Controlla l'accesso a StorageGRID

StorageGRID software

NetApp
July 23, 2026

Sommario

Controlla l’accesso a StorageGRID

Controlla l’accesso a StorageGRID

Puoi controllare chi può accedere a StorageGRID e quali attività gli utenti possono svolgere creando o importando gruppi e utenti e assegnando le autorizzazioni a ciascun gruppo. Inoltre, puoi abilitare il single sign-on (SSO), creare certificati client e modificare le password della grid.

Controlla l’accesso al Grid Manager

Puoi determinare chi può accedere a Grid Manager e all’API di gestione di Grid importando gruppi e utenti da un servizio di federazione delle identità oppure configurando gruppi e utenti locali.

Usare "federazione di identità" rende più veloce la configurazione di "gruppi" e "${post_edited_translations.segment}" e permette agli utenti di accedere a StorageGRID usando le credenziali che già conoscono. Puoi configurare la federazione delle identità se usi Active Directory, OpenLDAP o Oracle Directory Server.

${post_edited_translations.segment}

Puoi determinare quali attività ogni utente può svolgere assegnando diversi "autorizzazioni" a ciascun gruppo. Ad esempio, potresti voler permettere agli utenti di un gruppo di gestire le regole ILM e agli utenti di un altro gruppo di eseguire attività di manutenzione. Un utente deve appartenere ad almeno un gruppo per accedere al sistema.

Facoltativamente, puoi configurare un gruppo come di sola lettura. Gli utenti di un gruppo di sola lettura possono solo visualizzare le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni in Grid Manager o Grid Management API.

Abilita single sign-on

Il sistema StorageGRID supporta il single sign-on (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0). Dopo aver "configura e abilita l’SSO", tutti gli utenti devono essere autenticati da un identity provider 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.

Modifica la passphrase di provisioning

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione e per scaricare il pacchetto di ripristino di StorageGRID. La passphrase è inoltre necessaria per scaricare i backup delle informazioni sulla topologia della grid e le chiavi di crittografia per il sistema StorageGRID. Puoi "${post_edited_translations.segment}" secondo necessità.

Cambia le password della console del nodo

Ogni nodo della tua griglia ha una password della console del nodo, che ti serve per accedere al nodo come "admin" tramite SSH o come utente root su una connessione alla console VM/fisica. Se necessario, puoi "cambia la password della console del nodo" per ogni nodo.

Modificare la passphrase di provisioning di StorageGRID

Usa questa procedura per cambiare la passphrase di provisioning di StorageGRID. La passphrase è necessaria per le procedure di ripristino, espansione e manutenzione. La passphrase è anche necessaria per scaricare i backup del pacchetto di ripristino che includono le informazioni sulla topologia della grid, le password della console dei nodi della grid e le chiavi di crittografia per il sistema StorageGRID.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai i permessi di accesso di manutenzione o utente root.
- Hai la passphrase di provisioning corrente.

Informazioni su questa attività

La passphrase di provisioning è necessaria per molte procedure di installazione e manutenzione, e per "download del pacchetto di ripristino". La passphrase di provisioning non è elencata nel file `Passwords.txt`. Assicurati di annotare la passphrase di provisioning e di conservarla in un luogo sicuro.

Passaggi

1. Seleziona **Configurazione** > **Controllo accessi** > **Password griglia**.
2. ${post_edited_translations.segment}
3. Inserisci la tua attuale passphrase di provisioning.
4. Inserisci la nuova frase di accesso. La frase di accesso deve contenere almeno 8 e non più di 32 caratteri. Le frasi di accesso distinguono tra maiuscole e minuscole.

   Conserva la passphrase di provisioning in un luogo sicuro. È necessaria per le procedure di installazione, espansione e manutenzione.

5. Reinserisci la nuova frase di accesso e seleziona **Salva**.

   ${post_edited_translations.segment}

6. Seleziona **Recovery Package**.
7. ${post_edited_translations.segment}

   Dopo aver modificato la passphrase di provisioning, devi scaricare immediatamente un nuovo pacchetto di ripristino. Il file del pacchetto di ripristino ti consente di ripristinare il sistema se si verifica un guasto.

Modificare le password della console dei nodi in StorageGRID

Ogni nodo della tua grid ha una password della console del nodo, che usi per accedere al

nodo. Per impostazione predefinita, ogni nodo ha una password univoca. Puoi modificare ciascuna password con una nuova password univoca, oppure puoi modificare la password di ogni nodo per utilizzare una password globale. Le password sono memorizzate nel pacchetto di ripristino.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di manutenzione o di accesso root".
- Hai la passphrase di provisioning corrente.

Informazioni su questa attività

Usi la password della console del nodo per accedere a un nodo come "admin" tramite SSH, oppure come utente root su una connessione alla console VM/fisica. Puoi cambiare le password della console del nodo usando una di queste opzioni:

- ${post_edited_translations.segment}
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

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

> Le "Password di accesso SSH" per 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.

Accedi al wizard

Passaggi

1. Seleziona **Configurazione** > **Controllo accessi** > **Password griglia**.
2. In **Modifica password della console del nodo**, seleziona **Effettua una modifica**.

${post_edited_translations.segment}

Prima di modificare le password della console del nodo, scarica il pacchetto di ripristino corrente. Puoi utilizzare le password in questo file se il processo di modifica della password non riesce per qualsiasi nodo.

Passaggi

1. Inserisci la passphrase di provisioning per la tua grid.
2. Seleziona **Scarica il pacchetto di ripristino**.
3. Copia il file del pacchetto di ripristino (`.zip` in due posizioni sicure, protette e separate.

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

4. Seleziona **Continue**.

Fornisci nuove password

1. ${post_edited_translations.segment}
   - **Automatico**: StorageGRID assegna automaticamente una nuova password casuale per la console a tutti i nodi.
   - ${post_edited_translations.segment}

${post_edited_translations.segment}

1. Seleziona **Continue**.

Personalizzato

1. Seleziona una delle seguenti:
   - **Password globale della console**: Applica la stessa password della console a tutti i nodi.
   - **Password univoche per la console**: Applica una password diversa a uno o più nodi.
2. Se hai selezionato **Password della console globale**, inserisci la password che vuoi usare per tutti i nodi.
3. Se hai selezionato **Password univoche per la console**, inserisci una password univoca per uno o più nodi.
4. Seleziona **Continue**.

Completa la modifica della password

1. ${post_edited_translations.segment}

   Non puoi annullare questo processo dopo che è stato avviato.

   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. Apri il file `.zip`.
4. Conferma che puoi accedere ai contenuti, 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 posizioni sicure, protette e separate.

   Non sovrascrivere il vecchio pacchetto di ripristino.

   ${post_edited_translations.segment}

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

   StorageGRID aggiorna la password per ciascun nodo.

   Se si verifica un errore durante il processo di aggiornamento, la barra di avanzamento mostra il numero di

nodi per i quali la modifica della password non è andata a buon fine. Il sistema riprova automaticamente il processo su qualsiasi nodo per il quale la modifica della password non è riuscita. Se al termine del processo alcuni nodi non hanno ancora la password modificata, compare il pulsante **Retry**.

8. Se l'aggiornamento della password non è riuscito per uno o più nodi:
   a. Esamina i messaggi di errore elencati nella tabella.
   b. Risolvi i problemi.
   c. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

9. Quando la barra di avanzamento indica che non ci sono più aggiornamenti, seleziona **Fine**.
10. Dopo aver modificato le password della console del nodo per tutti i nodi, elimina il primo pacchetto di ripristino che hai scaricato.

Modificare le password di accesso SSH per i nodi di amministrazione di StorageGRID

La modifica delle password di accesso SSH per i nodi di amministrazione aggiorna anche i set univoci di chiavi SSH interne per ciascun nodo della griglia. Il nodo di amministrazione principale utilizza queste chiavi SSH per accedere ai nodi tramite un'autenticazione sicura e senza password.

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

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di manutenzione o di accesso root".
- Hai la passphrase di provisioning corrente.

Informazioni su questa attività

Le nuove password di accesso per i nodi Admin 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. Queste non vengono modificate da questa procedura.

Accedi al wizard

Passaggi

1. Seleziona **Configurazione** > **Controllo accessi** > **Password griglia**.
2. ${post_edited_translations.segment}

${post_edited_translations.segment}

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

Passaggi

1. Inserisci la passphrase di provisioning per la tua grid.
2. Seleziona **Scarica il pacchetto di ripristino**.
3. Copia il file del pacchetto di ripristino (`.zip` in due posizioni sicure, protette e separate.

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

4. Seleziona **Continue**.
5. ${post_edited_translations.segment}

   Non puoi annullare questo processo dopo che è stato avviato.

Modifica le chiavi di accesso SSH

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

Passaggi

1. ${post_edited_translations.segment}
2. Quando il pulsante "Scarica nuovo pacchetto di ripristino" è abilitato, seleziona **Scarica nuovo pacchetto di ripristino** e salva il file del nuovo pacchetto di ripristino (`.zip` in due posizioni sicure, protette e separate.
3. Al termine del download:

   a. Apri il file `.zip`.

   b. Conferma di poter accedere ai contenuti, 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 posizioni sicure, protette e separate.

      Non sovrascrivere il vecchio pacchetto di ripristino.

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

4. Attendi che le chiavi si aggiornino su ciascun nodo, potrebbe volerci qualche minuto.

   ${post_edited_translations.segment}

   Se si verifica un errore durante il processo di aggiornamento, un messaggio banner elenca il numero di nodi per i quali non è stato possibile modificare le chiavi. Il sistema riproverà automaticamente il processo su qualsiasi nodo per cui non è stato possibile modificare la chiave. Se il processo termina e per alcuni nodi la chiave non è stata ancora modificata, viene visualizzato il pulsante **Riprova**.

${post_edited_translations.segment}

a. Esamina i messaggi di errore elencati nella tabella.

b. Risolvi i problemi.

c. ${post_edited_translations.segment}

${post_edited_translations.segment}

5. Dopo aver modificato le chiavi di accesso SSH per tutti i nodi, elimina il file primo pacchetto di ripristino che hai scaricato.
6. Facoltativamente, seleziona **Manutenzione** > **Sistema** > **Pacchetto di ripristino** per scaricare una copia aggiuntiva del nuovo pacchetto di ripristino.

Usa la federazione delle identità in StorageGRID

${post_edited_translations.segment}

Configura la federazione delle identità per Grid Manager

Puoi configurare la federazione delle identità in Grid Manager se vuoi che i gruppi di amministratori e gli utenti siano gestiti in un altro sistema, come 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".
- Hai "autorizzazioni di accesso specifiche".
- Stai utilizzando Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server come provider di identità.

> Se vuoi usare un servizio LDAP v3 che non è presente nell'elenco, contatta il supporto tecnico.

- Se vuoi usare OpenLDAP, devi configurare il server OpenLDAP. Vedi <<${post_edited_translations.segment}>>.
- Se intendi abilitare il single sign-on (SSO), hai esaminato il "requisiti e considerazioni per single sign-on".
- Se prevedi di utilizzare Transport Layer Security (TLS) per le comunicazioni con il LDAP server, il provider di identità utilizza TLS 1.2 o 1.3. Vedi "Algoritmi di crittografia supportati per le connessioni TLS in uscita".

Informazioni su questa attività

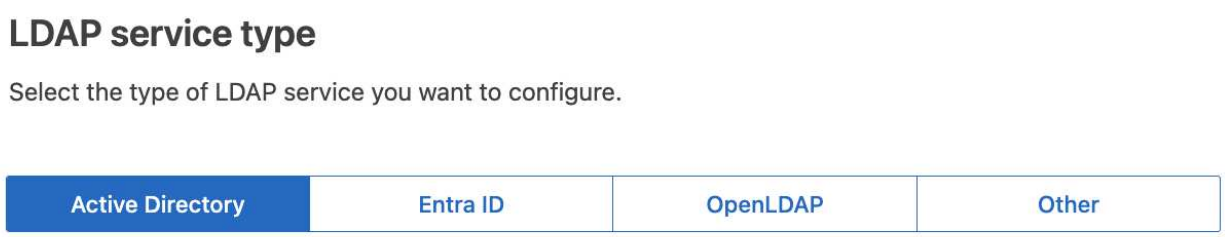
Puoi configurare un'origine di identità per Grid Manager se vuoi importare gruppi da un altro sistema come Active Directory, Microsoft Entra ID, OpenLDAP o Oracle Directory Server. Puoi importare i seguenti tipi di gruppi:

- Gruppi admin. Gli utenti nei gruppi admin possono accedere a Grid Manager ed eseguire attività, in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per i tenant che non utilizzano la propria origine dell'identità. Gli utenti nei gruppi tenant possono accedere al Tenant Manager ed eseguire attività, in base ai permessi assegnati al gruppo nel Tenant Manager. Vedi "Crea account tenant" e "Usa un tenant account" per i dettagli.

Inserisci la configurazione

Passaggi

1. ${post_edited_translations.segment}
2. Seleziona **Abilita federazione delle identità**.
3. Nella sezione relativa al tipo di servizio LDAP, seleziona il tipo di servizio LDAP che vuoi configurare.



   Seleziona **Altro** per configurare i valori per un LDAP server che usa Oracle Directory Server.

4. Se hai selezionato **Altro**, compila i campi nella sezione Attributi LDAP. Altrimenti, passa al passaggio successivo.
   - **Nome univoco utente**: Il nome dell'attributo che contiene l'identificativo 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'identificativo 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 a 16 byte o stringa, dove i trattini vengono ignorati.
   - **Nome univoco del gruppo**: il nome dell'attributo che contiene l'identificativo 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 del gruppo**: Il nome dell'attributo che contiene l'identificativo 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 a 16 byte o stringa, dove i trattini vengono ignorati.
5. Per tutti i tipi di servizio LDAP, inserisci le informazioni richieste sul server LDAP e sulla connessione di rete nella sezione Configura server LDAP.
   - **Hostname**: Il fully qualified domain name (FQDN) o l'indirizzo IP del LDAP server.
   - **Porta**: La porta utilizzata per connettersi al LDAP server.

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

   - **Nome utente**: Il full path del distinguished name (DN) dell'utente che si connetterà al LDAP server.

     Per Active Directory, puoi anche specificare il Down-Level Logon Name o lo User Principal Name.

L'utente specificato deve avere l'autorizzazione per visualizzare l'elenco di 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`
- **Entra ID**: `accountEnabled` e `userPrincipalName`

◦ **Password**: La password associata al nome utente.

> Se in futuro cambierai la password, dovrai aggiornarla su questa pagina.

◦ **DN di base del gruppo**: il full path del nome distinto (DN) per un sottoalbero LDAP in cui vuoi cercare i gruppi. Nell'esempio di Active Directory (sotto), tutti i gruppi il cui nome distinto è relativo al DN di base (DC=storagegrid,DC=example,DC=com) possono essere usati come gruppi federati.

> ${post_edited_translations.segment}

◦ **DN della base utente**: Il full path del nome distinto (DN) di un sottoalbero LDAP in cui vuoi cercare gli utenti.

> I valori del **nome univoco utente** devono essere univoci all'interno del **User Base DN** a cui appartengono.

◦ ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

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

  Inserisci **[USERNAME]** esattamente come è scritto.

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

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

7. Se hai selezionato STARTTLS o LDAPS, scegli il certificato utilizzato per proteggere la connessione.
   - **Utilizza il certificato CA del sistema operativo**: Utilizza il certificato CA Grid predefinito installato sul sistema operativo per proteggere le connessioni.
   - **Utilizza un certificato CA personalizzato**: Utilizza un certificato di sicurezza personalizzato.

     Se selezioni questa impostazione, copia e incolla il certificato di sicurezza personalizzato nella casella di testo del certificato CA.

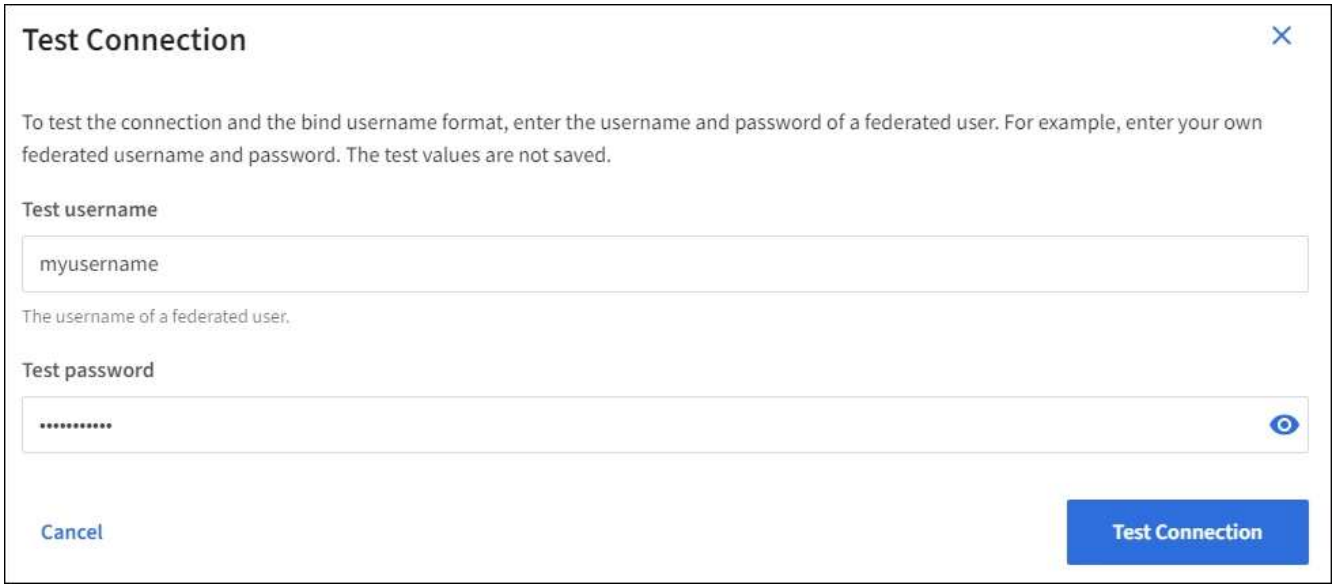
Verifica la connessione e salva la configurazione

Dopo aver inserito tutti i valori, devi testare la connessione prima di poter salvare la configurazione. StorageGRID verifica le impostazioni di connessione per il LDAP server e il formato del nome utente di bind, se ne hai fornito uno.

Passaggi

1. Seleziona **Test connessione**.
2. Se non hai fornito un formato per il nome utente bind:
   - Viene visualizzato il messaggio "Test di connessione riuscito" se le impostazioni di connessione sono valide. Seleziona **Salva** per salvare la configurazione.
   - Viene visualizzato il messaggio "Impossibile stabilire la connessione di prova" se le impostazioni di connessione non sono valide. Seleziona **Chiudi**. Quindi, risolvi eventuali problemi e prova nuovamente la connessione.
3. Se hai specificato un formato di nome utente di bind, inserisci il nome utente e la password di un utente federato valido.

   Ad esempio, inserisci il tuo nome utente e la tua password. Non includere caratteri speciali nel nome utente, come @ o /.



   - Viene visualizzato il messaggio "Test di connessione riuscito" se le impostazioni di connessione sono valide. Seleziona **Salva** per salvare la configurazione.

- Viene visualizzato un messaggio di errore se le impostazioni di connessione, il formato del nome utente di bind o il nome utente e la password di test non sono validi. Risolvi eventuali problemi e prova nuovamente la connessione.

${post_edited_translations.segment}

Il sistema StorageGRID sincronizza periodicamente gruppi e utenti federati dalla sorgente di identità. Puoi forzare l'avvio della sincronizzazione se vuoi abilitare o limitare le autorizzazioni degli utenti il più rapidamente possibile.

Passaggi

1. Vai alla pagina di federazione delle identità.
2. ${post_edited_translations.segment}

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

   ${post_edited_translations.segment}

Disabilita la federazione delle identità

Puoi disabilitare 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 delle identità. Tuttavia, tutte le impostazioni che hai configurato vengono mantenute, permettendoti di riattivare facilmente la federazione delle identità in futuro.

Informazioni su questa attività

Prima di disabilitare la federazione delle identità, dovresti tenere presente quanto segue:

- Gli utenti federati non potranno accedere.
- Gli utenti federati attualmente connessi manterranno l'accesso al sistema StorageGRID fino alla scadenza della loro sessione, ma non potranno accedere dopo la scadenza della sessione.
- ${post_edited_translations.segment}
- La casella di controllo **Abilita federazione delle identità** è disabilitata se lo stato del single sign-on (SSO) è **Abilitato** o **Modalità Sandbox**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabilitato** prima di poter disabilitare la federazione delle identità. Vedi "${post_edited_translations.segment}".

Passaggi

1. Vai alla pagina di federazione delle identità.
2. Deseleziona la casella di controllo **Abilita federazione delle identità**.

${post_edited_translations.segment}

Se vuoi usare un server OpenLDAP per la federazione delle identità, devi configurare impostazioni specifiche sul server OpenLDAP.

Per le origini di identità diverse da Active Directory o Microsoft Entra ID, StorageGRID non bloccherà automaticamente l'accesso S3 per gli utenti disabilitati esternamente. Per bloccare l'accesso S3, elimina tutte le chiavi S3 dell'utente o rimuovi l'utente da tutti i gruppi.

Sovrapposizioni Memberof e Refint

Le sovrapposizioni memberof e refint devono essere abilitate. Per ulteriori informazioni, consulta le istruzioni per la manutenzione della membership inversa del gruppo nel "Documentazione di OpenLDAP: Guida dell'amministratore versione 2.4".

Indicizzazione

${post_edited_translations.segment}

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

Inoltre, assicurati che i campi menzionati nell'aiuto per Nome utente siano indicizzati per prestazioni ottimali.

Vedi le informazioni sulla manutenzione dell'appartenenza inversa ai gruppi nel "Documentazione di OpenLDAP: Guida dell'amministratore versione 2.4".

Gestisci i gruppi di amministratori in StorageGRID

Puoi creare gruppi di amministratori per gestire le autorizzazioni di sicurezza per uno o più utenti amministratori. Gli utenti devono appartenere a un gruppo per ottenere l'accesso al sistema StorageGRID.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".
- Se vuoi importare un gruppo federato, devi aver configurato la federazione delle identità e il gruppo federato deve già esistere nell'origine identità configurata.

Crea un gruppo di amministratori

I gruppi di amministratori ti permettono di decidere quali utenti possono accedere a quali funzionalità e operazioni in Grid Manager e nella Grid Management API.

Accedi al wizard

Passaggi

1. Seleziona **Configuration** > **Access control** > **Admin groups**.
2. Seleziona **Crea gruppo**.

Scegli un tipo di gruppo

Puoi creare un gruppo locale o importare un gruppo federato.

- Crea un gruppo locale se vuoi assegnare autorizzazioni agli utenti locali.
- Crea un gruppo federato per importare utenti dalla fonte di identità.

Gruppo locale

Passaggi

1. Seleziona **Gruppo locale**.
2. Inserisci un nome visualizzato per il gruppo, che puoi aggiornare in seguito in base alle esigenze. Ad esempio, "Maintenance Users" o "ILM Administrators."
3. Inserisci un nome univoco per il gruppo, che non puoi aggiornare in seguito.
4. Seleziona **Continue**.

Gruppo federato

Passaggi

1. Seleziona **Gruppo federato**.
2. Inserisci il nome del gruppo che vuoi importare, esattamente come appare nell'origine identità configurata.
   - Per Active Directory e Microsoft Entra ID, usa sAMAccountName.
   - Per OpenLDAP, usa il CN (Common Name).
   - Per un altro LDAP, usa il nome univoco appropriato per il LDAP server.
3. Seleziona **Continue**.

Gestisci le autorizzazioni di gruppo

Passaggi

1. Per la **Modalità di accesso**, seleziona se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nella Grid Management API oppure se possono solo visualizzare impostazioni e funzionalità.
   - **Lettura-scrittura** (impostazione predefinita): puoi modificare le impostazioni ed eseguire le operazioni consentite dalle tue autorizzazioni di gestione.
   - **Sola lettura**: Gli utenti possono solo visualizzare le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nel Grid Manager o Grid Management API. Gli utenti locali con privilegi di sola lettura possono cambiare la propria password.

     Se un utente appartiene a più gruppi e uno qualsiasi di essi è impostato su **Read-only**, l'utente avrà accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

2. Seleziona uno o più "permessi del gruppo admin".

   Devi assegnare almeno un'autorizzazione a ogni gruppo; altrimenti, gli utenti che appartengono al gruppo non potranno accedere a StorageGRID.

3. Se stai creando un gruppo locale, seleziona **Continua**. Se stai creando un gruppo federato, seleziona **Crea gruppo** e **Fine**.

Aggiungi utenti (solo gruppi locali)

Passaggi

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

Se non hai ancora creato utenti locali, puoi salvare il gruppo senza aggiungere utenti. Puoi aggiungere questo gruppo all'utente nella pagina Utenti. Vedi "Gestisci utenti" per i dettagli.

2. Seleziona **Crea gruppo** e **Fine**.

Visualizza e modifica i gruppi di amministratori

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

- Per visualizzare le informazioni di base relative a tutti i gruppi, consulta la tabella nella pagina Gruppi.
- ${post_edited_translations.segment}

Attività	Menu azioni	Pagina dei dettagli
Visualizza i dettagli del gruppo	a. ${post_edited_translations.segment} b. Seleziona **Azioni** > **Visualizza dettagli del gruppo**.	Seleziona il nome del gruppo nella tabella.
Modifica il nome visualizzato (solo gruppi locali)	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. Seleziona **Salva modifiche**.	a. Seleziona il nome del gruppo per visualizzarne i dettagli. b. Seleziona l'icona di modifica . c. ${post_edited_translations.segment} d. Seleziona **Salva modifiche**.
Modifica la modalità di accesso o le autorizzazioni	a. ${post_edited_translations.segment} b. Seleziona **Azioni** > **Visualizza dettagli del gruppo**. c. ${post_edited_translations.segment} d. Facoltativamente, seleziona o deseleziona "permessi del gruppo admin". e. Seleziona **Salva modifiche**.	a. Seleziona il nome del gruppo per visualizzarne i dettagli. b. ${post_edited_translations.segment} c. Facoltativamente, seleziona o deseleziona "permessi del gruppo admin". d. Seleziona **Salva modifiche**.

${post_edited_translations.segment}

Passaggi

1. ${post_edited_translations.segment}
2. Seleziona **Azioni** > **Duplica gruppo**.
3. Completa la procedura guidata Duplica gruppo.

Elimina un gruppo

Puoi eliminare un gruppo admin quando desideri rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni associate al gruppo. L'eliminazione di un gruppo admin rimuove tutti gli utenti dal gruppo, ma non elimina gli utenti.

Passaggi

1. Dalla pagina Gruppi, seleziona la casella di controllo per ogni gruppo che vuoi rimuovere.
2. Seleziona **Azioni** > **Elimina gruppo**.
3. ${post_edited_translations.segment}

Autorizzazioni del gruppo amministratore in StorageGRID

Quando crei gruppi di utenti admin, selezioni una o più autorizzazioni per controllare l'accesso a specifiche funzionalità di Grid Manager. Puoi poi assegnare ogni utente a uno o più di questi gruppi admin per decidere quali attività può svolgere.

Devi assegnare almeno un'autorizzazione a ciascun gruppo; altrimenti, gli utenti appartenenti a quel gruppo non potranno accedere a Grid Manager o alla Grid Management API.

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

- Accedi al Grid Manager
- Visualizza la dashboard
- Visualizza le pagine dei nodi
- Visualizza gli avvisi correnti e risolti
- Cambiare la propria password (solo per utenti locali)
- Visualizza alcune informazioni fornite nelle pagine di configurazione e manutenzione

Interazione tra autorizzazioni e modalità di accesso

Per tutte le autorizzazioni, l'impostazione **Modalità di accesso** del gruppo determina se puoi modificare le impostazioni ed eseguire operazioni oppure se puoi solo visualizzare le impostazioni e le funzionalità correlate. Se appartieni a più gruppi e uno qualsiasi di essi è impostato su **Sola lettura**, avrai accesso in sola lettura a tutte le impostazioni e funzionalità selezionate.

Le sezioni seguenti descrivono le autorizzazioni che puoi assegnare quando crei o modifichi un gruppo di amministratori. Qualsiasi funzionalità non esplicitamente menzionata richiede l'autorizzazione **Root access**.

Accesso root

Questa autorizzazione consente l'accesso a tutte le funzionalità di amministrazione della griglia.

Cambia la password di root del tenant

Questa autorizzazione fornisce l'accesso all'opzione **Modifica password root** nella pagina Tenant, consentendoti 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 la funzionalità di importazione delle chiavi S3 è abilitata. Gli utenti che non hanno questa autorizzazione non possono visualizzare l'opzione **Modifica password root**.

> Per concedere l'accesso alla pagina Tenant, che contiene l'opzione **Cambia password di root**, assegna anche l'autorizzazione **Account Tenant**.

ILM

Questa autorizzazione consente l'accesso alle seguenti opzioni del menu **ILM**:

- Regole
- ${post_edited_translations.segment}
- Tag dei criteri
- Pool di storage
- classi di storage
- Regioni
- ${post_edited_translations.segment}

${post_edited_translations.segment}

Manutenzione

Gli utenti devono avere l'autorizzazione di manutenzione per usare queste opzioni:

- **Configurazione** > **Controllo accessi**:
  - ${post_edited_translations.segment}
- **Configurazione** > **Rete**:
  - ${post_edited_translations.segment}
- **Manutenzione** > **Attività**:
  - ${post_edited_translations.segment}
  - Espansione
  - Verifica dell'esistenza dell'oggetto
  - Recupero
- ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
  - ${post_edited_translations.segment}
- **Support** > **Strumenti**:
  - ${post_edited_translations.segment}

Gli utenti che non dispongono dell'autorizzazione di manutenzione possono visualizzare, ma non modificare, queste pagine:

- ${post_edited_translations.segment}
  - Server DNS
  - ${post_edited_translations.segment}
  - Server NTP
- ${post_edited_translations.segment}
  - Licenza

- **Configurazione** > **Rete**:
  - ${post_edited_translations.segment}
- ${post_edited_translations.segment}
  - Certificati
- ${post_edited_translations.segment}
  - Server di audit e syslog

Gestisci gli avvisi

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

${post_edited_translations.segment}

${post_edited_translations.segment}

- **Support** > **Strumenti** > **Metriche** page
- Query personalizzate delle metriche di Prometheus usando la sezione **Metriche** della Grid Management API
- Schede del dashboard di Grid Manager che contengono metriche

${post_edited_translations.segment}

Questa autorizzazione consente l'accesso alla pagina **ILM** > **Ricerca metadati oggetto**.

Altre configurazioni della griglia

${post_edited_translations.segment}

- **ILM**:
  - classi di storage
- **Configurazione** > **Sistema**:
- **Assistenza** > **Altro**:
  - Costo del collegamento

${post_edited_translations.segment}

Questa autorizzazione consente di:

- Accesso a E-Series SANtricity System Manager sulle appliance di storage tramite Grid Manager.
- La possibilità di eseguire attività di risoluzione dei problemi e di manutenzione nella scheda Gestisci unità per i dispositivi che supportano queste operazioni.

Account tenant

${post_edited_translations.segment}

- ${post_edited_translations.segment}
- Visualizza le politiche di classificazione del traffico esistenti
- ${post_edited_translations.segment}

Gestisci gli utenti in StorageGRID

Puoi visualizzare gli utenti locali e federati. Puoi anche creare utenti locali e assegnarli a gruppi di amministratori locali per determinare a quali funzionalità di Grid Manager questi utenti possono accedere.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Crea un utente locale

Puoi creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi locali. Le autorizzazioni del gruppo controllano a quali funzionalità di Grid Manager e Grid Management API l'utente può accedere.

Puoi creare solo utenti locali. Usa l'origine di identità esterna per gestire utenti e gruppi federati.

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

Se single sign-on (SSO) è abilitato, gli utenti locali non possono accedere a StorageGRID.

Accedi al wizard

Passaggi

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

Inserisci le credenziali utente

Passaggi

1. ${post_edited_translations.segment}
2. Facoltativamente, seleziona **Sì** se questo utente non deve avere accesso a Grid Manager o Grid Management API.
3. Seleziona **Continue**.

Assegna ai gruppi

Passaggi

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

   Se non hai ancora creato gruppi, puoi salvare l'utente senza selezionare gruppi. Puoi aggiungere questo utente a un gruppo nella pagina Gruppi.

   Se un utente appartiene a più gruppi, le autorizzazioni sono cumulative. Vedi "${post_edited_translations.segment}" per i dettagli.

2. Seleziona **Crea utente** e seleziona **Fine**.

Visualizza e modifica gli utenti locali

Puoi visualizzare i dettagli per gli utenti locali e federati esistenti. Puoi modificare un utente locale per cambiarne il nome completo, la password o l'appartenenza ai gruppi. Puoi anche impedire temporaneamente a un utente di accedere a Grid Manager e alla Grid Management API.

Puoi modificare solo gli utenti locali. Usa l'origine dell'identità esterna per gestire gli utenti federati.

- Per visualizzare le informazioni di base relative a tutti gli utenti locali e federati, consulta la tabella nella pagina Utenti.
- Per visualizzare tutti i dettagli di un utente specifico, modificare un utente locale o cambiare la password di un utente locale, usa il menu **Azioni** o la pagina dei dettagli.

  ${post_edited_translations.segment}

> Gli utenti locali possono cambiare la propria password usando l'opzione **Cambia password** nel banner di Grid Manager.

Attività	Menu azioni	Pagina dei dettagli
Visualizza i dettagli dell'utente	a. Seleziona la casella di controllo per l'utente. b. ${post_edited_translations.segment}	Seleziona il nome dell'utente nella tabella.
Modifica il nome completo (solo per utenti locali)	a. Seleziona la casella di controllo per l'utente. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. Seleziona **Salva modifiche**.	a. ${post_edited_translations.segment} b. Seleziona l'icona di modifica . c. ${post_edited_translations.segment} d. Seleziona **Salva modifiche**.
Negare o consentire l'accesso a StorageGRID	a. Seleziona la casella di controllo per l'utente. b. ${post_edited_translations.segment} c. Seleziona la scheda Access. d. Seleziona **Sì** per impedire all'utente di accedere a Grid Manager o alla Grid Management API, oppure seleziona **No** per consentire all'utente di accedere. e. Seleziona **Salva modifiche**.	a. ${post_edited_translations.segment} b. Seleziona la scheda Access. c. Seleziona **Sì** per impedire all'utente di accedere a Grid Manager o alla Grid Management API, oppure seleziona **No** per consentire all'utente di accedere. d. Seleziona **Salva modifiche**.

Attività	Menu azioni	Pagina dei dettagli
${post_edited_translations.segment}	a. Seleziona la casella di controllo per l'utente. b. ${post_edited_translations.segment} c. ${post_edited_translations.segment} d. Inserisci una nuova password. e. Seleziona **Cambia password**.	a. ${post_edited_translations.segment} b. ${post_edited_translations.segment} c. Inserisci una nuova password. d. Seleziona **Cambia password**.
${post_edited_translations.segment}	a. Seleziona la casella di controllo per l'utente. b. ${post_edited_translations.segment} c. Seleziona la scheda Gruppi. d. Facoltativamente, seleziona il link accanto al nome di un gruppo per visualizzarne i dettagli in una nuova scheda del browser. e. Seleziona **Modifica gruppi** per selezionare gruppi diversi. f. Seleziona **Salva modifiche**.	a. ${post_edited_translations.segment} b. Seleziona la scheda Gruppi. c. Facoltativamente, seleziona il link accanto al nome di un gruppo per visualizzarne i dettagli in una nuova scheda del browser. d. Seleziona **Modifica gruppi** per selezionare gruppi diversi. e. Seleziona **Salva modifiche**.

Importa utenti federati

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

Passaggi

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

   Per inserire più voci, aggiungi ogni UUID o nome utente su una nuova riga.

4. Seleziona **Import**.

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

   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}

${post_edited_translations.segment}

Duplica un utente

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

Passaggi

1. Seleziona la casella di controllo per l'utente.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}

Elimina un utente

Puoi eliminare un utente locale per rimuoverlo definitivamente dal sistema.

Non puoi eliminare l'utente root.

Passaggi

1. Dalla pagina Utenti, seleziona la casella di controllo per ogni utente che vuoi rimuovere.
2. Seleziona **Azioni** > **Elimina utente**.
3. Seleziona **Elimina utente**.

Usa single sign-on (SSO)

Scopri l'SSO di StorageGRID

Quando il single sign-on (SSO) è abilitato, 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 il single sign-on (SSO) utilizzando lo standard Security Assertion Markup Language 2.0 (SAML 2.0).

Prima di abilitare il single sign-on (SSO), verifica come i processi di accesso e disconnessione di StorageGRID vengono influenzati quando l'SSO è abilitato.

${post_edited_translations.segment}

Quando l'SSO è abilitato e accedi a StorageGRID, vieni reindirizzato alla pagina SSO della tua organizzazione per convalidare le tue credenziali.

Passaggi

1. Inserisci il fully qualified domain name o l'indirizzo IP di qualsiasi StorageGRID Admin Node in un browser web.

   Viene visualizzata la pagina di accesso di StorageGRID.

   - ${post_edited_translations.segment}
   - Se in precedenza hai effettuato l'accesso a Grid Manager o a Tenant Manager, ti viene chiesto di selezionare un account recente o di inserire un account ID.

La pagina di accesso di StorageGRID non viene visualizzata quando inserisci l'URL completo per un tenant account (cioè un fully qualified domain name o un indirizzo IP seguito da `/?accountId=20-digit-account-id`). Invece, vieni immediatamente reindirizzato alla pagina di accesso SSO della tua organizzazione, dove puoi Accedi con le tue credenziali SSO.

2. ${post_edited_translations.segment}
   - Per accedere a Grid Manager, lascia vuoto il campo **ID account**, inserisci **0** come ID account oppure seleziona **Grid Manager** se compare nell'elenco degli account recenti.
   - Per accedere al Tenant Manager, inserisci l'ID account tenant di 20 cifre oppure seleziona un tenant per nome se compare nell'elenco degli account recenti.
3. ${post_edited_translations.segment}

   StorageGRID ti reindirizza alla pagina di accesso SSO della tua organizzazione. Ad esempio:

4. Accedi con le tue credenziali SSO.

   ${post_edited_translations.segment}

   a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
   b. StorageGRID convalida la risposta di autenticazione.
   c. ${post_edited_translations.segment}

   Se l'account di servizio non è accessibile, puoi comunque accedere, purché tu sia un utente esistente che appartiene a un gruppo federato con autorizzazioni di accesso a StorageGRID.

5. Facoltativamente, puoi accedere ad altri Admin Node, oppure al Grid Manager o al Tenant Manager, se hai le autorizzazioni adeguate.

   Non devi reinserire le credenziali SSO.

${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

1. Individua il link **Esci** nell'angolo in alto a destra dell'interfaccia utente.
2. Seleziona **Esci**.

   Viene visualizzata la pagina di accesso a StorageGRID. Il menu a tendina **Account recenti** viene aggiornato per includere **Grid Manager** o il nome del tenant, così puoi accedere più rapidamente a queste interfacce utente in futuro.

   La tabella riassume cosa succede quando esci se stai usando una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID tramite più sessioni del browser, devi uscire da ogni sessione separatamente.

Se hai effettuato l'accesso a…	E ti disconnetti da…	Sei uscito da…
Grid Manager su uno o più Admin Node	Grid Manager su qualsiasi Admin Node	Grid Manager su tutti i nodi di amministrazione **Nota:** Se usi Entra ID per il single sign-on, potrebbe volerci qualche minuto per essere disconnesso da tutti i nodi di amministrazione.
Tenant Manager su uno o più Admin Node	Tenant Manager su qualsiasi nodo amministrativo	${post_edited_translations.segment}
Sia Grid Manager che Tenant Manager	Grid Manager	Solo Grid Manager. Devi disconnetterti anche da Tenant Manager per disconnetterti da SSO.

Requisiti e considerazioni per StorageGRID SSO

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

Requisiti dell'identity provider

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

- Active Directory Federation Service (AD FS)
- Microsoft Entra ID
- PingFederate

Devi configurare la federazione delle identità per il sistema StorageGRID prima di poter configurare un provider di identità SSO. Il tipo di servizio LDAP che usi per la federazione delle identità determina quale tipo di SSO puoi implementare.

Tipo di servizio LDAP configurato	${post_edited_translations.segment}
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Requisiti AD FS

Puoi usare una qualsiasi delle seguenti versioni di AD FS:

- Windows Server 2022 AD FS

- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

> Windows Server 2016 dovrebbe utilizzare la "Aggiornamento KB3201845", o superiore.

Requisiti aggiuntivi

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

Considerazioni per Entra ID

Se usi Entra ID come tipo di single sign-on e gli utenti hanno nomi principali utente che non usano sAMAccountName come prefisso, possono verificarsi problemi di accesso se StorageGRID perde la connessione con il LDAP server. Per permettere agli utenti di accedere, devi ripristinare la connessione al LDAP server.

Requisiti del certificato del server

Per impostazione predefinita, StorageGRID utilizza un certificato di interfaccia di gestione su ciascun Admin Node per proteggere l'accesso a Grid Manager, Tenant Manager, Grid Management API e Tenant Management API. Quando configuri relying party trusts (AD FS), enterprise applications (Entra ID) o service provider connections (PingFederate) per StorageGRID, usi il certificato del server come certificato di firma per le richieste StorageGRID.

Se non l'hai ancora fatto "ho configurato un certificato personalizzato per l'interfaccia di gestione", dovresti farlo ora. Quando installi un certificato server personalizzato, viene utilizzato per tutti gli Admin Node e puoi usarlo in tutte le relying party trust, applicazioni enterprise o connessioni SP di StorageGRID.

> Si sconsiglia di utilizzare il certificato server predefinito di un Admin Node in una relying party trust, enterprise application o connessione SP. Se il nodo si guasta e lo ripristini, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo ripristinato, devi aggiornare la relying party trust, enterprise application o connessione SP con il nuovo certificato.

Puoi accedere al certificato server di un Admin Node effettuando l'accesso alla shell dei comandi del nodo e andando nella `/var/local/mgmt-api` directory. Un certificato server personalizzato si chiama `custom-server.crt`. Il certificato server predefinito del nodo si chiama `server.crt`.

Requisiti delle porte

Il single sign-on (SSO) non è disponibile sulle porte con restrizioni di Grid Manager o Tenant Manager. Devi usare la porta HTTPS predefinita (443) se vuoi che gli utenti si autentichino con il single sign-on. Vedi "Controlla l'accesso tramite firewall esterno".

${post_edited_translations.segment}

${post_edited_translations.segment}

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

- ${post_edited_translations.segment}

Passaggi

1. ${post_edited_translations.segment}

   Quando abiliti l'SSO, l'origine di identità configurata nel Tenant Manager viene sovrascritta dall'origine di identità configurata nel Grid Manager. Gli utenti appartenenti all'origine di identità del tenant non potranno più accedere a meno che non abbiano un account con l'origine di identità del Grid Manager.

   a. Accedi al Tenant Manager per ciascun tenant account.
   b. Seleziona **Gestione accessi** > **Federazione delle identità**.
   c. Verifica che la casella di controllo **Abilita federazione delle identità** non sia selezionata.
   d. ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   a. Da Grid Manager, seleziona **Configurazione** > **Controllo accessi** > **Gruppi di amministratori**.
   b. Assicurati che almeno un gruppo federato sia stato importato dall'origine identità di Active Directory e che gli sia stato assegnato il permesso di accesso Root.
   c. ${post_edited_translations.segment}
   d. Conferma che puoi accedere nuovamente a Grid Manager come utente del gruppo federato.
3. Se sono presenti account tenant, verifica che un utente federato con autorizzazione di accesso Root possa effettuare l'accesso:
   a. Dal Grid Manager, seleziona **Tenants**.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}

      ${post_edited_translations.segment}

   e. ${post_edited_translations.segment}
   f. ${post_edited_translations.segment}
   g. Assicurati che ad almeno un gruppo federato del Grid Manager sia stato assegnato il permesso di accesso Root per questo tenant.
   h. ${post_edited_translations.segment}
   i. Conferma che puoi accedere di nuovo al tenant come utente del gruppo federato.

Informazioni correlate

- "Requisiti e considerazioni per single sign-on"
- "${post_edited_translations.segment}"
- "Usa un tenant account"

Configura il single sign-on in StorageGRID

Puoi seguire la procedura guidata di configurazione dell'SSO ed entrare in modalità

sandbox per configurare e testare il single sign-on (SSO) prima di abilitarlo per tutti gli utenti di StorageGRID. Dopo che l'SSO è stato abilitato, puoi tornare alla modalità sandbox quando necessario per modificare o ritestare la configurazione.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai il "Permesso di accesso root".
- ${post_edited_translations.segment}
- ${post_edited_translations.segment}

Tipo di servizio LDAP configurato	${post_edited_translations.segment}
Active Directory Federation Service (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

Informazioni su questa attività

Quando l'SSO è abilitato e un utente tenta di accedere a un Admin Node, StorageGRID invia una richiesta di autenticazione al SSO identity provider. A sua volta, il SSO identity provider invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autenticazione ha avuto successo. Per le richieste riuscite:

- La risposta di Active Directory o PingFederate include un identificatore univoco universale (UUID) per l'utente.
- La risposta di Entra ID include un User Principal Name (UPN).

Per consentire a StorageGRID (il service provider) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti, devi completare queste attività:

1. ${post_edited_translations.segment}
2. Usa il software del provider di identità SSO per creare un'attendibilità relying party (AD FS), un'applicazione aziendale (Entra ID) o un Service Provider (PingFederate) per ciascun Admin Node.
3. Torna a StorageGRID per abilitare l'SSO.

La modalità sandbox semplifica la configurazione avanti e indietro e ti permette di testare tutte le impostazioni prima di abilitare SSO. Quando usi la modalità sandbox, gli utenti non possono accedere tramite SSO.

Accedi al wizard

Passaggi

1. Seleziona **Configurazione** > **Controllo dell'accesso** > **Single sign-on**. Viene visualizzata la pagina Single sign-on.

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

2. Seleziona **Configure SSO settings**. Viene visualizzata la pagina Provide identity provider details.

Fornisci i dettagli del provider di identità

Passaggi

1. ${post_edited_translations.segment}
2. Se hai selezionato Active Directory come tipo di SSO, inserisci il **Federation service name** per il provider di identità, esattamente come appare in Active Directory Federation Service (AD FS).

   Per individuare il nome del servizio di federazione, vai su Windows Server Manager. Seleziona **Tools** > **AD FS Management**. Dal menu Action, seleziona **Edit Federation Service Properties**. Il Federation Service Name viene mostrato nel secondo campo.

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

     Se selezioni questa impostazione, copia il testo del certificato personalizzato e incollalo nella casella di testo **Certificato CA**.

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

     Se modifichi il certificato CA, "${post_edited_translations.segment}"e verifica subito che l'SSO in Grid Manager abbia esito positivo.

4. Seleziona **Continua**. Viene visualizzata la pagina Fornisci l'identificativo del relying party.

Fornisci l'identificativo della relying party

1. Completa i campi nella pagina "Fornisci l'identificativo della relying party" in base al tipo di SSO che hai selezionato.

Active Directory

a. Specifica l'**identificatore del relying party** per StorageGRID. Questo valore controlla il nome utilizzato per ciascun trust del relying party in AD FS.

   - Ad esempio, se la griglia ha un solo nodo amministratore e non pensi di aggiungerne altri in futuro, inserisci `SG` o `StorageGRID`.
   - Se la tua grid include più di un nodo Admin, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. L'inclusione di questa stringa genera una tabella che mostra l'identificatore del relying party per ciascun nodo Admin nella grid, in base all'hostname del nodo.

   > Devi creare una relazione di attendibilità relying party per ciascun Admin Node nel tuo sistema StorageGRID. La presenza di una relazione di attendibilità relying party per ciascun Admin Node garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node.

b. Seleziona **Salva ed entra in modalità sandbox**.

Entra ID

a. Nella sezione Applicazione aziendale, specifica il **nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome che usi per ogni applicazione aziendale in Entra ID.

   - Ad esempio, se la griglia ha un solo nodo amministratore e non pensi di aggiungerne altri in futuro, inserisci `SG` o `StorageGRID`.
   - Se la tua griglia include più di un Admin Node, includi la stringa `[HOSTNAME]` nell'identificatore. Per esempio, `SG-[HOSTNAME]`. Includere questa stringa genera una tabella che mostra un nome di applicazione aziendale per ciascun Admin Node nel tuo sistema, in base all'hostname del nodo.

   > Devi creare un'applicazione aziendale per ciascun nodo Admin nel tuo sistema StorageGRID. La presenza di un'applicazione aziendale per ciascun nodo Admin garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi nodo Admin.

b. Segui i passaggi descritti in "${post_edited_translations.segment}" per creare un'applicazione aziendale per ciascun Admin Node elencato nella tabella.

c. Da Entra ID, copia l'URL dei metadati di federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **Federation metadata URL** corrispondente in StorageGRID.

d. Dopo aver copiato e incollato un URL dei metadati di federazione per tutti gli Admin Node, seleziona **Salva ed entra in modalità sandbox**.

PingFederate

a. Nella sezione service provider (SP), specifica l'**ID connessione SP** per StorageGRID. Questo valore controlla il nome che utilizzi per ciascuna connessione SP in PingFederate.

   - Ad esempio, se la griglia ha un solo nodo amministratore e non pensi di aggiungerne altri in futuro, inserisci `SG` o `StorageGRID`.
   - Se la tua griglia include più di un Admin Node, includi la stringa `[HOSTNAME]` nell'identificatore. Per esempio, `SG-[HOSTNAME]`. Includere questa stringa genera una tabella che mostra l'ID di connessione SP per ogni Admin Node nel tuo sistema, in base

all'hostname del nodo.

> Devi creare una connessione SP per ciascun Admin Node nel tuo sistema StorageGRID. La presenza di una connessione SP per ciascun Admin Node garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node.

b. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

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

c. Seleziona **Salva ed entra in modalità sandbox**.

${post_edited_translations.segment}

${post_edited_translations.segment}

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

Active Directory

Passaggi

1. Vai su Active Directory Federation Services (AD FS).
2. Crea uno o più relying party trust per StorageGRID, utilizzando ciascun relying party identifier mostrato nella tabella nella pagina Configura SSO.

   Devi creare una relazione di trust per ogni Admin Node mostrato nella tabella.

   Per le istruzioni, vai a "Crea trust di parti affidabili in AD FS".

Entra ID

Passaggi

1. Dalla pagina Single sign-on per l'Admin Node a cui sei attualmente connesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministratore nella tua griglia, ripeti questi passaggi:
   a. Accedi al nodo.
   b. Seleziona **Configurazione** > **Controllo accessi** > **Single sign-on**.
   c. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. Segui i passaggi in "${post_edited_translations.segment}" per caricare il file di metadati SAML per ciascun Admin Node nella corrispondente applicazione enterprise Entra ID.

PingFederate

Passaggi

1. Dalla pagina Single sign-on per l'Admin Node a cui sei attualmente connesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministratore nella tua griglia, ripeti questi passaggi:
   a. Accedi al nodo.
   b. Seleziona **Configurazione** > **Controllo accessi** > **Single sign-on**.
   c. ${post_edited_translations.segment}
3. Vai su PingFederate.
4. "Crea una o più connessioni service provider (SP) per StorageGRID". Usa l'ID di connessione SP per ogni nodo Admin (mostrato nella tabella nella pagina Configura SSO) e i metadati SAML che hai scaricato per quel nodo Admin.

   Devi creare una connessione SP per ogni Admin Node mostrato nella tabella.

${post_edited_translations.segment}

Prima di imporre l'utilizzo del single sign-on per l'intero sistema StorageGRID, assicurati che single sign-on e single logout siano configurati correttamente per ciascun Admin Node.

Active Directory

Passaggi

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

2. Seleziona il link oppure copia e incolla l'URL in un browser per accedere alla pagina di sign-on del tuo identity provider.
3. ${post_edited_translations.segment}
4. Inserisci il tuo nome utente federato e la tua password.
   - ${post_edited_translations.segment}
   - Se l'operazione SSO non va a buon fine, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
5. ${post_edited_translations.segment}

Entra ID

Passaggi

1. Vai alla pagina di single sign-on nel portale Azure.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Se l'operazione SSO non va a buon fine, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
4. ${post_edited_translations.segment}

PingFederate

Passaggi

1. ${post_edited_translations.segment}

   ${post_edited_translations.segment}

2. ${post_edited_translations.segment}
   - ${post_edited_translations.segment}
   - Se l'operazione SSO non va a buon fine, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
3. ${post_edited_translations.segment}

   Se visualizzi il messaggio "Pagina scaduta", seleziona il pulsante **Indietro** nel tuo browser e inserisci nuovamente le tue credenziali.

Abilita single sign-on

${post_edited_translations.segment}

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

Passaggi

1. ${post_edited_translations.segment}
2. ${post_edited_translations.segment}

   Il single sign-on è ora abilitato. Viene visualizzata la pagina Single sign-on, che ora include i dettagli per l'SSO che hai appena configurato.

3. Per modificare la configurazione, seleziona **Modifica**.
4. ${post_edited_translations.segment}

Se usi il portale di Azure e accedi a StorageGRID dallo stesso computer che usi per accedere a Entra ID, assicurati che l'utente del portale di Azure sia anche un utente autorizzato di StorageGRID (un utente in un gruppo federato importato in StorageGRID) oppure esci dal portale di Azure prima di provare ad accedere a StorageGRID.

Crea trust di relying party in AD FS per StorageGRID

Devi usare Active Directory Federation Services (AD FS) per creare una relying party trust per ogni Admin Node nel tuo sistema. Puoi creare relying party trust usando i comandi PowerShell, importando i metadati SAML da StorageGRID o inserendo i dati manualmente.

Prima di iniziare

- ${post_edited_translations.segment}
- Hai "modalità sandbox attivata" in Grid Manager.
- Conosci il fully qualified domain name (o l'indirizzo IP) e l'identificatore del relying party per ciascun Admin Node nel tuo sistema. Puoi trovare questi valori nella tabella dei dettagli degli Admin Node nella pagina Configure SSO di StorageGRID.

  Devi creare una relazione di attendibilità relying party per ciascun Admin Node nel tuo sistema StorageGRID. La presenza di una relazione di attendibilità relying party per ciascun Admin Node garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi Admin Node.

- ${post_edited_translations.segment}
- Stai utilizzando lo snap-in Gestione AD FS e appartieni al gruppo Administrators.
- ${post_edited_translations.segment}

Informazioni su questa attività

Queste istruzioni si applicano a Windows Server 2016 AD FS. Se usi una versione diversa di AD FS, noterai lievi differenze nella procedura. Consulta la documentazione di Microsoft AD FS se hai domande.

Crea un trust di relying party utilizzando Windows PowerShell

Puoi usare Windows PowerShell per creare rapidamente uno o più trust di terze parti.

Passaggi

1. Dal menu Start di Windows, fai clic con il pulsante destro del mouse sull'icona PowerShell e seleziona **Esegui come amministratore**.
2. Al prompt dei comandi di PowerShell, immetti il seguente comando:

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

   - Per *Admin_Node_Identifier*, inserisci il Relying Party Identifier per l'Admin Node, esattamente come appare nella pagina di single sign-on. Ad esempio, `SG-DC1-ADM1`.
   - Per *Admin_Node_FQDN*, inserisci il fully qualified domain name per lo stesso Admin Node. (Se necessario, puoi usare l'indirizzo IP del nodo invece. Tuttavia, se inserisci un indirizzo IP qui, tieni presente che dovrai aggiornare o ricreare questa relying party trust se quell'indirizzo IP dovesse mai cambiare.)
3. Da Windows Server Manager, seleziona **Strumenti** > **Gestione AD FS**.

   Viene visualizzato lo strumento di gestione di AD FS.
4. Seleziona **AD FS** > **Relying Party Trusts**.

   Viene visualizzato l'elenco dei relying party trust.
5. Aggiungi una policy di controllo degli accessi al trust della relying party appena creato:
   a. Individua il trust della parte affidabile che hai appena creato.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. ${post_edited_translations.segment}
6. Aggiungi una Claim Issuance Policy al Relying Party Trust appena creato:
   a. Individua il trust della parte affidabile che hai appena creato.
   b. ${post_edited_translations.segment}
   c. ${post_edited_translations.segment}
   d. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come attestazioni** dall'elenco e seleziona **Avanti**.
   e. ${post_edited_translations.segment}

      Ad esempio, **ObjectGUID to Name ID** o **UPN to Name ID**.

   f. Per l'archivio attributi, seleziona **Active Directory**.
   g. Nella colonna Attributo LDAP della tabella Mapping, digita **objectGUID** oppure seleziona **User-Principal-Name**.
   h. Nella colonna Tipo di reclamo in uscita della tabella di mappatura, seleziona **Name ID** dall'elenco a discesa.
   i. Seleziona **Fine** e seleziona **OK**.

7. Conferma che i metadati sono stati importati correttamente.
   a. Fai clic con il pulsante destro del mouse sul relying party trust per aprirne le proprietà.
   b. Conferma che i campi nelle schede **Endpoints**, **Identifiers** e **Signature** siano compilati.

      Se i metadati sono mancanti, verifica che l'indirizzo dei metadati della Federation sia corretto oppure inserisci i valori manualmente.
8. Ripeti questi passaggi per configurare una relying party trust per tutti i nodi di amministrazione nel tuo sistema StorageGRID.
9. Al termine, torna a StorageGRID e "testa tutti i trust della relying party" per verificare che siano configurati correttamente.

Crea un trust della relying party importando i metadati di federazione

Puoi importare i valori per ogni relying party trust accedendo ai metadati SAML per ogni Admin Node.

Passaggi

1. In Windows Server Manager, seleziona **Strumenti** e poi **Gestione AD FS**.
2. Nella sezione Azioni, seleziona **Aggiungi attendibilità della parte affidabile**.
3. Nella pagina di benvenuto, scegli **Claims aware** e seleziona **Start**.
4. Seleziona **Importa i dati relativi alla parte affidabile pubblicati online o su una rete locale**.
5. In **Federation metadata address (host name o URL)**, digita la posizione dei metadati SAML per questo Admin Node:

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

   Per *`Admin_Node_FQDN`*, inserisci il fully qualified domain name per lo stesso Admin Node. (Se necessario, puoi usare l'indirizzo IP del nodo invece. Tuttavia, se inserisci un indirizzo IP qui, tieni presente che dovrai aggiornare o ricreare questa relying party trust se quell'indirizzo IP dovesse mai cambiare.)
6. Completa la procedura guidata per la creazione del trust della relying party, salva il trust della relying party e chiudi la procedura guidata.

   Quando inserisci il nome visualizzato, usa il Relying Party Identifier per l'Admin Node, esattamente come appare nella pagina single sign-on nel Grid Manager. Ad esempio, `SG-DC1-ADM1`.
7. Aggiungi una regola di claim:
   a. ${post_edited_translations.segment}
   b. ${post_edited_translations.segment}
   c. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come attestazioni** dall'elenco e seleziona **Avanti**.
   d. ${post_edited_translations.segment}

      Ad esempio, **ObjectGUID to Name ID** o **UPN to Name ID**.
   e. Per l'archivio attributi, seleziona **Active Directory**.
   f. Nella colonna Attributo LDAP della tabella Mapping, digita **objectGUID** oppure seleziona **User-**

Principal-Name.

g. Nella colonna Tipo di reclamo in uscita della tabella di mappatura, seleziona **Name ID** dall'elenco a discesa.

h. Seleziona **Fine** e seleziona **OK**.

8. Conferma che i metadati sono stati importati correttamente.

a. Fai clic con il pulsante destro del mouse sul relying party trust per aprirne le proprietà.

b. Conferma che i campi nelle schede **Endpoints**, **Identifiers** e **Signature** siano compilati.

Se i metadati sono mancanti, verifica che l'indirizzo dei metadati della Federation sia corretto oppure inserisci i valori manualmente.

9. Ripeti questi passaggi per configurare una relying party trust per tutti i nodi di amministrazione nel tuo sistema StorageGRID.

10. Quando hai finito, torna a StorageGRID e "testa tutti i trust della relying party" per confermare che siano configurati correttamente.

Crea manualmente un trust della relying party

${post_edited_translations.segment}

Passaggi

1. In Windows Server Manager, seleziona **Strumenti** e poi **Gestione AD FS**.
2. Nella sezione Azioni, seleziona **Aggiungi attendibilità della parte affidabile**.
3. Nella pagina di benvenuto, scegli **Claims aware** e seleziona **Start**.
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}

a. ${post_edited_translations.segment}

Per coerenza, usa il Relying Party Identifier per il nodo Admin, esattamente come appare nella pagina Single Sign-on in Grid Manager. Ad esempio, `SG-DC1-ADM1`.

b. Salta il passaggio per configurare un certificato di crittografia del token facoltativo.

c. Nella pagina Configura URL, seleziona la casella di controllo **Abilita il supporto per il protocollo SAML 2.0 WebSSO**.

d. Inserisci l'URL dell'endpoint del servizio SAML per l'Admin Node:

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

Per *`Admin_Node_FQDN`*, inserisci il fully qualified domain name per l'Admin Node. (Se necessario, puoi usare l'indirizzo IP del nodo al suo posto. Tuttavia, se inserisci un indirizzo IP qui, tieni presente che dovrai aggiornare o ricreare questa relying party trust se quell'indirizzo IP dovesse mai cambiare.)

e. Nella pagina Configura identificatori, specifica l'identificativo della Relying Party per lo stesso Admin Node:

`Admin_Node_Identifier`

Per *`Admin_Node_Identifier`*, inserisci il Relying Party Identifier per l'Admin Node, esattamente

come appare nella pagina di single sign-on. Ad esempio, `SG-DC1-ADM1`.

f. ${post_edited_translations.segment}

Viene visualizzata la finestra di dialogo Edit Claim Issuance Policy.

> Se la finestra di dialogo non viene visualizzata, fai clic con il pulsante destro del mouse sul trust e seleziona **Modifica i criteri di emissione dei sinistri**.

6. Per avviare la procedura guidata Regola di rivendicazione, seleziona **Aggiungi regola**:
   a. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come attestazioni** dall'elenco e seleziona **Avanti**.
   b. ${post_edited_translations.segment}

      Ad esempio, **ObjectGUID to Name ID** o **UPN to Name ID**.

   c. Per l'archivio attributi, seleziona **Active Directory**.
   d. Nella colonna Attributo LDAP della tabella Mapping, digita **objectGUID** oppure seleziona **User-Principal-Name**.
   e. Nella colonna Tipo di reclamo in uscita della tabella di mappatura, seleziona **Name ID** dall'elenco a discesa.
   f. Seleziona **Fine** e seleziona **OK**.
7. Fai clic con il pulsante destro del mouse sul relying party trust per aprirne le proprietà.
8. Nella scheda **Endpoint**, configura l'endpoint per il single logout (SLO):
   a. Seleziona **Aggiungi SAML**.
   b. ${post_edited_translations.segment}
   c. Seleziona **Associazione** > **Reindirizzamento**.
   d. ${post_edited_translations.segment}

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

   Per *`Admin_Node_FQDN`*, inserisci il fully qualified domain name del nodo Admin. (Se necessario, puoi usare l'indirizzo IP del nodo invece. Tuttavia, se inserisci un indirizzo IP qui, tieni presente che dovrai aggiornare o ricreare questa relying party trust se quell'indirizzo IP dovesse mai cambiare.)

   a. Seleziona **OK**.
9. ${post_edited_translations.segment}
   a. ${post_edited_translations.segment}
      - ${post_edited_translations.segment}
      - Se non hai il certificato personalizzato, accedi al nodo di amministrazione, vai alla directory `/var/local/mgmt-api` del nodo di amministrazione e aggiungi il file del certificato `custom-server.crt`.

> L'utilizzo del certificato predefinito dell'Admin Node (`server.crt`) non è consigliato. Se l'Admin Node si guasta, il certificato predefinito verrà rigenerato quando ripristini il nodo e dovrai aggiornare il relying party trust.

b. Seleziona **Applica** e poi **OK**.

${post_edited_translations.segment}

10. Ripeti questi passaggi per configurare una relying party trust per tutti i nodi di amministrazione nel tuo sistema StorageGRID.
11. Quando hai finito, torna a StorageGRID e "testa tutti i trust della relying party" per confermare che siano configurati correttamente.

Crea applicazioni aziendali in Entra ID per StorageGRID

Usi Entra ID per creare un'applicazione aziendale per ogni Admin Node nel tuo sistema.

Prima di iniziare

- Hai iniziato a configurare il single sign-on per StorageGRID e hai selezionato **Entra ID** come tipo di SSO.
- Hai "modalità sandbox attivata" in Grid Manager.
- Hai il **Enterprise application name** per ogni Admin Node nel tuo sistema. Puoi copiare questi valori dalla tabella dei dettagli dell'Admin Node nella pagina Configura SSO.

> Devi creare un'applicazione aziendale per ciascun nodo Admin nel tuo sistema StorageGRID. La presenza di un'applicazione aziendale per ciascun nodo Admin garantisce che gli utenti possano accedere e disconnettersi in modo sicuro da qualsiasi nodo Admin.

- Hai esperienza nella creazione di applicazioni aziendali in Entra ID.
- ${post_edited_translations.segment}
- Hai uno dei seguenti ruoli nell'account Entra ID: Global Administrator, Cloud Application Administrator, Application Administrator o owner del service principal.

Accedi Entra ID

Passaggi

1. Accedi al "Azure Portal".
2. Vai a "Entra ID".
3. Seleziona "Applicazioni aziendali".

${post_edited_translations.segment}

Per salvare la configurazione SSO per Entra ID in StorageGRID, devi usare Entra ID per creare un'applicazione aziendale per ogni Admin Node. Copia gli URL dei metadati di federazione da Entra ID e incollali nei corrispondenti campi **Federation metadata URL** nella pagina Configura SSO.

Passaggi

1. Ripeti i seguenti passaggi per ciascun Admin Node.
   a. ${post_edited_translations.segment}
   b. Seleziona **Crea la tua applicazione**.
   c. Per il nome, inserisci il **nome dell'applicazione aziendale** che hai copiato dalla tabella dei dettagli dell'Admin Node nella pagina Configura SSO.

d. Lascia selezionata l'opzione **Integra qualsiasi altra applicazione che non trovi nella galleria (Non-gallery)**.

e. Seleziona **Create**.

f. Seleziona il collegamento **Inizia** nella **2. Configura single sign-on** oppure seleziona il collegamento **single sign-on** nel margine sinistro.

g. Seleziona la casella **SAML**.

h. ${post_edited_translations.segment}

i. Vai alla pagina Configura SSO e incolla l'URL nel campo **Federation metadata URL** che corrisponde al **Enterprise application name** che hai utilizzato.

2. ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

1. Ripeti questi passaggi per ogni Admin Node.
   a. ${post_edited_translations.segment}
   b. Seleziona **Configurazione** > **Controllo accessi** > **Single sign-on**.
   c. Seleziona il pulsante per scaricare i metadati SAML per quel nodo amministratore.
   d. Salva il file, che caricherai su Entra ID.

${post_edited_translations.segment}

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

Passaggi

1. Torna al portale Azure.
2. Ripeti questi passaggi per ogni applicazione aziendale:

   > Potresti dover aggiornare la pagina delle applicazioni aziendali per vedere le applicazioni che hai aggiunto in precedenza nell'elenco.

   a. Vai alla pagina Proprietà dell'applicazione aziendale.
   b. Imposta **Assegnazione richiesta** su **No** (a meno che tu non voglia configurare le assegnazioni separatamente).
   c. Vai alla pagina di single sign-on.
   d. Completa la configurazione SAML.
   e. Seleziona il pulsante **Carica file di metadati** e seleziona il file di metadati SAML che hai scaricato per il nodo Admin corrispondente.
   f. Dopo il caricamento del file, seleziona **Salva** e poi **X** per chiudere il riquadro. Tornerai alla pagina Set up Single Sign-On with SAML.
3. "Testa ogni applicazione".

Crea connessioni service provider in PingFederate per StorageGRID

Usi PingFederate per creare una connessione service provider (SP) per ogni Admin Node nel tuo sistema. Per velocizzare il processo, importerai i metadati SAML da StorageGRID.

Prima di iniziare

- Hai configurato il single sign-on per StorageGRID e hai selezionato **Ping Federate** come tipo di SSO.
- Hai "modalità sandbox attivata" in Grid Manager.
- Disponi dell'**ID connessione SP** per ciascun nodo di amministrazione nel tuo sistema. Puoi trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina Configura SSO.
- Hai scaricato i **metadati SAML** per ciascun Admin Node nel tuo sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Hai il "Guida di riferimento per l'amministratore" per il server PingFederate. La documentazione di PingFederate fornisce istruzioni dettagliate passo passo e spiegazioni.
- Hai il "Autorizzazione amministratore" per il server PingFederate.

Informazioni su questa attività

Queste istruzioni riassumono come configurare il server PingFederate versione 10.3 come provider SSO per StorageGRID. Se stai utilizzando un'altra versione di PingFederate, potresti dover adattare queste istruzioni. Consulta la documentazione del server PingFederate per istruzioni dettagliate relative alla tua versione.

Completa i prerequisiti in PingFederate

Prima di poter creare le connessioni SP che utilizzerai per StorageGRID, devi completare le attività preliminari in PingFederate. Utilizzerai le informazioni di questi prerequisiti quando configurerai le connessioni SP.

Crea archivio dati

Se non l'hai ancora fatto, crea un archivio dati per connettere PingFederate al LDAP server di AD FS. Utilizza i valori che hai usato quando "configurare la federazione delle identità" in StorageGRID.

- **Tipo**: Directory (LDAP)
- **Tipo di LDAP**: Active Directory
- **Nome attributo binario**: Inserisci **objectGUID** nella scheda Attributi binari LDAP esattamente come mostrato.

Crea un validatore di credenziali password

Se non l'hai ancora fatto, crea un validatore di credenziali per le password.

- **Tipo**: Validatore di credenziali LDAP Username Password
- ${post_edited_translations.segment}
- **Base di ricerca**: Inserisci le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca**: sAMAccountName=${username}
- ${post_edited_translations.segment}

${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

1. Vai su **Autenticazione** > **Integrazione** > **IdP Adapters**.
2. Seleziona **Crea nuova istanza**.
3. Nella scheda Tipo, seleziona **HTML Form IdP Adapter**.
4. ${post_edited_translations.segment}
5. Seleziona validatore delle credenziali della password che hai creato.
6. ${post_edited_translations.segment}
7. Seleziona **Salva**.

Crea o importa un certificato di firma

Se non l'hai ancora fatto, crea o importa il certificato di firma.

Passaggi

1. ${post_edited_translations.segment}
2. Crea o importa il certificato di firma.

Crea una connessione SP in PingFederate

Quando crei una connessione SP in PingFederate, importi i metadati SAML scaricati da StorageGRID per l'Admin Node. Il file dei metadati contiene molti dei valori specifici di cui hai bisogno.

> Devi creare una connessione SP per ogni Admin Node nel tuo sistema StorageGRID, così gli utenti possono accedere e disconnettersi in modo sicuro da qualsiasi nodo. Usa queste istruzioni per creare la prima connessione SP. Poi, vai su Crea connessioni SP aggiuntive per creare tutte le connessioni aggiuntive di cui hai bisogno.

Scegli il tipo di connessione SP

Passaggi

1. Vai su **Applicazioni** > **Integrazione** > **SP Connections**.
2. ${post_edited_translations.segment}
3. ${post_edited_translations.segment}
4. Seleziona **Profili SSO del browser** e **SAML 2.0** come protocollo.

Importa metadati SP

Passaggi

1. Nella scheda Importa metadati, seleziona **File**.
2. Scegli il file di metadati SAML che hai scaricato dalla pagina Configura SSO per l'Admin Node.
3. ${post_edited_translations.segment}

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

nodo di amministrazione di StorageGRID.

4. Seleziona **Next**.

${post_edited_translations.segment}

Passaggi

1. Nella scheda SSO del browser, seleziona **Configura SSO del browser**.
2. ${post_edited_translations.segment}
3. Seleziona **Next**.
4. ${post_edited_translations.segment}
5. ${post_edited_translations.segment}
   a. Nella scheda Mappatura identità, seleziona **Standard**.
   b. Nella scheda Contratto attributo, usa **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato che è stato importato.
6. Per estendere il contratto, seleziona **Elimina** per rimuovere l' `urn:oid`, che non viene utilizzato.

Istanza dell'adattatore di mappa

Passaggi

1. ${post_edited_translations.segment}
2. Nella scheda Istanza adattatore, seleziona l'istanza dell'adattatore che hai creato.
3. ${post_edited_translations.segment}
4. Nella scheda Origine attributi e ricerca utente, seleziona **Aggiungi origine attributi**.
5. Nella scheda Archivio dati, inserisci una descrizione e seleziona l'datastoreelemento che hai aggiunto.
6. Nella scheda Ricerca nella directory LDAP:
   - ${post_edited_translations.segment}
   - Per l'ambito di ricerca, seleziona **Sottostruttura**.
   - Per la classe oggetto radice, cerca e aggiungi uno di questi attributi: **objectGUID** o **userPrincipalName**.
7. ${post_edited_translations.segment}
8. Nella scheda Filtro LDAP, inserisci **sAMAccountName=${username}**.
9. Nella scheda Attribute Contract Fulfillment, seleziona **LDAP (attribute)** dal menu a discesa Source e seleziona **objectGUID** o **userPrincipalName** dal menu a discesa Value.
10. Rivedi e poi salva l'origine degli attributi.
11. Nella scheda Origine attributi Failsave, seleziona **Annulla la transazione SSO**.
12. ${post_edited_translations.segment}
13. ${post_edited_translations.segment}

Configura le impostazioni del protocollo

Passaggi

1. ${post_edited_translations.segment}

2. Nella scheda URL del servizio di consumo delle asserzioni, accetta i valori predefiniti, importati dai metadati SAML di StorageGRID (**POST** per Binding e `/api/saml-response` per Endpoint URL).
3. Nella scheda URL del servizio SLO, accetta i valori predefiniti, importati dai metadati StorageGRID (**REDIRECT** per Binding e `/api/saml-logout` per Endpoint URL).
4. Nella scheda "Associazioni SAML consentite", deseleziona **ARTIFACT** e **SOAP**. Sono obbligatori solo **POST** e **REDIRECT**.
5. ${post_edited_translations.segment}
6. Nella scheda Criteri di crittografia, seleziona **Nessuno**.
7. ${post_edited_translations.segment}
8. ${post_edited_translations.segment}

${post_edited_translations.segment}

Passaggi

1. Dalla scheda Connessione SP, seleziona **Credenziali**.
2. Dalla scheda Credenziali, seleziona **Configura credenziali**.
3. Seleziona il ${post_edited_translations.segment} che hai creato o importato.
4. Seleziona **Avanti** per andare su **Gestisci impostazioni di verifica della firma**.
   a. ${post_edited_translations.segment}
   b. Nella scheda Certificato di verifica della firma, controlla le informazioni del certificato di firma, che sono state importate dai metadati SAML di StorageGRID.
5. Esamina le schermate di riepilogo e seleziona **Salva** per salvare la connessione SP.

Crea connessioni SP aggiuntive

Puoi copiare la prima connessione SP per creare le connessioni SP di cui hai bisogno per ogni Admin Node nella tua grid. Carichi nuovi metadati per ogni copia.

${post_edited_translations.segment}

Passaggi

1. ${post_edited_translations.segment}
2. Inserisci l'ID di connessione e il nome della connessione per la copia e seleziona **Salva**.
3. Scegli il file di metadati corrispondente all'Admin Node:
   a. Seleziona **Action** > **Aggiorna con metadati**.
   b. Seleziona **Scegli file** e carica i metadati.
   c. Seleziona **Next**.
   d. Seleziona **Salva**.
4. Risolvi l'errore dovuto all'attributo non utilizzato:
   a. Seleziona la nuova connessione.
   b. ${post_edited_translations.segment}
   c. Elimina la voce per **urn:oid**.

d. Seleziona **Salva**.

Disabilita SSO in StorageGRID

Puoi disabilitare il single sign-on (SSO) se non vuoi più utilizzare questa funzionalità. Devi disabilitare il single sign-on prima di poter disabilitare la federazione delle identità.

Prima di iniziare

- Sei connesso a Grid Manager utilizzando un "browser web supportato".
- Hai "autorizzazioni di accesso specifiche".

Passaggi

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

   Viene visualizzata la pagina di single sign-on.

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

   ${post_edited_translations.segment}

La prossima volta che effettuerai l'accesso a StorageGRID, verrà visualizzata la pagina di accesso di StorageGRID e dovrai inserire il nome utente e la password di un utente StorageGRID locale o federato.

Disabilitare e riabilitare temporaneamente il single sign-on (SSO) per un nodo Admin di StorageGRID

Potresti non riuscire ad accedere a Grid Manager se il sistema di single sign-on (SSO) non funziona. In questo caso, puoi disabilitare e riabilitare temporaneamente il single sign-on per un Admin Node. Per disabilitare e poi riabilitare il single sign-on, devi accedere alla shell dei comandi del nodo.

Prima di iniziare

- Hai "autorizzazioni di accesso specifiche".
- Hai il file `Passwords.txt`.
- Conosci la password dell'utente root.

Informazioni su questa attività

Dopo che hai disabilitato l'SSO per un Admin Node, puoi accedere a Grid Manager come utente root locale. Per proteggere il tuo sistema StorageGRID, devi usare la shell dei comandi del nodo per riabilitare l'SSO sull'Admin Node non appena esci.

La disattivazione dell'SSO per un Admin Node non influisce sulle impostazioni SSO degli altri Admin Node nella grid. La casella di controllo **Enable SSO** nella pagina Single Sign-on del Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute a meno che tu non le aggiorni.

Passaggi

1. Accedi a un nodo amministratore:
   a. Inserisci il seguente comando: `ssh admin@Admin_Node_IP`
   b. Inserisci la password indicata nel file `Passwords.txt`.
   c. Inserisci il seguente comando per passare all'utente root: `su -`
   d. Inserisci la password indicata nel file `Passwords.txt`.

      Quando sei connesso 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 Admin Node.

3. ${post_edited_translations.segment}

   Un messaggio indica che il single sign-on è disabilitato sul nodo.

4. ${post_edited_translations.segment}

   Ora viene visualizzata la pagina di accesso di Grid Manager perché SSO è stato disabilitato.

5. Accedi con il nome utente root e la password dell'utente root locale.
6. ${post_edited_translations.segment}
   a. Seleziona **Configurazione** > **Controllo accessi** > **Single sign-on**.
   b. Modifica le impostazioni SSO errate o non aggiornate.
   c. Seleziona **Salva**.

      Selezionando **Salva** dalla pagina di single sign-on, l'SSO viene automaticamente riattivato per l'intera grid.

7. Se hai disabilitato temporaneamente l'SSO perché avevi bisogno di accedere a Grid Manager per qualche altro motivo:

   a. ${post_edited_translations.segment}
   b. Seleziona **Esci** e chiudi Grid Manager.
   c. Riattiva l'SSO sul nodo Admin. Puoi eseguire una delle seguenti operazioni:

      - Eseguire il seguente comando: `enable-saml`

        Un messaggio indica che il comando si applica solo a questo Admin Node.

      Conferma che vuoi abilitare l'SSO.

   ${post_edited_translations.segment}

   ◦ Riavvia il nodo della griglia: `reboot`
8. Da un browser web, accedi al Grid Manager dallo stesso Admin Node.
9. ${post_edited_translations.segment}

Informazioni sul copyright

Informazioni sul marchio commerciale