Utilizzare l'accesso singolo (SSO)

StorageGRID software

NetApp
December 03, 2025

Sommario

Utilizzare l’accesso singolo (SSO)

Configurare l’accesso singolo

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.

Come funziona l’accesso singolo

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

Prima di abilitare l’accesso Single Sign-On (SSO), esaminare in che modo i processi di accesso e disconnessione StorageGRID vengono influenzati dall’abilitazione dell’SSO.

Sign in quando SSO è abilitato

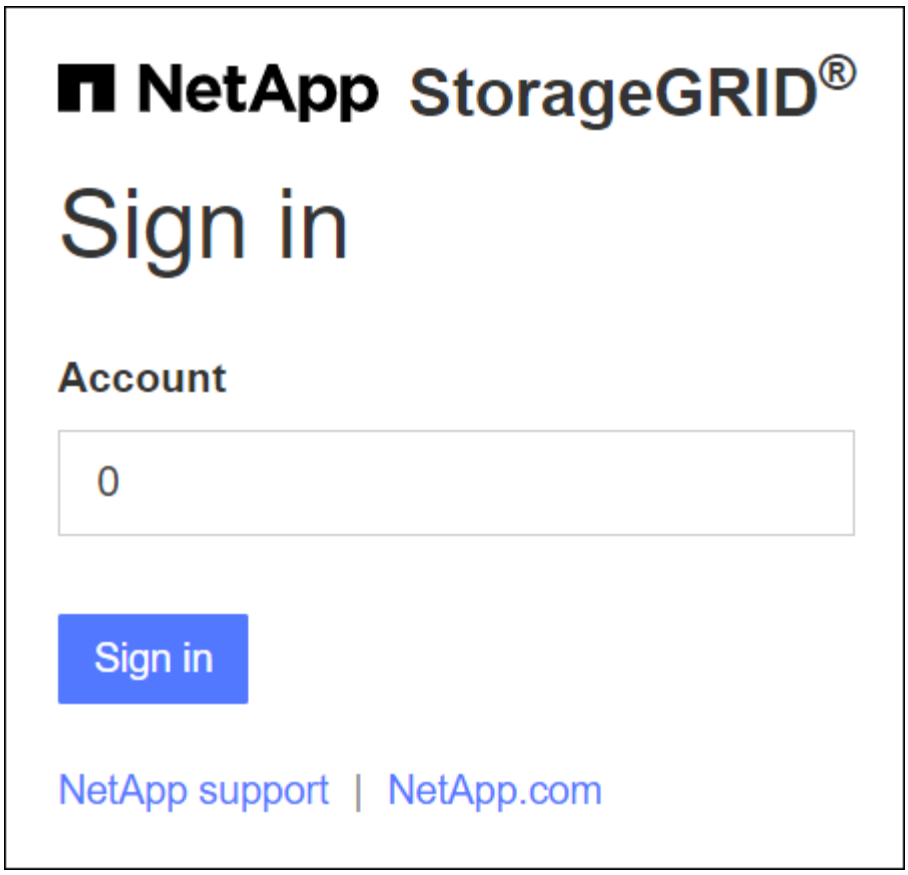
Quando l’SSO è abilitato e accedi a StorageGRID, verrai reindirizzato alla pagina SSO della tua organizzazione per convalidare le tue credenziali.

Passi

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 Sign in a StorageGRID .

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

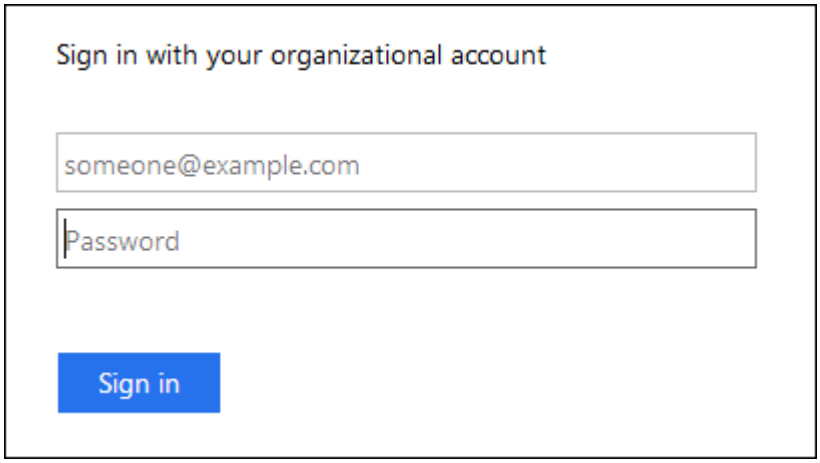


- Se hai già effettuato l'accesso a Grid Manager o Tenant Manager, ti verrà chiesto di selezionare un account recente o di immettere un ID account:

La pagina Sign in 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`). Invece, verrai immediatamente reindirizzato alla pagina di accesso SSO della tua organizzazione, dove potraiaccedi con le tue credenziali SSO .

2. Indica se desideri accedere al Grid Manager o al Tenant Manager:
   - Per accedere a Grid Manager, lasciare vuoto il campo **ID account**, immettere **0** come ID account oppure selezionare **Grid Manager** se compare nell'elenco degli account recenti.
   - Per accedere a Tenant Manager, immettere l'ID account del tenant a 20 cifre oppure selezionare un tenant per nome se compare nell'elenco degli account recenti.
3. Seleziona * Sign in*

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



4. Sign in con le tue credenziali SSO.

   Se le tue 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 si appartiene a un gruppo federato con autorizzazioni di accesso StorageGRID , si accede a Grid Manager o Tenant Manager, a seconda dell'account selezionato.

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

5. Facoltativamente, accedi ad altri nodi amministrativi oppure a Grid Manager o Tenant Manager, se disponi delle autorizzazioni adeguate.

   Non è necessario reinserire le credenziali SSO.

Disconnettersi quando SSO è abilitato

Quando SSO è abilitato per StorageGRID, ciò che accade quando ci si disconnette dipende dall'account a cui si è effettuato l'accesso e da dove ci si disconnette.

Passi

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

   Viene visualizzata la pagina Sign in a StorageGRID . Il menu a discesa **Account recenti** è stato aggiornato per includere **Grid Manager** o il nome del tenant, in modo da poter accedere più rapidamente a queste interfacce utente in futuro.

Se hai effettuato l'accesso a…	E ti disconnetti da…	Hai effettuato la disconnessione da…
Grid Manager su uno o più nodi amministrativi	Grid Manager su qualsiasi nodo di amministrazione	Grid Manager su tutti i nodi amministrativi **Nota:** se si utilizza Azure per SSO, potrebbero essere necessari alcuni minuti per uscire da tutti i nodi amministrativi.
Tenant Manager su uno o più nodi amministrativi	Tenant Manager su qualsiasi nodo amministrativo	Tenant Manager su tutti i nodi amministrativi
Sia Grid Manager che Tenant Manager	Responsabile della griglia	Solo il Grid Manager. Per uscire dall'SSO è necessario anche disconnettersi da Tenant Manager.

La tabella riassume cosa succede quando ci si disconnette se si utilizza una singola sessione del browser. Se hai effettuato l'accesso a StorageGRID in più sessioni del browser, devi disconnetterti da tutte le sessioni del browser separatamente.

Requisiti e considerazioni per l'accesso singolo

Prima di abilitare l'accesso Single Sign-On (SSO) per un sistema StorageGRID , esaminare i requisiti e le considerazioni.

Requisiti del fornitore di identità

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

- Servizio federativo di Active Directory (AD FS)
- Azure Active Directory (Azure AD)
- 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 la federazione delle identità determina il tipo di SSO che è possibile implementare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	• Directory attiva • Azzurro • PingFederate
Azzurro	Azzurro

Requisiti AD FS

È possibile utilizzare una qualsiasi delle seguenti versioni di AD FS:

- Windows Server 2022 ADFS
- Windows Server 2019 ADFS
- Windows Server 2016 ADFS

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

Requisiti aggiuntivi

- Sicurezza del livello di trasporto (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

Considerazioni per Azure

Se si utilizza Azure come tipo di SSO e gli utenti hanno nomi di entità 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 del certificato 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 (Azure) 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 l'hai già fatto"configurato un certificato personalizzato per l'interfaccia di gestione" , dovresti farlo ora. Quando si installa un certificato server personalizzato, questo viene utilizzato per tutti i nodi amministrativi e può essere utilizzato in tutti i trust relying party StorageGRID , nelle applicazioni aziendali o nelle connessioni SP .

Non è consigliabile utilizzare il certificato server predefinito di un nodo di amministrazione in un trust di relying party, in un'applicazione aziendale o in una connessione SP . Se il nodo fallisce e lo si ripristina, viene generato un nuovo certificato server predefinito. Prima di poter accedere al nodo recuperato, è necessario aggiornare il trust della relying party, l'applicazione aziendale o la connessione SP con il nuovo certificato.

È possibile accedere al certificato del server di un nodo di amministrazione effettuando l'accesso alla shell dei comandi del nodo e andando su `/var/local/mgmt-api` elenco. Un certificato server personalizzato è denominato `custom-server.crt` . Il certificato del server predefinito del nodo è denominato `server.crt` .

Requisiti portuali

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

Conferma che gli utenti federati possono accedere

Prima di abilitare l'accesso Single Sign-On (SSO), è necessario confermare che almeno un utente federato possa accedere a Grid Manager e a Tenant Manager per tutti gli account tenant esistenti.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Hai"autorizzazioni di accesso specifiche" .
- Hai già configurato la federazione delle identità.

Passi

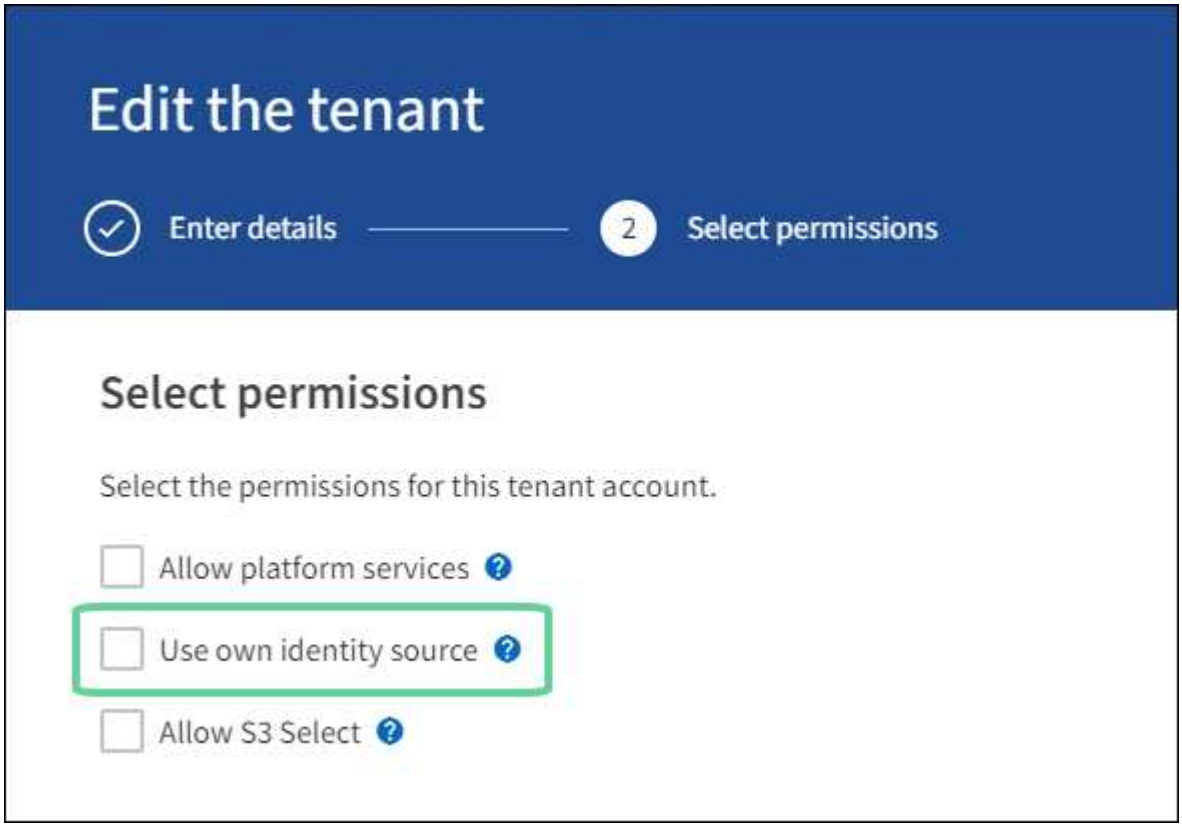
1. Se sono già presenti account tenant, verificare che nessuno dei tenant utilizzi la propria fonte di identità.

   Quando si abilita SSO, un'origine identità configurata in Tenant Manager viene sostituita dall'origine identità configurata in Grid Manager. Gli utenti appartenenti all'origine identità del tenant non potranno più effettuare l'accesso a meno che non dispongano di un account con l'origine identità di Grid Manager.

   a. Sign in al Tenant Manager per ogni account tenant.
   b. Selezionare **GESTIONE ACCESSI** > **Federazione identità**.
   c. Verificare che la casella di controllo **Abilita federazione delle identità** non sia selezionata.
   d. In tal caso, verificare che tutti i gruppi federati eventualmente utilizzati per questo account tenant non siano più necessari, deselezionare la casella di controllo e selezionare **Salva**.

2. Verificare che un utente federato possa accedere a Grid Manager:
   a. Da Grid Manager, seleziona **CONFIGURAZIONE** > **Controllo accessi** > **Gruppi amministratori**.
   b. Assicurarsi che almeno un gruppo federato sia stato importato dall'origine identità di Active Directory e che gli sia stata assegnata l'autorizzazione di accesso Root.
   c. Disconnessione.
   d. Conferma di poter accedere nuovamente a Grid Manager come utente del gruppo federato.
3. Se sono presenti account tenant, verificare che un utente federato con autorizzazione di accesso Root possa accedere:
   a. Da Grid Manager, seleziona **TENANTS**.
   b. Selezionare l'account tenant e selezionare **Azioni** > **Modifica**.
   c. Nella scheda Inserisci dettagli, seleziona **Continua**.

d. Se è selezionata la casella di controllo **Usa la propria fonte di identità**, deselezionarla e selezionare **Salva**.



Viene visualizzata la pagina Inquilino.

a. Selezionare l'account tenant, selezionare * Sign in* e accedere all'account tenant come utente root locale.
b. Da Tenant Manager, seleziona **GESTIONE ACCESSI** > **Gruppi**.
c. Assicurarsi che almeno a un gruppo federato di Grid Manager sia stata assegnata l'autorizzazione di accesso Root per questo tenant.
d. Disconnessione.
e. Conferma di poter accedere nuovamente al tenant come utente nel gruppo federato.

Informazioni correlate

- "Requisiti e considerazioni per l'accesso singolo"
- "Gestisci gruppi di amministratori"
- "Utilizzare un account tenant"

Utilizza la modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare l'accesso singolo (SSO) prima di abilitarlo per tutti gli utenti StorageGRID . Dopo aver abilitato l'SSO, puoi tornare alla modalità sandbox ogni volta che hai bisogno di modificare o testare nuovamente la configurazione.

Prima di iniziare

- Hai effettuato l'accesso a Grid Manager utilizzando un"browser web supportato" .
- Tu hai il"Permesso 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 Azure, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Directory attiva	• Directory attiva • Azzurro • PingFederate
Azzurro	Azzurro

Informazioni su questo compito

Quando l'SSO è abilitato e un utente tenta di accedere a un nodo di amministrazione, 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 è andata a buon fine. Per richieste andate a buon fine:

- La risposta da Active Directory o PingFederate include un identificatore univoco universale (UUID) per l'utente.
- La risposta di Azure include un nome dell'entità utente (UPN).

Per consentire a StorageGRID (il fornitore del servizio) e al provider di identità SSO di comunicare in modo sicuro sulle richieste di autenticazione degli utenti, è necessario configurare determinate impostazioni in StorageGRID. Successivamente, è necessario utilizzare il software del provider di identità SSO per creare un trust della relying party (AD FS), un'applicazione aziendale (Azure) o un provider di servizi (PingFederate) per ciascun nodo di amministrazione. Infine, è necessario tornare a StorageGRID per abilitare SSO.

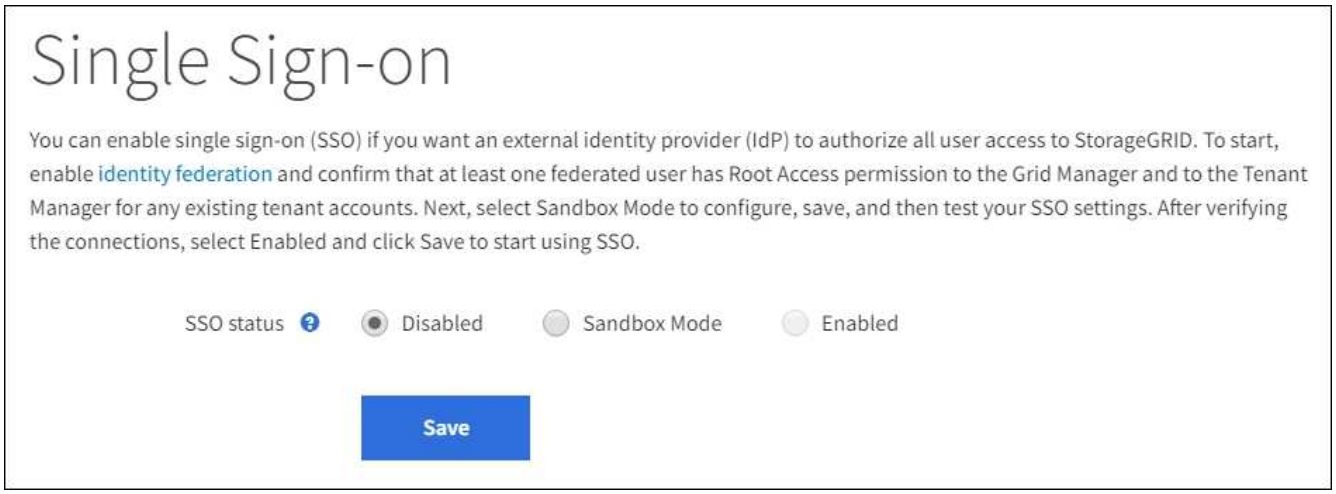
La modalità sandbox semplifica l'esecuzione di questa configurazione avanti e indietro e il test di tutte le impostazioni prima di abilitare l'SSO. Quando si utilizza la modalità sandbox, gli utenti non possono accedere tramite SSO.

Accedi alla modalità sandbox

Passi

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

   Viene visualizzata la pagina Single Sign-on, con l'opzione **Disabilitato** selezionata.



Se le opzioni di stato SSO non vengono visualizzate, verificare di aver configurato il provider di identità come origine dell'identità federata. Vedere "Requisiti e considerazioni per l'accesso singolo" .

2. Selezionare **Modalità Sandbox**.

   Viene visualizzata la sezione Provider di identità.

Inserisci i dettagli del provider di identità

Passi

1. Selezionare il **tipo SSO** dall'elenco a discesa.
2. Compila i campi nella sezione Identity Provider in base al tipo di SSO selezionato.

Directory attiva

a. Immettere 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 Windows Server Manager. Selezionare **Strumenti** > **Gestione AD FS**. Dal menu Azione, seleziona **Modifica proprietà del servizio federativo**. Nel secondo campo viene visualizzato il nome del servizio federativo.

b. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo**: utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza 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 utilizzare TLS**: non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica il certificato CA, immediatamente"riavviare il servizio mgmt-api sui nodi amministrativi" e testare un SSO riuscito nel Grid Manager.

c. Nella sezione Relying Party, specificare l'**identificatore del relying party** per StorageGRID. Questo valore controlla il nome utilizzato per ogni trust della relying party in AD FS.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG` O `StorageGRID` .
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]` . Viene generata una tabella che mostra l'identificatore della parte affidabile per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.

> È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

Azzurro

a. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

- **Utilizza il certificato CA del sistema operativo**: utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
- **Utilizza 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 utilizzare TLS**: non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica il certificato CA, immediatamente"riavviare il servizio mgmt-api sui nodi amministrativi" e testare un SSO riuscito nel Grid Manager.

b. Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ogni applicazione aziendale in Azure AD.

   - Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG` O `StorageGRID` .
   - Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]` . Viene generata una tabella che mostra il nome dell'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 amministrativo nel sistema StorageGRID . Disporre di un'applicazione aziendale per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

c. Segui i passaggi in"Crea applicazioni aziendali in Azure AD" per creare un'applicazione aziendale per ogni nodo amministrativo elencato nella tabella.

d. Da Azure AD, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.

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

   Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

PingFederate

a. Specificare quale certificato TLS verrà utilizzato per proteggere la connessione quando il provider di identità invia informazioni di configurazione SSO in risposta alle richieste StorageGRID .

   - **Utilizza il certificato CA del sistema operativo**: utilizza il certificato CA predefinito installato sul sistema operativo per proteggere la connessione.
   - **Utilizza 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 utilizzare TLS**: non utilizzare un certificato TLS per proteggere la connessione.

> Se si modifica il certificato CA, immediatamente"riavviare il servizio mgmt-api sui nodi amministrativi" e testare un SSO riuscito nel Grid Manager.

b. Nella sezione Fornitore di servizi (SP), specificare l'ID di connessione SP per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.

- Ad esempio, se la tua griglia ha un solo nodo amministrativo e non prevedi di aggiungerne altri in futuro, inserisci `SG` O `StorageGRID` .
- Se la griglia include più di un nodo di amministrazione, includi la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]` . Viene generata 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 amministrativo nel sistema StorageGRID . Disporre di una connessione SP per ciascun nodo amministrativo garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo amministrativo.

c. Specificare l'URL dei metadati della federazione per ciascun nodo di amministrazione nel campo **URL dei metadati della federazione**.

Utilizzare il seguente formato:

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

d. Seleziona **Salva**.

Per alcuni secondi sul pulsante **Salva** apparirà un segno di spunta verde.

Configurare trust di relying party, applicazioni aziendali o connessioni SP

Una volta salvata la configurazione, viene visualizzato l'avviso di conferma della modalità Sandbox. Questa nota conferma che la modalità sandbox è ora abilitata e fornisce istruzioni generali.

StorageGRID può rimanere in modalità sandbox per tutto il tempo necessario. Tuttavia, quando nella pagina Single Sign-on è selezionata la **Modalità Sandbox**, l'SSO è disabilitato per tutti gli utenti StorageGRID . Possono effettuare l'accesso solo gli utenti locali.

Seguire questi passaggi per configurare trust di relying party (Active Directory), completare applicazioni aziendali (Azure) o configurare connessioni SP (PingFederate).

Directory attiva

Passi

1. Vai ad 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 Single Sign-on StorageGRID .

   È necessario creare un trust per ogni nodo amministrativo mostrato nella tabella.

   Per le istruzioni, vai a"Creare trust di relying party in AD FS" .

Azzurro

Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
   a. Sign in al nodo.
   b. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.
   c. Scarica e salva i metadati SAML per quel nodo.
3. Vai al portale di Azure.
4. Segui i passaggi in"Crea applicazioni aziendali in Azure AD" per caricare il file di metadati SAML per ciascun nodo di amministrazione nella corrispondente applicazione aziendale di Azure.

PingFederate

Passi

1. Dalla pagina Single Sign-On per il nodo di amministrazione a cui hai effettuato l'accesso, seleziona il pulsante per scaricare e salvare i metadati SAML.
2. Quindi, per tutti gli altri nodi amministrativi nella griglia, ripeti questi passaggi:
   a. Sign in al nodo.
   b. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.
   c. Scarica e salva i metadati SAML per quel nodo.
3. Vai su PingFederate.
4. "Creare una o più connessioni al fornitore di servizi (SP) per StorageGRID" . Utilizzare l'ID di connessione SP per ciascun nodo amministrativo (mostrato nella tabella nella pagina StorageGRID Single Sign-on) e i metadati SAML scaricati per tale nodo amministrativo.

   È necessario creare una connessione SP per ogni nodo amministrativo mostrato nella tabella.

Test delle connessioni SSO

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

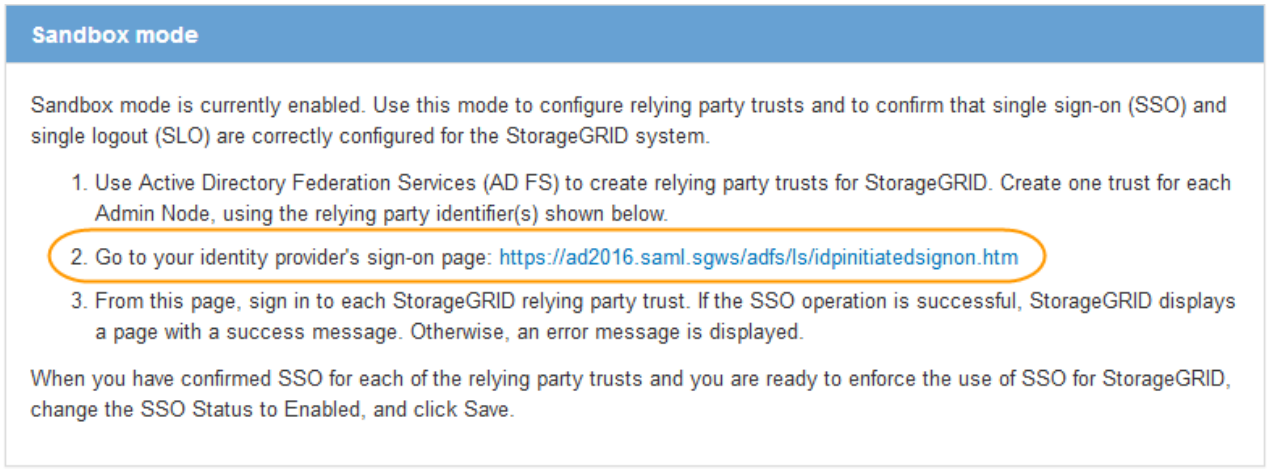
amministrazione.

Directory attiva

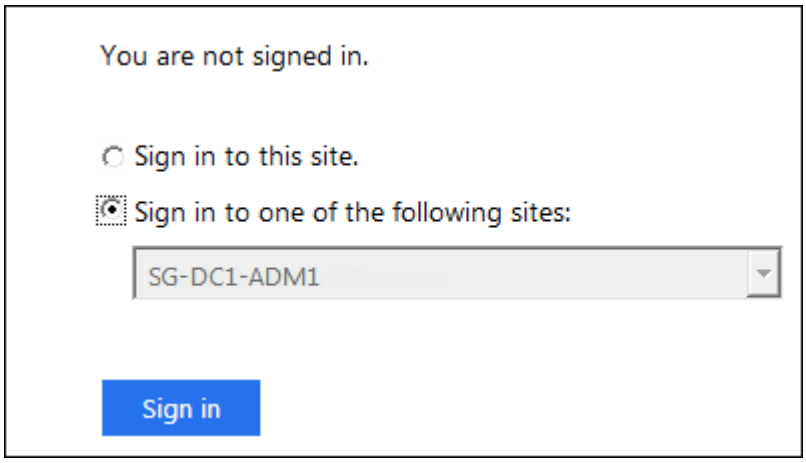
Passi

1. Nella pagina StorageGRID Single Sign-on, individuare il collegamento nel messaggio della modalità Sandbox.

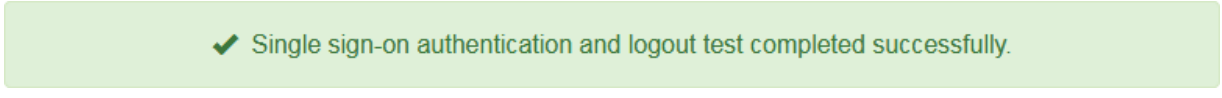
   L'URL deriva dal valore immesso nel campo **Nome del servizio federativo**.



2. Seleziona il collegamento oppure copia e incolla l'URL in un browser per accedere alla pagina di accesso del tuo provider di identità.
3. Per confermare di poter utilizzare SSO per accedere a StorageGRID, seleziona * Sign in a uno dei seguenti siti*, seleziona l'identificativo della parte affidabile per il tuo nodo di amministrazione primario e seleziona * Sign in*.



4. Inserisci il tuo nome utente e la tua password federati.
   - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.



   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
5. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella

griglia.

Azzurro

Passi

1. Vai alla pagina Single Sign-On nel portale di Azure.
2. Seleziona **Prova questa applicazione**.
3. Inserisci le credenziali di un utente federato.
   - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

     ✔ Single sign-on authentication and logout test completed successfully.

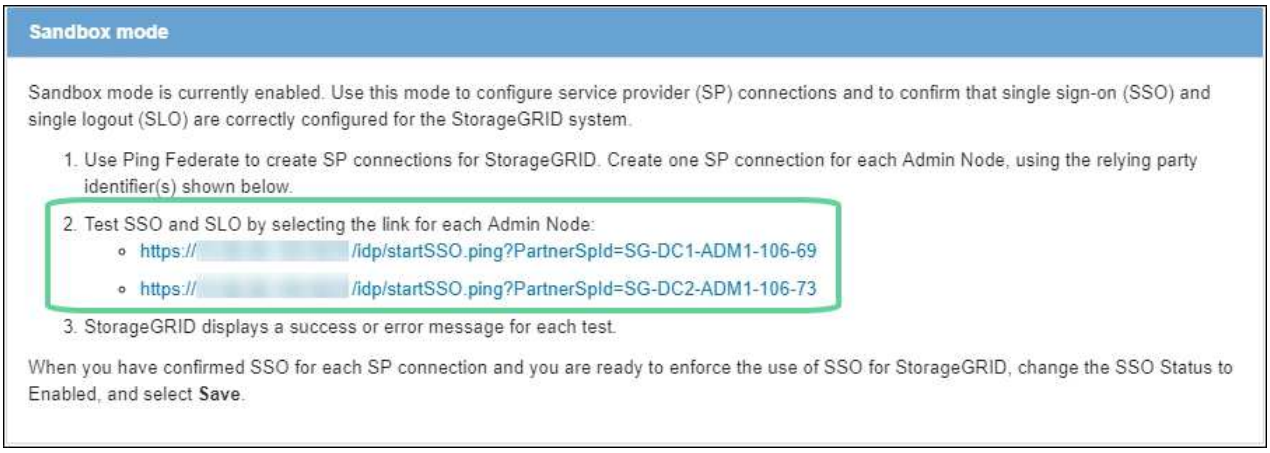
   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
4. Ripetere questi passaggi per verificare la connessione SSO per ciascun nodo amministrativo nella griglia.

PingFederate

Passi

1. Dalla pagina StorageGRID Single Sign-on, selezionare il primo collegamento nel messaggio della modalità Sandbox.

   Seleziona e testa un collegamento alla volta.



2. Inserisci le credenziali di un utente federato.
   - Se le operazioni di accesso e disconnessione SSO vanno a buon fine, viene visualizzato un messaggio di conferma.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvi il problema, cancella i cookie del browser e riprova.
3. Seleziona il collegamento successivo per verificare la connessione SSO per ciascun nodo di amministrazione nella tua griglia.

Se vedi un messaggio di pagina scaduta, seleziona il pulsante **Indietro** nel tuo browser e invia nuovamente le tue credenziali.

Abilita l'accesso singolo

Dopo aver confermato di poter utilizzare SSO per accedere a ciascun nodo di amministrazione, puoi abilitare SSO per l'intero sistema StorageGRID .

Quando SSO è abilitato, 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.

Passi

1. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.
2. Modificare lo stato SSO in **Abilitato**.
3. Seleziona **Salva**.
4. Rivedere il messaggio di avviso e selezionare **OK**.

   Ora è abilitato l'accesso singolo.

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

Creare trust di relying party in AD FS

È necessario utilizzare Active Directory Federation Services (AD FS) per creare un trust della relying party per ogni nodo amministrativo nel sistema. È possibile creare trust di relying party utilizzando i comandi di PowerShell, importando metadati SAML da StorageGRID o immettendo i dati manualmente.

Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **AD FS** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "Utilizza la modalità sandbox" .
- 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 StorageGRID Single Sign-on.

  È necessario creare un trust della relying party per ciascun nodo amministrativo nel sistema StorageGRID . La presenza di un trust di parte affidabile per ogni nodo di amministrazione garantisce che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo di amministrazione.

- Hai esperienza nella creazione di trust relying party in AD FS oppure hai accesso alla documentazione di Microsoft AD FS.

- Stai utilizzando lo snap-in Gestione AD FS e appartieni al gruppo Amministratori.
- Se si crea manualmente il trust della relying party, si dispone del certificato personalizzato caricato per l'interfaccia di gestione StorageGRID oppure si sa come accedere a un nodo di amministrazione dalla shell dei comandi.

Informazioni su questo compito

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. Per qualsiasi domanda, consultare la documentazione di Microsoft AD FS.

Creare un trust della relying party utilizzando Windows PowerShell

È possibile utilizzare Windows PowerShell per creare rapidamente uno o più trust relying party.

Passi

1. Dal menu Start di Windows, seleziona con il pulsante destro del mouse l'icona di PowerShell e seleziona **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 della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1` .
   - Per *Admin_Node_FQDN* , immettere il nome di dominio completo per lo stesso nodo di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)
3. Da Windows Server Manager, selezionare **Strumenti** > **Gestione AD FS**.

   Viene visualizzato lo strumento di gestione AD FS.
4. Selezionare **AD FS** > **Trust delle parti affidabili**.

   Viene visualizzato l'elenco dei trust delle parti affidanti.
5. Aggiungere 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. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica criterio di controllo degli accessi**.
   c. Selezionare una politica di controllo degli accessi.
   d. Selezionare **Applica** e selezionare **OK**
6. Aggiungere una politica di emissione dei reclami al trust della parte affidabile appena creato:
   a. Individua il trust della parte affidabile che hai appena creato.
   b. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
   c. Seleziona **Aggiungi regola**.

d. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.

e. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

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

f. Per l'Attribute Store, selezionare **Active Directory**.

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

h. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.

i. Selezionare **Fine** e quindi **OK**.

7. Verificare che i metadati siano stati importati correttamente.
   a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
   b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

      Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

8. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .
9. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere"Utilizzare la modalità Sandbox" per istruzioni.

Creare un trust della parte affidabile importando i metadati della federazione

È possibile importare i valori per ciascun trust della relying party accedendo ai metadati SAML per ciascun nodo di amministrazione.

Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.
2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.
3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.
4. Selezionare **Importa dati sulla parte affidabile pubblicati online o su una rete locale**.
5. In **Indirizzo metadati federazione (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 di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

6. Completare la procedura guidata Trust della parte affidabile, salvare il trust della parte affidabile e chiudere la procedura guidata.

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

7. Aggiungi una regola di rivendicazione:
   a. Fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.
   b. Seleziona **Aggiungi regola**:
   c. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.
   d. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

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

   e. Per l'Attribute Store, selezionare **Active Directory**.
   f. Nella colonna Attributo LDAP della tabella Mapping, digitare **objectGUID** oppure selezionare **User-Principal-Name**.
   g. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.
   h. Selezionare **Fine** e quindi **OK**.
8. Verificare che i metadati siano stati importati correttamente.
   a. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.
   b. Verificare che i campi nelle schede **Endpoint**, **Identificatori** e **Firma** siano compilati.

      Se i metadati sono mancanti, verificare che l'indirizzo dei metadati della Federazione sia corretto oppure immettere i valori manualmente.

9. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .
10. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere"Utilizzare la modalità Sandbox" per istruzioni.

Creare manualmente un trust della parte affidabile

Se si sceglie di non importare i dati per i trust delle parti affidabili, è possibile immettere i valori manualmente.

Passi

1. In Windows Server Manager, seleziona **Strumenti**, quindi seleziona **Gestione AD FS**.
2. In Azioni, seleziona **Aggiungi trust della parte affidabile**.
3. Nella pagina di benvenuto, seleziona **Richiedi informazioni** e seleziona **Avvia**.
4. Selezionare **Inserisci manualmente i dati sulla parte affidabile** e selezionare **Avanti**.
5. Completare la procedura guidata Trust della parte affidabile:
   a. Inserisci un nome visualizzato per questo nodo di amministrazione.

      Per coerenza, utilizzare l'identificatore della parte affidabile per il nodo di amministrazione, 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 token facoltativo.

c. Nella pagina Configura URL, seleziona la casella di controllo **Abilita supporto per il protocollo SAML 2.0 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 di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

e. Nella pagina Configura identificatori, specificare l'identificatore della parte affidabile per lo stesso nodo di amministrazione:

Admin_Node_Identifier

Per *Admin_Node_Identifier*, immettere l'identificatore della parte affidabile per il nodo di amministrazione, esattamente come appare nella pagina Single Sign-on. Ad esempio, `SG-DC1-ADM1`.

f. Rivedere le impostazioni, salvare il trust della relying party e chiudere la procedura guidata.

Viene visualizzata la finestra di dialogo Modifica policy di emissione reclami.

> Se la finestra di dialogo non viene visualizzata, fare clic con il pulsante destro del mouse sul trust e selezionare **Modifica policy di emissione reclami**.

6. Per avviare la procedura guidata Claim Rules, seleziona **Aggiungi regola**:

a. Nella pagina Seleziona modello di regola, seleziona **Invia attributi LDAP come claim** dall'elenco e seleziona **Avanti**.

b. Nella pagina Configura regola, immettere un nome visualizzato per questa regola.

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

c. Per l'Attribute Store, selezionare **Active Directory**.

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

e. Nella colonna Tipo di richiesta in uscita della tabella Mapping, selezionare **ID nome** dall'elenco a discesa.

f. Selezionare **Fine** e quindi **OK**.

7. Fare clic con il pulsante destro del mouse sul trust della relying party per aprirne le proprietà.

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

a. Selezionare **Aggiungi SAML**.

b. Selezionare **Tipo di endpoint** > **Disconnessione SAML**.

c. Selezionare **Associa** > **Reindirizza**.

d. Nel campo **URL attendibile**, 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 di amministrazione. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, tenere presente che sarà necessario aggiornare o ricreare questo trust della relying party se l'indirizzo IP dovesse cambiare.)

a. Selezionare **OK**.

9. Nella scheda **Firma**, specificare il certificato di firma per questo trust della parte affidabile:
   a. Aggiungi il certificato personalizzato:
      - Se disponi del certificato di gestione personalizzato caricato su StorageGRID, seleziona tale certificato.
      - Se non si dispone del certificato personalizzato, accedere al nodo di amministrazione, andare su `/var/local/mgmt-api` directory del nodo di amministrazione e aggiungere il `custom-server.crt` file del certificato.

> Utilizzo del certificato predefinito del nodo di amministrazione(`server.crt`) non è raccomandato. Se il nodo di amministrazione non funziona, il certificato predefinito verrà rigenerato quando si ripristina il nodo e sarà necessario aggiornare il trust della parte affidabile.

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

      Le proprietà del relying party vengono salvate e chiuse.

10. Ripetere questi passaggi per configurare un trust della relying party per tutti i nodi amministrativi nel sistema StorageGRID .
11. Al termine, torna a StorageGRID e verifica tutti i trust delle relying party per confermare che siano configurati correttamente. Vedere"Utilizza la modalità sandbox" per istruzioni.

Crea applicazioni aziendali in Azure AD

Puoi utilizzare Azure AD per creare un'applicazione aziendale per ogni nodo di amministrazione del tuo sistema.

Prima di iniziare

- Hai iniziato a configurare l'accesso Single Sign-On per StorageGRID e hai selezionato **Azure** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "Utilizza la modalità sandbox" .
- 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 Single Sign-on StorageGRID .

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

- Hai esperienza nella creazione di applicazioni aziendali in Azure Active Directory.
- Hai un account Azure con una sottoscrizione attiva.
- Nell'account Azure ricopri uno dei seguenti ruoli: amministratore globale, amministratore dell'applicazione cloud, amministratore dell'applicazione o proprietario dell'entità servizio.

Accedi ad Azure AD

Passi

1. Accedi al "Portale di Azure" .
2. Vai a "Azure Active Directory" .
3. Selezionare "Applicazioni aziendali" .

Crea applicazioni aziendali e salva la configurazione StorageGRID SSO

Per salvare la configurazione SSO per Azure in StorageGRID, è necessario utilizzare Azure per creare un'applicazione aziendale per ciascun nodo di amministrazione. Copiare gli URL dei metadati della federazione da Azure e incollarli nei campi **URL metadati della federazione** corrispondenti nella pagina Single Sign-on di StorageGRID .

Passi

1. Ripetere i seguenti passaggi per ciascun nodo di amministrazione.
   a. Nel riquadro Applicazioni aziendali di Azure, seleziona **Nuova applicazione**.
   b. Seleziona **Crea la tua applicazione**.
   c. Per il nome, immettere il **Nome dell'applicazione aziendale** copiato dalla tabella dei dettagli del nodo di amministrazione nella pagina Single Sign-on StorageGRID .
   d. Lascia selezionato il pulsante di opzione **Integra qualsiasi altra applicazione non presente nella galleria (Non nella galleria)**.
   e. Seleziona **Crea**.
   f. Selezionare il link **Inizia** nel **2. Impostare la casella Single Sign-On** oppure selezionare il collegamento **Single Sign-On** sul margine sinistro.
   g. Selezionare la casella **SAML**.
   h. Copia l'**URL dei metadati della federazione app**, che puoi trovare in **Certificato di firma SAML del passaggio 3**.
   i. Vai alla pagina StorageGRID Single Sign-on e incolla l'URL nel campo **URL metadati federazione** che corrisponde al **Nome applicazione aziendale** utilizzato.
2. Dopo aver incollato un URL dei metadati di federazione per ciascun nodo di amministrazione e aver apportato tutte le altre modifiche necessarie alla configurazione SSO, selezionare **Salva** nella pagina StorageGRID Single Sign-on.

Scarica i metadati SAML per ogni nodo amministrativo

Dopo aver salvato la configurazione SSO, puoi scaricare un file di metadati SAML per ogni nodo amministrativo nel tuo sistema StorageGRID .

Passi

1. Ripetere questi passaggi per ogni nodo di amministrazione.

a. Sign in a StorageGRID dal nodo di amministrazione.
b. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.
c. Selezionare il pulsante per scaricare i metadati SAML per quel nodo di amministrazione.
d. Salva il file che caricherai in Azure AD.

Carica i metadati SAML in ogni applicazione aziendale

Dopo aver scaricato un file di metadati SAML per ogni nodo di amministrazione StorageGRID , eseguire i seguenti passaggi in Azure AD:

Passi

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

> ⓘ Potrebbe essere necessario aggiornare la pagina Applicazioni aziendali per visualizzare le applicazioni aggiunte in precedenza all'elenco.

a. Vai 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 metadati** e selezionare il file metadati SAML scaricato per il nodo di amministrazione corrispondente.
f. Dopo aver caricato il file, seleziona **Salva** e poi **X** per chiudere il riquadro. Verrai reindirizzato alla pagina Imposta Single Sign-On con SAML.

3. Segui i passaggi in"Utilizza la modalità sandbox" per testare ogni applicazione.

Crea connessioni al fornitore di servizi (SP) in PingFederate

Puoi utilizzare PingFederate per creare una connessione al provider di servizi (SP) per ogni nodo amministrativo del tuo sistema. Per velocizzare il processo, importerai i metadati SAML da StorageGRID.

Prima di iniziare

- Hai configurato l'accesso Single Sign-On per StorageGRID e hai selezionato **Ping Federate** come tipo di SSO.
- La **modalità sandbox** è selezionata nella pagina Single sign-on in Grid Manager. Vedere "Utilizza la modalità sandbox" .
- Hai l'*ID di connessione SP * per ogni nodo amministrativo nel tuo sistema. È possibile trovare questi valori nella tabella dei dettagli dei nodi di amministrazione nella pagina StorageGRID Single Sign-on.
- Hai scaricato i **metadati SAML** per ogni nodo amministrativo nel tuo sistema.
- Hai esperienza nella creazione di connessioni SP in PingFederate Server.
- Tu hai ilhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_refere

nce_guide.html["Guida di riferimento dell'amministratore"^] per PingFederate Server. La documentazione di PingFederate fornisce istruzioni e spiegazioni dettagliate passo dopo passo.

- Tu hai il"Autorizzazione di amministratore" per PingFederate Server.

Informazioni su questo compito

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 tua versione, consulta la documentazione di PingFederate Server.

Prerequisiti completi in PingFederate

Prima di poter creare le connessioni SP che utilizzerai per StorageGRID, devi completare le attività preliminari in PingFederate. Le informazioni ricavate da questi prerequisiti verranno utilizzate durante la configurazione delle connessioni SP .

Crea archivio dati

Se non lo hai già fatto, crea un archivio dati per connettere PingFederate al server LDAP di AD FS. Utilizza i valori che hai utilizzato quando"configurazione della federazione delle identità" in StorageGRID.

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

Crea un validatore di credenziali password

Se non l'hai già fatto, crea un validatore di credenziali password.

- **Tipo**: Nome utente LDAP Password Validatore credenziali
- **Archivio dati**: seleziona l'archivio dati che hai creato.
- **Base di ricerca**: immettere le informazioni da LDAP (ad esempio, DC=saml,DC=sgws).
- **Filtro di ricerca**: sAMAccountName=${username}
- **Ambito**: Sottoalbero

Crea istanza dell'adattatore IdP

Se non l'hai già fatto, crea un'istanza dell'adattatore IdP.

Passi

1. Vai su **Autenticazione** > **Integrazione** > **Schede IdP**.
2. Selezionare **Crea nuova istanza**.
3. Nella scheda Tipo, seleziona **Adattatore IdP modulo HTML**.
4. Nella scheda IdP Adapter, seleziona **Aggiungi una nuova riga a 'Validatori di credenziali'**.
5. Seleziona ilvalidatore di credenziali password che hai creato.
6. Nella scheda Attributi adattatore, selezionare l'attributo **username** per **Pseudonimo**.
7. Seleziona **Salva**.

Crea o importa il certificato di firma

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

Passi

1. Vai a **Sicurezza** > **Chiavi e certificati di firma e decrittazione**.
2. Creare o importare il certificato di firma.

Crea 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 di cui hai bisogno.

È necessario creare una connessione SP per ciascun nodo di amministrazione nel sistema StorageGRID , in modo che gli utenti possano accedere e uscire in modo sicuro da qualsiasi nodo. Utilizzare queste istruzioni per creare la prima connessione SP . Poi vai aCrea connessioni SP aggiuntive per creare eventuali connessioni aggiuntive di cui hai bisogno.

Scegli il tipo di connessione SP

Passi

1. Vai su **Applicazioni** > **Integrazione** > *Connessioni SP *.
2. Seleziona **Crea connessione**.
3. Seleziona **Non utilizzare un modello per questa connessione**.
4. Selezionare **Profili SSO del browser** e **SAML 2.0** come protocollo.

Importa metadati SP

Passi

1. Nella scheda Importa metadati, seleziona **File**.
2. Seleziona il file di metadati SAML scaricato dalla pagina Single Sign-On StorageGRID per il nodo di amministrazione.
3. Esaminare il Riepilogo dei metadati e le informazioni fornite nella scheda Informazioni generali.

   L'ID entità del partner e il nome della connessione sono impostati sull'ID di 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 l'SSO del browser IdP

Passi

1. Dalla scheda Browser SSO, seleziona **Configura Browser SSO**.
2. Nella scheda Profili SAML, seleziona le opzioni * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Durata asserzione, non apportare modifiche.

5. Nella scheda Creazione asserzione, selezionare **Configura creazione asserzione**.
   a. Nella scheda Mappatura identità, selezionare **Standard**.
   b. Nella scheda Contratto attributo, utilizzare **SAML_SUBJECT** come Contratto attributo e il formato del nome non specificato che è stato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere il `urn:oid` , che non viene utilizzato.

Istanza dell'adattatore della mappa

Passi

1. Nella scheda Mapping origine autenticazione, selezionare **Mappa nuova istanza adattatore**.
2. Nella scheda Istanza adattatore, selezionareistanza dell'adattatore che hai creato.
3. Nella scheda Metodo di mappatura, seleziona **Recupera attributi aggiuntivi da un archivio dati**.
4. Nella scheda Origine attributo e ricerca utente, seleziona **Aggiungi origine attributo**.
5. Nella scheda Archivio dati, fornire una descrizione e selezionarearchivio dati hai aggiunto.
6. Nella scheda Ricerca directory LDAP:
   - Immettere il **DN di base**, che deve corrispondere esattamente al valore immesso in StorageGRID per il server LDAP.
   - Per l'ambito di ricerca, selezionare **Sottoalbero**.
   - Per la classe dell'oggetto radice, cercare e aggiungere uno di questi attributi: **objectGUID** o **userPrincipalName**.
7. Nella scheda Tipi di codifica degli attributi binari LDAP, selezionare **Base64** per l'attributo **objectGUID**.
8. Nella scheda Filtro LDAP, immettere **sAMAccountName=${username}**.
9. Nella scheda Adempimento contratto attributi, seleziona **LDAP (attributo)** dal menu a discesa Origine e seleziona **objectGUID** o **userPrincipalName** dal menu a discesa Valore.
10. Rivedere e quindi salvare la fonte dell'attributo.
11. Nella scheda Failsave Attribute Source, seleziona **Abort the SSO Transaction**.
12. Rivedi il riepilogo e seleziona **Fine**.
13. Selezionare **Fatto**.

Configurare le impostazioni del protocollo

Passi

1. Nella scheda **Connessione SP * > *SSO browser** > **Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL del servizio consumer di asserzione, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**POST** per Binding e `/api/saml-response` per l'URL dell'endpoint).
3. Nella scheda URL del servizio SLO, accettare i valori predefiniti, che sono stati importati dai metadati SAML StorageGRID (**REDIRECT** per Binding e `/api/saml-logout` per l'URL dell'endpoint.
4. Nella scheda Binding SAML consentiti, deselezionare **ARTIFACT** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Criterio di firma, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste di autorizzazione** e **Firma sempre l'asserzione**.

6. Nella scheda Criterio di crittografia, selezionare **Nessuno**.
7. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni del protocollo.
8. Rivedi il riepilogo e seleziona **Fine** per salvare le impostazioni SSO del browser.

Configurare le credenziali

Passi

1. Dalla scheda Connessione SP , selezionare **Credenziali**.
2. Dalla scheda Credenziali, seleziona **Configura credenziali**.
3. Seleziona ilcertificato di firma che hai creato o importato.
4. Selezionare **Avanti** per andare a **Gestisci impostazioni di verifica della firma**.
   a. Nella scheda Modello di fiducia, seleziona **Non ancorato**.
   b. Nella scheda Certificato di verifica della firma, rivedere le informazioni sul certificato di firma, importate dai metadati SAML StorageGRID .
5. Rivedere le schermate di riepilogo e selezionare **Salva** per salvare la connessione SP .

Crea connessioni SP aggiuntive

Puoi copiare la prima connessione SP per creare le connessioni SP necessarie per ogni nodo amministrativo nella tua griglia. Carichi nuovi metadati per ogni copia.

> Le connessioni SP per diversi nodi amministrativi utilizzano impostazioni identiche, ad eccezione dell'ID entità del partner, dell'URL di base, dell'ID connessione, del nome della connessione, della verifica della firma e dell'URL di risposta SLO.

Passi

1. Selezionare **Azione** > **Copia** per creare una copia della connessione SP iniziale per ogni nodo amministrativo aggiuntivo.
2. Inserisci l'ID connessione e il Nome connessione per la copia e seleziona **Salva**.
3. Selezionare il file di metadati corrispondente al nodo di amministrazione:
   a. Selezionare **Azione** > **Aggiorna con metadati**.
   b. Seleziona **Scegli file** e carica i metadati.
   c. Selezionare **Avanti**.
   d. Seleziona **Salva**.
4. Risolvi l'errore dovuto all'attributo non utilizzato:
   a. Selezionare la nuova connessione.
   b. Selezionare **Configura SSO browser > Configura creazione asserzione > Contratto attributo**.
   c. Elimina la voce per **urn:oid**.
   d. Seleziona **Salva**.

Disabilitare l'accesso singolo

Se non si desidera più utilizzare questa funzionalità, è possibile disattivare l'accesso

Single Sign-On (SSO). È necessario disabilitare l'accesso singolo prima di poter disabilitare la federazione delle identità.

Prima di iniziare

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

Passi

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

   Viene visualizzata la pagina Single Sign-on.

2. Selezionare l'opzione **Disabilitato**.
3. Seleziona **Salva**.

   Viene visualizzato un messaggio di avviso che indica che ora gli utenti locali potranno effettuare l'accesso.

4. Selezionare **OK**.

   Al successivo accesso a StorageGRID , verrà visualizzata la pagina Sign in a StorageGRID e sarà necessario immettere il nome utente e la password di un utente StorageGRID locale o federato.

Disattivare e riattivare temporaneamente l'accesso singolo per un nodo di amministrazione

Potresti non essere in grado di accedere a Grid Manager se il sistema Single Sign-On (SSO) non funziona. In questo caso, puoi disattivare e riattivare temporaneamente l'SSO per un nodo di amministrazione. Per disattivare e riattivare l'SSO, è necessario accedere alla shell dei comandi del nodo.

Prima di iniziare

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

Informazioni su questo compito

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

> La disabilitazione dell'SSO per un nodo amministrativo non influisce sulle impostazioni SSO per gli altri nodi amministrativi nella griglia. La casella di controllo **Abilita SSO** nella pagina Single Sign-on in Grid Manager rimane selezionata e tutte le impostazioni SSO esistenti vengono mantenute a meno che non vengano aggiornate.

Passi

1. Accedi a un nodo di amministrazione:
   a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`

b. Inserisci la password elencata nel `Passwords.txt` file.

c. Immettere il seguente comando per passare alla root: `su -`

d. Inserisci la password elencata nel `Passwords.txt` file.

Quando si accede 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. Conferma che vuoi disabilitare l'SSO.

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

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

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

5. Sign in con il nome utente root e la password dell'utente root locale.
6. Se hai disabilitato temporaneamente l'SSO perché dovevi correggere la configurazione dell'SSO:
   a. Selezionare **CONFIGURAZIONE** > **Controllo accessi** > **Single sign-on**.
   b. Modifica le impostazioni SSO errate o obsolete.
   c. Seleziona **Salva**.

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

7. Se hai disabilitato temporaneamente l'SSO perché avevi bisogno di accedere a Grid Manager per qualche altro motivo:
   a. Esegui qualsiasi compito o compiti che devi svolgere.
   b. Selezionare **Esci** e chiudere Grid Manager.
   c. Riattivare SSO sul nodo di amministrazione. È possibile eseguire uno dei seguenti passaggi:

      - Eseguire il seguente comando: `enable-saml`

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

      Conferma di voler abilitare l'SSO.

   Un messaggio indica che l'accesso singolo è abilitato 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 Sign in a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

Informazioni sul copyright

Informazioni sul marchio commerciale