Gestione dei tenant

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

Gestione dei tenant . . . 1
Quali sono gli account tenant . . . 1
Creazione e configurazione di account tenant . . . 1
Configurazione dei tenant S3 . . . 2
Configurazione dei tenant Swift . . . 2
Creazione di un account tenant . . . 3
Modifica della password per l'utente root locale del tenant . . . 10
Modifica di un account tenant . . . 12
Eliminazione di un account tenant . . . 14
Gestione dei servizi della piattaforma per gli account tenant S3 . . . 15

Gestione dei 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.

Quali 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.

Creazione e configurazione di 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.

  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.

Configurazione dei 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.

Configurazione dei tenant 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 Root Access per accedere a Tenant Manager. Tuttavia, l'autorizzazione Root Access non consente agli utenti di autenticarsi nell'API SWIFT REST 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"

Creazione di un account tenant

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

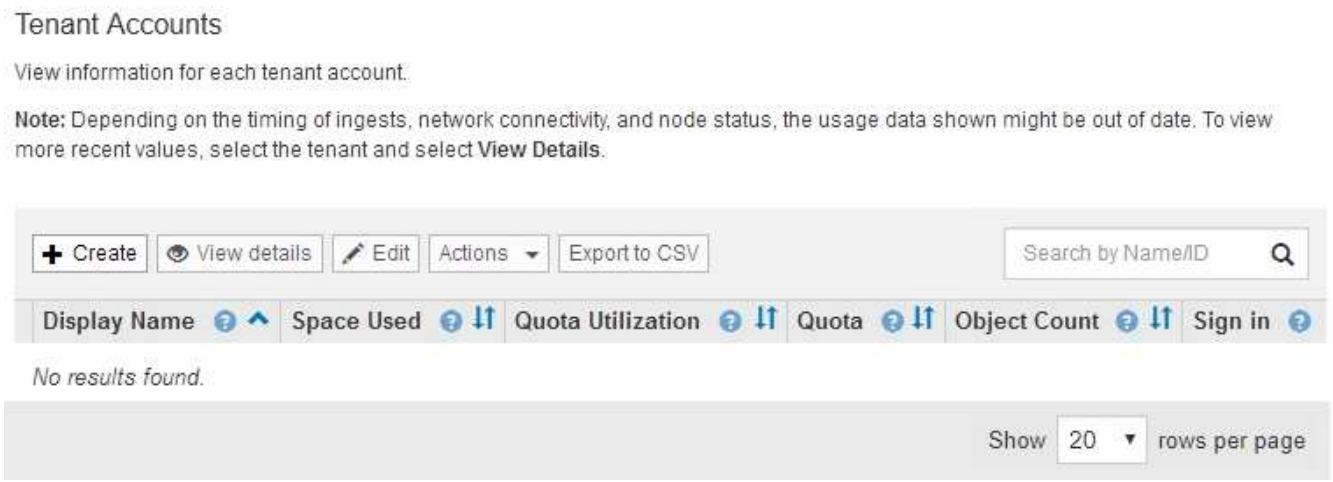
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **tenant**.

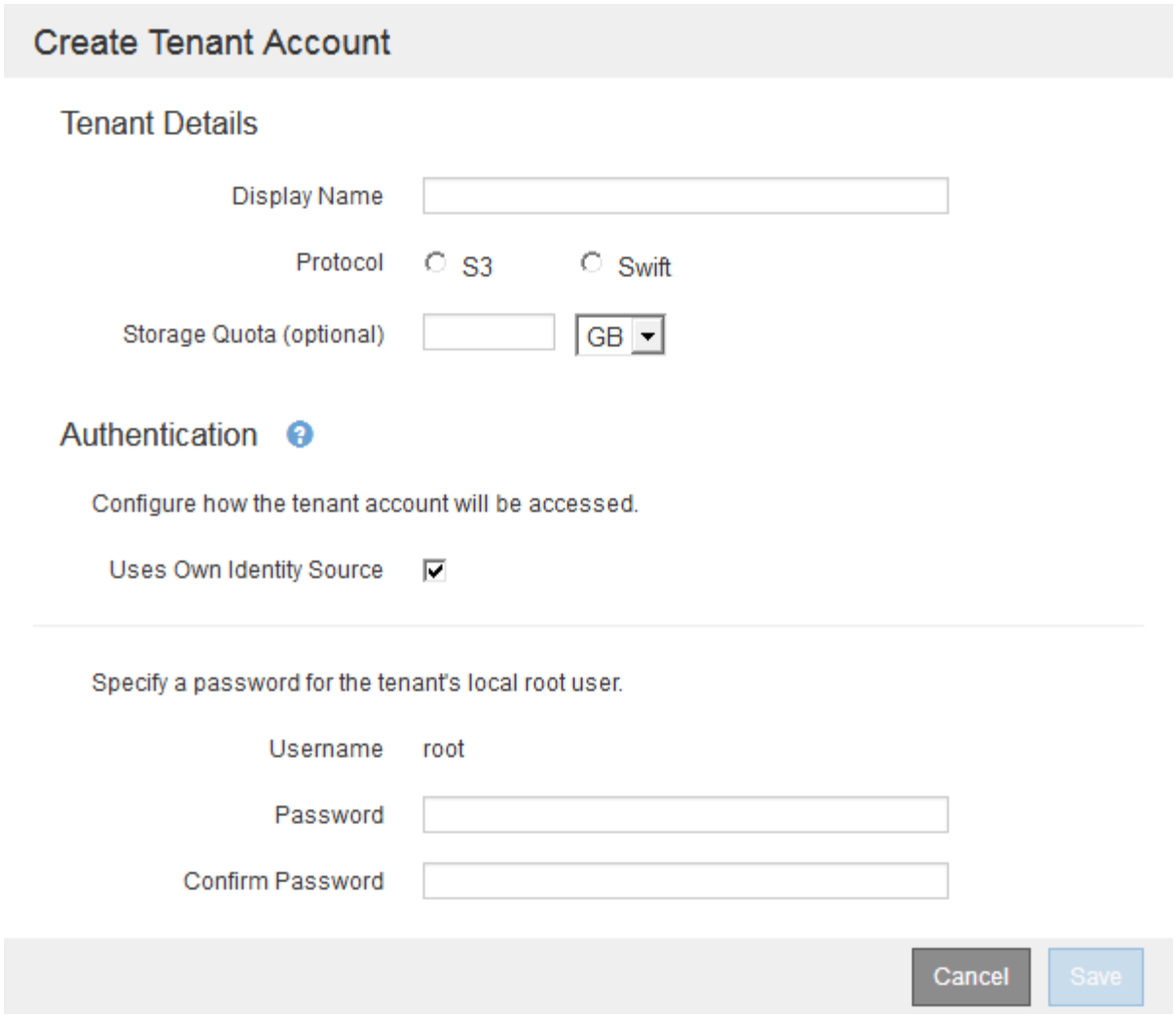
   Viene visualizzata la pagina account tenant che elenca gli account tenant esistenti.



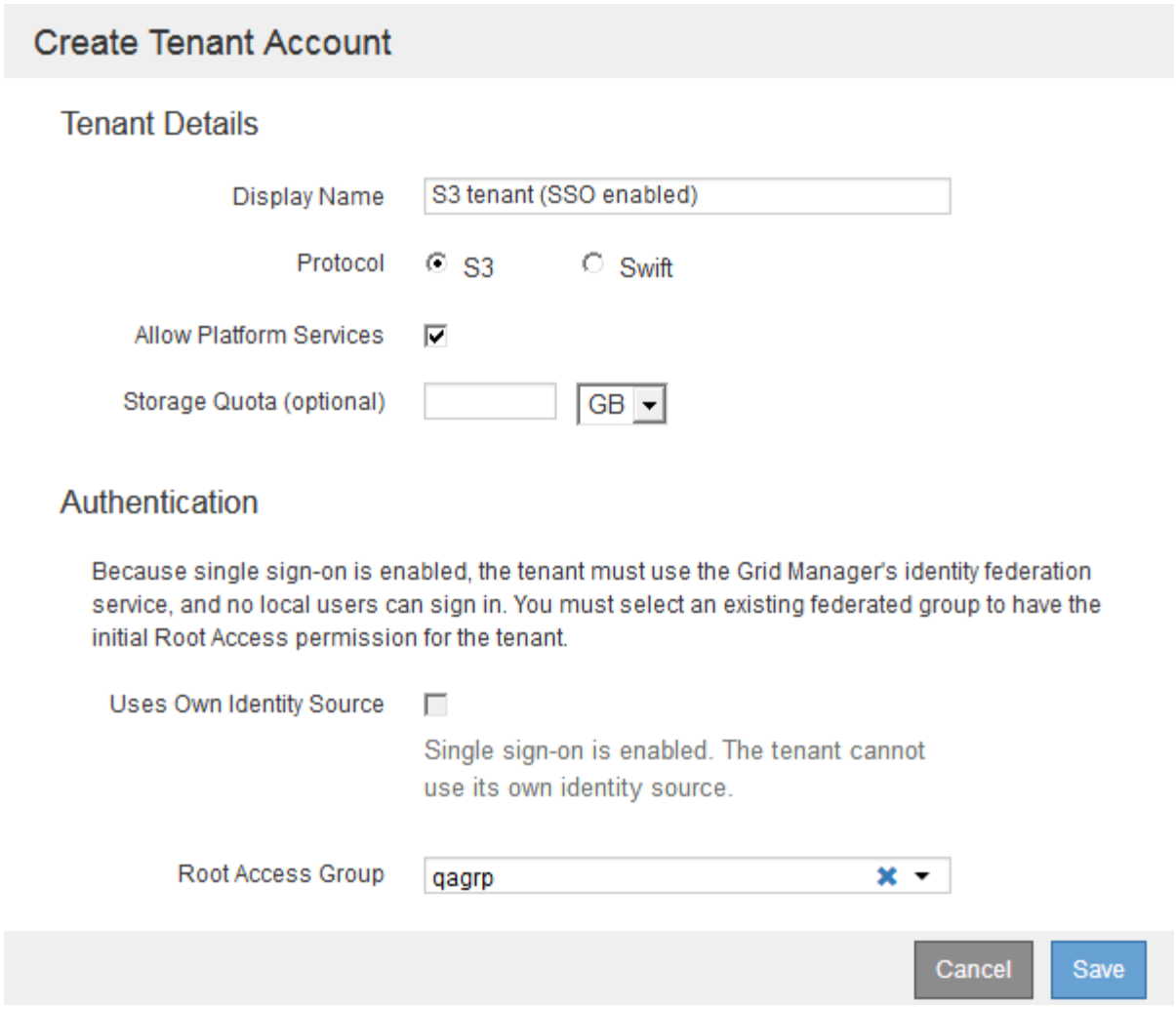
2. Selezionare **Crea**.

   Viene visualizzata la pagina Create tenant account (Crea account tenant). I campi inclusi nella pagina dipendono dall'attivazione o meno di SSO (Single Sign-on) per il sistema StorageGRID.

   - Se non viene utilizzato SSO, la pagina Create tenant account (Crea account tenant) è simile a questa.



◦ Se SSO è attivato, la pagina Create tenant account (Crea account tenant) è simile a questa.



Informazioni correlate

"Utilizzo della federazione delle identità"

"Configurazione del single sign-on"

Creazione di un account tenant se StorageGRID non utilizza SSO

Quando si crea un account tenant, specificare un nome, un protocollo client e, facoltativamente, una quota di storage. Se StorageGRID non utilizza SSO (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.

A proposito di questa attività

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, è necessario aver importato tale gruppo federated in Grid Manager. Non è necessario assegnare alcuna autorizzazione Grid Manager a questo gruppo di amministratori. Consultare le istruzioni per "gestione dei gruppi di amministratori".

Fasi

1. Nella casella di testo **Display Name** (Nome visualizzato), immettere un nome visualizzato per l'account tenant.

I nomi visualizzati non devono essere univoci. Una volta creato, l'account tenant riceve un ID account univoco e numerico.

2. Selezionare il protocollo client che verrà utilizzato da questo account tenant, **S3** o **Swift**.
3. Per gli account tenant S3, mantenere la casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) selezionata, a meno che non si desideri che il tenant non utilizzi i servizi della piattaforma per i bucket S3.

   Se i servizi della piattaforma sono attivati, un tenant può utilizzare funzionalità, come la replica CloudMirror, che accedono ai servizi esterni. È possibile disattivare l'utilizzo di queste funzioni per limitare la quantità di larghezza di banda di rete o di altre risorse consumate dal tenant. Vedere "Managing platform Services".

4. Nella casella di testo **quota di storage**, immettere il numero massimo di gigabyte, terabyte o petabyte che si desidera rendere disponibili per gli oggetti del tenant. Quindi, selezionare le unità dall'elenco a discesa.

   Lasciare vuoto questo campo se si desidera che il tenant abbia una quota illimitata.

   La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco). Le copie ILM e la codifica di cancellazione non contribuiscono alla quantità di quota utilizzata. Se la quota viene superata, l'account tenant non può creare nuovi oggetti.

   Per monitorare l'utilizzo dello storage di ciascun account tenant, selezionare **Usage** (utilizzo). Gli account tenant possono anche monitorare il proprio utilizzo dello storage dalla dashboard in Tenant Manager o con l'API di gestione tenant. Si noti che i valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi nella griglia. I totali verranno aggiornati al ripristino della connettività di rete.

5. Se il tenant gestirà i propri gruppi e utenti, attenersi alla seguente procedura.
   a. Selezionare la casella di controllo **utilizza origine identità** (impostazione predefinita).

      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. Consultare le istruzioni per l'utilizzo degli account tenant.

   b. Specificare una password per l'utente root locale del tenant.
6. Se il tenant utilizza i gruppi e gli utenti configurati per Grid Manager, attenersi alla seguente procedura.
   a. Deselezionare la casella di controllo **utilizza origine identità**.
   b. Eseguire una o entrambe le operazioni seguenti:
      - Nel campo Root Access Group (Gruppo di accesso principale), selezionare un gruppo federated esistente da Grid Manager che deve disporre dell'autorizzazione di accesso principale iniziale per il tenant.

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

      - Specificare una password per l'utente root locale del tenant.
7. Fare clic su **Save** (Salva).

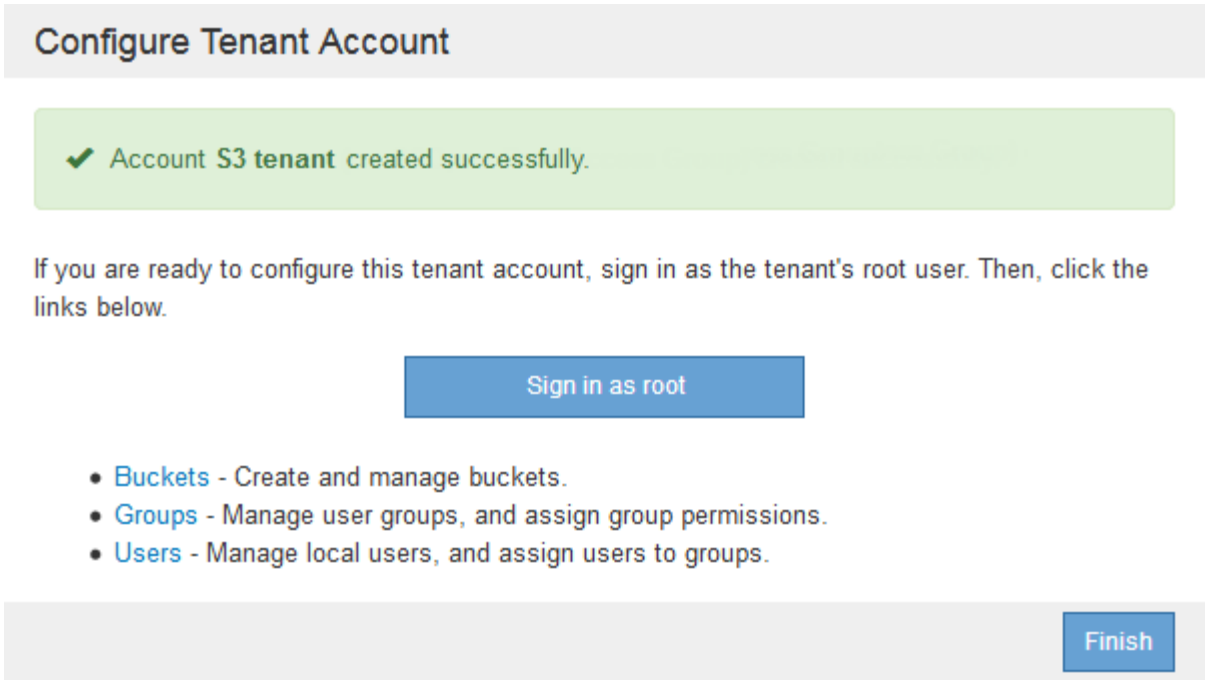
Viene creato l'account tenant.

8. In alternativa, accedere al nuovo tenant. In caso contrario, passare al punto per accesso al tenant in un secondo momento.

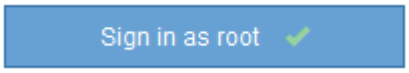
Se sei…	Eseguire questa operazione…
Accesso a Grid Manager su una porta con restrizioni	Fare clic su **Restricted** per ulteriori informazioni sull'accesso a questo account tenant. L'URL del tenant manager ha il seguente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *`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
Accesso a Grid Manager sulla porta 443 ma non è stata impostata una password per l'utente root locale	Fare clic su **Accedi** e immettere le credenziali per un utente nel gruppo federated di accesso root.
Accedendo a Grid Manager sulla porta 443, viene impostata una password per l'utente root locale	Passare alla fase successiva da a. accedi come root.

9. Accedi al tenant come root:

   a. Dalla finestra di dialogo Configura account tenant, fare clic sul pulsante **Accedi come root**.



Sul pulsante viene visualizzato un segno di spunta verde, a indicare che si è ora effettuato l'accesso all'account tenant come utente root.



a. Fare clic sui collegamenti per configurare l'account tenant.

   Ciascun collegamento apre la pagina corrispondente in Tenant Manager. Per completare la pagina, consultare le istruzioni per l'utilizzo degli account tenant.

b. Fare clic su **fine**.

10. per accedere al tenant in un secondo momento:

Se si utilizza…	Eseguire una di queste operazioni…
Porta 443	• Da Grid Manager, selezionare **tenant** e fare clic su **Sign in** (Accedi) a destra del nome del tenant. • Inserire l'URL del tenant in un browser Web: `https://FQDN_or_Admin_Node_IP/?accountId=20-digit-account-id/` ◦ *FQDN_or_Admin_Node_IP* È un nome di dominio completo o l'indirizzo IP di un nodo amministratore ◦ *20-digit-account-id* È l'ID account univoco del tenant

Se si utilizza…	Eseguire una di queste operazioni…
Una porta con restrizioni	• In Grid Manager, selezionare **tenant** e fare clic su **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"

"Gestione dei servizi della piattaforma per gli account tenant S3"

"Utilizzare un account tenant"

Creazione di un account tenant se SSO è attivato

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.

Fasi

1. Nella casella di testo **Display Name** (Nome visualizzato), immettere un nome visualizzato per l'account tenant.

   I nomi visualizzati non devono essere univoci. Una volta creato, l'account tenant riceve un ID account univoco e numerico.

2. Selezionare il protocollo client che verrà utilizzato da questo account tenant, **S3** o **Swift**.
3. Per gli account tenant S3, mantenere la casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) selezionata, a meno che non si desideri che il tenant non utilizzi i servizi della piattaforma per i bucket S3.

   Se i servizi della piattaforma sono attivati, un tenant può utilizzare funzionalità, come la replica CloudMirror, che accedono ai servizi esterni. È possibile disattivare l'utilizzo di queste funzioni per limitare la quantità di larghezza di banda di rete o di altre risorse consumate dal tenant. Vedere "Managing platform Services".

4. Nella casella di testo **quota di storage**, immettere il numero massimo di gigabyte, terabyte o petabyte che si desidera rendere disponibili per gli oggetti del tenant. Quindi, selezionare le unità dall'elenco a discesa.

   Lasciare vuoto questo campo se si desidera che il tenant abbia una quota illimitata.

La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco). Le copie ILM e la codifica di cancellazione non contribuiscono alla quantità di quota utilizzata. Se la quota viene superata, l'account tenant non può creare nuovi oggetti.

Per monitorare l'utilizzo dello storage di ciascun account tenant, selezionare **Usage** (utilizzo). Gli account tenant possono anche monitorare il proprio utilizzo dello storage dalla dashboard in Tenant Manager o con l'API di gestione tenant. Si noti che i valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi nella griglia. I totali verranno aggiornati al ripristino della connettività di rete.

5. Si noti che la casella di controllo **utilizza origine identità** è deselezionata e disattivata.

   Poiché SSO è attivato, il tenant deve utilizzare l'origine dell'identità configurata per Grid Manager. Nessun utente locale può accedere.

6. Nel campo **Root Access Group**, 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, quando si fa clic sul campo vengono elencati i gruppi federated esistenti di Grid Manager. In caso contrario, immettere il nome univoco del gruppo.

7. Fare clic su **Save** (Salva).

   Viene creato l'account tenant. Viene visualizzata la pagina account tenant, che include una riga per il nuovo tenant.

8. Se si è un utente del gruppo Root Access, fare clic sul collegamento **Sign in** (Accedi) per accedere immediatamente al tenant Manager, dove è possibile configurare il tenant. In caso contrario, fornire l'URL del collegamento **Accedi** all'amministratore dell'account tenant. (L'URL di un tenant è il nome di dominio completo o l'indirizzo IP di qualsiasi nodo di amministrazione, seguito da `/?accountId=20-digit-account-id`.)

   Se si fa clic su **Sign in** (accesso negato), ma non si appartiene al gruppo Root Access per l'account tenant, viene visualizzato un messaggio di accesso negato.

Informazioni correlate

"Configurazione del single sign-on"

"Gestione dei servizi della piattaforma per gli account tenant S3"

"Utilizzare un account tenant"

Modifica della 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

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

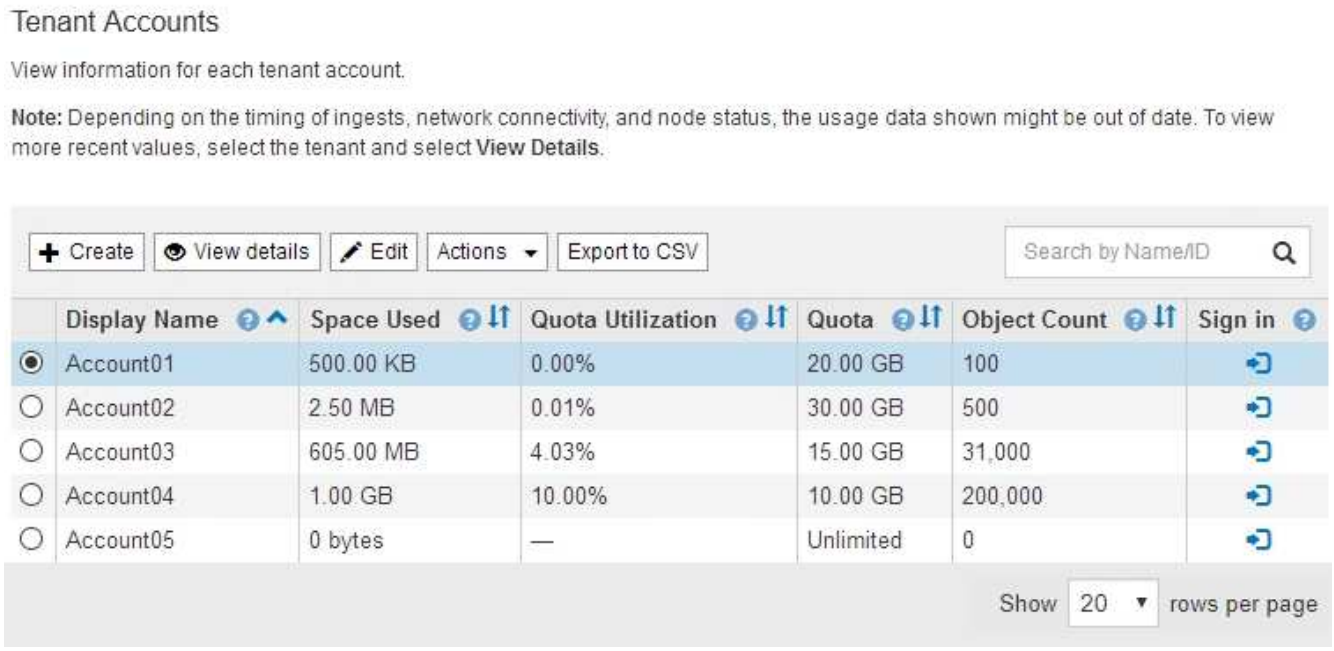
A proposito di questa attività

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**.

   Viene visualizzata la pagina account tenant che elenca tutti gli account tenant esistenti.

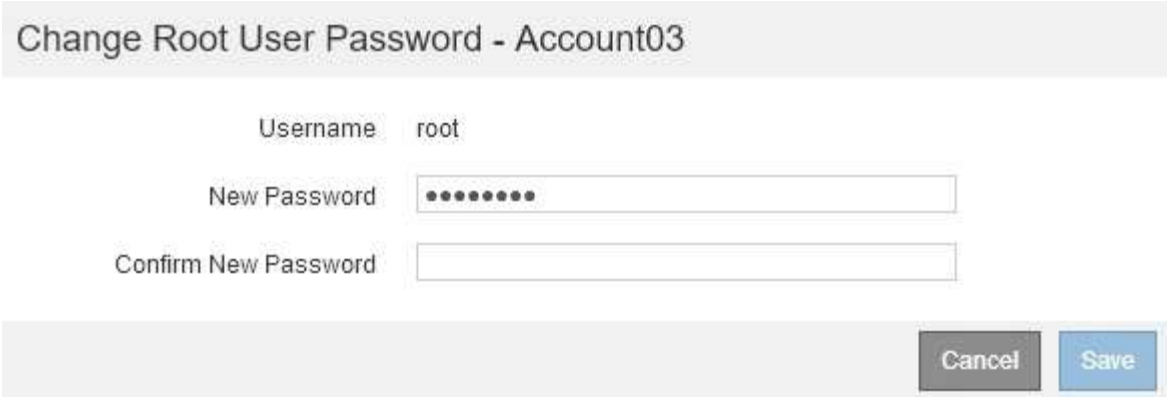


2. Selezionare l'account tenant che si desidera modificare.

   Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. Utilizzare la casella di ricerca per cercare un account tenant in base al nome visualizzato o all'ID tenant.

   Vengono attivati i pulsanti Visualizza dettagli, Modifica e azioni.

3. Dal menu a discesa **Actions** (azioni), selezionare **Change Root Password** (Modifica password root).



4. Inserire la nuova password per l'account tenant.
5. Selezionare **Salva**.

Informazioni correlate

"Controllo dell'accesso amministratore a StorageGRID"

Modifica di un 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.

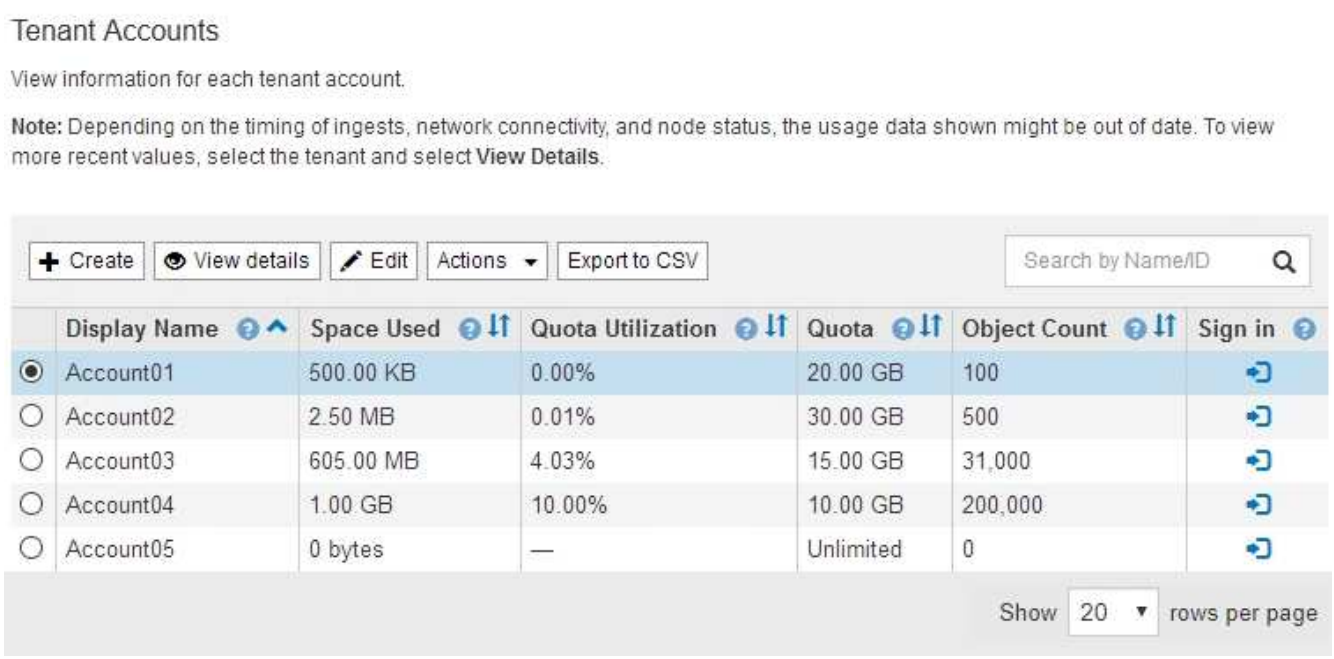
Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.

Fasi

1. Selezionare **tenant**.

   Viene visualizzata la pagina account tenant che elenca tutti gli account tenant esistenti.

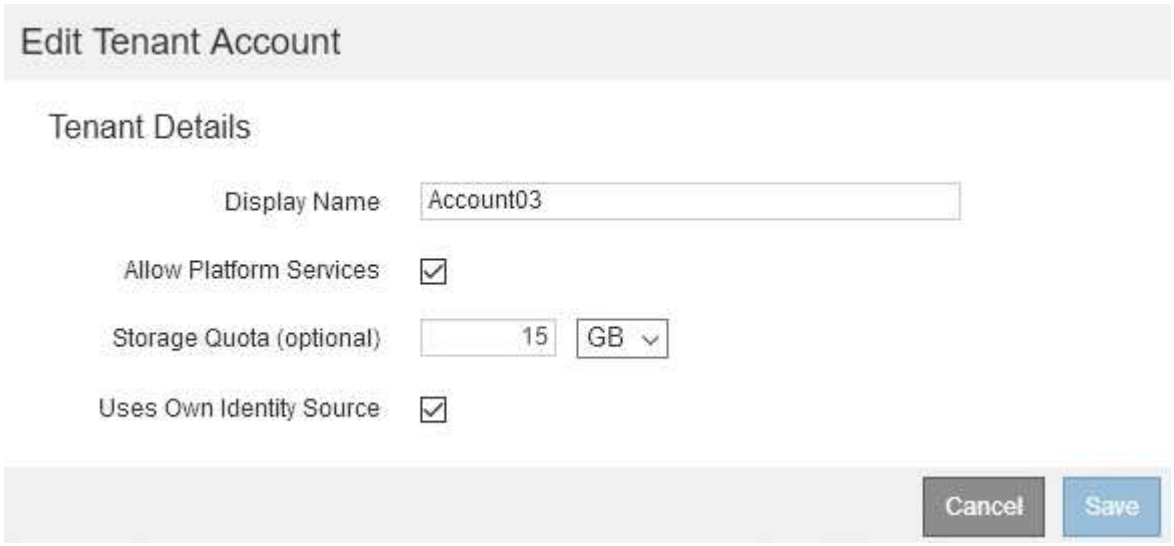


2. Selezionare l'account tenant che si desidera modificare.

   Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. Utilizzare la casella di ricerca per cercare un account tenant in base al nome visualizzato o all'ID tenant.

3. Selezionare **Modifica**.

   Viene visualizzata la pagina Edit tenant account (Modifica account tenant). 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 dei campi come richiesto.
   a. Modificare il nome visualizzato per questo account tenant.
   b. Modificare l'impostazione della casella di controllo **Allow Platform Services** (Consenti servizi piattaforma) per determinare se l'account tenant può utilizzare i servizi della piattaforma per i bucket S3.

> Se si disattivano i servizi della piattaforma 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.

c. Per **quota di storage**, modificare il numero massimo di gigabyte, terabyte o petabyte disponibili per gli oggetti del tenant oppure lasciare vuoto il campo se si desidera che il tenant abbia una quota illimitata.

   La quota di storage di un tenant rappresenta una quantità logica (dimensione dell'oggetto), non una quantità fisica (dimensione sul disco). Le copie ILM e la codifica di cancellazione non contribuiscono alla quantità di quota utilizzata.

   > Per monitorare l'utilizzo dello storage di ciascun account tenant, selezionare **Usage** (utilizzo). Gli account tenant possono anche monitorare il proprio utilizzo dalla dashboard in Tenant Manager o con l'API di gestione tenant. Si noti che i valori di utilizzo dello storage di un tenant potrebbero non essere aggiornati se i nodi sono isolati da altri nodi nella griglia. I totali verranno aggiornati al ripristino della connettività di rete.

d. Modificare l'impostazione della casella di controllo **Use Own Identity Source** (utilizza origine identità propria) per determinare se l'account tenant utilizzerà la propria origine identità o l'origine identità configurata per Grid Manager.

   > Se la casella di controllo **utilizza 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.

5. Selezionare **Salva**.

Informazioni correlate

"Gestione dei servizi della piattaforma per gli account tenant S3"

"Utilizzare un account tenant"

Eliminazione di un 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 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.

   Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. Utilizzare la casella di ricerca per cercare un account tenant in base al nome visualizzato o all'ID tenant.

3. Dal menu a discesa **azioni**, selezionare **Rimuovi**.
4. Selezionare **OK**.

Informazioni correlate

"Controllo dell'accesso amministratore a StorageGRID"

Gestione dei 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.

- "Quali sono i servizi della piattaforma"
- "Networking e porte per i servizi della piattaforma"
- "Erogazione per sito di messaggi relativi ai servizi della piattaforma"
- "Risoluzione dei problemi relativi ai servizi della piattaforma"

Quali 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, è necessario conoscere i seguenti consigli:

- 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.
- 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.

Informazioni correlate

"Utilizzare un account tenant"

"Configurazione delle impostazioni del proxy di storage"

"Monitor risoluzione dei problemi"

Networking 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 configurare anche le impostazioni del proxy di storage per consentire l'invio dei messaggi a endpoint esterni, ad esempio un endpoint su Internet.

Informazioni correlate

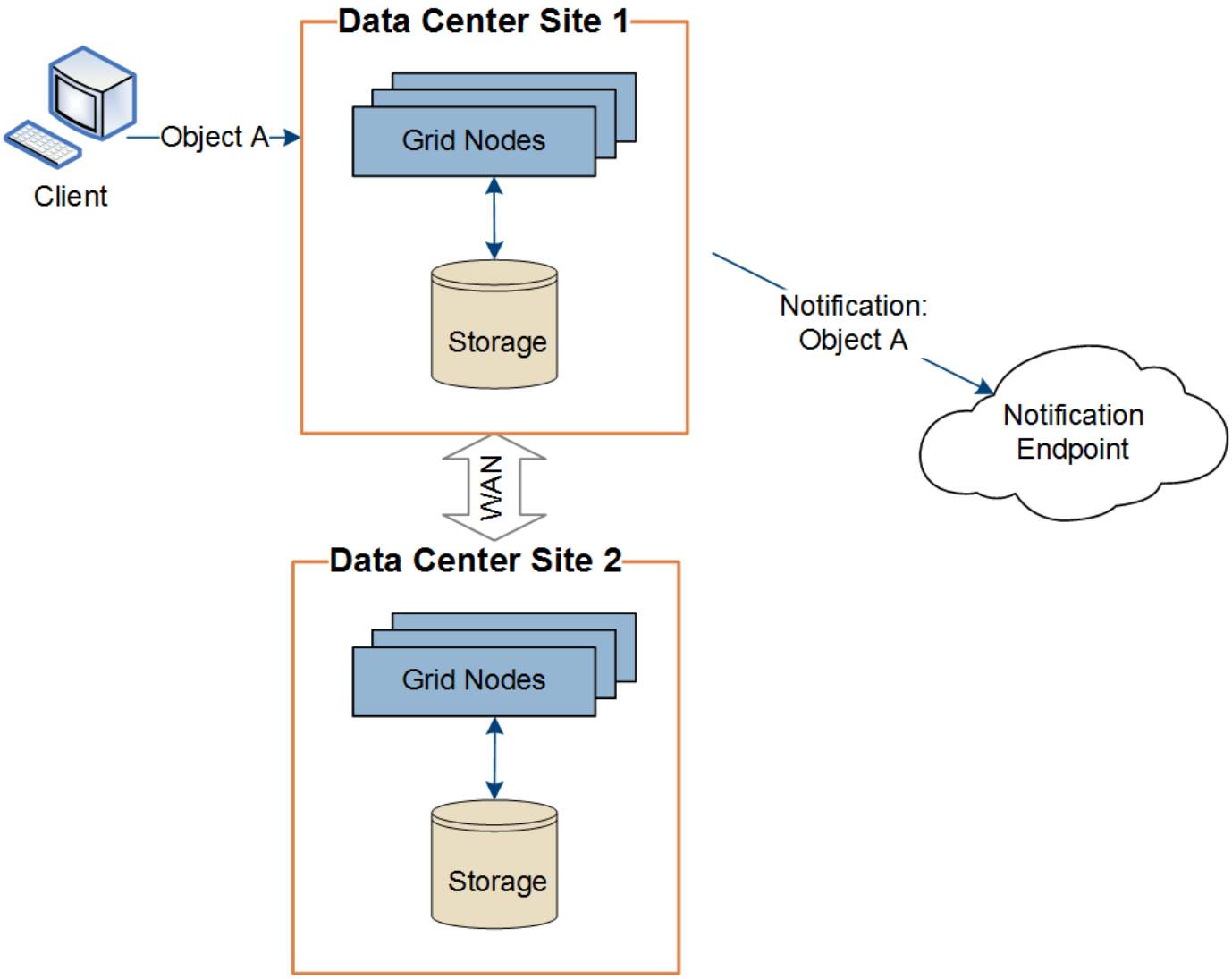
"Configurazione delle impostazioni del proxy di storage"

"Utilizzare un account tenant"

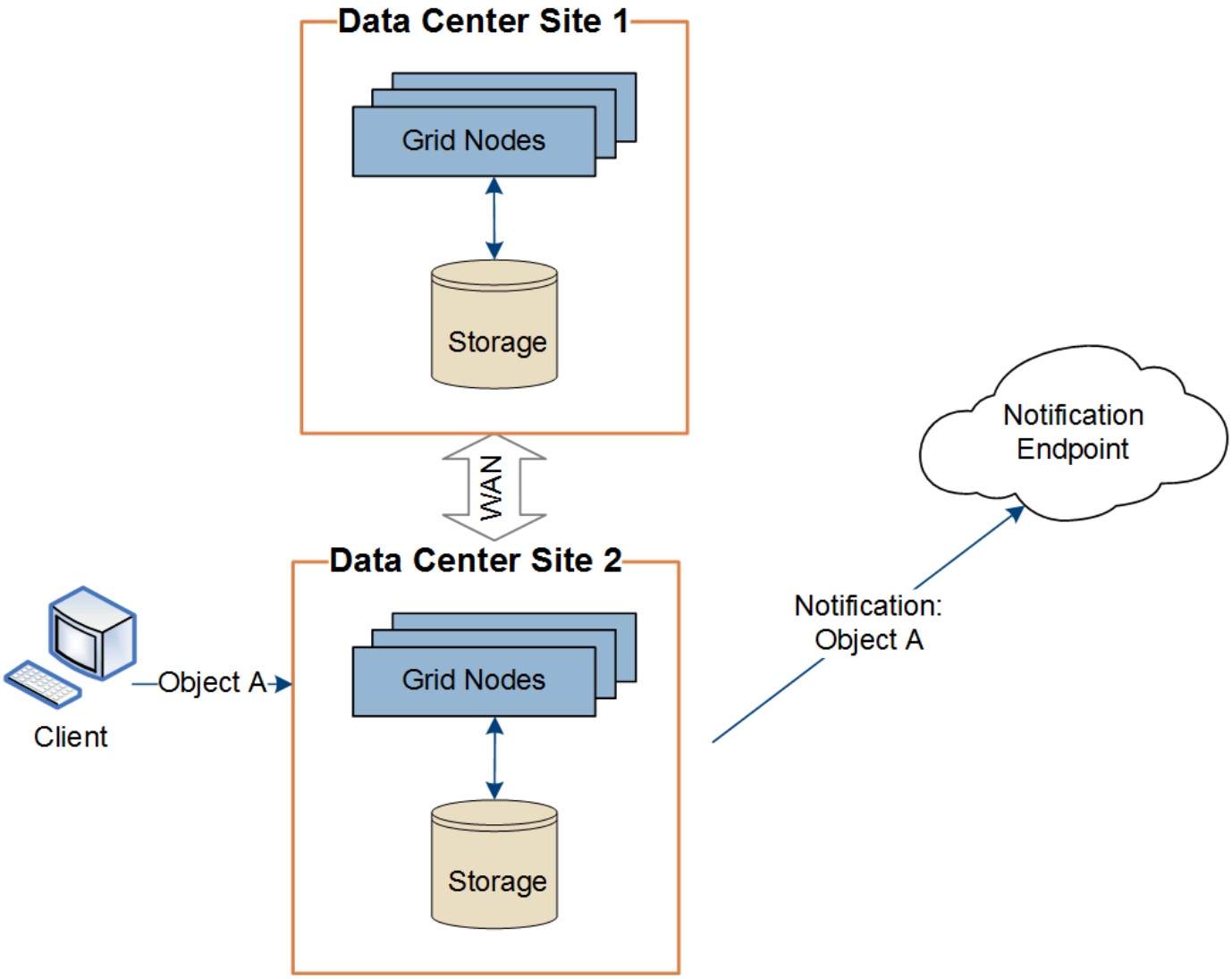
Erogazione per sito di messaggi relativi ai servizi della piattaforma

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.

Risoluzione dei 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

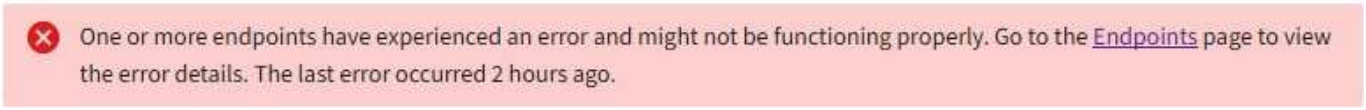
ogni sito.

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.

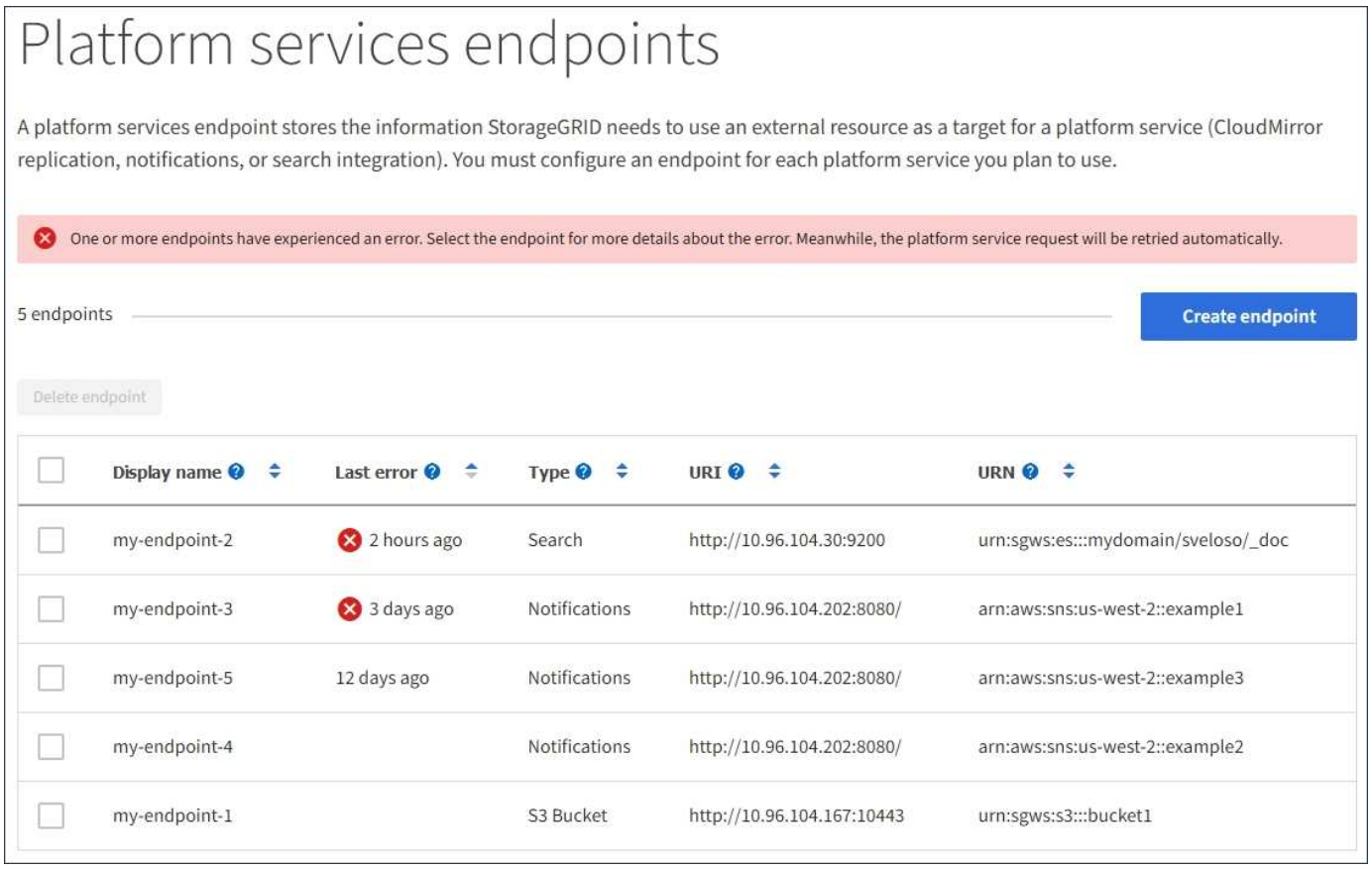
La creazione dell'endpoint non riesce se i servizi della piattaforma non sono abilitati per l'account tenant.

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 **supporto** > **Strumenti** > **topologia griglia**.
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 Eventi totali (SMTT) viene attivato in Gestione griglia. Per visualizzare l'allarme Total Events (Eventi totali):

1. Selezionare **nodi**.
2. Selezionare ***Site Grid Node* Events**.
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. Fare clic su **Reset event count** (Ripristina conteggi 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 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. Visualizzare 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, consultare le istruzioni per l'utilizzo degli account tenant.

"Utilizzare un account tenant"

Informazioni correlate

"Monitor risoluzione dei problemi"

"Configurazione delle impostazioni del proxy di storage"

Informazioni sul copyright

Informazioni sul marchio commerciale