Controllo dell'accesso a StorageGRID

StorageGRID software

NetApp
January 14, 2026

Sommario

Controllo dell'accesso a StorageGRID

Controllare l'accesso a StorageGRID

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

Controlla l'accesso a Grid Manager

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

L'utilizzo di "federazione delle identità" rende l'impostazione "gruppi"e "utenti" più veloce, e consente agli utenti di accedere a StorageGRID utilizzando credenziali familiari. È possibile configurare la federazione delle identità se si utilizza Active Directory, OpenLDAP o Oracle Directory Server.

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

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

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

Attiva single sign-on

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

Modificare la passphrase di provisioning

La passphrase di provisioning è necessaria per numerose procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino StorageGRID . La passphrase è necessaria anche per scaricare i backup delle informazioni sulla topologia della griglia e le chiavi di crittografia per il sistema StorageGRID . Puoi"modificare la passphrase" come richiesto.

Modificare le password della console dei nodi

Ogni nodo nella griglia ha una password per la console del nodo, necessaria per accedere al nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. Se necessario, puoi"modificare la password della console del nodo" per ogni nodo.

Modificare la passphrase di provisioning

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

Prima di iniziare

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

A proposito di questa attività

La passphrase di provisioning è richiesta per molte procedure di installazione e manutenzione e per"scaricando il pacchetto di ripristino" . La passphrase di provisioning non è elencata in `Passwords.txt` file. Assicuratevi di documentare la passphrase di provisioning e di conservarla in un luogo sicuro e protetto.

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Password griglia**.
2. In **Cambia passphrase di provisioning**, selezionare **effettua una modifica**
3. Inserire la passphrase di provisioning corrente.
4. Inserire la nuova passphrase. La passphrase deve contenere almeno 8 e non più di 32 caratteri. Le passphrase sono sensibili al maiuscolo/minuscolo.

   Conservare la passphrase di provisioning in un luogo sicuro. È necessario per le procedure di installazione, ampliamento e manutenzione.

5. Immettere nuovamente la nuova passphrase e selezionare **Save** (Salva).

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

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

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

Modificare le password della console dei nodi

Ogni nodo della griglia ha una password della console del nodo, che puoi utilizzare per accedere al nodo. Per impostazione predefinita, ogni nodo ha una password univoca. È

possibile modificare ciascuna password con una nuova password univoca oppure è possibile modificare la password di ogni nodo per utilizzare una password globale. Le password vengono memorizzate nel pacchetto di ripristino.

Prima di iniziare

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

A proposito di questa attività

Si utilizza una password della console del nodo per accedere a un nodo come "admin" tramite SSH oppure come utente root su una connessione alla console fisica/VM. È possibile modificare le password della console del nodo utilizzando una di queste opzioni:

- Applica automaticamente password casuali a ciascun nodo
- Specificare e applicare una password globale a tutti i nodi
- Specificare e applicare una password univoca a uno o più nodi

Le password vengono memorizzate in un file aggiornato `Passwords.txt` file nel pacchetto di ripristino. Le password sono elencate nella colonna Password del file.

> IL"Password di accesso SSH" poiché le chiavi SSH utilizzate per la comunicazione tra i nodi sono separate dalle password della console del nodo. Questa procedura non modifica le password di accesso SSH.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Password griglia**.
2. In **Cambia password console nodo**, selezionare **effettua una modifica**.

Scarica il pacchetto di ripristino corrente

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

Fasi

1. Inserire la passphrase di provisioning per la griglia.
2. Selezionare **Download recovery package** (Scarica pacchetto di ripristino).
3. Copia il file del pacchetto di ripristino(`.zip`) in due luoghi sicuri, protetti e separati.

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

4. Selezionare **continua**.

Fornire nuove password

1. Seleziona il metodo di modifica della password che desideri utilizzare.
   - **Automatico**: StorageGRID assegna automaticamente una nuova password casuale della console a tutti i nodi.
   - **Personalizzato**: fornisci le password della console.

Automatico

1. Selezionare **continua**.

Personalizzato

1. Selezionare una delle seguenti opzioni:
   - **Password console globale**: applica la stessa password console a tutti i nodi.
   - **Password univoche della console**: applica una password diversa su uno o più nodi.
2. Se hai selezionato **Password console globale**, inserisci la password che desideri utilizzare per tutti i nodi.
3. Se hai selezionato **Password console univoche**, inserisci una password univoca per uno o più nodi.
4. Selezionare **continua**.

Completa la modifica della password

1. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì** se si è pronti affinché StorageGRID inizi a modificare le password della console del nodo.

   Non puoi annullare questo processo dopo l'avvio.

   StorageGRID genera un nuovo pacchetto di ripristino contenente la nuova password.

2. Quando il nuovo pacchetto di ripristino è pronto, seleziona **Scarica nuovo pacchetto di ripristino** e salva il pacchetto di ripristino.
3. Aprire il `.zip` file.
4. Verificare che sia possibile accedere al contenuto, incluso il `Passwords.txt` file, che contiene le nuove password della console del nodo.
5. Copia il nuovo file del pacchetto di ripristino(`.zip`) in due luoghi sicuri, protetti e separati.

   Non sovrascrivere il vecchio pacchetto di ripristino.

   È necessario proteggere il file di ripristino, poiché contiene chiavi di crittografia e password che possono essere utilizzate per ottenere dati dal sistema StorageGRID .

6. Seleziona la casella di controllo per indicare che hai scaricato il nuovo pacchetto di ripristino e ne hai verificato il contenuto.
7. Selezionare **continua**.

   StorageGRID aggiorna la password per ciascun nodo.

Se si verifica un errore durante il processo di aggiornamento, la barra di avanzamento elenca il numero di nodi le cui password non sono state modificate. Il sistema riproverà automaticamente il processo su qualsiasi nodo la cui password non è riuscita a cambiare. Se il processo termina con alcuni nodi che non hanno ancora modificato la password, viene visualizzato il pulsante **Riprova**.

8. Se l'aggiornamento della password non è riuscito per uno o più nodi:
   a. Esaminare i messaggi di errore elencati nella tabella.
   b. Risolvere i problemi.
   c. Selezionare **Riprova**.

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

9. Quando la barra di avanzamento indica che non ci sono aggiornamenti rimanenti, selezionare **Fine**.
10. Dopo aver modificato le password della console del nodo per tutti i nodi, eliminare ilprimo pacchetto di ripristino scaricato .

Modificare le password di accesso SSH per i nodi Admin

La modifica delle password di accesso SSH per i nodi Admin aggiorna anche i set univoci di chiavi SSH interne per ogni nodo nella griglia. Il nodo amministrativo primario utilizza queste chiavi SSH per accedere ai nodi utilizzando un'autenticazione protetta e senza password.

Utilizzare una chiave SSH per accedere a un nodo come `admin` o all'utente root su una connessione VM o console fisica.

Prima di iniziare

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

A proposito di questa attività

Le nuove password di accesso per i nodi di amministrazione e le nuove chiavi interne per ciascun nodo sono memorizzate nel `Passwords.txt` file nel pacchetto di ripristino. Le chiavi sono elencate nella colonna Password di quel file.

Esistono password di accesso SSH separate per le chiavi SSH utilizzate per la comunicazione tra i nodi. Questi non vengono modificati da questa procedura.

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Password griglia**.
2. In **Cambia chiavi SSH**, selezionare **effettua una modifica**.

Scarica il pacchetto di ripristino corrente

Prima di modificare le chiavi di accesso SSH, scaricare il pacchetto di ripristino corrente. È possibile utilizzare le chiavi contenute in questo file se il processo di modifica delle chiavi non riesce per un nodo.

Fasi

1. Inserire la passphrase di provisioning per la griglia.
2. Selezionare **Download recovery package** (Scarica pacchetto di ripristino).
3. Copia il file del pacchetto di ripristino(`.zip`) in due luoghi sicuri, protetti e separati.

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

4. Selezionare **continua**.
5. Quando viene visualizzata la finestra di dialogo di conferma, selezionare **Sì** se si è pronti a cambiare le chiavi di accesso SSH.

   Non puoi annullare questo processo dopo l'avvio.

Modificare le chiavi di accesso SSH

Quando viene avviato il processo di modifica delle chiavi di accesso SSH, viene generato un nuovo pacchetto di ripristino che include le nuove chiavi. Quindi, le chiavi vengono aggiornate su ciascun nodo.

Fasi

1. Attendi che venga generato il nuovo pacchetto di ripristino, operazione che potrebbe richiedere alcuni minuti.
2. Quando il pulsante Scarica nuovo pacchetto di ripristino è abilitato, seleziona **Scarica nuovo pacchetto di ripristino** e salva il nuovo file del pacchetto di ripristino(`.zip`) in due luoghi sicuri, protetti e separati.
3. Al termine del download:

   a. Aprire il `.zip` file.

   b. Verificare che sia possibile accedere al contenuto, incluso il `Passwords.txt` file, che contiene le nuove chiavi di accesso SSH.

   c. Copia il nuovo file del pacchetto di ripristino(`.zip`) in due luoghi sicuri, protetti e separati.

      Non sovrascrivere il vecchio pacchetto di ripristino.

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

4. Attendere l'aggiornamento delle chiavi su ciascun nodo, operazione che potrebbe richiedere alcuni minuti.

   Se le chiavi vengono modificate per tutti i nodi, viene visualizzato un banner di successo verde.

   Se si verifica un errore durante il processo di aggiornamento, un messaggio di intestazione elenca il numero di nodi che non sono riusciti a modificare le chiavi. Il sistema ritenta automaticamente il processo su qualsiasi nodo che non ha modificato la chiave. Se il processo termina con alcuni nodi che non hanno

ancora una chiave modificata, viene visualizzato il pulsante **Riprova**.

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

a. Esaminare i messaggi di errore elencati nella tabella.
b. Risolvere i problemi.
c. Selezionare **Riprova**.

   Il nuovo tentativo modifica solo le chiavi di accesso SSH sui nodi che hanno avuto esito negativo durante i precedenti tentativi di modifica della chiave.

5. Dopo aver modificato le chiavi di accesso SSH per tutti i nodi, eliminareprimo pacchetto di ripristino scaricato .
6. Facoltativamente, selezionare **Manutenzione** > **Sistema** > **Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo pacchetto di ripristino.

USA la federazione delle identità

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

Configurare la federazione delle identità per Grid Manager

È possibile configurare la federazione delle identità in Grid Manager se si desidera che i gruppi di amministratori e gli utenti vengano gestiti in un altro sistema, ad esempio Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai"autorizzazioni di accesso specifiche" .
- Stai utilizzando Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server come provider di identità.

  Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare l'assistenza tecnica.

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

A proposito di questa attività

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

- Gruppi di amministratori. Gli utenti dei gruppi di amministrazione possono accedere a Grid Manager ed

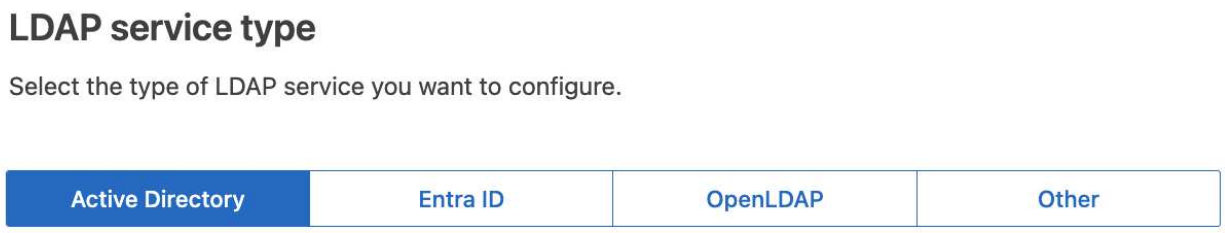
eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.

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

Inserire la configurazione

Fasi

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



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

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

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

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

  Per Active Directory, è anche possibile specificare il nome di accesso di livello inferiore o il nome principale dell'utente.

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

  - `sAMAccountName` o. `uid`
  - `objectGUID`, , `entryUUID` o `nsuniqueid`
  - `cn`
  - `memberOf` o. `isMemberOf`
  - **Active Directory**: `objectSid`, `primaryGroupID`, `userAccountControl` E `userPrincipalName`
  - **ID di ingresso**: `accountEnabled` E `userPrincipalName`
- **Password**: La password associata al nome utente.

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

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

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

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

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

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

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

  Immettere uno di questi modelli:

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

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

6. Nella sezione Transport Layer Security (TLS), selezionare un'impostazione di protezione.
   - **Usa STARTTLS**: usa STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata per Active Directory, OpenLDAP o Altro, ma non è supportata per Microsoft Entra ID.
   - **Usa LDAPS**: l'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. È necessario selezionare questa opzione per Microsoft Entra ID.
   - **Non utilizzare TLS**: il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto. Questa opzione non è supportata per Microsoft Entra ID.

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

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

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

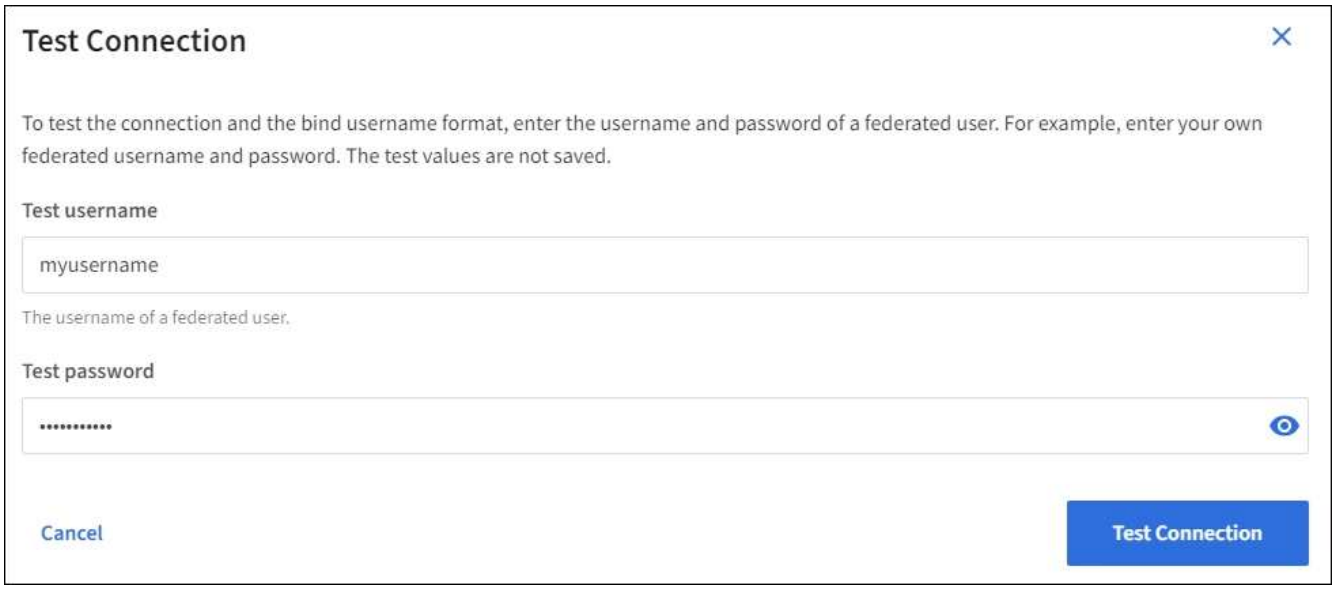
Verificare la connessione e salvare la configurazione

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

Fasi

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

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



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

Forzare la sincronizzazione con l'origine dell'identità

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

Fasi

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

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

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

Disattiva la federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione delle identità per gruppi e utenti. Quando la federazione delle identità è disabilitata, non c'è comunicazione tra StorageGRID e l'origine dell'identità. Tuttavia, tutte le impostazioni configurate vengono mantenute, consentendoti di riattivare facilmente la federazione delle identità in futuro.

A proposito di questa attività

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

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

- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non verrà eseguita e non verranno generati avvisi per gli account che non sono stati sincronizzati.
- La casella di controllo **Abilita federazione delle identità** è disabilitata se lo stato Single Sign-On (SSO) è **Abilitato** o **Modalità sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedere "Disattiva single sign-on" .

Fasi

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

Linee guida per la configurazione di un server OpenLDAP

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

> Per le origini identità che non sono Active Directory o Microsoft Entra ID, StorageGRID non bloccherà automaticamente l'accesso S3 agli utenti disabilitati esternamente. Per bloccare l'accesso S3, eliminare tutte le chiavi S3 dell'utente o rimuovere l'utente da tutti i gruppi.

MemberOf e refint overlay

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

Indicizzazione

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

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

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

Vedere le informazioni sulla manutenzione dell'appartenenza al gruppo inverso nella "Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4".

Gestire i gruppi di amministratori

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

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

Creare un gruppo di amministratori

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

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Gruppi amministratori**.
2. Selezionare **Crea gruppo**.

Scegliere un tipo di gruppo

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

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

Gruppo locale

Fasi

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

Gruppo federated

Fasi

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

Gestire le autorizzazioni di gruppo

Fasi

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

impostazioni e funzionalità.

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

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

2. Selezionare uno o più "autorizzazioni del gruppo di amministrazione".

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

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

Aggiunta di utenti (solo gruppi locali)

Fasi

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

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

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

Visualizzare e modificare i gruppi di amministratori

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

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

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli del gruppo	a. Selezionare la casella di controllo del gruppo. b. Selezionare **azioni** > **Visualizza dettagli gruppo**.	Selezionare il nome del gruppo nella tabella.

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

Duplicare un gruppo

Fasi

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

Eliminare un gruppo

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

Fasi

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

Autorizzazioni del gruppo di amministrazione

Quando si creano gruppi di utenti admin, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile

assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare quali attività possono essere eseguite dall'utente.

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

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

- Accedi a Grid Manager
- Visualizza la dashboard
- Visualizzare le pagine dei nodi
- Visualizzare gli avvisi correnti e risolti
- Modifica della propria password (solo utenti locali)
- Visualizzare alcune informazioni fornite nelle pagine Configurazione e manutenzione

Interazione tra permessi e modalità di accesso

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

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

Accesso root

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

Modificare la password root del tenant

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

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

ILM

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

- Regole
- Policy
- Tag policy

- Pool di storage
- Gradi di storage
- Regioni
- Ricerca dei metadati degli oggetti

> Per gestire i livelli di archiviazione, gli utenti devono disporre dell'autorizzazione **Altra configurazione della griglia**.

Manutenzione

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

- **Configurazione** > **Controllo accessi**:
  - Password di rete
- **Configurazione** > **Rete**:
  - Nomi di dominio degli endpoint S3
- **Manutenzione** > **Attività**:
  - Decommissionare
  - Espansione
  - Controllo dell'esistenza dell'oggetto
  - Recovery (recupero)
- **Manutenzione** > **Sistema**:
  - Pacchetto di recovery
  - Aggiornamento del software
- **Supporto** > **Strumenti**:
  - Registri

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

- **Manutenzione** > **Rete**:
  - Server DNS
  - Grid Network
  - Server NTP
- **Manutenzione** > **Sistema**:
  - Licenza
- **Configurazione** > **Rete**:
  - Nomi di dominio degli endpoint S3
- **Configurazione** > **Sicurezza**:
  - Certificati
- **Configurazione** > **Monitoraggio**:

    - Server syslog e audit

Gestire gli avvisi

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

Query sulle metriche

Questa autorizzazione consente di accedere a:

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

Ricerca dei metadati degli oggetti

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

Altra configurazione della griglia

Questa autorizzazione fornisce l'accesso alle seguenti opzioni aggiuntive di configurazione della griglia:

- **ILM**:
    - Gradi di storage
- **Configurazione** > **Sistema**:
- **Supporto** > **Altro**:
    - Costo del collegamento

Amministratore dell'appliance di storage

Questa autorizzazione fornisce:

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

Account tenant

Questa autorizzazione consente di:

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

Gestire gli utenti

È possibile visualizzare utenti locali e federati. È inoltre possibile creare utenti locali e

assegnarli a gruppi di amministratori locali per determinare a quali funzioni di Grid Manager possono accedere questi utenti.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "autorizzazioni di accesso specifiche".

Creare un utente locale

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

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

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

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

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Utenti amministratori**.
2. Selezionare **Crea utente**.

Immettere le credenziali dell'utente

Fasi

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

Assegnare ai gruppi

Fasi

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

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

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

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

Visualizzare e modificare gli utenti locali

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

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

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

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

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

Attività	Menu delle azioni	Pagina dei dettagli
Visualizzare i dettagli dell'utente	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**.	Selezionare il nome dell'utente nella tabella.
Modifica nome completo (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Modifica nome completo**. c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare l'icona di modifica . c. Inserire il nuovo nome. d. Selezionare **Save Changes** (Salva modifiche).
Negare o consentire l'accesso a StorageGRID	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda Access (accesso). d. Selezionare **Sì** per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare **No** per consentire all'utente di accedere. e. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Access (accesso). c. Selezionare **Sì** per impedire all'utente di accedere a Grid Manager o all'API Grid Management oppure selezionare **No** per consentire all'utente di accedere. d. Selezionare **Save Changes** (Salva modifiche).

Attività	Menu delle azioni	Pagina dei dettagli
Modifica della password (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda Password. d. Inserire una nuova password. e. Selezionare **Cambia password**.	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda Password. c. Inserire una nuova password. d. Selezionare **Cambia password**.
Modifica dei gruppi (solo utenti locali)	a. Selezionare la casella di controllo dell'utente. b. Selezionare **azioni** > **Visualizza dettagli utente**. c. Selezionare la scheda gruppi. d. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. e. Selezionare **Edit groups** (Modifica gruppi) per selezionare diversi gruppi. f. Selezionare **Save Changes** (Salva modifiche).	a. Selezionare il nome dell'utente per visualizzare i dettagli. b. Selezionare la scheda gruppi. c. Se si desidera, selezionare il collegamento dopo il nome di un gruppo per visualizzare i dettagli del gruppo in una nuova scheda del browser. d. Selezionare **Edit groups** (Modifica gruppi) per selezionare diversi gruppi. e. Selezionare **Save Changes** (Salva modifiche).

Importa utenti federati

È possibile importare uno o più utenti federati, fino a un massimo di 100 utenti, direttamente nella pagina Utenti.

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Utenti amministratori**.
2. Seleziona **Importa utenti federati**.
3. Inserisci l'UUID o il nome utente di uno o più utenti federati.

   Per voci multiple, aggiungere ogni UUID o nome utente su una nuova riga.

4. Selezionare **Importa**.

   Se l'importazione nel campo Utenti non riesce per uno o più utenti, procedere come segue:

   a. Espandi **Utenti non importati** e seleziona **Copia utenti**.
   b. Riprovare l'importazione selezionando **Precedente** e incollando gli utenti copiati nella finestra di dialogo **Importa utenti federati**.

   Dopo aver chiuso la finestra di dialogo **Importa utenti federati**, le informazioni sugli utenti federati

vengono visualizzate nella pagina Utenti per gli utenti importati correttamente.

Duplicare un utente

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

Fasi

1. Selezionare la casella di controllo dell'utente.
2. Selezionare **azioni** > **utente duplicato**.
3. Completare la procedura guidata Duplica utente.

Eliminare un utente

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

Impossibile eliminare l'utente root.

Fasi

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

Utilizzo di SSO (Single Sign-on)

Come funziona SSO

Quando è abilitato l'accesso Single Sign-On (SSO), gli utenti possono accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API solo se le loro credenziali sono autorizzate tramite il processo di accesso SSO implementato dalla tua organizzazione. Gli utenti locali non possono accedere a StorageGRID.

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

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

Effettuare l'accesso quando SSO è attivato

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

Fasi

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

   Viene visualizzata la pagina di accesso a StorageGRID.

   - Se è la prima volta che accedi all'URL su questo browser, ti verrà richiesto un ID account.

- Se hai già effettuato l'accesso a Grid Manager o Tenant Manager, ti verrà chiesto di selezionare un account recente o di immettere un ID account.

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

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

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

4. Accedi con le tue credenziali SSO.

   Se le credenziali SSO sono corrette:

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

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

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

   Non è necessario immettere nuovamente le credenziali SSO.

Disconnettersi quando SSO è attivato

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

Fasi

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

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

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

Se hai effettuato l'accesso a…	E ti disconnetterai da…	Sei disconnesso da…
Grid Manager su uno o più nodi di amministrazione	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi di amministrazione **Nota:** se si utilizza l'ID Entra per SSO, potrebbero essere necessari alcuni minuti per uscire da tutti i nodi amministrativi.
Tenant Manager su uno o più nodi di amministrazione	Tenant Manager su qualsiasi nodo di amministrazione	Tenant Manager su tutti i nodi di amministrazione
Sia Grid Manager che tenant Manager	Grid Manager	Solo Grid Manager. Per disconnettersi da SSO, devi anche disconnetterti da Tenant Manager.

Requisiti e considerazioni per SSO

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

Requisiti del provider di identità

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

- Active Directory Federation Service (ad FS)
- ID di accesso Microsoft
- PingFederate

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

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

Requisiti AD FS

È possibile utilizzare una delle seguenti versioni di ad FS:

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

> Windows Server 2016 deve utilizzare il "Aggiornamento KB3201845" o una versione successiva.

Requisiti aggiuntivi

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

Considerazioni per Entra ID

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

Requisiti dei certificati del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun nodo di amministrazione per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Quando si configurano trust di relying party (AD FS), applicazioni aziendali (Entra ID) o connessioni del provider di servizi (PingFederate) per StorageGRID, si utilizza il certificato del server come certificato di firma per le richieste StorageGRID .

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

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

È possibile accedere al certificato del server di un nodo amministrativo accedendo alla shell dei comandi del nodo e andando alla `/var/local/mgmt-api` directory. Un certificato server personalizzato è denominato `custom-server.crt`. Il certificato server predefinito del nodo è denominato `server.crt`.

Requisiti delle porte

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

Confermare che gli utenti federati possono accedere

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

Prima di iniziare

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

Fasi

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

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

   a. Accedi al tenant manager per ogni account tenant.
   b. Selezionare **Gestione accessi** > **Federazione identità**.
   c. Verificare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
   d. In tal caso, verificare che i gruppi federati che potrebbero essere in uso per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.
2. Verificare che un utente federated possa accedere a Grid Manager:
   a. Da Grid Manager, seleziona **Configurazione** > **Controllo accessi** > **Gruppi amministratori**.
   b. Assicurarsi che almeno un gruppo federated sia stato importato dall'origine dell'identità di Active Directory e che sia stata assegnata l'autorizzazione di accesso root.
   c. Disconnettersi.
   d. Confermare che è possibile accedere nuovamente a Grid Manager come utente nel gruppo federated.
3. Se sono presenti account tenant, verificare che un utente federated che dispone dell'autorizzazione di accesso root possa effettuare l'accesso:
   a. Da Grid Manager, seleziona **Inquilini**.
   b. Selezionare l'account tenant e selezionare **azioni** > **Modifica**.
   c. Nella scheda Immetti dettagli, selezionare **continua**.
   d. Se la casella di controllo **Usa origine identità propria** è selezionata, deselezionare la casella e selezionare **Salva**.

      Viene visualizzata la pagina del tenant.

   e. Selezionare l'account tenant, selezionare **Accedi** e accedere all'account tenant come utente root locale.
   f. Da Tenant Manager, seleziona **Gestione accessi** > **Gruppi**.
   g. Assicurarsi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di

accesso root per questo tenant.

h. Disconnettersi.

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

Informazioni correlate

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

Configurare SSO

È possibile seguire la procedura guidata Configura SSO e accedere alla modalità sandbox per configurare e testare l'accesso Single Sign-On (SSO) prima di abilitarlo per tutti gli utenti StorageGRID . Dopo aver abilitato l'SSO, è possibile tornare alla modalità sandbox quando necessario per modificare o testare nuovamente la configurazione.

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".
- Si dispone di "Autorizzazione di accesso root".
- Hai configurato la federazione delle identità per il tuo sistema StorageGRID.
- Per il tipo di servizio LDAP di federazione delle identità, hai selezionato Active Directory o Entra ID, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory Federation Service (ad FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

A proposito di questa attività

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

- La risposta di Active Directory o PingFederate include un UUID (Universally Unique Identifier) per l'utente.
- La risposta da Entra ID include un nome principale utente (UPN).

Per consentire a StorageGRID (il fornitore del servizio) e al fornitore di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti, è necessario completare queste attività:

1. Configurare le impostazioni in StorageGRID.
2. Utilizzare il software del provider di identità SSO per creare un trust della relying party (AD FS), un'applicazione aziendale (Entra ID) o un provider di servizi (PingFederate) per ciascun nodo

amministrativo.

3. Tornare a StorageGRID per abilitare SSO.

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

Accedere alla procedura guidata

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Single sign-on**. Viene visualizzata la pagina Single Sign-On.

   Se il pulsante Configura impostazioni SSO è disabilitato, conferma di aver configurato il provider di identità come origine dell'identità federata. Fare riferimento a "Requisiti e considerazioni per il single sign-on" .

2. Seleziona **Configura impostazioni SSO**. Viene visualizzata la pagina Fornisci dettagli provider di identità.

Fornire i dettagli del provider di identità

Fasi

1. Selezionare **tipo SSO** dall'elenco a discesa.
2. Se hai selezionato Active Directory come tipo di SSO, immetti il **Nome del servizio federativo** per il provider di identità, esattamente come appare in Active Directory Federation Service (AD FS).

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

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

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

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

     Se si modifica il certificato CA, eseguire immediatamente "Riavviare il servizio Mgmt-api sui nodi Admin"il test di un SSO corretto in Grid Manager.

4. Selezionare **Continua**. Viene visualizzata la pagina Fornisci l'identificativo della parte affidabile.

Fornire l’identificatore della parte affidabile

1. Compilare i campi nella pagina Fornisci identificatore della parte affidabile in base al tipo di SSO selezionato.

Active Directory

a. Specificare l'**identificatore della parte affidabile** per StorageGRID. Questo valore controlla il nome utilizzato per ogni trust della relying party in AD FS.

   - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere `SG` o `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]` . L'inclusione di questa stringa genera una tabella che mostra l'identificatore della parte affidabile per ciascun nodo di amministrazione nella griglia, in base al nome host del nodo.

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

b. Seleziona **Salva e accedi alla modalità sandbox**.

Entra ID

a. Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ciascuna applicazione aziendale in Entra ID.

   - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere `SG` o `StorageGRID`.
   - Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]` . L'inclusione di questa stringa genera una tabella che mostra il nome di un'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

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

b. Segui i passaggi in"Crea applicazioni aziendali in Entra ID" per creare un'applicazione aziendale per ogni nodo amministrativo elencato nella tabella.

c. Dall'ID Entra, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.

d. Dopo aver copiato e incollato un URL dei metadati di federazione per tutti i nodi amministrativi, seleziona **Salva e accedi alla modalità sandbox**.

PingFederate

a. Nella sezione Provider di servizi (SP), specificare **ID connessione SP** per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.

   - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere `SG` o `StorageGRID`.

- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]` . L'inclusione di questa stringa genera una tabella che mostra l'ID di connessione SP per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

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

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

   Utilizzare il seguente formato:

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

c. Seleziona **Salva e accedi alla modalità sandbox**.

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

Dopo aver salvato la configurazione ed essere entrati in modalità sandbox, è possibile completare e testare la configurazione per il tipo di SSO selezionato.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, solo gli utenti federati e gli utenti locali possono effettuare l'accesso.

Active Directory

Fasi

1. Accedere a Active Directory Federation Services (ad FS).
2. Creare uno o più trust di relying party per StorageGRID, utilizzando ciascun identificatore di relying party mostrato nella tabella nella pagina Configura SSO.

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

   Per istruzioni, vedere "Creazione di trust di parti di base in ad FS".

Entra ID

Fasi

1. Dalla pagina Single Sign-on (accesso singolo) per il nodo di amministrazione a cui si è attualmente connessi, selezionare il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi di amministrazione della griglia, ripetere questi passaggi:
   a. Accedere al nodo.
   b. Selezionare **Configurazione** > **Controllo accessi** > **Single sign-on**.
   c. Scaricare e salvare i metadati SAML per quel nodo.
3. Vai al portale di Azure.
4. Segui i passaggi in"Crea applicazioni aziendali in Entra ID" per caricare il file di metadati SAML per ciascun nodo amministrativo nella corrispondente applicazione aziendale Entra ID.

PingFederate

Fasi

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

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

Configurazione di prova

Prima di imporre l'uso dell'accesso singolo per l'intero sistema StorageGRID , verificare che l'accesso singolo e la disconnessione singola siano configurati correttamente per ciascun nodo di amministrazione.

Active Directory

Fasi

1. Nella pagina Configura SSO, individua il collegamento nel passaggio Configurazione test della procedura guidata.

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

2. Selezionare il collegamento oppure copiare e incollare l'URL in un browser per accedere alla pagina di accesso del provider di identità.
3. Per confermare che è possibile utilizzare SSO per accedere a StorageGRID, selezionare **Accedi a uno dei seguenti siti**, selezionare l'identificativo della parte di base per il nodo di amministrazione principale e selezionare **Accedi**.
4. Immettere il nome utente e la password federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.
   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
5. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

Entra ID

Fasi

1. Vai alla pagina Single Sign-on nel portale Azure.
2. Selezionare **Test dell'applicazione**.
3. Immettere le credenziali di un utente federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.
   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
4. Ripetere questa procedura per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

PingFederate

Fasi

1. Dalla pagina Configura SSO, seleziona il primo collegamento nel messaggio della modalità Sandbox.

   Selezionare e verificare un collegamento alla volta.

2. Immettere le credenziali di un utente federated.
   - Se le operazioni di accesso e disconnessione SSO hanno esito positivo, viene visualizzato un messaggio di esito positivo.
   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
3. Selezionare il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella griglia.

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

Attiva single sign-on

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

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

Fasi

1. Nel passaggio Configurazione test della procedura guidata di configurazione SSO, seleziona **Abilita SSO**.
2. Rivedi il messaggio di avviso e seleziona **Abilita SSO**.

   Ora è abilitato l'accesso singolo. Viene visualizzata la pagina Single Sign-On, che ora include i dettagli per l'SSO appena configurato.

3. Per modificare la configurazione, selezionare **Modifica**.
4. Per disabilitare l'accesso singolo, seleziona **Disabilita SSO**.

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

Creazione di trust di parti di base in ad FS

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

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **ad FS** come tipo di SSO.
- Hai"entrato in modalità sandbox" in Grid Manager.
- Conosci il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte affidabile per ciascun nodo di amministrazione nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina Configura SSO StorageGRID .

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

- Si dispone di esperienza nella creazione di trust di parti di supporto in ad FS o si dispone dell'accesso alla documentazione di Microsoft ad FS.

- Si sta utilizzando lo snap-in di gestione di ad FS e si appartiene al gruppo Administrators.
- Se si crea manualmente l'attendibilità del componente di base, si dispone del certificato personalizzato caricato per l'interfaccia di gestione di StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

A proposito di questa attività

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

Creare un trust di parte con Windows PowerShell

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

Fasi

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

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

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

   Viene visualizzato lo strumento di gestione di ad FS.
4. Selezionare **ad FS** > **Trust di parte**.

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

as Claims (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).

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

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

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

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

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

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

7. Verificare che i metadati siano stati importati correttamente.

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

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

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

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

9. Al termine, tornare a StorageGRID e"testare tutti i trust delle parti affidanti" per confermare che siano configurati correttamente.

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

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

Fasi

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

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

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

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

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

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

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

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

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

9. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
10. Al termine, tornare a StorageGRID e"testare tutti i trust delle parti affidanti" per confermare che siano configurati correttamente.

Creare manualmente un trust per la parte che si basa

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

Fasi

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

      Per coerenza, utilizzare l'identificativo parte di base per il nodo di amministrazione, esattamente come

appare nella pagina Single Sign-on in Grid Manager. Ad esempio, `SG-DC1-ADM1`.

b. Saltare il passaggio per configurare un certificato di crittografia token opzionale.

c. Nella pagina Configure URL (Configura URL), selezionare la casella di controllo **Enable support for the SAML 2.0 WebSSO Protocol** (attiva supporto per il protocollo SAML WebSSO).

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

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

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

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

Admin_Node_Identifier

Per *Admin_Node_Identifier*, immettere l'identificatore del gruppo di riferimento per il nodo di amministrazione, esattamente come viene visualizzato nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1`.

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

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

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

6. Per avviare la procedura guidata Claim Rule, selezionare **Add Rule**:

a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).

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

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

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

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

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

f. Selezionare **fine**, quindi **OK**.

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

8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):

a. Selezionare **Add SAML** (Aggiungi SAML).

b. Selezionare **Endpoint Type** > **SAML Logout**.

c. Selezionare **binding** > **Redirect**.

d. Nel campo **Trusted URL**, immettere l'URL utilizzato per la disconnessione singola (SLO) da questo nodo di amministrazione:

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

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

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per il trust della parte che si basa:

a. Aggiungere il certificato personalizzato:

- Se si dispone del certificato di gestione personalizzato caricato su StorageGRID, selezionare il certificato.
- Se non si dispone del certificato personalizzato, accedere al nodo Admin, andare nella directory del nodo `/var/local/mgmt-api` Admin e aggiungere il file del `custom-server.crt` certificato.

> (`server.crt`Si sconsiglia l'utilizzo del certificato predefinito del nodo amministrativo). Se il nodo Admin non riesce, il certificato predefinito viene rigenerato quando si ripristina il nodo ed è necessario aggiornare il trust della parte che si basa.

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

Le proprietà della parte di base vengono salvate e chiuse.

10. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
11. Al termine, tornare a StorageGRID e"testare tutti i trust delle parti affidanti" per confermare che siano configurati correttamente.

Crea applicazioni aziendali in Entra ID

Puoi utilizzare Entra ID per creare un'applicazione aziendale per ogni nodo amministrativo del tuo sistema.

Prima di iniziare

- Hai iniziato a configurare l'accesso Single Sign-On per StorageGRID e hai selezionato **Entra ID** come tipo di SSO.
- Hai"entrato in modalità sandbox" in Grid Manager.
- Per ogni nodo amministrativo del sistema è disponibile il **nome dell'applicazione aziendale**. È possibile copiare questi valori dalla tabella dei dettagli del nodo di amministrazione nella pagina Configura SSO.

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

- Hai esperienza nella creazione di applicazioni aziendali in Entra ID.

- Hai un account Entra ID con un abbonamento attivo.
- Nell'account Entra ID ricopri uno dei seguenti ruoli: Amministratore globale, Amministratore dell'applicazione cloud, Amministratore dell'applicazione o proprietario del servizio principale.

Accedi Entra ID

Fasi

1. Accedere a "Portale Azure".
2. Vai a "Entra ID" .
3. Selezionare "Applicazioni aziendali".

Creare applicazioni aziendali e salvare la configurazione SSO di StorageGRID

Per salvare la configurazione SSO per Entra ID in StorageGRID, è necessario utilizzare Entra ID per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copia gli URL dei metadati della federazione dall'ID Entra e incollali nei campi **URL metadati della federazione** corrispondenti nella pagina Configura SSO.

Fasi

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

Scarica i metadati SAML per ogni nodo di amministrazione

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

Fasi

1. Ripetere questi passaggi per ciascun nodo di amministrazione.
   a. Accedere a StorageGRID dal nodo di amministrazione.
   b. Selezionare **Configurazione** > **Controllo accessi** > **Single sign-on**.

c. Selezionare il pulsante per scaricare i metadati SAML per il nodo di amministrazione.

d. Salva il file che caricherai in Entra ID.

Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ciascun nodo di amministrazione StorageGRID , eseguire i seguenti passaggi in Entra ID:

Fasi

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

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

   a. Accedere alla pagina Proprietà dell'applicazione aziendale.

   b. Impostare **assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).

   c. Vai alla pagina Single Sign-on.

   d. Completare la configurazione SAML.

   e. Selezionare il pulsante **carica file di metadati** e selezionare il file di metadati SAML scaricato per il nodo di amministrazione corrispondente.

   f. Una volta caricato il file, selezionare **Salva**, quindi selezionare **X** per chiudere il riquadro. Viene visualizzata nuovamente la pagina Set up Single Sign-on with SAML (Configura Single Sign-on con SAML).

3. "Testare ogni applicazione" .

Creare connessioni SP (service provider) in PingFederate

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

Prima di iniziare

- È stato configurato Single Sign-on per StorageGRID ed è stato selezionato **Ping Federate** come tipo di SSO.
- Hai"entrato in modalità sandbox" in Grid Manager.
- Hai l'*ID di connessione SP * per ogni nodo amministrativo nel tuo sistema. Puoi trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina Configura SSO.
- Sono stati scaricati i **metadati SAML** per ciascun nodo di amministrazione nel sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Si dispone di "Guida di riferimento per l'amministratore" per PingFederate Server. La documentazione di PingFederate fornisce istruzioni dettagliate e spiegazioni dettagliate.
- Tu hai il"Autorizzazione amministratore" per PingFederate Server.

A proposito di questa attività

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

Completare i prerequisiti in PingFederate

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

Creare un archivio di dati

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

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

Crea validatore credenziale password

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

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

Crea istanza dell'adattatore IdP

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

Fasi

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

Creare o importare un certificato di firma

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

Fasi

1. Accedere a **sicurezza** > **chiavi e certificati di firma e decrittografia**.

2. Creare o importare il certificato di firma.

Creare una connessione SP in PingFederate

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

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

Scegliere il tipo di connessione SP

Fasi

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

Importare metadati SP

Fasi

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

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

4. Selezionare **Avanti**.

Configurare IdP browser SSO

Fasi

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

Istanza dell'adattatore di mappatura

Fasi

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

Configurare le impostazioni del protocollo

Fasi

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

Configurare le credenziali

Fasi

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

Creare ulteriori connessioni SP

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

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

Fasi

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

Disabilitare SSO

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

Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "browser web supportato".

- Si dispone di "autorizzazioni di accesso specifiche".

Fasi

1. Selezionare **Configurazione** > **Controllo accessi** > **Single sign-on**.

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

2. Seleziona **Disabilita SSO**.
3. Selezionare **Sì**.

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

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

Disabilitare e riabilitare temporaneamente SSO per un nodo di amministrazione

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

Prima di iniziare

- Si dispone di "autorizzazioni di accesso specifiche".
- Si dispone del `Passwords.txt` file.
- Si conosce la password dell'utente root locale.

A proposito di questa attività

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

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

Fasi

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

      Quando si è collegati come root, il prompt cambia da `$` a `#`.

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

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

3. Confermare che si desidera disattivare SSO.

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

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

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

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

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

7. Se l'SSO è stato disattivato temporaneamente perché era necessario accedere a Grid Manager per un altro motivo:
   a. Eseguire qualsiasi attività o attività da eseguire.
   b. Selezionare **Disconnetti** e chiudere Grid Manager.
   c. Riabilitare SSO sul nodo di amministrazione. È possibile eseguire una delle seguenti operazioni:

      - Eseguire il seguente comando: `enable-saml`

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

      Confermare che si desidera attivare SSO.

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

      - Riavviare il nodo della griglia: `reboot`

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

Informazioni sul copyright

Informazioni sul marchio commerciale