Amministrare StorageGRID

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/it-it/storagegrid-116/admin/index.html on October 03, 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 a utilizzare StorageGRID . . . 1
Requisiti del browser Web . . . 1
Accedi a Grid Manager . . . 1
Disconnettersi da Grid Manager . . . 5
Modificare la password . . . 6
Modificare il timeout della sessione del browser . . . 7
Visualizzare le informazioni sulla licenza StorageGRID . . . 8
Aggiornare le informazioni sulla licenza StorageGRID . . . 9
Utilizzare l'API . . . 9
Controllo dell'accesso a StorageGRID . . . 29
Modificare la passphrase di provisioning . . . 29
Modificare le password della console dei nodi . . . 31
Controllo dell'accesso tramite firewall . . . 33
USA la federazione delle identità . . . 34
Gestire i gruppi di amministratori . . . 39
Disattivare le funzioni con l'API . . . 45
Gestire gli utenti . . . 47
Utilizzo di SSO (Single Sign-on) . . . 50
Gestire le impostazioni di sicurezza . . . 78
Gestire i certificati . . . 78
Configurare i server di gestione delle chiavi . . . 109
Gestire le impostazioni del proxy . . . 138
Gestire reti client non attendibili . . . 141
Gestire i tenant . . . 143
Gestire i tenant . . . 143
Creare un account tenant . . . 145
Modificare la password per l'utente root locale del tenant . . . 149
Modificare l'account tenant . . . 150
Elimina account tenant . . . 153
Gestire i servizi della piattaforma . . . 153
Manage S3 (Gestisci S3): Selezionare per gli account tenant . . . 162
Configurare le connessioni client S3 e Swift . . . 163
Informazioni sulle connessioni client S3 e Swift . . . 163
Riepilogo: Indirizzi IP e porte per le connessioni client . . . 163
Configurare le interfacce VLAN . . . 166
Gestire i gruppi ad alta disponibilità . . . 170
Gestire il bilanciamento del carico . . . 182
Configurare i nomi di dominio degli endpoint API S3 . . . 193
Abilitare HTTP per le comunicazioni client . . . 195

Controllare quali operazioni client sono consentite . . . 196
Gestire reti e connessioni . . . 197
Linee guida per le reti StorageGRID . . . 197
Visualizzare gli indirizzi IP . . . 198
Crittografia supportata per le connessioni TLS in uscita . . . 199
Modificare la crittografia del trasferimento di rete . . . 200
Gestire le policy di classificazione del traffico . . . 201
Gestire i costi di collegamento . . . 214
USA AutoSupport . . . 217
Che cos'è AutoSupport? . . . 217
Configurare AutoSupport . . . 218
Attivare manualmente un messaggio AutoSupport . . . 224
Risolvere i problemi relativi ai messaggi AutoSupport . . . 224
Invia messaggi AutoSupport e-Series tramite StorageGRID . . . 226
Gestire i nodi di storage . . . 230
Informazioni sulla gestione dei nodi di storage . . . 230
Che cos'è un nodo di storage? . . . 230
Gestire le opzioni di storage . . . 234
Gestire lo storage dei metadati degli oggetti . . . 239
Configurare le impostazioni globali per gli oggetti memorizzati . . . 246
Impostazioni di configurazione del nodo di storage . . . 249
Gestire nodi storage completi . . . 254
Gestire i nodi di amministrazione . . . 254
Che cos'è un nodo amministratore . . . 254
Utilizzare più nodi di amministrazione . . . 255
Identificare il nodo di amministrazione principale . . . 256
Selezionare un mittente preferito . . . 257
Visualizzare lo stato delle notifiche e le code . . . 258
Modalità di visualizzazione degli allarmi riconosciuti da Admin Node (sistema legacy) . . . 259
Configurare l'accesso al client di audit . . . 260
Gestire i nodi di archiviazione . . . 277
Che cos'è un nodo di archivio . . . 277
Archiviazione nel cloud tramite l'API S3 . . . 278
Archiviazione su nastro tramite middleware TSM . . . 285
Configurare le impostazioni di recupero del nodo di archiviazione . . . 290
Configurare la replica del nodo di archiviazione . . . 291
Impostare gli allarmi personalizzati per il nodo di archiviazione . . . 293
Integrare Tivoli Storage Manager . . . 293
Migrare i dati in StorageGRID . . . 300
Confermare la capacità del sistema StorageGRID . . . 300
Determinare il criterio ILM per i dati migrati . . . 300
Impatto della migrazione sulle operazioni . . . 301
Pianificare e monitorare la migrazione dei dati . . . 301

Amministrare StorageGRID

Administer StorageGRID: Panoramica

Seguire queste istruzioni per configurare e amministrare un sistema StorageGRID.

A proposito di queste istruzioni

Queste istruzioni descrivono come utilizzare Grid Manager per configurare gruppi e utenti, creare account tenant per consentire alle applicazioni client S3 e Swift di memorizzare e recuperare oggetti, configurare e gestire reti StorageGRID, configurare AutoSupport, gestire le impostazioni dei nodi e molto altro ancora.

Queste istruzioni sono destinate al personale tecnico che configurerà, amministrerà e supporterà un sistema StorageGRID dopo l'installazione.

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 a utilizzare StorageGRID

Requisiti del browser Web

È necessario utilizzare un browser Web supportato.

Browser Web	Versione minima supportata
Google Chrome	96
Microsoft Edge	96
Mozilla Firefox	94

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.

Di cosa hai bisogno

- Si dispone delle credenziali di accesso.
- Hai l'URL per Grid Manager.
- Si sta utilizzando un browser web supportato.
- I cookie sono attivati nel browser Web.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

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.

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.

Fasi

1. Avviare un browser Web supportato.
2. Nella barra degli indirizzi del browser, immettere l'URL per Grid Manager:

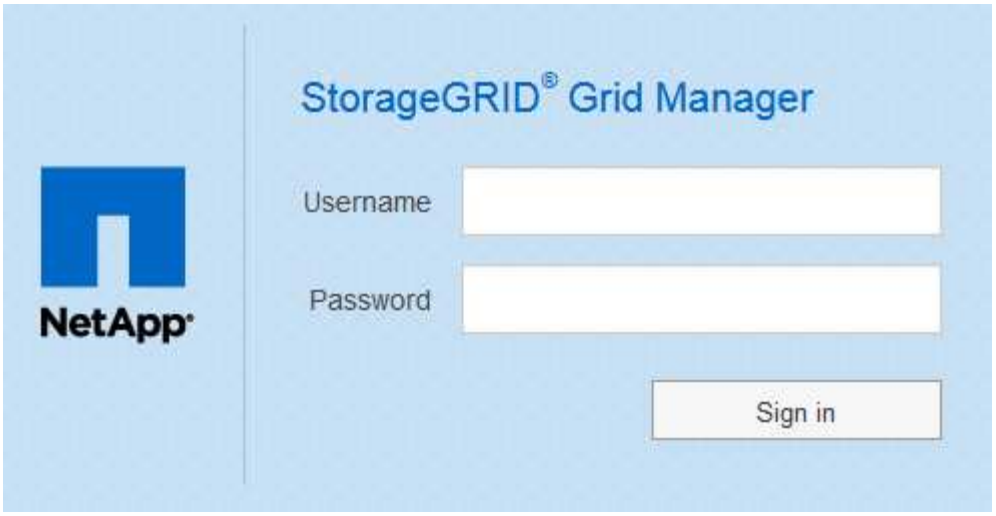
   `https://FQDN_or_Admin_Node_IP/`

   dove *`FQDN_or_Admin_Node_IP`* È un nome di dominio completo o l'indirizzo IP di un nodo di amministrazione o l'indirizzo IP virtuale di un gruppo ha di nodi di amministrazione.

   Se è necessario accedere a Grid Manager su una porta diversa da quella standard per HTTPS (443), immettere la seguente voce, dove *`FQDN_or_Admin_Node_IP`* È un nome di dominio completo o un indirizzo IP e porta è il numero di porta:

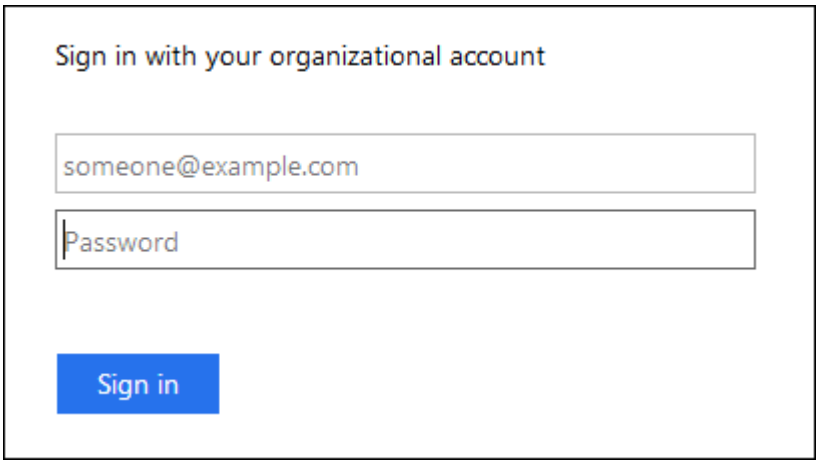
   `https://FQDN_or_Admin_Node_IP:port/`

3. Se viene richiesto un avviso di protezione, installare il certificato utilizzando l'installazione guidata del browser (vedere Informazioni sui certificati di sicurezza).
4. Accedi a Grid Manager:
   - Se il sistema StorageGRID non utilizza il Single Sign-on (SSO):
     i. Immettere il nome utente e la password per Grid Manager.
     ii. Selezionare **Accedi**.



- Se SSO è attivato per il sistema StorageGRID ed è la prima volta che si accede all'URL dal browser:
  i. Selezionare **Accedi**. È possibile lasciare vuoto il campo ID centro di costo.

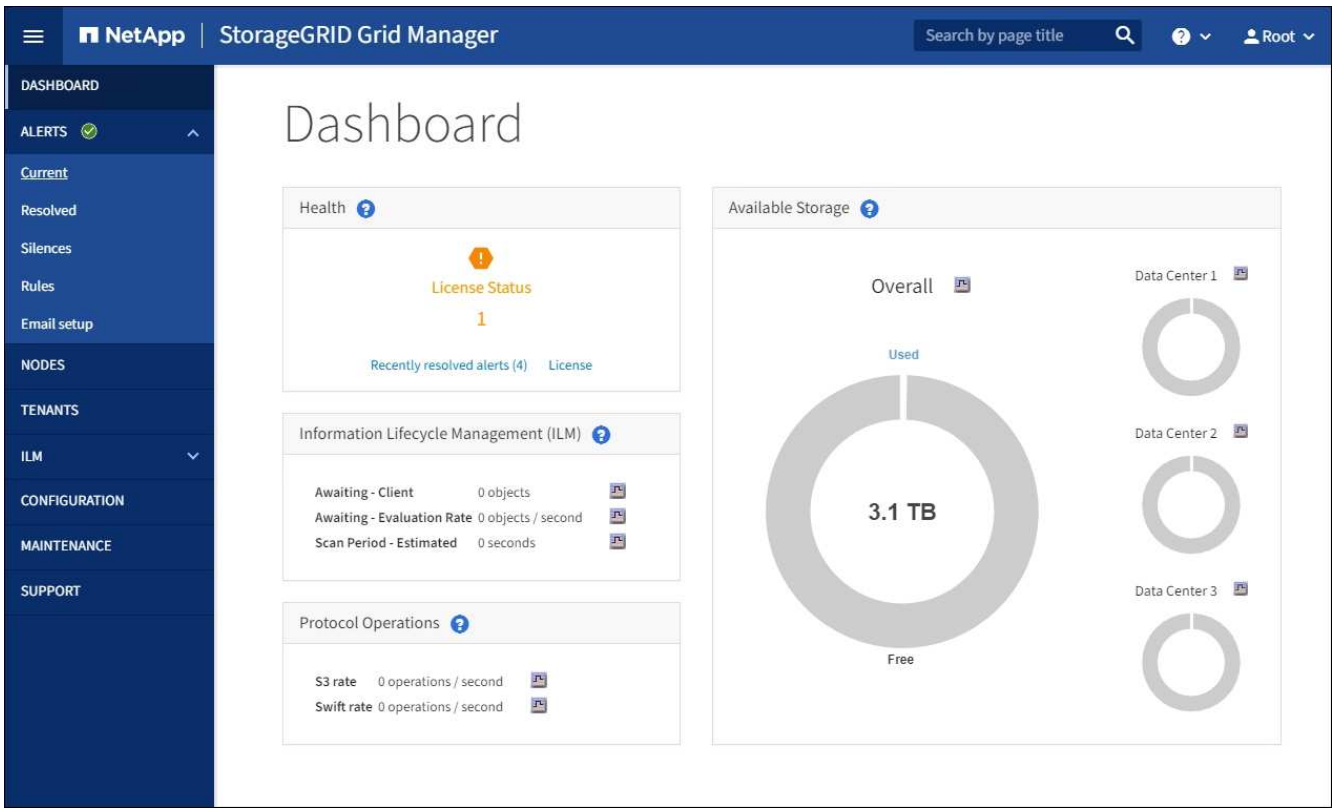
  ii. Immettere le credenziali SSO standard nella pagina di accesso SSO dell'organizzazione. Ad esempio:



- Se SSO è abilitato per il sistema StorageGRID e si è precedentemente effettuato l'accesso a Grid Manager o a un account tenant:
  i. Effettuare una delle seguenti operazioni:

- Inserire **0** (l'ID account per Grid Manager) e selezionare **Accedi**.
- Selezionare **Grid Manager** se compare nell'elenco degli account recenti e selezionare **Sign in** (Accedi).

ii. 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 Visualizza la dashboard.



5. Se si desidera accedere a un altro nodo amministratore:

Opzione	Fasi
SSO non abilitato	a. 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. b. Immettere il nome utente e la password per Grid Manager. c. Selezionare **Accedi**.
SSO attivato	Nella barra degli indirizzi del browser, inserire il nome di dominio completo o l'indirizzo IP dell'altro nodo di amministrazione. Se si è effettuato l'accesso a un nodo di amministrazione, è possibile accedere ad altri nodi di amministrazione senza dover effettuare nuovamente l'accesso. Tuttavia, se la sessione SSO scade, vengono richieste nuovamente le credenziali. **Nota:** SSO non è disponibile sulla porta limitata di Grid Manager. Se si desidera che gli utenti eseguano l'autenticazione con Single Sign-on, è necessario utilizzare la porta HTTPS predefinita (443).

Informazioni correlate

- Controllo dell'accesso tramite firewall
- Configurare il single sign-on
- Gestire i gruppi di amministratori
- Gestire i gruppi ad alta disponibilità
- Utilizzare un account tenant
- Monitorare e risolvere i problemi

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 per disconnettersi da SSO.

Informazioni correlate

- Configurare il single sign-on
- Utilizzare un account tenant

Modificare la password

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

Di cosa hai bisogno

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

A proposito di questa attività

Se si effettua l'accesso 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**.

Modificare il timeout della sessione del browser

È possibile controllare se gli utenti di Grid Manager e Tenant Manager vengono disconnessi se rimangono inattivi per più di un certo periodo di tempo.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Il valore predefinito del timeout di inattività della GUI è 900 secondi (15 minuti). Se la sessione del browser di un utente non è attiva per questo periodo di tempo, la sessione viene chiusa.

Se necessario, è possibile aumentare o diminuire il periodo di timeout impostando l'opzione di visualizzazione Timeout inattività GUI.

Se è attivato il Single Sign-on (SSO) e la sessione del browser di un utente va in timeout, il sistema si comporta come se l'utente selezionasse **Disconnetti** manualmente. L'utente deve immettere nuovamente le proprie credenziali SSO per accedere nuovamente a StorageGRID. Vedere Configurare il single sign-on.

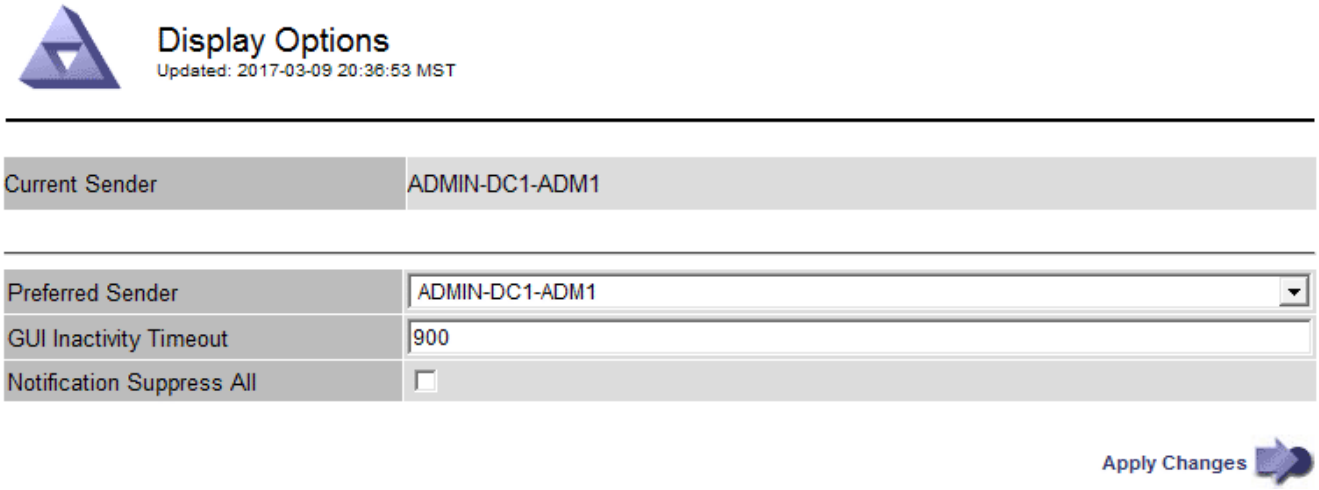
Il timeout della sessione utente può essere controllato anche da:

- Un timer StorageGRID separato, non configurabile, incluso per la sicurezza del sistema. Per impostazione predefinita, ogni token di autenticazione dell'utente scade 16 ore dopo l'accesso. Al termine dell'autenticazione, l'utente viene automaticamente disconnesso, anche se non viene raggiunto il valore per il timeout di inattività della GUI. Per rinnovare il token, l'utente deve effettuare nuovamente l'accesso.
- Impostazioni di timeout per il provider di identità, presupponendo che SSO sia abilitato per StorageGRID.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni di visualizzazione**.
2. Per **GUI Inactivity Timeout** (Timeout inattività GUI), immettere un periodo di timeout di almeno 60 secondi.

   Impostare questo campo su 0 se non si desidera utilizzare questa funzionalità. Gli utenti vengono disconnessi 16 ore dopo l'accesso, quando scadono i token di autenticazione.



3. Selezionare **Applica modifiche**.

   La nuova impostazione non influisce sugli utenti attualmente registrati. Gli utenti devono effettuare nuovamente l'accesso o aggiornare il browser per rendere effettiva la nuova impostazione di timeout.

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.

Di cosa hai bisogno

- 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, il pannello Stato del dashboard include un'icona Stato licenza e un collegamento **licenza**. Il numero indica il numero di problemi relativi alla licenza.

Fase

Per visualizzare la licenza, effettuare una delle seguenti operazioni:

- Dal pannello Health (Stato) della 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.

- Selezionare **MANUTENZIONE sistema licenza**.

Viene visualizzata la pagina License (licenza) che fornisce le seguenti informazioni di sola lettura sulla licenza corrente:

- ID sistema StorageGRID, che è il numero di identificazione univoco per l'installazione di StorageGRID
- Numero di serie della licenza
- Capacità di storage concessa in licenza del grid
- Data di fine della licenza software
- Data di fine del contratto di assistenza
- Contenuto del file di testo della licenza

> Per le licenze rilasciate prima di StorageGRID 10.3, la capacità dello storage concesso in licenza non è inclusa nel file di licenza e viene visualizzato il messaggio "vedere il contratto di licenza" invece di un valore.

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.

Di cosa hai bisogno

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

Fasi

1. Selezionare **MANUTENZIONE sistema licenza**.
2. Inserire la passphrase di provisioning per il sistema StorageGRID nella casella di testo **Passphrase di provisioning**.
3. Selezionare **Sfoglia**.
4. Nella finestra di dialogo Apri, individuare e selezionare il nuovo file di licenza (`.txt`), quindi selezionare **Apri**.

   Il nuovo file di licenza viene validato e visualizzato.

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.

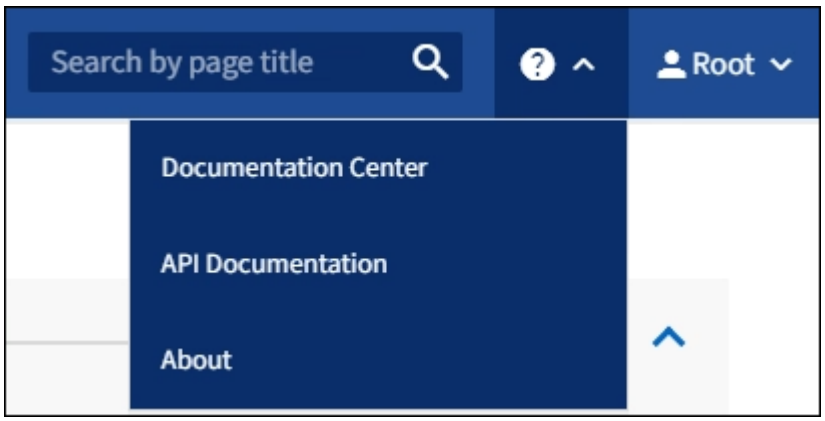
Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

> Tutte le operazioni API eseguite utilizzando la pagina web 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 **API Documentation** (documentazione API).



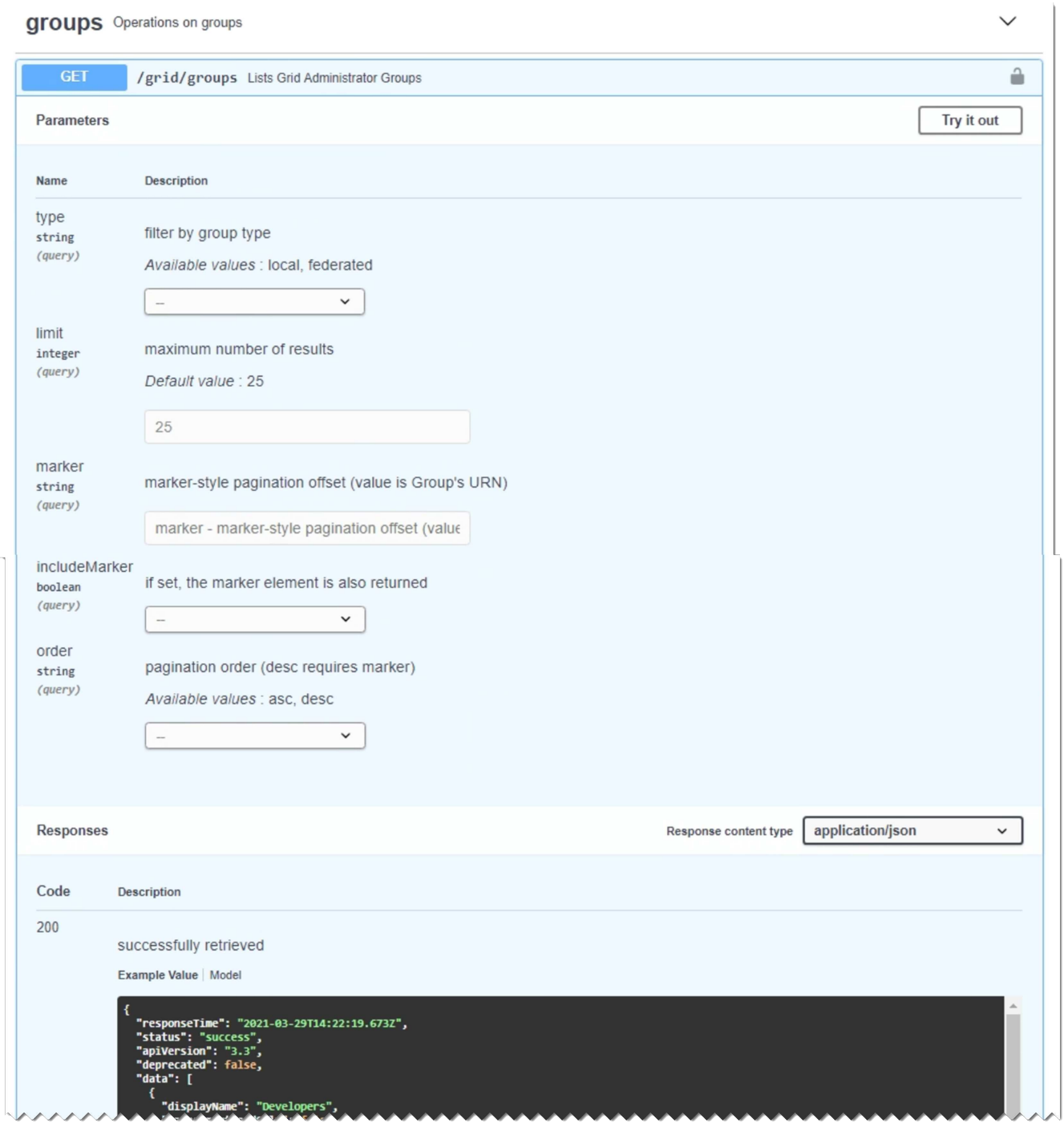
2. Per eseguire un'operazione con l'API privata, selezionare **Vai alla documentazione API privata** nella pagina API di gestione StorageGRID.

   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 gestire gli 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 sugli 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 su silenzi di allerta.
- **Alerts** — operazioni sugli avvisi.
- **Audit** — operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth** — operazioni per eseguire 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*").

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

  Per informazioni su come migliorare la sicurezza dell'autenticazione, consultare "Protecting Against Cross-Site Request Fjery".

- **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.
- **Nomi-dominio-endpoint** — operazioni per elencare e modificare i nomi di dominio degli endpoint.
- **Erasure-coding** — operazioni sui profili di codifica Erasure.
- **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).
- **Licenza** — operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs** — operazioni per la raccolta e il download dei file di log.
- **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.
- **ntp-servers** — operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects** — operazioni su oggetti e metadati di oggetti.
- **Recovery** — operazioni per la procedura di recovery.
- **Recovery-package** — operazioni per scaricare il pacchetto di ripristino.
- **Regioni** — operazioni per visualizzare e creare regioni.
- **s3-Object-lock** — operazioni sulle impostazioni generali di blocco oggetti S3.
- **Certificato-server** — operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp** — operazioni sulla configurazione SNMP corrente.
- **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 3 dell'API.

`https://hostname_or_ip_address/api/v3/authorize`

La versione principale dell'API di gestione tenant viene bloccata quando vengono apportate modifiche ***non compatibili*** con le versioni precedenti. La versione minore dell'API di gestione tenant viene ridotta 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 di gestione griglia. 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 utilizzare l'API Grid Management per configurare le versioni supportate. Per ulteriori informazioni, consultare la sezione "config" della documentazione dell'API Swagger. Disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API Grid Management 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 v1 API at POST "/api/v1/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare la seguente richiesta API per restituire un elenco delle versioni principali dell'API supportate:

```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2019-01-10T20:41:00.845Z",
  "status": "success",
  "apiVersion": "3.0",
  "data": [
    2,
    3
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione dell'API utilizzando un parametro path (`/api/v3`) o un'intestazione (`Api-Version: 3`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v3/grid/accounts

curl -H "Api-Version: 3" 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.

Anche le richieste che dispongono di un set di cookie token CSRF applicheranno `"Content-Type: application/json"` Intestazione 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.

Di cosa hai bisogno

- 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 o CentOS, `./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. Passare 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, puoi disconnetterti dall'API StorageGRID semplicemente disconnettendoti dalla singola pagina di disconnessione della tua 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

Di cosa hai bisogno

- 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 o CentOS, `./debs` Per Ubuntu o Debian, e. `./vsphere` Per VMware).

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

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

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

Fasi

1. Installare le dipendenze richieste, come indicato di seguito:
   a. Installare Node.js (vedere "https://nodejs.org/en/download/").
   b. Installare i moduli Node.js richiesti (puppeteer e jsdom):

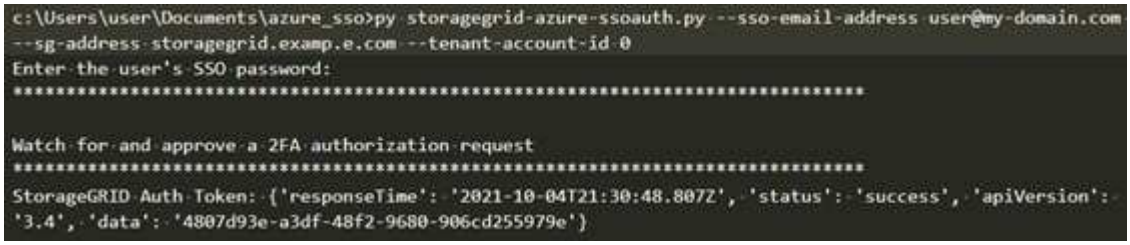
      ```
      npm install -g <module>
      ```

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

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

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

4. Quando richiesto, inserire la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.



> Lo script presuppone che l'autenticazione MFA venga eseguita utilizzando Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'immissione di un codice ricevuto tramite SMS).

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

Di cosa hai bisogno

- 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 o CentOS, `./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. Passare 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. Puoi 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, puoi disconnetterti dall'API StorageGRID semplicemente disconnettendoti dalla singola pagina di disconnessione della tua 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
```

Controllo dell'accesso a StorageGRID

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.

Di cosa hai bisogno

- 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.

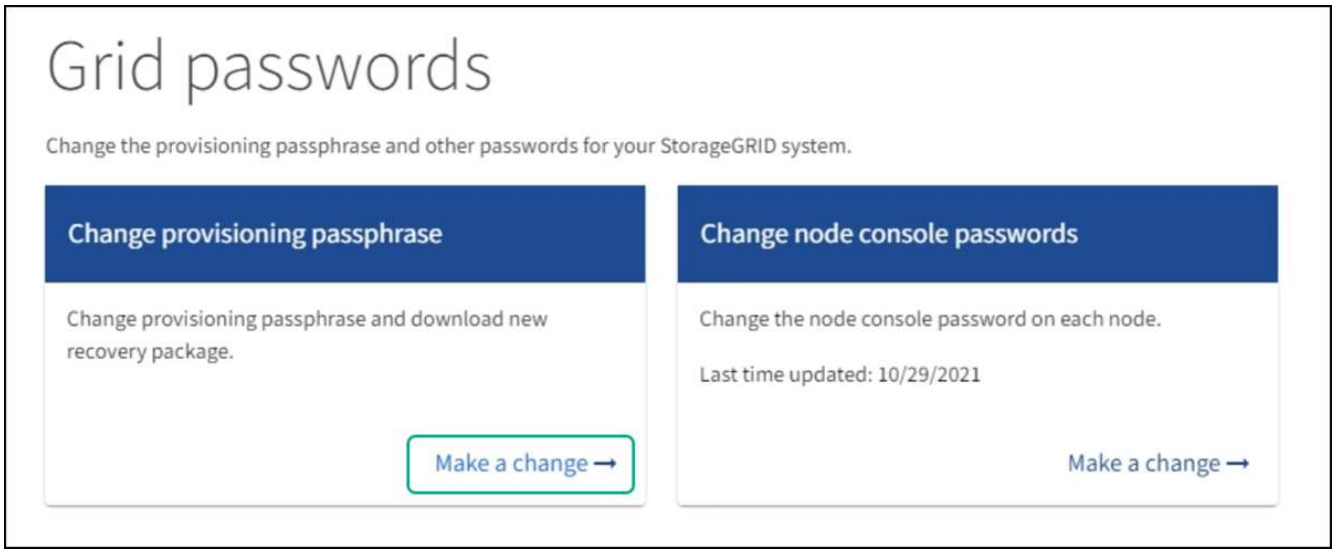
A proposito di questa attività

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.

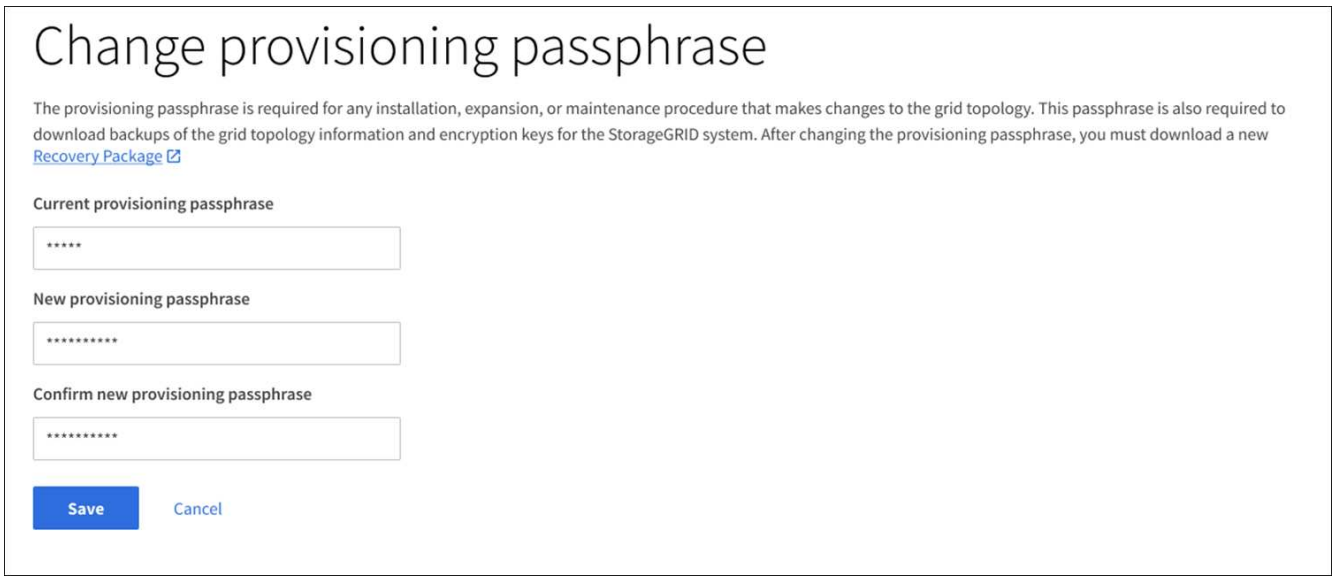
Assicurarsi di documentare la passphrase di provisioning e conservarla in una posizione sicura.

Fasi

1. Selezionare **CONFIGURATION Access control Grid passwords**.

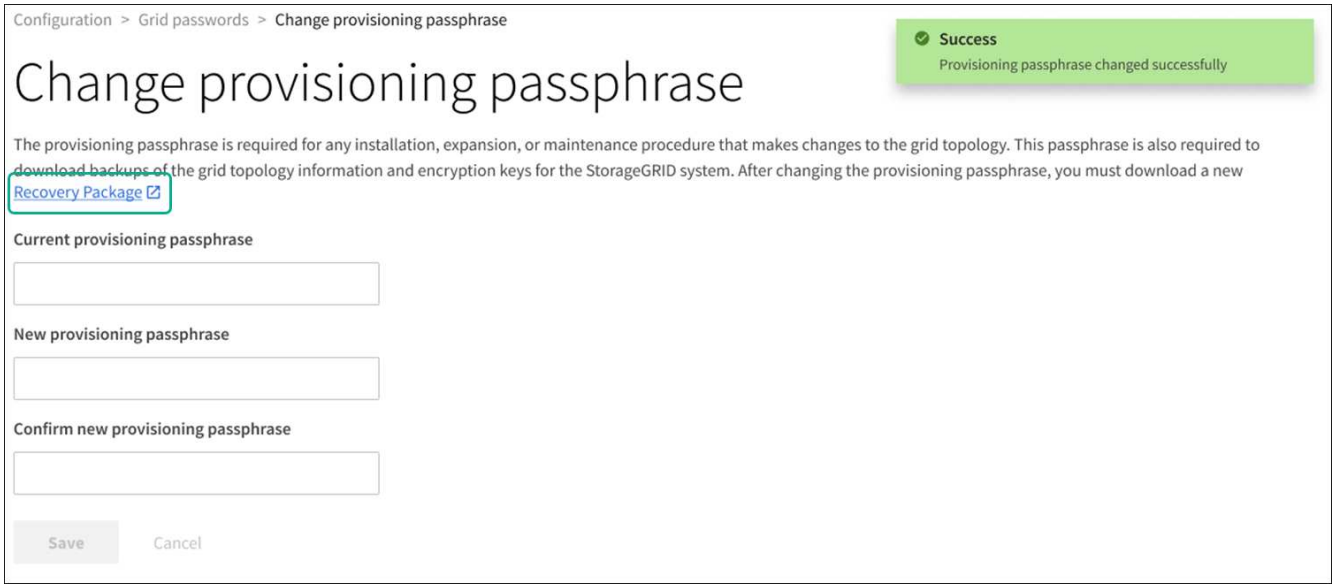


2. Selezionare **effettuare una modifica** in **Modifica passphrase di provisioning**.



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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone dell'autorizzazione di accesso Maintenance o 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 `Passwords.txt` file.

> 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 verificato il contenuto.

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 Recovery Package.

Controllo dell'accesso tramite firewall

Quando si desidera controllare l'accesso tramite firewall, aprire o chiudere porte specifiche sul firewall esterno.

Controllare l'accesso al 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.

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.

Porta	Descrizione	Se la porta è aperta…
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

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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 per l'utilizzo del 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.

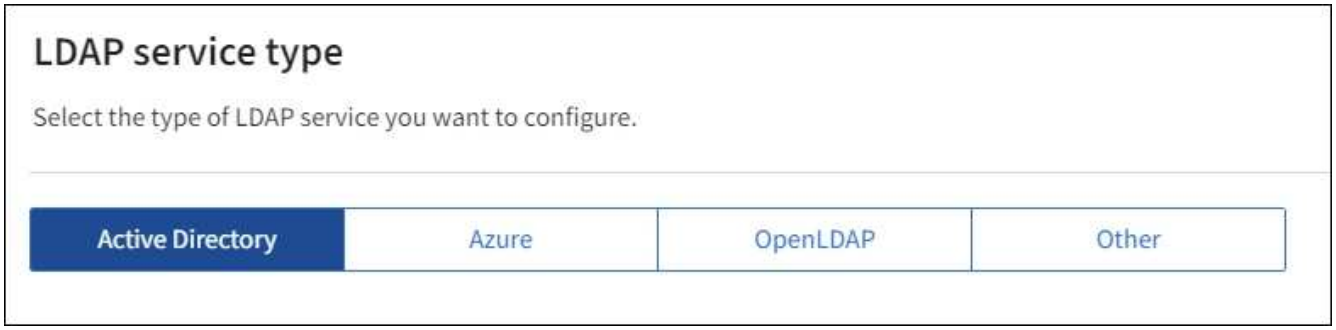
A proposito di questa attività

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

1. Selezionare **CONFIGURAZIONE controllo accessi federazione identità**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).
3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.



   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.
   - **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.

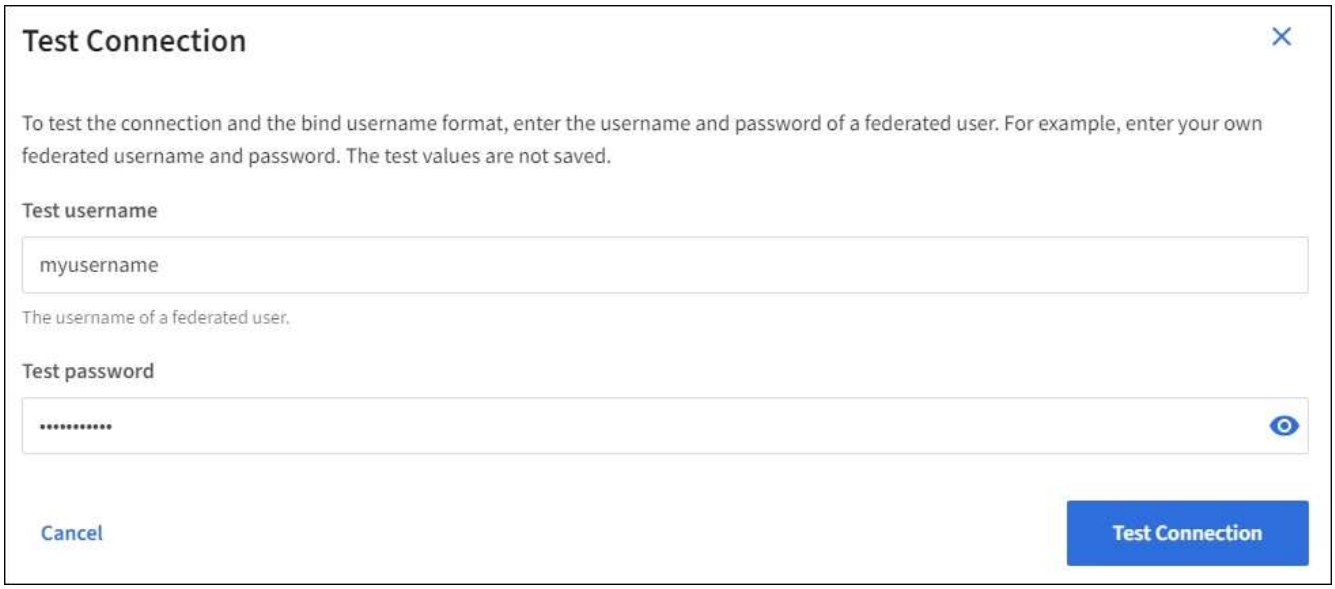
     Se si seleziona questa impostazione, copiare e incollare il certificato di protezione personalizzato nella casella di testo del certificato CA.

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.

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 di connessione riuscito". Selezionare **Salva** per salvare la configurazione.
   - Se le impostazioni di connessione non sono valide, viene visualizzato il messaggio "verifica connessione impossibile". 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 di 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 origini delle 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 e 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 inhttp://www.openldap.org/doc/admin24/index.html["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 sezionehttp://www.openldap.org/doc/admin24/index.html["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.

Di cosa hai bisogno

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

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

Creare un gruppo di amministratori

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

Accedere alla procedura guidata

1. Selezionare **CONFIGURAZIONE controllo accessi gruppi amministratori**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

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

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

Gruppo locale

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

Gruppo federated

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

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 Permessi di gruppo.

   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)

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. VedereGestire 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 relativa al 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 relativa al 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 relativa al gruppo. b. Selezionare **azioni Visualizza dettagli gruppo**. c. In alternativa, modificare la modalità di accesso del gruppo. d. Facoltativamente, selezionare o deselezionare Permessi di gruppo. 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 Permessi di gruppo. d. Selezionare **Save Changes** (Salva modifiche).

Duplicare un gruppo

1. Selezionare la casella di controllo relativa al gruppo.
2. Selezionare **azioni Gruppo duplicato**.
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.

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

Permessi di gruppo

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 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
- **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 di manutenzione possono visualizzare, ma non modificare, le seguenti pagine:

- **MANUTENZIONE rete**:
  - Server DNS
  - Grid Network
  - Server NTP
- **MANUTENZIONE sistema**:
  - Licenza
- **CONFIGURAZIONE sicurezza**:
  - Certificati
  - Nomi di dominio
- **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 alla pagina **SUPPORT Tools Metrics**. Questa autorizzazione consente inoltre di accedere alle query metriche Prometheus personalizzate utilizzando la sezione **metriche** dell'API Grid Management.

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 rete**:
  - Costo del collegamento
- **CONFIGURAZIONE sistema**:
  - Opzioni di visualizzazione
  - Opzioni della griglia
  - Opzioni di storage
- **SUPPORTO Allarmi (legacy)**:
  - Eventi personalizzati
  - Allarmi globali
  - Configurazione della posta elettronica legacy

Amministratore dell'appliance di storage

Questa autorizzazione consente di accedere al gestore di sistema e-Series SANtricity sulle appliance di storage tramite Grid Manager.

Account tenant

Questa autorizzazione consente di accedere alla pagina tenant, in cui è possibile creare, modificare e rimuovere account tenant. Questa autorizzazione consente inoltre agli utenti di visualizzare le policy di classificazione del traffico esistenti.

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 root tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenta di modificare la password root per un tenant non riuscirà con "403 proibita".

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 **ActivateFeatures**. 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 } }
```

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

Creare un utente locale

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

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

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

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

Accedere alla procedura guidata

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

Immettere le credenziali dell'utente

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

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. VedereGestire 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 **Change Password** (Modifica password).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Password. c. Inserire una nuova password. d. Selezionare **Change Password** (Modifica 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.

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.

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.

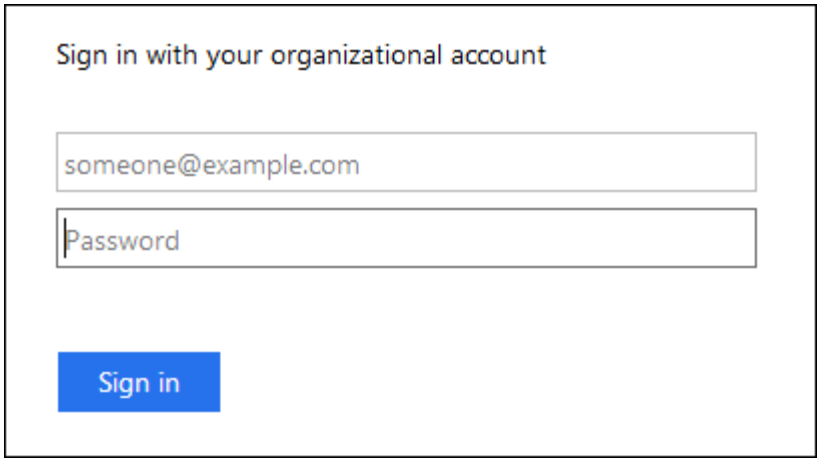
   - Se si accede per la prima volta all'URL del browser, viene richiesto di inserire un ID account:

- 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 per l'utilizzo del single sign-on

Prima di attivare il Single Sign-on (SSO) per un sistema StorageGRID, esaminare i requisiti di questa sezione.

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.

- AD FS 3.0, incluso nell'aggiornamento di Windows Server 2012 R2 o superiore.

Requisiti aggiuntivi

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

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 Controllo dell'accesso tramite firewall.

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.

Di cosa hai bisogno

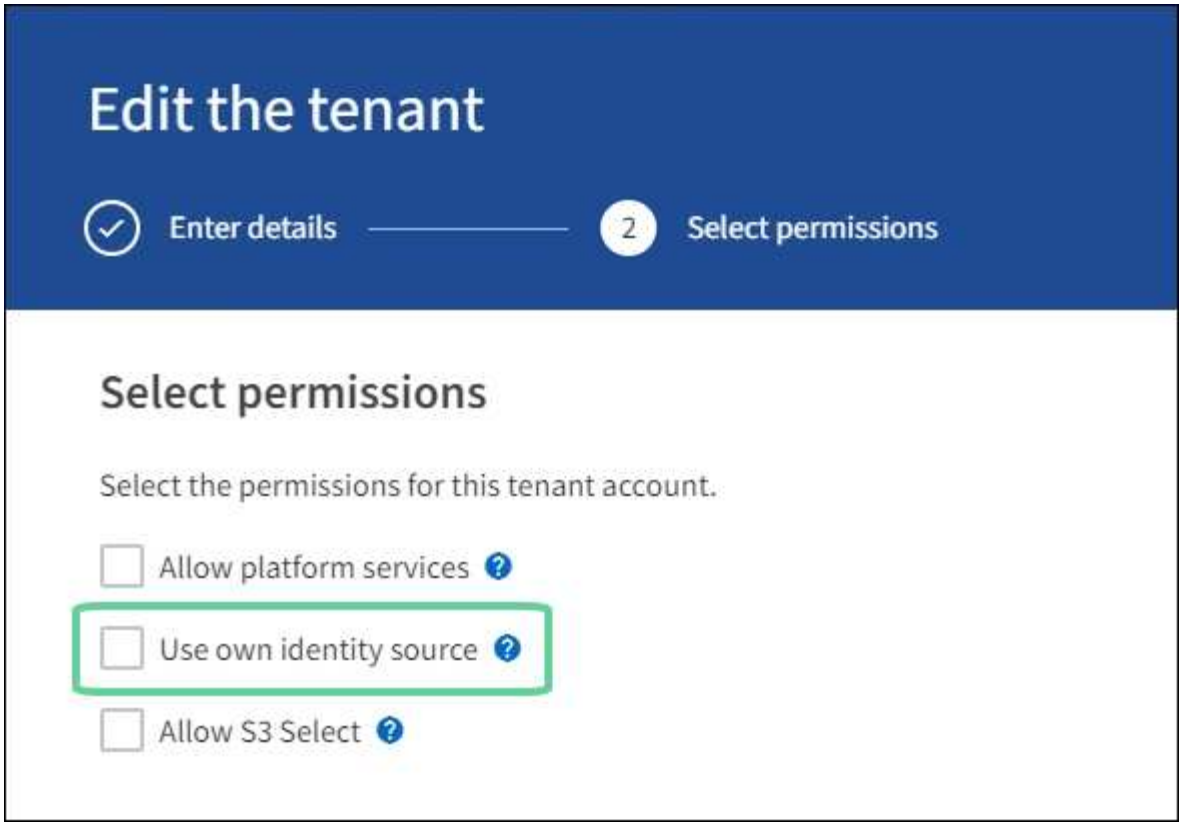
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.
- La federazione delle identità è già stata configurata.

Fasi

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

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

   a. Accedi al tenant manager per ogni account tenant.
   b. Selezionare **ACCESS MANAGEMENT** > **Identity Federation**.
   c. Confermare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
   d. In tal caso, verificare che i gruppi federated 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 **GESTIONE ACCESSI gruppi**.
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 per l'utilizzo del 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'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).

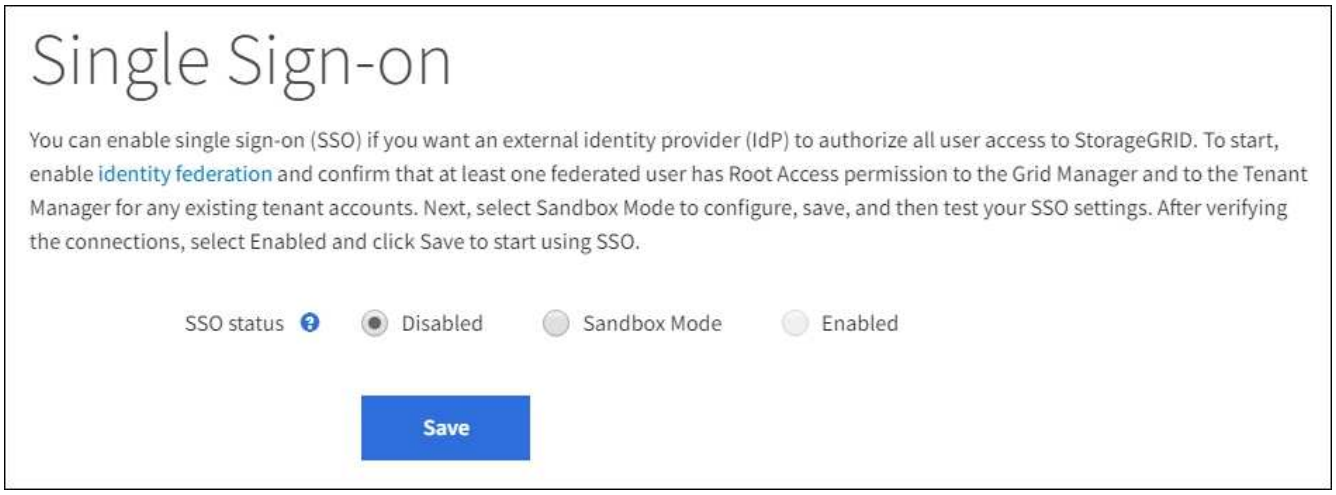
Per consentire a StorageGRID (il provider di servizi) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione dell'utente, è necessario configurare alcune impostazioni in StorageGRID. Quindi, è necessario utilizzare il software del provider di identità SSO per creare 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

1. Selezionare **CONFIGURAZIONE controllo di accesso 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 per l'utilizzo del single sign-on.

2. Selezionare **Sandbox Mode**.

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

Inserire i dettagli del provider di identità

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.
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.

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.
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

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

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **CONFIGURAZIONE controllo di accesso 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

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **CONFIGURAZIONE controllo di accesso 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.

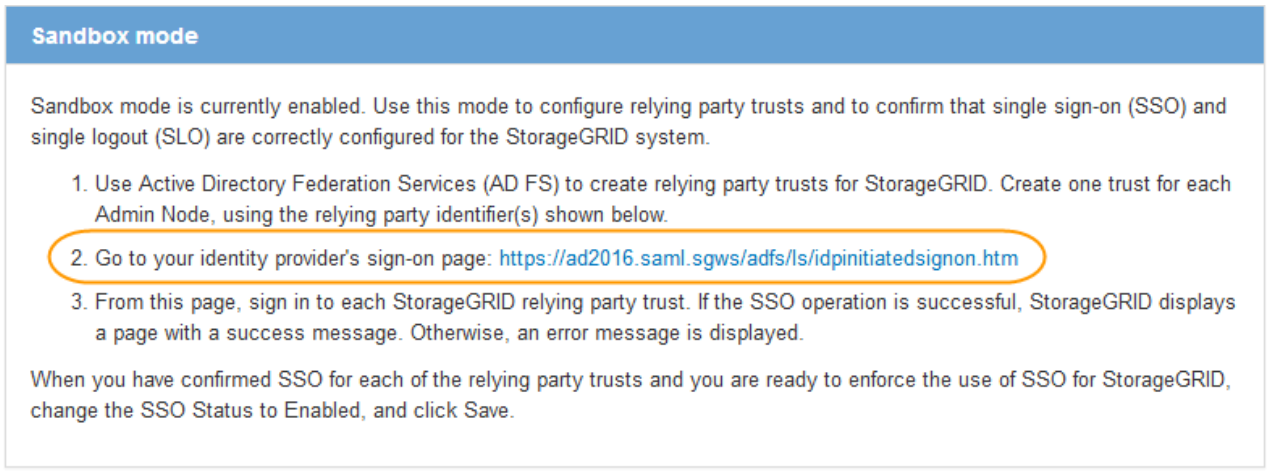
Verificare le connessioni SSO

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

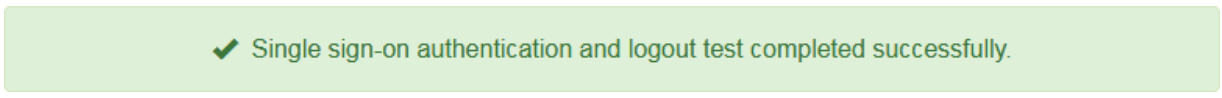
1. Dalla pagina Single Sign-on di StorageGRID, individuare il collegamento nel messaggio in modalità sandbox.

   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

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.

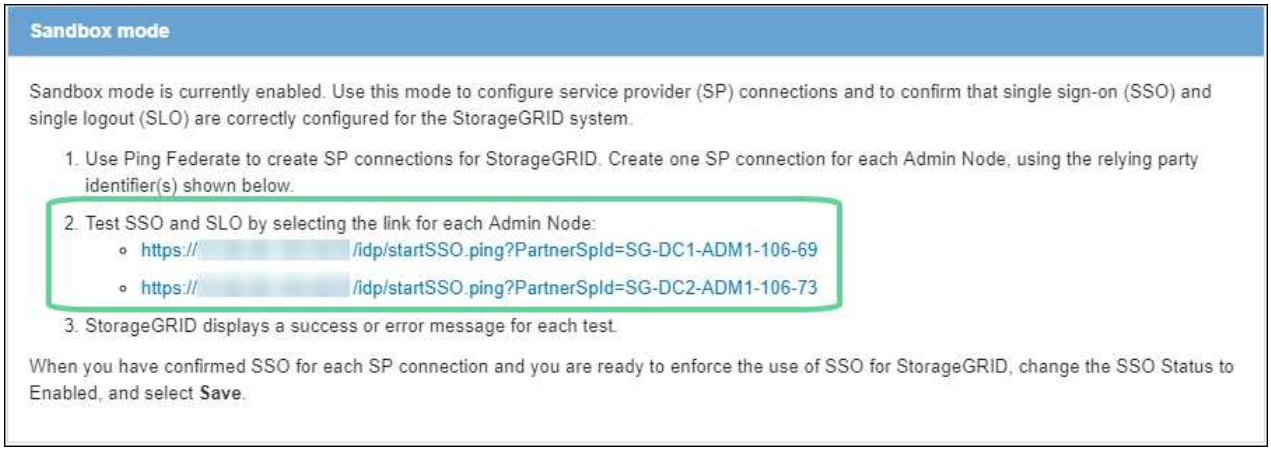
     ✔ Single sign-on authentication and logout test completed successfully.

   - 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

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.

1. Selezionare **CONFIGURAZIONE controllo di accesso 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.

Di cosa hai bisogno

- 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 di base**.

   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, da **objectGUID a ID nome**.

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

g. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.

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 o semplicemente 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, da **objectGUID a ID nome**.

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

f. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.

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 o semplicemente 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, da **objectGUID a ID nome**.

   c. Per l'archivio attributi, selezionare **Active Directory**.
   d. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.
   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.

Di cosa hai bisogno

- 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

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.

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.

Ripetere questi passaggi per ciascun nodo di amministrazione:

1. Accedere a StorageGRID dal nodo di amministrazione.
2. Selezionare **CONFIGURAZIONE controllo di accesso Single Sign-on**.
3. Selezionare il pulsante per scaricare i metadati SAML per il nodo di amministrazione.
4. 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:

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.

Di cosa hai bisogno

- 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 ilhttps://docs.pingidentity.com/bundle/pingfederate-103/page/kfj1564002962494.html["Guida di riferimento per l'amministratore"^] Per PingFederate Server. La documentazione di PingFederate fornisce istruzioni dettagliate e spiegazioni dettagliate.
- Si dispone dell'autorizzazione Admin 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.

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.

1. Accedere a **sicurezza Firma chiavi di decrittare certificati**.
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

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

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 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

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

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 Attribute Source User Lookup (Ricerca utente origine attributo), selezionare **Add Attribute Source** (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 oggetto root, cercare l'attributo **objectGUID** e aggiungerlo.

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 Attribute Contract Fulfillment, selezionare **LDAP (attributo)** dall'elenco a discesa Source (origine) e selezionare **objectGUID** dall'elenco a discesa Value (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

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 (Policy firma), lasciare selezionate le caselle di controllo **Request Authn to be firmed** (Richiedi firma richiesta) e **Always Sign Assertion** (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

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.

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

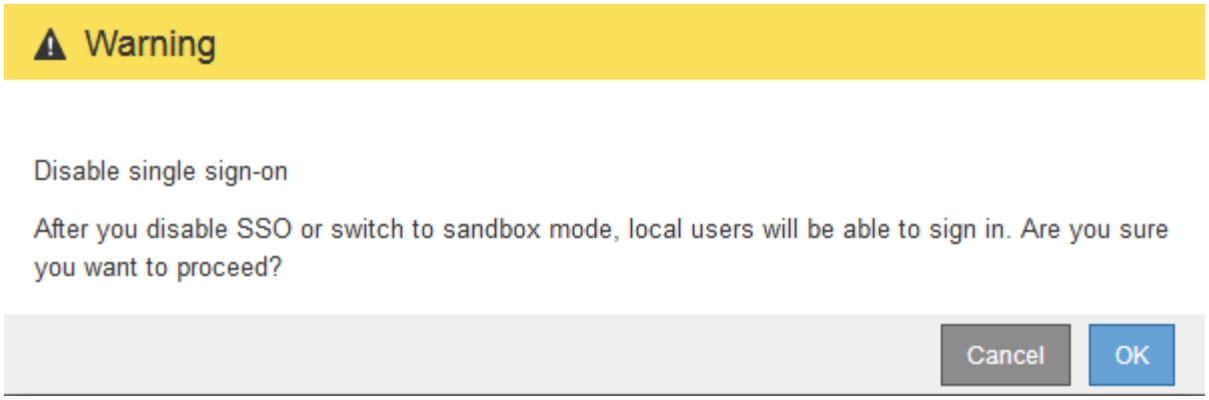
Fasi

1. Selezionare **CONFIGURAZIONE controllo di accesso 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.

Di cosa hai bisogno

- Si dispone di 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 **CONFIGURAZIONE controllo di accesso 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.

Gestire le impostazioni di sicurezza

Gestire i certificati

Informazioni sui certificati di sicurezza

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 le 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).

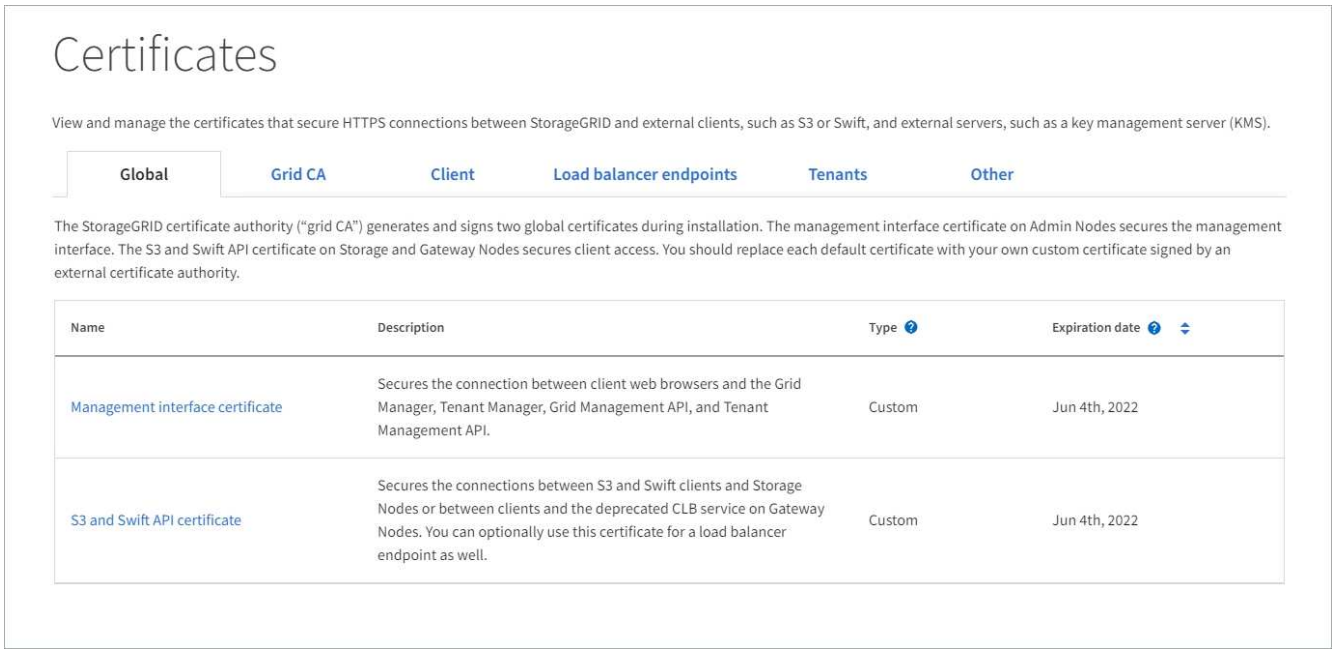
> StorageGRID include anche certificati CA del sistema operativo che sono gli stessi su tutte le griglie. Negli ambienti di produzione, assicurarsi di specificare un certificato personalizzato firmato da un'autorità di certificazione esterna al posto del certificato CA del sistema operativo.

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.

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 solo se si dispone dell'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 maggiore sicurezza della griglia, è necessario utilizzare sempre un certificato personalizzato.
- **Data di scadenza**: Se si utilizza il certificato predefinito, non viene visualizzata alcuna data di scadenza.

È possibile:

- Sostituire i certificati predefiniti con certificati personalizzati firmati da un'autorità di certificazione esterna per una maggiore sicurezza della griglia:
  - Sostituire il certificato predefinito dell'interfaccia di gestione generata da StorageGRID Utilizzato per le connessioni di Grid Manager e Tenant Manager.
  - Sostituire il certificato API S3 e Swift Utilizzato per le connessioni Storage Node, CLB service (obsoleto) e load balancer endpoint (opzionale).
- 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, Che vengono caricati o generati, proteggono le connessioni tra i client S3 e Swift e il servizio bilanciamento del carico StorageGRID sui nodi gateway e sui nodi amministrativi.

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:

- Selezionare un nome di endpoint per aprire una scheda del browser con informazioni sull'endpoint del 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 di federazione delle identità
- Certificati Cloud Storage Pool
- Certificati KMS (Key Management Server)
- Certificati Single Sign-on
- Certificati di notifica degli avvisi via email
- Certificati server syslog esterni

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 dell'autorizzazione appropriata.

È possibile:

- 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 un certificato Cloud Storage Pool per S3, C2S S3 o Azure
- Specificare manualmente un certificato SSO per l'attendibilità della parte che si basa
- Specificare un certificato per le notifiche e-mail di avviso
- Specificare un certificato server syslog esterno

Dettagli del certificato di sicurezza

Di seguito sono descritti i tipi di certificato di protezione, con collegamenti ad articoli che contengono istruzioni di implementazione.

Certificato dell'interfaccia di gestione

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione tra i browser Web client e l'interfaccia di gestione di StorageGRID, consentendo agli utenti di accedere a Grid Manager e Tenant Manager senza avvisi di sicurezza. Questo certificato autentica anche le connessioni API Grid Management e API Tenant Management. È possibile utilizzare il certificato predefinito creato durante l'installazione o caricare un certificato personalizzato.	**CONFIGURAZIONE sicurezza certificati**, selezionare la scheda **Globale**, quindi selezionare **certificato dell'interfaccia di gestione**	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 protette S3 o Swift a un nodo di storage, al servizio di bilanciamento del carico di connessione (CLB) obsoleto su un nodo gateway e agli endpoint del bilanciamento del carico (opzionale).	**CONFIGURAZIONE sicurezza certificati**, selezionare la scheda **Globale**, quindi selezionare **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 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 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 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 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 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

Certificato di notifica degli avvisi via email

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server e client	Autentica la connessione tra un server e-mail SMTP e StorageGRID utilizzato per le notifiche degli avvisi. • Se le comunicazioni con il server SMTP richiedono TLS (Transport Layer Security), è necessario specificare il certificato CA del server di posta elettronica. • Specificare un certificato client solo se il server di posta SMTP richiede certificati client per l'autenticazione.	**AVVISI Configurazione e-mail**	Imposta le notifiche via email per gli avvisi

Certificato server syslog esterno

Tipo di certificato	Descrizione	Posizione di navigazione	Dettagli
Server	Autentica la connessione TLS o RELP/TLS tra un server syslog esterno che registra gli eventi in StorageGRID. **Nota:** non è richiesto un certificato server syslog esterno per le connessioni TCP, RELP/TCP e UDP a un server syslog esterno.	**CONFIGURAZIONE monitoraggio Audit e server syslog**, quindi selezionare **Configura server syslog esterno**	Configurare un server syslog esterno

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).

Per ulteriori informazioni su come StorageGRID protegge le connessioni client per l'API REST, vedere Utilizzare S3 oppure USA 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 224 bit o superiori. 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:
   - **Domain name**: 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.
   - **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.
c. Selezionare **generate**.

d. Selezionare **Dettagli certificato** per visualizzare i metadati del certificato generato.

   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

     Ad esempio: `storagegrid_certificate.pem`

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.

e. Selezionare **Salva**. Il certificato dell'interfaccia di gestione personalizzata viene utilizzato per tutte le nuove connessioni successive a Grid Manager, Tenant Manager, Grid Manager API o tenant Manager API.

5. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

   Dopo aver caricato o generato un nuovo certificato, attendere fino a un giorno per la cancellazione degli avvisi relativi alla scadenza del certificato.

6. Dopo aver aggiunto un certificato dell'interfaccia di gestione personalizzata, la pagina del certificato dell'interfaccia di gestione visualizza informazioni dettagliate sul certificato per i certificati in uso. + è possibile scaricare o copiare il PEM del certificato secondo necessità.

Ripristinare il certificato dell'interfaccia di gestione predefinita

È possibile ripristinare l'utilizzo del certificato dell'interfaccia di gestione predefinita per Grid Manager e Tenant Manager Connections.

Fasi

1. Selezionare **CONFIGURAZIONE sicurezza certificati**.
2. Nella scheda **Global**, selezionare **Management interface certificate**.
3. Selezionare **Usa certificato predefinito**.

   Quando si ripristina il certificato dell'interfaccia di gestione predefinita, i file di certificato del server personalizzati configurati vengono cancellati e non possono essere ripristinati dal sistema. Il certificato predefinito dell'interfaccia di gestione viene utilizzato per tutte le nuove connessioni client successive.

4. Aggiornare la pagina per assicurarsi che il browser Web sia aggiornato.

Utilizzare uno script per generare un nuovo certificato autofirmato dell'interfaccia di gestione

Se è richiesta una convalida rigorosa del nome host, è possibile utilizzare uno script per generare il certificato dell'interfaccia di gestione.

Di cosa hai bisogno

- Si dispone di 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, al servizio di bilanciamento del carico di connessione (CLB) obsoleto sui nodi gateway 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 224 bit o superiori. 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:
   - **Domain name**: 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.
   - **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.
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 PEM del certificato secondo necessità.

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 e al servizio CLB obsoleto sui nodi gateway. 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 e al servizio CLB obsoleto sui nodi gateway.

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 S3
- USA Swift
- Configurare i nomi di dominio degli endpoint API 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Se è stato configurato un certificato server personalizzato, le applicazioni client devono verificare il server utilizzando il certificato server personalizzato. Non devono copiare il certificato CA dal sistema StorageGRID.

Fasi

1. Selezionare **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.

Di cosa hai bisogno

- Si dispone di 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.

> Il servizio di bilanciamento del carico di connessione (CLB) separato sui nodi gateway è obsoleto e non è consigliato per l'utilizzo con 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.

Consultare le informazioni su utilizzo generale dei certificati di sicurezza e. configurazione di 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.

Di cosa hai bisogno

- 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 un certificato client, seguire la procedura relativa allo scenario in uso:

- 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 di certificato contenente almeno 1 e non più di 32 caratteri.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
5. Nella sezione **tipo di certificato**, caricare il certificato dell'interfaccia di gestione `.pem` file.
   a. Selezionare **carica certificato**, quindi selezionare **continua**.
   b. Caricare 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.
6. 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.

f. 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.

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 di certificato contenente almeno 1 e non più di 32 caratteri.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
6. Nella sezione **tipo di certificato**, caricare il certificato client, la chiave privata e il bundle CA `.pem` file:
   a. Selezionare **carica certificato**, quindi selezionare **continua**.
   b. Caricare 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.

7. 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.

   f. 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.

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 di certificato contenente almeno 1 e non più di 32 caratteri.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
5. Nella sezione **tipo di certificato**, selezionare **genera certificato**.
6. Specificare le informazioni del certificato:
   - **Domain name**: Uno o più nomi di dominio pienamente qualificati del nodo admin da includere nel certificato. Utilizzare un * come carattere jolly per rappresentare più nomi di dominio.
   - **IP**: Uno o più indirizzi IP del nodo amministrativo da includere nel certificato.

- **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.

7. Selezionare **generate**.
8. 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.

9. Selezionare **Crea** per salvare il certificato in Grid Manager.

   Il nuovo certificato viene visualizzato nella scheda Client.

10. In Grid Manager, selezionare **CONFIGURATION Security Certificates**, quindi selezionare la scheda **Global**.
11. Selezionare **certificato interfaccia di gestione**.
12. Selezionare **Usa certificato personalizzato**.
13. 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 **Crea** per salvare il certificato in Grid Manager.

       Il nuovo certificato viene visualizzato nella scheda Client.

14. 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 del client dell'interfaccia di gestione per **CA Cert** e **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.

f. Salvare e verificare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

   Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo tool di monitoraggio esterno.

Per informazioni sulle metriche, vedere Istruzioni per il monitoraggio di StorageGRID.

Modificare i certificati client

È possibile modificare un certificato client amministratore per modificarne il nome, abilitare o disabilitare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

Fasi

1. Selezionare **CONFIGURAZIONE sicurezza certificati**, 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 di certificato contenente almeno 1 e non più di 32 caratteri.
5. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare **Allow Prometheus** (Consenti Prometheus).
6. Selezionare **continua** per salvare il certificato in Grid Manager.

   Il certificato aggiornato viene visualizzato nella scheda Client.

Allegare un nuovo certificato client

È possibile caricare un nuovo certificato una volta scaduto il certificato corrente.

Fasi

1. Selezionare **CONFIGURAZIONE sicurezza certificati**, 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:
   - **Domain name**: 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.
   - **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
   - **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.
c. Selezionare **generate**.
d. Selezionare **Dettagli certificato client** per visualizzare i metadati del certificato e il PEM del certificato.

   > Non sarà possibile visualizzare la chiave privata del certificato dopo aver chiuso la finestra di dialogo. Copiare o scaricare la chiave in un luogo sicuro.

   - Selezionare **Copy certificate PEM** (Copia PEM certificato) per copiare il contenuto del certificato e incollarlo altrove.
   - Selezionare **Download certificate** (Scarica certificato) per salvare il file del certificato.

     Specificare il nome del file del certificato e la posizione di download. Salvare il file con l'estensione `.pem`.

   Ad esempio: `storagegrid_certificate.pem`

- Selezionare **Copy private key** (Copia chiave privata) per copiare la chiave privata del certificato e incollarla altrove.
- Selezionare **Download private key** (Scarica chiave privata) per salvare la chiave privata come file.

  Specificare il nome del file della chiave privata e la posizione di download.

e. Selezionare **Crea** per salvare il certificato in Grid Manager.

Il nuovo certificato viene visualizzato nella scheda Client.

Scaricare o copiare i certificati client

È possibile scaricare o copiare un certificato client da utilizzare altrove.

Fasi

1. Selezionare **CONFIGURAZIONE sicurezza certificati**, 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 **CONFIGURAZIONE sicurezza certificati**, 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 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.

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.

Esaminare i metodi di crittografia StorageGRID

StorageGRID offre una serie di opzioni per la crittografia dei dati. È necessario esaminare i metodi disponibili per determinare quali metodi soddisfano i requisiti di protezione dei dati.

La tabella fornisce un riepilogo generale dei metodi di crittografia disponibili in StorageGRID.

Opzione di crittografia	Come funziona	Valido per
Server di gestione delle chiavi (KMS) in Grid Manager	Configurare un server di gestione delle chiavi per il sito StorageGRID (**CONFIGURAZIONE sicurezza server di gestione delle chiavi**) 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. La gestione delle chiavi di crittografia con un KMS è supportata solo per i nodi di storage e le appliance di servizio.
Protezione dei dischi in Gestione di sistema SANtricity	Se la funzione protezione disco è attivata per un'appliance di storage, è possibile utilizzare Gestione sistema di SANtricity per creare e gestire la chiave di sicurezza. La chiave è necessaria per accedere ai dati sui dischi protetti.	Appliance di storage con dischi FDE (Full Disk Encryption) o FIPS (Federal Information Processing Standard). Tutti i dati presenti sulle unità protette sono protetti da perdita fisica o rimozione dal data center. Non può essere utilizzato con alcune appliance di storage o con altre appliance di servizio. • Appliance di storage SG6000 • Appliance di storage SG5700 • Appliance di storage SG5600
Opzione della griglia di crittografia degli oggetti memorizzati	L'opzione **Stored Object Encryption** può essere attivata in Grid Manager (**CONFIGURATION System Grid options**). 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. • Configurare la crittografia degli oggetti memorizzati

Opzione di crittografia	Come funziona	Valido per
Crittografia bucket S3	Viene inviata una richiesta di crittografia PUT Bucket per abilitare la crittografia per il bucket. Tutti i nuovi oggetti non 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. • Utilizzare S3
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 S3
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 S3
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:

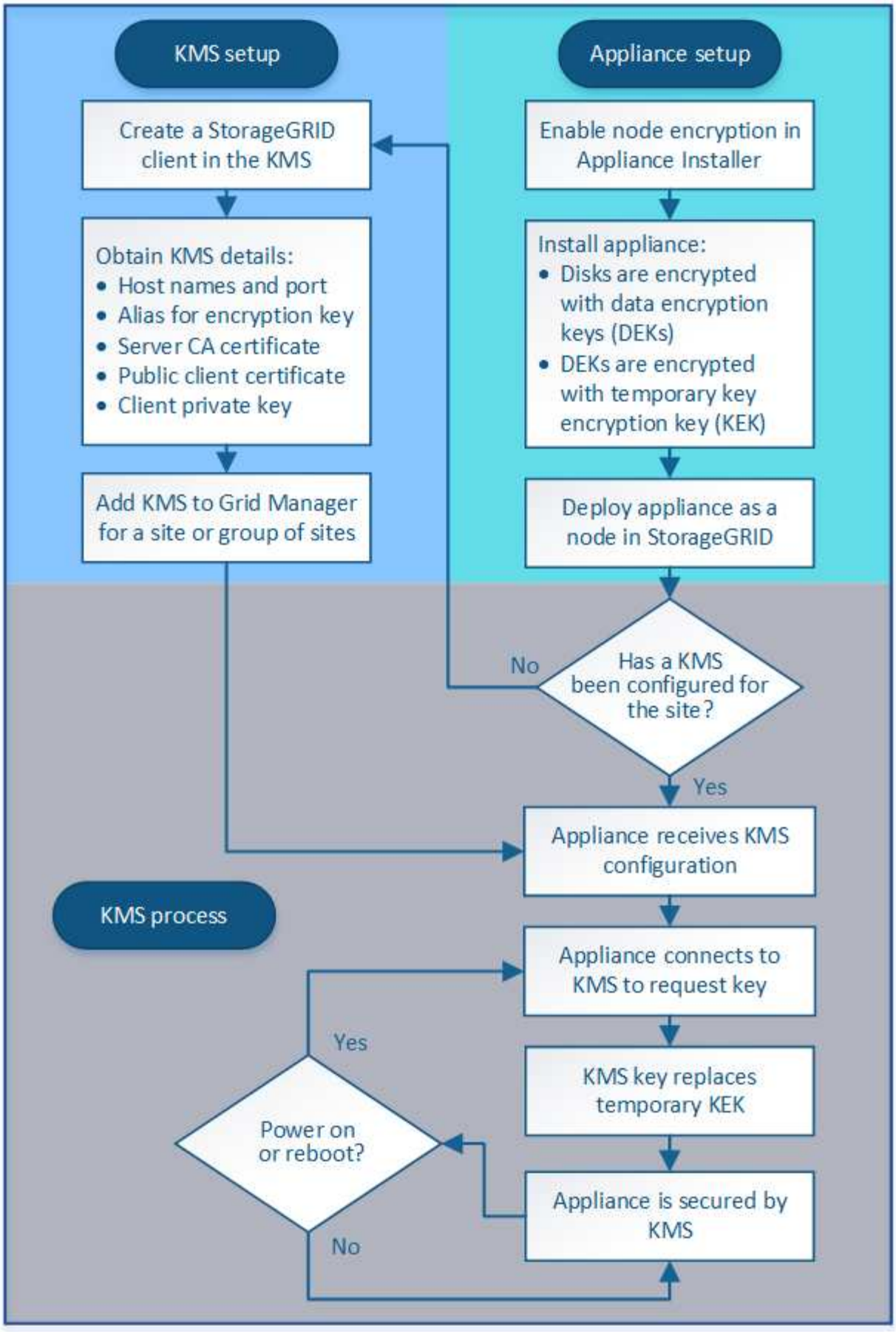
- È possibile utilizzare un KMS per proteggere i nodi dell'appliance e la funzione di sicurezza del disco di Gestione di sistema di SANtricity per "crittografare `din doppio`" i dati sulle unità con crittografia automatica delle stesse appliance.
- È possibile utilizzare un KMS per proteggere i dati sui nodi dell'appliance e l'opzione griglia crittografia 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.

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
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 del nodo abilitata.

2. Eseguire il programma di installazione dell'appliance StorageGRID. Durante l'installazione, a ciascun volume dell'appliance viene assegnata una chiave di crittografia dei dati casuale (DEK), come segue:
   - I DEK vengono utilizzati per crittografare i dati su ciascun volume. Queste chiavi vengono generate utilizzando la crittografia del disco Linux Unified Key Setup (LUKS) nel sistema operativo dell'appliance e non possono essere modificate.
   - Ogni singolo DEK viene crittografato mediante una chiave di crittografia della chiave master (KEK). La chiave iniziale KEK è una chiave temporanea che crittografa i DEK fino a quando l'appliance non riesce a connettersi al KMS.
3. Aggiungere il nodo appliance a StorageGRID.

Per ulteriori informazioni, fare riferimento a quanto segue:

- Appliance di servizi SG100 e SG1000
- Appliance di storage SG6000
- Appliance di storage SG5700
- Appliance di storage SG5600

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.

Quali sono i requisiti KMIP?

StorageGRID supporta KMIP versione 1.4.

"Key Management Interoperability Protocol Specification versione 1.4"

Le comunicazioni tra i nodi dell'appliance e il KMS configurato utilizzano connessioni TLS sicure. StorageGRID supporta i seguenti cifrari TLS v1.2 per KMIP:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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.

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.

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 attivato la crittografia dei nodi.

È possibile utilizzare il KMS configurato per i seguenti appliance StorageGRID e nodi appliance:

Appliance	Tipo di nodo
Appliance di servizi SG1000	Nodo Admin o nodo gateway
Appliance di servizi SG100	Nodo Admin o nodo gateway
Appliance di storage SG6000	Nodo di storage
Appliance di storage SG5700	Nodo di storage
Appliance di storage SG5600	Nodo di storage

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.

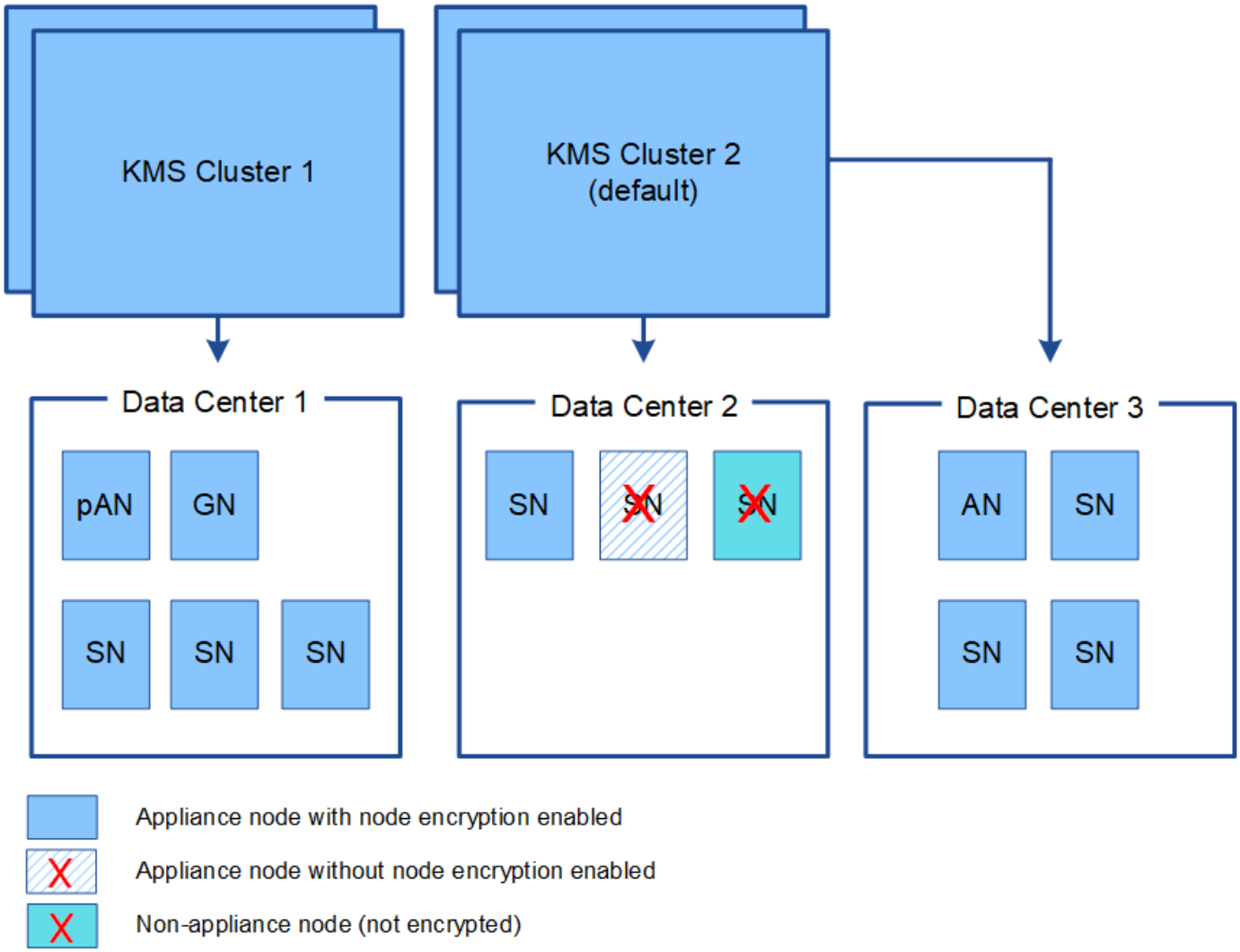
Quanti server di gestione delle chiavi sono necessari?

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 ruotare periodicamente la chiave di crittografia utilizzata da ciascun KMS configurato.

Quando si ruota la chiave di crittografia, utilizzare il software KMS per eseguire la rotazione dall'ultima versione della chiave utilizzata a una nuova versione della stessa chiave. Non ruotare su una chiave completamente diversa.

> Non tentare mai di ruotare una chiave modificando il nome della chiave (alias) per il KMS in Grid Manager. Al contrario, ruotare la chiave aggiornando la versione della chiave nel software KMS. Utilizzare lo stesso alias per le nuove chiavi utilizzato per le chiavi precedenti. Se si modifica l'alias della chiave per un KMS configurato, StorageGRID potrebbe non essere in grado di decrittare i dati.

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.

Informazioni correlate

- Appliance di servizi SG100 e SG1000
- Appliance di storage SG6000
- Appliance di storage SG5700
- Appliance di storage SG5600

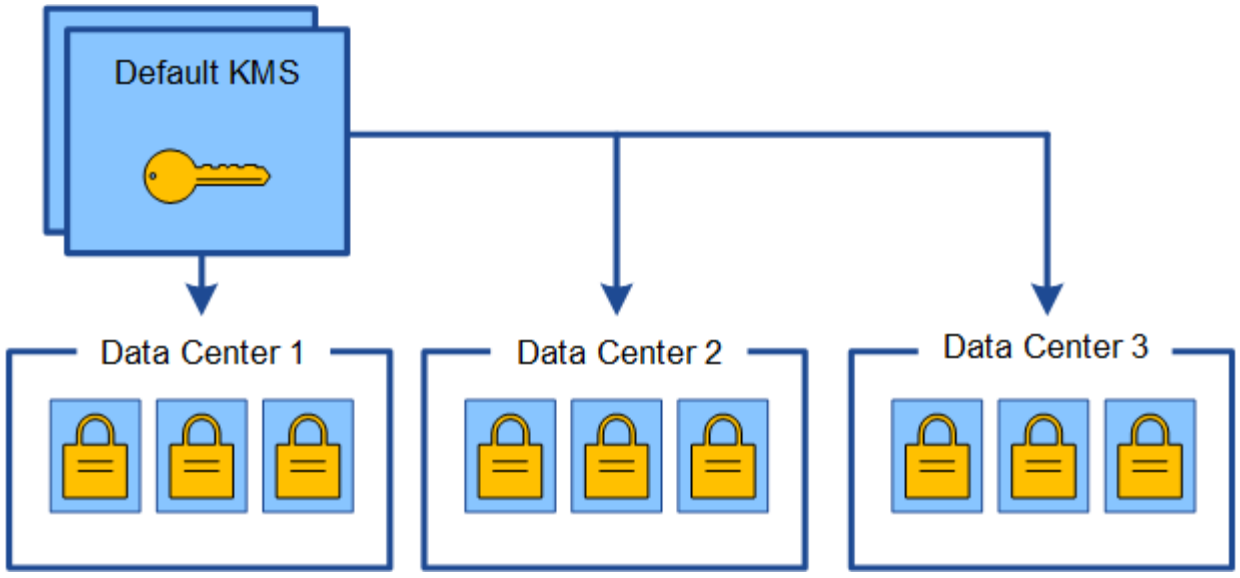
Considerazioni per la modifica del KMS per un sito

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.

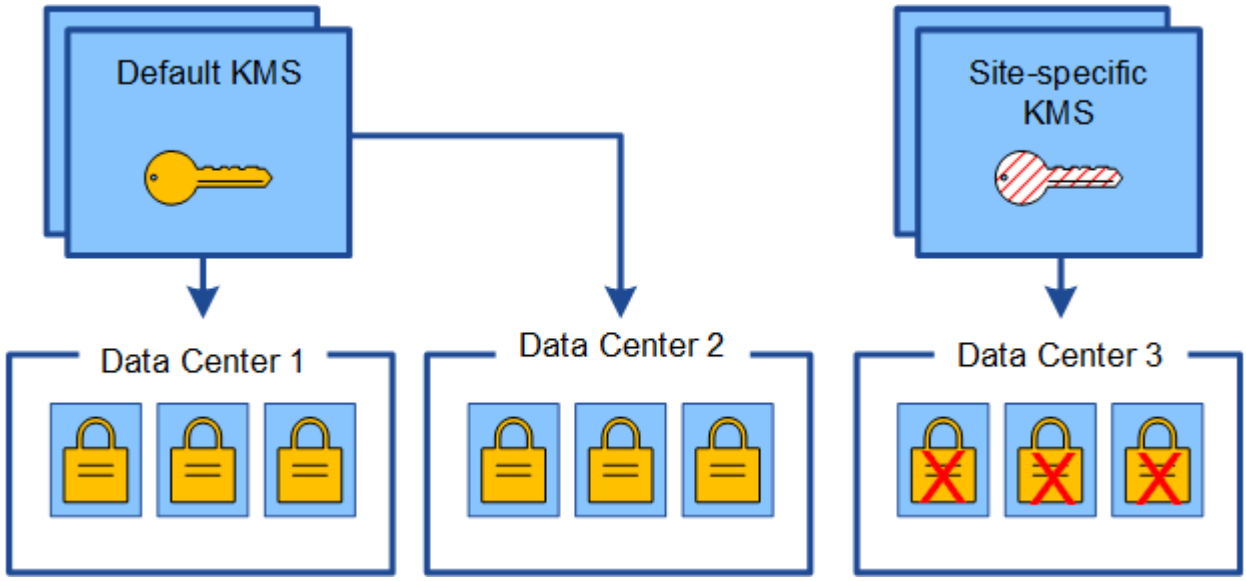
Se si modifica il KMS utilizzato per un sito, è necessario assicurarsi che i nodi appliance precedentemente crittografati in quel sito possano essere decifrati utilizzando la chiave memorizzata nel nuovo KMS. In alcuni casi, potrebbe essere necessario copiare la versione corrente della chiave di crittografia 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:

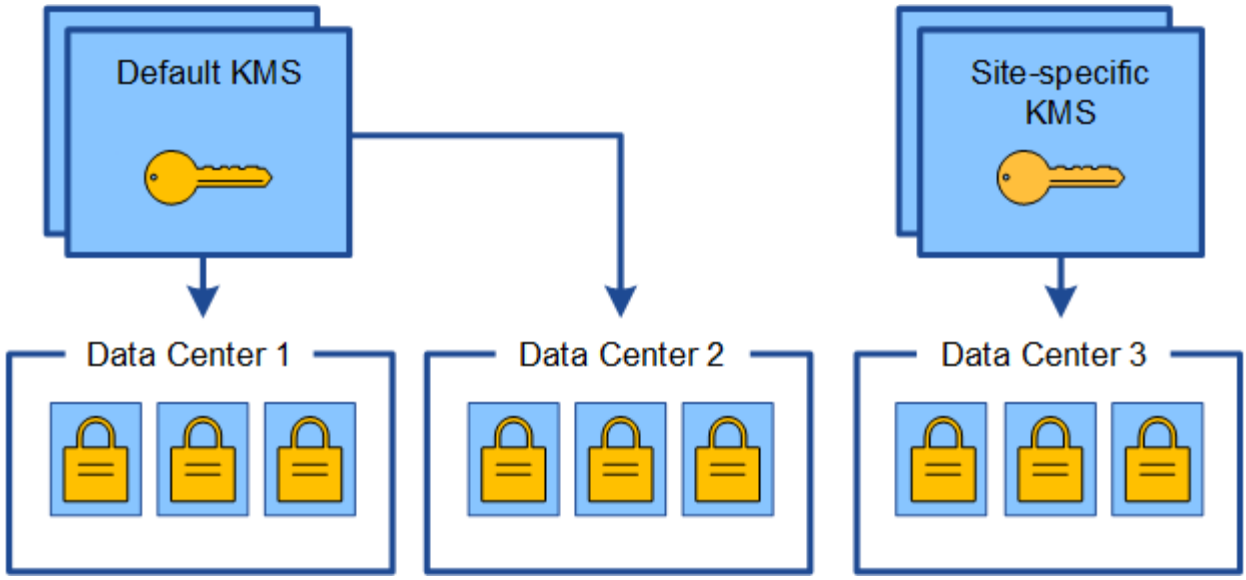
1. Inizialmente si configura un KMS predefinito che si applica a tutti i siti che non dispongono di un KMS dedicato.
2. Una volta salvato il KMS, tutti i nodi appliance con l'impostazione **Node Encryption** attivata si connettono al KMS e richiedono la chiave di crittografia. Questa chiave viene utilizzata 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)

Caso d'utilizzo per la modifica del KMS di un sito	Passaggi richiesti
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.

A proposito di questa attività

Queste istruzioni si applicano a Thales CipherTrust Manager k170v, versioni 2.0, 2.1 e 2.2. In caso di domande sull'utilizzo di un altro server di gestione delle chiavi con StorageGRID, contattare il supporto tecnico.

"Thales CipherTrust Manager"

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. Dal software KMS, creare una chiave di crittografia AES per ogni cluster KMS o KMS.

   La chiave di crittografia deve essere esportabile.

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.

   > La chiave di crittografia deve già esistere nel KMS. StorageGRID non crea o gestisce chiavi 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.

Di cosa hai bisogno

- Hai esaminato il considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi.
- Lo hai fatto StorageGRID configurato come client nel KMSE si dispone delle informazioni necessarie per ogni cluster KMS o KMS.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'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.

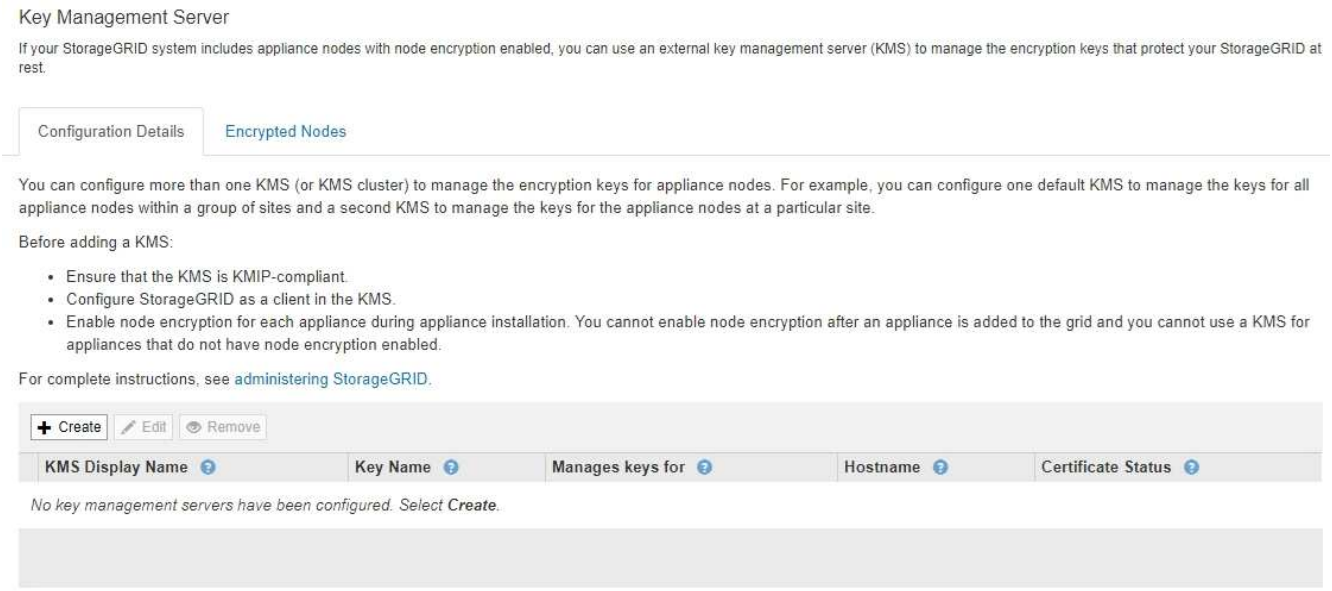
Fase 1: Inserire i dettagli KMS

Nella fase 1 (inserire i dettagli KMS) della procedura guidata Add a Key Management Server (Aggiungi un server di gestione delle chiavi), vengono forniti i dettagli relativi al cluster KMS o KMS.

Fasi

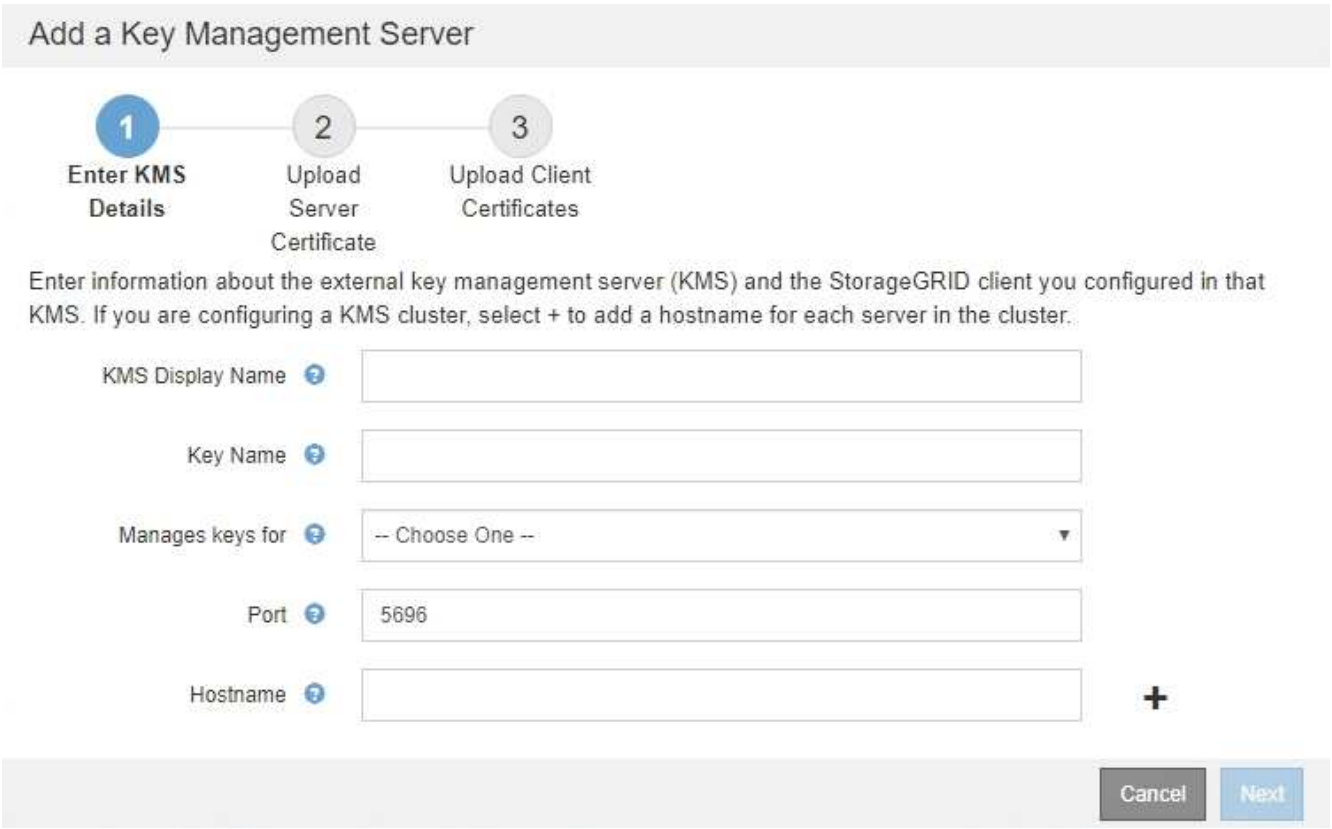
1. Selezionare **CONFIGURATION Security Key management server**.

   Viene visualizzata la pagina Key Management Server (Server di gestione chiavi) con la scheda Configuration Details (Dettagli configurazione) selezionata.



2. Selezionare **Crea**.

   Viene visualizzata la fase 1 (immettere i 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 visualizzato DI KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.

Campo	Descrizione
Key Name (Nome chiave)	L'alias esatto della chiave per il client StorageGRID nel KMS. Deve essere compreso tra 1 e 255 caratteri.
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 da applicare 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.
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. **Nota:** il campo 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.

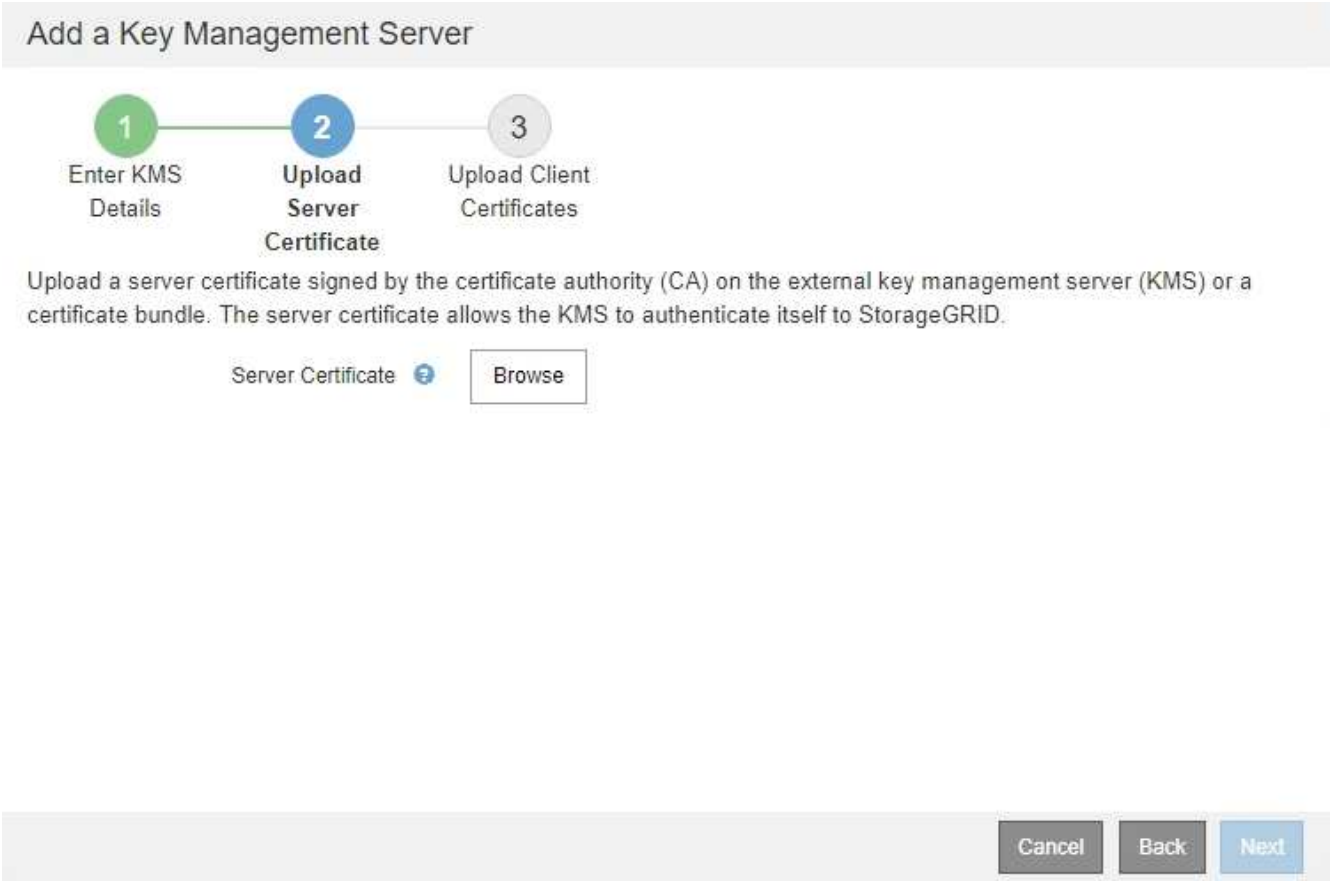
4. Se si utilizza un cluster KMS, selezionare il segno più ➕ per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Avanti**.

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.

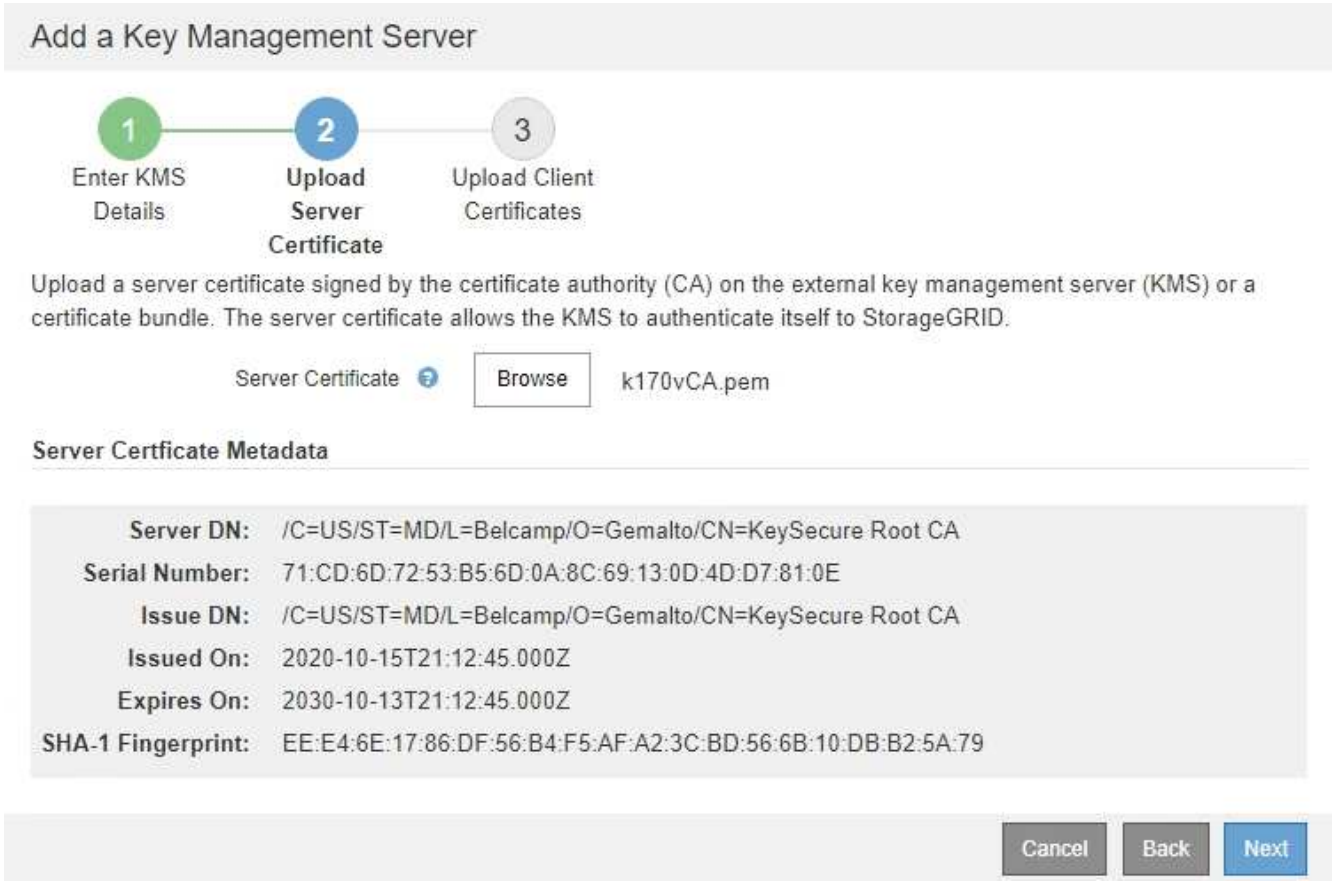
Fasi

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.

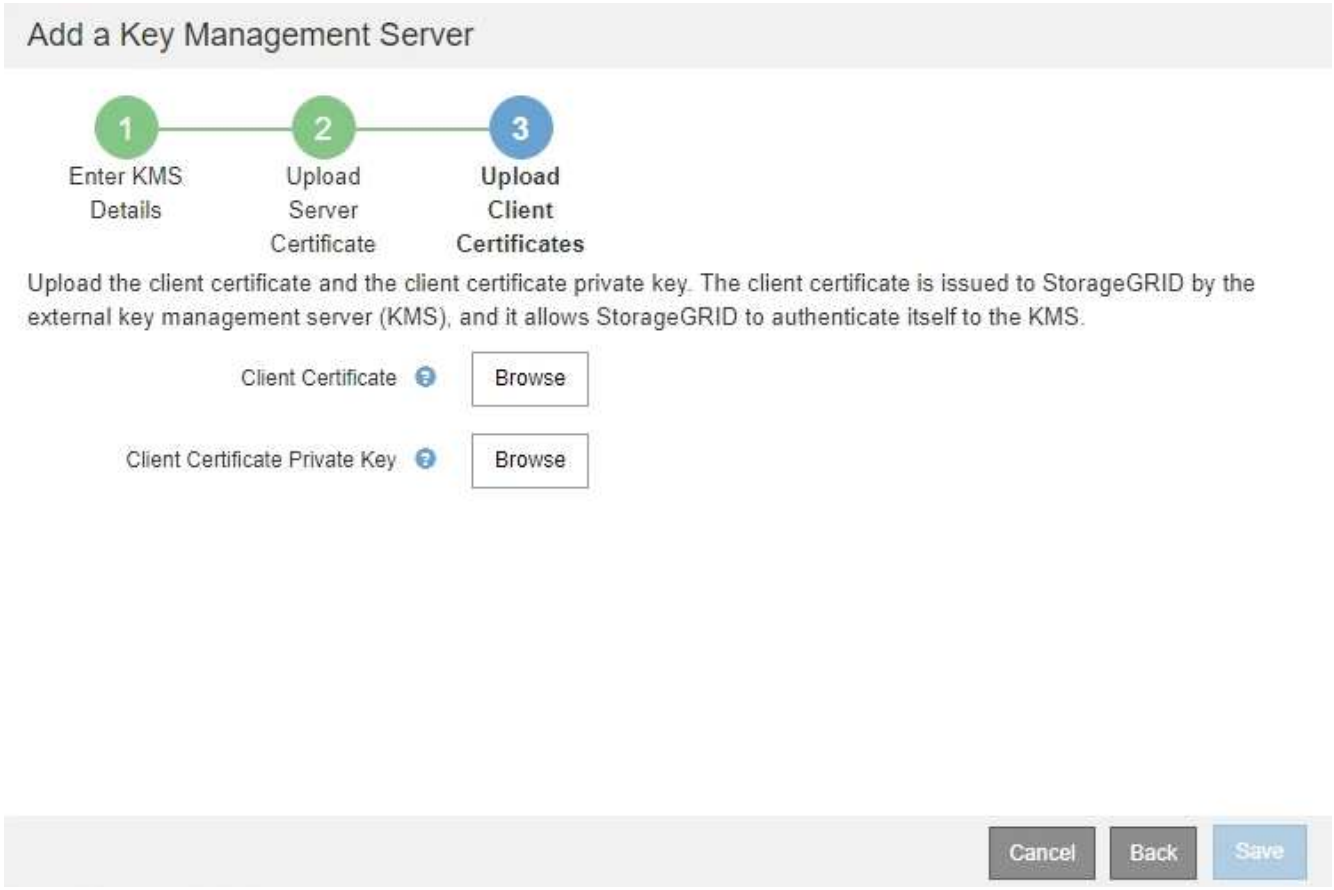
3. Selezionare **Avanti**.

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.

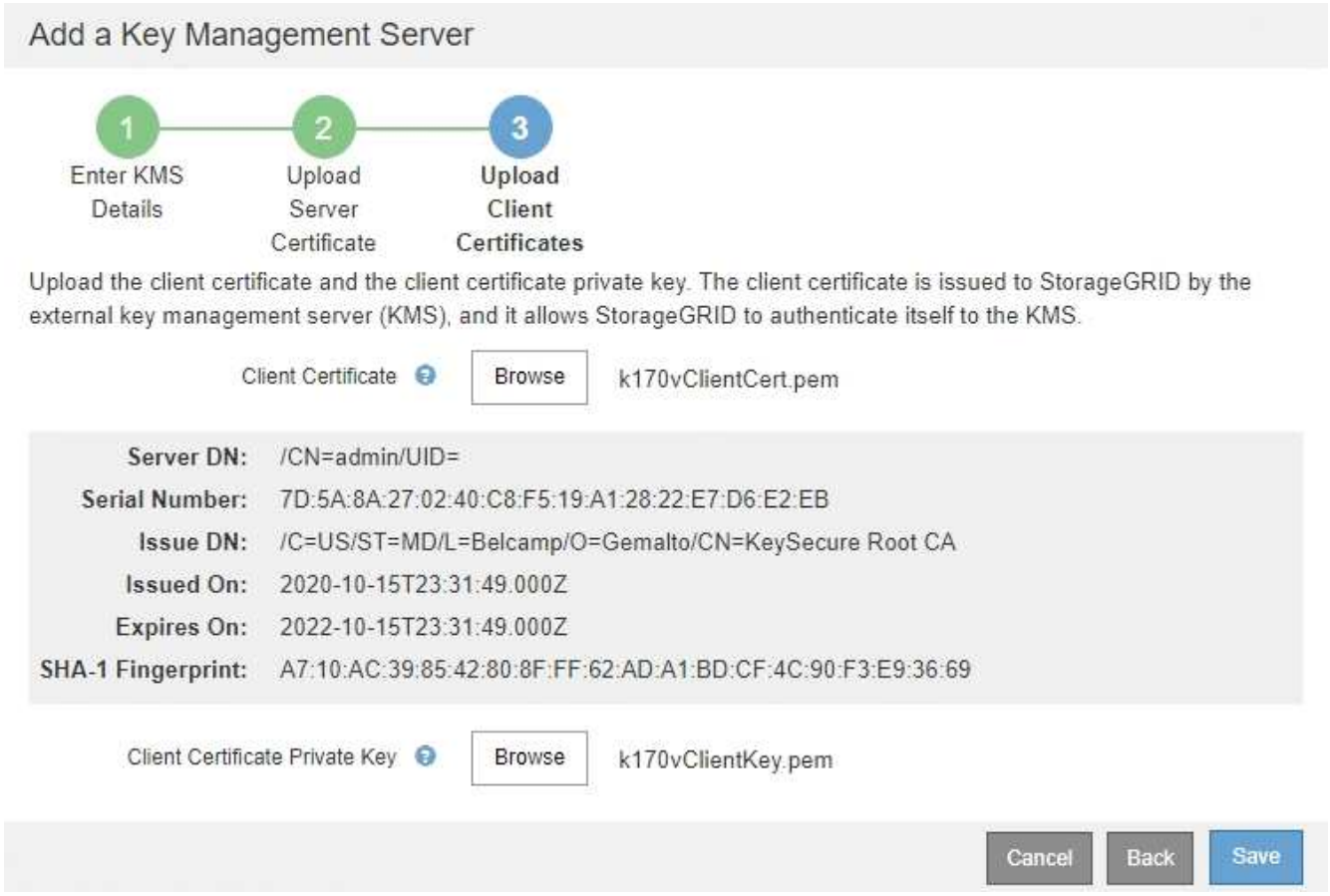


2. Caricare il file di certificato del client.

   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.

   Vengono visualizzati i metadati per il certificato client e la chiave privata del certificato client.



5. Selezionare **Salva**.

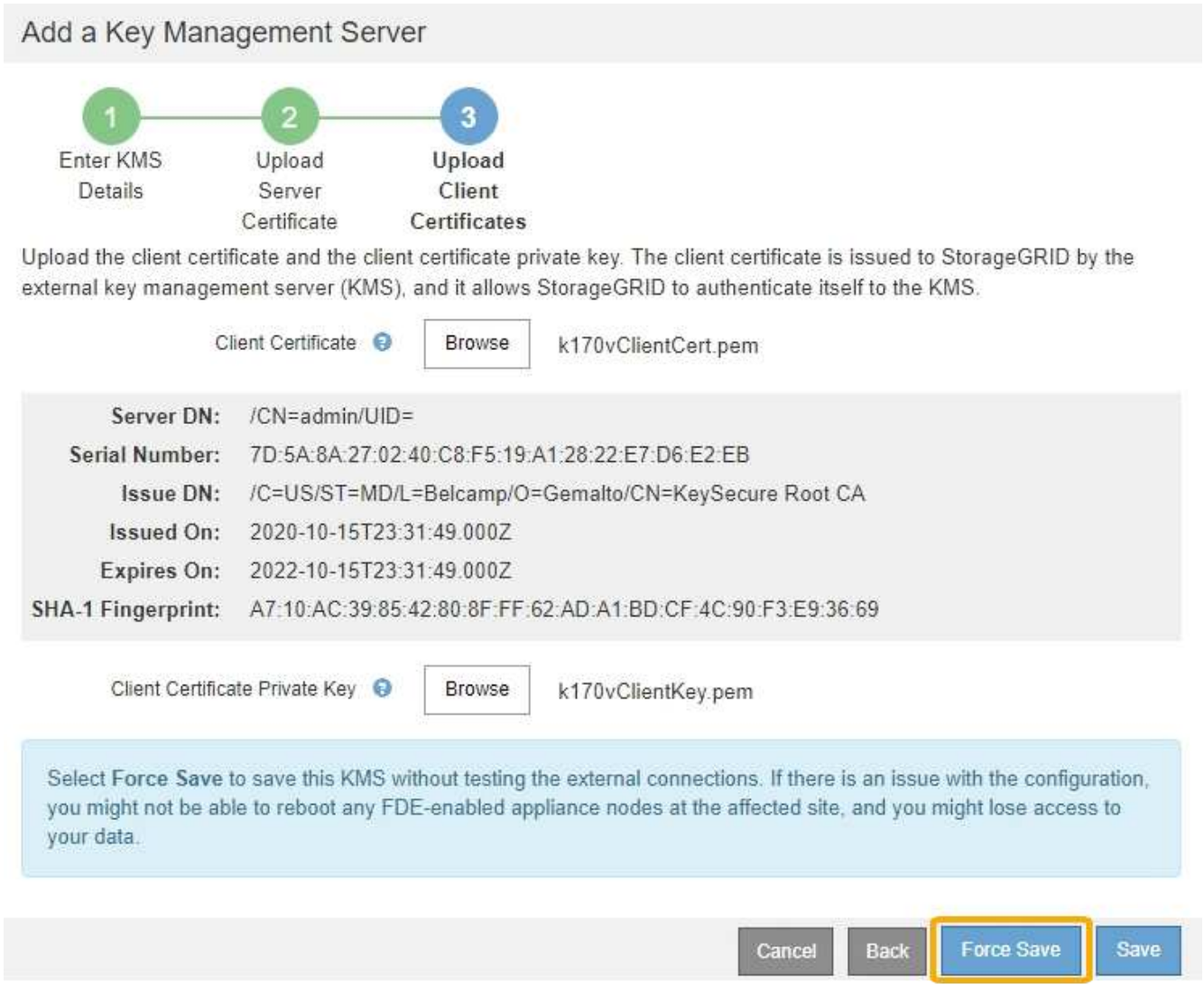
   Vengono verificate le connessioni tra il server di gestione delle chiavi e i nodi dell'appliance. Se tutte le connessioni sono valide e la chiave corretta viene trovata nel KMS, il nuovo server di gestione delle chiavi viene aggiunto alla tabella nella pagina Server di gestione delle chiavi.

   > 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 **Salva**, rivedere i dettagli del messaggio e selezionare **OK**.

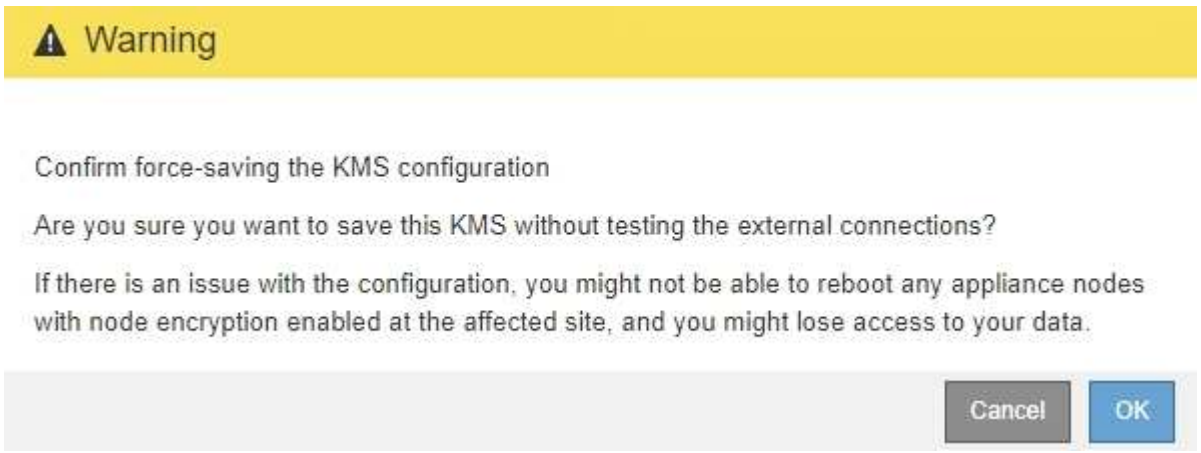
   Ad esempio, se un test di connessione non riesce, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

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.

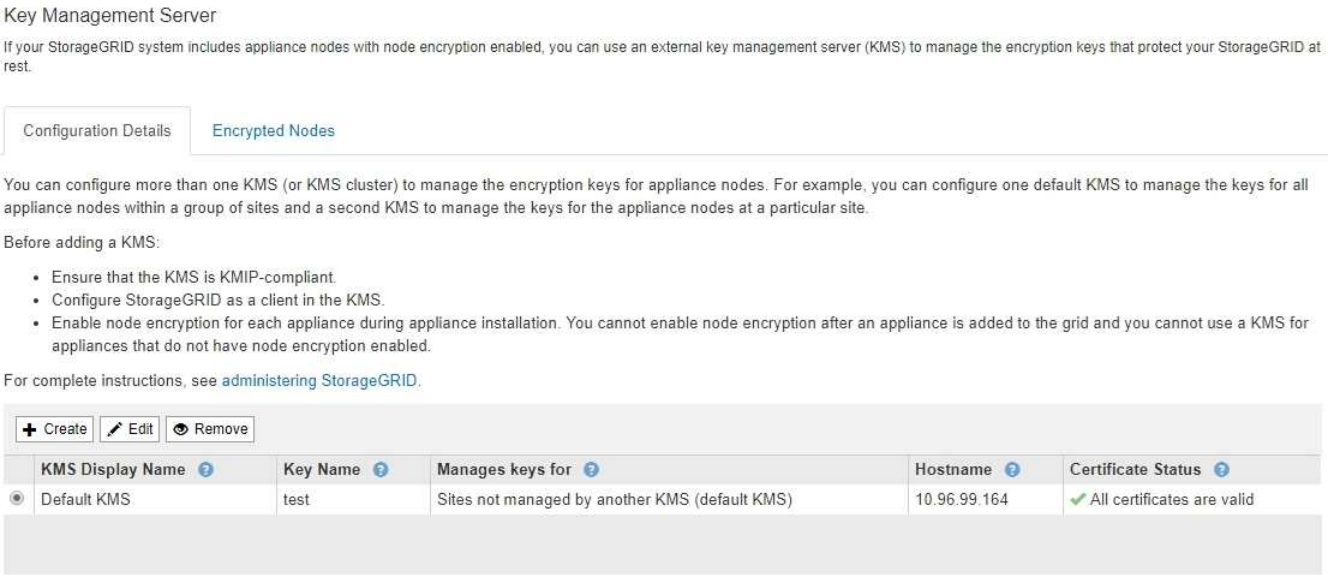
Visualizza i dettagli di KMS

È possibile visualizzare informazioni su ciascun server di gestione delle chiavi (KMS) nel sistema StorageGRID, incluso lo stato corrente dei certificati server e client.

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. Rivedere le informazioni nella tabella per ciascun KMS.

Campo	Descrizione
Nome visualizzato DI KMS	Il nome descrittivo del KMS.
Key Name (Nome chiave)	L'alias della chiave per il client StorageGRID nel KMS.
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).**

Campo	Descrizione
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 quindi selezionare **Edit**.
Stato del certificato	Stato corrente del certificato del server, del certificato CA opzionale e del certificato del client: Valido, scaduto, in fase di scadenza o sconosciuto. **Nota:** potrebbero essere necessari 30 minuti per ottenere gli aggiornamenti dello stato del certificato da parte di StorageGRID. È necessario aggiornare il browser Web per visualizzare i valori correnti.

3. Se lo stato del certificato è sconosciuto, attendere fino a 30 minuti, quindi aggiornare il browser Web.

> 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 effettivo.

4. Se la colonna Stato certificato indica che un certificato è scaduto o sta per scadere, risolvere il problema il prima possibile.

   Consultare le azioni consigliate per gli avvisi **scadenza certificato CA KMS**, **scadenza certificato client KMS** e **scadenza certificato server KMS** nelle istruzioni per Monitoraggio e risoluzione dei problemi di StorageGRID.

> Per mantenere l'accesso ai dati, è necessario risolvere al più presto eventuali problemi di certificato.

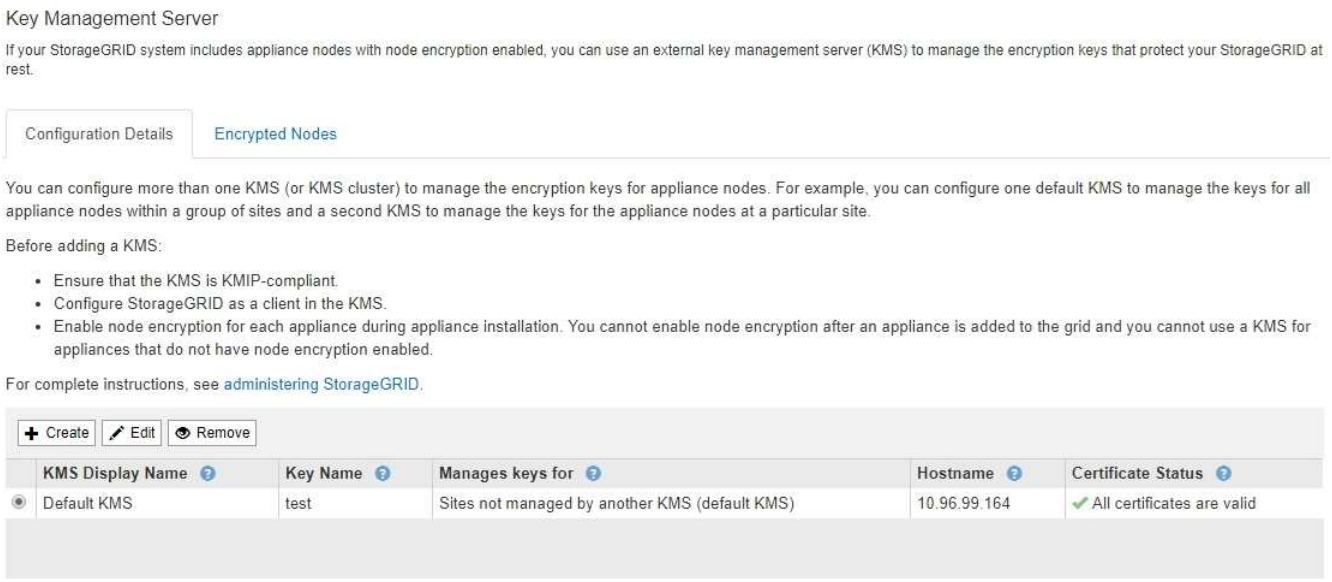
Visualizzare i nodi crittografati

È possibile visualizzare informazioni sui nodi appliance nel sistema StorageGRID per i quali è stata attivata l'impostazione **crittografia nodo**.

Fasi

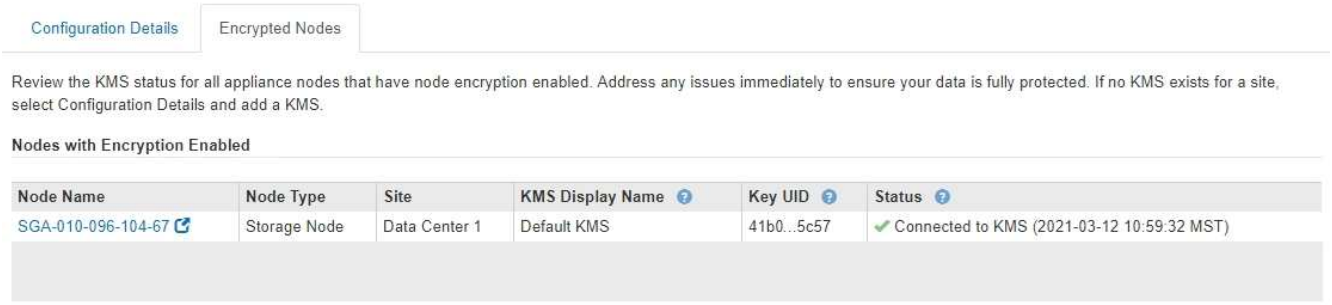
1. Selezionare **CONFIGURATION Security Key management server**.

   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.

Colonna	Descrizione
Tipo di nodo	Il tipo di nodo: Storage, Admin o Gateway.
Sito	Il nome del sito StorageGRID in cui è installato il nodo.
Nome visualizzato DI KMS	Il nome descrittivo del KMS utilizzato per il nodo. Se non è elencato alcun KMS, selezionare la scheda Dettagli di configurazione per aggiungere un KMS. Aggiunta di un server di gestione delle chiavi (KMS)
UID chiave	ID univoco della chiave di crittografia utilizzata per crittografare e decrittare i dati sul nodo dell'appliance. Per visualizzare un intero UID chiave, spostare il cursore sulla cella. 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:** per visualizzare i nuovi valori, è necessario aggiornare il browser Web.

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

   Consultare le azioni consigliate per questi avvisi nelle istruzioni di Monitoraggio e risoluzione dei problemi di StorageGRID.

   È necessario affrontare immediatamente qualsiasi problema per garantire la completa protezione dei dati.

Modifica di un server di gestione delle chiavi (KMS)

Potrebbe essere necessario modificare la configurazione di un server di gestione delle chiavi, ad esempio, se un certificato sta per scadere.

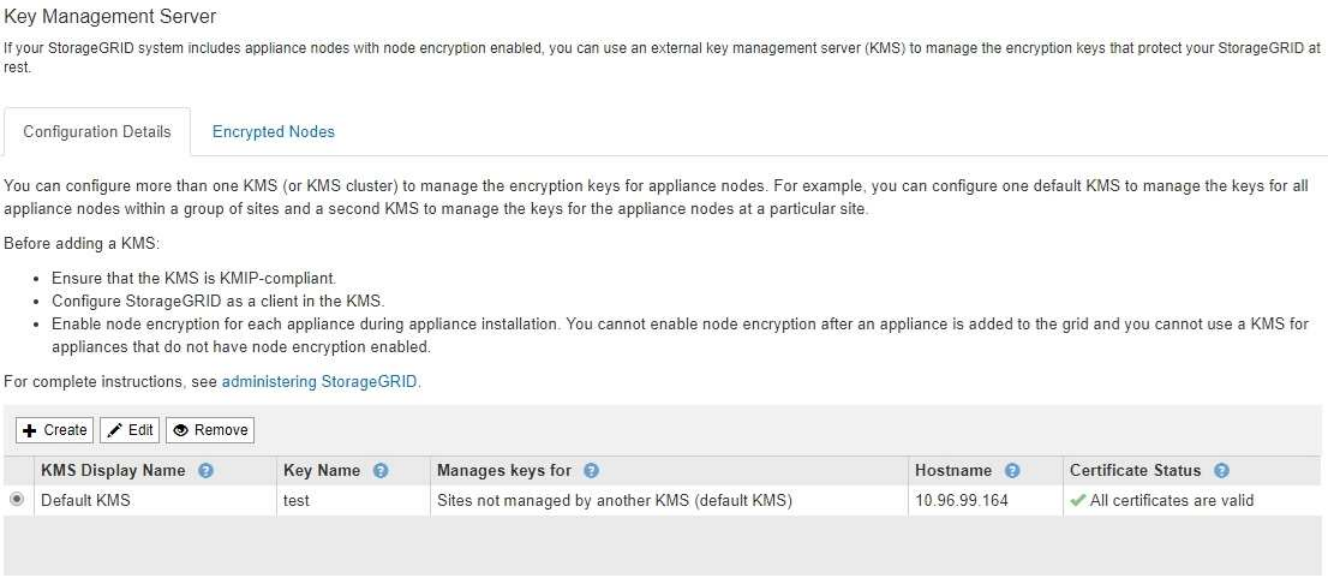
Di cosa hai bisogno

- Hai esaminato il considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi.
- 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.
- Si dispone dell'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 **Edit** (Modifica).
3. Se si desidera, aggiornare i dettagli nel **Passo 1 (Immetti dettagli KMS)** della procedura guidata Modifica un server di gestione delle chiavi.

Campo	Descrizione
Nome visualizzato DI KMS	Un nome descrittivo per aiutarti a identificare questo KMS. Deve essere compreso tra 1 e 64 caratteri.

Campo	Descrizione
Key Name (Nome 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. Non tentare mai di ruotare una chiave cambiando il nome della chiave (alias) per il KMS. Al contrario, ruotare la chiave aggiornando la versione della chiave nel software 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. Considerazioni e requisiti per l'utilizzo di un server di gestione delle chiavi
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 si modifica un KMS specifico del sito, non è possibile selezionare un altro sito. Se si sta modificando il KMS predefinito, non è possibile selezionare un sito specifico.
Porta	La porta utilizzata dal server KMS per le comunicazioni KMIP (Key Management Interoperability Protocol). Il valore predefinito è 5696, ovvero la porta standard KMIP.
Nome host	Il nome di dominio completo o l'indirizzo IP del KMS. **Nota:** il campo 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 il segno più ➕ per aggiungere un nome host per ciascun server nel cluster.
5. Selezionare **Avanti**.

   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 **Avanti**.

   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 **Salva**.

   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**.

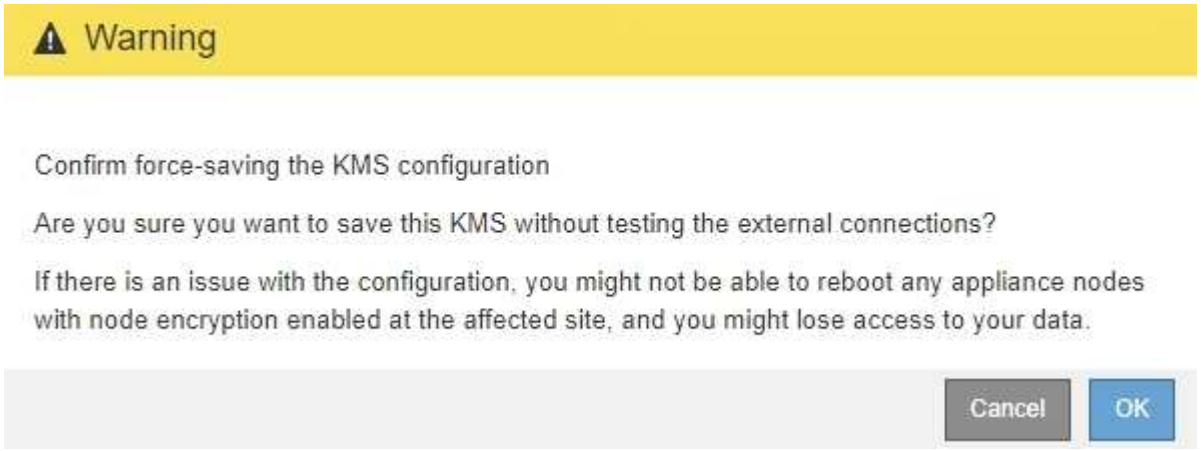
    Ad esempio, se il sito selezionato per questo KMS è già gestito da un altro KMS o se un test di connessione non ha avuto esito positivo, potrebbe essere visualizzato un errore 422: Unprocessable Entity.

11. Se è necessario salvare la configurazione corrente prima di risolvere gli errori di connessione, selezionare **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.

    La configurazione KMS viene salvata.

12. 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.

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.

Di cosa hai bisogno

- 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.
- Si dispone dell'autorizzazione di accesso root.

A proposito di questa attività

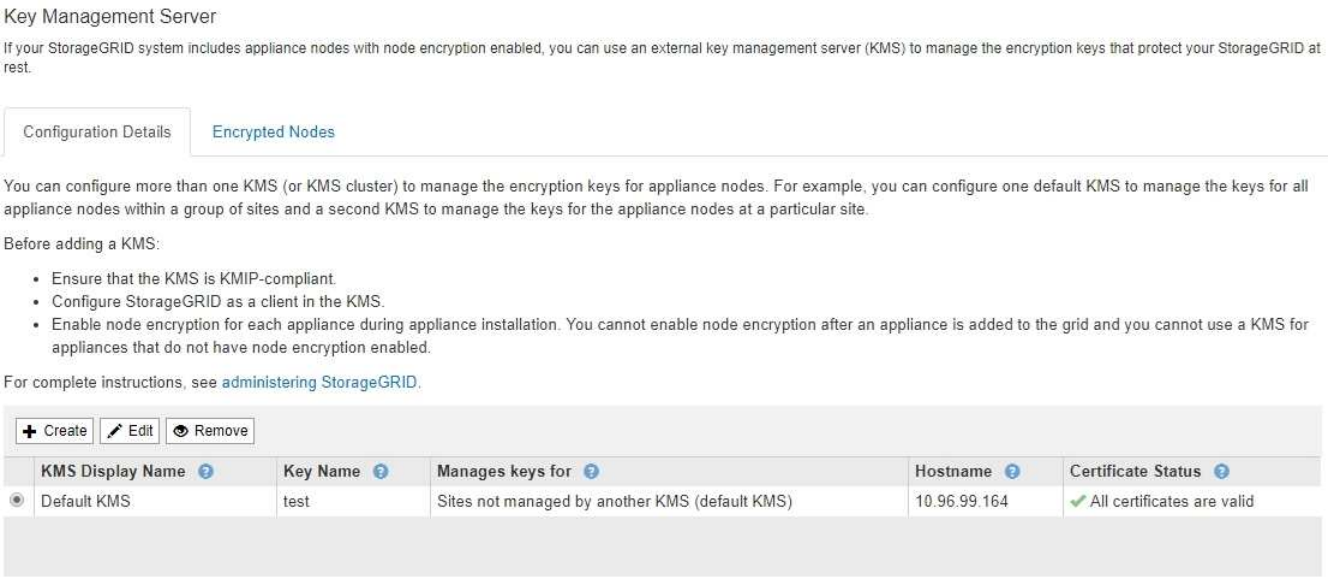
È possibile rimuovere un KMS nei seguenti casi:

- 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.

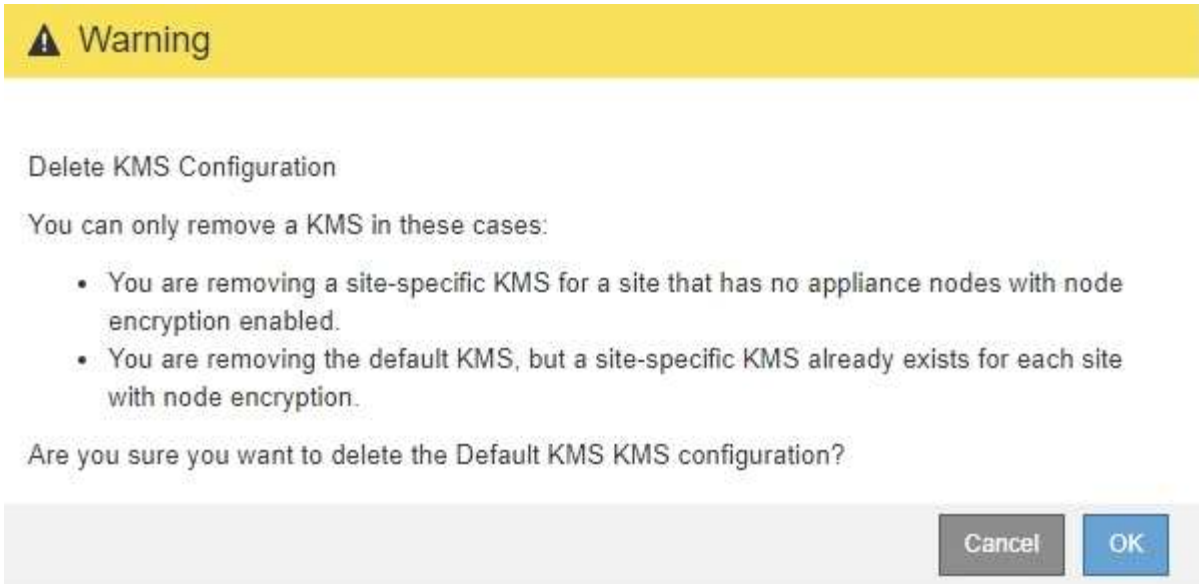
Fasi

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 pulsante di opzione relativo al KMS che si desidera rimuovere e selezionare **Remove** (Rimuovi).
3. Esaminare le considerazioni nella finestra di dialogo di avviso.



4. Selezionare **OK**.

   La configurazione KMS viene rimossa.

Gestire le impostazioni del proxy

Configurare le impostazioni del proxy di storage

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.

Di cosa hai bisogno

- Si dispone di autorizzazioni di accesso specifiche.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.

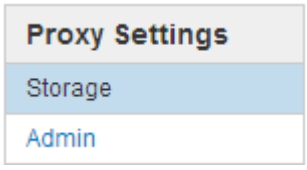
A proposito di questa attività

È possibile configurare le impostazioni per un singolo Storage Proxy.

Fasi

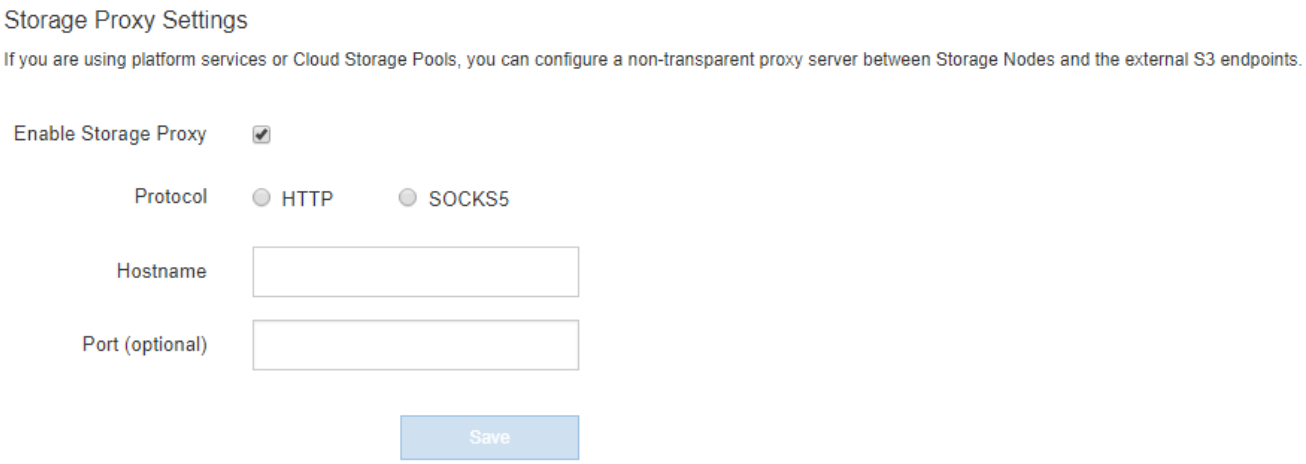
1. Selezionare **CONFIGURAZIONE sicurezza Impostazioni proxy**.

   Viene visualizzata la pagina Storage Proxy Settings (Impostazioni proxy storage). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.



2. Selezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage).

Vengono visualizzati i campi per la configurazione di un proxy di storage.



3. Selezionare il protocollo per il proxy dello storage non trasparente.
4. Immettere il nome host o l'indirizzo IP del server proxy.
5. Facoltativamente, inserire la porta utilizzata per connettersi al server proxy.

   È possibile lasciare vuoto questo campo se si utilizza la porta predefinita per il protocollo: 80 per HTTP o 1080 per SOCKS5.

6. Selezionare **Salva**.

   Una volta salvato il proxy dello storage, è possibile configurare e testare i 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.

Al termine

Se è necessario disattivare un proxy di storage, deselezionare la casella di controllo **Enable Storage Proxy** (attiva proxy di storage) e selezionare **Save** (Salva).

Informazioni correlate

- Rete e porte per i servizi della piattaforma
- Gestire gli oggetti con ILM

Configurare le impostazioni del proxy amministratore

Se si inviano messaggi AutoSupport utilizzando HTTP o HTTPS (vedere Configurare AutoSupport), è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico (AutoSupport).

Di cosa hai bisogno

- Si dispone di autorizzazioni di accesso specifiche.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.

A proposito di questa attività

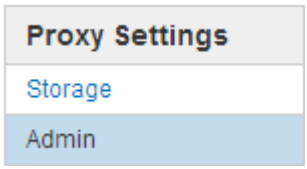
È possibile configurare le impostazioni per un singolo proxy Admin.

Fasi

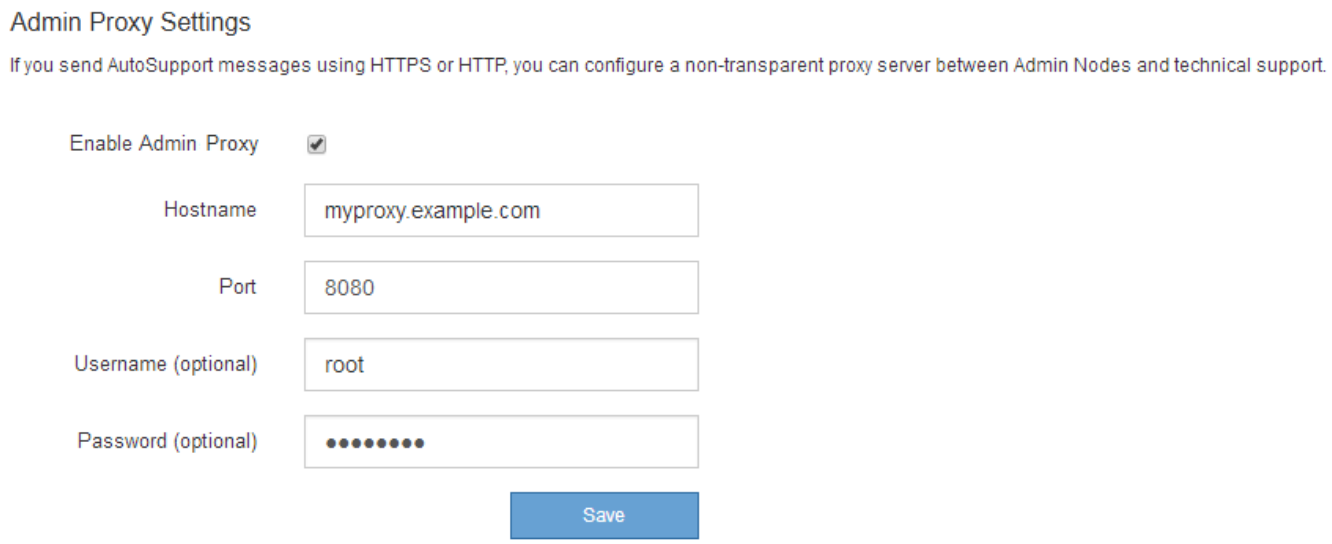
1. Selezionare **CONFIGURAZIONE sicurezza Impostazioni proxy**.

   Viene visualizzata la pagina Admin Proxy Settings (Impostazioni proxy amministratore). Per impostazione predefinita, nel menu della barra laterale è selezionata l'opzione **Storage**.

2. Dal menu della barra laterale, selezionare **Admin**.



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. Se si desidera, inserire il nome utente del proxy.

   Lasciare vuoto questo campo se il server proxy non richiede un nome utente.

7. Se si desidera, inserire la password del proxy.

   Lasciare vuoto questo campo se il server proxy non richiede una password.

8. Selezionare **Salva**.

   Una volta salvato il proxy Admin, 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, deselezionare la casella di controllo **Enable Admin Proxy** (attiva

proxy amministratore) e selezionare **Save** (Salva).

Gestire reti client non attendibili

Gestisci reti client non attendibili: Panoramica

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 tutte le porte esterne disponibili (vedere le informazioni sulle comunicazioni esterne nella sezione Linee guida per il networking).

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.

Esempio 1: Il nodo gateway accetta solo richieste HTTPS S3

Si supponga che un nodo gateway rifiuti tutto il traffico in entrata sulla rete client, ad eccezione delle richieste HTTPS S3. Eseguire le seguenti operazioni generali:

1. Dalla pagina degli endpoint del bilanciamento del carico, configurare un endpoint del bilanciamento del carico per S3 su HTTPS sulla porta 443.
2. Nella pagina Untrusted Client Networks (reti client non attendibili), 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 abilitare il traffico di servizio 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:

- Nella pagina Untrusted Client Networks (reti client non attendibili), indicare che la rete client sul nodo di storage non è attendibile.

Dopo aver salvato la configurazione, il nodo di storage non accetta più il traffico in entrata sulla rete client, ma continua a consentire le richieste in uscita ad Amazon Web Services.

Specificare che la rete client del nodo non è attendibile

Se si utilizza una rete client, è possibile specificare se la rete client di ciascun nodo è attendibile o meno. È inoltre possibile specificare l'impostazione predefinita per i nuovi nodi aggiunti in un'espansione.

Di cosa hai bisogno

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

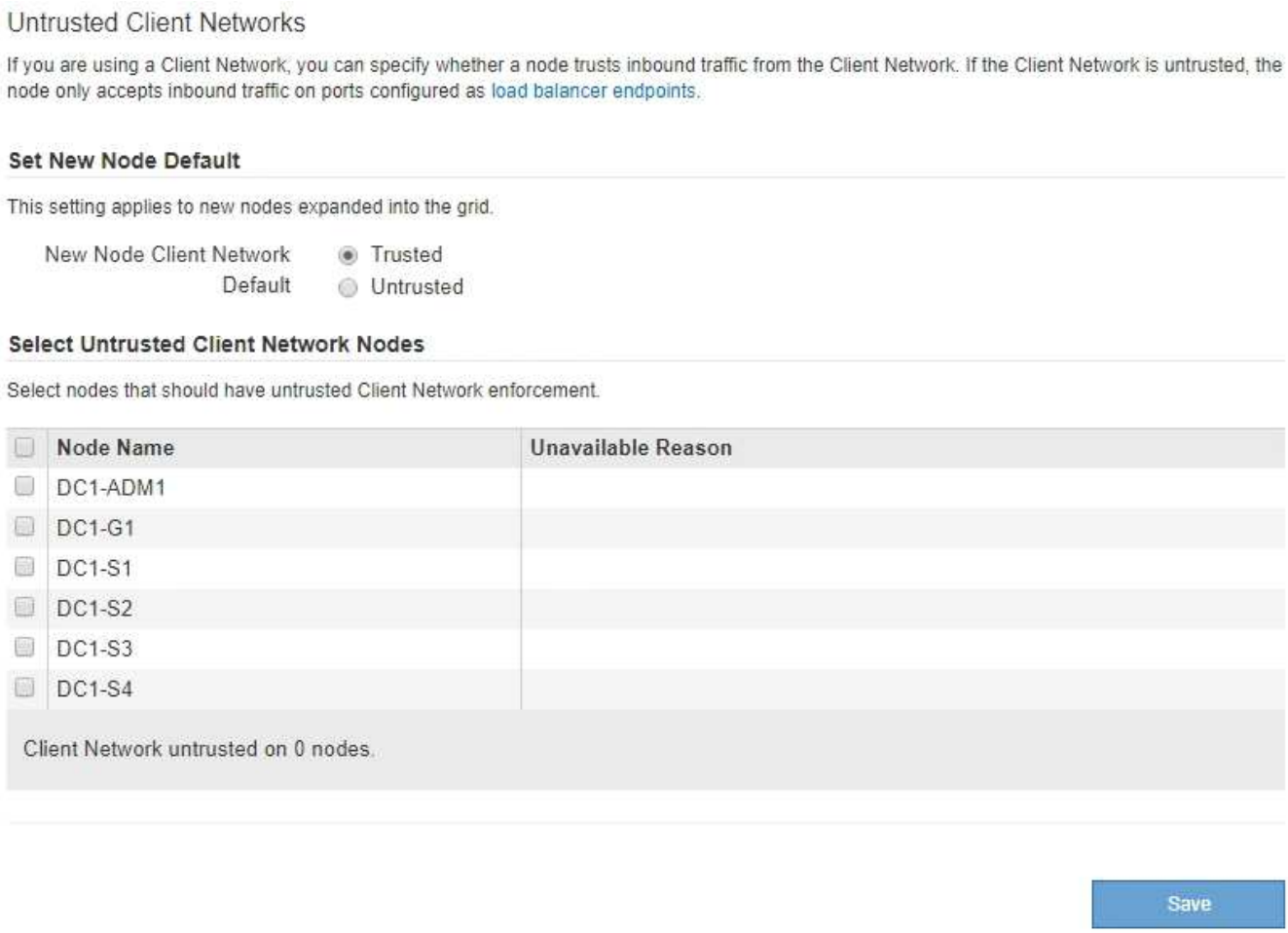
- Si dispone dell'autorizzazione di accesso root.
- Se si desidera che un nodo Admin o un nodo gateway accetti il traffico in entrata solo su endpoint configurati esplicitamente, sono stati definiti gli endpoint del bilanciamento del carico.

> Le connessioni client esistenti potrebbero non riuscire se gli endpoint del bilanciamento del carico non sono stati configurati.

Fasi

1. Selezionare **CONFIGURAZIONE sicurezza reti client non attendibili**.

   La pagina reti client non attendibili elenca tutti i nodi nel sistema StorageGRID. La colonna motivo non disponibile include una voce se la rete client del nodo deve essere attendibile.



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**: Quando un nodo viene aggiunto in un'espansione, la sua rete client è attendibile.
   - **Untrusted**: Quando un nodo viene aggiunto in un'espansione, la sua rete client non è attendibile. Se necessario, tornare a questa pagina per modificare l'impostazione di un nuovo nodo specifico.

   > Questa impostazione non influisce sui nodi esistenti nel sistema StorageGRID.

3. Nella sezione **Select untrusted Client Network Nodes** (Seleziona nodi di rete client non attendibili), selezionare i nodi che devono consentire le connessioni client solo su endpoint del bilanciamento del

carico configurati esplicitamente.

È possibile selezionare o deselezionare la casella di controllo nel titolo per selezionare o deselezionare tutti i nodi.

4. Selezionare **Salva**.

Le nuove regole del firewall vengono aggiunte 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

In qualità di amministratore di grid, è possibile creare e gestire gli account tenant utilizzati dai client S3 e Swift per memorizzare e recuperare oggetti, monitorare l'utilizzo dello storage e gestire le azioni che i client sono in grado di eseguire utilizzando il sistema StorageGRID.

Cosa sono gli account tenant?

Gli account tenant consentono alle applicazioni client che utilizzano l'API REST di S3 (Simple Storage Service) o l'API DI Swift REST di memorizzare e recuperare oggetti su StorageGRID.

Ogni account tenant supporta l'utilizzo di un singolo protocollo, che viene specificato quando si crea l'account. Per memorizzare e recuperare oggetti in un sistema StorageGRID con entrambi i protocolli, è necessario creare due account tenant: Uno per i bucket S3 e gli oggetti e uno per i container Swift e gli oggetti. Ogni account tenant dispone di un proprio ID account, di gruppi e utenti autorizzati, di bucket o container e di oggetti.

Se si desidera separare gli oggetti memorizzati nel sistema da diverse entità, è possibile creare ulteriori account tenant. Ad esempio, è possibile configurare più account tenant in 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 semplicemente i bucket S3 e le policy bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Per ulteriori informazioni, consultare le istruzioni per l'implementazione delle applicazioni client S3.

- **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.

Creare e configurare account tenant

Quando si crea un account tenant, si specificano le seguenti informazioni:

- Visualizza il nome dell'account tenant.
- Quale protocollo client verrà utilizzato dall'account tenant (S3 o Swift).
- Per gli account tenant S3: Se l'account tenant dispone dell'autorizzazione per utilizzare i servizi della piattaforma con i bucket S3. Se si consente agli account tenant di utilizzare i servizi della piattaforma, è necessario assicurarsi che la griglia sia configurata per supportare il loro utilizzo. Vedere "Managing platform Services".
- Facoltativamente, una quota di storage per l'account tenant, ovvero il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant. Se la quota viene superata, il tenant non può creare nuovi oggetti.

> La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco).

- Se la federazione delle identità è attivata per il sistema StorageGRID, il gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant.
- Se l'SSO (Single Sign-on) non è in uso per il sistema StorageGRID, se l'account tenant utilizzerà la propria origine di identità o condividerà l'origine di identità della griglia e la password iniziale per l'utente root locale del tenant.

Una volta creato un account tenant, è possibile eseguire le seguenti attività:

- **Gestisci i servizi della piattaforma per il grid**: Se abiliti i servizi della piattaforma per gli account tenant, assicurati di comprendere come vengono inviati i messaggi dei servizi della piattaforma e i requisiti di rete che l'utilizzo dei servizi della piattaforma comporta nella tua implementazione StorageGRID.
- **Monitorare l'utilizzo dello storage di un account tenant**: Una volta che i tenant iniziano a utilizzare i propri account, è possibile utilizzare Grid Manager per monitorare la quantità di storage consumata da ciascun tenant.

> I valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi della griglia. I totali verranno aggiornati al ripristino della connettività di rete.

  Se sono state impostate le quote per i tenant, è possibile attivare l'avviso **quota elevata del tenant** per determinare se i tenant consumano le quote. Se attivato, questo avviso viene attivato quando un tenant utilizza il 90% della propria quota. Per ulteriori informazioni, consultare il riferimento agli avvisi nelle istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

- **Configure client Operations** (Configura operazioni client): È possibile configurare se alcuni tipi di operazioni client sono vietate.

Configurare i tenant S3

Una volta creato un account tenant S3, gli utenti tenant possono accedere a tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali
- Gestione delle chiavi di accesso S3
- Creazione e gestione di bucket S3
- Monitoraggio dell'utilizzo dello storage

- Utilizzo dei servizi della piattaforma (se abilitati)

> Gli utenti del tenant S3 possono creare e gestire la chiave di accesso S3 e i bucket con Tenant Manager, ma devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti.

Configurare i tenant di Swift

Dopo la creazione di un account tenant Swift, l'utente root del tenant può accedere al tenant Manager per eseguire attività come le seguenti:

- Impostazione della federazione delle identità (a meno che l'origine delle identità non sia condivisa con la griglia) e creazione di gruppi e utenti locali
- Monitoraggio dell'utilizzo dello storage

> Gli utenti Swift devono disporre dell'autorizzazione di accesso root per accedere a Tenant Manager. Tuttavia, l'autorizzazione di accesso root non consente agli utenti di autenticarsi 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.

Informazioni correlate

Utilizzare un account tenant

Creare un account tenant

È necessario creare almeno un account tenant per controllare l'accesso allo storage nel sistema StorageGRID.

Quando si crea un account tenant, specificare un nome, un protocollo client e, facoltativamente, una quota di storage. Se SSO (Single Sign-on) è attivato per StorageGRID, specificare anche quale gruppo federato dispone dell'autorizzazione di accesso root per configurare l'account tenant. Se StorageGRID non utilizza il single sign-on, è necessario specificare se l'account tenant utilizzerà la propria origine di identità e configurare la password iniziale per l'utente root locale del tenant.

Grid Manager offre una procedura guidata che illustra la procedura per la creazione di un account tenant. I passaggi variano in base al tipo di operazione 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.
- 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 istruzioni per la gestione dei gruppi di amministratori.

Fasi

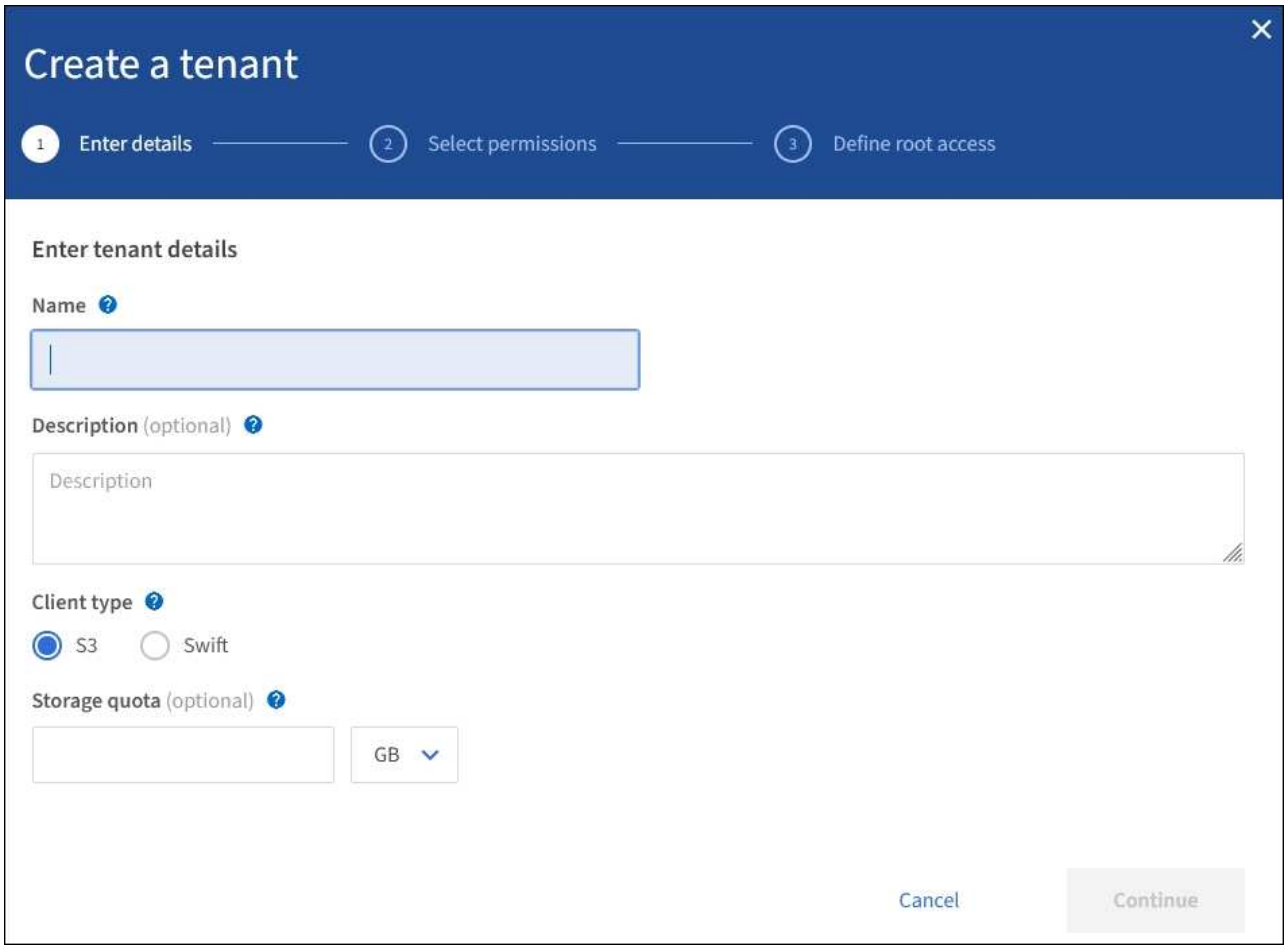
1. Selezionare **TENANT**.
2. Selezionare **Create** (Crea) e immettere le seguenti informazioni per il tenant:
   a. **Nome**: Immettere un nome per l'account tenant. I nomi dei tenant non devono essere univoci. Una

volta creato, l'account tenant riceve un ID account numerico univoco.

b. **Descrizione** (opzionale): Inserire una descrizione che consenta di identificare il tenant.

c. **Client type** (tipo client): Selezionare il tipo di client **S3** o **Swift**.

d. **Storage quota** (opzionale): Se si desidera che il tenant disponga di una quota di storage, immettere un valore numerico per la quota e selezionare le unità corrette (GB, TB o PB).



3. Selezionare **continua** e configurare il tenant S3 o Swift.

Tenant S3

Selezionare le autorizzazioni appropriate per il tenant. Alcune di queste autorizzazioni hanno requisiti aggiuntivi. Per ulteriori informazioni, consultare la guida in linea per ciascuna autorizzazione.

- Consentire i servizi della piattaforma
- USA origine identità propria (selezionabile solo se SSO non viene utilizzato)
- Allow S3 Select (Consenti selezione S3) (vedere Manage S3 (Gestisci S3): Selezionare per gli account tenant)

Tenant rapido

Se il tenant utilizzerà la propria origine di identità, selezionare **Usa origine di identità propria** (selezionabile solo se SSO non viene utilizzato).

1. Selezionare **continua** e definire l'accesso root per l'account tenant.

Federazione di identità non configurata

1. Immettere una password per l'utente root locale.
2. Selezionare **Crea tenant**.

SSO attivato

Quando SSO è abilitato per StorageGRID, il tenant deve utilizzare l'origine dell'identità configurata per il gestore di griglia. Nessun utente locale può accedere. Specificare quale gruppo federato dispone dell'autorizzazione di accesso Root per configurare l'account tenant.

1. Selezionare un gruppo federated esistente da Grid Manager per ottenere l'autorizzazione di accesso root iniziale per il tenant.

   Se si dispone di autorizzazioni adeguate, i gruppi federated esistenti di Grid Manager vengono elencati quando si seleziona il campo. In caso contrario, immettere il nome univoco del gruppo.

2. Selezionare **Crea tenant**.

SSO non abilitato

1. Completare i passaggi descritti nella tabella a seconda che il tenant gestisca i propri gruppi e utenti o utilizzi l'origine dell'identità configurata per Grid Manager.

Se il tenant…	Eseguire questa operazione…
Gestire i propri gruppi e utenti	a. Selezionare **Usa origine propria identità**. **Nota**: Se questa casella di controllo è selezionata e si desidera utilizzare la federazione di identità per gruppi e utenti tenant, il tenant deve configurare la propria origine di identità. Vedere istruzioni per l'utilizzo degli account tenant. b. Specificare una password per l'utente root locale del tenant, quindi selezionare **Crea tenant**. c. Selezionare **Accedi come root** per configurare il tenant oppure selezionare **fine** per configurarlo in un secondo momento.
Utilizzare i gruppi e gli utenti configurati per Grid Manager	a. Eseguire una o entrambe le operazioni seguenti: ◦ Selezionare un gruppo federated esistente da Grid Manager che deve disporre dell'autorizzazione di accesso root iniziale per il tenant. **Nota**: Se si dispone di autorizzazioni adeguate, i gruppi federated esistenti di Grid Manager vengono elencati quando si seleziona il campo. In caso contrario, immettere il nome univoco del gruppo. ◦ Specificare una password per l'utente root locale del tenant. b. Selezionare **Crea tenant**.

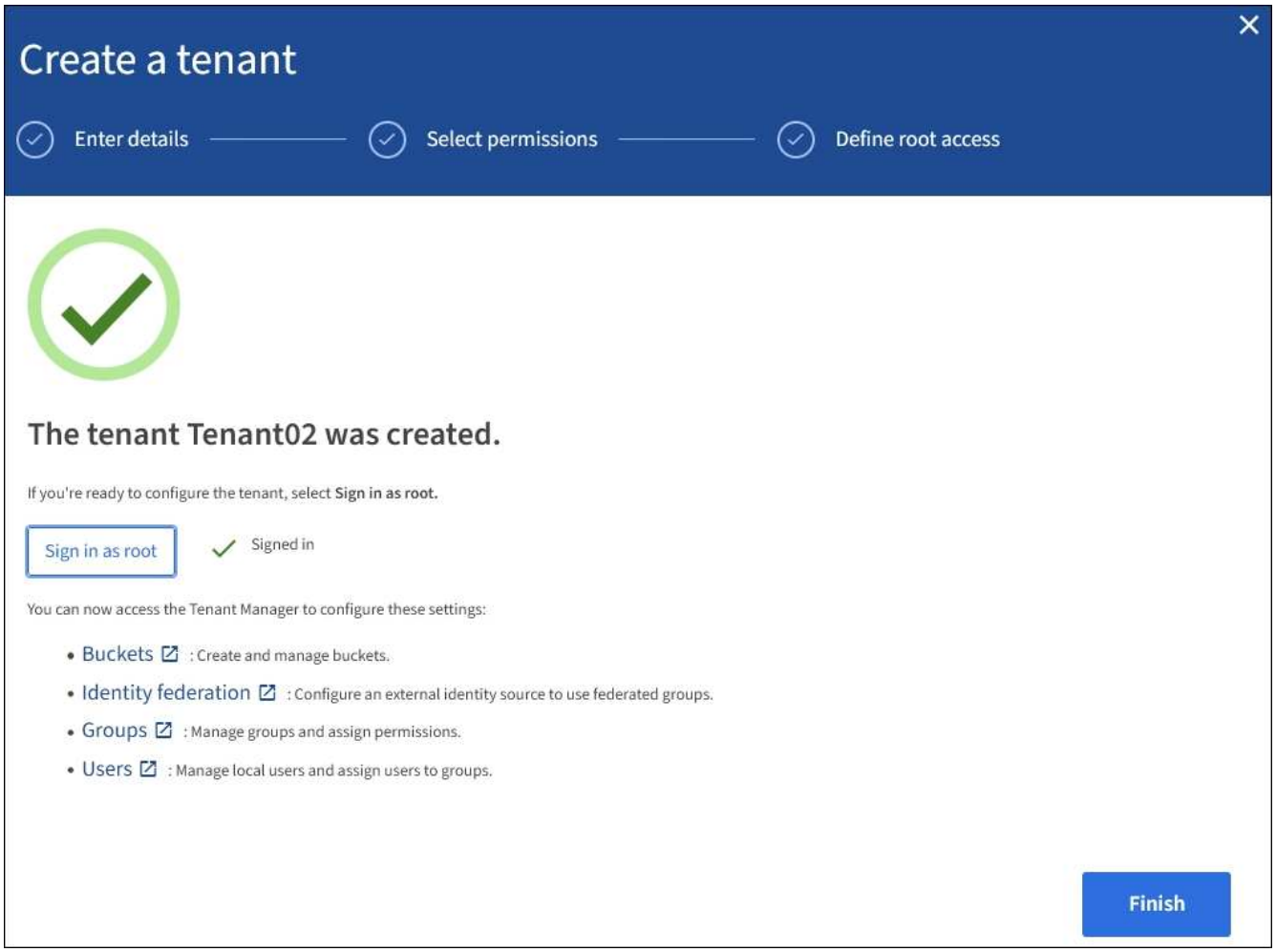
1. Per accedere subito al tenant:
   - Se si accede a Grid Manager su una porta con restrizioni, selezionare **Restricted** nella tabella tenant per ulteriori informazioni sull'accesso a questo account tenant.

     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
   - Se si accede a Grid Manager sulla porta 443 ma non è stata impostata una password per l'utente root locale, nella tabella tenant di Grid Manager, selezionare **Sign in** (Accedi) e immettere le credenziali per un utente nel gruppo federated di accesso root.
   - Se si accede a Grid Manager sulla porta 443 e si imposta una password per l'utente root locale:
     i. Selezionare **Accedi come root** per configurare il tenant ora.

        Al momento dell'accesso, vengono visualizzati i collegamenti per la configurazione di bucket o container, federazione di identità, gruppi e utenti.



i. 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.

ii. In caso contrario, selezionare **fine** per accedere al tenant in un secondo momento.

2. Per accedere al tenant in un secondo momento:

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
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

Informazioni correlate

- Controllo dell'accesso tramite firewall
- Gestire i servizi della piattaforma per gli account tenant S3

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

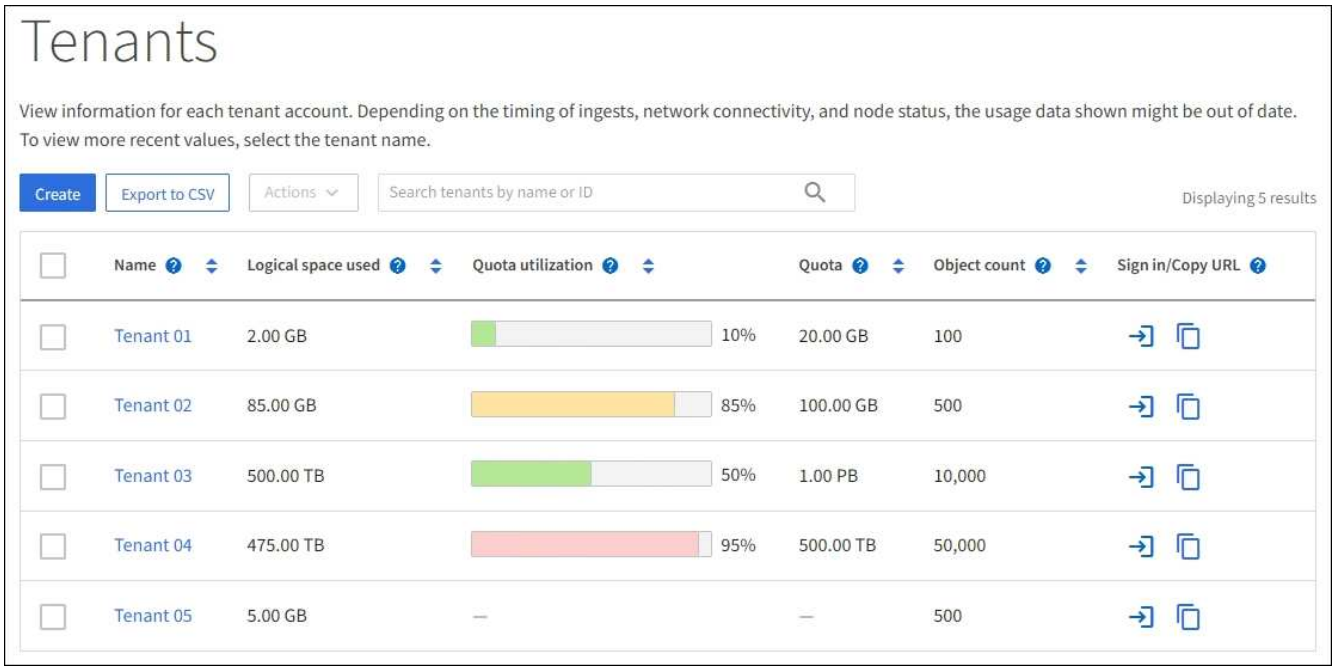
A proposito di questa attività

Se il sistema StorageGRID è abilitato per il Single Sign-on (SSO), l'utente root locale non può accedere

all'account tenant. Per eseguire le attività dell'utente root, gli utenti devono appartenere a un gruppo federated che disponga dell'autorizzazione di accesso root per il tenant.

Fasi

1. Selezionare **TENANT**.



2. Selezionare l'account tenant che si desidera modificare.

   Il pulsante Actions (azioni) viene attivato.

3. Dal menu a discesa **azioni**, selezionare **Modifica password root**.
4. Inserire la nuova password per l'account tenant.
5. Selezionare **Salva**.

Modificare l'account tenant

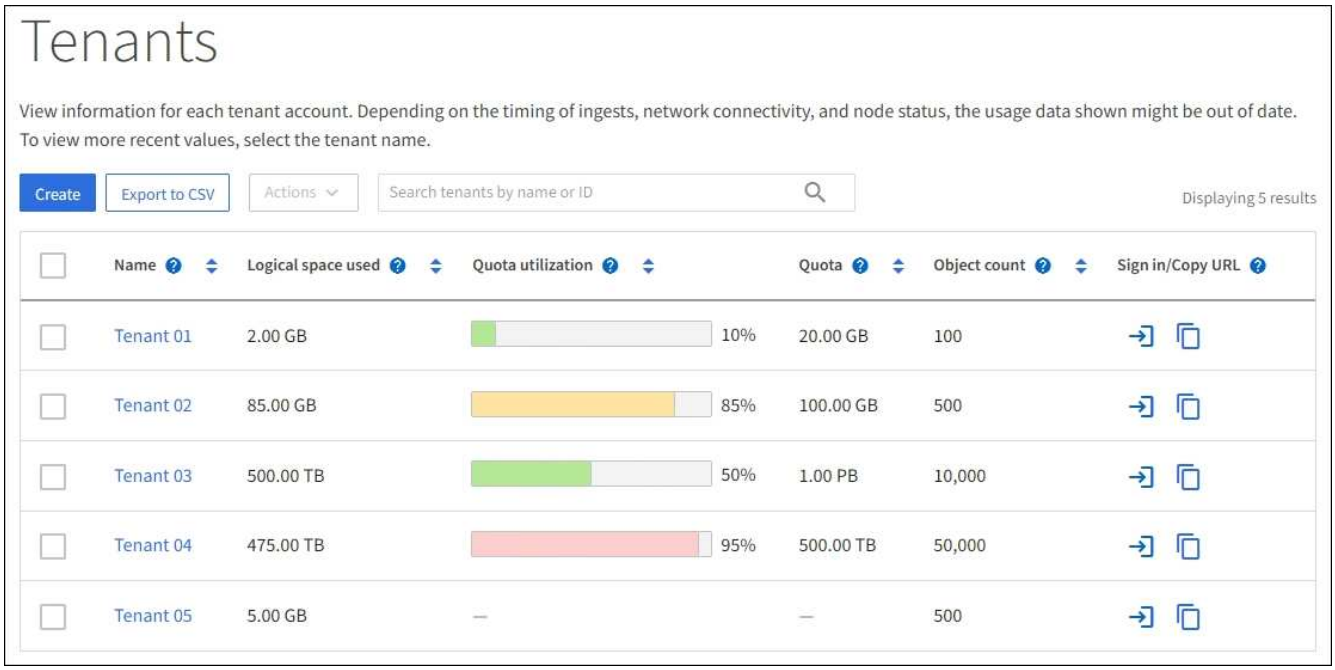
È possibile modificare un account tenant per modificare il nome visualizzato, modificare l'impostazione dell'origine dell'identità, consentire o non consentire i servizi della piattaforma o immettere una quota di storage.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **TENANT**.

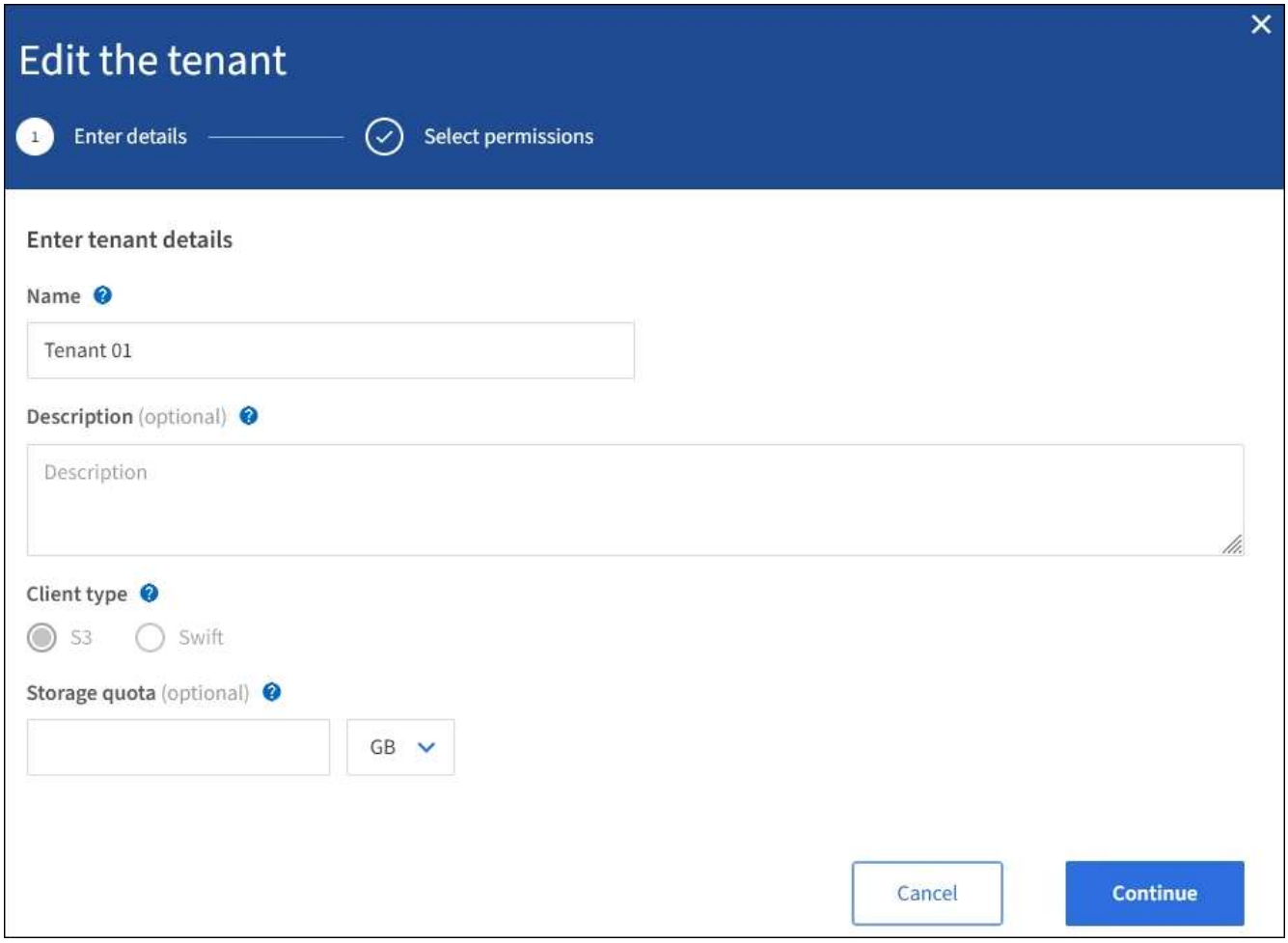


2. Selezionare l'account tenant che si desidera modificare.

   Utilizzare la casella di ricerca per cercare un account tenant in base al nome o all'ID tenant.

3. Dal menu a discesa Actions (azioni), selezionare **Edit** (Modifica).

   Questo esempio si intende per una griglia che non utilizza SSO (Single Sign-on). Questo account tenant non ha configurato la propria origine di identità.



4. Modificare i valori di questi campi come richiesto:
   - **Nome**
   - **Descrizione**
   - **Tipo di client**
   - **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.
   - Modificare l'impostazione della casella di controllo **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 la casella di controllo **utilizza la propria origine 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 deselezionato, SSO è attivato per il sistema StorageGRID. Il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager.
    - Attivare o disattivare **S3 Select** in base alle esigenze. Vedere Manage S3 (Gestisci S3): Selezionare per gli account tenant.
7. Selezionare **Salva**.

Informazioni correlate

- Gestire i servizi della piattaforma per gli account tenant S3
- Utilizzare un account tenant

Elimina account tenant

È possibile eliminare un account tenant se si desidera rimuovere in modo permanente l'accesso del tenant al sistema.

Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario rimuovere tutti i bucket (S3), i container (Swift) e gli oggetti associati all'account tenant.

Fasi

1. Selezionare **TENANT**.
2. Selezionare l'account tenant che si desidera eliminare.

   Utilizzare la casella di ricerca per cercare un account tenant in base al nome o all'ID tenant.
3. Dal menu a discesa **azioni**, selezionare **Elimina**.
4. Selezionare **OK**.

Gestire i servizi della piattaforma

Gestire i servizi della piattaforma per gli account tenant S3

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.

Questi servizi consentono ai tenant di utilizzare le seguenti funzionalità con i bucket S3:

- **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 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 servizio Amazon Simple Notification Service™ (SNS) esterno specificato.

  Ad esempio, è possibile configurare gli avvisi da inviare agli amministratori in merito a ciascun oggetto aggiunto a un bucket, in cui gli oggetti rappresentano i file di registro associati a un evento di sistema critico.

  > Sebbene la notifica degli eventi possa essere configurata su un bucket con blocco oggetti S3 attivato, i metadati del blocco oggetti S3 (inclusi lo stato Mantieni fino alla data e conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

- **Search Integration service**: Il servizio di integrazione della ricerca viene utilizzato per inviare metadati di oggetti S3 a un indice Elasticsearch specificato, dove 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

- Utilizzare un account tenant
- Configurare le impostazioni del proxy di storage

- Monitorare e risolvere i problemi

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
- Applicazione locale che supporta la ricezione di messaggi SNS (Simple Notification Service)
- 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
- **443**: Per gli URI endpoint che iniziano con https

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.

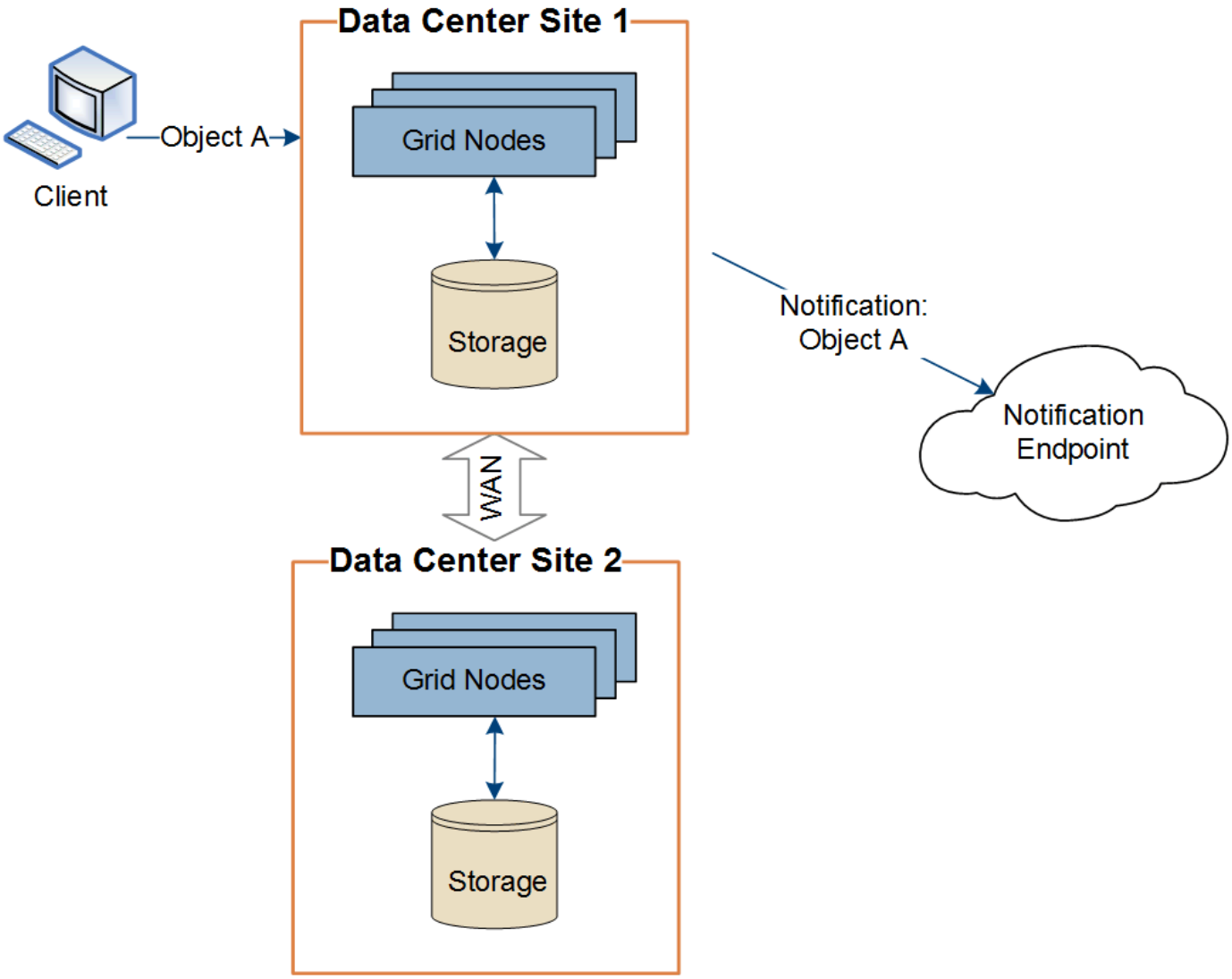
Informazioni correlate

- Utilizzare un account tenant

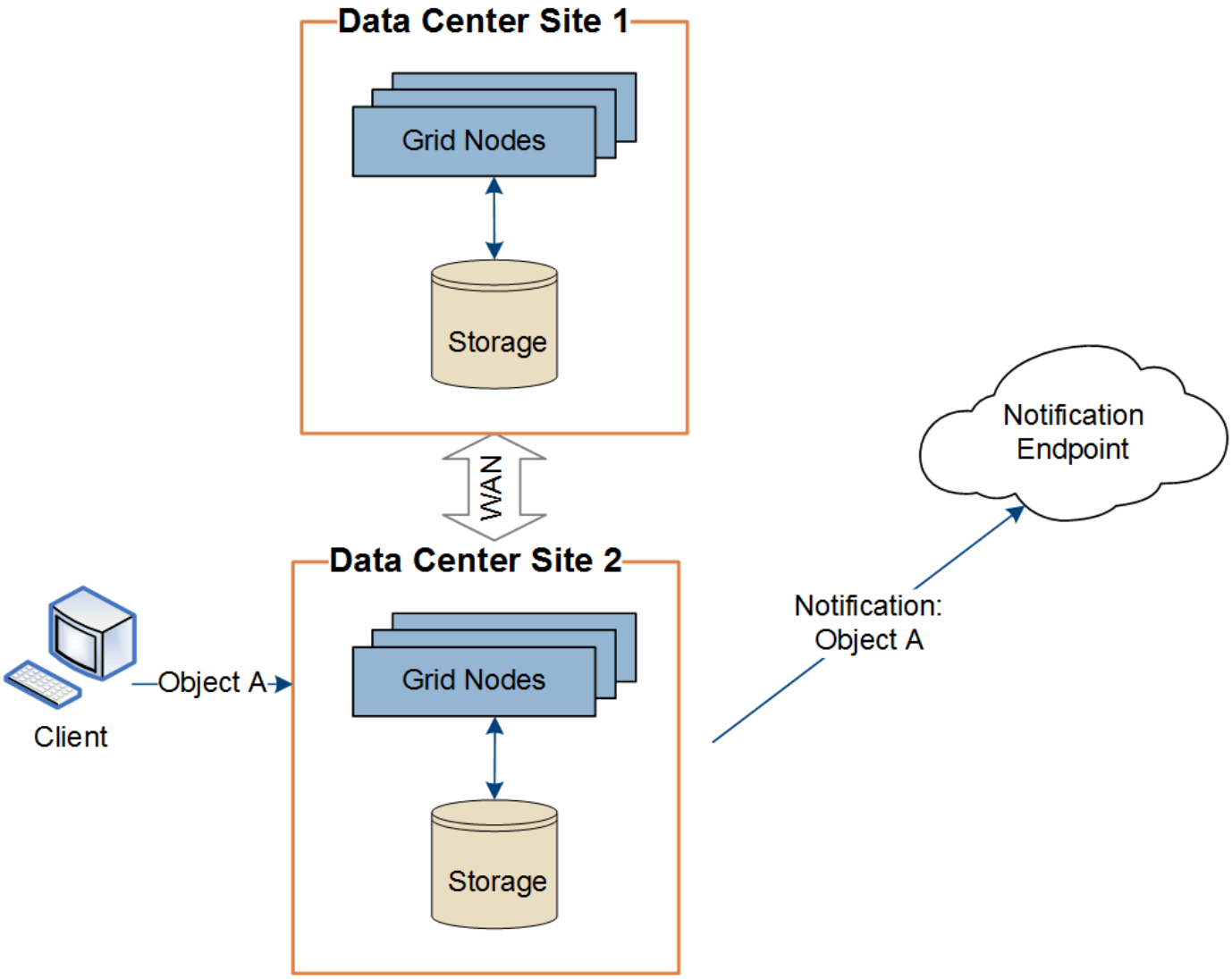
Erogazione per sito di messaggi relativi ai servizi della piattaforma

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. Ogni endpoint rappresenta una destinazione esterna per un servizio di piattaforma, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un semplice argomento del servizio di notifica 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.

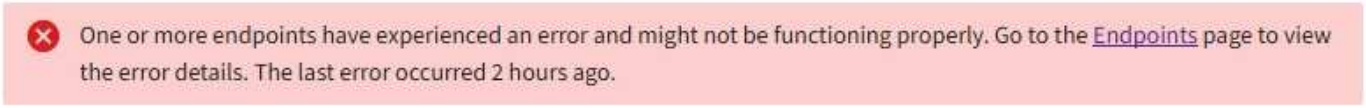
Quando un tenant crea un endpoint, il sistema StorageGRID convalida che l'endpoint esiste e che può essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in ogni sito.

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.

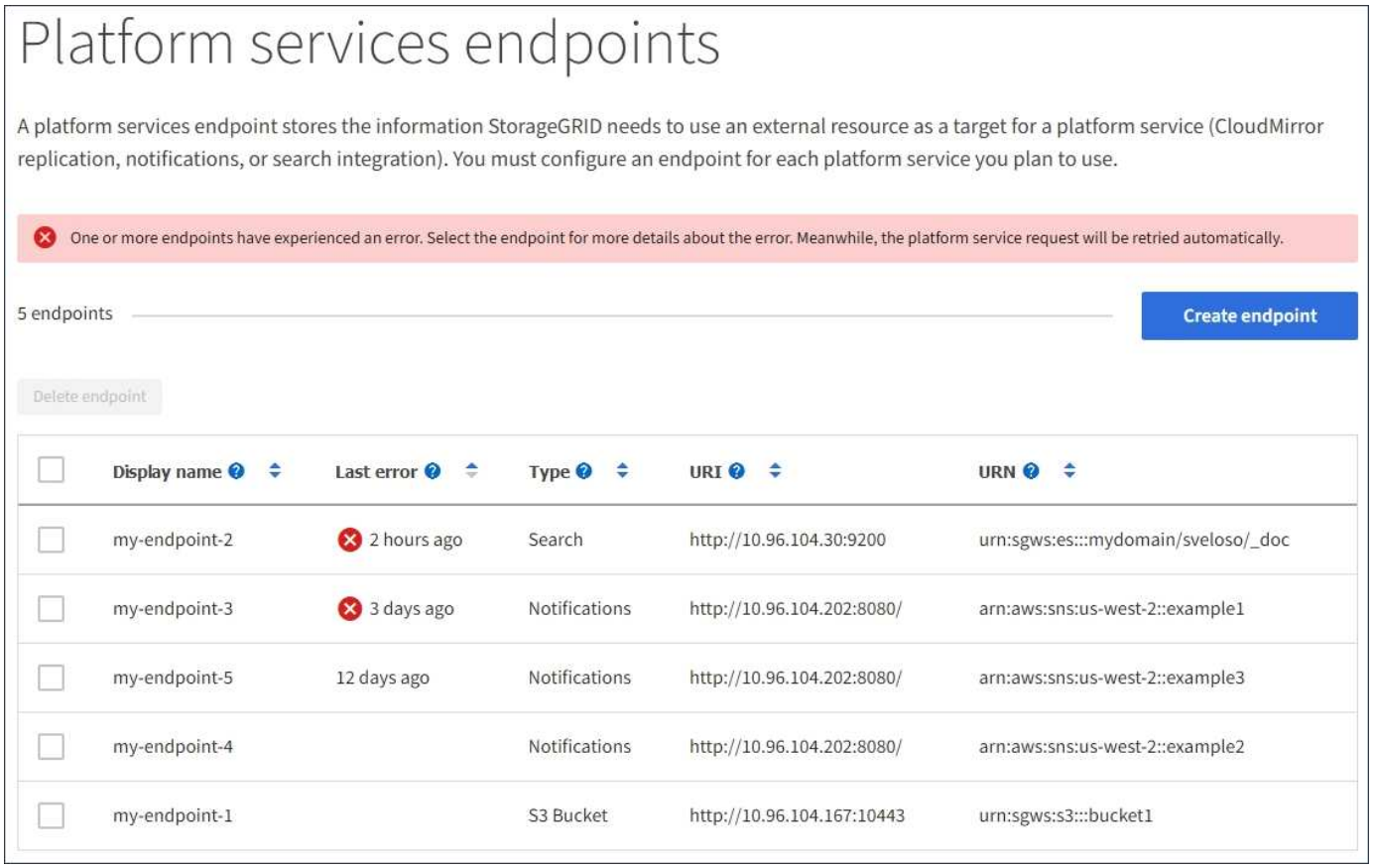
La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant.

Problemi con gli endpoint esistenti

Se si verifica un errore quando StorageGRID tenta di raggiungere un endpoint esistente, viene visualizzato un messaggio nella dashboard di 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, la 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.
- La notifica non può essere inviata.

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.

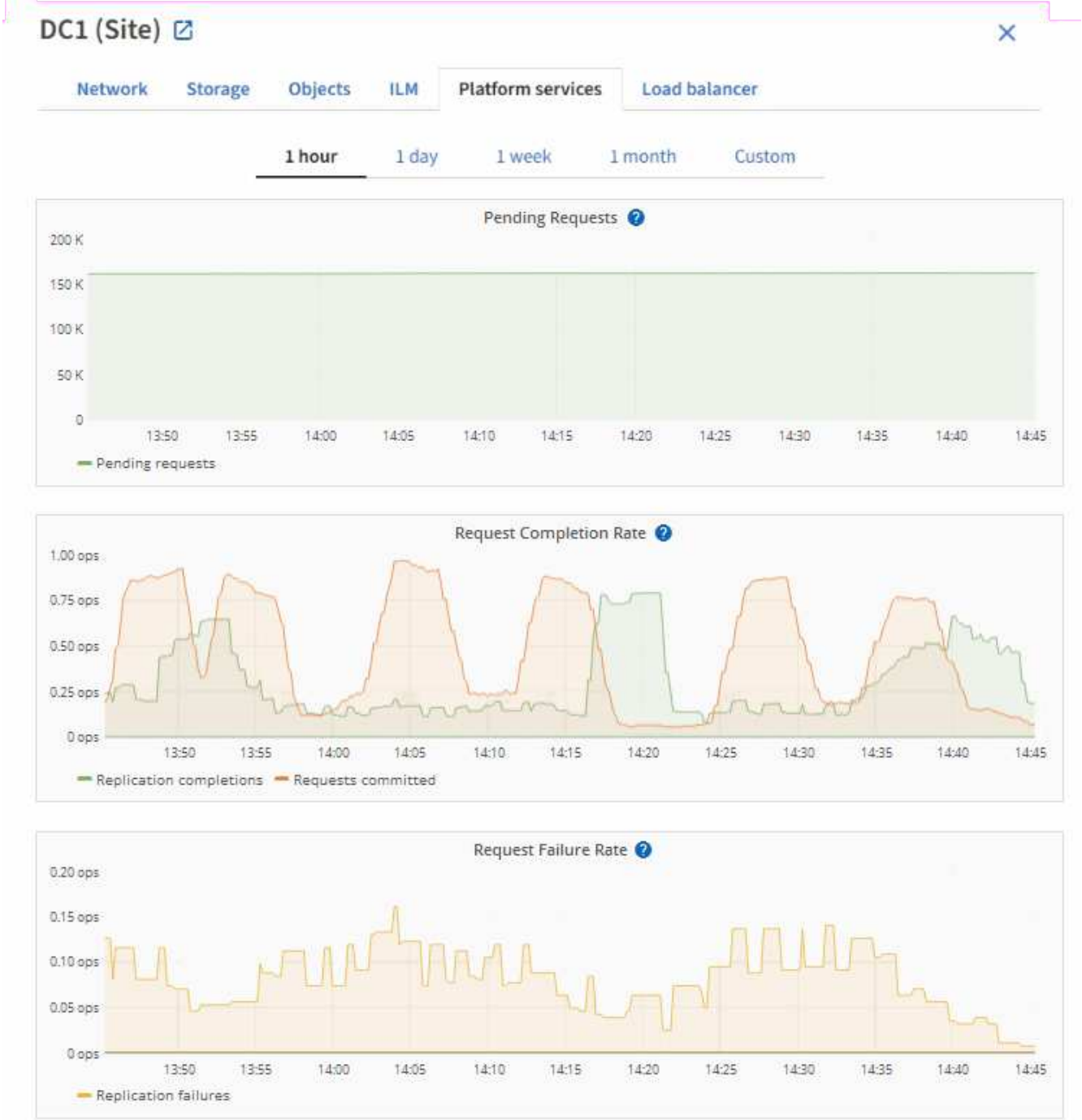
L'unico effetto visibile è che l'esecuzione delle richieste S3 in entrata richiederà più tempo. Se si inizia a rilevare performance significativamente più lente, è necessario ridurre il tasso di acquisizione o utilizzare un endpoint con capacità superiore. Se il backlog delle richieste continua a crescere, 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 sulla risoluzione dei problemi degli endpoint dei servizi della piattaforma, vedere le istruzioni per utilizzando un account tenant.

Informazioni correlate

- Monitorare e risolvere i problemi
- Configurare le impostazioni del proxy di storage

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

StorageGRID richiede quanto segue per le query S3 Select:

- L'oggetto che si desidera sottoporre a query è in formato CSV oppure è un file compresso GZIP o BZIP2 contenente un file in formato CSV.
- Ai tenant deve essere concessa l'abilità S3 Select dall'amministratore della griglia. Selezionare **Allow S3 Select** when (Consenti selezione S3) creazione di un tenant oppure modifica di un tenant.
- La richiesta SelectObjectContent deve essere inviata a Endpoint del bilanciamento del carico di StorageGRID. I nodi Admin e Gateway utilizzati dall'endpoint devono essere nodi appliance SG100 o SG1000 o nodi software basati su VMware.

Tenere presente le seguenti limitazioni:

- I nodi bare-metal di bilanciamento del carico non sono supportati.
- Le query non possono essere inviate direttamente ai nodi di storage.
- Le query inviate tramite il servizio CLB obsoleto non sono supportate.

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 S3 e Swift

Informazioni sulle connessioni client S3 e Swift

In qualità di amministratore di grid, gestisci le opzioni di configurazione che controllano il modo in cui i tenant S3 e Swift possono connettere le applicazioni client al sistema StorageGRID per memorizzare e recuperare i dati. Esistono diverse opzioni per soddisfare i diversi requisiti di client e tenant.

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

- Il servizio Load Balancer sui nodi Admin o Gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità (ha) di nodi Admin o nodi Gateway
- Il servizio CLB sui nodi gateway o, facoltativamente, l'indirizzo IP virtuale di un gruppo ad alta disponibilità di nodi gateway

> Il servizio CLB è obsoleto. I client configurati prima della release StorageGRID 11.3 possono continuare a utilizzare il servizio CLB sui nodi gateway. Tutte le altre applicazioni client che dipendono da StorageGRID per fornire il bilanciamento del carico devono connettersi utilizzando il servizio bilanciamento del carico.

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

È possibile configurare le seguenti funzioni sul sistema StorageGRID:

- **Interfacce VLAN**: È possibile creare interfacce LAN virtuali (VLAN) su nodi Admin e nodi Gateway per isolare e partizionare il traffico client e tenant per garantire sicurezza, flessibilità e performance. Dopo aver creato un'interfaccia VLAN, aggiungerla a un gruppo ad alta disponibilità (ha).
- **Gruppi ad alta disponibilità**: È possibile creare un gruppo ha delle interfacce per i nodi gateway o i nodi di amministrazione per creare una configurazione di backup attivo oppure utilizzare un DNS round-robin o un bilanciamento del carico di terze parti e più gruppi ha per ottenere una configurazione Active-Active. Le connessioni client vengono eseguite utilizzando gli indirizzi IP virtuali dei gruppi ha.
- **Servizio Load Balancer**: È possibile consentire ai client di utilizzare il servizio Load Balancer creando endpoint di bilanciamento del carico per le connessioni client. Quando si crea un endpoint di bilanciamento del carico, specificare un numero di porta, se l'endpoint accetta connessioni HTTP o HTTPS, il tipo di client (S3 o Swift) che utilizzerà l'endpoint e il certificato da utilizzare per le connessioni HTTPS (se applicabile).
- **Untrusted Client Network**: È possibile rendere la rete client più sicura configurandola come non attendibile. Quando la rete client non è attendibile, i client possono connettersi solo utilizzando endpoint di bilanciamento del carico.

È inoltre possibile abilitare l'utilizzo di HTTP per i client che si connettono a StorageGRID direttamente ai nodi di storage o utilizzando il servizio CLB (obsoleto) ed è possibile configurare i nomi di dominio degli endpoint API S3 per i client S3.

Riepilogo: Indirizzi IP e porte per le connessioni client

Le applicazioni client possono connettersi a StorageGRID utilizzando l'indirizzo IP di un

nodo Grid e il numero di porta di un servizio su tale nodo. Se sono configurati gruppi ad alta disponibilità (ha), le applicazioni client possono connettersi utilizzando l'indirizzo IP virtuale del gruppo ha.

A proposito di questa attività

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. Le istruzioni descrivono come trovare queste informazioni in Grid Manager se gli endpoint del bilanciamento del carico e i gruppi ad alta disponibilità (ha) sono già configurati.

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 endpoint del bilanciamento del carico
Gruppo HA	CLB **Nota:** il servizio CLB è obsoleto.	Indirizzo IP virtuale di un gruppo ha	Porte S3 predefinite: • HTTPS: 8082 • HTTP: 8084 Porte Swift predefinite: • HTTPS:8083 • HTTP:8085
Nodo Admin	Bilanciamento del carico	Indirizzo IP del nodo di amministrazione	• Porta endpoint del bilanciamento del carico
Nodo gateway	Bilanciamento del carico	Indirizzo IP del nodo gateway	• Porta endpoint del bilanciamento del carico
Nodo gateway	CLB **Nota:** il servizio CLB è obsoleto.	Indirizzo IP del nodo gateway **Nota:** per impostazione predefinita, le porte HTTP per CLB e LDR non sono attivate.	Porte S3 predefinite: • HTTPS: 8082 • HTTP: 8084 Porte Swift predefinite: • HTTPS:8083 • HTTP:8085

Dove viene stabilita la connessione	Servizio a cui si connette il client	Indirizzo IP	Porta
Nodo di storage	LDR	Indirizzo IP del nodo di storage	Porte S3 predefinite: • HTTPS: 18082 • HTTP: 18084 Porte Swift predefinite: • HTTPS: 18083 • HTTP:18085

Esempi

Per connettere un client S3 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 di un endpoint di bilanciamento del carico S3 è 10443, un client S3 potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.5:10443`

Per connettere un client Swift 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 192.0.2.6 e il numero di porta di un endpoint di bilanciamento del carico di Swift è 10444, un client Swift potrebbe utilizzare il seguente URL per connettersi a StorageGRID:

- `https://192.0.2.6:10444`

È possibile configurare un nome DNS per l'indirizzo IP utilizzato dai client per la connessione a StorageGRID. Contattare l'amministratore di rete locale.

Fasi

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**.

      Viene visualizzata la pagina Load Balancer Endpoint, che mostra l'elenco degli endpoint già configurati.

   b. Selezionare un endpoint e selezionare **Modifica endpoint**.

      Viene visualizzata la finestra Edit Endpoint (Modifica endpoint) che visualizza ulteriori dettagli sull'endpoint.

   c. Verificare che l'endpoint selezionato sia configurato per l'utilizzo con il protocollo corretto (S3 o Swift), quindi selezionare **Annulla**.
   d. Annotare il numero di porta dell'endpoint che si desidera utilizzare per una connessione client.

> 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.

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 o CentOS (prima di installare il nodo)**: Creare file di configurazione del nodo
  - **Ubuntu o Debian (prima di installare il nodo)**: Creare file di configurazione del nodo
  - **RHEL, CentOS, Ubuntu o Debian (dopo aver installato il nodo)**: Linux: Aggiunta di interfacce di accesso o trunk a un nodo

Creare un'interfaccia VLAN

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'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

1. Selezionare **CONFIGURAZIONE rete interfacce VLAN**.
2. Selezionare **Crea**.

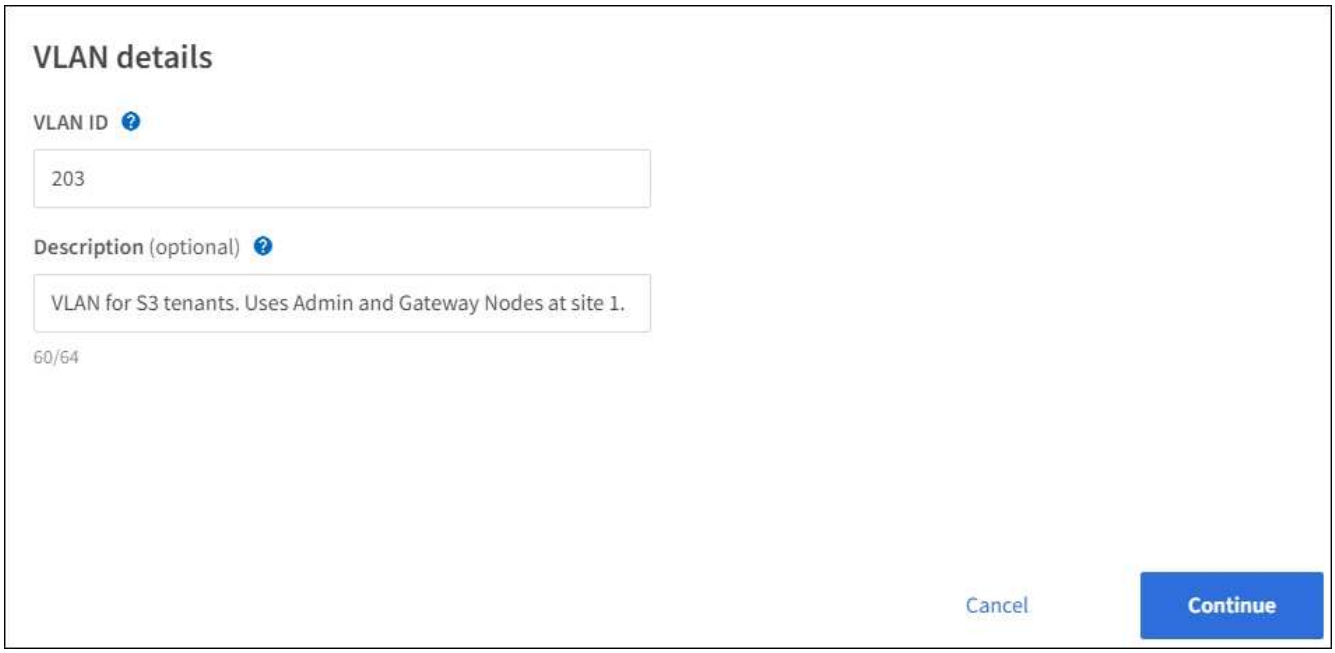
Inserire i dettagli delle interfacce VLAN

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. È possibile continuare a creare un'altra interfaccia VLAN per lo stesso ID VLAN oppure selezionare **Annulla** e modificare l'ID esistente.

2. Facoltativamente, inserire una breve descrizione per l'interfaccia VLAN.



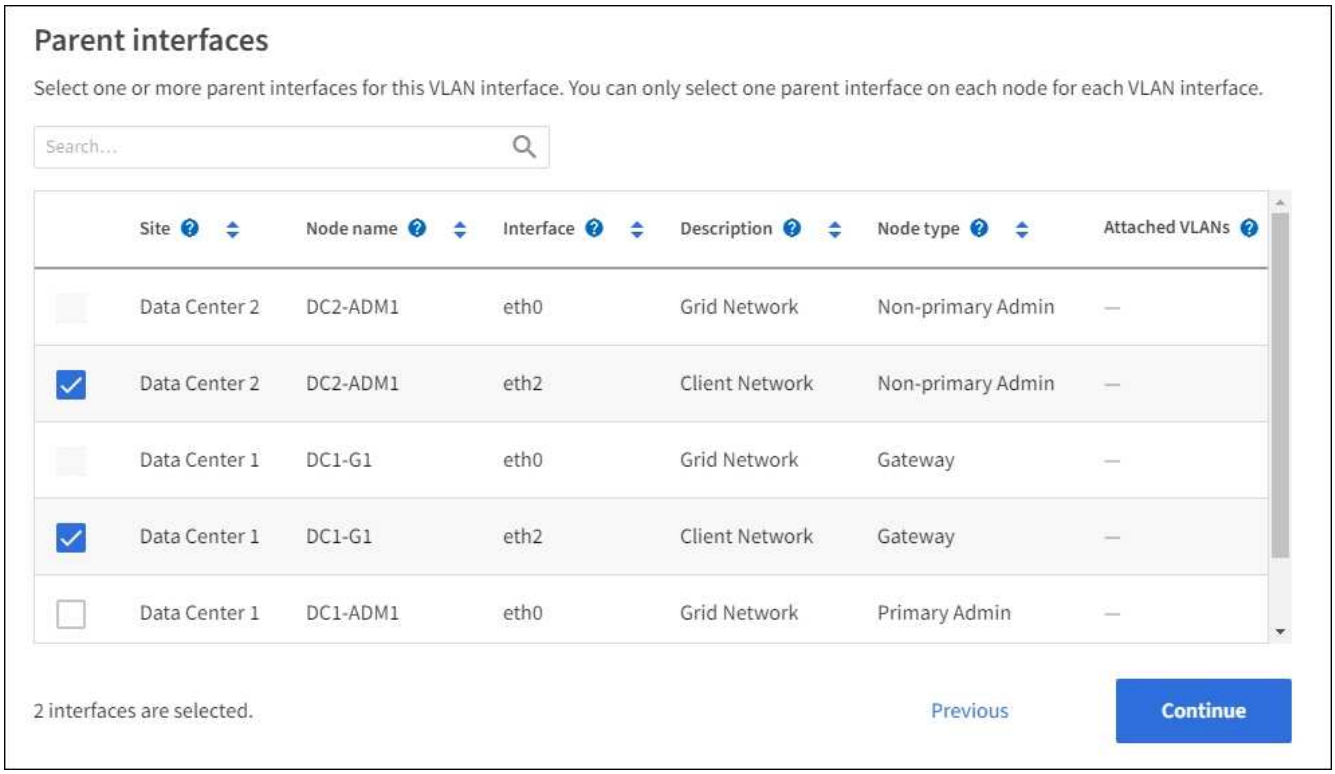
3. Selezionare **continua**.

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.

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

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 inutilizzata per il nodo B, ma non è possibile rimuovere l'interfaccia padre utilizzata per il nodo A.

Fasi

1. Selezionare **CONFIGURAZIONE rete interfacce VLAN**.
2. Selezionare la casella di controllo dell'interfaccia VLAN che si desidera modificare. Quindi, selezionare **azioni Modifica**.
3. Facoltativamente, aggiornare l'ID VLAN o la descrizione. Quindi, selezionare **continua**.

   Non è possibile aggiornare un ID VLAN se la VLAN viene utilizzata in un gruppo ha.

4. Facoltativamente, selezionare o deselezionare le caselle di controllo per aggiungere interfacce padre o rimuovere interfacce inutilizzate. Quindi, selezionare **continua**.
5. Esaminare la configurazione e apportare eventuali modifiche.
6. Selezionare **Salva**.

Rimuovere un'interfaccia VLAN

È possibile rimuovere una o più interfacce VLAN.

Non è possibile rimuovere un'interfaccia VLAN se è attualmente utilizzata in un gruppo ha. È necessario rimuovere l'interfaccia VLAN dal gruppo ha prima di poterla rimuovere.

Per evitare interruzioni del traffico client, è consigliabile eseguire una delle seguenti operazioni:

- Aggiungere una nuova interfaccia VLAN al gruppo ha prima di rimuovere questa interfaccia VLAN.
- Creare un nuovo gruppo ha che non utilizzi questa interfaccia VLAN.
- Se l'interfaccia VLAN che si desidera rimuovere è attualmente attiva, modificare il gruppo ha. Spostare l'interfaccia VLAN che si desidera rimuovere in fondo all'elenco delle priorità. Attendere che la comunicazione venga stabilita sulla nuova interfaccia principale, quindi rimuovere la vecchia interfaccia dal gruppo ha. Infine, eliminare l'interfaccia VLAN su quel nodo.

Fasi

1. Selezionare **CONFIGURAZIONE rete interfacce VLAN**.
2. Selezionare la casella di controllo per ogni interfaccia VLAN che si desidera rimuovere. Quindi, selezionare **azioni Elimina**.
3. Selezionare **Sì** per confermare la selezione.

   Tutte le interfacce VLAN selezionate vengono rimosse. Nella pagina delle interfacce VLAN viene visualizzato un banner verde di successo.

Gestire i gruppi ad alta disponibilità

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 SG100 o SG1000 e nodi software basati su VMware può fornire connessioni altamente disponibili per S3 tenant che utilizzano S3 Select. I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.

Come crei un gruppo ha?

1. Selezionare un'interfaccia di rete per uno o più nodi Admin o Gateway. È possibile utilizzare un'interfaccia Grid Network (eth0), un'interfaccia Client Network (eth2), un'interfaccia VLAN o un'interfaccia di accesso aggiunta al nodo.

   > Non è possibile aggiungere un'interfaccia a un gruppo ha se dispone di un indirizzo IP assegnato da DHCP.

2. Specificare un'interfaccia come principale. L'interfaccia principale è l'interfaccia attiva a meno che non si verifichi un errore.
3. È possibile determinare l'ordine di priorità per le interfacce di backup.
4. Al gruppo vengono assegnati da uno a 10 indirizzi IP virtuali (VIP). Le applicazioni client possono utilizzare uno qualsiasi di questi indirizzi VIP per connettersi a StorageGRID.

Per istruzioni, vedere Configurare i gruppi ad alta disponibilità.

Che cos'è l'interfaccia attiva?

Durante il normale funzionamento, tutti gli indirizzi VIP per il gruppo ha vengono aggiunti all'interfaccia primaria, che è la prima interfaccia nell'ordine di priorità. Finché l'interfaccia primaria rimane disponibile, viene utilizzata quando i client si connettono a qualsiasi indirizzo VIP del gruppo. Cioè, durante il normale funzionamento, l'interfaccia principale è l'interfaccia "Active" per il gruppo.

Analogamente, durante il normale funzionamento, tutte le interfacce con priorità inferiore per il gruppo ha agiscono come interfacce "backup". Queste interfacce di backup non vengono utilizzate a meno che l'interfaccia primaria (attualmente attiva) non diventi disponibile.

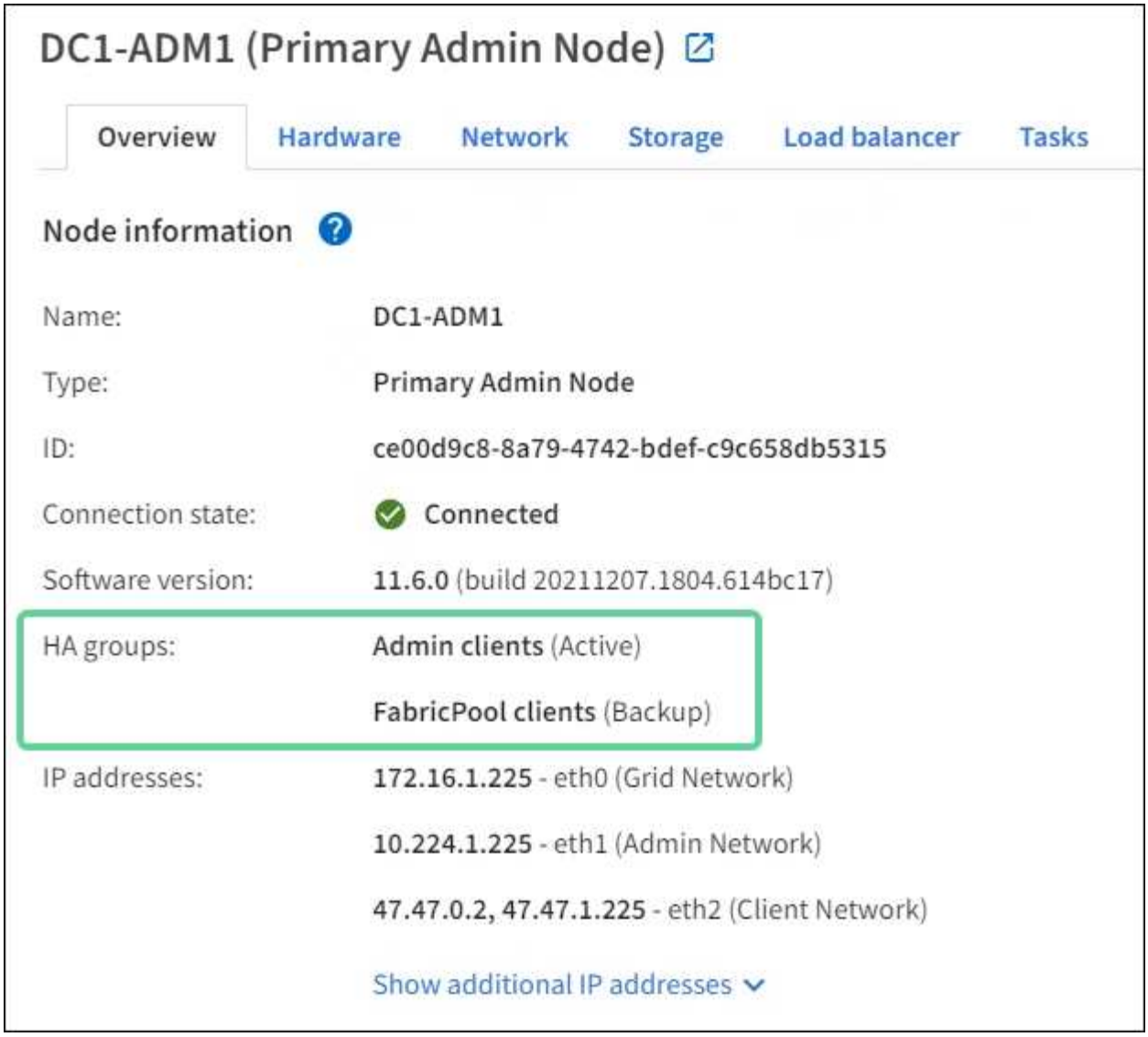
Visualizzare lo stato corrente del gruppo ha di un nodo

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 dal guasto del servizio CLB (obsoleto) o dei servizi per Grid Manager o il 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 e il servizio CLB (obsoleto).

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
Accesso al client S3 per S3 Seleziona	• Appliance SG100 o SG1000 • Nodi software basati su VMware **Nota**: I gruppi HA sono consigliati quando si utilizza S3 Select, ma non sono richiesti.
Accesso client S3 o Swift — Servizio CLB **Nota:** il servizio CLB è obsoleto.	• Nodi gateway

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.

Limitazioni dell'utilizzo di gruppi ha con il servizio CLB

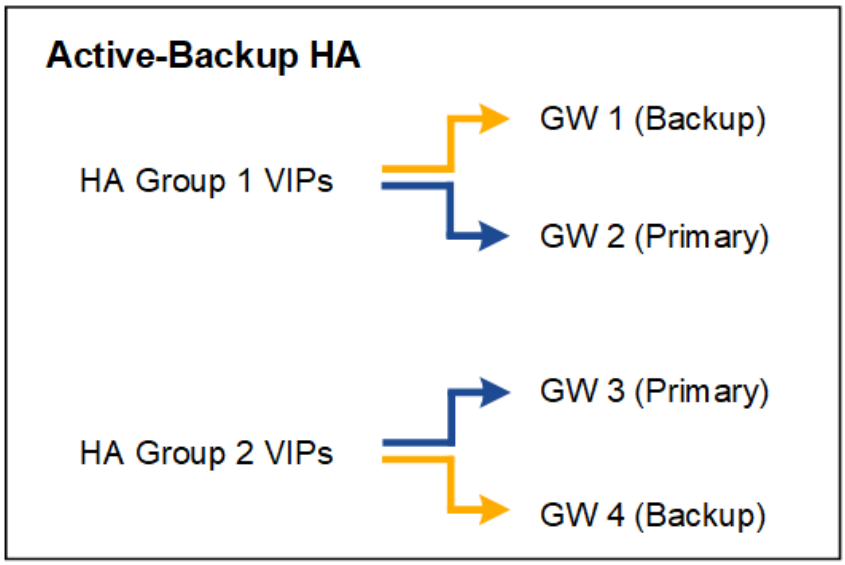
Il guasto del servizio CLB non attiva il failover all'interno del gruppo ha.

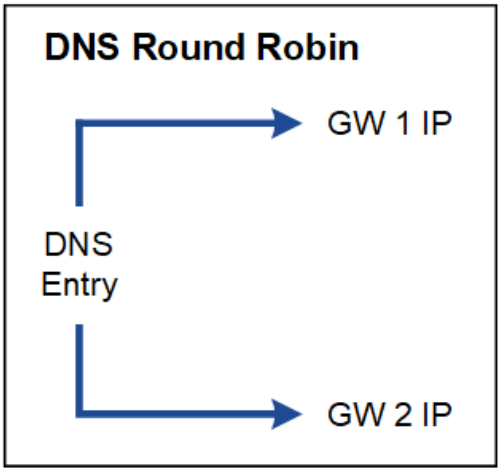
Il servizio CLB è obsoleto.

Opzioni di configurazione per i gruppi ha

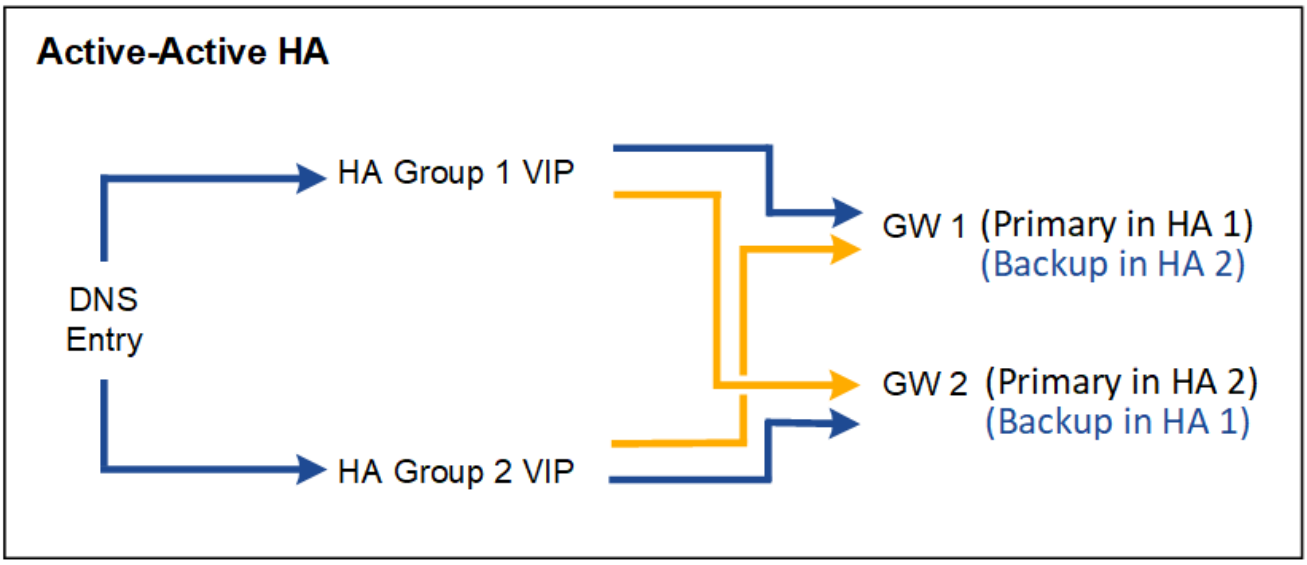
I seguenti diagrammi forniscono esempi di diversi modi per configurare i gruppi ha. Ogni opzione presenta vantaggi e svantaggi.

Nei diagrammi, il blu indica l'interfaccia principale nel gruppo ha e il giallo indica l'interfaccia di backup nel gruppo ha.





GW = Gateway Node
VIP = Virtual IP address



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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'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 o CentOS (prima di installare il nodo)**: Creare file di configurazione del nodo
  - **Ubuntu o Debian (prima di installare il nodo)**: Creare file di configurazione del nodo
  - **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.

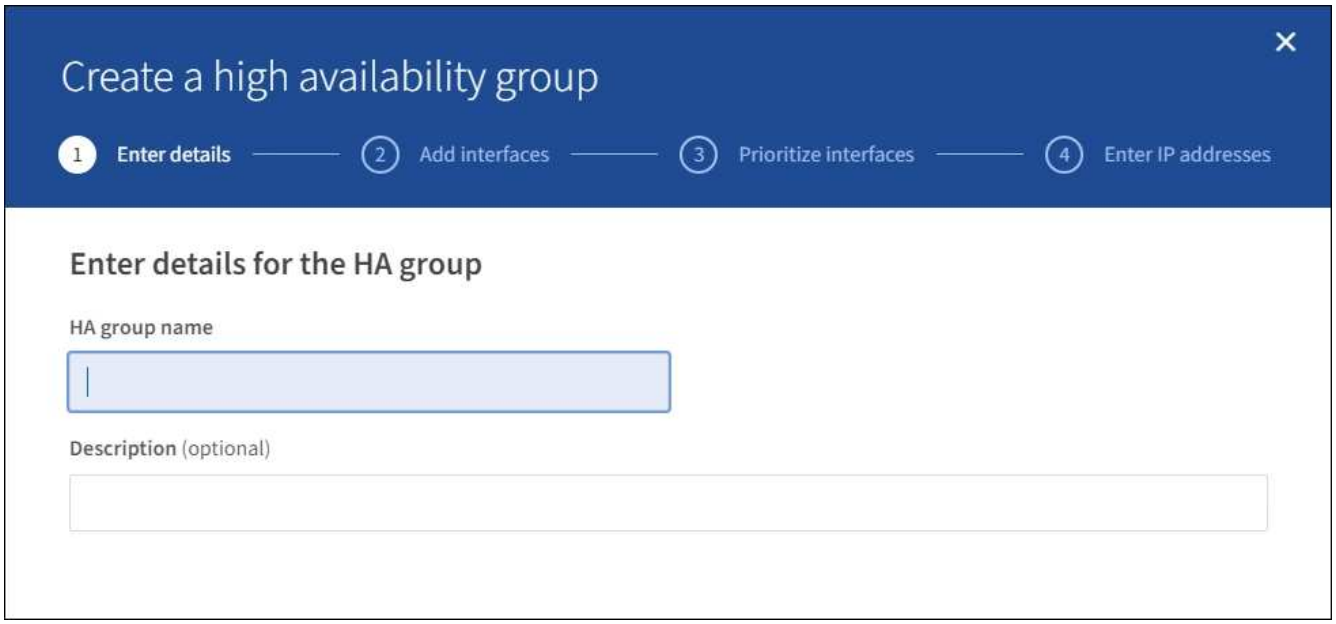
Un'interfaccia deve essere un nodo gateway o un nodo amministratore per essere incluso in un gruppo ha. Un gruppo ha può utilizzare solo un'interfaccia per un dato nodo; tuttavia, altre interfacce per lo stesso nodo possono essere utilizzate in altri gruppi ha.

Accedere alla procedura guidata

1. Selezionare **CONFIGURATION** > **Network** > **High Availability groups**.
2. Selezionare **Crea**.

Inserire i dettagli del gruppo ha

1. Fornire un nome univoco per il gruppo ha.

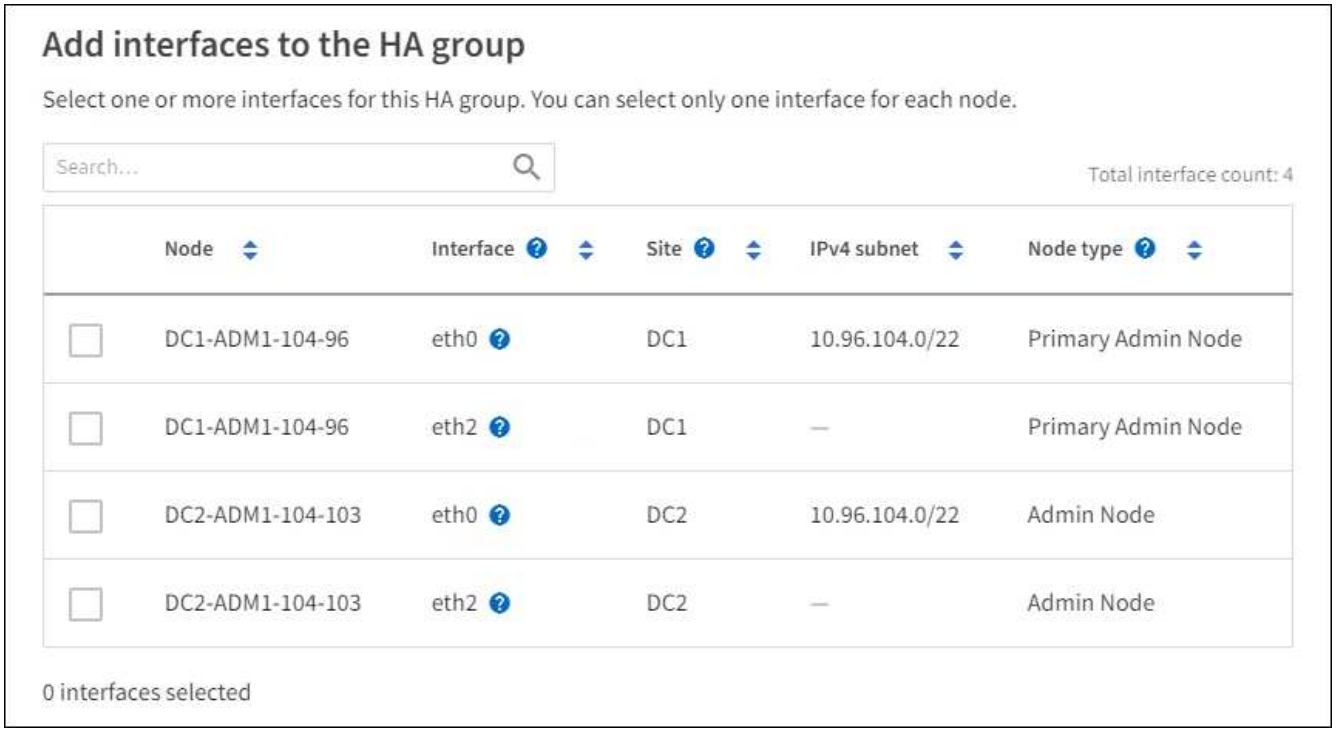


2. Facoltativamente, inserire una descrizione per il gruppo ha.
3. Selezionare **continua**.

Aggiungere interfacce al gruppo ha

1. Selezionare una o più interfacce da aggiungere a questo gruppo ha.

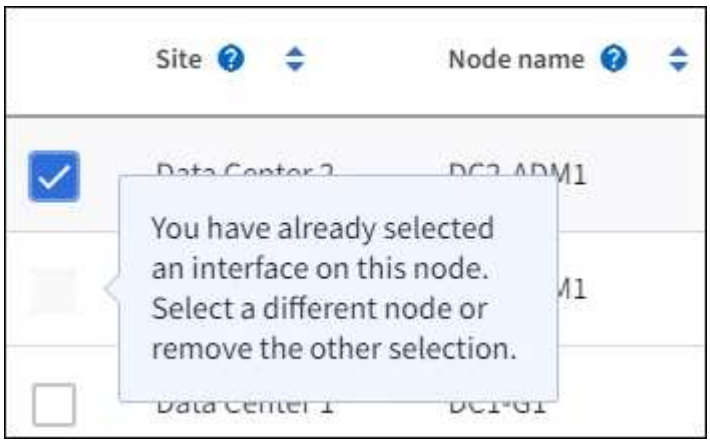
   Utilizzare le intestazioni di colonna per ordinare le righe o inserire un termine di ricerca per individuare le interfacce più rapidamente.



> 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 il gruppo ha è per la protezione ha del servizio CLB obsoleto, selezionare le interfacce solo sui nodi gateway.
- 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 amministratore di backup non può eseguire tutte le procedure di manutenzione che il nodo amministratore primario può fornire.
- Se non è possibile selezionare un'interfaccia, la relativa casella di controllo è disattivata. Il suggerimento fornisce ulteriori informazioni.



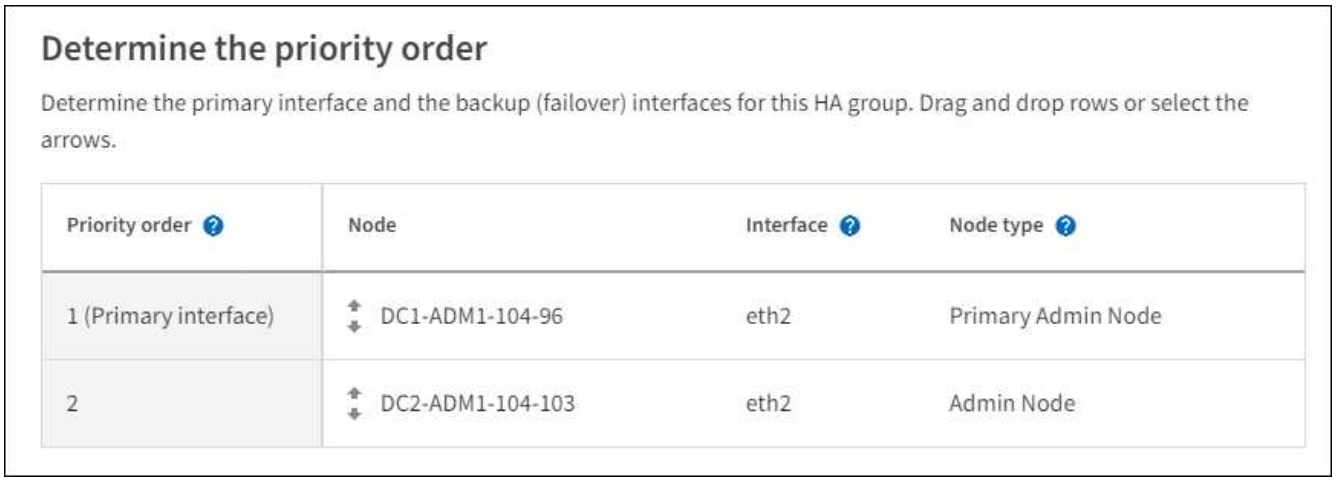
- Non è possibile selezionare un'interfaccia se il relativo valore di sottorete o il gateway è in conflitto con un'altra interfaccia selezionata.
- Non è possibile selezionare un'interfaccia configurata se non dispone di un indirizzo IP statico.

2. Selezionare **continua**.

Determinare l'ordine di priorità

1. Determinare l'interfaccia primaria e le interfacce di backup (failover) per questo gruppo ha.

   Trascinare e rilasciare le righe per modificare i valori nella colonna **Ordine di priorità**.



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.

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 primaria 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.

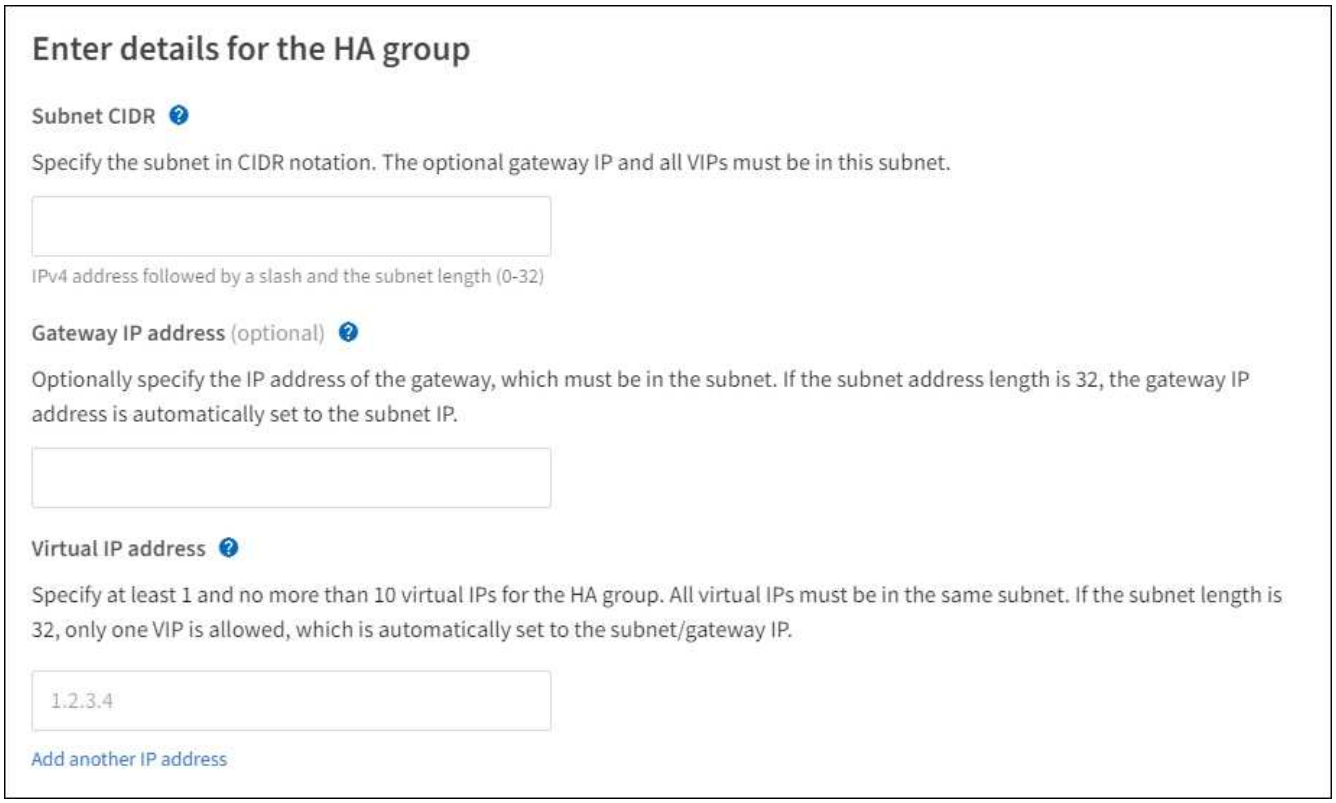
2. Selezionare **continua**.

Inserire gli indirizzi IP

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 uno o più **indirizzi IP virtuali** per il gruppo ha. È possibile aggiungere fino a 10 indirizzi IP. Tutti i VIP devono trovarsi all'interno della subnet VIP.

   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.

Attendere fino a 15 minuti per applicare le modifiche a un gruppo ha a tutti i nodi.

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

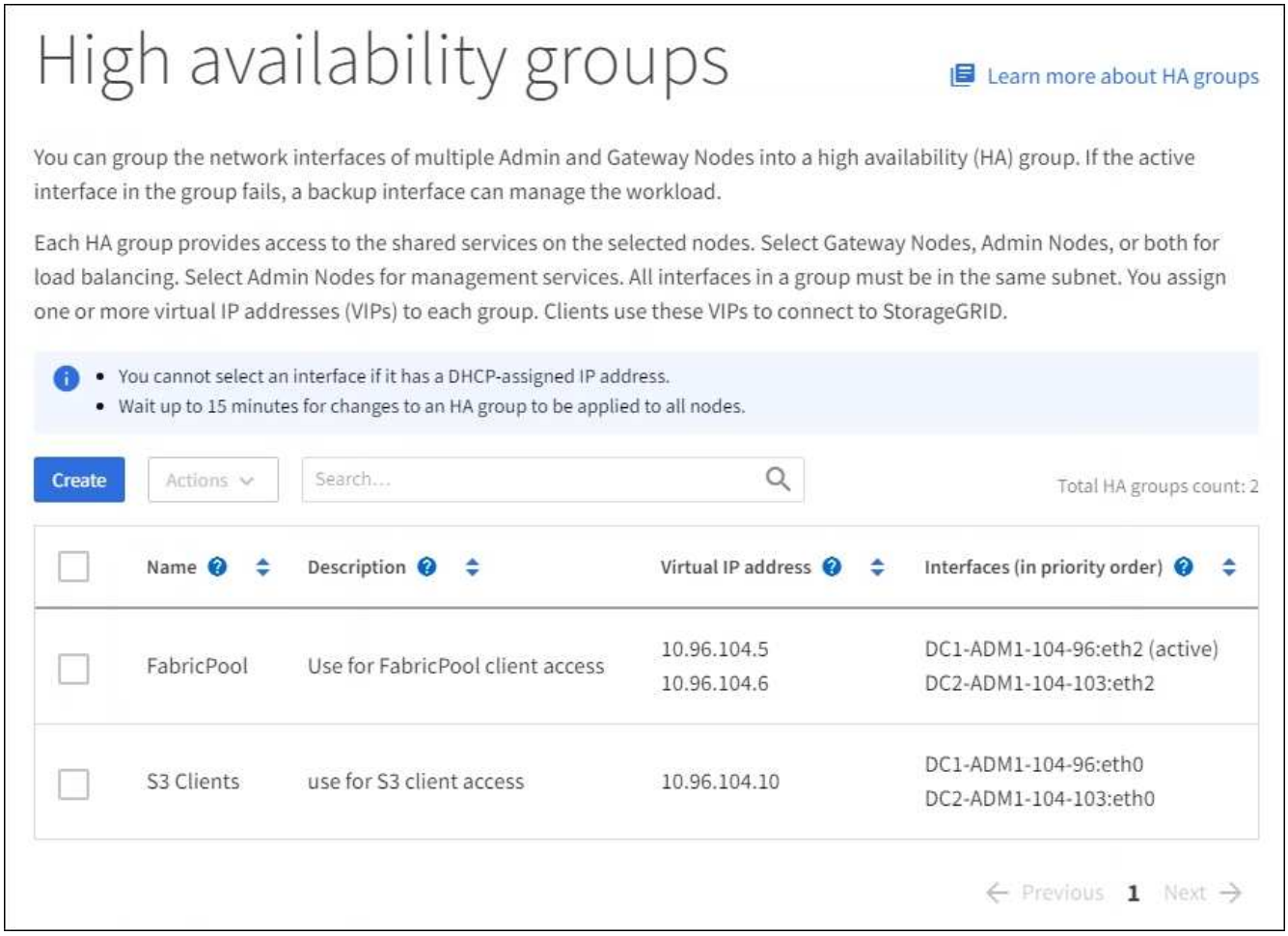
È possibile modificare un gruppo ad alta disponibilità (ha) per modificarne nome e descrizione, aggiungere o rimuovere interfacce, modificare l'ordine di priorità o aggiungere o aggiornare indirizzi IP virtuali.

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 relativa al 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 e rilasciare le righe per modificare l'ordine di priorità dell'interfaccia primaria e di qualsiasi interfaccia di backup per questo gruppo ha.

d. Facoltativamente, aggiornare gli indirizzi IP virtuali.

e. Selezionare **Salva**, quindi **fine**.

Attendere fino a 15 minuti per applicare le modifiche a un gruppo ha a tutti i nodi.

Rimuovere un gruppo ad alta disponibilità

È possibile rimuovere uno o più gruppi ad alta disponibilità (ha) alla volta. Tuttavia, non è possibile rimuovere un gruppo ha se è associato a uno o più endpoint del bilanciamento del carico.

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. Selezionare la casella di controllo per ciascun gruppo ha che si desidera rimuovere. Quindi, selezionare **azioni Rimuovi gruppo ha**.
3. 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

Gestire il bilanciamento del carico: Panoramica

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

Puoi bilanciare il carico dei carichi di lavoro dei client nei seguenti modi:

- Utilizzare il servizio Load Balancer, installato nei nodi Admin e nei nodi Gateway. Il servizio Load Balancer fornisce il bilanciamento del carico di livello 7 ed esegue la terminazione TLS delle richieste dei client, ispeziona le richieste e stabilisce nuove connessioni sicure ai nodi di storage. Si tratta del meccanismo di bilanciamento del carico consigliato.

  Vedere Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico.

- Utilizzare il servizio di bilanciamento del carico di connessione (CLB) obsoleto, installato solo sui nodi gateway. Il servizio CLB fornisce il bilanciamento del carico di livello 4 e supporta i costi di collegamento.

Vedere Come funziona il bilanciamento del carico - servizio CLB (obsoleto).

- Integrare un bilanciamento del carico di terze parti. Per ulteriori informazioni, contatta il tuo account rappresentante NetApp.

Come funziona il bilanciamento del carico - Servizio di bilanciamento del carico

Il servizio Load Balancer distribuisce le connessioni di rete in entrata dalle applicazioni client ai nodi di storage. Per abilitare il bilanciamento del carico, è necessario configurare gli endpoint del bilanciamento del carico utilizzando Grid Manager.

È possibile configurare gli endpoint del bilanciamento del carico solo per i nodi Admin o Gateway, poiché questi tipi di nodi contengono il servizio Load Balancer. Non è possibile configurare gli endpoint per i nodi di storage o i nodi di archiviazione.

Ogni endpoint del bilanciamento del carico specifica una porta, un protocollo di rete (HTTP o HTTPS), un tipo di client (S3 o Swift) e una modalità di binding. Gli endpoint HTTPS richiedono un certificato server. Le modalità di binding consentono di limitare l'accessibilità delle porte degli endpoint a:

- Gli indirizzi IP virtuali (VIP) di specifici gruppi ad alta disponibilità (ha)
- Interfacce di rete specifiche di nodi Admin e Gateway specifici

Considerazioni sulle porte

I client possono accedere a qualsiasi endpoint configurato su qualsiasi nodo che esegue il servizio Load Balancer, con due eccezioni: Le porte 80 e 443 sono riservate sui nodi di amministrazione, in modo che gli endpoint configurati su queste porte supportino le operazioni di bilanciamento del carico solo sui nodi gateway.

Se sono state rimappate delle porte, non è possibile utilizzare le stesse porte per configurare gli endpoint del bilanciamento del carico. È possibile creare endpoint utilizzando porte rimappate, ma tali endpoint verranno rimappati alle porte e al servizio CLB originali, non al servizio Load Balancer. Seguire la procedura descritta in Rimuovere i rimap delle porte.

Il servizio CLB è obsoleto.

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.
- 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. Solo le appliance SG100 o SG1000 e i nodi software basati su VMware sono consentiti per gli endpoint del bilanciamento del carico utilizzati per S3 Select.
- 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. VedereConfigurare i certificati API S3 e Swift.

    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`. Vedere Configurare i nomi di dominio degli endpoint API S3.

Creare un endpoint per il bilanciamento del carico

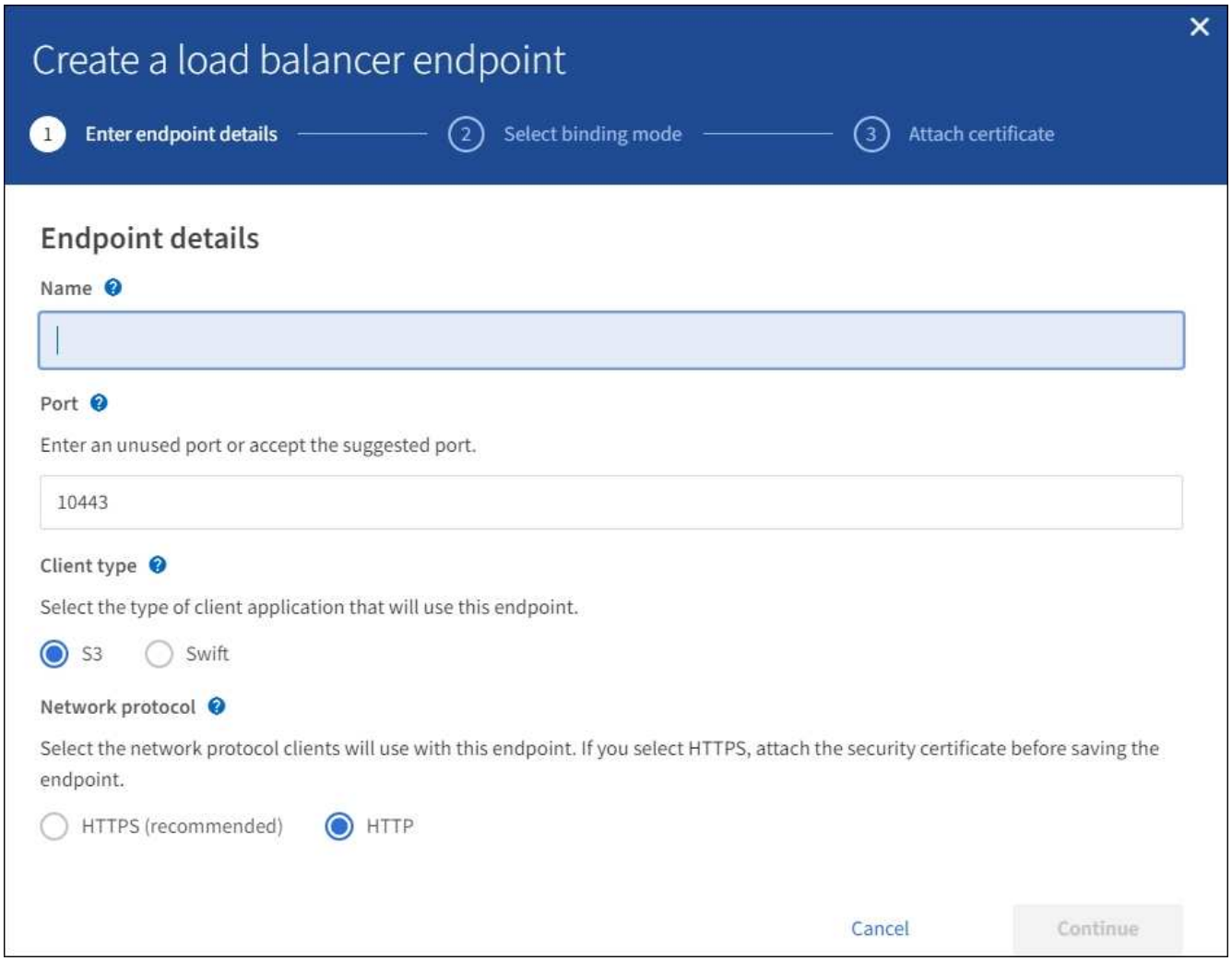
Ogni endpoint del bilanciamento del carico specifica una porta, un tipo di client (S3 o Swift) e un protocollo di rete (HTTP o HTTPS).

Accedere alla procedura guidata

1. Selezionare **CONFIGURATION** > **Network** > **Load Balancer Endpoints**.
2. Selezionare **Crea**.

Inserire i dettagli dell'endpoint

1. Inserire i dettagli per l'endpoint.



Campo	Descrizione
Nome	Un nome descrittivo per l'endpoint, che verrà visualizzato nella tabella della pagina endpoint del bilanciamento del carico.
Porta	I client delle porte utilizzeranno per connettersi al servizio Load Balancer sui nodi Admin e sui nodi Gateway. Accettare il numero di porta consigliato o inserire una porta esterna non utilizzata da un altro servizio di rete. Inserire un valore compreso tra 1 e 65535. Se si immette **80** o **443**, l'endpoint viene configurato solo sui nodi gateway. Queste porte sono riservate sui nodi di amministrazione. Vedere Linee guida per il networking per informazioni sulle porte esterne.
Tipo di client	Il tipo di applicazione client che utilizzerà questo endpoint, **S3** o **Swift**.

Campo	Descrizione
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.

2. Selezionare **continua**.

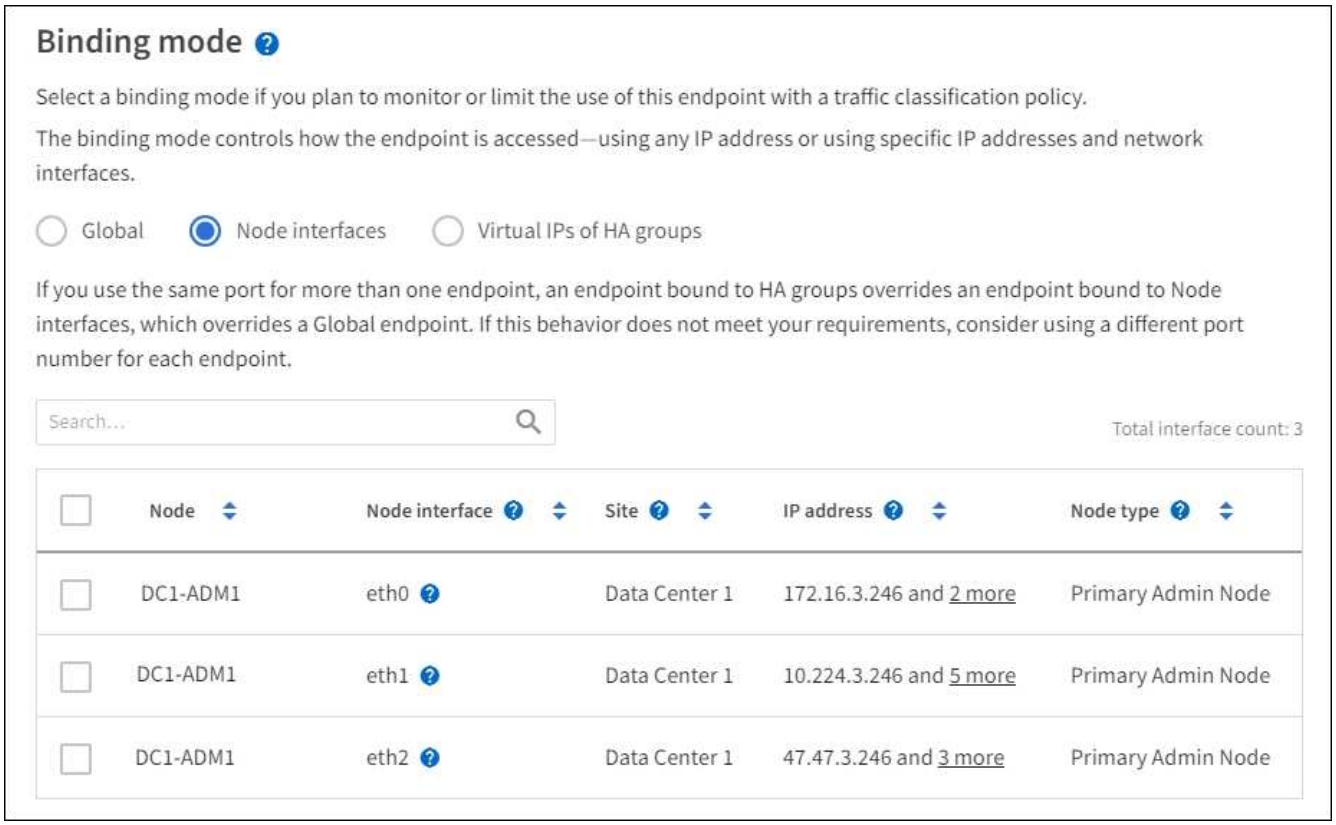
Selezionare la modalità di binding

1. Selezionare una modalità di binding per l'endpoint per controllare le modalità di accesso all'endpoint.

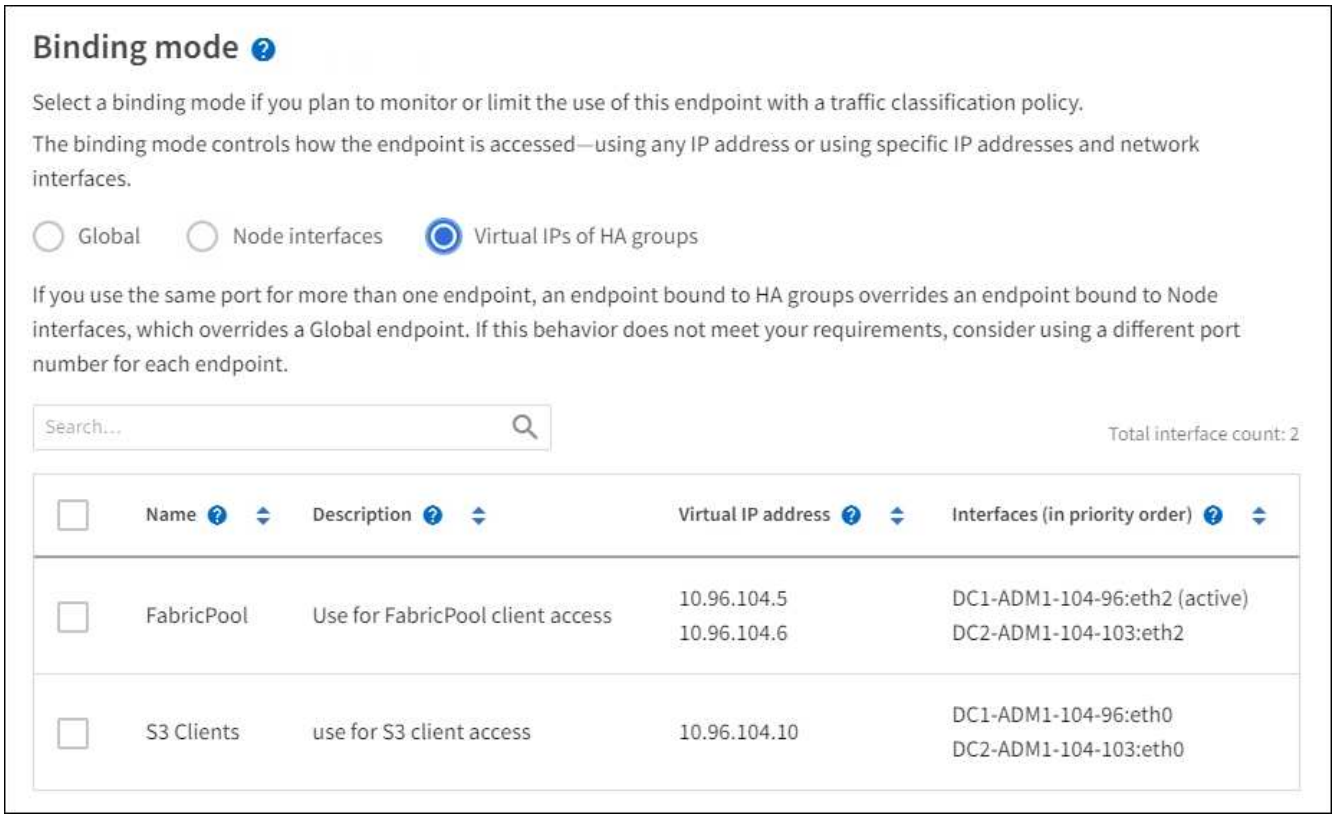
Opzione	Descrizione
Globale (impostazione predefinita)	I client possono accedere all'endpoint utilizzando un FQDN (Fully Qualified Domain Name), l'indirizzo IP di qualsiasi nodo gateway o nodo amministratore o l'indirizzo IP virtuale di qualsiasi gruppo ha su qualsiasi rete. Utilizzare l'impostazione **Global** (predefinita) a meno che non sia necessario limitare l'accessibilità di questo endpoint.
Interfacce di nodo	I client devono utilizzare l'indirizzo IP di un nodo e di un'interfaccia di rete selezionati per accedere a questo endpoint.
IP virtuali dei gruppi ha	I client devono utilizzare un indirizzo IP virtuale di un gruppo ha per accedere a questo endpoint. 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. Gli endpoint con questa modalità possono utilizzare tutti lo stesso numero di porta purché le interfacce selezionate per gli endpoint non si sovrappongano.

Se si utilizza la stessa porta per più di un endpoint, un endpoint che utilizza la modalità **Virtual IP of ha groups** sovrascrive un endpoint utilizzando la modalità **Node interfaces**, che sovrascrive un endpoint utilizzando la modalità **Global**.

2. 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.



3. Se si seleziona **IP virtuali dei gruppi ha**, selezionare uno o più gruppi ha.



4. 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

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. VedereConfigurare i certificati API S3 e Swift.

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 224 bit o superiori. 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 e l'endpoint.

Generare un certificato

a. Selezionare **genera certificato**.

b. Specificare le informazioni del certificato:

- **Domain name**: 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.
- **Oggetto**: Nome distinto (DN) o oggetto X.509 del proprietario del certificato.
- **Giorni validi**: Numero di giorni successivi alla creazione della scadenza del certificato.

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 e questo endpoint.

[[dopo la fine]]al termine

1. Se si utilizza un sistema di nomi di dominio (DNS), assicurarsi che il DNS includa un record per associare il nome di dominio completo 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 qualsiasi nodo gateway o 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.

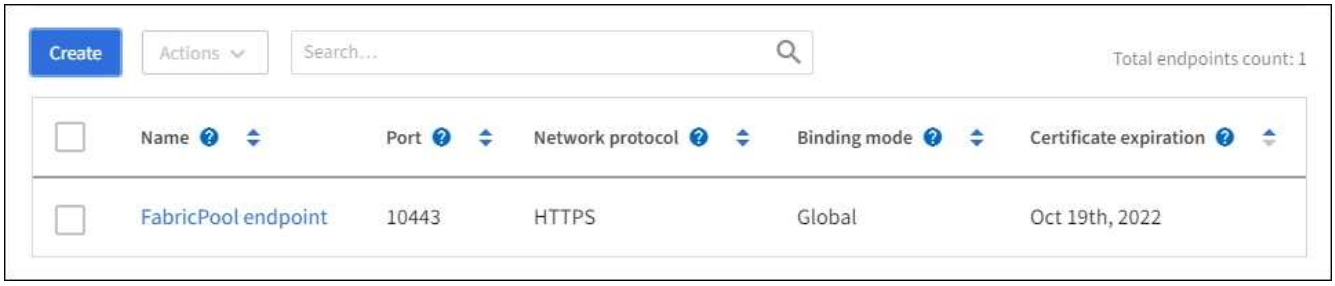
2. Fornire ai client S3 e Swift le informazioni necessarie per connettersi all'endpoint:
   - Numero di porta
   - Nome di dominio completo o indirizzo IP
   - Tutti i dettagli del certificato richiesti

Visualizzare e modificare gli endpoint del bilanciamento del carico

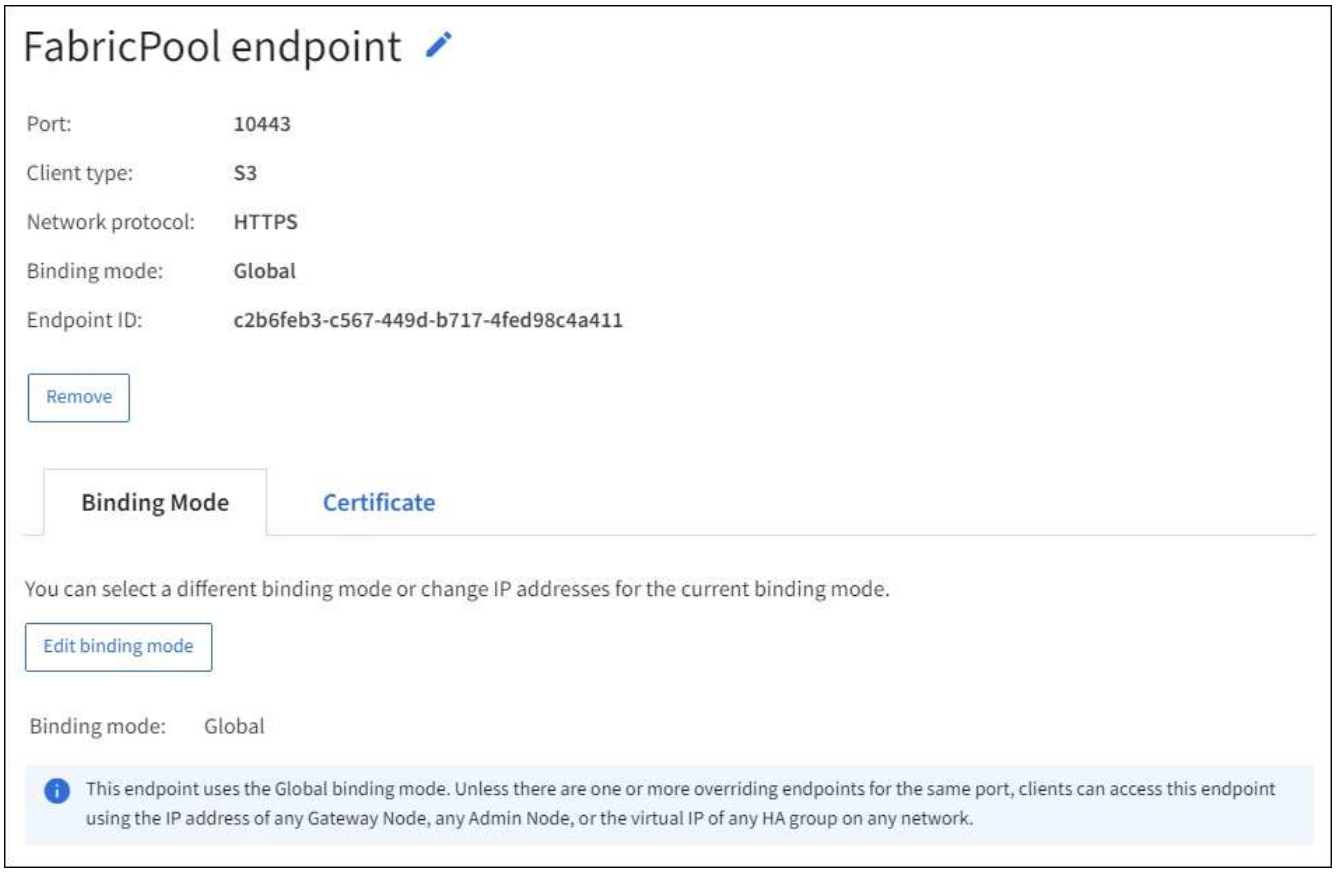
È possibile visualizzare i dettagli degli endpoint del bilanciamento del carico esistenti, inclusi i metadati del certificato per un endpoint protetto. È inoltre possibile modificare il nome o la modalità di binding di un endpoint e aggiornare eventuali certificati associati.

Non è possibile modificare il tipo di servizio (S3 o Swift), la porta o il protocollo (HTTP o HTTPS).

- Per visualizzare le informazioni di base per tutti gli endpoint del bilanciamento del carico, consultare la tabella nella pagina endpoint 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.



- Per modificare un endpoint, utilizzare il menu **azioni** nella pagina endpoint del bilanciamento del carico o nella pagina dei dettagli di un endpoint specifico.

> 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 modalità di associazione degli endpoint	a. Selezionare la casella di controllo per l'endpoint. b. Selezionare **Actions Edit endpoint binding mode**. 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).

Attività	Menu delle azioni	Pagina dei dettagli
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).

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.

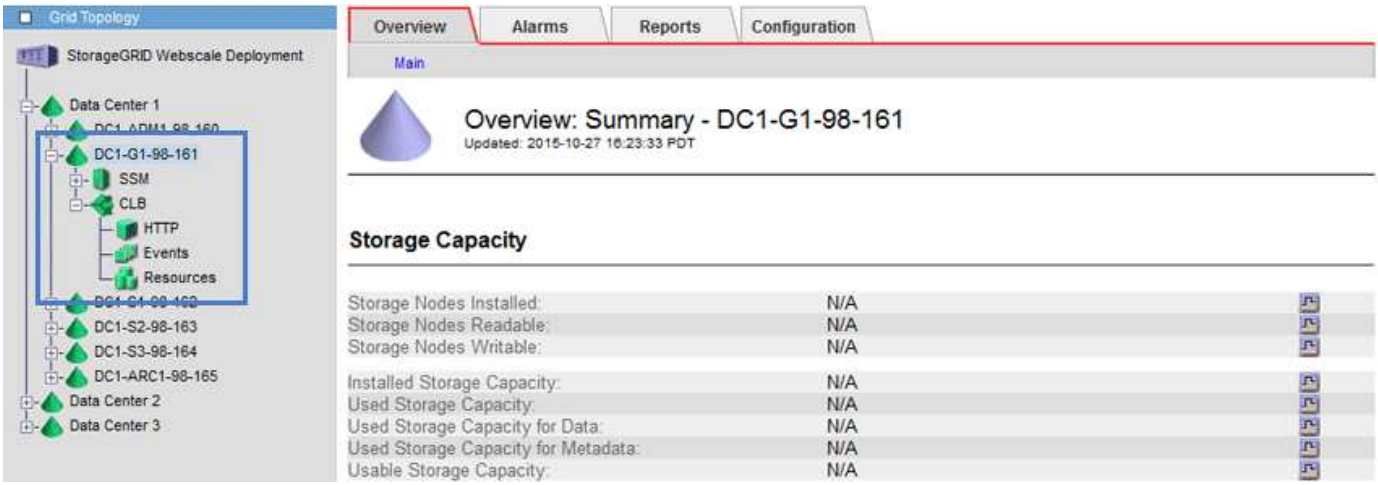
- Per rimuovere uno o più endpoint:
  a. Dalla pagina bilanciamento del carico, selezionare la casella di controllo per ciascun endpoint che si desidera rimuovere.
  b. Selezionare **azioni Rimuovi**.
  c. Selezionare **OK**.
- Per rimuovere un endpoint dalla pagina dei dettagli:
  a. Dalla pagina bilanciamento del carico. selezionare il nome dell'endpoint.
  b. Selezionare **Rimuovi** nella pagina dei dettagli.
  c. Selezionare **OK**.

Come funziona il bilanciamento del carico - servizio CLB (obsoleto)

Il servizio di bilanciamento del carico di connessione (CLB) sui nodi gateway è obsoleto. Il servizio Load Balancer è ora il meccanismo di bilanciamento del carico consigliato.

Il servizio CLB utilizza il bilanciamento del carico di livello 4 per distribuire le connessioni di rete TCP in entrata dalle applicazioni client al nodo di storage ottimale in base alla disponibilità, al carico di sistema e al costo del collegamento configurato dall'amministratore. Quando si sceglie il nodo di storage ottimale, il servizio CLB stabilisce una connessione di rete bidirezionale e inoltra il traffico da e verso il nodo selezionato. La CLB non prende in considerazione la configurazione Grid Network quando indirizza le connessioni di rete in entrata.

Per visualizzare le informazioni sul servizio CLB, selezionare **SUPPORT Tools Grid topology**, quindi espandere un nodo gateway fino a quando non è possibile selezionare **CLB** e le opzioni sottostanti.



Se si sceglie di utilizzare il servizio CLB, si consiglia di configurare i costi di collegamento per il sistema StorageGRID.

- Quali sono i costi di collegamento
- Aggiornare i costi dei collegamenti

Configurare i nomi di dominio degli endpoint API S3

Per supportare le richieste in stile host virtuale S3, è necessario utilizzare Grid Manager per configurare l'elenco dei nomi di dominio degli endpoint a cui si connettono i client S3.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.
- Hai confermato che non è in corso un aggiornamento della griglia.

> Non apportare modifiche alla configurazione del nome di dominio quando è in corso un aggiornamento della griglia.

A proposito di questa attività

Per consentire ai client di utilizzare i nomi di dominio degli endpoint S3, è necessario eseguire tutte le seguenti operazioni:

- Utilizzare Grid Manager per aggiungere i nomi di dominio degli endpoint S3 al sistema StorageGRID.
- Assicurarsi che il certificato utilizzato dal client per le connessioni HTTPS a StorageGRID sia 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 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.

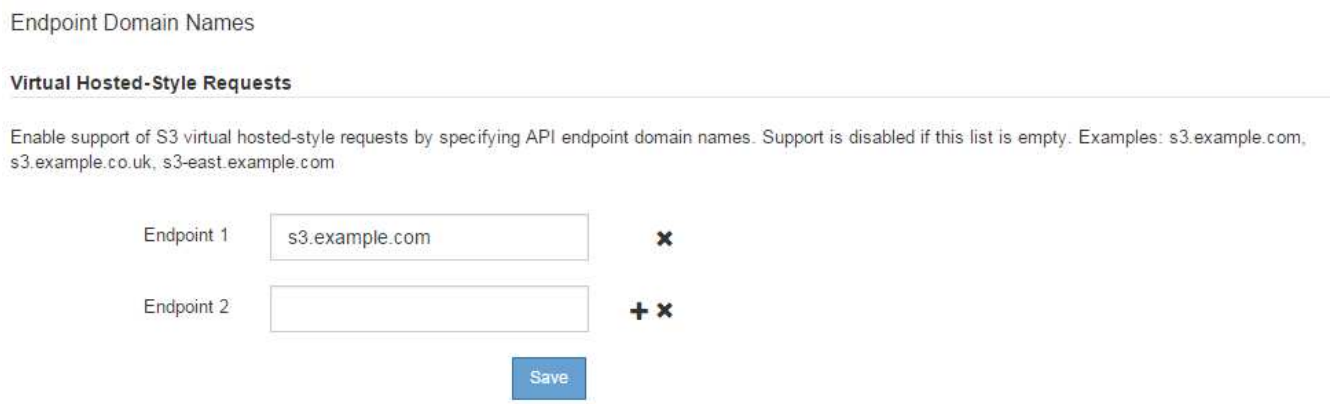
I client che utilizzano connessioni HTTPS (consigliate) alla griglia possono utilizzare uno dei seguenti certificati:

- 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 in modo da riconoscere nomi di dominio degli endpoint diversi.
- I client che si connettono a un endpoint di bilanciamento del carico, direttamente a un nodo di storage o direttamente al servizio CLB obsoleto su un nodo gateway possono personalizzare il certificato globale S3 e Swift API per includere tutti i nomi di dominio degli endpoint richiesti.

Fasi

1. Selezionare **CONFIGURAZIONE rete nomi di dominio**.

   Viene visualizzata la pagina Endpoint Domain Names (nomi dominio endpoint).



2. Immettere l'elenco dei nomi di dominio degli endpoint API S3 nei campi **Endpoint**. Utilizzare + per aggiungere altri campi.

   Se l'elenco è vuoto, il supporto per le richieste di tipo host virtuale S3 viene disattivato.

3. Selezionare **Salva**.
4. Assicurarsi che i certificati server utilizzati dai client corrispondano ai nomi di dominio degli endpoint 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 API globale S3 e Swift, direttamente ai nodi di storage o al servizio CLB sui nodi gateway, aggiornare il certificato API globale S3 e Swift.
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.

Informazioni correlate

- Utilizzare S3
- Visualizzare gli indirizzi IP
- Configurare i gruppi ad alta disponibilità
- Configurare i certificati API S3 e Swift
- Configurare gli endpoint del bilanciamento del carico

Abilitare HTTP per le comunicazioni client

Per impostazione predefinita, le applicazioni client utilizzano il protocollo di rete HTTPS per tutte le connessioni ai nodi di storage o al servizio CLB obsoleto sui nodi gateway. È possibile attivare il protocollo HTTP per queste connessioni, ad esempio durante il test di un grid non di produzione.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Completare questa attività solo se i client S3 e Swift devono stabilire connessioni HTTP direttamente ai nodi di storage o al servizio CLB obsoleto sui nodi gateway.

Non è necessario completare questa attività per i client che utilizzano solo connessioni HTTPS o per i client che si connettono al servizio Load Balancer (poiché è possibile configurare ciascun endpoint Load Balancer in modo che utilizzi HTTP o HTTPS). Per ulteriori informazioni, vedere le informazioni sulla configurazione degli endpoint del bilanciamento del carico.

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 o al servizio CLB obsoleto utilizzando HTTP o HTTPS

> Prestare attenzione quando si attiva HTTP per una griglia di produzione perché le richieste verranno inviate senza crittografia.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Opzioni di rete, selezionare la casella di controllo **attiva connessione HTTP**.

3. Selezionare **Salva**.

Informazioni correlate

- Configurare gli endpoint del bilanciamento del carico
- Utilizzare S3
- USA Swift

Controllare quali operazioni client sono consentite

È possibile selezionare l'opzione Impedisci modifica client per negare specifiche operazioni del client HTTP.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Impedisci modifica client è un'impostazione a livello di sistema. Quando si seleziona l'opzione Impedisci modifica client, le seguenti richieste vengono rifiutate:

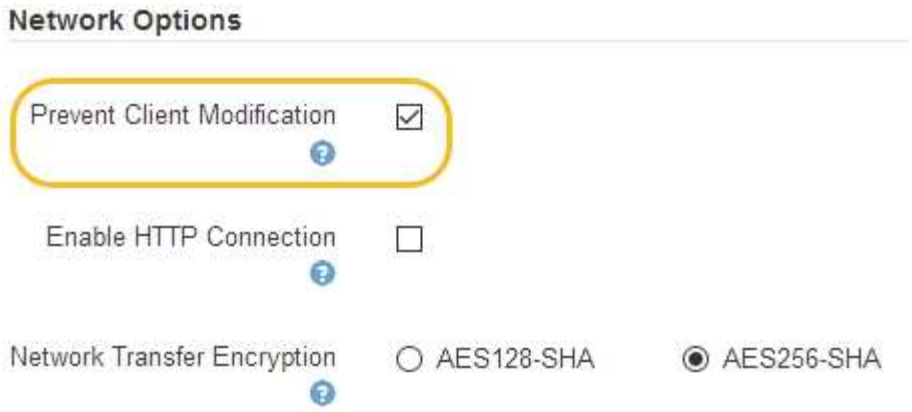
- **S3 REST API**
  - Elimina richieste bucket
  - Qualsiasi richiesta di modifica dei dati di un oggetto esistente, dei metadati definiti dall'utente o del tagging degli oggetti S3

> Questa impostazione non si applica ai bucket con versione attivata. Il controllo delle versioni impedisce già le modifiche ai dati degli oggetti, ai metadati definiti dall'utente e all'etichettatura degli oggetti.

- **API REST Swift**
  - 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.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Opzioni di rete, selezionare la casella di controllo **Impedisci modifica client**.



3. Selezionare **Salva**.

Gestire reti e connessioni

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 della griglia StorageGRID richiede un'interfaccia di rete dedicata, un indirizzo IP, una subnet mask e un gateway per ciascuna rete a cui è assegnato.

- Un nodo Grid non può avere più di un'interfaccia su una rete.
- È supportato un singolo gateway, per rete, per nodo di rete, che deve trovarsi sulla stessa sottorete del nodo. Se necessario, è possibile implementare un routing più complesso nel gateway.
- Su ciascun nodo, ogni rete viene mappata a una specifica interfaccia di rete.

Rete	Nome dell'interfaccia
Griglia	eth0
Admin (opzionale)	eth1
Client (opzionale)	eth2

- Se il nodo è collegato a un'appliance StorageGRID, vengono utilizzate porte specifiche per ciascuna rete. Per ulteriori informazioni, consultare le istruzioni di installazione dell'apparecchio.
- Il percorso predefinito viene generato automaticamente, per nodo. Se eth2 è attivato, 0.0.0.0/0 utilizza la rete client su eth2. Se eth2 non è abilitato, 0.0.0.0/0 utilizza Grid Network su eth0.
- La rete client non diventa operativa fino a quando il nodo grid non si è Unito alla griglia
- La rete amministrativa può essere configurata durante l'implementazione del nodo grid per consentire l'accesso all'interfaccia utente dell'installazione prima che la griglia sia completamente installata.

Interfacce opzionali

In alternativa, è possibile aggiungere interfacce aggiuntive a un nodo. Ad esempio, è possibile aggiungere un'interfaccia 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
- **RHEL o CentOS (prima di installare il nodo)**: Creare file di configurazione del nodo
- **Ubuntu o Debian (prima di installare il nodo)**: Creare file di configurazione del nodo
- **RHEL, CentOS, Ubuntu o Debian (dopo aver installato il nodo)**: Linux: Aggiunta di interfacce di accesso o trunk a un nodo

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.

Di cosa hai bisogno

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

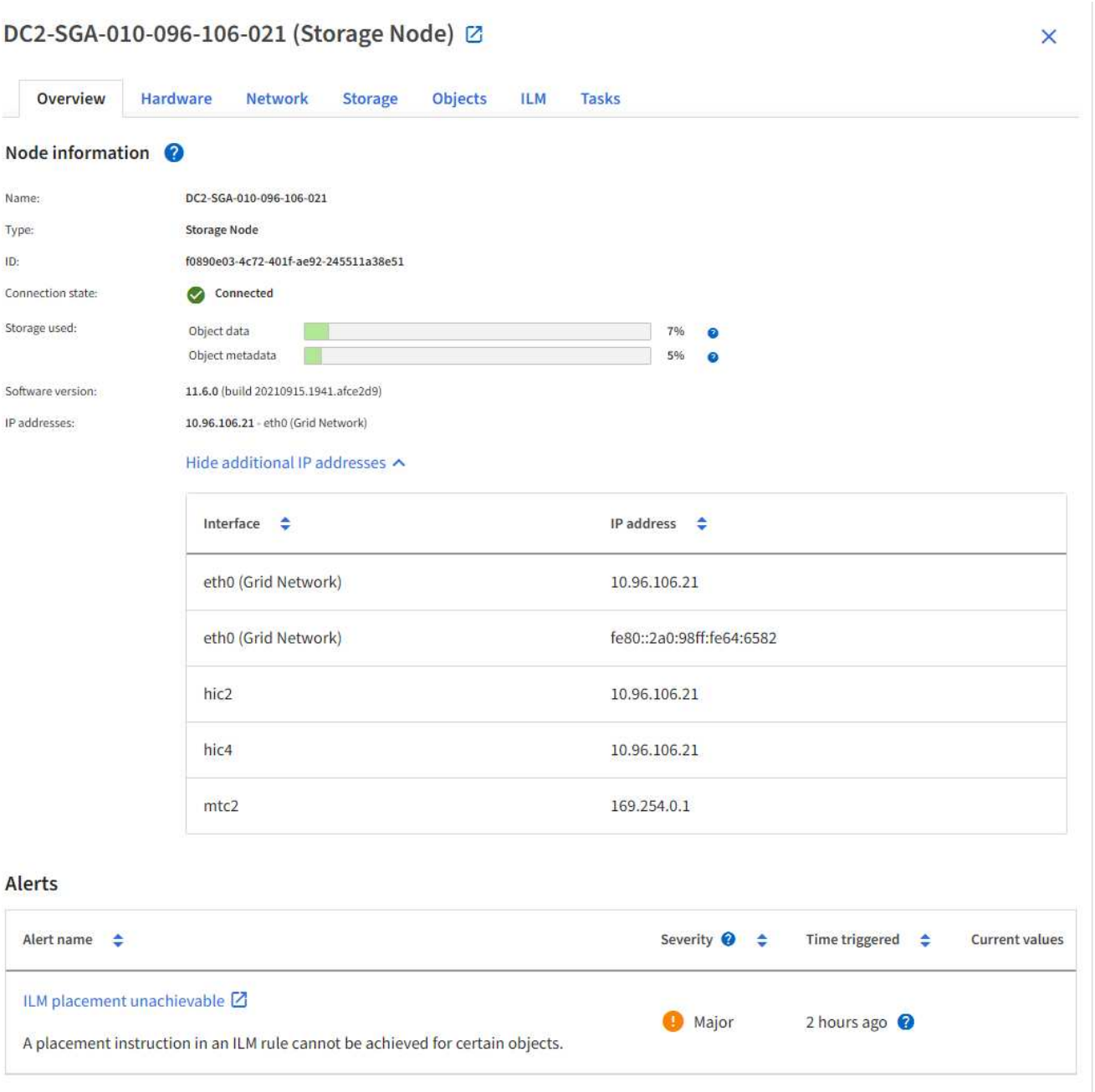
A proposito di questa attività

Per informazioni sulla modifica degli indirizzi IP, vedere Ripristino e manutenzione.

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.



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.

> Le opzioni di configurazione TLS, quali 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.

Suite di crittografia TLS 1.2 supportate

Sono supportate le seguenti suite di crittografia TLS 1.2:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384

Suite di crittografia TLS 1.3 supportate

Sono supportate le seguenti suite di crittografia TLS 1.3:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256

Modificare la crittografia del trasferimento di rete

Il sistema StorageGRID utilizza TLS (Transport Layer Security) per proteggere il traffico di controllo interno tra i nodi di rete. L'opzione Network Transfer Encryption (crittografia trasferimento di rete) imposta l'algoritmo utilizzato da TLS per crittografare il traffico di controllo tra i nodi della griglia. Questa impostazione non influisce sulla crittografia dei dati.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impostazione predefinita, la crittografia del trasferimento di rete utilizza l'algoritmo AES256-SHA. Il traffico

di controllo può anche essere crittografato utilizzando l'algoritmo AES128-SHA.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Network Options (Opzioni di rete), impostare Network Transfer Encryption (crittografia trasferimento di rete) su **AES128-SHA** o **AES256-SHA** (impostazione predefinita).

3. Selezionare **Salva**.

Gestire le policy di classificazione del traffico

Gestire le policy di classificazione del traffico

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
- Tenant
- Subnet (subnet IPv4 contenente il client)
- Endpoint (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

Facoltativamente, è possibile impostare limiti per una policy in base ai seguenti parametri:

- Larghezza di banda aggregata in

- Larghezza di banda aggregata in uscita
- Richieste di lettura simultanee
- Richieste di scrittura simultanee
- Larghezza di banda per richiesta in
- Larghezza di banda per richiesta in uscita
- Velocità richiesta di lettura
- Tasso di richieste di scrittura

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. 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.

I limiti di classificazione del traffico vengono implementati per 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.

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	Performance	Costo
Oro	1 PB di storage consentito	3 copia regola ILM	25 K richieste/sec Larghezza di banda di 5 GB/sec (40 Gbps)	€ al mese

Livello di servizio	Capacità	Protezione dei dati	Performance	Costo
Argento	250 TB di storage consentiti	2 copia regola ILM	10 K richieste/sec Larghezza di banda di 1.25 GB/sec (10 Gbps)	dollari al mese
Bronzo	100 TB di storage consentiti	2 copia regola ILM	5 K richieste/sec Larghezza di banda di 1 GB/sec (8 Gbps)	dollari al mese

Creare policy di classificazione del traffico

È possibile creare criteri di classificazione del traffico se si desidera monitorare e, facoltativamente, limitare il traffico di rete per bucket, tenant, subnet IP o endpoint del bilanciamento del carico. Facoltativamente, è possibile impostare limiti per una policy in base alla larghezza di banda, al numero di richieste simultanee o alla velocità di richiesta.

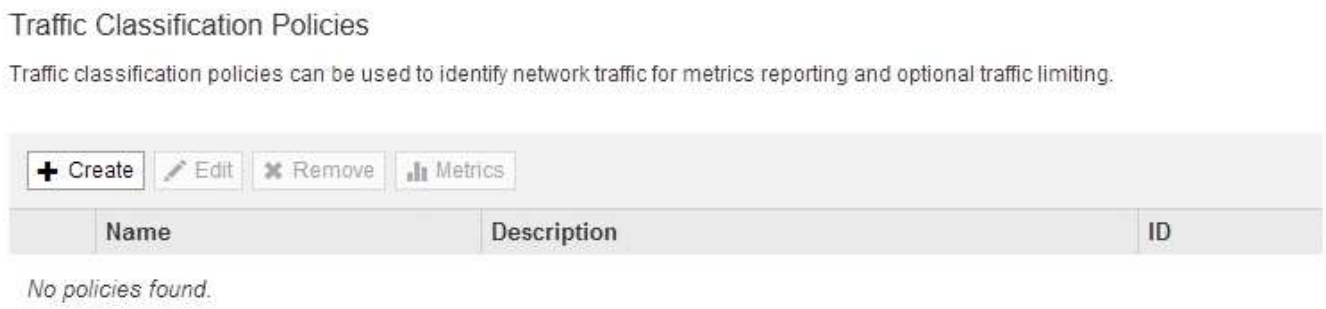
Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.
- Sono stati creati endpoint di bilanciamento del carico che si desidera associare.
- Hai creato i tenant che desideri abbinare.

Fasi

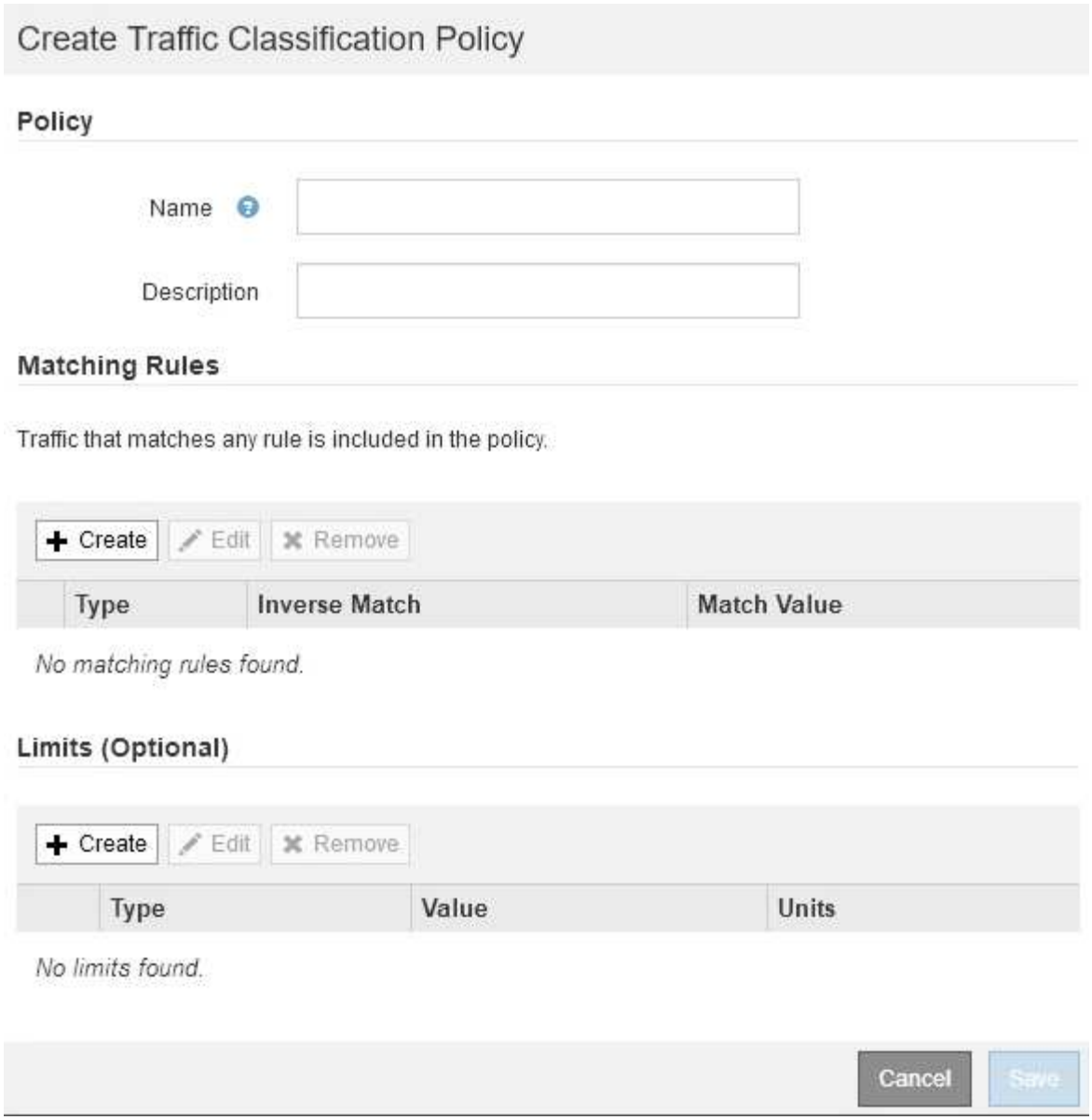
1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Criteri di classificazione del traffico.



2. Selezionare **Crea**.

   Viene visualizzata la finestra di dialogo Crea policy di classificazione del traffico.



3. Nel campo **Nome**, immettere un nome per la policy.

   Immettere un nome descrittivo per poter riconoscere il criterio.

4. Facoltativamente, aggiungere una descrizione per la policy nel campo **Descrizione**.

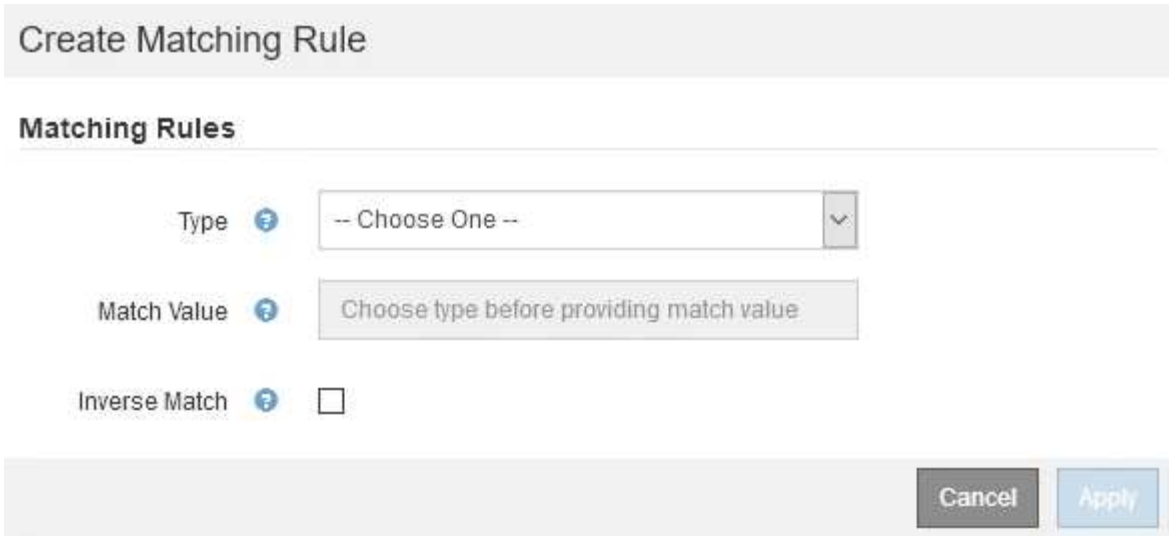
   Ad esempio, descrivi a cosa si applica questa policy di classificazione del traffico e a cosa limiterà.

5. Creare una o più regole corrispondenti per il criterio.

   Le regole corrispondenti controllano le entità interessate da questa policy di classificazione del traffico. Ad esempio, selezionare tenant se si desidera che questo criterio venga applicato al traffico di rete di un tenant specifico. In alternativa, selezionare Endpoint se si desidera applicare questo criterio al traffico di rete su un endpoint specifico del bilanciamento del carico.

   a. Selezionare **Crea** nella sezione **regole corrispondenti**.

      Viene visualizzata la finestra di dialogo Create Matching Rule (Crea regola corrispondente).



b. Dal menu a discesa **Type**, selezionare il tipo di entità da includere nella regola di corrispondenza.

c. Nel campo **valore di corrispondenza**, immettere un valore di corrispondenza in base al tipo di entità scelta.

   - Bucket (bucket): Immettere il nome di un bucket.
   - Bucket Regex (Regex bucket): Immettere un'espressione regolare che verrà utilizzata per far corrispondere un set di nomi di bucket.

     L'espressione regolare non è ancorata. Utilizzare l'ancora ^ per trovare la corrispondenza all'inizio del nome del bucket e utilizzare l'ancora per la corrispondenza alla fine del nome.

   - CIDR: Immettere una subnet IPv4, nella notazione CIDR, che corrisponda alla subnet desiderata.
   - Endpoint: Selezionare un endpoint dall'elenco degli endpoint esistenti. Questi sono gli endpoint del bilanciamento del carico definiti nella pagina endpoint del bilanciamento del carico. Vedere Configurare gli endpoint del bilanciamento del carico.
   - Tenant (tenant): Selezionare un tenant dall'elenco dei tenant esistenti. L'abbinamento dei tenant si basa sulla proprietà del bucket a cui si accede. L'accesso anonimo a un bucket corrisponde al tenant proprietario del bucket.

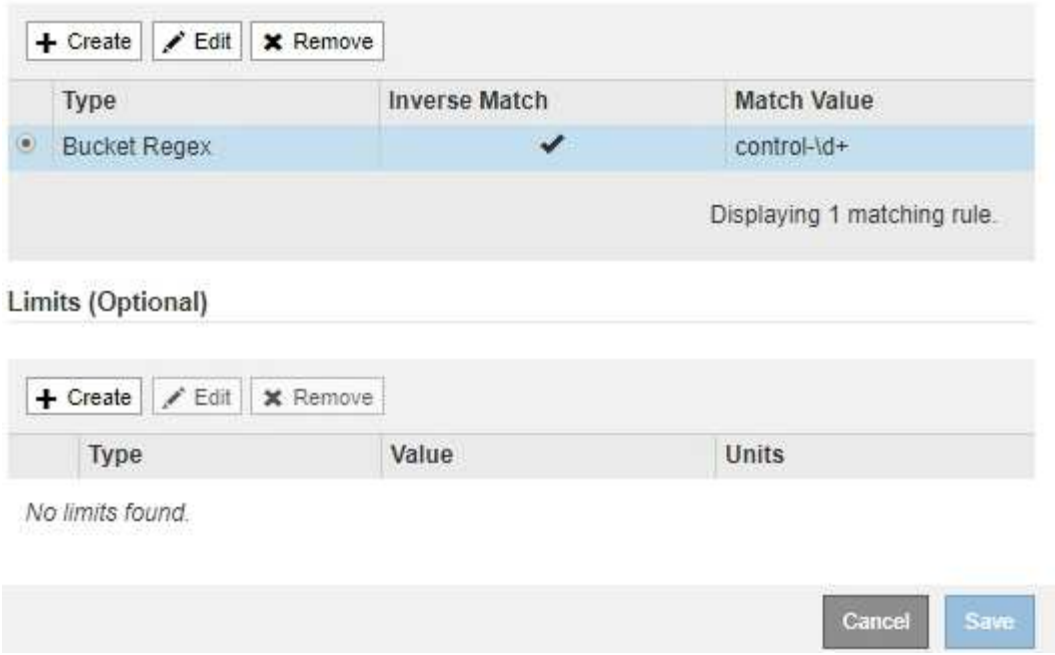
d. Se si desidera far corrispondere tutto il traffico di rete *tranne* corrispondente al valore Type and Match appena definito, selezionare la casella di controllo **Inverse**. In caso contrario, lasciare deselezionata la casella di controllo.

   Ad esempio, se si desidera che questo criterio venga applicato a tutti gli endpoint del bilanciamento del carico tranne uno, specificare l'endpoint del bilanciamento del carico da escludere e selezionare **inverso**.

   > 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.

e. Selezionare **Applica**.

   La regola viene creata ed elencata nella tabella regole corrispondenti.



a. Ripetere questi passaggi per ogni regola che si desidera creare per il criterio.

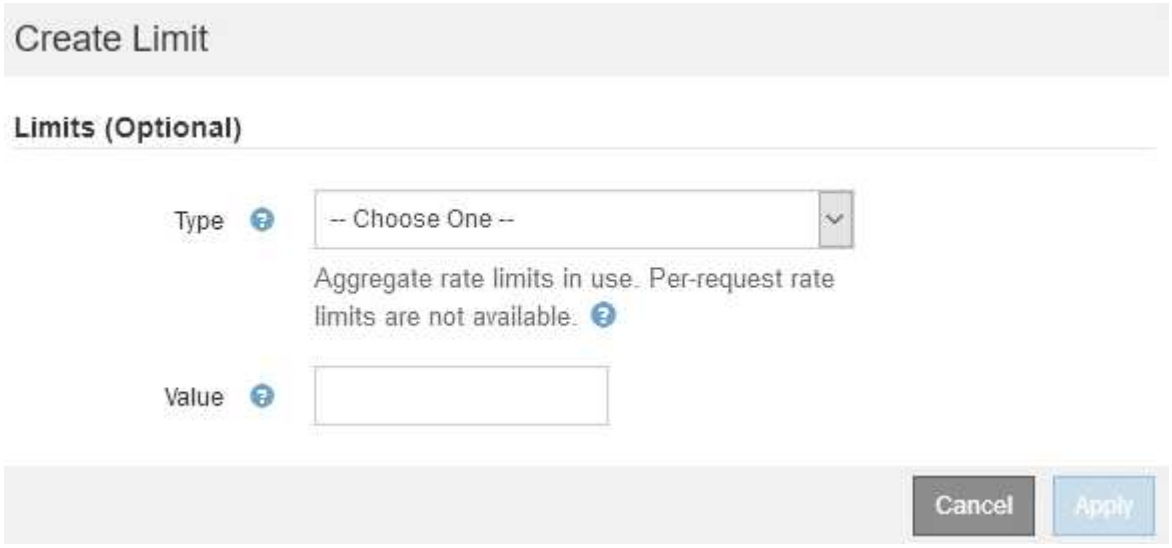
> Il traffico che corrisponde a qualsiasi regola viene gestito dal criterio.

6. Facoltativamente, creare limiti per la policy.

> Anche se non si creano limiti, StorageGRID raccoglie le metriche in modo da poter monitorare il traffico di rete corrispondente alla policy.

a. Selezionare **Crea** nella sezione **limiti**.

Viene visualizzata la finestra di dialogo Create Limit (Crea limite).



b. Nell'elenco a discesa **tipo**, selezionare il tipo di limite che si desidera applicare al criterio.

Nell'elenco seguente, **in** si riferisce al traffico dai client S3 o Swift al bilanciamento del carico StorageGRID, mentre **out** si riferisce al traffico dal bilanciamento del carico ai client S3 o Swift.

- Larghezza di banda aggregata in
- Larghezza di banda aggregata in uscita
- Richieste di lettura simultanee
- Richieste di scrittura simultanee
- Larghezza di banda per richiesta in
- Larghezza di banda per richiesta in uscita
- Velocità richiesta di lettura
- Tasso di richieste di scrittura

> 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, 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 "Best" per i limiti di larghezza di banda nel seguente ordine:

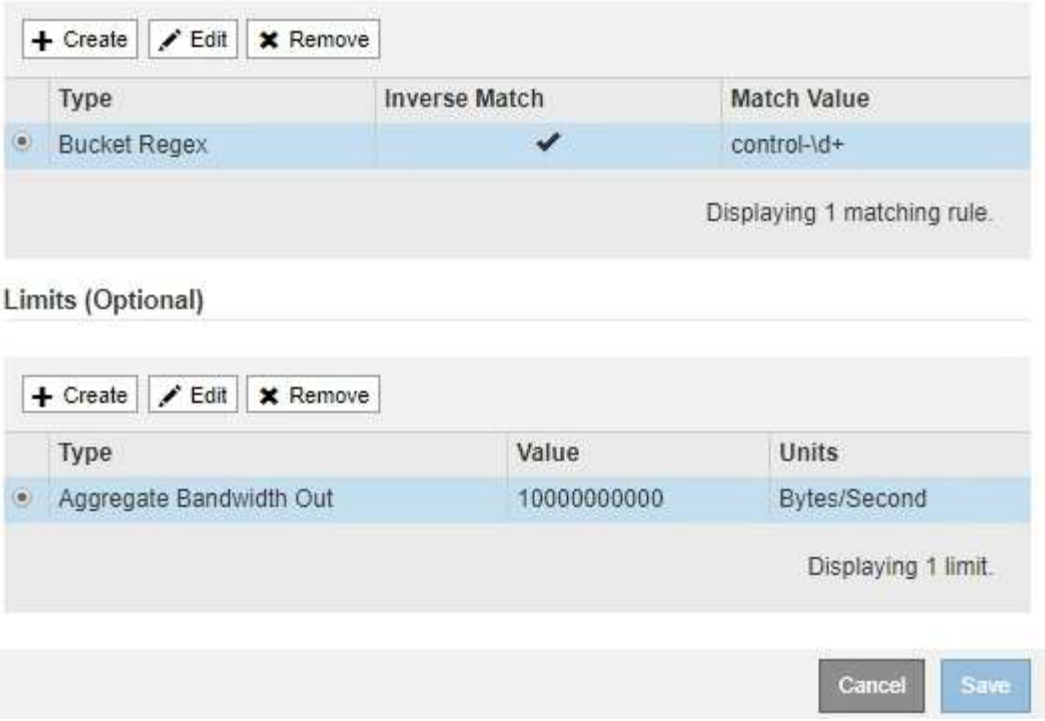
- Indirizzo IP esatto (/32 mask)
- Nome esatto del bucket
- Regex. Bucket
- Tenant
- Endpoint
- Corrispondenze CIDR non esatte (non /32)
- Corrispondenze inverse

c. Nel campo **valore**, immettere un valore numerico per il tipo di limite scelto.

   Le unità previste vengono visualizzate quando si seleziona un limite.

d. Selezionare **Applica**.

   Il limite viene creato ed è elencato nella tabella dei limiti.



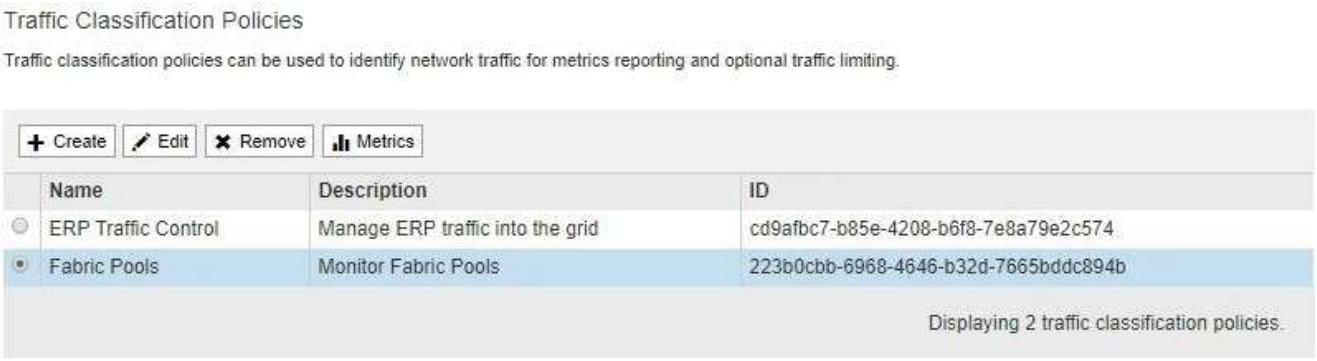
e. Ripetere questi passaggi per ciascun limite che si desidera aggiungere al criterio.

   Ad esempio, se si desidera creare un limite di larghezza di banda di 40 Gbps per un livello SLA, creare un limite di larghezza di banda aggregata in limite e un limite di larghezza di banda aggregato in uscita e impostare ciascuno su 40 Gbps.

> Per convertire megabyte al secondo in gigabit al secondo, moltiplicare per otto. Ad esempio, 125 MB/s equivale a 1,000 Mbps o 1 Gbps.

7. Al termine della creazione di regole e limiti, selezionare **Salva**.

   La policy viene salvata ed è elencata nella tabella Traffic Classification Policies (Criteri di classificazione del traffico).



   Il traffico dei client S3 e Swift viene ora 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. Vedere Visualizzare le metriche del traffico di rete.

Modificare una 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.

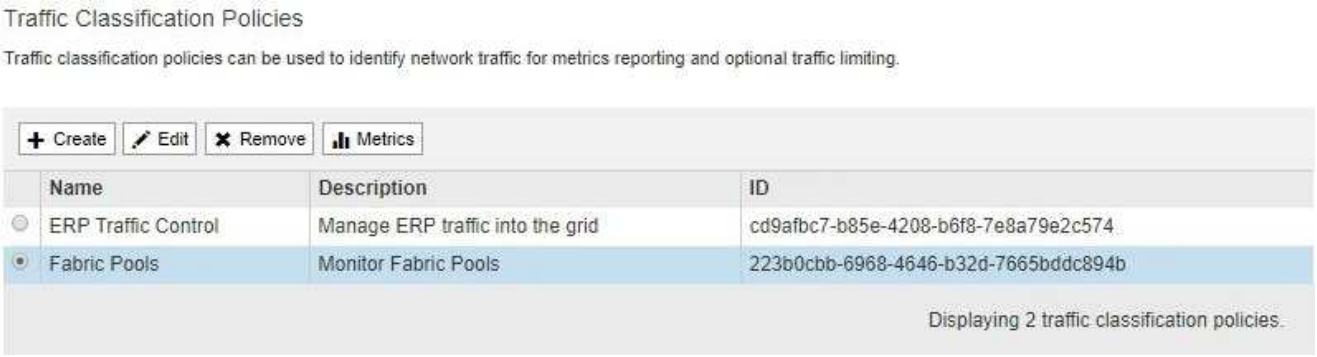
Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.

Fasi

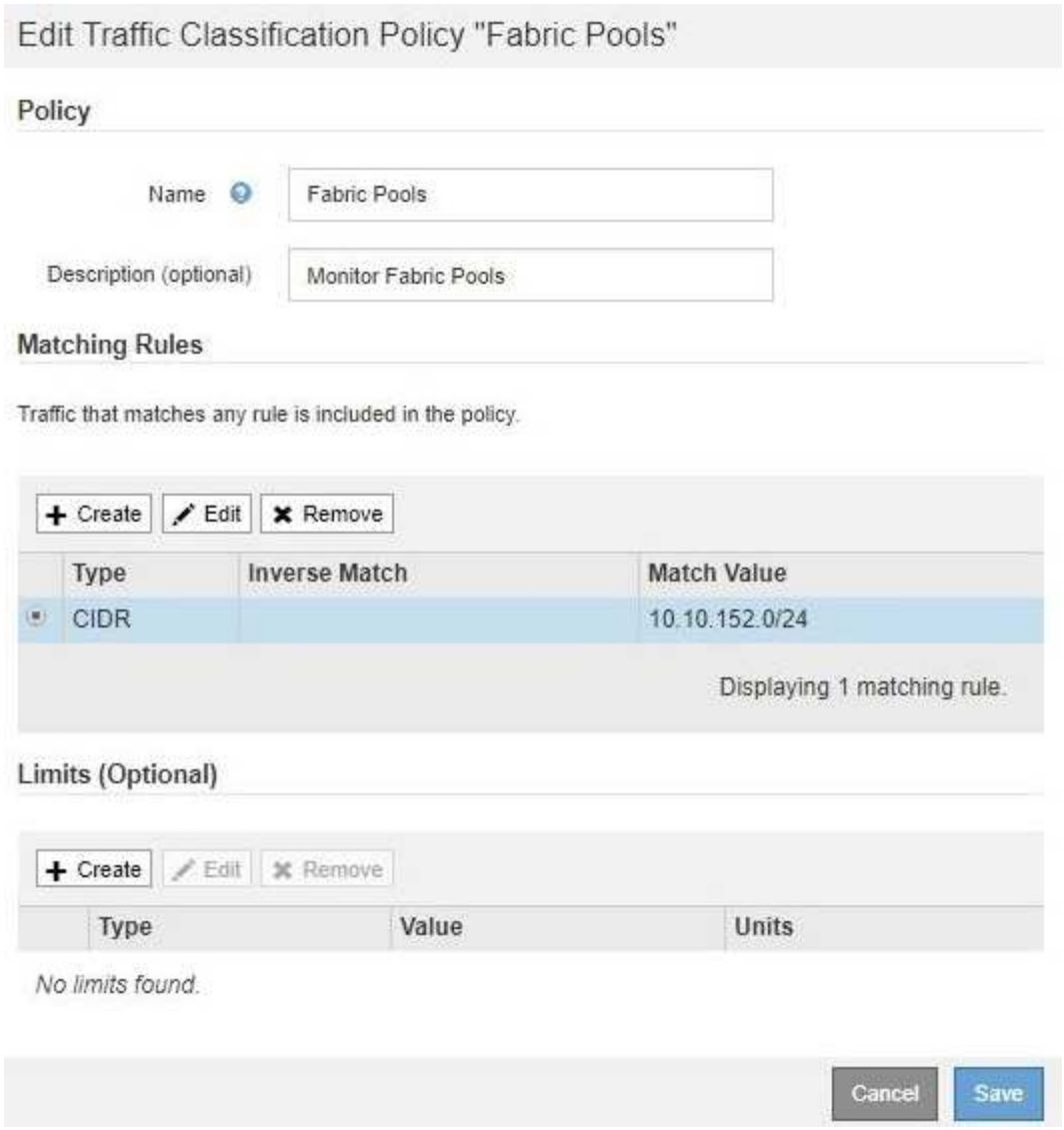
1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



2. Selezionare il pulsante di opzione a sinistra del criterio che si desidera modificare.
3. Selezionare **Modifica**.

   Viene visualizzata la finestra di dialogo Modifica policy di classificazione del traffico.



4. Creare, modificare o rimuovere regole e limiti corrispondenti in base alle esigenze.
   a. Per creare una regola o un limite corrispondente, selezionare **Crea** e seguire le istruzioni per creare una regola o un limite.
   b. Per modificare una regola o un limite corrispondente, selezionare il pulsante di opzione corrispondente alla regola o al limite, selezionare **Edit** (Modifica) nella sezione **Matching Rules** (regole corrispondenti) o nella sezione **Limits** (limiti) e seguire le istruzioni per creare una regola o un limite.
   c. Per rimuovere una regola o un limite corrispondente, selezionare il pulsante di opzione corrispondente alla regola o al limite e selezionare **Rimuovi**. Quindi, selezionare **OK** per confermare che si desidera rimuovere la regola o il limite.
5. Una volta creata o modificata una regola o un limite, selezionare **Apply** (Applica).
6. Una volta terminata la modifica del criterio, selezionare **Salva**.

   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

Se non è più necessario un criterio di classificazione del traffico, è possibile eliminarlo.

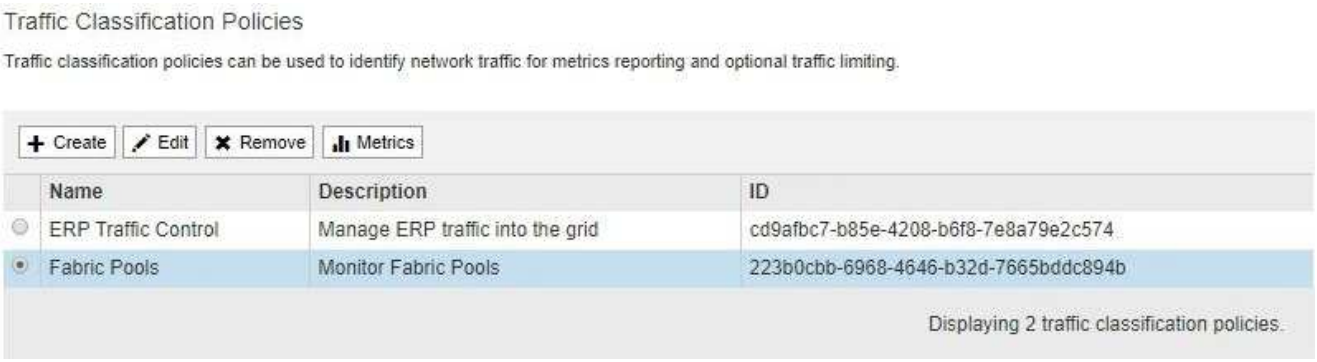
Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root.

Fasi

1. Selezionare **CONFIGURAZIONE** > **rete** > **classificazione del traffico**.

   Viene visualizzata la pagina Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



2. Selezionare il pulsante di opzione a sinistra del criterio che si desidera eliminare.
3. Selezionare **Rimuovi**.

   Viene visualizzata la finestra di dialogo Avviso.

4. Selezionare **OK** 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 Traffic Classification Policies (Criteri di classificazione del traffico).

Di cosa hai bisogno

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

- Si dispone dell'autorizzazione di accesso root o dell'autorizzazione account tenant.

A proposito di questa attività

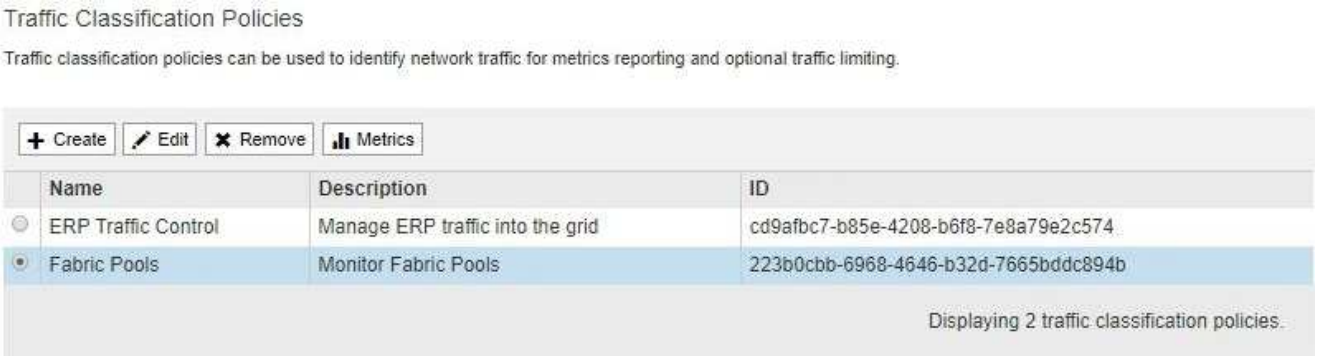
Per qualsiasi criterio di classificazione del traffico esistente, è possibile visualizzare le metriche per il servizio Load Balancer per determinare se il criterio limita correttamente il traffico nella rete. I dati nei grafici possono aiutare a determinare se è necessario modificare la policy.

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 Traffic Classification Policies (Criteri di classificazione del traffico) e i criteri esistenti sono elencati nella tabella.



   I pulsanti **Crea**, **Modifica** e **Rimuovi** sono disattivati se si dispone dell'autorizzazione account tenant ma non si dispone dell'autorizzazione di accesso root.

2. Selezionare il pulsante di opzione a sinistra della policy per la quale si desidera visualizzare le metriche.
3. Selezionare **metriche**.

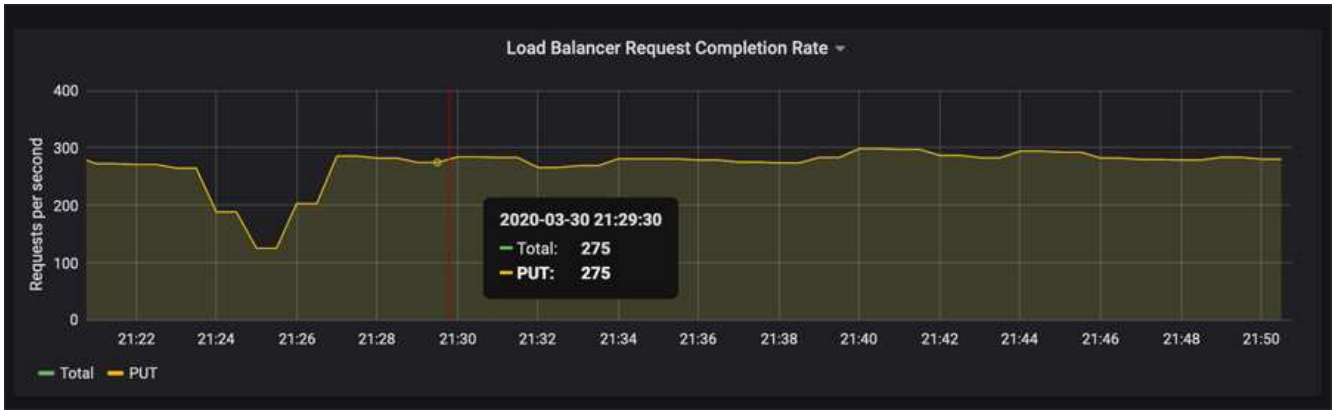
   Viene visualizzata una nuova finestra del browser e i grafici della policy di classificazione del traffico. I grafici visualizzano le metriche solo per il traffico corrispondente al criterio selezionato.

   È possibile selezionare altri criteri da visualizzare utilizzando l'elenco a discesa **policy**.

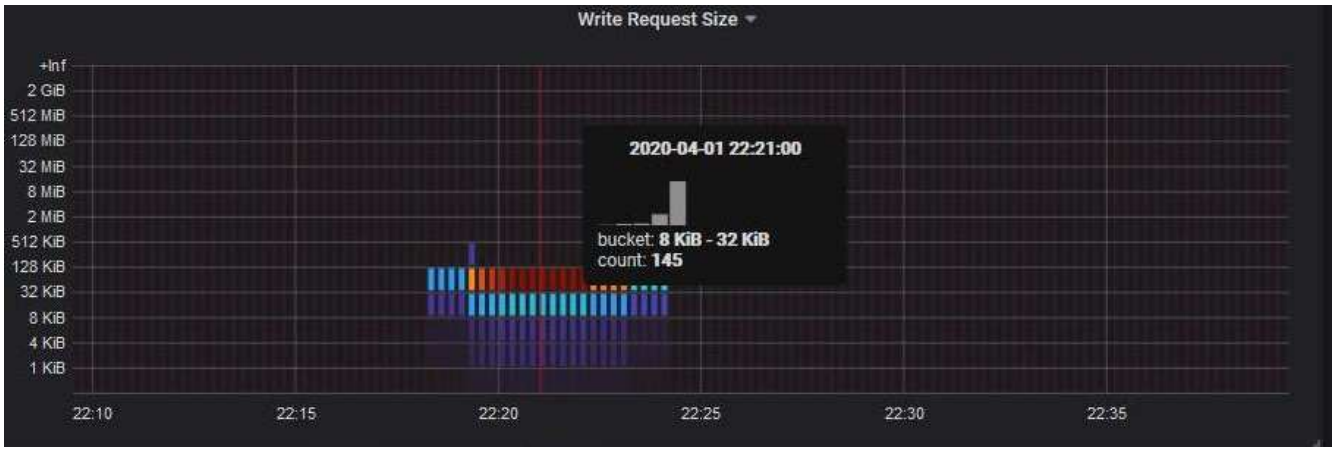
I grafici seguenti sono inclusi nella pagina Web.

- Load Balancer Request Traffic: Questo grafico fornisce una media mobile di 3 minuti del throughput dei dati trasmessi tra gli endpoint del bilanciamento del carico e i client che eseguono le richieste, in bit al secondo.
- Tasso di completamento della richiesta di bilanciamento del carico: Questo grafico fornisce una media mobile di 3 minuti del numero di richieste completate al secondo, suddiviso per tipo di richiesta (GET, PUT, HEAD e DELETE). Questo valore viene aggiornato quando le intestazioni di una nuova richiesta sono state convalidate.
- Tasso di risposta agli errori: Questo grafico fornisce una media mobile di 3 minuti del numero di risposte agli errori restituite ai client al secondo, suddiviso per codice di risposta agli errori.
- Durata media della richiesta (non errore): Questo grafico fornisce una media mobile di 3 minuti delle durate della richiesta, suddivisa per tipo di richiesta (GET, PUT, HEAD e DELETE). Ogni durata della richiesta inizia quando un'intestazione di richiesta viene analizzata dal servizio Load Balancer e termina quando il corpo di risposta completo viene restituito al client.
- Write Request Rate by Object Size (velocità di richiesta di scrittura per dimensione oggetto): Questa mappa termica fornisce una media mobile di 3 minuti della velocità di completamento delle richieste di scrittura in base alle dimensioni dell'oggetto. In questo contesto, le richieste di scrittura si riferiscono solo alle richieste PUT.
- Read Request Rate by Object Size (velocità richiesta di lettura per dimensione oggetto): Questa mappa termica fornisce una media mobile di 3 minuti della velocità di completamento delle richieste di lettura in base alle dimensioni dell'oggetto. In questo contesto, le richieste di lettura si riferiscono solo alle richieste GET. I colori nella mappa termica indicano la frequenza relativa delle dimensioni di un oggetto all'interno di un singolo grafico. I colori più freddi (ad esempio, viola e blu) indicano tassi relativi inferiori, mentre i colori più caldi (ad esempio, arancione e rosso) indicano tassi relativi più elevati.

4. Posizionare il cursore su un grafico a linee per visualizzare una finestra a comparsa di valori su una parte specifica del grafico.



5. Spostare il cursore su una mappa termica 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.



6. Utilizzare l'elenco a discesa **Policy** in alto a sinistra per selezionare un criterio diverso.

   Vengono visualizzati i grafici relativi al criterio selezionato.

7. In alternativa, accedere ai grafici dal menu **SUPPORT**.
   a. Selezionare **SUPPORT Tools Metrics**.
   b. Nella sezione **Grafana** della pagina, selezionare **Traffic Classification Policy**.
   c. Selezionare il criterio dall'elenco a discesa in alto a sinistra nella pagina.

      Le policy di classificazione del traffico sono identificate dal loro ID. Gli ID policy sono elencati nella pagina Traffic Classification Policies.

8. Analizzare i grafici per determinare la frequenza con cui il criterio limita il traffico e se è necessario modificare il criterio.

Informazioni correlate

Monitorare e risolvere i problemi

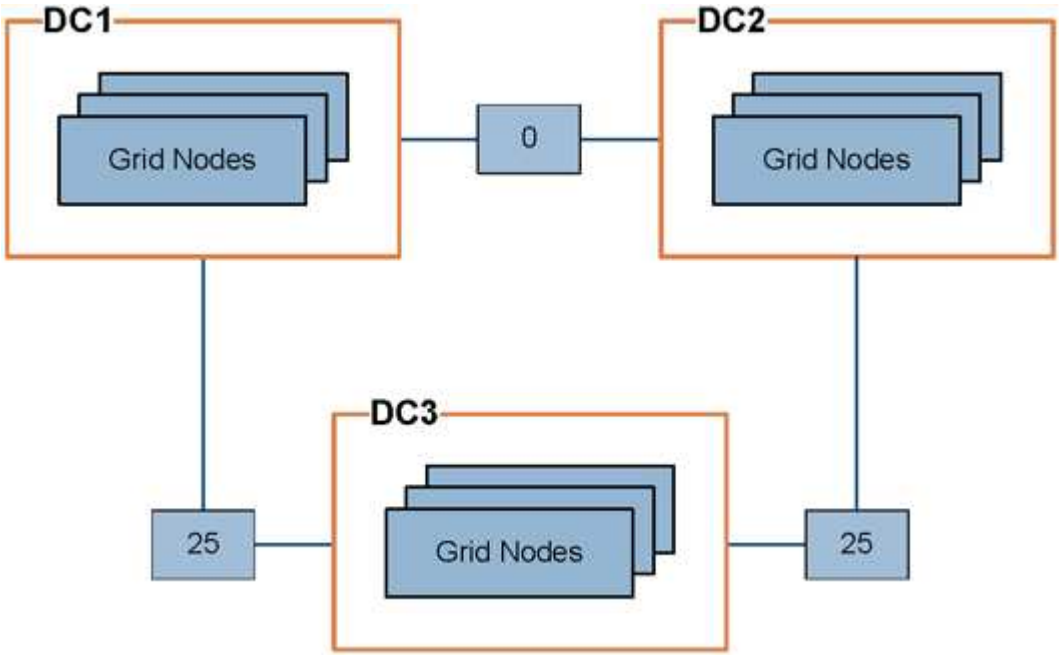
Gestire i costi di collegamento

Quali sono 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.

- 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 di bilanciamento del carico di connessione (CLB) obsoleto sui nodi gateway per indirizzare le connessioni client. Vedere Come funziona il bilanciamento del carico - servizio CLB.

Il diagramma mostra una griglia a tre siti con costi di collegamento configurati tra i siti:



- Il servizio CLB sui nodi gateway distribuisce in modo uguale le connessioni client a tutti i nodi di 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, perché il costo del collegamento da DC1 a D2 è 0, che è inferiore al costo del 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

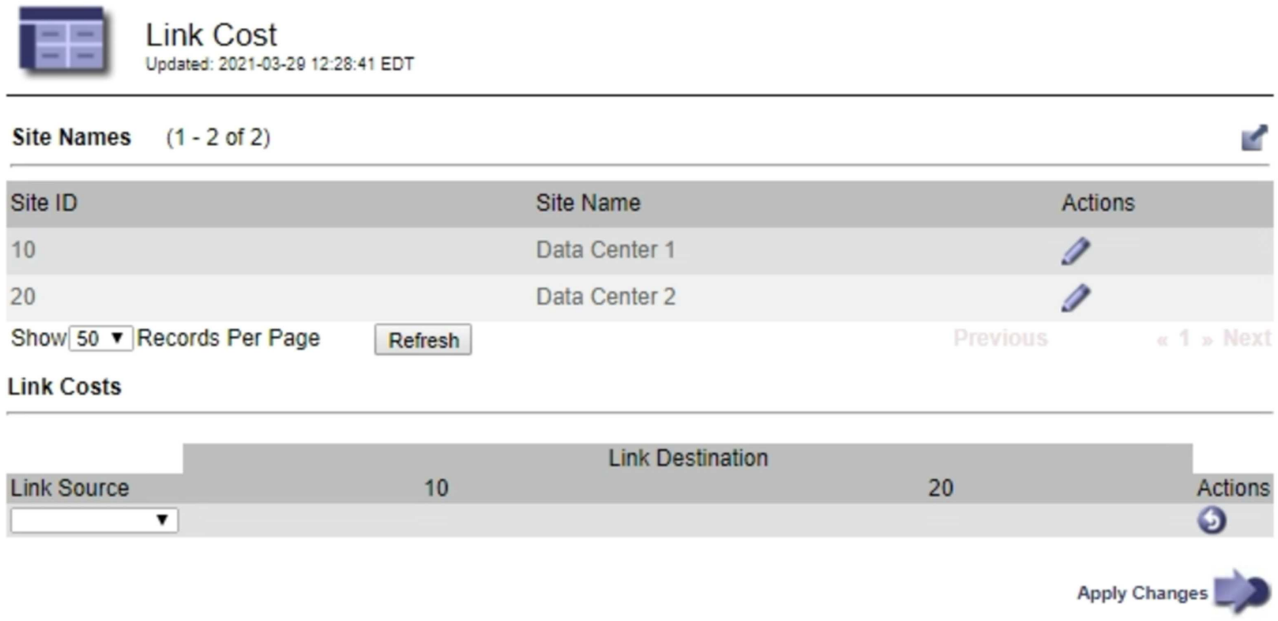
È possibile aggiornare i costi di collegamento tra i siti del data center per riflettere la latenza tra i siti.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Grid Topology Page Configuration (Configurazione pagina topologia griglia).

Fasi

1. Selezionare **CONFIGURAZIONE rete 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 è possibile 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

Che cos'è AutoSupport?

La funzione AutoSupport consente al sistema StorageGRID di inviare messaggi di stato e di stato al supporto tecnico.

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

Informazioni incluse nei messaggi AutoSupport

I messaggi AutoSupport includono informazioni quali:

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

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

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

Cos'è Digital Advisor?

Digital Advisor è basato su cloud e sfrutta gli analytics predittivi e le conoscenze 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.

È necessario attivare AutoSupport se si desidera utilizzare i dashboard e le funzionalità di Digital Advisor sul sito del supporto NetApp.

"Documentazione di Digital Advisor"

Protocolli per l'invio di messaggi AutoSupport

È possibile scegliere uno dei tre protocolli per l'invio dei messaggi AutoSupport:

- HTTPS
- HTTP
- SMTP

Se si inviano messaggi AutoSupport utilizzando HTTPS o HTTP, è possibile configurare un server proxy non trasparente tra i nodi di amministrazione e il supporto tecnico.

Se si utilizza SMTP come protocollo per i messaggi AutoSupport, è necessario configurare un server di posta SMTP.

Opzioni AutoSupport

È possibile utilizzare qualsiasi combinazione delle seguenti opzioni per inviare messaggi AutoSupport al supporto tecnico:

- **Settimanale**: Invia automaticamente i messaggi AutoSupport una volta alla settimana. Impostazione predefinita: Enabled (attivato).
- **Evento attivato**: Invia automaticamente i messaggi 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 messaggi AutoSupport, utile quando si verifica un problema (richiede il protocollo di trasmissione HTTPS AutoSupport). Impostazione predefinita: Disattivata.
- **Attivato dall'utente**: Consente di inviare manualmente i messaggi AutoSupport in qualsiasi momento.

Informazioni correlate

"Supporto NetApp"

Configurare AutoSupport

È possibile attivare la funzione AutoSupport e le singole opzioni AutoSupport quando si installa StorageGRID per la prima volta oppure attivarle in un secondo momento.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root o di altra configurazione della griglia.
- Se si utilizza il protocollo HTTPS o HTTP per l'invio di messaggi AutoSupport, è stato fornito l'accesso a Internet in uscita al nodo di amministrazione primario, direttamente o tramite un server proxy (non sono richieste connessioni in entrata).
- Se si utilizza il protocollo HTTPS o HTTP e si desidera utilizzare un server proxy, è possibile scegliere

Configurato un server proxy Admin.

- Se si utilizza SMTP come protocollo per i messaggi 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).

Specificare il protocollo per i messaggi AutoSupport

Per inviare messaggi AutoSupport è possibile utilizzare uno dei seguenti protocolli:

- **HTTPS**: Impostazione predefinita e consigliata per le nuove installazioni. Il protocollo HTTPS utilizza la porta 443. Se si desidera attivare la funzione AutoSupport on Demand, è necessario utilizzare il protocollo HTTPS.
- **HTTP**: Questo protocollo non è sicuro, a meno che non venga utilizzato in un ambiente attendibile in cui il server proxy converte in HTTPS durante l'invio di dati su Internet. Il protocollo HTTP utilizza la porta 80.
- **SMTP**: Utilizzare questa opzione se si desidera che i messaggi AutoSupport vengano inviati tramite e-mail. Se si utilizza SMTP come protocollo per i messaggi AutoSupport, è necessario configurare un server di posta SMTP nella pagina Configurazione posta elettronica legacy (**SUPPORT Alarms (legacy) Configurazione posta legacy**).

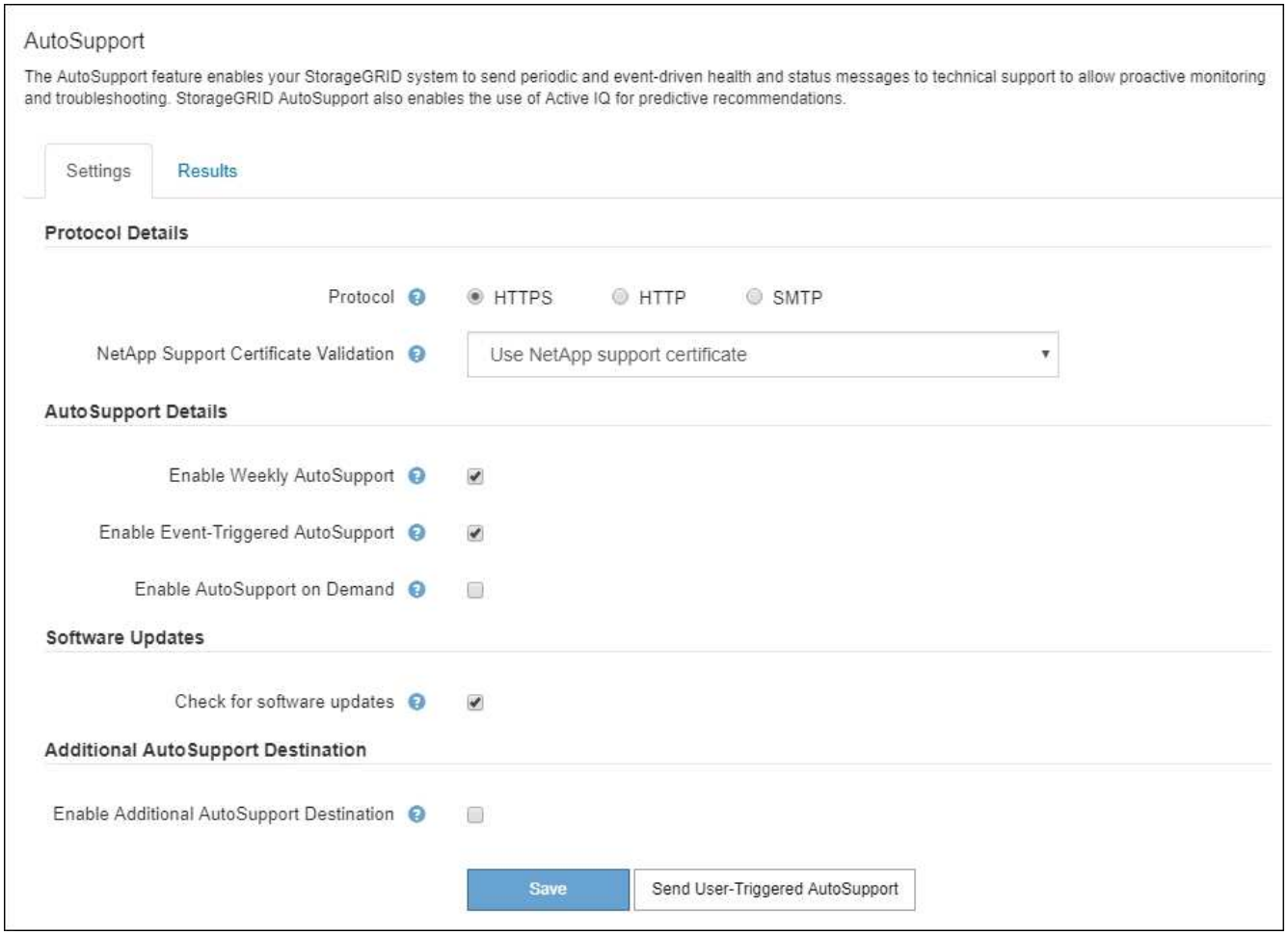
> SMTP era l'unico protocollo disponibile per i messaggi AutoSupport prima della release di StorageGRID 11.2. Se inizialmente è stata installata una versione precedente di StorageGRID, il protocollo selezionato potrebbe essere SMTP.

Il protocollo impostato viene utilizzato per l'invio di tutti i tipi di messaggi AutoSupport.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.

   Viene visualizzata la pagina AutoSupport (Impostazioni) e viene selezionata la scheda **Settings** (Impostazioni).



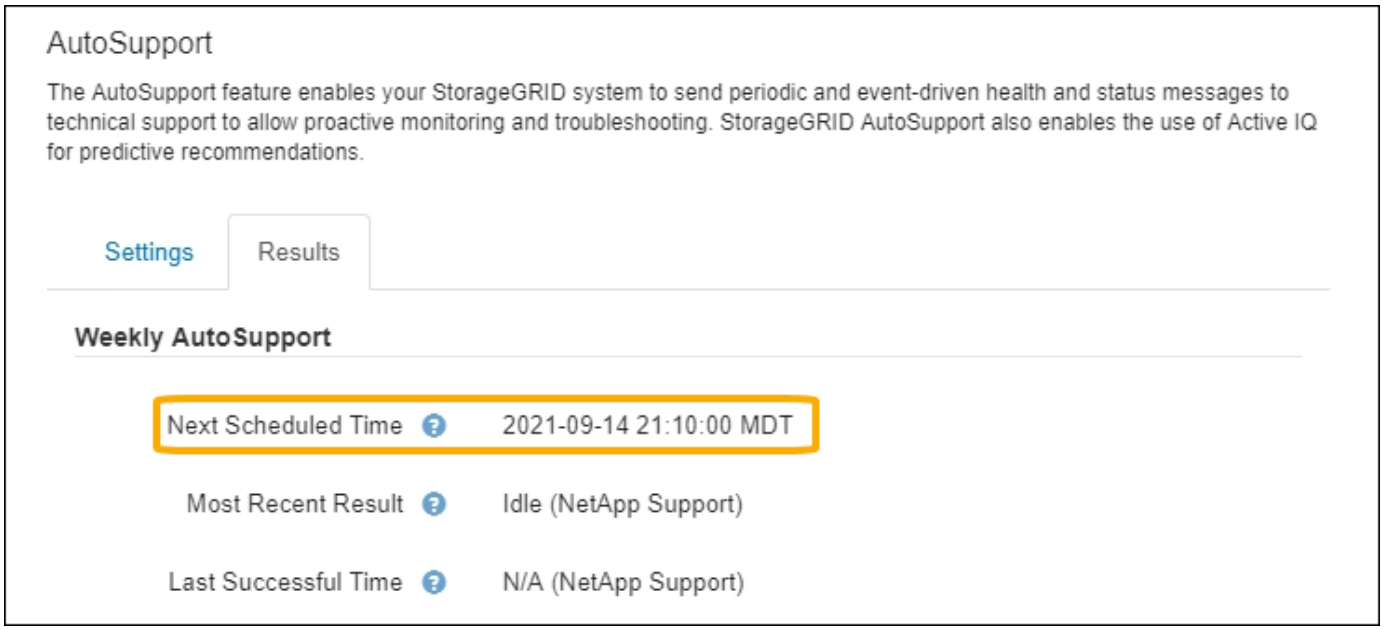
2. Selezionare il protocollo che si desidera utilizzare per inviare messaggi AutoSupport.
3. Se si seleziona **HTTPS**, selezionare se utilizzare un certificato TLS per proteggere la connessione al server di supporto NetApp.
   - **Usa il certificato di supporto NetApp** (impostazione predefinita): La convalida del certificato garantisce la sicurezza della trasmissione dei messaggi AutoSupport. 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 messaggi settimanali, attivati dall'utente e attivati dagli eventi vengono inviati utilizzando il protocollo selezionato.

Disattiva i messaggi AutoSupport settimanali

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un messaggio AutoSupport al supporto NetApp una volta alla settimana.

Per determinare quando verrà inviato il messaggio AutoSupport settimanale, accedere alla scheda **AutoSupport Results**. Nella sezione **Weekly AutoSupport**, esaminare il valore di **Next Scheduled Time** (ora pianificata successiva).



È possibile disattivare l'invio automatico dei messaggi AutoSupport settimanali in qualsiasi momento.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.
2. Deselezionare la casella di controllo **Enable Weekly AutoSupport** (attiva impostazioni settimanali).
3. Selezionare **Salva**.

Disattiva i messaggi AutoSupport attivati dagli eventi

Per impostazione predefinita, il sistema StorageGRID è configurato per inviare un messaggio AutoSupport al supporto NetApp quando si verifica un avviso importante o un altro evento significativo del sistema.

È possibile disattivare i messaggi AutoSupport attivati da eventi in qualsiasi momento.

> I messaggi AutoSupport attivati dagli eventi vengono eliminati anche quando si sopprimono le notifiche e-mail a livello di sistema. (Selezionare **CONFIGURAZIONE sistema Opzioni di visualizzazione**. Quindi, selezionare **Notification Sopprimi tutto**.)

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.
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 l'invio automatico dei messaggi AutoSupport da parte del sistema StorageGRID. Il supporto tecnico può anche impostare l'intervallo di tempo di polling per le query AutoSupport on Demand.

Il supporto tecnico non può attivare o disattivare AutoSupport on Demand.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.
2. Selezionare **HTTPS** per il protocollo.
3. Selezionare la casella di controllo **Enable Weekly AutoSupport** (attiva impostazioni settimanali).
4. Selezionare la casella di controllo **attiva AutoSupport su richiesta**.
5. Selezionare **Salva**.

   AutoSupport on Demand è attivato e il supporto tecnico può inviare richieste AutoSupport on Demand a StorageGRID.

Disattiva i controlli per gli aggiornamenti software

Per impostazione predefinita, StorageGRID contatta NetApp per determinare se sono disponibili aggiornamenti software per il sistema. Se è disponibile una correzione rapida StorageGRID o una nuova versione, la nuova versione viene visualizzata nella pagina aggiornamento StorageGRID.

Se necessario, è possibile disattivare la verifica degli aggiornamenti software. Ad esempio, se il sistema non dispone di accesso WAN, disattivare il controllo per evitare errori di download.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.
2. Deselezionare la casella di controllo **Controlla aggiornamenti software**.
3. Selezionare **Salva**.

Aggiungere una destinazione AutoSupport aggiuntiva

Quando si attiva AutoSupport, vengono inviati messaggi di stato e di salute al supporto NetApp. È possibile specificare una destinazione aggiuntiva per tutti i messaggi AutoSupport.

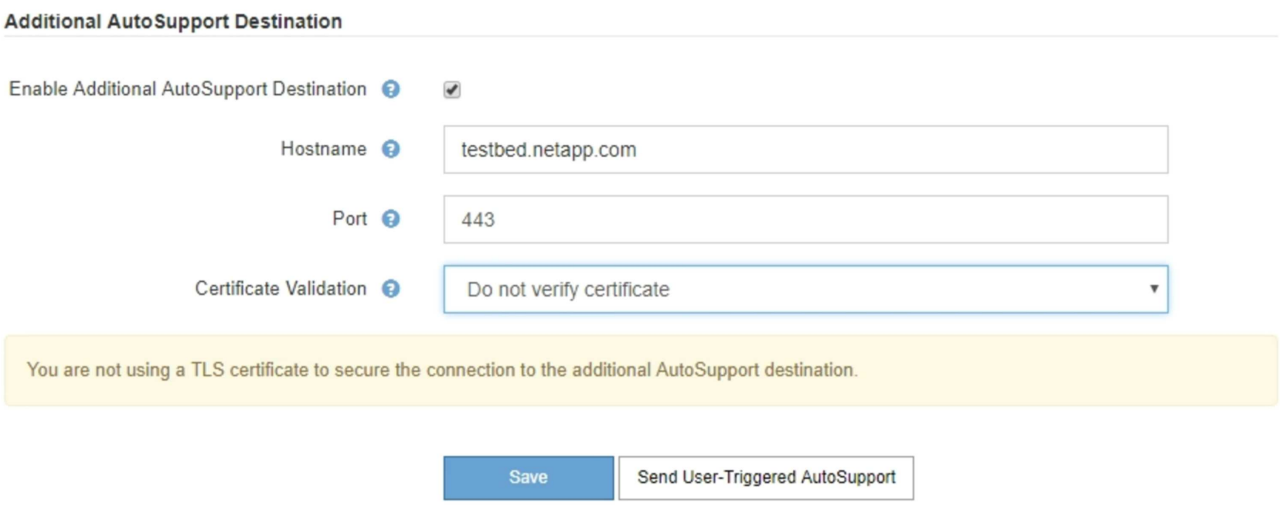
Per verificare o modificare il protocollo utilizzato per inviare messaggi AutoSupport, consultare le istruzioni a. Specificare il protocollo per i messaggi AutoSupport.

> Non è possibile utilizzare il protocollo SMTP per inviare messaggi AutoSupport a una destinazione aggiuntiva.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.
2. Selezionare **Abilita destinazione AutoSupport aggiuntiva**.

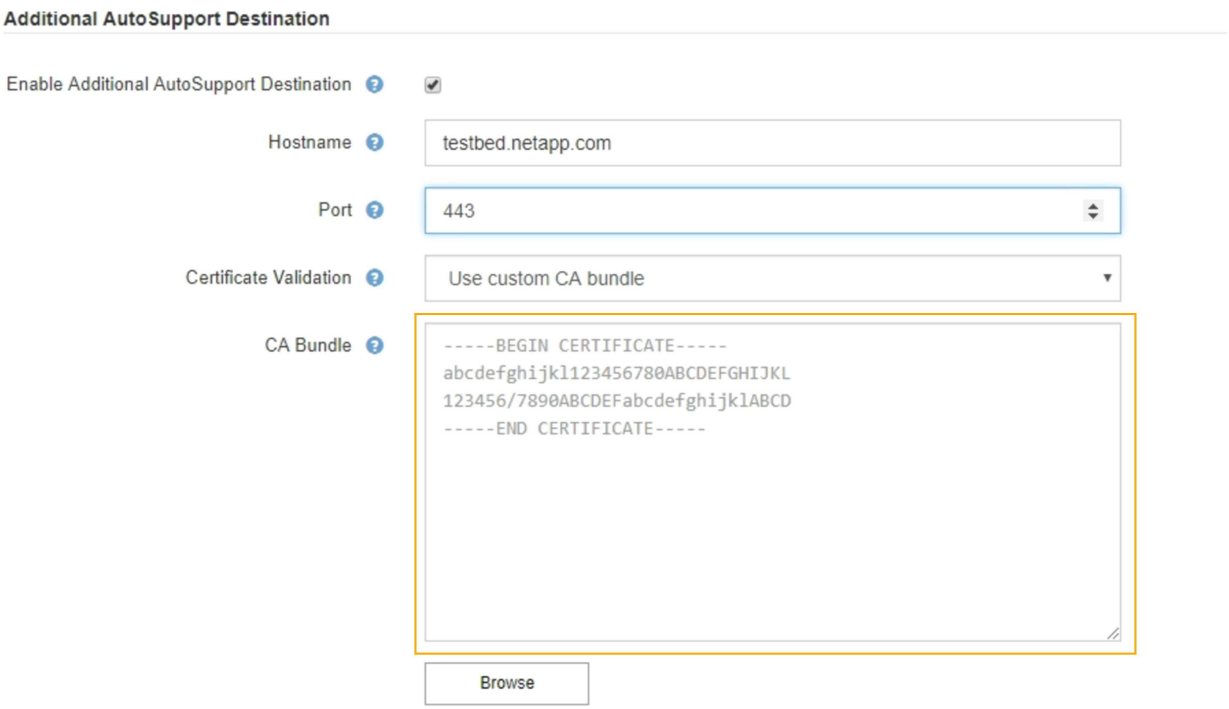
   Vengono visualizzati i campi destinazione AutoSupport aggiuntiva.



3. Immettere il nome host del server o l'indirizzo IP di un server di destinazione AutoSupport aggiuntivo.

   È possibile inserire solo una destinazione aggiuntiva.

4. Inserire la porta utilizzata per la connessione a un server di destinazione AutoSupport aggiuntivo (l'impostazione predefinita è la porta 80 per HTTP o la porta 443 per HTTPS).
5. Per inviare i messaggi AutoSupport con la convalida del certificato, selezionare **Usa bundle CA personalizzato** nell'elenco a discesa **convalida certificato**. Quindi, eseguire una delle seguenti operazioni:
   - Utilizzare uno strumento di modifica per copiare e incollare tutto il contenuto di ciascun file di certificato CA con codifica PEM nel campo **bundle CA**, concatenato in ordine di catena del certificato. È necessario includere `----BEGIN CERTIFICATE----` e. `----END CERTIFICATE----` nella selezione.



   - Selezionare **Sfoglia**, individuare il file contenente i certificati, quindi selezionare **Apri** per caricare il file. La convalida del certificato garantisce la sicurezza della trasmissione dei messaggi AutoSupport.

6. Per inviare i messaggi AutoSupport senza convalida del certificato, selezionare **non verificare il certificato** nell'elenco a discesa **convalida 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.

   Viene visualizzato un messaggio di attenzione: "Non si sta utilizzando un certificato TLS per proteggere la connessione alla destinazione AutoSupport aggiuntiva."

7. Selezionare **Salva**.

   Tutti i messaggi AutoSupport futuri, generati da eventi e attivati dall'utente, verranno inviati alla destinazione aggiuntiva.

Attivare manualmente un messaggio AutoSupport

Per assistere il supporto tecnico nella risoluzione dei problemi relativi al sistema StorageGRID, è possibile attivare manualmente l'invio di un messaggio AutoSupport.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione di accesso root o di altra configurazione della griglia.

Fasi

1. Selezionare **SUPPORTO Strumenti AutoSupport**.

   Viene visualizzata la pagina AutoSupport (Impostazioni) con la scheda **Settings** (Impostazioni) selezionata.

2. Selezionare **Invia AutoSupport attivato dall'utente**.

   StorageGRID tenta di inviare un messaggio AutoSupport al supporto tecnico. Se il tentativo ha esito positivo, i valori **risultato più recente** e **tempo ultimo successo** nella scheda **risultati** vengono aggiornati. In caso di problemi, il valore **risultato più recente** viene aggiornato a "non riuscito" e StorageGRID non tenta di inviare nuovamente il messaggio AutoSupport.

   > Dopo aver inviato un messaggio AutoSupport attivato dall'utente, aggiornare la pagina AutoSupport del browser dopo 1 minuto per accedere ai risultati più recenti.

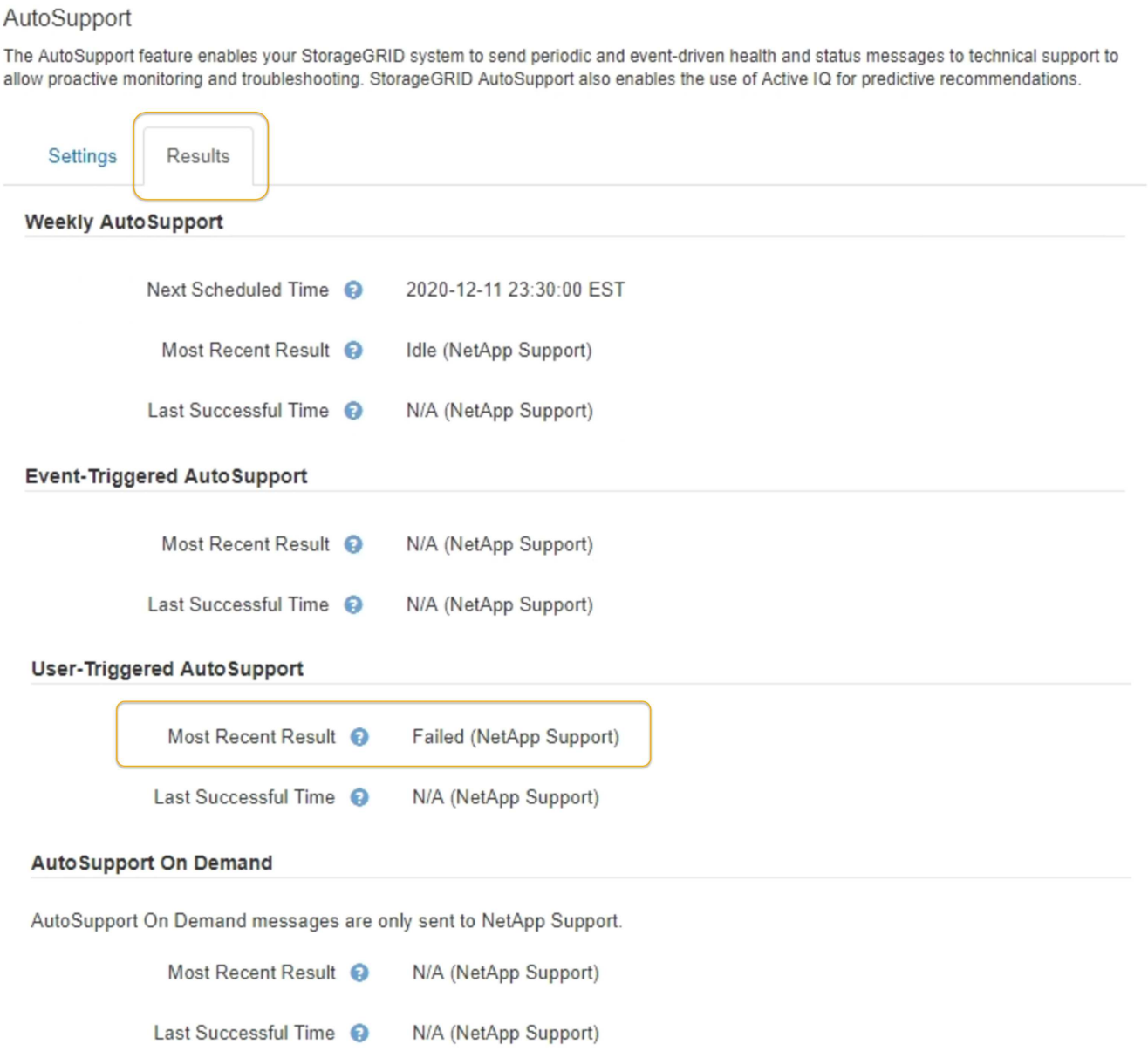
Risolvere i problemi relativi ai messaggi AutoSupport

Se un tentativo di inviare un messaggio AutoSupport non riesce, il sistema StorageGRID esegue diverse azioni a seconda del tipo di messaggio AutoSupport. Puoi controllare lo stato dei messaggi AutoSupport selezionando **SUPPORT Tools AutoSupport Results**.

> I messaggi AutoSupport attivati dagli eventi vengono soppressi quando si sopprimono le notifiche e-mail a livello di sistema. (Selezionare **CONFIGURAZIONE sistema Opzioni di visualizzazione**. Quindi, selezionare **Notification Sopprimi tutto**.)

Quando il messaggio AutoSupport non viene inviato, nella scheda **Results** della pagina **AutoSupport** viene

visualizzato “Failed”.



Errore settimanale del messaggio AutoSupport

Se un messaggio 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 messaggio 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 messaggio AutoSupport all’ora successiva pianificata.
5. Mantiene la normale pianificazione AutoSupport se il messaggio non riesce perché il servizio NMS non è disponibile e se un messaggio viene inviato prima del termine di sette giorni.
6. Quando il servizio NMS è nuovamente disponibile, invia immediatamente un messaggio AutoSupport se non viene inviato alcun messaggio per almeno sette giorni.

Errore messaggio AutoSupport attivato dall'utente o attivato da evento

Se un messaggio AutoSupport attivato dall'utente o attivato da un evento non viene inviato, 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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`
2. Non tenta di inviare nuovamente il messaggio.
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 (**SUPPORTO Allarmi (legacy)** * Configurazione e-mail legacy*). Nella pagina AutoSupport potrebbe essere visualizzato il seguente messaggio di errore: `AutoSupport messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Informazioni su come configurare le impostazioni del server di posta elettronica in istruzioni per il monitoraggio e la risoluzione dei problemi.

Correggere un errore di messaggio 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 messages cannot be sent using SMTP protocol due to incorrect settings on the E-mail Server page.`

Invia messaggi AutoSupport e-Series tramite StorageGRID

È possibile inviare messaggi AutoSupport di Gestione di sistema di e-Series SANtricity al supporto tecnico tramite un nodo di amministrazione StorageGRID anziché la porta di gestione dell'appliance di storage.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone dell'autorizzazione Storage Appliance Administrator o Root Access.

> È necessario disporre del firmware SANtricity 8.70 (11.7) o superiore per accedere a Gestore di sistema SANtricity utilizzando Gestione griglia.

A proposito di questa attività

I messaggi AutoSupport di e-Series contengono informazioni dettagliate sull'hardware di storage e sono più specifici degli altri messaggi AutoSupport inviati dal sistema StorageGRID.

Configurare uno speciale indirizzo del server proxy in Gestore di sistema di SANtricity per fare in modo che i messaggi AutoSupport vengano trasmessi attraverso un nodo di amministrazione di StorageGRID senza utilizzare la porta di gestione dell'appliance. I messaggi AutoSupport trasmessi in questo modo rispettano le impostazioni del proxy di amministrazione e mittente preferite che potrebbero essere state configurate in Gestione griglia.

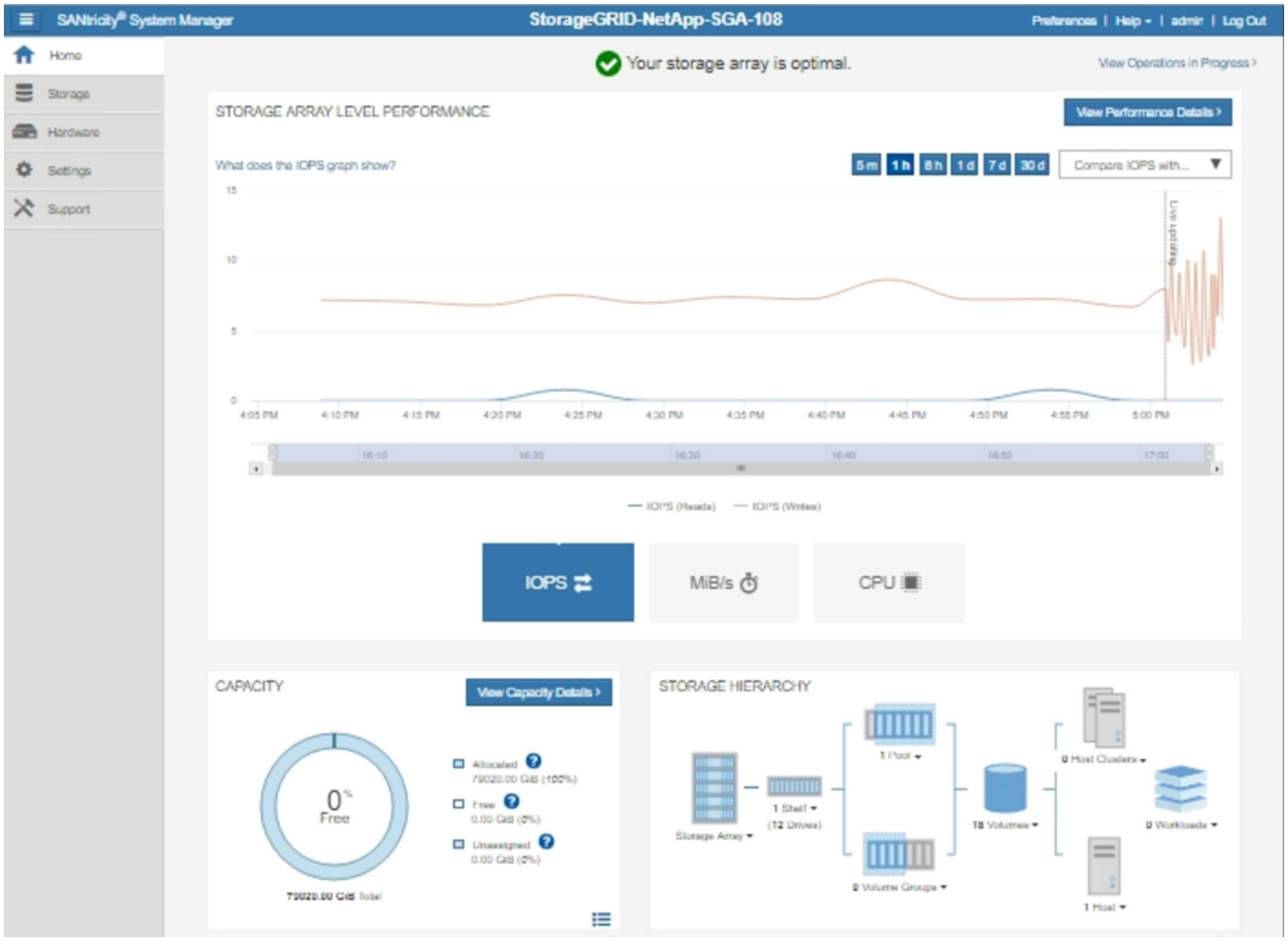
Se si desidera configurare il server proxy Admin in Grid Manager, vedere Configurare le impostazioni del proxy amministratore.

> Questa procedura è valida solo per la configurazione di un server proxy StorageGRID per i messaggi AutoSupport e-Series. Per ulteriori informazioni sulla configurazione di e-Series AutoSupport, consultare "Documentazione NetApp e-Series e SANtricity".

Fasi

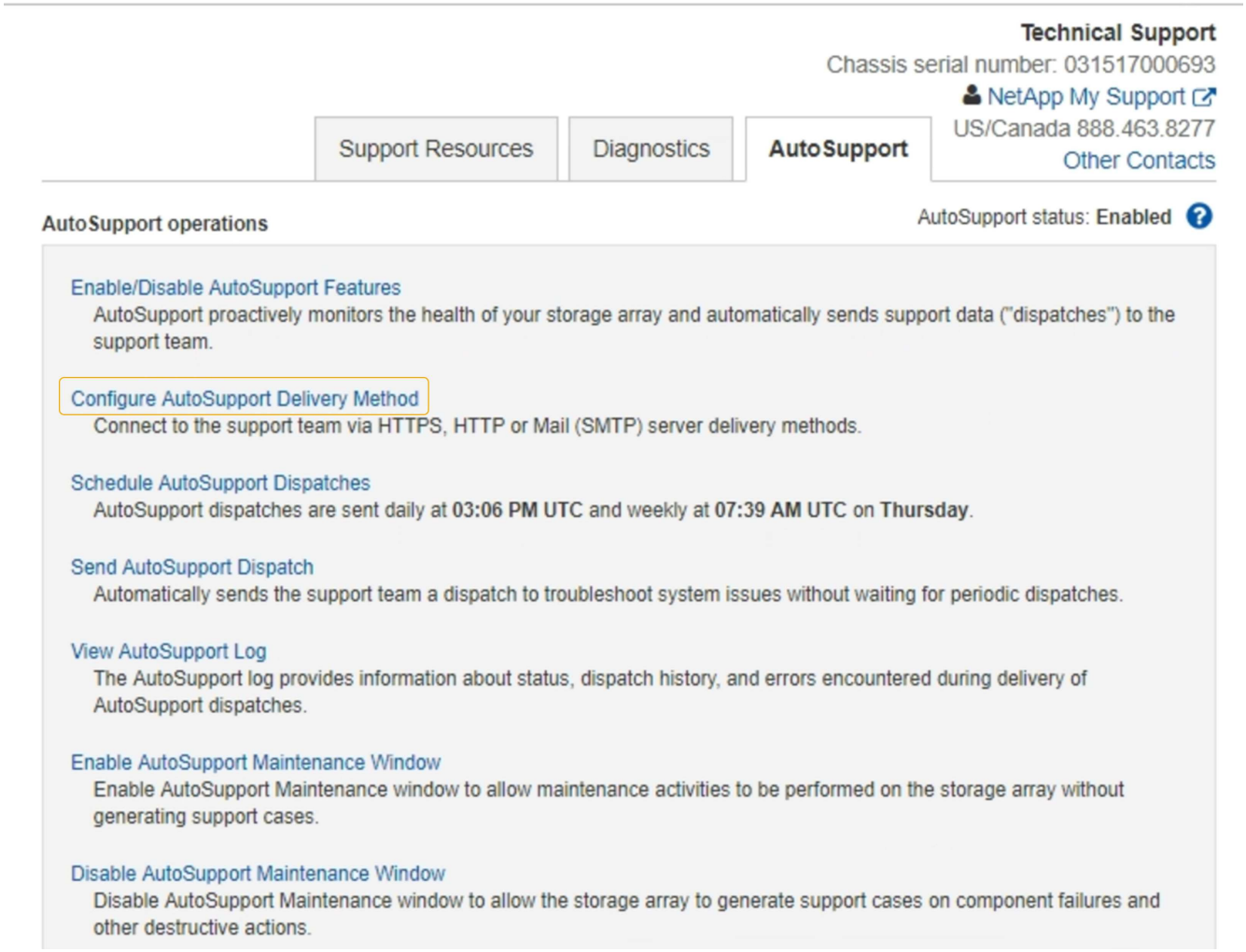
1. In Grid Manager, selezionare **NODES**.
2. Dall'elenco dei nodi a sinistra, selezionare il nodo dell'appliance di storage che si desidera configurare.
3. Selezionare **Gestore di sistema SANtricity**.

   Viene visualizzata la home page di Gestore di sistema di SANtricity.



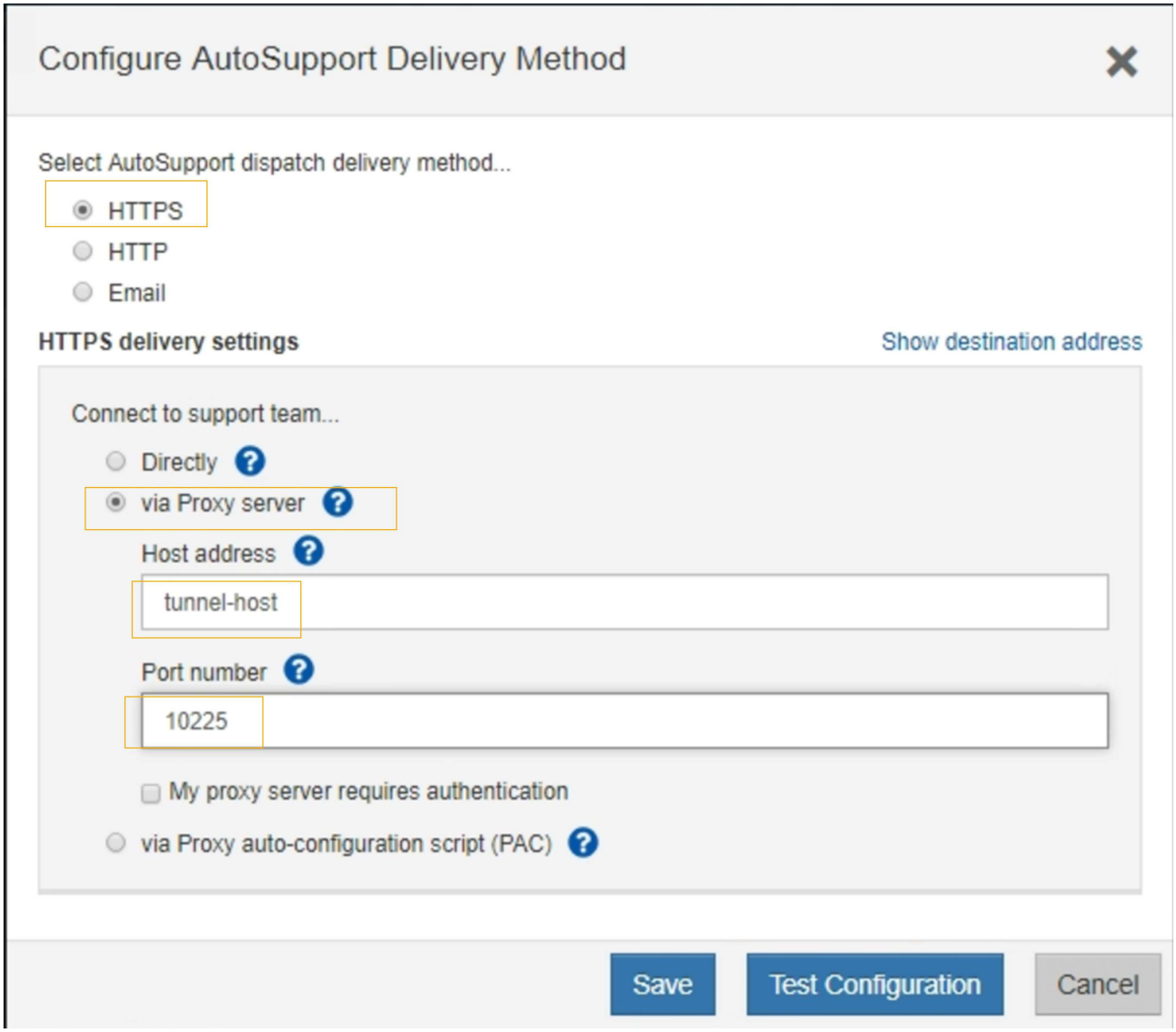
4. Selezionare **SUPPORT Support Center AutoSupport**.

   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 il protocollo HTTPS è preinstallato.

7. Selezionare **via Proxy server**.
8. Invio `tunnel-host` Per l'indirizzo **host**.

   `tunnel-host` È l'indirizzo speciale per l'utilizzo di un nodo amministrativo per l'invio di messaggi AutoSupport e-Series.

9. Invio `10225` Per il numero di porta *.

   `10225` È il numero di porta sul server proxy StorageGRID che riceve i messaggi AutoSupport dal controller e-Series nell'appliance.

10. Selezionare **verifica configurazione** per verificare l'instradamento e la configurazione del server proxy AutoSupport.

    Se la risposta è corretta, 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, assicurarsi che il nodo di amministrazione mittente preferito possa connettersi al sito di supporto NetApp e riprovare il test.

11. Selezionare **Salva**.

La configurazione viene salvata e viene visualizzato un messaggio di conferma: “AutoSupport delivery method has been configured”.

Gestire i nodi di storage

Informazioni sulla gestione dei nodi di storage

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

Che cos’è un nodo di storage?

I nodi di storage gestiscono e memorizzano i dati e i metadati degli oggetti. Ogni sistema StorageGRID deve avere almeno tre nodi di storage. Se si dispone di più siti, ogni sito all’interno del sistema StorageGRID deve avere anche tre nodi di storage.

Un nodo di storage include i servizi e i processi necessari per memorizzare, spostare, verificare e recuperare i dati degli oggetti e i metadati sul disco. È possibile visualizzare informazioni dettagliate sui nodi di storage nella pagina **NODI**.

Che cos’è il servizio ADC?

Il servizio ADC (Administrative Domain Controller) autentica i nodi della griglia e le relative connessioni tra loro. Il servizio ADC è ospitato su ciascuno dei primi tre nodi di storage di un sito.

Il servizio ADC mantiene le informazioni sulla topologia, inclusa la posizione e la disponibilità dei servizi. Quando un nodo della griglia richiede informazioni da un altro nodo della griglia o un’azione da eseguire da un altro nodo della griglia, contatta un servizio ADC per trovare il nodo della griglia migliore per elaborare la sua richiesta. Inoltre, il servizio ADC conserva una copia dei bundle di configurazione dell’implementazione StorageGRID, consentendo a qualsiasi nodo grid di recuperare le informazioni di configurazione correnti. È possibile visualizzare le informazioni ADC per un nodo di storage nella pagina topologia griglia (**SUPPORTO topologia griglia**).

Per facilitare le operazioni distribuite e islanded, ciascun servizio ADC sincronizza certificati, bundle di

configurazione e informazioni sui servizi e sulla topologia con gli altri servizi ADC nel sistema StorageGRID.

In generale, tutti i nodi di rete mantengono una connessione ad almeno un servizio ADC. In questo modo, i nodi della griglia accedono sempre alle informazioni più recenti. Quando i nodi di rete si connettono, memorizzano nella cache i certificati` degli altri nodi di rete, consentendo ai sistemi di continuare a funzionare con nodi di rete noti anche quando un servizio ADC non è disponibile. I nuovi nodi di rete possono stabilire connessioni solo utilizzando un servizio ADC.

La connessione di ciascun nodo di rete consente al servizio ADC di raccogliere informazioni sulla topologia. Queste informazioni sul nodo della griglia includono il carico della CPU, lo spazio su disco disponibile (se dotato di storage), i servizi supportati e l'ID del sito del nodo della griglia. Altri servizi richiedono al servizio ADC informazioni sulla topologia tramite query sulla topologia. Il servizio ADC risponde a ogni richiesta con le informazioni più recenti ricevute dal sistema StorageGRID.

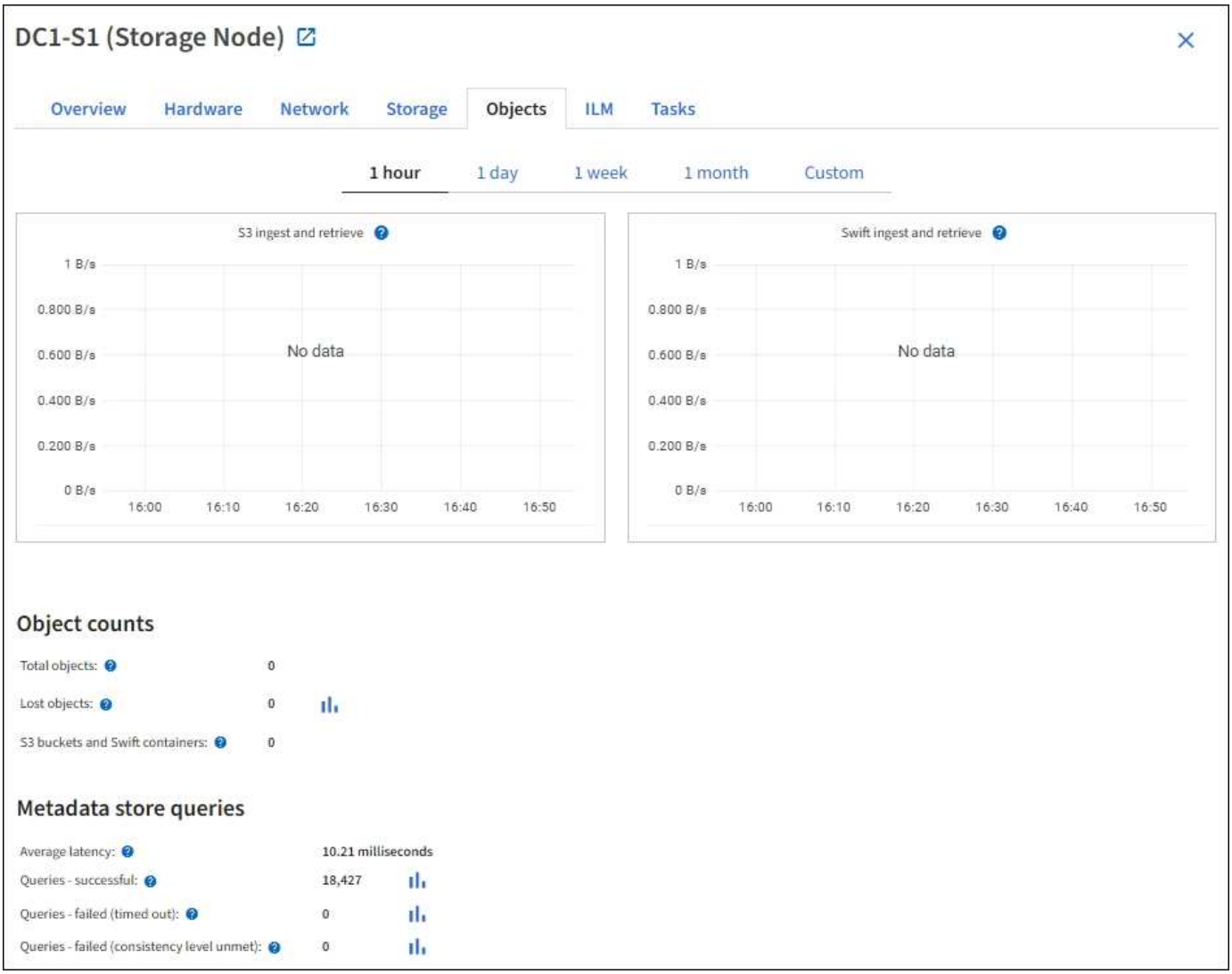
Che cos'è il servizio DDS?

Ospitato da un nodo di storage, il servizio DDS (Distributed Data Store) si interfaccia con il database Cassandra per eseguire attività in background sui metadati degli oggetti memorizzati nel sistema StorageGRID.

Numero di oggetti

Il servizio DDS tiene traccia del numero totale di oggetti acquisiti nel sistema StorageGRID e del numero totale di oggetti acquisiti attraverso ciascuna delle interfacce supportate dal sistema (S3 o Swift).

È possibile visualizzare il numero totale di oggetti nella scheda oggetti della pagina nodi per qualsiasi nodo di storage.



Query

È possibile identificare il tempo medio necessario per eseguire una query sull'archivio di metadati tramite il servizio DDS specifico, il numero totale di query riuscite e il numero totale di query non riuscite a causa di un problema di timeout.

È possibile rivedere le informazioni sulle query per monitorare lo stato dell'archivio di metadati, Cassandra, che influisce sulle prestazioni di acquisizione e recupero del sistema. Ad esempio, se la latenza di una query media è lenta e il numero di query non riuscite a causa dei timeout è elevato, l'archivio di metadati potrebbe riscontrare un carico maggiore o eseguire un'altra operazione.

È inoltre possibile visualizzare il numero totale di query non riuscite a causa di errori di coerenza. Gli errori del livello di coerenza derivano da un numero insufficiente di archivi di metadati disponibili nel momento in cui viene eseguita una query attraverso il servizio DDS specifico.

È possibile utilizzare la pagina Diagnostics (Diagnostica) per ottenere ulteriori informazioni sullo stato corrente della griglia. Vedere Eseguire la diagnostica.

Garanzie e controlli di coerenza

StorageGRID garantisce la coerenza di lettura dopo scrittura per gli oggetti appena creati. Qualsiasi operazione GET successiva a un'operazione PUT completata con successo sarà in grado di leggere i dati

appena scritti. Le sovrascritture degli oggetti esistenti, gli aggiornamenti dei metadati e le eliminazioni rimangono alla fine coerenti.

Che cos'è il servizio LDR?

Ospitato da ciascun nodo di storage, il servizio router di distribuzione locale (LDR) gestisce il trasporto dei contenuti per il sistema StorageGRID. Il trasporto dei contenuti comprende molte attività, tra cui storage dei dati, routing e gestione delle richieste. Il servizio LDR esegue la maggior parte del lavoro del sistema StorageGRID gestendo i carichi di trasferimento dei dati e le funzioni di traffico dei dati.

Il servizio LDR gestisce le seguenti attività:

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

Il servizio LDR gestisce inoltre la mappatura degli oggetti S3 e Swift sugli univoci "content handle" (UUID) assegnati dal sistema StorageGRID a ciascun oggetto acquisito.

Query

Le query LDR includono query per la posizione degli oggetti durante le operazioni di recupero e archiviazione. È possibile identificare il tempo medio necessario per eseguire una query, il numero totale di query riuscite e il numero totale di query non riuscite a causa di un problema di timeout.

È possibile rivedere le informazioni sulle query per monitorare lo stato dell'archivio di metadati, che influisce sulle prestazioni di acquisizione e recupero del sistema. Ad esempio, se la latenza di una query media è lenta e il numero di query non riuscite a causa dei timeout è elevato, l'archivio di metadati potrebbe riscontrare un carico maggiore o eseguire un'altra operazione.

È inoltre possibile visualizzare il numero totale di query non riuscite a causa di errori di coerenza. Gli errori del livello di coerenza derivano da un numero insufficiente di archivi di metadati disponibili nel momento in cui viene eseguita una query attraverso il servizio LDR specifico.

È possibile utilizzare la pagina Diagnostics (Diagnostica) per ottenere ulteriori informazioni sullo stato corrente della griglia. Vedere Eseguire la diagnostica.

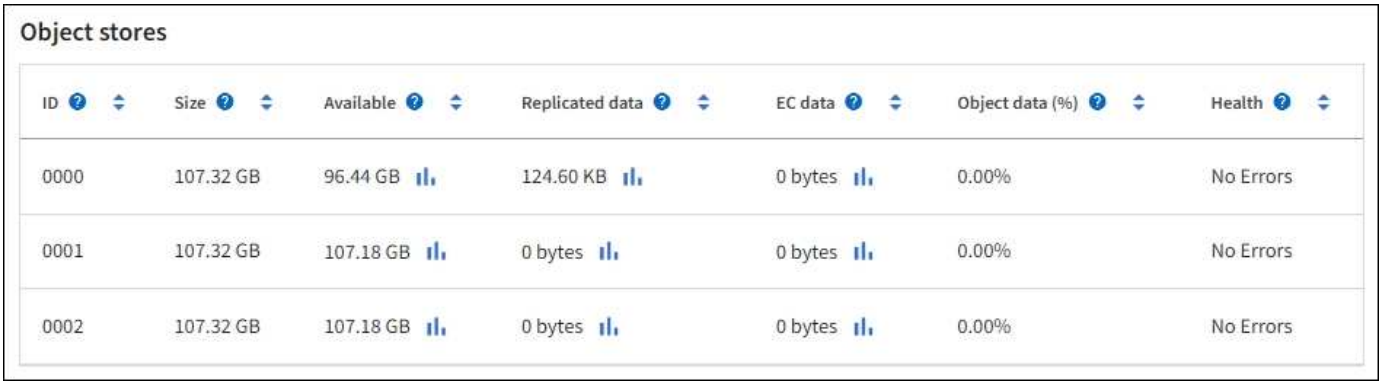
Attività ILM

Le metriche ILM (Information Lifecycle Management) consentono di monitorare la velocità di valutazione degli oggetti per l'implementazione ILM. È possibile visualizzare queste metriche nella dashboard o in **NODES** ***Storage Node*** **ILM**.

Archivi di oggetti

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

È possibile visualizzare gli archivi di oggetti per un nodo di storage nella scheda Storage della pagina Nodes.



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

Per garantire un utilizzo uniforme dello spazio per le copie replicate, i dati degli oggetti per un determinato oggetto vengono memorizzati in un archivio di oggetti in base allo spazio di storage disponibile. Quando uno o più archivi di oggetti riempiono la capacità, gli archivi di oggetti rimanenti continuano a memorizzare gli oggetti fino a quando non c'è più spazio nel nodo di storage.

Protezione dei metadati

I metadati degli oggetti sono informazioni correlate o una descrizione di un oggetto, ad esempio il tempo di modifica dell'oggetto o la posizione di storage. StorageGRID memorizza i metadati degli oggetti in un database Cassandra, che si interfaccia con il servizio LDR.

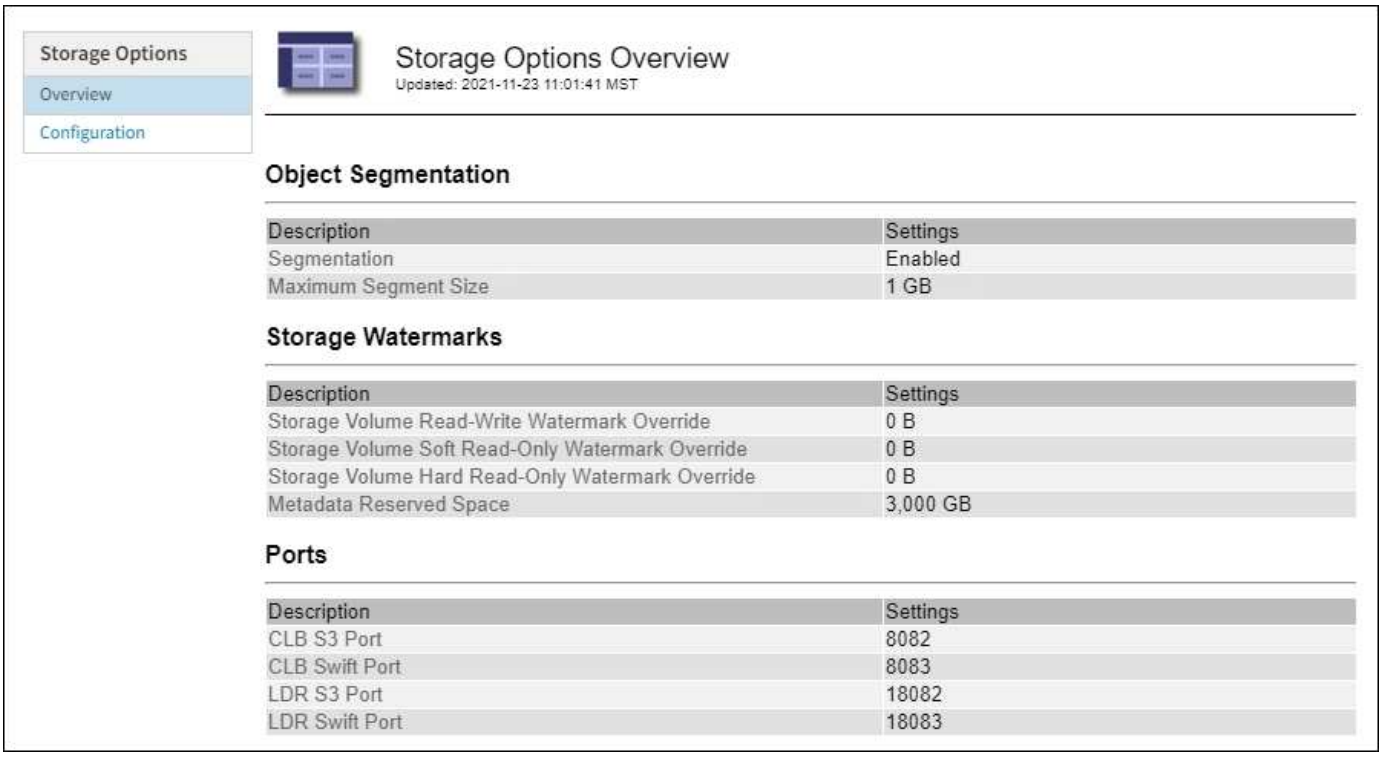
Per garantire la ridondanza e quindi la protezione contro la perdita, vengono conservate tre copie dei metadati degli oggetti in ogni sito. Le copie vengono distribuite in modo uniforme in tutti i nodi di storage di ogni sito. Questa replica non è configurabile ed è eseguita automaticamente.

Gestire lo storage dei metadati degli oggetti

Gestire le opzioni di storage

Le opzioni di storage includono le impostazioni di segmentazione degli oggetti, i valori correnti per le filigrane dei volumi di storage e l'impostazione spazio riservato metadati. È inoltre possibile visualizzare le porte S3 e Swift utilizzate dal servizio CLB obsoleto sui nodi gateway e dal servizio LDR sui nodi storage.

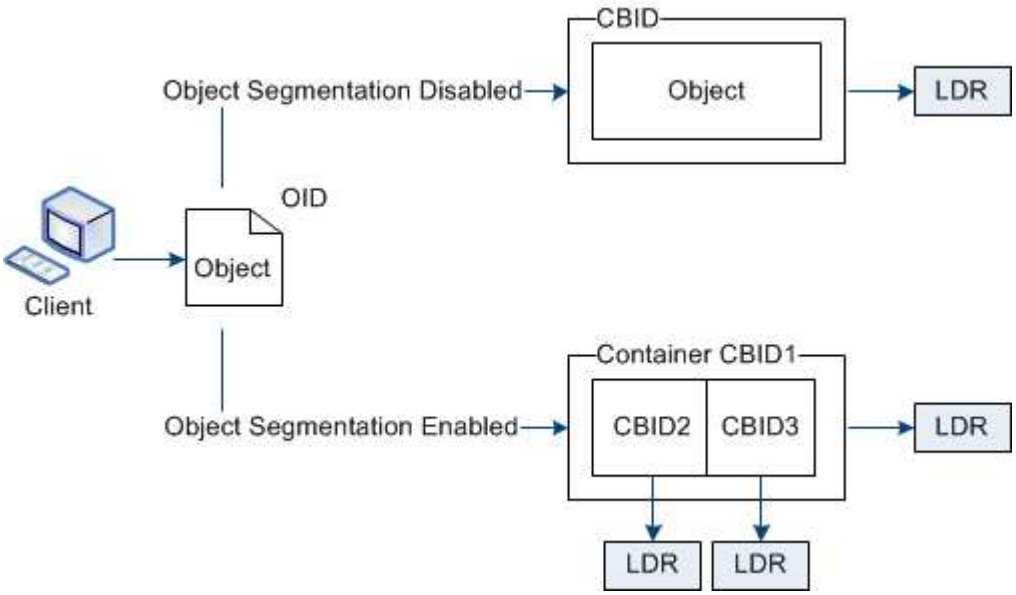
Per informazioni sulle assegnazioni delle porte, vedere Riepilogo: Indirizzi IP e porte per le connessioni client.



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 nello 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:

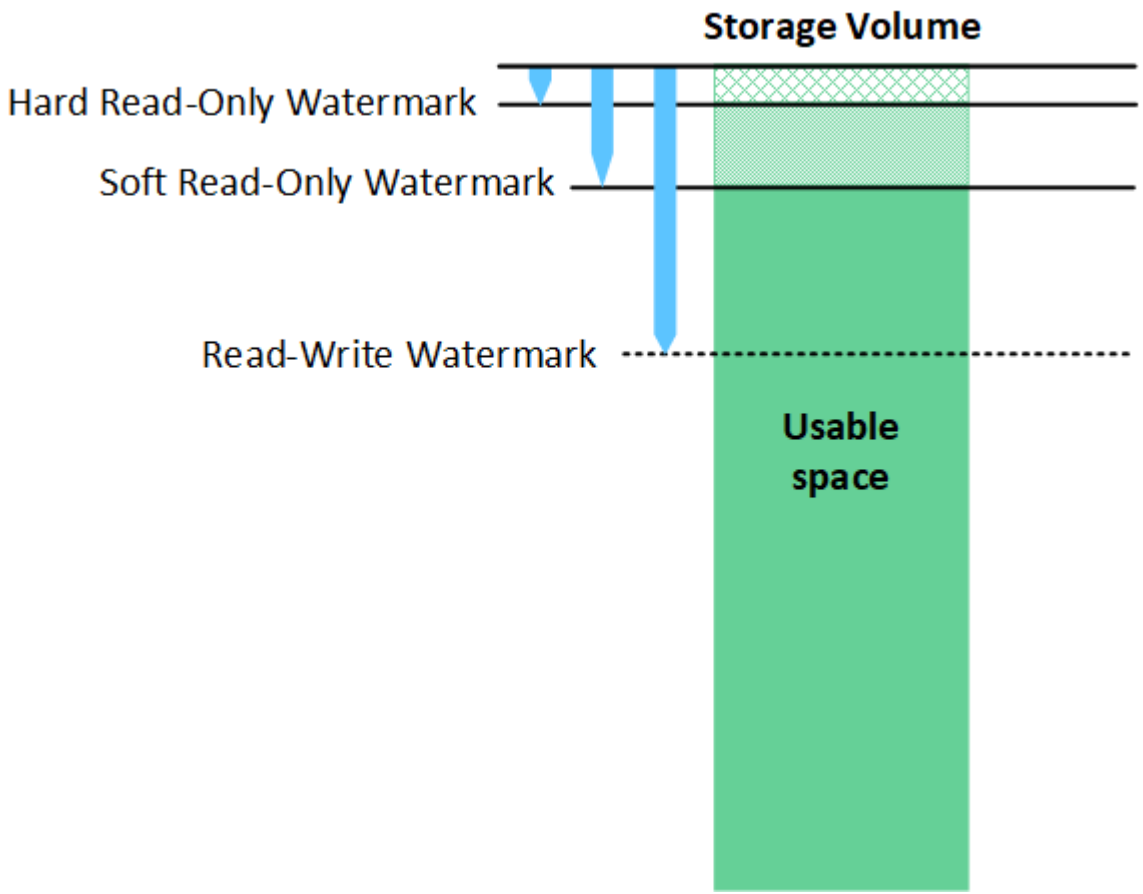
container di segmenti + segmento 1 + segmento 2 = tre oggetti memorizzati

È possibile migliorare le prestazioni durante la gestione di oggetti di grandi dimensioni garantendo che:

- Ciascun gateway e nodo di storage dispone di una larghezza di banda di rete sufficiente per il throughput richiesto. Ad esempio, configurare reti client e Grid separate su interfacce Ethernet a 10 Gbps.
- Vengono implementati un numero sufficiente di gateway e nodi storage per il throughput richiesto.
- Ogni nodo di storage dispone di prestazioni i/o su disco sufficienti per il throughput richiesto.

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 WebGestire 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.

Di cosa hai bisogno

- L'aggiornamento a StorageGRID 11.6 è stato completato.
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.

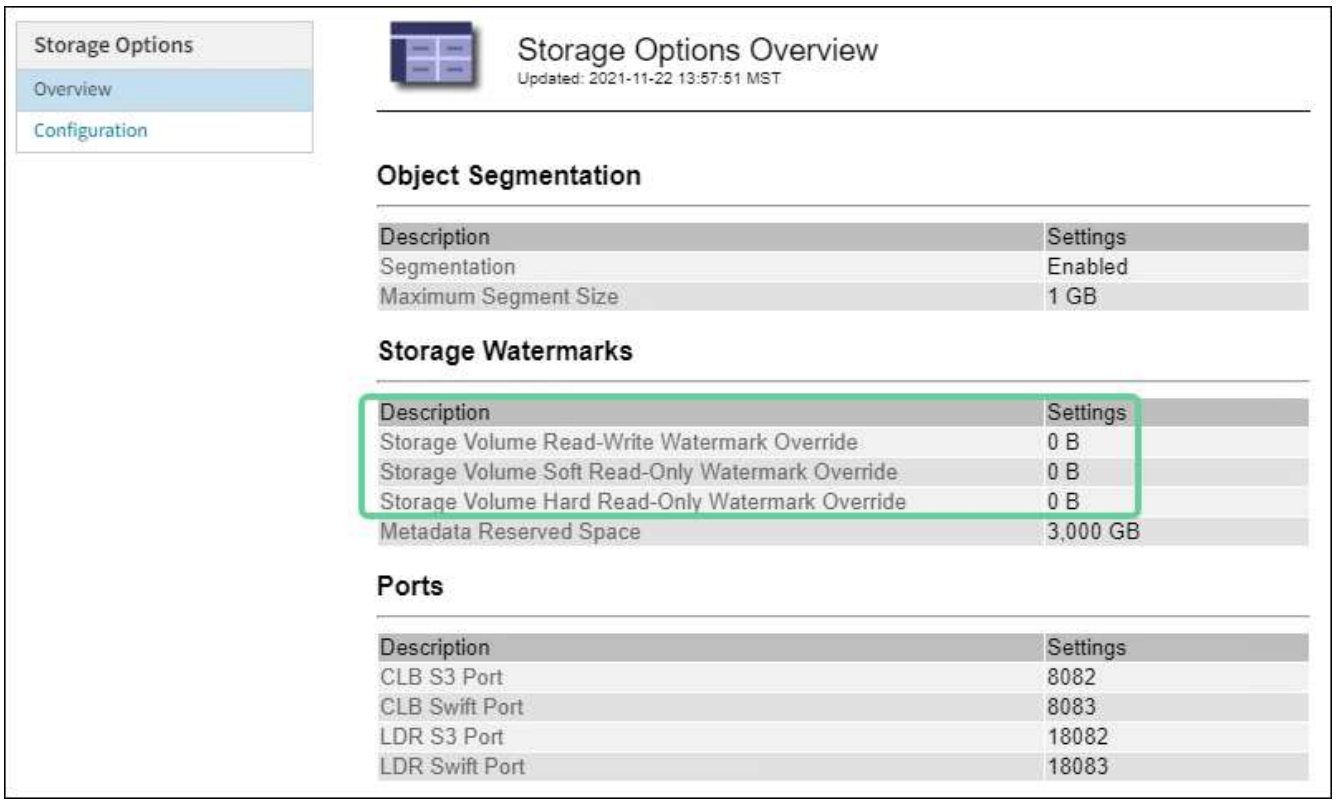
- Si dispone dell'autorizzazione di accesso root.

Consente di visualizzare le impostazioni correnti del watermark

È possibile visualizzare le impostazioni correnti del filigrana dello storage in Grid Manager.

Fasi

1. Selezionare **CONFIGURATION** > **System** > **Storage options**.
2. Nella sezione Storage Watermarks (Filigrane di archiviazione), esaminare le impostazioni per i tre override del watermark del volume di archiviazione.



   - Se le sostituzioni del watermark sono **0**, tutte e tre le filigrane sono ottimizzate per ogni volume di storage su ogni nodo di storage, in base alle dimensioni del nodo di storage e alla capacità relativa del volume.

     Questa è l'impostazione predefinita e consigliata. Non aggiornare questi valori. Se necessario, è possibile scegliere Visualizza filigrane di storage ottimizzate.

   - Se le sostituzioni del watermark non sono valori 0, 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.

Visualizza filigrane di storage 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:

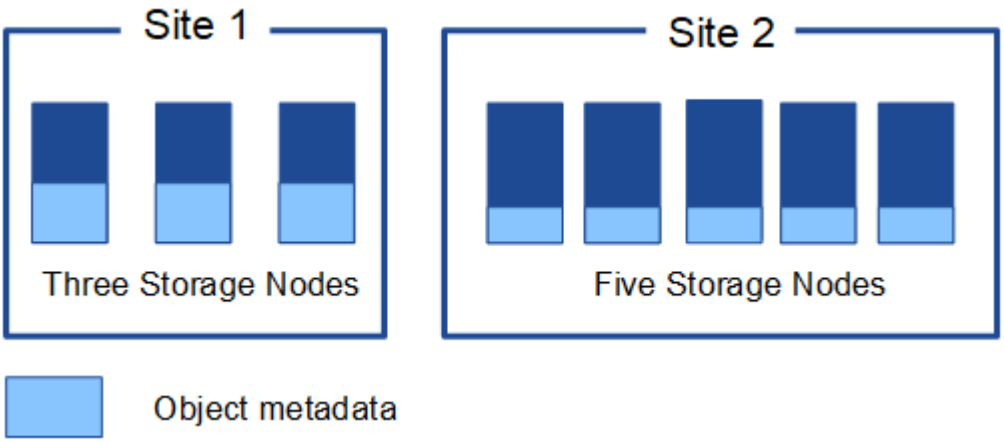
- Metadati di sistema, tra cui un ID univoco per ciascun oggetto (UUID), il nome dell'oggetto, il nome del bucket S3 o del container Swift, il nome o l'ID dell'account tenant, la dimensione logica dell'oggetto, la data e l'ora in cui l'oggetto è stato creato per la prima volta, e la data e l'ora dell'ultima 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. Le tre copie

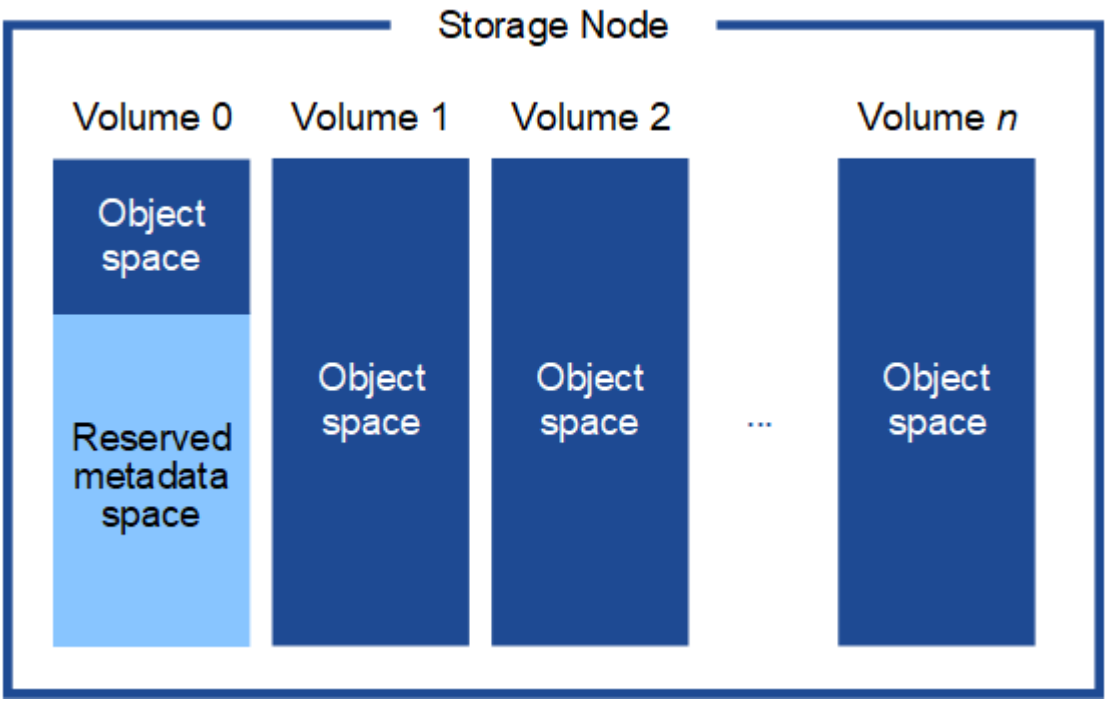
dei metadati degli oggetti sono distribuite in modo uniforme in tutti i nodi di storage di ciascun sito.

Questa figura rappresenta i nodi di storage in due siti. Ogni sito ha la stessa quantità di metadati degli oggetti, che sono distribuiti in modo uguale tra 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 una serie di fattori, descritti di seguito.

Impostazione spazio riservato metadati

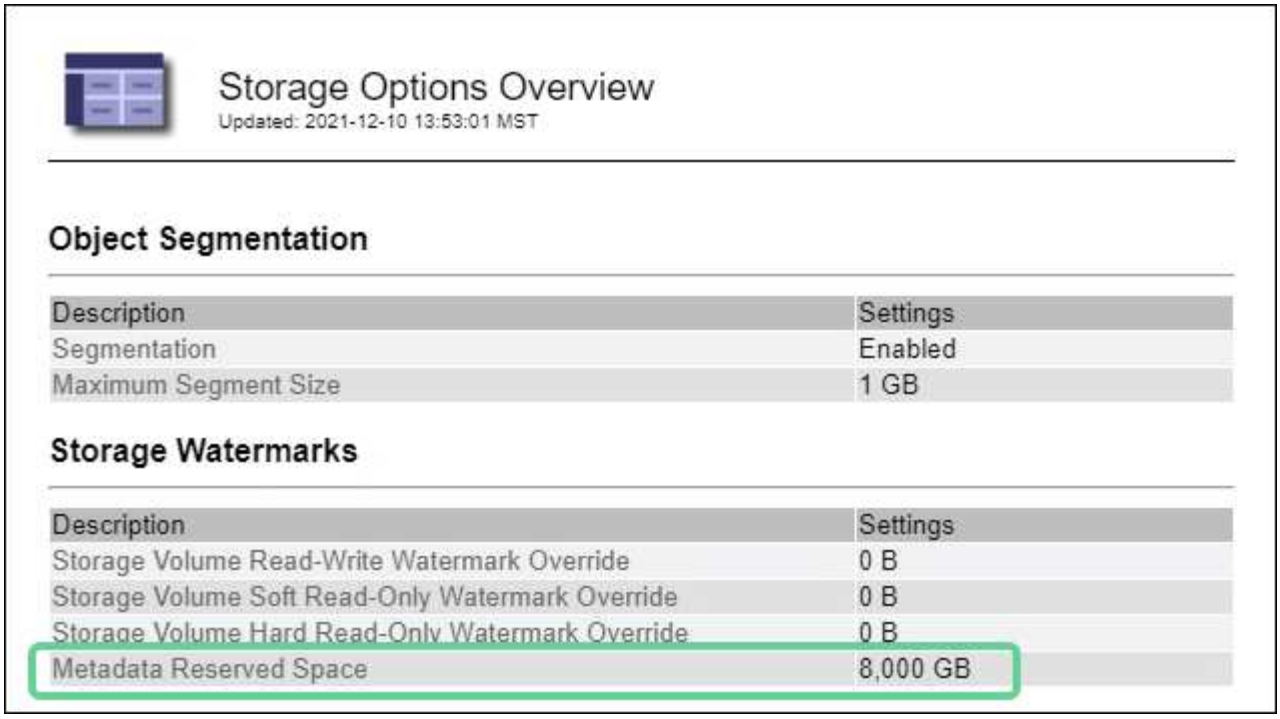
L' *Metadata Reserved Space* è un'impostazione a livello di sistema che rappresenta la quantità di spazio che verrà riservata ai metadati sul volume 0 di ogni nodo di storage. Come mostrato nella tabella, il valore predefinito di questa impostazione per StorageGRID 11.6 si basa su quanto segue:

- 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 per StorageGRID 11.6
11.5/11.6	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 versioni precedenti	Qualsiasi importo	2 TB (2,000 GB)

Per visualizzare l'impostazione spazio riservato metadati per il sistema StorageGRID:

1. Selezionare **CONFIGURATION** > **System** > **Storage options**.
2. Nella tabella Storage Watermarks, individuare **Metadata Reserved Space**.



Nella schermata, il valore **Metadata Reserved Space** è 8,000 GB (8 TB). Questa è l'impostazione predefinita per una nuova installazione di StorageGRID 11.6 in cui ogni nodo di storage dispone di almeno 128 GB di RAM.

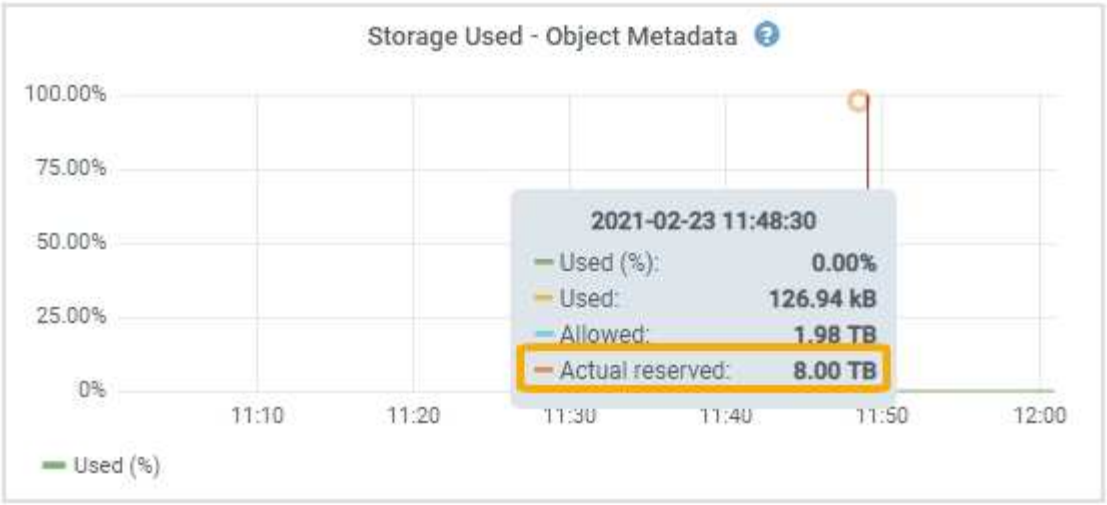
Spazio riservato effettivo per i metadati

A differenza dell'impostazione spazio riservato metadati a livello di sistema, per ciascun nodo di storage viene determinato l' *spazio riservato effettivo* per i metadati dell'oggetto. Per qualsiasi nodo di storage, lo spazio riservato effettivo per i metadati dipende dalle dimensioni del volume 0 per il nodo e dall'impostazione **Metadata Reserved Space** 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 superiore	Il minore di questi valori: • Volume 0 • Impostazione spazio riservato metadati

Per visualizzare lo spazio riservato effettivo per i metadati su un nodo di storage specifico:

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 spazio riservato metadati a livello di sistema è inferiore al volume 0 per questo nodo di storage, lo spazio riservato effettivo per questo nodo corrisponde all'impostazione spazio riservato metadati.

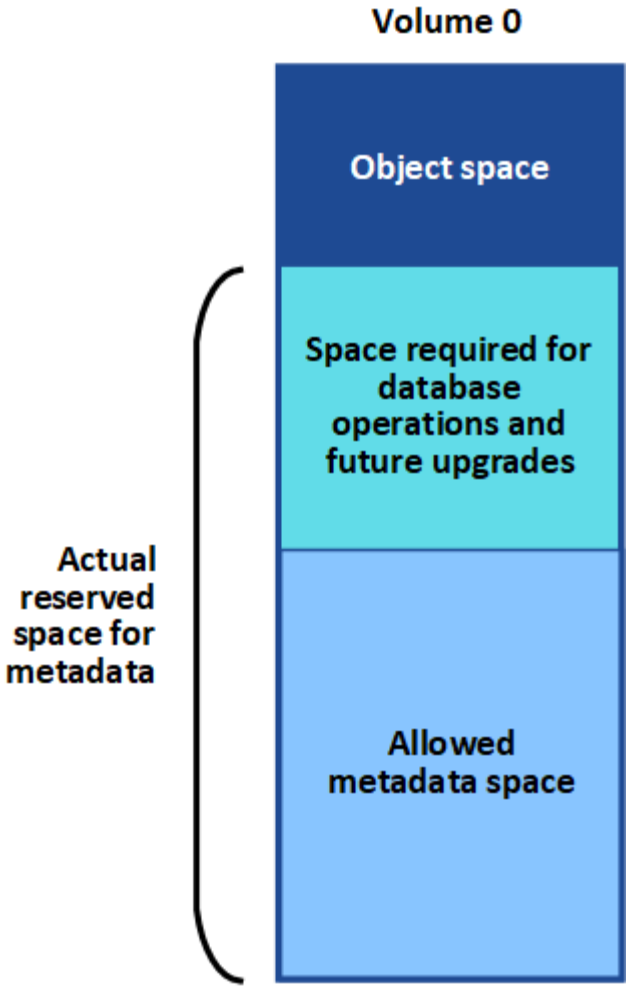
Esempio di spazio riservato effettivo dei metadati

Si supponga di installare un nuovo 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:

- L'opzione **Metadata Reserved Space** a livello di sistema è impostata su 8 TB. (Questo è il valore predefinito per una nuova installazione di StorageGRID 11.6 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 **Metadata Reserved Space**).

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.



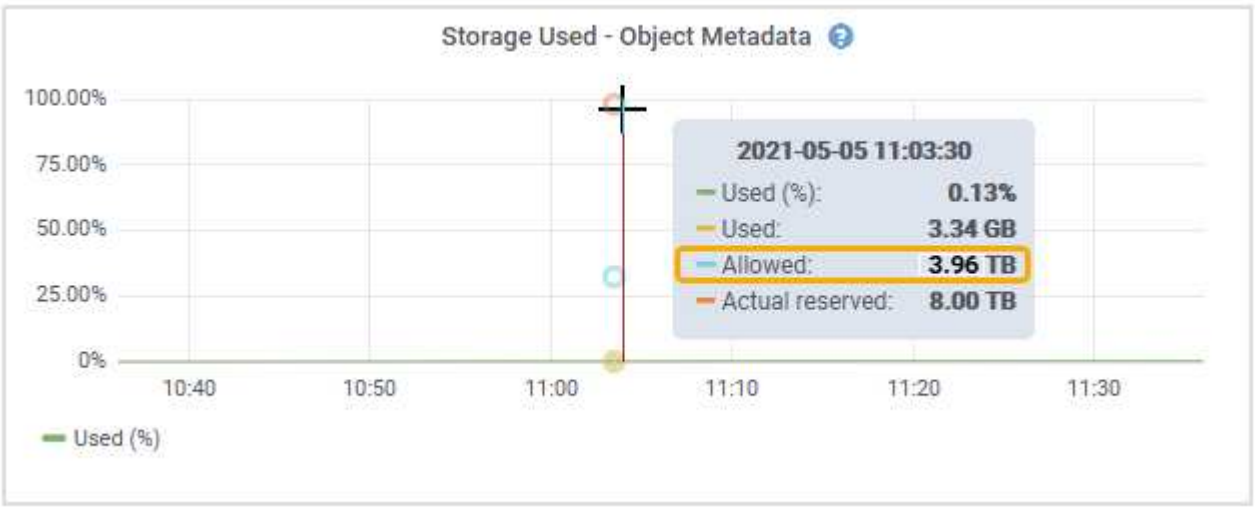
La seguente tabella mostra come StorageGRID calcola lo spazio di metadati consentito* per diversi nodi di storage, in base alla quantità di memoria per il nodo e allo spazio riservato effettivo per i metadati.

		Quantità di memoria sul nodo di storage	
	lt; 128 GB	gt;= 128 GB	**Spazio riservato effettivo per i metadati**
lt;= 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	gt; 4 TB

Per visualizzare lo spazio di metadati consentito per un nodo di storage:

1. Da Grid Manager, selezionare **NODES**.
2. Selezionare il nodo di storage.
3. Selezionare la scheda **Storage**.

4. Posizionare il cursore del mouse sul grafico Storage used — Object Metadata (Storage utilizzato — metadati oggetto) e individuare il valore **Allowed** (consentito).



Nella schermata, il valore **Allowed** è 3.96 TB, ovvero il valore massimo per un nodo di storage 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:

- L'opzione **Metadata Reserved Space** a livello di sistema è impostata su 8 TB. (Questo è il valore predefinito per StorageGRID 11.6 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 **Metadata Reserved Space**).
- 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.

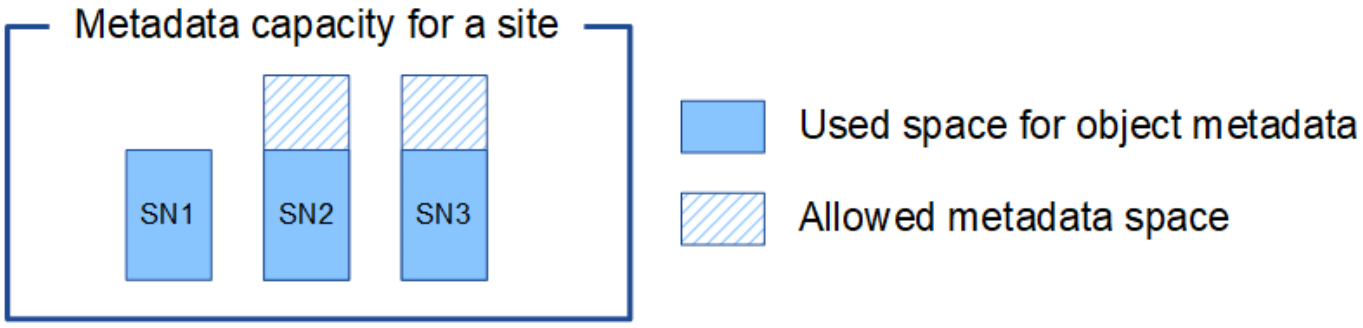
Si consideri il seguente esempio:

- Si dispone di un grid a sito singolo contenente tre nodi di storage di dimensioni diverse.
- L'impostazione **Metadata Reserved Space** 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. Non è possibile utilizzare i 0.66 TB aggiuntivi di spazio consentito per i metadati SN2 e SN3.



Analogamente, poiché StorageGRID gestisce tutti i metadati degli oggetti per un sistema StorageGRID in ogni sito, la capacità complessiva dei metadati di un sistema StorageGRID è determinata dalla capacità dei metadati degli oggetti del sito più piccolo.

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, visitare il sito Web all'indirizzo Monitorare e risolvere i problemi.
- Per aumentare la capacità dei metadati degli oggetti per il sistema, aggiungere nuovi nodi di storage. Passare a. Espandi il tuo grid.

Configurare le impostazioni globali per gli oggetti memorizzati

Configurare la compressione degli oggetti memorizzati

È possibile utilizzare l'opzione Compress Stored Objects Grid per ridurre le dimensioni degli oggetti memorizzati in StorageGRID, in modo che gli oggetti consumino meno spazio di storage.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

Per impostazione predefinita, l'opzione Compress Stored Objects Grid (Comprimi oggetti memorizzati) è disattivata. Se si attiva questa opzione, 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 questa opzione, tenere presente quanto segue:

- Non attivare la compressione 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, l'attivazione della compressione degli oggetti memorizzati non ridurrà ulteriormente la dimensione di un oggetto.
- Non attivare la compressione se si utilizza NetApp FabricPool con StorageGRID.
- Se l'opzione Compress Stored Objects Grid è attivata, le applicazioni client S3 e Swift dovrebbero evitare di eseguire operazioni GET Object che specificano la restituzione di un intervallo di byte. Queste operazioni "range Read" sono inefficienti perché StorageGRID deve decomprimere efficacemente gli oggetti per accedere ai byte richiesti. LE operazioni GET Object che richiedono un piccolo intervallo di byte da un oggetto molto grande sono particolarmente inefficienti; ad esempio, è 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 Opzioni griglia**.
2. Nella sezione Opzioni oggetto memorizzato, selezionare la casella di controllo **Comprimi oggetti memorizzati**.

3. Selezionare **Salva**.

Configurare la crittografia degli oggetti memorizzati

È possibile crittografare gli oggetti memorizzati se si desidera garantire che i dati non possano essere recuperati in un formato leggibile se un archivio di oggetti viene compromesso. Per impostazione predefinita, gli oggetti non vengono crittografati.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

La crittografia degli oggetti memorizzati consente la crittografia di tutti i dati degli oggetti durante l'acquisizione tramite S3 o Swift. 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.

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.

Gli oggetti memorizzati possono essere crittografati utilizzando l'algoritmo di crittografia AES-128 o AES-256.

L'impostazione crittografia oggetti memorizzati si applica solo agli oggetti S3 che non sono stati crittografati mediante crittografia a livello di bucket o a livello di oggetto.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Stored Object Options, impostare l'opzione Stored Object Encryption su **None** (Nessuna) (impostazione predefinita), **AES-128** o **AES-256**.

3. Selezionare **Salva**.

Configurare l'hashing degli oggetti memorizzati

L'opzione di hashing degli oggetti memorizzati specifica l'algoritmo di hashing utilizzato per verificare l'integrità degli oggetti.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

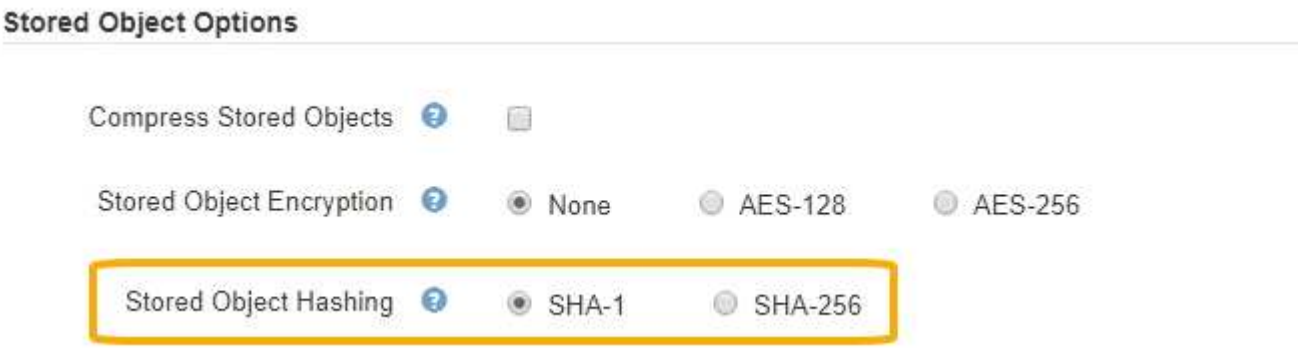
A proposito di questa attività

Per impostazione predefinita, i dati degli oggetti vengono hash utilizzando l'algoritmo SHA-1. L'algoritmo SHA-256 richiede risorse CPU aggiuntive e generalmente non è consigliato per la verifica dell'integrità.

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.

Fasi

1. Selezionare **CONFIGURAZIONE sistema Opzioni griglia**.
2. Nella sezione Stored Object Options, modificare l'hashing degli oggetti memorizzati in **SHA-1** (impostazione predefinita) o **SHA-256**.



3. Selezionare **Salva**.

Impostazioni di configurazione del nodo di storage

Ogni nodo di storage utilizza una serie di 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:

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
Stato HTTP	HSTE	Lo stato corrente del protocollo 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
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.

Data store LDR

Nome attributo	Codice	Descrizione
Ripristina conteggio oggetti persi	RCOR	Ripristina il contatore per il numero di oggetti persi su questo servizio.

Storage LDR

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 dello storage in sola lettura e interrompe l'accettazione del nuovo contenuto. 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.

Verifica LDR

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.

Nome attributo	Codice	Descrizione
Tasso di verifica	VPRI	Imposta la velocità con cui avviene la verifica in background. Vedere le informazioni sulla configurazione del tasso 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). Per ulteriori informazioni, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.
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.

Codifica LDR Erasure

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.
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.

Nome attributo	Codice	Descrizione
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.

Replica LDR

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.
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 non possono essere recuperati dal nodo di storage per essere copiati in altre posizioni nel sistema StorageGRID. Il servizio LDR è di sola scrittura.

Informazioni correlate

Monitorare e risolvere i problemi

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 storage dell'appliance StorageGRID, come SG6060, possono 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

Che cos'è un nodo amministratore

I nodi di amministrazione forniscono servizi di gestione quali configurazione, monitoraggio e registrazione del sistema. Ogni grid deve avere un nodo di amministrazione primario e può avere un numero qualsiasi di nodi di amministrazione non primari per la ridondanza.

Quando si accede a Grid Manager o al tenant Manager, si sta effettuando la connessione a un nodo amministratore. È possibile connettersi a qualsiasi nodo amministratore e ciascun nodo amministratore visualizza una vista simile del sistema StorageGRID. Tuttavia, le procedure di manutenzione devono essere eseguite utilizzando il nodo di amministrazione primario.

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

I nodi di amministrazione ospitano i seguenti servizi:

- Servizio AMS
- Servizio CMN
- Servizio NMS
- Servizio Prometheus

- Servizi Load Balancer e High Availability (per supportare il traffico client S3 e Swift)

I nodi di amministrazione supportano anche la Management Application Program Interface (Mgmt-api) per elaborare le richieste provenienti dall'API Grid Management e dall'API Tenant Management. Vedere Utilizzare l'API Grid Management.

Che cos'è il servizio AMS

Il servizio Audit Management System (AMS) tiene traccia dell'attività e degli eventi del sistema.

Che cos'è il servizio CMN

Il servizio CMN (Configuration Management Node) gestisce le configurazioni a livello di sistema di connettività e le funzionalità di protocollo necessarie a tutti i servizi. Inoltre, il servizio CMN viene utilizzato per eseguire e monitorare le attività della griglia. Esiste un solo servizio CMN per implementazione StorageGRID. Il nodo di amministrazione che ospita il servizio CMN è noto come nodo di amministrazione primario.

Che cos'è il servizio NMS

Il servizio del sistema di gestione della rete (NMS) alimenta le opzioni di monitoraggio, reporting e configurazione visualizzate tramite Grid Manager, l'interfaccia basata su browser del sistema StorageGRID.

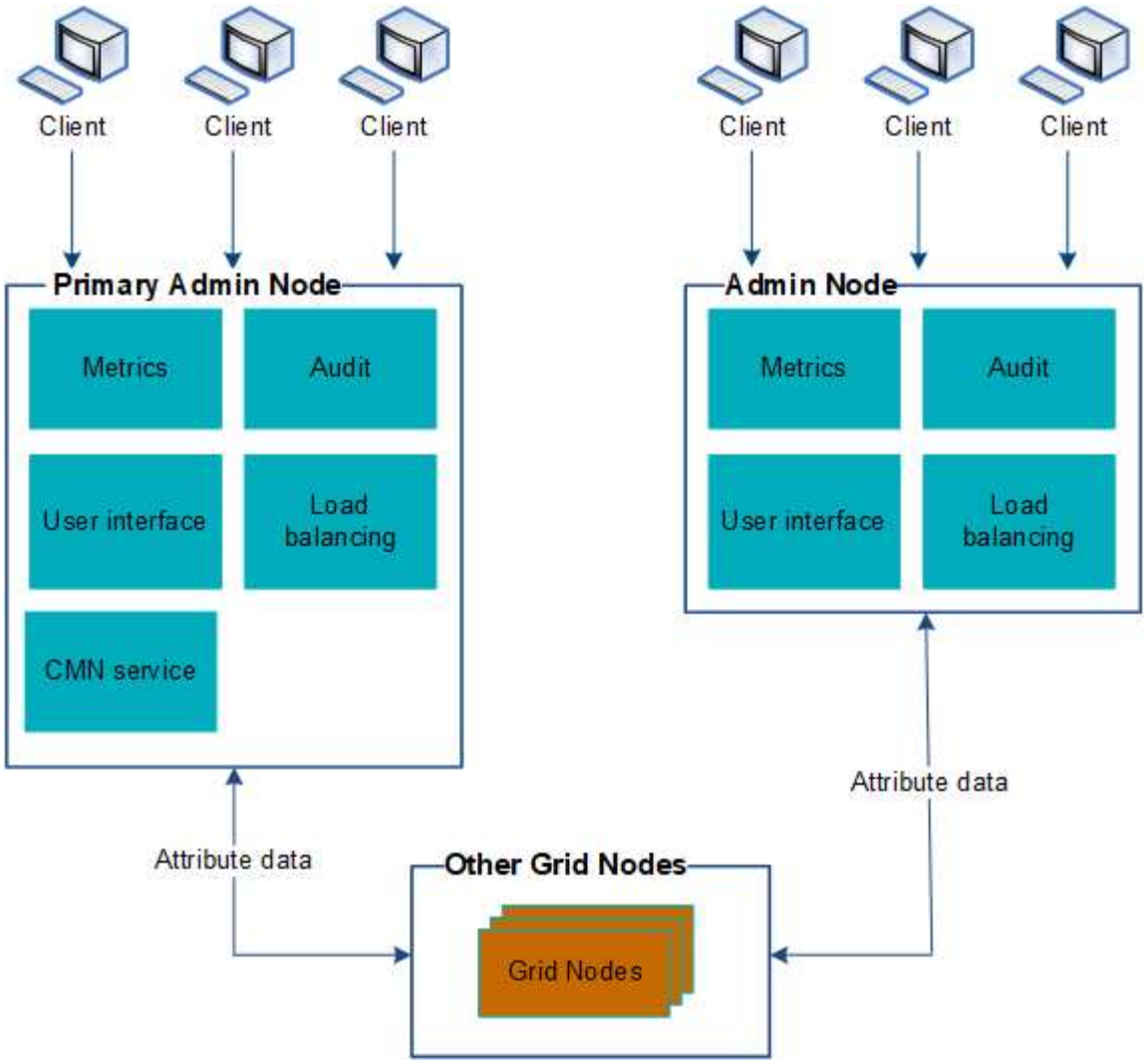
Che cos'è il servizio Prometheus

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

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 amministratore non è più disponibile, l'elaborazione degli attributi continua, gli avvisi e gli allarmi (sistema legacy) vengono ancora attivati e le notifiche e-mail e i messaggi AutoSupport vengono ancora inviati. Tuttavia, la presenza di più nodi di amministrazione non fornisce la protezione di failover ad eccezione delle notifiche e dei messaggi 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 se il nodo di amministrazione master non riesce. 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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.

Selezionare un mittente preferito

Se l'implementazione di StorageGRID include più nodi di amministrazione, è possibile selezionare quale nodo di amministrazione deve essere il mittente preferito delle notifiche. Per impostazione predefinita, viene selezionato il nodo di amministrazione principale, ma qualsiasi nodo di amministrazione può essere il mittente preferito.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

La pagina **CONFIGURAZIONE sistema Opzioni di visualizzazione** mostra quale nodo amministrativo è attualmente selezionato come mittente preferito. Per impostazione predefinita, viene selezionato il nodo di amministrazione principale.

Nelle normali operazioni di sistema, solo il mittente preferito invia le seguenti notifiche:

- Messaggi AutoSupport
- Notifiche SNMP
- E-mail di avviso
- Email di allarme (sistema legacy)

Tuttavia, tutti gli altri nodi di amministrazione (mittenti in standby) monitorano il mittente preferito. Se viene rilevato un problema, anche un mittente in standby può inviare queste notifiche.

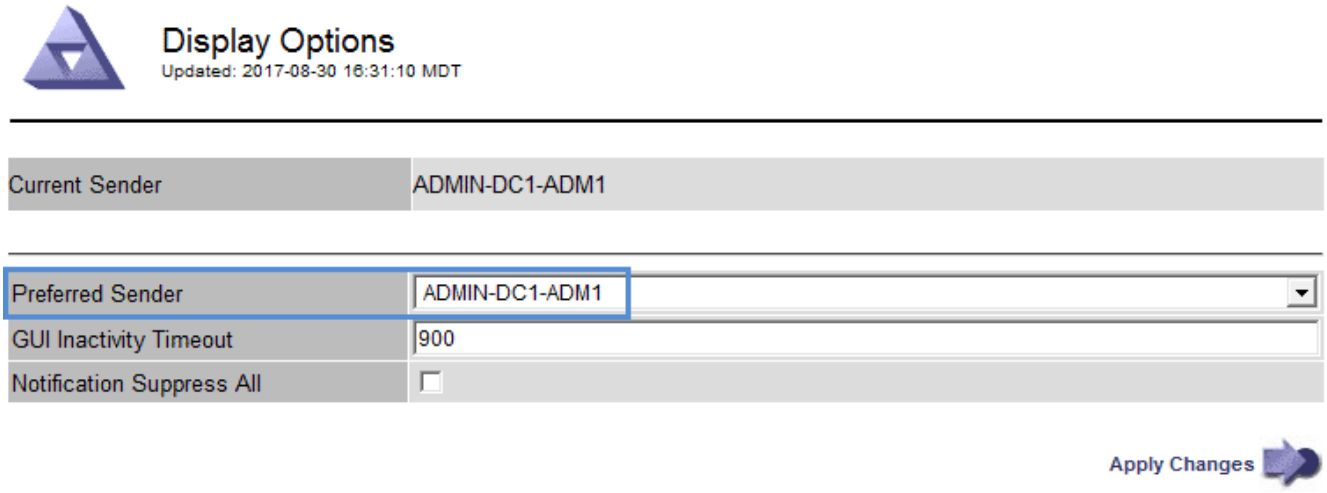
Sia il mittente preferito che il mittente in standby potrebbero inviare notifiche nei seguenti casi:

- Se i nodi di amministrazione diventano "islanded" l'uno dall'altro, sia il mittente preferito che i mittenti di standby tenteranno di inviare notifiche e potrebbero essere ricevute più copie delle notifiche.
- Dopo che un mittente in standby rileva problemi con il mittente preferito e inizia a inviare notifiche, il mittente preferito potrebbe riacquistare la capacità di inviare notifiche. In questo caso, potrebbero essere inviate notifiche duplicate. Il mittente in standby interrompe l'invio di notifiche quando non rileva più errori sul mittente preferito.

Quando si testano le notifiche di allarme e i messaggi AutoSupport, tutti i nodi di amministrazione inviano l'email di test. Quando si verificano le notifiche di avviso, è necessario accedere a ogni nodo amministratore per verificare la connettività.

Fasi

1. Selezionare **CONFIGURAZIONE** > **sistema** > **Opzioni di visualizzazione**.
2. Dal menu Display Options (Opzioni di visualizzazione), selezionare **Options** (Opzioni).
3. Selezionare il nodo Admin che si desidera impostare come mittente preferito dall'elenco a discesa.



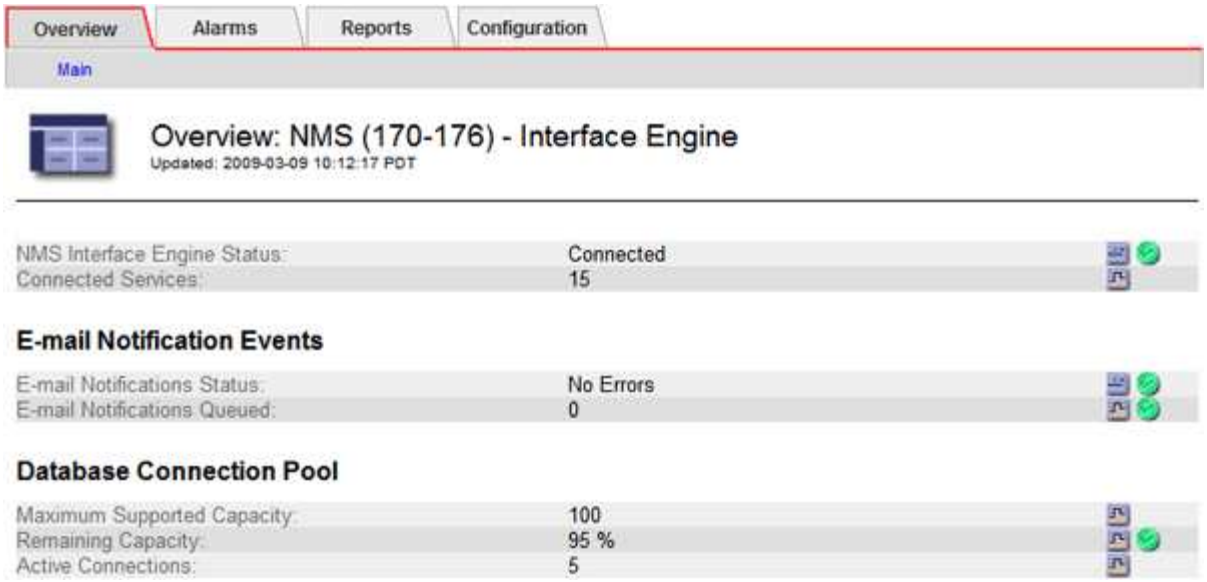
4. Selezionare **Applica modifiche**.

   L'Admin Node viene impostato come mittente preferito delle notifiche.

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**.

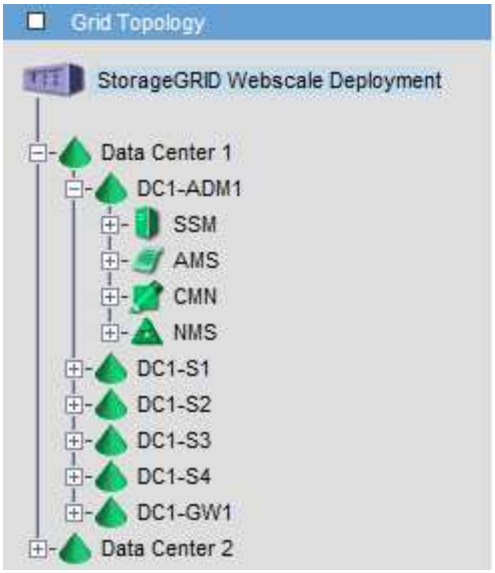


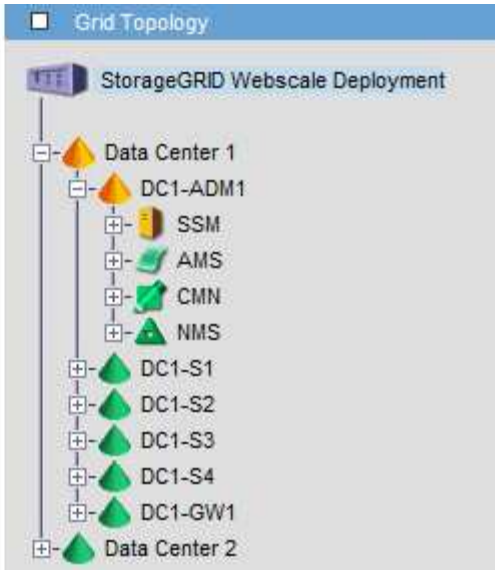
Le notifiche vengono elaborate tramite la coda di notifica e-mail e inviate al server di posta una dopo l'altra nell'ordine in cui vengono attivate. Se si verifica un problema (ad esempio, un errore di connessione di rete) e il server di posta non è disponibile quando si tenta di inviare la notifica, 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. Nel caso in cui una notifica venga 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

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. Per un facile accesso ai registri di audit, è possibile configurare l'accesso client per le condivisioni di audit per CIFS e NFS.

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.

> L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID. Se hai la possibilità di utilizzare CIFS o NFS, scegli NFS.

Configurare i client di audit per CIFS

La procedura utilizzata per configurare un client di audit dipende dal metodo di autenticazione: Windows Workgroup o Windows Active Directory (ad). Una volta aggiunta, la condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

> L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Configurare i client di audit per Workgroup

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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: `storagegrid-status`

   Se tutti i servizi non sono 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 CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Impostare l'autenticazione per Windows Workgroup:

   Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

   a. Inserire: `set-authentication`
   b. Quando viene richiesto di installare Windows Workgroup o Active Directory, immettere: `workgroup`
   c. Quando richiesto, immettere un nome per il gruppo di lavoro: *`workgroup_name`*

d. Quando richiesto, creare un nome NetBIOS significativo: *netbios_name*

   oppure

   Premere **Invio** per utilizzare il nome host del nodo di amministrazione come nome NetBIOS.

Lo script riavvia il server Samba e le modifiche vengono applicate. Questa operazione dovrebbe richiedere meno di un minuto. Dopo aver impostato l'autenticazione, aggiungere un client di audit.

a. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione CIFS.

6. Aggiungere un client di audit:

   a. Inserire: `add-audit-share`

      La condivisione viene aggiunta automaticamente in sola lettura.

   b. Quando richiesto, aggiungere un utente o un gruppo: *user*

   c. Quando richiesto, inserire il nome utente per l'audit: *audit_user_name*

   d. Quando richiesto, inserire una password per l'utente di controllo: *password*

   e. Quando richiesto, immettere nuovamente la stessa password per confermarla: *password*

   f. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

      Non è necessario inserire una directory. Il nome della directory di controllo è predefinito.

7. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere gli utenti aggiuntivi:

   a. Inserire: `add-user-to-share`

      Viene visualizzato un elenco numerato di condivisioni abilitate.

   b. Quando richiesto, inserire il numero della condivisione audit-export: *share_number*

   c. Quando richiesto, aggiungere un utente o un gruppo: `user`

      oppure `group`

   d. Quando richiesto, inserire il nome dell'utente o del gruppo di controllo: *audit_user or audit_group*

   e. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

   f. Ripetere questi passaggi secondari per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

8. In alternativa, verificare la configurazione: `validate-config`

I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. Quando richiesto, premere **Invio**.

   Viene visualizzata la configurazione del client di audit.

b. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione CIFS.

9. Chiudere l'utilità di configurazione CIFS: `exit`
10. Avviare il servizio Samba: `service smbd start`
11. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

    oppure

    Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, attivare questa condivisione 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 la procedura per configurare la condivisione di controllo per ogni nodo amministrativo aggiuntivo.
    c. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`
12. Disconnettersi dalla shell dei comandi: `exit`

Configurare i client di audit per Active Directory

Eseguire questa procedura per ogni nodo amministratore in un'implementazione StorageGRID da cui si desidera recuperare i messaggi di controllo.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- Si dispone del nome utente e della password di CIFS Active Directory.
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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: `storagegrid-status`

   Se tutti i servizi non sono 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 CIFS: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------
```

5. Impostare l'autenticazione per Active Directory: `set-authentication`

   Nella maggior parte delle implementazioni, è necessario impostare l'autenticazione prima di aggiungere il client di audit. Se l'autenticazione è già stata impostata, viene visualizzato un messaggio di avviso. Se l'autenticazione è già stata impostata, passare alla fase successiva.

   a. Quando viene richiesto di installare Workgroup o Active Directory: `ad`
   b. Quando richiesto, inserire il nome del dominio ad (nome di dominio breve).
   c. Quando richiesto, inserire l'indirizzo IP o il nome host DNS del controller di dominio.
   d. Quando richiesto, inserire il nome completo del dominio.

      Utilizzare lettere maiuscole.

   e. Quando viene richiesto di attivare il supporto winbind, digitare **y**.

Winbind viene utilizzato per risolvere le informazioni di utenti e gruppi dai server ad.

f. Quando richiesto, inserire il nome NetBIOS.

g. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

6. Unirsi al dominio:

a. Se non è già stato avviato, avviare l'utility di configurazione CIFS: `config_cifs.rb`

b. Unirsi al dominio: `join-domain`

c. Viene richiesto di verificare se l'Admin Node è attualmente un membro valido del dominio. Se questo nodo di amministrazione non ha precedentemente aderito al dominio, immettere: `no`

d. Quando richiesto, fornire il nome utente dell'amministratore: *`administrator_username`*

dove *`administrator_username`* È il nome utente di CIFS Active Directory, non il nome utente di StorageGRID.

e. Quando richiesto, fornire la password dell'amministratore: *`administrator_password`*

erano *`administrator_password`* È il nome utente di CIFS Active Directory, non la password di StorageGRID.

f. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

7. Verificare di aver inserito correttamente il dominio:

a. Unirsi al dominio: `join-domain`

b. Quando viene richiesto di verificare se il server è attualmente un membro valido del dominio, immettere: `y`

Se viene visualizzato il messaggio "Join is OK," significa che l'accesso al dominio è stato eseguito correttamente. Se non si ottiene questa risposta, provare a impostare nuovamente l'autenticazione e ad accedere al dominio.

c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

8. Aggiungere un client di audit: `add-audit-share`

a. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `user`

b. Quando viene richiesto di inserire il nome utente per l'audit, inserire il nome utente per l'audit.

c. Quando richiesto, premere **Invio**.

Viene visualizzata l'utility di configurazione CIFS.

9. Se più di un utente o gruppo è autorizzato ad accedere alla condivisione di controllo, aggiungere altri utenti: `add-user-to-share`

Viene visualizzato un elenco numerato di condivisioni abilitate.

a. Inserire il numero della condivisione audit-export.
b. Quando viene richiesto di aggiungere un utente o un gruppo, immettere: `group`

   Viene richiesto il nome del gruppo di audit.

c. Quando viene richiesto il nome del gruppo di audit, immettere il nome del gruppo di utenti di audit.
d. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione CIFS.

e. Ripetere questo passaggio per ogni utente o gruppo aggiuntivo che ha accesso alla condivisione di controllo.

10. In alternativa, verificare la configurazione: `validate-config`

    I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-filesystem.inc`
    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-interfaces.inc`
    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-custom-config.inc`
    - Impossibile trovare il file di inclusione `/etc/samba/includes/cifs-shares.inc`
    - Rlimit_max: Aumento di rlimit_max (1024) al limite minimo di Windows (16384)

      > Non combinare l'impostazione 'security=ads' con il parametro 'password server'. (Per impostazione predefinita, Samba rileverà automaticamente il DC corretto da contattare).

      i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
      ii. Quando richiesto, premere **Invio**.

      Viene visualizzata l'utility di configurazione CIFS.

11. Chiudere l'utilità di configurazione CIFS: `exit`
12. Se l'implementazione di StorageGRID è un singolo sito, passare alla fase successiva.

    oppure

    Facoltativamente, se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, abilitare 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: `exit`

13. Disconnettersi dalla shell dei comandi: `exit`

Aggiungere un utente o un gruppo a una condivisione di audit CIFS

È possibile aggiungere un utente o un gruppo a una condivisione di audit CIFS integrata con l'autenticazione ad.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

La seguente procedura riguarda una condivisione di controllo integrata con l'autenticazione ad.

> L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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 tutti i servizi non sono 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 CIFS: `config_cifs.rb`

```
-------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------------
```

5. Iniziare ad aggiungere un utente o un gruppo: `add-user-to-share`

   Viene visualizzato un elenco numerato di condivisioni di controllo configurate.

6. Quando richiesto, inserire il numero per la condivisione dell'audit (audit-export): *`audit_share_number`*

   Viene richiesto se si desidera concedere a un utente o a un gruppo l'accesso a questa condivisione di controllo.

7. Quando richiesto, aggiungere un utente o un gruppo: `user` oppure `group`
8. Quando viene richiesto il nome dell'utente o del gruppo per questa condivisione di audit ad, immettere il nome.

   L'utente o il gruppo viene aggiunto in sola lettura per la condivisione di controllo sia nel sistema operativo del server che nel servizio CIFS. La configurazione di Samba viene ricaricata per consentire all'utente o al gruppo di accedere alla condivisione del client di audit.

9. Quando richiesto, premere **Invio**.

   Viene visualizzata l'utility di configurazione CIFS.

10. Ripetere questa procedura per ogni utente o gruppo che ha accesso alla condivisione di controllo.
11. In alternativa, verificare la configurazione: `validate-config`

    I servizi vengono controllati e visualizzati. È possibile ignorare i seguenti messaggi:

    - Impossibile trovare il file include /etc/samba/includes/cifs-interfaces.inc
    - Impossibile trovare il file include /etc/samba/includes/cifs-filesystem.inc
    - Impossibile trovare il file include /etc/samba/includes/cifs-custom-config.inc
    - Impossibile trovare il file include /etc/samba/includes/cifs-shares.inc
      i. Quando richiesto, premere **Invio** per visualizzare la configurazione del client di controllo.
      ii. Quando richiesto, premere **Invio**.

12. Chiudere l'utilità di configurazione CIFS: `exit`
13. Determinare se è necessario attivare ulteriori condivisioni di audit, come segue:

- 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 di amministrazione di un 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 questa procedura per configurare le condivisioni di controllo per ciascun nodo di amministrazione.
  iii. Chiudere l'accesso remoto sicuro alla shell nel nodo di amministrazione remoto: `exit`

14. Disconnettersi dalla shell dei comandi: `exit`

Rimuovere un utente o un gruppo da una condivisione di audit CIFS

Non è possibile rimuovere l'ultimo utente o gruppo autorizzato ad accedere alla condivisione di controllo.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con le password dell'account root (disponibili in DETTO pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

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 CIFS: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

3. Iniziare a rimuovere un utente o un gruppo: `remove-user-from-share`

   Viene visualizzato un elenco numerato delle condivisioni di audit disponibili per il nodo di amministrazione. La condivisione dell'audit è etichettata audit-export.

4. Inserire il numero della condivisione di controllo: *`audit_share_number`*
5. Quando viene richiesto di rimuovere un utente o un gruppo: `user` oppure `group`

   Viene visualizzato un elenco numerato di utenti o gruppi per la condivisione dell'audit.

6. Inserire il numero corrispondente all'utente o al gruppo che si desidera rimuovere: *`number`*

   La condivisione di controllo viene aggiornata e l'utente o il gruppo non può più accedere alla condivisione di controllo. Ad esempio:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Chiudere l'utilità di configurazione CIFS: `exit`
8. Se l'implementazione di StorageGRID include nodi di amministrazione in altri siti, disattivare la condivisione di controllo in ciascun sito secondo necessità.
9. Disconnettersi da ogni shell dei comandi al termine della configurazione: `exit`

Modificare il nome di un utente o di un gruppo di condivisione dell'audit CIFS

È possibile modificare il nome di un utente o di un gruppo per una condivisione di audit CIFS aggiungendo un nuovo utente o gruppo ed eliminando quello precedente.

A proposito di questa attività

L'esportazione dell'audit tramite CIFS/Samba è stata deprecata e verrà rimossa in una release futura di StorageGRID.

Fasi

1. Aggiungere un nuovo utente o gruppo con il nome aggiornato alla condivisione di controllo.
2. Eliminare il vecchio nome utente o gruppo.

Informazioni correlate

- Aggiungere un utente o un gruppo a una condivisione di audit CIFS
- Rimuovere un utente o un gruppo da una condivisione di audit CIFS

Verificare l'integrazione dell'audit CIFS

La condivisione dell'audit è di sola lettura. I file di log devono essere letti dalle applicazioni del computer e la verifica non include l'apertura di un file. Si ritiene sufficiente verificare che i file di registro di controllo vengano visualizzati in una finestra di Esplora risorse. Dopo la verifica della connessione, chiudere tutte le finestre.

Configurare il client di audit per NFS

La condivisione di controllo viene attivata automaticamente come condivisione di sola lettura.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password root/admin (disponibile nel pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).
- 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.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).
- 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/audit/export`

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.

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 comando Linux di esempio è (inserire su una riga):

   `mount -t nfs -o hard,intr Admin_Node_IP_address:/var/local/audit/export 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.

Di cosa hai bisogno

- Hai il `Passwords.txt` File con la password dell'account root/admin (disponibile nel pacchetto).
- Hai il `Configuration.txt` File (disponibile in DETTO pacchetto).

A proposito di questa attività

Non è possibile rimuovere l'ultimo indirizzo IP consentito per accedere alla condivisione 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. 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/audit/export`

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

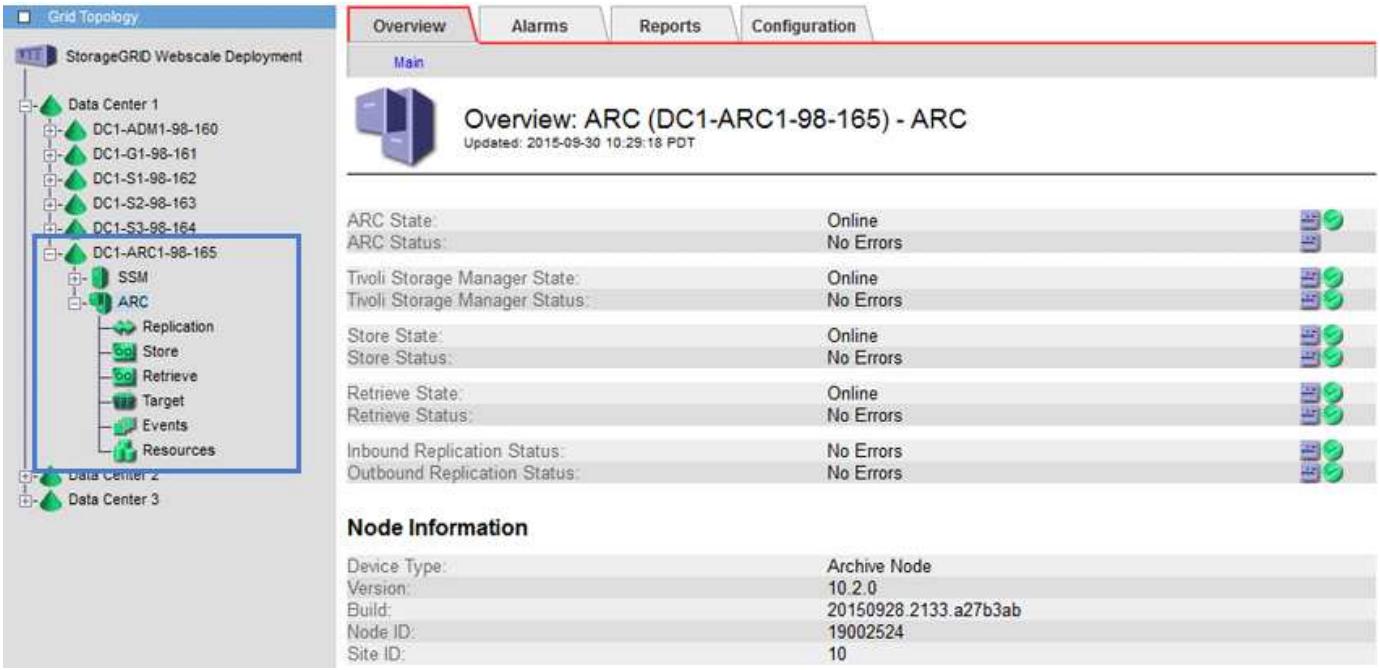
- Aggiungere un client di audit NFS a una condivisione di audit
- Rimuovere un client di audit NFS dalla condivisione di audit

Gestire i nodi di archiviazione

Che cos’è un nodo di archivio

Facoltativamente, ogni sito del data center StorageGRID può essere implementato con un nodo di archiviazione, che consente di connettersi a un sistema di storage di archiviazione esterno mirato, come Tivoli Storage Manager (TSM).

Il nodo di archiviazione fornisce un’interfaccia attraverso la quale è possibile indirizzare un sistema di storage di archiviazione esterno per lo storage a lungo termine dei dati a oggetti. Il nodo di archiviazione monitora inoltre questa connessione e il trasferimento dei dati degli oggetti tra il sistema StorageGRID e il sistema di archiviazione esterno di destinazione.



Dopo aver configurato le connessioni alla destinazione esterna, è possibile configurare il nodo di archiviazione in modo da ottimizzare le prestazioni del TSM, disattivare un nodo di archiviazione quando un server TSM si avvicina alla capacità o non è disponibile e configurare le impostazioni di replica e recupero. È inoltre possibile impostare allarmi personalizzati per il nodo di archiviazione.

I dati degli oggetti che non possono essere cancellati, ma a cui non si accede regolarmente, possono essere spostati in qualsiasi momento dai dischi rotanti di uno Storage Node e su uno storage di archiviazione esterno, come il cloud o il nastro. Questa archiviazione dei dati a oggetti viene eseguita attraverso la configurazione del nodo di archivio di un sito del data center e quindi la configurazione delle regole ILM in cui questo nodo di archivio viene selezionato come "destinazione" per le istruzioni di posizionamento del contenuto. Il nodo di archiviazione non gestisce i dati degli oggetti archiviati in sé; ciò viene ottenuto dal dispositivo di archiviazione esterno.

I metadati degli oggetti non vengono archiviati, ma rimangono nei nodi di storage.

Che cos'è il servizio ARC

Il servizio Archive (ARC) sui nodi di archiviazione fornisce l'interfaccia di gestione che è possibile utilizzare per configurare le connessioni allo storage di archiviazione esterno, come ad esempio il nastro attraverso il middleware TSM.

È il servizio ARC che interagisce con un sistema di storage di archiviazione esterno, inviando dati a oggetti per lo storage nearline ed eseguendo recuperi quando un'applicazione client richiede un oggetto archiviato. Quando un'applicazione client richiede un oggetto archiviato, un nodo di storage richiede i dati dell'oggetto al servizio ARC. Il servizio ARC invia una richiesta al sistema di storage di archiviazione esterno, che recupera i dati dell'oggetto richiesti e li invia al servizio ARC. Il servizio ARC verifica i dati dell'oggetto e li inoltra al nodo di storage, che a sua volta restituisce l'oggetto all'applicazione client richiedente.

Le richieste di dati a oggetti archiviati su nastro tramite il middleware TSM vengono gestite per garantire l'efficienza dei recuperi. Le richieste possono essere ordinate in modo che gli oggetti memorizzati in ordine sequenziale su nastro vengano richiesti nello stesso ordine sequenziale. Le richieste vengono quindi messe in coda per l'invio al dispositivo di storage. A seconda del dispositivo di archiviazione, è possibile elaborare contemporaneamente più richieste di oggetti su diversi volumi.

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.

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. L'opzione **Cloud Tiering - Simple Storage Service (S3)** è ancora supportata, ma potresti preferire implementare i Cloud Storage Pool.

Se stai utilizzando un nodo di archiviazione con l'opzione **Cloud Tiering - Simple Storage Service (S3)**, prendi in considerazione la migrazione degli oggetti a un pool di storage cloud. Consultare le istruzioni per Gestione degli oggetti con 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.

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. L'opzione **Cloud Tiering - Simple Storage Service (S3)** è ancora supportata, ma potresti preferire implementare i Cloud Storage Pool.

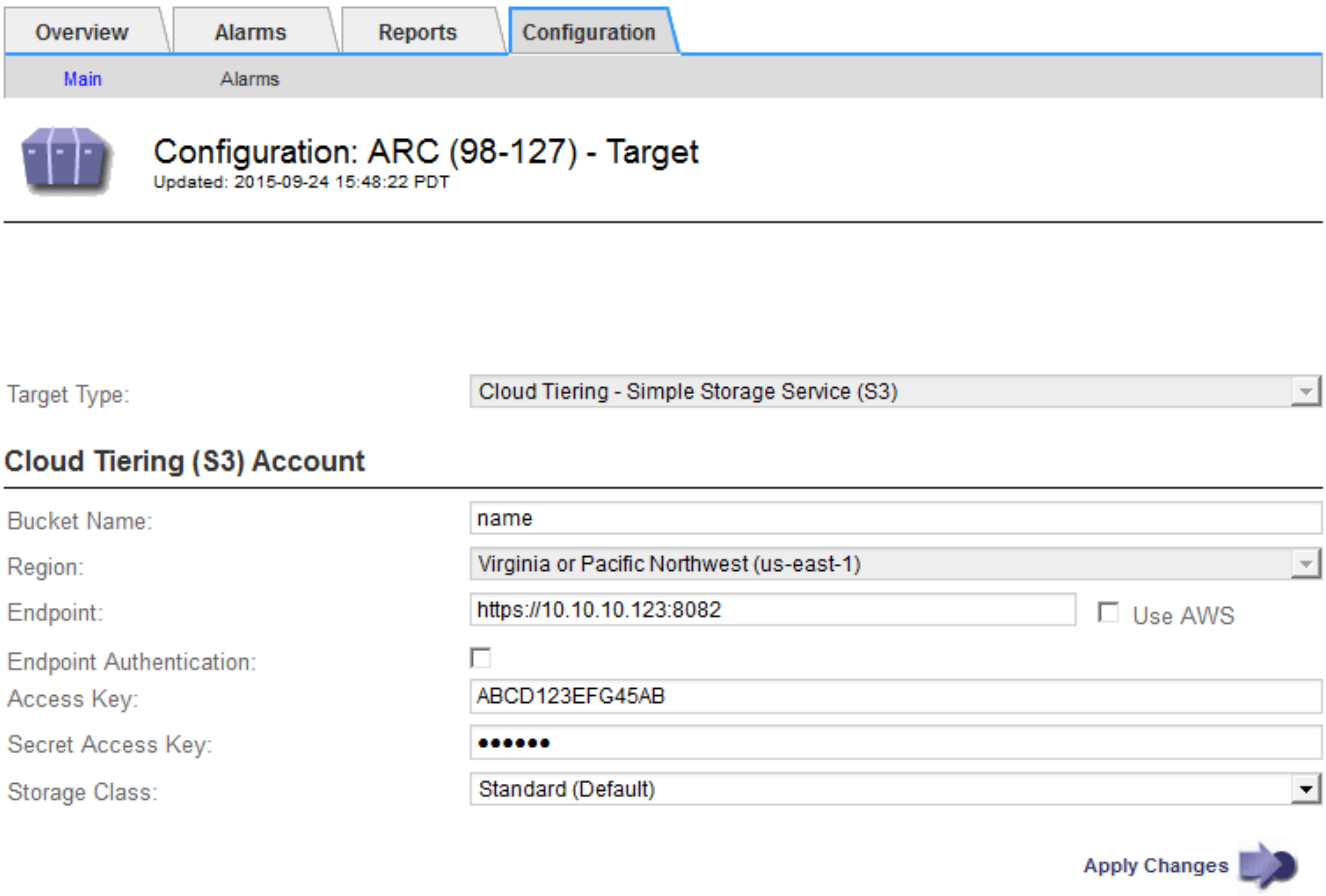
Se stai utilizzando un nodo di archiviazione con l'opzione **Cloud Tiering - Simple Storage Service (S3)**, prendi in considerazione la migrazione degli oggetti a un pool di storage cloud. Vedere Gestire gli oggetti con ILM.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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 sul 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 configurata, la destinazione non può essere modificata.

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.

Di cosa hai bisogno

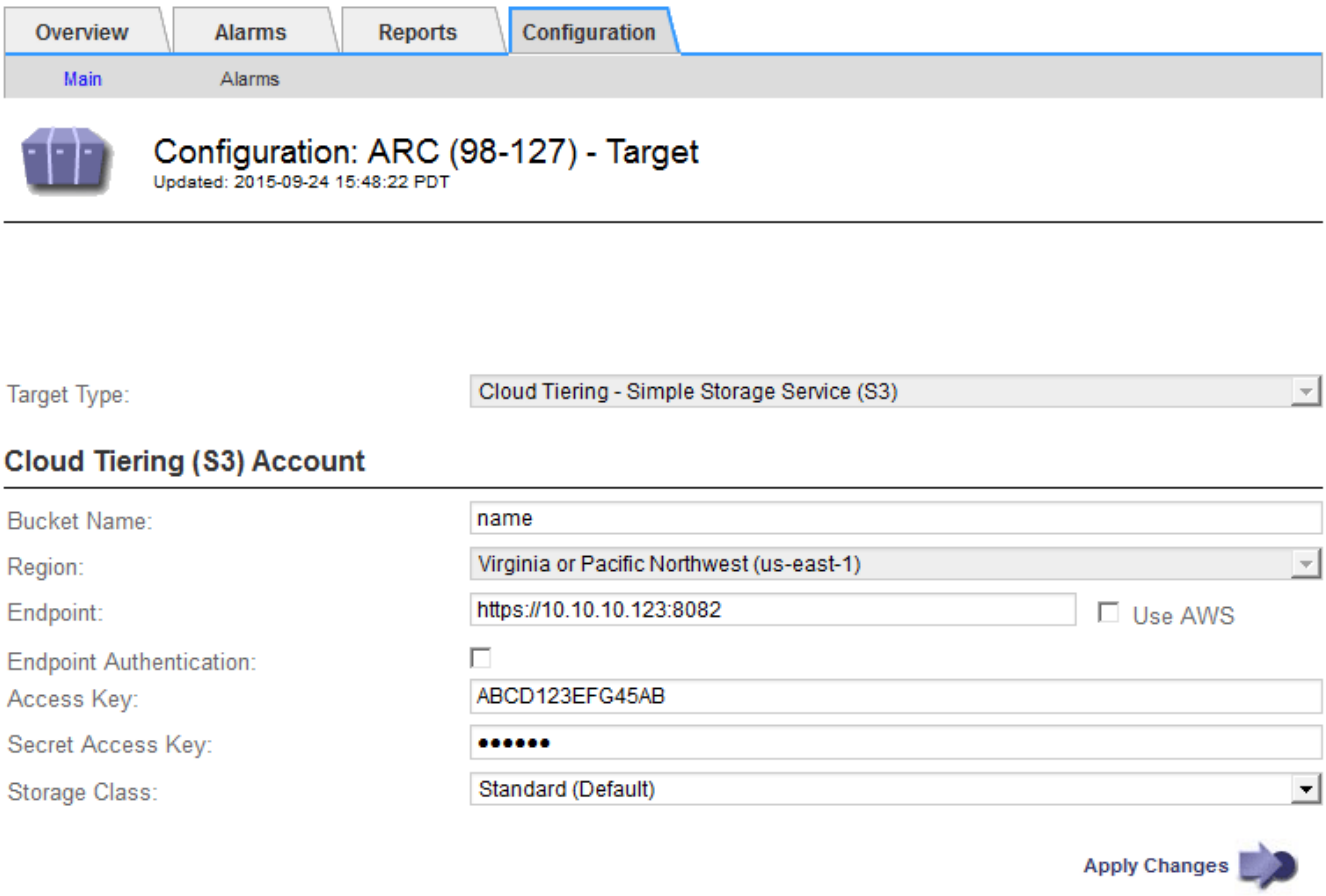
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

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.

Di cosa hai bisogno

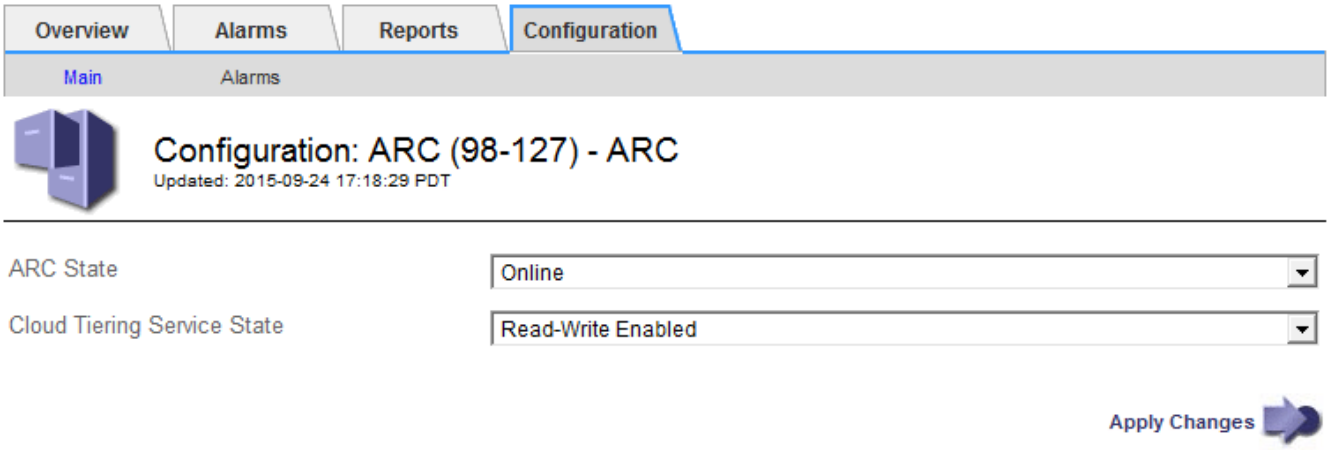
- È necessario accedere a Grid Manager utilizzando un browser web supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Il nodo di archiviazione deve essere configurato.

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

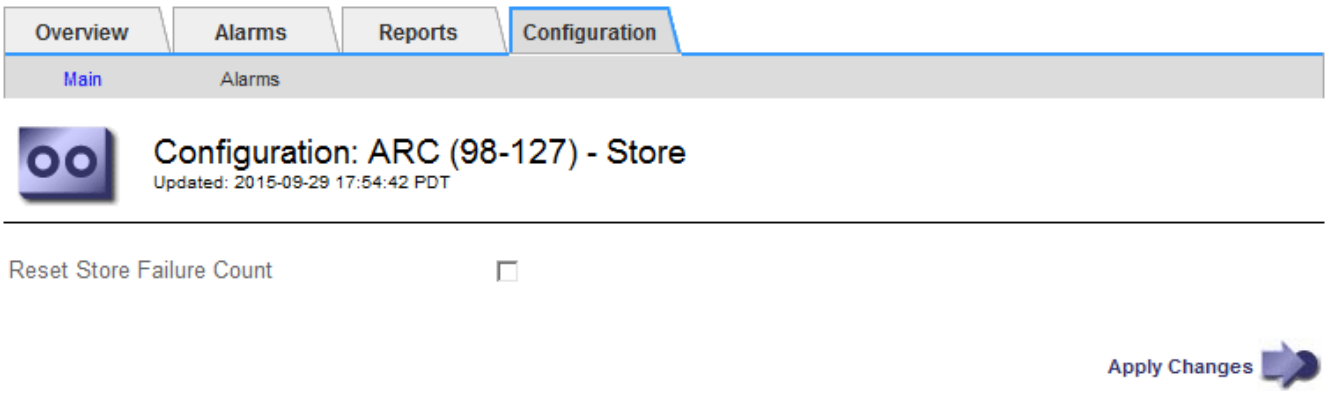
Se il nodo di archiviazione si connette a un sistema di storage di archiviazione tramite l'API S3, è possibile reimpostare il numero di errori di archiviazione, che può essere utilizzato per cancellare l'allarme ARVF (Store Failures).

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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 stai utilizzando la funzionalità **Cloud Tiering - Simple Storage Service (S3)** per tierare i dati degli oggetti in un bucket S3, prendi in considerazione la migrazione degli 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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 nel criterio ILM attivo 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.

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.

Di cosa hai bisogno

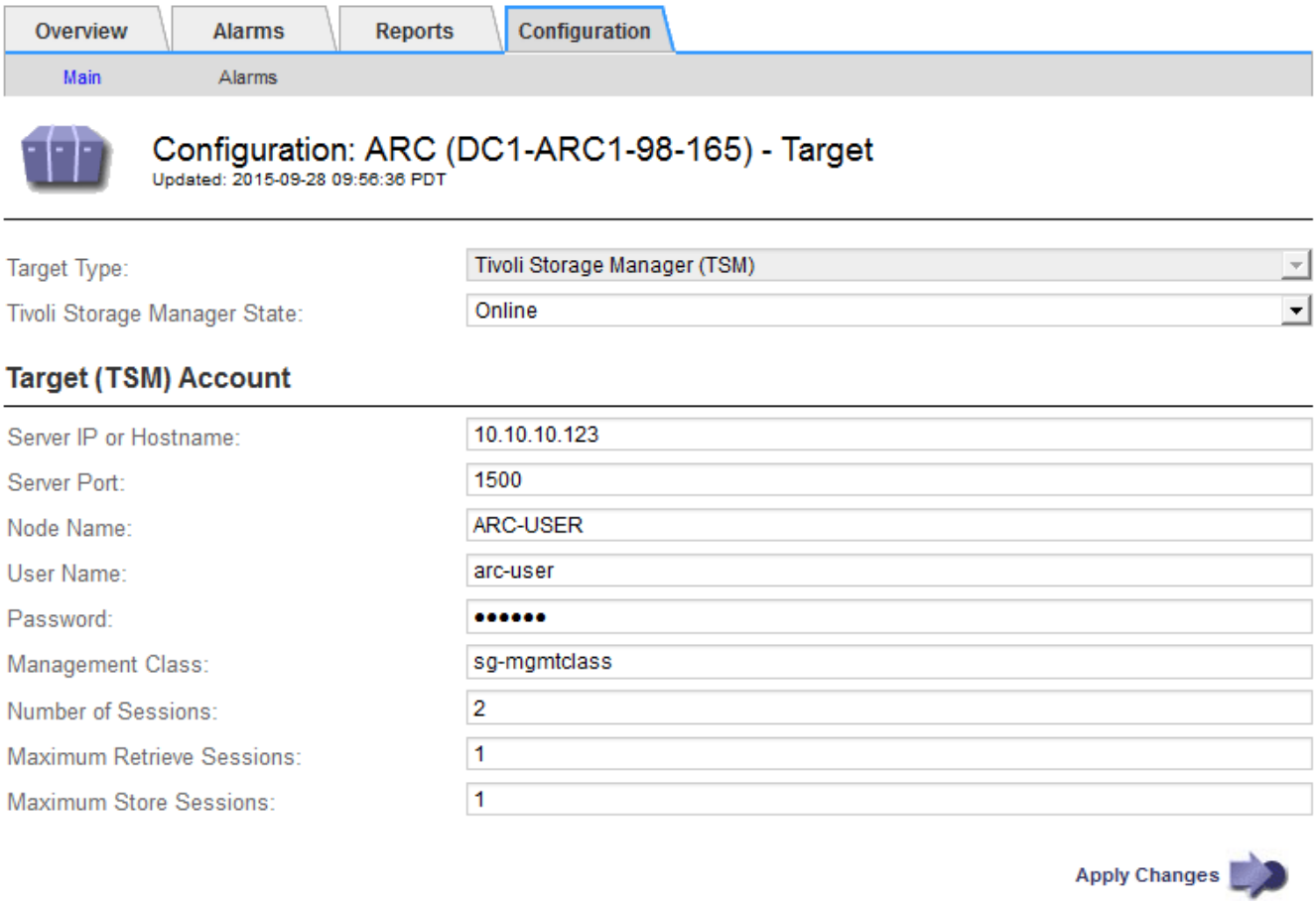
- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

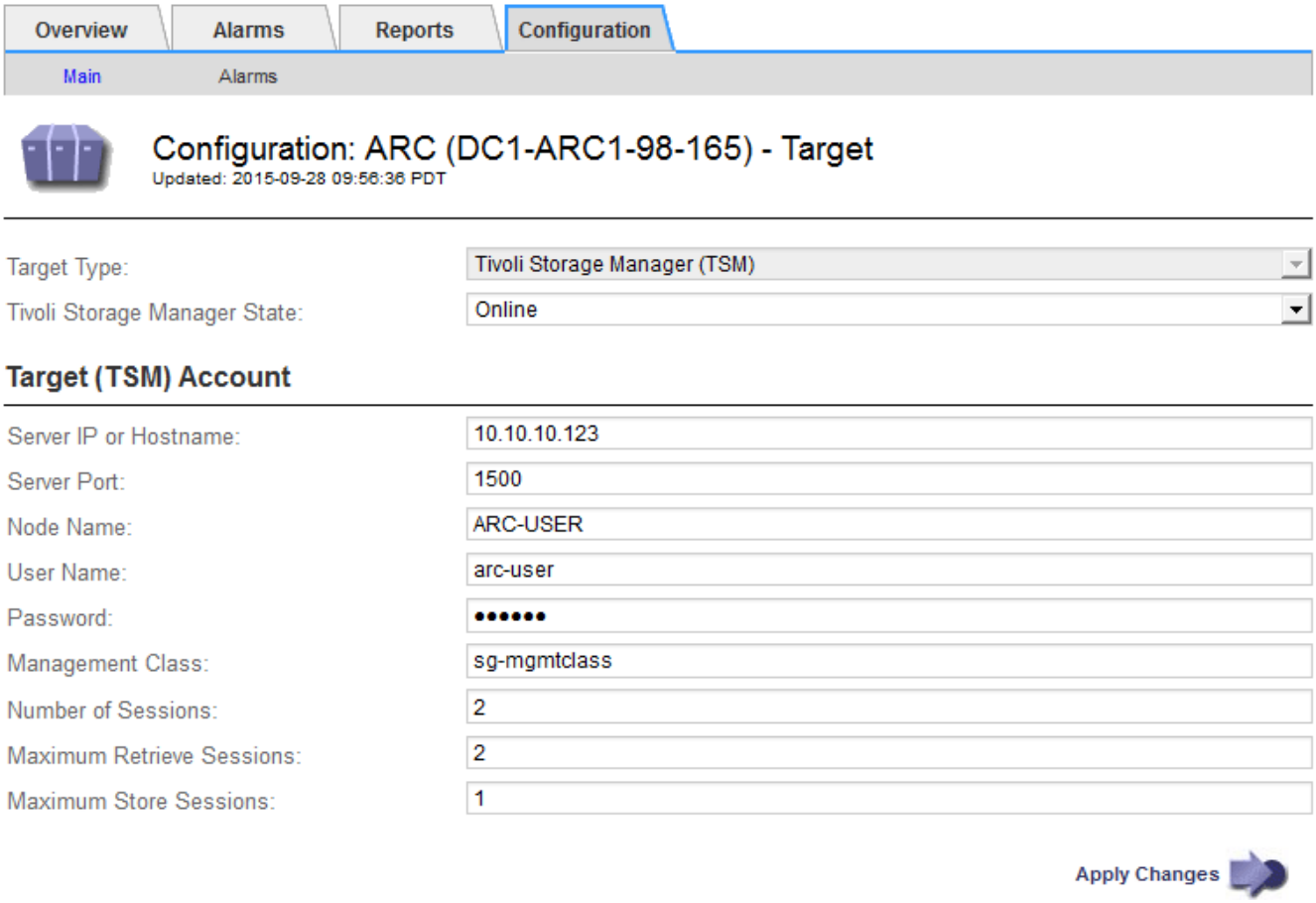
A proposito di questa attività

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

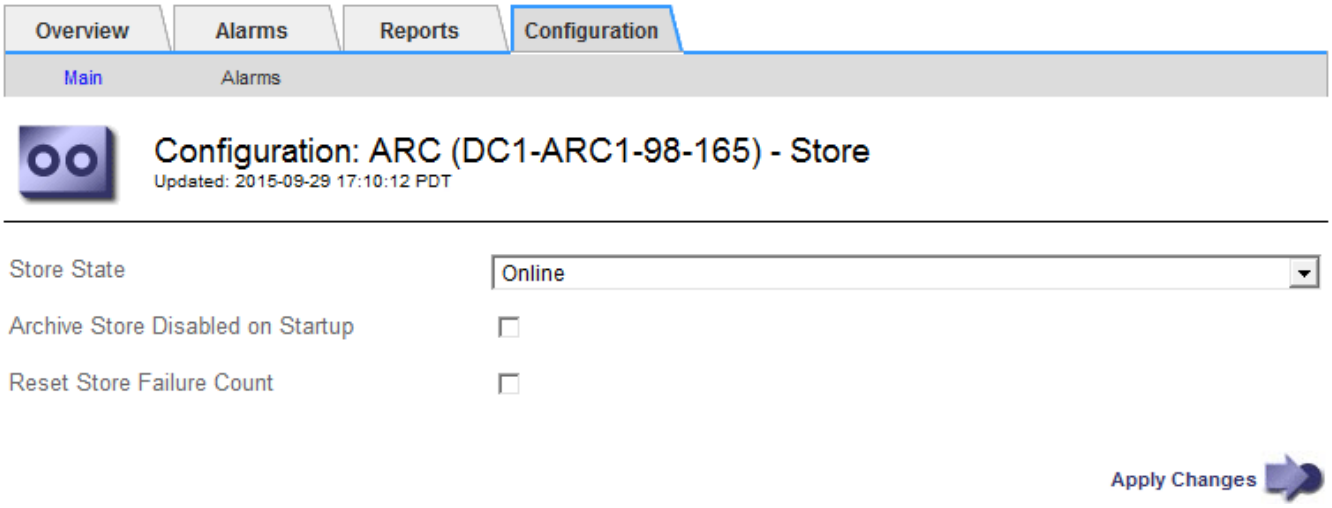
Se il nodo di archiviazione si connette a un server middleware TSM, è possibile configurare lo stato dell'archivio di un nodo di archiviazione su Online o Offline. È inoltre possibile disattivare l'archivio al primo avvio del nodo di archiviazione o ripristinare il conteggio degli errori rilevati per l'allarme associato.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di autorizzazioni di accesso specifiche.

A proposito di questa attività

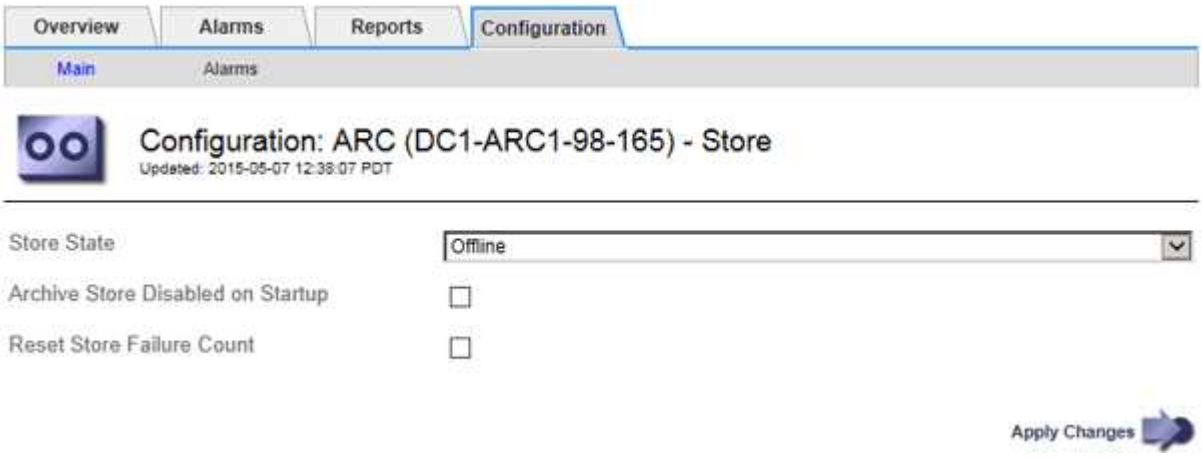
Il nodo di archiviazione continua ad accettare i dati dell'oggetto per il trasferimento al server TSM dopo che il server TSM ha interrotto l'accettazione del nuovo contenuto. Questo contenuto non può essere scritto su supporti gestiti dal server TSM. In questo caso, viene attivato un allarme.

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

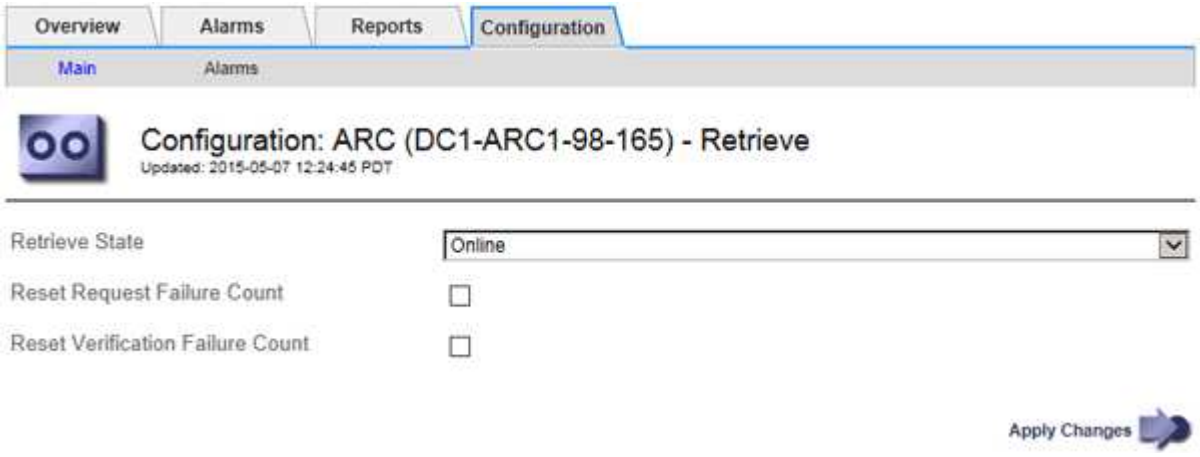
impostare lo stato su Online o Offline, oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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 per gli errori della 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

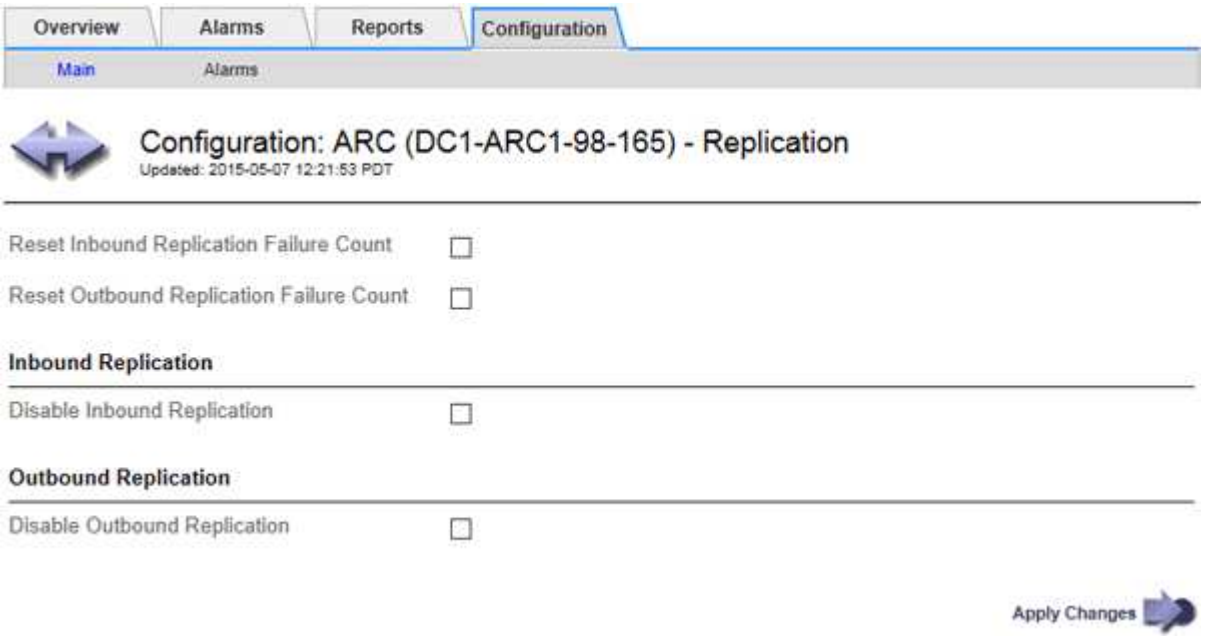
È possibile configurare le impostazioni di replica per un nodo di archiviazione e disattivare la replica in entrata e in uscita oppure reimpostare i conteggi degli errori rilevati per gli allarmi associati.

Di cosa hai bisogno

- Hai effettuato l'accesso a Grid Manager utilizzando un browser web supportato.
- Si dispone di 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. Vedere Monitorare e risolvere i problemi.

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, le copie vengono eseguite in tutte le posizioni richieste, inclusi i nodi di archiviazione, in base alle regole di gestione del ciclo di vita delle informazioni (ILM) 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 la preparazione di un server TSM seguendo le Best practice del 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 una serie di 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 dsmacmc 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 storage 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, “Disk storage pool for the Archive Node.”
   - *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 Configuration Main Maximum Store Sessions** 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 Configuration Main Number of Sessions** in 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` La policy di dominio è una versione modificata della policy di dominio "standard", configurata per la scrittura su nastro e con la destinazione dell'archivio impostata come pool di storage 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 "no backup copy group" visualizzato quando si immette il comando Activate.

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.

La sezione seguente è una guida alla comprensione e alla pianificazione di 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 (come il nastro), assicurarsi che lo storage del nodo di archiviazione disponga di 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. Monitorare e risolvere i problemi.

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.

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 di questo capitolo 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 assicurarsi che i vari 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 di 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.