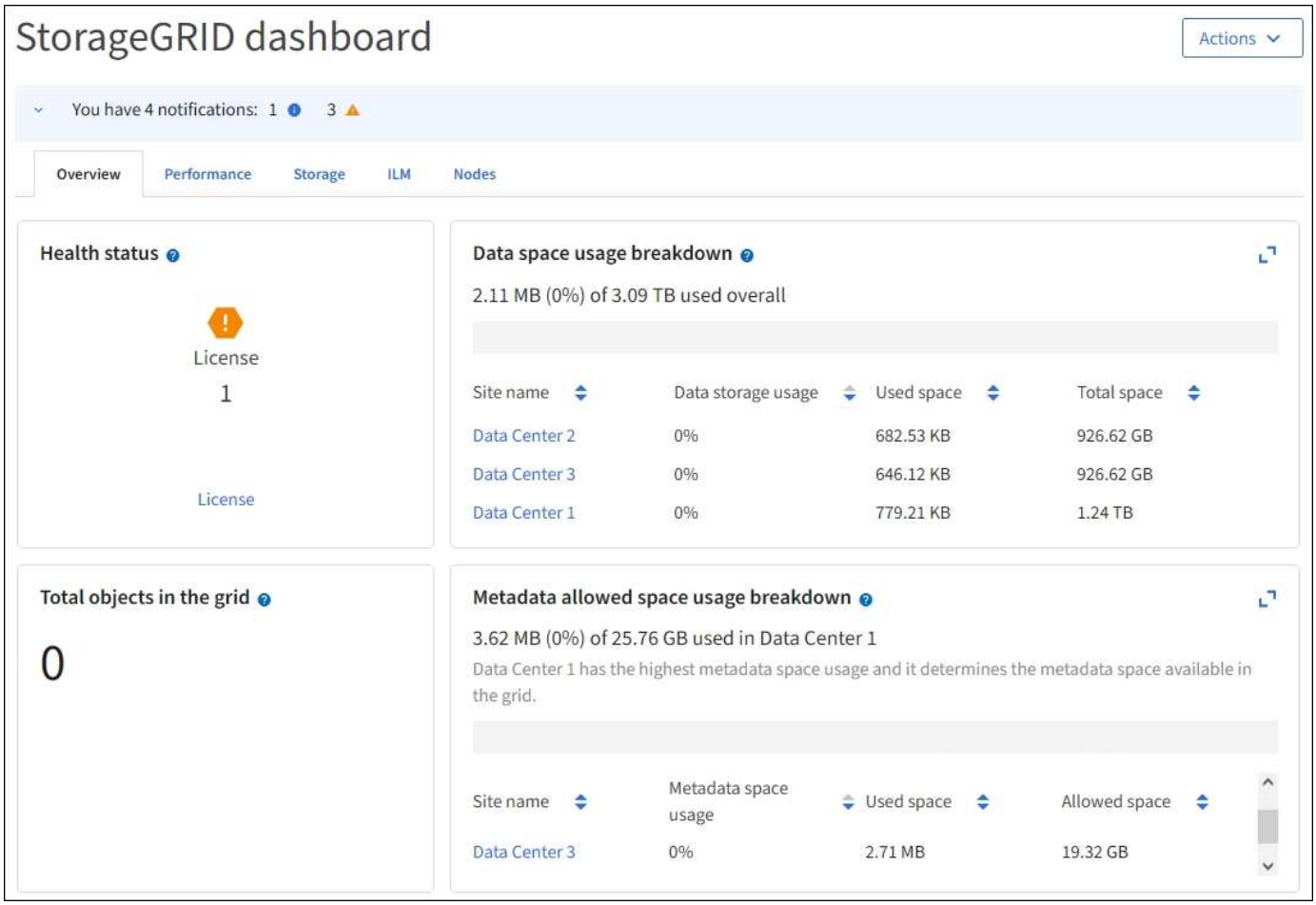
- Se StorageGRID utilizza SSO e si è precedentemente effettuato l'accesso a Grid Manager o a un account tenant:

  i. Inserire **0** (l'ID account per Grid Manager) o selezionare **Grid Manager** se compare nell'elenco degli account recenti.

ii. Selezionare **Accedi**.

iii. Accedi con le tue credenziali SSO standard nella pagina di accesso SSO della tua organizzazione.

Una volta effettuato l'accesso, viene visualizzata la home page di Grid Manager, che include la dashboard. Per informazioni sulle informazioni fornite, vedere "Visualizzare e gestire la dashboard".



Accedere a un altro nodo amministratore

Per accedere a un altro nodo amministratore, procedere come segue.

Non si utilizza SSO

Fasi

1. Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Includere il numero di porta come richiesto.
2. Immettere il nome utente e la password per Grid Manager.
3. Selezionare **Accedi**.

Utilizzo di SSO

Se StorageGRID utilizza SSO ed è stato effettuato l'accesso a un nodo amministratore, è possibile accedere ad altri nodi amministrativi senza dover effettuare nuovamente l'accesso.

Fasi

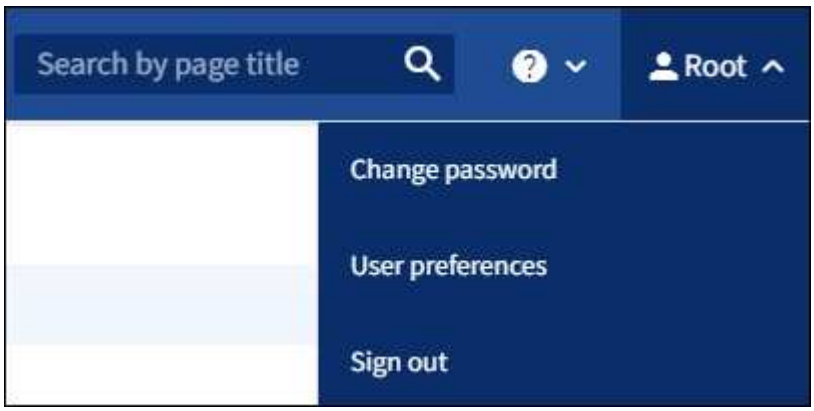
1. Inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione nella barra degli indirizzi del browser.
2. Se la sessione SSO è scaduta, immettere nuovamente le credenziali.

Disconnettersi da Grid Manager

Una volta terminato l'utilizzo di Grid Manager, è necessario disconnettersi per garantire che gli utenti non autorizzati non possano accedere al sistema StorageGRID. La chiusura del browser potrebbe non disconnettersi dal sistema, in base alle impostazioni dei cookie del browser.

Fasi

1. Selezionare il nome utente nell'angolo in alto a destra.



2. Selezionare **Disconnetti**.

Opzione	Descrizione
SSO non in uso	Si è disconnessi dal nodo di amministrazione. Viene visualizzata la pagina di accesso di Grid Manager. **Nota:** se si è effettuato l'accesso a più di un nodo Admin, è necessario disconnettersi da ciascun nodo.
SSO attivato	Si è disconnessi da tutti i nodi di amministrazione ai quali si stava accedendo. Viene visualizzata la pagina di accesso a StorageGRID. **Grid Manager** è elencato come predefinito nell'elenco a discesa **Recent Accounts** (account recenti) e il campo **account ID** (ID account) mostra 0. **Nota:** se SSO è attivato e si è anche connessi al tenant manager, è necessario "disconnettersi dall'account tenant" a. "Disconnettersi da SSO".

Modificare la password

Gli utenti locali di Grid Manager possono modificare la propria password.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

Se si accede a StorageGRID come utente federato o se è attivato il Single Sign-on (SSO), non è possibile modificare la password in Grid Manager. È invece necessario modificare la password nell'origine dell'identità esterna, ad esempio Active Directory o OpenLDAP.

Fasi

1. Dall'intestazione Grid Manager, selezionare ***Nome*** > **Modifica password**.
2. Inserire la password corrente.
3. Digitare una nuova password.

   La password deve contenere almeno 8 e non più di 32 caratteri. Le password distinguono tra maiuscole e minuscole.

4. Immettere nuovamente la nuova password.
5. Selezionare **Salva**.

Visualizzare le informazioni sulla licenza StorageGRID

Se necessario, è possibile visualizzare le informazioni sulla licenza del sistema StorageGRID, ad esempio la capacità di storage massima del grid.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

In caso di problemi con la licenza software per questo sistema StorageGRID, la scheda di stato dello stato di salute sul dashboard include un'icona di stato della licenza e un collegamento **licenza**. Il numero indica il numero di problemi relativi alla licenza.

Fasi

1. Accedere alla pagina License (licenza) effettuando una delle seguenti operazioni:
   - Selezionare **MANUTENZIONE** > **sistema** > **licenza**.
   - Dalla scheda Health status (Stato) sul dashboard, selezionare l'icona License status (Stato licenza) o il collegamento **License** (licenza).

     Questo collegamento viene visualizzato solo in caso di problemi con la licenza.

2. Visualizzare i dettagli di sola lettura per la licenza corrente:
   - ID sistema StorageGRID, che è il numero di identificazione univoco per l'installazione di StorageGRID
   - Numero di serie della licenza
   - Tipo di licenza, **Perpetual** o **Subscription**
   - Capacità di storage concessa in licenza del grid
   - Capacità di storage supportata
   - Data di fine della licenza. **N/A** appare per una licenza perpetua.
   - Data di fine supporto

     Questa data viene letta dal file di licenza corrente e potrebbe non essere aggiornata se si estende o si rinnova il contratto del servizio di supporto dopo aver ottenuto il file di licenza. Per aggiornare questo valore, vedere "Aggiornare le informazioni sulla licenza StorageGRID". È inoltre possibile visualizzare la data di fine effettiva del contratto utilizzando Active IQ.

   - Contenuto del file di testo della licenza

Aggiornare le informazioni sulla licenza StorageGRID

È necessario aggiornare le informazioni di licenza per il sistema StorageGRID in qualsiasi momento in cui i termini della licenza cambiano. Ad esempio, è necessario aggiornare le informazioni sulla licenza se si acquista ulteriore capacità di storage per il grid.

Prima di iniziare

- Si dispone di un nuovo file di licenza da applicare al sistema StorageGRID.
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Si dispone della passphrase di provisioning.

Fasi

1. Selezionare **MANUTENZIONE** > **sistema** > **licenza**.
2. Nella sezione Aggiorna licenza, selezionare **Sfoglia**.
3. Individuare e selezionare il nuovo file di licenza (`.txt`).

   Il nuovo file di licenza viene validato e visualizzato.

4. Inserire la passphrase di provisioning.
5. Selezionare **Salva**.

Utilizzare l'API

Utilizzare l'API Grid Management

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management invece dell'interfaccia utente di Grid Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

Risorse di alto livello

L'API Grid Management fornisce le seguenti risorse di primo livello:

- `/grid`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate.
- `/org`: L'accesso è limitato agli utenti che appartengono a un gruppo LDAP locale o federato per un account tenant. Per ulteriori informazioni, vedere "Utilizzare un account tenant".
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

Emettere richieste API

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di eseguire operazioni in tempo reale in StorageGRID con l'API.

L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.

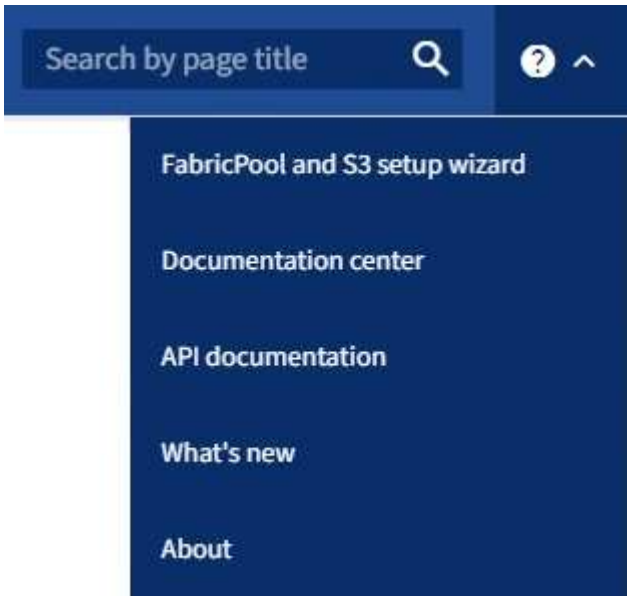
Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

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

Fasi

1. Dall'intestazione Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.



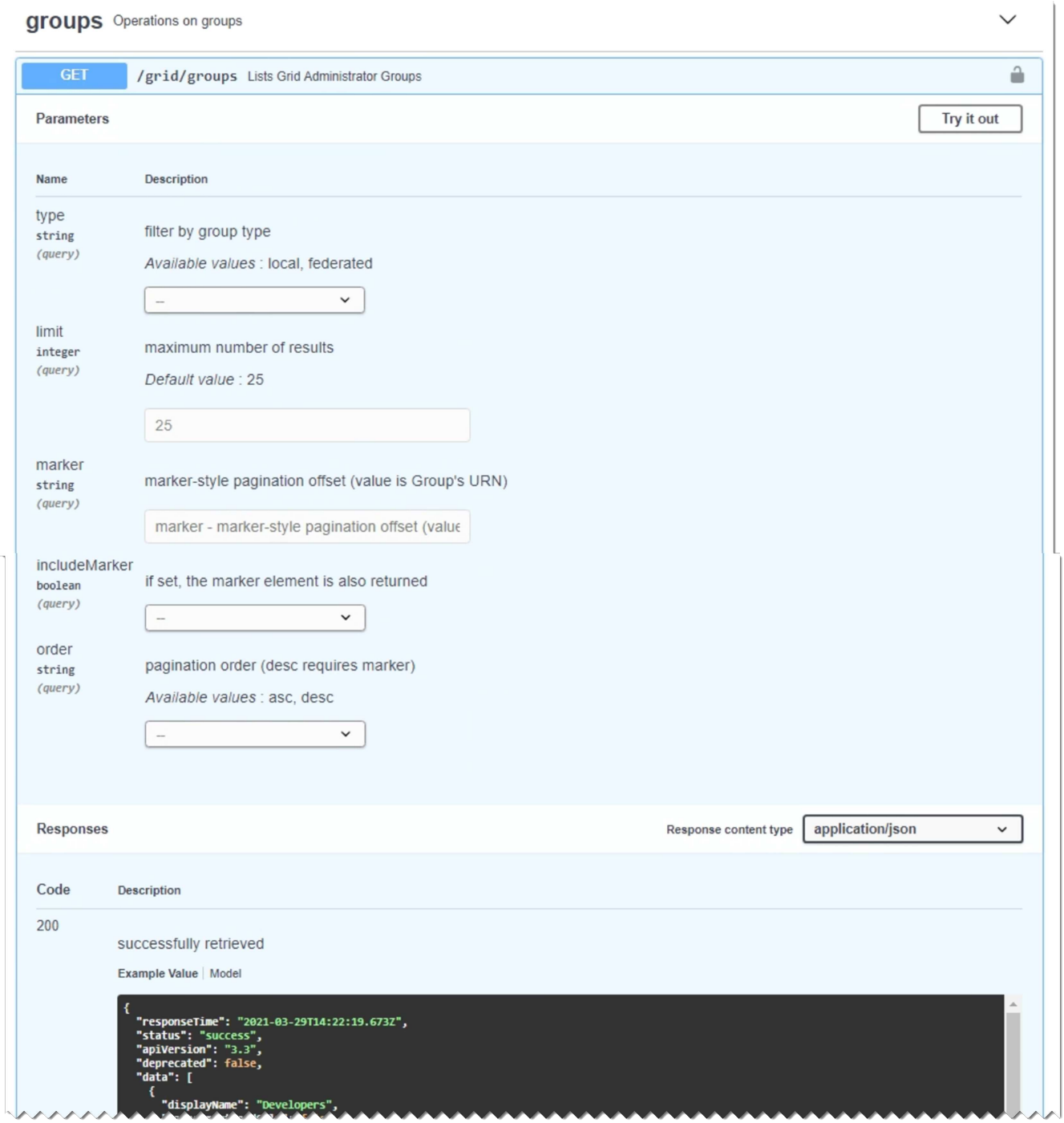
2. Per eseguire un'operazione con l'API privata, selezionare **Vai alla documentazione API privata** nella pagina API di gestione StorageGRID.

   Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Selezionare l'operazione desiderata.

   Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, ad esempio GET, PUT, UPDATE ed DELETE.

4. Selezionare un'azione HTTP per visualizzare i dettagli della richiesta, tra cui l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.



5. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.

6. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.
7. Selezionare **Provalo**.
8. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
9. Selezionare **Esegui**.
10. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Operazioni API di Grid Management

L'API Grid Management organizza le operazioni disponibili nelle seguenti sezioni.

> Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **Account**: Operazioni per la gestione degli account del tenant di storage, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.
- **Alarms**: Operazioni per elencare gli allarmi correnti (sistema legacy) e restituire informazioni sullo stato della griglia, inclusi gli avvisi correnti e un riepilogo degli stati di connessione del nodo.
- **Alert-history**: Operazioni su avvisi risolti.
- **Ricevitori di avvisi**: Operazioni sui destinatari di notifiche di avvisi (e-mail).
- **Alert-rules**: Operazioni sulle regole di allerta.
- **Silenzi di allerta**: Operazioni di silenzi di allerta.
- **Alerts**: Operazioni sugli avvisi.
- **Audit**: Operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth**: Operazioni per l'autenticazione della sessione utente.

  L'API Grid Management supporta lo schema di autenticazione del token del bearer. Per effettuare l'accesso, inserisci un nome utente e una password nel corpo JSON della richiesta di autenticazione (ovvero `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("Authorization: Bearer *token*"). Il token scade dopo 16 ore.

  > Se per il sistema StorageGRID è attivato il single sign-on, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "autenticazione nell'API se è attivato il single sign-on".

  Per informazioni sul miglioramento della protezione dell'autenticazione, vedere "protezione contro la contraffazione delle richieste tra siti".

- **Certificati-client**: Operazioni per configurare i certificati client in modo che sia possibile accedere in modo sicuro a StorageGRID utilizzando strumenti di monitoraggio esterni.
- **Config**: Operazioni relative alla release del prodotto e alle versioni dell'API Grid Management. È possibile elencare la versione del prodotto e le principali versioni dell'API Grid Management supportate da tale release ed è possibile disattivare le versioni obsolete dell'API.
- **Disattivato-funzioni**: Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **dns-servers**: Operazioni per elencare e modificare i server DNS esterni configurati.
- **Dettagli unità**: Operazioni su unità per modelli di appliance di archiviazione specifici.

- **Nomi-dominio-endpoint**: Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **Erasure coding**: Operazioni sui profili di erasure coding.
- **Espansione**: Operazioni di espansione (a livello di procedura).
- **Expansion-node**: Operazioni di espansione (a livello di nodo).
- **Expansion-sites**: Operazioni di espansione (a livello di sito).
- **Grid-networks**: Operazioni per elencare e modificare l'elenco Grid Network.
- **Grid-password**: Operazioni per la gestione delle password grid.
- **Gruppi**: Operazioni per gestire i gruppi di amministratori di griglia locali e recuperare i gruppi di amministratori di griglia federati da un server LDAP esterno.
- **Identity-source**: Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm**: Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **Procedure in corso**: Recupera le procedure di manutenzione attualmente in corso.
- **Licenza**: Operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs**: Operazioni per la raccolta e il download dei file di log.v
- **Metriche**: Operazioni su metriche StorageGRID, incluse query metriche istantanee in un singolo punto nel tempo e query metriche di intervallo in un intervallo di tempo. L'API Grid Management utilizza lo strumento di monitoraggio dei sistemi Prometheus come origine dei dati back-end. Per informazioni sulla creazione di query Prometheus, visitare il sito Web Prometheus.

> Metriche che includono `private` i loro nomi sono destinati esclusivamente all'uso interno. Queste metriche sono soggette a modifiche senza preavviso tra le versioni di StorageGRID.

- **Node-details**: Operazioni sui dettagli del nodo.
- **Node-Health**: Operazioni sullo stato di salute del nodo.
- **Node-storage-state**: Operazioni sullo stato dello storage del nodo.
- **ntp-servers**: Operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects**: Operazioni su oggetti e metadati di oggetti.
- **Recovery**: Operazioni per la procedura di recovery.
- **Recovery-package**: Operazioni per il download del Recovery Package.
- **Regioni**: Operazioni per visualizzare e creare regioni.
- **s3-Object-lock**: Operazioni sulle impostazioni generali di blocco oggetti S3.
- **Server-certificate**: Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp**: Operazioni sulla configurazione SNMP corrente.
- **Filigrane-archiviazione**: Filigrane del nodo di archiviazione.
- **Classi di traffico**: Operazioni per le policy di classificazione del traffico.
- **Untrusted-client-network**: Operazioni sulla configurazione Untrusted Client Network.
- **Utenti**: Operazioni per visualizzare e gestire gli utenti di Grid Manager.

Versione dell'API Grid Management

L'API Grid Management utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

`https://hostname_or_ip_address/api/v4/authorize`

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.

> È possibile configurare le versioni supportate. Vedere la sezione **config** della documentazione Swagger API per "API di Grid Management" per ulteriori informazioni. È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare `GET /versions` Richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione dell'API utilizzando un parametro path (`/api/v4`) o un'intestazione (`Api-Version: 4`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare `csrfToken` parametro a. `true` durante l'autenticazione. L'impostazione predefinita è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept:
application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando è vero, un `GridCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Grid Manager e a. `AccountCsrfToken` Il cookie viene impostato con un valore casuale per l'accesso a Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- Il `X-Csrf-Token` Header, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo con codifica a modulo: A. `csrfToken` parametro del corpo della richiesta codificato dal modulo.

Per ulteriori esempi e dettagli, consultare la documentazione API online.

> Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione "Content-Type: Application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare l'API se è attivato il Single Sign-on

Utilizzare l'API se è attivato il single sign-on (Active Directory)

Se lo hai fatto "SSO (Single Sign-on) configurato e abilitato" Se si utilizza Active Directory come provider SSO, è necessario emettere una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Il `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per VMware).

- Un esempio di workflow di richieste di curl.

  Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: `A valid SubjectConfirmation was not found on this Response`.

  > L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare `storagegrid-ssoauth.py` Script Python. Andare alla fase 2.
   - USA richieste di curl. Passare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` Passare lo script all'interprete Python ed eseguirlo.

   Quando richiesto, inserire i valori per i seguenti argomenti:

   - Il metodo SSO. Immettere ADFS o adfs.
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se si desidera accedere all'API di gestione tenant.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: adfs
   saml_user: my-sso-username
   saml_domain: my-domain
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.

   a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export SAMLDOMAIN='my-domain'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
export AD_FS_ADDRESS='adfs.example.com'
```

Per accedere all'API Grid Management, utilizzare 0 AS `TENANTACCOUNTID`.

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta DI POST a. `/api/v3/authorize-saml`E rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per `TENANTACCOUNTID`. I risultati verranno passati a. `python -m json.tool` Per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...
sSl%2BfQ33cvfwA%3D&RelayState=12345",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sSl%2BfQ33cvfwA%3D'
```

d. Ottenere un URL completo che includa l'ID della richiesta del client da ad FS.

Un'opzione consiste nel richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post"
id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off"
novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13)
Login.submitLoginRequest();" action="/adfs/ls/?
SAMLRequest=fZHRToMwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&clie
nt-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salvare l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Inviare le credenziali all'azione del modulo della risposta precedente.

```
curl -X POST "https://$AD_FS_ADDRESS
/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client
-request-id=$SAMLREQUESTID" \
--data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=
$SAMLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.

> Se l'autenticazione a più fattori (MFA) è attivata per il sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRToMwFIZfhb...UJikvo
77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-
ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs;
HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salvare `MSISAuth` cookie dalla risposta.

```
export MSISAuth='AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY='
```

h. Inviare una richiesta GET alla posizione specificata con i cookie del POST di autenticazione.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=
$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-
id=$SAMLREQUESTID" \
--cookie "MSISAuth=$MSISAuth" --include
```

Le intestazioni delle risposte conterranno le informazioni della sessione di ad FS per un utilizzo successivo della disconnessione e il corpo della risposta conterrà la risposta SAMLin un campo di forma nascosto.

```
HTTP/1.1 200 OK
Cache-Control: no-cache,no-store
Pragma: no-cache
Content-Length: 5665
Content-Type: text/html; charset=utf-8
Expires: -1
Server: Microsoft-HTTPAPI/2.0
P3P: ADFS doesn't have P3P policy, please contact your site's admin
for more details
Set-Cookie:
SamlSession=a3dpbnRlcnMtUHJpbWFyeS1BZG1pbi0xNzgmRmFsc2Umcng4NnJDZmFKV
XFxVWx3bkl1MnFuUSUzZCUzZCYmJiYmXzE3MjAyZTA5LThmMDgtNDRkZC04Yzg5LTQ3ND
UxYzA3ZjkzYw==; path=/adfs; HttpOnly; Secure
Set-Cookie: MSISAuthenticated=MTEvNy8yMDE4IDQ6MzI6NTkgUE0=;
path=/adfs; HttpOnly; Secure
Set-Cookie: MSISLoopDetectionCookie=MjAxOC0xMS0wNzoxNjozMjo1OVpcMQ==;
path=/adfs; HttpOnly; Secure
Date: Wed, 07 Nov 2018 16:32:59 GMT

<form method="POST" name="hiddenform"
action="https://storagegrid.example.com:443/api/saml-response">
  <input type="hidden" name="SAMLResponse"
value="PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4=" /><input
type="hidden" name="RelayState" value="12345" />
```

i. Salvare `SAMLResponse` dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato `SAMLResponse`, Creare un StorageGRID`/api/saml-response` Richiesta di generazione di un token di autenticazione StorageGRID.

Per `RelayState`, Utilizzare l'ID account tenant o utilizzare 0 se si desidera accedere all'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La risposta include il token di autenticazione.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salvare il token di autenticazione nella risposta con nome `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi utilizzare `MYTOKEN` Per le altre richieste, in modo simile a come si utilizza l'API se SSO non viene utilizzato.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management. Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API StorageGRID disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
    "apiVersion": "3.0",
    "data":
"https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3
D",
    "responseTime": "2018-11-20T22:20:30.839Z",
    "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%
3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: MSISSignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018
22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

R `204 No Content` la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzare l'API se è attivato il single sign-on (Azure)

Se lo hai fatto "SSO (Single Sign-on) configurato e abilitato" Inoltre, come provider SSO, Azure consente di utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Accedere all'API se Azure Single Sign-on è attivato

Queste istruzioni sono valide se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Si conoscono l'indirizzo e-mail SSO e la password di un utente federato che appartiene a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- Il `storagegrid-ssoauth-azure.py` Script Python
- Il `storagegrid-ssoauth-azure.js` Script node.js

Entrambi gli script si trovano nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per VMware).

Per scrivere la propria integrazione API con Azure, vedere `storagegrid-ssoauth-azure.py` script. Lo script Python effettua due richieste direttamente a StorageGRID (prima per ottenere la SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure per eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è semplice. Il modulo Puppeteer Node.js viene utilizzato per scrapare l'interfaccia SSO di Azure.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Installare le dipendenze richieste, come indicato di seguito:

a. Installare Node.js (vedere "https://nodejs.org/en/download/").

b. Installare i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

   Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO di Azure.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):
   - Indirizzo e-mail SSO utilizzato per accedere ad Azure
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se si desidera accedere all'API di gestione tenant
4. Quando richiesto, inserire la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.

```
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 se è attivato il Single Sign-on (PingFederate)

Se lo hai fatto "SSO (Single Sign-on) configurato e abilitato" E si utilizza PingFederate come provider SSO, è necessario emettere una serie di richieste API per ottenere un token di autenticazione valido per l'API Grid Management o l'API Tenant Management.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Il `storagegrid-ssoauth.py` Script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` Per Red Hat Enterprise Linux, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per

VMware).

- Un esempio di workflow di richieste di curl.

  Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: `A valid SubjectConfirmation was not found on this Response`.

  L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

  Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
   - Utilizzare `storagegrid-ssoauth.py` Script Python. Andare alla fase 2.
   - USA richieste di curl. Passare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` Passare lo script all'interprete Python ed eseguirlo.

   Quando richiesto, inserire i valori per i seguenti argomenti:

   - Il metodo SSO. È possibile inserire qualsiasi variazione di "pingfederate" (PINGFEDERATE, pingfederate e così via).
   - Il nome utente SSO
   - Il dominio in cui è installato StorageGRID. Questo campo non viene utilizzato per PingFederate. È possibile lasciare vuoto il campo o inserire un valore qualsiasi.
   - L'indirizzo per StorageGRID
   - L'ID account tenant, se si desidera accedere all'API di gestione tenant.

   ```
   python3 storagegrid-ssoauth.py
   sso_method: pingfederate
   saml_user: my-sso-username
   saml_domain:
   sg_address: storagegrid.example.com
   tenant_account_id: 12345
   Enter the user's SAML password:
   ********************************************************************************

   ********************************************************************************
   StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
   ```

   Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.

   a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'
export SAMLPASSWORD='my-password'
export TENANTACCOUNTID='12345'
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```

Per accedere all'API Grid Management, utilizzare 0 AS `TENANTACCOUNTID`.

b. Per ricevere un URL di autenticazione firmato, inviare una richiesta DI POST a. `/api/v3/authorize-saml`E rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati verranno passati a python -m json.tool per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \
  -H "accept: application/json" -H  "Content-Type: application/json"
\
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m
json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{
    "apiVersion": "3.0",
    "data": "https://my-pf-baseurl/idp/SSO.saml2?...",
    "responseTime": "2018-11-06T16:30:23.355Z",
    "status": "success"
}
```

c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

d. Esportare la risposta e il cookie e visualizzare la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"
id="pf.adapterId"'
```

e. Esportare il valore 'pf.adapterId' e visualizzare la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esportare il valore 'href' (rimuovere la barra finale /) e visualizzare la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esportare il valore "azione":

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia cookie con credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \
--data "pf.username=$SAMLUSER&pf.pass=
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER"
--include
```

i. Salvare `SAMLResponse` dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato `SAMLResponse`, Creare un StorageGRID `/api/saml-response` Richiesta di generazione di un token di autenticazione StorageGRID.

Per `RelayState`, Utilizzare l'ID account tenant o utilizzare 0 se si desidera accedere all'API Grid Management.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \
  -H "accept: application/json" \
  --data-urlencode "SAMLResponse=$SAMLResponse" \
  --data-urlencode "RelayState=$TENANTACCOUNTID" \
  | python -m json.tool
```

La risposta include il token di autenticazione.

```
{
    "apiVersion": "3.0",
    "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
    "responseTime": "2018-11-07T21:32:53.486Z",
    "status": "success"
}
```

a. Salvare il token di autenticazione nella risposta con nome `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

Ora puoi utilizzare `MYTOKEN` Per le altre richieste, in modo simile a come si utilizza l'API se SSO non viene utilizzato.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management. Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API StorageGRID disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
    "apiVersion": "3.0",
    "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
    "responseTime": "2021-10-12T22:20:30.839Z",
    "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--include
```

R `204 No Content` la risposta indica che l'utente è ora disconnesso.

```
HTTP/1.1 204 No Content
```

Disattivare le funzioni con l'API

È possibile utilizzare l'API di gestione griglia per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzione viene disattivata, non è possibile assegnare a nessuno le autorizzazioni per eseguire le attività correlate a tale funzione.

A proposito di questa attività

Il sistema Disattivato consente di impedire l'accesso a determinate funzioni del sistema StorageGRID. La disattivazione di una funzione è l'unico modo per impedire all'utente root o agli utenti appartenenti a gruppi di amministratori con autorizzazione **Root Access** di utilizzare tale funzione.

Per comprendere come questa funzionalità potrebbe essere utile, considerare il seguente scenario:

L'azienda A è un provider di servizi che affitta la capacità di storage del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei titolari di leasing, la Società A desidera garantire che i propri dipendenti non possano mai accedere a alcun account tenant dopo l'implementazione dell'account.

*L'azienda A è in grado di raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API Grid Management. Disattivando completamente la funzione **Cambia password root tenant** in Grid Manager (sia l'interfaccia utente che l'API), la società A può garantire che nessun utente Admin, incluso l'utente root e gli utenti appartenenti a gruppi con l'autorizzazione **Root access**, possa modificare la password per qualsiasi utente root dell'account tenant.*

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia. Vedere "Utilizzare l'API Grid Management".
2. Individuare l'endpoint Deactivate Features.
3. Per disattivare una funzione, ad esempio Modifica password root tenant, inviare un corpo all'API come segue:

   ```
   { "grid": {"changeTenantRootPassword": true} }
   ```

   Al termine della richiesta, la funzione Modifica password root tenant viene disattivata. L'autorizzazione di gestione **Modifica password principale tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password principale per un tenant non riesce con "403 Proibito".

Riattivare le funzioni disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzione disattivata. Tuttavia, se si desidera evitare che le funzioni disattivate vengano riattivate, è possibile disattivare la funzione **ActivateFeatures**.

> Impossibile riattivare la funzione **ActivateCaratures**. Se decidi di disattivare questa funzione, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzione disattivata. È necessario contattare il supporto tecnico per ripristinare eventuali funzionalità perse.

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia.

2. Individuare l'endpoint Deactivate Features.
3. Per riattivare tutte le funzioni, inviare un corpo all'API come segue:

```
{ "grid": null }
```

Una volta completata la richiesta, tutte le funzioni, inclusa la funzione Change tenant root password, vengono riattivate. L'autorizzazione di gestione **Change tenant root password** viene ora visualizzata nell'interfaccia utente e tutte le richieste API che tentano di modificare la password root per un tenant avranno esito positivo, presupponendo che l'utente disponga dell'autorizzazione di gestione **Root access** o **Change tenant root password**.

> L'esempio precedente causa la riattivazione di *tutte* le funzioni disattivate. Se sono state disattivate altre funzioni che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzione Modifica password root tenant e continuare a disattivare la funzione di riconoscimento allarme, inviare la seguente richiesta PUT:
>
> ```
> { "grid": { "alarmAcknowledgment": true } }
> ```

Controllo dell'accesso a StorageGRID

Control StorageGRID access: Panoramica

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

Controlla l'accesso a Grid Manager

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

Utilizzo di "federazione delle identità" rende la configurazione "gruppi" e. "utenti" Più veloce e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari. È possibile configurare la federazione delle identità se si utilizza Active Directory, OpenLDAP o Oracle Directory Server.

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

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

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

Attiva single sign-on

Il sistema StorageGRID supporta SSO (Single Sign-on) utilizzando lo standard SAML 2.0 (Security Assertion Markup Language 2.0). Dopo di lei "Configurare e abilitare SSO", Tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.

Modificare la passphrase di provisioning

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino StorageGRID. La passphrase è necessaria anche per scaricare i backup delle informazioni sulla topologia della griglia e delle chiavi di crittografia per il sistema StorageGRID. È possibile "modificare la passphrase" secondo necessità.

Modificare le password della console dei nodi

Ciascun nodo della griglia dispone di una password univoca per la console del nodo, che deve essere utilizzata per accedere al nodo come "admin" utilizzando SSH o all'utente root con una connessione VM/console fisica. In base alle esigenze, è possibile "modificare la password della console del nodo" per ogni nodo.

Modificare la passphrase di provisioning

Utilizzare questa procedura per modificare la passphrase di provisioning StorageGRID. La passphrase è necessaria per le procedure di ripristino, espansione e manutenzione. La passphrase è necessaria anche per scaricare i backup del pacchetto di ripristino che includono le informazioni sulla topologia della griglia, le password della console del nodo della griglia e le chiavi di crittografia per il sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone delle autorizzazioni di accesso Maintenance o Root.
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per "Download del pacchetto di ripristino". La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicurarsi di documentare la passphrase di provisioning e conservarla in una posizione sicura.

Fasi

1. Selezionare **CONFIGURATION** > **Access control**> **Grid passwords**.
2. In **Cambia passphrase di provisioning**, selezionare **effettua una modifica**
3. Inserire la passphrase di provisioning corrente.
4. Inserire la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili al maiuscolo/minuscolo.
5. Memorizzare la nuova passphrase di provisioning in una posizione sicura. È necessario per le procedure di installazione, espansione e manutenzione.
6. Immettere nuovamente la nuova passphrase e selezionare **Save** (Salva).

Al termine della modifica della passphrase di provisioning, il sistema visualizza un banner verde di successo.

7. Selezionare **Recovery Package** (pacchetto di ripristino).
8. Inserire la nuova passphrase di provisioning per scaricare il nuovo Recovery Package.

> Dopo aver modificato la passphrase di provisioning, è necessario scaricare immediatamente un nuovo pacchetto di ripristino. Il file Recovery Package consente di ripristinare il sistema in caso di errore.

Modificare le password della console dei nodi

Ogni nodo della griglia dispone di una password univoca per la console del nodo, che è necessario accedere al nodo. Seguire questa procedura per modificare ogni password univoca della console dei nodi per ciascun nodo della griglia.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di manutenzione o di accesso root".
- Si dispone della passphrase di provisioning corrente.

A proposito di questa attività

Utilizzare la password della console del nodo per accedere a un nodo come "admin" utilizzando SSH o all'utente root su una connessione VM/console fisica. Il processo di modifica della password della console dei nodi crea nuove password per ciascun nodo della griglia e le memorizza in un aggiornato `Passwords.txt` nel pacchetto di ripristino. Le password sono elencate nella colonna Password del file Passwords.txt.

> Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questa procedura non modifica le password di accesso SSH.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Grid passwords**.
2. In **Cambia password console nodo**, selezionare **effettua una modifica**.

Inserire la passphrase di provisioning

Fasi

1. Inserire la passphrase di provisioning per la griglia.
2. Selezionare **continua**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le password della console dei nodi, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le password in questo file se il processo di modifica della password non riesce per qualsiasi nodo.

Fasi

1. Selezionare **Download recovery package** (Scarica pacchetto di ripristino).
2. Copiare il file del pacchetto di ripristino (`.zip`) in due posizioni sicure e separate.

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

3. Selezionare **continua**.
4. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Yes** (Sì) se si desidera iniziare a modificare le password della console del nodo.

   Non puoi annullare questo processo dopo l'avvio.

Modificare le password della console dei nodi

All'avvio del processo di password della console dei nodi, viene generato un nuovo pacchetto di ripristino che include le nuove password. Quindi, le password vengono aggiornate su ciascun nodo.

Fasi

1. Attendere che venga generato il nuovo pacchetto di ripristino, che potrebbe richiedere alcuni minuti.
2. Selezionare **Scarica nuovo pacchetto di ripristino**.
3. Al termine del download:

   a. Aprire `.zip` file.

   b. Verificare che sia possibile accedere ai contenuti, incluso il `Passwords.txt` che contiene le nuove password della console dei nodi.

   c. Copiare il nuovo file del pacchetto di ripristino (`.zip`) in due posizioni sicure e separate.

      > Non sovrascrivere il vecchio pacchetto di ripristino.

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

4. Selezionare la casella di controllo per indicare che il nuovo pacchetto di ripristino è stato scaricato e che il contenuto è stato verificato.
5. Selezionare **Change node console passwords** (Modifica password console nodi) e attendere che tutti i nodi vengano aggiornati con le nuove password. L'operazione potrebbe richiedere alcuni minuti.

   Se le password vengono modificate per tutti i nodi, viene visualizzato un banner verde di successo. Passare alla fase successiva.

   Se si verifica un errore durante il processo di aggiornamento, un messaggio di intestazione indica il numero di nodi che non sono riusciti a modificare le password. Il sistema riprova automaticamente il processo su qualsiasi nodo che non ha modificato la password. Se il processo termina con alcuni nodi che non hanno ancora una password modificata, viene visualizzato il pulsante **Riprova**.

   Se l'aggiornamento della password non è riuscito per uno o più nodi:

   a. Esaminare i messaggi di errore elencati nella tabella.

b. Risolvere i problemi.

c. Selezionare **Riprova**.

> Il nuovo tentativo modifica solo le password della console dei nodi sui nodi che non sono riusciti durante i precedenti tentativi di modifica della password.

6. Una volta modificate le password della console del nodo per tutti i nodi, eliminare primo pacchetto di ripristino scaricato.
7. Facoltativamente, utilizzare il collegamento **Recovery package** per scaricare una copia aggiuntiva del nuovo pacchetto di ripristino.

USA la federazione delle identità

L'utilizzo della federazione delle identità rende più rapida la configurazione di gruppi e utenti e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari.

Configurare la federazione delle identità per Grid Manager

È possibile configurare la federazione delle identità in Grid Manager se si desidera che i gruppi amministrativi e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, Azure Active Directory (Azure ad), OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Si utilizza Active Directory, Azure ad, OpenLDAP o Oracle Directory Server come provider di identità.

> Se si desidera utilizzare un servizio LDAP v3 non elencato, contattare il supporto tecnico.

- Se si intende utilizzare OpenLDAP, è necessario configurare il server OpenLDAP. Vedere Linee guida per la configurazione di un server OpenLDAP.
- Se si prevede di attivare il Single Sign-on (SSO), è stata esaminata la "requisiti e considerazioni per il single sign-on".
- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità utilizza TLS 1.2 o 1.3. Vedere "Crittografia supportata per le connessioni TLS in uscita".

A proposito di questa attività

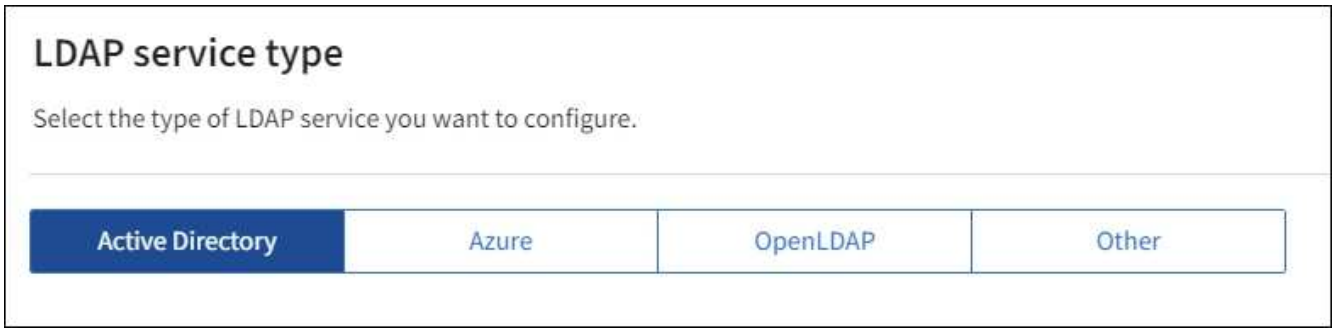
È possibile configurare un'origine identità per Grid Manager se si desidera importare gruppi da un altro sistema, ad esempio Active Directory, Azure ad, OpenLDAP o Oracle Directory Server. È possibile importare i seguenti tipi di gruppi:

- Gruppi di amministratori. Gli utenti dei gruppi di amministrazione possono accedere a Grid Manager ed eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per tenant che non utilizzano la propria origine di identità. Gli utenti dei gruppi di tenant possono accedere al tenant manager ed eseguire le attività in base alle autorizzazioni assegnate al gruppo nel tenant manager. Vedere "Creare un account tenant" e. "Utilizzare un account tenant" per ulteriori informazioni.

Inserire la configurazione

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Identity Federation**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.



   Selezionare **Altro** per configurare i valori per un server LDAP che utilizza Oracle Directory Server.

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP. In caso contrario, passare alla fase successiva.
   - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
   - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
   - **Group Unique Name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a. `sAMAccountName` Per Active Directory e. `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
   - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a. `objectGUID` Per Active Directory e. `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, inserire le informazioni richieste relative al server LDAP e alla connessione di rete nella sezione Configura server LDAP.
   - **Nome host**: Il nome di dominio completo (FQDN) o l'indirizzo IP del server LDAP.
   - **Port** (porta): Porta utilizzata per la connessione al server LDAP.

     La porta predefinita per STARTTLS è 389 e la porta predefinita per LDAPS è 636. Tuttavia, è possibile utilizzare qualsiasi porta purché il firewall sia configurato correttamente.

   - **Username**: Percorso completo del nome distinto (DN) per l'utente che si connette al server LDAP.

     Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome

principale dell'utente.

L'utente specificato deve disporre dell'autorizzazione per elencare gruppi e utenti e per accedere ai seguenti attributi:

- `sAMAccountName` oppure `uid`
- `objectGUID`, `entryUUID`, o. `nsuniqueid`
- `cn`
- `memberOf` oppure `isMemberOf`
- **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl`, e. `userPrincipalName`
- **Azure**: `accountEnabled` e. `userPrincipalName`

◦ **Password**: La password associata al nome utente.

> Se si modifica la password in futuro, è necessario aggiornarla in questa pagina.

◦ **DN base gruppo**: Il percorso completo del nome distinto (DN) per una sottostruttura LDAP che si desidera cercare gruppi. Nell'esempio di Active Directory (riportato di seguito), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere utilizzati come gruppi federati.

> I valori **Group unique name** devono essere univoci all'interno del **Group base DN** a cui appartengono.

◦ **User base DN**: Percorso completo del nome distinto (DN) di una sottostruttura LDAP che si desidera cercare gli utenti.

> I valori **Nome univoco utente** devono essere univoci all'interno del **DN base utente** a cui appartengono.

◦ **Bind username format** (opzionale): Il modello di nome utente predefinito che StorageGRID deve utilizzare se il modello non può essere determinato automaticamente.

Si consiglia di fornire il formato **bind username** perché può consentire agli utenti di accedere se StorageGRID non è in grado di collegarsi con l'account del servizio.

Immettere uno di questi modelli:

- **Modello UserPrincipalName (Active Directory e Azure)**: `[USERNAME]@*example*.com`
- **Modello di nome di accesso di livello inferiore (Active Directory e Azure)**: `*example*\[USERNAME]`
- **Modello nome distinto**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Includi **[NOME UTENTE]** esattamente come scritto.

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.
   ◦ **Usa STARTTLS**: Utilizza STARTTLS per proteggere le comunicazioni con il server LDAP. Si tratta dell'opzione consigliata per Active Directory, OpenLDAP o altro, ma questa opzione non è supportata

per Azure.

- **Usa LDAPS**: L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Selezionare questa opzione per Azure.
- **Non utilizzare TLS**: Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Azure.

> L'utilizzo dell'opzione **non utilizzare TLS** non è supportato se il server Active Directory applica la firma LDAP. È necessario utilizzare STARTTLS o LDAPS.

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.
   - **Usa certificato CA del sistema operativo**: Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
   - **Usa certificato CA personalizzato**: Utilizza un certificato di protezione personalizzato.

     Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

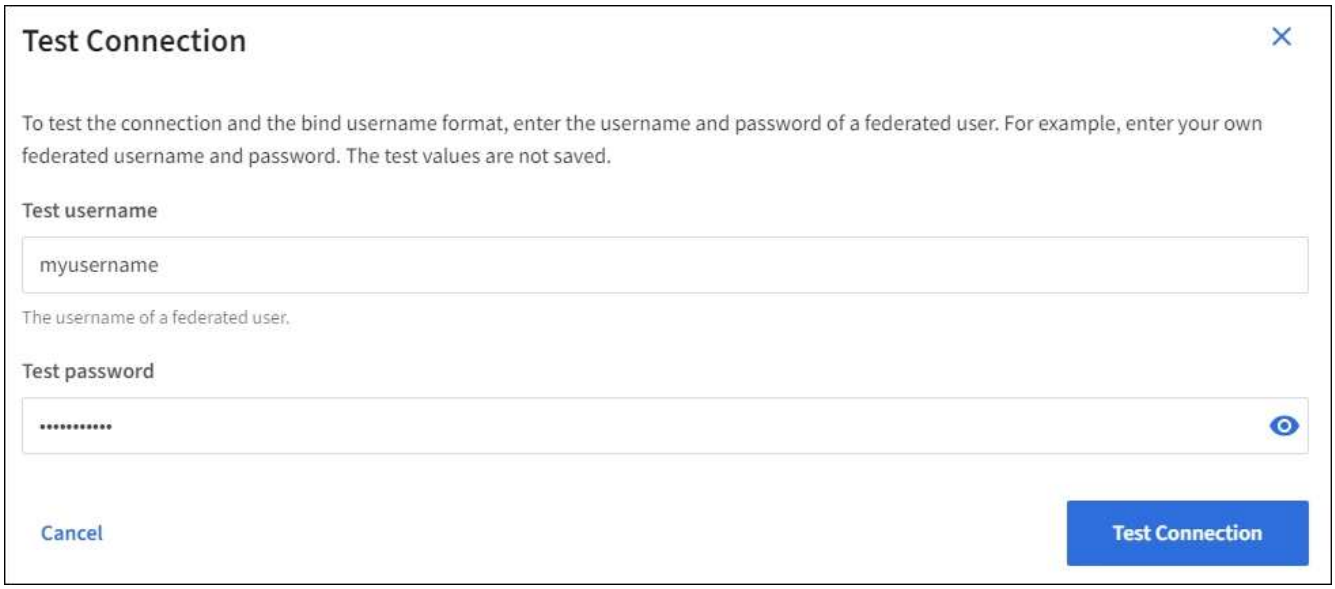
Verificare la connessione e salvare la configurazione

Dopo aver inserito tutti i valori, è necessario verificare la connessione prima di salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il server LDAP e il formato del nome utente BIND, se fornito.

Fasi

1. Selezionare **Test di connessione**.
2. Se non è stato fornito un formato nome utente BIND:
   - Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
   - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "Impossibile stabilire la connessione di prova". Selezionare **Chiudi**. Quindi, risolvere eventuali problemi e verificare nuovamente la connessione.
3. Se è stato fornito un formato BIND Username, inserire il nome utente e la password di un utente federato valido.

   Ad esempio, inserire il proprio nome utente e la propria password. Non includere caratteri speciali nel nome utente, ad esempio @ o /.



- Se le impostazioni di connessione sono valide, viene visualizzato il messaggio "Test connessione riuscito". Selezionare **Salva** per salvare la configurazione.
- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente BIND o il nome utente e la password di prova non sono validi. Risolvere eventuali problemi e verificare nuovamente la connessione.

Forzare la sincronizzazione con l'origine dell'identità

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dall'origine dell'identità. È possibile forzare l'avvio della sincronizzazione se si desidera attivare o limitare le autorizzazioni utente il più rapidamente possibile.

Fasi

1. Vai alla pagina Identity Federation.
2. Selezionare **Sync server** nella parte superiore della pagina.

   Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.

   L'avviso **errore di sincronizzazione federazione identità** viene attivato se si verifica un problema durante la sincronizzazione di utenti e gruppi federati dall'origine dell'identità.

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione di identità per gruppi e utenti. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riabilitare facilmente la federazione delle identità in futuro.

A proposito di questa attività

Prima di disattivare la federazione delle identità, è necessario tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.

- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita e non vengono generati avvisi o allarmi per gli account che non sono stati sincronizzati.
- La casella di controllo **Enable Identity Federation** (attiva federazione identità) è disattivata se Single Sign-on (SSO) è impostato su **Enabled** o **Sandbox Mode**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabled** prima di poter disattivare la federazione delle identità. Vedere "Disattiva single sign-on".

Fasi

1. Vai alla pagina Identity Federation.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).

Linee guida per la configurazione di un server OpenLDAP

Se si desidera utilizzare un server OpenLDAP per la federazione delle identità, è necessario configurare impostazioni specifiche sul server OpenLDAP.

> Per le fonti di identità che non sono Active Directory o Azure, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare eventuali chiavi S3 per l'utente o rimuovere l'utente da tutti i gruppi.

MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo in "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Indicizzazione

È necessario configurare i seguenti attributi OpenLDAP con le parole chiave di indice specificate:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Inoltre, assicurarsi che i campi indicati nella guida per Nome utente siano indicizzati per ottenere prestazioni ottimali.

Consultare le informazioni relative alla manutenzione dell'appartenenza al gruppo inverso nella sezione "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Gestire i gruppi di amministratori

È possibile creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Gli utenti devono appartenere a un gruppo per poter accedere al sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

- Se si intende importare un gruppo federated, la federazione delle identità è stata configurata e il gruppo federated esiste già nell'origine delle identità configurata.

Creare un gruppo di amministratori

I gruppi di amministratori consentono di determinare quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nell'API Grid Management.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Admin groups**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

È possibile creare un gruppo locale o importare un gruppo federated.

- Creare un gruppo locale se si desidera assegnare le autorizzazioni agli utenti locali.
- Creare un gruppo federated per importare gli utenti dall'origine dell'identità.

Gruppo locale

Fasi

1. Selezionare **Gruppo locale**.
2. Inserire un nome visualizzato per il gruppo, che sarà possibile aggiornare in seguito secondo necessità. Ad esempio, "Maintenance Users" (manutenzione utenti) o "ILM Administrators" (amministratori ILM).
3. Immettere un nome univoco per il gruppo, che non è possibile aggiornare in seguito.
4. Selezionare **continua**.

Gruppo federated

Fasi

1. Selezionare **Federated group**.
2. Immettere il nome del gruppo che si desidera importare, esattamente come appare nell'origine identità configurata.
   - Per Active Directory e Azure, utilizzare sAMAccountName.
   - Per OpenLDAP, utilizzare il CN (Common Name).
   - Per un altro LDAP, utilizzare il nome univoco appropriato per il server LDAP.
3. Selezionare **continua**.

Gestire le autorizzazioni di gruppo

Fasi

1. Per la modalità **Access**, selezionare se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API Grid Management o se possono visualizzare solo impostazioni e funzionalità.

- **Read-write** (valore predefinito): Gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle autorizzazioni di gestione.
- **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management. Gli utenti locali di sola lettura possono modificare le proprie password.

> Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Selezionare una o più opzioni "autorizzazioni del gruppo di amministrazione".

   È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti al gruppo non potranno accedere a StorageGRID.

3. Se si sta creando un gruppo locale, selezionare **continua**. Se si sta creando un gruppo federated, selezionare **Crea gruppo** e **fine**.

Aggiunta di utenti (solo gruppi locali)

Fasi

1. Facoltativamente, selezionare uno o più utenti locali per questo gruppo.

   Se non sono ancora stati creati utenti locali, è possibile salvare il gruppo senza aggiungere utenti. È possibile aggiungere questo gruppo all'utente nella pagina utenti. Vedere "Gestire gli utenti" per ulteriori informazioni.

2. Selezionare **Crea gruppo** e **fine**.

Visualizzare e modificare i gruppi di amministratori

È possibile visualizzare i dettagli dei gruppi esistenti, modificare un gruppo o duplicare un gruppo.

- Per visualizzare le informazioni di base per tutti i gruppi, consultare la tabella nella pagina gruppi.
- Per visualizzare tutti i dettagli di un gruppo specifico o per modificarlo, utilizzare il menu **azioni** o la pagina dei dettagli.

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli del gruppo	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Visualizza dettagli gruppo**.	Selezionare il nome del gruppo nella tabella.
Modifica nome visualizzato (solo gruppi locali)	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Modifica nome gruppo**. c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome del gruppo per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare la modalità di accesso o le autorizzazioni	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Visualizza dettagli gruppo**. c. In alternativa, modificare la modalità di accesso del gruppo. d. Facoltativamente, selezionare o deselezionare "autorizzazioni del gruppo di amministrazione". e. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome del gruppo per visualizzare i dettagli. b. In alternativa, modificare la modalità di accesso del gruppo. c. Facoltativamente, selezionare o deselezionare "autorizzazioni del gruppo di amministrazione". d. Selezionare **Save Changes** (Salva modifiche).

Duplicare un gruppo

Fasi

1. Selezionare la casella di controllo del gruppo.
2. Selezionare **azioni** > **Duplica gruppo**.
3. Completare la procedura guidata Duplica gruppo.

Eliminare un gruppo

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni associate al gruppo. L'eliminazione di un gruppo di amministratori rimuove gli utenti dal gruppo, ma non li elimina.

Fasi

1. Dalla pagina Groups (gruppi), selezionare la casella di controllo per ciascun gruppo che si desidera rimuovere.
2. Selezionare **azioni** > **Elimina gruppo**.
3. Selezionare **Elimina gruppi**.

Autorizzazioni del gruppo di amministrazione

Quando si creano gruppi di utenti admin, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare quali attività possono essere eseguite dall'utente.

È necessario assegnare almeno un'autorizzazione a ciascun gruppo; in caso contrario, gli utenti appartenenti a tale gruppo non potranno accedere a Grid Manager o all'API Grid Management.

Per impostazione predefinita, qualsiasi utente appartenente a un gruppo che dispone di almeno un'autorizzazione può eseguire le seguenti attività:

- Accedi a Grid Manager

- Visualizza la dashboard
- Visualizzare le pagine dei nodi
- Monitorare la topologia della griglia
- Visualizzare gli avvisi correnti e risolti
- Visualizzazione degli allarmi correnti e storici (sistema legacy)
- Modifica della propria password (solo utenti locali)
- Visualizzare alcune informazioni fornite nelle pagine Configurazione e manutenzione

Interazione tra permessi e modalità di accesso

Per tutte le autorizzazioni, l'impostazione **modalità di accesso** del gruppo determina se gli utenti possono modificare le impostazioni ed eseguire operazioni o se possono visualizzare solo le relative impostazioni e funzionalità. Se un utente appartiene a più gruppi e un gruppo è impostato su **sola lettura**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Le sezioni seguenti descrivono le autorizzazioni che è possibile assegnare durante la creazione o la modifica di un gruppo amministrativo. Qualsiasi funzionalità non esplicitamente menzionata richiede l'autorizzazione **Root access**.

Accesso root

Questa autorizzazione consente di accedere a tutte le funzioni di amministrazione della griglia.

Riconoscere gli allarmi (legacy)

Questa autorizzazione consente di riconoscere e rispondere agli allarmi (sistema legacy). Tutti gli utenti che hanno effettuato l'accesso possono visualizzare gli allarmi correnti e storici.

Se si desidera che un utente monitori la topologia della griglia e riconosca solo gli allarmi, è necessario assegnare questa autorizzazione.

Modificare la password root del tenant

Questa autorizzazione consente di accedere all'opzione **Modifica password root** nella pagina tenant, consentendo di controllare chi può modificare la password per l'utente root locale del tenant. Questa autorizzazione viene utilizzata anche per la migrazione delle chiavi S3 quando è attivata la funzione di importazione delle chiavi S3. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Modifica password root**.

> Per consentire l'accesso alla pagina dei tenant, che contiene l'opzione **Modifica password root**, assegnare anche l'autorizzazione **account tenant**.

Configurazione della pagina della topologia della griglia

Questa autorizzazione consente di accedere alle schede di configurazione nella pagina **SUPPORTO** > **Strumenti** > **topologia griglia**.

ILM

Questa autorizzazione consente di accedere alle seguenti opzioni del menu **ILM**:

- Regole
- Policy
- Erasure coding
- Regioni
- Pool di storage

> Gli utenti devono disporre delle autorizzazioni **altra configurazione griglia** e **Configurazione della pagina topologia griglia** per gestire i gradi di storage.

Manutenzione

Gli utenti devono disporre dell'autorizzazione Maintenance per utilizzare queste opzioni:

- **CONFIGURAZIONE** > **controllo degli accessi**:
  - Password di rete
- **CONFIGURAZIONE** > **rete**:
  - Nomi di dominio degli endpoint S3
- **MANUTENZIONE** > **attività**:
  - Decommissionare
  - Espansione
  - Controllo dell'esistenza dell'oggetto
  - Recovery (recupero)
- **MANUTENZIONE** > **sistema**:
  - Pacchetto di recovery
  - Aggiornamento del software
- **SUPPORTO** > **Strumenti**:
  - Registri

Gli utenti che non dispongono dell'autorizzazione Maintenance possono visualizzare, ma non modificare, le seguenti pagine:

- **MANUTENZIONE** > **rete**:
  - Server DNS
  - Grid Network
  - Server NTP
- **MANUTENZIONE** > **sistema**:
  - Licenza
- **CONFIGURAZIONE** > **rete**:
  - Nomi di dominio degli endpoint S3
- **CONFIGURAZIONE** > **sicurezza**:
  - Certificati

- **CONFIGURAZIONE** > **monitoraggio**:
  - Server syslog e audit

Gestire gli avvisi

Questa autorizzazione consente di accedere alle opzioni per la gestione degli avvisi. Gli utenti devono disporre di questa autorizzazione per gestire silenzi, notifiche di avviso e regole di avviso.

Query sulle metriche

Questa autorizzazione consente di accedere a:

- **SUPPORTO** > **Strumenti** > pagina **metriche**
- Query di metriche Prometheus personalizzate utilizzando la sezione **metriche** dell'API Grid Management
- Schede dashboard di Grid Manager che contengono metriche

Ricerca dei metadati degli oggetti

Questa autorizzazione consente di accedere alla pagina **ILM** > **Object metadata lookup**.

Altra configurazione della griglia

Questa autorizzazione consente di accedere a ulteriori opzioni di configurazione della griglia.

> Per visualizzare queste opzioni aggiuntive, gli utenti devono anche disporre dell'autorizzazione **Grid topology page Configuration** (Configurazione pagina topologia griglia).

- **ILM**:
  - Gradi di storage
- **CONFIGURAZIONE** > **sistema**:
  - Opzioni di storage
- **SUPPORTO** > **Allarmi (legacy)**:
  - Eventi personalizzati
  - Allarmi globali
  - Configurazione della posta elettronica legacy
- **SUPPORTO** > **altro**:
  - Costo del collegamento

Amministratore dell'appliance di storage

Questa autorizzazione fornisce:

- Accesso al System Manager di e-Series SANtricity sulle appliance di storage tramite il Grid Manager.
- La possibilità di eseguire attività di troubleshooting e manutenzione nella scheda Manage drives (Gestione dischi) per le appliance che supportano queste operazioni.

Account tenant

Questa autorizzazione consente di:

- Accedere alla pagina tenant, in cui è possibile creare, modificare e rimuovere gli account tenant
- Visualizzare le policy di classificazione del traffico esistenti
- Visualizza le schede dashboard di Grid Manager che contengono i dettagli del tenant

Gestire gli utenti

È possibile visualizzare utenti locali e federati. È inoltre possibile creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzioni di Grid Manager possono accedere questi utenti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Creare un utente locale

È possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi locali. Le autorizzazioni del gruppo controllano a quali funzioni dell'API Grid Manager e Grid Management l'utente può accedere.

È possibile creare solo utenti locali. Utilizzare l'origine dell'identità esterna per gestire utenti e gruppi federati.

Grid Manager include un utente locale predefinito, denominato "root". Non puoi rimuovere l'utente root.

Se è attivato il Single Sign-on (SSO), gli utenti locali non possono accedere a StorageGRID.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Admin users**.
2. Selezionare **Crea utente**.

Immettere le credenziali dell'utente

Fasi

1. Immettere il nome completo dell'utente, un nome utente univoco e una password.
2. Se si desidera, selezionare **Sì** se l'utente non deve avere accesso all'API Grid Manager o Grid Management.
3. Selezionare **continua**.

Assegnare ai gruppi

Fasi

1. Facoltativamente, assegnare l'utente a uno o più gruppi per determinare le autorizzazioni dell'utente.

   Se non sono ancora stati creati gruppi, è possibile salvare l'utente senza selezionare i gruppi. È possibile aggiungere questo utente a un gruppo nella pagina gruppi.

Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Vedere "Gestire i gruppi di amministratori" per ulteriori informazioni.

2. Selezionare **Crea utente** e selezionare **fine**.

Visualizzare e modificare gli utenti locali

È possibile visualizzare i dettagli degli utenti locali e federati esistenti. È possibile modificare un utente locale per modificare il nome completo, la password o l'appartenenza al gruppo dell'utente. È inoltre possibile impedire temporaneamente a un utente di accedere a Grid Manager e all'API Grid Management.

È possibile modificare solo gli utenti locali. Utilizzare l'origine dell'identità esterna per gestire gli utenti federati.

- Per visualizzare le informazioni di base per tutti gli utenti locali e federati, consultare la tabella nella pagina utenti.
- Per visualizzare tutti i dettagli di un utente specifico, modificare un utente locale o modificare la password di un utente locale, utilizzare il menu **azioni** o la pagina dei dettagli.

  Tutte le modifiche vengono applicate alla successiva disconnessione dell'utente e all'accesso a Grid Manager.

  Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Change password** (Modifica password) nel banner Grid Manager.

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli dell'utente	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**.	Selezionare il nome dell'utente nella tabella.
Modifica nome completo (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Modifica nome completo**. c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Negare o consentire l'accesso a StorageGRID	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda Access (accesso). d. Selezionare **Sì** per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare **No** per consentire all'utente di accedere. e. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Access (accesso). c. Selezionare **Sì** per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare **No** per consentire all'utente di accedere. d. Selezionare **Save Changes** (Salva modifiche).
Modifica della password (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda Password. d. Inserire una nuova password. e. Selezionare **Cambia password**.	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Password. c. Inserire una nuova password. d. Selezionare **Cambia password**.
Modifica dei gruppi (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda gruppi. d. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. e. Selezionare **Edit groups** (Modifica gruppi) per selezionare diversi gruppi. f. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda gruppi. c. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. d. Selezionare **Edit groups** (Modifica gruppi) per selezionare diversi gruppi. e. Selezionare **Save Changes** (Salva modifiche).

Duplicare un utente

È possibile duplicare un utente esistente per creare un nuovo utente con le stesse autorizzazioni.

Fasi

1. Selezionare la casella di controllo dell'utente.

2. Selezionare **azioni** > **utente duplicato**.
3. Completare la procedura guidata Duplica utente.

Eliminare un utente

È possibile eliminare un utente locale per rimuoverlo definitivamente dal sistema.

Impossibile eliminare l'utente root.

Fasi

1. Nella pagina utenti, selezionare la casella di controllo per ciascun utente che si desidera rimuovere.
2. Selezionare **azioni** > **Elimina utente**.
3. Selezionare **Delete user** (Elimina utente).

Utilizzo di SSO (Single Sign-on)

Configurare il single sign-on

Quando è attivato il Single Sign-on (SSO), gli utenti possono accedere a Grid Manager, Tenant Manager, Grid Management API o tenant Management API solo se le loro credenziali sono autorizzate utilizzando il processo di accesso SSO implementato dall'organizzazione. Gli utenti locali non possono accedere a StorageGRID.

Come funziona il single sign-on

Il sistema StorageGRID supporta SSO (Single Sign-on) utilizzando lo standard SAML 2.0 (Security Assertion Markup Language 2.0).

Prima di attivare SSO (Single Sign-on), esaminare in che modo i processi di accesso e disconnessione di StorageGRID vengono influenzati quando SSO è attivato.

Effettuare l'accesso quando SSO è attivato

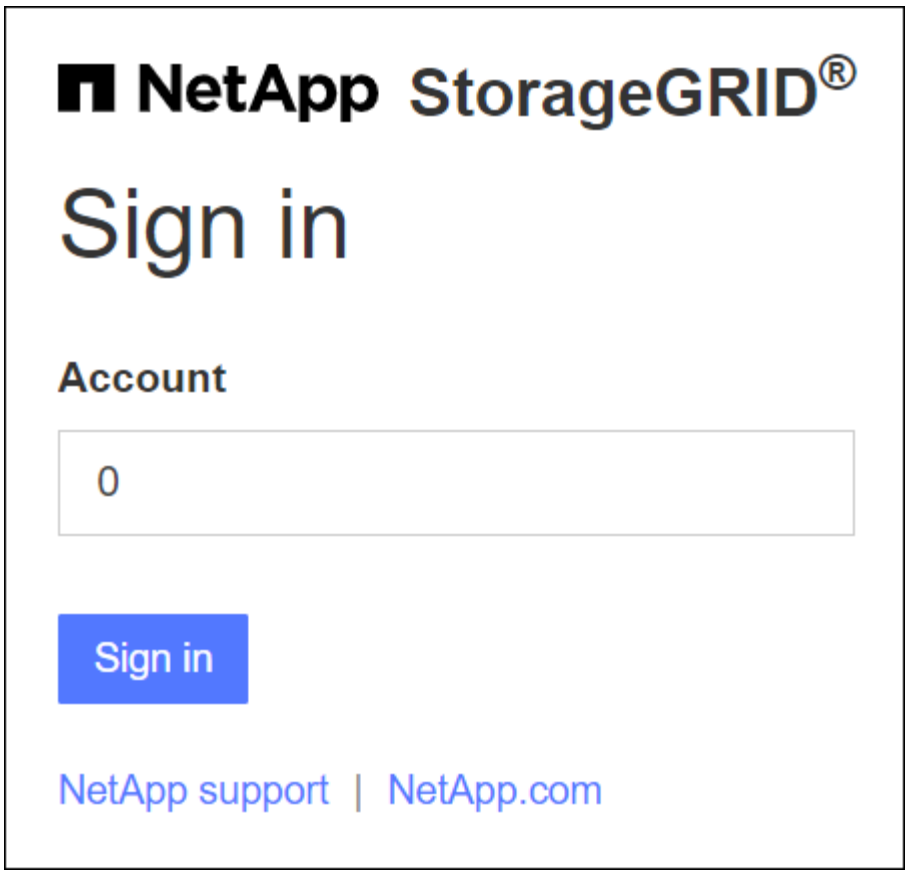
Quando SSO è attivato e si accede a StorageGRID, si viene reindirizzati alla pagina SSO dell'organizzazione per convalidare le credenziali.

Fasi

1. Immettere il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione StorageGRID in un browser Web.

   Viene visualizzata la pagina di accesso a StorageGRID.

   - Se si accede per la prima volta all'URL del browser, viene richiesto di inserire un ID account:

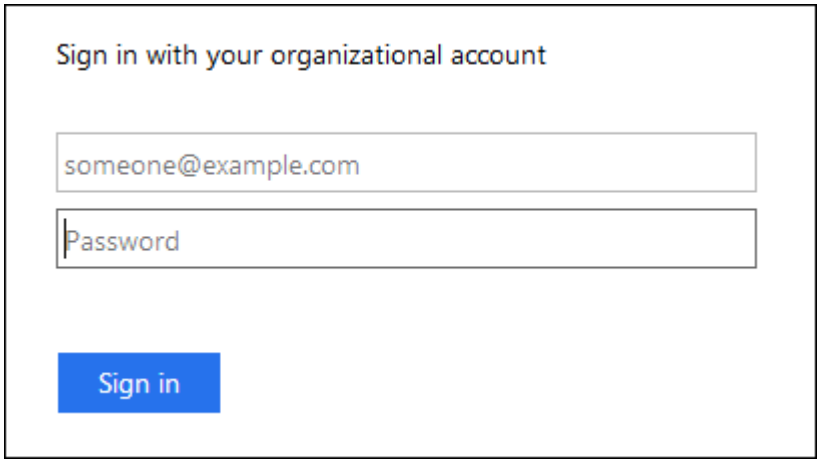


- Se in precedenza hai effettuato l'accesso a Grid Manager o al Tenant Manager, ti verrà richiesto di selezionare un account recente o di inserire un ID account:

La pagina di accesso a StorageGRID non viene visualizzata quando si inserisce l'URL completo di un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da) `/?accountId=20-digit-account-id`). Al contrario, si viene immediatamente reindirizzati alla pagina di accesso SSO dell'organizzazione, dove è possibile Accedi con le tue credenziali SSO.

2. Indicare se si desidera accedere a Grid Manager o al tenant Manager:
   - Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, inserire **0** come ID account o selezionare **Grid Manager** se compare nell'elenco degli account recenti.
   - Per accedere al tenant Manager, inserire l'ID account tenant di 20 cifre o selezionare un tenant in base al nome, se visualizzato nell'elenco degli account recenti.
3. Selezionare **Accedi**

   StorageGRID reindirizza l'utente alla pagina di accesso SSO della propria organizzazione. Ad esempio:



4. Accedi con le tue credenziali SSO.

   Se le credenziali SSO sono corrette:

   a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
   b. StorageGRID convalida la risposta di autenticazione.
   c. Se la risposta è valida e l'utente appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID, l'utente ha effettuato l'accesso a Gestione griglia o a Gestione tenant, a seconda dell'account selezionato.

   Se l'account del servizio non è accessibile, è comunque possibile effettuare l'accesso, purché si sia un utente esistente che appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID.

5. Se si dispone di autorizzazioni adeguate, è possibile accedere ad altri nodi di amministrazione o a Grid Manager o Tenant Manager.

   Non è necessario immettere nuovamente le credenziali SSO.

Disconnettersi quando SSO è attivato

Quando SSO è abilitato per StorageGRID, ciò che accade quando si effettua la disconnessione dipende da ciò che si effettua l'accesso e da dove si effettua la disconnessione.

Fasi

1. Individuare il collegamento **Disconnetti** nell'angolo in alto a destra dell'interfaccia utente.
2. Selezionare **Disconnetti**.

   Viene visualizzata la pagina di accesso a StorageGRID. Il menu a discesa **Recent Accounts** (account recenti) viene aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere a queste interfacce utente più rapidamente in futuro.

Se hai effettuato l'accesso a…	E ti disconnetterai da…	Sei disconnesso da…
Grid Manager su uno o più nodi di amministrazione	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi di amministrazione **Nota:** se si utilizza Azure per SSO, la disconnessione da tutti i nodi Admin potrebbe richiedere alcuni minuti.
Tenant Manager su uno o più nodi di amministrazione	Tenant Manager su qualsiasi nodo di amministrazione	Tenant Manager su tutti i nodi di amministrazione
Sia Grid Manager che tenant Manager	Grid Manager	Solo Grid Manager. Per disconnettersi da SSO, devi anche disconnetterti da Tenant Manager.

La tabella riassume ciò che accade quando si effettua la disconnessione se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti separatamente da tutte le sessioni del browser.

Requisiti e considerazioni per il single sign-on

Prima di abilitare il single sign-on (SSO) per un sistema StorageGRID, esaminare i requisiti e le considerazioni.

Requisiti del provider di identità

StorageGRID supporta i seguenti provider di identità SSO (IdP):

- Active Directory Federation Service (ad FS)
- Azure Active Directory (Azure ad)
- PingFederate

È necessario configurare la federazione delle identità per il sistema StorageGRID prima di poter configurare un provider di identità SSO. Il tipo di servizio LDAP utilizzato per i controlli di federazione delle identità che

consentono di implementare il tipo di SSO.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

Requisiti AD FS

È possibile utilizzare una delle seguenti versioni di ad FS:

- Windows Server 2022 ad FS
- Windows Server 2019 ad FS
- Windows Server 2016 ad FS

> Windows Server 2016 dovrebbe utilizzare "Aggiornamento KB3201845", o superiore.

Requisiti aggiuntivi

- Transport Layer Security (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Considerazioni per Azure

Se si utilizza Azure come tipo SSO e gli utenti dispongono di nomi principali che non utilizzano il nome sAMAccountName come prefisso, possono verificarsi problemi di accesso se StorageGRID perde la connessione con il server LDAP. Per consentire agli utenti di accedere, è necessario ripristinare la connessione al server LDAP.

Requisiti dei certificati del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun nodo di amministrazione per garantire l'accesso al gestore di griglia, al gestore del tenant, all'API di gestione del grid e all'API di gestione del tenant. Quando si configurano i trust delle parti di base (ad FS), le applicazioni aziendali (Azure) o le connessioni del provider di servizi (PingFederate) per StorageGRID, il certificato del server viene utilizzato come certificato di firma per le richieste StorageGRID.

Se non lo hai già fatto "ha configurato un certificato personalizzato per l'interfaccia di gestione", dovresti farlo ora. Quando si installa un certificato server personalizzato, viene utilizzato per tutti i nodi di amministrazione e può essere utilizzato in tutti i trust, le applicazioni aziendali o le connessioni SP di StorageGRID.

> Si sconsiglia di utilizzare il certificato server predefinito di un nodo di amministrazione in una connessione SP, un'applicazione aziendale o un trust di parte attiva. Se il nodo si guasta e viene ripristinato, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della parte che si basa, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo amministratore accedendo alla shell dei comandi del nodo e accedendo a. `/var/local/mgmt-api` directory. Viene assegnato un nome a un certificato server personalizzato `custom-server.crt`. Il certificato server predefinito del nodo viene denominato `server.crt`.

Requisiti delle porte

Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443). Vedere "Controllare l'accesso al firewall esterno".

Confermare che gli utenti federati possono accedere

Prima di attivare il Single Sign-on (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per qualsiasi account tenant esistente.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- La federazione delle identità è già stata configurata.

Fasi

1. Se esistono account tenant, verificare che nessuno dei tenant utilizzi la propria origine di identità.

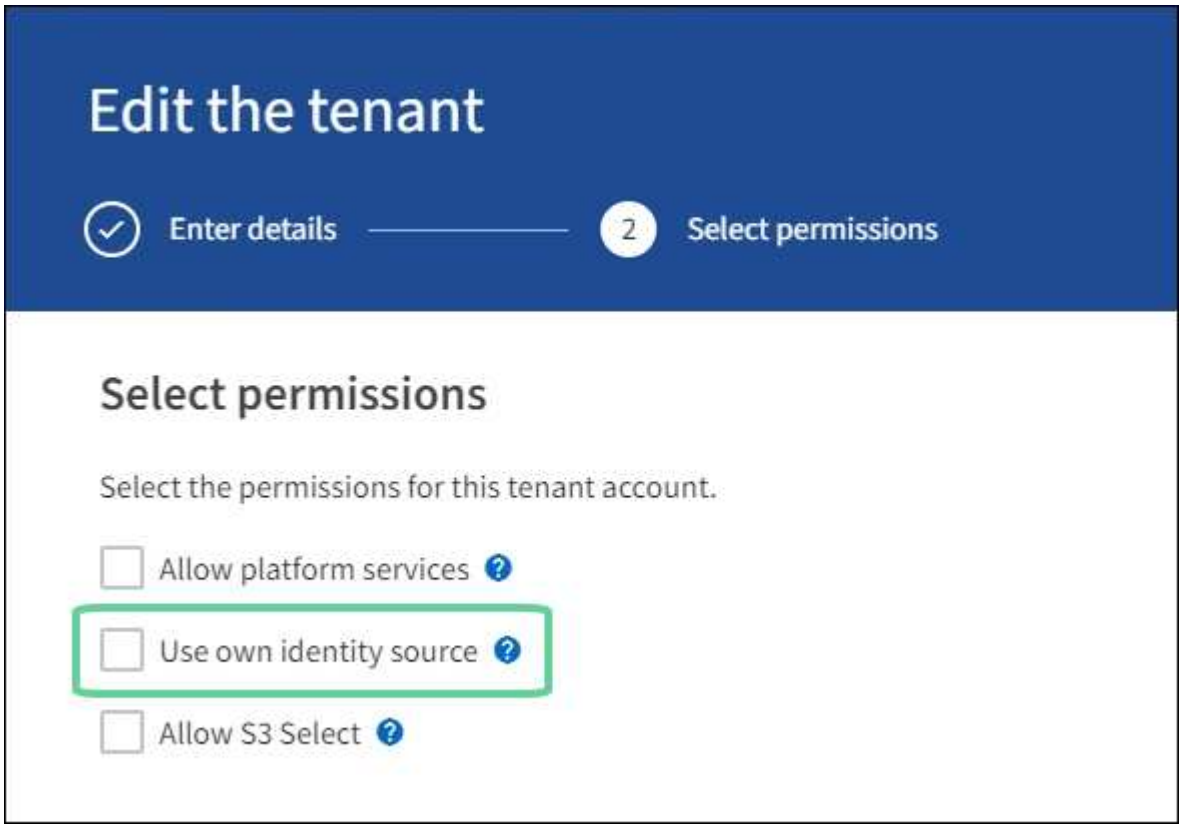
   Quando si attiva SSO, un'origine identità configurata in Tenant Manager viene ignorata dall'origine identità configurata in Grid Manager. Gli utenti che appartengono all'origine dell'identità del tenant non potranno più accedere a meno che non dispongano di un account con l'origine dell'identità di Grid Manager.

   a. Accedi al tenant manager per ogni account tenant.
   b. Selezionare **ACCESS MANAGEMENT** > **Identity Federation**.
   c. Verificare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
   d. In tal caso, verificare che i gruppi federati che potrebbero essere in uso per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.

2. Verificare che un utente federated possa accedere a Grid Manager:
   a. Da Grid Manager, selezionare **CONFIGURATION** > **Access control** > **Admin groups**.
   b. Assicurarsi che almeno un gruppo federated sia stato importato dall'origine dell'identità di Active Directory e che sia stata assegnata l'autorizzazione di accesso root.
   c. Disconnettersi.
   d. Confermare che è possibile accedere nuovamente a Grid Manager come utente nel gruppo federated.
3. Se sono presenti account tenant, verificare che un utente federated che dispone dell'autorizzazione di accesso root possa effettuare l'accesso:
   a. In Grid Manager, selezionare **TENANT**.
   b. Selezionare l'account tenant e selezionare **azioni** > **Modifica**.

c. Nella scheda Immetti dettagli, selezionare **continua**.

d. Se la casella di controllo **Usa origine identità propria** è selezionata, deselezionare la casella e selezionare **Salva**.



Viene visualizzata la pagina del tenant.

a. Selezionare l'account tenant, selezionare **Accedi** e accedere all'account tenant come utente root locale.

b. Da Tenant Manager, selezionare **ACCESS MANAGEMENT** > **Groups**.

c. Assicurarsi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di accesso root per questo tenant.

d. Disconnettersi.

e. Confermare che è possibile accedere nuovamente al tenant come utente nel gruppo federated.

Informazioni correlate

- "Requisiti e considerazioni per il single sign-on"
- "Gestire i gruppi di amministratori"
- "Utilizzare un account tenant"

USA la modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare SSO (Single Sign-on) prima di attivarla per tutti gli utenti StorageGRID. Una volta attivato SSO, è possibile tornare alla modalità sandbox ogni volta che è necessario modificare o ripetere il test della configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Hai configurato la federazione delle identità per il tuo sistema StorageGRID.
- Per la federazione di identità **tipo di servizio LDAP**, è stato selezionato Active Directory o Azure, in base al provider di identità SSO che si intende utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory	• Active Directory • Azure • PingFederate
Azure	Azure

A proposito di questa attività

Quando SSO è attivato e un utente tenta di accedere a un nodo amministratore, StorageGRID invia una richiesta di autenticazione al provider di identità SSO. A sua volta, il provider di identità SSO invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autenticazione ha avuto esito positivo. Per le richieste riuscite:

- La risposta di Active Directory o PingFederate include un UUID (Universally Unique Identifier) per l'utente.
- La risposta di Azure include un User Principal Name (UPN).

Per consentire a StorageGRID (il provider di servizi) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione dell'utente, è necessario configurare alcune impostazioni in StorageGRID. Quindi, è necessario utilizzare il software del provider di identità SSO per creare un trust di parte (ad FS), un'applicazione aziendale (Azure) o un provider di servizi (PingFederate) per ciascun nodo di amministrazione. Infine, è necessario tornare a StorageGRID per attivare SSO.

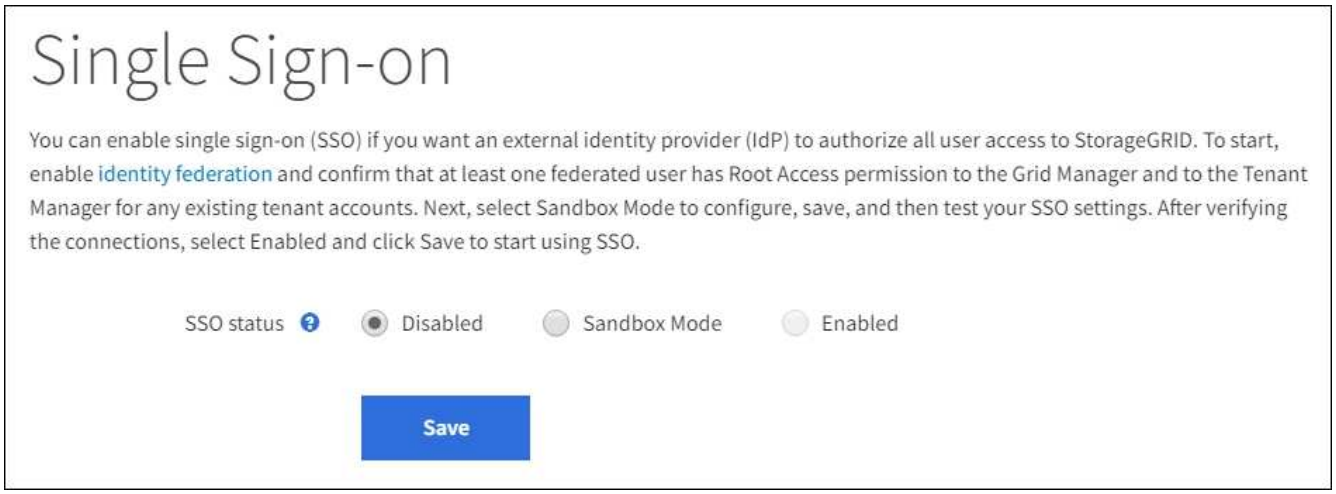
La modalità sandbox semplifica l'esecuzione di questa configurazione e il test di tutte le impostazioni prima di attivare SSO. Quando si utilizza la modalità sandbox, gli utenti non possono accedere utilizzando SSO.

Accedere alla modalità sandbox

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.

   Viene visualizzata la pagina Single Sign-on (accesso singolo), con l'opzione **Disabled** (Disattivato) selezionata.



Se le opzioni di stato SSO non vengono visualizzate, verificare di aver configurato il provider di identità come origine dell'identità federata. Vedere "Requisiti e considerazioni per il single sign-on".

2. Selezionare **Sandbox Mode**.

   Viene visualizzata la sezione Identity Provider (Provider di identità).

Inserire i dettagli del provider di identità

Fasi

1. Selezionare **tipo SSO** dall'elenco a discesa.
2. Compilare i campi nella sezione Identity Provider (Provider di identità) in base al tipo di SSO selezionato.

Active Directory

1. Inserire il nome del servizio Federazione* del provider di identità, esattamente come appare in Active Directory Federation Service (ad FS).

   Per individuare il nome del servizio federativo, accedere a Gestione server Windows. Selezionare **Tools** > **ad FS Management**. Dal menu Action (azione), selezionare **Edit Federation Service Properties** (Modifica proprietà servizio federazione). Il nome del servizio della federazione viene visualizzato nel secondo campo.

2. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.
   - **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
   - **Usa certificato CA personalizzato**: Utilizza un certificato CA personalizzato per proteggere la connessione.

     Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

   - **Non utilizzare TLS**: Non utilizzare un certificato TLS per proteggere la connessione.

     Se si modifica immediatamente il certificato CA "Riavviare il servizio Mgmt-api sui nodi Admin" E testare un SSO di successo in Grid Manager.

3. Nella sezione parte che si basa, specificare il **identificativo della parte che si basa** per StorageGRID. Questo valore controlla il nome utilizzato per ciascun trust di parte che si basa in ad FS.
   - Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che mostra l'identificativo del componente di base per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

   È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

4. Selezionare **Salva**.

   Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.

Azure

1. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità

invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.

- **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Usa certificato CA personalizzato**: Utilizza un certificato CA personalizzato per proteggere la connessione.

  Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

- **Non utilizzare TLS**: Non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica immediatamente il certificato CA "Riavviare il servizio Mgmt-api sui nodi Admin" E testare un SSO di successo in Grid Manager.

2. Nella sezione applicazione aziendale, specificare **Nome applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ogni applicazione aziendale in Azure ad.

   - Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che mostra il nome di un'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

> È necessario creare un'applicazione aziendale per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un'applicazione aziendale per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

3. Seguire la procedura descritta in "Creare applicazioni aziendali in Azure ad" Per creare un'applicazione aziendale per ciascun nodo amministratore elencato nella tabella.
4. Da Azure ad, copiare l'URL dei metadati della federazione per ciascuna applicazione aziendale. Quindi, incolla questo URL nel corrispondente campo **URL metadati federazione** in StorageGRID.
5. Dopo aver copiato e incollato un URL dei metadati della federazione per tutti i nodi di amministrazione, selezionare **Salva**.

   Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.

PingFederate

1. Specificare il certificato TLS da utilizzare per proteggere la connessione quando il provider di identità invia le informazioni di configurazione SSO in risposta alle richieste StorageGRID.
   - **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
   - **Usa certificato CA personalizzato**: Utilizza un certificato CA personalizzato per proteggere la connessione.

Se si seleziona questa impostazione, copiare il testo del certificato personalizzato e incollarlo nella casella di testo **certificato CA**.

- **Non utilizzare TLS**: Non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica immediatamente il certificato CA "Riavviare il servizio Mgmt-api sui nodi Admin" E testare un SSO di successo in Grid Manager.

2. Nella sezione Provider di servizi (SP), specificare **ID connessione SP** per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.
   - Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che mostra l'ID di connessione SP per ciascun nodo amministratore del sistema, in base al nome host del nodo.

> È necessario creare una connessione SP per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di una connessione SP per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

3. Specificare l'URL dei metadati della federazione per ciascun nodo amministratore nel campo **URL metadati federazione**.

   Utilizzare il seguente formato:

```
https://<Federation Service Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP Connection ID>
```

4. Selezionare **Salva**.

   Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.

Configurare i trust, le applicazioni aziendali o le connessioni SP della parte che si basa

Una volta salvata la configurazione, viene visualizzato l'avviso di conferma della modalità Sandbox. Questo avviso conferma che la modalità sandbox è ora attivata e fornisce istruzioni generali.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, quando si seleziona **modalità sandbox** nella pagina Single Sign-on (accesso singolo), SSO viene disattivato per tutti gli utenti StorageGRID. Solo gli utenti locali possono effettuare l'accesso.

Attenersi alla procedura descritta di seguito per configurare i trust (Active Directory), le applicazioni aziendali

complete (Azure) o le connessioni SP (PingFederate).

Active Directory

Fasi

1. Accedere a Active Directory Federation Services (ad FS).
2. Creare uno o più trust di parti di supporto per StorageGRID, utilizzando ciascun identificatore di parte di supporto mostrato nella tabella della pagina di accesso singolo di StorageGRID.

   È necessario creare un trust per ciascun nodo di amministrazione mostrato nella tabella.

   Per istruzioni, visitare il sito Web all'indirizzo "Creazione di trust di parti di base in ad FS".

Azure

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   c. Scaricare e salvare i metadati SAML per quel nodo.
3. Accedere al portale Azure.
4. Seguire la procedura descritta in "Creare applicazioni aziendali in Azure ad" Per caricare il file di metadati SAML per ciascun nodo di amministrazione nella relativa applicazione aziendale Azure corrispondente.

PingFederate

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   c. Scaricare e salvare i metadati SAML per quel nodo.
3. Accedere a PingFederate.
4. "Creare una o più connessioni del provider di servizi (SP) per StorageGRID". Utilizzare l'ID connessione SP per ciascun nodo amministratore (mostrato nella tabella della pagina accesso singolo StorageGRID) e i metadati SAML scaricati per tale nodo amministratore.

   È necessario creare una connessione SP per ciascun nodo di amministrazione mostrato nella tabella.

Verificare le connessioni SSO

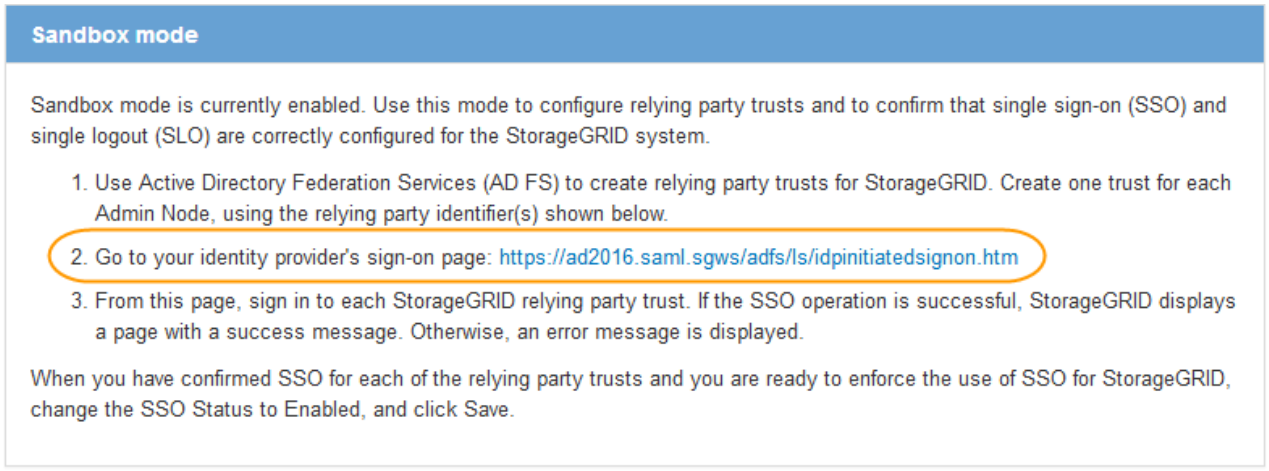
Prima di imporre l'utilizzo del single sign-on per l'intero sistema StorageGRID, è necessario confermare che il single sign-on e il singolo logout sono configurati correttamente per ciascun nodo di amministrazione.

Active Directory

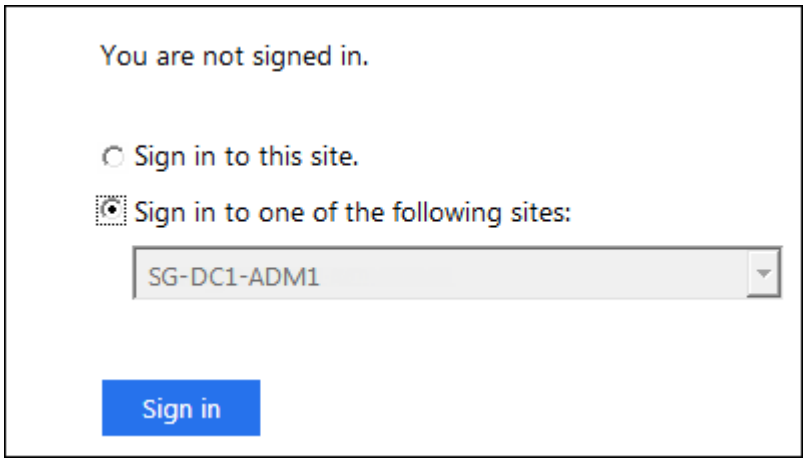
Fasi

1. Dalla pagina Single Sign-on di StorageGRID, individuare il collegamento nel messaggio in modalità sandbox.

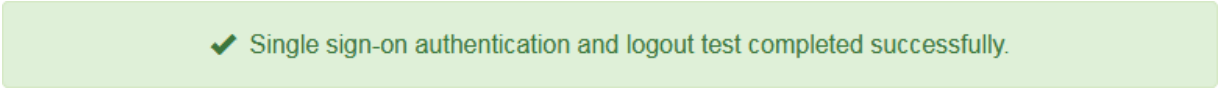
   L'URL deriva dal valore immesso nel campo **Federation service name**.



2. Selezionare il collegamento oppure copiare e incollare l'URL in un browser per accedere alla pagina di accesso del provider di identità.
3. Per confermare che è possibile utilizzare SSO per accedere a StorageGRID, selezionare **Accedi a uno dei seguenti siti**, selezionare l'identificativo della parte di base per il nodo di amministrazione principale e selezionare **Accedi**.



4. Immettere il nome utente e la password federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.



   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
5. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione

nella griglia.

Azure

Fasi

1. Vai alla pagina Single Sign-on nel portale Azure.
2. Selezionare **Test dell'applicazione**.
3. Immettere le credenziali di un utente federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.

     ✔ Single sign-on authentication and logout test completed successfully.

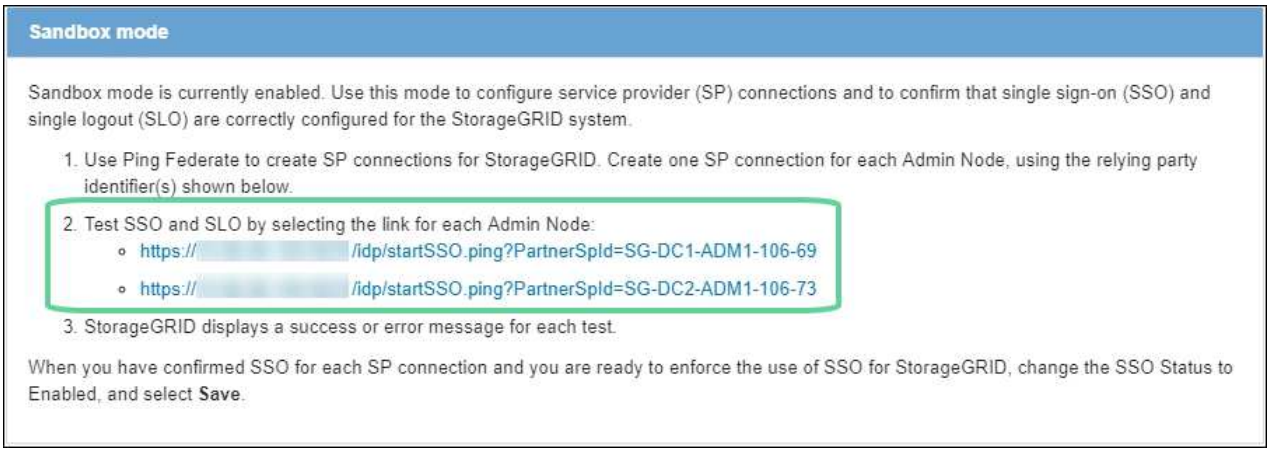
   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
4. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

PingFederate

Fasi

1. Dalla pagina accesso singolo StorageGRID, selezionare il primo collegamento nel messaggio in modalità sandbox.

   Selezionare e verificare un collegamento alla volta.



2. Immettere le credenziali di un utente federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
3. Selezionare il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

Se viene visualizzato un messaggio Page Expired (pagina scaduta), selezionare il pulsante **Back** (Indietro) nel browser e inviare nuovamente le credenziali.

Attiva single sign-on

Una volta confermata la possibilità di utilizzare SSO per accedere a ciascun nodo amministrativo, è possibile attivare SSO per l'intero sistema StorageGRID.

Quando SSO è attivato, tutti gli utenti devono utilizzare SSO per accedere a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Gli utenti locali non possono più accedere a StorageGRID.

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
2. Impostare lo stato SSO su **Enabled**.
3. Selezionare **Salva**.
4. Esaminare il messaggio di avviso e selezionare **OK**.

   Il Single Sign-on è ora attivato.

Se si utilizza il portale Azure e si accede a StorageGRID dallo stesso computer utilizzato per accedere ad Azure, assicurarsi che l'utente sia anche un utente StorageGRID autorizzato (un utente di un gruppo federato importato in StorageGRID) Oppure disconnettersi dal portale Azure prima di tentare di accedere a StorageGRID.

Creazione di trust di parti di base in ad FS

È necessario utilizzare Active Directory Federation Services (ad FS) per creare un trust di parte per ciascun nodo di amministrazione nel sistema. È possibile creare trust di parti che utilizzano i comandi PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **ad FS** come tipo di SSO.
- **La modalità Sandbox** è selezionata nella pagina Single Sign-on di Grid Manager. Vedere "USA la modalità sandbox".
- Si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo di amministrazione nel sistema. Questi valori sono disponibili nella tabella dei dettagli dei nodi di amministrazione nella pagina accesso singolo StorageGRID.

  È necessario creare un trust per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un trust per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.
- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.

- Se si crea manualmente l'attendibilità del componente di base, si dispone del certificato personalizzato caricato per l'interfaccia di gestione di StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

A proposito di questa attività

Queste istruzioni si applicano a Windows Server 2016 ad FS. Se si utilizza una versione diversa di ad FS, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

Creare un trust di parte con Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust di parti.

Fasi

1. Dal menu Start di Windows, selezionare con il pulsante destro del mouse l'icona PowerShell e selezionare **Esegui come amministratore**.
2. Al prompt dei comandi di PowerShell, immettere il seguente comando:

   `Add-AdfsRelyingPartyTrust -Name "Admin_Node_identifer" -MetadataURL "https://Admin_Node_FQDN/api/saml-metadata"

   - Per *`Admin_Node_Identifier`*, Immettere l'identificativo della parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1`.
   - Per *`Admin_Node_FQDN`*, Immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).
3. Da Gestione server Windows, selezionare **Strumenti** > **Gestione di ad FS**.

   Viene visualizzato lo strumento di gestione di ad FS.

4. Selezionare **ad FS** > **Trust di parte**.

   Viene visualizzato l'elenco dei trust della parte che si basa.

5. Aggiungere un criterio di controllo degli accessi al trust della parte di base appena creato:
   a. Individuare la fiducia della parte di base appena creata.
   b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit Access Control Policy** (Modifica policy di controllo degli accessi).
   c. Selezionare un criterio di controllo degli accessi.
   d. Selezionare **Applica** e **OK**
6. Aggiungere una policy di emissione delle richieste di rimborso al nuovo Trust della parte di base creato:
   a. Individuare la fiducia della parte di base appena creata.
   b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
   c. Selezionare **Aggiungi regola**.
   d. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).

e. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

   Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

f. Per l'archivio attributi, selezionare **Active Directory**.

g. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.

h. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.

i. Selezionare **fine**, quindi **OK**.

7. Verificare che i metadati siano stati importati correttamente.

   a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.

   b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

      Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.

8. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.

9. Una volta completata l'operazione, tornare a StorageGRID e verificare tutti i trust delle parti di base per verificare che siano configurati correttamente. Vedere "Utilizzare la modalità Sandbox" per istruzioni.

Creare un trust per la parte che si basa importando i metadati della federazione

È possibile importare i valori per ciascun trust di parte che si basa accedendo ai metadati SAML per ciascun nodo di amministrazione.

Fasi

1. In Gestione server Windows, selezionare **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, selezionare **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e selezionare **Avvia**.
4. Selezionare **Importa dati relativi alla parte che si basa pubblicati online o su una rete locale**.
5. In **Federation metadata address (nome host o URL)**, digitare la posizione dei metadati SAML per questo nodo di amministrazione:

   `https://Admin_Node_FQDN/api/saml-metadata`

   Per *`Admin_Node_FQDN`*, Immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

6. Completare la procedura guidata Trust Party, salvare il trust della parte che si basa e chiudere la procedura guidata.

   Quando si immette il nome visualizzato, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, `SG-DC1-ADM1`.

7. Aggiungere una regola di richiesta di rimborso:
   a. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
   b. Selezionare **Aggiungi regola**:
   c. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
   d. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

      Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

   e. Per l'archivio attributi, selezionare **Active Directory**.
   f. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
   g. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
   h. Selezionare **fine**, quindi **OK**.
8. Verificare che i metadati siano stati importati correttamente.
   a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
   b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

      Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.

9. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
10. Una volta completata l'operazione, tornare a StorageGRID e verificare tutti i trust delle parti di base per verificare che siano configurati correttamente. Vedere "Utilizzare la modalità Sandbox" per istruzioni.

Creare manualmente un trust per la parte che si basa

Se si sceglie di non importare i dati per i trust della parte di base, è possibile inserire i valori manualmente.

Fasi

1. In Gestione server Windows, selezionare **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, selezionare **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e selezionare **Avvia**.
4. Selezionare **inserire manualmente i dati relativi alla parte di base** e selezionare **Avanti**.
5. Completare la procedura guidata Trust Party:
   a. Immettere un nome visualizzato per questo nodo di amministrazione.

      Per coerenza, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, `SG-DC1-ADM1`.

   b. Saltare il passaggio per configurare un certificato di crittografia token opzionale.
   c. Nella pagina Configure URL (Configura URL), selezionare la casella di controllo **Enable support for**

the SAML 2.0 WebSSO Protocol (attiva supporto per il protocollo SAML WebSSO).

d. Digitare l'URL dell'endpoint del servizio SAML per il nodo di amministrazione:

`https://Admin_Node_FQDN/api/saml-response`

Per *Admin_Node_FQDN*, Immettere il nome di dominio completo per il nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

e. Nella pagina Configure Identifier (Configura identificatori), specificare l'identificativo della parte di base per lo stesso nodo di amministrazione:

Admin_Node_Identifier

Per *Admin_Node_Identifier*, Immettere l'identificativo della parte di base per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1`.

f. Rivedere le impostazioni, salvare l'attendibilità della parte che si basa e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Edit Claim Issuance Policy (Modifica policy di emissione richieste di

> Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).

6. Per avviare la procedura guidata Claim Rule, selezionare **Add Rule**:
   a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
   b. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

      Ad esempio, **objectGUID a ID nome** o **UPN a ID nome**.

   c. Per l'archivio attributi, selezionare **Active Directory**.
   d. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
   e. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
   f. Selezionare **fine**, quindi **OK**.
7. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
   a. Selezionare **Add SAML** (Aggiungi SAML).
   b. Selezionare **Endpoint Type** > **SAML Logout**.
   c. Selezionare **binding** > **Redirect**.
   d. Nel campo **Trusted URL**, immettere l'URL utilizzato per la disconnessione singola (SLO) da questo nodo di amministrazione:

      `https://Admin_Node_FQDN/api/saml-logout`

Per *Admin_Node_FQDN*, Immettere il nome di dominio completo del nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per il trust della parte che si basa:
   a. Aggiungere il certificato personalizzato:
      - Se si dispone del certificato di gestione personalizzato caricato su StorageGRID, selezionare il certificato.
      - Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, quindi passare a. `/var/local/mgmt-api` Della directory Admin Node e aggiungere `custom-server.crt` file di certificato.

        Nota: utilizzando il certificato predefinito del nodo di amministrazione (`server.crt`) non è consigliato. Se il nodo Admin non riesce, il certificato predefinito viene rigenerato quando si ripristina il nodo ed è necessario aggiornare il trust della parte che si basa.

   b. Selezionare **Applica** e **OK**.

      Le proprietà della parte di base vengono salvate e chiuse.

10. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
11. Una volta completata l'operazione, tornare a StorageGRID e verificare tutti i trust delle parti di base per verificare che siano configurati correttamente. Vedere "USA la modalità sandbox" per istruzioni.

Creare applicazioni aziendali in Azure ad

Azure ad consente di creare un'applicazione aziendale per ciascun nodo di amministrazione del sistema.

Prima di iniziare

- È stata avviata la configurazione del single sign-on per StorageGRID ed è stato selezionato **Azure** come tipo di SSO.
- **La modalità Sandbox** è selezionata nella pagina Single Sign-on di Grid Manager. Vedere "USA la modalità sandbox".
- Si dispone del nome dell'applicazione aziendale* per ciascun nodo di amministrazione nel sistema. È possibile copiare questi valori dalla tabella Dettagli nodo amministratore nella pagina accesso singolo StorageGRID.

> È necessario creare un'applicazione aziendale per ciascun nodo amministratore nel sistema StorageGRID. La disponibilità di un'applicazione aziendale per ciascun nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di applicazioni aziendali in Azure Active Directory.
- Hai un account Azure con un abbonamento attivo.
- Nell'account Azure hai uno dei seguenti ruoli: Amministratore globale, amministratore dell'applicazione cloud, amministratore dell'applicazione o proprietario del service principal.

Accedere ad Azure ad

Fasi

1. Accedere a. "Portale Azure".
2. Selezionare "Azure Active Directory".
3. Selezionare "Applicazioni aziendali".

Creare applicazioni aziendali e salvare la configurazione SSO di StorageGRID

Per salvare la configurazione SSO per Azure in StorageGRID, è necessario utilizzare Azure per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copiare gli URL dei metadati della federazione da Azure e incollarli nei corrispondenti campi **URL metadati federazione** nella pagina di accesso singolo di StorageGRID.

Fasi

1. Ripetere i passaggi seguenti per ciascun nodo di amministrazione.
   a. Nel riquadro Azure Enterprise Applications (applicazioni aziendali Azure), selezionare **New application** (Nuova applicazione).
   b. Selezionare **Crea la tua applicazione**.
   c. Per il nome, inserire il nome dell'applicazione aziendale copiato dalla tabella dei dettagli del nodo amministrativo nella pagina accesso singolo StorageGRID.
   d. Lasciare selezionato il pulsante di opzione **integra qualsiasi altra applicazione che non trovi nella galleria (non-gallery)**.
   e. Selezionare **Crea**.
   f. Selezionare il collegamento **Get Started** nel campo **2. Impostare la casella Single Sign on** (accesso singolo) oppure selezionare il collegamento **Single Sign-on** (accesso singolo) nel margine sinistro.
   g. Selezionare la casella **SAML**.
   h. Copiare l'URL * dei metadati dell'App Federation, disponibile nella sezione **fase 3 certificato di firma SAML**.
   i. Accedere alla pagina Single Sign-on di StorageGRID e incollare l'URL nel campo **Federation metadata URL** che corrisponde al **nome dell'applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati della federazione per ciascun nodo amministratore e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, selezionare **Salva** nella pagina accesso singolo StorageGRID.

Scarica i metadati SAML per ogni nodo di amministrazione

Una volta salvata la configurazione SSO, è possibile scaricare un file di metadati SAML per ciascun nodo amministratore nel sistema StorageGRID.

Fasi

1. Ripetere questi passaggi per ciascun nodo di amministrazione.
   a. Accedere a StorageGRID dal nodo di amministrazione.
   b. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   c. Selezionare il pulsante per scaricare i metadati SAML per il nodo di amministrazione.
   d. Salvare il file che verrà caricato in Azure ad.

Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ciascun nodo amministrativo StorageGRID, eseguire la seguente procedura in Azure ad:

Fasi

1. Tornare al portale Azure.
2. Ripetere questi passaggi per ogni applicazione aziendale:

   > Potrebbe essere necessario aggiornare la pagina Enterprise Applications (applicazioni aziendali) per visualizzare le applicazioni aggiunte in precedenza nell'elenco.

   a. Accedere alla pagina Proprietà dell'applicazione aziendale.
   b. Impostare **assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).
   c. Vai alla pagina Single Sign-on.
   d. Completare la configurazione SAML.
   e. Selezionare il pulsante **carica file di metadati** e selezionare il file di metadati SAML scaricato per il nodo di amministrazione corrispondente.
   f. Una volta caricato il file, selezionare **Salva**, quindi selezionare **X** per chiudere il riquadro. Viene visualizzata nuovamente la pagina Set up Single Sign-on with SAML (Configura Single Sign-on con SAML).
3. Seguire la procedura descritta in "USA la modalità sandbox" per testare ogni applicazione.

Creare connessioni SP (service provider) in PingFederate

Utilizzare PingFederate per creare una connessione SP (Service Provider) per ciascun nodo amministratore del sistema. Per accelerare il processo, importare i metadati SAML da StorageGRID.

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **Ping Federate** come tipo di SSO.
- **La modalità Sandbox** è selezionata nella pagina Single Sign-on di Grid Manager. Vedere "USA la modalità sandbox".
- Si dispone dell'ID di connessione **SP** per ciascun nodo amministratore del sistema. Questi valori sono disponibili nella tabella dei dettagli dei nodi di amministrazione nella pagina accesso singolo StorageGRID.
- Sono stati scaricati i **metadati SAML** per ciascun nodo di amministrazione nel sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Hai il "Guida di riferimento per l'amministratore" Per PingFederate Server. La documentazione di PingFederate fornisce istruzioni dettagliate e spiegazioni dettagliate.
- Hai il "Autorizzazione amministratore" Per PingFederate Server.

A proposito di questa attività

Queste istruzioni riepilogano come configurare PingFederate Server versione 10.3 come provider SSO per StorageGRID. Se si utilizza un'altra versione di PingFederate, potrebbe essere necessario adattare queste istruzioni. Per istruzioni dettagliate sulla release, consultare la documentazione di PingFederate Server.

Completare i prerequisiti in PingFederate

Prima di poter creare le connessioni SP da utilizzare per StorageGRID, è necessario completare le attività dei prerequisiti in PingFederate. Quando si configurano le connessioni SP, verranno utilizzate le informazioni di questi prerequisiti.

Creare un archivio di dati

Se non lo si è già fatto, creare un archivio dati per connettere PingFederate al server LDAP di ad FS. Utilizzare i valori utilizzati quando "configurazione della federazione delle identità" In StorageGRID.

- **Tipo**: Directory (LDAP)
- **LDAP Type**: Active Directory
- **Binary Attribute Name** (Nome attributo binario): Inserire **objectGUID** nella scheda LDAP Binary Attributes (attributi binari LDAP) esattamente come mostrato.

Crea validatore credenziale password

Se non l'hai ancora fatto, crea una convalida delle credenziali per la password.

- **Type**: LDAP Username Password Credential Validator
- **Data store**: Selezionare il data store creato.
- **Base di ricerca**: Immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca**: SAMAccountName={nomeutente}
- **Scopo**: Sottostruttura

Crea istanza dell'adattatore IdP

Se non lo si è già fatto, creare un'istanza dell'adattatore IdP.

Fasi

1. Accedere a **Authentication** > **Integration** > **IdP Adapter**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda tipo, selezionare **HTML Form IdP Adapter**.
4. Nella scheda IdP Adapter, selezionare **Aggiungi una nuova riga a "Credential Validators"**.
5. Selezionare validatore delle credenziali per la password creato.
6. Nella scheda attributi adattatore, selezionare l'attributo **nome utente** per **pseudonimo**.
7. Selezionare **Salva**.

Creare o importare un certificato di firma

Se non lo si è già fatto, creare o importare il certificato di firma.

Fasi

1. Accedere a **sicurezza** > **chiavi e certificati di firma e decrittografia**.
2. Creare o importare il certificato di firma.

Creare una connessione SP in PingFederate

Quando si crea una connessione SP in PingFederate, si importano i metadati SAML scaricati da StorageGRID per il nodo di amministrazione. Il file di metadati contiene molti dei valori specifici necessari.

È necessario creare una connessione SP per ciascun nodo amministratore nel sistema StorageGRID, in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Seguire queste istruzioni per creare la prima connessione SP. Quindi, passare a. Creare ulteriori connessioni SP per creare eventuali connessioni aggiuntive necessarie.

Scegliere il tipo di connessione SP

Fasi

1. Accedere a **applicazioni** > **integrazione** > **connessioni SP**.
2. Selezionare **Crea connessione**.
3. Selezionare **non utilizzare un modello per questa connessione**.
4. Selezionare **browser SSO Profiles** (profili SSO browser) e **SAML 2.0** come protocollo.

Importare metadati SP

Fasi

1. Nella scheda Importa metadati, selezionare **file**.
2. Scegliere il file di metadati SAML scaricato dalla pagina di accesso singolo StorageGRID per il nodo di amministrazione.
3. Esaminare il riepilogo dei metadati e le informazioni fornite nella scheda General Info (informazioni generali).

   L'ID dell'entità del partner e il nome della connessione sono impostati sull'ID della connessione StorageGRID SP. (Ad esempio, 10.96.105.200-DC1-ADM1-105-200). L'URL di base è l'IP del nodo di amministrazione StorageGRID.

4. Selezionare **Avanti**.

Configurare IdP browser SSO

Fasi

1. Dalla scheda SSO del browser, selezionare **Configure browser SSO** (Configura SSO browser).
2. Nella scheda SAML profiles (profili SAML), selezionare le opzioni **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Assertion Lifetime (durata asserzione), non apportare modifiche.
5. Nella scheda Assertion Creation (creazione asserzione), selezionare **Configure Assertion Creation (Configura creazione asserzione)**.
   a. Nella scheda Identity Mapping (mappatura identità), selezionare **Standard**.
   b. Nella scheda Contratto attributo, utilizzare **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere `urn:oid`, che non viene utilizzato.

Istanza dell'adattatore di mappatura

Fasi

1. Nella scheda Authentication Source Mapping (mappatura origine autenticazione), selezionare **Map New Adapter Instance** (mappatura nuova istanza adattatore).
2. Nella scheda Adapter instance (istanza adattatore), selezionare istanza dell'adattatore creato.
3. Nella scheda Mapping Method (metodo di mappatura), selezionare **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda origine attributo e Ricerca utente, selezionare **Aggiungi origine attributo**.
5. Nella scheda Data Store (Archivio dati), fornire una descrizione e selezionare archivio di dati hai aggiunto.
6. Nella scheda LDAP Directory Search (Ricerca directory LDAP):
   - Inserire il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
   - Per l'ambito di ricerca, selezionare **sottostruttura**.
   - Per la classe di oggetti Root, cercare e aggiungere uno dei seguenti attributi: **ObjectGUID** o **userPrincipalName**.
7. Nella scheda LDAP Binary Attribute Encoding Types (tipi di codifica attributi binari LDAP), selezionare **Base64** come attributo **objectGUID**.
8. Nella scheda filtro LDAP, immettere **sAMAccountName={nome utente}**.
9. Nella scheda adempimento contratto attributo, selezionare **LDAP (attributo)** dall'elenco a discesa origine e selezionare **objectGUID** o **userPrincipalName** dall'elenco a discesa valore.
10. Esaminare e salvare l'origine dell'attributo.
11. Nella scheda origine attributo failsaved, selezionare **Interrompi transazione SSO**.
12. Esaminare il riepilogo e selezionare **fine**.
13. Selezionare **fine**.

Configurare le impostazioni del protocollo

Fasi

1. Nella scheda **connessione SP** > **SSO browser** > **Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL servizio clienti asserzione, accettare i valori predefiniti, che sono stati importati dai metadati SAML di StorageGRID (**POST** per il binding e. `/api/saml-response` Per URL endpoint).
3. Nella scheda URL servizio SLO, accettare i valori predefiniti, importati dai metadati SAML di StorageGRID (**REDIRECT** per l'associazione e. `/api/saml-logout` Per URL endpoint.
4. Nella scheda Allowable SAML Bindings (Binding SAML autorizzati), deselezionare **ARTEFATTO** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Firma Policy, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste Authn** e **Firma sempre asserzione**.
6. Nella scheda Encryption Policy (Criteri di crittografia), selezionare **None** (Nessuno).
7. Esaminare il riepilogo e selezionare **Done** (fine) per salvare le impostazioni del protocollo.
8. Esaminare il riepilogo e selezionare **fine** per salvare le impostazioni SSO del browser.

Configurare le credenziali

Fasi

1. Dalla scheda connessione SP, selezionare **credenziali**.
2. Dalla scheda credenziali, selezionare **Configura credenziali**.
3. Selezionare firma del certificato creato o importato.
4. Selezionare **Avanti** per accedere a **Gestisci impostazioni di verifica della firma**.
   a. Nella scheda Trust Model (modello di attendibilità), selezionare **Unancored** (non ancorato).
   b. Nella scheda certificato di verifica della firma, esaminare le informazioni del certificato di firma importate dai metadati SAML di StorageGRID.
5. Esaminare le schermate di riepilogo e selezionare **Save** (Salva) per salvare la connessione SP.

Creare ulteriori connessioni SP

È possibile copiare la prima connessione SP per creare le connessioni SP necessarie per ciascun nodo di amministrazione nella griglia. Vengono caricati nuovi metadati per ogni copia.

> Le connessioni SP per diversi nodi di amministrazione utilizzano impostazioni identiche, ad eccezione di ID entità del partner, URL di base, ID connessione, nome connessione, verifica firma, E SLO Response URL.

Fasi

1. Selezionare **Action** > **Copy** per creare una copia della connessione SP iniziale per ogni nodo Admin aggiuntivo.
2. Immettere l'ID connessione e il nome connessione per la copia, quindi selezionare **Salva**.
3. Scegliere il file di metadati corrispondente al nodo di amministrazione:
   a. Selezionare **azione** > **Aggiorna con metadati**.
   b. Selezionare **Scegli file** e caricare i metadati.
   c. Selezionare **Avanti**.
   d. Selezionare **Salva**.
4. Risolvere l'errore dovuto all'attributo inutilizzato:
   a. Selezionare la nuova connessione.
   b. Selezionare **Configure browser SSO > Configure Assertion Creation > Attribute Contract**.
   c. Elimina la voce per **urn:oid**.
   d. Selezionare **Salva**.

Disattiva single sign-on

È possibile disattivare SSO (Single Sign-on) se non si desidera più utilizzare questa funzionalità. È necessario disattivare il Single Sign-on prima di poter disattivare la federazione delle identità.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.

   Viene visualizzata la pagina Single Sign-on (accesso singolo).

2. Selezionare l'opzione **Disabled**.
3. Selezionare **Salva**.

   Viene visualizzato un messaggio di avviso che indica che gli utenti locali potranno accedere.

4. Selezionare **OK**.

   Al successivo accesso a StorageGRID, viene visualizzata la pagina di accesso a StorageGRID e sono necessari il nome utente e la password di un utente StorageGRID locale o federato.

Disattivare e riabilitare temporaneamente il Single Sign-on per un nodo di amministrazione

Se il sistema SSO (Single Sign-on) non funziona, potrebbe non essere possibile accedere a Grid Manager. In questo caso, è possibile disattivare e riabilitare temporaneamente SSO per un nodo di amministrazione. Per disattivare e riabilitare SSO, è necessario accedere alla shell dei comandi del nodo.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai il `Passwords.txt` file.
- Si conosce la password dell'utente root locale.

A proposito di questa attività

Dopo aver disattivato SSO per un nodo di amministrazione, è possibile accedere a Grid Manager come utente root locale. Per proteggere il sistema StorageGRID, è necessario utilizzare la shell dei comandi del nodo per riabilitare SSO sul nodo di amministrazione non appena si effettua la disconnessione.

> La disattivazione di SSO per un nodo di amministrazione non influisce sulle impostazioni SSO per qualsiasi altro nodo di amministrazione nella griglia. La casella di controllo **Enable SSO** (attiva SSO) nella pagina Single Sign-on (accesso singolo) di Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute, a meno che non vengano aggiornate.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il seguente comando:`disable-saml`

   Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

3. Confermare che si desidera disattivare SSO.

   Un messaggio indica che l'accesso singolo è disattivato sul nodo.

4. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.

   Viene visualizzata la pagina di accesso di Grid Manager perché SSO è stato disattivato.

5. Accedere con il nome utente root e la password dell'utente root locale.
6. Se SSO è stato disattivato temporaneamente perché era necessario correggere la configurazione SSO:
   a. Selezionare **CONFIGURATION** > **Access control** > **Single Sign-on**.
   b. Modificare le impostazioni SSO non corrette o non aggiornate.
   c. Selezionare **Salva**.

      Selezionando **Save** (Salva) dalla pagina Single Sign-on (accesso singolo), l'SSO viene riattivato automaticamente per l'intera griglia.

7. Se l'SSO è stato disattivato temporaneamente perché era necessario accedere a Grid Manager per un altro motivo:

   a. Eseguire qualsiasi attività o attività da eseguire.
   b. Selezionare **Disconnetti** e chiudere Grid Manager.
   c. Riabilitare SSO sul nodo di amministrazione. È possibile eseguire una delle seguenti operazioni:

      - Eseguire il seguente comando: `enable-saml`

        Un messaggio indica che il comando si applica solo a questo nodo di amministrazione.

      Confermare che si desidera attivare SSO.

   Un messaggio indica che il Single Sign-on è attivato sul nodo.

      - Riavviare il nodo Grid: `reboot`

8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.
9. Verificare che venga visualizzata la pagina di accesso a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

USA la federazione di grid

Che cos'è la federazione di griglie?

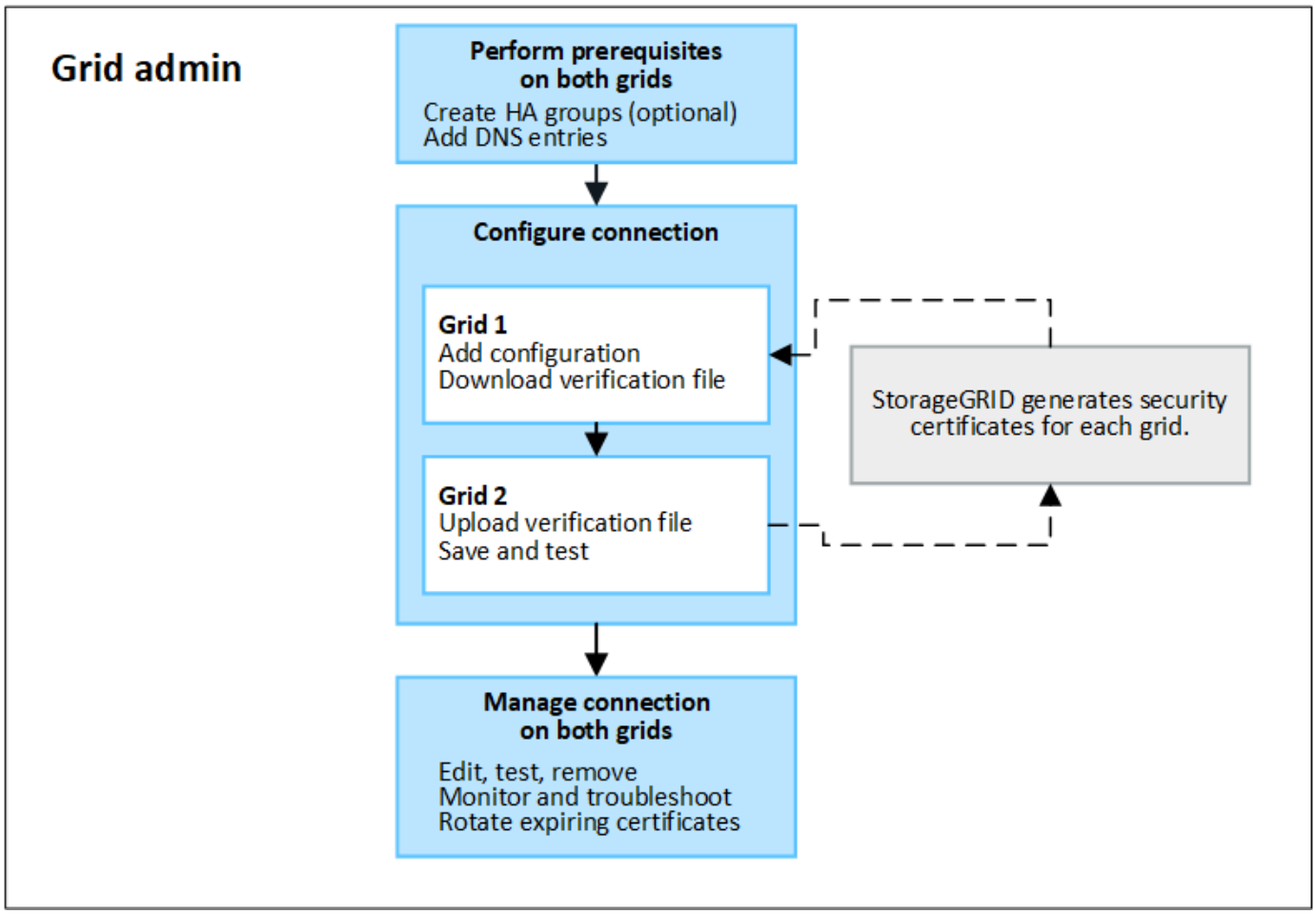
È possibile utilizzare la federazione di grid per clonare i tenant e replicare i loro oggetti tra due sistemi StorageGRID per il disaster recovery.

Che cos'è una connessione a federazione di griglie?

Una connessione a federazione di griglie è una connessione bidirezionale, affidabile e sicura tra i nodi amministratore e gateway in due sistemi StorageGRID.

Workflow per la federazione di grid

Il diagramma del flusso di lavoro riassume i passaggi per la configurazione di una connessione a federazione di griglie tra due griglie.



Considerazioni e requisiti per le connessioni a federazione di griglie

- Entrambe le griglie utilizzate per la federazione delle griglie devono eseguire StorageGRID 11,7 o versioni successive.
- Una griglia può avere una o più connessioni di federazione di griglia ad altre griglie. Ogni connessione a federazione di griglie è indipendente da qualsiasi altra connessione. Ad esempio, se la griglia 1 ha una connessione con la griglia 2 e una seconda connessione con la griglia 3, non esiste alcuna connessione implicita tra la griglia 2 e la griglia 3.
- Le connessioni a federazione di griglie sono bidirezionali. Una volta stabilita la connessione, è possibile monitorare e gestire la connessione da entrambe le griglie.
- Prima di poter utilizzare, deve esistere almeno una connessione di federazione di griglie "clone dell'account" oppure "replica cross-grid".

Requisiti di rete e indirizzo IP

- Le connessioni a federazione di griglie possono avvenire su Grid Network, Admin Network o Client Network.
- Una connessione a federazione di griglie collega una griglia a un'altra griglia. La configurazione per ogni griglia specifica un endpoint della federazione di griglia sull'altro griglia che consiste in nodi di amministrazione, nodi gateway o entrambi.
- La procedura consigliata è quella di connettersi "Gruppi ad alta disponibilità (ha)" Dei nodi Gateway e Admin su ogni griglia. L'utilizzo di gruppi ha consente di garantire che le connessioni a federazione di griglie rimangano online se i nodi non sono più disponibili. Se l'interfaccia attiva in uno dei gruppi ha non riesce, la connessione può utilizzare un'interfaccia di backup.
- Si sconsiglia di creare una connessione a federazione di griglie che utilizzi l'indirizzo IP di un singolo nodo di amministrazione o di un nodo gateway. Se il nodo diventa non disponibile, anche la connessione a federazione di griglie non sarà disponibile.
- "Replica cross-grid" Of Objects (numero di oggetti) richiede che i nodi di storage su ogni griglia siano in grado di accedere ai nodi Admin e Gateway configurati sull'altra griglia. Per ogni griglia, verificare che tutti i nodi di storage dispongano di un percorso a elevata larghezza di banda verso i nodi Admin o Gateway utilizzati per la connessione.

Utilizzare FQDN per bilanciare il carico della connessione

Per un ambiente di produzione, utilizzare FQDN (Fully Qualified Domain Name) per identificare ogni griglia della connessione. Quindi, creare le voci DNS appropriate, come indicato di seguito:

- L'FQDN per la griglia 1 è mappato a uno o più indirizzi IP virtuali (VIP) per i gruppi ha nella griglia 1 o all'indirizzo IP di uno o più nodi Admin o Gateway nella griglia 1.
- L'FQDN per la griglia 2 è mappato a uno o più indirizzi VIP per la griglia 2 o all'indirizzo IP di uno o più nodi Admin o Gateway nella griglia 2.

Quando si utilizzano più voci DNS, le richieste per utilizzare la connessione vengono bilanciate dal carico, come segue:

- Le voci DNS associate agli indirizzi VIP di più gruppi ha vengono bilanciate in base al carico tra i nodi attivi nei gruppi ha.
- Le voci DNS associate agli indirizzi IP di più nodi Admin o Gateway vengono bilanciate in base al carico tra i nodi mappati.

Requisiti delle porte

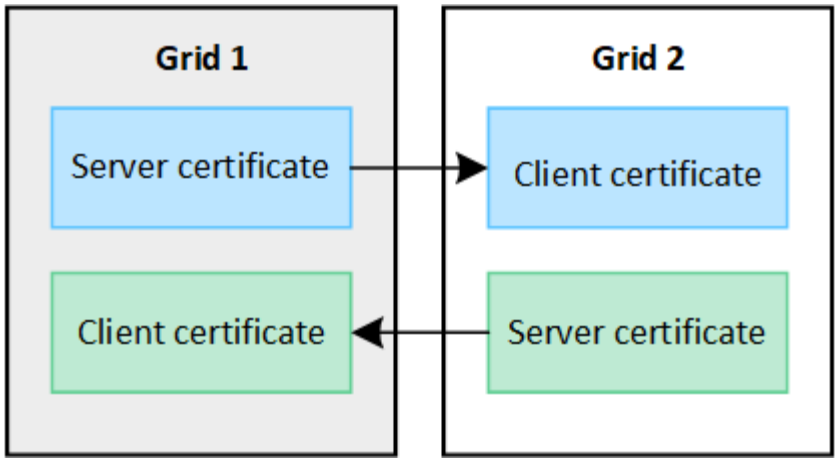
Quando si crea una connessione a federazione di griglie, è possibile specificare qualsiasi numero di porta inutilizzato compreso tra 23000 e 23999. Entrambe le griglie di questa connessione utilizzeranno la stessa porta.

È necessario assicurarsi che nessun nodo di una delle griglie utilizzi questa porta per altre connessioni.

Requisiti del certificato

Quando si configura una connessione a federazione di griglie, StorageGRID genera automaticamente quattro certificati SSL:

- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 1 alla griglia 2
- Certificati server e client per autenticare e crittografare le informazioni inviate dalla griglia 2 alla griglia 1



Per impostazione predefinita, i certificati sono validi per 730 giorni (2 anni). Quando questi certificati sono prossimi alla data di scadenza, L'avviso **scadenza del certificato di federazione griglia** ricorda di ruotare i certificati, operazione che è possibile eseguire utilizzando Grid Manager.

> Se i certificati a una delle due estremità della connessione scadono, la connessione non funziona più. La replica dei dati sarà in sospeso fino all'aggiornamento dei certificati.

Scopri di più

- "Creare connessioni di federazione di griglie"
- "Gestire le connessioni a federazione di griglie"
- "Risolvere i problemi relativi agli errori di federazione della griglia"

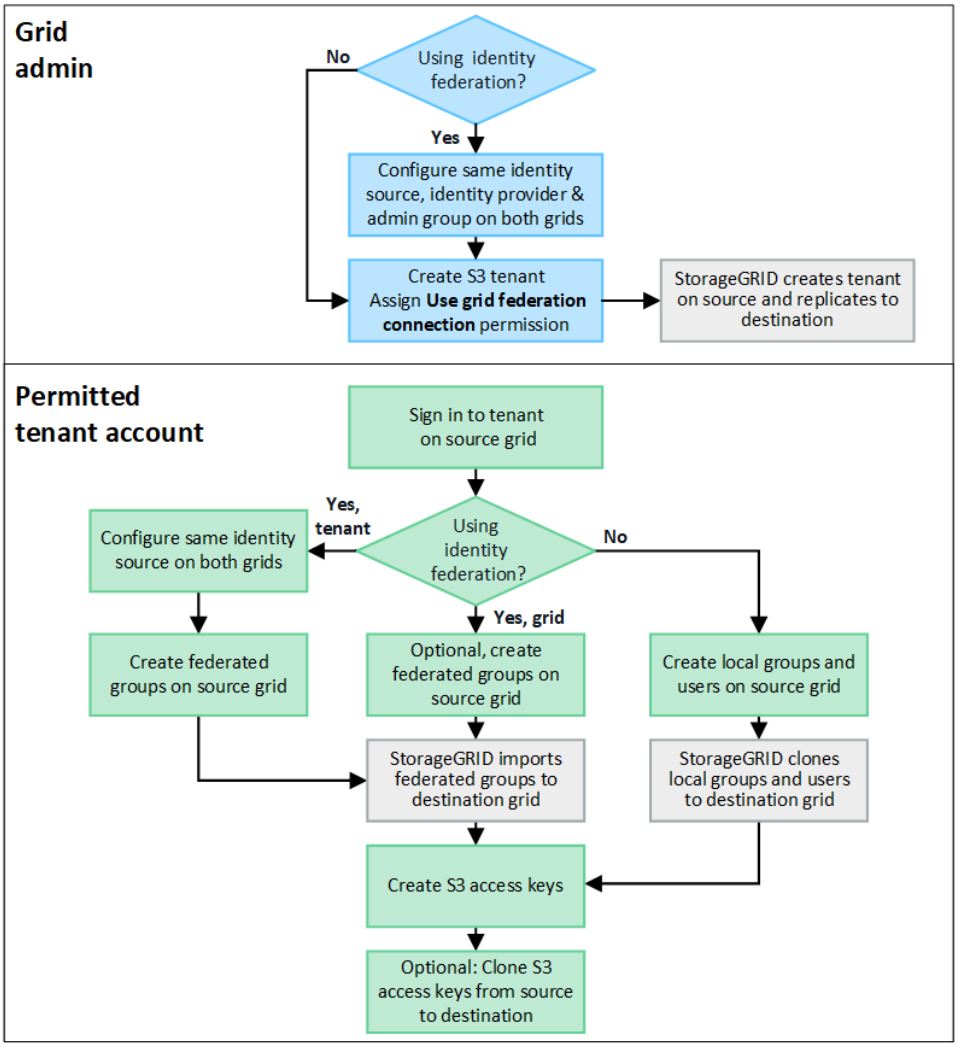
Che cos'è il clone dell'account?

Il clone dell'account è la replica automatica di un account tenant, di gruppi tenant, di utenti tenant e, facoltativamente, S3 access key tra i sistemi StorageGRID in un "connessione a federazione di griglie".

Il clone dell'account è necessario per "replica cross-grid". La clonazione delle informazioni sugli account da un sistema StorageGRID di origine a un sistema StorageGRID di destinazione garantisce che gli utenti e i gruppi tenant possano accedere ai bucket e agli oggetti corrispondenti su entrambe le griglie.

Workflow per il clone dell'account

Il diagramma del flusso di lavoro mostra i passaggi che gli amministratori della griglia e i tenant autorizzati eseguiranno per impostare il clone dell'account. Questi passaggi vengono eseguiti dopo "la connessione a federazione di griglie è configurata".



Workflow di amministrazione della griglia

Le operazioni eseguite dagli amministratori della griglia dipendono dal fatto che i sistemi StorageGRID in siano o meno presenti in "connessione a federazione di griglie" Utilizzare SSO (Single Sign-on) o federazione di identità.

Configura SSO per il clone dell'account (opzionale)

Se uno dei sistemi StorageGRID nella connessione a federazione di griglie utilizza SSO, entrambe le griglie devono utilizzare SSO. Prima di creare gli account tenant per la federazione di griglie, gli amministratori di griglie per le griglie di origine e di destinazione del tenant devono eseguire questi passaggi.

Fasi

1. Configurare la stessa origine di identità per entrambe le griglie. Vedere "USA la federazione delle identità".
2. Configurare lo stesso provider di identità SSO (IdP) per entrambe le griglie. Vedere "Configurare il single sign-on".
3. "Creare lo stesso gruppo di amministratori" su entrambe le griglie importando lo stesso gruppo federated.

   Quando si crea il tenant, si seleziona questo gruppo per disporre dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione.

Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non viene replicato nella destinazione.

Configura federazione di identità a livello di griglia per il clone dell'account (opzionale)

Se uno dei sistemi StorageGRID utilizza la federazione delle identità senza SSO, entrambe le griglie devono utilizzare la federazione delle identità. Prima di creare gli account tenant per la federazione di griglie, gli amministratori di griglie per le griglie di origine e di destinazione del tenant devono eseguire questi passaggi.

Fasi

1. Configurare la stessa origine di identità per entrambe le griglie. Vedere "USA la federazione delle identità".
2. Facoltativamente, se un gruppo federated disporrà dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione, "creare lo stesso gruppo di amministratori" su entrambe le griglie importando lo stesso gruppo federated.

   Se si assegna l'autorizzazione di accesso root a un gruppo federated che non esiste su entrambe le griglie, il tenant non viene replicato nella griglia di destinazione.

3. Se non si desidera che un gruppo federated disponga dell'autorizzazione di accesso root iniziale per entrambi gli account, specificare una password per l'utente root locale.

Creare un account tenant S3 consentito

Dopo la configurazione opzionale di SSO o federazione di identità, un amministratore di grid esegue questi passaggi per determinare quali tenant possono replicare gli oggetti bucket in altri sistemi StorageGRID.

Fasi

1. Determinare quale griglia si desidera essere la griglia di origine del tenant per le operazioni di cloni degli account.

   La griglia in cui viene creato il tenant è nota come *griglia di origine* del tenant. La griglia in cui viene replicato il tenant è nota come *griglia di destinazione* del tenant.

2. In tale griglia, creare un nuovo account tenant S3 o modificare un account esistente.
3. Assegnare l'autorizzazione **Usa connessione federazione griglia**.
4. Se l'account tenant gestirà i propri utenti federati, assegnare l'autorizzazione **use own Identity source**.

   Se questa autorizzazione viene assegnata, gli account tenant di origine e di destinazione devono configurare la stessa origine identità prima di creare gruppi federati. I gruppi federati aggiunti al tenant di origine non possono essere clonati nel tenant di destinazione a meno che entrambe le griglie non utilizzino la stessa origine di identità.

5. Selezionare una connessione a federazione di griglie specifica.
6. Salvare il tenant nuovo o modificato.

   Quando viene salvato un nuovo tenant con l'autorizzazione **use grid Federation Connection**, StorageGRID crea automaticamente una replica del tenant sull'altro grid, come segue:

   - Entrambi gli account tenant hanno lo stesso ID account, il nome, la quota di storage e le stesse autorizzazioni assegnate.

- Se è stato selezionato un gruppo federated per disporre dell'autorizzazione di accesso root per il tenant, tale gruppo viene clonato nel tenant di destinazione.
- Se si seleziona un utente locale per disporre dell'autorizzazione di accesso root per il tenant, tale utente viene clonato nel tenant di destinazione. Tuttavia, la password per quell'utente non viene clonata.

Per ulteriori informazioni, vedere "Gestire i tenant autorizzati per la federazione di grid".

Flusso di lavoro account tenant consentito

Dopo che un tenant con l'autorizzazione **Usa connessione federazione griglia** è stato replicato nella griglia di destinazione, gli account tenant autorizzati possono eseguire queste operazioni per clonare gruppi tenant, utenti e chiavi di accesso S3.

Fasi

1. Accedere all'account tenant sulla griglia di origine del tenant.
2. Se consentito, configurare la federazione di identificazione sugli account tenant di origine e di destinazione.
3. Creare gruppi e utenti nel tenant di origine.

   Quando vengono creati nuovi gruppi o utenti nel tenant di origine, StorageGRID li clonerà automaticamente nel tenant di destinazione, ma non si verificherà alcun cloning dalla destinazione all'origine.
4. Creare chiavi di accesso S3.
5. Facoltativamente, clonare le chiavi di accesso S3 dal tenant di origine al tenant di destinazione.

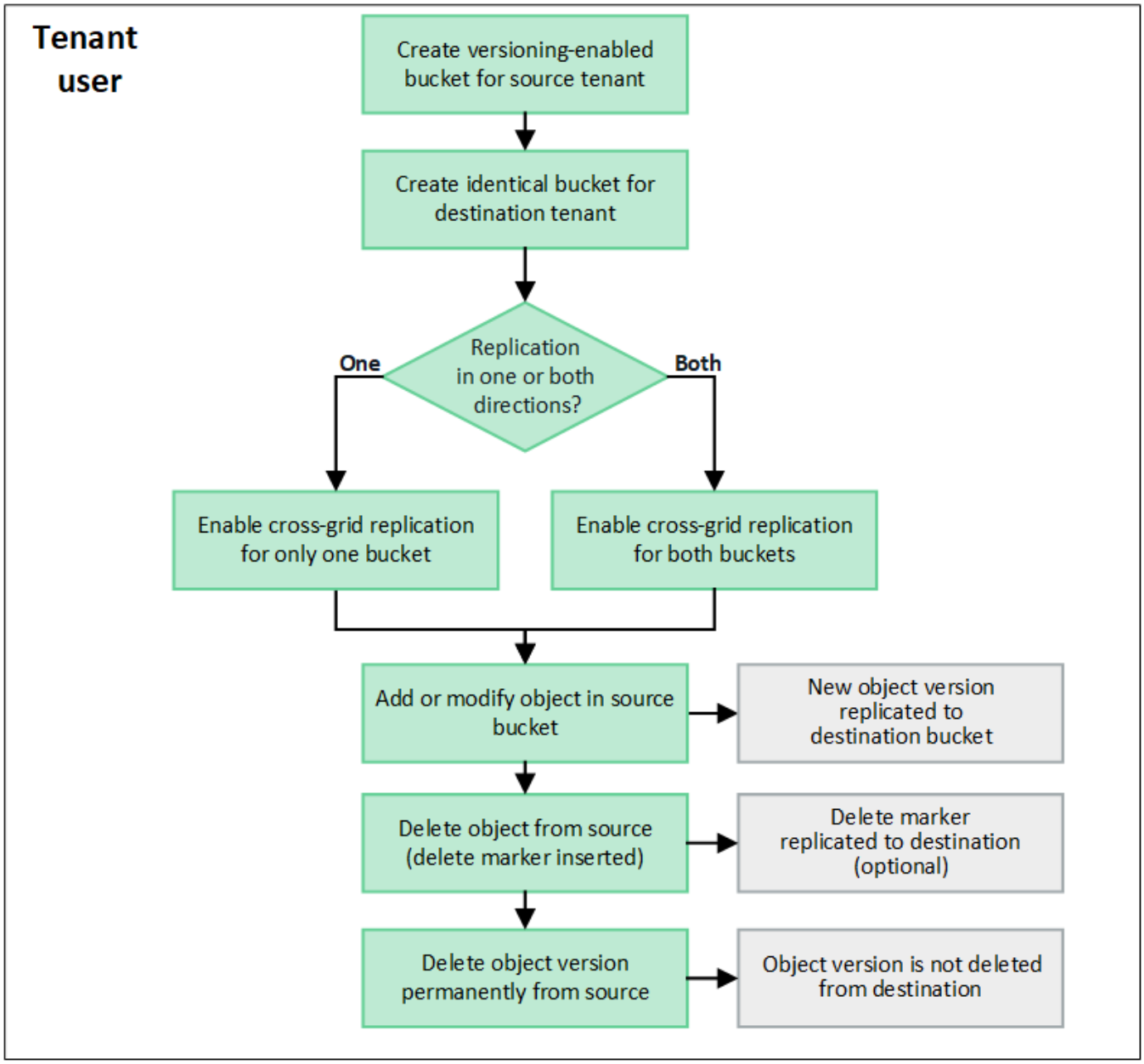
Per ulteriori informazioni sul flusso di lavoro dell'account tenant consentito e su come clonare gruppi, utenti e chiavi di accesso S3, vedere "Clonare utenti e gruppi tenant" e. "Clonare le chiavi di accesso S3 utilizzando l'API".

Che cos'è la replica cross-grid?

La replica cross-grid è la replica automatica degli oggetti tra bucket S3 selezionati in due sistemi StorageGRID collegati in un "connessione a federazione di griglie". "Clone dell'account" è necessario per la replica cross-grid.

Workflow per la replica cross-grid

Il diagramma del flusso di lavoro riassume i passaggi per la configurazione della replica cross-grid tra bucket su due griglie.



Requisiti per la replica cross-grid

Se un account tenant dispone dell'autorizzazione **Usa connessione federazione griglia** per utilizzare uno o più account "connessioni a federazione di griglie", Un utente tenant con autorizzazione di accesso Root può creare bucket identici negli account tenant corrispondenti su ogni griglia. Questi bucket:

- Deve avere lo stesso nome ma possono avere regioni diverse
- È necessario attivare la versione
- È necessario che S3 Object Lock sia disattivato
- Deve essere vuoto

Una volta creati entrambi i bucket, è possibile configurare la replica cross-grid per uno o entrambi i bucket.

Scopri di più

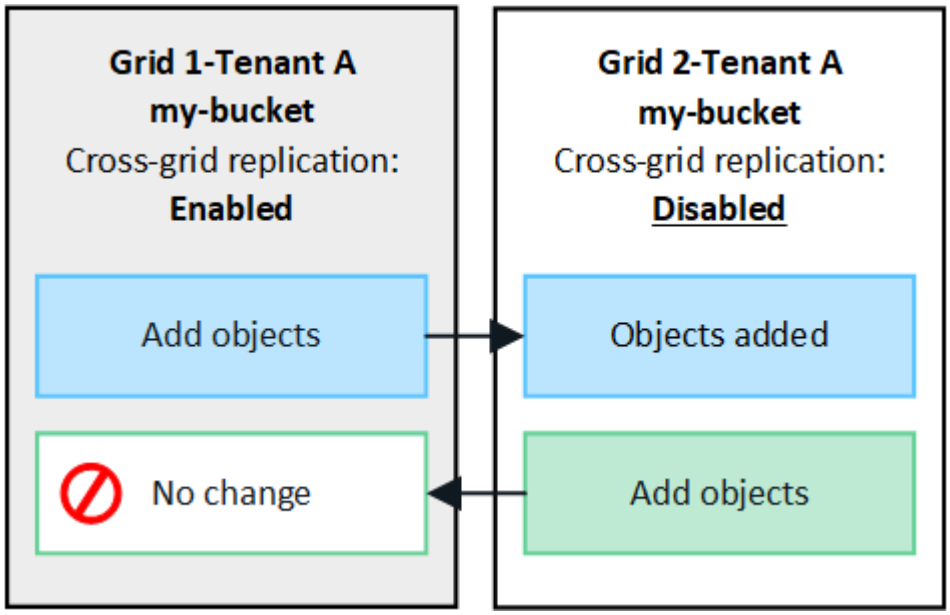
"Gestire la replica cross-grid"

Come funziona la replica cross-grid

È possibile configurare la replica cross-grid in modo che avvenga in una direzione o in entrambe le direzioni.

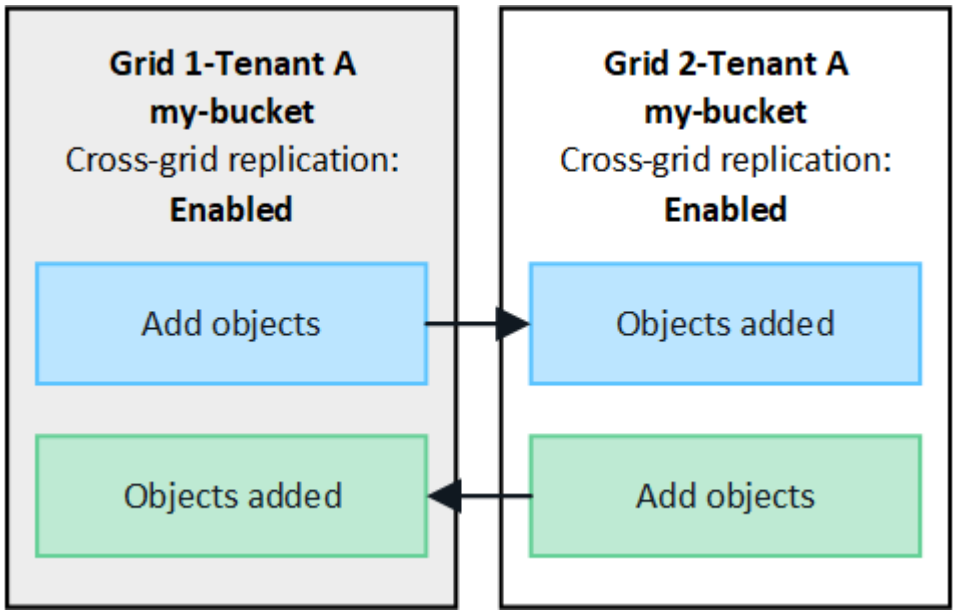
Replica in un'unica direzione

Se si attiva la replica cross-grid per un bucket su una sola griglia, gli oggetti aggiunti a quel bucket (il bucket di origine) vengono replicati nel bucket corrispondente sull'altra griglia (il bucket di destinazione). Tuttavia, gli oggetti aggiunti al bucket di destinazione non vengono replicati di nuovo nell'origine. Nella figura, la replica cross-grid è attivata per `my-bucket` Dalla griglia 1 alla griglia 2, ma non è attivata nell'altra direzione.



Replica in entrambe le direzioni

Se si attiva la replica cross-grid per lo stesso bucket su entrambe le griglie, gli oggetti aggiunti a entrambi i bucket vengono replicati nell'altra griglia. Nella figura, la replica cross-grid è attivata per `my-bucket` in entrambe le direzioni.



Cosa succede quando gli oggetti vengono acquisiti?

Quando un client S3 aggiunge un oggetto a un bucket con replica cross-grid attivata, si verifica quanto segue:

1. StorageGRID replica automaticamente l'oggetto dal bucket di origine al bucket di destinazione. Il tempo necessario per eseguire questa operazione di replica in background dipende da diversi fattori, tra cui il numero di altre operazioni di replica in sospeso.

   Il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject o HeadObject. La risposta include uno specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori: Il client S3 può verificare lo stato di replica di un oggetto inviando una richiesta GetObject o HeadObject. La risposta include uno specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **SUCCESSO**: La replica è riuscita per tutte le connessioni alla rete. • **PENDING**: L'oggetto non è stato replicato in almeno una connessione di rete. • **GUASTO**: La replica non è in sospeso per nessuna connessione alla rete e almeno una ha avuto esito negativo con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

   > StorageGRID non supporta `x-amz-replication-status` intestazione.

2. StorageGRID utilizza i criteri ILM attivi di ciascuna griglia per gestire gli oggetti, esattamente come per qualsiasi altro oggetto. Ad esempio, l'oggetto A sulla griglia 1 potrebbe essere memorizzato come due copie replicate e conservato per sempre, mentre la copia dell'oggetto A replicata sulla griglia 2 potrebbe essere memorizzata utilizzando la codifica di cancellazione 2+1 ed eliminata dopo tre anni.

Cosa succede quando gli oggetti vengono cancellati?

Come descritto in "Eliminare il flusso di dati", StorageGRID può eliminare un oggetto per uno dei seguenti motivi:

- Il client S3 invia una richiesta di eliminazione.
- Un utente tenant Manager seleziona "Eliminare gli oggetti nel bucket" opzione per rimuovere tutti gli oggetti da un bucket.
- Il bucket ha una configurazione del ciclo di vita che scade.
- L'ultimo periodo di tempo nella regola ILM per l'oggetto termina e non sono stati specificati ulteriori posizionamenti.

Quando StorageGRID elimina un oggetto a causa di un'operazione Delete Objects (Elimina oggetti) nel bucket, della scadenza del ciclo di vita del bucket o della scadenza del posizionamento ILM, l'oggetto replicato non viene mai cancellato dall'altra griglia in una connessione a federazione di griglie. Tuttavia, i marker di eliminazione aggiunti al bucket di origine da S3 client Delete possono essere replicati nel bucket di destinazione.

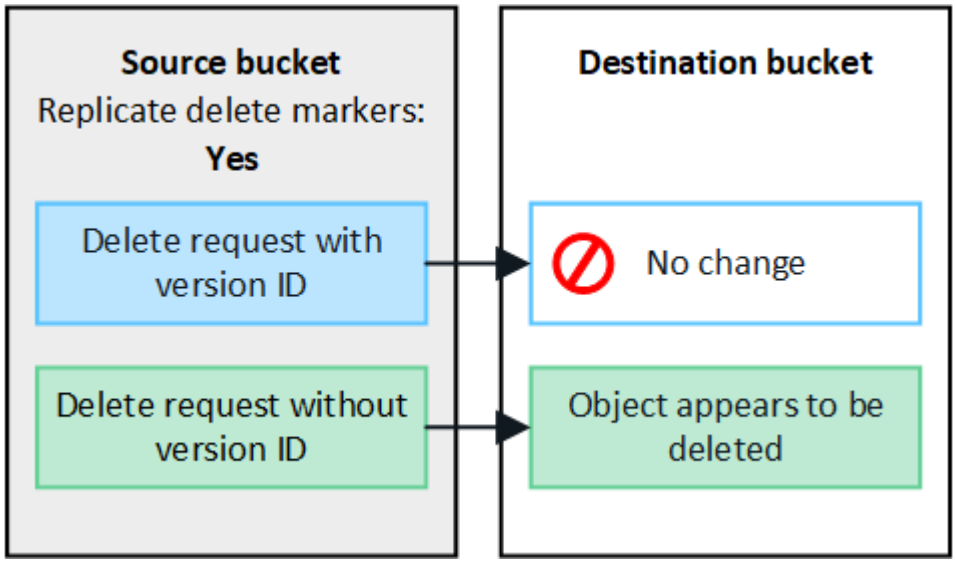
Per capire cosa accade quando un client S3 elimina oggetti da un bucket che ha la replica cross-grid attivata, rivedere come i client S3 eliminano oggetti dai bucket che hanno la versione attivata, come segue:

- Se un client S3 invia una richiesta di eliminazione che include un ID di versione, la versione dell'oggetto viene rimossa in modo permanente. Nessun marker di eliminazione aggiunto al bucket.
- Se un client S3 invia una richiesta di eliminazione che non include un ID di versione, StorageGRID non elimina alcuna versione di oggetto. Al contrario, aggiunge un contrassegno di eliminazione al bucket. Il contrassegno DELETE fa sì che StorageGRID agisca come se l'oggetto fosse stato cancellato:
  - Una richiesta GetObject senza ID versione non riesce con `404 No Object Found`
  - Una richiesta GetObject con un ID di versione valido avrà esito positivo e restituirà la versione dell'oggetto richiesta.

Quando un client S3 elimina un oggetto da un bucket con la replica cross-grid attivata, StorageGRID determina se replicare la richiesta di eliminazione nella destinazione, come segue:

- Se la richiesta di eliminazione include un ID di versione, la versione dell'oggetto viene rimossa in modo permanente dalla griglia di origine. Tuttavia, StorageGRID non replica le richieste di eliminazione che includono un ID di versione, pertanto la stessa versione dell'oggetto non viene eliminata dalla destinazione.
- Se la richiesta di eliminazione non include un ID di versione, StorageGRID può facoltativamente replicare il marker di eliminazione, in base alla configurazione della replica cross-grid per il bucket:
  - Se si sceglie di replicare i marker di eliminazione (impostazione predefinita), un marker di eliminazione viene aggiunto al bucket di origine e replicato nel bucket di destinazione. In effetti, l'oggetto sembra essere cancellato su entrambe le griglie.
  - Se si sceglie di non replicare i marker di eliminazione, un marker di eliminazione viene aggiunto al bucket di origine ma non viene replicato nel bucket di destinazione. In effetti, gli oggetti eliminati nella griglia di origine non vengono cancellati nella griglia di destinazione.

Nella figura, **Replicate delete markers** è stato impostato su **Yes** quando "la replica cross-grid è stata attivata". Le richieste di eliminazione per il bucket di origine che includono un ID di versione non elimineranno gli oggetti dal bucket di destinazione. Le richieste di eliminazione per il bucket di origine che non includono un ID di versione verranno visualizzate per eliminare gli oggetti nel bucket di destinazione.



Se si desidera mantenere le eliminazioni degli oggetti sincronizzate tra le griglie, creare le corrispondenti "Configurazioni del ciclo di vita S3" per i bucket su entrambe le griglie.

Modalità di replica degli oggetti crittografati

Quando si utilizza la replica cross-grid per replicare oggetti tra griglie, è possibile crittografare singoli oggetti, utilizzare la crittografia bucket predefinita o configurare la crittografia a livello di griglia. È possibile aggiungere, modificare o rimuovere le impostazioni di crittografia predefinite del bucket o dell'intera griglia prima o dopo aver attivato la replica cross-grid per un bucket.

Per crittografare singoli oggetti, è possibile utilizzare SSE (crittografia lato server con chiavi gestite da StorageGRID) quando si aggiungono gli oggetti al bucket di origine. Utilizzare `x-amz-server-side-encryption` richiedi intestazione e specifica `AES256`. Vedere "Utilizzare la crittografia lato server".

L'utilizzo di SSE-C (crittografia lato server con chiavi fornite dal cliente) non è supportato per la replica cross-grid. L'operazione di acquisizione non riesce.

Per utilizzare la crittografia predefinita per un bucket, utilizzare una richiesta PutBucketEncryption e impostare `SSEAlgorithm` parametro a. `AES256`. La crittografia a livello di bucket si applica a tutti gli oggetti acquisiti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere "Operazioni sui bucket".

Per utilizzare la crittografia a livello di griglia, impostare l'opzione **Stored Object Encryption** su **AES-256**. La crittografia a livello di griglia si applica a tutti gli oggetti che non sono crittografati a livello di bucket o che sono acquisiti senza `x-amz-server-side-encryption` intestazione della richiesta. Vedere "Configurare le opzioni di rete e degli oggetti".

SSE non supporta AES-128. Se l'opzione **Stored Object Encryption** è attivata per la griglia di origine utilizzando l'opzione **AES-128**, l'utilizzo dell'algoritmo AES-128 non verrà propagato all'oggetto replicato. L'oggetto replicato utilizzerà invece l'impostazione predefinita del bucket o della crittografia a livello di griglia della destinazione, se disponibile.

Quando si determina come crittografare gli oggetti di origine, StorageGRID applica le seguenti regole:

1. Utilizzare `x-amz-server-side-encryption` acquisire l'intestazione, se presente.
2. Se non è presente un'intestazione di acquisizione, utilizzare l'impostazione di crittografia predefinita del bucket, se configurata.
3. Se un'impostazione bucket non è configurata, utilizzare l'impostazione di crittografia a livello di griglia, se configurata.
4. Se non è presente un'impostazione a livello di griglia, non crittografare l'oggetto di origine.

Quando si determina come crittografare gli oggetti replicati, StorageGRID applica queste regole nel seguente ordine:

1. Utilizzare la stessa crittografia dell'oggetto di origine, a meno che tale oggetto non utilizzi la crittografia AES-128.
2. Se l'oggetto di origine non è crittografato o utilizza AES-128, utilizzare l'impostazione di crittografia predefinita del bucket di destinazione, se configurato.
3. Se il bucket di destinazione non dispone di un'impostazione di crittografia, utilizzare l'impostazione di crittografia a livello di griglia della destinazione, se configurata.
4. Se non è presente un'impostazione a livello di griglia, non crittografare l'oggetto di destinazione.

PutObjectTagging e DeleteObjectTagging non sono supportati

Le richieste PutObjectTagging e DeleteObjectTagging non sono supportate per gli oggetti nei bucket in cui è abilitata la replica cross-grid.

Se un client S3 esegue una richiesta PutObjectTagging o DeleteObjectTagging, `501 Not Implemented` viene restituito. Il messaggio è `Put(Delete) ObjectTagging is not available for buckets that have cross-grid replication configured`.

Come vengono replicati gli oggetti segmentati

Le dimensioni massime dei segmenti della griglia di origine si applicano agli oggetti replicati nella griglia di destinazione. Quando gli oggetti vengono replicati in un'altra griglia, l'impostazione **Maximum Segment Size** (**CONFIGURATION** > **System** > **Storage options**) della griglia di origine viene utilizzata su entrambe le griglie. Ad esempio, supponiamo che la dimensione massima del segmento per la griglia di origine sia di 1 GB, mentre la dimensione massima del segmento della griglia di destinazione sia di 50 MB. Se si riceve un oggetto da 2 GB nella griglia di origine, tale oggetto viene salvato come due segmenti da 1 GB. Inoltre, verrà replicato nella griglia di destinazione come due segmenti da 1 GB, anche se la dimensione massima del segmento della griglia è di 50 MB.

Confronta la replica cross-grid e la replica CloudMirror

Mentre inizi a utilizzare la federazione di griglie, esamina le analogie e le differenze tra "replica cross-grid" e a. "Servizio di replica di StorageGRID CloudMirror".

	Replica cross-grid	**Servizio di replica di CloudMirror**
Qual è lo scopo principale?	Un sistema StorageGRID funge da sistema di disaster recovery. Gli oggetti in un bucket possono essere replicati tra le griglie in una o entrambe le direzioni.	Consente a un tenant di replicare automaticamente gli oggetti da un bucket in StorageGRID (origine) a un bucket S3 esterno (destinazione). La replica di CloudMirror crea una copia indipendente di un oggetto in un'infrastruttura S3 indipendente. Questa copia indipendente non viene utilizzata come backup, ma viene spesso ulteriormente elaborata nel cloud.
Come viene configurato?	1. Configurare una connessione a federazione di griglie tra due griglie. 2. Aggiungere nuovi account tenant, che vengono clonati automaticamente nell'altra griglia. 3. Aggiungere nuovi gruppi di tenant e utenti, che vengono clonati. 4. Creare bucket corrispondenti su ogni griglia e consentire la replica cross-grid in una o entrambe le direzioni.	1. Un utente tenant configura la replica di CloudMirror definendo un endpoint CloudMirror (indirizzo IP, credenziali e così via) utilizzando Tenant Manager o l'API S3. 2. Qualsiasi bucket di proprietà dell'account tenant può essere configurato per puntare all'endpoint CloudMirror.

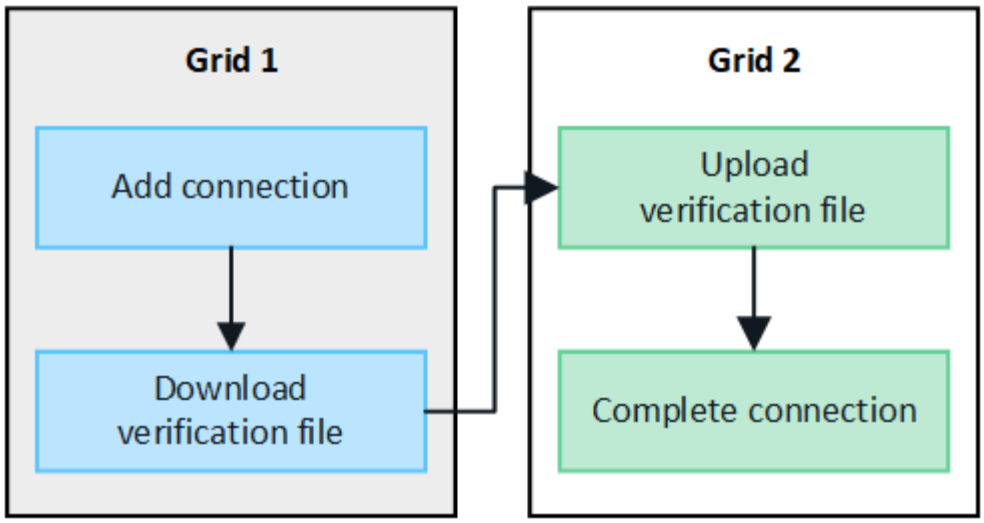
	Replica cross-grid	Servizio di replica di CloudMirror
Chi è responsabile della sua configurazione?	• Un amministratore di grid configura la connessione e i tenant. • Gli utenti tenant configurano gruppi, utenti, chiavi e bucket.	In genere, un utente tenant.
Qual è la destinazione?	Un bucket S3 corrispondente e identico sull'altro sistema StorageGRID nella connessione a federazione di griglia.	• Qualsiasi infrastruttura S3 compatibile (incluso Amazon S3). • Piattaforma Google Cloud (GCP)
È necessario il controllo della versione degli oggetti?	Sì, sia il bucket di origine che quello di destinazione devono avere attivato la versione degli oggetti.	No, la replica di CloudMirror supporta qualsiasi combinazione di bucket senza versioni e con versioni sia sull'origine che sulla destinazione.
Qual è la causa dello spostamento degli oggetti nella destinazione?	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket con replica cross-grid attivata.	Gli oggetti vengono replicati automaticamente quando vengono aggiunti a un bucket configurato con un endpoint CloudMirror. Gli oggetti che esistevano nel bucket di origine prima della configurazione del bucket con l'endpoint CloudMirror non vengono replicati, a meno che non vengano modificati.
Come vengono replicati gli oggetti?	La replica cross-grid crea oggetti con versione e replica l'ID della versione dal bucket di origine al bucket di destinazione. Ciò consente di mantenere l'ordine delle versioni in entrambe le griglie.	La replica di CloudMirror non richiede bucket abilitati per il controllo delle versioni, pertanto CloudMirror può eseguire l'ordine solo per una chiave all'interno di un sito. Non vi sono garanzie che l'ordine venga mantenuto per le richieste a un oggetto in un sito diverso.
Cosa succede se un oggetto non può essere replicato?	L'oggetto viene messo in coda per la replica, in base ai limiti di storage dei metadati.	L'oggetto viene messo in coda per la replica, in base ai limiti dei servizi della piattaforma (vedere "Consigli per l'utilizzo dei servizi della piattaforma").
I metadati di sistema dell'oggetto sono replicati?	Sì, quando un oggetto viene replicato nell'altra griglia, vengono replicati anche i relativi metadati di sistema. I metadati saranno identici su entrambe le griglie.	No, quando un oggetto viene replicato nel bucket esterno, i relativi metadati di sistema vengono aggiornati. I metadati variano in base al tempo di acquisizione e al comportamento dell'infrastruttura S3 indipendente.

	Replica cross-grid	Servizio di replica di CloudMirror
Come vengono recuperati gli oggetti?	Le applicazioni possono recuperare o leggere gli oggetti effettuando una richiesta al bucket su una griglia.	Le applicazioni possono recuperare o leggere oggetti effettuando una richiesta a StorageGRID o alla destinazione S3. Si supponga, ad esempio, di utilizzare la replica CloudMirror per eseguire il mirroring degli oggetti in un'organizzazione partner. Il partner può utilizzare le proprie applicazioni per leggere o aggiornare gli oggetti direttamente dalla destinazione S3. Non è necessario utilizzare StorageGRID.
Cosa succede se un oggetto viene cancellato?	• Le richieste di eliminazione che includono un ID di versione non vengono mai replicate nella griglia di destinazione. • Le richieste di eliminazione che non includono un ID di versione aggiungono un contrassegno di eliminazione al bucket di origine, che può essere facoltativamente replicato nella griglia di destinazione. • Se la replica cross-grid è configurata per una sola direzione, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.	I risultati variano in base allo stato di versione dei bucket di origine e di destinazione (che non devono essere identici): • Se entrambi i bucket sono con versione, una richiesta di eliminazione aggiungerà un indicatore di eliminazione in entrambe le posizioni. • Se viene configurato solo il bucket di origine, una richiesta di eliminazione aggiungerà un indicatore di eliminazione all'origine, ma non alla destinazione. • Se nessuno dei bucket è dotato di versione, una richiesta di eliminazione elimina l'oggetto dall'origine ma non dalla destinazione. Allo stesso modo, gli oggetti nel bucket di destinazione possono essere cancellati senza influire sull'origine.

Creare connessioni di federazione di griglie

È possibile creare una connessione a federazione di griglie tra due sistemi StorageGRID se si desidera clonare i dettagli del tenant e replicare i dati degli oggetti.

Come illustrato nella figura, la creazione di una connessione a federazione di griglie include operazioni su entrambe le griglie. La connessione viene aggiunta su una griglia e completata sull'altra. È possibile iniziare da una delle due griglie.



Prima di iniziare

- Hai esaminato il "considerazioni e requisiti" per la configurazione delle connessioni di federazione di griglie.
- Se si intende utilizzare FQDN (Fully Qualified Domain Name) per ogni griglia invece degli indirizzi IP o VIP, si conoscono i nomi da utilizzare e si conferma che il server DNS per ogni griglia dispone delle voci appropriate.
- Si sta utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root e della passphrase di provisioning per entrambe le griglie.

Aggiungi connessione

Eseguire questa procedura su uno dei due sistemi StorageGRID.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare **Aggiungi connessione**.
4. Inserire i dettagli della connessione.

Campo	Descrizione
Nome della connessione	Un nome univoco che consente di riconoscere questa connessione, ad esempio "Grid 1-Grid 2".
FQDN o IP per questa griglia	Una delle seguenti opzioni: • L'FQDN della griglia a cui si è attualmente connessi • Indirizzo VIP di un gruppo ha su questa griglia • Indirizzo IP di un nodo Admin o di un nodo Gateway in questa griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla griglia di destinazione.

Campo	Descrizione
Porta	La porta che si desidera utilizzare per questa connessione. È possibile immettere un numero di porta inutilizzato compreso tra 23000 e 23999. Entrambe le griglie di questa connessione utilizzeranno la stessa porta. È necessario assicurarsi che nessun nodo di una delle griglie utilizzi questa porta per altre connessioni.
Giorni di validità del certificato per questa griglia	Il numero di giorni in cui si desidera che i certificati di protezione per questa griglia nella connessione siano validi. Il valore predefinito è 730 giorni (2 anni), ma è possibile immettere un valore compreso tra 1 e 762 giorni. StorageGRID genera automaticamente certificati client e server per ogni griglia quando si salva la connessione.
Passphrase di provisioning per questa griglia	La passphrase di provisioning per la griglia a cui hai effettuato l'accesso.
FQDN o IP per l'altra griglia	Una delle seguenti opzioni: • L'FQDN della griglia a cui si desidera connettersi • Indirizzo VIP di un gruppo ha sull'altra griglia • Indirizzo IP di un nodo Admin o di un nodo Gateway nell'altra griglia. L'IP può trovarsi su qualsiasi rete raggiungibile dalla rete di origine.

5. Selezionare **Salva e continua**.
6. Per la fase Download verfica file, selezionare **Download verfica file**.

   Una volta completata la connessione sull'altra griglia, non è più possibile scaricare il file di verifica da nessuna griglia.

7. Individuare il file scaricato (*`connection-name`*`.grid-federation`) e salvarlo in una posizione sicura.

   Questo file contiene segreti (mascherati come *****) e altri dettagli sensibili e devono essere memorizzati e trasmessi in modo sicuro.

8. Selezionare **Close** (Chiudi) per tornare alla pagina Grid Federation (federazione griglia).
9. Verificare che sia visualizzata la nuova connessione e che il relativo **stato della connessione** sia **in attesa di connessione**.
10. Fornire il *`connection-name`*`.grid-federation` all'amministratore della griglia per l'altra griglia.

Connessione completa

Eseguire questa procedura sul sistema StorageGRID a cui si sta effettuando la connessione (l'altra griglia).

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare **carica file di verifica** per accedere alla pagina carica.
4. Selezionare **carica file di verifica**. Quindi, individuare e selezionare il file scaricato dalla prima griglia (*connection-name*`.grid-federation`).

   Vengono visualizzati i dettagli della connessione.

5. Se si desidera, immettere un numero diverso di giorni validi per i certificati di sicurezza per questa griglia. Per impostazione predefinita, la voce **Certificate Valid Days** (giorni validi certificato) corrisponde al valore immesso nella prima griglia, ma ciascuna griglia può utilizzare date di scadenza diverse.

   In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

   > Se i certificati a una delle due estremità della connessione scadono, la connessione smette di funzionare e le repliche saranno in sospeso fino all'aggiornamento dei certificati.

6. Inserire la passphrase di provisioning per la griglia a cui si è attualmente connessi.
7. Selezionare **Save and test** (Salva e verifica).

   I certificati vengono generati e la connessione viene testata. Se la connessione è valida, viene visualizzato un messaggio di esito positivo e la nuova connessione viene elencata nella pagina Grid Federation. Lo stato **Connection** sarà **Connected**.

   Se viene visualizzato un messaggio di errore, risolvere eventuali problemi. Vedere "Risolvere i problemi relativi agli errori di federazione della griglia".

8. Accedere alla pagina Grid Federation (federazione griglia) nella prima griglia e aggiornare il browser. Verificare che lo stato della connessione sia ora **connesso**.
9. Una volta stabilita la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

   Se si modifica questa connessione, viene creato un nuovo file di verifica. Il file originale non può essere riutilizzato.

Al termine

- Esaminare le considerazioni per "gestione dei tenant autorizzati".
- "Creare uno o più nuovi account tenant", Assegnare l'autorizzazione **Usa connessione federazione griglia** e selezionare la nuova connessione.
- "Gestire la connessione" secondo necessità. È possibile modificare i valori di connessione, verificare una connessione, ruotare i certificati di connessione o rimuovere una connessione.
- "Monitorare la connessione" Come parte delle normali attività di monitoraggio StorageGRID.
- "Risolvere i problemi di connessione", inclusa la risoluzione di eventuali avvisi ed errori relativi al clone dell'account e alla replica cross-grid.

Gestire le connessioni a federazione di griglie

La gestione delle connessioni a federazione di griglie tra sistemi StorageGRID include la modifica dei dettagli di connessione, la rotazione dei certificati, la rimozione delle autorizzazioni del tenant e la rimozione delle connessioni inutilizzate.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su una delle griglie utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per la griglia a cui si è effettuato l'accesso.

Modifica una connessione a federazione di griglie

È possibile modificare una connessione a federazione di griglie effettuando l'accesso al nodo di amministrazione primario su una delle griglie della connessione. Una volta apportate le modifiche alla prima griglia, è necessario scaricare un nuovo file di verifica e caricarlo nell'altra griglia.

> ⓘ Durante la modifica della connessione, le richieste di replica cross-grid o clone dell'account continueranno a utilizzare le impostazioni di connessione esistenti. Tutte le modifiche apportate alla prima griglia vengono salvate localmente, ma non vengono utilizzate fino a quando non vengono caricate nella seconda griglia, salvate e testate.

Avviare la modifica della connessione

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **NODI** e verificare che tutti gli altri nodi Admin del sistema siano in linea.

   > ⓘ Quando si modifica una connessione a federazione di griglie, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi di amministrazione della prima griglia. Se il file non può essere salvato in tutti i nodi di amministrazione, viene visualizzato un messaggio di avviso quando si seleziona **Salva e test**.

3. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
4. Modificare i dettagli della connessione utilizzando il menu **azioni** della pagina Grid Federation o la pagina dei dettagli per una connessione specifica. Vedere "Creare connessioni di federazione di griglie" per cosa partecipare.

   Menu delle azioni

   a. Selezionare il pulsante di opzione per la connessione.
   b. Selezionare **azioni** > **Modifica**.
   c. Inserire le nuove informazioni.

   Pagina dei dettagli

   a. Selezionare un nome di connessione per visualizzarne i dettagli.
   b. Selezionare **Modifica**.
   c. Inserire le nuove informazioni.

5. Inserire la passphrase di provisioning per la griglia a cui si è connessi.
6. Selezionare **Salva e continua**.

   I nuovi valori vengono salvati, ma non vengono applicati alla connessione fino a quando non si carica il nuovo file di verifica sull'altra griglia.

7. Selezionare **Scarica file di verifica**.

   Per scaricare il file in un secondo momento, accedere alla pagina dei dettagli della connessione.

8. Individuare il file scaricato (*connection-name*`.grid-federation`) e salvarlo in una posizione sicura.

   Il file di verifica contiene segreti e deve essere memorizzato e trasmesso in modo sicuro.

9. Selezionare **Close** (Chiudi) per tornare alla pagina Grid Federation (federazione griglia).
10. Verificare che lo stato della connessione sia **Pending EDIT** (Modifica in sospeso).

    Se lo stato della connessione era diverso da **connesso** quando si inizia a modificare la connessione, non verrà modificato in **in attesa di modifica**.

11. Fornire il *connection-name*`.grid-federation` all'amministratore della griglia per l'altra griglia.

Terminare la modifica della connessione

Terminare la modifica della connessione caricando il file di verifica sull'altra griglia.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare **carica file di verifica** per accedere alla pagina di caricamento.
4. Selezionare **carica file di verifica**. Quindi, individuare e selezionare il file scaricato dalla prima griglia.
5. Inserire la passphrase di provisioning per la griglia a cui si è attualmente connessi.
6. Selezionare **Save and test** (Salva e verifica).

   Se è possibile stabilire la connessione utilizzando i valori modificati, viene visualizzato un messaggio di esito positivo. In caso contrario, viene visualizzato un messaggio di errore. Esaminare il messaggio e risolvere eventuali problemi.

7. Chiudere la procedura guidata per tornare alla pagina Grid Federation.
8. Verificare che lo stato della connessione sia **connesso**.
9. Accedere alla pagina Grid Federation (federazione griglia) nella prima griglia e aggiornare il browser. Verificare che lo stato della connessione sia ora **connesso**.
10. Una volta stabilita la connessione, eliminare in modo sicuro tutte le copie del file di verifica.

Test di una connessione a federazione di griglie

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Verificare la connessione utilizzando il menu **azioni** della pagina Grid Federation o la pagina dei dettagli per una connessione specifica.

Menu delle azioni

a. Selezionare il pulsante di opzione per la connessione.

b. Selezionare **azioni** > **Test**.

Pagina dei dettagli

a. Selezionare un nome di connessione per visualizzarne i dettagli.

b. Selezionare **Test di connessione**.

4. Controllare lo stato della connessione:

Stato della connessione	Descrizione
Connesso	Entrambe le griglie sono collegate e comunicano normalmente.
Errore	La connessione si trova in uno stato di errore. Ad esempio, un certificato è scaduto o un valore di configurazione non è più valido.
In attesa di modifica	La connessione su questa griglia è stata modificata, ma la connessione sta ancora utilizzando la configurazione esistente. Per completare la modifica, caricare il nuovo file di verifica nell'altra griglia.
In attesa di connessione	La connessione è stata configurata su questa griglia, ma la connessione non è stata completata sull'altra griglia. Scarica il file di verifica da questa griglia e caricalo nell'altra griglia.
Sconosciuto	La connessione si trova in uno stato sconosciuto, probabilmente a causa di un problema di rete o di un nodo offline.

5. Se lo stato della connessione è **Error**, risolvere eventuali problemi. Quindi, selezionare di nuovo **Test di connessione** per confermare che il problema è stato risolto.

rotazione dei certificati di connessione

Ogni connessione a federazione di griglie utilizza quattro certificati SSL generati automaticamente per proteggere la connessione. Quando i due certificati per ogni griglia si avvicinano alla data di scadenza, l'avviso **scadenza del certificato federazione griglia** ricorda di ruotare i certificati.

> Se i certificati a una delle due estremità della connessione scadono, la connessione smette di funzionare e le repliche saranno in sospeso fino all'aggiornamento dei certificati.

Fasi

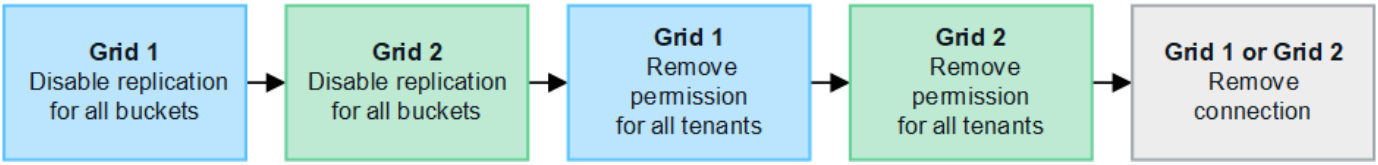
1. Accedere a Grid Manager dal nodo di amministrazione principale su una griglia.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Da una delle schede della pagina Grid Federation, selezionare il nome della connessione per visualizzarne i dettagli.

4. Selezionare la scheda **certificati**.
5. Selezionare **ruota certificati**.
6. Specificare il numero di giorni in cui i nuovi certificati devono essere validi.
7. Inserire la passphrase di provisioning per la griglia a cui si è connessi.
8. Selezionare **ruota certificati**.
9. Se necessario, ripetere questi passaggi sull'altra griglia della connessione.

   In generale, utilizzare lo stesso numero di giorni per i certificati su entrambi i lati della connessione.

Rimuovi una connessione a federazione di griglie

È possibile rimuovere una connessione a federazione di griglia da una delle griglie della connessione. Come illustrato nella figura, è necessario eseguire i passaggi necessari su entrambe le griglie per confermare che la connessione non viene utilizzata da alcun tenant su nessuna griglia.



Prima di rimuovere una connessione, tenere presente quanto segue:

- La rimozione di una connessione non elimina gli elementi già copiati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti del tenant presenti in entrambe le griglie non vengono cancellati da nessuna griglia quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Quando si rimuove una connessione, la replica di tutti gli oggetti in sospeso (acquisiti ma non ancora replicati nell'altra griglia) avrà esito negativo in modo permanente.

Disattiva la replica per tutti i bucket del tenant

Fasi

1. Partendo da una griglia, accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **tenant consentiti**, determinare se la connessione viene utilizzata da qualsiasi tenant.
5. Se sono elencati dei tenant, chiedere a tutti i tenant di "disattiva la replica cross-grid" per tutti i bucket su entrambe le griglie della connessione.

> Non è possibile rimuovere l'autorizzazione **use grid Federation Connection** (Usa connessione federazione griglia) se alcuni bucket tenant hanno attivato la replica cross-grid. Ciascun account tenant deve disattivare la replica cross-grid per i bucket su entrambe le griglie.

Rimuovere i permessi per ciascun tenant

Una volta disattivata la replica cross-grid per tutti i bucket del tenant, rimuovere l'autorizzazione **Usa federazione grid** da tutti i tenant su entrambe le grid.

Fasi

1. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
2. Selezionare il nome della connessione per visualizzarne i dettagli.
3. Per ciascun tenant nella scheda **tenant consentiti**, rimuovere l'autorizzazione **Usa connessione federazione griglia** da ciascun tenant. Vedere "Gestire i tenant autorizzati".
4. Ripetere questi passaggi per i tenant consentiti sull'altra griglia.

Rimuovere la connessione

Fasi

1. Se nessun tenant su una griglia sta utilizzando la connessione, selezionare **Remove** (Rimuovi).
2. Controllare il messaggio di conferma e selezionare **Rimuovi**.
   - Se è possibile rimuovere la connessione, viene visualizzato un messaggio di conferma. La connessione a federazione di griglie viene ora rimossa da entrambe le griglie.
   - Se la connessione non può essere rimossa (ad esempio, è ancora in uso o si è verificato un errore di connessione), viene visualizzato un messaggio di errore. È possibile effettuare una delle seguenti operazioni:
     - Risolvere l'errore (consigliato). Vedere "Risolvere i problemi relativi agli errori di federazione della griglia".
     - Rimuovere la connessione con la forza. Vedere la sezione successiva.

Rimuovi una connessione a federazione di griglie con la forza

Se necessario, è possibile forzare la rimozione di una connessione che non ha lo stato **Connected**.

La rimozione forzata elimina solo la connessione dalla griglia locale. Per rimuovere completamente la connessione, eseguire le stesse operazioni su entrambe le griglie.

Fasi

1. Dalla finestra di dialogo di conferma, selezionare **Force remove** (forza rimozione).

   Viene visualizzato un messaggio di successo. Questa connessione a federazione di griglie non può più essere utilizzata. Tuttavia, i bucket tenant potrebbero avere ancora la replica cross-grid attivata e alcune copie degli oggetti potrebbero essere già state replicate tra le griglie della connessione.

2. Dall'altra griglia della connessione, accedere a Grid Manager dal nodo di amministrazione primario.
3. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
4. Selezionare il nome della connessione per visualizzarne i dettagli.
5. Selezionare **Rimuovi** e **Sì**.
6. Selezionare **forza rimozione** per rimuovere la connessione da questa griglia.

Gestire i tenant consentiti per la federazione di grid

È possibile consentire agli account tenant S3 di utilizzare una connessione di federazione di griglie tra due sistemi StorageGRID. Quando ai tenant viene consentito di utilizzare una connessione, sono necessari passaggi speciali per modificare i dettagli del tenant o per rimuovere in modo permanente l'autorizzazione di un tenant a utilizzare la

connessione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager su una delle griglie utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per la griglia a cui si è effettuato l'accesso.
- Lo hai fatto "creazione di una connessione a federazione di griglie" tra due griglie.
- Hai esaminato i flussi di lavoro per "clone dell'account" e. "replica cross-grid".
- Come richiesto, è già stato configurato il Single Sign-on (SSO) o l'identificazione della federazione per entrambe le griglie della connessione. Vedere "Cos'è il clone dell'account".

Creare un tenant consentito

Se si desidera consentire a un account tenant nuovo o esistente di utilizzare una connessione di federazione griglia per la clonazione dell'account e la replica cross-grid, seguire le istruzioni generali riportate a. "Creare un nuovo tenant S3" oppure "modificare un account tenant" e prendere nota di quanto segue:

- È possibile creare il tenant da una griglia della connessione. La griglia in cui viene creato un tenant è la griglia di origine del *tenant*.
- Lo stato della connessione deve essere **connesso**.
- Quando il tenant viene creato o modificato per attivare l'autorizzazione **Usa connessione federazione griglia** e quindi salvato nella prima griglia, un tenant identico viene replicato automaticamente nell'altra griglia. La griglia in cui viene replicato il tenant è la griglia di destinazione del *tenant*.
- I tenant di entrambe le griglie avranno lo stesso ID account a 20 cifre, il nome, la descrizione, la quota e le autorizzazioni. In alternativa, è possibile utilizzare il campo **Description** per identificare il tenant di origine e il tenant di destinazione. Ad esempio, questa descrizione per un tenant creato sulla griglia 1 verrà visualizzata anche per il tenant replicato sulla griglia 2: "Questo tenant è stato creato sulla griglia 1".
- Per motivi di sicurezza, la password di un utente root locale non viene copiata nella griglia di destinazione.

> Prima che un utente root locale possa accedere al tenant replicato sulla griglia di destinazione, un amministratore della griglia deve "modificare la password per l'utente root locale".

- Una volta che il tenant nuovo o modificato è disponibile su entrambi i grid, gli utenti tenant possono eseguire queste operazioni:
  - Dalla griglia di origine del tenant, creare gruppi e utenti locali, che vengono clonati automaticamente nella griglia di destinazione del tenant. Vedere "Clonare utenti e gruppi tenant".
  - Creare nuove chiavi di accesso S3, che possono essere eventualmente clonate nella griglia di destinazione del tenant. Vedere "Clonare le chiavi di accesso S3 utilizzando l'API".
  - Creare bucket identici su entrambe le griglie della connessione e abilitare la replica cross-grid in una direzione o in entrambe le direzioni. Vedere "Gestire la replica cross-grid".

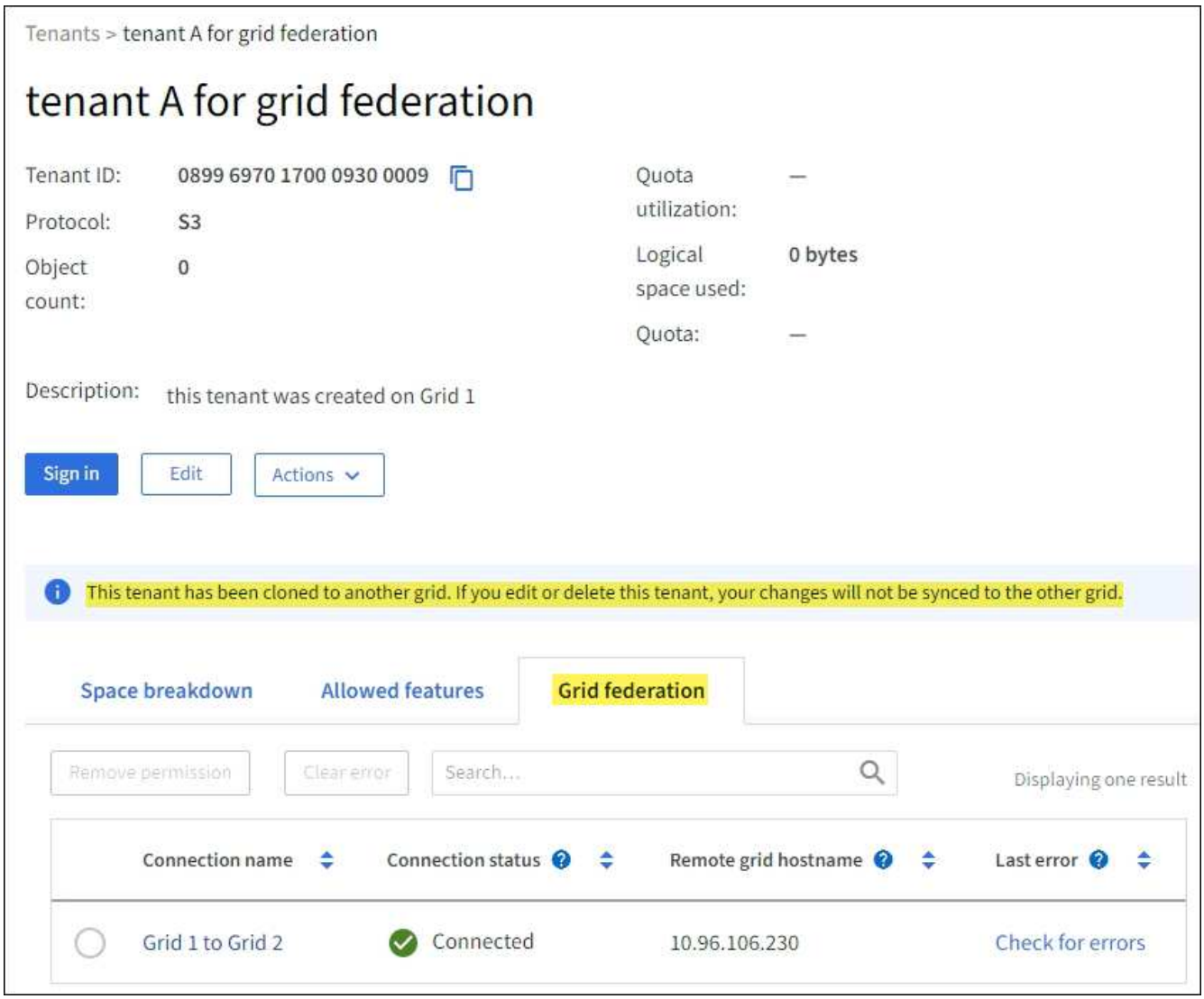
Visualizzare un tenant consentito

È possibile visualizzare i dettagli di un tenant autorizzato a utilizzare una connessione a federazione di griglie.

Fasi

1. Selezionare **TENANT**.
2. Dalla pagina tenant, selezionare il nome del tenant per visualizzare la pagina dei dettagli del tenant.

Se si tratta della griglia di origine del tenant (ovvero, se il tenant è stato creato in questa griglia), viene visualizzato un banner per ricordare che il tenant è stato clonato in un'altra griglia. Se modifichi o elimini questo tenant, le modifiche non verranno sincronizzate con l'altra griglia.



3. Se si desidera, selezionare la scheda **Grid Federation** in "monitorare la connessione alla federazione di griglie".

Modificare un tenant consentito

Se è necessario modificare un tenant con l'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per "modifica di un account tenant" e prendere nota di quanto segue:

- Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da una delle griglie della connessione. Tuttavia, qualsiasi modifica apportata non verrà copiata nell'altra griglia. Se si desidera mantenere sincronizzati i dettagli del tenant tra le griglie, è necessario apportare le stesse modifiche su entrambe.
- Non è possibile cancellare l'autorizzazione **Usa connessione federazione griglia** quando si modifica un tenant.
- Non è possibile selezionare una connessione a federazione di griglie diversa quando si modifica un tenant.

Eliminare un tenant consentito

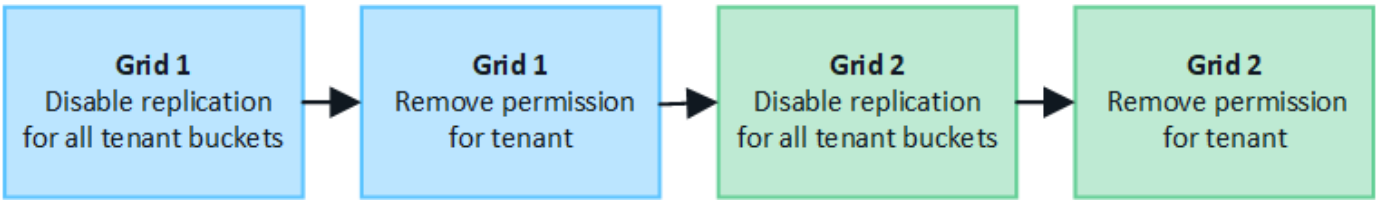
Se è necessario rimuovere un tenant con l'autorizzazione **Usa connessione federazione griglia**, seguire le istruzioni generali per "eliminazione di un account tenant" e prendere nota di quanto segue:

- Prima di rimuovere il tenant originale dalla griglia di origine, è necessario rimuovere tutti i bucket dell'account sulla griglia di origine.
- Prima di poter rimuovere il tenant clonato nella griglia di destinazione, è necessario rimuovere tutti i bucket dell'account nella griglia di destinazione.
- Se si rimuove il tenant originale o clonato, l'account non può più essere utilizzato per la replica cross-grid.
- Se si rimuove il tenant originale dalla griglia di origine, i gruppi di tenant, gli utenti o le chiavi clonati nella griglia di destinazione non verranno influenzati. È possibile eliminare il tenant clonato o consentirne la gestione di gruppi, utenti, chiavi di accesso e bucket.
- Se si rimuove il tenant clonato nella griglia di destinazione, si verificano errori di clonazione se vengono aggiunti nuovi gruppi o utenti al tenant originale.

  Per evitare questi errori, rimuovere l'autorizzazione del tenant per utilizzare la connessione di federazione della griglia prima di eliminare il tenant da questa griglia.

Rimuovi l'autorizzazione Usa connessione federazione griglia

Per impedire a un tenant di utilizzare una connessione a federazione di griglie, è necessario rimuovere l'autorizzazione **Usa connessione a federazione di griglie**.



Prima di rimuovere l'autorizzazione di un tenant a utilizzare una connessione a federazione di griglie, tenere presente quanto segue:

- Non è possibile rimuovere l'autorizzazione **Usa connessione federazione griglia** se uno dei bucket del tenant ha attivato la replica cross-grid. L'account tenant deve prima disattivare la replica cross-grid per tutti i bucket.
- La rimozione dell'autorizzazione **Usa connessione federazione griglia** non elimina gli elementi che sono già stati replicati tra le griglie. Ad esempio, gli utenti, i gruppi e gli oggetti del tenant presenti in entrambe le griglie non vengono cancellati da nessuna griglia quando viene rimossa l'autorizzazione del tenant. Se si desidera eliminare questi elementi, è necessario eliminarli manualmente da entrambe le griglie.
- Se si desidera riattivare questa autorizzazione con la stessa connessione di federazione della griglia, eliminare prima questo tenant sulla griglia di destinazione; in caso contrario, riabilitare questa autorizzazione causerà un errore.

> Riattivando l'autorizzazione **Use grid Federation Connection**, la griglia locale diventa la griglia di origine e attiva la clonazione alla griglia remota specificata dalla connessione di federazione della griglia selezionata. Se l'account tenant è già presente nella griglia remota, la clonazione causerà un errore di conflitto.

Prima di iniziare

- Si sta utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root" per entrambe le griglie.

Disattiva la replica per i bucket tenant

Come primo passo, disattivare la replica cross-grid per tutti i bucket del tenant.

Fasi

1. Partendo da una griglia, accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare il nome della connessione per visualizzarne i dettagli.
4. Nella scheda **tenant consentiti**, determinare se il tenant sta utilizzando la connessione.
5. Se il tenant è presente nell'elenco, chiedere al tenant di farlo "disattiva la replica cross-grid" per tutti i bucket su entrambe le griglie della connessione.

> Non è possibile rimuovere l'autorizzazione **use grid Federation Connection** (Usa connessione federazione griglia) se alcuni bucket tenant hanno attivato la replica cross-grid. Il tenant deve disattivare la replica cross-grid per i bucket su entrambe le griglie.

Rimuovere l'autorizzazione per il tenant

Una volta disattivata la replica cross-grid per i bucket tenant, è possibile rimuovere il permesso del tenant per utilizzare la connessione di federazione grid.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Rimuovere l'autorizzazione dalla pagina Grid Federation o dalla pagina tenant.

Pagina Grid Federation

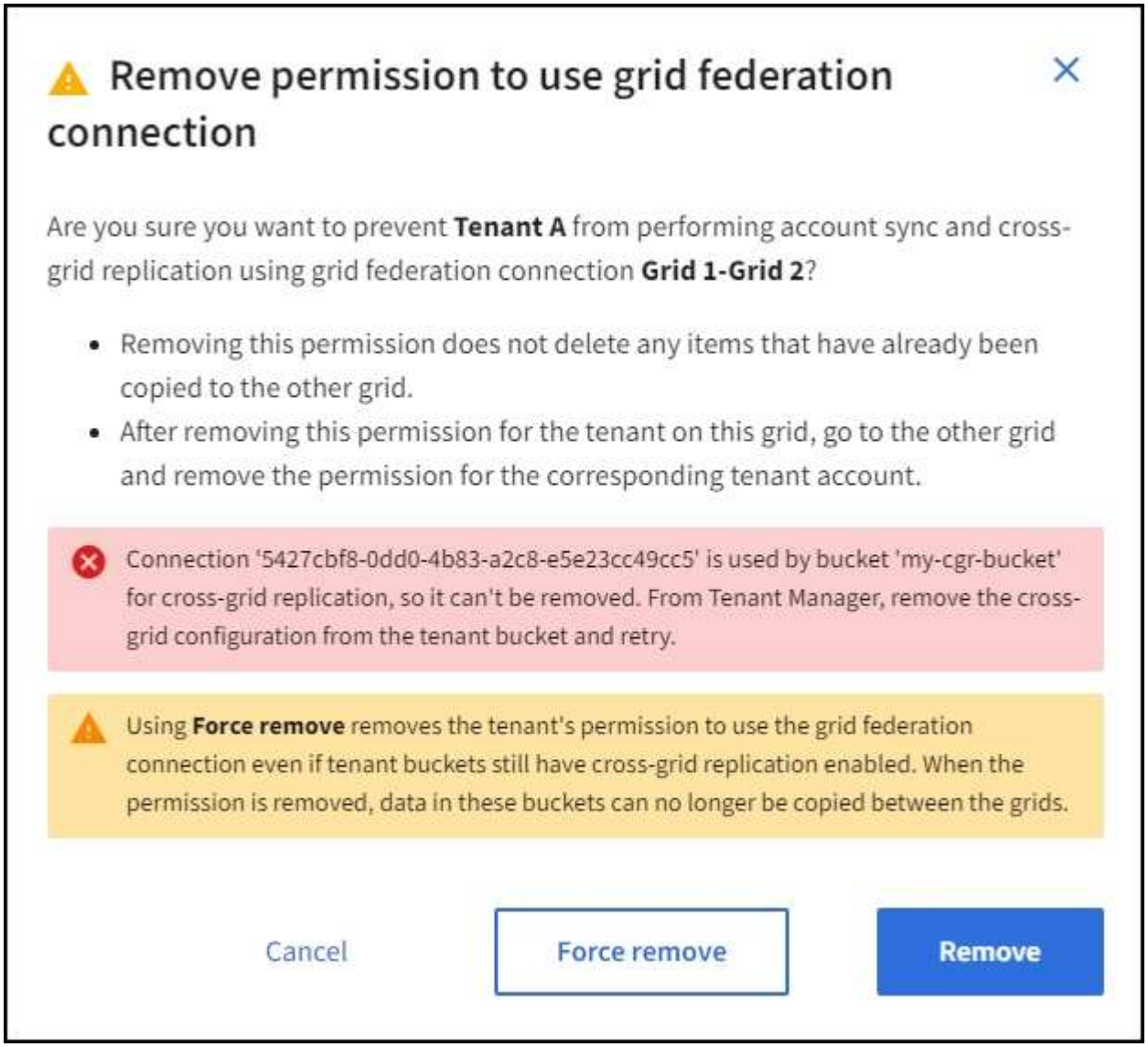
a. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
b. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
c. Nella scheda **tenant consentiti**, selezionare il pulsante di opzione corrispondente al tenant.
d. Selezionare **Rimuovi permesso**.

Pagina tenant

a. Selezionare **TENANT**.
b. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
c. Nella scheda **Grid Federation**, selezionare il pulsante di opzione per la connessione.
d. Selezionare **Rimuovi permesso**.

3. Esaminare gli avvisi nella finestra di dialogo di conferma e selezionare **Rimuovi**.
   - Se l'autorizzazione può essere rimossa, viene visualizzata nuovamente la pagina dei dettagli e viene visualizzato un messaggio di conferma. Questo tenant non può più utilizzare la connessione a federazione di grid.

◦ Se in uno o più bucket tenant è ancora attivata la replica cross-grid, viene visualizzato un errore.



È possibile effettuare una delle seguenti operazioni:

- (Consigliato). Accedere a Tenant Manager e disattivare la replica per ciascuno dei bucket del tenant. Vedere "Gestire la replica cross-grid". Quindi, ripetere la procedura per rimuovere l'autorizzazione **Usa connessione alla rete**.
- Rimuovere l'autorizzazione forzatamente. Vedere la sezione successiva.

4. Passare all'altra griglia e ripetere questa procedura per rimuovere l'autorizzazione per lo stesso tenant sull'altra griglia.

Rimuovi l'autorizzazione in base alla forza

Se necessario, è possibile forzare la rimozione dell'autorizzazione di un tenant per utilizzare una connessione a federazione di griglia anche se i bucket tenant hanno la replica cross-grid attivata.

Prima di rimuovere il permesso di un tenant per forza, prendere nota delle considerazioni generali per rimozione dell'autorizzazione oltre a queste considerazioni aggiuntive:

- Se si rimuove l'autorizzazione **Usa connessione federazione griglia** per forza, tutti gli oggetti che sono in attesa di replica nell'altra griglia (acquisiti ma non ancora replicati) continueranno a essere replicati. Per evitare che questi oggetti in-process raggiungano il bucket di destinazione, è necessario rimuovere anche l'autorizzazione del tenant sull'altra griglia.
- Qualsiasi oggetto acquisito nel bucket di origine dopo la rimozione dell'autorizzazione **Usa connessione federazione griglia** non verrà mai replicato nel bucket di destinazione.

Fasi

1. Accedere a Grid Manager dal nodo di amministrazione principale.
2. Selezionare **CONFIGURATION** > **System** > **Grid Federation**.
3. Selezionare il nome della connessione per visualizzarne la pagina dei dettagli.
4. Nella scheda **tenant consentiti**, selezionare il pulsante di opzione corrispondente al tenant.
5. Selezionare **Rimuovi permesso**.
6. Rivedere gli avvisi nella finestra di dialogo di conferma e selezionare **forza rimozione**.

   Viene visualizzato un messaggio di successo. Questo tenant non può più utilizzare la connessione a federazione di grid.

7. Se necessario, passare all'altra griglia e ripetere questa procedura per forzare la rimozione dell'autorizzazione per lo stesso account tenant sull'altra griglia. Ad esempio, è necessario ripetere questi passaggi sull'altra griglia per evitare che gli oggetti in-process raggiungano il bucket di destinazione.

Risolvere i problemi relativi agli errori di federazione della griglia

Potrebbe essere necessario risolvere gli avvisi e gli errori relativi alle connessioni di federazione di griglie, al clone dell'account e alla replica cross-grid.

Avvisi ed errori di connessione a Grid Federation

È possibile che si ricevano avvisi o si verifichino errori con le connessioni della federazione di griglie.

Dopo aver apportato qualsiasi modifica per risolvere un problema di connessione, verificare che lo stato della connessione torni a **connesso**. Per istruzioni, vedere "Gestire le connessioni a federazione di griglie".

Avviso di errore di connessione della federazione di griglie

Problema

È stato attivato l'avviso **errore di connessione federazione griglia**.

Dettagli

Questo avviso indica che la connessione a federazione di griglie tra le griglie non funziona.

Azioni consigliate

1. Esaminare le impostazioni della pagina Grid Federation per entrambe le griglie. Verificare che tutti i valori siano corretti. Vedere "Gestire le connessioni a federazione di griglie".
2. Esaminare i certificati utilizzati per la connessione. Assicurarsi che non ci siano avvisi per i certificati di federazione griglia scaduti e che i dettagli di ciascun certificato siano validi. Consultare le istruzioni per la rotazione dei certificati di connessione in "Gestire le connessioni a federazione di griglie".
3. Verificare che tutti i nodi Admin e Gateway in entrambe le griglie siano online e disponibili. Risolvere

eventuali avvisi che potrebbero interessare questi nodi e riprovare.

4. Se è stato fornito un nome di dominio completo (FQDN) per la griglia locale o remota, verificare che il server DNS sia in linea e disponibile. Vedere "Che cos'è la federazione di griglie?" Per i requisiti di rete, indirizzo IP e DNS.

Scadenza dell'avviso del certificato di federazione griglia

Problema

È stato attivato l'avviso **scadenza del certificato federazione griglia**.

Dettagli

Questo avviso indica che uno o più certificati di federazione griglia stanno per scadere.

Azioni consigliate

Consultare le istruzioni per la rotazione dei certificati di connessione in "Gestire le connessioni a federazione di griglie".

Errore durante la modifica di una connessione a federazione di griglie

Problema

Quando si modifica una connessione a federazione di griglie, viene visualizzato il seguente messaggio di avviso quando si seleziona **Salva e test**: "Impossibile creare un file di configurazione candidato su uno o più nodi."

Dettagli

Quando si modifica una connessione a federazione di griglie, StorageGRID tenta di salvare un file di "configurazione candidata" su tutti i nodi di amministrazione della prima griglia. Viene visualizzato un messaggio di avviso se il file non può essere salvato in tutti i nodi di amministrazione, ad esempio perché un nodo di amministrazione non è in linea.

Azioni consigliate

1. Dalla griglia utilizzata per modificare la connessione, selezionare **NODES** (NODI).
2. Verificare che tutti i nodi Admin per la griglia siano in linea.
3. Se alcuni nodi sono offline, ripristinarli online e provare a modificare nuovamente la connessione.

Errori di cloni dell'account

Impossibile accedere a un account tenant clonato

Problema

Impossibile accedere a un account tenant clonato. Il messaggio di errore nella pagina di accesso di Tenant Manager è "le credenziali per questo account non sono valide. Riprovare."

Dettagli

Per motivi di sicurezza, quando un account tenant viene clonato dalla griglia di origine del tenant alla griglia di destinazione del tenant, la password impostata per l'utente root locale del tenant non viene clonata. Allo stesso modo, quando un tenant crea utenti locali sulla griglia di origine, le password utente locali non vengono clonate nella griglia di destinazione.

Azioni consigliate

Prima che l'utente root possa accedere alla griglia di destinazione del tenant, un amministratore della griglia

deve prima "modificare la password per l'utente root locale" sulla griglia di destinazione.

Prima che un utente locale clonato possa accedere alla griglia di destinazione del tenant, l'utente root del tenant clonato deve aggiungere una password per l'utente nella griglia di destinazione. Per istruzioni, vedere "Gestire gli utenti locali" Nelle istruzioni per l'utilizzo di Tenant Manager.

Tenant creato senza un clone

Problema

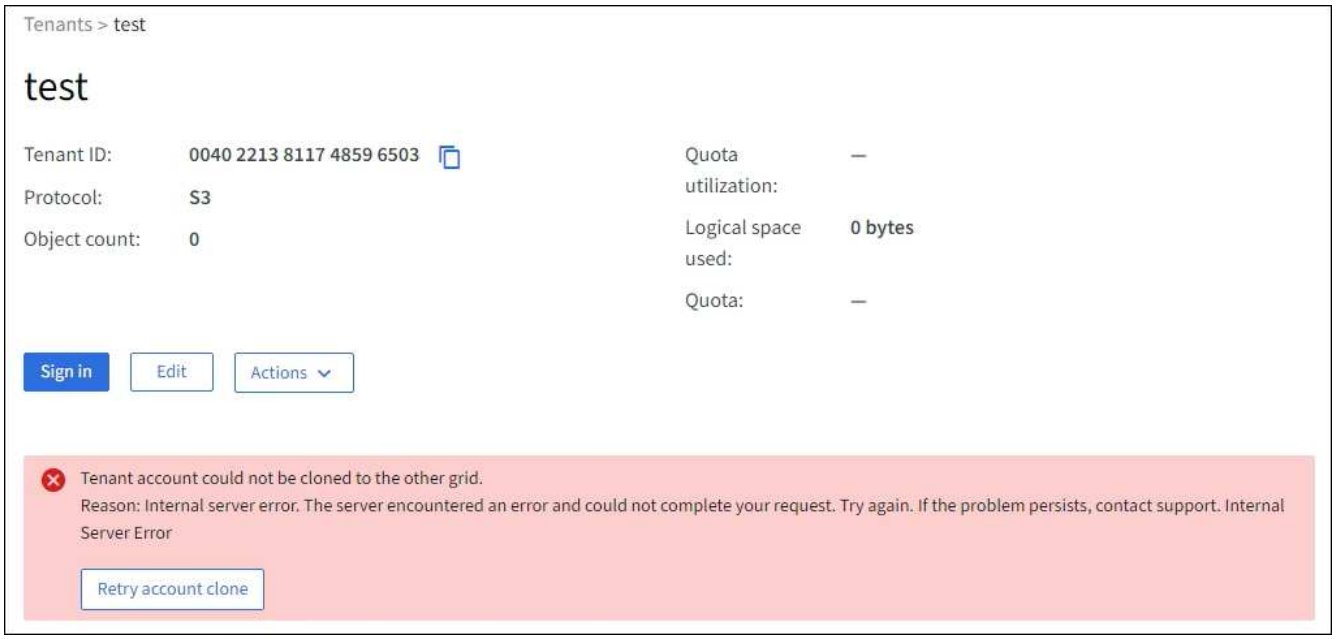
Viene visualizzato il messaggio "tenant creato senza clone" dopo aver creato un nuovo tenant con l'autorizzazione **Usa connessione federazione griglia**.

Dettagli

Questo problema può verificarsi se gli aggiornamenti allo stato della connessione vengono posticipati, causando l'elenco di una connessione non funzionante come **connessa**.

Azioni consigliate

1. Esaminare i motivi elencati nel messaggio di errore e risolvere eventuali problemi di rete o di altro tipo che potrebbero impedire il funzionamento della connessione. Vedere Avvisi ed errori di connessione Grid Federation.
2. Seguire le istruzioni per verificare la connessione a una federazione di griglie in "Gestire le connessioni a federazione di griglie" per confermare che il problema è stato risolto.
3. Dalla griglia di origine del tenant, selezionare **TENANT**.
4. Individuare l'account tenant che non è stato clonato.
5. Selezionare il nome del tenant per visualizzare la pagina dei dettagli.
6. Selezionare **Retry account clone**.



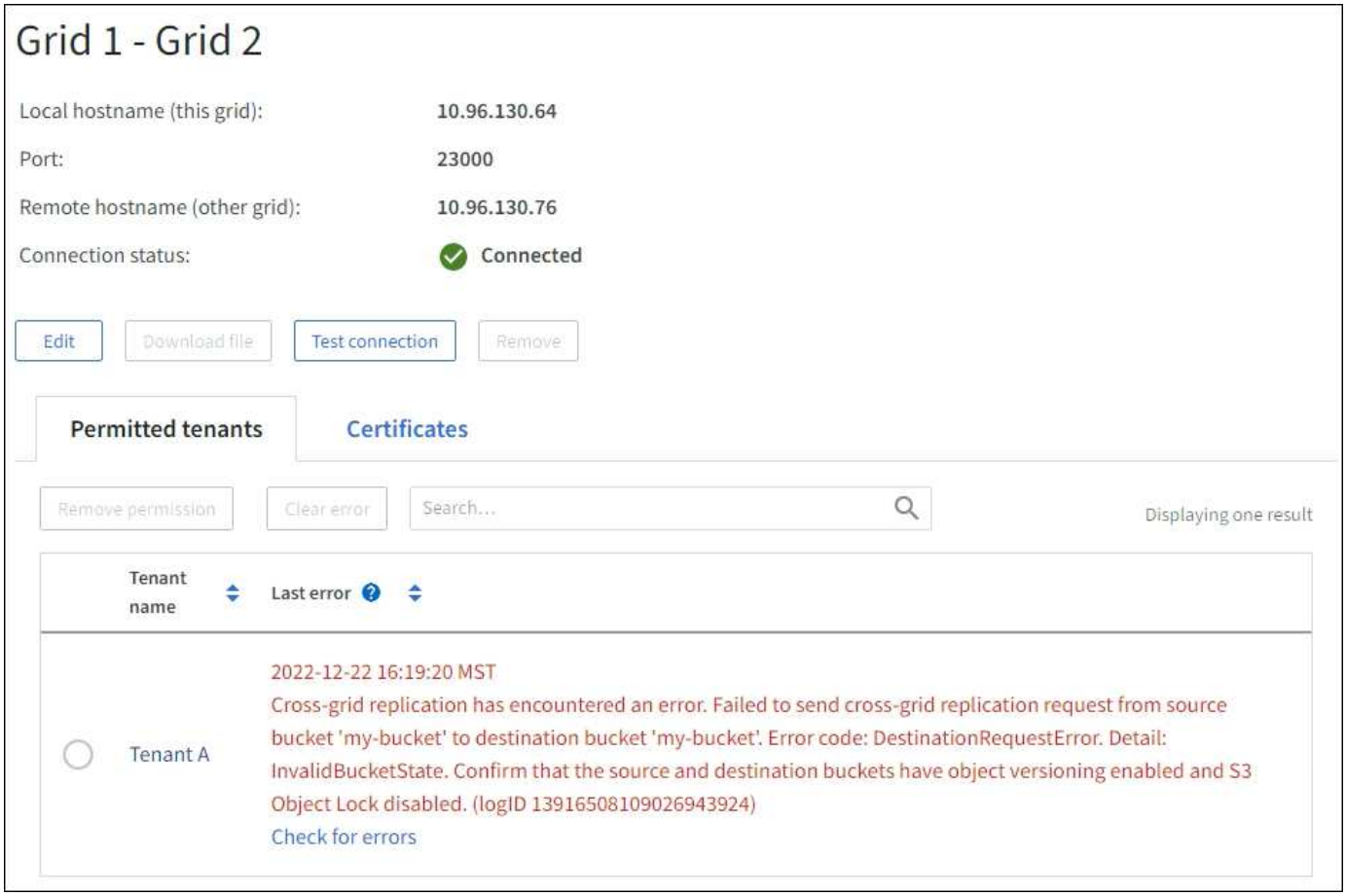
Se l'errore è stato risolto, l'account tenant verrà clonato nell'altra griglia.

Avvisi ed errori di replica cross-grid

Viene visualizzato l'ultimo errore per la connessione o il tenant

Problema

Quando "visualizzazione di una connessione a federazione di griglie" (o quando "gestione dei tenant consentiti" Per una connessione), si verifica un errore nella colonna **ultimo errore** della pagina dei dettagli di connessione. Ad esempio:



Dettagli

Per ogni connessione a federazione di griglie, la colonna **ultimo errore** mostra l'errore più recente che si verifica, se presente, quando i dati di un tenant venivano replicati nell'altro grid. In questa colonna viene visualizzato solo l'ultimo errore di replica tra griglie; gli errori precedenti che potrebbero essere stati rilevati non verranno visualizzati. In questa colonna potrebbe verificarsi un errore per uno dei seguenti motivi:

- Versione dell'oggetto di origine non trovata.
- Bucket di origine non trovato.
- Il bucket di destinazione è stato cancellato.
- Il bucket di destinazione è stato ricreato da un account diverso.
- Il bucket di destinazione ha la versione sospesa.
- Il bucket di destinazione è stato ricreato dallo stesso account, ma ora non è più disponibile.

Azioni consigliate

Se nella colonna **ultimo errore** viene visualizzato un messaggio di errore, attenersi alla seguente procedura:

1. Rivedere il testo del messaggio.

2. Eseguire le azioni consigliate. Ad esempio, se il controllo delle versioni è stato sospeso nel bucket di destinazione per la replica cross-grid, riabilitare il controllo delle versioni per quel bucket.
3. Selezionare la connessione o l'account tenant dalla tabella.
4. Selezionare **Cancella errore**.
5. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.
6. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.

   Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

   Dopo aver corretto l'errore, potrebbe essere visualizzato un nuovo **ultimo errore** se gli oggetti vengono acquisiti in un bucket diverso che presenta anche un errore.

7. Per determinare se non è stato possibile replicare oggetti a causa dell'errore del bucket, vedere "Identificare e riprovare le operazioni di replica non riuscite".

Avviso di errore permanente della replica cross-grid

Problema

È stato attivato l'avviso **errore permanente replica cross-grid**.

Dettagli

Questo avviso indica che gli oggetti tenant non possono essere replicati tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per la risoluzione. Questo avviso è generalmente causato da una modifica al bucket di origine o di destinazione.

Azioni consigliate

1. Accedere alla griglia in cui è stato attivato l'avviso.
2. Accedere a **CONFIGURATION** > **System** > **Grid Federation** e individuare il nome della connessione elencato nell'avviso.
3. Nella scheda Permitted tenant (tenant consentiti), esaminare la colonna **Last error** (ultimo errore) per determinare quali account tenant presentano errori.
4. Per ulteriori informazioni sull'errore, consultare le istruzioni in "Monitorare le connessioni a federazione di griglie" per rivedere le metriche di replica cross-grid.
5. Per ciascun account tenant interessato:
   a. Consultare le istruzioni in "Monitorare l'attività del tenant" per confermare che il tenant non ha superato la quota sulla griglia di destinazione per la replica cross-grid.
   b. Se necessario, aumentare la quota del tenant sulla griglia di destinazione per consentire il salvataggio di nuovi oggetti.
6. Per ogni tenant interessato, accedi a tenant Manager su entrambe le griglie, in modo da poter confrontare l'elenco dei bucket.
7. Per ogni bucket con replica cross-grid attivata, confermare quanto segue:
   - Esiste un bucket corrispondente per lo stesso tenant sull'altra griglia (deve utilizzare il nome esatto).
   - Entrambi i bucket hanno attivato la versione degli oggetti (la versione non può essere sospesa su nessuna griglia).

- Entrambi i bucket hanno S3 Object Lock disattivato.
- Nessuno dei due bucket si trova nello stato **Deleting Objects: Read-only**.

8. Per confermare che il problema è stato risolto, consultare le istruzioni in "Monitorare le connessioni a federazione di griglie" per rivedere le metriche di replica cross-grid o eseguire questi passaggi:

   a. Torna alla pagina Grid Federation.

   b. Selezionare il tenant interessato e selezionare **Cancella errore** nella colonna **ultimo errore**.

   c. Selezionare **Sì** per cancellare il messaggio e aggiornare lo stato del sistema.

   d. Attendere 5-6 minuti, quindi inserire un nuovo oggetto nel bucket. Verificare che il messaggio di errore non venga più visualizzato.

   > Per assicurarsi che il messaggio di errore venga cancellato, attendere almeno 5 minuti dopo l'indicazione dell'ora nel messaggio prima di acquisire un nuovo oggetto.

   > Una volta risolto, l'avviso potrebbe richiedere fino a un giorno.

   a. Passare a. "Identificare e riprovare le operazioni di replica non riuscite" per identificare gli oggetti o eliminare i marcatori che non sono riusciti a replicare nell'altra griglia e riprovare la replica secondo necessità.

Avviso di risorsa di replica cross-grid non disponibile

Problema

È stato attivato l'avviso **risorsa di replica cross-grid non disponibile**.

Dettagli

Questo avviso indica che le richieste di replica cross-grid sono in sospeso perché una risorsa non è disponibile. Ad esempio, potrebbe essere presente un errore di rete.

Azioni consigliate

1. Monitorare l'avviso per verificare se il problema si risolve da solo.
2. Se il problema persiste, determinare se una griglia presenta un avviso di errore di connessione * federazione griglia per la stessa connessione o un avviso di errore di comunicazione * con nodo * per un nodo. Questo avviso potrebbe essere risolto quando si risolvono tali avvisi.
3. Per ulteriori informazioni sull'errore, consultare le istruzioni in "Monitorare le connessioni a federazione di griglie" per rivedere le metriche di replica cross-grid.
4. Se non riesci a risolvere l'avviso, contatta il supporto tecnico.

La replica cross-grid procederà normalmente dopo la risoluzione del problema.

Identificare e riprovare le operazioni di replica non riuscite

Dopo aver risolto l'avviso **errore permanente replica cross-grid**, è necessario determinare se non è stato possibile replicare oggetti o marker di eliminazione nell'altra griglia. È quindi possibile recuperare questi oggetti o utilizzare l'API Grid Management per riprovare la replica.

L'avviso **errore permanente di replica cross-grid** indica che gli oggetti tenant non possono essere replicati

tra i bucket su due griglie per un motivo che richiede l'intervento dell'utente per la risoluzione. Questo avviso è generalmente causato da una modifica al bucket di origine o di destinazione. Per ulteriori informazioni, vedere "Risolvere i problemi relativi agli errori di federazione della griglia".

Determinare se non è stato possibile replicare oggetti

Per determinare se gli oggetti o i marker di eliminazione non sono stati replicati nell'altra griglia, è possibile eseguire una ricerca nel registro di controllo "CGRR (Cross-Grid Replication Request)" messaggi. Questo messaggio viene aggiunto al registro quando StorageGRID non riesce a replicare un oggetto, un oggetto multiparte o un indicatore di eliminazione nel bucket di destinazione.

È possibile utilizzare "tool di verifica-spiegazione" per tradurre i risultati in un formato più facile da leggere.

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- Hai il `Passwords.txt` file.
- Si conosce l'indirizzo IP del nodo di amministrazione primario.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Cercare i messaggi CGRR in audit.log e utilizzare lo strumento di spiegazione dell'audit per formattare i risultati.

   Ad esempio, questo comando si grep per tutti i messaggi CGRR negli ultimi 30 minuti e utilizza lo strumento audit-exclaring.

   ```
   # awk -vdate=$(date -d "30 minutes ago" '+%Y-%m-%dT%H:%M:%S') '$1$2 >= date { print }' audit.log | grep CGRR | audit-explain
   ```

Il risultato del comando sarà simile a questo esempio, che contiene voci per sei messaggi CGRR. Nell'esempio, tutte le richieste di replica cross-grid hanno restituito un errore generale perché non è stato possibile replicare l'oggetto. I primi tre errori riguardano le operazioni "Replicate Object", mentre gli ultimi tre errori riguardano le operazioni "Replicate delete marker".

```
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-0"
version:QjRBNDIzODAtNjQ3My0xMUVELTg2QjEtODJBMjAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
object" bucket:bucket123 object:"audit-3"
version:QjRDOTRCOUMtNjQ3My0xMUVELTkzM0YtOTg1MTAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-1"
version:NUQ0OEYxMDAtNjQ3NC0xMUVELTg2NjMtOTY5NzAwQkI3NEM4 error:general
error
CGRR Cross-Grid Replication Request tenant:50736445269627437748
connection:447896B6-6F9C-4FB2-95EA-AEBF93A774E9 operation:"replicate
delete marker" bucket:bucket123 object:"audit-5"
version:NUQ1ODUwQkUtNjQ3NC0xMUVELTg1NTItRDkwNzAwQkI3NEM4 error:general
error
```

Ciascuna voce contiene le seguenti informazioni:

Campo	Descrizione
Richiesta di replica CGRR Cross-Grid	Il nome della richiesta
tenant	ID account del tenant
connessione	L'ID della connessione a federazione di griglie
operazione	Il tipo di operazione di replica che si stava tentando di eseguire: • oggetto replicate • marker di eliminazione replicato • replica di un oggetto multiparte
bucket	Il nome del bucket
oggetto	Il nome dell'oggetto
versione	L'ID versione dell'oggetto

Campo	Descrizione
errore	Il tipo di errore. Se la replica cross-grid non riesce, l'errore è "General error" (errore generale).

Riprovare a eseguire repliche non riuscite

Dopo aver generato un elenco di oggetti e marker di eliminazione che non sono stati replicati nel bucket di destinazione e aver risolto i problemi sottostanti, è possibile riprovare la replica in due modi:

- Inserire ciascun oggetto nel bucket di origine.
- Utilizzare l'API privata Grid Management, come descritto.

Fasi

1. Nella parte superiore di Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.
2. Selezionare **Vai alla documentazione API privata**.

> Gli endpoint dell'API StorageGRID contrassegnati come "privati" sono soggetti a modifica senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Nella sezione **cross-grid-Replication-Advanced**, selezionare il seguente endpoint:

   `POST /private/cross-grid-replication-retry-failed`

4. Selezionare **Provalo**.
5. Nella casella di testo **body**, sostituire la voce di esempio per **versionID** con un ID di versione di audit.log che corrisponde a una richiesta di replica cross-grid non riuscita.

   Assicurarsi di conservare le virgolette doppie intorno alla stringa.

6. Selezionare **Esegui**.
7. Verificare che il codice di risposta del server sia **204**, a indicare che l'oggetto o il marker di eliminazione è stato contrassegnato come in sospeso per la replica cross-grid sull'altra griglia.

> In sospeso indica che la richiesta di replica cross-grid è stata aggiunta alla coda interna per l'elaborazione.

Monitorare i tentativi di replica

È necessario monitorare le operazioni di ripetizione della replica per assicurarsi che vengano completate.

> La replica di un oggetto o di un marker di eliminazione nell'altra griglia potrebbe richiedere diverse ore o più.

È possibile monitorare le operazioni di ripetizione in due modi:

- Utilizzare un S3 "HeadObject (oggetto intestazione)" oppure "GetObject" richiesta. La risposta include lo specifico StorageGRID `x-ntap-sg-cgr-replication-status` intestazione della risposta, che avrà uno dei seguenti valori:

Griglia	Stato della replica
Origine	• **SUCCESSO**: La replica è riuscita. • **PENDING**: L'oggetto non è stato ancora replicato. • **ERRORE**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.
Destinazione	**REPLICA**: L'oggetto è stato replicato dalla griglia di origine.

- Utilizzare l'API privata Grid Management, come descritto.

Fasi

1. Nella sezione **cross-grid-Replication-Advanced** della documentazione dell'API privata, selezionare il seguente endpoint:

   ```
   GET /private/cross-grid-replication-object-status/{id}
   ```

2. Selezionare **Provalo**.
3. Nella sezione Parameter (parametro), inserire l'ID versione utilizzato in `cross-grid-replication-retry-failed` richiesta.
4. Selezionare **Esegui**.
5. Verificare che il codice di risposta del server sia **200**.
6. Esaminare lo stato della replica, che sarà uno dei seguenti:
   - **PENDING**: L'oggetto non è stato ancora replicato.
   - **COMPLETATO**: La replica è riuscita.
   - **FAILED**: La replica non è riuscita con un errore permanente. Un utente deve risolvere l'errore.

Gestire la sicurezza

Gestione della sicurezza: Panoramica

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

Gestire la crittografia

StorageGRID offre diverse opzioni per la crittografia dei dati. Dovresti "esaminare i metodi di crittografia disponibili" per determinare quali soddisfano i tuoi requisiti di protezione dei dati.

Gestire i certificati

È possibile "configurare e gestire i certificati del server" Utilizzato per le connessioni HTTP o i certificati client utilizzati per autenticare un'identità client o utente nel server.

Configurare i server di gestione delle chiavi

Utilizzando un "server di gestione delle chiavi" Consente di proteggere i dati StorageGRID anche se

un'appliance viene rimossa dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.

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

Gestire le impostazioni del proxy

Se si utilizzano i servizi della piattaforma S3 o i Cloud Storage Pool, è possibile configurare un "server proxy di archiviazione" Tra i nodi di storage e gli endpoint S3 esterni. Se si inviano pacchetti AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un "admin proxy server (server proxy amministratore)" Tra nodi di amministrazione e supporto tecnico.

Firewall di controllo

Per migliorare la sicurezza del sistema, è possibile controllare l'accesso ai nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche in "firewall esterno". È inoltre possibile controllare l'accesso di rete a ciascun nodo configurandone l'accesso "firewall interno". È possibile impedire l'accesso a tutte le porte, ad eccezione di quelle necessarie per l'implementazione.

Esaminare i metodi di crittografia StorageGRID

StorageGRID offre diverse opzioni per la crittografia dei dati. È necessario esaminare i metodi disponibili per determinare quali metodi soddisfano i requisiti di protezione dei dati.

La tabella fornisce un riepilogo generale dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Server di gestione delle chiavi (KMS) in Grid Manager	Tu "configurare un server di gestione delle chiavi" Per il sito StorageGRID e. "abilitare la crittografia dei nodi per l'appliance". Quindi, un nodo appliance si connette al KMS per richiedere una chiave di crittografia a chiave (KEK). Questa chiave crittografa e decrta la chiave di crittografia dei dati (DEK) su ciascun volume.	Nodi appliance con **Node Encryption** attivato durante l'installazione. Tutti i dati dell'appliance sono protetti da perdite fisiche o rimozione dal data center. **Nota**: La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di archiviazione e le appliance di servizi.

Opzione di crittografia	Come funziona	Valido per
Pagina crittografia unità nel programma di installazione dell'appliance StorageGRID	Se l'appliance contiene unità che supportano la crittografia hardware, è possibile impostare una passphrase dell'unità durante l'installazione. Quando si imposta una passphrase di unità, è impossibile per chiunque recuperare dati validi dalle unità rimosse dal sistema, a meno che non conoscano la passphrase. Prima di iniziare l'installazione, andare a **Configure hardware** > **Drive Encryption** per impostare una passphrase di unità che si applica a tutte le unità gestite da StorageGRID con crittografia automatica in un nodo.	Appliance che contengono dischi con crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. La crittografia dei dischi non si applica ai dischi gestiti da SANtricity. Se hai un'appliance storage con dischi a crittografia automatica e controller SANtricity, puoi abilitare la sicurezza dei dischi in SANtricity.
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione di protezione dell'unità è attivata per l'appliance StorageGRID, è possibile utilizzare "Gestore di sistema di SANtricity" per creare e gestire la chiave di protezione. La chiave è necessaria per accedere ai dati sui dischi protetti.	Appliance storage con dischi FDE (Full Disk Encryption) o dischi a crittografia automatica. Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non è utilizzabile con alcune appliance di storage o con alcuna appliance di servizi.
Crittografia degli oggetti memorizzati	Attivare il "Crittografia degli oggetti memorizzati" In Grid Manager. Quando questa opzione è attivata, tutti i nuovi oggetti che non sono crittografati a livello di bucket o a livello di oggetto vengono crittografati durante l'acquisizione.	Dati S3 e Swift di recente acquisizione. Gli oggetti memorizzati esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati.
Crittografia bucket S3	Viene inviata una richiesta PutBucketEncryption per abilitare la crittografia per il bucket. Tutti i nuovi oggetti che non sono crittografati a livello di oggetto vengono crittografati durante l'acquisizione.	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per il bucket. Gli oggetti bucket esistenti non vengono crittografati. I metadati degli oggetti e altri dati sensibili non vengono crittografati. "Operazioni sui bucket"

Opzione di crittografia	Come funziona	Valido per
Crittografia a oggetti lato server (SSE) S3	Viene inviata una richiesta S3 per memorizzare un oggetto e includere `x-amz-server-side-encryption` intestazione della richiesta.	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. StorageGRID gestisce le chiavi. "Utilizzare la crittografia lato server"
Crittografia a oggetti S3 lato server con chiavi fornite dal cliente (SSE-C)	Viene inviata una richiesta S3 per memorizzare un oggetto e includere tre intestazioni di richiesta. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Solo i dati S3 degli oggetti acquisiti di recente. È necessario specificare la crittografia per l'oggetto. I metadati degli oggetti e altri dati sensibili non vengono crittografati. Le chiavi vengono gestite al di fuori di StorageGRID. "Utilizzare la crittografia lato server"
Crittografia di un volume esterno o di un datastore	Se la piattaforma di implementazione lo supporta, si utilizza un metodo di crittografia esterno a StorageGRID per crittografare un intero volume o datastore.	Tutti i dati degli oggetti, i metadati e i dati di configurazione del sistema, presupponendo che ogni volume o datastore sia crittografato. Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati.

Opzione di crittografia	Come funziona	Valido per
Crittografia degli oggetti al di fuori di StorageGRID	Si utilizza un metodo di crittografia esterno a StorageGRID per crittografare i dati degli oggetti e i metadati prima che vengano acquisiti in StorageGRID.	Solo dati a oggetti e metadati (i dati di configurazione del sistema non sono crittografati). Un metodo di crittografia esterno offre un controllo più rigoroso sugli algoritmi e sulle chiavi di crittografia. Può essere combinato con gli altri metodi elencati. "Amazon Simple Storage Service - Guida per gli sviluppatori: Protezione dei dati mediante crittografia lato client"

Utilizzare più metodi di crittografia

A seconda dei requisiti, è possibile utilizzare più metodi di crittografia alla volta. Ad esempio:

- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e utilizzare la funzionalità di sicurezza del disco in Gestione sistema di SANtricity per "crittografare due volte" i dati sui dischi con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e utilizzare l'opzione di crittografia degli oggetti memorizzati per crittografare tutti gli oggetti quando vengono acquisiti.

Se solo una piccola parte degli oggetti richiede la crittografia, prendere in considerazione il controllo della crittografia a livello di bucket o di singolo oggetto. L'abilitazione di più livelli di crittografia comporta un costo aggiuntivo per le performance.

Gestire i certificati

Gestione dei certificati di sicurezza: Panoramica

I certificati di sicurezza sono piccoli file di dati utilizzati per creare connessioni sicure e affidabili tra i componenti di StorageGRID e tra i componenti di StorageGRID e i sistemi esterni.

StorageGRID utilizza due tipi di certificati di sicurezza:

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

Quando un client si connette al server utilizzando HTTPS, il server risponde con il certificato del server, che contiene una chiave pubblica. Il client verifica questo certificato confrontando la firma del server con la firma sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione con il server utilizzando la stessa chiave pubblica.

StorageGRID funziona come server per alcune connessioni (come l'endpoint del bilanciamento del carico) o come client per altre connessioni (come il servizio di replica di CloudMirror).

Certificato Grid CA predefinito

StorageGRID include un'autorità di certificazione (CA) incorporata che genera un certificato Grid CA interno durante l'installazione del sistema. Il certificato Grid CA viene utilizzato, per impostazione predefinita, per proteggere il traffico StorageGRID interno. Un'autorità di certificazione esterna (CA) può emettere certificati personalizzati pienamente conformi ai criteri di sicurezza delle informazioni dell'organizzazione. Sebbene sia possibile utilizzare il certificato Grid CA per un ambiente non di produzione, la procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna. Sono supportate anche connessioni non protette senza certificato, ma non sono consigliate.

- I certificati CA personalizzati non rimuovono i certificati interni; tuttavia, i certificati personalizzati devono essere quelli specificati per la verifica delle connessioni al server.
- Tutti i certificati personalizzati devono soddisfare il "linee guida per la protezione avanzata del sistema per i certificati server".
- StorageGRID supporta il raggruppamento di certificati da una CA in un singolo file (noto come bundle di certificati CA).

> StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

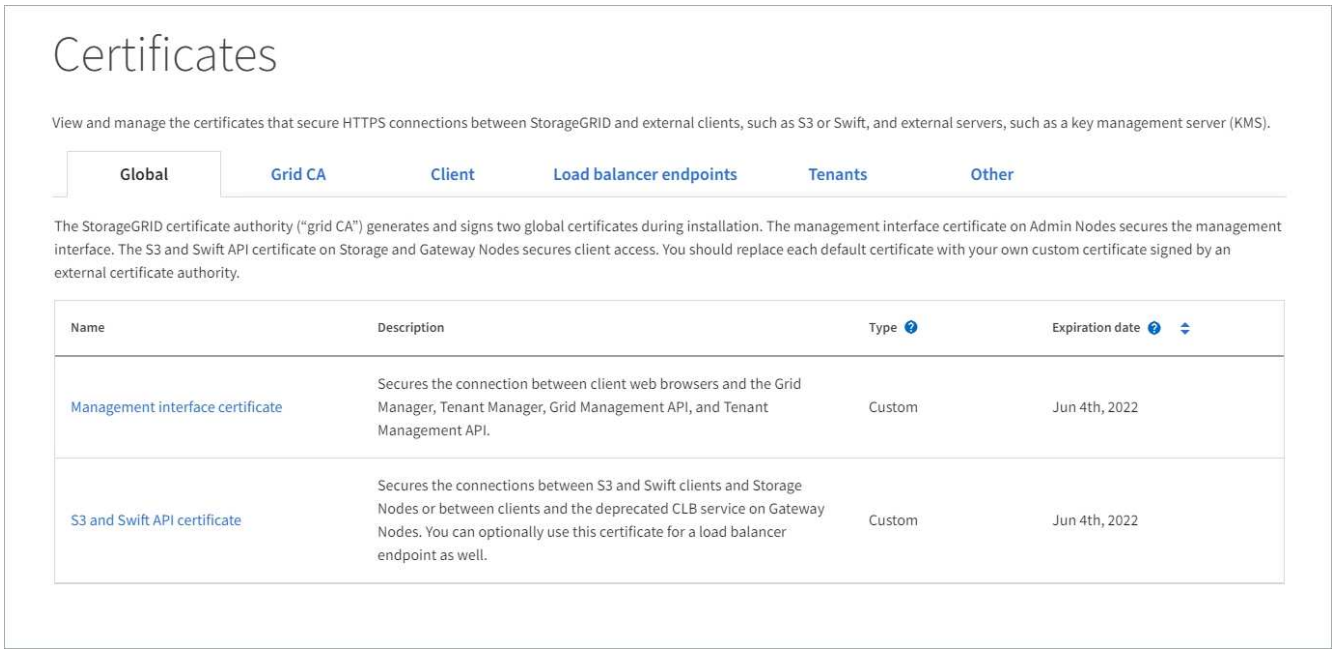
Le varianti dei tipi di certificato server e client vengono implementate in diversi modi. Prima di configurare il sistema, è necessario disporre di tutti i certificati necessari per la configurazione specifica di StorageGRID.

Accesso ai certificati di sicurezza

È possibile accedere alle informazioni su tutti i certificati StorageGRID in una singola posizione, insieme ai collegamenti al flusso di lavoro di configurazione per ciascun certificato.

Fasi

1. Da Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**.



2. Selezionare una scheda nella pagina certificati per informazioni su ciascuna categoria di certificati e per accedere alle impostazioni del certificato. È possibile accedere a una scheda se si dispone di "autorizzazione appropriata".

   - **Globale**: Protegge l'accesso a StorageGRID da browser Web e client API esterni.
   - **Grid CA**: Protegge il traffico StorageGRID interno.
   - **Client**: Protegge le connessioni tra client esterni e il database StorageGRID Prometheus.
   - **Endpoint del bilanciamento del carico**: Protegge le connessioni tra i client S3 e Swift e il bilanciamento del carico StorageGRID.
   - **Tenant**: Protegge le connessioni ai server di federazione delle identità o dagli endpoint dei servizi della piattaforma alle risorse di storage S3.
   - **Altro**: Protegge le connessioni StorageGRID che richiedono certificati specifici.

   Ciascuna scheda viene descritta di seguito con collegamenti a dettagli aggiuntivi del certificato.

Globale

I certificati globali proteggono l'accesso a StorageGRID dai browser Web e dai client API S3 e Swift esterni. Durante l'installazione, l'autorità di certificazione StorageGRID genera inizialmente due certificati globali. La procedura consigliata per un ambiente di produzione consiste nell'utilizzare certificati personalizzati firmati da un'autorità di certificazione esterna.

- Certificato dell'interfaccia di gestione: Protegge le connessioni del browser Web client alle interfacce di gestione StorageGRID.
- Certificato API S3 e Swift: Protegge le connessioni API del client ai nodi di storage, ai nodi di amministrazione e ai nodi gateway, utilizzati dalle applicazioni client S3 e Swift per caricare e scaricare i dati degli oggetti.

Le informazioni sui certificati globali installati includono:

- **Nome**: Nome del certificato con collegamento alla gestione del certificato.
- **Descrizione**
- **Type**: Personalizzato o predefinito.
  Per una migliore protezione della griglia, è sempre consigliabile utilizzare un certificato personalizzato.
- **Data di scadenza**: Se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

È possibile:

- Sostituire i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per una maggiore sicurezza della griglia:
  - "Sostituire il certificato predefinito dell'interfaccia di gestione generata da StorageGRID" Utilizzato per le connessioni di Grid Manager e Tenant Manager.
  - "Sostituire il certificato API S3 e Swift" Utilizzato per le connessioni endpoint (opzionali) del nodo di storage e del bilanciamento del carico.
- "Ripristinare il certificato dell'interfaccia di gestione predefinita."
- "Ripristinare il certificato API S3 e Swift predefinito."
- "Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione."
- Copiare o scaricare "certificato dell'interfaccia di gestione" oppure "Certificato API S3 e Swift".

CA griglia

Il Certificato Grid CA, Generata dall'autorità di certificazione StorageGRID durante l'installazione di StorageGRID, protegge tutto il traffico StorageGRID interno.

Le informazioni sul certificato includono la data di scadenza del certificato e il contenuto del certificato.

È possibile "Copia o scarica il certificato Grid CA", ma non è possibile modificarla.

Client

Certificati client, Generata da un'autorità di certificazione esterna, protegge le connessioni tra i tool di monitoraggio esterni e il database StorageGRID Prometheus.

La tabella dei certificati contiene una riga per ciascun certificato client configurato e indica se il certificato può essere utilizzato per l'accesso al database Prometheus, insieme alla data di scadenza del certificato.

È possibile:

- "Caricare o generare un nuovo certificato client."
- Selezionare il nome di un certificato per visualizzare i dettagli del certificato in cui è possibile:
  - "Modificare il nome del certificato client."
  - "Impostare l'autorizzazione di accesso Prometheus."
  - "Caricare e sostituire il certificato del client."
  - "Copiare o scaricare il certificato client."
  - "Rimuovere il certificato client."
- Selezionare **azioni** per eseguire rapidamente "modifica", "allega", o. "rimuovere" un certificato client. È possibile selezionare fino a 10 certificati client e rimuoverli contemporaneamente utilizzando **azioni** > **Rimuovi**.

Endpoint del bilanciamento del carico

Certificati endpoint per il bilanciamento del carico Proteggere le connessioni tra i client S3 e Swift e il servizio di bilanciamento del carico StorageGRID sui nodi gateway e sui nodi di amministrazione.

La tabella degli endpoint del bilanciamento del carico dispone di una riga per ciascun endpoint del bilanciamento del carico configurato e indica se per l'endpoint viene utilizzato il certificato API S3 e Swift globale o un certificato dell'endpoint del bilanciamento del carico personalizzato. Viene visualizzata anche la data di scadenza di ciascun certificato.

> ⓘ Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

È possibile:

- "Visualizzare un endpoint di bilanciamento del carico", inclusi i dettagli del certificato.
- "Specificare un certificato endpoint per il bilanciamento del carico per FabricPool."
- "Utilizza il certificato globale S3 e Swift API" invece di generare un nuovo certificato endpoint per il bilanciamento del carico.

Tenant

I tenant possono utilizzare certificati del server di federazione delle identità oppure certificati endpoint del servizio di piattaforma Per proteggere le connessioni con StorageGRID.

La tabella tenant ha una riga per ciascun tenant e indica se ciascun tenant dispone dell'autorizzazione per utilizzare la propria origine di identità o i propri servizi di piattaforma.

È possibile:

- "Selezionare il nome di un tenant per accedere al tenant manager"
- "Selezionare un nome tenant per visualizzare i dettagli della federazione delle identità del tenant"
- "Selezionare un nome tenant per visualizzare i dettagli dei servizi della piattaforma tenant"
- "Specificare un certificato endpoint del servizio di piattaforma durante la creazione dell'endpoint"

Altro

StorageGRID utilizza altri certificati di sicurezza per scopi specifici. Questi certificati sono elencati in base

al nome funzionale. Altri certificati di sicurezza includono:

- Certificati Cloud Storage Pool
- Certificati di notifica degli avvisi via email
- Certificati server syslog esterni
- Certificati di connessione Grid Federation
- Certificati di federazione delle identità
- Certificati KMS (Key Management Server)
- Certificati Single Sign-on

Le informazioni indicano il tipo di certificato utilizzato da una funzione e le relative date di scadenza del certificato server e client, a seconda dei casi. Selezionando il nome di una funzione si apre una scheda del browser in cui è possibile visualizzare e modificare i dettagli del certificato.

> ⓘ È possibile visualizzare e accedere alle informazioni relative ad altri certificati solo se si dispone di "autorizzazione appropriata".

È possibile:

- "Specificare un certificato Cloud Storage Pool per S3, C2S S3 o Azure"
- "Specificare un certificato per le notifiche e-mail di avviso"
- "Utilizzare un certificato per un server syslog esterno"
- "Ruotare i certificati di connessione Grid Federation"
- "Visualizzare e modificare un certificato di federazione delle identità"
- "Caricare i certificati del server e del client del server di gestione delle chiavi (KMS)"
- "Specificare manualmente un certificato SSO per un trust della parte che si basa"

Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti alle istruzioni di implementazione.

Certificato dell'interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management. È possibile utilizzare il certificato predefinito creato durante l'installazione o caricare un certificato personalizzato.	**CONFIGURATION** > **Security** > **Certificates**, selezionare la scheda **Global**, quindi selezionare **Management interface certificate**	"Configurare i certificati dell'interfaccia di gestione"

Certificato API S3 e Swift

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica le connessioni client sicure S3 o Swift a un nodo di storage e agli endpoint del bilanciamento del carico (opzionale).	**CONFIGURATION** > **Security** > **Certificates**, selezionare la scheda **Global**, quindi **S3 and Swift API certificate**	"Configurare i certificati API S3 e Swift"

Certificato Grid CA

Vedere Descrizione del certificato Grid CA predefinito.

Certificato del client di amministratore

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Client	Installato su ciascun client, consentendo a StorageGRID di autenticare l'accesso client esterno. • Consente ai client esterni autorizzati di accedere al database StorageGRID Prometheus. • Consente il monitoraggio sicuro di StorageGRID utilizzando strumenti esterni.	**CONFIGURAZIONE** > **sicurezza** > **certificati**, quindi selezionare la scheda **Client**	"Configurare i certificati client"

Certificato endpoint per il bilanciamento del carico

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i client S3 o Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway e sui nodi di amministrazione. È possibile caricare o generare un certificato di bilanciamento del carico quando si configura un endpoint di bilanciamento del carico. Le applicazioni client utilizzano il certificato di bilanciamento del carico durante la connessione a StorageGRID per salvare e recuperare i dati degli oggetti. È anche possibile utilizzare una versione personalizzata del Global Certificato API S3 e Swift Certificato per autenticare le connessioni al servizio Load Balancer. Se il certificato globale viene utilizzato per autenticare le connessioni del bilanciamento del carico, non è necessario caricare o generare un certificato separato per ciascun endpoint del bilanciamento del carico. **Nota:** il certificato utilizzato per l'autenticazione del bilanciamento del carico è il certificato più utilizzato durante il normale funzionamento StorageGRID.	**CONFIGURAZIONE** > **rete** > **endpoint del bilanciamento del carico**	• "Configurare gli endpoint del bilanciamento del carico" • "Creare un endpoint di bilanciamento del carico per FabricPool"

Certificato endpoint Cloud Storage Pool

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione da un pool di storage cloud StorageGRID a una posizione di storage esterna, ad esempio lo storage S3 Glacier o Microsoft Azure Blob. Per ogni tipo di cloud provider è necessario un certificato diverso.	**ILM** > **Storage Pools**	"Creare un pool di storage cloud"

Certificato di notifica degli avvisi via email

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi. • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione.	**ALERTS** > **email setup**	"Imposta le notifiche via email per gli avvisi"

Certificato server syslog esterno

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione TLS o RELP/TLS tra un server syslog esterno che registra gli eventi in StorageGRID. **Nota:** non è richiesto un certificato server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	**CONFIGURAZIONE** > **monitoraggio** > **Audit and syslog server**	"Utilizzare un server syslog esterno"

certificato di connessione Grid Federation

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autenticare e crittografare le informazioni inviate tra il sistema StorageGRID corrente e un'altra griglia in una connessione a federazione di griglie.	**CONFIGURAZIONE** > **sistema** > **federazione griglia**	• "Creare connessioni di federazione di griglie" • "Ruotare i certificati di connessione"

Certificato di federazione delle identità

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra StorageGRID e un provider di identità esterno, ad esempio Active Directory, OpenLDAP o Oracle Directory Server. Utilizzato per la federazione delle identità, che consente ai gruppi di amministrazione e agli utenti di essere gestiti da un sistema esterno.	**CONFIGURAZIONE** > **controllo accessi** > **federazione identità**	"USA la federazione delle identità"

Certificato del Key Management Server (KMS)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra StorageGRID e un KMS (Key Management Server) esterno, che fornisce chiavi di crittografia ai nodi appliance StorageGRID.	**CONFIGURAZIONE** > **sicurezza** > **Server di gestione delle chiavi**	"Aggiunta del server di gestione delle chiavi (KMS)"

Certificato endpoint dei servizi di piattaforma

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione dal servizio della piattaforma StorageGRID a una risorsa di storage S3.	**Tenant Manager** > **STORAGE (S3)** > **endpoint dei servizi della piattaforma**	"Creare endpoint di servizi di piattaforma" "Modifica dell'endpoint dei servizi della piattaforma"

Certificato SSO (Single Sign-on)

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i servizi di federazione delle identità, come ad FS (Active Directory Federation Services) e StorageGRID, utilizzati per le richieste SSO (Single Sign-on).	**CONFIGURAZIONE** > **controllo di accesso** > **Single Sign-on**	"Configurare il single sign-on"

Esempi di certificati

Esempio 1: Servizio di bilanciamento del carico

In questo esempio, StorageGRID agisce come server.

1. È possibile configurare un endpoint di bilanciamento del carico e caricare o generare un certificato server in StorageGRID.
2. È possibile configurare una connessione client S3 o Swift all'endpoint del bilanciamento del carico e caricare lo stesso certificato nel client.
3. Quando il client desidera salvare o recuperare i dati, si connette all'endpoint del bilanciamento del carico utilizzando HTTPS.
4. StorageGRID risponde con il certificato del server, che contiene una chiave pubblica, e con una firma basata sulla chiave privata.

5. Il client verifica questo certificato confrontando la firma del server con la firma sulla copia del certificato. Se le firme corrispondono, il client avvia una sessione utilizzando la stessa chiave pubblica.
6. Il client invia i dati dell'oggetto a StorageGRID.

Esempio 2: Server KMS (Key Management Server) esterno

In questo esempio, StorageGRID agisce come client.

1. Utilizzando il software del server di gestione delle chiavi esterno, è possibile configurare StorageGRID come client KMS e ottenere un certificato server con firma CA, un certificato client pubblico e la chiave privata per il certificato client.
2. Utilizzando Grid Manager, è possibile configurare un server KMS e caricare i certificati server e client e la chiave privata del client.
3. Quando un nodo StorageGRID necessita di una chiave di crittografia, effettua una richiesta al server KMS che include i dati del certificato e una firma basata sulla chiave privata.
4. Il server KMS convalida la firma del certificato e decide che può fidarsi di StorageGRID.
5. Il server KMS risponde utilizzando la connessione validata.

Configurare i certificati del server

Tipi di certificato server supportati

Il sistema StorageGRID supporta certificati personalizzati crittografati con RSA o ECDSA (algoritmo di firma digitale a curva ellittica).

> Il tipo di crittografia per il criterio di protezione deve corrispondere al tipo di certificato del server. Ad esempio, le crittografia RSA richiedono certificati RSA e le crittografia ECDSA richiedono certificati ECDSA. Vedere "Gestire i certificati di sicurezza". Se si configura un criterio di protezione personalizzato non compatibile con il certificato del server, è possibile "ripristinare temporaneamente il criterio di protezione predefinito".

Per ulteriori informazioni su come StorageGRID protegge le connessioni client, vedere "Sicurezza per client S3 e Swift".

Configurare i certificati dell'interfaccia di gestione

È possibile sostituire il certificato dell'interfaccia di gestione predefinita con un singolo certificato personalizzato che consente agli utenti di accedere a Grid Manager e a Tenant Manager senza incontrare avvisi di sicurezza. È inoltre possibile ripristinare il certificato dell'interfaccia di gestione predefinita o generarne uno nuovo.

A proposito di questa attività

Per impostazione predefinita, ogni nodo amministrativo riceve un certificato firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato dell'interfaccia di gestione personalizzata comune e dalla chiave privata corrispondente.

Poiché per tutti i nodi di amministrazione viene utilizzato un singolo certificato di interfaccia di gestione personalizzata, è necessario specificare il certificato come carattere jolly o certificato multidominio se i client devono verificare il nome host durante la connessione a Grid Manager e Tenant Manager. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi Admin nella griglia.

È necessario completare la configurazione sul server e, a seconda dell'autorità di certificazione principale (CA) utilizzata, gli utenti potrebbero dover installare il certificato Grid CA nel browser Web che utilizzeranno per accedere a Grid Manager e a Tenant Manager.

Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza del certificato del server per l'interfaccia di gestione** viene attivato quando il certificato del server sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE** > **sicurezza** > **certificati** e osservando la data di scadenza del certificato dell'interfaccia di gestione nella scheda Globale.

Se si accede a Grid Manager o Tenant Manager utilizzando un nome di dominio invece di un indirizzo IP, il browser mostra un errore di certificato senza l'opzione di ignorare se si verifica una delle seguenti condizioni:

- Il certificato dell'interfaccia di gestione personalizzata scade.
- Tu ripristinare da un certificato dell'interfaccia di gestione personalizzata al certificato server predefinito.

Aggiungere un certificato di interfaccia di gestione personalizzata

Per aggiungere un certificato di interfaccia di gestione personalizzato, è possibile fornire un certificato personalizzato o generarne uno utilizzando Grid Manager.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

> Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere 2048 bit o superiori.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Salva**.
Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

Generare un certificato

Generare i file dei certificati del server.

> La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato dell'interfaccia di gestione personalizzata firmato da un'autorità di certificazione esterna.

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.

Campo	Descrizione
IP	Uno o più indirizzi IP da includere nel certificato.
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.
Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o Tenant Manager API.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

> Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Dopo aver aggiunto un certificato dell'interfaccia di gestione personalizzata, la pagina del certificato dell'interfaccia di gestione visualizza informazioni dettagliate sul certificato per i certificati in uso.
È possibile scaricare o copiare il certificato PEM come richiesto.

Ripristinare il certificato dell'interfaccia di gestione predefinita

È possibile ripristinare l'utilizzo del certificato dell'interfaccia di gestione predefinita per Grid Manager e Tenant Manager Connections.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato predefinito**.

   Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato predefinito dell'interfaccia di gestione viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione

Se è richiesta una convalida rigorosa del nome host, è possibile utilizzare uno script per generare il certificato dell'interfaccia di gestione.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai il `Passwords.txt` file.

A proposito di questa attività

La procedura consigliata per un ambiente di produzione consiste nell'utilizzare un certificato firmato da un'autorità di certificazione esterna.

Fasi

1. Ottenere il nome di dominio completo (FQDN) di ciascun nodo di amministrazione.
2. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

3. Configurare StorageGRID con un nuovo certificato autofirmato.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Per `--domains`, Utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi di amministrazione. Ad esempio, `*.ui.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `admin1.ui.storagegrid.example.com` e. `admin2.ui.storagegrid.example.com`.
   - Impostare `--type` a. `management` Per configurare il certificato dell'interfaccia di gestione, utilizzato da Grid Manager e Tenant Manager.

◦ Per impostazione predefinita, i certificati generati sono validi per un anno (365 giorni) e devono essere ricreati prima della scadenza. È possibile utilizzare `--days` argomento per eseguire l'override del periodo di validità predefinito.

> Il periodo di validità di un certificato inizia quando `make-certificate` è eseguito. È necessario assicurarsi che il client di gestione sia sincronizzato con la stessa origine temporale di StorageGRID; in caso contrario, il client potrebbe rifiutare il certificato.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

L'output risultante contiene il certificato pubblico necessario al client API di gestione.

4. Selezionare e copiare il certificato.

   Includere i tag BEGIN e END nella selezione.

5. Disconnettersi dalla shell dei comandi. `$ exit`
6. Verificare che il certificato sia stato configurato:
   a. Accedere a Grid Manager.
   b. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**
   c. Nella scheda **Global**, selezionare **Management interface certificate**.
7. Configurare il client di gestione in modo che utilizzi il certificato pubblico copiato. Includere i tag inizio e FINE.

Scaricare o copiare il certificato dell'interfaccia di gestione

È possibile salvare o copiare il contenuto del certificato dell'interfaccia di gestione per utilizzarlo altrove.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scaricare il file di certificato o il bundle CA

Scarica il certificato o il bundle CA `.pem` file. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato** o **Scarica bundle CA**.

   Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

   Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati API S3 e Swift

È possibile sostituire o ripristinare il certificato server utilizzato per le connessioni client S3 o Swift ai nodi di storage o agli endpoint del bilanciamento del carico. Il certificato del server personalizzato sostitutivo è specifico dell'organizzazione.

A proposito di questa attività

Per impostazione predefinita, ogni nodo di storage viene emesso un certificato server X.509 firmato dalla CA della griglia. Questi certificati firmati dalla CA possono essere sostituiti da un singolo certificato server personalizzato comune e dalla chiave privata corrispondente.

Per tutti i nodi di storage viene utilizzato un singolo certificato server personalizzato, pertanto è necessario specificare il certificato come certificato wildcard o multi-dominio se i client devono verificare il nome host durante la connessione all'endpoint di storage. Definire il certificato personalizzato in modo che corrisponda a tutti i nodi di storage nella griglia.

Una volta completata la configurazione sul server, potrebbe essere necessario installare anche il certificato Grid CA nel client S3 o Swift API che verrà utilizzato per accedere al sistema, a seconda dell'autorità di certificazione (CA) root in uso.

Per garantire che le operazioni non vengano interrotte da un certificato server guasto, l'avviso **scadenza del certificato server globale per S3 e Swift API** viene attivato quando il certificato del server root sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE** > **sicurezza** > **certificati** e osservando la data di scadenza del certificato API S3 e Swift nella scheda Globale.

È possibile caricare o generare un certificato S3 e Swift API personalizzato.

Aggiungere un certificato API S3 e Swift personalizzato

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare **Usa certificato personalizzato**.
4. Caricare o generare il certificato.

Carica certificato

Caricare i file dei certificati del server richiesti.

a. Selezionare **carica certificato**.
b. Caricare i file dei certificati del server richiesti:
   - **Server certificate**: Il file di certificato del server personalizzato (con codifica PEM).
   - **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

     > Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere 2048 bit o superiori.

   - **Bundle CA**: Un singolo file opzionale contenente i certificati di ciascuna autorità di certificazione di emissione intermedia. Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.
c. Selezionare i dettagli del certificato per visualizzare i metadati e il PEM per ogni certificato S3 e Swift API personalizzato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.
   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.
d. Selezionare **Salva**.

   Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3 e Swift.

Generare un certificato

Generare i file dei certificati del server.

a. Selezionare **genera certificato**.
b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati e il PEM per il certificato S3 e Swift API personalizzato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**.

   Il certificato server personalizzato viene utilizzato per le successive nuove connessioni client S3 e Swift.

5. Selezionare una scheda per visualizzare i metadati per il certificato del server StorageGRID predefinito, un certificato CA firmato caricato o un certificato personalizzato generato.

   Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

7. Dopo aver aggiunto un certificato API S3 e Swift personalizzato, la pagina del certificato API S3 e Swift visualizza informazioni dettagliate sul certificato per il certificato API S3 e Swift personalizzato in uso.

È possibile scaricare o copiare il certificato PEM come richiesto.

Ripristinare il certificato API S3 e Swift predefinito

È possibile ripristinare l'utilizzo del certificato API S3 e Swift predefinito per le connessioni dei client S3 e Swift ai nodi di storage. Tuttavia, non è possibile utilizzare il certificato S3 e Swift API predefinito per un endpoint di bilanciamento del carico.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare **Usa certificato predefinito**.

   Quando si ripristina la versione predefinita del certificato globale S3 e Swift API, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato API S3 e Swift predefinito verrà utilizzato per le successive nuove connessioni dei client S3 e Swift ai nodi di storage.

4. Selezionare **OK** per confermare l'avviso e ripristinare il certificato S3 e Swift API predefinito.

   Se si dispone dell'autorizzazione di accesso Root ed è stato utilizzato il certificato S3 e Swift API personalizzato per le connessioni degli endpoint del bilanciamento del carico, viene visualizzato un elenco degli endpoint del bilanciamento del carico che non saranno più accessibili utilizzando il certificato S3 e Swift API predefinito. Passare a. "Configurare gli endpoint del bilanciamento del carico" per modificare o rimuovere gli endpoint interessati.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Scaricare o copiare il certificato API S3 e Swift

È possibile salvare o copiare i contenuti dei certificati API S3 e Swift per utilizzarli altrove.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **certificati**.
2. Nella scheda **Global**, selezionare **S3 and Swift API certificate**.
3. Selezionare la scheda **Server** o **bundle CA**, quindi scaricare o copiare il certificato.

Scaricare il file di certificato o il bundle CA

Scarica il certificato o il bundle CA `.pem` file. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Scarica certificato** o **Scarica bundle CA**.

   Se si sta scaricando un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono scaricati come un singolo file.

b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato o pacchetto CA PEM

Copiare il testo del certificato per incollarlo altrove. Se si utilizza un bundle CA opzionale, ciascun certificato del bundle viene visualizzato nella propria sottoscheda.

a. Selezionare **Copy certificate PEM** or **Copy CA bundle PEM**.

   Se si copia un bundle CA, tutti i certificati contenuti nelle schede secondarie del bundle CA vengono copiati insieme.

b. Incollare il certificato copiato in un editor di testo.

c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Utilizzare l'API REST di Swift"
- "Configurare i nomi di dominio degli endpoint S3"

Copiare il certificato Grid CA

StorageGRID utilizza un'autorità di certificazione interna (CA) per proteggere il traffico interno. Questo certificato non cambia se si caricano i propri certificati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Grid CA**.
2. Nella sezione **Certificate PEM**, scaricare o copiare il certificato.

Scaricare il file del certificato

Scarica il certificato `.pem` file.

a. Selezionare **Scarica certificato**.
b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato PEM

Copiare il testo del certificato per incollarlo altrove.

a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
b. Incollare il certificato copiato in un editor di testo.
c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Configurare i certificati StorageGRID per FabricPool

Per i client S3 che eseguono una convalida rigorosa del nome host e non supportano la disattivazione della convalida rigorosa del nome host, ad esempio i client ONTAP che utilizzano FabricPool, è possibile generare o caricare un certificato server quando si configura l'endpoint del bilanciamento del carico.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

Quando si crea un endpoint di bilanciamento del carico, è possibile generare un certificato server autofirmato o caricare un certificato firmato da un'autorità di certificazione (CA) nota. Negli ambienti di produzione, è necessario utilizzare un certificato firmato da una CA nota. I certificati firmati da una CA possono essere ruotati senza interruzioni. Sono inoltre più sicuri perché offrono una migliore protezione contro gli attacchi man-in-the-middle.

La procedura riportata di seguito fornisce linee guida generali per i client S3 che utilizzano FabricPool. Per informazioni e procedure più dettagliate, vedere "Configurare StorageGRID per FabricPool".

Fasi

1. Facoltativamente, configurare un gruppo ad alta disponibilità (ha) da utilizzare per FabricPool.
2. Creare un endpoint di bilanciamento del carico S3 da utilizzare per FabricPool.

Quando si crea un endpoint di bilanciamento del carico HTTPS, viene richiesto di caricare il certificato del server, la chiave privata del certificato e il bundle CA opzionale.

3. Collega StorageGRID come Tier cloud in ONTAP.

   Specificare la porta endpoint del bilanciamento del carico e il nome di dominio completo utilizzato nel certificato CA caricato. Quindi, fornire il certificato CA.

   Se una CA intermedia ha emesso il certificato StorageGRID, è necessario fornire il certificato CA intermedio. Se il certificato StorageGRID è stato emesso direttamente dalla CA principale, è necessario fornire il certificato della CA principale.

Configurare i certificati client

I certificati client consentono ai client esterni autorizzati di accedere al database StorageGRID Prometheus, fornendo un modo sicuro per i tool esterni di monitorare StorageGRID.

Se si desidera accedere a StorageGRID utilizzando uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client utilizzando Grid Manager e copiare le informazioni del certificato nello strumento esterno.

Vedere "Gestire i certificati di sicurezza" e. "Configurare certificati server personalizzati".

Per garantire che le operazioni non vengano interrotte da un certificato del server guasto, l'avviso **scadenza dei certificati client configurati nella pagina certificati** viene attivato quando il certificato del server sta per scadere. Se necessario, è possibile visualizzare la scadenza del certificato corrente selezionando **CONFIGURAZIONE** > **sicurezza** > **certificati** e osservando la data di scadenza del certificato client nella scheda Client.

Se si utilizza un server di gestione delle chiavi (KMS) per proteggere i dati su nodi appliance appositamente configurati, consultare le informazioni specifiche su "Caricamento di un certificato del client KMS".

Prima di iniziare

- Si dispone dell'autorizzazione di accesso root.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Per configurare un certificato client:
  - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
  - Se è stato configurato il certificato dell'interfaccia di gestione StorageGRID, si dispone della CA, del certificato client e della chiave privata utilizzati per configurare il certificato dell'interfaccia di gestione.
  - Per caricare il certificato, la chiave privata del certificato è disponibile sul computer locale.
  - La chiave privata deve essere stata salvata o registrata al momento della creazione. Se non si dispone della chiave privata originale, è necessario crearne una nuova.
- Per modificare un certificato client:
  - Si dispone dell'indirizzo IP o del nome di dominio del nodo di amministrazione.
  - Per caricare il proprio certificato o un nuovo certificato, la chiave privata, il certificato client e la CA (se utilizzata) sono disponibili sul computer locale.

Aggiungere certificati client

Per aggiungere il certificato client, attenersi a una delle seguenti procedure:

- Certificato dell'interfaccia di gestione già configurato
- CERTIFICATO client emesso DALLA CA
- Certificato generato da Grid Manager

Certificato dell'interfaccia di gestione già configurato

Utilizzare questa procedura per aggiungere un certificato client se un certificato dell'interfaccia di gestione è già configurato utilizzando una CA, un certificato client e una chiave privata forniti dal cliente.

Fasi

1. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, caricare il certificato dell'interfaccia di gestione.
   a. Selezionare **carica certificato**.
   b. Selezionare **Sfoglia** e selezionare il file di certificato dell'interfaccia di gestione (`.pem`).
      - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
   c. Selezionare **Crea** per salvare il certificato in Grid Manager.

      Il nuovo certificato viene visualizzato nella scheda Client.
7. Configurare uno strumento di monitoraggio esterno, Come Grafana.

CERTIFICATO client emesso DALLA CA

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza un certificato client emesso dalla CA e una chiave privata.

Fasi

1. Eseguire i passi da a. "configurare un certificato dell'interfaccia di gestione".
2. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
3. Selezionare **Aggiungi**.
4. Immettere un nome per il certificato.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare

Allow prometheus (Consenti prometheus).

6. Selezionare **continua**.
7. Per il passo **Allega certificati**, caricare i file di certificato client, chiave privata e bundle CA:
   a. Selezionare **carica certificato**.
   b. Selezionare **Sfoglia** e selezionare i file di certificato client, chiave privata e bundle CA (`.pem`).
      - Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.
      - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
   c. Selezionare **Crea** per salvare il certificato in Grid Manager.

      I nuovi certificati vengono visualizzati nella scheda Client.
8. Configurare uno strumento di monitoraggio esterno, Come Grafana.

Certificato generato da Grid Manager

Utilizzare questa procedura per aggiungere un certificato client amministratore se non è stato configurato un certificato dell'interfaccia di gestione e si intende aggiungere un certificato client per Prometheus che utilizza la funzione di generazione del certificato in Grid Manager.

Fasi

1. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare **Aggiungi**.
3. Immettere un nome per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
5. Selezionare **continua**.
6. Per il passo **Allega certificati**, selezionare **genera certificato**.
7. Specificare le informazioni del certificato:
   - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
   - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

     Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.
8. Selezionare **generate**.
9. selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

- Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

  Specificare il nome del file della chiave privata e la posizione di download.

10. Selezionare **Crea** per salvare il certificato in Grid Manager.

    Il nuovo certificato viene visualizzato nella scheda Client.

11. In Grid Manager, selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Global**.
12. Selezionare **certificato interfaccia di gestione**.
13. Selezionare **Usa certificato personalizzato**.
14. Caricare i file certificate.pem e private_key.pem da dettagli del certificato del client fase. Non è necessario caricare il bundle CA.
    a. Selezionare **carica certificato**, quindi selezionare **continua**.
    b. Caricare ciascun file di certificato (`.pem`).
    c. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.

       Il nuovo certificato viene visualizzato nella pagina Management Interface certificate (certificato interfaccia di gestione).

15. Configurare uno strumento di monitoraggio esterno, Come Grafana.

Configura uno strumento di monitoraggio esterno

Fasi

1. Configurare le seguenti impostazioni sullo strumento di monitoraggio esterno, ad esempio Grafana.
   a. **Nome**: Immettere un nome per la connessione.

      StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per verificare la connessione.

   b. **URL**: Immettere il nome di dominio o l'indirizzo IP per il nodo di amministrazione. Specificare HTTPS e la porta 9091.

      Ad esempio: `https://admin-node.example.com:9091`

c. Abilitare **TLS Client Auth** e **con CA Certate**.

d. In TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL), copiare e incollare:

   - Il certificato CA dell'interfaccia di gestione a **CA Cert**
   - Il certificato del client a **Client Cert**
   - La chiave privata per **chiave client**

e. **ServerName**: Immettere il nome di dominio del nodo di amministrazione.

   Il nome server deve corrispondere al nome di dominio così come appare nel certificato dell'interfaccia di gestione.

2. Salvare e verificare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

   Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo tool di monitoraggio esterno.

   Per informazioni sulle metriche, vedere "Istruzioni per il monitoraggio di StorageGRID".

Modificare i certificati client

È possibile modificare un certificato client amministratore per modificarne il nome, abilitare o disabilitare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.

   Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.
3. Selezionare **Modifica**, quindi selezionare **Modifica nome e permesso**
4. Immettere un nome per il certificato.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow prometheus** (Consenti prometheus).
6. Selezionare **continua** per salvare il certificato in Grid Manager.

   Il certificato aggiornato viene visualizzato nella scheda Client.

Allegare un nuovo certificato client

È possibile caricare un nuovo certificato una volta scaduto il certificato corrente.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.

   Le date di scadenza del certificato e le autorizzazioni di accesso Prometheus sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

2. Selezionare il certificato che si desidera modificare.

3. Selezionare **Edit** (Modifica), quindi un’opzione di modifica.

Carica certificato

Copiare il testo del certificato per incollarlo altrove.

a. Selezionare **carica certificato**, quindi selezionare **continua**.
b. Caricare il nome del certificato client (`.pem`).

   Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
c. Selezionare **Crea** per salvare il certificato in Grid Manager.

   Il certificato aggiornato viene visualizzato nella scheda Client.

Generare un certificato

Generare il testo del certificato da incollare altrove.

a. Selezionare **genera certificato**.
b. Specificare le informazioni del certificato:

   - **Oggetto** (opzionale): Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Il numero di giorni in cui il certificato generato è valido, a partire dal momento in cui viene generato.
   - **Add key usage Extensions** (Aggiungi estensioni utilizzo chiave): Se selezionata (impostazione predefinita e consigliata), l'utilizzo della chiave e le estensioni estese dell'utilizzo della chiave vengono aggiunte al certificato generato.

     Queste estensioni definiscono lo scopo della chiave contenuta nel certificato.

     Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.
c. Selezionare **generate**.
d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del

certificato e incollarlo altrove.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

  Specificare il nome del file della chiave privata e la posizione di download.

e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scaricare o copiare i certificati client

È possibile scaricare o copiare un certificato client da utilizzare altrove.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera copiare o scaricare.
3. Scaricare o copiare il certificato.

Scaricare il file del certificato

Scarica il certificato `.pem` file.

a. Selezionare **Scarica certificato**.
b. Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Copia certificato

Copiare il testo del certificato per incollarlo altrove.

a. Selezionare **Copy certificate PEM** (Copia certificato PEM).
b. Incollare il certificato copiato in un editor di testo.
c. Salvare il file di testo con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

Rimuovere i certificati client

Se non è più necessario un certificato client amministratore, è possibile rimuoverlo.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Certificates**, quindi selezionare la scheda **Client**.
2. Selezionare il certificato che si desidera rimuovere.
3. Selezionare **Delete** (Elimina), quindi confermare.

> Per rimuovere fino a 10 certificati, selezionare ciascun certificato da rimuovere nella scheda Client, quindi selezionare **azioni** > **Elimina**.

Dopo la rimozione di un certificato, i client che hanno utilizzato il certificato devono specificare un nuovo certificato client per accedere al database StorageGRID Prometheus.

Configurare le impostazioni di sicurezza

Gestire i criteri TLS e SSH

I criteri TLS e SSH determinano i protocolli e le crittografia utilizzati per stabilire connessioni TLS sicure con le applicazioni client e connessioni SSH sicure ai servizi StorageGRID interni.

Il criterio di sicurezza controlla il modo in cui TLS e SSH crittografano i dati in movimento. In generale, utilizzare il criterio di compatibilità moderno (predefinito), a meno che il sistema non debba essere conforme ai criteri comuni o non sia necessario utilizzare altre crittografia.

> Alcuni servizi StorageGRID non sono stati aggiornati per utilizzare le crittografia di questi criteri.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Selezionare una policy di sicurezza

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.

   La scheda **TLS and SSH policies** (Criteri TLS e SSH) mostra i criteri disponibili. Il criterio attualmente attivo è contrassegnato da un segno di spunta verde sul riquadro del criterio.

2. Consulta i riquadri per scoprire le policy disponibili.

Policy	Descrizione
Compatibilità moderna (impostazione predefinita)	Utilizzare il criterio predefinito se è necessaria una crittografia avanzata e se non si dispone di requisiti speciali. Questo criterio è compatibile con la maggior parte dei client TLS e SSH.
Compatibilità con le versioni precedenti	Utilizzare questo criterio se sono necessarie ulteriori opzioni di compatibilità per i client meno recenti. Le opzioni aggiuntive di questa policy potrebbero renderla meno sicura rispetto alla moderna policy di compatibilità.
Criteri comuni	Utilizzare questa policy se si richiede la certificazione Common Criteria.
FIPS rigoroso	Utilizzare questo criterio se si richiede la certificazione Common Criteria e si deve utilizzare il modulo di protezione Cryptographic NetApp 3.0.8 per connessioni client esterne agli endpoint di bilanciamento del carico, a Gestore tenant e a Gestione griglia. L'utilizzo di questo criterio potrebbe ridurre le performance. **Nota**: Dopo aver selezionato questo criterio, tutti i nodi devono essere "riavviato in modo scorrevole" Per attivare il modulo di protezione crittografica NetApp. Utilizzare **manutenzione** > **riavvio in sequenza** per avviare e riavviare il monitor.
Personalizzato	Creare un criterio personalizzato se è necessario applicare le proprie crittografia.

3. Per visualizzare i dettagli relativi a crittografia, protocolli e algoritmi di ogni policy, selezionare **Visualizza dettagli**.
4. Per modificare la policy corrente, selezionare **Usa policy**.

   Un segno di spunta verde viene visualizzato accanto a **policy corrente** nel riquadro del criterio.

Creare una policy di sicurezza personalizzata

È possibile creare una policy personalizzata se è necessario applicare le proprie crittografia.

Fasi

1. Dal riquadro del criterio più simile al criterio personalizzato che si desidera creare, selezionare **Visualizza dettagli**.
2. Selezionare **Copia negli Appunti**, quindi selezionare **Annulla**.

3. Dal riquadro **Custom policy**, selezionare **Configure and use** (Configura e utilizza).
4. Incollare il JSON copiato e apportare le modifiche necessarie.
5. Selezionare **Usa policy**.

   Un segno di spunta verde viene visualizzato accanto a **Current policy** (policy corrente) nel riquadro Custom policy (policy personalizzate).

6. Facoltativamente, selezionare **Edit Configuration** (Modifica configurazione) per apportare ulteriori modifiche al nuovo criterio personalizzato.

Ripristinare temporaneamente il criterio di protezione predefinito

Se è stato configurato un criterio di protezione personalizzato, potrebbe non essere possibile accedere a Grid Manager se il criterio TLS configurato non è compatibile con "certificato server configurato".

È possibile ripristinare temporaneamente i criteri di protezione predefiniti.

Fasi

1. Accedere a un nodo amministratore:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

      Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Eseguire il seguente comando:

   ```
   restore-default-cipher-configurations
   ```

3. Da un browser Web, accedere a Grid Manager sullo stesso nodo di amministrazione.
4. Seguire la procedura descritta in Selezionare una policy di sicurezza per configurare nuovamente il criterio.

Configurare la sicurezza della rete e degli oggetti

È possibile configurare la sicurezza di rete e degli oggetti per crittografare gli oggetti memorizzati, per impedire determinate richieste S3 e Swift o per consentire alle connessioni client ai nodi di storage di utilizzare HTTP invece di HTTPS.

Crittografia degli oggetti memorizzati

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3. Per impostazione predefinita, gli oggetti memorizzati non vengono crittografati, ma è possibile scegliere di crittografare gli oggetti utilizzando l'algoritmo di crittografia AES-128 o AES-256. Quando si attiva l'impostazione, tutti gli oggetti inseriti di recente vengono crittografati, ma non vengono apportate modifiche agli oggetti memorizzati esistenti. Se si disattiva la crittografia, gli oggetti attualmente crittografati rimangono crittografati, ma gli oggetti appena acquisiti non vengono crittografati.

L'impostazione di crittografia degli oggetti memorizzati si applica solo agli oggetti S3 che non sono stati crittografati mediante crittografia a livello di bucket o a livello di oggetto.

Per ulteriori informazioni sui metodi di crittografia StorageGRID, vedere "Esaminare i metodi di crittografia StorageGRID".

Impedire la modifica del client

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione **Impedisci modifica client**, le seguenti richieste vengono rifiutate.

API REST S3

- Richieste DeleteBucket
- Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3

API Swift REST

- Eliminare le richieste di container
- Richiede di modificare qualsiasi oggetto esistente. Ad esempio, le seguenti operazioni sono negate: Put Overwrite (Inserisci sovrascrittura), Delete (Elimina), Metadata Update (aggiornamento metadati) e così via.

Abilitare HTTP per le connessioni dei nodi di storage

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per qualsiasi connessione diretta ai nodi di storage. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Utilizzare HTTP per le connessioni dei nodi di storage solo se i client S3 e Swift devono stabilire connessioni HTTP direttamente ai nodi di storage. Non è necessario utilizzare questa opzione per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (perché è possibile "configurare ciascun endpoint del bilanciamento del carico" Per utilizzare HTTP o HTTPS).

Vedere "Riepilogo: Indirizzi IP e porte per le connessioni client" Per sapere quali porte S3 e i client Swift utilizzano per la connessione ai nodi di storage utilizzando HTTP o HTTPS.

Selezionare le opzioni

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso root.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.
2. Selezionare la scheda **rete e oggetti**.
3. Per la crittografia degli oggetti memorizzati, utilizzare l'impostazione **None** (predefinita) se non si desidera crittografare gli oggetti memorizzati oppure selezionare **AES-128** o **AES-256** per crittografare gli oggetti memorizzati.
4. Se si desidera impedire ai client S3 e Swift di effettuare richieste specifiche, selezionare **Impedisci modifica client**.

   Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

5. Se si desidera utilizzare connessioni HTTP, selezionare **Enable HTTP for Storage Node Connections** (attiva HTTP per connessioni nodo di storage) se i client si connettono direttamente ai nodi di storage.

   Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

6. Selezionare **Salva**.

Modificare le impostazioni di sicurezza dell'interfaccia

Le impostazioni di protezione dell'interfaccia consentono di controllare se gli utenti sono disconnessi se sono inattivi per un periodo di tempo superiore a quello specificato e se una traccia dello stack è inclusa nelle risposte di errore API.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "Autorizzazione di accesso root".

A proposito di questa attività

La pagina **Impostazioni di protezione** include le impostazioni **Timeout inattività browser** e **traccia stack API di gestione**.

Timeout di inattività del browser

Indica per quanto tempo il browser di un utente può rimanere inattivo prima che l'utente venga disconnesso. L'impostazione predefinita è 15 minuti.

Il timeout di inattività del browser è controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Alla scadenza dell'autenticazione di un utente, l'utente viene automaticamente disconnesso, anche se il timeout di inattività del browser è disattivato o

non è stato raggiunto il valore di timeout del browser. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.

- Impostazioni di timeout per il provider di identità, presupponendo che SSO (Single Sign-on) sia abilitato per StorageGRID.

  Se SSO è attivato e il browser dell'utente si disinserisce, l'utente deve immettere nuovamente le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere "Configurare il single sign-on".

Traccia stack API di gestione

Controlla se una traccia di stack viene restituita nelle risposte di errore delle API di Gestione griglia e di Gestione tenant.

Questa opzione è disattivata per impostazione predefinita, ma potrebbe essere necessario attivarla per un ambiente di test. In generale, è necessario lasciare disattivata la traccia dello stack negli ambienti di produzione per evitare di rivelare i dettagli del software interno quando si verificano errori API.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Security settings**.
2. Selezionare la scheda **interfaccia**.
3. Per modificare l'impostazione del timeout di inattività del browser:
   a. Espandere la fisarmonica.
   b. Per modificare il periodo di timeout, specificare un valore compreso tra 60 secondi e 7 giorni. Il timeout predefinito è di 15 minuti.
   c. Per disattivare questa funzione, deselezionare la casella di controllo.
   d. Selezionare **Salva**.

      La nuova impostazione non influisce sugli utenti che hanno effettuato l'accesso. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser per rendere effettiva la nuova impostazione di timeout.

4. Per modificare l'impostazione per la traccia stack API di gestione:
   a. Espandere la fisarmonica.
   b. Selezionare la casella di controllo per restituire una traccia di stack nelle risposte agli errori di API di Gestione griglia e di Gestione tenant.

      > ⚠ Lasciare la traccia dello stack disattivata negli ambienti di produzione per evitare di rivelare dettagli software interni quando si verificano errori API.

   c. Selezionare **Salva**.

Configurare i server di gestione delle chiavi

Configurazione dei server di gestione delle chiavi: Panoramica

È possibile configurare uno o più server di gestione delle chiavi (KMS) esterni per proteggere i dati su nodi appliance appositamente configurati.

StorageGRID supporta solo alcuni server di gestione delle chiavi. Per un elenco dei prodotti e delle versioni supportate, utilizzare "Tool di matrice di interoperabilità NetApp (IMT)".

Che cos'è un server di gestione delle chiavi (KMS)?

Un server di gestione delle chiavi (KMS) è un sistema esterno di terze parti che fornisce chiavi di crittografia ai nodi dell'appliance StorageGRID nel sito StorageGRID associato utilizzando il protocollo KMIP (Key Management Interoperability Protocol).

È possibile utilizzare uno o più server di gestione delle chiavi per gestire le chiavi di crittografia dei nodi di qualsiasi appliance StorageGRID con l'impostazione **crittografia dei nodi** attivata durante l'installazione. L'utilizzo di server di gestione delle chiavi con questi nodi appliance consente di proteggere i dati anche in caso di rimozione di un'appliance dal data center. Una volta crittografati i volumi dell'appliance, non è possibile accedere ai dati dell'appliance a meno che il nodo non sia in grado di comunicare con il KMS.

StorageGRID non crea o gestisce le chiavi esterne utilizzate per crittografare e decrittare i nodi dell'appliance. Se si intende utilizzare un server di gestione delle chiavi esterno per proteggere i dati StorageGRID, è necessario comprendere come configurare tale server e come gestire le chiavi di crittografia. L'esecuzione delle attività di gestione chiave non rientra nell'ambito di queste istruzioni. Per assistenza, consultare la documentazione relativa al server di gestione delle chiavi o contattare il supporto tecnico.

Panoramica di KMS e configurazione dell'appliance

Prima di utilizzare un server di gestione delle chiavi (KMS) per proteggere i dati StorageGRID sui nodi appliance, è necessario completare due attività di configurazione: La configurazione di uno o più server KMS e l'abilitazione della crittografia dei nodi per i nodi appliance. Una volta completate queste due attività di configurazione, il processo di gestione delle chiavi viene eseguito automaticamente.

Il diagramma di flusso mostra i passaggi di alto livello per l'utilizzo di un KMS per proteggere i dati StorageGRID sui nodi dell'appliance.

Il diagramma di flusso mostra la configurazione di KMS e dell'appliance in parallelo; tuttavia, è possibile configurare i server di gestione delle chiavi prima o dopo aver attivato la crittografia dei nodi per i nuovi nodi appliance, in base ai requisiti.

Configurare il server di gestione delle chiavi (KMS)

La configurazione di un server di gestione delle chiavi include i seguenti passaggi di alto livello.

Fase	Fare riferimento a.
Accedere al software KMS e aggiungere un client per StorageGRID a ciascun cluster KMS o KMS.	"Configurare StorageGRID come client nel KMS"
Ottenere le informazioni richieste per il client StorageGRID sul KMS.	"Configurare StorageGRID come client nel KMS"

Fase	Fare riferimento a.
Aggiungere il KMS al Grid Manager, assegnarlo a un singolo sito o a un gruppo predefinito di siti, caricare i certificati richiesti e salvare la configurazione del KMS.	"Aggiunta di un server di gestione delle chiavi (KMS)"

Configurare l'apparecchio

La configurazione di un nodo appliance per l'utilizzo di KMS include i seguenti passaggi di alto livello.

1. Durante la fase di configurazione hardware dell'installazione dell'appliance, utilizzare il programma di installazione dell'appliance StorageGRID per attivare l'impostazione **crittografia del nodo** dell'appliance.

> Non è possibile attivare l'impostazione **Node Encryption** dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non dispongono della crittografia dei nodi abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID. Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dei dati casuale (DEK), come segue:
   - I DEK vengono utilizzati per crittografare i dati su ciascun volume. Queste chiavi vengono generate utilizzando la crittografia del disco Linux Unified Key Setup (LUKS) nel sistema operativo dell'appliance e non possono essere modificate.
   - Ogni singolo DEK viene crittografato mediante una chiave di crittografia della chiave master (KEK). La chiave iniziale KEK è una chiave temporanea che crittografa i DEK fino a quando l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo appliance a StorageGRID.

Vedere "Abilitare la crittografia del nodo" per ulteriori informazioni.

Processo di crittografia per la gestione delle chiavi (si verifica automaticamente)

La crittografia per la gestione delle chiavi include i seguenti passaggi di alto livello che vengono eseguiti automaticamente.

1. Quando si installa un'appliance che ha attivato la crittografia dei nodi nella griglia, StorageGRID determina se esiste una configurazione KMS per il sito che contiene il nuovo nodo.
   - Se un KMS è già stato configurato per il sito, l'appliance riceve la configurazione KMS.
   - Se non è ancora stato configurato un KMS per il sito, i dati dell'appliance continuano a essere crittografati dalla KEK temporanea fino a quando non si configura un KMS per il sito e l'appliance non riceve la configurazione KMS.
2. L'appliance utilizza la configurazione KMS per connettersi al KMS e richiedere una chiave di crittografia.
3. Il KMS invia una chiave di crittografia all'appliance. La nuova chiave del KMS sostituisce la KEK temporanea e viene ora utilizzata per crittografare e decrittare i DEK per i volumi dell'appliance.

> Tutti i dati che esistono prima che il nodo dell'appliance crittografato si connetta al KMS configurato vengono crittografati con una chiave temporanea. Tuttavia, i volumi dell'appliance non devono essere considerati protetti dalla rimozione dal data center fino a quando la chiave temporanea non viene sostituita dalla chiave di crittografia KMS.

4. Se l'appliance viene accesa o riavviata, si ricollega al KMS per richiedere la chiave. La chiave, che viene salvata nella memoria volatile, non può sopravvivere a una perdita di alimentazione o a un riavvio.

Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi

Prima di configurare un KMS (Key Management Server) esterno, è necessario comprendere le considerazioni e i requisiti.

Quale versione di KMIP è supportata?

StorageGRID supporta KMIP versione 1.4.

"Key Management Interoperability Protocol Specification versione 1.4"

Quali sono le considerazioni sulla rete?

Le impostazioni del firewall di rete devono consentire a ciascun nodo dell'appliance di comunicare attraverso la porta utilizzata per le comunicazioni KMIP (Key Management Interoperability Protocol). La porta KMIP predefinita è 5696.

È necessario assicurarsi che ogni nodo dell'appliance che utilizza la crittografia del nodo disponga dell'accesso di rete al cluster KMS o KMS configurato per il sito.

Quali versioni di TLS sono supportate?

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID può supportare il protocollo TLS 1,2 o TLS 1,3 quando stabilisce connessioni KMIP a un cluster KMS o KMS, in base a ciò che il KMS supporta e a quale "Policy TLS e SSH" si sta utilizzando.

StorageGRID negozia il protocollo e il cifrario (TLS 1,2) o la suite di cifratura (TLS 1,3) con il KMS quando effettua la connessione. Per vedere quali versioni di protocollo e pacchetti di crittografia sono disponibili, consultare `tlsOutbound` Sezione del criterio TLS e SSH attivo della griglia (**CONFIGURAZIONE** > **sicurezza Impostazioni di sicurezza**).

Quali appliance sono supportate?

È possibile utilizzare un server di gestione delle chiavi (KMS) per gestire le chiavi di crittografia per qualsiasi appliance StorageGRID nel grid con l'impostazione **crittografia nodo** attivata. Questa impostazione può essere attivata solo durante la fase di configurazione hardware dell'installazione dell'appliance mediante il programma di installazione dell'appliance StorageGRID.

> Non è possibile attivare la crittografia dei nodi dopo l'aggiunta di un'appliance alla griglia e non è possibile utilizzare la gestione delle chiavi esterne per le appliance che non hanno la crittografia dei nodi abilitata.

È possibile utilizzare il KMS configurato per appliance StorageGRID e nodi appliance.

Non è possibile utilizzare il KMS configurato per i nodi software-based (non-appliance), inclusi i seguenti:

- Nodi implementati come macchine virtuali (VM)
- Nodi implementati all'interno di motori container su host Linux

I nodi implementati su queste altre piattaforme possono utilizzare la crittografia all'esterno di StorageGRID a livello di datastore o disco.

Quando è necessario configurare i server di gestione delle chiavi?

Per una nuova installazione, in genere è necessario configurare uno o più server di gestione delle chiavi in Grid Manager prima di creare tenant. Questo ordine garantisce che i nodi siano protetti prima che i dati degli oggetti siano memorizzati su di essi.

È possibile configurare i server di gestione delle chiavi in Grid Manager prima o dopo l'installazione dei nodi appliance.

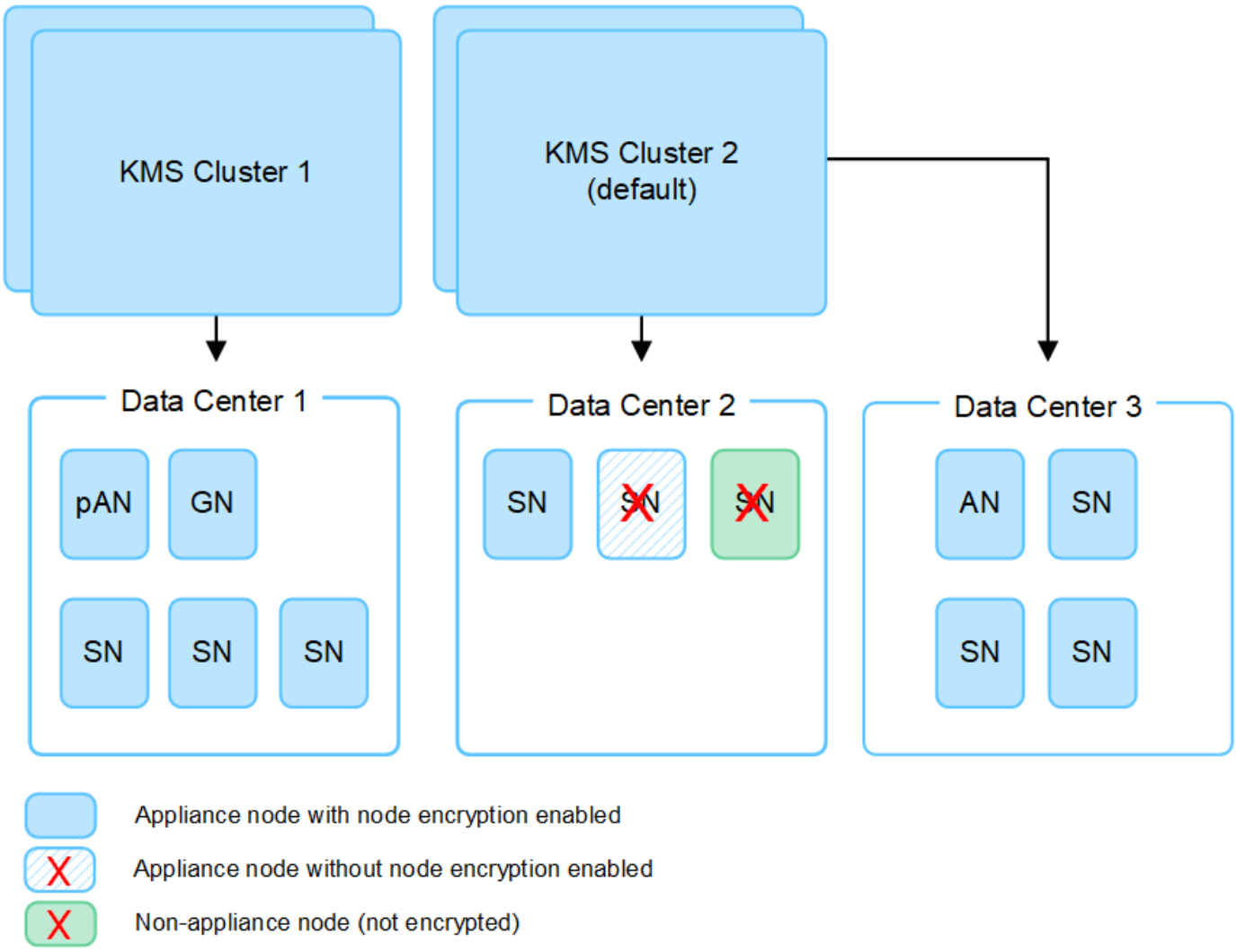
Quanti server di gestione delle chiavi sono necessari?

È possibile configurare uno o più server di gestione delle chiavi esterni per fornire chiavi di crittografia ai nodi dell'appliance nel sistema StorageGRID. Ogni KMS fornisce una singola chiave di crittografia ai nodi dell'appliance StorageGRID in un singolo sito o in un gruppo di siti.

StorageGRID supporta l'utilizzo di cluster KMS. Ogni cluster KMS contiene più server di gestione delle chiavi replicati che condividono le impostazioni di configurazione e le chiavi di crittografia. Si consiglia di utilizzare i cluster KMS per la gestione delle chiavi perché migliora le funzionalità di failover di una configurazione ad alta disponibilità.

Si supponga, ad esempio, che il sistema StorageGRID disponga di tre siti per data center. È possibile configurare un cluster KMS per fornire una chiave a tutti i nodi appliance nel data center 1 e un secondo cluster KMS per fornire una chiave a tutti i nodi appliance in tutti gli altri siti. Quando si aggiunge il secondo cluster KMS, è possibile configurare un KMS predefinito per Data Center 2 e Data Center 3.

Tenere presente che non è possibile utilizzare un KMS per i nodi non appliance o per i nodi appliance che non hanno attivato l'impostazione **Node Encryption** durante l'installazione.



Cosa succede quando si ruota una chiave?

Come Best practice per la sicurezza, è necessario effettuare periodicamente "ruotare la chiave di crittografia" Utilizzato da ciascun KMS configurato.

Quando è disponibile la nuova versione della chiave:

- Viene distribuito automaticamente ai nodi appliance crittografati nel sito o nei siti associati al KMS. La distribuzione deve avvenire entro un'ora dalla rotazione della chiave.
- Se il nodo dell'appliance crittografato non è in linea quando viene distribuita la nuova versione della chiave, il nodo riceverà la nuova chiave non appena verrà riavviato.
- Se la nuova versione della chiave non può essere utilizzata per crittografare i volumi dell'appliance per qualsiasi motivo, viene attivato l'avviso **rotazione chiave di crittografia KMS non riuscita** per il nodo dell'appliance. Potrebbe essere necessario contattare il supporto tecnico per ottenere assistenza nella risoluzione di questo avviso.

È possibile riutilizzare un nodo appliance dopo averlo crittografato?

Se è necessario installare un'appliance crittografata in un altro sistema StorageGRID, è necessario prima decommissionare il nodo Grid per spostare i dati degli oggetti in un altro nodo. Quindi, è possibile utilizzare il programma di installazione dell'appliance StorageGRID per "Cancellare la configurazione KMS". La

cancellazione della configurazione KMS disattiva l'impostazione **crittografia nodo** e rimuove l'associazione tra il nodo appliance e la configurazione KMS per il sito StorageGRID.

> Senza l'accesso alla chiave di crittografia KMS, i dati che rimangono sull'appliance non possono più essere utilizzati e bloccati in modo permanente.

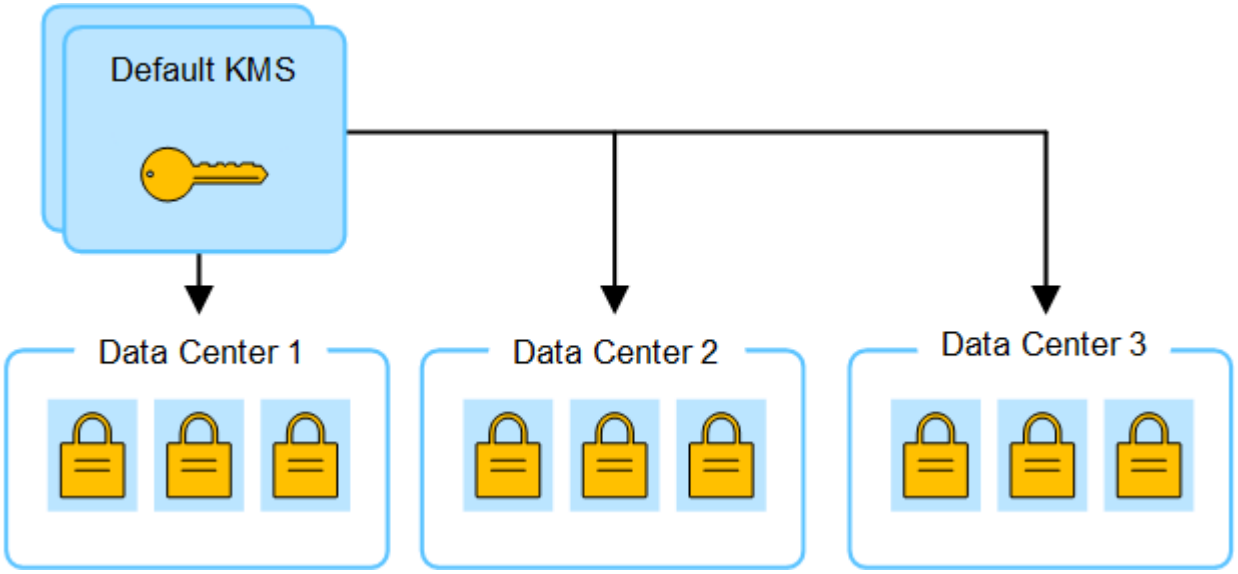
Considerazioni per la modifica del KMS per un sito

Ciascun server di gestione delle chiavi (KMS) o cluster KMS fornisce una chiave di crittografia a tutti i nodi appliance di un singolo sito o di un gruppo di siti. Se è necessario modificare il KMS utilizzato per un sito, potrebbe essere necessario copiare la chiave di crittografia da un KMS all'altro.

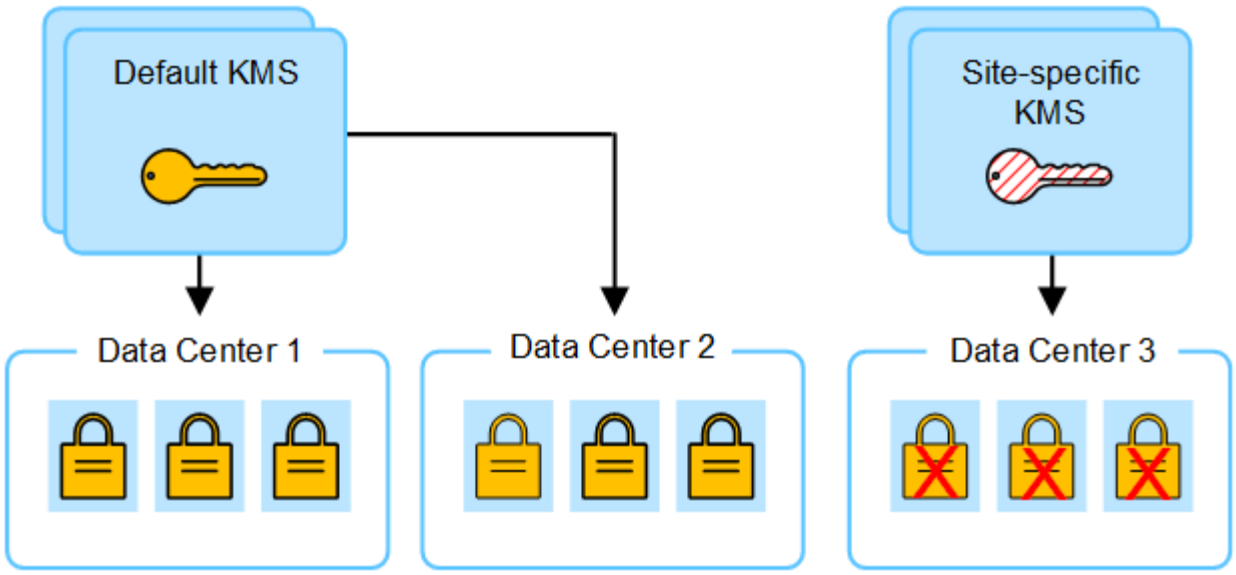
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia dal KMS originale al nuovo KMS. È necessario assicurarsi che il KMS disponga della chiave corretta per decrittare i nodi crittografati dell'appliance nel sito.

Ad esempio:

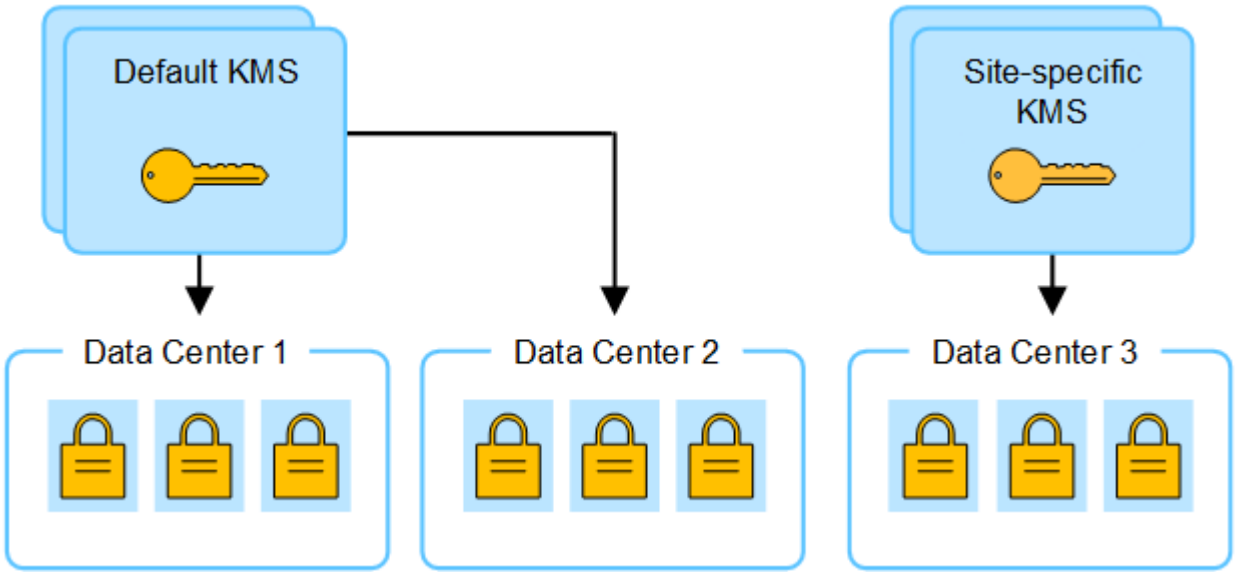
1. Inizialmente, viene configurato un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata per crittografare i nodi dell'appliance in tutti i siti. La stessa chiave deve essere utilizzata anche per decrittare tali appliance.



3. Si decide di aggiungere un KMS specifico del sito per un sito (data center 3 nella figura). Tuttavia, poiché i nodi dell'appliance sono già crittografati, si verifica un errore di convalida quando si tenta di salvare la configurazione per il KMS specifico del sito. L'errore si verifica perché il KMS specifico del sito non dispone della chiave corretta per decrittare i nodi in quel sito.



4. Per risolvere il problema, copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Tecnicamente, si copia la chiave originale in una nuova chiave con lo stesso alias. La chiave originale diventa una versione precedente della nuova chiave). Il KMS specifico del sito dispone ora della chiave corretta per decrittare i nodi dell'appliance nel data center 3, in modo che possa essere salvato in StorageGRID.



Casi di utilizzo per la modifica del KMS utilizzato per un sito

La tabella riassume i passaggi necessari per i casi più comuni di modifica del KMS per un sito.

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
Si dispone di una o più voci KMS specifiche del sito e si desidera utilizzarne una come KMS predefinito.	Modificare il KMS specifico del sito. Nel campo **Gestisci chiavi per**, selezionare **Siti non gestiti da un altro KMS (KMS predefinito)**. Il KMS specifico del sito verrà ora utilizzato come KMS predefinito. Si applica a tutti i siti che non dispongono di un KMS dedicato. "Modifica di un server di gestione delle chiavi (KMS)"
Si dispone di un KMS predefinito e si aggiunge un nuovo sito in un'espansione. Non si desidera utilizzare il KMS predefinito per il nuovo sito.	1. Se i nodi dell'appliance nel nuovo sito sono già stati crittografati con il KMS predefinito, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS predefinito a un nuovo KMS. 2. Utilizzando Grid Manager, aggiungere il nuovo KMS e selezionare il sito. "Aggiunta di un server di gestione delle chiavi (KMS)"
Si desidera che il KMS di un sito utilizzi un server diverso.	1. Se i nodi dell'appliance nel sito sono già stati crittografati dal KMS esistente, utilizzare il software KMS per copiare la versione corrente della chiave di crittografia dal KMS esistente al nuovo KMS. 2. Utilizzando Grid Manager, modificare la configurazione KMS esistente e inserire il nuovo nome host o indirizzo IP. "Aggiunta di un server di gestione delle chiavi (KMS)"

Configurare StorageGRID come client nel KMS

È necessario configurare StorageGRID come client per ogni server di gestione delle chiavi esterno o cluster KMS prima di poter aggiungere KMS a StorageGRID.

Queste istruzioni si applicano a Thales CipherTrust Manager e Hashicorp Vault. Per un elenco dei prodotti e delle versioni supportate, utilizzare "Tool di matrice di interoperabilità NetApp (IMT)".

Fasi

1. Dal software KMS, creare un client StorageGRID per ogni cluster KMS o KMS che si intende utilizzare.

   Ogni KMS gestisce una singola chiave di crittografia per i nodi delle appliance StorageGRID in un singolo sito o in un gruppo di siti.

2. creare una chiave utilizzando uno dei due metodi seguenti:
   - Utilizzare la pagina di gestione delle chiavi del prodotto KMS. Creare una chiave di crittografia AES per ogni cluster KMS o KMS.

     La chiave di crittografia deve essere 2,048 bit o superiore e deve essere esportabile.

   - Chiedere a StorageGRID di creare la chiave. Viene richiesto quando si esegue il test e si salva dopo "caricamento dei certificati client".

3. Registrare le seguenti informazioni per ciascun cluster KMS o KMS.

   Queste informazioni sono necessarie quando si aggiunge il KMS a StorageGRID:

   - Nome host o indirizzo IP per ciascun server.
   - Porta KMIP utilizzata dal KMS.
   - Alias chiave per la chiave di crittografia nel KMS.

4. Per ogni cluster KMS o KMS, ottenere un certificato server firmato da un'autorità di certificazione (CA) o un bundle di certificati che contenga ciascuno dei file di certificato CA con codifica PEM, concatenati nell'ordine della catena di certificati.

   Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

   - Il certificato deve utilizzare il formato X.509 codificato con Privacy Enhanced Mail (PEM) base-64.
   - Il campo Subject alternative Name (SAN) in ciascun certificato del server deve includere il nome di dominio completo (FQDN) o l'indirizzo IP a cui StorageGRID si connetterà.

     > Quando si configura il KMS in StorageGRID, è necessario immettere gli stessi FQDN o indirizzi IP nel campo **Nome host**.

   - Il certificato del server deve corrispondere al certificato utilizzato dall'interfaccia KMIP del KMS, che in genere utilizza la porta 5696.

5. Ottenere il certificato del client pubblico rilasciato a StorageGRID dal KMS esterno e la chiave privata per il certificato del client.

   Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Aggiunta di un server di gestione delle chiavi (KMS)

Utilizzare la procedura guidata del server di gestione delle chiavi StorageGRID per aggiungere ogni cluster KMS o KMS.

Prima di iniziare

- Hai esaminato il "considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi".
- Lo hai fatto "StorageGRID configurato come client nel KMS"E si dispone delle informazioni necessarie per ogni cluster KMS o KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

Se possibile, configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. Se si crea prima il KMS predefinito, tutte le appliance crittografate con nodo nella griglia verranno crittografate con il KMS predefinito. Se si desidera creare un KMS specifico del sito in un secondo momento, è necessario prima copiare la versione corrente della chiave di crittografia dal KMS predefinito al nuovo KMS. Vedere "Considerazioni per la modifica del KMS per un sito" per ulteriori informazioni.

Fase 1: Dettagli DI KMS

Nella fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono forniti dettagli sul cluster KMS o KMS.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) con la scheda Configuration details (Dettagli di configurazione) selezionata.

2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi).

3. Immettere le seguenti informazioni per il KMS e il client StorageGRID configurati in tale KMS.

Campo	Descrizione
NOME DEL KM	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. **Nota**: Se non è stata creata una chiave utilizzando il prodotto KMS, verrà richiesto di fare in modo che StorageGRID crei la chiave.
Gestisce le chiavi per	Il sito StorageGRID che sarà associato a questo KMS. Se possibile, è necessario configurare qualsiasi server di gestione delle chiavi specifico del sito prima di configurare un KMS predefinito che si applica a tutti i siti non gestiti da un altro KMS. • Selezionare un sito se il KMS gestirà le chiavi di crittografia per i nodi dell'appliance in un sito specifico. • Selezionare **Siti non gestiti da un altro KMS (KMS predefinito)** per configurare un KMS predefinito che si applicherà a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti nelle espansioni successive. **Nota:** Quando si salva la configurazione KMS, si verifica Un errore di convalida se si seleziona un sito precedentemente crittografato dal KMS predefinito ma non si fornisce la versione corrente della chiave di crittografia originale al nuovo KMS.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.

Campo	Descrizione
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. **Nota:** il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
5. Selezionare **continua**.

Fase 2: Caricare il certificato del server

Nella fase 2 (carica certificato server) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), viene caricato il certificato del server (o bundle di certificati) per il KMS. Il certificato del server consente al KMS esterno di autenticarsi su StorageGRID.

Fasi

1. Dal **passaggio 2 (carica certificato server)**, individuare la posizione del certificato server o del bundle di certificati salvato.
2. Caricare il file del certificato.

   Vengono visualizzati i metadati del certificato del server.

   Se hai caricato un bundle di certificati, i metadati di ciascun certificato vengono visualizzati nella relativa scheda.

3. Selezionare **continua**.

Fase 3: Caricare i certificati client

Nella fase 3 (carica certificati client) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono caricati il certificato client e la chiave privata del certificato client. Il certificato client consente a StorageGRID di autenticarsi nel KMS.

Fasi

1. Dal **passaggio 3 (carica certificati client)**, individuare la posizione del certificato client.
2. Caricare il file di certificato del client.

   Vengono visualizzati i metadati del certificato client.

3. Individuare la posizione della chiave privata per il certificato client.
4. Caricare il file della chiave privata.
5. Selezionare **Test e salvare**.

   Se una chiave non esiste, viene richiesto di crearne una da StorageGRID.

   Vengono verificate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata nel KMS, il nuovo server di gestione delle chiavi

viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

> Subito dopo aver aggiunto un KMS, lo stato del certificato nella pagina Server gestione chiavi viene visualizzato come Sconosciuto. Per ottenere lo stato effettivo di ciascun certificato, StorageGRID potrebbe impiegare fino a 30 minuti. È necessario aggiornare il browser Web per visualizzare lo stato corrente.

6. Se viene visualizzato un messaggio di errore quando si seleziona **Test and Save** (verifica e salva), rivedere i dettagli del messaggio e selezionare **OK**.

   Ad esempio, se un test di connessione non riesce, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

7. Se si desidera salvare la configurazione corrente senza verificare la connessione esterna, selezionare **Force Save** (forza salvataggio).

   > Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

8. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

   La configurazione KMS viene salvata ma la connessione al KMS non viene verificata.

Gestire un KMS

La gestione di un server di gestione delle chiavi (KMS) comporta la visualizzazione o la modifica dei dettagli, la gestione dei certificati, la visualizzazione dei nodi crittografati e la rimozione di un KMS quando non è più necessario.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "autorizzazione di accesso richiesta".

Visualizza i dettagli di KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, inclusi i dettagli delle chiavi e lo stato corrente dei certificati server e client.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina del server di gestione delle chiavi con le seguenti informazioni:

   - La scheda Dettagli configurazione elenca tutti i server di gestione delle chiavi configurati.
   - La scheda nodi crittografati elenca tutti i nodi con la crittografia dei nodi abilitata.

2. Per visualizzare i dettagli di un KMS specifico ed eseguire operazioni su tale KMS, selezionare il nome del KMS. Nella pagina dei dettagli del KMS sono elencate le seguenti informazioni:

Campo	Descrizione
Gestisce le chiavi per	Il sito StorageGRID associato al KMS. Questo campo visualizza il nome di un sito StorageGRID specifico o **Siti non gestiti da un altro KMS (KMS predefinito).**
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. Se è presente un cluster di due server di gestione delle chiavi, vengono elencati il nome di dominio completo o l'indirizzo IP di entrambi i server. Se in un cluster sono presenti più di due server di gestione delle chiavi, viene elencato il nome di dominio completo o l'indirizzo IP del primo KMS insieme al numero di server di gestione delle chiavi aggiuntivi nel cluster. Ad esempio: `10.10.10.10 and 10.10.10.11` oppure `10.10.10.10 and 2 others`. Per visualizzare tutti i nomi host in un cluster, selezionare un KMS e selezionare **Modifica** o **azioni** > **Modifica**.

3. Selezionare una scheda nella pagina dei dettagli KMS per visualizzare le seguenti informazioni:

Scheda	Campo	Descrizione
Dettagli chiave	Nome della chiave	L'alias della chiave per il client StorageGRID nel KMS.
UID chiave	L'identificatore univoco dell'ultima versione della chiave.	Ultima modifica
La data e l'ora dell'ultima versione della chiave.	Certificato del server	Metadati
I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.	Certificato PEM	Il contenuto del file PEM (privacy Enhanced mail) per il certificato.
Certificato del client	Metadati	I metadati del certificato, come il numero di serie, la data e l'ora di scadenza e il PEM del certificato.

4. tutte le volte che richiesto dalle procedure di sicurezza dell'organizzazione, selezionare **Rotate key**, oppure utilizzare il software KMS, per creare una nuova versione della chiave.

   Quando la rotazione della chiave ha esito positivo, i campi UID chiave e ultima modifica vengono aggiornati.

Se si ruota la chiave di crittografia utilizzando il software KMS, ruotarla dall'ultima versione utilizzata della chiave a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.

Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. StorageGRID richiede che tutte le versioni delle chiavi utilizzate in precedenza (così come quelle future) siano accessibili dal KMS con lo stesso alias della chiave. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

Gestire i certificati

Risolvere tempestivamente eventuali problemi relativi ai certificati server o client. Se possibile, sostituire i certificati prima che scadano.

Per mantenere l'accesso ai dati, è necessario risolvere al più presto eventuali problemi di certificato.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.
2. Nella tabella, esaminare il valore della scadenza del certificato per ogni KMS.
3. Se la scadenza del certificato per qualsiasi KMS è sconosciuta, attendere fino a 30 minuti, quindi aggiornare il browser Web.
4. Se la colonna scadenza certificato indica che un certificato è scaduto o è prossimo alla scadenza, selezionare il KMS per accedere alla pagina dei dettagli del KMS.
   a. Selezionare **certificato server** e verificare il valore del campo "scade il".
   b. Per sostituire il certificato, selezionare **Modifica certificato** per caricare un nuovo certificato.
   c. Ripetere questi passaggi secondari e selezionare **Client certificate** invece di Server certificate (certificato server).
5. Quando vengono attivati gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS**, annotare la descrizione di ciascun avviso ed eseguire le azioni consigliate.

Per ottenere gli aggiornamenti alla scadenza del certificato, StorageGRID potrebbe richiedere fino a 30 minuti. Aggiornare il browser Web per visualizzare i valori correnti.

Visualizzare i nodi crittografati

È possibile visualizzare informazioni sui nodi appliance nel sistema StorageGRID per i quali è stata attivata l'impostazione **crittografia nodo**.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key Management Server (Server di gestione delle chiavi). La scheda Dettagli configurazione mostra tutti i server di gestione delle chiavi configurati.

2. Nella parte superiore della pagina, selezionare la scheda **nodi crittografati**.

La scheda nodi crittografati elenca i nodi appliance nel sistema StorageGRID con l'impostazione **crittografia nodo** attivata.

3. Esaminare le informazioni contenute nella tabella per ciascun nodo appliance.

Colonna	Descrizione
Nome del nodo	Il nome del nodo appliance.
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
NOME DEL KM	Il nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli di configurazione per aggiungere un KMS. "Aggiunta di un server di gestione delle chiavi (KMS)"
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un UID chiave completo, selezionare il testo. Un trattino (--) indica che l'UID della chiave non è noto, probabilmente a causa di un problema di connessione tra il nodo dell'appliance e il KMS.
Stato	Lo stato della connessione tra il KMS e il nodo dell'appliance. Se il nodo è connesso, l'indicatore data e ora viene aggiornato ogni 30 minuti. L'aggiornamento dello stato di connessione può richiedere alcuni minuti dopo le modifiche della configurazione KMS. **Nota:** aggiornare il browser Web per visualizzare i nuovi valori.

4. Se la colonna Status (Stato) indica un problema KMS, risolverlo immediatamente.

   Durante le normali operazioni KMS, lo stato sarà **connesso a KMS**. Se un nodo viene disconnesso dalla rete, viene visualizzato lo stato di connessione del nodo (amministrativamente inattivo o Sconosciuto).

   Gli altri messaggi di stato corrispondono agli avvisi StorageGRID con gli stessi nomi:

   - Impossibile caricare la configurazione KMS
   - Errore di connettività KMS
   - Nome chiave di crittografia KMS non trovato
   - Rotazione della chiave di crittografia KMS non riuscita
   - La chiave KMS non è riuscita a decrittare un volume dell'appliance
   - KMS non configurato

   Eseguire le azioni consigliate per questi avvisi.

È necessario affrontare immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Modificare un KMS

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio, se un certificato sta per scadere.

Prima di iniziare

- Se si prevede di aggiornare il sito selezionato per un KMS, è stata esaminata la "Considerazioni per la modifica del KMS per un sito".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera modificare e selezionare **azioni** > **Modifica**.

   Puoi anche modificare un KMS selezionando il nome del KMS nella tabella e selezionando **Edit** nella pagina dei dettagli del KMS.

3. Facoltativamente, aggiornare i dettagli nel **Passo 1 (dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
NOME DEL KM	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.
Nome della chiave	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri. È sufficiente modificare il nome della chiave solo in rari casi. Ad esempio, è necessario modificare il nome della chiave se l'alias viene rinominato in KMS o se tutte le versioni della chiave precedente sono state copiate nella cronologia delle versioni del nuovo alias.
Gestisce le chiavi per	Se si sta modificando un KMS specifico del sito e non si dispone già di un KMS predefinito, selezionare **Sites Not Managed by another KMS (default KMS)** (Siti non gestiti da un altro KMS (default KMS)*). Questa selezione converte un KMS specifico del sito nel KMS predefinito, che verrà applicato a tutti i siti che non dispongono di un KMS dedicato e a tutti i siti aggiunti in un'espansione. **Nota:** se stai modificando un KMS specifico del sito, non puoi selezionare un altro sito. Se stai modificando il KMS predefinito, non puoi selezionare un sito specifico.

Campo	Descrizione
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. **Nota:** il campo Subject alternative Name (SAN) del certificato del server deve includere l'FQDN o l'indirizzo IP immesso qui. In caso contrario, StorageGRID non sarà in grado di connettersi al KMS o a tutti i server di un cluster KMS.

4. Se si sta configurando un cluster KMS, selezionare **Add another hostname** (Aggiungi un altro nome host) per aggiungere un nome host per ciascun server del cluster.
5. Selezionare **continua**.

   Viene visualizzata la fase 2 (carica certificato server) della procedura guidata Modifica un server di gestione delle chiavi.

6. Se è necessario sostituire il certificato del server, selezionare **Sfoglia** e caricare il nuovo file.
7. Selezionare **continua**.

   Viene visualizzata la fase 3 (carica certificati client) della procedura guidata Modifica un server di gestione delle chiavi.

8. Se è necessario sostituire il certificato client e la chiave privata del certificato client, selezionare **Browse** (Sfoglia) e caricare i nuovi file.
9. Selezionare **Test e salvare**.

   Vengono testate le connessioni tra il server di gestione delle chiavi e tutti i nodi di appliance con crittografia a nodo nei siti interessati. Se tutte le connessioni dei nodi sono valide e la chiave corretta viene trovata nel KMS, il server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

10. Se viene visualizzato un messaggio di errore, esaminare i dettagli del messaggio e selezionare **OK**.

    Ad esempio, se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non ha avuto esito positivo, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **Imponi salvataggio**.

    > Selezionando **forza salvataggio** viene salvata la configurazione KMS, ma non viene eseguita una verifica della connessione esterna da ciascuna appliance a quel KMS. In caso di problemi con la configurazione, potrebbe non essere possibile riavviare i nodi dell'appliance che hanno attivato la crittografia dei nodi nel sito interessato. È possibile che l'accesso ai dati venga perso fino a quando i problemi non vengono risolti.

    La configurazione KMS viene salvata.

12. Controllare l'avviso di conferma e selezionare **OK** se si desidera forzare il salvataggio della configurazione.

La configurazione del KMS viene salvata, ma la connessione al KMS non viene verificata.

Rimozione di un server di gestione delle chiavi (KMS)

In alcuni casi, potrebbe essere necessario rimuovere un server di gestione delle chiavi. Ad esempio, è possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato.

Prima di iniziare

- Hai esaminato il "considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

A proposito di questa attività

È possibile rimuovere un KMS nei seguenti casi:

- È possibile rimuovere un KMS specifico del sito se il sito è stato decommissionato o se il sito non include nodi appliance con crittografia del nodo attivata.
- È possibile rimuovere il KMS predefinito se esiste già un KMS specifico del sito per ogni sito che ha nodi appliance con crittografia del nodo attivata.

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Key management server**.

   Viene visualizzata la pagina Key management server (Server di gestione delle chiavi) che mostra tutti i server di gestione delle chiavi configurati.

2. Selezionare il KMS che si desidera rimuovere e selezionare **azioni** > **Rimuovi**.

   Puoi anche rimuovere un KMS selezionando il nome del KMS nella tabella e selezionando **Remove** dalla pagina dei dettagli del KMS.

3. Verificare che quanto segue sia vero:
   - Si sta rimuovendo un KMS specifico del sito per un sito che non dispone di un nodo appliance con crittografia del nodo attivata.
   - Si sta rimuovendo il KMS predefinito, ma esiste già un KMS specifico del sito per ogni sito con crittografia del nodo.
4. Selezionare **Sì**.

   La configurazione KMS viene rimossa.

Gestire le impostazioni del proxy

Configurare il proxy di archiviazione

Se si utilizzano servizi di piattaforma o Cloud Storage Pool, è possibile configurare un proxy non trasparente tra i nodi di storage e gli endpoint S3 esterni. Ad esempio, potrebbe essere necessario un proxy non trasparente per consentire l'invio dei messaggi dei servizi della piattaforma a endpoint esterni, ad esempio un endpoint su Internet.

Le impostazioni proxy di storage configurate non si applicano agli endpoint dei servizi della piattaforma Kafka.

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy di archiviazione.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **Impostazioni proxy**.
2. Nella scheda **archiviazione**, selezionare la casella di controllo **Abilita proxy di archiviazione**.
3. Selezionare il protocollo per il proxy di archiviazione.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

   Lasciare vuoto questo campo per utilizzare la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Selezionare **Salva**.

   Dopo il salvataggio del proxy di storage, è possibile configurare e testare nuovi endpoint per i servizi della piattaforma o i pool di cloud storage.

   Le modifiche del proxy possono richiedere fino a 10 minuti.

7. Controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma da StorageGRID non vengano bloccati.
8. Se è necessario disattivare un proxy di archiviazione, deselezionare la casella di controllo e selezionare **Salva**.

Configurare le impostazioni del proxy amministratore

Se si inviano pacchetti AutoSupport utilizzando HTTP o HTTPS, è possibile configurare un server proxy non trasparente tra i nodi Admin e il supporto tecnico (AutoSupport).

Per ulteriori informazioni su AutoSupport, vedere "Configurare AutoSupport".

Prima di iniziare

- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

A proposito di questa attività

È possibile configurare le impostazioni per un singolo proxy amministratore.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sicurezza** > **Impostazioni proxy**.

Viene visualizzata la pagina Impostazioni proxy. Per impostazione predefinita, l'opzione Storage (archiviazione) è selezionata nel menu Tab (scheda).

2. Selezionare la scheda **Ammin**.
3. Selezionare la casella di controllo **Enable Admin Proxy** (attiva proxy amministratore).
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Inserire la porta utilizzata per la connessione al server proxy.
6. Facoltativamente, immettere un nome utente e una password per il server proxy.

   Se il server proxy non richiede un nome utente o una password, lasciare vuoti questi campi.

7. Selezionare una delle seguenti opzioni:

   - Se si desidera proteggere la connessione al proxy amministratore, selezionare **verifica certificato proxy**. Caricare un pacchetto CA per verificare l'autenticità dei certificati SSL presentati dal server proxy amministratore.

     AutoSupport on Demand, e-Series AutoSupport tramite StorageGRID e la determinazione del percorso di aggiornamento nella pagina dell'upgrade della StorageGRID non funzionano se viene verificato un certificato proxy.

   Dopo aver caricato il pacchetto CA, vengono visualizzati i relativi metadati.

   - Se non si desidera convalidare i certificati quando si comunica con il server proxy dell'amministratore, selezionare **non verificare il certificato proxy**.

8. Selezionare **Salva**.

   Dopo aver salvato il proxy dell'amministratore, viene configurato il server proxy tra i nodi Admin e il supporto tecnico.

   Le modifiche del proxy possono richiedere fino a 10 minuti.

9. Se è necessario disattivare il proxy amministratore, deselezionare la casella di controllo **Abilita proxy amministratore**, quindi selezionare **Salva**.

Firewall di controllo

Controllare l'accesso al firewall esterno

È possibile aprire o chiudere porte specifiche sul firewall esterno.

È possibile controllare l'accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, è possibile impedire ai tenant di connettersi a Grid Manager dal firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Se si desidera configurare il firewall interno di StorageGRID, vedere "Configurare il firewall interno".

Porta	Descrizione	Se la porta è aperta…
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API. **Nota:** la porta 443 viene utilizzata anche per il traffico interno.
8443	Porta Grid Manager limitata sui nodi di amministrazione	• I browser Web e i client API di gestione possono accedere a Grid Manager e all'API di Grid Management utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a tenant Manager o all'API di gestione tenant. • Le richieste di contenuto interno verranno rifiutate.
9443	Porta limitata di Tenant Manager sui nodi di amministrazione	• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione tenant utilizzando HTTPS. • I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API di Grid Management. • Le richieste di contenuto interno verranno rifiutate.

Single Sign-on (SSO) non è disponibile sulle porte limitate di Grid Manager o Tenant Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- "Accedi a Grid Manager"
- "Creare un account tenant"
- "Comunicazioni esterne"

Gestire i controlli firewall interni

StorageGRID include un firewall interno su ciascun nodo che migliora la sicurezza della rete consentendo di controllare l'accesso alla rete. Utilizzare il firewall per impedire l'accesso alla rete su tutte le porte, ad eccezione di quelle necessarie per l'implementazione della griglia specifica. Le modifiche apportate alla configurazione nella pagina di controllo Firewall vengono distribuite a ciascun nodo.

Utilizzare le tre schede della pagina di controllo Firewall per personalizzare l'accesso necessario per la griglia.

- **Privileged address list**: Utilizzare questa scheda per consentire l'accesso selezionato alle porte chiuse. È possibile aggiungere indirizzi IP o sottoreti nella notazione CIDR che possono accedere alle porte chiuse utilizzando la scheda Manage external access (Gestisci accesso esterno).

- **Gestisci accesso esterno**: Utilizzare questa scheda per chiudere le porte aperte per impostazione predefinita o riaprire le porte chiuse in precedenza.
- **Untrusted Client Network**: Utilizzare questa scheda per specificare se un nodo considera attendibile il traffico in entrata dalla rete client.

  Le impostazioni di questa scheda sovrascrivono quelle della scheda Gestisci accesso esterno.

  - Un nodo con una rete client non attendibile accetta solo le connessioni sulle porte endpoint del bilanciamento del carico configurate su quel nodo (endpoint globali, di interfaccia di nodo e di tipo di nodo).
  - Le porte endpoint del bilanciamento del carico *sono le uniche porte aperte* sulle reti client non attendibili, indipendentemente dalle impostazioni nella scheda Gestisci reti esterne.
  - Se attendibili, tutte le porte aperte nella scheda Manage external access (Gestisci accesso esterno) sono accessibili, così come tutti gli endpoint del bilanciamento del carico aperti nella rete client.

> Le impostazioni effettuate in una scheda possono influire sulle modifiche di accesso apportate in un'altra scheda. Verificare le impostazioni di tutte le schede per assicurarsi che la rete funzioni nel modo previsto.

Per configurare i controlli firewall interni, vedere "Configurare i controlli firewall".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere "Controllare l'accesso al firewall esterno".

Elenco degli indirizzi privilegiati e schede di gestione degli accessi esterni

La scheda Privileged address list (elenco indirizzi privilegiati) consente di registrare uno o più indirizzi IP ai quali viene concesso l'accesso alle porte della griglia chiuse. La scheda Manage external access (Gestisci accesso esterno) consente di chiudere l'accesso esterno alle porte esterne selezionate o a tutte le porte esterne aperte (le porte esterne sono porte accessibili per impostazione predefinita dai nodi non grid). Queste due schede spesso possono essere utilizzate insieme per personalizzare l'esatto accesso di rete necessario per la griglia.

> Per impostazione predefinita, gli indirizzi IP privilegiati non dispongono dell'accesso alla porta della griglia interna.

Esempio 1: Utilizzare un host di collegamento per le attività di manutenzione

Si supponga di voler utilizzare un host jump (un host con protezione avanzata) per l'amministrazione di rete. È possibile utilizzare questi passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi privilegiati) per aggiungere l'indirizzo IP dell'host di collegamento.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.

> Aggiungere l'indirizzo IP privilegiato prima di bloccare le porte 443 e 8443. Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, tutte le porte esterne sul nodo di amministrazione nella griglia verranno

bloccate per tutti gli host, ad eccezione dell'host di collegamento. È quindi possibile utilizzare l'host jump per eseguire attività di manutenzione sulla griglia in modo più sicuro.

Esempio 2: Bloccare le porte sensibili

Si supponga di voler bloccare le porte sensibili e il servizio su tale porta (ad esempio, SSH sulla porta 22). È possibile utilizzare i seguenti passaggi generali:

1. Utilizzare la scheda Privileged address list (elenco indirizzi con privilegi) per concedere l'accesso solo agli host che devono accedere al servizio.
2. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte.

> Aggiungere l'indirizzo IP con privilegi prima di bloccare l'accesso a tutte le porte assegnate per accedere a Grid Manager e Tenant Manager (le porte preimpostate sono 443 e 8443). Tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Dopo aver salvato la configurazione, la porta 22 e il servizio SSH saranno disponibili per gli host nell'elenco degli indirizzi privilegiati. A tutti gli altri host verrà negato l'accesso al servizio, indipendentemente dall'interfaccia da cui proviene la richiesta.

Esempio 3: Disabilitare l'accesso ai servizi non utilizzati

A livello di rete, è possibile disattivare alcuni servizi che non si intende utilizzare. Ad esempio, se non si fornisce l'accesso a Swift, attenersi alla seguente procedura generale:

1. Utilizzare il pulsante di commutazione nella scheda Manage external access (Gestisci accesso esterno) per bloccare la porta 18083.
2. Utilizzare l'interruttore sulla scheda Gestisci accesso esterno per bloccare la porta 18085.

Dopo aver salvato la configurazione, Storage Node non consente più la connettività Swift, ma continua a consentire l'accesso ad altri servizi su porte sbloccate.

Scheda Untrusted Client Networks

Se si utilizza una rete client, è possibile proteggere StorageGRID da attacchi ostili accettando il traffico client in entrata solo su endpoint configurati esplicitamente.

Per impostazione predefinita, la rete client su ciascun nodo della griglia è *trusted*. Ovvero, per impostazione predefinita, StorageGRID considera attendibili le connessioni in entrata a ciascun nodo della griglia su tutti "porte esterne disponibili".

È possibile ridurre la minaccia di attacchi ostili al sistema StorageGRID specificando che la rete client di ciascun nodo è *non attendibile*. Se la rete client di un nodo non è attendibile, il nodo accetta solo connessioni in entrata su porte esplicitamente configurate come endpoint del bilanciamento del carico. Vedere "Configurare gli endpoint del bilanciamento del carico" e. "Configurare i controlli firewall".

Esempio 1: Il nodo gateway accetta solo richieste HTTPS S3

Si supponga che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Eseguire le seguenti operazioni generali:

1. Dal "Endpoint del bilanciamento del carico" Configurare un endpoint di bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Dalla pagina di controllo Firewall, selezionare Untrusted (non attendibile) per specificare che la rete client sul nodo gateway non è attendibile.

Dopo aver salvato la configurazione, tutto il traffico in entrata sulla rete client del nodo gateway viene interrotto, ad eccezione delle richieste HTTPS S3 sulla porta 443 e delle richieste ICMP echo (ping).

Esempio 2: Storage Node invia richieste di servizi della piattaforma S3

Si supponga di voler attivare il traffico dei servizi della piattaforma S3 in uscita da un nodo di storage, ma di voler impedire qualsiasi connessione in entrata a tale nodo di storage sulla rete client. Eseguire questa fase generale:

- Dalla scheda Untrusted Client Networks (reti client non attendibili) della pagina di controllo Firewall, indicare che la rete client nel nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più alcun traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita verso destinazioni di servizi della piattaforma configurate.

Esempio 3: Limitazione dell'accesso a Grid Manager a una subnet

Si supponga di voler consentire l'accesso a Grid Manager solo su una subnet specifica. Attenersi alla seguente procedura:

1. Collegare la rete client dei nodi di amministrazione alla subnet.
2. Utilizzare la scheda Untrusted Client Network (rete client non attendibile) per configurare la rete client come non attendibile.
3. Quando si crea un endpoint per il bilanciamento del carico dell'interfaccia di gestione, immettere la porta e selezionare l'interfaccia di gestione a cui la porta accede.
4. Selezionare **Sì** per la rete client non attendibile.
5. Utilizzare la scheda Manage external access (Gestisci accesso esterno) per bloccare tutte le porte esterne (con o senza indirizzi IP privilegiati impostati per gli host esterni alla subnet).

Dopo aver salvato la configurazione, solo gli host della subnet specificata possono accedere a Grid Manager. Tutti gli altri host sono bloccati.

Configurare il firewall interno

È possibile configurare il firewall StorageGRID per controllare l'accesso di rete a porte specifiche sui nodi StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Le informazioni sono state esaminate in "Gestire i controlli firewall" e. "Linee guida per il networking".
- Se si desidera che un nodo Admin o un nodo gateway accetti il traffico in entrata solo su endpoint configurati esplicitamente, sono stati definiti gli endpoint del bilanciamento del carico.

Quando si modifica la configurazione della rete client, le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

A proposito di questa attività

StorageGRID include un firewall interno su ciascun nodo che consente di aprire o chiudere alcune porte sui nodi della griglia. È possibile utilizzare le schede di controllo Firewall per aprire o chiudere le porte aperte per impostazione predefinita in Grid Network, Admin Network e Client Network. È inoltre possibile creare un elenco di indirizzi IP privilegiati che possono accedere alle porte della griglia chiuse. Se si utilizza una rete client, è possibile specificare se un nodo considera attendibile il traffico in entrata dalla rete client ed è possibile configurare l'accesso a porte specifiche sulla rete client.

Limitare il numero di porte aperte agli indirizzi IP esterni alla griglia solo a quelle assolutamente necessarie migliora la sicurezza della griglia. Utilizzare le impostazioni di ciascuna delle tre schede di controllo del firewall per assicurarsi che siano aperte solo le porte necessarie.

Per ulteriori informazioni sull'utilizzo dei controlli firewall, inclusi esempi, vedere "Gestire i controlli firewall".

Per ulteriori informazioni sui firewall esterni e sulla sicurezza di rete, vedere "Controllare l'accesso al firewall esterno".

Accedere ai controlli firewall

Fasi

1. Selezionare **CONFIGURATION** > **Security** > **Firewall control**.

   Le tre schede di questa pagina sono descritte nella "Gestire i controlli firewall".

2. Selezionare una scheda qualsiasi per configurare i controlli del firewall.

   È possibile utilizzare queste schede in qualsiasi ordine. Le configurazioni impostate su una scheda non limitano le operazioni che è possibile eseguire sulle altre schede; tuttavia, le modifiche alla configurazione apportate su una scheda potrebbero modificare il comportamento delle porte configurate su altre schede.

Elenco di indirizzi con privilegi

La scheda elenco indirizzi privilegiati consente agli host di accedere alle porte chiuse per impostazione predefinita o chiuse dalle impostazioni della scheda Gestisci accesso esterno.

Per impostazione predefinita, gli indirizzi IP e le subnet privilegiati non dispongono di accesso alla rete interna. Inoltre, gli endpoint del bilanciamento del carico e le porte aggiuntive aperte nella scheda Privileged address list (elenco indirizzi con privilegi) sono accessibili anche se bloccati nella scheda Manage external access (Gestisci accesso esterno).

Le impostazioni della scheda elenco indirizzi privilegiati non possono sostituire quelle della scheda rete client non attendibile.

Fasi

1. Nella scheda Privileged address list (elenco indirizzi privilegiati), inserire l'indirizzo o la subnet IP che si desidera concedere l'accesso alle porte chiuse.
2. Facoltativamente, selezionare **Aggiungi un altro indirizzo IP o subnet nella notazione CIDR** per aggiungere altri client con privilegi.

Aggiungere il minor numero possibile di indirizzi all'elenco dei privilegi.

3. Facoltativamente, selezionare **Allow Privileged IP address to access StorageGRID internal ports** (Consenti indirizzi IP privilegiati per l'accesso alle porte interne di Vedere "Porte interne StorageGRID".

Questa opzione rimuove alcune protezioni per i servizi interni. Se possibile, lasciarlo disattivato.

4. Selezionare **Salva**.

Gestire l'accesso esterno

Quando una porta viene chiusa nella scheda Manage external access (Gestisci accesso esterno), non è possibile accedervi da alcun indirizzo IP non Grid, a meno che non si aggiunga l'indirizzo IP all'elenco degli indirizzi privilegiati. Per impostazione predefinita, è possibile chiudere solo le porte aperte e solo quelle chiuse.

Le impostazioni della scheda Manage external access (Gestisci accesso esterno) non possono sostituire quelle della scheda Untrusted Client Network (rete client non attendibile). Ad esempio, se un nodo non è attendibile, la porta SSH/22 viene bloccata sulla rete client anche se è aperta nella scheda Manage external access (Gestisci accesso esterno). Le impostazioni della scheda Untrusted Client Network (rete client non attendibile) sovrascrivono le porte chiuse (ad esempio 443, 8443, 9443) della rete client.

Fasi

1. Selezionare **Gestisci accesso esterno**. La scheda visualizza una tabella con tutte le porte esterne (porte accessibili per impostazione predefinita dai nodi non griglia) per i nodi della griglia.
2. Configurare le porte che si desidera aprire e chiudere utilizzando le seguenti opzioni:
   - Utilizzare il pulsante di commutazione accanto a ciascuna porta per aprire o chiudere la porta selezionata.
   - Selezionare **Open all displayed ports** (Apri tutte le porte visualizzate) per aprire tutte le porte elencate nella tabella.
   - Selezionare **Chiudi tutte le porte visualizzate** per chiudere tutte le porte elencate nella tabella.

Se si chiudono le porte 443 o 8443 di Grid Manager, tutti gli utenti attualmente connessi a una porta bloccata, incluso l'utente, perderanno l'accesso a Grid Manager, a meno che il loro indirizzo IP non sia stato aggiunto all'elenco degli indirizzi privilegiati.

Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutte le porte disponibili. Utilizzare il campo di ricerca per trovare le impostazioni di qualsiasi porta esterna immettendo un numero di porta. È possibile inserire un numero di porta parziale. Ad esempio, se si immette **2**, vengono visualizzate tutte le porte che hanno la stringa "2" come parte del loro nome.

3. Selezionare **Salva**

Rete client non attendibile

Se la rete client di un nodo non è attendibile, il nodo accetta solo il traffico in entrata sulle porte configurate come endpoint del bilanciamento del carico e, facoltativamente, le porte aggiuntive selezionate in questa

scheda. È inoltre possibile utilizzare questa scheda per specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

> Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Le modifiche apportate alla configurazione nella scheda **Untrusted Client Network** (rete client non attendibile) sovrascrivono le impostazioni nella scheda **Manage external access** (Gestisci accesso esterno).

Fasi

1. Selezionare **Untrusted Client Network**.
2. Nella sezione Set New Node Default (Imposta nuovo nodo predefinito), specificare l'impostazione predefinita quando si aggiungono nuovi nodi alla griglia in una procedura di espansione.
   - **Trusted** (impostazione predefinita): Quando un nodo viene aggiunto in un'espansione, la sua rete client viene considerata attendibile.
   - **Untrusted**: Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile.

     Se necessario, è possibile tornare a questa scheda per modificare l'impostazione di un nuovo nodo specifico.

     > Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.
3. Utilizzare le seguenti opzioni per selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del carico configurati esplicitamente o su porte selezionate aggiuntive:
   - Selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi visualizzati nella tabella all'elenco Untrusted Client Network (rete client non attendibile).
   - Selezionare **Trust on displayed nodes** per rimuovere tutti i nodi visualizzati nella tabella dall'elenco Untrusted Client Network (rete client non attendibile).
   - Utilizzare l'interruttore accanto a ciascun nodo per impostare la rete client come attendibile o non attendibile per il nodo selezionato.

     Ad esempio, è possibile selezionare **Untrust on displayed nodes** per aggiungere tutti i nodi all'elenco Untrusted Client Network (rete client non attendibile), quindi utilizzare il pulsante di attivazione accanto a un singolo nodo per aggiungere tale singolo nodo all'elenco Trusted Client Network (rete client attendibile).

     > Utilizzare la barra di scorrimento sul lato destro della tabella per verificare di aver visualizzato tutti i nodi disponibili. Utilizzare il campo di ricerca per trovare le impostazioni per qualsiasi nodo immettendo il nome del nodo. È possibile immettere un nome parziale. Ad esempio, se si immette un valore **GW**, vengono visualizzati tutti i nodi che hanno la stringa "GW" come parte del loro nome.
4. Selezionare **Salva**.

   Le nuove impostazioni del firewall vengono applicate e applicate immediatamente. Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Gestire i tenant

Gestire i tenant: Panoramica

In qualità di amministratore di grid, è possibile creare e gestire gli account tenant utilizzati dai client S3 e Swift per memorizzare e recuperare gli oggetti.

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

Cosa sono gli account tenant?

Un account tenant consente di utilizzare l'API REST di S3 (Simple Storage Service) o l'API REST di Swift per memorizzare e recuperare oggetti in un sistema StorageGRID.

Ogni account tenant dispone di gruppi federati o locali, utenti, bucket S3 o container Swift e oggetti.

Gli account tenant possono essere utilizzati per separare gli oggetti memorizzati da diverse entità. Ad esempio, è possibile utilizzare più account tenant per uno dei seguenti casi di utilizzo:

- **Caso d'utilizzo aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, è possibile separare lo storage a oggetti del grid dai diversi reparti dell'organizzazione. In questo caso, è possibile creare account tenant per il reparto Marketing, il reparto Assistenza clienti, il reparto risorse umane e così via.

  Se si utilizza il protocollo client S3, è possibile utilizzare i bucket S3 e le policy bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Vedere le istruzioni per l'implementazione "Bucket S3 e policy bucket" per ulteriori informazioni.

- **Caso d'utilizzo del provider di servizi:** se si amministra un sistema StorageGRID come provider di servizi, è possibile separare lo storage a oggetti della griglia dalle diverse entità che affitteranno lo storage sulla griglia. In questo caso, è necessario creare account tenant per la società A, la società B, la società C e così via.

Per ulteriori informazioni, vedere "Utilizzare un account tenant".

Come si crea un account tenant?

Quando si crea un account tenant, si specificano le seguenti informazioni:

- Informazioni di base, tra cui il nome del tenant, il tipo di client (S3 o Swift) e la quota di storage opzionale.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine di identità, utilizzare S3 Select o utilizzare una connessione a federazione di griglie.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione di identità o SSO (Single Sign-on).

Inoltre, è possibile attivare l'impostazione blocco oggetti S3 per il sistema StorageGRID se gli account tenant S3 devono soddisfare i requisiti normativi. Quando S3 Object Lock è attivato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

A cosa serve il tenant manager?

Dopo aver creato l'account tenant, gli utenti tenant possono accedere a tenant Manager per eseguire attività come le seguenti:

- Configurare la federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia)
- Gestire gruppi e utenti
- Utilizza la federazione di grid per il clone dell'account e la replica cross-grid
- Gestire le chiavi di accesso S3
- Creare e gestire i bucket S3
- Utilizzare i servizi della piattaforma S3
- USA S3 Select
- Monitorare l'utilizzo dello storage

Mentre gli utenti del tenant S3 possono creare e gestire chiavi di accesso S3 e bucket con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Vedere "UTILIZZARE L'API REST S3" per ulteriori informazioni.

Gli utenti Swift devono disporre dell'autorizzazione di accesso root per accedere a Tenant Manager. Tuttavia, l'autorizzazione di accesso root non consente agli utenti di autenticarsi nell'API REST di Swift per creare container e acquisire oggetti. Gli utenti devono disporre dell'autorizzazione di amministratore Swift per autenticarsi nell'API DI Swift REST.

Creare un account tenant

È necessario creare almeno un account tenant per controllare l'accesso allo storage nel sistema StorageGRID.

I passaggi per la creazione di un account tenant variano in base al tipo di account "federazione delle identità" e. "single sign-on" Sono configurati e se l'account Grid Manager utilizzato per creare l'account tenant appartiene a un gruppo amministrativo con l'autorizzazione di accesso root.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".
- Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso root per l'account tenant a un gruppo federato, il gruppo federated è stato importato in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Vedere "Gestire i gruppi di amministratori".
- Se si desidera consentire a un tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket in un altro grid utilizzando una connessione a federazione di grid:
  - Lo hai fatto "configurazione della connessione a federazione di griglie".
  - Lo stato della connessione è **connesso**.
  - Si dispone dell'autorizzazione di accesso root.
  - Hai esaminato le considerazioni per "gestione dei tenant consentiti per la federazione di grid".

- Se l'account tenant utilizza l'origine dell'identità configurata per Grid Manager, lo stesso gruppo federated è stato importato in Grid Manager su entrambe le griglie.

  Quando si crea il tenant, si seleziona questo gruppo per disporre dell'autorizzazione di accesso root iniziale per gli account tenant di origine e di destinazione.

> Se questo gruppo di amministratori non esiste su entrambe le griglie prima di creare il tenant, il tenant non viene replicato nella destinazione.

Accedere alla procedura guidata

Fasi

1. Selezionare **TENANT**.
2. Selezionare **Crea**.

Inserire i dettagli

Fasi

1. Inserire i dettagli del tenant.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Quando viene creato, l'account tenant riceve un ID account univoco di 20 cifre.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant. Se si crea un tenant che utilizzerà una connessione a federazione di griglie, utilizzare questo campo per identificare il tenant di origine e il tenant di destinazione. Ad esempio, questa descrizione per un tenant creato sulla griglia 1 verrà visualizzata anche per il tenant replicato sulla griglia 2: "Questo tenant è stato creato sulla griglia 1".
Tipo di client	Il tipo di protocollo client utilizzato dal tenant, **S3** o **Swift**. **Nota**: Il supporto per le applicazioni client Swift è stato obsoleto e verrà rimosso in una release futura.
Quota di storage (opzionale)	Se si desidera che il tenant disponga di una quota di storage, un valore numerico per la quota e le unità.

2. Selezionare **continua**.

selezionare le autorizzazioni

Fasi

1. Se si desidera, selezionare le autorizzazioni desiderate per il tenant.

> Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, selezionare l'icona della guida per ciascuna autorizzazione.

Permesso	Se selezionato…
Consentire i servizi della piattaforma	Il tenant può utilizzare servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3".
Utilizza la propria origine di identità	Il tenant può configurare e gestire la propria origine di identità per gruppi e utenti federati. Questa opzione è disattivata se si dispone di "SSO configurato" Per il tuo sistema StorageGRID.
Consenti selezione S3	Il tenant può emettere richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant". **Importante**: Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.
USA connessione a federazione di griglie	Il tenant può utilizzare una connessione a federazione di grid. Selezionando questa opzione: • Consente di clonare questo tenant e tutti i gruppi tenant e gli utenti aggiunti all'account da questa griglia (la *griglia di origine*) all'altra griglia della connessione selezionata (la *griglia di destinazione*). • Consente a questo tenant di configurare la replica cross-grid tra i bucket corrispondenti su ogni grid. Vedere "Gestire i tenant consentiti per la federazione di grid".

2. Se si seleziona **Usa connessione federazione griglia**, selezionare una delle connessioni federazione griglia disponibili.

3. Selezionare **continua**.

Definire l'accesso root e creare il tenant

Fasi

1. Definire l'accesso root per l'account tenant, a seconda che il sistema StorageGRID utilizzi la federazione di identità, il single sign-on (SSO) o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

2. Selezionare **Crea tenant**.

   Viene visualizzato un messaggio di successo e il nuovo tenant viene elencato nella pagina tenant. Per informazioni su come visualizzare i dettagli del tenant e monitorare l'attività del tenant, vedere "Monitorare l'attività del tenant".

3. Se è stata selezionata l'autorizzazione **Usa connessione federazione griglia** per il tenant:
   a. Verificare che un tenant identico sia stato replicato nell'altra griglia della connessione. I tenant di entrambe le griglie avranno lo stesso ID account a 20 cifre, il nome, la descrizione, la quota e le autorizzazioni.

      Se viene visualizzato il messaggio di errore "tenant creato senza clone", fare riferimento alle istruzioni riportate nella "Risolvere i problemi relativi agli errori di federazione della griglia".

   b. Se è stata fornita una password utente root locale durante la definizione dell'accesso root, "modificare la password per l'utente root locale" per il tenant replicato.

      Un utente root locale non può accedere a Tenant Manager nella griglia di destinazione fino a quando la password non viene modificata.

Accesso al tenant (facoltativo)

Se necessario, è possibile accedere al nuovo tenant ora per completare la configurazione oppure accedere al tenant in un secondo momento. La procedura di accesso dipende dal fatto che si sia effettuato l'accesso a Grid Manager utilizzando la porta predefinita (443) o una porta con restrizioni. Vedere "Controllare l'accesso al firewall esterno".

Accedi subito

Se si utilizza…	Eseguire questa operazione…
Porta 443 e viene impostata una password per l'utente root locale	1. Selezionare **Accedi come root**. Al momento dell'accesso, vengono visualizzati i collegamenti per la configurazione di bucket, federazione di identità, gruppi e utenti. 2. Selezionare i collegamenti per configurare l'account tenant. Ciascun collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, consultare "istruzioni per l'utilizzo degli account tenant".
Porta 443 e non è stata impostata una password per l'utente root locale	Selezionare **Accedi** e immettere le credenziali per un utente nel gruppo federated di accesso root.
Una porta con restrizioni	1. Selezionare **fine** 2. Selezionare **limitato** nella tabella tenant per ulteriori informazioni sull'accesso a questo account tenant. L'URL del tenant manager ha il seguente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *port* è la porta solo tenant ◦ *20-digit-account-id* È l'ID account univoco del tenant

Accedi più tardi

Se si utilizza…	Eseguire una di queste operazioni…
Porta 443	• Da Grid Manager, selezionare **TENANT** e selezionare **Sign in** (Accedi) a destra del nome del tenant. • Inserire l'URL del tenant in un browser Web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *20-digit-account-id* È l'ID account univoco del tenant

Se si utilizza…	Eseguire una di queste operazioni…
Una porta con restrizioni	• Da Grid Manager, selezionare **TENANT** e selezionare **Restricted**. • Inserire l'URL del tenant in un browser Web: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *port* è la porta limitata solo tenant ◦ *20-digit-account-id* È l'ID account univoco del tenant

Configurare il tenant

Seguire le istruzioni riportate in "Utilizzare un account tenant" Per gestire gruppi di tenant e utenti, chiavi di accesso S3, bucket, servizi di piattaforma e replica di cloni di account e cross-grid.

Modificare l'account tenant

È possibile modificare un account tenant per modificare il nome visualizzato, la quota di storage o le autorizzazioni del tenant.

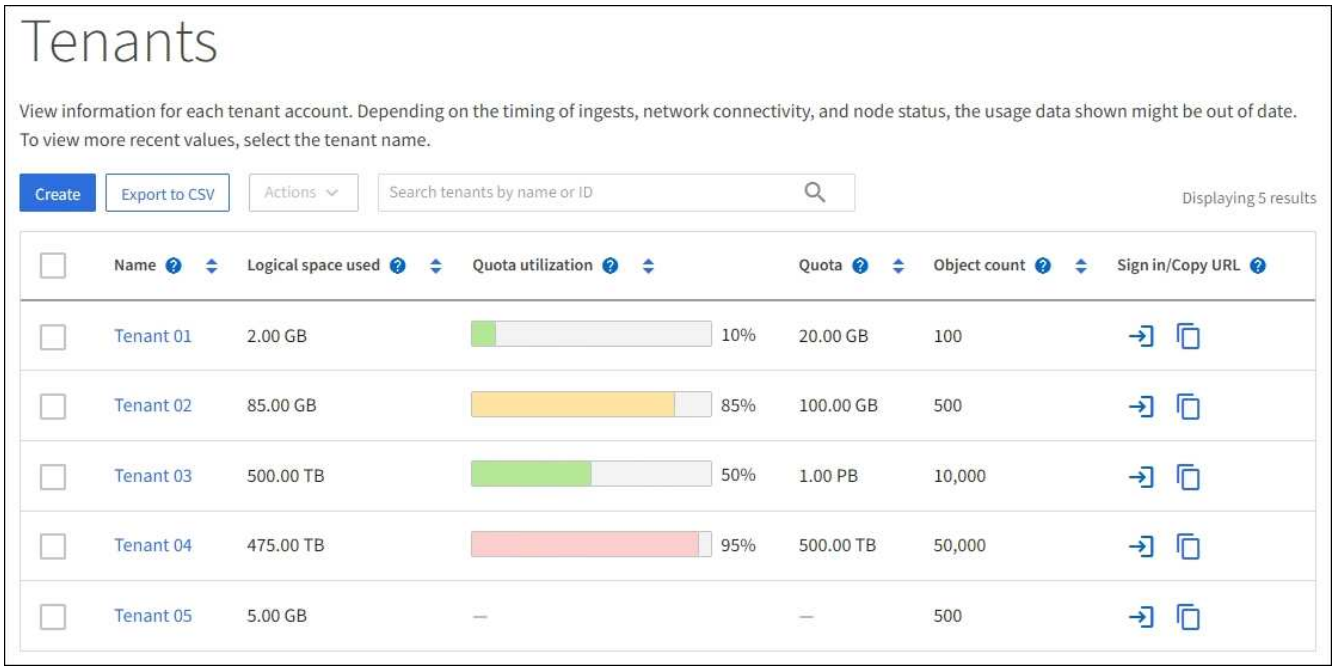
Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da una delle griglie della connessione. Tuttavia, qualsiasi modifica apportata su una griglia della connessione non verrà copiata nell'altra griglia. Se si desidera mantenere i dettagli del tenant perfettamente sincronizzati tra le griglie, apportare le stesse modifiche su entrambe le griglie. Vedere "Gestire i tenant consentiti per la connessione a federazione di grid".

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".

Fasi

1. Selezionare **TENANT**.



2. Individuare l'account tenant che si desidera modificare.

   Utilizzare la casella di ricerca per cercare un tenant in base al nome o all'ID del tenant.

3. Selezionare il tenant. È possibile effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo del tenant e selezionare **azioni** > **Modifica**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **Modifica**.
4. Facoltativamente, modificare i valori per questi campi:
   - **Nome**
   - **Descrizione**
   - **Quota di storage**
5. Selezionare **continua**.
6. Selezionare o deselezionare le autorizzazioni per l'account tenant.
   - Se si disattiva **Platform Services** per un tenant che li sta già utilizzando, i servizi configurati per i bucket S3 smetteranno di funzionare. Non viene inviato alcun messaggio di errore al tenant. Ad esempio, se il tenant ha configurato la replica CloudMirror per un bucket S3, può comunque memorizzare oggetti nel bucket, ma le copie di tali oggetti non verranno più eseguite nel bucket S3 esterno configurato come endpoint. Vedere "Gestire i servizi della piattaforma per gli account tenant S3".
   - Modificare l'impostazione di **utilizza la propria origine dell'identità** per determinare se l'account tenant utilizzerà la propria origine dell'identità o l'origine dell'identità configurata per Grid Manager.

     Se **utilizza la propria origine di identità** è:

     - Disattivato e selezionato, il tenant ha già attivato la propria origine di identità. Un tenant deve disattivare l'origine dell'identità prima di poter utilizzare l'origine dell'identità configurata per Grid Manager.
     - Disattivato e non selezionato, SSO è attivato per il sistema StorageGRID. Il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager.

- Selezionare o deselezionare l'autorizzazione **Allow S3 Select** (Consenti selezione S3) in base alle necessità. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant".
- Per rimuovere l'autorizzazione **Use grid Federation Connection**:
  i. Vai alla pagina dei dettagli del locatario.
  ii. Selezionare la scheda **federazione griglia**.
  iii. Selezionare **Rimuovi permesso**.
- Per aggiungere l'autorizzazione **Use grid Federation Connection**:
  i. Selezionare la casella di controllo **Usa connessione federazione griglia**.
  ii. Facoltativamente, selezionare **Clona utenti e gruppi locali esistenti** per clonarli nella griglia remota. Se si desidera, è possibile interrompere la clonazione in corso o riprovare a eseguire la clonazione se la clonazione di alcuni utenti o gruppi locali non è riuscita una volta completata l'ultima operazione di clonazione.

Modificare la password per l'utente root locale del tenant

Potrebbe essere necessario modificare la password per l'utente root locale di un tenant se l'utente root è bloccato dall'account.

Prima di iniziare

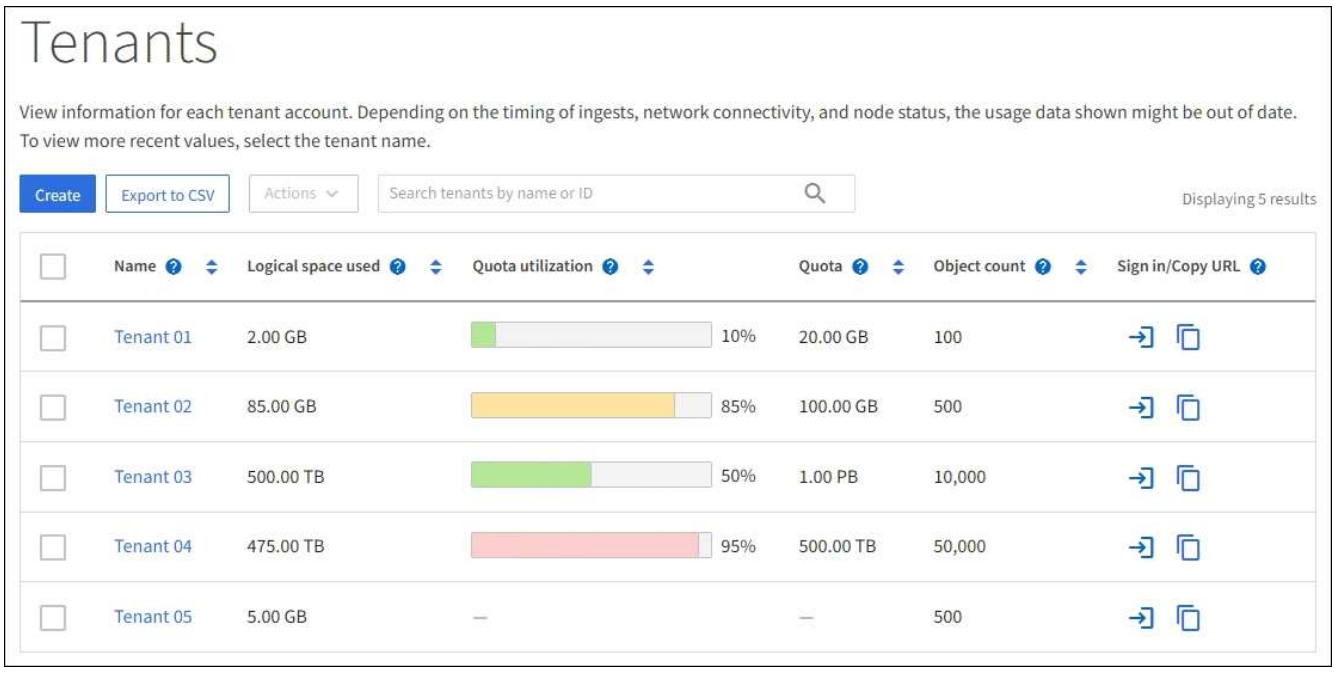
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Se il sistema StorageGRID è abilitato per il Single Sign-on (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire le attività dell'utente root, gli utenti devono appartenere a un gruppo federated che disponga dell'autorizzazione di accesso root per il tenant.

Fasi

1. Selezionare **TENANT**.



2. Selezionare l'account tenant. È possibile effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo del tenant e selezionare **azioni** > **Modifica password root**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **azioni** > **Modifica password root**.
3. Inserire la nuova password per l'account tenant.
4. Selezionare **Salva**.

Elimina account tenant

È possibile eliminare un account tenant se si desidera rimuovere in modo permanente l'accesso del tenant al sistema.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Sono stati rimossi tutti i bucket (S3), i container (Swift) e gli oggetti associati all'account tenant.
- Se il tenant è autorizzato a utilizzare una connessione a federazione di griglie, sono state esaminate le considerazioni per "Eliminazione di un tenant con l'autorizzazione di connessione Usa federazione griglia".

Fasi

1. Selezionare **TENANT**.
2. Individuare l'account tenant o gli account che si desidera eliminare.

   Utilizzare la casella di ricerca per cercare un tenant in base al nome o all'ID del tenant.

3. Per eliminare più tenant, selezionare le caselle di controllo e selezionare **azioni** > **Elimina**.
4. Per eliminare un singolo tenant, effettuare una delle seguenti operazioni:
   - Selezionare la casella di controllo e selezionare **azioni** > **Elimina**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **azioni** > **Elimina**.
5. Selezionare **Sì**.

Gestire i servizi della piattaforma

Gestione dei servizi di piattaforma per i tenant: Panoramica

Se si abilitano i servizi della piattaforma per gli account tenant S3, è necessario configurare il grid in modo che i tenant possano accedere alle risorse esterne necessarie per l'utilizzo di questi servizi.

Cosa sono i servizi della piattaforma?

I servizi della piattaforma includono la replica di CloudMirror, le notifiche degli eventi e il servizio di integrazione della ricerca.

Replica di CloudMirror

Il servizio di replica di StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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

> La replica di CloudMirror presenta alcune importanti analogie differenze con la funzionalità di replica cross-grid. Per ulteriori informazioni, vedere "Confronta la replica cross-grid e la replica CloudMirror".

> La replica di CloudMirror non è supportata se il bucket di origine ha attivato il blocco oggetti S3.

Notifiche

Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite su oggetti a un cluster Kafka esterno specifico o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.

> Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantieni fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

Servizio di integrazione della ricerca

Il servizio di integrazione della ricerca viene utilizzato per inviare i metadati degli oggetti S3 a un indice Elasticsearch specificato, in cui è possibile cercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, è possibile configurare i bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. È quindi possibile utilizzare Elasticsearch per eseguire ricerche tra bucket ed eseguire analisi sofisticate dei modelli presenti nei metadati degli oggetti.

> Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock attivato, i metadati S3 Object Lock (inclusi Retain until Date e Legal Hold status) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono ai tenant la possibilità di utilizzare risorse di storage esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione dei servizi della piattaforma è generalmente esterna alla distribuzione di StorageGRID, è necessario decidere se consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o modificano gli account tenant. È inoltre necessario configurare la rete in modo che i messaggi dei servizi della piattaforma generati dai tenant possano raggiungere le proprie destinazioni.

Consigli per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, tenere presenti i seguenti consigli:

- Se in un bucket S3 nel sistema StorageGRID sono attivate sia la versione che la replica CloudMirror, è necessario attivare anche la versione del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica di CloudMirror di generare versioni di oggetti simili sull'endpoint.

- Non utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica CloudMirror, le notifiche e l'integrazione della ricerca. La presenza di più di 100 tenant attivi può rallentare le performance del client S3.
- Le richieste a un endpoint che non possono essere completate verranno messe in coda per un massimo di 500,000 richieste. Questo limite è equamente condiviso tra i tenant attivi. I nuovi tenant possono superare temporaneamente questo limite di 500,000, in modo che i nuovi tenant non vengano penalizzati in modo ingiusto.

Informazioni correlate

- "Gestire i servizi della piattaforma"
- "Configurare le impostazioni del proxy di storage"
- "Monitorare StorageGRID"

Rete e porte per i servizi della piattaforma

Se si consente a un tenant S3 di utilizzare i servizi della piattaforma, è necessario configurare la rete per la griglia per garantire che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

È possibile abilitare i servizi della piattaforma per un account tenant S3 quando si crea o si aggiorna l'account tenant. Se i servizi della piattaforma sono attivati, il tenant può creare endpoint che fungono da destinazione per la replica CloudMirror, le notifiche di eventi o i messaggi di integrazione di ricerca dai bucket S3. Questi messaggi dei servizi della piattaforma vengono inviati dai nodi di storage che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Cluster Elasticsearch ospitato localmente
- Un'applicazione locale che supporta la ricezione di messaggi Amazon Simple Notification Service
- Un cluster Kafka ospitato localmente
- Un bucket S3 ospitato localmente sulla stessa o su un'altra istanza di StorageGRID
- Un endpoint esterno, ad esempio un endpoint su Amazon Web Services.

Per garantire che i messaggi dei servizi della piattaforma possano essere inviati, è necessario configurare la rete o le reti contenenti i nodi di storage ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi della piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati alle seguenti porte:

- **80**: Per gli URI endpoint che iniziano con http (la maggior parte degli endpoint)
- **443**: Per gli URI endpoint che iniziano con https (la maggior parte degli endpoint)
- **9092**: Per gli URI endpoint che iniziano con http o https (solo endpoint Kafka)

I tenant possono specificare una porta diversa quando creano o modificano un endpoint.

> Se si utilizza un'implementazione StorageGRID come destinazione della replica di CloudMirror, i messaggi di replica potrebbero essere ricevuti su una porta diversa da 80 o 443. Assicurarsi che la porta utilizzata per S3 dall'implementazione StorageGRID di destinazione sia specificata nell'endpoint.

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

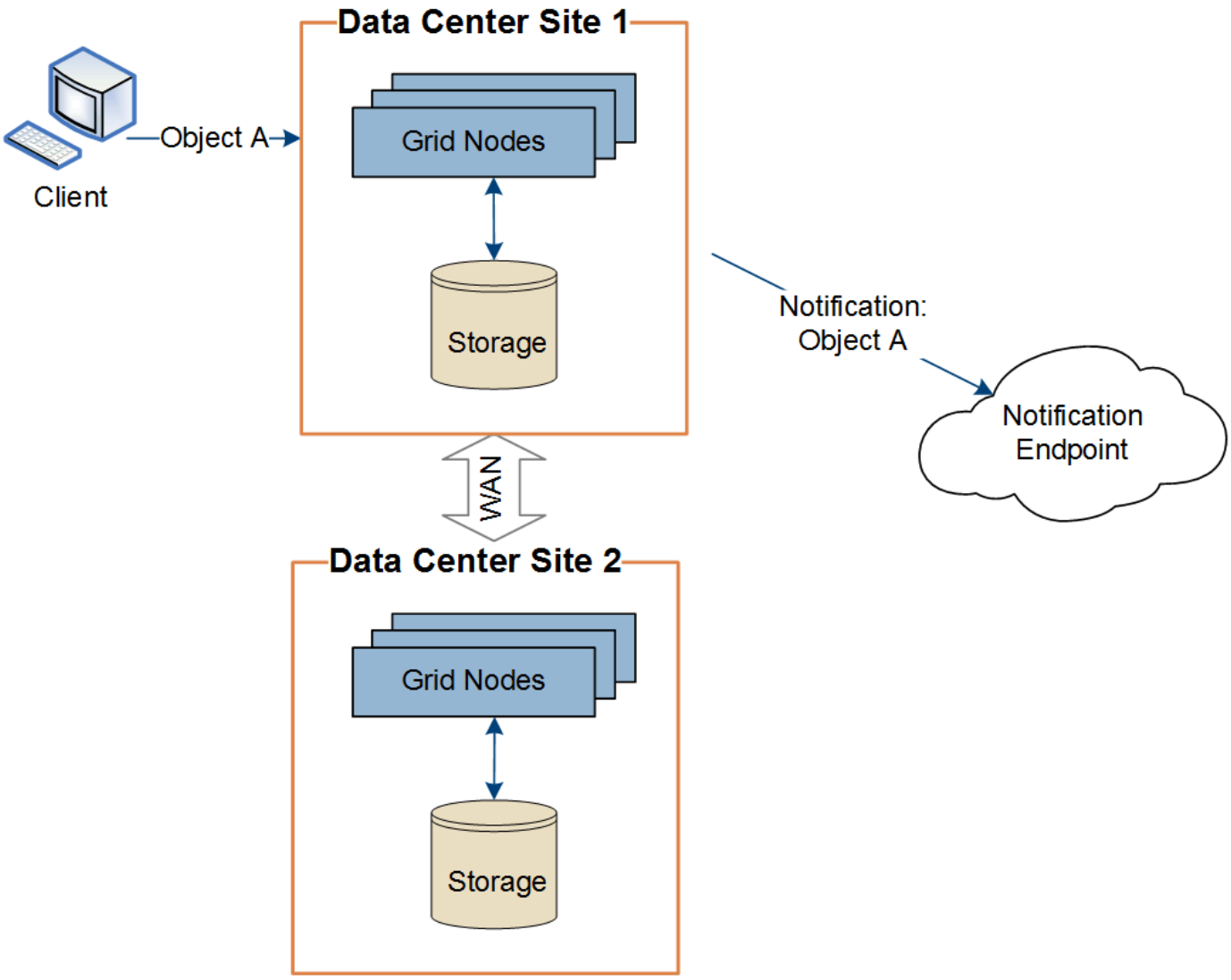
Informazioni correlate

- "Utilizzare un account tenant"

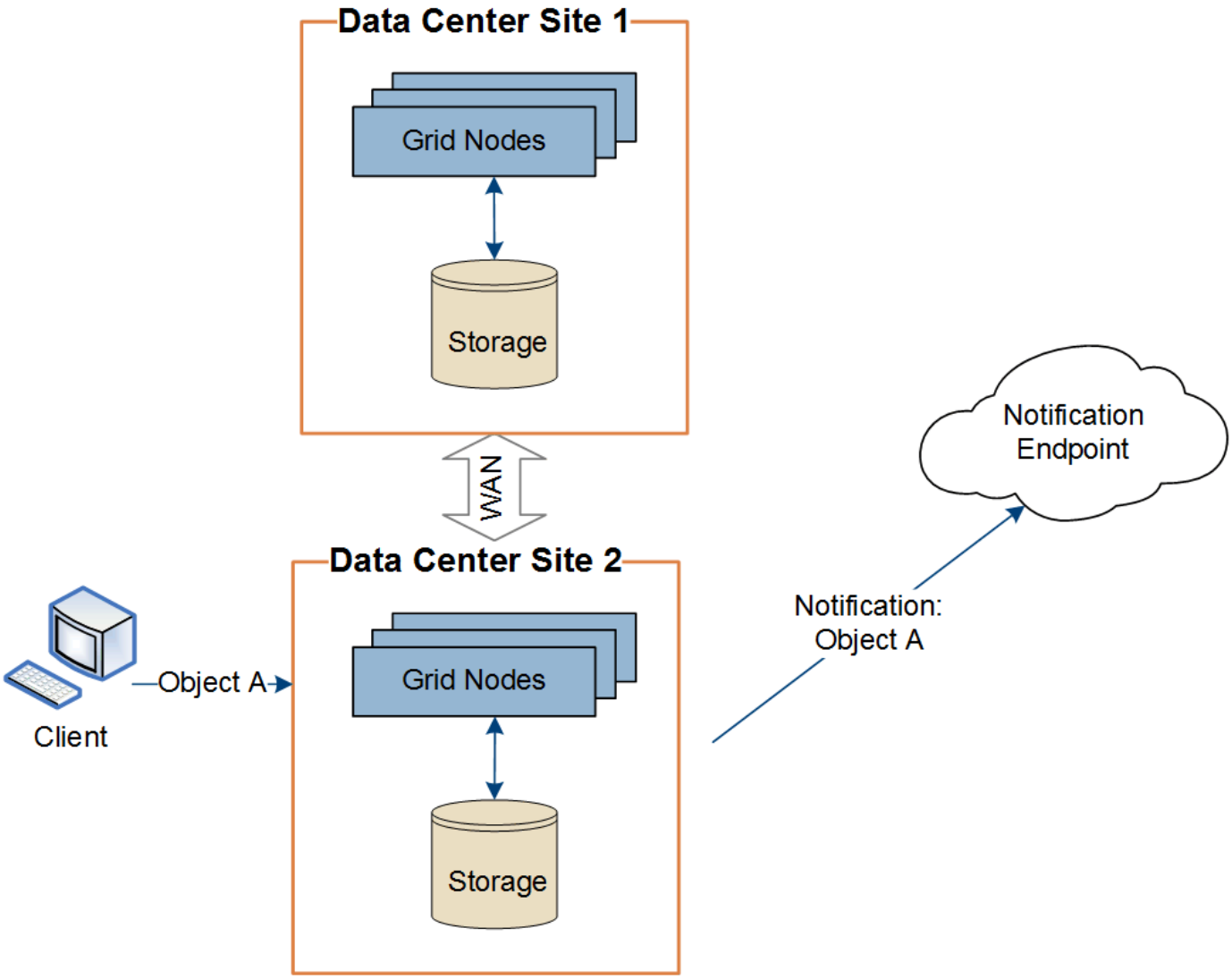
Erogazione per sito di messaggi relativi ai servizi della piattaforma

Tutte le operazioni dei servizi della piattaforma vengono eseguite in base al sito.

Cioè, se un tenant utilizza un client per eseguire un'operazione S3 API Create su un oggetto connettendosi a un nodo gateway nel sito 1 del data center, la notifica relativa a tale azione viene attivata e inviata dal sito 1 del data center.



Se il client esegue successivamente un'operazione di eliminazione API S3 sullo stesso oggetto dal sito del data center 2, la notifica relativa all'azione di eliminazione viene attivata e inviata dal sito del data center 2.



Assicurarsi che la rete di ciascun sito sia configurata in modo che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risolvere i problemi relativi ai servizi della piattaforma

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti del tenant in Tenant Manager; tuttavia, se un tenant ha problemi nella configurazione o nell'utilizzo dei servizi della piattaforma, potrebbe essere possibile utilizzare Grid Manager per risolvere il problema.

Problemi con i nuovi endpoint

Prima che un tenant possa utilizzare i servizi della piattaforma, deve creare uno o più endpoint utilizzando il tenant Manager. Ciascun endpoint rappresenta una destinazione esterna per un servizio di piattaforma, come un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento del servizio di notifica semplice Amazon, un argomento di Kafka o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna che le credenziali necessarie per accedere a tale risorsa.

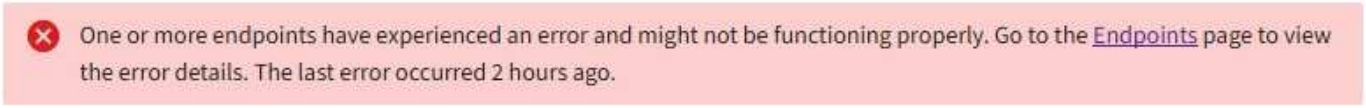
Quando un tenant crea un endpoint, il sistema StorageGRID convalida che l'endpoint esiste e che può essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

Se la convalida degli endpoint non riesce, viene visualizzato un messaggio di errore che spiega perché la convalida degli endpoint non è riuscita. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.

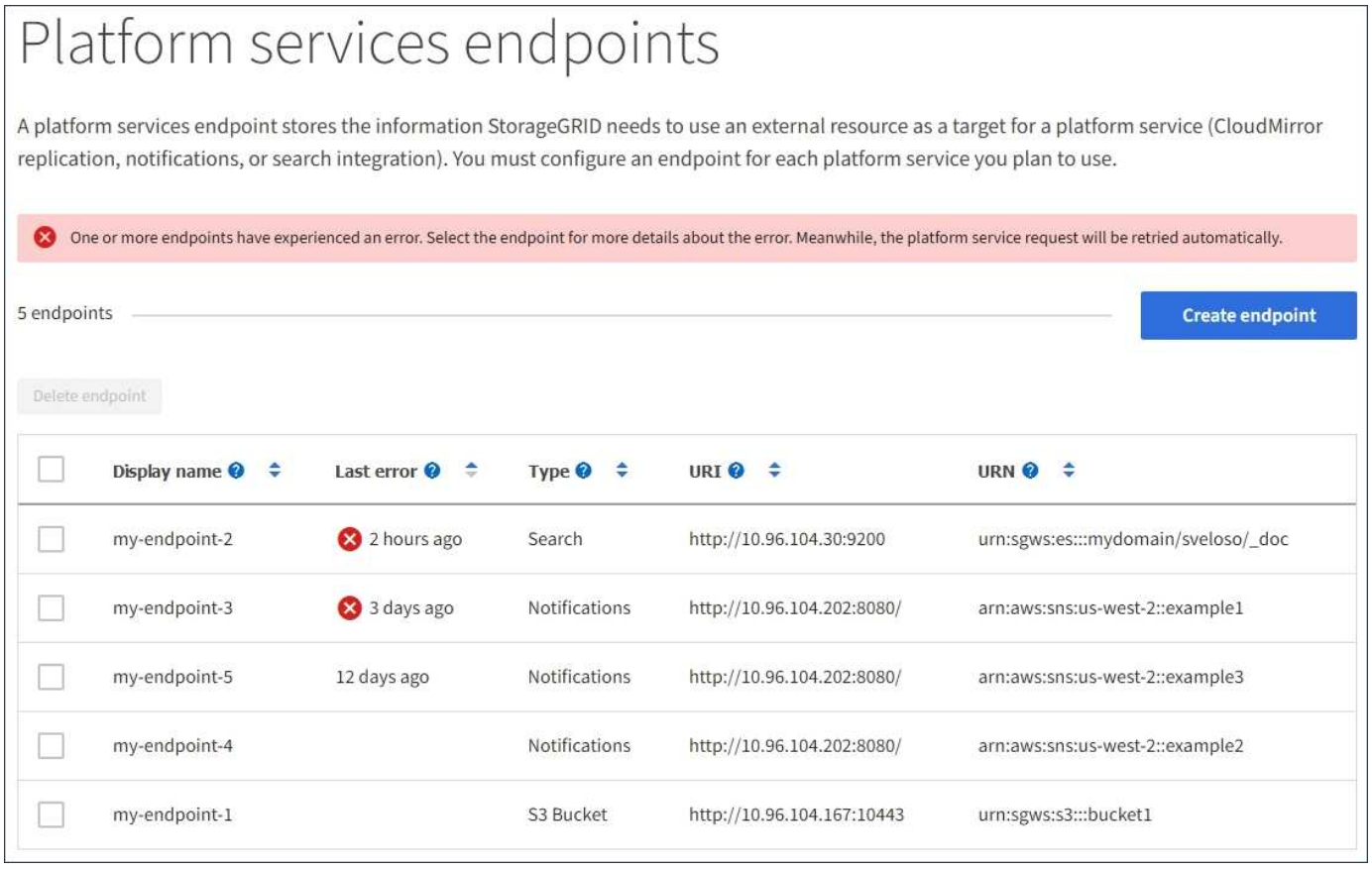
La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant.

Problemi con gli endpoint esistenti

Se si verifica un errore quando StorageGRID tenta di raggiungere un endpoint esistente, viene visualizzato un messaggio sul dashboard in Gestione tenant.



Gli utenti del tenant possono accedere alla pagina degli endpoint per esaminare il messaggio di errore più recente per ciascun endpoint e per determinare quanto tempo fa si è verificato l'errore. La colonna **ultimo errore** visualizza il messaggio di errore più recente per ciascun endpoint e indica per quanto tempo si è verificato l'errore. Errori che includono si è verificata negli ultimi 7 giorni.



Alcuni messaggi di errore nella colonna **ultimo errore** potrebbero includere un LOGID tra parentesi. Un amministratore della griglia o il supporto tecnico può utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se è stato configurato un "proxy di storage" Tra i nodi di storage e gli endpoint del servizio della piattaforma, potrebbero verificarsi errori se il servizio proxy non consente messaggi da StorageGRID. Per risolvere questi problemi, controllare le impostazioni del server proxy per assicurarsi che i messaggi relativi al servizio della piattaforma non siano bloccati.

Determinare se si è verificato un errore

Se si sono verificati errori degli endpoint negli ultimi 7 giorni, il dashboard di Tenant Manager visualizza un messaggio di avviso. È possibile accedere alla pagina Endpoint per ulteriori dettagli sull'errore.

Le operazioni del client non riescono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il malfunzionamento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non vengono eseguite correttamente se il servizio RSM (Replicated state Machine) interno viene arrestato o se sono presenti troppi messaggi dei servizi della piattaforma in coda per il recapito.

Per controllare lo stato dei servizi:

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node*** > **SSM** > **Services**.

Errori degli endpoint ripristinabili e non ripristinabili

Una volta creati gli endpoint, gli errori di richiesta del servizio della piattaforma possono verificarsi per diversi motivi. Alcuni errori possono essere ripristinati con l'intervento dell'utente. Ad esempio, potrebbero verificarsi errori ripristinabili per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o scadute.
- Il bucket di destinazione non esiste.
- Impossibile ricevere la notifica.

Se StorageGRID rileva un errore ripristinabile, la richiesta di servizio della piattaforma verrà rievitata fino a quando non avrà esito positivo.

Altri errori non sono ripristinabili. Ad esempio, se l'endpoint viene cancellato, si verifica un errore irreversibile.

Se StorageGRID rileva un errore irreversibile dell'endpoint, l'allarme legacy Eventi totali (SMTT) viene attivato in Gestione griglia. Per visualizzare l'allarme legacy Total Events (Eventi totali):

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***site*** > ***node*** > **SSM** > **Eventi**.
3. Visualizza ultimo evento nella parte superiore della tabella.

   I messaggi degli eventi sono elencati anche nella `/var/local/log/bycast-err.log`.

4. Seguire le indicazioni fornite nel contenuto degli allarmi SMTT per correggere il problema.
5. Selezionare la scheda **Configurazione** per ripristinare i conteggi degli eventi.
6. Notificare al tenant gli oggetti i cui messaggi dei servizi della piattaforma non sono stati recapitati.
7. Chiedere al tenant di riattivare la replica o la notifica non riuscita aggiornando i metadati o i tag

dell'oggetto.

Il tenant può reinviare i valori esistenti per evitare modifiche indesiderate.

I messaggi dei servizi della piattaforma non possono essere inviati

Se la destinazione incontra un problema che impedisce l'accettazione dei messaggi dei servizi della piattaforma, l'operazione client sul bucket riesce, ma il messaggio dei servizi della piattaforma non viene recapitato. Ad esempio, questo errore potrebbe verificarsi se le credenziali vengono aggiornate sulla destinazione in modo che StorageGRID non possa più autenticare il servizio di destinazione.

Se i messaggi dei servizi della piattaforma non possono essere inviati a causa di un errore irreversibile, l'allarme legacy SMTT (Total Events) viene attivato in Grid Manager.

Performance più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe ridurre le richieste S3 in entrata per un bucket se la velocità con cui le richieste vengono inviate supera la velocità con cui l'endpoint di destinazione può ricevere le richieste. La limitazione si verifica solo quando è presente un backlog di richieste in attesa di essere inviate all'endpoint di destinazione.

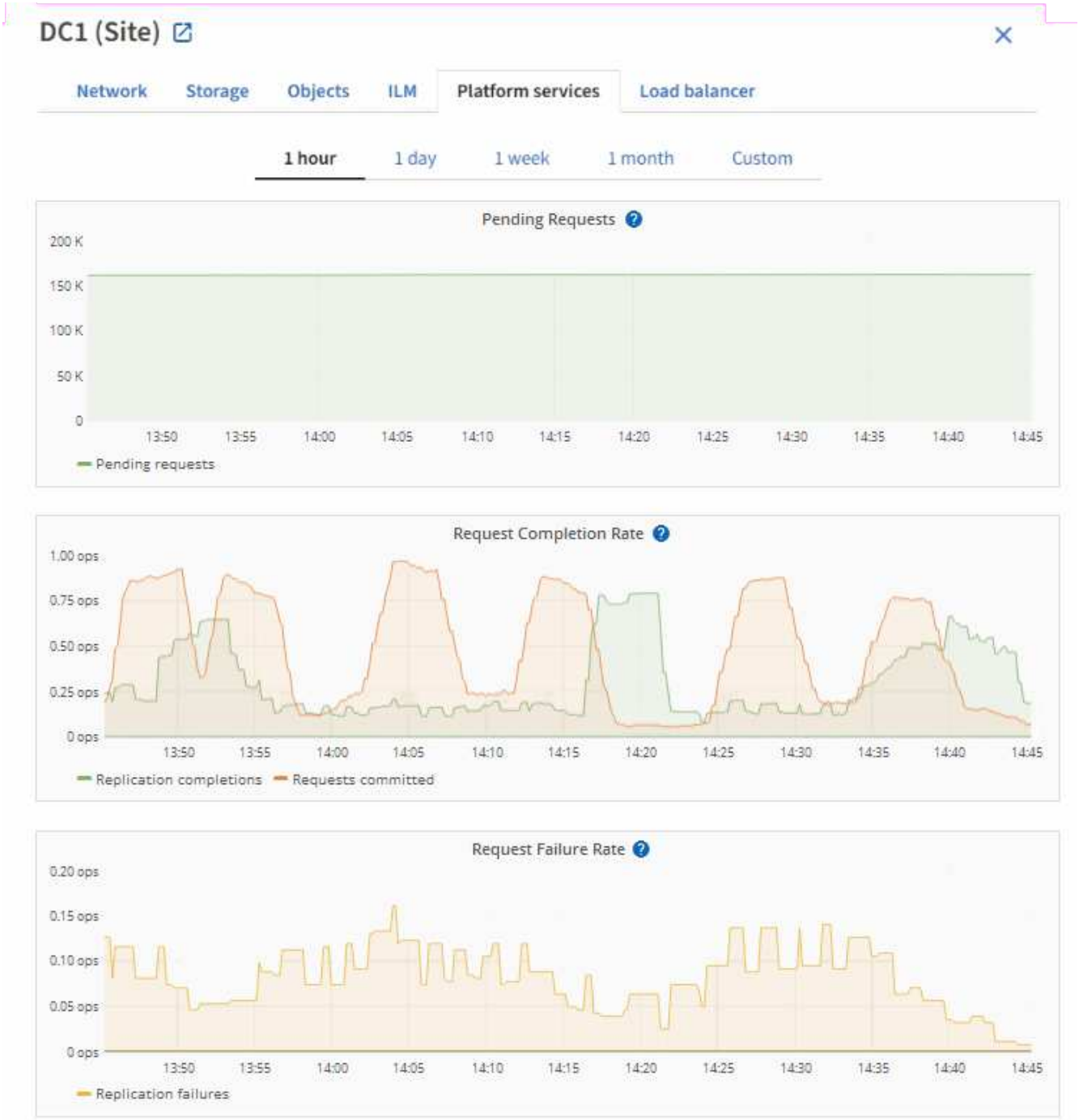
L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, le operazioni del client S3 (come LE richieste PUT) finiranno per fallire.

È più probabile che le richieste CloudMirror siano influenzate dalle performance dell'endpoint di destinazione, perché queste richieste comportano in genere un maggior numero di trasferimenti di dati rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma non vengono soddisfatte

Per visualizzare il tasso di errore della richiesta per i servizi della piattaforma:

1. Selezionare **NODI**.
2. Selezionare ***Site*** > **Platform Services**.
3. Visualizza il grafico tasso di errore della richiesta.



Avviso di servizi della piattaforma non disponibili

L'avviso **Platform Services unavailable** (servizi piattaforma non disponibili) indica che non è possibile eseguire operazioni di servizio della piattaforma in un sito perché sono in esecuzione o disponibili troppi nodi di storage con il servizio RSM.

Il servizio RSM garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.

Per risolvere questo avviso, determinare quali nodi di storage del sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di storage che includono anche il servizio ADC). Quindi, assicurarsi che la maggior parte di questi nodi di storage sia in esecuzione e disponibile.

Se più di un nodo di storage che contiene il servizio RSM si guasta in un sito, si perdono le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori linee guida per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni, vedere **Utilizzare un account tenant › risolvere i problemi relativi agli endpoint dei servizi della piattaforma**.

Informazioni correlate

- "Risolvere i problemi relativi al sistema StorageGRID"

Manage S3 (Gestisci S3): Selezionare per gli account tenant

È possibile consentire a determinati tenant S3 di utilizzare S3 Select per emettere richieste SelectObjectContent su singoli oggetti.

S3 Select offre un modo efficiente per cercare grandi quantità di dati senza dover implementare un database e le risorse associate per abilitare le ricerche. Inoltre, riduce i costi e la latenza del recupero dei dati.

Che cos'è S3 Select?

S3 Select consente ai client S3 di utilizzare le richieste SelectObjectContent per filtrare e recuperare solo i dati necessari da un oggetto. L'implementazione StorageGRID di S3 Select include un sottoinsieme di comandi e funzionalità S3 Select.

Considerazioni e requisiti per l'utilizzo di S3 Select

Requisiti di amministrazione della griglia

L'amministratore della griglia deve concedere ai tenant l'abilità S3 Select. Selezionare **Allow S3 Select** when (Consenti selezione S3) "creazione di un tenant" oppure "modifica di un tenant".

Requisiti di formato degli oggetti

L'oggetto che si desidera sottoporre a query deve essere in uno dei seguenti formati:

- **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
- **Parquet**. Requisiti aggiuntivi per gli oggetti in parquet:
  - S3 Select supporta solo la compressione colonnare con GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti parquet.
  - S3 Select non supporta l'output parquet. Specificare il formato di output come CSV o JSON.
  - La dimensione massima del gruppo di righe non compresso è di 512 MB.
  - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
  - Non è possibile utilizzare TIPI logici INTERVAL, JSON, LIST, TIME o UUID.

Requisiti degli endpoint

La richiesta SelectObjectContent deve essere inviata a "Endpoint del bilanciamento del carico di StorageGRID".

I nodi Admin e Gateway utilizzati dall'endpoint devono essere uno dei seguenti:

- Un nodo di appliance per i servizi
- Nodo software basato su VMware
- Nodo bare metal che esegue un kernel con cgroup v2 abilitato

Considerazioni generali

Le query non possono essere inviate direttamente ai nodi di storage.

> Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.

Vedere "Istruzioni per l'utilizzo di S3 Select".

Per visualizzare "Grafici Grafana" Per le operazioni S3 Select nel tempo, selezionare **SUPPORT** > **Tools** > **Metrics** in Grid Manager.

Configurare le connessioni client

Configurazione delle connessioni client S3 e Swift: Panoramica

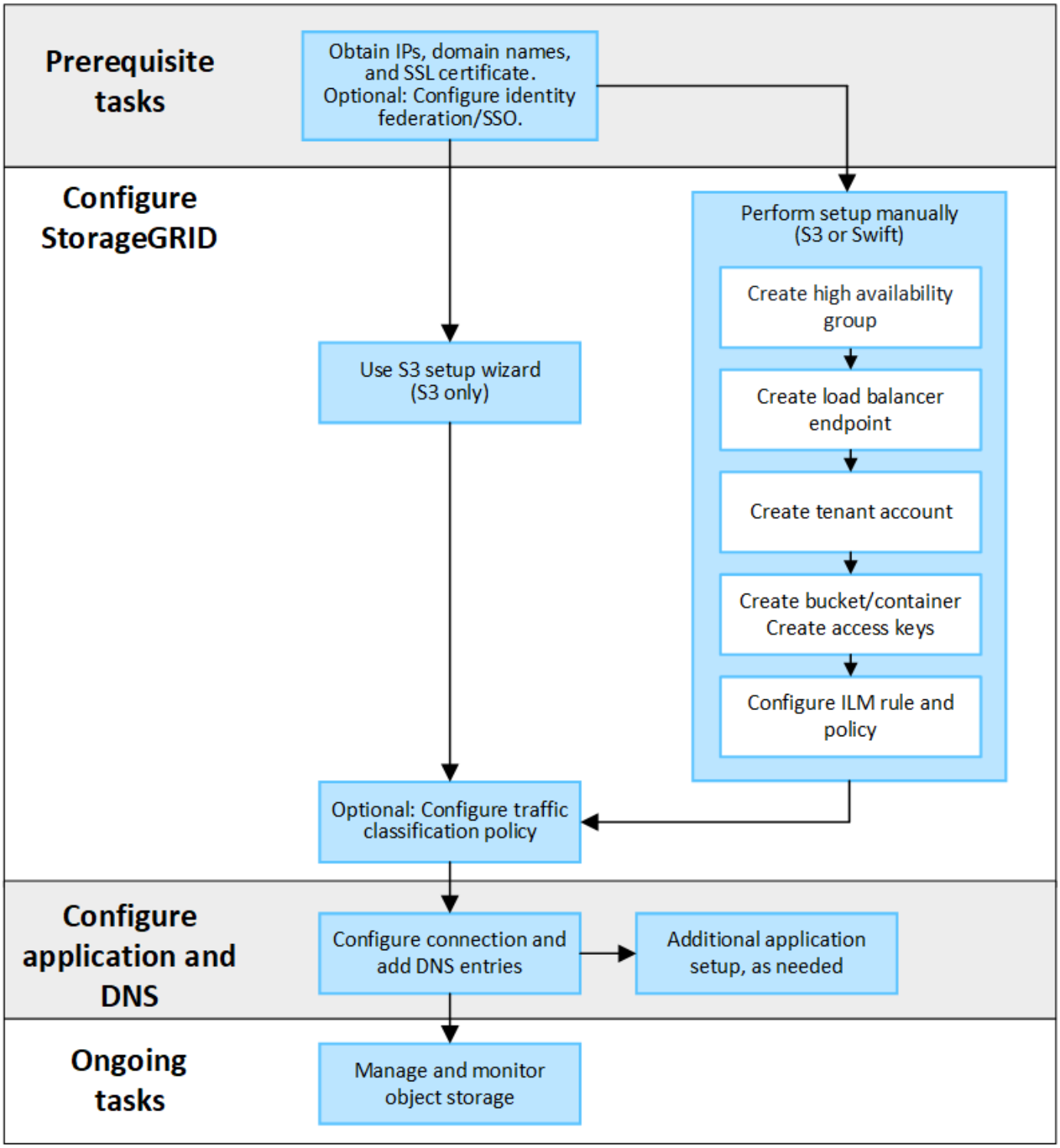
In qualità di amministratore di grid, gestisci le opzioni di configurazione che controllano il modo in cui le applicazioni client S3 e Swift si connettono al sistema StorageGRID per memorizzare e recuperare i dati.

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

Workflow di configurazione

Come illustrato nel diagramma del flusso di lavoro, sono disponibili quattro passaggi principali per la connessione di StorageGRID a qualsiasi applicazione S3 o Swift:

1. Eseguire attività preliminari in StorageGRID, in base al modo in cui l'applicazione client si connetterà a StorageGRID.
2. Utilizzare StorageGRID per ottenere i valori necessari all'applicazione per connettersi alla griglia. È possibile utilizzare l'installazione guidata S3 o configurare manualmente ogni entità StorageGRID.
3. Utilizzare l'applicazione S3 o Swift per completare la connessione a StorageGRID. Creare voci DNS per associare gli indirizzi IP ai nomi di dominio che si intende utilizzare.
4. Eseguire attività in corso nell'applicazione e in StorageGRID per gestire e monitorare lo storage a oggetti nel tempo.



Informazioni necessarie per collegare StorageGRID a un'applicazione client

Prima di poter collegare StorageGRID a un'applicazione client S3 o Swift, è necessario eseguire i passaggi di configurazione in StorageGRID e ottenere un determinato valore.

Di quali valori ho bisogno?

La seguente tabella mostra i valori da configurare in StorageGRID e i valori utilizzati dall'applicazione S3 o Swift e dal server DNS.

Valore	Dove è configurato il valore	Dove viene utilizzato il valore
Indirizzi IP virtuali (VIP)	StorageGRID > Gruppo ha	Voce DNS
Porta	StorageGRID > endpoint del bilanciamento del carico	Applicazione client
Certificato SSL	StorageGRID > endpoint del bilanciamento del carico	Applicazione client
Nome server (FQDN)	StorageGRID > endpoint del bilanciamento del carico	• Applicazione client • Voce DNS
ID chiave di accesso S3 e chiave di accesso segreta	StorageGRID > tenant e bucket	Applicazione client
Nome bucket/container	StorageGRID > tenant e bucket	Applicazione client

Come si ottengono questi valori?

In base alle proprie esigenze, è possibile effettuare una delle seguenti operazioni per ottenere le informazioni necessarie:

- **Utilizzare il "Installazione guidata S3"**. L'installazione guidata S3 consente di configurare rapidamente i valori richiesti in StorageGRID e di creare uno o due file da utilizzare per la configurazione dell'applicazione S3. La procedura guidata guida l'utente attraverso i passaggi richiesti e aiuta a verificare che le impostazioni siano conformi alle Best practice di StorageGRID.

  > Se si sta configurando un'applicazione S3, si consiglia di utilizzare la procedura guidata di configurazione S3, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

- **Utilizzare il "Installazione guidata di FabricPool"**. Analogamente all'installazione guidata di S3, l'installazione guidata di FabricPool consente di configurare rapidamente i valori richiesti e di creare un file da utilizzare quando si configura un livello cloud FabricPool in ONTAP.

  > Se si prevede di utilizzare StorageGRID come sistema di storage a oggetti per un livello cloud FabricPool, si consiglia di utilizzare la procedura guidata di installazione di FabricPool, a meno che non si sappiano requisiti speciali o l'implementazione richieda una personalizzazione significativa.

- **Configurare gli elementi manualmente**. Se si sta effettuando la connessione a un'applicazione Swift (o si sta effettuando la connessione a un'applicazione S3 e si preferisce non utilizzare l'installazione guidata S3), è possibile ottenere i valori richiesti eseguendo la configurazione manualmente. Attenersi alla seguente procedura:

  a. Configurare il gruppo ad alta disponibilità (ha) che si desidera utilizzare per l'applicazione S3 o Swift. Vedere "Configurare i gruppi ad alta disponibilità".

  b. Creare l'endpoint del bilanciamento del carico che verrà utilizzato dall'applicazione S3 o Swift. Vedere "Configurare gli endpoint del bilanciamento del carico".

c. Creare l'account tenant utilizzato dall'applicazione S3 o Swift. Vedere "Creare un account tenant".

d. Per un tenant S3, accedere all'account tenant e generare un ID della chiave di accesso e una chiave di accesso segreta per ogni utente che accede all'applicazione. Vedere "Creare le proprie chiavi di accesso".

e. Creare uno o più bucket S3 o container Swift all'interno dell'account tenant. Per S3, vedere "Creare un bucket S3". Per Swift, utilizzare "INSERIRE la richiesta di container".

f. Per aggiungere istruzioni di posizionamento specifiche per gli oggetti appartenenti al nuovo tenant o bucket/container, creare una nuova regola ILM e attivare un nuovo criterio ILM per utilizzare tale regola. Vedere "Creare una regola ILM" e. "Creare un criterio ILM".

Sicurezza per client S3 o Swift

Gli account tenant di StorageGRID utilizzano applicazioni client S3 o Swift per salvare i dati degli oggetti in StorageGRID. È necessario esaminare le misure di protezione implementate per le applicazioni client.

Riepilogo

La tabella seguente riassume il modo in cui viene implementata la sicurezza per le API REST S3 e Swift:

Problema di sicurezza	Implementazione per API REST
Sicurezza della connessione	TLS
Autenticazione del server	Certificato server X.509 firmato dalla CA di sistema o certificato server personalizzato fornito dall'amministratore
Autenticazione del client	**S3** Account S3 (ID chiave di accesso e chiave di accesso segreta) **Rapido** Account Swift (nome utente e password)
Autorizzazione del client	**S3** Proprietà dei bucket e tutte le policy di controllo degli accessi applicabili **Rapido** Accesso al ruolo di amministratore

In che modo StorageGRID fornisce la protezione per le applicazioni client

Le applicazioni client S3 e Swift possono connettersi al servizio Load Balancer su nodi gateway o nodi amministrativi o direttamente ai nodi storage.

- I client che si connettono al servizio Load Balancer possono utilizzare HTTPS o HTTP, in base alla modalità di utilizzo "configurare l'endpoint del bilanciamento del carico".

  HTTPS fornisce una comunicazione sicura e crittografata TLS ed è consigliato. È necessario allegare un

certificato di protezione all'endpoint.

HTTP fornisce comunicazioni meno sicure e non crittografate e dovrebbe essere utilizzato solo per reti non di produzione o di test.

- I client che si connettono ai nodi di archiviazione possono anche utilizzare HTTPS o HTTP.

  HTTPS è l'impostazione predefinita ed è consigliata.

  HTTP fornisce una comunicazione meno sicura e non crittografata, ma può essere opzionale "attivato" per reti non di produzione o di prova.

- Le comunicazioni tra StorageGRID e il client vengono crittografate mediante TLS.
- Le comunicazioni tra il servizio Load Balancer e i nodi di storage all'interno della griglia vengono crittografate indipendentemente dal fatto che l'endpoint del bilanciamento del carico sia configurato per accettare connessioni HTTP o HTTPS.
- I client devono fornire le intestazioni di autenticazione HTTP a StorageGRID per eseguire operazioni REST API. Vedere "Autenticare le richieste" e. "Endpoint API Swift supportati".

Certificati di sicurezza e applicazioni client

In tutti i casi, le applicazioni client possono stabilire connessioni TLS utilizzando un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dal sistema StorageGRID:

- Quando le applicazioni client si connettono al servizio Load Balancer, utilizzano il certificato configurato per l'endpoint del bilanciamento del carico. Ogni endpoint del bilanciatore di carico dispone di un proprio certificato—un certificato server personalizzato caricato dall'amministratore della griglia o un certificato generato dall'amministratore della griglia in StorageGRID durante la configurazione dell'endpoint.

  Vedere "Considerazioni per il bilanciamento del carico".

- Quando le applicazioni client si connettono direttamente a un nodo di storage, utilizzano i certificati server generati dal sistema e generati per i nodi di storage al momento dell'installazione del sistema StorageGRID (firmati dall'autorità di certificazione del sistema), oppure un singolo certificato server personalizzato fornito per la griglia da un amministratore della griglia. Vedere "Aggiunta di un certificato API S3 o Swift personalizzato".

I client devono essere configurati in modo da considerare attendibile l'autorità di certificazione che ha firmato il certificato utilizzato per stabilire connessioni TLS.

Algoritmi di hashing e crittografia supportati per le librerie TLS

Il sistema StorageGRID supporta un insieme di pacchetti di crittografia che le applicazioni client possono utilizzare quando stabiliscono una sessione TLS. Per configurare le crittografia, andare a **CONFIGURATION** > **Security** > **Security settings** e selezionare **TLS and SSH policy**.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3.

SSLv3 e TLS 1.1 (o versioni precedenti) non sono più supportati.

Utilizzare l’installazione guidata S3

Utilizzare l’installazione guidata S3: Considerazioni e requisiti

È possibile utilizzare l’installazione guidata S3 per configurare StorageGRID come sistema di storage a oggetti per un’applicazione S3.

Quando utilizzare l’installazione guidata S3

L’installazione guidata S3 guida l’utente attraverso ogni fase della configurazione di StorageGRID per l’utilizzo con un’applicazione S3. Durante il completamento della procedura guidata, è possibile scaricare i file da utilizzare per immettere i valori nell’applicazione S3. Utilizzare la procedura guidata per configurare il sistema più rapidamente e per assicurarsi che le impostazioni siano conformi alle Best practice StorageGRID.

Se si dispone di "Autorizzazione di accesso root", È possibile completare l’installazione guidata di S3 quando si inizia a utilizzare il Gestore griglie di StorageGRID oppure è possibile accedere e completare la procedura guidata in qualsiasi momento. A seconda dei requisiti, è possibile configurare manualmente alcuni o tutti gli elementi richiesti e utilizzare la procedura guidata per assemblare i valori richiesti da un’applicazione S3.

Prima di utilizzare la procedura guidata

Prima di utilizzare la procedura guidata, verificare di aver completato questi prerequisiti.

Ottenere gli indirizzi IP e configurare le interfacce VLAN

Se si configura un gruppo ad alta disponibilità (ha), si conoscono i nodi a cui si connetterà l’applicazione S3 e la rete StorageGRID da utilizzare. Si conoscono anche i valori da inserire per la subnet CIDR, l’indirizzo IP del gateway e gli indirizzi IP virtuali (VIP).

Se si intende utilizzare una LAN virtuale per separare il traffico dall’applicazione S3, l’interfaccia VLAN è già stata configurata. Vedere "Configurare le interfacce VLAN".

Configurare la federazione di identità e SSO

Se si prevede di utilizzare la federazione di identità o il Single Sign-on (SSO) per il sistema StorageGRID, queste funzionalità sono state attivate. Si sa anche quale gruppo federato deve disporre dell’accesso root per l’account tenant utilizzato dall’applicazione S3. Vedere "USA la federazione delle identità" e. "Configurare il single sign-on".

Ottenere e configurare i nomi di dominio

Si conosce il nome di dominio completo (FQDN) da utilizzare per StorageGRID. Le voci DNS (Domain Name Server) associano questo FQDN agli indirizzi IP virtuali (VIP) del gruppo ha creato utilizzando la procedura guidata.

Se si prevede di utilizzare le richieste in stile host virtuale S3, è necessario "Nomi di dominio degli endpoint S3 configurati". Si consiglia di utilizzare richieste virtuali in stile host.

Esaminare i requisiti del bilanciamento del carico e del certificato di sicurezza

Se si intende utilizzare il bilanciamento del carico StorageGRID, sono state esaminate le considerazioni generali sul bilanciamento del carico. Si dispone dei certificati da caricare o dei valori necessari per generare un certificato.

Se si intende utilizzare un endpoint esterno (di terze parti) per il bilanciamento del carico, si dispone del nome di dominio completo (FQDN), della porta e del certificato per il bilanciamento del carico.

Configurare le connessioni di federazione di griglie

Se si desidera consentire al tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket in un'altra griglia utilizzando una connessione a federazione di griglie, prima di avviare la procedura guidata, confermare quanto segue:

- Lo hai fatto "configurazione della connessione a federazione di griglie".
- Lo stato della connessione è **connesso**.
- Si dispone dell'autorizzazione di accesso root.

Accedere e completare l'installazione guidata di S3

È possibile utilizzare l'installazione guidata S3 per configurare StorageGRID per l'utilizzo con un'applicazione S3. L'installazione guidata fornisce i valori necessari all'applicazione per accedere a un bucket StorageGRID e per salvare gli oggetti.

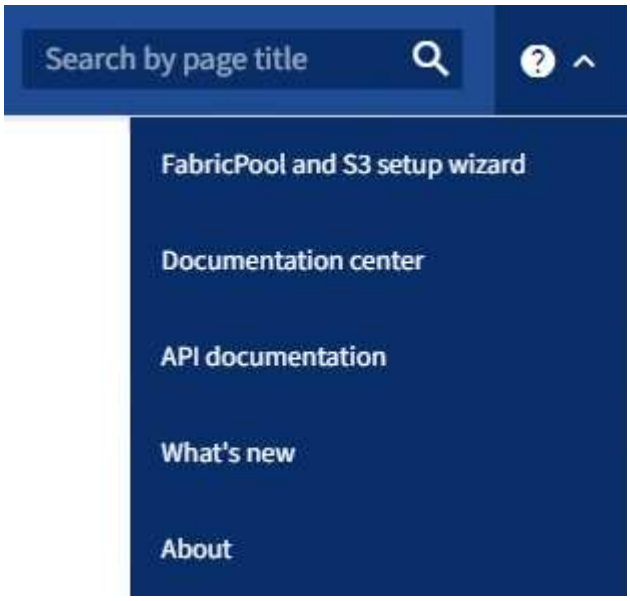
Prima di iniziare

- Hai il "Autorizzazione di accesso root".
- Hai esaminato il "considerazioni e requisiti" per utilizzare la procedura guidata.

Accedere alla procedura guidata

Fasi

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Se nella dashboard viene visualizzato il banner **FabricPool and S3 setup wizard**, selezionare il link nel banner. Se il banner non viene più visualizzato, selezionare l'icona della guida dalla barra di intestazione in Gestione griglia e selezionare **Installazione guidata FabricPool and S3**.



3. Nella sezione dell'applicazione S3 della pagina di installazione guidata di FabricPool e S3, selezionare **Configura ora**.

Fase 1 di 6: Configurare il gruppo ha

Un gruppo ha è un insieme di nodi che contengono ciascuno il servizio bilanciamento del carico StorageGRID.

Un gruppo ha può contenere nodi gateway, nodi di amministrazione o entrambi.

È possibile utilizzare un gruppo ha per mantenere disponibili le connessioni dati S3. Se l'interfaccia attiva nel gruppo ha si guasta, un'interfaccia di backup può gestire il carico di lavoro con un impatto minimo sulle operazioni S3.

Per ulteriori informazioni su questa attività, vedere "Gestire i gruppi ad alta disponibilità".

Fasi

1. Se si prevede di utilizzare un bilanciamento del carico esterno, non è necessario creare un gruppo ha. Selezionare **Ignora questo passaggio** e passare a. Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico.
2. Per utilizzare il bilanciamento del carico StorageGRID, è possibile creare un nuovo gruppo ha o utilizzare un gruppo ha esistente.

Creare un gruppo ha

a. Per creare un nuovo gruppo ha, selezionare **Crea gruppo ha**.

b. Per la fase **inserire i dettagli**, completare i seguenti campi.

Campo	Descrizione
Nome del gruppo HA	Un nome di visualizzazione univoco per questo gruppo ha.
Descrizione (opzionale)	La descrizione di questo gruppo ha.

c. Per il passo **Add interfaces**, selezionare le interfacce di nodo che si desidera utilizzare in questo gruppo ha.

   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.

   È possibile selezionare uno o più nodi, ma è possibile selezionare una sola interfaccia per ciascun nodo.

d. Per la fase **prioritize interfaces**, determinare l'interfaccia primaria e le interfacce di backup per questo gruppo ha.

   Trascinare le righe per modificare i valori nella colonna **Ordine di priorità**.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.

   Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi IP virtuali (VIP) si spostano nella prima interfaccia di backup nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano all'interfaccia di backup successiva e così via. Quando i guasti vengono risolti, gli indirizzi VIP tornano all'interfaccia con la priorità più alta disponibile.

e. Per il passo **inserire gli indirizzi IP**, completare i seguenti campi.

Campo	Descrizione
Subnet CIDR	L'indirizzo della subnet VIP nella notazione CIDR e n. 8212; un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32). L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.
Indirizzo IP del gateway (opzionale)	Se gli indirizzi IP S3 utilizzati per accedere a StorageGRID non si trovano sulla stessa sottorete degli indirizzi VIP StorageGRID, inserire l'indirizzo IP del gateway locale VIP StorageGRID. L'indirizzo IP del gateway locale deve trovarsi all'interno della subnet VIP.

Campo	Descrizione
Virtual IP address (Indirizzo IP virtuale)	Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP. Almeno un indirizzo deve essere IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

f. Selezionare **Create ha group** (Crea gruppo ha), quindi selezionare **Finish** (fine) per tornare all'installazione guidata S3.

g. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Utilizzare il gruppo ha esistente

a. Per utilizzare un gruppo ha esistente, selezionare il nome del gruppo ha dal menu **Select an ha group** (Seleziona un gruppo ha).

b. Selezionare **continua** per passare alla fase di bilanciamento del carico.

Fase 2 di 6: Configurare l'endpoint del bilanciamento del carico

StorageGRID utilizza un bilanciamento del carico per gestire il carico di lavoro dalle applicazioni client. Il bilanciamento del carico massimizza la velocità e la capacità di connessione tra più nodi di storage.

È possibile utilizzare il servizio bilanciamento del carico StorageGRID, disponibile su tutti i nodi gateway e di amministrazione, oppure connettersi a un bilanciamento del carico esterno (di terze parti). Si consiglia di utilizzare il bilanciamento del carico StorageGRID.

Per ulteriori informazioni su questa attività, vedere "Considerazioni per il bilanciamento del carico".

Per utilizzare il servizio bilanciamento del carico di StorageGRID, selezionare la scheda **StorageGRID load balancer**, quindi creare o selezionare l'endpoint di bilanciamento del carico che si desidera utilizzare. Per utilizzare un bilanciamento del carico esterno, selezionare la scheda **bilanciamento del carico esterno** e fornire i dettagli sul sistema già configurato.

Creare l'endpoint

Fasi

1. Per creare un endpoint di bilanciamento del carico, selezionare **Crea endpoint**.
2. Per il passo **inserire i dettagli dell'endpoint**, completare i seguenti campi.

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è 10433 per il primo endpoint creato, ma è possibile inserire qualsiasi porta esterna non utilizzata. Se si immette 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché queste porte sono riservate sui nodi Admin. **Nota:** le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete".
Tipo di client	Deve essere **S3**.
Protocollo di rete	Selezionare **HTTPS**. **Nota**: La comunicazione con StorageGRID senza crittografia TLS è supportata ma non consigliata.

3. Per il passo **Select binding mode**, specificare la modalità di binding. La modalità di associazione controlla l'accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

Modalità	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Global** (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.

Modalità	Descrizione
Tipo di nodo	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

4. Per la fase di accesso del tenant, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

5. Per il passo **Allega certificato**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Carica certificato (consigliato)	Utilizzare questa opzione per caricare un certificato server firmato dalla CA, una chiave privata del certificato e un bundle CA opzionale.
Generare un certificato	Utilizzare questa opzione per generare un certificato autofirmato. Vedere "Configurare gli endpoint del bilanciamento del carico" per informazioni dettagliate su cosa inserire.
Utilizza il certificato StorageGRID S3 e Swift	Utilizzare questa opzione solo se è già stata caricata o generata una versione personalizzata del certificato globale StorageGRID. Vedere "Configurare i certificati API S3 e Swift" per ulteriori informazioni.

6. Selezionare **fine** per tornare all'installazione guidata S3.
7. Selezionare **continua** per passare al punto tenant e bucket.

> Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

Utilizzare l'endpoint del bilanciamento del carico esistente

Fasi

1. Per utilizzare un endpoint esistente, selezionarne il nome dal campo **Select a load balancer endpoint**.

2. Selezionare **continua** per passare al punto tenant e bucket.

Utilizzare un bilanciamento del carico esterno

Fasi

1. Per utilizzare un bilanciamento del carico esterno, completare i seguenti campi.

Campo	Descrizione
FQDN	Il nome di dominio completo (FQDN) del bilanciamento del carico esterno.
Porta	Il numero di porta che l'applicazione S3 utilizzerà per connettersi al bilanciamento del carico esterno.
Certificato	Copiare il certificato del server per il bilanciamento del carico esterno e incollarlo in questo campo.

2. Selezionare **continua** per passare al punto tenant e bucket.

Fase 3 di 6: Creazione di tenant e bucket

Un tenant è un'entità che può utilizzare le applicazioni S3 per memorizzare e recuperare oggetti in StorageGRID. Ogni tenant dispone di utenti, chiavi di accesso, bucket, oggetti e un set specifico di funzionalità. È necessario creare il tenant prima di poter creare il bucket che l'applicazione S3 utilizzerà per memorizzare i propri oggetti.

Un bucket è un container utilizzato per memorizzare gli oggetti e i metadati degli oggetti di un tenant. Anche se alcuni tenant potrebbero avere molti bucket, la procedura guidata consente di creare un tenant e un bucket nel modo più rapido e semplice. Puoi utilizzare il tenant Manager in un secondo momento per aggiungere altri bucket necessari.

È possibile creare un nuovo tenant da utilizzare per questa applicazione S3. In alternativa, è anche possibile creare un bucket per il nuovo tenant. Infine, è possibile consentire alla procedura guidata di creare le chiavi di accesso S3 per l'utente root del tenant.

Per ulteriori informazioni su questa attività, vedere "Creare un account tenant" e. "Creare un bucket S3".

Fasi

1. Selezionare **Crea tenant**.
2. Per la procedura di inserimento dei dettagli, immettere le seguenti informazioni.

Campo	Descrizione
Nome	Un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una volta creato, l'account tenant riceve un ID account numerico univoco.
Descrizione (opzionale)	Una descrizione che aiuta a identificare il tenant.

Campo	Descrizione
Tipo di client	Il tipo di protocollo client utilizzato dal tenant. Per l'installazione guidata S3, è selezionato **S3** e il campo è disattivato.
Quota di storage (opzionale)	Se si desidera che il tenant disponga di una quota di storage, un valore numerico per la quota e le unità.

3. Selezionare **continua**.
4. Se si desidera, selezionare le autorizzazioni desiderate per il tenant.

> Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, selezionare l'icona della guida per ciascuna autorizzazione.

Permesso	Se selezionato…
Consentire i servizi della piattaforma	Il tenant può utilizzare servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3".
Utilizza la propria origine di identità	Il tenant può configurare e gestire la propria origine di identità per gruppi e utenti federati. Questa opzione è disattivata se si dispone di "SSO configurato" Per il tuo sistema StorageGRID.
Consenti selezione S3	Il tenant può emettere richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Manage S3 (Gestisci S3): Selezionare per gli account tenant". **Importante**: Le richieste SelectObjectContent possono ridurre le performance di bilanciamento del carico per tutti i client S3 e per tutti i tenant. Attivare questa funzione solo quando richiesto e solo per tenant attendibili.
USA connessione a federazione di griglie	Il tenant può utilizzare una connessione a federazione di grid. Selezionando questa opzione: • Consente di clonare questo tenant e tutti i gruppi tenant e gli utenti aggiunti all'account da questa griglia (la *griglia di origine*) all'altra griglia della connessione selezionata (la *griglia di destinazione*). • Consente a questo tenant di configurare la replica cross-grid tra i bucket corrispondenti su ogni grid. Vedere "Gestire i tenant consentiti per la federazione di grid".

5. Se si seleziona **Usa connessione federazione griglia**, selezionare una delle connessioni federazione griglia disponibili.
6. Definire l'accesso root per l'account tenant, in base all'utilizzo o meno da parte del sistema StorageGRID "federazione delle identità", "SSO (Single Sign-on)", o entrambi.

Opzione	Eseguire questa operazione
Se la federazione delle identità non è attivata	Specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se è attivata la federazione delle identità	a. Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si effettua l'accesso al tenant come utente root locale.
Se sono attivate sia la federazione di identità che il single sign-on (SSO)	Selezionare un gruppo federated esistente per disporre dell'autorizzazione di accesso root per il tenant. Nessun utente locale può accedere.

7. Se si desidera che la procedura guidata crei l'ID della chiave di accesso e la chiave di accesso segreta per l'utente root, selezionare **Crea automaticamente la chiave di accesso S3 dell'utente root**.

   Selezionare questa opzione se l'unico utente per il tenant sarà l'utente root. Se altri utenti utilizzeranno questo tenant, utilizzare Tenant Manager per configurare le chiavi e le autorizzazioni.

8. Selezionare **continua**.
9. Per il passo Create bucket, è possibile creare un bucket per gli oggetti del tenant. Altrimenti, selezionare **Create tenant without bucket** (Crea tenant senza bucket) per accedere a. fase di download dei dati.

   Se S3 Object Lock è attivato per la griglia, il bucket creato in questa fase non ha S3 Object Lock abilitato. Se è necessario utilizzare un bucket S3 Object Lock per questa applicazione S3, selezionare **Create tenant without bucket** (Crea tenant senza bucket). Quindi, utilizzare Tenant Manager per "creare il bucket" invece.

   a. Immettere il nome del bucket utilizzato dall'applicazione S3. Ad esempio, `S3-bucket`.

      Non è possibile modificare il nome del bucket dopo averlo creato.

   b. Selezionare **Region** per questo bucket.

      Utilizzare la regione predefinita (`us-east-1`) A meno che non si preveda di utilizzare ILM in futuro per filtrare gli oggetti in base all'area del bucket.

   c. Selezionare **Enable object versioning** (attiva versione oggetto) se si desidera memorizzare ogni versione di ciascun oggetto in questo bucket.
   d. Selezionare **Create tenant and bucket** (Crea tenant e bucket) e passare alla fase di download dei dati.

fase 4 di 6: Download dei dati

Nella fase di download dei dati, è possibile scaricare uno o due file per salvare i dettagli di ciò che si è appena configurato.

Fasi

1. Se è stato selezionato **Create root user S3 access key automatically** (Crea chiave di accesso S3 utente root automaticamente), eseguire una o entrambe le operazioni seguenti:
   - Selezionare **Download access key** (Scarica chiavi di accesso) per scaricare un `.csv` File contenente il nome dell'account tenant, l'ID della chiave di accesso e la chiave di accesso segreta.
   - Selezionare l'icona di copia ( ) Per copiare l'ID della chiave di accesso e la chiave di accesso segreta negli Appunti.
2. Selezionare **Download Configuration Values** (Scarica valori di configurazione) per scaricare un `.txt` file contenente le impostazioni per l'endpoint del bilanciamento del carico, il tenant, il bucket e l'utente root.
3. Salvare queste informazioni in una posizione sicura.

> Non chiudere questa pagina prima di aver copiato entrambi i tasti di accesso. I tasti non saranno disponibili dopo la chiusura di questa pagina. Assicurarsi di salvare queste informazioni in una posizione sicura perché possono essere utilizzate per ottenere dati dal sistema StorageGRID.

4. Se richiesto, selezionare la casella di controllo per confermare che le chiavi sono state scaricate o copiate.
5. Selezionare **continua** per passare alla regola ILM e al passaggio del criterio.

Fase 5 di 6: Esaminare la regola ILM e il criterio ILM per S3

Le regole ILM (Information Lifecycle Management) controllano il posizionamento, la durata e il comportamento di acquisizione di tutti gli oggetti nel sistema StorageGRID. Il criterio ILM incluso in StorageGRID crea due copie replicate di tutti gli oggetti. Questo criterio è attivo fino a quando non si attiva almeno un nuovo criterio.

Fasi

1. Esaminare le informazioni fornite nella pagina.
2. Se si desidera aggiungere istruzioni specifiche per gli oggetti appartenenti al nuovo tenant o bucket, creare una nuova regola e una nuova policy. Vedere "Creare una regola ILM" e. "Criteri ILM: Panoramica".
3. Selezionare **ho esaminato questi passaggi e ho compreso cosa devo fare**.
4. Selezionare la casella di controllo per indicare che si comprende cosa fare in seguito.
5. Selezionare **continua** per accedere a **Riepilogo**.

Fase 6 di 6: Riepilogo

Fasi

1. Esaminare il riepilogo.
2. Prendere nota dei dettagli nei passaggi successivi, che descrivono la configurazione aggiuntiva che potrebbe essere necessaria prima di connettersi al client S3. Ad esempio, selezionando **Accedi come root** si passa a Tenant Manager, dove è possibile aggiungere utenti tenant, creare bucket aggiuntivi e aggiornare le impostazioni del bucket.
3. Selezionare **fine**.
4. Configurare l'applicazione utilizzando il file scaricato da StorageGRID o i valori ottenuti manualmente.

Gestire i gruppi ha

Gestire i gruppi ad alta disponibilità (ha): Panoramica

È possibile raggruppare le interfacce di rete di più nodi Admin e Gateway in un gruppo ad alta disponibilità (ha). Se l'interfaccia attiva nel gruppo ha non riesce, un'interfaccia di backup può gestire il carico di lavoro.

Che cos'è un gruppo ha?

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

Ciascun gruppo ha fornisce l'accesso ai servizi condivisi sui nodi selezionati.

- I gruppi HA che includono nodi gateway, nodi di amministrazione o entrambi forniscono connessioni dati altamente disponibili per i client S3 e Swift.
- I gruppi HA che includono solo nodi Admin forniscono connessioni altamente disponibili al Grid Manager e al Tenant Manager.
- Un gruppo ha che include solo appliance di servizi e nodi software basati su VMware può offrire connessioni ad alta disponibilità per "S3 tenant che utilizzano S3 Select". I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Come crei un gruppo ha?

1. Selezionare un'interfaccia di rete per uno o più nodi Admin o Gateway. È possibile utilizzare un'interfaccia Grid Network (eth0), un'interfaccia Client Network (eth2), un'interfaccia VLAN o un'interfaccia di accesso aggiunta al nodo.

   > Non è possibile aggiungere un'interfaccia a un gruppo ha se dispone di un indirizzo IP assegnato da DHCP.

2. Specificare un'interfaccia come principale. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.
3. È possibile determinare l'ordine di priorità per le interfacce di backup.
4. Al gruppo vengono assegnati da uno a 10 indirizzi IP virtuali (VIP). Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per istruzioni, vedere "Configurare i gruppi ad alta disponibilità".

Che cos'è l'interfaccia attiva?

Durante il normale funzionamento, tutti gli indirizzi VIP per il gruppo ha vengono aggiunti all'interfaccia primaria, che è la prima interfaccia nell'ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Cioè, durante il normale funzionamento, l'interfaccia primaria è l'interfaccia "attiva" per il gruppo.

Analogamente, durante il normale funzionamento, qualsiasi interfaccia a priorità inferiore per il gruppo ha agisce come interfacce di "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi disponibile.

Visualizzare lo stato corrente del gruppo ha di un nodo

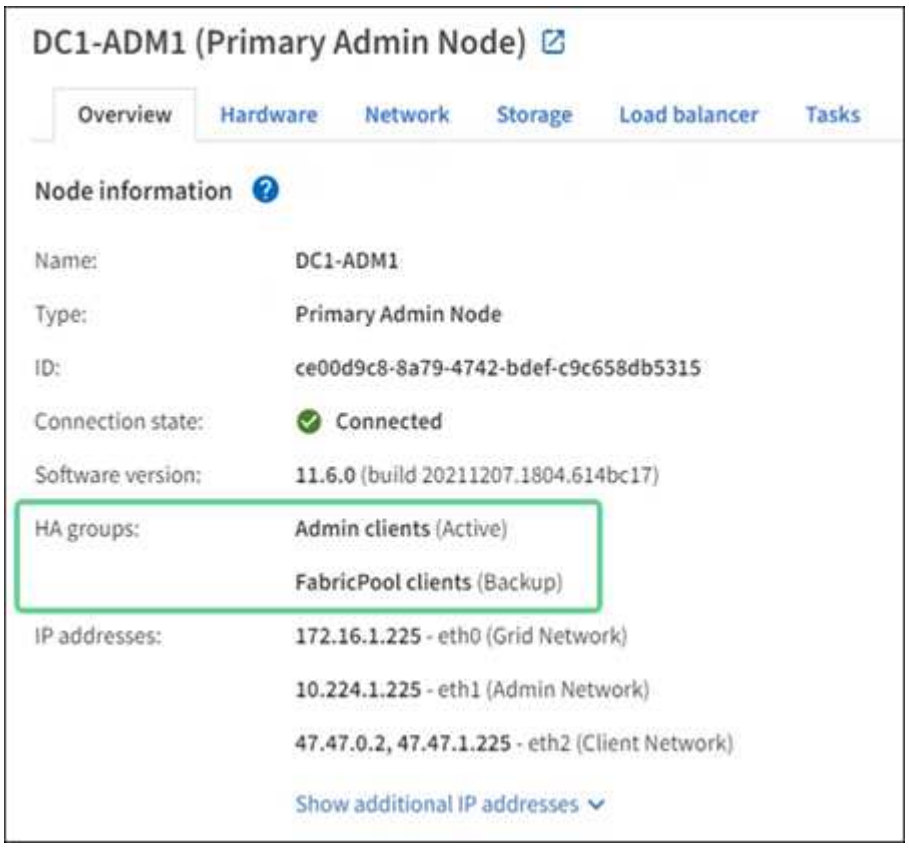
Per verificare se un nodo è assegnato a un gruppo ha e determinarne lo stato corrente, selezionare **NODES** >

Node.

Se la scheda **Panoramica** include una voce per **gruppi ha**, il nodo viene assegnato ai gruppi ha elencati. Il valore dopo il nome del gruppo corrisponde allo stato corrente del nodo nel gruppo ha:

- **Attivo**: Il gruppo ha è attualmente ospitato su questo nodo.
- **Backup**: Il gruppo ha non sta attualmente utilizzando questo nodo; si tratta di un'interfaccia di backup.
- **Arrestato**: Il gruppo ha non può essere ospitato su questo nodo perché il servizio ad alta disponibilità (keepalived) è stato arrestato manualmente.
- **Fault**: Il gruppo ha non può essere ospitato su questo nodo a causa di uno o più dei seguenti fattori:
  - Il servizio Load Balancer (nginx-gw) non è in esecuzione sul nodo.
  - L'interfaccia eth0 o VIP del nodo non è disponibile.
  - Il nodo non è attivo.

In questo esempio, il nodo di amministrazione primario è stato aggiunto a due gruppi ha. Questo nodo è attualmente l'interfaccia attiva per il gruppo di client di amministrazione e un'interfaccia di backup per il gruppo di client FabricPool.



Cosa succede quando l'interfaccia attiva non funziona?

L'interfaccia che attualmente ospita gli indirizzi VIP è l'interfaccia attiva. Se il gruppo ha include più di un'interfaccia e l'interfaccia attiva non riesce, gli indirizzi VIP si spostano sulla prima interfaccia di backup disponibile nell'ordine di priorità. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia di backup disponibile e così via.

Il failover può essere attivato per uno dei seguenti motivi:

- Il nodo su cui è configurata l'interfaccia non funziona.
- Il nodo su cui è configurata l'interfaccia perde la connettività con tutti gli altri nodi per almeno 2 minuti.
- L'interfaccia attiva non funziona.
- Il servizio Load Balancer si arresta.
- Il servizio High Availability si interrompe.

> Il failover potrebbe non essere attivato da guasti di rete esterni al nodo che ospita l'interfaccia attiva. Allo stesso modo, il failover non viene attivato dai servizi per Grid Manager o Tenant Manager.

Il processo di failover richiede in genere solo pochi secondi ed è abbastanza rapido da consentire alle applicazioni client di avere un impatto minimo e può fare affidamento sui normali comportamenti di ripetizione per continuare a funzionare.

Quando il guasto viene risolto e un'interfaccia con priorità più alta diventa nuovamente disponibile, gli indirizzi VIP vengono automaticamente spostati nell'interfaccia con priorità più alta disponibile.

Come vengono utilizzati i gruppi ha?

È possibile utilizzare gruppi ad alta disponibilità (ha) per fornire connessioni altamente disponibili a StorageGRID per i dati a oggetti e per l'utilizzo amministrativo.

- Un gruppo ha può fornire connessioni amministrative altamente disponibili al Grid Manager o al tenant Manager.
- Un gruppo ha può fornire connessioni dati altamente disponibili per i client S3 e Swift.
- Un gruppo ha che contiene una sola interfaccia consente di fornire molti indirizzi VIP e di impostare esplicitamente gli indirizzi IPv6.

Un gruppo ha può fornire alta disponibilità solo se tutti i nodi inclusi nel gruppo forniscono gli stessi servizi. Quando si crea un gruppo ha, aggiungere interfacce dai tipi di nodi che forniscono i servizi richiesti.

- **Admin Node**: Include il servizio Load Balancer e abilita l'accesso al Grid Manager o al Tenant Manager.
- **Gateway Node**: Include il servizio Load Balancer.

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso a Grid Manager	• Nodo amministratore primario (**primario**) • Nodi amministrativi non primari **Nota:** l'Admin Node primario deve essere l'interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.
Accesso solo al tenant manager	• Nodi di amministrazione primari o non primari
Accesso client S3 o Swift — Servizio Load Balancer	• Nodi di amministrazione • Nodi gateway

Scopo del gruppo ha	Aggiungere nodi di questo tipo al gruppo ha
Accesso al client S3 per "S3 Seleziona"	• Appliance di servizi • Nodi software basati su VMware **Nota**: I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Limitazioni dell'utilizzo di gruppi ha con Grid Manager o Tenant Manager

Se un servizio Grid Manager o Tenant Manager non funziona, il failover del gruppo ha non viene attivato.

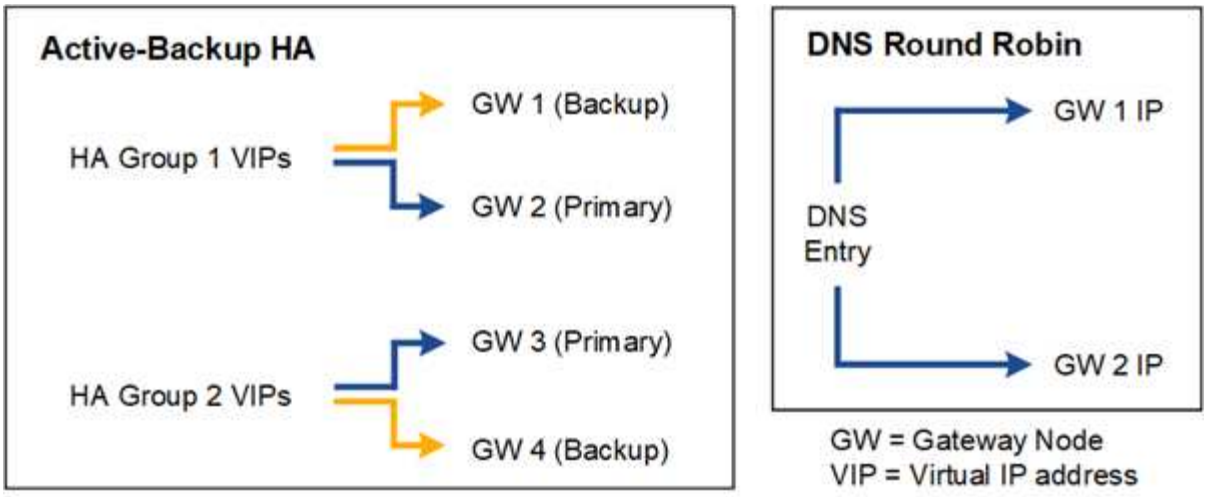
Se hai effettuato l'accesso a Grid Manager o a Tenant Manager quando si verifica il failover, sei disconnesso e devi effettuare nuovamente l'accesso per riprendere l'attività.

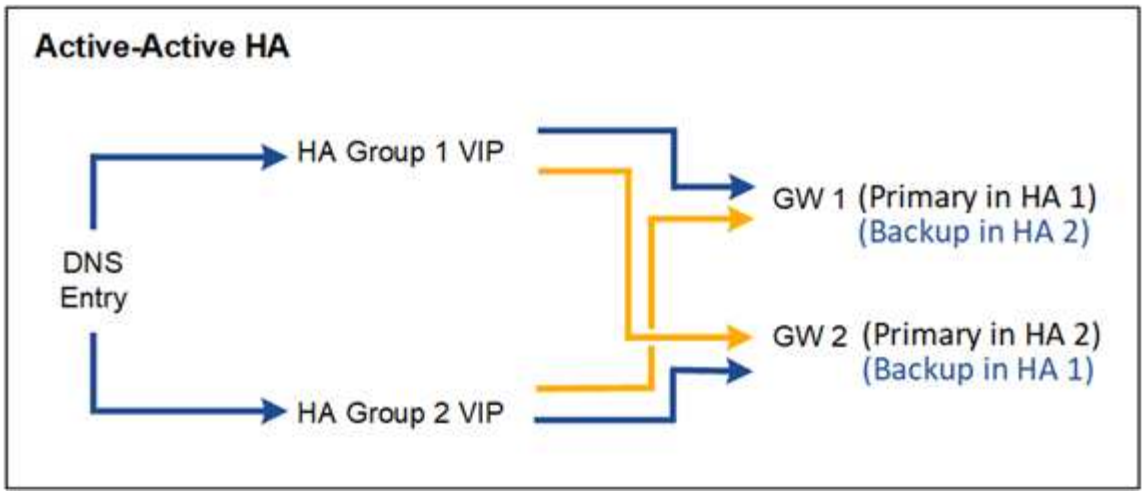
Non è possibile eseguire alcune procedure di manutenzione quando il nodo di amministrazione primario non è disponibile. Durante il failover, è possibile utilizzare Grid Manager per monitorare il sistema StorageGRID.

Opzioni di configurazione per i gruppi ha

I seguenti diagrammi forniscono esempi di diversi modi per configurare i gruppi ha. Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia principale nel gruppo ha e il giallo indica l'interfaccia di backup nel gruppo ha.





La tabella riassume i vantaggi di ciascuna configurazione ha mostrata nel diagramma.

Configurazione	Vantaggi	Svantaggi
Ha Active-Backup	• Gestito da StorageGRID senza dipendenze esterne. • Failover rapido.	• Solo un nodo in un gruppo ha è attivo. Almeno un nodo per gruppo ha sarà inattivo.
DNS Round Robin	• Maggiore throughput aggregato. • Nessun host inattivo.	• Failover lento, che potrebbe dipendere dal comportamento del client. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Ha bisogno di un controllo dello stato di salute implementato dal cliente.

Configurazione	Vantaggi	Svantaggi
Ha Active-Active	• Il traffico viene distribuito tra più gruppi ha. • Throughput aggregato elevato che si adatta al numero di gruppi ha. • Failover rapido.	• Più complesso da configurare. • Richiede la configurazione dell'hardware al di fuori di StorageGRID. • Ha bisogno di un controllo dello stato di salute implementato dal cliente.

Configurare i gruppi ad alta disponibilità

È possibile configurare i gruppi ad alta disponibilità (ha) per fornire l'accesso altamente disponibile ai servizi sui nodi Admin o Gateway.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Se si intende utilizzare un'interfaccia VLAN in un gruppo ha, l'interfaccia VLAN è stata creata. Vedere "Configurare le interfacce VLAN".
- Se si intende utilizzare un'interfaccia di accesso per un nodo in un gruppo ha, l'interfaccia è stata creata:
  - **Red Hat Enterprise Linux (prima di installare il nodo)**: "Creare file di configurazione del nodo"
  - **Ubuntu o Debian (prima di installare il nodo)**: "Creare file di configurazione del nodo"
  - **Linux (dopo l'installazione del nodo)**: "Linux: Aggiunta di interfacce di accesso o trunk a un nodo"
  - **VMware (dopo l'installazione del nodo)**: "VMware: Aggiunta di interfacce di accesso o trunk a un nodo"

Creare un gruppo ad alta disponibilità

Quando si crea un gruppo ad alta disponibilità, selezionare una o più interfacce e organizzarle in ordine di priorità. Quindi, assegnare uno o più indirizzi VIP al gruppo.

Un'interfaccia deve essere un nodo gateway o un nodo amministratore per essere incluso in un gruppo ha. Un gruppo ha può utilizzare solo un'interfaccia per un dato nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi ha.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selezionare **Crea**.

Inserire i dettagli del gruppo ha

Fasi

1. Fornire un nome univoco per il gruppo ha.
2. Facoltativamente, inserire una descrizione per il gruppo ha.

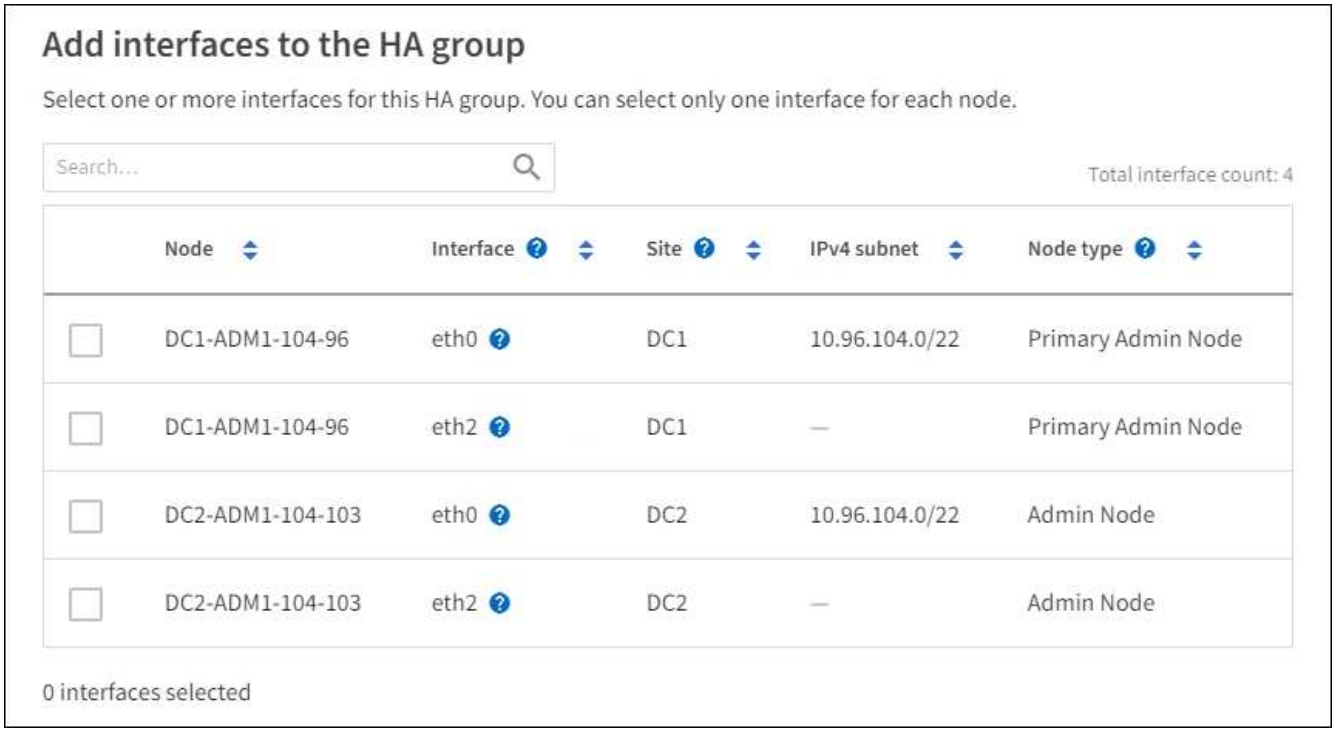
3. Selezionare **continua**.

Aggiungere interfacce al gruppo ha

Fasi

1. Selezionare una o più interfacce da aggiungere a questo gruppo ha.

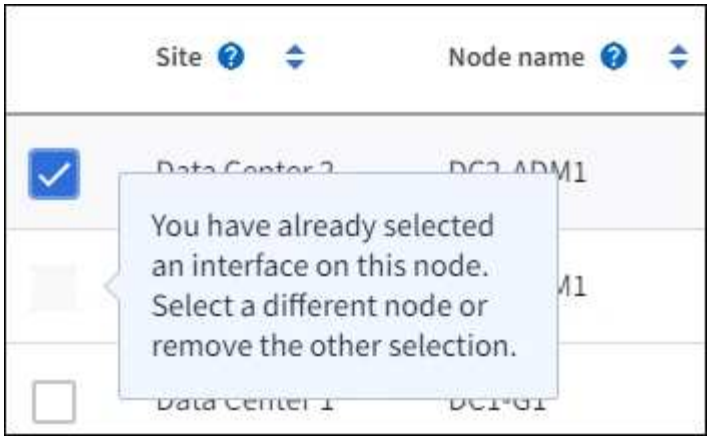
   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.



> Dopo aver creato un'interfaccia VLAN, attendere fino a 5 minuti per visualizzare la nuova interfaccia nella tabella.

Linee guida per la selezione delle interfacce

- Selezionare almeno un'interfaccia.
- È possibile selezionare una sola interfaccia per un nodo.
- Se il gruppo ha è per la protezione ha dei servizi Admin Node, che includono Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se il gruppo ha è per la protezione ha del traffico client S3 o Swift, selezionare le interfacce sui nodi di amministrazione, sui nodi gateway o su entrambi.
- Se si selezionano interfacce su diversi tipi di nodi, viene visualizzata una nota informativa. Si ricorda che, in caso di failover, i servizi forniti dal nodo precedentemente attivo potrebbero non essere disponibili sul nodo appena attivo. Ad esempio, un nodo gateway di backup non può fornire la protezione ha dei servizi del nodo amministratore. Analogamente, un nodo Admin di backup non può eseguire tutte le procedure di manutenzione che il nodo Admin primario può fornire.
- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. Il suggerimento fornisce ulteriori informazioni.



- Non è possibile selezionare un'interfaccia se il relativo valore di sottorete o il gateway è in conflitto con un'altra interfaccia selezionata.
- Non è possibile selezionare un'interfaccia configurata se non dispone di un indirizzo IP statico.

2. Selezionare **continua**.

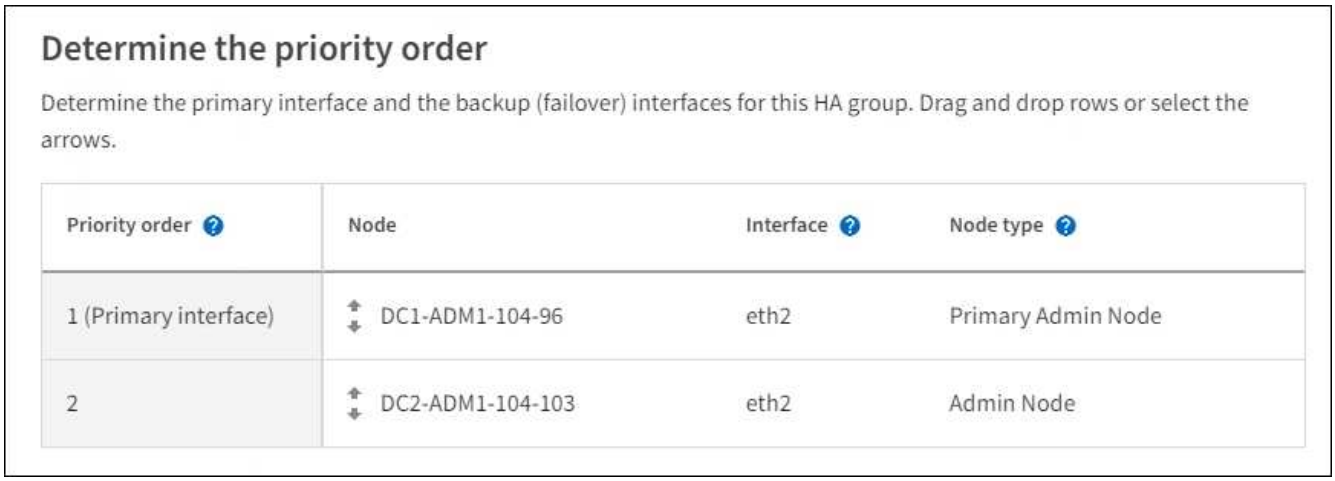
Determinare l'ordine di priorità

Se il gruppo ha include più di un'interfaccia, è possibile determinare quale sia l'interfaccia primaria e quali siano le interfacce di backup (failover). Se l'interfaccia principale non funziona, gli indirizzi VIP passano all'interfaccia con la priorità più alta disponibile. Se l'interfaccia non funziona, gli indirizzi VIP passano alla successiva interfaccia con la priorità più alta disponibile e così via.

Fasi

1. Trascinare le righe nella colonna **Ordine di priorità** per determinare l'interfaccia primaria e le interfacce di backup.

   La prima interfaccia nell'elenco è l'interfaccia primaria. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.



> Se il gruppo ha fornisce l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario.

2. Selezionare **continua**.

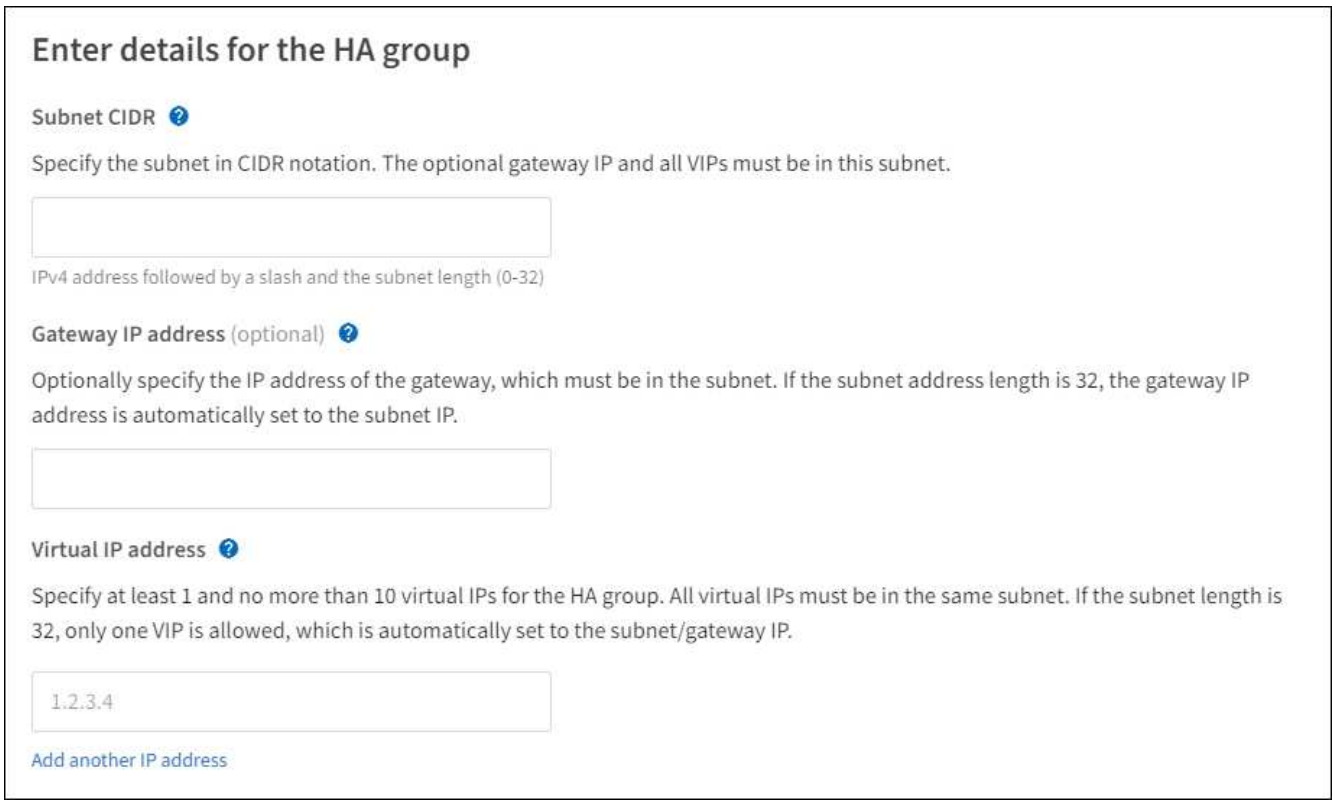
Inserire gli indirizzi IP

Fasi

1. Nel campo **Subnet CIDR**, specificare la subnet VIP nella notazione CIDR: Un indirizzo IPv4 seguito da una barra e dalla lunghezza della subnet (0-32).

   L'indirizzo di rete non deve avere bit host impostati. Ad esempio, `192.16.0.0/22`.

   > Se si utilizza un prefisso a 32 bit, l'indirizzo di rete VIP funge anche da indirizzo del gateway e da indirizzo VIP.



2. Facoltativamente, se un client S3, Swift, amministrativo o tenant accede a questi indirizzi VIP da una sottorete diversa, immettere l'indirizzo IP del gateway*. L'indirizzo del gateway deve trovarsi all'interno della subnet VIP.

   Gli utenti client e admin utilizzeranno questo gateway per accedere agli indirizzi IP virtuali.

3. Inserire almeno uno e non più di dieci indirizzi VIP per l'interfaccia attiva nel gruppo ha. Tutti gli indirizzi VIP devono trovarsi all'interno della subnet VIP e tutti saranno attivi contemporaneamente sull'interfaccia attiva.

   Specificare almeno un indirizzo IPv4. In alternativa, è possibile specificare ulteriori indirizzi IPv4 e IPv6.

4. Selezionare **Create ha group** (Crea gruppo ha) e selezionare **Finish** (fine).

   Viene creato il gruppo ha ed è ora possibile utilizzare gli indirizzi IP virtuali configurati.

Passi successivi

Se si utilizza questo gruppo ha per il bilanciamento del carico, creare un endpoint per il bilanciamento del carico per determinare il protocollo di porta e di rete e per allegare eventuali certificati richiesti. Vedere "Configurare gli endpoint del bilanciamento del carico".

Modificare un gruppo ad alta disponibilità

È possibile modificare un gruppo ad alta disponibilità (ha) per modificarne nome e descrizione, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o aggiornare indirizzi IP virtuali.

Ad esempio, potrebbe essere necessario modificare un gruppo ha se si desidera rimuovere il nodo associato a un'interfaccia selezionata in una procedura di decommissionamento del sito o del nodo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.

   La pagina High Availability groups (gruppi ad alta disponibilità) mostra tutti i gruppi ha esistenti.

2. Selezionare la casella di controllo del gruppo ha che si desidera modificare.
3. Eseguire una delle seguenti operazioni in base a quanto si desidera aggiornare:
   - Selezionare **azioni** > **Modifica indirizzo IP virtuale** per aggiungere o rimuovere indirizzi VIP.
   - Selezionare **azioni** > **Modifica gruppo ha** per aggiornare il nome o la descrizione del gruppo, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o rimuovere indirizzi VIP.
4. Se si seleziona **Modifica indirizzo IP virtuale**:
   a. Aggiornare gli indirizzi IP virtuali per il gruppo ha.
   b. Selezionare **Salva**.
   c. Selezionare **fine**.
5. Se si seleziona **Edit ha group** (Modifica gruppo ha):
   a. Facoltativamente, aggiornare il nome o la descrizione del gruppo.
   b. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere o rimuovere interfacce.

      Se il gruppo ha fornisce l'accesso a Grid Manager, è necessario selezionare un'interfaccia sul nodo di amministrazione primario come interfaccia primaria. Alcune procedure di manutenzione possono essere eseguite solo dal nodo di amministrazione primario

   c. Facoltativamente, trascinare le righe per modificare l'ordine di priorità dell'interfaccia primaria e delle interfacce di backup per questo gruppo ha.
   d. Facoltativamente, aggiornare gli indirizzi IP virtuali.
   e. Selezionare **Salva**, quindi **fine**.

Rimuovere un gruppo ad alta disponibilità

È possibile rimuovere uno o più gruppi ad alta disponibilità (ha) alla volta.

Non è possibile rimuovere un gruppo ha se è associato a un endpoint di bilanciamento del carico. Per eliminare un gruppo ha, è necessario rimuoverlo da tutti gli endpoint del bilanciamento del carico che lo utilizzano.

Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift prima di rimuovere un gruppo ha. Aggiornare ciascun client per la connessione utilizzando un altro indirizzo IP, ad esempio l'indirizzo IP virtuale di un gruppo ha diverso o l'indirizzo IP configurato per un'interfaccia durante l'installazione.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Esaminare la colonna **endpoint del bilanciamento del carico** per ciascun gruppo ha che si desidera rimuovere. Se sono elencati endpoint del bilanciamento del carico:
   a. Andare a **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
   b. Selezionare la casella di controllo per l'endpoint.
   c. Selezionare **azioni** > **Modifica modalità di associazione endpoint**.
   d. Aggiornare la modalità di binding per rimuovere il gruppo ha.
   e. Selezionare **Save Changes** (Salva modifiche).
3. Se non sono elencati endpoint del bilanciamento del carico, selezionare la casella di controllo per ciascun gruppo ha che si desidera rimuovere.
4. Selezionare **azioni** > **Rimuovi gruppo ha**.
5. Esaminare il messaggio e selezionare **Delete ha group** (Elimina gruppo ha) per confermare la selezione.

   Tutti i gruppi ha selezionati vengono rimossi. Nella pagina dei gruppi ad alta disponibilità viene visualizzato un banner verde di successo.

Gestire il bilanciamento del carico

Considerazioni per il bilanciamento del carico

È possibile utilizzare il bilanciamento del carico per gestire i carichi di lavoro di acquisizione e recupero dai client S3 e Swift.

Cos'è il bilanciamento del carico?

Quando un'applicazione client salva o recupera i dati da un sistema StorageGRID, StorageGRID utilizza un sistema di bilanciamento del carico per gestire il carico di lavoro di acquisizione e recupero. Il bilanciamento del carico massimizza la velocità e la capacità di connessione distribuendo il carico di lavoro tra più nodi di storage.

Il servizio bilanciamento del carico StorageGRID viene installato su tutti i nodi di amministrazione e su tutti i nodi gateway e fornisce il bilanciamento del carico di livello 7. Esegue la terminazione TLS (Transport Layer Security) delle richieste client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage.

Il servizio Load Balancer su ciascun nodo funziona in modo indipendente quando si inoltra il traffico client ai nodi di storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU.

Anche se il servizio bilanciamento del carico di StorageGRID è il meccanismo di bilanciamento del carico consigliato, potrebbe essere necessario integrare un bilanciamento del carico di terze parti. Per informazioni, contattare il rappresentante commerciale NetApp o visitare il sito Web all'indirizzo "TR-4626: Bilanciatori di carico globali e di terze parti StorageGRID".

Quanti nodi per il bilanciamento del carico sono necessari?

Come Best practice generale, ogni sito del sistema StorageGRID deve includere due o più nodi nel servizio bilanciamento del carico. Ad esempio, un sito potrebbe includere due nodi gateway o sia un nodo amministratore che un nodo gateway. Assicurati che sia disponibile un'infrastruttura di rete, hardware o virtualizzazione adeguata per ogni nodo di bilanciamento del carico, sia che si utilizzino appliance per i servizi, nodi bare metal o nodi basati su macchine virtuali (VM).

Che cos'è un endpoint di bilanciamento del carico?

Un endpoint di bilanciamento del carico definisce la porta e il protocollo di rete (HTTPS o HTTP) che le richieste dell'applicazione client in entrata e in uscita utilizzeranno per accedere ai nodi che contengono il servizio Load Balancer. L'endpoint definisce anche il tipo di client (S3 o Swift), la modalità di binding e, facoltativamente, un elenco di tenant consentiti o bloccati.

Per creare un endpoint di bilanciamento del carico, selezionare **CONFIGURAZIONE** > **rete** > **endpoint di bilanciamento del carico** oppure completare la configurazione guidata di FabricPool e S3. Per istruzioni:

- "Configurare gli endpoint del bilanciamento del carico"
- "Utilizzare l'installazione guidata S3"
- "Utilizzare l'installazione guidata di FabricPool"

Considerazioni per la porta

Per impostazione predefinita, la porta di un endpoint di bilanciamento del carico è 10433 per il primo endpoint creato, ma è possibile specificare qualsiasi porta esterna inutilizzata compresa tra 1 e 65535. Se si utilizza la porta 80 o 443, l'endpoint utilizzerà il servizio Load Balancer solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. Se si utilizza la stessa porta per più di un endpoint, è necessario specificare una modalità di binding diversa per ciascun endpoint.

Le porte utilizzate da altri servizi di rete non sono consentite. Vedere "Riferimento porta di rete".

Considerazioni sul protocollo di rete

Nella maggior parte dei casi, le connessioni tra le applicazioni client e StorageGRID devono utilizzare la crittografia TLS (Transport Layer Security). La connessione a StorageGRID senza crittografia TLS è supportata ma non consigliata, soprattutto negli ambienti di produzione. Quando si seleziona il protocollo di rete per l'endpoint del bilanciamento del carico StorageGRID, selezionare **HTTPS**.

Considerazioni per i certificati endpoint del bilanciamento del carico

Se si seleziona **HTTPS** come protocollo di rete per l'endpoint del bilanciamento del carico, è necessario fornire un certificato di sicurezza. È possibile utilizzare una di queste tre opzioni quando si crea l'endpoint del bilanciamento del carico:

- **Caricare un certificato firmato (consigliato)**. Il certificato può essere firmato da un'autorità di certificazione pubblica o privata. L'utilizzo di un certificato del server CA pubblicamente attendibile per proteggere la connessione è la procedura consigliata. A differenza dei certificati generati, i certificati firmati

da una CA possono essere ruotati senza interruzioni, in modo da evitare problemi di scadenza.

Prima di creare l'endpoint del bilanciamento del carico, è necessario ottenere i seguenti file:

- Il file di certificato del server personalizzato.
- Il file di chiave privata del certificato del server personalizzato.
- Facoltativamente, un bundle CA dei certificati di ciascuna autorità di certificazione di emissione intermedia.

- **Generare un certificato autofirmato**.
- **Utilizzare il certificato globale StorageGRID S3 e Swift**. È necessario caricare o generare una versione personalizzata del certificato prima di poterla selezionare per l'endpoint del bilanciamento del carico. Vedere "Configurare i certificati API S3 e Swift".

Di quali valori ho bisogno?

Per creare il certificato, è necessario conoscere tutti i nomi di dominio e gli indirizzi IP utilizzati dalle applicazioni client S3 o Swift per accedere all'endpoint.

La voce **Subject DN** (Distinguished Name) per il certificato deve includere il nome di dominio completo che l'applicazione client utilizzerà per StorageGRID. Ad esempio:

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Se necessario, il certificato può utilizzare i caratteri jolly per rappresentare i nomi di dominio completi di tutti i nodi Admin e Gateway che eseguono il servizio Load Balancer. Ad esempio, `*.storagegrid.example.com` utilizza il carattere jolly * per rappresentare `adm1.storagegrid.example.com` e. `gn1.storagegrid.example.com`.

Se si prevede di utilizzare richieste in stile host virtuali S3, il certificato deve includere anche una voce **Nome alternativo** per ciascuna "Nome di dominio dell'endpoint S3" sono stati configurati, inclusi i nomi con caratteri jolly. Ad esempio:

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

Se si utilizzano caratteri jolly per i nomi di dominio, consultare "Linee guida per la protezione avanzata dei certificati server".

È inoltre necessario definire una voce DNS per ciascun nome nel certificato di protezione.

Come si gestiscono i certificati in scadenza?

Se il certificato utilizzato per proteggere la connessione tra l'applicazione S3 e StorageGRID scade, l'applicazione potrebbe perdere temporaneamente l'accesso a StorageGRID.

Per evitare problemi di scadenza del certificato, attenersi alle seguenti Best practice:

- Monitorare attentamente gli avvisi che avvisano di avvicinarsi alle date di scadenza del certificato, come ad

esempio **scadenza del certificato endpoint del bilanciamento del carico** e **scadenza del certificato server globale per gli avvisi S3 e Swift API**.

- Mantenere sempre sincronizzate le versioni del certificato delle applicazioni StorageGRID e S3. Se si sostituisce o si rinnova il certificato utilizzato per un endpoint di bilanciamento del carico, è necessario sostituire o rinnovare il certificato equivalente utilizzato dall'applicazione S3.
- Utilizzare un certificato CA con firma pubblica. Se si utilizza un certificato firmato da una CA, è possibile sostituire i certificati in scadenza senza interruzioni.
- Se è stato generato un certificato StorageGRID autofirmato e il certificato sta per scadere, è necessario sostituirlo manualmente in StorageGRID e nell'applicazione S3 prima della scadenza del certificato esistente.

Considerazioni per la modalità di binding

La modalità di binding consente di controllare quali indirizzi IP possono essere utilizzati per accedere a un endpoint del bilanciamento del carico. Se un endpoint utilizza una modalità di binding, le applicazioni client possono accedere all'endpoint solo se utilizzano un indirizzo IP consentito o il corrispondente FQDN (Fully Qualified Domain Name). Le applicazioni client che utilizzano qualsiasi altro indirizzo IP o FQDN non possono accedere all'endpoint.

È possibile specificare una delle seguenti modalità di binding:

- **Globale** (impostazione predefinita): Le applicazioni client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare questa impostazione a meno che non sia necessario limitare l'accessibilità di un endpoint.
- **IP virtuali dei gruppi ha**. Le applicazioni client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha.
- **Interfacce nodo**. I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate.
- **Tipo di nodo**. In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway.

Considerazioni sull'accesso al tenant

L'accesso tenant è una funzionalità di sicurezza opzionale che consente di controllare quali account tenant StorageGRID possono utilizzare un endpoint di bilanciamento del carico per accedere ai bucket. È possibile consentire a tutti i tenant di accedere a un endpoint (impostazione predefinita) oppure specificare un elenco dei tenant consentiti o bloccati per ciascun endpoint.

È possibile utilizzare questa funzionalità per fornire un migliore isolamento della sicurezza tra i tenant e i relativi endpoint. Ad esempio, è possibile utilizzare questa funzione per garantire che i materiali top-secret o altamente classificati di proprietà di un tenant rimangano completamente inaccessibili agli altri tenant.

> Ai fini del controllo degli accessi, il tenant viene determinato dalle chiavi di accesso utilizzate nella richiesta del client; se non vengono fornite chiavi di accesso come parte della richiesta (ad esempio con accesso anonimo), il proprietario del bucket viene utilizzato per determinare il tenant.

Esempio di accesso al tenant

Per comprendere il funzionamento di questa funzionalità di sicurezza, si consideri il seguente esempio:

1. Sono stati creati due endpoint di bilanciamento del carico, come segue:
   - Endpoint **Public**: Utilizza la porta 10443 e consente l'accesso a tutti i tenant.
   - Endpoint **Top secret**: Utilizza la porta 10444 e consente l'accesso solo al tenant **Top secret**. Tutti gli altri tenant non possono accedere a questo endpoint.
2. Il `top-secret.pdf` Si trova in un bucket di proprietà del tenant **Top Secret**.

Per accedere a. `top-secret.pdf`, Un utente nel tenant **Top secret** può inviare una richiesta GET a. `https://w.x.y.z:10444/top-secret.pdf`. Poiché a questo tenant è consentito utilizzare l'endpoint 10444, l'utente può accedere all'oggetto. Tuttavia, se un utente appartenente a un altro tenant invia la stessa richiesta allo stesso URL, riceve un messaggio di accesso immediato negato. L'accesso viene negato anche se le credenziali e la firma sono valide.

Disponibilità della CPU

Il servizio Load Balancer su ciascun nodo Admin e nodo Gateway opera in modo indipendente quando inoltra il traffico S3 o Swift ai nodi Storage. Attraverso un processo di ponderazione, il servizio Load Balancer indirizza più richieste ai nodi di storage con una maggiore disponibilità della CPU. Le informazioni sul carico della CPU del nodo vengono aggiornate ogni pochi minuti, ma la ponderazione potrebbe essere aggiornata più frequentemente. A tutti i nodi di storage viene assegnato un valore minimo di peso di base, anche se un nodo riporta un utilizzo pari al 100% o non ne riporta l'utilizzo.

In alcuni casi, le informazioni sulla disponibilità della CPU sono limitate al sito in cui si trova il servizio Load Balancer.

Configurare gli endpoint del bilanciamento del carico

Gli endpoint del bilanciamento del carico determinano le porte e i protocolli di rete che i client S3 e Swift possono utilizzare per la connessione al bilanciamento del carico StorageGRID sui nodi gateway e di amministrazione. È inoltre possibile utilizzare gli endpoint per accedere a Grid Manager, Tenant Manager o a entrambi.

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Hai esaminato il "considerazioni per il bilanciamento del carico".
- Se in precedenza è stata rimappata una porta che si intende utilizzare per l'endpoint del bilanciamento del carico, è possibile "rimosso il remap della porta".
- Hai creato tutti i gruppi ad alta disponibilità (ha) che intendi utilizzare. I gruppi HA sono consigliati, ma non richiesti. Vedere "Gestire i gruppi ad alta disponibilità".
- Se l'endpoint del bilanciamento del carico verrà utilizzato da "S3 tenant per S3 Select", Non deve utilizzare gli indirizzi IP o FQDN di nodi bare-metal. Per gli endpoint del bilanciamento del carico utilizzati per S3 Select sono consentiti solo le appliance di servizi e i nodi software basati su VMware.
- Sono state configurate le interfacce VLAN che si intende utilizzare. Vedere "Configurare le interfacce

VLAN".

- Se si crea un endpoint HTTPS (consigliato), si dispone delle informazioni per il certificato del server.

  > Le modifiche a un certificato endpoint possono richiedere fino a 15 minuti per essere applicate a tutti i nodi.

  - Per caricare un certificato, è necessario disporre del certificato del server, della chiave privata del certificato e, facoltativamente, di un bundle CA.
  - Per generare un certificato, sono necessari tutti i nomi di dominio e gli indirizzi IP utilizzati dai client S3 o Swift per accedere all'endpoint. Devi anche conoscere l'oggetto (Nome distinto).
  - Se si desidera utilizzare il certificato API StorageGRID S3 e Swift (che può essere utilizzato anche per le connessioni dirette ai nodi di storage), il certificato predefinito è già stato sostituito con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "Configurare i certificati API S3 e Swift".

Creare un endpoint per il bilanciamento del carico

Ogni endpoint del bilanciamento del carico dei client S3 o Swift specifica una porta, un tipo di client (S3 o Swift) e un protocollo di rete (HTTP o HTTPS). Gli endpoint del bilanciamento del carico dell'interfaccia di gestione specificano una porta, un tipo di interfaccia e una rete client non attendibile.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
2. Per creare un endpoint per un client S3 o Swift, selezionare la scheda **S3 o Swift client**.
3. Per creare un endpoint per l'accesso a Grid Manager, Tenant Manager o entrambi, selezionare la scheda **interfaccia di gestione**.
4. Selezionare **Crea**.

Inserire i dettagli dell'endpoint

Fasi

1. Selezionare le istruzioni appropriate per inserire i dettagli per il tipo di endpoint che si desidera creare.

Client S3 o Swift

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per il bilanciamento del carico. Per impostazione predefinita, questo campo è impostato su 10433 per il primo endpoint creato, ma è possibile immettere qualsiasi porta esterna non utilizzata compresa tra 1 e 65535. Se si immette **80** o **8443**, l'endpoint viene configurato solo sui nodi Gateway, a meno che non sia stata liberata la porta 8443. Quindi è possibile utilizzare la porta 8443 come endpoint S3 e la porta verrà configurata su entrambi i nodi Gateway e Admin.
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, **S3** o **Swift**.
Protocollo di rete	Il protocollo di rete che i client utilizzeranno per la connessione a questo endpoint. • Selezionare **HTTPS** per la comunicazione sicura con crittografia TLS (scelta consigliata). È necessario allegare un certificato di sicurezza prima di poter salvare l'endpoint. • Selezionare **HTTP** per comunicazioni meno sicure e non crittografate. Utilizzare HTTP solo per una griglia non di produzione.

Interfaccia di gestione

Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	La porta StorageGRID che si desidera utilizzare per accedere a Gestore griglia, Gestore tenant o entrambi. • Gestore griglia: **8443** • Responsabile del tenant: **9443** • Sia Grid Manager che Tenant Manager: **443** **Nota**: È possibile utilizzare queste porte preimpostate o altre porte disponibili.
Tipo di interfaccia	Selezionare il pulsante di opzione per l'interfaccia StorageGRID a cui si accede utilizzando questo endpoint.

Campo	Descrizione
Rete client non attendibile	Selezionare **Sì** se l'endpoint deve essere accessibile alle reti client non attendibili. In caso contrario, selezionare **No**. Quando si seleziona **Sì**, la porta è aperta su tutte le reti client non attendibili. **Nota**: È possibile configurare una porta per essere aperta o chiusa a reti client non attendibili solo quando si crea l'endpoint di bilanciamento del carico.

1. Selezionare **continua**.

Selezionare una modalità di binding

Fasi

1. Selezionare una modalità di associazione per l'endpoint per controllare la modalità di accesso all'endpoint utilizzando qualsiasi indirizzo IP o specifici indirizzi IP e interfacce di rete.

   Alcune modalità di associazione sono disponibili per gli endpoint client o per gli endpoint dell'interfaccia di gestione. Tutte le modalità per entrambi i tipi di endpoint sono elencate di seguito.

Modalità	Descrizione
Globale (impostazione predefinita per gli endpoint client)	I client possono accedere all'endpoint utilizzando l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore, l'indirizzo IP virtuale (VIP) di qualsiasi gruppo ha su qualsiasi rete o un FQDN corrispondente. Utilizzare l'impostazione **Globale** a meno che non sia necessario limitare l'accessibilità di questo endpoint.
IP virtuali dei gruppi ha	Per accedere a questo endpoint, i client devono utilizzare un indirizzo IP virtuale (o un FQDN corrispondente) di un gruppo ha. Gli endpoint con questa modalità di binding possono utilizzare tutti lo stesso numero di porta, purché i gruppi ha selezionati per gli endpoint non si sovrappongano.
Interfacce di nodo	I client devono utilizzare gli indirizzi IP (o gli FQDN corrispondenti) delle interfacce dei nodi selezionate per accedere a questo endpoint.
Tipo di nodo (solo endpoint client)	In base al tipo di nodo selezionato, i client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di amministrazione o l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo di gateway per accedere a questo endpoint.

Modalità	Descrizione
Tutti i nodi amministrativi (impostazione predefinita per gli endpoint dell'interfaccia di gestione)	I client devono utilizzare l'indirizzo IP (o il corrispondente FQDN) di qualsiasi nodo amministrativo per accedere a questo endpoint.

Se più di un endpoint utilizza la stessa porta, StorageGRID utilizza questo ordine di priorità per decidere quale endpoint utilizzare: **IP virtuali dei gruppi ha** > **interfacce nodo** > **tipo di nodo** > **Globale**.

Se si stanno creando endpoint dell'interfaccia di gestione, sono consentiti solo i nodi Admin.

2. Se si seleziona **IP virtuali dei gruppi ha**, selezionare uno o più gruppi ha.

   Se si stanno creando endpoint dell'interfaccia di gestione, selezionare VIP associati solo ai nodi Admin.

3. Se si seleziona **Node interfaces**, selezionare una o più interfacce di nodo per ciascun nodo Admin o nodo gateway che si desidera associare a questo endpoint.
4. Se si seleziona **Node type** (tipo nodo), selezionare Admin Node (nodi amministratore), che include sia l'Admin Node primario che qualsiasi Admin Node non primario, oppure Gateway Node (nodi gateway).

Controllo dell'accesso al tenant

Un endpoint dell'interfaccia di gestione può controllare l'accesso al tenant solo quando l'endpoint dispone di Tipo di interfaccia di Tenant Manager.

Fasi

1. Per il passaggio **accesso tenant**, selezionare una delle seguenti opzioni:

Campo	Descrizione
Allow all tenant (Consenti tutti i tenant) (impostazione predefinita	Tutti gli account tenant possono utilizzare questo endpoint per accedere ai bucket. Selezionare questa opzione se non sono ancora stati creati account tenant. Dopo aver aggiunto account tenant, è possibile modificare l'endpoint del bilanciamento del carico per consentire o bloccare account specifici.
Consenti tenant selezionati	Solo gli account tenant selezionati possono utilizzare questo endpoint per accedere ai bucket.
Blocca i tenant selezionati	Gli account tenant selezionati non possono utilizzare questo endpoint per accedere ai bucket. Tutti gli altri tenant possono utilizzare questo endpoint.

2. Se si crea un endpoint **HTTP**, non è necessario allegare un certificato. Selezionare **Create** per aggiungere il nuovo endpoint del bilanciamento del carico. Quindi, passare a. Al termine. In caso contrario, selezionare **continua** per allegare il certificato.

Allega certificato

Fasi

1. Se si sta creando un endpoint **HTTPS**, selezionare il tipo di certificato di sicurezza che si desidera allegare all'endpoint.

   Il certificato protegge le connessioni tra i client S3 e Swift e il servizio Load Balancer sui nodi Admin Node o Gateway.

   - **Carica certificato**. Selezionare questa opzione se si dispone di certificati personalizzati da caricare.
   - **Genera certificato**. Selezionare questa opzione se si dispone dei valori necessari per generare un certificato personalizzato.
   - **Utilizzare il certificato StorageGRID S3 e Swift**. Selezionare questa opzione se si desidera utilizzare il certificato globale S3 e Swift API, che può essere utilizzato anche per le connessioni dirette ai nodi di storage.

     Non è possibile selezionare questa opzione a meno che non sia stato sostituito il certificato S3 e Swift API predefinito, firmato dalla CA Grid, con un certificato personalizzato firmato da un'autorità di certificazione esterna. Vedere "Configurare i certificati API S3 e Swift".

   - **Utilizza certificato interfaccia di gestione**. Selezionare questa opzione se si desidera utilizzare il certificato dell'interfaccia di gestione globale, che può essere utilizzato anche per le connessioni dirette ai nodi amministrativi.
2. Se non si utilizza il certificato StorageGRID S3 e Swift, caricare o generare il certificato.

Carica certificato

a. Selezionare **carica certificato**.

b. Caricare i file dei certificati del server richiesti:

- **Server certificate**: Il file di certificato del server personalizzato in codifica PEM.
- **Certificate private key** (chiave privata certificato): Il file di chiave privata del certificato del server personalizzato (`.key`).

> Le chiavi private EC devono essere di almeno 224 bit. Le chiavi private RSA devono essere 2048 bit o superiori.

- **Bundle CA**: Un singolo file opzionale contenente i certificati di ogni autorità di certificazione di emissione intermedia (CA). Il file deve contenere ciascuno dei file di certificato CA con codifica PEM, concatenati in ordine di catena del certificato.

c. Espandere **Dettagli certificato** per visualizzare i metadati di ciascun certificato caricato. Se è stato caricato un bundle CA opzionale, ciascun certificato viene visualizzato nella propria scheda.

- Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato oppure selezionare **Download CA bundle** (Scarica pacchetto CA) per salvare il bundle del certificato.

  Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

  Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy certificate PEM** or **Copy CA bundle PEM** per copiare il contenuto del certificato e incollarlo altrove.

d. Selezionare **Crea**.
Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift o l'interfaccia di gestione e l'endpoint.

Generare un certificato

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

Campo	Descrizione
Nome di dominio	Uno o più nomi di dominio completi da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
IP	Uno o più indirizzi IP da includere nel certificato.

Campo	Descrizione
Soggetto (facoltativo)	X.509 nome soggetto o nome distinto (DN) del proprietario del certificato. Se in questo campo non viene immesso alcun valore, il certificato generato utilizza il primo nome di dominio o indirizzo IP come nome comune (CN) del soggetto.
Giorni di validità	Numero di giorni successivi alla creazione della scadenza del certificato.
Aggiungere estensioni di utilizzo chiave	Se selezionata (impostazione predefinita e consigliata), l'utilizzo delle chiavi e le estensioni estese dell'utilizzo delle chiavi vengono aggiunte al certificato generato. Queste estensioni definiscono lo scopo della chiave contenuta nel certificato. **Nota**: Lasciare questa casella di controllo selezionata a meno che non si verifichino problemi di connessione con client meno recenti quando i certificati includono queste estensioni.

c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Crea**.

   Viene creato l'endpoint del bilanciamento del carico. Il certificato personalizzato viene utilizzato per tutte le nuove connessioni successive tra i client S3 e Swift o l'interfaccia di gestione e questo endpoint.

Al termine

Fasi

1. Se si utilizza un DNS, assicurarsi che il DNS includa un record per associare il nome di dominio completo (FQDN, Fully Qualified Domain Name) di StorageGRID a ciascun indirizzo IP utilizzato dai client per effettuare le connessioni.

   L'indirizzo IP inserito nel record DNS dipende dall'utilizzo di un gruppo ha di nodi per il bilanciamento del carico:

- Se è stato configurato un gruppo ha, i client si connetteranno agli indirizzi IP virtuali di quel gruppo ha.
- Se non si utilizza un gruppo ha, i client si connetteranno al servizio bilanciamento del carico StorageGRID utilizzando l'indirizzo IP di un nodo gateway o di un nodo amministratore.

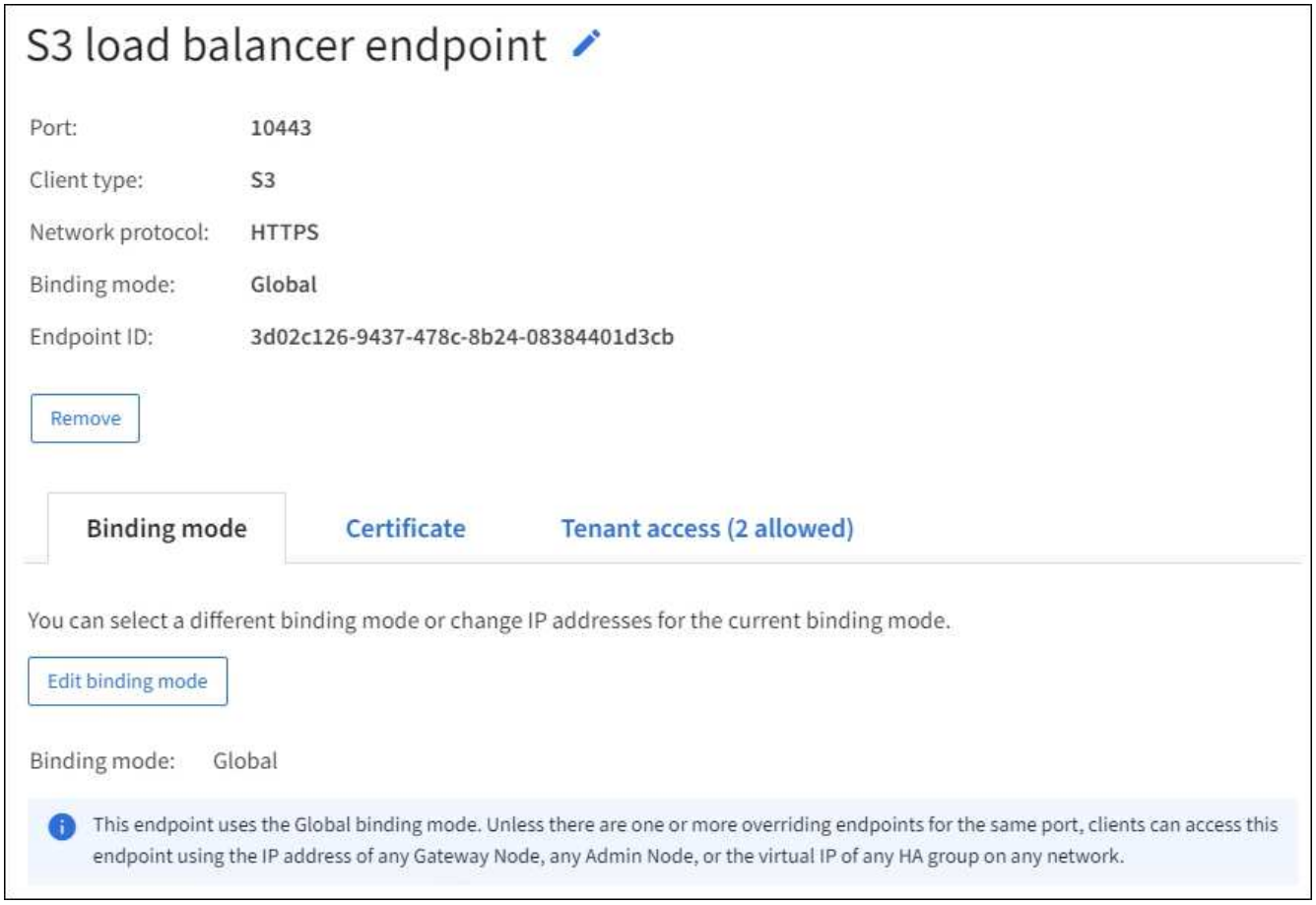
  È inoltre necessario assicurarsi che il record DNS faccia riferimento a tutti i nomi di dominio degli endpoint richiesti, inclusi i nomi con caratteri jolly.

2. Fornire ai client S3 e Swift le informazioni necessarie per connettersi all'endpoint:
   - Numero di porta
   - Nome di dominio completo o indirizzo IP
   - Tutti i dettagli del certificato richiesti

Visualizzare e modificare gli endpoint del bilanciamento del carico

È possibile visualizzare i dettagli degli endpoint del bilanciamento del carico esistenti, inclusi i metadati del certificato per un endpoint protetto. È possibile modificare determinate impostazioni per un endpoint.

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, esaminare le tabelle nella pagina Endpoints del bilanciamento del carico.
- Per visualizzare tutti i dettagli relativi a un endpoint specifico, inclusi i metadati del certificato, selezionare il nome dell'endpoint nella tabella. Le informazioni visualizzate variano a seconda del tipo di endpoint e della sua configurazione.



- Per modificare un endpoint, utilizzare il menu **azioni** nella pagina Endpoints del bilanciamento del carico.

Se si perde l'accesso a Grid Manager durante la modifica della porta di un endpoint dell'interfaccia di gestione, aggiornare l'URL e la porta per riottenere l'accesso.

Dopo aver modificato un endpoint, potrebbe essere necessario attendere fino a 15 minuti per applicare le modifiche a tutti i nodi.

Attività	Menu delle azioni	Pagina dei dettagli
Modificare il nome dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica nome endpoint**. c. Inserire il nuovo nome. d. Selezionare **Salva**.	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Salva**.
Modificare la porta dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica porta endpoint** c. Immettere un numero di porta valido. d. Selezionare **Salva**.	*n/a*
Modificare la modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica modalità di associazione endpoint**. c. Aggiornare la modalità di binding secondo necessità. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare **Edit binding mode** (Modifica modalità di associazione). c. Aggiornare la modalità di binding secondo necessità. d. Selezionare **Save Changes** (Salva modifiche).
Modificare il certificato dell'endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica certificato endpoint**. c. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda **certificato**. c. Selezionare **Modifica certificato**. d. Caricare o generare un nuovo certificato personalizzato o iniziare a utilizzare il certificato globale S3 e Swift, come richiesto. e. Selezionare **Save Changes** (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modificare l'accesso al tenant	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **azioni** > **Modifica accesso tenant**. c. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'endpoint per visualizzare i dettagli. b. Selezionare la scheda **accesso tenant**. c. Selezionare **Edit tenant access** (Modifica accesso tenant). d. Scegliere un'opzione di accesso diversa, selezionare o rimuovere i tenant dall'elenco oppure eseguire entrambe le operazioni. e. Selezionare **Save Changes** (Salva modifiche).

Rimuovere gli endpoint del bilanciamento del carico

È possibile rimuovere uno o più endpoint dal menu **azioni** oppure rimuovere un singolo endpoint dalla pagina dei dettagli.

> Per evitare interruzioni del client, aggiornare le applicazioni client S3 o Swift interessate prima di rimuovere un endpoint di bilanciamento del carico. Aggiornare ogni client per la connessione utilizzando una porta assegnata a un altro endpoint del bilanciamento del carico. Assicurarsi di aggiornare anche tutte le informazioni di certificato richieste.

> Se si perde l'accesso a Grid Manager durante la rimozione di un endpoint dell'interfaccia di gestione, aggiornare l'URL.

- Per rimuovere uno o più endpoint:
  a. Dalla pagina bilanciamento del carico, selezionare la casella di controllo per ciascun endpoint che si desidera rimuovere.
  b. Selezionare **azioni** > **Rimuovi**.
  c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
  a. Dalla pagina bilanciamento del carico. selezionare il nome dell'endpoint.
  b. Selezionare **Rimuovi** nella pagina dei dettagli.
  c. Selezionare **OK**.

Configurare i nomi di dominio degli endpoint S3

Per supportare le richieste in stile virtual-hosted S3, è necessario utilizzare Grid Manager per configurare l'elenco dei nomi di dominio degli endpoint S3 a cui si connettono i client S3.

L'utilizzo di un indirizzo IP per un nome di dominio endpoint non è supportato. Le versioni future impediranno questa configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai confermato che non è in corso un aggiornamento della griglia.

Non apportare modifiche alla configurazione del nome di dominio quando è in corso un aggiornamento della griglia.

A proposito di questa attività

Per consentire ai client di utilizzare i nomi di dominio degli endpoint S3, è necessario eseguire tutte le seguenti operazioni:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il "Certificato utilizzato dal client per le connessioni HTTPS a StorageGRID" è firmato per tutti i nomi di dominio richiesti dal client.

  Ad esempio, se l'endpoint è `s3.company.com`, È necessario assicurarsi che il certificato utilizzato per le connessioni HTTPS includa `s3.company.com` Endpoint e SAN (Subject alternative Name) con caratteri jolly dell'endpoint: `*.s3.company.com`.

- Configurare il server DNS utilizzato dal client. Includere i record DNS per gli indirizzi IP utilizzati dai client per effettuare le connessioni e assicurarsi che i record riferiscano a tutti i nomi di dominio degli endpoint S3 richiesti, inclusi i nomi con caratteri jolly.

I client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo gateway, di un nodo amministratore o di un nodo di storage oppure connettendosi all'indirizzo IP virtuale di un gruppo ad alta disponibilità. È necessario comprendere il modo in cui le applicazioni client si connettono alla griglia in modo da includere gli indirizzi IP corretti nei record DNS.

I client che utilizzano connessioni HTTPS (consigliate) alla griglia possono utilizzare uno dei seguenti certificati:

- I client che si connettono a un endpoint di bilanciamento del carico possono utilizzare un certificato personalizzato per tale endpoint. Ogni endpoint del bilanciamento del carico può essere configurato per riconoscere diversi nomi di dominio degli endpoint S3.
- I client che si connettono a un endpoint di bilanciamento del carico o direttamente a un nodo di storage possono personalizzare il certificato globale S3 e Swift API per includere tutti i nomi di dominio degli endpoint S3 richiesti.

Se non si aggiungono nomi di dominio degli endpoint S3 e l'elenco è vuoto, il supporto per le richieste in stile virtual-hosted S3 viene disattivato.

Aggiungere un nome di dominio dell'endpoint S3

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **S3 endpoint domain name**.
2. Inserire il nome di dominio nel campo **Domain name 1**. Selezionare **Aggiungi un altro nome di dominio** per aggiungere altri nomi di dominio.
3. Selezionare **Salva**.
4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint S3 richiesti.
   - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il proprio certificato, "aggiornare il certificato associato all'endpoint".
   - Se i client si connettono a un endpoint di bilanciamento del carico che utilizza il certificato globale S3 e Swift API o direttamente ai nodi di storage, "Aggiornare il certificato globale S3 e Swift API".
5. Aggiungere i record DNS necessari per garantire che le richieste dei nomi di dominio degli endpoint possano essere risolte.

Risultato

Ora, quando i client utilizzano l'endpoint `bucket.s3.company.com`, Il server DNS si risolve nell'endpoint corretto e il certificato autentica l'endpoint come previsto.

Rinominare un nome di dominio endpoint S3

Se si modifica un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **S3 endpoint domain name**.
2. Selezionare il campo del nome di dominio che si desidera modificare e apportare le modifiche necessarie.
3. Selezionare **Salva**.
4. Selezionare **Sì** per confermare la modifica.

Eliminare un nome di dominio dell'endpoint S3

Se si rimuove un nome utilizzato dalle applicazioni S3, le richieste di tipo virtual-hosted non avranno esito positivo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **S3 endpoint domain name**.
2. Selezionare l'icona di eliminazione ✕ accanto al nome di dominio.
3. Selezionare **Sì** per confermare l'eliminazione.

Informazioni correlate

- "UTILIZZARE L'API REST S3"
- "Visualizzare gli indirizzi IP"
- "Configurare i gruppi ad alta disponibilità"

Riepilogo: Indirizzi IP e porte per le connessioni client

Per memorizzare o recuperare oggetti, le applicazioni client S3 e Swift si connettono al servizio Load Balancer, incluso in tutti i nodi Admin e Gateway, o al servizio Local

Distribution Router (LDR), incluso in tutti i nodi Storage.

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un nodo Grid e il numero di porta del servizio su tale nodo. Facoltativamente, è possibile creare gruppi ad alta disponibilità (ha) di nodi di bilanciamento del carico per fornire connessioni ad alta disponibilità che utilizzano indirizzi IP virtuali (VIP). Se si desidera connettersi a StorageGRID utilizzando un nome di dominio completo (FQDN) invece di un indirizzo IP o VIP, è possibile configurare le voci DNS.

Questa tabella riassume i diversi modi in cui i client possono connettersi a StorageGRID e gli indirizzi IP e le porte utilizzati per ciascun tipo di connessione. Se sono già stati creati endpoint di bilanciamento del carico e gruppi ad alta disponibilità (ha), vedere Dove trovare gli indirizzi IP Per individuare questi valori in Grid Manager.

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Gruppo HA	Bilanciamento del carico	Indirizzo IP virtuale di un gruppo ha	Porta assegnata all'endpoint del bilanciamento del carico
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	Porta assegnata all'endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	Porta assegnata all'endpoint del bilanciamento del carico
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084 Porte Swift predefinite: • HTTPS: 18083 • HTTP:18085

URL di esempio

Per connettere un'applicazione client all'endpoint Load Balancer di un gruppo ha di nodi gateway, utilizzare un URL strutturato come mostrato di seguito:

`https://VIP-of-HA-group:LB-endpoint-port`

Ad esempio, se l'indirizzo IP virtuale del gruppo ha è 192.0.2.5 e il numero di porta dell'endpoint del bilanciamento del carico è 10443, un'applicazione potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

`https://192.0.2.5:10443`

Dove trovare gli indirizzi IP

1. Accedere a Grid Manager utilizzando un "browser web supportato".
2. Per trovare l'indirizzo IP di un nodo Grid:
   a. Selezionare **NODI**.
   b. Selezionare il nodo Admin, il nodo gateway o il nodo di storage a cui si desidera connettersi.
   c. Selezionare la scheda **Panoramica**.
   d. Nella sezione Node Information (informazioni sul nodo), annotare gli indirizzi IP del nodo.
   e. Selezionare **Mostra altro** per visualizzare gli indirizzi IPv6 e le mappature dell'interfaccia.

      È possibile stabilire connessioni dalle applicazioni client a uno qualsiasi degli indirizzi IP presenti nell'elenco:

      - **Eth0:** Grid Network
      - **Eth1:** Admin Network (opzionale)
      - **Eth2:** rete client (opzionale)

      > Se si sta visualizzando un nodo Admin o un nodo Gateway e si tratta del nodo attivo di un gruppo ad alta disponibilità, l'indirizzo IP virtuale del gruppo ha viene visualizzato su eth2.

3. Per trovare l'indirizzo IP virtuale di un gruppo ad alta disponibilità:
   a. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
   b. Nella tabella, annotare l'indirizzo IP virtuale del gruppo ha.
4. Per trovare il numero di porta di un endpoint Load Balancer:
   a. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
   b. Annotare il numero di porta dell'endpoint che si desidera utilizzare.

      > Se il numero di porta è 80 o 443, l'endpoint viene configurato solo sui nodi gateway, poiché tali porte sono riservate sui nodi Admin. Tutte le altre porte sono configurate sia sui nodi Gateway che sui nodi Admin.

   c. Selezionare il nome dell'endpoint dalla tabella.
   d. Verificare che il **tipo di client** (S3 o Swift) corrisponda all'applicazione client che utilizzerà l'endpoint.

Gestire reti e connessioni

Configurazione delle impostazioni di rete: Panoramica

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

Configurare le interfacce VLAN

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

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

Policy di classificazione del traffico

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

Linee guida per le reti StorageGRID

È possibile utilizzare Grid Manager per configurare e gestire le reti e le connessioni StorageGRID.

Vedere "Configurare le connessioni client S3 e Swift" Per scoprire come connettere i client S3 o Swift.

Reti StorageGRID predefinite

Per impostazione predefinita, StorageGRID supporta tre interfacce di rete per nodo di rete, consentendo di configurare la rete per ogni singolo nodo di rete in modo che corrisponda ai requisiti di sicurezza e accesso.

Per ulteriori informazioni sulla topologia di rete, vedere "Linee guida per il networking".

Grid Network

Obbligatorio. La rete griglia viene utilizzata per tutto il traffico StorageGRID interno. Fornisce connettività tra tutti i nodi della rete, in tutti i siti e le subnet.

Admin Network (rete amministrativa)

Opzionale. La rete di amministrazione viene generalmente utilizzata per l'amministrazione e la manutenzione del sistema. Può essere utilizzato anche per l'accesso al protocollo client. La rete di amministrazione è in genere una rete privata e non deve essere instradabile tra i siti.

Rete client

Opzionale. La rete client è una rete aperta, generalmente utilizzata per fornire l'accesso alle applicazioni client S3 e Swift, in modo che la rete grid possa essere isolata e protetta. La rete client può comunicare con qualsiasi subnet raggiungibile tramite il gateway locale.

Linee guida

- Ogni nodo StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ogni rete a cui è assegnato.
- Un nodo Grid non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway, per rete, per nodo di rete, che deve trovarsi sulla stessa sottorete del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ciascun nodo, ogni rete viene mappata a una specifica interfaccia di rete.

Rete	Nome dell'interfaccia
Griglia	eth0

Rete	Nome dell'interfaccia
Admin (opzionale)	eth1
Client (opzionale)	eth2

- Se il nodo è collegato a un'appliance StorageGRID, vengono utilizzate porte specifiche per ciascuna rete. Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è attivato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza Grid Network su eth0.
- La rete client non diventa operativa fino a quando il nodo grid non si è Unito alla griglia
- La rete amministrativa può essere configurata durante l'implementazione del nodo grid per consentire l'accesso all'interfaccia utente dell'installazione prima che la griglia sia completamente installata.

Interfacce opzionali

In alternativa, è possibile aggiungere interfacce aggiuntive a un nodo. Ad esempio, è possibile aggiungere un'interfaccia di linea a un nodo Admin o Gateway, in modo da poterlo utilizzare "Interfacce VLAN" separare il traffico che appartiene a diverse applicazioni o tenant. In alternativa, è possibile aggiungere un'interfaccia di accesso da utilizzare in "Gruppo ad alta disponibilità (ha)".

Per aggiungere trunk o interfacce di accesso, vedere quanto segue:

- **VMware (dopo l'installazione del nodo)**: "VMware: Aggiunta di interfacce di accesso o trunk a un nodo"
  - **Red Hat Enterprise Linux (prima di installare il nodo)**: "Creare file di configurazione del nodo"
  - **Ubuntu o Debian (prima di installare il nodo)**: "Creare file di configurazione del nodo"
  - **RHEL, Ubuntu o Debian (dopo aver installato il nodo)**: "Linux: Aggiunta di interfacce di accesso o trunk a un nodo"

Visualizzare gli indirizzi IP

È possibile visualizzare l'indirizzo IP di ciascun nodo della griglia nel sistema StorageGRID. È quindi possibile utilizzare questo indirizzo IP per accedere al nodo Grid dalla riga di comando ed eseguire varie procedure di manutenzione.

Prima di iniziare

Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

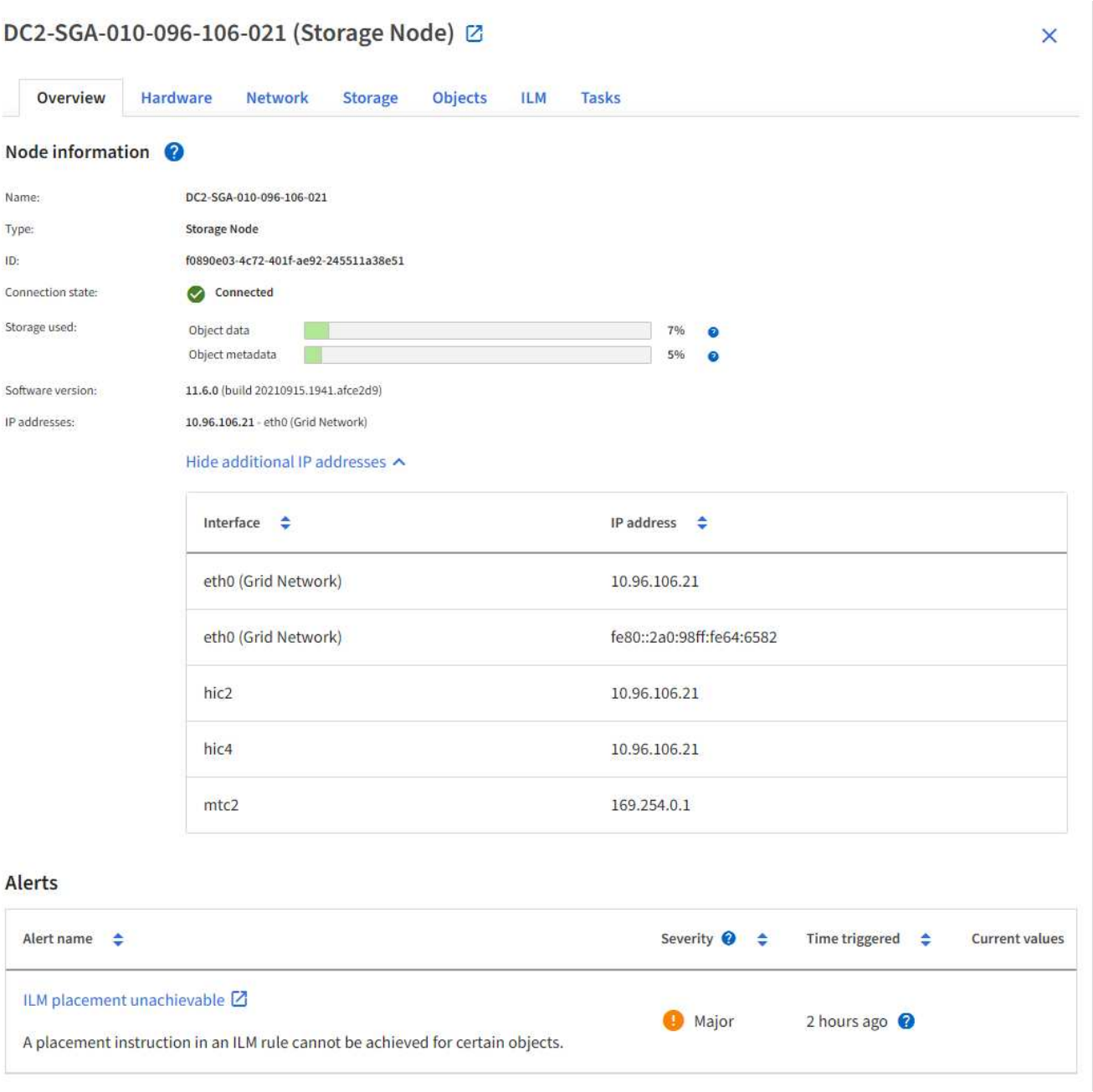
A proposito di questa attività

Per informazioni sulla modifica degli indirizzi IP, vedere "Configurare gli indirizzi IP".

Fasi

1. Selezionare **NODES** > ***Grid Node*** > **Overview**.
2. Selezionare **Mostra altri** a destra del titolo indirizzi IP.

   Gli indirizzi IP per il nodo della griglia sono elencati in una tabella.



Configurare le interfacce VLAN

È possibile creare interfacce LAN virtuale (VLAN) su nodi Admin e nodi Gateway e utilizzarle in gruppi ha ed endpoint di bilanciamento del carico per isolare e partizionare il traffico per garantire sicurezza, flessibilità e performance.

Considerazioni per le interfacce VLAN

- Per creare un'interfaccia VLAN, immettere un ID VLAN e scegliere un'interfaccia principale su uno o più nodi.
- Un'interfaccia principale deve essere configurata come interfaccia di linea sullo switch.
- Un'interfaccia padre può essere Grid Network (eth0), Client Network (eth2) o un'interfaccia trunk aggiuntiva per la macchina virtuale o l'host bare-metal (ad esempio, ens256).

- Per ogni interfaccia VLAN, è possibile selezionare solo un'interfaccia principale per un nodo specifico. Ad esempio, non è possibile utilizzare l'interfaccia Grid Network e l'interfaccia Client Network sullo stesso nodo gateway dell'interfaccia principale per la stessa VLAN.
- Se l'interfaccia VLAN è per il traffico Admin Node, che include il traffico correlato a Grid Manager e Tenant Manager, selezionare le interfacce solo sui nodi Admin.
- Se l'interfaccia VLAN è per il traffico client S3 o Swift, selezionare le interfacce sui nodi Admin o Gateway.
- Per ulteriori informazioni sull'aggiunta di interfacce di linea, consultare quanto segue:
  - **VMware (dopo l'installazione del nodo)**: "VMware: Aggiunta di interfacce di accesso o trunk a un nodo"
  - **RHEL (prima di installare il nodo)**: "Creare file di configurazione del nodo"
  - **Ubuntu o Debian (prima di installare il nodo)**: "Creare file di configurazione del nodo"
  - **RHEL, Ubuntu o Debian (dopo aver installato il nodo)**: "Linux: Aggiunta di interfacce di accesso o trunk a un nodo"

Creare un'interfaccia VLAN

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Un'interfaccia di linea è stata configurata nella rete e collegata al nodo VM o Linux. Si conosce il nome dell'interfaccia di linea.
- Si conosce l'ID della VLAN che si sta configurando.

A proposito di questa attività

L'amministratore di rete potrebbe aver configurato una o più interfacce di trunk e una o più VLAN per separare il traffico client o amministrativo che appartiene a diverse applicazioni o tenant. Ogni VLAN è identificata da un ID numerico o da un tag. Ad esempio, la rete potrebbe utilizzare la VLAN 100 per il traffico FabricPool e la VLAN 200 per un'applicazione di archiviazione.

È possibile utilizzare Grid Manager per creare interfacce VLAN che consentono ai client di accedere a StorageGRID su una VLAN specifica. Quando si creano interfacce VLAN, specificare l'ID VLAN e selezionare le interfacce principali (trunk) su uno o più nodi.

Accedere alla procedura guidata

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selezionare **Crea**.

Inserire i dettagli delle interfacce VLAN

Fasi

1. Specificare l'ID della VLAN nella rete. È possibile immettere un valore compreso tra 1 e 4094.

   Gli ID VLAN non devono essere univoci. Ad esempio, è possibile utilizzare l'ID VLAN 200 per il traffico amministrativo in un sito e lo stesso ID VLAN per il traffico client in un altro sito. È possibile creare interfacce VLAN separate con diversi set di interfacce padre in ogni sito. Tuttavia, due interfacce VLAN con lo stesso ID non possono condividere la stessa interfaccia su un nodo. Se si specifica un ID già utilizzato, viene visualizzato un messaggio.

2. Facoltativamente, inserire una breve descrizione per l'interfaccia VLAN.
3. Selezionare **continua**.

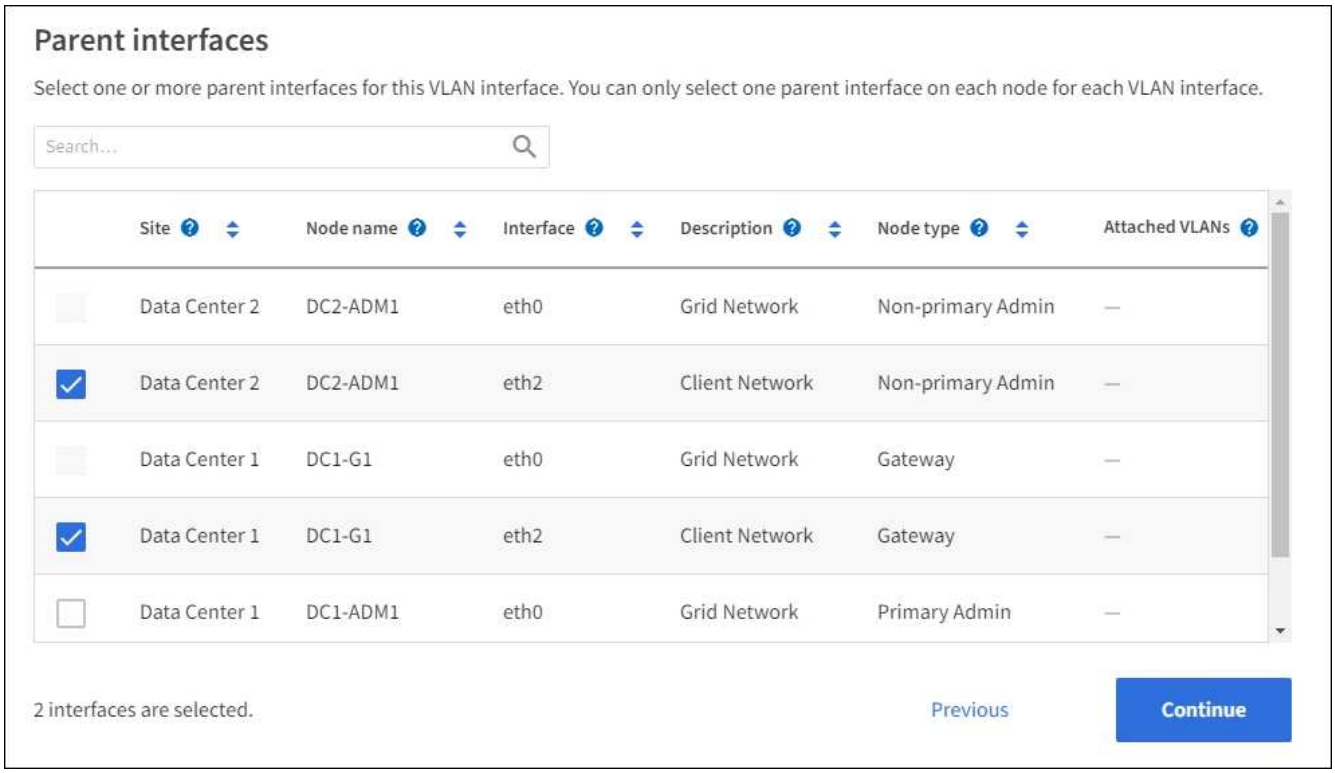
Scegliere le interfacce padre

La tabella elenca le interfacce disponibili per tutti i nodi Admin e Gateway in ogni sito della griglia. Le interfacce Admin Network (eth1) non possono essere utilizzate come interfacce padre e non vengono visualizzate.

Fasi

1. Selezionare una o più interfacce padre a cui collegare questa VLAN.

   Ad esempio, è possibile collegare una VLAN all'interfaccia di rete client (eth2) per un nodo gateway e un nodo amministratore.



2. Selezionare **continua**.

Confermare le impostazioni

Fasi

1. Esaminare la configurazione e apportare eventuali modifiche.
   - Se è necessario modificare l'ID o la descrizione della VLAN, selezionare **Enter VLAN details** (Inserisci dettagli VLAN) nella parte superiore della pagina.
   - Per modificare un'interfaccia padre, selezionare **Choose parent interfaces** (Scegli interfacce padre) nella parte superiore della pagina oppure selezionare **Previous** (precedente).
   - Se è necessario rimuovere un'interfaccia padre, selezionare il cestino .
2. Selezionare **Salva**.
3. Attendere fino a 5 minuti che la nuova interfaccia venga visualizzata come selezione nella pagina High Availability groups (gruppi ad alta disponibilità) e sia elencata nella tabella **Network interfaces** (interfacce

di rete) per il nodo (**NODES** > ***parent interface node*** > **Network**).

Modificare un'interfaccia VLAN

Quando si modifica un'interfaccia VLAN, è possibile apportare i seguenti tipi di modifiche:

- Modificare l'ID o la descrizione della VLAN.
- Aggiungere o rimuovere interfacce padre.

Ad esempio, se si intende decommissionare il nodo associato, è possibile rimuovere un'interfaccia principale da un'interfaccia VLAN.

Tenere presente quanto segue:

- Non è possibile modificare un ID VLAN se l'interfaccia VLAN viene utilizzata in un gruppo ha.
- Non è possibile rimuovere un'interfaccia padre se tale interfaccia padre è utilizzata in un gruppo ha.

  Ad esempio, si supponga che la VLAN 200 sia collegata alle interfacce padre sui nodi A e B. Se un gruppo ha utilizza l'interfaccia VLAN 200 per il nodo A e l'interfaccia eth2 per il nodo B, è possibile rimuovere l'interfaccia padre non utilizzata per il nodo B, ma non è possibile rimuovere l'interfaccia padre utilizzata per il nodo A.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selezionare la casella di controllo dell'interfaccia VLAN che si desidera modificare. Quindi, selezionare **azioni** > **Modifica**.
3. Facoltativamente, aggiornare l'ID VLAN o la descrizione. Quindi, selezionare **continua**.

   Non è possibile aggiornare un ID VLAN se la VLAN viene utilizzata in un gruppo ha.

4. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere interfacce padre o per rimuovere interfacce inutilizzate. Quindi, selezionare **continua**.
5. Esaminare la configurazione e apportare eventuali modifiche.
6. Selezionare **Salva**.

Rimuovere un'interfaccia VLAN

È possibile rimuovere una o più interfacce VLAN.

Non è possibile rimuovere un'interfaccia VLAN se è attualmente utilizzata in un gruppo ha. È necessario rimuovere l'interfaccia VLAN dal gruppo ha prima di poterla rimuovere.

Per evitare interruzioni del traffico client, è consigliabile eseguire una delle seguenti operazioni:

- Aggiungere una nuova interfaccia VLAN al gruppo ha prima di rimuovere questa interfaccia VLAN.
- Creare un nuovo gruppo ha che non utilizzi questa interfaccia VLAN.
- Se l'interfaccia VLAN che si desidera rimuovere è attualmente attiva, modificare il gruppo ha. Spostare l'interfaccia VLAN che si desidera rimuovere in fondo all'elenco delle priorità. Attendere che la comunicazione venga stabilita sulla nuova interfaccia principale, quindi rimuovere la vecchia interfaccia dal gruppo ha. Infine, eliminare l'interfaccia VLAN su quel nodo.

Fasi

1. Selezionare **CONFIGURATION** > **Network** > **VLAN interfaces**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, selezionare **azioni** > **Elimina**.
3. Selezionare **Sì** per confermare la selezione.

   Tutte le interfacce VLAN selezionate vengono rimosse. Nella pagina delle interfacce VLAN viene visualizzato un banner verde di successo.

Gestire le policy di classificazione del traffico

Gestire le policy di classificazione del traffico: Panoramica

Per migliorare la qualità del servizio (QoS), è possibile creare policy di classificazione del traffico per identificare e monitorare diversi tipi di traffico di rete. Queste policy possono essere utili per la limitazione e il monitoraggio del traffico.

I criteri di classificazione del traffico vengono applicati agli endpoint del servizio bilanciamento del carico StorageGRID per i nodi gateway e i nodi di amministrazione. Per creare criteri di classificazione del traffico, è necessario aver già creato endpoint di bilanciamento del carico.

Regole corrispondenti

Ogni policy di classificazione del traffico contiene una o più regole corrispondenti per identificare il traffico di rete correlato a una o più delle seguenti entità:

- Bucket
- Subnet
- Tenant
- Endpoint del bilanciamento del carico

StorageGRID monitora il traffico che corrisponde a qualsiasi regola all'interno del criterio in base agli obiettivi della regola. Qualsiasi traffico corrispondente a qualsiasi regola di un criterio viene gestito da tale criterio. Al contrario, è possibile impostare le regole in modo che corrispondano a tutto il traffico ad eccezione di un'entità specificata.

Limitazione del traffico

In alternativa, è possibile aggiungere i seguenti tipi di limite a un criterio:

- Larghezza di banda aggregata
- Larghezza di banda per richiesta
- Richieste simultanee
- Tasso di richiesta

I valori limite vengono applicati in base al bilanciamento del carico. Se il traffico viene distribuito simultaneamente tra più bilanciatori di carico, i tassi massimi totali sono un multiplo dei limiti di velocità specificati.

È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato.

Per i limiti di larghezza di banda aggregati o per richiesta, le richieste vengono trasmesse in streaming alla velocità impostata. StorageGRID può applicare una sola velocità, quindi la corrispondenza di policy più specifica, in base al tipo di matcher, è quella applicata. La larghezza di banda consumata dalla richiesta non viene contata rispetto ad altre policy di corrispondenza meno specifiche contenenti policy di limite della larghezza di banda aggregate. Per tutti gli altri tipi di limite, le richieste client vengono ritardate di 250 millisecondi e ricevono una risposta lenta di 503 per le richieste che superano qualsiasi limite di policy corrispondente.

In Grid Manager, è possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Utilizzare i criteri di classificazione del traffico con gli SLA

È possibile utilizzare le policy di classificazione del traffico insieme ai limiti di capacità e alla protezione dei dati per applicare gli SLA (Service-Level Agreement) che forniscono specifiche per capacità, protezione dei dati e performance.

Nell'esempio riportato di seguito vengono illustrati tre livelli di uno SLA. È possibile creare criteri di classificazione del traffico per raggiungere gli obiettivi di performance di ciascun livello SLA.

Livello di servizio	Capacità	Protezione dei dati	Massime performance consentite	Costo
Oro	1 PB di storage consentito	3 copia regola ILM	25 K richieste/sec 5 GB/sec (40 Gbps) di larghezza di banda	€ al mese
Argento	250 TB di storage consentiti	2 copia regola ILM	10 richieste K/sec Larghezza di banda di 1.25 GB/sec (10 Gbps)	dollari al mese
Bronzo	100 TB di storage consentito	2 copia regola ILM	5 richieste K/sec 1 GB/sec (8 Gbps) di larghezza di banda	dollari al mese

Creare policy di classificazione del traffico

È possibile creare policy di classificazione del traffico se si desidera monitorare e, facoltativamente, limitare il traffico di rete per bucket, bucket regex, CIDR, endpoint del bilanciamento del carico o tenant. Facoltativamente, è possibile impostare limiti per una

policy in base alla larghezza di banda, al numero di richieste simultanee o alla velocità di richiesta.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Sono stati creati endpoint di bilanciamento del carico che si desidera associare.
- Hai creato i tenant che desideri abbinare.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.
2. Selezionare **Crea**.
3. Inserire un nome e una descrizione (opzionale) per la policy e selezionare **continua**.

   Ad esempio, descrivi a cosa si applica questa policy di classificazione del traffico e a cosa limiterà.

4. Selezionare **Aggiungi regola** e specificare i seguenti dettagli per creare una o più regole corrispondenti per il criterio. I criteri creati devono avere almeno una regola corrispondente. Selezionare **continua**.

Campo	Descrizione
Tipo	Selezionare i tipi di traffico a cui si applica la regola corrispondente. I tipi di traffico sono bucket, bucket regex, CIDR, endpoint del bilanciamento del carico e tenant.
Valore corrispondente	Inserire il valore corrispondente al tipo selezionato. • Bucket: Immettere uno o più nomi di bucket. • Secchio regex: Immettere una o più espressioni regolari utilizzate per far corrispondere un insieme di nomi di bucket. L'espressione regolare non è ancorata. USA l'ancora ^ per trovare la corrispondenza all'inizio del nome del bucket e usa l'ancora per la corrispondenza alla fine del nome. La corrispondenza delle espressioni regolari supporta un sottoinsieme della sintassi PCRE (Perl Compatible Regular Expression). • CIDR: Inserire una o più subnet IPv4, nella notazione CIDR, che corrispondono alla subnet desiderata. • Endpoint del bilanciamento del carico: Selezionare il nome di un endpoint. Questi sono gli endpoint del bilanciamento del carico definiti in "Configurare gli endpoint del bilanciamento del carico". • Tenant: Il tenant matching utilizza l'ID della chiave di accesso. Se la richiesta non contiene un ID della chiave di accesso (ad esempio, l'accesso anonimo), viene utilizzata la proprietà del bucket a cui si accede per determinare il tenant.

Campo	Descrizione
Corrispondenza inversa	Se si desidera far corrispondere tutto il traffico di rete *tranne* coerente con il valore Type and Match appena definito, selezionare la casella di controllo **Inverse Match** (corrispondenza inversa). In caso contrario, lasciare deselezionata la casella di controllo. Ad esempio, se si desidera applicare questo criterio a tutti gli endpoint del bilanciamento del carico tranne uno, specificare l'endpoint del bilanciamento del carico da escludere e selezionare **corrispondenza inversa**. Per un criterio contenente più adattatori in cui almeno uno è un adattatore inverso, fare attenzione a non creare un criterio che corrisponda a tutte le richieste.

5. Facoltativamente, selezionare **Aggiungi un limite** e selezionare i seguenti dettagli per aggiungere uno o più limiti per controllare il traffico di rete associato a una regola.

> StorageGRID raccoglie le metriche anche se non si aggiungono limiti, in modo da poter comprendere le tendenze del traffico.

Campo	Descrizione
Tipo	Il tipo di limite che si desidera applicare al traffico di rete associato alla regola. Ad esempio, è possibile limitare la larghezza di banda o il tasso di richiesta. **Nota**: È possibile creare policy per limitare la larghezza di banda aggregata o per limitare la larghezza di banda per richiesta. Tuttavia, StorageGRID non può limitare entrambi i tipi di larghezza di banda contemporaneamente. Quando la larghezza di banda aggregata è in uso, la larghezza di banda per richiesta non è disponibile. Al contrario, quando viene utilizzata la larghezza di banda per richiesta, la larghezza di banda aggregata non è disponibile. I limiti di larghezza di banda aggregati potrebbero imporre un ulteriore impatto minore sulle performance sul traffico non limitato. Per i limiti di larghezza di banda, StorageGRID applica la policy che meglio corrisponde al tipo di limite impostato. Ad esempio, se si dispone di una policy che limita il traffico in una sola direzione, il traffico nella direzione opposta sarà illimitato, anche se il traffico corrisponde a criteri aggiuntivi con limiti di larghezza di banda. StorageGRID implementa le corrispondenze "migliori" per i limiti di larghezza di banda nel seguente ordine: • Indirizzo IP esatto (/32 mask) • Nome esatto del bucket • Regex. Bucket • Tenant • Endpoint • Corrispondenze CIDR non esatte (non /32) • Corrispondenze inverse

Campo	Descrizione
Valido per	Se questo limite si applica alle richieste di lettura del client (GET o HEAD) o alle richieste di scrittura (PUT, POST o DELETE).
Valore	Il valore a cui il traffico di rete sarà limitato, in base all'unità selezionata. Ad esempio, immettere 10 e selezionare MiB/s per impedire che il traffico di rete associato a questa regola superi i 10 MiB/s. **Nota**: A seconda dell'impostazione delle unità, le unità disponibili saranno binarie (ad esempio, GiB) o decimali (ad esempio, GB). Per modificare l'impostazione delle unità, selezionare l'elenco a discesa User (utente) in alto a destra in Grid Manager, quindi selezionare **User Preferences** (Preferenze utente).
Unità	L'unità che descrive il valore immesso.

Ad esempio, se si desidera creare un limite di larghezza di banda di 40 GB/s per un livello SLA, creare due limiti di larghezza di banda aggregati: GET/HEAD a 40 GB/s e PUT/POST/DELETE a 40 GB/s.

6. Selezionare **continua**.
7. Leggere e rivedere la policy di classificazione del traffico. Utilizzare il pulsante **precedente** per tornare indietro e apportare le modifiche necessarie. Quando si è soddisfatti della policy, selezionare **Salva e continua**.

   Il traffico dei client S3 e Swift viene ora gestito in base alla policy di classificazione del traffico.

Al termine

"Visualizzare le metriche del traffico di rete" per verificare che i criteri stiano applicando i limiti di traffico previsti.

Modificare la policy di classificazione del traffico

È possibile modificare un criterio di classificazione del traffico per modificarne il nome o la descrizione oppure per creare, modificare o eliminare eventuali regole o limiti per il criterio.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti vengono elencati in una tabella.

2. Modificare il criterio utilizzando il menu azioni o la pagina dei dettagli. Vedere "creare policy di classificazione del traffico" per cosa partecipare.

Menu delle azioni

a. Selezionare la casella di controllo per la policy.

b. Selezionare **azioni** > **Modifica**.

Pagina dei dettagli

a. Selezionare il nome del criterio.

b. Selezionare il pulsante **Edit** (Modifica) accanto al nome del criterio.

3. Per il passo inserire il nome del criterio, modificare facoltativamente il nome o la descrizione del criterio e selezionare **continua**.
4. Per il passo Add Matching rules (Aggiungi regole di corrispondenza), aggiungere una regola o modificare **Type** e **Match value** della regola esistente, quindi selezionare **Continue** (continua).
5. Per la fase Set Limits (Imposta limiti), aggiungere, modificare o eliminare un limite e selezionare **Continue** (continua).
6. Esaminare la policy aggiornata e selezionare **Salva e continua**.

   Le modifiche apportate alla policy vengono salvate e il traffico di rete viene gestito in base alle policy di classificazione del traffico. È possibile visualizzare i diagrammi di traffico e verificare che i criteri stiano applicando i limiti di traffico previsti.

Eliminare una policy di classificazione del traffico

È possibile eliminare una policy di classificazione del traffico se non è più necessaria. Assicurarsi di eliminare la policy corretta perché non è possibile recuperare una policy quando viene eliminata.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico con i criteri esistenti elencati in una tabella.

2. Eliminare il criterio utilizzando il menu azioni o la pagina dei dettagli.

Menu delle azioni

a. Selezionare la casella di controllo per la policy.

b. Selezionare **azioni** > **Rimuovi**.

Pagina dei dettagli della policy

a. Selezionare il nome del criterio.

b. Selezionare il pulsante **Remove** accanto al nome del criterio.

3. Selezionare **Sì** per confermare che si desidera eliminare il criterio.

   La policy viene eliminata.

Visualizzare le metriche del traffico di rete

È possibile monitorare il traffico di rete visualizzando i grafici disponibili nella pagina Criteri di classificazione del traffico.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Accesso root o autorizzazione account tenant".

A proposito di questa attività

Per qualsiasi criterio di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio di bilanciamento del carico per determinare se il criterio limita correttamente il traffico nella rete. I dati nei grafici possono aiutare a determinare se è necessario modificare la policy.

Anche se non vengono impostati limiti per una policy di classificazione del traffico, vengono raccolte le metriche e i grafici forniscono informazioni utili per comprendere le tendenze del traffico.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico e i criteri esistenti vengono elencati nella tabella.

2. Selezionare il nome del criterio di classificazione del traffico per il quale si desidera visualizzare le metriche.
3. Selezionare la scheda **metriche**.

   Vengono visualizzati i grafici dei criteri di classificazione del traffico. I grafici visualizzano le metriche solo per il traffico corrispondente al criterio selezionato.

   I grafici riportati di seguito sono inclusi nella pagina.

   - Tasso di richiesta: Questo grafico fornisce la quantità di larghezza di banda corrispondente a questa policy gestita da tutti i bilanciatori di carico. I dati ricevuti includono intestazioni di richiesta per tutte le richieste e dimensioni dei dati del corpo per le risposte che hanno dati del corpo. Inviato include le intestazioni delle risposte per tutte le richieste e le dimensioni dei dati del corpo delle risposte per le richieste che includono i dati del corpo nella risposta.

     > Quando le richieste sono complete, questo grafico mostra solo l'utilizzo della larghezza di banda. Per le richieste di oggetti lenti o di grandi dimensioni, la larghezza di banda istantanea effettiva potrebbe differire dai valori riportati in questo grafico.

   - Tasso di risposta agli errori: Questo grafico fornisce una velocità approssimativa alla quale le richieste corrispondenti a questa policy restituiscono errori (codice di stato HTTP >= 400) ai client.
   - Durata media della richiesta (non errore): Questo grafico fornisce una durata media delle richieste riuscite corrispondenti a questa policy.
   - Utilizzo della larghezza di banda della policy: Questo grafico fornisce la quantità di larghezza di banda

corrispondente a questa policy gestita da tutti i bilanciatori di carico. I dati ricevuti includono intestazioni di richiesta per tutte le richieste e dimensioni dei dati del corpo per le risposte che hanno dati del corpo. Inviato include le intestazioni delle risposte per tutte le richieste e le dimensioni dei dati del corpo delle risposte per le richieste che includono i dati del corpo nella risposta.

4. Posizionare il cursore su un grafico a linee per visualizzare una finestra a comparsa di valori su una parte specifica del grafico.
5. Selezionare **Grafana dashboard** sotto il titolo metriche per visualizzare tutti i grafici di una policy. Oltre ai quattro grafici della scheda **metriche**, è possibile visualizzare altri due grafici:
   - Write request rate by object size (tasso di richiesta di scrittura per dimensione oggetto): Tasso di richieste PUT/POST/DELETE corrispondenti a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le velocità mostrate nella vista con il passaggio del mouse sono troncate in conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
   - Read request rate by object size (tasso richiesta di lettura per dimensione oggetto): Il tasso per le richieste GET/HEAD corrispondenti a questa policy. Il posizionamento su una singola cella mostra le velocità al secondo. Le velocità mostrate nella vista con il passaggio del mouse sono troncate in conteggi interi e potrebbero riportare 0 quando nel bucket sono presenti richieste diverse da zero.
6. In alternativa, accedere ai grafici dal menu **SUPPORT**.
   a. Selezionare **SUPPORT** > **Tools** > **Metrics**.
   b. Selezionare **Traffic Classification Policy** dalla sezione **Grafana**.
   c. Selezionare il criterio dal menu in alto a sinistra della pagina.
   d. Posizionare il cursore su un grafico per visualizzare una finestra a comparsa che mostra la data e l'ora del campione, le dimensioni degli oggetti aggregati nel conteggio e il numero di richieste al secondo durante tale periodo di tempo.

      Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID delle policy sono elencati nella pagina delle policy di classificazione del traffico.
7. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Crittografia supportata per le connessioni TLS in uscita

Il sistema StorageGRID supporta un set limitato di suite di crittografia per le connessioni TLS (Transport Layer Security) ai sistemi esterni utilizzati per la federazione di identità e i pool di storage cloud.

Versioni supportate di TLS

StorageGRID supporta TLS 1.2 e TLS 1.3 per le connessioni a sistemi esterni utilizzati per la federazione delle identità e i pool di storage cloud.

I cifrari TLS supportati per l'utilizzo con sistemi esterni sono stati selezionati per garantire la compatibilità con una vasta gamma di sistemi esterni. L'elenco è più grande dell'elenco di cifrature supportate per l'utilizzo con le applicazioni client S3 o Swift. Per configurare le crittografia, andare a **CONFIGURATION** > **Security** > **Security settings** e selezionare **TLS and SSH policy**.

Le opzioni di configurazione TLS, come versioni di protocollo, crittografia, algoritmi di scambio delle chiavi e algoritmi MAC, non sono configurabili in StorageGRID. Se hai richieste specifiche su queste impostazioni, contatta il tuo rappresentante NetApp.

Vantaggi delle connessioni HTTP attive, inattive e simultanee

La modalità di configurazione delle connessioni HTTP può influire sulle prestazioni del sistema StorageGRID. Le configurazioni variano a seconda che la connessione HTTP sia attiva o inattiva o che si dispongano di più connessioni simultanee.

È possibile identificare i vantaggi in termini di prestazioni per i seguenti tipi di connessioni HTTP:

- Connessioni HTTP inattive
- Connessioni HTTP attive
- Connessioni HTTP simultanee

I vantaggi di mantenere aperte le connessioni HTTP inattive

È necessario mantenere aperte le connessioni HTTP anche quando le applicazioni client sono inattive per consentire alle applicazioni client di eseguire transazioni successive sulla connessione aperta. In base alle misurazioni del sistema e all'esperienza di integrazione, è necessario mantenere aperta una connessione HTTP inattiva per un massimo di 10 minuti. StorageGRID potrebbe chiudere automaticamente una connessione HTTP che rimane aperta e inattiva per più di 10 minuti.

Le connessioni HTTP aperte e inattive offrono i seguenti vantaggi:

- Latenza ridotta dal momento in cui il sistema StorageGRID stabilisce di eseguire una transazione HTTP al momento in cui il sistema StorageGRID può eseguire la transazione

  La latenza ridotta è il vantaggio principale, in particolare per il tempo necessario per stabilire connessioni TCP/IP e TLS.

- Aumento della velocità di trasferimento dei dati mediante l'attivazione dell'algoritmo di avvio lento TCP/IP con i trasferimenti eseguiti in precedenza
- Notifica istantanea di diverse classi di condizioni di errore che interrompono la connettività tra l'applicazione client e il sistema StorageGRID

Determinare per quanto tempo mantenere aperta una connessione inattiva è un compromesso tra i benefici dell'avvio lento associati alla connessione esistente e l'allocazione ideale della connessione alle risorse di sistema interne.

Vantaggi delle connessioni HTTP attive

Per le connessioni dirette ai nodi di storage, è necessario limitare la durata di una connessione HTTP attiva a un massimo di 10 minuti, anche se la connessione HTTP esegue continuamente transazioni.

La determinazione della durata massima per cui una connessione deve essere mantenuta aperta è un compromesso tra i benefici della persistenza della connessione e l'allocazione ideale della connessione alle risorse di sistema interne.

Per le connessioni client ai nodi di storage, la limitazione delle connessioni HTTP attive offre i seguenti vantaggi:

- Consente un bilanciamento ottimale del carico nel sistema StorageGRID.

  Con il passare del tempo, una connessione HTTP potrebbe non essere più ottimale con il variare dei requisiti di bilanciamento del carico. Il sistema esegue il miglior bilanciamento del carico quando le applicazioni client stabiliscono una connessione HTTP separata per ciascuna transazione, ma questo nega i guadagni molto più preziosi associati alle connessioni persistenti.

- Consente alle applicazioni client di indirizzare le transazioni HTTP ai servizi LDR che dispongono di spazio disponibile.
- Consente l'avvio delle procedure di manutenzione.

  Alcune procedure di manutenzione vengono avviate solo dopo il completamento di tutte le connessioni HTTP in corso.

Per le connessioni client al servizio Load Balancer, la limitazione della durata delle connessioni aperte può essere utile per consentire l'avvio tempestivo di alcune procedure di manutenzione. Se la durata delle connessioni client non è limitata, potrebbero essere necessari alcuni minuti per terminare automaticamente le connessioni attive.

Vantaggi delle connessioni HTTP simultanee

Tenere aperte più connessioni TCP/IP al sistema StorageGRID per consentire il parallelismo, aumentando così le performance. Il numero ottimale di connessioni parallele dipende da diversi fattori.

Le connessioni HTTP simultanee offrono i seguenti vantaggi:

- Latenza ridotta

  Le transazioni possono iniziare immediatamente invece di attendere il completamento di altre transazioni.

- Maggiore throughput

  Il sistema StorageGRID può eseguire transazioni parallele e aumentare il throughput delle transazioni aggregate.

Le applicazioni client devono stabilire più connessioni HTTP. Quando un'applicazione client deve eseguire una transazione, può selezionare e utilizzare immediatamente qualsiasi connessione stabilita che non sta elaborando una transazione.

La topologia di ciascun sistema StorageGRID presenta un throughput di picco diverso per le transazioni e le connessioni simultanee prima che le performance comincino a degradarsi. Il throughput massimo dipende da fattori quali risorse di calcolo, risorse di rete, risorse di storage e collegamenti WAN. Anche il numero di server e servizi e il numero di applicazioni supportate dal sistema StorageGRID sono fattori.

I sistemi StorageGRID spesso supportano più applicazioni client. Tenere presente questo aspetto quando si determina il numero massimo di connessioni simultanee utilizzate da un'applicazione client. Se l'applicazione client è costituita da più entità software che stabiliscono connessioni al sistema StorageGRID, è necessario sommare tutte le connessioni tra le entità. Potrebbe essere necessario regolare il numero massimo di connessioni simultanee nelle seguenti situazioni:

- La topologia del sistema StorageGRID influisce sul numero massimo di transazioni e connessioni simultanee supportate dal sistema.
- Le applicazioni client che interagiscono con il sistema StorageGRID su una rete con larghezza di banda

limitata potrebbero dover ridurre il grado di concorrenza per garantire che le singole transazioni vengano completate in un tempo ragionevole.

- Quando molte applicazioni client condividono il sistema StorageGRID, potrebbe essere necessario ridurre il grado di concorrenza per evitare di superare i limiti del sistema.

Separazione dei pool di connessione HTTP per le operazioni di lettura e scrittura

È possibile utilizzare pool separati di connessioni HTTP per le operazioni di lettura e scrittura e controllare la quantità di un pool da utilizzare per ciascuno di essi. I pool separati di connessioni HTTP consentono di controllare meglio le transazioni e bilanciare i carichi.

Le applicazioni client possono creare carichi dominanti dal recupero (lettura) o dominanti dal negozio (scrittura). Con pool separati di connessioni HTTP per le transazioni di lettura e scrittura, è possibile regolare la quantità di ciascun pool da dedicare alle transazioni di lettura o scrittura.

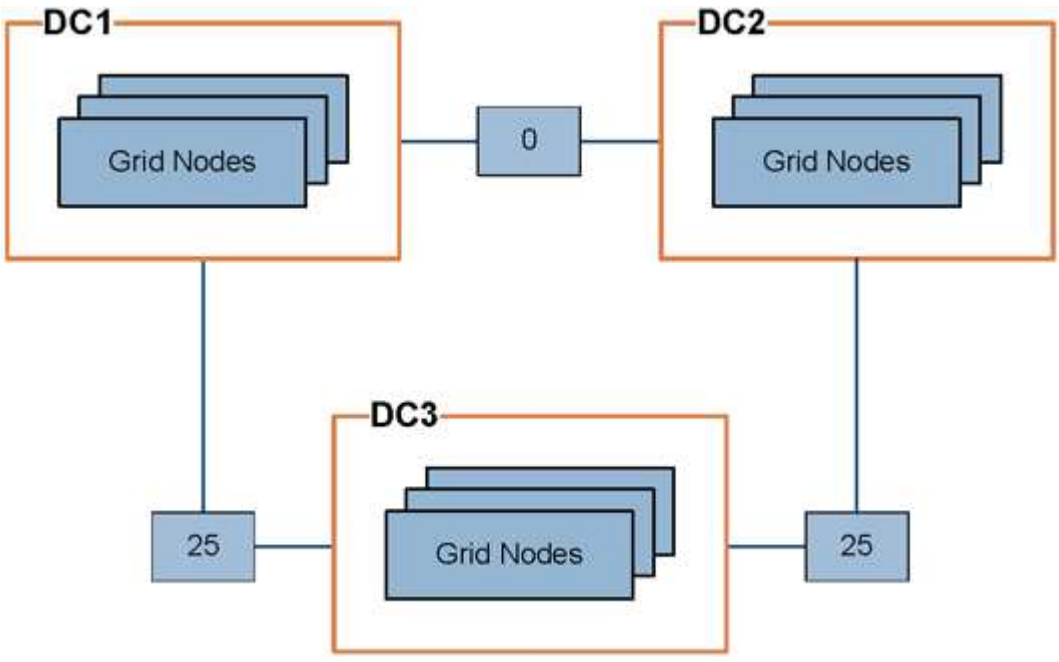
Gestire i costi di collegamento

I costi di collegamento consentono di assegnare la priorità al sito del data center che fornisce un servizio richiesto quando esistono due o più siti del data center. È possibile regolare i costi di collegamento in modo da riflettere la latenza tra i siti.

Quali sono i costi di collegamento?

- I costi di collegamento vengono utilizzati per assegnare la priorità alla copia oggetto utilizzata per soddisfare i recuperi di oggetti.
- I costi di collegamento vengono utilizzati dall'API di gestione del grid e dall'API di gestione del tenant per determinare i servizi StorageGRID interni da utilizzare.
- I costi di collegamento vengono utilizzati dal servizio Load Balancer sui nodi Admin e sui nodi Gateway per indirizzare le connessioni client. Vedere "Considerazioni per il bilanciamento del carico".

Il diagramma mostra una griglia a tre siti con costi di collegamento configurati tra i siti:



- Il servizio Load Balancer sui nodi Admin e Gateway distribuisce in modo uguale le connessioni client a tutti i nodi Storage nello stesso sito del data center e a qualsiasi sito del data center con un costo di collegamento pari a 0.

  Nell'esempio, un nodo gateway nel sito 1 del data center (DC1) distribuisce in modo uguale le connessioni client ai nodi di storage in DC1 e ai nodi di storage in DC2. Un nodo gateway in DC3 invia le connessioni client solo ai nodi di storage in DC3.

- Quando si recupera un oggetto che esiste come copie replicate multiple, StorageGRID recupera la copia nel data center che ha il costo di collegamento più basso.

  Nell'esempio, se un'applicazione client in DC2 recupera un oggetto memorizzato sia in DC1 che in DC3, l'oggetto viene recuperato da DC1, poiché il costo di collegamento da DC1 a DC2 è 0, che è inferiore al costo di collegamento da DC3 a DC2 (25).

I costi di collegamento sono numeri relativi arbitrari senza unità di misura specifica. Ad esempio, un costo di collegamento di 50 viene utilizzato in modo meno preferenziale rispetto a un costo di collegamento di 25. La tabella mostra i costi di collegamento comunemente utilizzati.

Collegamento	Costo del collegamento	Note
Tra siti fisici di data center	25 (impostazione predefinita)	Data center connessi tramite un collegamento WAN.
Tra i siti del data center logico nella stessa posizione fisica	0	Data center logici nello stesso edificio fisico o campus connessi da una LAN.

Aggiornare i costi dei collegamenti

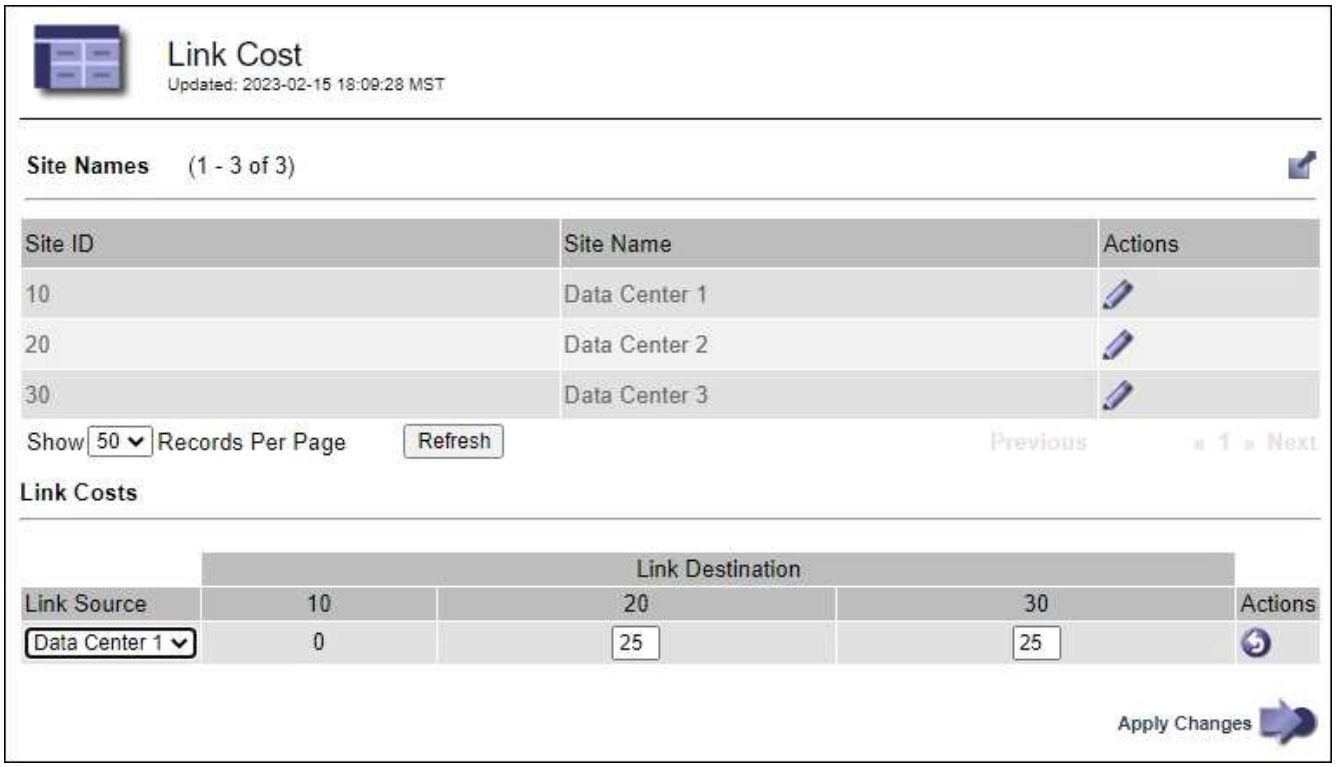
È possibile aggiornare i costi di collegamento tra i siti del data center per riflettere la latenza tra i siti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di configurazione della pagina della topologia della griglia".

Fasi

1. Selezionare **SUPPORTO** > **Altro** > **costo collegamento**.



2. Selezionare un sito in **link Source** (origine collegamento) e immettere un valore di costo compreso tra 0 e 100 in **link Destination** (destinazione collegamento).

   Non puoi modificare il costo del collegamento se l'origine è la stessa della destinazione.

   Per annullare le modifiche, selezionare **Ripristina**.

3. Selezionare **Applica modifiche**.

USA AutoSupport

Use AutoSupport: Panoramica

La funzione AutoSupport consente a StorageGRID di inviare pacchetti di stato e integrità al supporto tecnico NetApp.

L'utilizzo di AutoSupport può accelerare notevolmente la determinazione e la risoluzione dei problemi. Il supporto tecnico può anche monitorare le esigenze di storage del sistema e aiutare a determinare se è necessario aggiungere nuovi nodi o siti. In alternativa, è possibile configurare i pacchetti AutoSupport da inviare a una destinazione aggiuntiva.

StorageGRID dispone di due tipi di AutoSupport:

StorageGRID AutoSupport

Segnala problemi relativi al software StorageGRID. Attivato per impostazione predefinita quando si installa StorageGRID per la prima volta. È possibile "Modificare la configurazione AutoSupport predefinita" se necessario.

Se StorageGRID AutoSupport non è abilitato, viene visualizzato un messaggio sul dashboard di Gestione griglia. Il messaggio include un collegamento alla pagina di configurazione di AutoSupport. Se si chiude il messaggio, questo non viene visualizzato fino a quando la cache del browser non viene cancellata, anche se AutoSupport rimane disattivato.

AutoSupport dell'hardware di appliance

Segnala problemi relativi all'appliance StorageGRID. È necessario "Configura AutoSupport hardware su ogni appliance".

Che cos'è Active IQ?

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

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

"Documentazione di Active IQ Digital Advisor"

Informazioni incluse nel pacchetto AutoSupport

Un pacchetto AutoSupport contiene i seguenti file XML e dettagli.

Nome del file	Campi	Descrizione
AUTOSUPPORT-HISTORY.XML	Numero di sequenza AutoSupport Destinazione per questo AutoSupport Evento trigger Stato di consegna Tentativi di consegna Oggetto AutoSupport URI di consegna Ultimo errore AutoSupport INSERISCI nome file Ora di generazione Dimensione compressa AutoSupport Dimensioni decompresse AutoSupport Tempo totale di raccolta (ms)	File di cronologia AutoSupport.

Nome del file	Campi	Descrizione
AUTOSUPPORT.XML	Nodo Protocollo per contattare il supporto URL di supporto per HTTP/HTTPS Indirizzo di assistenza Stato OnDemand AutoSupport URL server OnDemand AutoSupport Intervallo di polling su richiesta AutoSupport	File di stato AutoSupport. Fornisce i dettagli del protocollo utilizzato, dell'URL e dell'indirizzo del supporto tecnico, dell'intervallo di polling e di OnDemand AutoSupport, se attivato o disattivato.
BUCKET.XML	ID benna ID account Versione build Configurazione vincolo posizione Conformità abilitata Configurazione conformità Blocco oggetto S3 abilitato S3 Configurazione blocco oggetto Configurazione di coerenza CORS abilitato Configurazione CORS Ora ultimo accesso attivata Criterio attivato Configurazione dei criteri Notifiche attivate Configurazione notifiche Cloud Mirror abilitato Configurazione del mirror cloud Ricerca abilitata Cerca configurazione Accesso rapido ACL di lettura attivato Configurazione ACL lettura rapida Swift Write ACL attivato Configurazione Swift Write ACL Etichettatura bucket abilitata Configurazione etichettatura bucket Configurazione delle versioni	Fornisce dettagli di configurazione e statistiche a livello di bucket. Esempi di configurazioni bucket includono servizi di piattaforma, conformità e coerenza dei bucket.

Nome del file	Campi	Descrizione
GRID-CONFIGURATIONS.XML	ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di informazioni sulla configurazione a livello di griglia. Contiene informazioni sui certificati Grid, sullo spazio riservato ai metadati, sulle impostazioni di configurazione a livello di grid (compliance, blocco degli oggetti S3, compressione degli oggetti, avvisi, syslog, e configurazione ILM), dettagli del profilo di erasure coding, nome DNS, "Nome NMS"e molto altro ancora.
GRID-SPEC.XML	Specifiche della griglia, XML non elaborato	Utilizzato per la configurazione e la distribuzione di StorageGRID. Contiene le specifiche della griglia, l'IP del server NTP, l'IP del server DNS, la topologia di rete e i profili hardware dei nodi.
GRID-TASKS.XML	Nodo Percorso di assistenza ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di stato delle attività della griglia (procedure di manutenzione). Fornisce i dettagli delle attività attive, terminate, completate, non riuscite e in sospeso della griglia.
GRID.JSON	Griglia + Revisione + versione software + Descrizione + licenza + password + DNS + NTP + Siti + nodi	Informazioni sulla griglia.
ILM-CONFIGURATION.XML	ID attributo Nome attributo Valore Indice ID tabella Nome tabella	Elenco degli attributi per le configurazioni ILM.
ILM-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di informazioni sulle metriche ILM. Contiene le velocità di valutazione ILM per ogni nodo e le metriche a livello di grid.

Nome del file	Campi	Descrizione
ILM.XML	XML raw ILM	File di criteri ILM attivo. Contiene dettagli sulle policy ILM attive, come ID del pool di storage, comportamento di acquisizione, filtri, regole e descrizione. Contiene inoltre l'XML per il criterio ILM predefinito.
LOG.TGZ	*n/a*	File di registro scaricabile. Contiene `bycast-err.log` e. `servermanager.log` da ogni nodo.
MANIFEST.XML	Ordine di ritiro Nome file contenuto AutoSupport per questi dati Descrizione di questa voce di dati Numero di byte raccolti Tempo impiegato per la raccolta Stato di questa voce dati Descrizione dell'errore Tipo di contenuto AutoSupport per questi dati	Contiene metadati AutoSupport e brevi descrizioni di tutti i file XML AutoSupport.
NMS-ENTITIES.XML	Indice attributo Entità OID ID nodo ID modello dispositivo Versione del modello del dispositivo Nome entità	Raggruppa e service entities in "Albero NMS". Fornisce dettagli sulla topologia della griglia. Il nodo può essere determinato in base ai servizi in esecuzione sul nodo.
OBJECTS-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	Stato dell'oggetto, incluso lo stato della scansione in background, il trasferimento attivo, la velocità di trasferimento, i trasferimenti totali, la velocità di eliminazione, frammenti corrotti, oggetti smarriti, oggetti mancanti, tentativo di riparazione, velocità di scansione, periodo di scansione stimato, stato di completamento della riparazione e altro ancora.

Nome del file	Campi	Descrizione
SERVER-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di eventi e configurazioni del server. Contiene i seguenti dettagli per ogni nodo: Tipo di piattaforma, sistema operativo, memoria installata, memoria disponibile, connettività storage, numero di serie dello chassis dell'appliance di storage, numero di dischi guasti dello storage controller, temperatura dello chassis del controller di calcolo, hardware di calcolo, numero di serie del controller di calcolo, alimentatore, dimensioni dei dischi, tipo di disco e altro ancora.
SERVICE-STATUS.XML	Nodo Percorso di servizio ID attributo Nome attributo Valore Indice ID tabella Nome tabella	File di informazioni sul nodo di servizio. Contiene dettagli quali spazio allocato nella tabella, spazio libero nella tabella, metriche del piano d'esame del database, durata della riparazione dei segmenti, durata del processo di riparazione, riavvii automatici del processo, interruzione automatica del processo, e molto altro ancora.
STORAGE-GRADE.XML	ID grado archiviazione Nome grado storage ID nodo storage Percorso del nodo storage	File di definizioni di livello di archiviazione per ogni nodo di archiviazione.
SUMMARY-ATTRIBUTES.XML	OID gruppo Percorso gruppo ID attributo riepilogo Nome attributo riepilogo Valore Indice ID tabella Nome tabella	Dati di stato del sistema di alto livello che riassumono le informazioni sull'utilizzo di StorageGRID. Fornisce dettagli quali nome della griglia, nomi dei siti, numero di nodi storage per grid e per sito, tipo di licenza, capacità e utilizzo della licenza, termini di supporto software e dettagli sulle operazioni di S3 e Swift.
SYSTEM-ALARMS.XML	Nodo Percorso di servizio Gravità Attributo allarme Nome attributo Stato Valore Tempo di attivazione Conferma ora	Allarmi di livello di sistema (deprecati) e dati di stato utilizzati per indicare attività anomale o potenziali problemi.

Nome del file	Campi	Descrizione
SYSTEM-ALERTS.XML	Nome Gravità Nome del nodo Stato avviso Nome sito Tempo di attivazione allarme Tempo risoluzione avviso ID regola ID nodo ID sito Silenziato Altre annotazioni Altre etichette	Avvisi di sistema correnti che indicano potenziali problemi nel sistema StorageGRID.
USERAGENTS.XML	Agente utente Numero di giorni Richieste HTTP totali Byte totali acquisiti Byte totali recuperati INSERIRE le richieste Richiedi ELIMINA richieste Richieste HEAD INVIA richieste OPZIONI richieste Tempo medio richiesta (ms) Tempo medio di richiesta PUT (ms) Tempo medio di richiesta di RECUPERO (ms) Tempo medio di richiesta di ELIMINAZIONE (ms) Tempo medio di richiesta TESTINA (ms) Tempo medio POST-richiesta (ms) Tempo medio richiesta OPZIONI (ms)	Statistiche basate sugli agenti utente dell'applicazione. Ad esempio, il numero di operazioni PUT/GET/DELETE/HEAD per agente utente e la dimensione totale dei byte di ciascuna operazione.
X-HEADER-DATA	X-NetApp-asup-generated-on X-NetApp-asup-hostname X-NetApp-asup-os-version X-NetApp-asup-serial-num X-NetApp-asup-subject X-NetApp-asup-system-id X-NetApp-asup-model-name	Dati di intestazione AutoSupport.

Configurare AutoSupport

Per impostazione predefinita, la funzione StorageGRID AutoSupport è attivata quando si

installa StorageGRID per la prima volta. Tuttavia, è necessario configurare AutoSupport hardware su ogni appliance. Se necessario, è possibile modificare la configurazione di AutoSupport.

Se si desidera modificare la configurazione di StorageGRID AutoSupport, apportare le modifiche solo al nodo amministrativo primario. È necessario Configurare l'AutoSupport dell'hardware su ciascun apparecchio.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".
- Se si utilizza HTTPS per l'invio di pacchetti AutoSupport, è stato fornito l'accesso Internet in uscita al nodo amministrativo principale, direttamente o. "utilizzando un server proxy" (non sono richieste connessioni in entrata).
- Se nella pagina StorageGRID AutoSupport è selezionato HTTP, è stato configurato un server proxy per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiuteranno i pacchetti inviati utilizzando il protocollo HTTP.

  "Informazioni sulla configurazione delle impostazioni proxy dell'amministratore".

- Se si utilizza SMTP come protocollo per i pacchetti AutoSupport, è stato configurato un server di posta SMTP. La stessa configurazione del server di posta viene utilizzata per le notifiche e-mail di allarme (sistema legacy).

A proposito di questa attività

È possibile utilizzare qualsiasi combinazione delle seguenti opzioni per inviare i pacchetti AutoSupport al supporto tecnico:

- **Settimanale**: Invia automaticamente i pacchetti AutoSupport una volta alla settimana. Impostazione predefinita: Enabled (attivato).
- **Evento attivato**: Invia automaticamente pacchetti AutoSupport ogni ora o quando si verificano eventi di sistema significativi. Impostazione predefinita: Enabled (attivato).
- **Su richiesta**: Consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente i pacchetti AutoSupport, il che è utile quando stanno lavorando attivamente a un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disattivata.
- **Attivato dall'utente**: Inviare manualmente i pacchetti AutoSupport in qualsiasi momento.

specifica il protocollo per i pacchetti AutoSupport

È possibile utilizzare uno dei seguenti protocolli per l'invio di pacchetti AutoSupport:

- **HTTPS**: Impostazione predefinita e consigliata per le nuove installazioni. Questo protocollo utilizza la porta 443. Se lo si desidera Attivare la funzione AutoSupport on Demand, È necessario utilizzare HTTPS.
- **HTTP**: Se si seleziona HTTP, è necessario configurare un server proxy per inoltrare i pacchetti AutoSupport come HTTPS. I server AutoSupport di NetApp rifiutano i pacchetti inviati mediante HTTP. Questo protocollo utilizza la porta 80.
- **SMTP**: Utilizzare questa opzione se si desidera che i pacchetti AutoSupport vengano inviati tramite e-mail. Se si utilizza SMTP come protocollo per i pacchetti AutoSupport, è necessario configurare un server di posta SMTP nella pagina di configurazione della posta elettronica precedente (**SUPPORT** > **Allarmi (legacy)** > **impostazione della posta elettronica precedente**).

Il protocollo impostato viene utilizzato per l'invio di tutti i tipi di pacchetti AutoSupport.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Selezionare il protocollo che si desidera utilizzare per inviare pacchetti AutoSupport.
3. Se è stato selezionato **HTTPS**, selezionare se utilizzare un certificato di supporto NetApp (certificato TLS) per proteggere la connessione al server del supporto tecnico.
   - **Verify certificate** (verifica certificato*) (impostazione predefinita): Garantisce che la trasmissione dei pacchetti AutoSupport sia sicura. Il certificato di supporto NetApp è già installato con il software StorageGRID.
   - **Non verificare il certificato**: Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.
4. Selezionare **Salva**. Tutti i pacchetti settimanali, attivati dall'utente e attivati da eventi vengono inviati utilizzando il protocollo selezionato.

Disattiva AutoSupport settimanale

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport all'assistenza tecnica una volta alla settimana.

Per determinare quando verrà inviato il pacchetto settimanale AutoSupport, andare alla scheda **AutoSupport** > **Results**. Nella sezione **AutoSupport settimanale**, osservare il valore per **ora pianificata successiva**.

È possibile disattivare l'invio automatico di pacchetti AutoSupport settimanali in qualsiasi momento.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Deselezionare la casella di controllo **Enable Weekly AutoSupport** (Abilita aggiornamento settimanale).
3. Selezionare **Salva**.

Disattiva AutoSupport attivato dagli eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un pacchetto AutoSupport all'assistenza tecnica ogni ora.

È possibile disattivare AutoSupport attivato da eventi in qualsiasi momento.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Deselezionare la casella di controllo **attiva AutoSupport attivato da eventi**.
3. Selezionare **Salva**.

Attiva AutoSupport on Demand

AutoSupport on Demand può aiutare a risolvere i problemi sui quali il supporto tecnico sta lavorando attivamente.

Per impostazione predefinita, AutoSupport on Demand è disattivato. L'attivazione di questa funzione consente al supporto tecnico di richiedere che il sistema StorageGRID invii automaticamente i pacchetti AutoSupport. Il

supporto tecnico può anche impostare l'intervallo di tempo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può attivare o disattivare AutoSupport on Demand.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Selezionare **HTTPS** per il protocollo.
3. Selezionare la casella di controllo **Enable Weekly AutoSupport** (Abilita aggiornamento settimanale).
4. Selezionare la casella di controllo **attiva AutoSupport su richiesta**.
5. Selezionare **Salva**.

   AutoSupport on Demand è attivato e il supporto tecnico può inviare richieste AutoSupport on Demand a StorageGRID.

Disattiva i controlli per gli aggiornamenti software

Per impostazione predefinita, StorageGRID contatta NetApp per determinare se sono disponibili aggiornamenti software per il sistema. Se è disponibile una correzione rapida StorageGRID o una nuova versione, la nuova versione viene visualizzata nella pagina aggiornamento StorageGRID.

Se necessario, è possibile disattivare la verifica degli aggiornamenti software. Ad esempio, se il sistema non dispone di accesso WAN, disattivare il controllo per evitare errori di download.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Deselezionare la casella di controllo **Controlla aggiornamenti software**.
3. Selezionare **Salva**.

Aggiungere una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, i pacchetti di stato e di integrità vengono inviati al supporto tecnico. È possibile specificare una destinazione aggiuntiva per tutti i pacchetti AutoSupport.

Per verificare o modificare il protocollo utilizzato per inviare pacchetti AutoSupport, vedere le istruzioni a. Specificare il protocollo per i pacchetti AutoSupport.

> Non è possibile utilizzare il protocollo SMTP per inviare pacchetti AutoSupport a una destinazione aggiuntiva.

Fasi

1. Selezionare **SUPPORT** > **Strumenti** > **AutoSupport** > **Impostazioni**.
2. Selezionare **attiva destinazione AutoSupport aggiuntiva**.
3. Specificare quanto segue:

   Nome host

   Il nome host del server o l'indirizzo IP di un server di destinazione AutoSupport aggiuntivo.

   > È possibile inserire solo una destinazione aggiuntiva.

Porta

Porta utilizzata per connettersi a un server di destinazione AutoSupport aggiuntivo. L'impostazione predefinita è la porta 80 per HTTP o la porta 443 per HTTPS.

Convalida del certificato

Se viene utilizzato un certificato TLS per proteggere la connessione alla destinazione aggiuntiva.

- Selezionare **verifica certificato** per utilizzare la convalida del certificato.
- Selezionare **non verificare il certificato** per inviare i pacchetti AutoSupport senza la convalida del certificato.

  Selezionare questa opzione solo se si dispone di un buon motivo per non utilizzare la convalida del certificato, ad esempio quando si verifica un problema temporaneo con un certificato.

4. Se è stato selezionato **verifica certificato**, procedere come segue:
   a. Individuare la posizione del certificato CA.
   b. Caricare il file del certificato CA.

      Vengono visualizzati i metadati del certificato CA.
5. Selezionare **Salva**.

   Tutti i futuri pacchetti AutoSupport settimanali, attivati da eventi e attivati dall'utente verranno inviati alla destinazione aggiuntiva.

Configurazione di AutoSupport per le appliance

AutoSupport per appliance segnala problemi di hardware StorageGRID e StorageGRID AutoSupport segnala problemi di software StorageGRID, con una sola eccezione: Per SGF6112, StorageGRID AutoSupport segnala problemi di hardware e software. È necessario configurare AutoSupport su ogni appliance, ad eccezione di SGF6112, che non richiede configurazione aggiuntiva. AutoSupport viene implementato in maniera differente per le appliance di servizi e di storage.

Puoi utilizzare SANtricity per abilitare AutoSupport per ciascuna appliance di storage. È possibile configurare SANtricity AutoSupport durante la configurazione iniziale dell'appliance o dopo l'installazione di un'appliance:

- Per le appliance SG6000 e SG5700, "Configurare AutoSupport in Gestore di sistema di SANtricity"

È possibile includere in StorageGRID AutoSupport i pacchetti AutoSupport delle appliance e-Series configurando l'erogazione di AutoSupport in base al proxy "Gestore di sistema di SANtricity".

StorageGRID AutoSupport non segnala problemi di hardware, ad esempio errori DIMM o HIC (host Interface Card). Tuttavia, potrebbero verificarsi alcuni guasti ai componenti "avvisi hardware". Per le appliance StorageGRID con un controller di gestione baseboard (BMC) è possibile configurare trap e-mail e SNMP per segnalare errori hardware:

- "Impostare le notifiche e-mail per gli avvisi BMC"
- "Configurare le impostazioni SNMP per BMC"

Informazioni correlate

"Supporto NetApp"

Attivare manualmente un pacchetto AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi del sistema StorageGRID, è possibile attivare manualmente l'invio di un pacchetto AutoSupport.

Prima di iniziare

- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- È necessario disporre dell'autorizzazione di accesso root o di altra configurazione della griglia.

Fasi

1. Selezionare **SUPPORTO** > **Strumenti** > **AutoSupport**.
2. Nella scheda **azioni**, selezionare **Invia AutoSupport** attivato dall'utente.

   StorageGRID tenta di inviare un pacchetto AutoSupport al sito di supporto NetApp. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. Se si verifica un problema, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il pacchetto AutoSupport.

   > ⓘ Dopo aver inviato un pacchetto AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport nel browser dopo 1 minuto per accedere ai risultati più recenti.

Risolvere i problemi relativi ai pacchetti AutoSupport

Se un tentativo di invio di un pacchetto AutoSupport non riesce, il sistema StorageGRID esegue azioni diverse a seconda del tipo di pacchetto AutoSupport. È possibile controllare lo stato dei pacchetti AutoSupport selezionando **SUPPORT** > **Tools** > **AutoSupport** > **Results**.

Quando il pacchetto AutoSupport non riesce a inviare, viene visualizzato "non riuscito" nella scheda **risultati** della pagina **AutoSupport**.

> ⓘ Se è stato configurato un server proxy per l'inoltro dei pacchetti AutoSupport a NetApp, è necessario "verificare che le impostazioni di configurazione del server proxy siano corrette".

Errore settimanale del pacchetto AutoSupport

Se un pacchetto AutoSupport settimanale non viene inviato, il sistema StorageGRID esegue le seguenti operazioni:

1. Aggiorna l'attributo dei risultati più recenti in Riprova.
2. Tenta di inviare nuovamente il pacchetto AutoSupport 15 volte ogni quattro minuti per un'ora.
3. Dopo un'ora di errori di invio, aggiorna l'attributo dei risultati più recenti su non riuscito.
4. Tenta di inviare nuovamente un pacchetto AutoSupport all'ora pianificata successiva.
5. Mantiene la normale pianificazione AutoSupport se il pacchetto non riesce perché il servizio NMS non è disponibile e se un pacchetto viene inviato prima del termine di sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un pacchetto AutoSupport se non è stato inviato per sette giorni o più.

Errore del pacchetto AutoSupport attivato dall'utente o dagli eventi

Se un pacchetto AutoSupport attivato dall'utente o da un evento non riesce a inviare, il sistema StorageGRID esegue le seguenti operazioni:

1. Visualizza un messaggio di errore se l'errore è noto. Ad esempio, se un utente seleziona il protocollo SMTP senza fornire le corrette impostazioni di configurazione dell'e-mail, viene visualizzato il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Non tenta di inviare nuovamente il pacchetto.
3. Registra l'errore in `nms.log`.

Se si verifica un errore e SMTP è il protocollo selezionato, verificare che il server e-mail del sistema StorageGRID sia configurato correttamente e che il server e-mail sia in esecuzione (**SUPPORT** > **Alarms (legacy)** > **> Configurazione e-mail legacy**). Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Scopri come "configurare le impostazioni del server di posta elettronica".

Correggere un errore del pacchetto AutoSupport

Se si verifica un errore e il protocollo SMTP è selezionato, verificare che il server e-mail del sistema StorageGRID sia configurato correttamente e che il server e-mail sia in esecuzione. Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport packages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Invio dei pacchetti e-Series AutoSupport tramite StorageGRID

Puoi inviare pacchetti AutoSupport di e-Series SANtricity System Manager al supporto tecnico tramite un nodo amministrativo StorageGRID piuttosto che la porta di gestione dell'appliance di storage.

Vedere "AutoSupport hardware e-Series" Per ulteriori informazioni sull'utilizzo di AutoSupport con le appliance e-Series.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root o amministratore dell'appliance di storage".
- Hai configurato SANtricity AutoSupport:
  - Per le appliance SG6000 e SG5700, "Configurare AutoSupport in Gestore di sistema di SANtricity"

> È necessario disporre del firmware SANtricity 8.70 o superiore per accedere a Gestione di sistema di SANtricity utilizzando Gestione griglia.

A proposito di questa attività

I pacchetti e-Series AutoSupport contengono dettagli sull'hardware di storage e sono più specifici degli altri pacchetti AutoSupport inviati dal sistema StorageGRID.

È possibile configurare un indirizzo speciale del server proxy in Gestione di sistema SANtricity per trasmettere

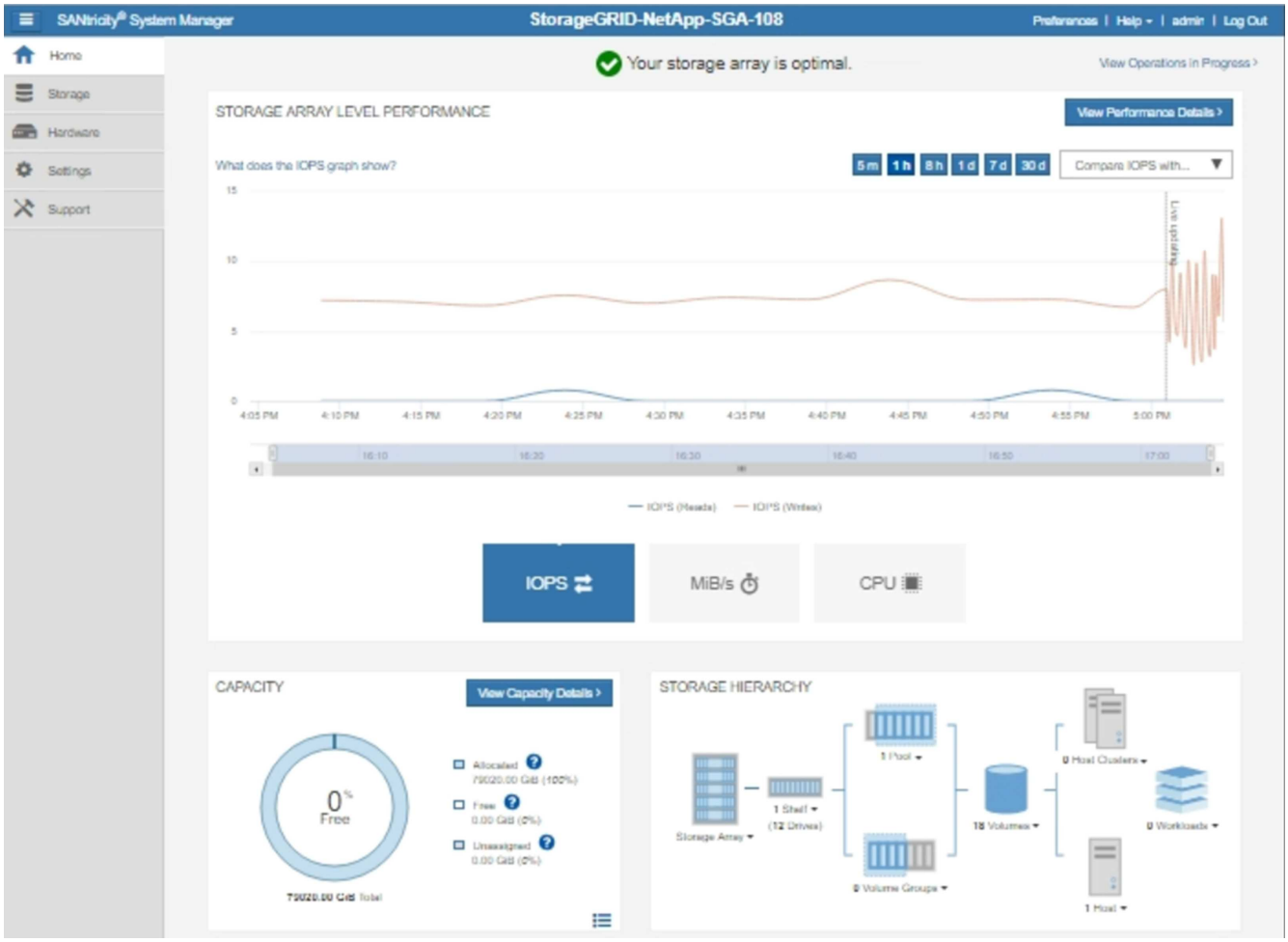
pacchetti AutoSupport tramite un nodo amministrativo StorageGRID senza l'utilizzo della porta di gestione dell'appliance. I pacchetti AutoSupport trasmessi in questo modo vengono inviati dal "Nodo Admin mittente preferito"e ne utilizzano uno "impostazioni proxy amministratore" Che sono stati configurati in Grid Manager.

> Questa procedura si applica solo alla configurazione di un server proxy StorageGRID per i pacchetti AutoSupport e-Series. Per ulteriori informazioni sulla configurazione di e-Series AutoSupport, consultare "Documentazione NetApp e-Series e SANtricity".

Fasi

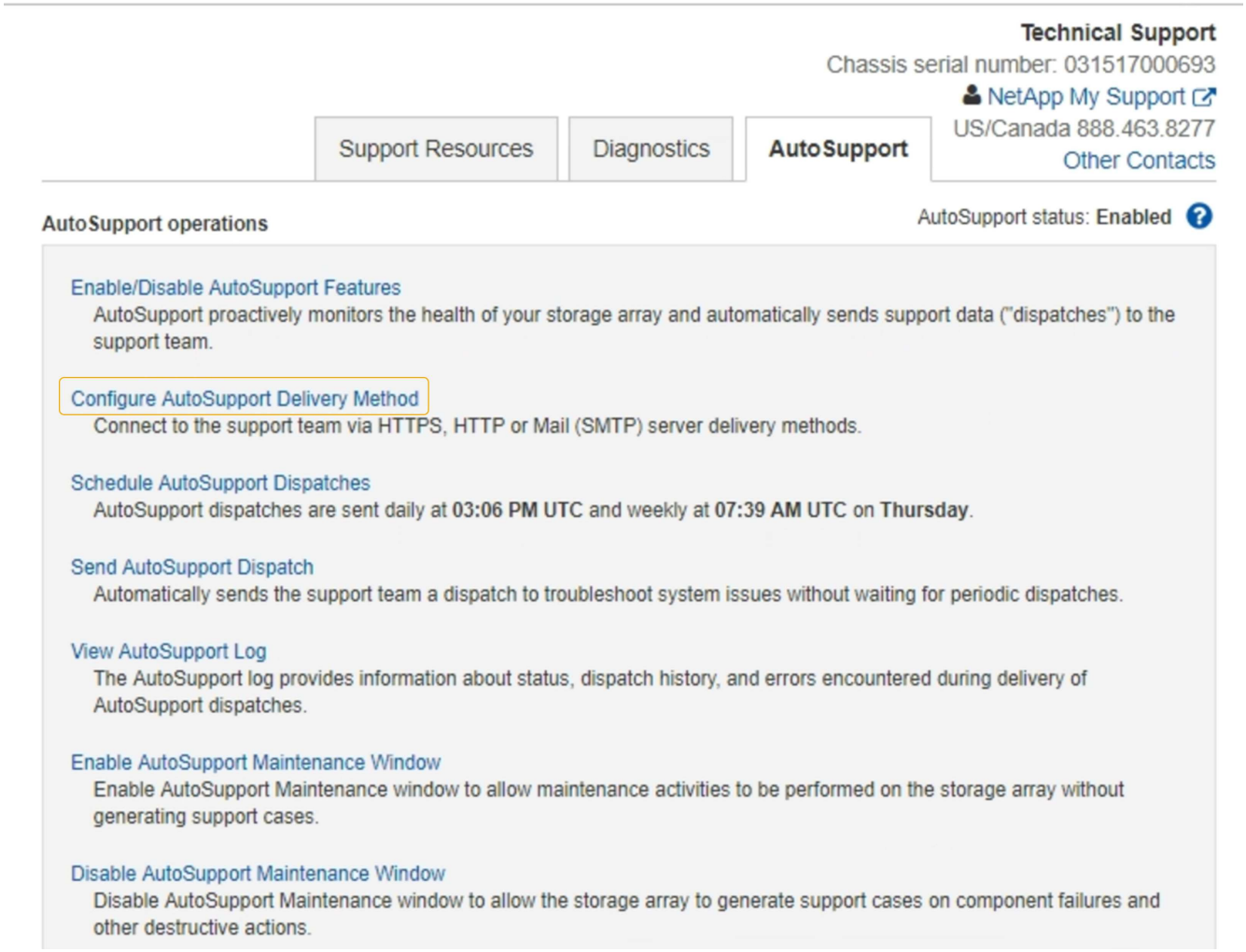
1. In Grid Manager, selezionare **NODES**.
2. Dall'elenco dei nodi a sinistra, selezionare il nodo dell'appliance di storage che si desidera configurare.
3. Selezionare **Gestore di sistema SANtricity**.

   Viene visualizzata la home page di Gestore di sistema di SANtricity.



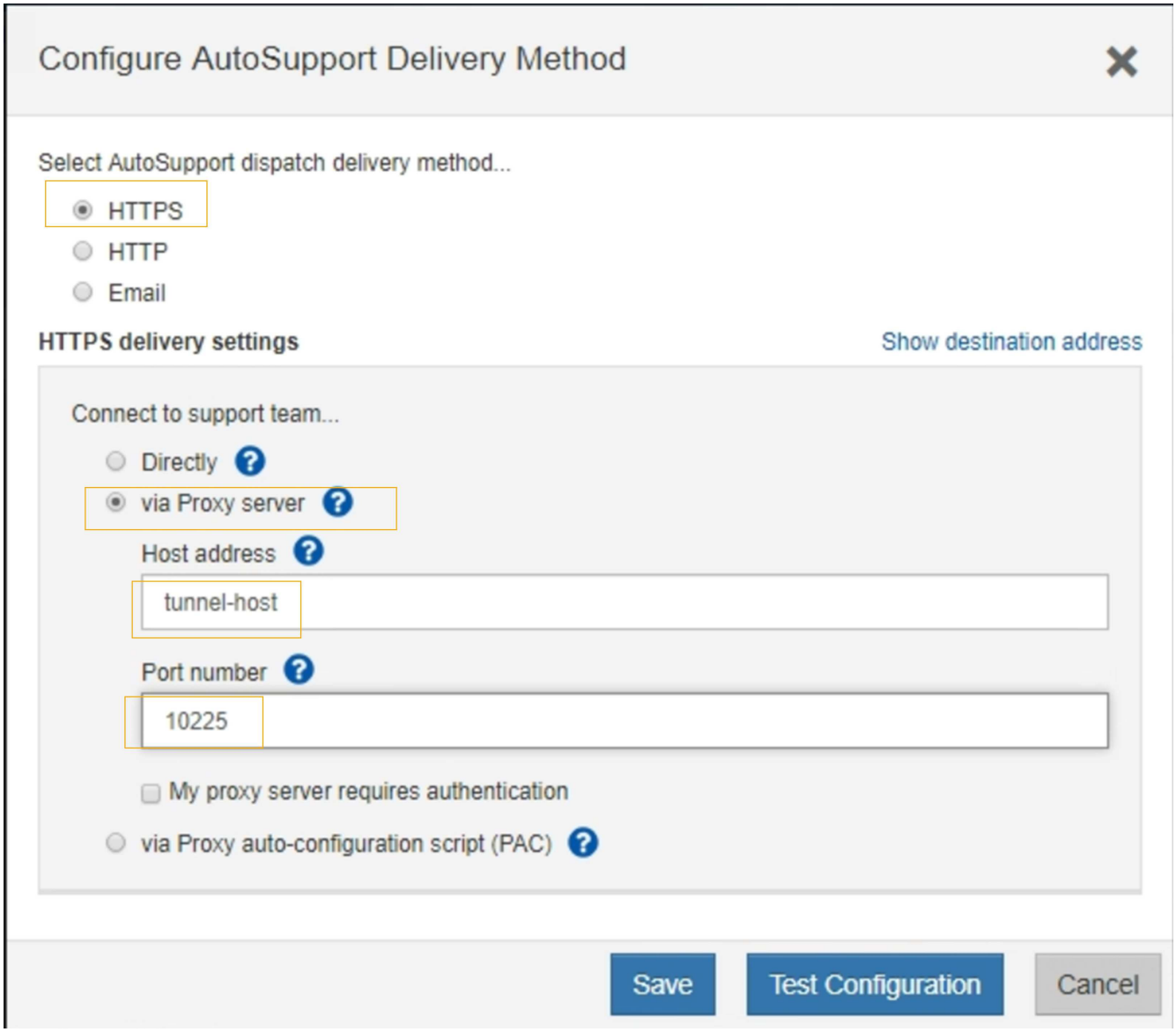
4. Selezionare **SUPPORT** > **Support Center** > **AutoSupport**.

   Viene visualizzata la pagina AutoSupport Operations.



5. Selezionare **Configura metodo di erogazione AutoSupport**.

   Viene visualizzata la pagina Configura metodo di erogazione AutoSupport.



6. Selezionare **HTTPS** per il metodo di consegna.

   Il certificato che abilita HTTPS è preinstallato.

7. Selezionare **via Proxy server**.
8. Invio `tunnel-host` Per l'indirizzo **host**.

   `tunnel-host` È l'indirizzo speciale che consente di utilizzare un nodo amministrativo per inviare pacchetti AutoSupport e-Series.

9. Invio `10225` Per il numero di porta *.

   `10225` È il numero di porta sul server proxy StorageGRID che riceve i pacchetti AutoSupport dal controller e-Series dell'appliance.

10. Selezionare **verifica configurazione** per verificare l'instradamento e la configurazione del server proxy AutoSupport.

    Se corretto, viene visualizzato un messaggio in un banner verde: "La configurazione AutoSupport è stata

verificata."

Se il test ha esito negativo, viene visualizzato un messaggio di errore su un banner rosso. Verificare le impostazioni DNS e la rete StorageGRID, quindi verificare "Nodo Admin mittente preferito" Può connettersi al sito di supporto NetApp e riprovare il test.

11. Selezionare **Salva**.

    La configurazione viene salvata e viene visualizzato un messaggio di conferma: "Il metodo di consegna AutoSupport è stato configurato".

Gestire i nodi di storage

Gestione dei nodi di storage: Panoramica

I nodi di storage forniscono servizi e capacità di storage su disco. La gestione dei nodi di storage comporta quanto segue:

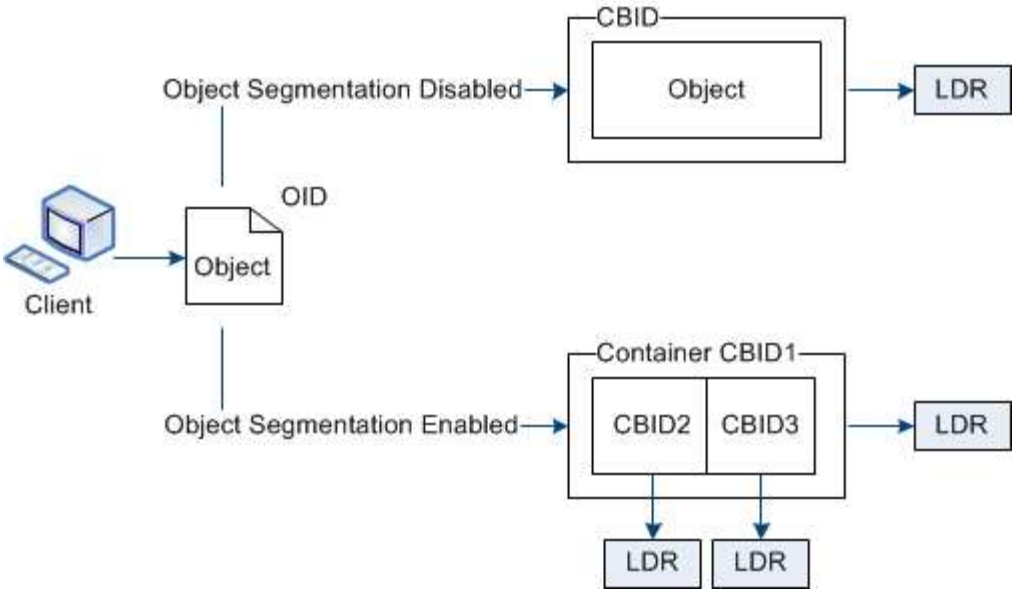
- Gestione delle opzioni di storage
- Comprendere quali sono le filigrane dei volumi di storage e come è possibile utilizzare le sovrascritture dei watermark per controllare quando i nodi di storage diventano di sola lettura
- Monitoraggio e gestione dello spazio utilizzato per i metadati degli oggetti
- Configurazione delle impostazioni globali per gli oggetti memorizzati
- Applicazione delle impostazioni di configurazione del nodo di storage
- Gestione dei nodi di storage completi

Utilizzare le opzioni di storage

Che cos'è la segmentazione degli oggetti?

La segmentazione degli oggetti è il processo di suddivisione di un oggetto in un insieme di oggetti di dimensioni fisse più piccole per ottimizzare l'utilizzo dello storage e delle risorse per oggetti di grandi dimensioni. Il caricamento multiparte S3 crea anche oggetti segmentati, con un oggetto che rappresenta ciascuna parte.

Quando un oggetto viene acquisito nel sistema StorageGRID, il servizio LDR suddivide l'oggetto in segmenti e crea un container di segmenti che elenca le informazioni di intestazione di tutti i segmenti come contenuto.



Al momento del recupero di un container di segmenti, il servizio LDR assembla l'oggetto originale dai suoi segmenti e lo restituisce al client.

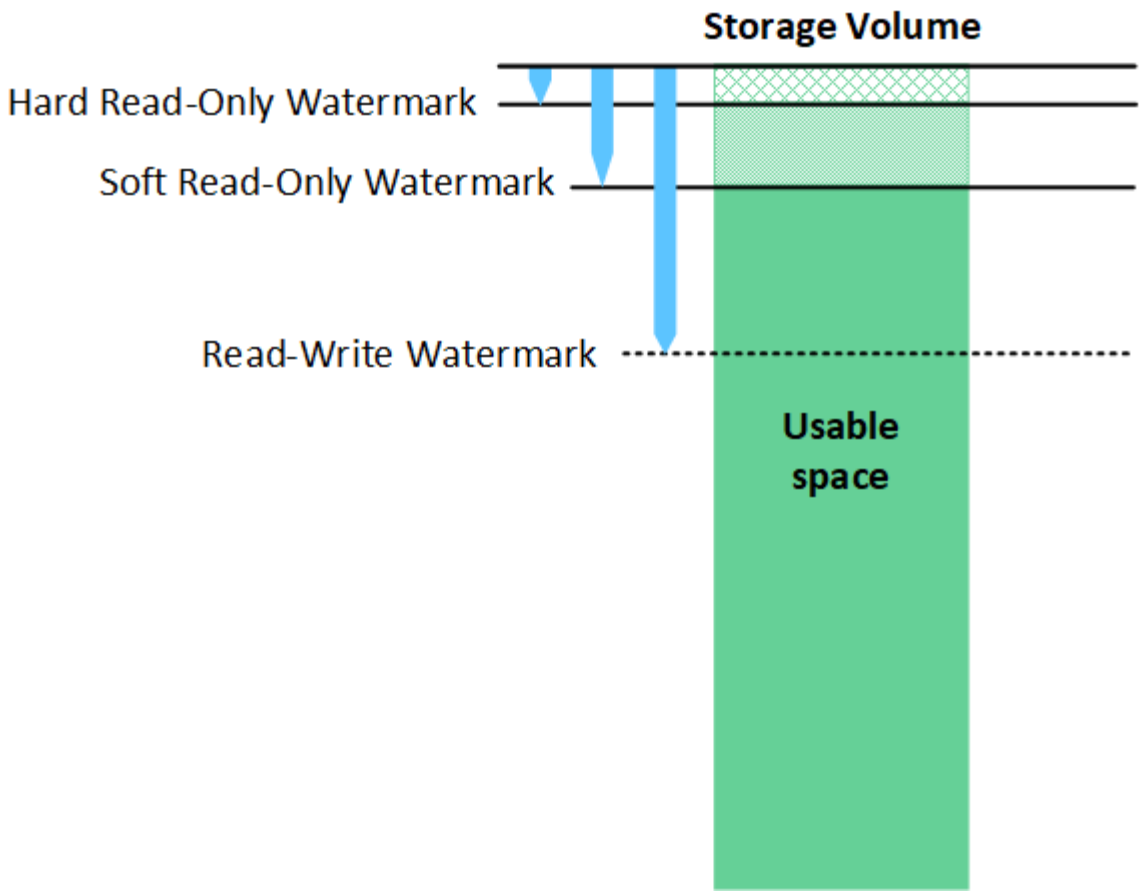
Il container e i segmenti non sono necessariamente memorizzati sullo stesso nodo di storage. Container e segmenti possono essere memorizzati in qualsiasi nodo di storage all'interno del pool di storage specificato nella regola ILM.

Ogni segmento viene trattato dal sistema StorageGRID in modo indipendente e contribuisce al conteggio di attributi come oggetti gestiti e oggetti memorizzati. Ad esempio, se un oggetto memorizzato nel sistema StorageGRID viene suddiviso in due segmenti, il valore degli oggetti gestiti aumenta di tre dopo il completamento dell'acquisizione, come segue:

```
segment container + segment 1 + segment 2 = three stored objects
```

Cosa sono le filigrane dei volumi di storage?

StorageGRID utilizza tre filigrane dei volumi di storage per garantire che i nodi di storage vengano trasferiti in modo sicuro in uno stato di sola lettura prima che lo spazio sia estremamente ridotto e per consentire ai nodi di storage che sono stati trasferiti in uno stato di sola lettura di tornare in lettura e scrittura.



Le filigrane dei volumi di storage si applicano solo allo spazio utilizzato per i dati degli oggetti replicati e codificati in cancellazione. Per ulteriori informazioni sullo spazio riservato ai metadati degli oggetti sul volume 0, visitare il sito Web "Gestire lo storage dei metadati degli oggetti".

Che cos'è la filigrana di sola lettura?

La filigrana **Storage Volume Soft Read-Only** è la prima filigrana a indicare che lo spazio utilizzabile di un nodo di storage per i dati dell'oggetto sta diventando pieno.

Se ogni volume in un nodo di storage ha meno spazio libero rispetto alla filigrana di sola lettura soft del volume, il nodo di storage passa alla *modalità di sola lettura*. La modalità di sola lettura indica che il nodo di storage annuncia servizi di sola lettura al resto del sistema StorageGRID, ma soddisfa tutte le richieste di scrittura in sospeso.

Ad esempio, si supponga che ogni volume in un nodo di storage abbia un watermark di sola lettura soft di 10 GB. Non appena ogni volume dispone di meno di 10 GB di spazio libero, il nodo di storage passa alla modalità di sola lettura.

Che cos'è la filigrana di sola lettura?

La filigrana **Storage Volume Hard Read-Only** è la filigrana successiva per indicare che lo spazio utilizzabile di un nodo per i dati dell'oggetto sta diventando pieno.

Se lo spazio libero su un volume è inferiore a quello della filigrana di sola lettura del volume, la scrittura sul volume non avrà esito positivo. Tuttavia, le scritture su altri volumi possono continuare fino a quando lo spazio libero su tali volumi non è inferiore alle filigrane di sola lettura.

Ad esempio, si supponga che ogni volume in un nodo di storage abbia un watermark di sola lettura hard di 5 GB. Non appena ogni volume dispone di meno di 5 GB di spazio libero, Storage Node non accetta più richieste di scrittura.

La filigrana hard Read-only è sempre inferiore alla filigrana soft Read-only.

Che cos'è la filigrana Read-Write?

Il watermark **Storage Volume Read-Write** si applica solo ai nodi di storage che sono passati alla modalità di sola lettura. Determina quando il nodo può diventare di nuovo in lettura/scrittura. Quando lo spazio libero su un volume di storage in un nodo di storage è superiore al watermark Read-Write di quel volume, il nodo ritorna automaticamente allo stato Read-write.

Ad esempio, supponiamo che il nodo di storage sia passato alla modalità di sola lettura. Si supponga inoltre che ogni volume abbia un watermark Read-Write di 30 GB. Non appena lo spazio libero per qualsiasi volume aumenta fino a 30 GB, il nodo diventa di nuovo in lettura/scrittura.

La filigrana Read-Write è sempre più grande della filigrana di sola lettura e della filigrana di sola lettura.

Visualizzare le filigrane dei volumi di storage

È possibile visualizzare le impostazioni correnti del watermark e i valori ottimizzati per il sistema. Se non si utilizzano filigrane ottimizzate, è possibile determinare se è possibile o necessario regolare le impostazioni.

Prima di iniziare

- L'aggiornamento a StorageGRID 11.6 o versione successiva è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root".

Consente di visualizzare le impostazioni correnti del watermark

È possibile visualizzare le impostazioni correnti del filigrana dello storage in Grid Manager.

Fasi

1. Selezionare **SUPPORT** > **other** > **Storage Watermarks**.
2. Nella pagina Storage Watermark (Filigrane di archiviazione), controllare la casella di controllo Use Optimized Values (Usa valori ottimizzati).
   - Se la casella di controllo è selezionata, tutte e tre le filigrane sono ottimizzate per ogni volume di archiviazione su ogni nodo di archiviazione, in base alle dimensioni del nodo di archiviazione e alla capacità relativa del volume.

     Questa è l'impostazione predefinita e consigliata. Non aggiornare questi valori. Se lo si desidera, è possibile Visualizza filigrane di storage ottimizzate.

   - Se la casella di controllo Usa valori ottimizzati non è selezionata, vengono utilizzate filigrane personalizzate (non ottimizzate). Si sconsiglia di utilizzare le impostazioni personalizzate della filigrana. Seguire le istruzioni per "Risoluzione dei problemi gli avvisi di override del watermark di sola lettura bassa" per determinare se è possibile o necessario regolare le impostazioni.

     Quando si specificano le impostazioni personalizzate della filigrana, è necessario immettere valori superiori a 0.

Visualizza filigrane di memorizzazione ottimizzate

StorageGRID utilizza due metriche Prometheus per mostrare i valori ottimizzati che ha calcolato per la filigrana di sola lettura del volume di storage **Soft Read-only**. È possibile visualizzare i valori minimi e massimi ottimizzati per ciascun nodo di storage nella griglia.

1. Selezionare **SUPPORT** > **Tools** > **Metrics**.
2. Nella sezione Prometheus, selezionare il collegamento per accedere all'interfaccia utente Prometheus.
3. Per visualizzare la filigrana minima di sola lettura soft consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_minimum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore minimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage. Se questo valore è superiore all'impostazione personalizzata per **Storage Volume Soft Read-Only Watermark**, viene attivato l'avviso **Low Read-only watermark override** per il nodo di storage.

4. Per visualizzare la filigrana di sola lettura soft massima consigliata, immettere la seguente metrica Prometheus e selezionare **Esegui**:

   ```
   storagegrid_storage_volume_maximum_optimized_soft_readonly_watermark
   ```

   L'ultima colonna mostra il valore massimo ottimizzato della filigrana di sola lettura soft per tutti i volumi di storage su ciascun nodo di storage.

Gestire lo storage dei metadati degli oggetti

La capacità dei metadati degli oggetti di un sistema StorageGRID controlla il numero massimo di oggetti che possono essere memorizzati in tale sistema. Per garantire che il sistema StorageGRID disponga di spazio sufficiente per memorizzare nuovi oggetti, è necessario comprendere dove e come StorageGRID memorizza i metadati degli oggetti.

Che cos'è il metadata a oggetti?

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

Per un oggetto in StorageGRID, i metadati dell'oggetto includono i seguenti tipi di informazioni:

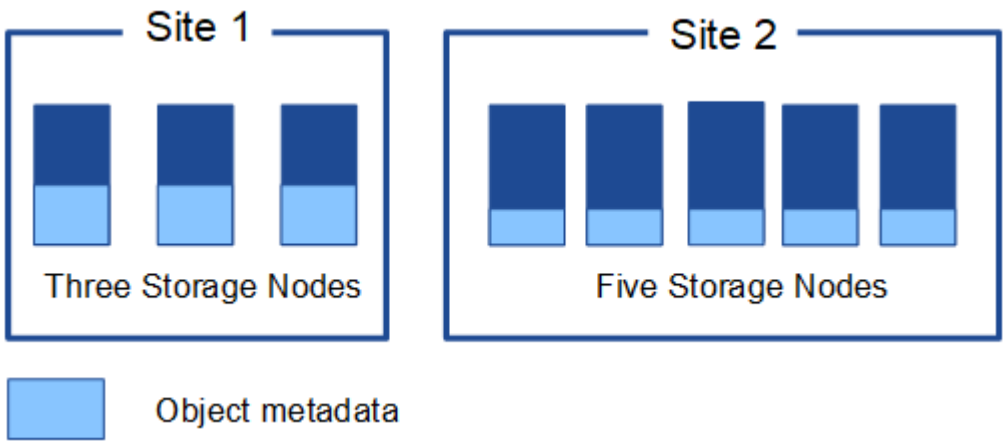
- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3 o del container Swift, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta, e la data e l'ora dell'ultima modifica dell'oggetto.
- Qualsiasi coppia di valori chiave metadati utente personalizzata associata all'oggetto.
- Per gli oggetti S3, qualsiasi coppia chiave-valore tag oggetto associata all'oggetto.
- Per le copie di oggetti replicate, la posizione di storage corrente di ciascuna copia.
- Per le copie di oggetti con codifica erasure, la posizione di storage corrente di ciascun frammento.
- Per le copie di oggetti in un Cloud Storage Pool, la posizione dell'oggetto, incluso il nome del bucket esterno e l'identificatore univoco dell'oggetto.

- Per oggetti segmentati e multiparte, identificatori di segmenti e dimensioni dei dati.

Come vengono memorizzati i metadati degli oggetti?

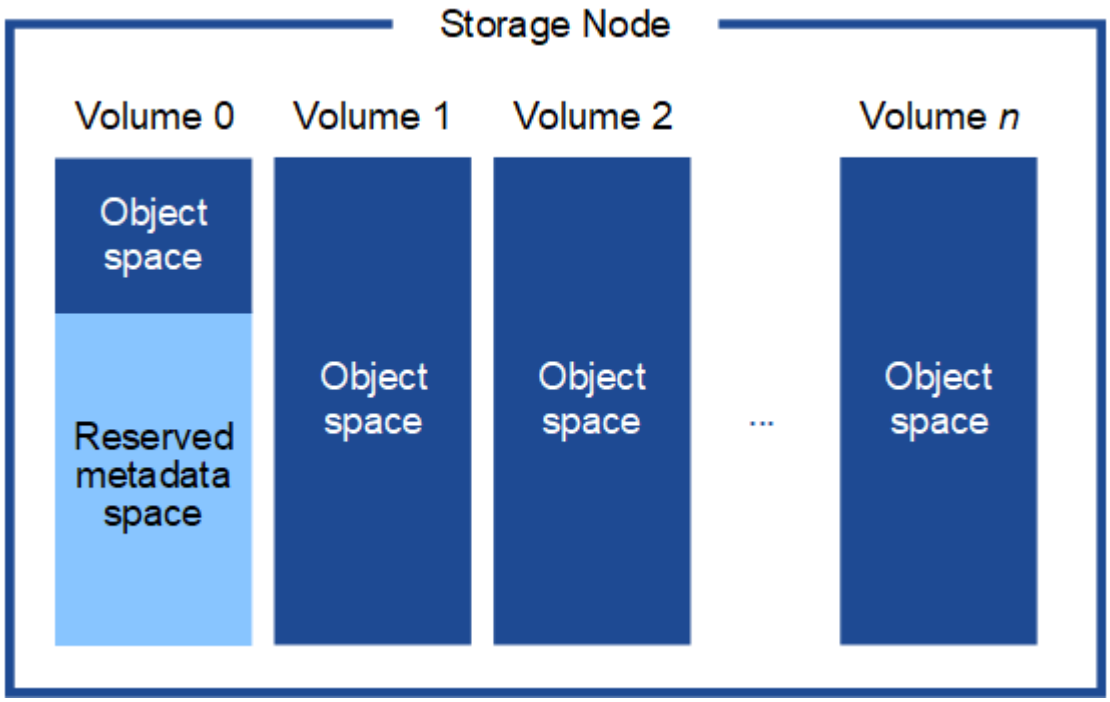
StorageGRID mantiene i metadati degli oggetti in un database Cassandra, che viene memorizzato indipendentemente dai dati degli oggetti. Per garantire la ridondanza e proteggere i metadati degli oggetti dalla perdita, StorageGRID memorizza tre copie dei metadati per tutti gli oggetti del sistema in ogni sito.

Questa figura rappresenta i nodi di storage in due siti. Ogni sito ha la stessa quantità di metadati oggetto e i metadati di ciascun sito sono suddivisi tra tutti i nodi di storage di quel sito.



Dove sono memorizzati i metadati degli oggetti?

Questa figura rappresenta i volumi di storage per un singolo nodo di storage.



Come mostrato nella figura, StorageGRID riserva spazio per i metadati degli oggetti sul volume di storage 0 di ciascun nodo di storage. Utilizza lo spazio riservato per memorizzare i metadati degli oggetti e per eseguire le operazioni essenziali del database. Qualsiasi spazio rimanente sul volume di storage 0 e tutti gli altri volumi di storage nel nodo di storage vengono utilizzati esclusivamente per i dati a oggetti (copie replicate e frammenti

con codifica di cancellazione).

La quantità di spazio riservato ai metadati degli oggetti su un nodo di storage specifico dipende da diversi fattori, descritti di seguito.

Impostazione dello spazio riservato dei metadati

Lo *spazio riservato metadati* è un'impostazione a livello di sistema che rappresenta la quantità di spazio che sarà riservata ai metadati sul volume 0 di ogni nodo di archiviazione. Come mostrato nella tabella, il valore predefinito di questa impostazione si basa su:

- La versione software utilizzata al momento dell'installazione iniziale di StorageGRID.
- La quantità di RAM su ciascun nodo di storage.

Versione utilizzata per l'installazione iniziale di StorageGRID	Quantità di RAM sui nodi di storage	Impostazione predefinita spazio riservato metadati
da 11,5 a 11,8	128 GB o più su ciascun nodo di storage nella griglia	8 TB (8,000 GB)
	Meno di 128 GB su qualsiasi nodo di storage nel grid	3 TB (3.000 GB)
da 11,1 a 11,4	128 GB o più su ciascun nodo di storage in un sito qualsiasi	4 TB (4.000 GB)
	Meno di 128 GB su qualsiasi nodo di storage in ogni sito	3 TB (3.000 GB)
11,0 o precedente	Qualsiasi importo	2 TB (2.000 GB)

Visualizza impostazione spazio riservato metadati

Per visualizzare l'impostazione dello spazio riservato ai metadati per il sistema StorageGRID, procedere come segue.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Impostazioni archiviazione**.
2. Nella pagina Impostazioni archiviazione, espandere la sezione **spazio riservato metadati**.

Per StorageGRID 11,8 o versione successiva, il valore dello spazio riservato dei metadati deve essere almeno 100 GB e non più di 1 PB.

L'impostazione predefinita per una nuova installazione di StorageGRID 11,6 o superiore in cui ogni nodo di archiviazione ha 128 GB o più di RAM è 8.000 GB (8 TB).

Spazio riservato effettivo per i metadati

A differenza dell'impostazione dello spazio riservato ai metadati a livello di sistema, per ogni nodo di archiviazione viene determinato lo *spazio riservato effettivo* per i metadati dell'oggetto. Per qualsiasi nodo di

archiviazione, lo spazio riservato effettivo per i metadati dipende dalla dimensione del volume 0 per il nodo e dall'impostazione dello spazio riservato metadati a livello di sistema.

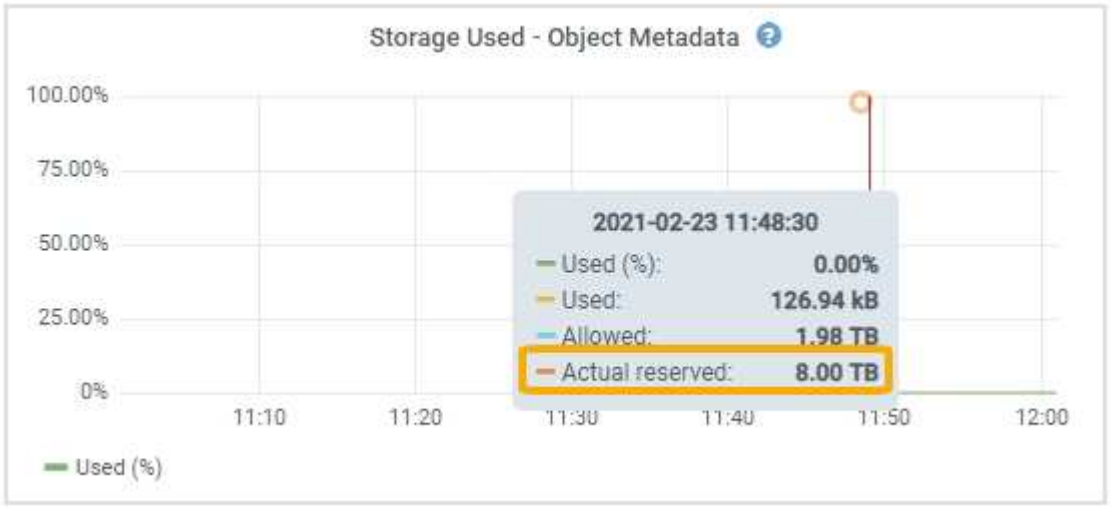
Dimensione del volume 0 per il nodo	Spazio riservato effettivo per i metadati
Meno di 500 GB (non in produzione)	10% del volume 0
500 GB o più o Nodi di storage solo metadati	Il minore di questi valori: • Volume 0 • Impostazione dello spazio riservato dei metadati **Nota**: È richiesto un solo rangedb per i nodi di archiviazione di solo metadati.

Visualizzare lo spazio riservato effettivo per i metadati

Per visualizzare lo spazio riservato effettivo per i metadati su un nodo di storage specifico, procedere come segue.

Fasi

1. Da Grid Manager, selezionare **NODES** > ***Storage Node***.
2. Selezionare la scheda **Storage**.
3. Posizionare il cursore sul grafico Storage used - Object Metadata (Storage utilizzato - metadati oggetto) e individuare il valore **Actual reserved** (riservato).



Nella schermata, il valore **effettivo riservato** è 8 TB. Questa schermata riguarda un nodo di storage di grandi dimensioni in una nuova installazione di StorageGRID 11.6. Poiché l'impostazione dello spazio riservato ai metadati a livello di sistema è inferiore al volume 0 per questo nodo di archiviazione, lo spazio riservato effettivo per questo nodo è uguale all'impostazione dello spazio riservato ai metadati.

Esempio di spazio riservato effettivo dei metadati

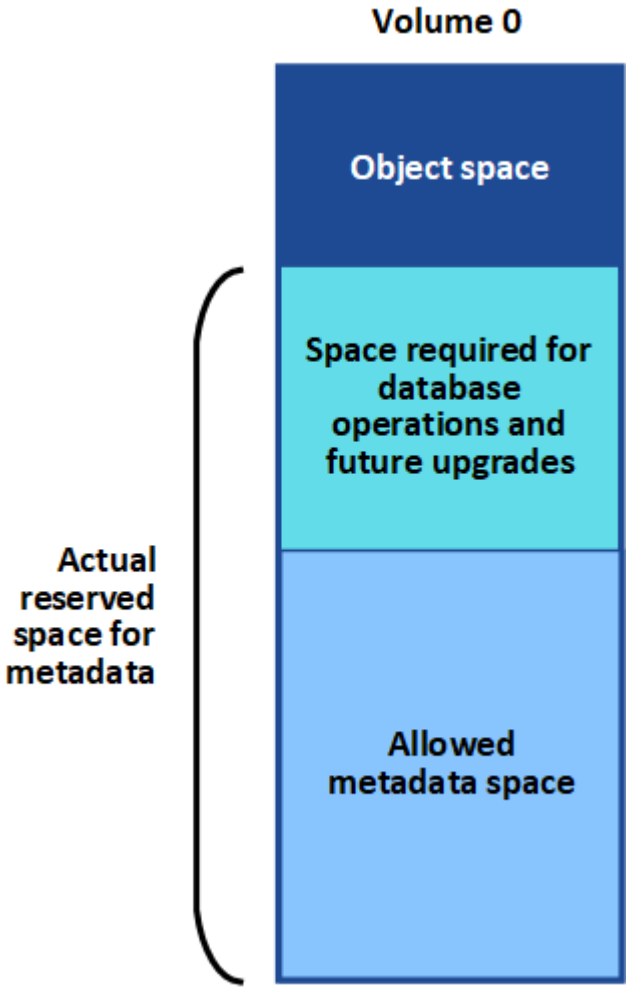
Si supponga di installare un nuovo sistema StorageGRID utilizzando la versione 11,7 o successiva. In questo esempio, si supponga che ogni nodo di storage abbia più di 128 GB di RAM e che il volume 0 del nodo di

storage 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo spazio riservato * dei metadati a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per una nuova installazione di StorageGRID 11.6 o superiore se ogni nodo di storage ha più di 128 GB di RAM).
- Lo spazio riservato effettivo per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **spazio riservato metadati**).

Spazio consentito di metadati

Lo spazio riservato effettivo di ciascun nodo di storage per i metadati viene suddiviso nello spazio disponibile per i metadati dell'oggetto (il *spazio consentito per i metadati*) e nello spazio necessario per le operazioni essenziali del database (come la compattazione e la riparazione) e per i futuri aggiornamenti hardware e software. Lo spazio consentito per i metadati regola la capacità complessiva degli oggetti.



La seguente tabella mostra come StorageGRID calcola lo spazio di metadati consentito* per diversi nodi di storage, in base alla quantità di memoria per il nodo e allo spazio riservato effettivo per i metadati.

		Quantità di memoria sul nodo di storage	

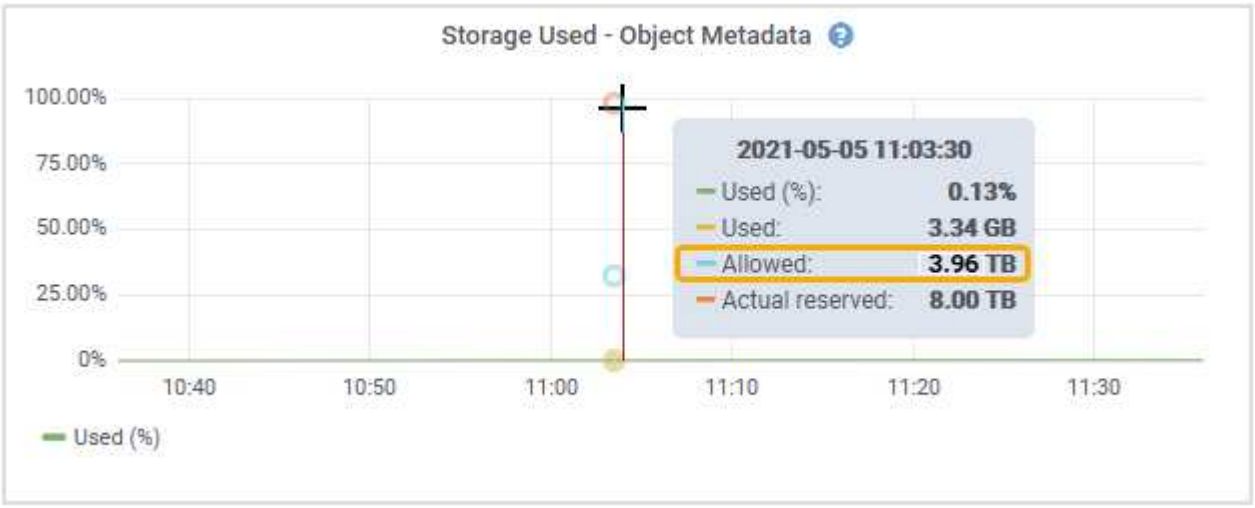
	≪ 128 GB	>= 128 GB	**Spazio riservato effettivo per i metadati**
≪= 4 TB	60% dello spazio riservato effettivo per i metadati, fino a un massimo di 1.32 TB	60% dello spazio riservato effettivo per i metadati, fino a un massimo di 1,98 TB	4 TB

Visualizzare lo spazio consentito per i metadati

Per visualizzare lo spazio di metadati consentito per un nodo di storage, procedere come segue.

Fasi

1. Da Grid Manager, selezionare **NODES**.
2. Selezionare il nodo di storage.
3. Selezionare la scheda **Storage**.
4. Posizionare il cursore sul grafico dei metadati Storage used - Object e individuare il valore **Allowed**.



Nella schermata, il valore **Allowed** è 3,96 TB, che è il valore massimo per un nodo di archiviazione il cui spazio riservato effettivo per i metadati è superiore a 4 TB.

Il valore **Allowed** corrisponde a questa metrica Prometheus:

```
storagegrid_storage_utilization_metadata_allowed_bytes
```

Esempio di spazio consentito per i metadati

Si supponga di installare un sistema StorageGRID utilizzando la versione 11.6. In questo esempio, si supponga che ogni nodo di storage abbia più di 128 GB di RAM e che il volume 0 del nodo di storage 1 (SN1) sia di 6 TB. In base a questi valori:

- Lo spazio riservato * dei metadati a livello di sistema è impostato su 8 TB. (Questo è il valore predefinito per StorageGRID 11.6 o superiore quando ogni nodo di storage ha più di 128 GB di RAM).
- Lo spazio riservato effettivo per i metadati per SN1 è di 6 TB. (L'intero volume è riservato perché il volume 0 è più piccolo dell'impostazione **spazio riservato metadati**).
- Lo spazio consentito per i metadati su SN1 è di 3 TB, in base al calcolo mostrato nella tabella per lo spazio consentito per i metadati: (Spazio riservato effettivo per i metadati − 1 TB) × 60%, fino a un massimo di 3.96 TB.

In che modo i nodi di storage di diverse dimensioni influiscono sulla capacità degli oggetti

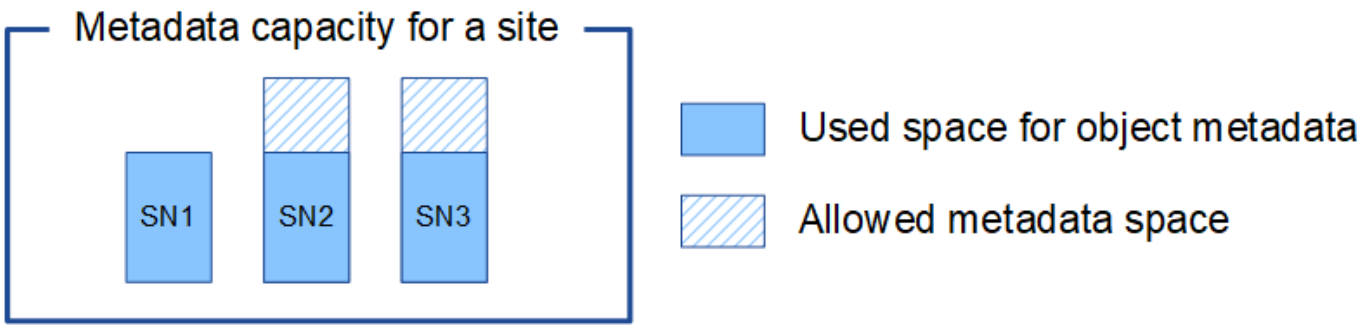
Come descritto in precedenza, StorageGRID distribuisce uniformemente i metadati degli oggetti nei nodi di storage di ciascun sito. Per questo motivo, se un sito contiene nodi di storage di dimensioni diverse, il nodo più piccolo del sito determina la capacità di metadati del sito.

Si consideri il seguente esempio:

- Si dispone di un grid a sito singolo contenente tre nodi di storage di dimensioni diverse.
- L'impostazione **spazio riservato metadati** è 4 TB.
- I nodi di storage hanno i seguenti valori per lo spazio riservato effettivo dei metadati e per lo spazio consentito dei metadati.

Nodo di storage	Dimensione del volume 0	Spazio riservato effettivo dei metadati	Spazio consentito di metadati
SN1	2,2 TB	2,2 TB	1,32 TB
SN2	5 TB	4 TB	1,98 TB
SN3	6 TB	4 TB	1,98 TB

Poiché i metadati degli oggetti sono distribuiti in modo uniforme tra i nodi di storage di un sito, ciascun nodo di questo esempio può contenere solo 1.32 TB di metadati. I 0.66 TB aggiuntivi di spazio consentito per i metadati SN2 e SN3 non possono essere utilizzati.



Analogamente, poiché StorageGRID gestisce tutti i metadati degli oggetti per un sistema StorageGRID in ogni sito, la capacità complessiva dei metadati di un sistema StorageGRID è determinata dalla capacità dei metadati degli oggetti del sito più piccolo.

Inoltre, poiché la capacità dei metadati degli oggetti controlla il numero massimo di oggetti, quando un nodo esaurisce la capacità dei metadati, la griglia è effettivamente piena.

Informazioni correlate

- Per informazioni su come monitorare la capacità dei metadati degli oggetti per ciascun nodo di storage, vedere le istruzioni per "Monitoraggio di StorageGRID".
- Per aumentare la capacità dei metadati degli oggetti per il sistema, "espandere una griglia" Aggiungendo nuovi nodi di storage.

Aumentare l'impostazione spazio riservato metadati

È possibile aumentare l'impostazione del sistema spazio riservato metadati se i nodi di archiviazione soddisfano requisiti specifici per la RAM e lo spazio disponibile.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Autorizzazione di accesso root o configurazione pagina topologia griglia e altre autorizzazioni di configurazione griglia".

A proposito di questa attività

Potrebbe essere possibile aumentare manualmente l'impostazione dello spazio riservato dei metadati a livello di sistema fino a 8 TB.

È possibile aumentare il valore dell'impostazione spazio riservato metadati a livello di sistema solo se entrambe le istruzioni sono vere:

- I nodi di storage di qualsiasi sito del sistema dispongono ciascuno di almeno 128 GB di RAM.
- I nodi di storage di qualsiasi sito del sistema dispongono ciascuno di spazio disponibile sufficiente sul volume di storage 0.

Se si aumenta questa impostazione, si riduce contemporaneamente lo spazio disponibile per lo storage a oggetti sul volume di storage 0 di tutti i nodi di storage. Per questo motivo, potrebbe essere preferibile impostare Metadata Reserved Space su un valore inferiore a 8 TB, in base ai requisiti previsti per i metadati degli oggetti.

> In generale, è meglio utilizzare un valore più alto invece di un valore più basso. Se l'impostazione spazio riservato metadati è troppo grande, è possibile ridurla in un secondo momento. Al contrario, se si aumenta il valore in un secondo momento, il sistema potrebbe dover spostare i dati dell'oggetto per liberare spazio.

Per una spiegazione dettagliata di come l'impostazione spazio riservato metadati influisce sullo spazio consentito per l'archiviazione dei metadati dell'oggetto su un nodo di archiviazione specifico, vedere "Gestire lo storage dei metadati degli oggetti".

Fasi

1. Determinare l'impostazione corrente di Metadata Reserved Space.
   a. Selezionare **CONFIGURATION** > **System** > **Storage options**.
   b. Nella sezione Storage Watermarks (Filigrane di archiviazione), annotare il valore **Metadata Reserved Space** (spazio riservato metadati).
2. Assicurarsi di disporre di spazio disponibile sufficiente sul volume di storage 0 di ciascun nodo di storage per aumentare questo valore.
   a. Selezionare **NODI**.

b. Selezionare il primo nodo di storage nella griglia.

c. Selezionare la scheda Storage (archiviazione).

d. Nella sezione Volumes (volumi), individuare la voce **/var/local/rangedb/0**.

e. Verificare che il valore disponibile sia uguale o superiore alla differenza tra il nuovo valore che si desidera utilizzare e il valore corrente dello spazio riservato dei metadati.

   Ad esempio, se l'impostazione spazio riservato metadati è attualmente di 4 TB e si desidera aumentarla a 6 TB, il valore disponibile deve essere pari o superiore a 2 TB.

f. Ripetere questi passaggi per tutti i nodi di storage.

   - Se uno o più nodi di storage non dispongono di spazio disponibile sufficiente, non è possibile aumentare il valore Metadata Reserved Space (spazio riservato metadati). Non continuare con questa procedura.
   - Se ogni nodo di storage dispone di spazio disponibile sufficiente sul volume 0, passare alla fase successiva.

3. Assicurarsi di disporre di almeno 128 GB di RAM su ciascun nodo di storage.

   a. Selezionare **NODI**.

   b. Selezionare il primo nodo di storage nella griglia.

   c. Selezionare la scheda **hardware**.

   d. Posizionare il cursore del mouse sul grafico utilizzo memoria. Assicurarsi che la memoria totale sia di almeno 128 GB.

   e. Ripetere questi passaggi per tutti i nodi di storage.

      - Se uno o più nodi di storage non dispongono di memoria totale sufficiente, non è possibile aumentare il valore Metadata Reserved Space (spazio riservato metadati). Non continuare con questa procedura.
      - Se ciascun nodo di storage dispone di almeno 128 GB di memoria totale, passare alla fase successiva.

4. Aggiornare l'impostazione Metadata Reserved Space (spazio riservato metadati).

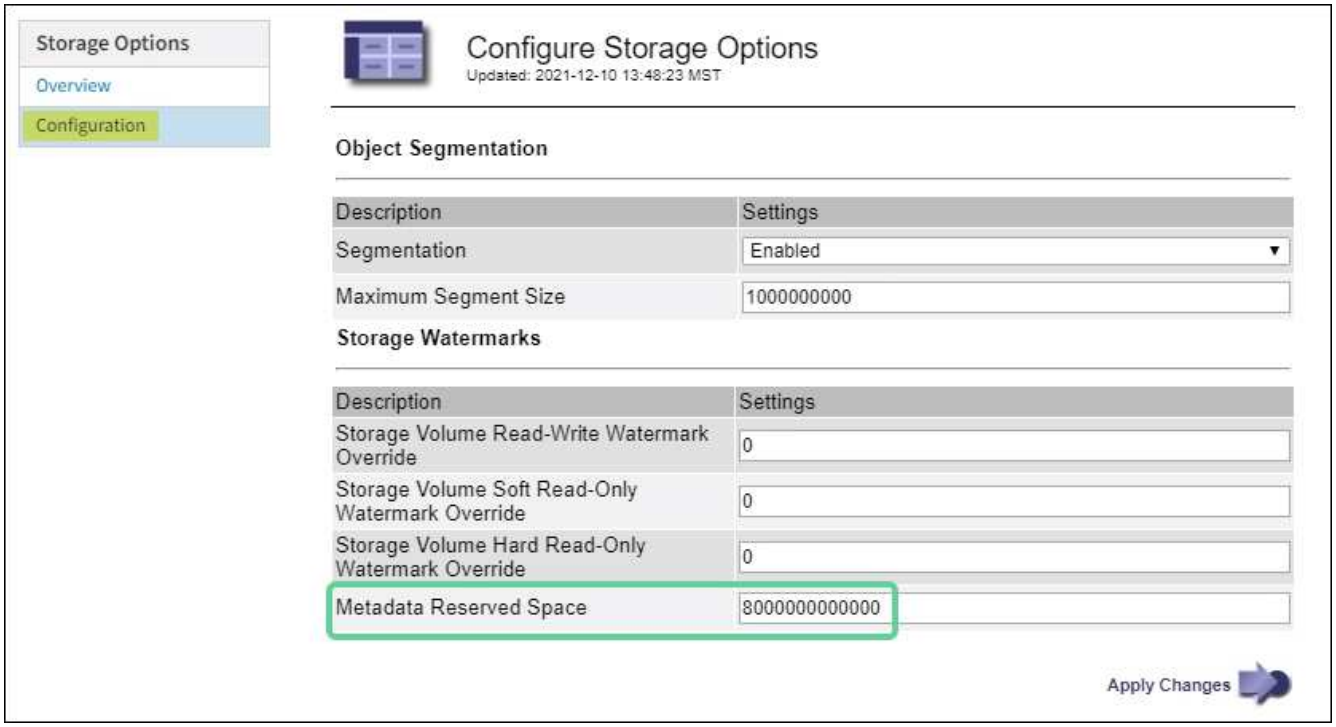
   a. Selezionare **CONFIGURATION** > **System** > **Storage options**.

   b. Selezionare la scheda Configurazione.

   c. Nella sezione Storage Watermarks (Filigrane di archiviazione), selezionare **Metadata Reserved Space** (spazio riservato metadati).

   d. Inserire il nuovo valore.

      Ad esempio, per inserire 8 TB, che è il valore massimo supportato, inserire **8000000000000** (8, seguito da 12 zeri)



a. Selezionare **Applica modifiche**.

Compressione degli oggetti memorizzati

È possibile attivare la compressione degli oggetti per ridurre le dimensioni degli oggetti memorizzati in StorageGRID, in modo che gli oggetti consumino meno spazio di storage.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Per impostazione predefinita, la compressione degli oggetti è disattivata. Se si attiva la compressione, StorageGRID tenta di comprimere ogni oggetto durante il salvataggio, utilizzando la compressione senza perdita di dati.

> Se si modifica questa impostazione, l'applicazione della nuova impostazione richiede circa un minuto. Il valore configurato viene memorizzato nella cache per le prestazioni e la scalabilità.

Prima di attivare la compressione degli oggetti, tenere presente quanto segue:

- Non selezionare **compress stored objects** a meno che non si sappia che i dati memorizzati sono comprimibili.
- Le applicazioni che salvano oggetti in StorageGRID potrebbero comprimere gli oggetti prima di salvarli. Se un'applicazione client ha già compresso un oggetto prima di salvarlo in StorageGRID, selezionando questa opzione non si ridurrà ulteriormente la dimensione di un oggetto.
- Non selezionare **compress stored objects** se si utilizza NetApp FabricPool con StorageGRID.
- Se si seleziona **compress stored objects**, le applicazioni client S3 e Swift devono evitare di eseguire operazioni GetObject che specificano un intervallo di byte da restituire. Queste operazioni di "lettura

dell'intervallo" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. Le operazioni GetObject che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è inefficiente leggere un intervallo di 10 MB da un oggetto compresso da 50 GB.

Se gli intervalli vengono letti da oggetti compressi, le richieste del client possono scadere.

> Se è necessario comprimere gli oggetti e l'applicazione client deve utilizzare le letture dell'intervallo, aumentare il timeout di lettura per l'applicazione.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Impostazioni archiviazione** > **compressione oggetti**.
2. Selezionare la casella di controllo **Comprimi oggetti memorizzati**.
3. Selezionare **Salva**.

Impostazioni di configurazione del nodo di storage

Ogni nodo di storage utilizza diverse impostazioni di configurazione e contatori. Potrebbe essere necessario visualizzare le impostazioni correnti o reimpostare i contatori per cancellare gli allarmi (sistema precedente).

> Ad eccezione di quando espressamente indicato nella documentazione, è necessario consultare il supporto tecnico prima di modificare le impostazioni di configurazione di Storage Node. Se necessario, è possibile reimpostare i contatori degli eventi per cancellare gli allarmi legacy.

Per accedere alle impostazioni di configurazione e ai contatori di un nodo di storage, procedere come segue.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > ***Storage Node***.
3. Espandere il nodo di storage e selezionare il servizio o il componente.
4. Selezionare la scheda **Configurazione**.

Le seguenti tabelle riassumono le impostazioni di configurazione del nodo di storage.

LDR

Nome attributo	Codice	Descrizione
HTTP state (Stato HTTP)	HSTE	Lo stato corrente di HTTP per S3, Swift e altro traffico StorageGRID interno: • Offline: Non sono consentite operazioni e qualsiasi applicazione client che tenta di aprire una sessione HTTP al servizio LDR riceve un messaggio di errore. Le sessioni attive vengono normalmente chiuse. • Online: Il funzionamento continua normalmente

Nome attributo	Codice	Descrizione
Avvio automatico HTTP	HTA	• Se selezionata, lo stato del sistema al riavvio dipende dallo stato del componente **LDR** > **Storage**. Se il componente **LDR** > **Storage** è di sola lettura al riavvio, anche l'interfaccia HTTP è di sola lettura. Se il componente **LDR** > **Storage** è Online, anche HTTP è Online. In caso contrario, l'interfaccia HTTP rimane in stato Offline. • Se l'opzione non è selezionata, l'interfaccia HTTP rimane offline fino a quando non viene attivata esplicitamente.

LDR > Archivio dati

Nome attributo	Codice	Descrizione
Ripristina conteggio oggetti persi	RCOR	Ripristina il contatore per il numero di oggetti persi su questo servizio.

LDR > Storage (Storage)

Nome attributo	Codice	Descrizione
Stato di storage — desiderato	SSD	Un'impostazione configurabile dall'utente per lo stato desiderato del componente di storage. Il servizio LDR legge questo valore e tenta di corrispondere allo stato indicato da questo attributo. Il valore è persistente durante i riavvii. Ad esempio, è possibile utilizzare questa impostazione per forzare lo storage a diventare di sola lettura anche in presenza di ampio spazio di storage disponibile. Questo può essere utile per la risoluzione dei problemi. L'attributo può assumere uno dei seguenti valori: • Offline: Quando lo stato desiderato è offline, il servizio LDR porta il componente **LDR** > **Storage** offline. • Sola lettura: Quando lo stato desiderato è di sola lettura, il servizio LDR sposta lo stato di archiviazione in sola lettura e interrompe l'accettazione del nuovo contenuto. Tuttavia, il servizio LDR continua ad accettare richieste di eliminazione e eliminazione S3 o gestite da ILM. Tenere presente che il contenuto potrebbe continuare a essere salvato nel nodo di storage per un breve periodo di tempo fino alla chiusura delle sessioni aperte. • Online: Lasciare il valore in Online durante le normali operazioni di sistema. Lo stato di storage — corrente del componente di storage viene impostato dinamicamente dal servizio in base alle condizioni del servizio LDR, ad esempio la quantità di spazio di storage a oggetti disponibile. Se lo spazio è basso, il componente diventa di sola lettura.
Timeout controllo stato di salute	STC	Il limite di tempo in secondi entro il quale deve essere completato un test di controllo dello stato di salute per poter considerare un volume di storage integro. Modificare questo valore solo se richiesto dal supporto.

LDR > verifica

Nome attributo	Codice	Descrizione
Ripristina numero oggetti mancanti	VCMI	Ripristina il numero di oggetti mancanti rilevati (OMIS). Utilizzare solo dopo il completamento del controllo dell'esistenza dell'oggetto. I dati degli oggetti replicati mancanti vengono ripristinati automaticamente dal sistema StorageGRID.
Tasso di verifica	VPRI	Imposta la velocità con cui avviene la verifica in background. Vedere le informazioni sulla configurazione della velocità di verifica in background.
Ripristina numero oggetti corrotti	VCCR	Ripristinare il contatore per i dati degli oggetti replicati danneggiati rilevati durante la verifica in background. Questa opzione può essere utilizzata per eliminare la condizione di allarme OCOR (Corrupt Objects Detected).
Elimina oggetti in quarantena	OQRT	Eliminare gli oggetti corrotti dalla directory di quarantena, azzerare il numero di oggetti in quarantena e annullare l'allarme di rilevamento oggetti in quarantena (OQRT). Questa opzione viene utilizzata dopo il ripristino automatico degli oggetti corrotti da parte del sistema StorageGRID. Se viene attivato un allarme oggetti persi, il supporto tecnico potrebbe voler accedere agli oggetti in quarantena. In alcuni casi, gli oggetti in quarantena potrebbero essere utili per il ripristino dei dati o per il debug dei problemi sottostanti che hanno causato le copie degli oggetti corrotte.

LDR > Erasure coding (codifica cancellazione)

Nome attributo	Codice	Descrizione
Azzera conteggio errori di scrittura	RSWF	Reimpostare il contatore per gli errori di scrittura dei dati degli oggetti con codifica erasure sul nodo di storage.
Il ripristino legge il numero di errori	RSRF	Reimpostare il contatore per gli errori di lettura dei dati degli oggetti con codifica erasure dal nodo di storage.
Ripristina Elimina numero di errori	RSDF	Reimpostare il contatore per gli errori di eliminazione dei dati degli oggetti con codifica erasure dal nodo di storage.

Nome attributo	Codice	Descrizione
Ripristina numero copie corrotte rilevate	RSCC	Reimpostare il contatore per il numero di copie corrotte dei dati degli oggetti con codifica di cancellazione sul nodo di storage.
Ripristina numero di frammenti corrotti rilevati	RSCD	Reimpostare il contatore per i frammenti corrotti di dati di oggetti con codifica di cancellazione sul nodo di storage.
Ripristina numero frammenti mancanti rilevati	RSMD	Reimpostare il contatore per i frammenti mancanti di dati di oggetti con codifica di cancellazione sul nodo di storage. Utilizzare solo dopo il completamento del controllo dell'esistenza dell'oggetto.

LDR > Replica

Nome attributo	Codice	Descrizione
Ripristina conteggio errori replica in entrata	RIC	Reimpostare il contatore per gli errori di replica in entrata. Questa opzione può essere utilizzata per cancellare l'allarme RIRF (Inbound Replication — Failed).
Ripristina conteggio errori replica in uscita	ROCR	Reimpostare il contatore per gli errori di replica in uscita. Questa opzione può essere utilizzata per cancellare l'allarme RORF (Outbound Replications — Failed).
Disattiva replica in entrata	DSIR	Selezionare questa opzione per disattivare la replica in entrata come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento. Quando la replica in entrata è disattivata, gli oggetti possono essere recuperati dal nodo di storage per la copia in altre posizioni nel sistema StorageGRID, ma gli oggetti non possono essere copiati in questo nodo di storage da altre posizioni: Il servizio LDR è di sola lettura.

Nome attributo	Codice	Descrizione
Disattiva la replica in uscita	DSOR	Selezionare questa opzione per disattivare la replica in uscita (incluse le richieste di contenuto per i retrievals HTTP) come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento. Quando la replica in uscita è disattivata, gli oggetti possono essere copiati in questo nodo di storage, ma gli oggetti non possono essere recuperati dal nodo di storage per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio LDR è di sola scrittura.

Gestire nodi storage completi

Man mano che i nodi di storage raggiungono la capacità, è necessario espandere il sistema StorageGRID con l'aggiunta di nuovo storage. Sono disponibili tre opzioni: Aggiunta di volumi di storage, aggiunta di shelf di espansione dello storage e aggiunta di nodi di storage.

Aggiungere volumi di storage

Ciascun nodo di storage supporta un numero massimo di volumi di storage. Il valore massimo definito varia in base alla piattaforma. Se un nodo di storage contiene meno del numero massimo di volumi di storage, è possibile aggiungere volumi per aumentarne la capacità. Consultare le istruzioni per "Espansione di un sistema StorageGRID".

Aggiungere shelf di espansione dello storage

Alcuni nodi di storage delle appliance StorageGRID, come SG6060 o SG6160, sono in grado di supportare shelf di storage aggiuntivi. Se si dispone di appliance StorageGRID con funzionalità di espansione che non sono già state estese alla capacità massima, è possibile aggiungere shelf di storage per aumentare la capacità. Consultare le istruzioni per "Espansione di un sistema StorageGRID".

Aggiungere nodi storage

È possibile aumentare la capacità dello storage aggiungendo nodi di storage. Quando si aggiunge lo storage, è necessario prendere in considerazione le regole ILM attualmente attive e i requisiti di capacità. Consultare le istruzioni per "Espansione di un sistema StorageGRID".

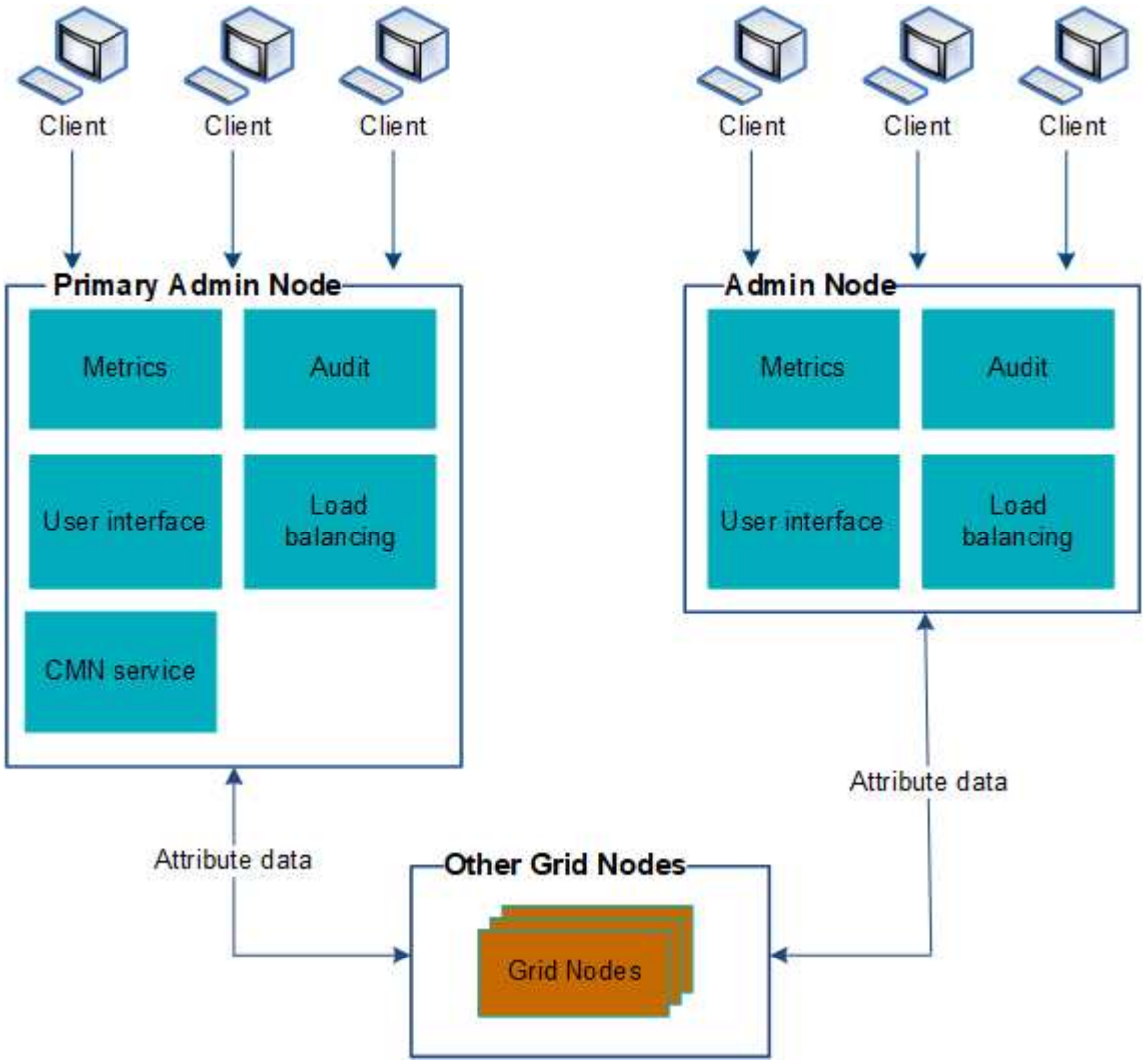
Gestire i nodi di amministrazione

Utilizzare più nodi di amministrazione

Un sistema StorageGRID può includere più nodi di amministrazione per consentire di monitorare e configurare continuamente il sistema StorageGRID anche in caso di guasto di un nodo di amministrazione.

Se un nodo amministrativo non è disponibile, l'elaborazione degli attributi continua, gli avvisi e gli allarmi

(sistema legacy) vengono ancora attivati e le notifiche e-mail e i pacchetti AutoSupport vengono ancora inviati. Tuttavia, la disponibilità di più nodi amministrativi non fornisce protezione dal failover, ad eccezione delle notifiche e dei pacchetti AutoSupport. In particolare, le conferme di allarme effettuate da un nodo di amministrazione non vengono copiate in altri nodi di amministrazione.



Sono disponibili due opzioni per continuare a visualizzare e configurare il sistema StorageGRID in caso di errore di un nodo di amministrazione:

- I client Web possono riconnettersi a qualsiasi altro nodo Admin disponibile.
- Se un amministratore di sistema ha configurato un gruppo di nodi di amministrazione ad alta disponibilità, i client Web possono continuare ad accedere a Grid Manager o a Tenant Manager utilizzando l'indirizzo IP virtuale del gruppo ha. Vedere "Gestire i gruppi ad alta disponibilità".

> Quando si utilizza un gruppo ha, l'accesso viene interrotto in caso di errore del nodo Admin attivo. Gli utenti devono effettuare nuovamente l'accesso dopo il failover dell'indirizzo IP virtuale del gruppo ha verso un altro nodo amministratore del gruppo.

Alcune attività di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario. In caso di guasto del nodo amministratore primario, è necessario ripristinarlo prima che il sistema StorageGRID funzioni nuovamente.

Identificare il nodo di amministrazione principale

Il nodo di amministrazione primario ospita il servizio CMN. Alcune procedure di manutenzione possono essere eseguite solo utilizzando il nodo di amministrazione primario.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Site*** > **Admin Node**, quindi scegliere ➕ Per espandere la struttura della topologia e mostrare i servizi ospitati su questo nodo di amministrazione.

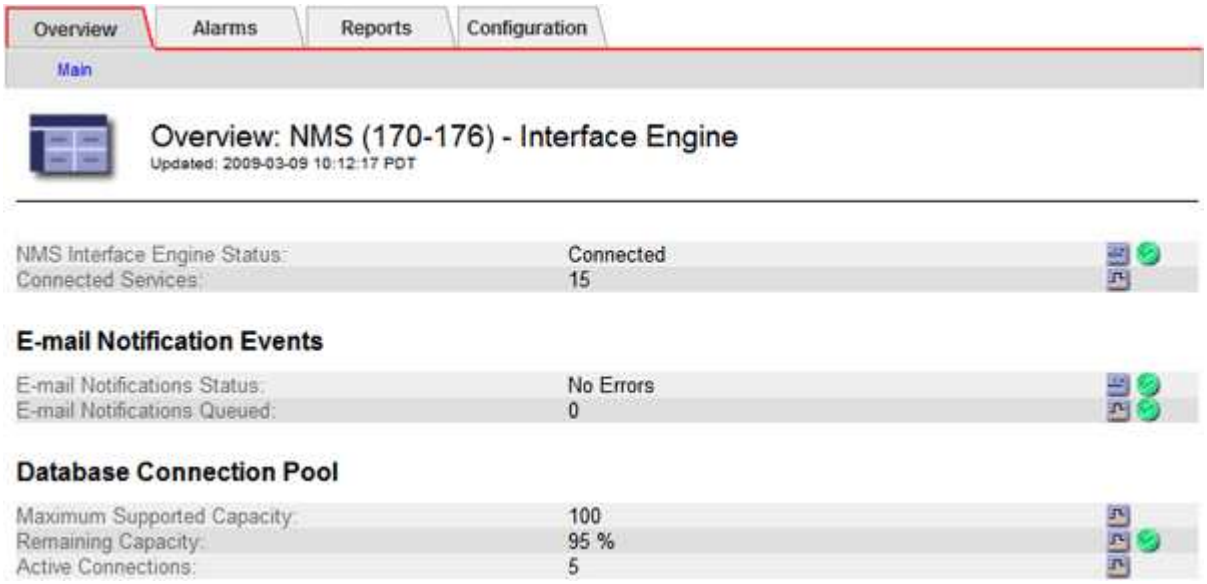
   Il nodo di amministrazione primario ospita il servizio CMN.

3. Se questo nodo di amministrazione non ospita il servizio CMN, controllare gli altri nodi di amministrazione.

Visualizzare lo stato delle notifiche e le code

Il servizio NMS (Network Management System) sui nodi di amministrazione invia notifiche al server di posta. È possibile visualizzare lo stato corrente del servizio NMS e le dimensioni della relativa coda di notifica nella pagina motore interfaccia.

Per accedere alla pagina Interface Engine, selezionare **SUPPORT** > **Tools** > **Grid topology**. Infine, selezionare ***Site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



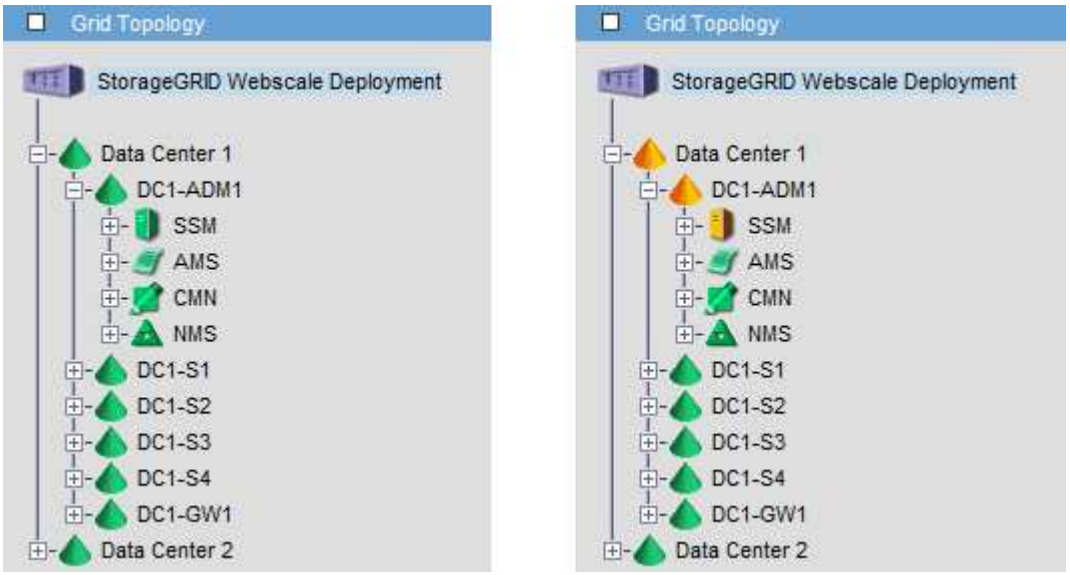
Le notifiche vengono elaborate tramite la coda di notifica e-mail e inviate al server di posta una dopo l'altra nell'ordine in cui vengono attivate. Se si verifica un problema (ad esempio, un errore di connessione di rete) e il server di posta non è disponibile quando si tenta di inviare la notifica, il tentativo più efficace di inviare nuovamente la notifica al server di posta continua per un periodo di 60 secondi. Se la notifica non viene inviata al server di posta dopo 60 secondi, la notifica viene interrotta dalla coda di notifica e viene eseguito un tentativo di invio della notifica successiva nella coda.

Poiché le notifiche possono essere interrotte dalla coda delle notifiche senza essere inviate, è possibile che un allarme possa essere attivato senza l'invio di una notifica. Se una notifica viene interrotta dalla coda senza essere inviata, viene attivato l'allarme minore MINUTI (Stato notifica e-mail).

Modalità di visualizzazione degli allarmi riconosciuti da Admin Node (sistema legacy)

Quando si riconosce un allarme su un nodo di amministrazione, l'allarme confermato non viene copiato in nessun altro nodo di amministrazione. Poiché i riconoscimenti non vengono copiati in altri nodi di amministrazione, l'albero topologia griglia potrebbe non avere lo stesso aspetto per ciascun nodo di amministrazione.

Questa differenza può essere utile quando si connettono client web. I client Web possono avere viste diverse del sistema StorageGRID in base alle esigenze dell'amministratore.



Si noti che le notifiche vengono inviate dal nodo di amministrazione in cui si verifica la conferma.

Configurare l'accesso al client di audit

Configurare l'accesso client di audit per NFS

Il nodo di amministrazione, tramite il servizio Audit Management System (AMS), registra tutti gli eventi di sistema controllati in un file di registro disponibile attraverso la condivisione dell'audit, che viene aggiunto a ciascun nodo di amministrazione al momento dell'installazione. La condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

Il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

Per accedere ai registri di audit, è possibile configurare l'accesso client per controllare le condivisioni per NFS. In alternativa, è possibile "utilizzare un server syslog esterno".

Il sistema StorageGRID utilizza il riconoscimento positivo per impedire la perdita dei messaggi di audit prima che vengano scritti nel file di log. Un messaggio rimane in coda in un servizio fino a quando il servizio AMS o

un servizio di inoltro di audit intermedio non ne ha riconosciuto il controllo. Per ulteriori informazioni, vedere "Esaminare i registri di audit".

Prima di iniziare

- Hai il `Passwords.txt` file con la password root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).
- Il client di audit utilizza NFS versione 3 (NFSv3).

A proposito di questa attività

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Verificare che tutti i servizi abbiano uno stato di esecuzione o verificato. Inserire: `storagegrid-status`

   Se alcuni servizi non sono elencati come in esecuzione o verificati, risolvere i problemi prima di continuare.

3. Tornare alla riga di comando. Premere **Ctrl+C**.
4. Avviare l'utility di configurazione NFS. Inserire: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

5. Aggiungere il client di audit: `add-audit-share`
   a. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: `client_IP_address`
   b. Quando richiesto, premere **Invio**.
6. Se più di un client di audit è autorizzato ad accedere alla condivisione di audit, aggiungere l'indirizzo IP dell'utente aggiuntivo: `add-ip-to-share`
   a. Inserire il numero della condivisione di controllo: *`audit_share_number`*

b. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: *client_IP_address*

c. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione NFS.

d. Ripetere questi passaggi secondari per ogni client di audit aggiuntivo che ha accesso alla condivisione di audit.

7. Se si desidera, verificare la configurazione.

   a. Immettere quanto segue: `validate-config`

      I servizi vengono controllati e visualizzati.

   b. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione NFS.

   c. Chiudere l'utility di configurazione NFS: `exit`

8. Determinare se è necessario abilitare le condivisioni di audit in altri siti.
   - Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.
   - Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare queste condivisioni di controllo come richiesto:
     i. Accedere in remoto al nodo Admin del sito:
        A. Immettere il seguente comando: `ssh admin@grid_node_IP`
        B. Immettere la password elencata in `Passwords.txt` file.
        C. Immettere il seguente comando per passare a root: `su -`
        D. Immettere la password elencata in `Passwords.txt` file.
     ii. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.
     iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto. Inserire: `exit`

9. Disconnettersi dalla shell dei comandi: `exit`

   Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di controllo a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione oppure rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Aggiungere un client di audit NFS a una condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. Concedere l'accesso alla condivisione di audit a un nuovo client di audit NFS aggiungendo il proprio indirizzo IP alla condivisione di audit.

Il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

Prima di iniziare

- Hai il `Passwords.txt` file con la password dell'account root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).
- Il client di audit utilizza NFS versione 3 (NFSv3).

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@`*`primary_Admin_Node_IP`*
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Inserire: `add-ip-to-share`

   Viene visualizzato un elenco di condivisioni di controllo NFS attivate nel nodo di amministrazione. La condivisione dell'audit è elencata come: `/var/local/log`

4. Inserire il numero della condivisione di controllo: *`audit_share_number`*
5. Quando richiesto, inserire l'indirizzo IP o l'intervallo di indirizzi IP del client di controllo per la condivisione di controllo: *`client_IP_address`*

   Il client di audit viene aggiunto alla condivisione di audit.

6. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione NFS.

7. Ripetere i passaggi per ogni client di audit da aggiungere alla condivisione di audit.
8. In alternativa, verificare la configurazione: `validate-config`

   I servizi vengono controllati e visualizzati.

   a. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione NFS.

9. Chiudere l'utility di configurazione NFS: `exit`
10. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

    In caso contrario, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare facoltativamente queste condivisioni di controllo come richiesto:

    a. Accedere in remoto al nodo di amministrazione di un sito:
        i. Immettere il seguente comando: `ssh admin@grid_node_IP`
        ii. Immettere la password elencata in `Passwords.txt` file.
        iii. Immettere il seguente comando per passare a root: `su -`
        iv. Immettere la password elencata in `Passwords.txt` file.
    b. Ripetere questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
    c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
11. Disconnettersi dalla shell dei comandi: `exit`

Verificare l'integrazione dell'audit NFS

Dopo aver configurato una condivisione di audit e aggiunto un client di audit NFS, è possibile montare la condivisione del client di audit e verificare che i file siano disponibili dalla condivisione di audit.

> Il supporto per NFS è stato obsoleto e verrà rimosso in una versione futura.

Fasi

1. Verificare la connettività (o la variante per il sistema client) utilizzando l'indirizzo IP lato client del nodo di amministrazione che ospita il servizio AMS. Inserire: `ping IP_address`

   Verificare che il server risponda, indicando la connettività.

2. Montare la condivisione di sola lettura dell'audit utilizzando un comando appropriato per il sistema operativo del client. Un esempio di comando Linux è (invio su una riga):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/log myAudit`

   Utilizzare l'indirizzo IP del nodo di amministrazione che ospita il servizio AMS e il nome di condivisione predefinito per il sistema di audit. Il punto di montaggio può essere qualsiasi nome selezionato dal client (ad esempio, *`myAudit`* nel comando precedente).

3. Verificare che i file siano disponibili dalla condivisione dell'audit. Inserire: `ls myAudit /*`

   dove *`myAudit`* è il punto di montaggio della condivisione dell'audit. Dovrebbe essere presente almeno un file di log.

Rimuovere un client di audit NFS dalla condivisione di audit

Ai client di audit NFS viene concesso l'accesso a una condivisione di audit in base al proprio indirizzo IP. È possibile rimuovere un client di audit esistente rimuovendo il relativo indirizzo IP.

Prima di iniziare

- Hai il `Passwords.txt` file con la password dell'account root/admin.
- Hai il `Configuration.txt` File (disponibile nel pacchetto di ripristino).

A proposito di questa attività

Non è possibile rimuovere l'ultimo indirizzo IP consentito per accedere alla condivisione dell'audit.

Fasi

1. Accedere al nodo di amministrazione principale:
   a. Immettere il seguente comando: `ssh admin@primary_Admin_Node_IP`
   b. Immettere la password elencata in `Passwords.txt` file.
   c. Immettere il seguente comando per passare a root: `su -`
   d. Immettere la password elencata in `Passwords.txt` file.

   Una volta effettuato l'accesso come root, il prompt cambia da `$` a. `#`.

2. Avviare l'utility di configurazione NFS: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Rimuovere l'indirizzo IP dalla condivisione dell'audit: `remove-ip-from-share`

   Viene visualizzato un elenco numerato di condivisioni di controllo configurate sul server. La condivisione dell'audit è elencata come: `/var/local/log`

4. Inserire il numero corrispondente alla condivisione di audit: *`audit_share_number`*

   Viene visualizzato un elenco numerato di indirizzi IP autorizzati ad accedere alla condivisione dell'audit.

5. Inserire il numero corrispondente all'indirizzo IP che si desidera rimuovere.

   La condivisione di audit viene aggiornata e l'accesso non è più consentito da alcun client di audit con questo indirizzo IP.

6. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione NFS.

7. Chiudere l'utility di configurazione NFS: `exit`
8. Se l'implementazione di StorageGRID è un'implementazione di più siti di data center con nodi amministrativi aggiuntivi negli altri siti, disattivare queste condivisioni di controllo secondo necessità:
   a. Accedere in remoto al nodo di amministrazione di ciascun sito:
      i. Immettere il seguente comando: `ssh admin@grid_node_IP`
      ii. Immettere la password elencata in `Passwords.txt` file.
      iii. Immettere il seguente comando per passare a root: `su -`
      iv. Immettere la password elencata in `Passwords.txt` file.
   b. Ripetere questi passaggi per configurare le condivisioni di controllo per ogni nodo amministrativo aggiuntivo.
   c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
9. Disconnettersi dalla shell dei comandi: `exit`

Modificare l'indirizzo IP di un client di audit NFS

Se si desidera modificare l'indirizzo IP di un client di audit NFS, attenersi alla procedura descritta di seguito.

Fasi

1. Aggiungere un nuovo indirizzo IP a una condivisione di audit NFS esistente.
2. Rimuovere l'indirizzo IP originale.

Informazioni correlate

- "Aggiungere un client di audit NFS a una condivisione di audit"
- "Rimuovere un client di audit NFS dalla condivisione di audit"

Gestire i nodi di archiviazione

Archiviazione nel cloud tramite l'API S3

È possibile configurare un nodo di archiviazione per la connessione diretta ai servizi Web Amazon o a qualsiasi altro sistema in grado di interfacciarsi con il sistema StorageGRID tramite l'API S3.

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

Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.

Inoltre, è necessario rimuovere i nodi di archiviazione dal criterio ILM attivo in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

Configurare le impostazioni di connessione per l'API S3

Se si sta effettuando la connessione a un nodo di archiviazione utilizzando l'interfaccia S3, è necessario configurare le impostazioni di connessione per l'API S3. Fino a quando queste impostazioni non vengono configurate, il servizio ARC rimane in uno stato di allarme principale in quanto non è in grado di comunicare con il sistema di storage di archiviazione esterno.

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

Anche l'opzione Cloud Tiering - Simple Storage Service (S3) è obsoleta. Se si utilizza attualmente un nodo di archiviazione con questa opzione, "Migrare gli oggetti in un pool di storage cloud" invece.

Inoltre, è necessario rimuovere i nodi di archiviazione dal criterio ILM attivo in StorageGRID 11,7 o versioni precedenti. La rimozione dei dati degli oggetti memorizzati nei nodi di archiviazione semplificherà gli aggiornamenti futuri. Vedere "Utilizzo delle regole ILM e delle policy ILM".

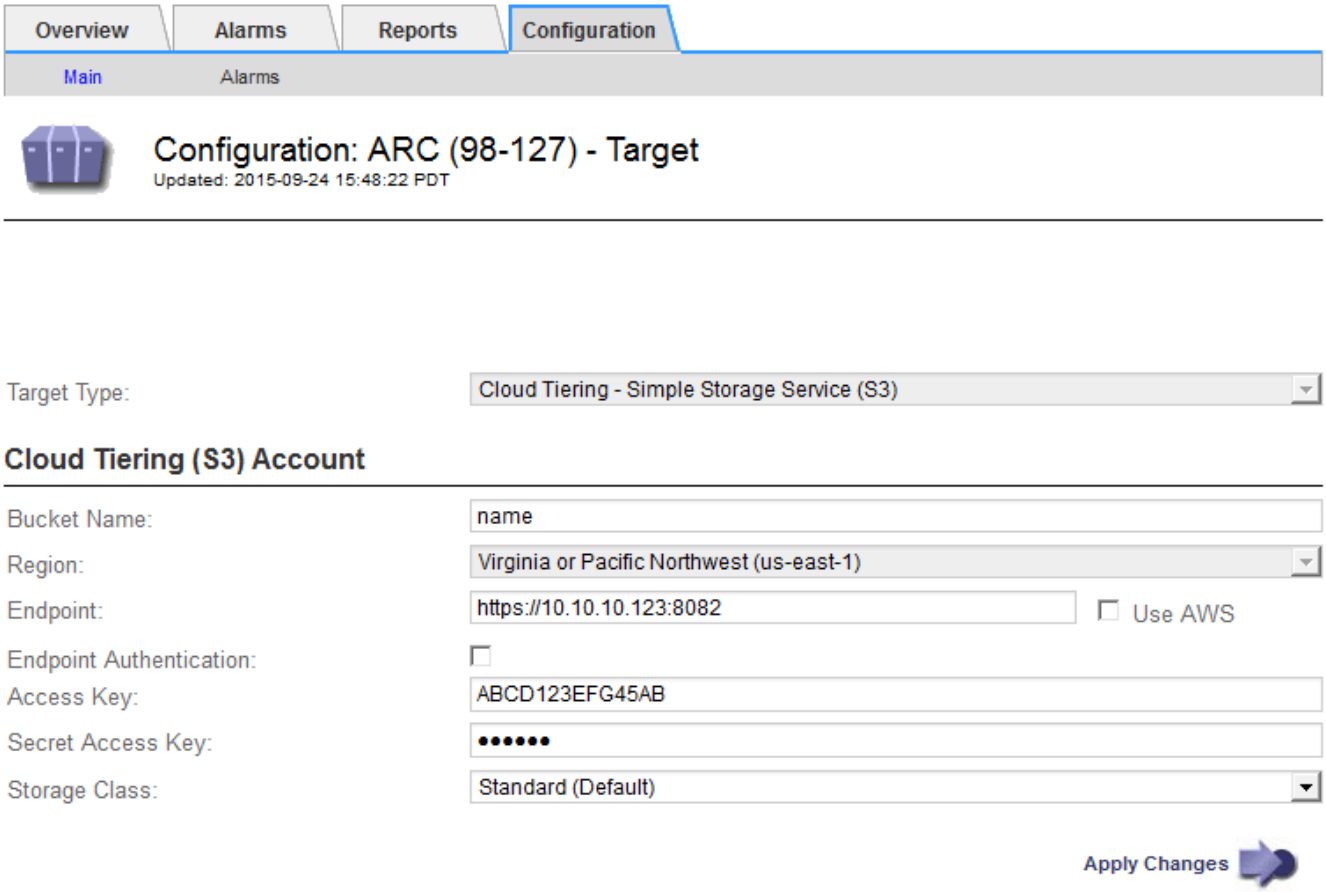
Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai creato un bucket sul sistema storage di archiviazione di destinazione:
  - Il bucket è dedicato a un singolo nodo di archiviazione. Non può essere utilizzato da altri nodi di archiviazione o altre applicazioni.
  - Nel bucket è stata selezionata la regione appropriata per la propria posizione.
  - Il bucket deve essere configurato con la versione sospesa.
- La segmentazione degli oggetti è attivata e la dimensione massima dei segmenti è inferiore o uguale a 4.5 GiB (4,831,838,208 byte). Le richieste API S3 che superano questo valore non avranno esito positivo se S3 viene utilizzato come sistema di storage di archiviazione esterno.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.

2. Selezionare **Archive Node** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.



4. Selezionare **Cloud Tiering - Simple Storage Service (S3)** dall'elenco a discesa Target Type (tipo di destinazione).

> Le impostazioni di configurazione non sono disponibili fino a quando non si seleziona un tipo di destinazione.

5. Configurare l'account di cloud tiering (S3) attraverso il quale il nodo di archiviazione si connetterà al sistema di archiviazione esterno di destinazione in grado di supportare S3.

   La maggior parte dei campi di questa pagina sono esplicativi. Di seguito vengono descritti i campi per i quali potrebbe essere necessario fornire assistenza.

   - **Regione**: Disponibile solo se è selezionato **Usa AWS**. La regione selezionata deve corrispondere a quella del bucket.
   - **Endpoint** e **Use AWS**: Per Amazon Web Services (AWS), selezionare **Use AWS**. **Endpoint** viene quindi compilato automaticamente con un URL dell'endpoint in base agli attributi Bucket Name e Region. Ad esempio:

     ```
     https://bucket.region.amazonaws.com
     ```

     Per una destinazione non AWS, inserire l'URL del sistema che ospita il bucket, incluso il numero di porta. Ad esempio:

`https://system.com:1080`

- **End Point Authentication**: Attivato per impostazione predefinita. Se la rete verso il sistema di storage di archiviazione esterno è attendibile, deselezionare la casella di controllo per disattivare la verifica del certificato SSL dell'endpoint e del nome host per il sistema di storage di archiviazione esterno di destinazione. Se un'altra istanza di un sistema StorageGRID è il dispositivo di archiviazione di destinazione e il sistema è configurato con certificati firmati pubblicamente, è possibile mantenere la casella di controllo selezionata.
- **Storage Class** (Classe di storage): Selezionare **Standard (predefinito)** per lo storage normale. Selezionare **Redundancy ridotta** solo per gli oggetti che possono essere ricreati facilmente. **Redundancy ridotta** offre storage a costi inferiori con minore affidabilità. Se il sistema storage di archiviazione di destinazione è un'altra istanza del sistema StorageGRID, **Classe storage** controlla quante copie intermedie dell'oggetto vengono eseguite al momento dell'acquisizione nel sistema di destinazione, se viene utilizzato il doppio commit quando vengono acquisiti oggetti.

6. Selezionare **Applica modifiche**.

   Le impostazioni di configurazione specificate vengono validate e applicate al sistema StorageGRID. Una volta applicate le impostazioni, il target non può essere modificato.

Modificare le impostazioni di connessione per l'API S3

Una volta configurato il nodo di archiviazione per la connessione a un sistema di archiviazione esterno tramite l'API S3, è possibile modificare alcune impostazioni in caso di modifica della connessione.

Prima di iniziare

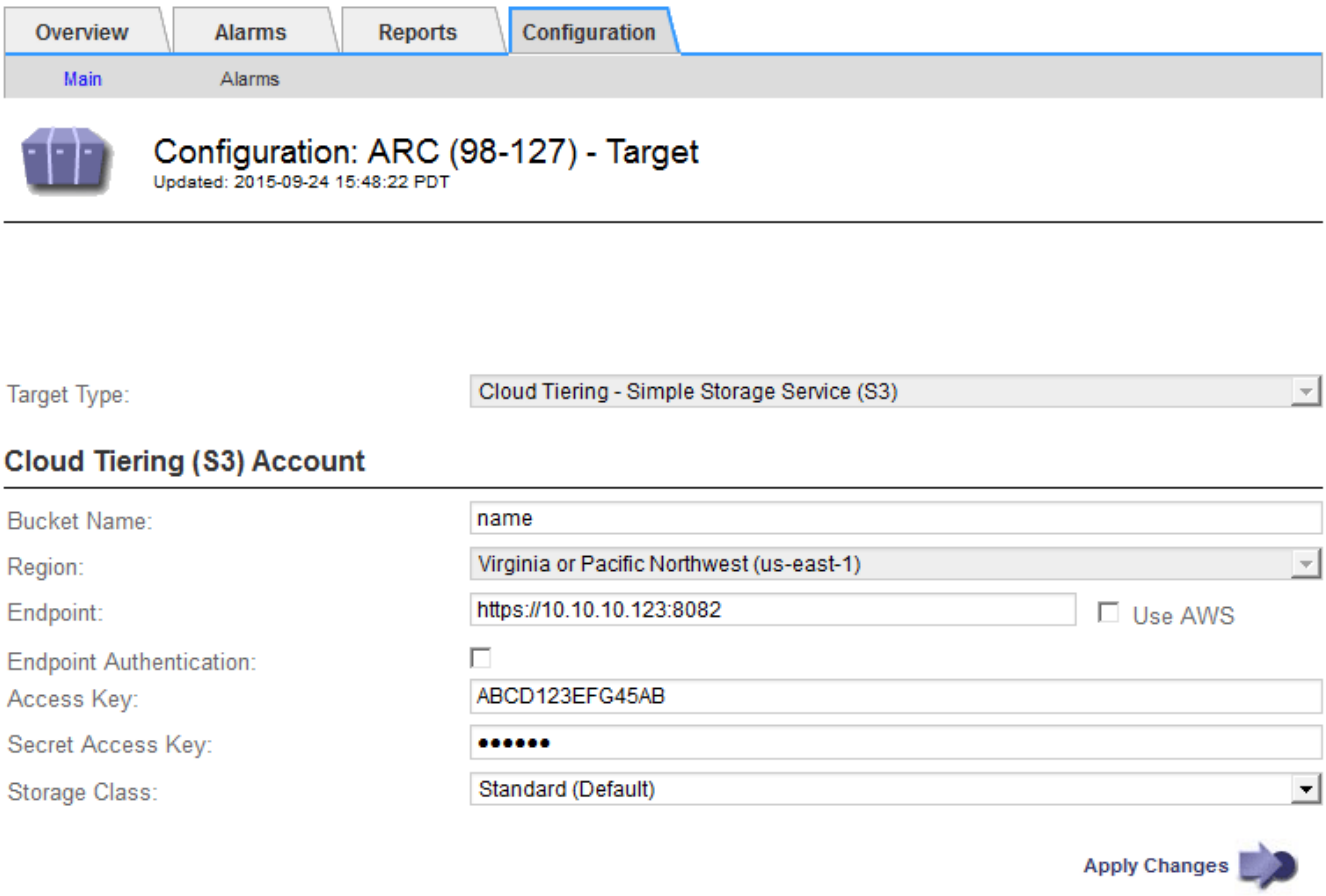
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Se si modifica l'account Cloud Tiering (S3), è necessario assicurarsi che le credenziali di accesso dell'utente abbiano accesso in lettura/scrittura al bucket, inclusi tutti gli oggetti precedentemente acquisiti dal nodo di archiviazione nel bucket.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le informazioni dell'account, se necessario.

   Se si modifica la classe di storage, i nuovi dati dell'oggetto vengono memorizzati con la nuova classe di storage. L'oggetto esistente continua ad essere memorizzato nella classe di storage impostata al momento dell'acquisizione.

   Nome bucket, regione ed endpoint, utilizza i valori AWS e non può essere modificato.

5. Selezionare **Applica modifiche**.

Modificare lo stato del Cloud Tiering Service

È possibile controllare la capacità di lettura e scrittura del nodo di archiviazione nel sistema storage di archiviazione esterno di destinazione che si connette attraverso l'API S3 modificando lo stato del servizio di tiering cloud.

Prima di iniziare

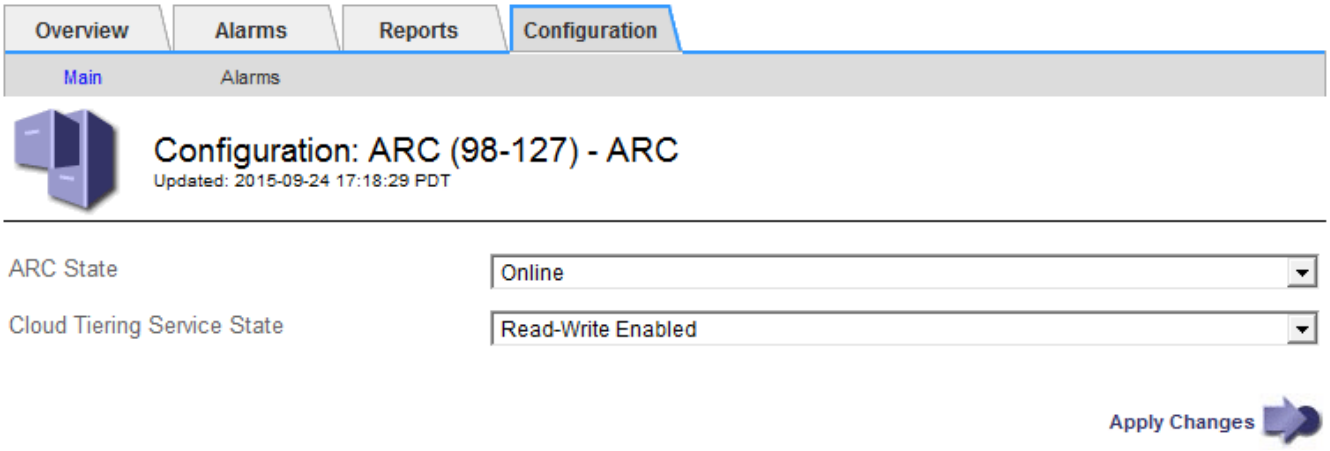
- È necessario accedere a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Il nodo di archiviazione deve essere configurato.

A proposito di questa attività

È possibile disattivare il nodo di archiviazione modificando lo stato del servizio di tiering cloud in **Read-Write Disabled**.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC**.
3. Selezionare **Configurazione** > **principale**.



4. Selezionare un **Cloud Tiering Service state**.
5. Selezionare **Applica modifiche**.

Ripristinare il numero di errori di archiviazione per la connessione API S3

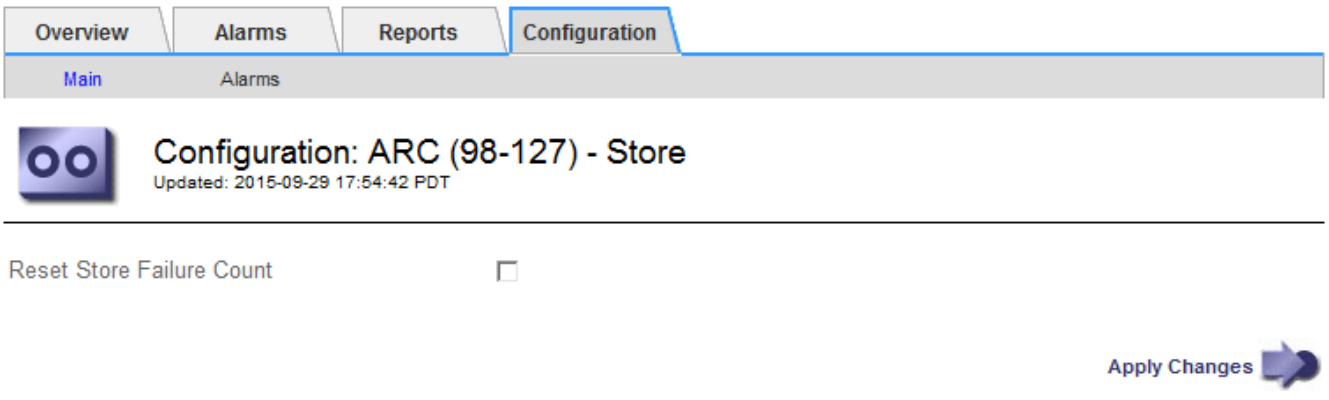
Se il nodo di archiviazione si connette a un sistema di storage di archiviazione tramite l'API S3, è possibile reimpostare il numero di errori di archiviazione, che può essere utilizzato per cancellare l'allarme ARVF (Store Failures).

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Store**.
3. Selezionare **Configurazione** > **principale**.



4. Selezionare **Reset Store Failure Count**.

5. Selezionare **Applica modifiche**.

   L'attributo Store Failures viene reimpostato su zero.

Migrazione di oggetti da Cloud Tiering - S3 a un Cloud Storage Pool

Se attualmente si utilizza la funzionalità **Cloud Tiering - Simple Storage Service (S3)** per tierare i dati degli oggetti in un bucket S3, è necessario migrare gli oggetti in un Cloud Storage Pool. I pool di cloud storage offrono un approccio scalabile che sfrutta tutti i nodi di storage nel sistema StorageGRID.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".
- Hai già memorizzato oggetti nel bucket S3 configurato per il Cloud Tiering.

> Prima di migrare i dati degli oggetti, contatta il tuo rappresentante NetApp per conoscere e gestire i costi associati.

A proposito di questa attività

Dal punto di vista di ILM, un pool di storage cloud è simile a un pool di storage. Tuttavia, mentre i pool di storage sono costituiti da nodi di storage o nodi di archiviazione all'interno del sistema StorageGRID, un pool di storage cloud è costituito da un bucket S3 esterno.

Prima di migrare gli oggetti da Tier cloud - S3 a un pool di storage cloud, è necessario prima creare un bucket S3 e poi creare il pool di storage cloud in StorageGRID. Quindi, è possibile creare un nuovo criterio ILM e sostituire la regola ILM utilizzata per memorizzare gli oggetti nel bucket Cloud Tiering con una regola ILM clonata che memorizza gli stessi oggetti nel Cloud Storage Pool.

> Quando gli oggetti vengono memorizzati in un pool di storage cloud, le copie di tali oggetti non possono essere memorizzate anche in StorageGRID. Se la regola ILM attualmente in uso per il Cloud Tiering è configurata per memorizzare oggetti in più posizioni contemporaneamente, considerare se si desidera eseguire questa migrazione facoltativa perché si perde tale funzionalità. Se si continua con questa migrazione, è necessario creare nuove regole invece di clonare quelle esistenti.

Fasi

1. Creare un pool di storage cloud.

   Utilizza un nuovo bucket S3 per il Cloud Storage Pool per garantire che contenga solo i dati gestiti dal Cloud Storage Pool.

2. Individuare eventuali regole ILM nelle policy ILM attive che causano l'archiviazione degli oggetti nel bucket Cloud Tiering.
3. Clonare ciascuna di queste regole.
4. Nelle regole clonate, modificare la posizione di posizionamento nel nuovo Cloud Storage Pool.
5. Salvare le regole clonate.
6. Creare una nuova policy che utilizzi le nuove regole.

7. Simulare e attivare la nuova policy.

   Quando la nuova policy viene attivata e si verifica la valutazione ILM, gli oggetti vengono spostati dal bucket S3 configurato per il Cloud Tiering al bucket S3 configurato per il Cloud Storage Pool. Lo spazio utilizzabile sulla griglia non viene compromesso. Una volta spostati nel Cloud Storage Pool, gli oggetti vengono rimossi dal bucket Cloud Tiering.

Informazioni correlate

"Gestire gli oggetti con ILM"

Archiviazione su nastro tramite middleware TSM

È possibile configurare un nodo di archiviazione in modo che utilizzi un server Tivoli Storage Manager (TSM) che fornisce un'interfaccia logica per l'archiviazione e il recupero dei dati degli oggetti su dispositivi di storage ad accesso casuale o sequenziale, incluse le librerie su nastro.

Il servizio ARC del nodo di archiviazione agisce come client per il server TSM, utilizzando Tivoli Storage Manager come middleware per la comunicazione con il sistema di storage di archiviazione.

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

Classi di gestione TSM

Le classi di gestione definite dal middleware TSM delineano il funzionamento delle operazioni di backup e archiviazione di TSM's e possono essere utilizzate per specificare le regole per il contenuto che vengono applicate dal server TSM. Tali regole funzionano indipendentemente dalla policy ILM del sistema StorageGRID e devono essere coerenti con il requisito del sistema StorageGRID che gli oggetti siano memorizzati in modo permanente e siano sempre disponibili per il recupero da parte del nodo di archiviazione. Dopo che i dati dell'oggetto sono stati inviati a un server TSM dal nodo di archiviazione, il ciclo di vita del TSM e le regole di conservazione vengono applicati mentre i dati dell'oggetto vengono memorizzati sul nastro gestito dal server TSM.

La classe di gestione TSM viene utilizzata dal server TSM per applicare regole per la posizione o la conservazione dei dati dopo che gli oggetti sono stati inviati al server TSM dal nodo di archiviazione. Ad esempio, gli oggetti identificati come backup del database (contenuto temporaneo che può essere sovrascritto con dati più recenti) potrebbero essere trattati in modo diverso rispetto ai dati dell'applicazione (contenuto fisso che deve essere conservato a tempo indeterminato).

Configurare le connessioni al middleware TSM

Prima che il nodo di archiviazione possa comunicare con il middleware Tivoli Storage Manager (TSM), è necessario configurare diverse impostazioni.

Prima di iniziare

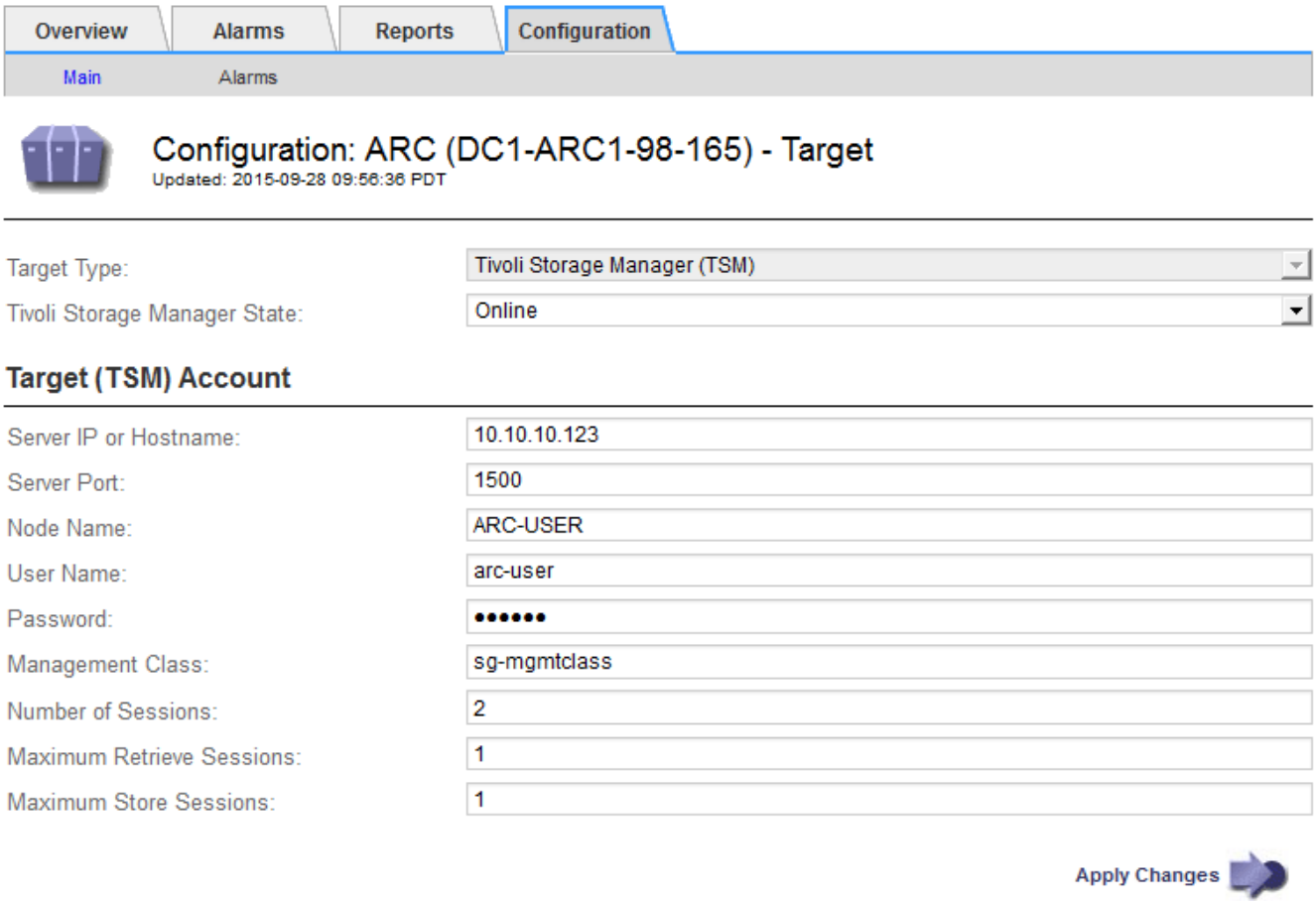
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

Fino a quando queste impostazioni non vengono configurate, il servizio ARC rimane in uno stato di allarme principale in quanto non è in grado di comunicare con Tivoli Storage Manager.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.



4. Dall'elenco a discesa **Target Type** (tipo di destinazione), selezionare **Tivoli Storage Manager (TSM)**.
5. Per lo stato di **Tivoli Storage Manager**, selezionare **Offline** per impedire il recupero dal server middleware TSM.

   Per impostazione predefinita, lo stato di Tivoli Storage Manager è impostato su Online, il che significa che il nodo di archiviazione è in grado di recuperare i dati degli oggetti dal server middleware TSM.

6. Completare le seguenti informazioni:

   - **Server IP (IP server) o Hostname (Nome host)**: Specificare l'indirizzo IP o il nome di dominio completo del server middleware TSM utilizzato dal servizio ARC. L'indirizzo IP predefinito è 127.0.0.1.
   - **Server Port** (porta server): Specificare il numero di porta sul server middleware TSM a cui si connetterà il servizio ARC. Il valore predefinito è 1500.
   - **Node Name** (Nome nodo): Specificare il nome del nodo di archiviazione. Immettere il nome (arco -utente) registrato sul server middleware TSM.
   - **User Name** (Nome utente): Specificare il nome utente utilizzato dal servizio ARC per accedere al server TSM. Immettere il nome utente predefinito (Arc-user) o l'utente amministrativo specificato per il nodo di archiviazione.
   - **Password**: Specificare la password utilizzata dal servizio ARC per accedere al server TSM.
   - **Classe di gestione**: Specificare la classe di gestione predefinita da utilizzare se non viene specificata una classe di gestione quando l'oggetto viene salvato nel sistema StorageGRID o se la classe di gestione specificata non viene definita nel server middleware TSM.
   - **Numero di sessioni**: Specificare il numero di unità nastro sul server middleware TSM dedicate al nodo di archiviazione. Il nodo di archiviazione crea contemporaneamente un massimo di una sessione per punto di montaggio più un piccolo numero di sessioni aggiuntive (meno di cinque).

     È necessario modificare questo valore in modo che sia uguale al valore impostato per MAXNUMMP (numero massimo di punti di montaggio) quando il nodo di archiviazione è stato registrato o aggiornato. (Nel comando register, il valore predefinito di MAXNUMMP utilizzato è 1, se non viene impostato alcun valore).

   È inoltre necessario modificare il valore di MAXSESSIONS per il server TSM con un numero pari almeno al numero di sessioni impostato per il servizio ARC. Il valore predefinito di MAXSESSIONS sul server TSM è 25.

   - **Numero massimo di sessioni di recupero**: Specificare il numero massimo di sessioni che il servizio ARC può aprire al server middleware TSM per le operazioni di recupero. Nella maggior parte dei casi, il valore appropriato è numero di sessioni meno numero massimo di sessioni del negozio. Se è necessario condividere un'unità a nastro per lo storage e il recupero, specificare un valore uguale al numero di sessioni.
   - **Numero massimo di sessioni di archiviazione**: Specificare il numero massimo di sessioni simultanee che il servizio ARC può aprire al server middleware TSM per le operazioni di archiviazione.

     Questo valore deve essere impostato su uno, tranne quando il sistema storage di archiviazione di destinazione è pieno e possono essere eseguiti solo i recuperi. Impostare questo valore su zero per utilizzare tutte le sessioni per i recuperi.

7. Selezionare **Applica modifiche**.

Ottimizza un nodo di archiviazione per sessioni middleware TSM

È possibile ottimizzare le prestazioni di un nodo di archiviazione che si connette a Tivoli Server Manager (TSM) configurando le sessioni del nodo di archiviazione.

Prima di iniziare

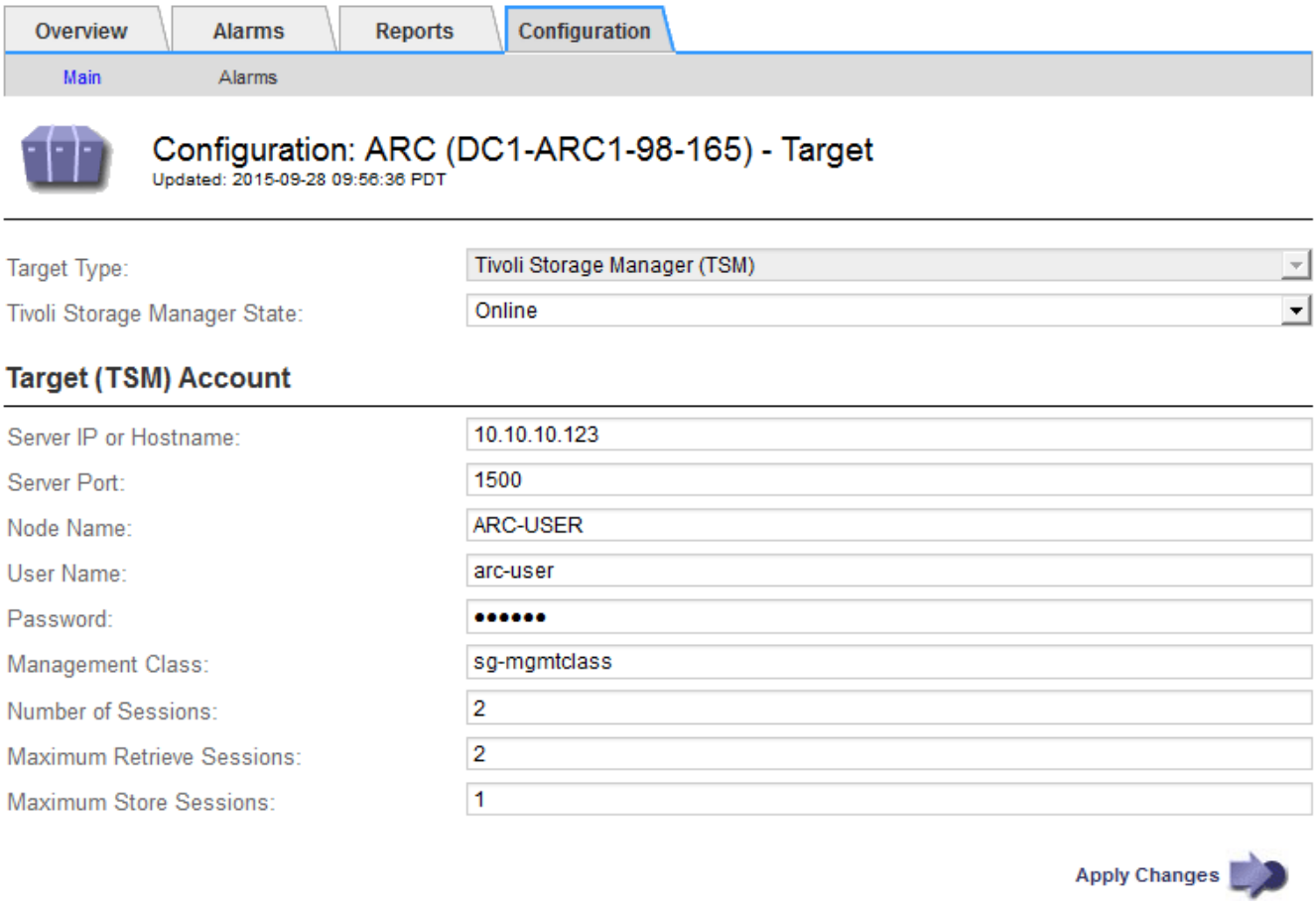
- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

In genere, il numero di sessioni simultanee che il nodo di archiviazione ha aperto al server middleware TSM viene impostato sul numero di unità a nastro dedicate dal server TSM al nodo di archiviazione. Un'unità a nastro viene allocata per lo storage, mentre le altre vengono allocate per il recupero. Tuttavia, nelle situazioni in cui un nodo di storage viene ricostruito dalle copie del nodo di archivio o il nodo di archivio opera in modalità di sola lettura, è possibile ottimizzare le prestazioni del server TSM impostando il numero massimo di sessioni di recupero sullo stesso numero di sessioni simultanee. Il risultato è che tutti i dischi possono essere utilizzati contemporaneamente per il recupero e, al massimo, uno di questi dischi può essere utilizzato anche per lo storage, se applicabile.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.
4. Modificare **numero massimo di sessioni di recupero** in modo che sia uguale a **numero di sessioni**.



5. Selezionare **Applica modifiche**.

Configurare lo stato di archiviazione e i contatori per TSM

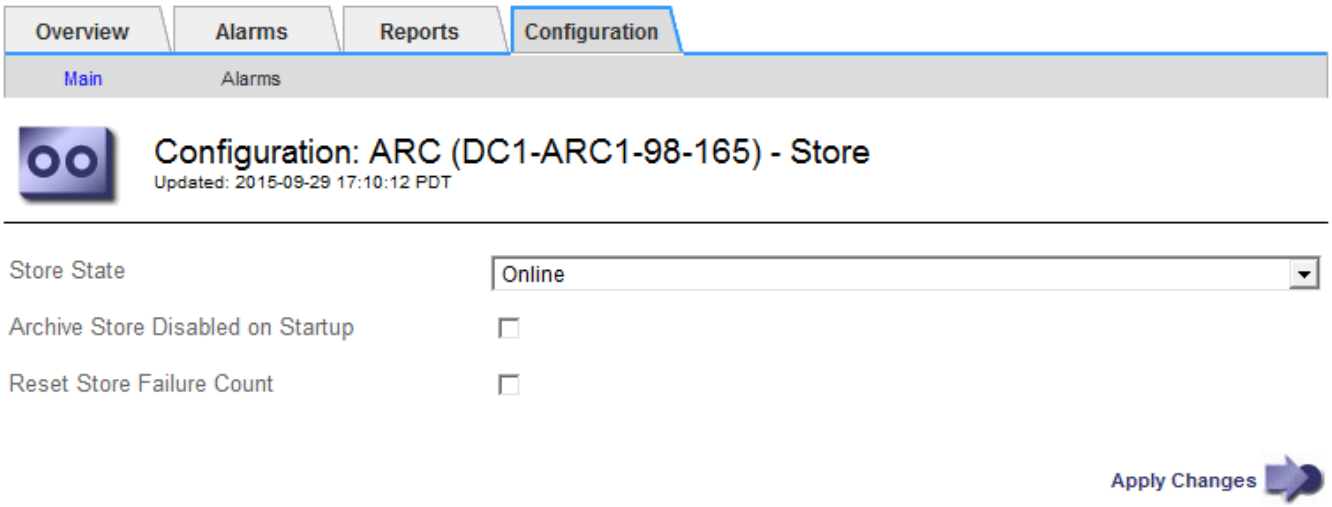
Se il nodo di archiviazione si connette a un server middleware TSM, è possibile configurare lo stato dell'archivio di un nodo di archiviazione su Online o Offline. È inoltre possibile disattivare l'archivio al primo avvio del nodo di archiviazione o ripristinare il conteggio degli errori rilevati per l'allarme associato.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Store**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le seguenti impostazioni, se necessario:
   - Store state (Stato di archiviazione): Impostare lo stato del componente su:
     - Online: Il nodo di archiviazione è disponibile per elaborare i dati a oggetti per lo storage nel sistema di storage di archiviazione.
     - Offline: Il nodo di archiviazione non è disponibile per elaborare i dati degli oggetti per lo storage nel sistema di storage di archiviazione.
   - Archivia archivio disattivata all'avvio: Se selezionato, il componente Archivia archivio rimane nello stato di sola lettura al riavvio. Utilizzato per disattivare in modo persistente lo storage nel sistema di storage di archiviazione di destinazione. Utile quando il sistema storage di archiviazione di destinazione non è in grado di accettare contenuti.
   - Reset Store Failure Count (Ripristina numero di guasti del punto vendita): Consente di reimpostare il contatore per gli errori Questa opzione può essere utilizzata per cancellare l'allarme ARVF (Memorizza guasto).
5. Selezionare **Applica modifiche**.

Informazioni correlate

"Gestire un nodo di archiviazione quando il server TSM raggiunge la capacità"

Gestire un nodo di archiviazione quando il server TSM raggiunge la capacità

Il server TSM non ha modo di notificare al nodo di archiviazione quando il database TSM o lo storage dei supporti di archiviazione gestito dal server TSM si avvicina alla capacità. Questa situazione può essere evitata attraverso il monitoraggio proattivo del server TSM.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

A proposito di questa attività

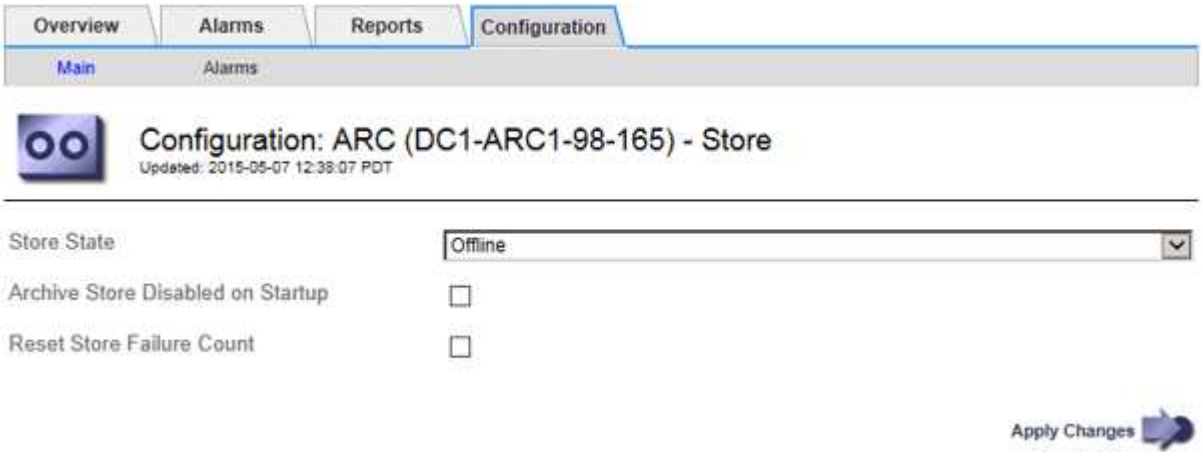
Il nodo di archiviazione continua ad accettare i dati dell'oggetto per il trasferimento al server TSM dopo che il server TSM ha interrotto l'accettazione del nuovo contenuto. Questo contenuto non può essere scritto su supporti gestiti dal server TSM. In questo caso, viene attivato un allarme.

Impedire al servizio ARC di inviare contenuto al server TSM

Per impedire al servizio ARC di inviare ulteriore contenuto al server TSM, è possibile disattivare il nodo di archiviazione portando il componente **ARC** > **Store** offline. Questa procedura può essere utile anche per prevenire gli allarmi quando il server TSM non è disponibile per la manutenzione.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Store**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare **Store state** in `Offline`.
5. Selezionare **Archivia archivio disabilitata all'avvio**.
6. Selezionare **Applica modifiche**.

Impostare Archive Node su Read-only se il middleware TSM raggiunge la capacità

Se il server middleware TSM di destinazione raggiunge la capacità, il nodo di archiviazione può essere ottimizzato per eseguire solo i recuperi.

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Target**.
3. Selezionare **Configurazione** > **principale**.
4. Impostare il numero massimo di sessioni di recupero in modo che sia uguale al numero di sessioni simultanee elencate in numero di sessioni.
5. Impostare il numero massimo di sessioni di memorizzazione su 0.

Se il nodo di archiviazione è di sola lettura, non è necessario modificare il numero massimo di sessioni di archiviazione su 0. Le sessioni del negozio non verranno create.

6. Selezionare **Applica modifiche**.

Configurare le impostazioni di recupero del nodo di archiviazione

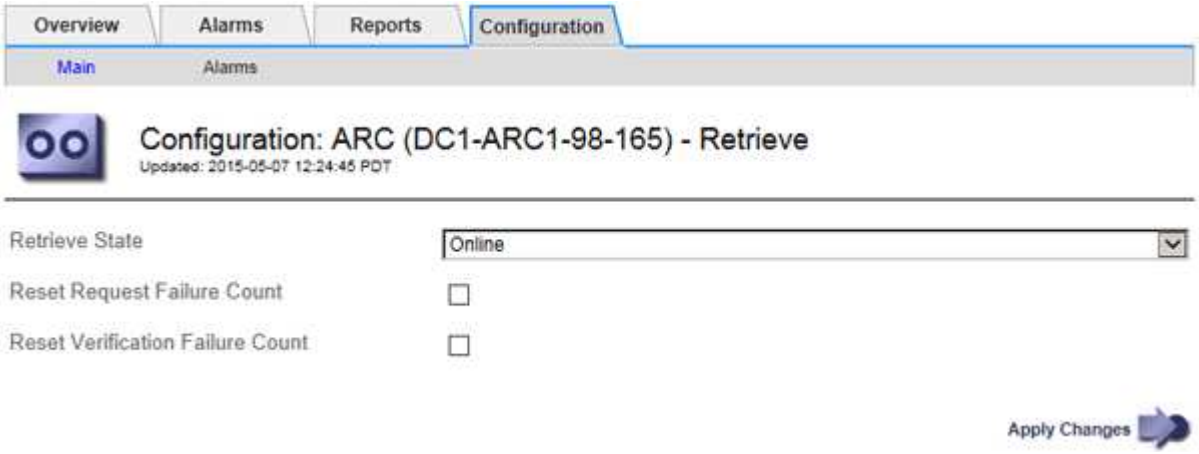
È possibile configurare le impostazioni di recupero per un nodo di archiviazione per impostare lo stato su Online o Offline, oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare **nodo archivio** > **ARC** > **Recupera**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le seguenti impostazioni, se necessario:
   - **Stato di recupero**: Impostare lo stato del componente su:
     - Online: Il nodo Grid è disponibile per recuperare i dati degli oggetti dal dispositivo di archiviazione.
     - Offline: Il nodo Grid non è disponibile per recuperare i dati dell'oggetto.
   - Reset Request Failures Count (Ripristina numero di errori richiesta): Selezionare la casella di controllo per azzerare il contatore dei guasti richiesta. Questa opzione può essere utilizzata per cancellare l'allarme ARRF (Request Failures).
   - Reset Verification Failure Count (Ripristina conteggio errori di verifica): Selezionare la casella di controllo per ripristinare il contatore per gli errori di verifica sui dati dell'oggetto recuperati. Questa opzione può essere utilizzata per cancellare l'allarme ARRV (Verification Failures) (errori di verifica).
5. Selezionare **Applica modifiche**.

Configurare la replica del nodo di archiviazione

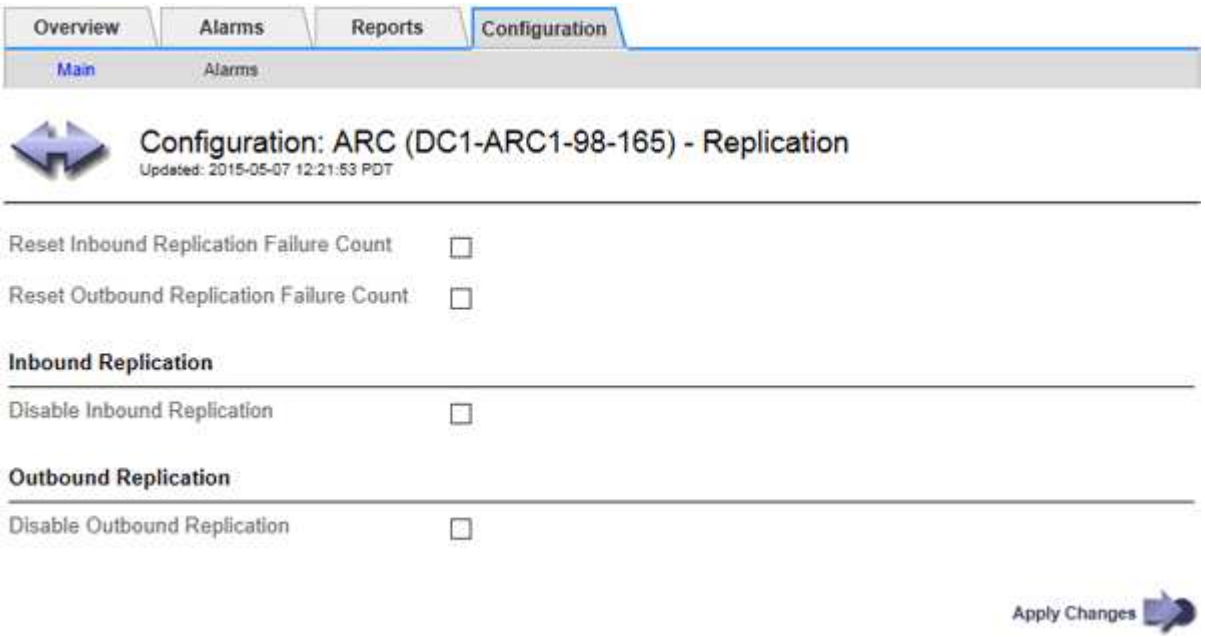
È possibile configurare le impostazioni di replica per un nodo di archiviazione e disattivare la replica in entrata e in uscita oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Lo hai fatto "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **SUPPORT** > **Tools** > **Grid topology**.
2. Selezionare ***Archive Node*** > **ARC** > **Replication**.
3. Selezionare **Configurazione** > **principale**.



4. Modificare le seguenti impostazioni, se necessario:
   - **Reset Inbound Replication Failure Count** (Ripristina conteggio errori replica in entrata): Selezionare per reimpostare il contatore per gli errori di replica in entrata. Questa opzione può essere utilizzata per cancellare l'allarme RIRF (Inbound Replications — Failed).
   - **Reset Outbound Replication Failure Count** (Ripristina conteggio errori replica in uscita): Selezionare per reimpostare il contatore per gli errori di replica in uscita. Questa opzione può essere utilizzata per cancellare l'allarme RORF (Outbound Replications — Failed).
   - **Disable Inbound Replication** (Disattiva replica in entrata): Selezionare questa opzione per disattivare la replica in entrata come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.

     Quando la replica in entrata è disattivata, i dati degli oggetti possono essere recuperati dal servizio ARC per la replica in altre posizioni nel sistema StorageGRID, ma gli oggetti non possono essere replicati in questo servizio ARC da altre posizioni del sistema. Il servizio ARC è di sola lettura-.

   - **Disable Outbound Replication** (Disattiva replica in uscita): Selezionare la casella di controllo per

disattivare la replica in uscita (incluse le richieste di contenuto per i recuperi HTTP) come parte di una procedura di manutenzione o test. Lasciare deselezionato durante il normale funzionamento.

Quando la replica in uscita è disattivata, i dati degli oggetti possono essere copiati in questo servizio ARC per soddisfare le regole ILM, ma i dati degli oggetti non possono essere recuperati dal servizio ARC per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio ARC è di sola-scrittura.

5. Selezionare **Applica modifiche**.

Impostare gli allarmi personalizzati per il nodo di archiviazione

È necessario stabilire allarmi personalizzati per gli attributi ARQL e ARRL utilizzati per monitorare la velocità e l'efficienza del recupero dei dati a oggetti dal sistema di storage di archiviazione da parte del nodo di archiviazione.

- ARQL: Lunghezza media della coda. Il tempo medio, in microsecondi, in cui i dati dell'oggetto vengono messi in coda per il recupero dal sistema di storage di archiviazione.
- ARRL: Latenza media della richiesta. Il tempo medio, in microsecondi, necessario al nodo di archiviazione per recuperare i dati degli oggetti dal sistema di storage di archiviazione.

I valori accettabili per questi attributi dipendono dalla configurazione e dall'utilizzo del sistema di storage di archiviazione. (Andare a **ARC** > **Recupera** > **Panoramica** > **principale**.) I valori impostati per i timeout delle richieste e il numero di sessioni rese disponibili per le richieste di recupero sono particolarmente influenti.

Una volta completata l'integrazione, monitorare i recuperi dei dati dell'oggetto del nodo di archiviazione per stabilire i valori relativi ai tempi di recupero e alle lunghezze della coda normali. Quindi, creare allarmi personalizzati per ARQL e ARRL che si attiveranno in caso di condizioni operative anomale. Consultare le istruzioni per "gestione degli allarmi (sistema legacy)".

Integrare Tivoli Storage Manager

Configurazione e funzionamento del nodo di archiviazione

Il sistema StorageGRID gestisce il nodo di archiviazione come una posizione in cui gli oggetti vengono memorizzati a tempo indeterminato e sono sempre accessibili.

Quando viene acquisito un oggetto, vengono create copie in tutte le posizioni richieste, inclusi i nodi di archivio, sulla base delle regole ILM (Information Lifecycle Management) definite per il sistema StorageGRID. Il nodo di archiviazione funge da client per un server TSM e le librerie del client TSM vengono installate sul nodo di archiviazione mediante il processo di installazione del software StorageGRID. I dati dell'oggetto indirizzati al nodo di archiviazione per lo storage vengono salvati direttamente nel server TSM quando vengono ricevuti. Il nodo di archiviazione non esegue lo stage dei dati dell'oggetto prima di salvarli nel server TSM, né esegue l'aggregazione di oggetti. Tuttavia, il nodo di archiviazione può inviare più copie al server TSM in una singola transazione quando la velocità dei dati lo giustifica.

Dopo che il nodo di archiviazione ha salvato i dati dell'oggetto nel server TSM, i dati dell'oggetto vengono gestiti dal server TSM utilizzando i relativi criteri di conservazione/ciclo di vita. Questi criteri di conservazione devono essere definiti in modo da essere compatibili con il funzionamento del nodo di archiviazione. Ovvero, i dati degli oggetti salvati dal nodo di archiviazione devono essere memorizzati a tempo indeterminato e devono essere sempre accessibili dal nodo di archiviazione, a meno che non vengano cancellati dal nodo di archiviazione.

Non esiste alcuna connessione tra le regole ILM del sistema StorageGRID e le policy di conservazione/ciclo di

vita del server TSM. Ciascuno di essi opera indipendentemente dall'altro; tuttavia, quando ciascun oggetto viene acquisito nel sistema StorageGRID, è possibile assegnargli una classe di gestione TSM. Questa classe di gestione viene passata al server TSM insieme ai dati dell'oggetto. L'assegnazione di diverse classi di gestione a diversi tipi di oggetti consente di configurare il server TSM in modo che i dati degli oggetti siano memorizzati in diversi pool di storage o di applicare criteri di migrazione o conservazione diversi in base alle esigenze. Ad esempio, gli oggetti identificati come backup del database (contenuto temporaneo che può essere sovrascritto con dati più recenti) potrebbero essere trattati in modo diverso rispetto ai dati dell'applicazione (contenuto fisso che deve essere conservato a tempo indeterminato).

Il nodo di archiviazione può essere integrato con un server TSM nuovo o esistente; non richiede un server TSM dedicato. I server TSM possono essere condivisi con altri client, a condizione che il server TSM sia dimensionato in modo appropriato per il carico massimo previsto. TSM deve essere installato su un server o una macchina virtuale separato dal nodo di archiviazione.

È possibile configurare più di un nodo di archiviazione per la scrittura sullo stesso server TSM; tuttavia, questa configurazione è consigliata solo se i nodi di archiviazione scrivono set di dati diversi nel server TSM. La configurazione di più di un nodo di archivio per la scrittura sullo stesso server TSM non è consigliata quando ciascun nodo di archivio scrive copie degli stessi dati dell'oggetto nell'archivio. In quest'ultimo scenario, entrambe le copie sono soggette a un singolo punto di errore (il server TSM) per quelle che si suppone siano copie ridondanti indipendenti dei dati dell'oggetto.

I nodi di archiviazione non utilizzano il componente HSM (Hierarchical Storage Management) di TSM.

Best practice per la configurazione

Quando si esegue il dimensionamento e la configurazione del server TSM, è necessario applicare le Best practice per ottimizzarlo e utilizzarlo con il nodo di archiviazione.

Durante il dimensionamento e la configurazione del server TSM, è necessario considerare i seguenti fattori:

- Poiché il nodo di archiviazione non aggrega gli oggetti prima di salvarli nel server TSM, il database TSM deve essere dimensionato in modo da contenere riferimenti a tutti gli oggetti che verranno scritti nel nodo di archiviazione.
- Il software Archive Node non è in grado di tollerare la latenza necessaria per la scrittura di oggetti direttamente su nastro o su altri supporti rimovibili. Pertanto, il server TSM deve essere configurato con un pool di storage su disco per la memorizzazione iniziale dei dati salvati dal nodo di archiviazione ogni volta che si utilizzano supporti rimovibili.
- È necessario configurare i criteri di conservazione TSM per utilizzare la conservazione basata su eventi-. Il nodo di archiviazione non supporta i criteri di conservazione TSM basati sulla creazione. Utilizzare le seguenti impostazioni consigliate di retmin=0 e retver=0 nel criterio di conservazione (che indica che la conservazione inizia quando il nodo di archiviazione attiva un evento di conservazione e viene mantenuta per 0 giorni dopo). Tuttavia, questi valori per retmin e retver sono facoltativi.

Il pool di dischi deve essere configurato per migrare i dati nel pool di nastri (ovvero, il pool di nastri deve essere il NXTSTGPOOL del pool di dischi). Il pool di nastri non deve essere configurato come pool di copie del pool di dischi con scrittura simultanea su entrambi i pool (ovvero, il pool di nastri non può essere un COPYSTGPOOL per il pool di dischi). Per creare copie non in linea dei nastri contenenti dati del nodo di archiviazione, configurare il server TSM con un secondo pool di nastri che è un pool di copie del pool di nastri utilizzato per i dati del nodo di archiviazione.

Completare la configurazione del nodo di archiviazione

Il nodo di archiviazione non funziona dopo aver completato il processo di installazione.

Prima che il sistema StorageGRID possa salvare gli oggetti nel nodo di archivio TSM, è necessario completare l'installazione e la configurazione del server TSM e configurare il nodo di archivio per comunicare con il server TSM.

Fare riferimento alla seguente documentazione IBM, se necessario, durante la preparazione del server TSM per l'integrazione con il nodo di archiviazione in un sistema StorageGRID:

- "Guida per l'installazione e l'utente dei driver di dispositivo su nastro IBM"
- "IBM Tape Device Drivers Programming Reference"

Installare un nuovo server TSM

È possibile integrare il nodo di archiviazione con un server TSM nuovo o esistente. Se si sta installando un nuovo server TSM, seguire le istruzioni nella documentazione del TSM per completare l'installazione.

> Un nodo di archiviazione non può essere co-ospitato con un server TSM.

Configurare il server TSM

Questa sezione include istruzioni di esempio per preparare un server TSM seguendo le Best practice TSM.

Le seguenti istruzioni guidano l'utente nel processo di:

- Definizione di un pool di storage su disco e di un pool di storage su nastro (se necessario) sul server TSM
- Definizione di un criterio di dominio che utilizza la classe di gestione TSM per i dati salvati dal nodo di archiviazione e registrazione di un nodo per utilizzare questo criterio di dominio

Queste istruzioni sono fornite esclusivamente a scopo informativo; non sono intese a sostituire la documentazione del TSM o a fornire istruzioni complete e complete adatte a tutte le configurazioni. Le istruzioni specifiche per l'implementazione devono essere fornite da un amministratore TSM che abbia familiarità con i requisiti dettagliati e con la documentazione completa di TSM Server.

Definire i pool di storage su disco e nastro TSM

Il nodo di archiviazione scrive in un pool di dischi di storage. Per archiviare il contenuto su nastro, è necessario configurare il pool di storage su disco per spostare il contenuto in un pool di storage su nastro.

A proposito di questa attività

Per un server TSM, è necessario definire un pool di storage su nastro e un pool di storage su disco in Tivoli Storage Manager. Una volta definito il pool di dischi, creare un volume di dischi e assegnarlo al pool di dischi. Non è necessario un pool di nastri se il server TSM utilizza lo storage solo-disco.

Prima di creare un pool di storage su nastro, è necessario completare diversi passaggi sul server TSM. Creare una libreria di nastri e almeno un'unità nella libreria di nastri. Definire un percorso dal server alla libreria e dal server ai dischi, quindi definire una classe di dispositivi per i dischi. I dettagli di questi passaggi possono variare a seconda della configurazione hardware e dei requisiti di storage del sito. Per ulteriori informazioni, consultare la documentazione del TSM.

Il seguente set di istruzioni illustra il processo. Tenere presente che i requisiti del sito potrebbero essere diversi a seconda dei requisiti dell'implementazione. Per informazioni dettagliate sulla configurazione e istruzioni, consultare la documentazione del TSM.

È necessario accedere al server con privilegi amministrativi e utilizzare lo strumento dsmadmc per eseguire i seguenti comandi.

Fasi

1. Creare una libreria di nastri.

   ```
   define library tapelibrary libtype=scsi
   ```

   Dove *tapelibrary* è un nome arbitrario scelto per la libreria di nastri e il valore di `libtype` può variare a seconda del tipo di libreria di nastri.

2. Definire un percorso dal server alla libreria di nastri.

   ```
   define path servername tapelibrary srctype=server desttype=library device=lib-devicename
   ```

   - *servername* È il nome del server TSM
   - *tapelibrary* è il nome della libreria di nastri definito
   - *lib-devicename* è il nome del dispositivo per la libreria di nastri

3. Definire un disco per la libreria.

   ```
   define drive tapelibrary drivename
   ```

   - *drivename* è il nome che si desidera specificare per l'unità
   - *tapelibrary* è il nome della libreria di nastri definito

     A seconda della configurazione dell'hardware, potrebbe essere necessario configurare uno o più dischi aggiuntivi. Ad esempio, se il server TSM è collegato a uno switch Fibre Channel con due ingressi da una libreria di nastri, è possibile definire un'unità per ciascun ingresso.

4. Definire un percorso dal server all'unità definita.

   ```
   define path servername drivename srctype=server desttype=drive
   library=tapelibrary device=drive-dname
   ```

   - *drive-dname* è il nome del dispositivo per il disco
   - *tapelibrary* è il nome della libreria di nastri definito

     Ripetere l'operazione per ogni disco definito per la libreria di nastri, utilizzando un disco separato *drivename* e. *drive-dname* per ciascun disco.

5. Definire una classe di dispositivi per i dischi.

   ```
   define devclass DeviceClassName devtype=lto library=tapelibrary
   format=tapetype
   ```

- *DeviceClassName* è il nome della classe device
- *lto* è il tipo di disco collegato al server
- *tapelibrary* è il nome della libreria di nastri definito
- *tapetype* è il tipo di nastro, ad esempio ultrium3

6. Aggiungere volumi su nastro all'inventario per la libreria.

   `checkin libvolume tapelibrary`

   tapelibrary è il nome della libreria di nastri definito.

7. Creare il pool di storage su nastro primario.

   `define stgpool SGWSTapePool DeviceClassName description=description collocate=filespace maxscratch=XX`

   - *SGWSTapePool* È il nome del pool di storage su nastro del nodo di archiviazione. È possibile selezionare qualsiasi nome per il pool di storage su nastro (purché il nome utilizzi le convenzioni di sintassi previste dal server TSM).
   - *DeviceClassName* è il nome della classe di dispositivi per la libreria di nastri.
   - *description* È una descrizione del pool di storage che può essere visualizzato sul server TSM utilizzando `query stgpool` comando. Ad esempio: "Pool di archiviazione su nastro per il nodo di archiviazione".
   - *collocate=filespace* Specifica che il server TSM deve scrivere oggetti dallo stesso spazio di file in un singolo nastro.
   - XX è uno dei seguenti:
     - Il numero di nastri vuoti nella libreria di nastri (nel caso in cui il nodo di archiviazione sia l'unica applicazione che utilizza la libreria).
     - Il numero di nastri allocati per l'utilizzo da parte del sistema StorageGRID (nei casi in cui la libreria di nastri è condivisa).

8. Su un server TSM, creare un pool di storage su disco. Nella console di amministrazione del server TSM, immettere

   `define stgpool SGWSDiskPool disk description=description maxsize=maximum_file_size nextstgpool=SGWSTapePool highmig=percent_high lowmig=percent_low`

   - *SGWSDiskPool* È il nome del pool di dischi del nodo di archiviazione. È possibile selezionare qualsiasi nome per il pool di storage su disco (purché il nome utilizzi le convenzioni di sintassi previste dal TSM).
   - *description* È una descrizione del pool di storage che può essere visualizzato sul server TSM utilizzando `query stgpool` comando. Ad esempio, "Pool di archiviazione su disco per il nodo di archiviazione".
   - *maximum_file_size* forza la scrittura diretta su nastro di oggetti di dimensioni superiori a tali, anziché la memorizzazione nella cache del pool di dischi. Si consiglia di impostare *maximum_file_size* A 10 GB.
   - *nextstgpool=SGWSTapePool* Fa riferimento al pool di storage su disco al pool di storage su nastro definito per il nodo di archiviazione.

- *percent_high* imposta il valore in corrispondenza del quale il pool di dischi inizia la migrazione del contenuto nel pool di nastri. Si consiglia di impostare *percent_high* a 0 in modo che la migrazione dei dati inizi immediatamente
- *percent_low* imposta il valore in corrispondenza del quale la migrazione al pool di nastri viene interrotta. Si consiglia di impostare *percent_low* a 0 per eliminare il pool di dischi.

9. Su un server TSM, creare uno o più volumi di dischi e assegnarli al pool di dischi.

   `define volume SGWSDiskPool volume_name formatsize=size`

   - *SGWSDiskPool* è il nome del pool di dischi.
   - *volume_name* è il percorso completo verso la posizione del volume (ad esempio, `/var/local/arc/stage6.dsm`) Sul server TSM in cui scrive il contenuto del pool di dischi in preparazione del trasferimento su nastro.
   - *size* È la dimensione, in MB, del volume del disco.

     Ad esempio, per creare un singolo volume di disco in modo che il contenuto di un pool di dischi occupi un singolo nastro, impostare il valore di size su 200000 quando il volume del nastro ha una capacità di 200 GB.

     Tuttavia, potrebbe essere consigliabile creare più volumi di dischi di dimensioni inferiori, in quanto il server TSM può scrivere su ciascun volume del pool di dischi. Ad esempio, se la dimensione del nastro è di 250 GB, creare 25 volumi di dischi con una dimensione di 10 GB (10000) ciascuno.

   Il server TSM preassegna lo spazio nella directory per il volume del disco. Il completamento di questa operazione può richiedere più di tre ore per un volume di disco da 200 GB.

Definire un criterio di dominio e registrare un nodo

È necessario definire un criterio di dominio che utilizzi la classe di gestione TSM per i dati salvati dal nodo di archiviazione, quindi registrare un nodo per utilizzare questo criterio di dominio.

> I processi del nodo di archiviazione possono perdere memoria se la password del client per il nodo di archiviazione in Tivoli Storage Manager (TSM) scade. Assicurarsi che il server TSM sia configurato in modo che il nome utente/la password del client per il nodo di archiviazione non scada mai.

Quando si registra un nodo sul server TSM per l'utilizzo del nodo di archiviazione (o per l'aggiornamento di un nodo esistente), è necessario specificare il numero di punti di montaggio che il nodo può utilizzare per le operazioni di scrittura specificando il parametro MAXNUMMP nel comando DEL NODO DI REGISTRO. Il numero di punti di montaggio equivale in genere al numero di testine del disco a nastro allocate al nodo di archiviazione. Il numero specificato per MAXNUMMP sul server TSM deve essere grande almeno quanto il valore impostato per **ARC** > **Target** > **Configurazione** > **principale** > **numero massimo di sessioni di archiviazione** per il nodo di archiviazione, Che è impostato su un valore pari a 0 o 1, in quanto le sessioni dello store simultanee non sono supportate dal nodo di archiviazione.

Il valore di MAXSESSIONS impostato per il server TSM controlla il numero massimo di sessioni che possono essere aperte al server TSM da tutte le applicazioni client. Il valore di MAXSESSIONS specificato nel TSM deve essere almeno grande quanto il valore specificato per **ARC** > **Target** > **Configurazione** > **principale** > **numero di sessioni** nel Grid Manager per il nodo di archiviazione. Il nodo di archiviazione crea

contemporaneamente al massimo una sessione per punto di montaggio più un piccolo numero (< 5) di sessioni aggiuntive.

Il nodo TSM assegnato al nodo di archiviazione utilizza una policy di dominio personalizzata `tsm-domain`. Il `tsm-domain` Il criterio di dominio è una versione modificata del criterio di dominio "standard", configurata per la scrittura su nastro e con la destinazione di archivio impostata come pool di archiviazione del sistema StorageGRID (*`SGWSDiskPool`*).

> È necessario accedere al server TSM con privilegi amministrativi e utilizzare lo strumento dsmacmc per creare e attivare i criteri di dominio.

Creare e attivare i criteri di dominio

È necessario creare un criterio di dominio e attivarlo per configurare il server TSM in modo da salvare i dati inviati dal nodo di archiviazione.

Fasi

1. Creare un criterio di dominio.

   ```
   copy domain standard tsm-domain
   ```

2. Se non si utilizza una classe di gestione esistente, immettere una delle seguenti informazioni:

   ```
   define policyset tsm-domain standard
   ```

   ```
   define mgmtclass tsm-domain standard default
   ```

   `default` è la classe di gestione predefinita per l'implementazione.

3. Creare un gruppo di copygroup nel pool di storage appropriato. Immettere (su una riga):

   ```
   define copygroup tsm-domain standard default type=archive
   destination=SGWSDiskPool retinit=event retmin=0 retver=0
   ```

   `default` È la classe di gestione predefinita per il nodo di archiviazione. I valori di `retinit`, `retmin`, e. `retver` Sono stati scelti per riflettere il comportamento di conservazione attualmente utilizzato dal nodo di archiviazione

   > Non impostare `retinit` a. `retinit=create`. Impostazione `retinit=create` Impedisce al nodo di archiviazione di eliminare il contenuto, poiché gli eventi di conservazione vengono utilizzati per rimuovere il contenuto dal server TSM.

4. Assegnare la classe di gestione come predefinita.

   ```
   assign defmgmtclass tsm-domain standard default
   ```

5. Impostare il nuovo set di criteri come attivo.

   ```
   activate policyset tsm-domain standard
   ```

   Ignorare l'avviso "nessun gruppo di copie di backup" visualizzato quando si immette il comando di attivazione.

6. Registrare un nodo per utilizzare il nuovo set di criteri sul server TSM. Sul server TSM, immettere (su una riga):

   ```
   register node arc-user arc-password passexp=0 domain=tsm-domain
   MAXNUMMP=number-of-sessions
   ```

   Arc-user e Arc-password sono lo stesso nome e password del nodo client definiti nel nodo di archiviazione e il valore di MAXNUMMP è impostato sul numero di unità nastro riservate per le sessioni di archiviazione del nodo di archiviazione.

   > Per impostazione predefinita, la registrazione di un nodo crea un ID utente amministrativo con l'autorità del proprietario del client, con la password definita per il nodo.

Migrare i dati in StorageGRID

È possibile migrare grandi quantità di dati nel sistema StorageGRID utilizzando contemporaneamente il sistema StorageGRID per le operazioni quotidiane.

Utilizza questa guida per pianificare una migrazione di grandi quantità di dati nel sistema StorageGRID. Non si tratta di una guida generale alla migrazione dei dati e non include procedure dettagliate per l'esecuzione di una migrazione. Seguire le linee guida e le istruzioni di questa sezione per garantire che i dati vengano migrati in modo efficiente nel sistema StorageGRID senza interferire con le operazioni quotidiane e che i dati migrati vengano gestiti in modo appropriato dal sistema StorageGRID.

Confermare la capacità del sistema StorageGRID

Prima di migrare grandi quantità di dati nel sistema StorageGRID, verificare che il sistema StorageGRID disponga della capacità del disco necessaria per gestire il volume previsto.

Se il sistema StorageGRID include un nodo di archiviazione e una copia degli oggetti migrati è stata salvata nello storage nearline (ad esempio su nastro), assicurarsi che lo storage del nodo di archiviazione abbia una capacità sufficiente per il volume previsto dei dati migrati.

Nell'ambito della valutazione della capacità, esaminare il profilo dei dati degli oggetti che si intende migrare e calcolare la quantità di capacità del disco richiesta. Per ulteriori informazioni sul monitoraggio della capacità del disco del sistema StorageGRID, vedere "Gestire i nodi di storage" e le istruzioni per "Monitoraggio di StorageGRID".

Determinare il criterio ILM per i dati migrati

Il criterio ILM del sistema StorageGRID determina il numero di copie eseguite, le posizioni in cui vengono memorizzate e il periodo di conservazione delle copie. Un criterio ILM è costituito da un insieme di regole ILM che descrivono come filtrare gli oggetti e gestire i dati degli oggetti nel tempo.

A seconda del modo in cui vengono utilizzati i dati migrati e dei requisiti per i dati migrati, è possibile definire regole ILM univoche per i dati migrati che sono diverse dalle regole ILM utilizzate per le operazioni quotidiane. Ad esempio, se esistono requisiti normativi diversi per la gestione quotidiana dei dati rispetto ai dati inclusi nella migrazione, è possibile che si desideri un numero diverso di copie dei dati migrati su un diverso livello di storage.

È possibile configurare regole che si applicano esclusivamente ai dati migrati se è possibile distinguere in modo univoco tra i dati migrati e i dati oggetto salvati dalle operazioni quotidiane.

Se è possibile distinguere in modo affidabile tra i tipi di dati utilizzando uno dei criteri dei metadati, è possibile utilizzare questi criteri per definire una regola ILM che si applica solo ai dati migrati.

Prima di iniziare la migrazione dei dati, assicurarsi di aver compreso il criterio ILM del sistema StorageGRID e il modo in cui verrà applicato ai dati migrati e di aver apportato e verificato eventuali modifiche al criterio ILM. Vedere "Gestire gli oggetti con ILM".

> Un criterio ILM specificato in modo non corretto può causare una perdita di dati irreversibile. Esaminare attentamente tutte le modifiche apportate a un criterio ILM prima di attivarlo per assicurarsi che il criterio funzioni come previsto.

Valutare l'impatto della migrazione sulle operazioni

Un sistema StorageGRID è progettato per fornire un funzionamento efficiente per lo storage e il recupero di oggetti e per fornire un'eccellente protezione contro la perdita di dati attraverso la creazione perfetta di copie ridondanti di dati a oggetti e metadati.

Tuttavia, la migrazione dei dati deve essere gestita con attenzione in base alle istruzioni contenute in questa guida per evitare di avere un impatto sulle operazioni quotidiane del sistema o, in casi estremi, mettere i dati a rischio di perdita in caso di guasto nel sistema StorageGRID.

La migrazione di grandi quantità di dati pone un carico aggiuntivo sul sistema. Quando il sistema StorageGRID viene caricato pesantemente, risponde più lentamente alle richieste di archiviazione e recupero degli oggetti. Ciò può interferire con le richieste di archiviazione e recupero che sono parte integrante delle operazioni quotidiane. La migrazione può anche causare altri problemi operativi. Ad esempio, quando un nodo di storage si sta avvicinando alla capacità, il carico intermittente elevato dovuto all'acquisizione batch può causare il ciclo del nodo di storage tra sola lettura e lettura/scrittura, generando notifiche.

Se il carico pesante persiste, è possibile sviluppare code per varie operazioni che il sistema StorageGRID deve eseguire per garantire la ridondanza completa dei dati degli oggetti e dei metadati.

La migrazione dei dati deve essere gestita con attenzione in base alle linee guida del presente documento per garantire un funzionamento sicuro ed efficiente del sistema StorageGRID durante la migrazione. Durante la migrazione dei dati, acquisire oggetti in batch o ridurre continuamente l'acquisizione. Quindi, monitorare continuamente il sistema StorageGRID per garantire che i diversi valori degli attributi non vengano superati.

Pianificare e monitorare la migrazione dei dati

La migrazione dei dati deve essere pianificata e monitorata, se necessario, per garantire che i dati vengano inseriti in base alla policy ILM entro i tempi richiesti.

Pianificazione della migrazione dei dati

Evita la migrazione dei dati durante le ore di funzionamento principali. Limitare la migrazione dei dati a serate, fine settimana e altri periodi in cui l'utilizzo del sistema è basso.

Se possibile, non pianificare la migrazione dei dati durante i periodi di attività elevata. Tuttavia, se non è pratico evitare completamente il periodo di attività elevato, è sicuro procedere finché si monitorano attentamente gli attributi pertinenti e si interviene se superano i valori accettabili.

Monitorare la migrazione dei dati

Questa tabella elenca gli attributi da monitorare durante la migrazione dei dati e i problemi che rappresentano.

Se si utilizzano criteri di classificazione del traffico con limiti di velocità per accelerare l'acquisizione, è possibile monitorare la velocità osservata insieme alle statistiche descritte nella tabella seguente e ridurre i limiti, se necessario.

Monitorare	Descrizione
Numero di oggetti in attesa di valutazione ILM	1. Selezionare **SUPPORT** > **Tools** > **Grid topology**. 2. Selezionare ***deployment*** > **Overview** > **Main**. 3. Nella sezione ILM Activity (attività ILM), monitorare il numero di oggetti visualizzati per i seguenti attributi: ◦ **In attesa - tutti (XQUZ)**: Il numero totale di oggetti in attesa di valutazione ILM. ◦ **In attesa - Client (XCQZ)**: Il numero totale di oggetti in attesa di valutazione ILM dalle operazioni del client (ad esempio, acquisizione). 4. Se il numero di oggetti visualizzato per uno di questi attributi supera 100,000, ridurre il tasso di acquisizione degli oggetti per ridurre il carico sul sistema StorageGRID.
Capacità di storage del sistema di archiviazione mirato	Se la policy ILM salva una copia dei dati migrati in un sistema storage di archiviazione di destinazione (nastro o cloud), monitorate la capacità del sistema storage di archiviazione di destinazione per garantire che vi sia una capacità sufficiente per i dati migrati.
Nodo archivio > **ARC** > **Memorizza**	Se viene attivato un allarme per l'attributo **Store Failures (ARVF)**, il sistema storage di archiviazione di destinazione potrebbe aver raggiunto la capacità. Controllare il sistema storage di archiviazione di destinazione e risolvere eventuali problemi che hanno generato un allarme.

Informazioni sul copyright

Copyright © 2025 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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