Gestire gli inquilini

StorageGRID software

NetApp
December 03, 2025

Sommario

Gestire gli inquilini

Cosa sono i conti degli inquilini?

Un account tenant consente di utilizzare l'API REST Simple Storage Service (S3) per archiviare e recuperare oggetti in un sistema StorageGRID .

I dettagli su Swift sono stati rimossi da questa versione del sito di documentazione. Vedere "StorageGRID 11.8: Gestisci i tenant" .

In qualità di amministratore della griglia, crei e gestisci gli account tenant che i client S3 utilizzano per archiviare e recuperare gli oggetti.

Ogni account tenant ha gruppi, utenti, bucket S3 e oggetti federati o locali.

Gli account tenant possono essere utilizzati per separare gli oggetti archiviati da entità diverse. Ad esempio, è possibile utilizzare più account tenant per uno qualsiasi di questi casi d'uso:

- **Caso d'uso aziendale:** se si amministra un sistema StorageGRID in un'applicazione aziendale, potrebbe essere opportuno separare l'archiviazione degli oggetti della griglia in base ai diversi reparti dell'organizzazione. In questo caso, potresti creare account tenant per il reparto Marketing, il reparto Assistenza Clienti, il reparto Risorse Umane e così via.

  Se si utilizza il protocollo client S3, è possibile utilizzare bucket S3 e policy di bucket per separare gli oggetti tra i reparti di un'azienda. Non è necessario utilizzare account tenant. Vedi le istruzioni per l'implementazione"Bucket S3 e policy dei bucket" per maggiori informazioni.

- **Caso d'uso del fornitore di servizi:** se si amministra un sistema StorageGRID come fornitore di servizi, è possibile separare l'archiviazione degli oggetti della griglia in base alle diverse entità che prenderanno in leasing l'archiviazione sulla griglia. In questo caso, dovresti creare account tenant per la Società A, la Società B, la Società C e così via.

Per ulteriori informazioni, consultare "Utilizzare un account tenant" .

Come posso creare un account tenant?

Utilizzare Grid Manager per creare un account tenant. Quando si crea un account tenant, si specificano le seguenti informazioni:

- Informazioni di base, tra cui il nome del tenant, il tipo di client (S3) e la quota di archiviazione facoltativa.
- Autorizzazioni per l'account tenant, ad esempio se l'account tenant può utilizzare i servizi della piattaforma S3, configurare la propria origine identità, utilizzare S3 Select o utilizzare una connessione di federazione di griglia.
- L'accesso root iniziale per il tenant, a seconda che il sistema StorageGRID utilizzi gruppi e utenti locali, federazione delle identità o Single Sign-On (SSO).

Inoltre, è possibile abilitare l'impostazione S3 Object Lock per il sistema StorageGRID se gli account tenant S3 devono essere conformi ai requisiti normativi. Quando S3 Object Lock è abilitato, tutti gli account tenant S3 possono creare e gestire bucket conformi.

A cosa serve Tenant Manager?

Dopo aver creato l'account tenant, gli utenti tenant possono accedere a Tenant Manager per eseguire attività come le seguenti:

- Impostare la federazione delle identità (a meno che l'origine dell'identità non sia condivisa con la griglia)
- Gestisci gruppi e utenti
- Utilizzare la federazione di griglia per la clonazione degli account e la replica tra griglie
- Gestisci le chiavi di accesso S3
- Crea e gestisci bucket S3
- Utilizzare i servizi della piattaforma S3
- Utilizzare S3 Select
- Monitorare l'utilizzo dello spazio di archiviazione

Mentre gli utenti tenant S3 possono creare e gestire bucket e chiavi di accesso S3 con Tenant Manager, devono utilizzare un'applicazione client S3 per acquisire e gestire gli oggetti. Vedere"Utilizzare l'API REST S3" per i dettagli.

Crea un account inquilino

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

I passaggi per la creazione di un account tenant variano a seconda che"federazione di identità" E"accesso unico" sono configurati e se l'account Grid Manager utilizzato per creare l'account tenant appartiene a un gruppo di amministratori con autorizzazione di accesso Root.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Accesso root o autorizzazione account tenant" .
- Se l'account tenant utilizzerà l'origine identità configurata per Grid Manager e si desidera concedere l'autorizzazione di accesso Root per l'account tenant a un gruppo federato, è stato importato tale gruppo federato in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Vedere "Gestisci gruppi di amministratori" .
- Se si desidera consentire a un tenant S3 di clonare i dati dell'account e replicare gli oggetti bucket su un'altra griglia utilizzando una connessione di federazione della griglia:
  - Hai"configurato la connessione della federazione di griglia" .
  - Lo stato della connessione è **Connesso**.
  - Hai i permessi di accesso Root.
  - Hai esaminato le considerazioni per"gestione degli inquilini autorizzati per la federazione della rete" .
  - Se l'account tenant utilizzerà l'origine identità configurata per Grid Manager, significa che hai importato lo stesso gruppo federato in Grid Manager su entrambe le griglie.

    Quando si crea il tenant, si selezionerà questo gruppo per avere l'autorizzazione di accesso Root iniziale sia per l'account tenant di origine che per quello di destinazione.

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

Accedi alla procedura guidata

Passi

1. Selezionare **INQUILINI**.
2. Seleziona **Crea**.

Inserisci i dettagli

Passi

1. Inserisci i dettagli dell'inquilino.

Campo	Descrizione
Nome	Un nome per l'account dell'inquilino. I nomi degli inquilini non devono essere univoci. Quando viene creato l'account tenant, questo riceve un ID account univoco di 20 cifre.
Descrizione (facoltativa)	Una descrizione che aiuti a identificare l'inquilino. Se si sta creando un tenant che utilizzerà una connessione di federazione di griglia, è possibile utilizzare questo campo per identificare il tenant di origine e quello di destinazione. Ad esempio, questa descrizione per un tenant creato sulla Griglia 1 apparirà anche per il tenant replicato sulla Griglia 2: "Questo tenant è stato creato sulla Griglia 1".
Tipo di cliente	Il tipo di protocollo client che questo tenant utilizzerà, **S3** o **Swift**. **Nota**: il supporto per le applicazioni client Swift è stato deprecato e verrà rimosso in una versione futura.
Quota di archiviazione (facoltativa)	Se si desidera che questo tenant disponga di una quota di archiviazione, specificare un valore numerico per la quota e le unità.

2. Selezionare **Continua**.

Seleziona autorizzazioni

Passi

1. Facoltativamente, seleziona le autorizzazioni di base che desideri assegnare a questo tenant.

Alcune di queste autorizzazioni prevedono requisiti aggiuntivi. Per maggiori dettagli, seleziona l'icona della guida per ogni autorizzazione.

Permesso	Se selezionato…
Consenti i servizi della piattaforma	Il tenant può utilizzare i servizi della piattaforma S3 come CloudMirror. Vedere "Gestire i servizi della piattaforma per gli account tenant S3" .
Utilizzare la propria fonte di identità	Il tenant può configurare e gestire la propria fonte di identità per gruppi e utenti federati. Questa opzione è disabilitata se hai"SSO configurato" per il tuo sistema StorageGRID .
Consenti selezione S3	Il tenant può inviare richieste API S3 SelectObjectContent per filtrare e recuperare i dati degli oggetti. Vedere "Gestisci S3 Select per gli account tenant" . **Importante**: le richieste SelectObjectContent possono ridurre le prestazioni del bilanciatore del carico per tutti i client S3 e tutti i tenant. Abilitare questa funzionalità solo quando necessario e solo per i tenant attendibili.

2. Facoltativamente, seleziona le autorizzazioni avanzate che desideri assegnare a questo tenant.

Permesso	Se selezionato…
Collegamento della federazione di rete	L'inquilino può utilizzare una connessione di federazione di rete, che: • Fa sì che questo tenant e tutti i gruppi e gli utenti tenant aggiunti all'account vengano clonati da questa griglia (la *griglia di origine*) all'altra griglia nella connessione selezionata (la *griglia di destinazione*). • Consente a questo tenant di configurare la replica tra griglie tra i bucket corrispondenti su ciascuna griglia. Vedere "Gestire gli inquilini autorizzati per la federazione della rete" .
Blocco oggetto S3	Consentire al tenant di utilizzare funzionalità specifiche di S3 Object Lock: • **Imposta periodo massimo di conservazione** definisce per quanto tempo i nuovi oggetti aggiunti a questo bucket devono essere conservati, a partire dal momento in cui vengono acquisiti. • **Consenti modalità di conformità** impedisce agli utenti di sovrascrivere o eliminare versioni di oggetti protetti durante il periodo di conservazione.

3. Selezionare **Continua**.

Definisci l'accesso root e crea il tenant

Passi

1. Definisci l'accesso root per l'account tenant, a seconda che il tuo sistema StorageGRID utilizzi la federazione delle identità, il Single Sign-On (SSO) o entrambi.

Opzione	Fai questo
Se la federazione delle identità non è abilitata	Specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se la federazione delle identità è abilitata	a. Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. b. Facoltativamente, specificare la password da utilizzare quando si accede al tenant come utente root locale.
Se sono abilitati sia la federazione delle identità che il Single Sign-On (SSO)	Selezionare un gruppo federato esistente per ottenere l'autorizzazione di accesso Root per il tenant. Nessun utente locale può effettuare l'accesso.

2. Selezionare **Crea tenant**.

   Viene visualizzato un messaggio di conferma e il nuovo inquilino viene elencato nella pagina Inquilini. Per informazioni su come visualizzare i dettagli degli inquilini e monitorarne l'attività, vedere"Monitorare l'attività degli inquilini" .

   > L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

3. Se hai selezionato l'autorizzazione **Usa connessione federata alla griglia** per il tenant:
   a. Verificare che un tenant identico sia stato replicato sull'altra griglia nella connessione. Gli inquilini su entrambe le griglie avranno lo stesso ID account di 20 cifre, nome, descrizione, quota e autorizzazioni.

      > Se viene visualizzato il messaggio di errore "Tenant creato senza un clone", fare riferimento alle istruzioni in"Risolvere gli errori di federazione della griglia" .

   b. Se hai fornito una password utente root locale quando hai definito l'accesso root,"cambiare la password per l'utente root locale" per l'inquilino replicato.

      > Un utente root locale non può accedere a Tenant Manager sulla griglia di destinazione finché non viene modificata la password.

Sign in al tenant (facoltativo)

Se necessario, puoi accedere subito al nuovo tenant per completare la configurazione oppure puoi accedere al tenant in un secondo momento. I passaggi per l'accesso variano a seconda che tu abbia effettuato l'accesso a Grid Manager tramite la porta predefinita (443) o una porta con restrizioni. Vedere "Controllare l'accesso al firewall esterno" .

Sign in ora

Se stai utilizzando…	Fai questo…
Porta 443 e si imposta una password per l'utente root locale	1. Seleziona * Sign in come root*. Quando effettui l'accesso, vengono visualizzati i link per configurare bucket, federazione delle identità, gruppi e utenti. 2. Selezionare i link per configurare l'account tenant. Ogni collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, vedere il"istruzioni per l'utilizzo degli account degli inquilini" .
Porta 443 e non hai impostato una password per l'utente root locale	Selezionare * Sign in* e immettere le credenziali di un utente nel gruppo federato con accesso root.
Un porto limitato	1. Seleziona **Fine** 2. Selezionare **Limitato** nella tabella Tenant per saperne di più sull'accesso a questo account tenant. L'URL per Tenant Manager ha questo formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `*port*`è la porta riservata al tenant ◦ `*20-digit-account-id*`è l'ID account univoco del tenant

Sign in più tardi

Se stai utilizzando…	Fai una di queste cose…
Porta 443	• Da Grid Manager, seleziona **TENANT** e seleziona * Sign in* a destra del nome del tenant. • Inserisci l'URL del tenant in un browser web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ `*FQDN_or_Admin_Node_IP*`è un nome di dominio completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `*20-digit-account-id*`è l'ID account univoco del tenant

Se stai utilizzando…	Fai una di queste cose…
Un porto limitato	• Da Grid Manager, seleziona **TENANTS** e seleziona **Restricted**. • Inserisci 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 completamente qualificato o l'indirizzo IP di un nodo di amministrazione ◦ `*port*` è la porta riservata solo al tenant ◦ `*20-digit-account-id*` è l'ID account univoco del tenant

Configurare il tenant

Seguire le istruzioni in"Utilizzare un account tenant" per gestire gruppi di tenant e utenti, chiavi di accesso S3, bucket, servizi di piattaforma, clonazione di account e replica tra griglie.

Modifica account inquilino

È possibile modificare un account tenant per cambiare il nome visualizzato, la quota di archiviazione o le autorizzazioni del tenant.

Se un tenant dispone dell'autorizzazione **Usa connessione federazione griglia**, è possibile modificare i dettagli del tenant da entrambe le griglie nella connessione. Tuttavia, tutte le modifiche apportate a una griglia nella connessione non verranno copiate nell'altra griglia. Se si desidera che i dettagli degli inquilini siano perfettamente sincronizzati tra le griglie, apportare le stesse modifiche su entrambe le griglie. Vedere "Gestire gli inquilini autorizzati per la connessione alla federazione di rete" .

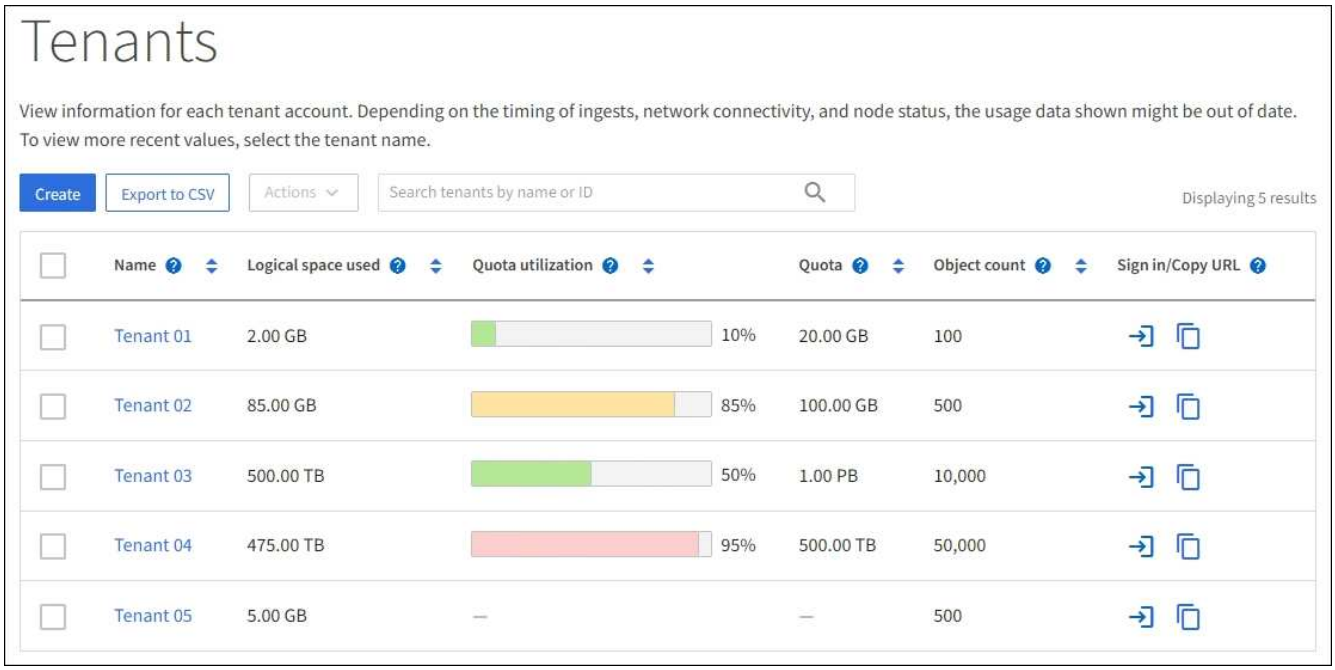
Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Accesso root o autorizzazione account tenant" .

L'applicazione delle impostazioni del tenant sulla griglia potrebbe richiedere 15 minuti o più, a seconda della connettività di rete, dello stato del nodo e delle operazioni di Cassandra.

Passi

1. Selezionare **INQUILINI**.



2. Individua l'account tenant che desideri modificare.

   Utilizzare la casella di ricerca per cercare un inquilino per nome o ID inquilino.

3. Selezionare l'inquilino. Puoi procedere in uno dei seguenti modi:
   - Selezionare la casella di controllo per il tenant e selezionare **Azioni** > **Modifica**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli e selezionare **Modifica**.
4. Facoltativamente, modifica i valori per questi campi:
   - **Nome**
   - **Descrizione**
   - **Quota di archiviazione**
5. Selezionare **Continua**.
6. Selezionare o deselezionare le autorizzazioni per l'account tenant.
   - Se disabiliti i **Servizi di piattaforma** per un tenant che li sta già utilizzando, i servizi che ha configurato per i suoi bucket S3 smetteranno di funzionare. Non viene inviato alcun messaggio di errore al tenant. Ad esempio, se il tenant ha configurato la replica CloudMirror per un bucket S3, può comunque archiviare oggetti nel bucket, ma le copie di tali oggetti non verranno più create nel bucket S3 esterno che ha configurato come endpoint. Vedere "Gestire i servizi della piattaforma per gli account tenant S3" .
   - Modificare l'impostazione **Usa la propria origine identità** per determinare se l'account tenant utilizzerà la propria origine identità o l'origine identità configurata per Grid Manager.

     Se **Utilizza la propria fonte di identità** è:

     - Disabilitato e selezionato, il tenant ha già abilitato la propria fonte di identità. Un tenant deve disabilitare la propria origine identità prima di poter utilizzare l'origine identità configurata per Grid Manager.
     - Disabilitato e non selezionato, SSO è abilitato per il sistema StorageGRID . Il tenant deve utilizzare l'origine identità configurata per Grid Manager.

- Selezionare o deselezionare l'autorizzazione **Consenti selezione S3** in base alle esigenze. Vedere "Gestisci S3 Select per gli account tenant" .
- Per rimuovere l'autorizzazione **Usa connessione federazione griglia**:
  i. Selezionare la scheda **Federazione di griglia**.
  ii. Seleziona **Rimuovi autorizzazione**.
- Per aggiungere l'autorizzazione **Usa connessione federata griglia**:
  i. Selezionare la scheda **Federazione di griglia**.
  ii. Selezionare la casella di controllo **Usa connessione federata alla griglia**.
  iii. Facoltativamente, seleziona **Clona utenti e gruppi locali esistenti** per clonarli nella griglia remota. Se lo desideri, puoi interrompere la clonazione in corso o riprovare se alcuni utenti o gruppi locali non sono riusciti a essere clonati dopo il completamento dell'ultima operazione di clonazione.
- Per impostare un periodo di conservazione massimo o consentire la modalità di conformità:

> Prima di poter utilizzare queste impostazioni, è necessario abilitare il blocco oggetti S3 sulla griglia.

  i. Selezionare la scheda **Blocco oggetto S3**.
  ii. Per **Imposta periodo massimo di conservazione**, immettere un valore e selezionare il periodo di tempo dal menu a discesa.
  iii. Per **Consenti modalità conformità**, seleziona la casella di controllo.

Cambia la password per l'utente root locale del tenant

Potrebbe essere necessario modificare la password per l'utente root locale di un tenant se l'utente root è bloccato fuori dall'account.

Prima di iniziare

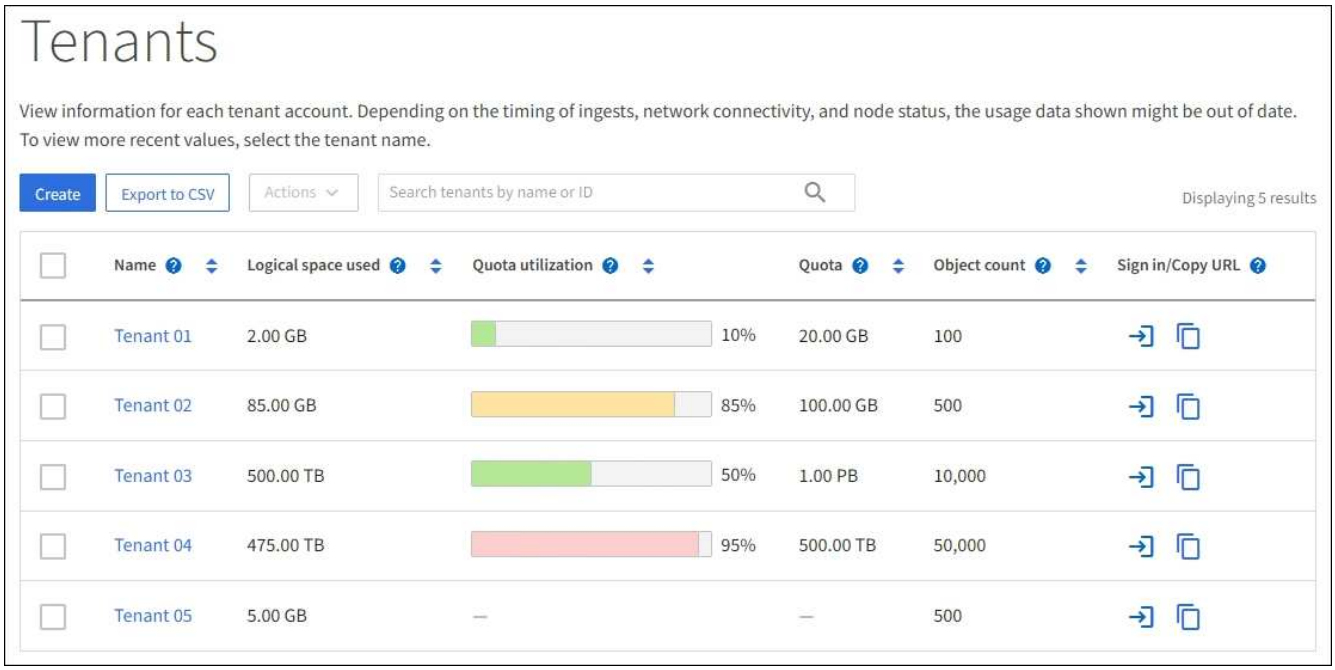
- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .

Informazioni su questo compito

Se per il sistema StorageGRID è abilitato l'accesso Single Sign-On (SSO), l'utente root locale non può accedere all'account tenant. Per eseguire attività come utente root, gli utenti devono appartenere a un gruppo federato che dispone dell'autorizzazione di accesso root per il tenant.

Passi

1. Selezionare **INQUILINI**.



2. Selezionare l'account dell'inquilino. Puoi procedere in uno dei seguenti modi:
   - Selezionare la casella di controllo per il tenant e selezionare **Azioni** > **Cambia password di root**.
   - Selezionare il nome del tenant per visualizzare la pagina dei dettagli e selezionare **Azioni** > **Modifica password root**.
3. Inserisci la nuova password per l'account tenant.
4. Seleziona **Salva**.

Elimina account inquilino

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

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Sono stati rimossi tutti i bucket e gli oggetti S3 associati all'account tenant.
- Se all'inquilino è consentito utilizzare una connessione di federazione di rete, hai esaminato le considerazioni per"eliminazione di un tenant con l'autorizzazione Usa connessione federazione griglia" .

Passi

1. Selezionare **INQUILINI**.
2. Individua l'account o gli account tenant che desideri eliminare.

   Utilizzare la casella di ricerca per cercare un inquilino per nome o ID inquilino.

3. Per eliminare più tenant, seleziona le caselle di controllo e seleziona **Azioni** > **Elimina**.
4. Per eliminare un singolo tenant, procedere in uno dei seguenti modi:
   - Selezionare la casella di controllo e selezionare **Azioni** > **Elimina**.

- Selezionare il nome del tenant per visualizzare la pagina dei dettagli, quindi selezionare **Azioni** > **Elimina**.

5. Selezionare **Sì**.

Gestire i servizi della piattaforma

Cosa sono i servizi di piattaforma?

I servizi della piattaforma includono la replica CloudMirror, le notifiche degli eventi e il servizio di integrazione della ricerca.

Se si abilitano i servizi della piattaforma per gli account tenant S3, è necessario configurare la griglia in modo che i tenant possano accedere alle risorse esterne necessarie per utilizzare questi servizi.

Replica CloudMirror

Il servizio di replica StorageGRID CloudMirror viene utilizzato per eseguire il mirroring di oggetti specifici da un bucket StorageGRID a una destinazione esterna specificata.

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

> La replica di CloudMirror presenta alcune importanti somiglianze e differenze con la funzionalità di replica tra griglie. Per saperne di più, vedere"Confronta la replicazione cross-grid e la replicazione CloudMirror" .

> La replica CloudMirror non è supportata se nel bucket di origine è abilitato S3 Object Lock.

Notifiche

Le notifiche degli eventi per bucket vengono utilizzate per inviare notifiche su azioni specifiche eseguite sugli oggetti a un cluster Kafka esterno specificato o ad Amazon Simple Notification Service.

Ad esempio, è possibile configurare l'invio di avvisi agli amministratori per ogni oggetto aggiunto a un bucket, dove gli oggetti rappresentano file di registro associati a un evento di sistema critico.

> Sebbene la notifica degli eventi possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Conserva fino alla data e Conservazione legale) degli oggetti non saranno inclusi nei messaggi di notifica.

Servizio di integrazione della ricerca

Il servizio di integrazione della ricerca viene utilizzato per inviare metadati di oggetti S3 a un indice Elasticsearch specificato, dove è possibile ricercare o analizzare i metadati utilizzando il servizio esterno.

Ad esempio, puoi configurare i tuoi bucket per inviare metadati di oggetti S3 a un servizio Elasticsearch remoto. Potresti quindi utilizzare Elasticsearch per effettuare ricerche tra i bucket e realizzare analisi sofisticate dei modelli presenti nei metadati degli oggetti.

Sebbene l'integrazione di Elasticsearch possa essere configurata su un bucket con S3 Object Lock abilitato, i metadati di S3 Object Lock (inclusi gli stati Retain Until Date e Legal Hold) degli oggetti non saranno inclusi nei messaggi di notifica.

I servizi della piattaforma offrono agli inquilini la possibilità di utilizzare risorse di archiviazione esterne, servizi di notifica e servizi di ricerca o analisi con i propri dati. Poiché la posizione di destinazione per i servizi della piattaforma è in genere esterna alla distribuzione StorageGRID , è necessario decidere se si desidera consentire ai tenant di utilizzare questi servizi. In tal caso, è necessario abilitare l'utilizzo dei servizi della piattaforma quando si creano o si modificano gli account tenant. È inoltre necessario configurare la rete in modo che i messaggi dei servizi della piattaforma generati dai tenant possano raggiungere le loro destinazioni.

Raccomandazioni per l'utilizzo dei servizi della piattaforma

Prima di utilizzare i servizi della piattaforma, tieni presente i seguenti consigli:

- Se in un bucket S3 del sistema StorageGRID sono abilitati sia il controllo delle versioni sia la replica CloudMirror, è necessario abilitare anche il controllo delle versioni del bucket S3 per l'endpoint di destinazione. Ciò consente alla replica CloudMirror di generare versioni di oggetti simili sull'endpoint.
- Non dovresti utilizzare più di 100 tenant attivi con richieste S3 che richiedono la replica, le notifiche e l'integrazione della ricerca di CloudMirror. Avere più di 100 tenant attivi può comportare prestazioni più lente del client S3.
- Le richieste a un endpoint che non possono essere completate verranno messe in coda fino a un massimo di 500.000 richieste. Questo limite è equamente ripartito tra gli inquilini attivi. Ai nuovi inquilini è consentito superare temporaneamente questo limite di 500.000 unità, in modo che i nuovi inquilini non vengano ingiustamente penalizzati.

Informazioni correlate

- "Gestire i servizi della piattaforma"
- "Configurare le impostazioni del proxy di archiviazione"
- "Monitorare StorageGRID"

Rete e porte per i servizi della piattaforma

Se si consente a un tenant S3 di utilizzare i servizi della piattaforma, è necessario configurare la rete per la griglia per garantire che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

È possibile abilitare i servizi della piattaforma per un account tenant S3 quando si crea o si aggiorna l'account tenant. Se i servizi della piattaforma sono abilitati, il tenant può creare endpoint che fungono da destinazione per la replica di CloudMirror, le notifiche degli eventi o i messaggi di integrazione della ricerca dai suoi bucket S3. Questi messaggi dei servizi di piattaforma vengono inviati dai nodi di archiviazione che eseguono il servizio ADC agli endpoint di destinazione.

Ad esempio, i tenant potrebbero configurare i seguenti tipi di endpoint di destinazione:

- Un cluster Elasticsearch ospitato localmente
- Un'applicazione locale che supporta la ricezione di messaggi Amazon Simple Notification Service
- Un cluster Kafka ospitato localmente
- Un bucket S3 ospitato localmente sulla stessa o su un'altra istanza di StorageGRID

- Un endpoint esterno, ad esempio un endpoint su Amazon Web Services.

Per garantire che i messaggi dei servizi della piattaforma possano essere recapitati, è necessario configurare la rete o le reti contenenti i nodi di archiviazione ADC. È necessario assicurarsi che le seguenti porte possano essere utilizzate per inviare messaggi di servizi di piattaforma agli endpoint di destinazione.

Per impostazione predefinita, i messaggi dei servizi della piattaforma vengono inviati sulle seguenti porte:

- **80**: Per gli URI degli endpoint che iniziano con http (la maggior parte degli endpoint)
- **443**: Per gli URI degli endpoint che iniziano con https (la maggior parte degli endpoint)
- **9092**: Per gli URI degli endpoint che iniziano con http o https (solo endpoint Kafka)

Gli inquilini possono specificare una porta diversa quando creano o modificano un endpoint.

> Se si utilizza una distribuzione StorageGRID come destinazione per la replica di CloudMirror, i messaggi di replica potrebbero essere ricevuti su una porta diversa da 80 o 443. Assicurarsi che la porta utilizzata per S3 dalla distribuzione StorageGRID di destinazione sia specificata nell'endpoint.

Se si utilizza un server proxy non trasparente, è necessario anche"configurare le impostazioni del proxy di archiviazione" per consentire l'invio di messaggi a endpoint esterni, ad esempio un endpoint su Internet.

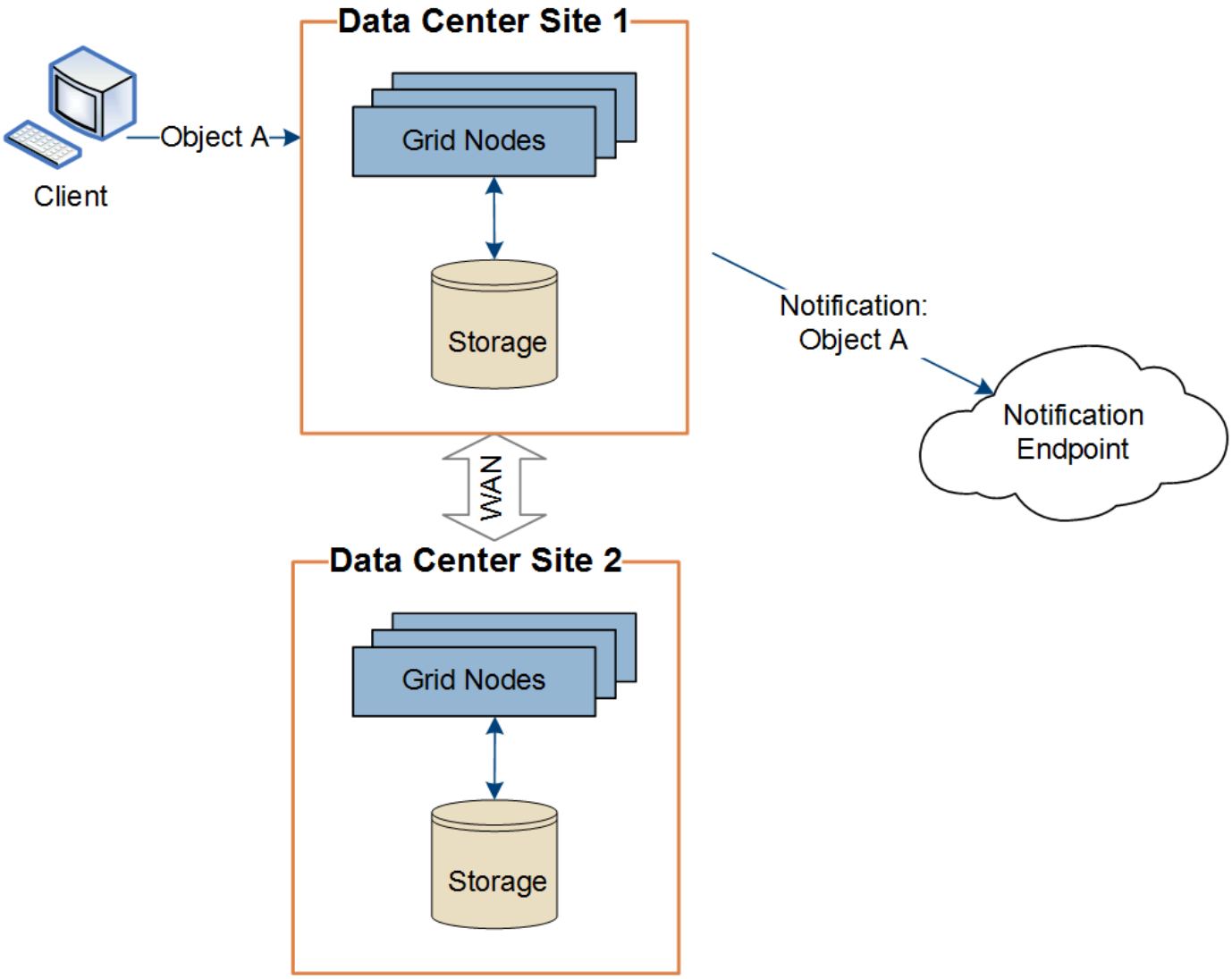
Informazioni correlate

"Utilizzare un account tenant"

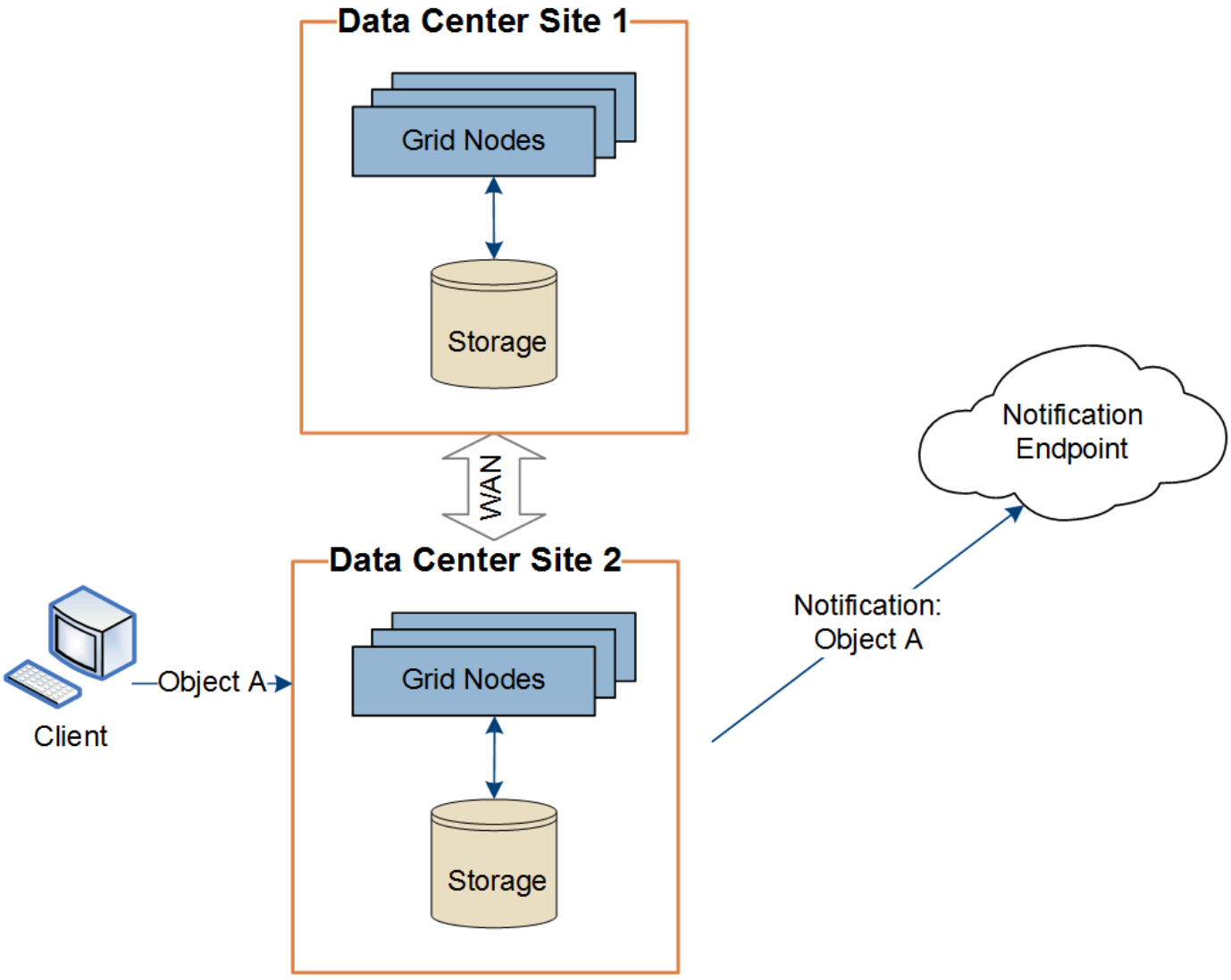
Consegna per sito di messaggi di servizi di piattaforma

Tutte le operazioni dei servizi della piattaforma vengono eseguite per ogni sito.

Ciò significa che se un tenant utilizza un client per eseguire un'operazione di creazione API S3 su un oggetto connettendosi a un nodo gateway nel sito del data center 1, la notifica relativa a tale azione viene attivata e inviata dal sito del data center 1.



Se successivamente il client esegue un'operazione di eliminazione dell'API S3 sullo stesso oggetto dal sito del Data Center 2, la notifica relativa all'azione di eliminazione viene attivata e inviata dal sito del Data Center 2.



Assicurarsi che la rete in ogni sito sia configurata in modo tale che i messaggi dei servizi della piattaforma possano essere recapitati alle rispettive destinazioni.

Risolvere i problemi dei servizi della piattaforma

Gli endpoint utilizzati nei servizi della piattaforma vengono creati e gestiti dagli utenti tenant in Tenant Manager; tuttavia, se un tenant riscontra problemi nella configurazione o nell'utilizzo dei servizi della piattaforma, è possibile utilizzare Grid Manager per risolvere il problema.

Problemi con i nuovi endpoint

Prima che un tenant possa utilizzare i servizi della piattaforma, deve creare uno o più endpoint utilizzando Tenant Manager. Ogni endpoint rappresenta una destinazione esterna per un servizio di piattaforma, ad esempio un bucket StorageGRID S3, un bucket Amazon Web Services, un argomento Amazon Simple Notification Service, un argomento Kafka o un cluster Elasticsearch ospitato localmente o su AWS. Ogni endpoint include sia la posizione della risorsa esterna sia le credenziali necessarie per accedere a tale risorsa.

Quando un tenant crea un endpoint, il sistema StorageGRID verifica che l'endpoint esista e che possa essere raggiunto utilizzando le credenziali specificate. La connessione all'endpoint viene convalidata da un nodo in

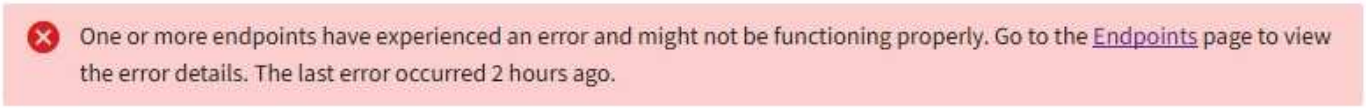
ogni sito.

Se la convalida dell'endpoint fallisce, un messaggio di errore ne spiega il motivo. L'utente tenant dovrebbe risolvere il problema, quindi provare a creare nuovamente l'endpoint.

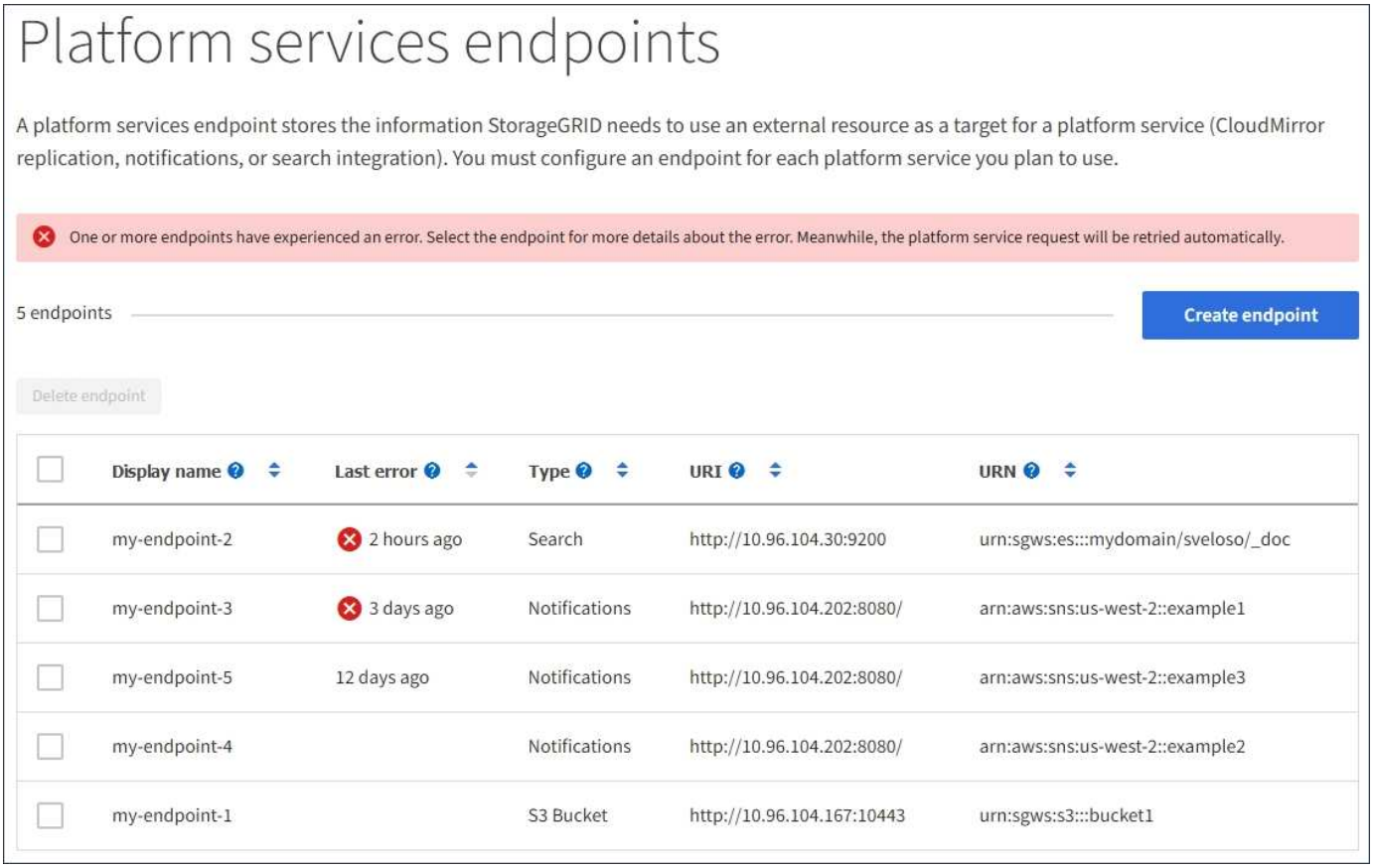
La creazione dell'endpoint non riuscirà se i servizi della piattaforma non sono abilitati per l'account tenant.

Problemi con gli endpoint esistenti

Se si verifica un errore quando StorageGRID tenta di raggiungere un endpoint esistente, viene visualizzato un messaggio nella dashboard di Tenant Manager.



Gli utenti tenant possono andare alla pagina Endpoint per esaminare il messaggio di errore più recente per ciascun endpoint e per determinare quanto tempo fa si è verificato l'errore. La colonna **Ultimo errore** visualizza il messaggio di errore più recente per ciascun endpoint e indica da quanto tempo si è verificato l'errore. Errori che includono il l'icona si è verificata negli ultimi 7 giorni.



Alcuni messaggi di errore nella colonna **Ultimo errore** potrebbero includere un logID tra parentesi. Un amministratore di rete o il supporto tecnico possono utilizzare questo ID per individuare informazioni più dettagliate sull'errore nel file bycast.log.

Problemi relativi ai server proxy

Se hai configurato un"proxy di archiviazione" tra i nodi di archiviazione e gli endpoint del servizio di piattaforma, potrebbero verificarsi errori se il servizio proxy non consente messaggi da StorageGRID. Per risolvere questi problemi, controlla le impostazioni del tuo server proxy per assicurarti che i messaggi relativi ai servizi della piattaforma non siano bloccati.

Determina se si è verificato un errore

Se si sono verificati errori dell'endpoint negli ultimi 7 giorni, la dashboard in Tenant Manager visualizza un messaggio di avviso. Puoi andare alla pagina Endpoint per vedere maggiori dettagli sull'errore.

Le operazioni del client falliscono

Alcuni problemi relativi ai servizi della piattaforma potrebbero causare il fallimento delle operazioni client sul bucket S3. Ad esempio, le operazioni del client S3 non riusciranno se il servizio RSM (Replicated State Machine) interno si arresta o se sono presenti troppi messaggi dei servizi della piattaforma in coda per la consegna.

Per verificare lo stato dei servizi:

1. Selezionare **SUPPORTO** > **Strumenti** > **Topologia griglia**.
2. Selezionare ***sito*** > ***Nodo di archiviazione*** > **SSM** > **Servizi**.

Errori di endpoint recuperabili e irrecuperabili

Dopo la creazione degli endpoint, possono verificarsi errori nella richiesta del servizio di piattaforma per vari motivi. Alcuni errori sono recuperabili con l'intervento dell'utente. Ad esempio, gli errori recuperabili potrebbero verificarsi per i seguenti motivi:

- Le credenziali dell'utente sono state eliminate o sono scadute.
- Il bucket di destinazione non esiste.
- La notifica non può essere recapitata.

Se StorageGRID riscontra un errore recuperabile, la richiesta del servizio di piattaforma verrà ripetuta finché non avrà esito positivo.

Altri errori non sono recuperabili. Ad esempio, se l'endpoint viene eliminato, si verifica un errore irrecuperabile.

Se StorageGRID riscontra un errore di endpoint irreversibile:

- In Grid Manager, vai su **Supporto** > **Strumenti** > **Metriche** > **Grafana** > **Panoramica dei servizi della piattaforma** per visualizzare i dettagli dell'errore.
- In Tenant Manager, vai su **STORAGE (S3)** > **Platform Services Endpoints** per visualizzare i dettagli dell'errore.
- Controlla il `/var/local/log/bycast-err.log` per errori correlati. I nodi di archiviazione dotati del servizio ADC contengono questo file di registro.

I messaggi dei servizi della piattaforma non possono essere recapitati

Se la destinazione riscontra un problema che le impedisce di accettare i messaggi dei servizi della piattaforma, l'operazione client sul bucket riesce, ma il messaggio dei servizi della piattaforma non viene recapitato. Ad esempio, questo errore potrebbe verificarsi se le credenziali vengono aggiornate sulla destinazione in modo

tale che StorageGRID non possa più autenticarsi al servizio di destinazione.

Controlla gli avvisi correlati.

Prestazioni più lente per le richieste di servizi della piattaforma

Il software StorageGRID potrebbe limitare le richieste S3 in arrivo per un bucket se la velocità con cui vengono inviate le richieste supera la velocità con cui l'endpoint di destinazione può riceverle. La limitazione si verifica solo quando è presente un arretrato di richieste in attesa di essere inviate all'endpoint di destinazione.

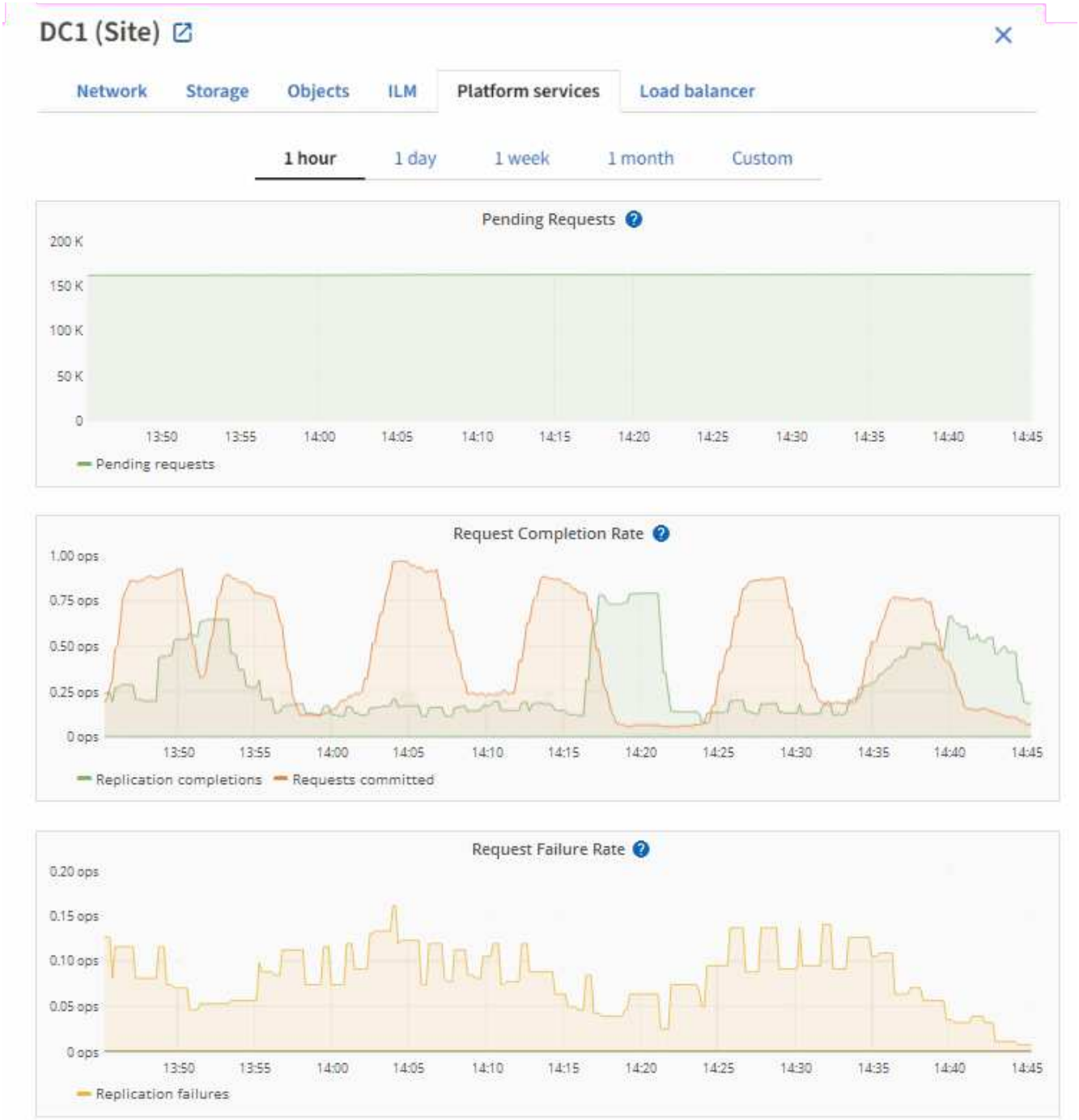
L'unico effetto visibile è che le richieste S3 in arrivo impiegheranno più tempo per essere eseguite. Se si inizia a rilevare un rallentamento significativo delle prestazioni, è opportuno ridurre la velocità di acquisizione o utilizzare un endpoint con capacità maggiore. Se l'arretrato di richieste continua ad aumentare, le operazioni S3 del client (come le richieste PUT) alla fine falliranno.

Le richieste CloudMirror hanno maggiori probabilità di essere influenzate dalle prestazioni dell'endpoint di destinazione, perché in genere comportano un trasferimento di dati maggiore rispetto alle richieste di integrazione della ricerca o di notifica degli eventi.

Le richieste di servizio della piattaforma falliscono

Per visualizzare il tasso di errore delle richieste per i servizi della piattaforma:

1. Selezionare **NODES**.
2. Seleziona ***site*** > **Servizi piattaforma**.
3. Visualizza il grafico del tasso di errore delle richieste.



Avviso di servizi di piattaforma non disponibili

L'avviso **Servizi di piattaforma non disponibili** indica che non è possibile eseguire alcuna operazione di servizio di piattaforma in un sito perché sono in esecuzione o disponibili troppi pochi nodi di archiviazione con il servizio RSM.

Il servizio RSM garantisce che le richieste di servizio della piattaforma vengano inviate ai rispettivi endpoint.

Per risolvere questo avviso, determinare quali nodi di archiviazione nel sito includono il servizio RSM. (Il servizio RSM è presente sui nodi di archiviazione che includono anche il servizio ADC.) Quindi, assicurarsi che la maggioranza semplice di tali nodi di archiviazione sia in esecuzione e disponibile.

Se più di un nodo di archiviazione contenente il servizio RSM si guasta in un sito, si perdono tutte le richieste di servizio della piattaforma in sospeso per quel sito.

Ulteriori indicazioni per la risoluzione dei problemi per gli endpoint dei servizi della piattaforma

Per ulteriori informazioni vedere**Utilizzare un account tenant › Risoluzione dei problemi degli endpoint dei servizi della piattaforma** .

Informazioni correlate

"Risoluzione dei problemi del sistema StorageGRID"

Gestisci S3 Select per gli account tenant

È possibile consentire a determinati tenant S3 di utilizzare S3 Select per inviare richieste SelectObjectContent su singoli oggetti.

S3 Select offre un modo efficiente per effettuare ricerche in grandi quantità di dati senza dover implementare un database e le risorse associate per abilitare le ricerche. Riduce inoltre i costi e la latenza del recupero dei dati.

Che cos'è S3 Select?

S3 Select consente ai client S3 di utilizzare le richieste SelectObjectContent per filtrare e recuperare solo i dati necessari da un oggetto. L'implementazione StorageGRID di S3 Select include un sottoinsieme di comandi e funzionalità di S3 Select.

Considerazioni e requisiti per l'utilizzo di S3 Select

Requisiti di amministrazione della rete

L'amministratore della rete deve concedere ai tenant la capacità S3 Select. Seleziona **Consenti selezione S3** quando"creazione di un inquilino" O"modifica di un inquilino" .

Requisiti del formato dell'oggetto

L'oggetto che si desidera interrogare deve essere in uno dei seguenti formati:

- **CSV**. Può essere utilizzato così com'è o compresso in archivi GZIP o BZIP2.
- **Parquet**. Requisiti aggiuntivi per gli oggetti Parquet:
  - S3 Select supporta solo la compressione colonnare tramite GZIP o Snappy. S3 Select non supporta la compressione dell'intero oggetto per gli oggetti Parquet.
  - S3 Select non supporta l'output Parquet. È necessario specificare il formato di output come CSV o JSON.
  - La dimensione massima del gruppo di righe non compresso è 512 MB.
  - È necessario utilizzare i tipi di dati specificati nello schema dell'oggetto.
  - Non è possibile utilizzare i tipi logici INTERVAL, JSON, LIST, TIME o UUID.

Requisiti dell'endpoint

La richiesta SelectObjectContent deve essere inviata a un"Endpoint del bilanciatore del carico StorageGRID" .

I nodi Admin e Gateway utilizzati dall'endpoint devono essere uno dei seguenti:

- Un nodo di appliance di servizi
- Un nodo software basato su VMware
- Un nodo bare metal che esegue un kernel con cgroup v2 abilitato

Considerazioni generali

Le query non possono essere inviate direttamente ai nodi di archiviazione.

> Le richieste SelectObjectContent possono ridurre le prestazioni del bilanciatore del carico per tutti i client S3 e tutti i tenant. Abilitare questa funzionalità solo quando necessario e solo per i tenant attendibili.

Vedi il"istruzioni per l'uso di S3 Select" .

Per visualizzare"Grafici Grafana" per le operazioni di selezione S3 nel tempo, selezionare **SUPPORTO** > **Strumenti** > **Metriche** in Grid Manager.