Creazione di un account tenant

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

Creazione di un account tenant

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

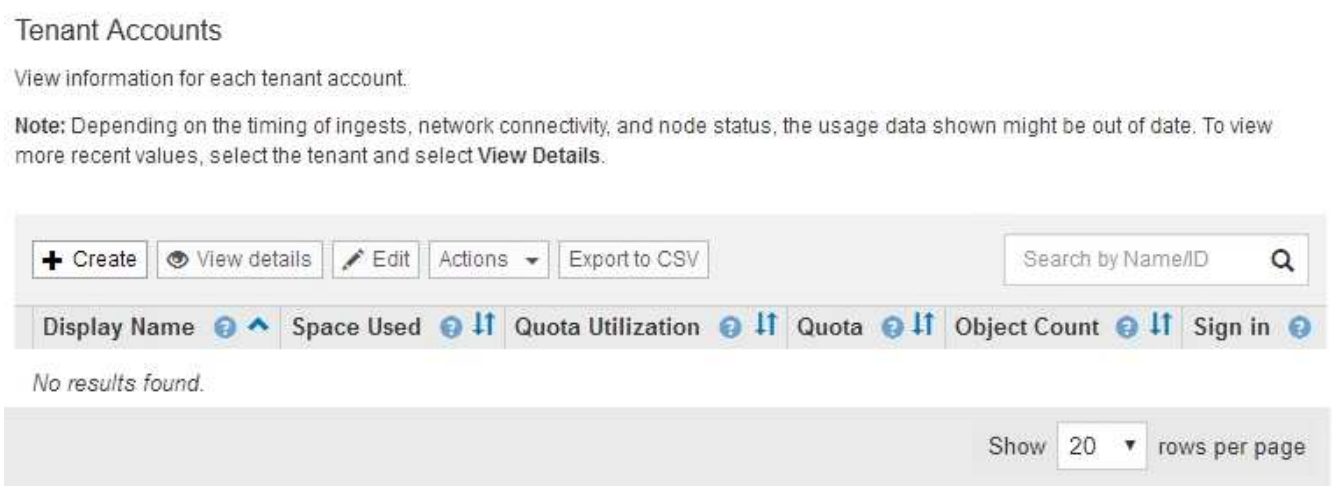
Di cosa hai bisogno

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

Fasi

1. Selezionare **tenant**.

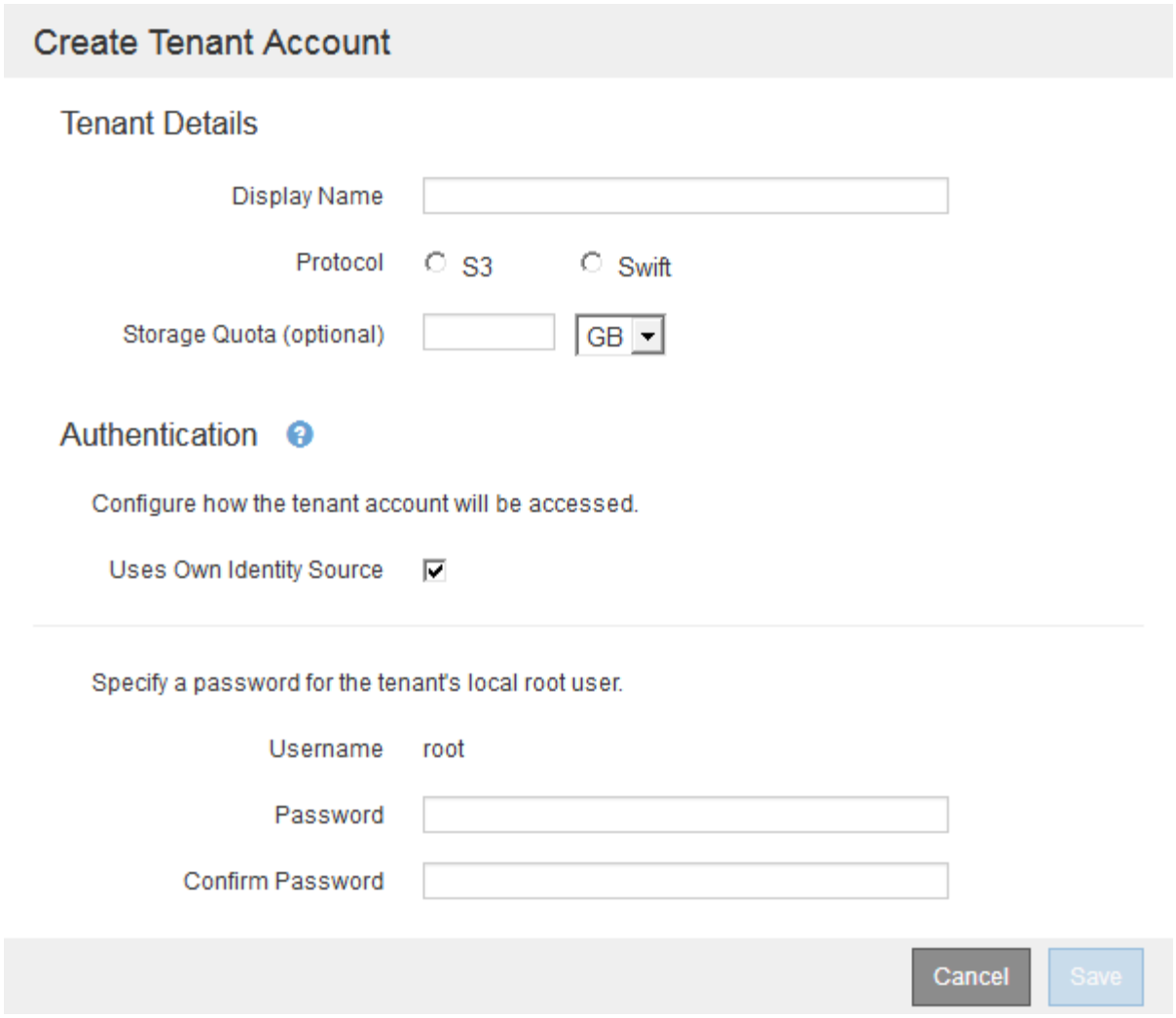
   Viene visualizzata la pagina account tenant che elenca gli account tenant esistenti.



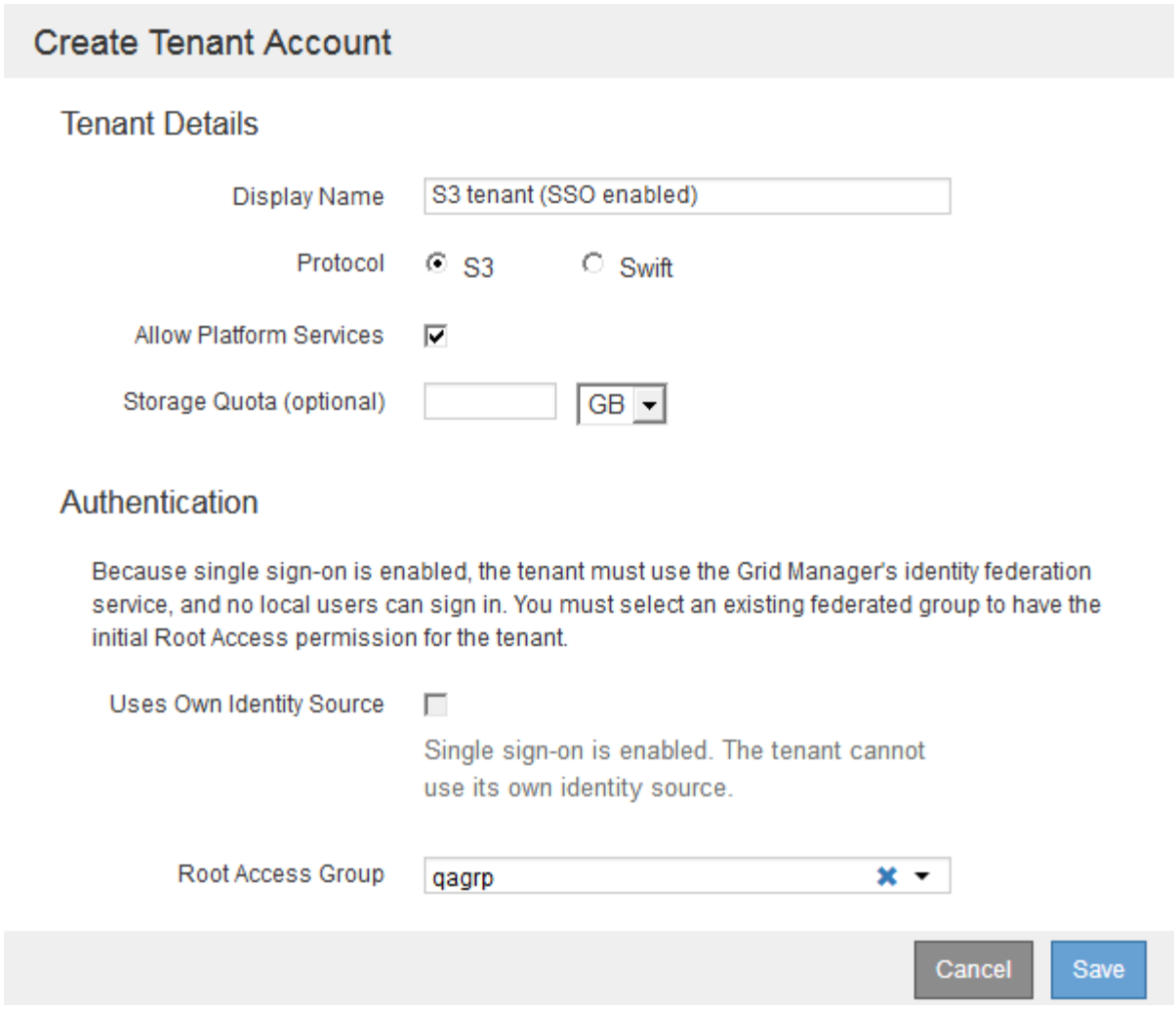
2. Selezionare **Crea**.

   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).

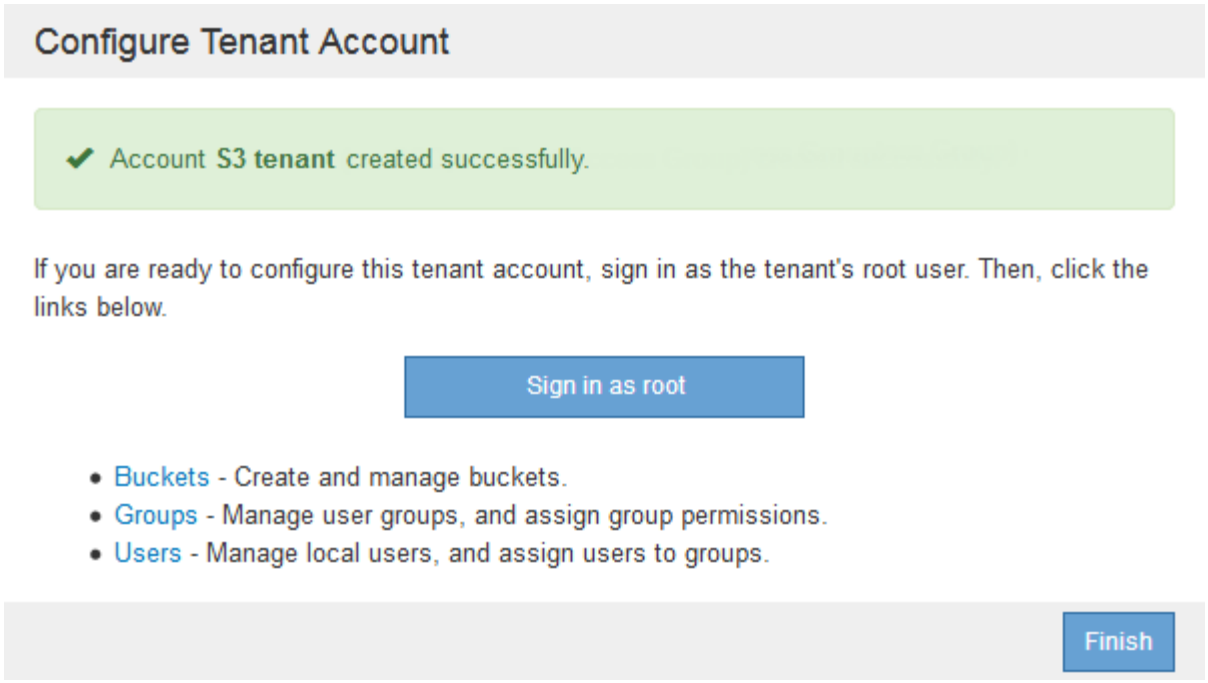
   Viene creato l'account tenant.

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

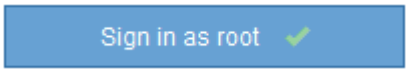
Se sei…	Eseguire questa operazione…
Accesso a Grid Manager su una porta con restrizioni	Fare clic su **Restricted** per ulteriori informazioni sull'accesso a questo account tenant. L'URL del tenant manager ha il seguente formato: `https://FQDN_or_Admin_Node_IP:port/?accountId=20-digit-account-id/` • *`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"