



# **Utilizzo di SSO (Single Sign-on)**

## StorageGRID software

NetApp  
January 14, 2026

# Sommario

Utilizzo di SSO (Single Sign-on) . . . . .	1
Come funziona SSO . . . . .	1
Effettuare l'accesso quando SSO è attivato . . . . .	1
Disconnettersi quando SSO è attivato . . . . .	2
Requisiti e considerazioni per SSO . . . . .	3
Requisiti del provider di identità . . . . .	3
Requisiti dei certificati del server . . . . .	4
Requisiti delle porte . . . . .	4
Confermare che gli utenti federati possono accedere . . . . .	4
Configurare SSO . . . . .	5
Accedere alla procedura guidata . . . . .	6
Fornire i dettagli del provider di identità . . . . .	7
Fornire l'identificatore della parte affidabile . . . . .	7
Configurare i trust, le applicazioni aziendali o le connessioni SP della parte che si basa . . . . .	9
Configurazione di prova . . . . .	10
Attiva single sign-on . . . . .	12
Creazione di trust di parti di base in ad FS . . . . .	12
Creare un trust di parte con Windows PowerShell . . . . .	13
Creare un trust per la parte che si basa importando i metadati della federazione . . . . .	14
Creare manualmente un trust per la parte che si basa . . . . .	15
Crea applicazioni aziendali in Entra ID . . . . .	17
Accedi Entra ID . . . . .	18
Creare applicazioni aziendali e salvare la configurazione SSO di StorageGRID . . . . .	18
Scarica i metadati SAML per ogni nodo di amministrazione . . . . .	18
Carica i metadati SAML in ogni applicazione aziendale . . . . .	19
Creare connessioni SP (service provider) in PingFederate . . . . .	19
Completare i prerequisiti in PingFederate . . . . .	20
Creare una connessione SP in PingFederate . . . . .	21
Disabilitare SSO . . . . .	23
Disabilitare e riabilitare temporaneamente SSO per un nodo di amministrazione . . . . .	24

# Utilizzo di SSO (Single Sign-on)

## Come funziona SSO

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

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

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

### Effettuare l'accesso quando SSO è attivato

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

#### Fasi

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

Viene visualizzata la pagina di accesso a StorageGRID.

- Se è la prima volta che accedi all'URL su questo browser, ti verrà richiesto un ID account.
- Se hai già effettuato l'accesso a Grid Manager o Tenant Manager, ti verrà chiesto di selezionare un account recente o di immettere un ID account.



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

2. Indicare se si desidera accedere a Grid Manager o al tenant Manager:

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

3. Selezionare **Accedi**

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

4. Accedi con le tue credenziali SSO.

Se le credenziali SSO sono corrette:

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



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

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

Non è necessario immettere nuovamente le credenziali SSO.

## Disconnettersi quando SSO è attivato

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

### Fasi

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

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



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

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

# Requisiti e considerazioni per SSO

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

## Requisiti del provider di identità

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

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

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

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory	<ul style="list-style-type: none"><li>• Active Directory</li><li>• Entra ID</li><li>• PingFederate</li></ul>
Entra ID	Entra ID

## Requisiti AD FS

È possibile utilizzare una delle seguenti versioni di ad FS:

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



Windows Server 2016 deve utilizzare il "[Aggiornamento KB3201845](#)" o una versione successiva.

## Requisiti aggiuntivi

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

## Considerazioni per Entra ID

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

## Requisiti dei certificati del server

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

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

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

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

## Requisiti delle porte

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

## Confermare che gli utenti federati possono accedere

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

### Prima di iniziare

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

### Fasi

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



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

- a. Accedi al tenant manager per ogni account tenant.
- b. Selezionare **Gestione accessi > Federazione identità**.

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

#### Informazioni correlate

- "[Requisiti e considerazioni per il single sign-on](#)"
- "[Gestire i gruppi di amministratori](#)"
- "[Utilizzare un account tenant](#)"

## Configurare SSO

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

#### Prima di iniziare

- L'utente ha effettuato l'accesso a Grid Manager utilizzando un "[browser web supportato](#)".
- Si dispone di "[Autorizzazione di accesso root](#)".

- Hai configurato la federazione delle identità per il tuo sistema StorageGRID.
- Per il tipo di servizio LDAP di federazione delle identità, hai selezionato Active Directory o Entra ID, in base al provider di identità SSO che intendi utilizzare.

Tipo di servizio LDAP configurato	Opzioni per il provider di identità SSO
Active Directory Federation Service (ad FS)	<ul style="list-style-type: none"> <li>• Active Directory</li> <li>• Entra ID</li> <li>• PingFederate</li> </ul>
Entra ID	Entra ID

### A proposito di questa attività

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

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

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

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

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

## Accedere alla procedura guidata

### Fasi

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



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

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

## Fornire i dettagli del provider di identità

### Fasi

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



Per individuare il nome del servizio federativo, accedere a Gestione server Windows.

Selezionare **Tools > ad FS Management**. Dal menu Action (azione), selezionare **Edit Federation Service Properties** (Modifica proprietà servizio federazione). Il nome del servizio della federazione viene visualizzato nel secondo campo.

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

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

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



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

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

## Fornire l'identificatore della parte affidabile

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

## Active Directory

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



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

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

## Entra ID

- a. Nella sezione Applicazione aziendale, specificare il **Nome dell'applicazione aziendale** per StorageGRID. Questo valore controlla il nome utilizzato per ciascuna applicazione aziendale in Entra ID.
  - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere SG o StorageGRID.
  - Se la griglia include più di un nodo di amministrazione, includi la stringa [HOSTNAME] nell'identificatore. Ad esempio, SG- [HOSTNAME] . L'inclusione di questa stringa genera una tabella che mostra il nome di un'applicazione aziendale per ciascun nodo di amministrazione nel sistema, in base al nome host del nodo.



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

- b. Segui i passaggi in "[Crea applicazioni aziendali in Entra ID](#)" per creare un'applicazione aziendale per ogni nodo amministrativo elencato nella tabella.
- c. Dall'ID Entra, copiare l'URL dei metadati della federazione per ogni applicazione aziendale. Quindi, incolla questo URL nel campo **URL metadati federazione** corrispondente in StorageGRID.
- d. Dopo aver copiato e incollato un URL dei metadati di federazione per tutti i nodi amministrativi, seleziona **Salva e accedi alla modalità sandbox**.

## PingFederate

- a. Nella sezione Provider di servizi (SP), specificare **ID connessione SP** per StorageGRID. Questo valore controlla il nome utilizzato per ogni connessione SP in PingFederate.
  - Ad esempio, se la griglia dispone di un solo nodo amministrativo e non si prevede di aggiungere altri nodi amministrativi in futuro, immettere SG o StorageGRID.

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



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

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

Utilizzare il seguente formato:

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

- Selezione **Salva e accedi alla modalità sandbox**.

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

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

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

## Active Directory

### Fasi

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

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

Per istruzioni, vedere "[Creazione di trust di parti di base in ad FS](#)".

## Entra ID

### Fasi

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

## PingFederate

### Fasi

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

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

## Configurazione di prova

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

## Active Directory

### Fasi

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

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

## Entra ID

### Fasi

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

## PingFederate

### Fasi

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

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

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

## Attiva single sign-on

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

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

### Fasi

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

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

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

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

## Creazione di trust di parti di base in ad FS

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

### Prima di iniziare

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



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

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

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

#### A proposito di questa attività

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

### Creare un trust di parte con Windows PowerShell

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

#### Fasi

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

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

- Per *Admin\_Node\_Identifier*, immettere l'identificatore del gruppo di riferimento per il nodo di amministrazione, esattamente come viene visualizzato nella pagina Single Sign-on. Ad esempio, SG-DC1-ADM1.
- Per *Admin\_Node\_FQDN*, immettere il nome di dominio completo per lo stesso nodo amministrativo. (Se necessario, è possibile utilizzare l'indirizzo IP del nodo. Tuttavia, se si immette un indirizzo IP, è necessario aggiornare o ricreare la fiducia della parte che si basa se tale indirizzo IP cambia).

3. Da Gestione server Windows, selezionare **Strumenti > Gestione di ad FS**.

Viene visualizzato lo strumento di gestione di ad FS.

4. Selezionare **ad FS > Trust di parte**.

Viene visualizzato l'elenco dei trust della parte che si basa.

5. Aggiungere un criterio di controllo degli accessi al trust della parte di base appena creato:

- Individuare la fiducia della parte di base appena creata.
- Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit Access Control Policy** (Modifica policy di controllo degli accessi).
- Selezionare un criterio di controllo degli accessi.
- Selezionare **Applica** e **OK**

6. Aggiungere una policy di emissione delle richieste di rimborso al nuovo Trust della parte di base creato:

- Individuare la fiducia della parte di base appena creata.
- Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
- Selezionare **Aggiungi regola**.

- d. Nella pagina Select Rule Template (Selezione modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next (Avanti)**.
  - e. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola. Ad esempio, **objectGUID a ID nome o UPN a ID nome**.
  - f. Per l'archivio attributi, selezionare **Active Directory**.
  - g. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
  - h. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID (ID nome)** dall'elenco a discesa.
  - i. Selezionare **fine**, quindi **OK**.
7. Verificare che i metadati siano stati importati correttamente.
- a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
  - b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.
- Se i metadati non sono presenti, verificare che l'indirizzo dei metadati della federazione sia corretto oppure inserire i valori manualmente.
8. Ripetere questa procedura per configurare un trust per tutti i nodi di amministrazione nel sistema StorageGRID.
9. Al termine, tornare a StorageGRID e ["testare tutti i trust delle parti affidanti"](#) per confermare che siano configurati correttamente.

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

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

### Fasi

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

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

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

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



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

7. Aggiungere una regola di richiesta di rimborso:

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

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

- e. Per l'archivio attributi, selezionare **Active Directory**.
- f. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
- g. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
- h. Selezionare **fine**, quindi **OK**.

8. Verificare che i metadati siano stati importati correttamente.

- a. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
- b. Verificare che i campi nelle schede **endpoint**, **identificatori** e **Firma** siano compilati.

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

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

10. Al termine, tornare a StorageGRID e "[testare tutti i trust delle parti affidanti](#)" per confermare che siano configurati correttamente.

## Creare manualmente un trust per la parte che si basa

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

### Fasi

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

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

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

- b. Saltare il passaggio per configurare un certificato di crittografia token opzionale.
- c. Nella pagina Configure URL (Configura URL), selezionare la casella di controllo **Enable support for the SAML 2.0 WebSSO Protocol** (attiva supporto per il protocollo SAML WebSSO).
- d. Digitare l'URL dell'endpoint del servizio SAML per il nodo di amministrazione:

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

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

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

`Admin_Node_Identifier`

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

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

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



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

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

- a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste di rimborso) dall'elenco e selezionare **Next** (Avanti).
- b. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.

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

- c. Per l'archivio attributi, selezionare **Active Directory**.
  - d. Nella colonna attributo LDAP della tabella Mapping, digitare **objectGUID** o selezionare **User-Principal-Name**.
  - e. Nella colonna Outgoing Claim Type (tipo di richiesta di rimborso in uscita) della tabella Mapping (mappatura), selezionare **Name ID** (ID nome) dall'elenco a discesa.
  - f. Selezionare **fine**, quindi **OK**.
7. Fare clic con il pulsante destro del mouse sull'attendibilità della parte che si basa per aprirne le proprietà.
  8. Nella scheda **Endpoint**, configurare l'endpoint per la disconnessione singola (SLO):
    - a. Selezionare **Add SAML** (Aggiungi SAML).
    - b. Selezionare **Endpoint Type > SAML Logout**.

c. Selezionare **binding > Redirect**.

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

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

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

a. Selezionare **OK**.

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

a. Aggiungere il certificato personalizzato:

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



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

b. Selezionare **Applica e OK**.

Le proprietà della parte di base vengono salvate e chiuse.

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

11. Al termine, tornare a StorageGRID e ["testare tutti i trust delle parti affidanti"](#) per confermare che siano configurati correttamente.

## Crea applicazioni aziendali in Entra ID

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

### Prima di iniziare

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



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

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

## Accedi Entra ID

### Fasi

1. Accedere a "[Portale Azure](#)".
2. Vai a "[Entra ID](#)".
3. Selezionare "[Applicazioni aziendali](#)".

## Creare applicazioni aziendali e salvare la configurazione SSO di StorageGRID

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

### Fasi

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

## Scarica i metadati SAML per ogni nodo di amministrazione

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

### Fasi

1. Ripetere questi passaggi per ciascun nodo di amministrazione.
  - a. Accedere a StorageGRID dal nodo di amministrazione.

- b. Selezionare **Configurazione > Controllo accessi > Single sign-on**.
- c. Selezionare il pulsante per scaricare i metadati SAML per il nodo di amministrazione.
- d. Salva il file che caricherai in Entra ID.

## Carica i metadati SAML in ogni applicazione aziendale

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

### Fasi

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



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

- a. Accedere alla pagina Proprietà dell'applicazione aziendale.
  - b. Impostare **assegnazione richiesta** su **No** (a meno che non si desideri configurare separatamente le assegnazioni).
  - c. Vai alla pagina Single Sign-on.
  - d. Completare la configurazione SAML.
  - e. Selezionare il pulsante **carica file di metadati** e selezionare il file di metadati SAML scaricato per il nodo di amministrazione corrispondente.
  - f. Una volta caricato il file, selezionare **Salva**, quindi selezionare **X** per chiudere il riquadro. Viene visualizzata nuovamente la pagina Set up Single Sign-on with SAML (Configura Single Sign-on con SAML).
3. ["Testare ogni applicazione"](#).

## Creare connessioni SP (service provider) in PingFederate

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

### Prima di iniziare

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

## A proposito di questa attività

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

## Completare i prerequisiti in PingFederate

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

### Creare un archivio di dati

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

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

### Crea validatore credenziale password

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

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

### Crea istanza dell'adattatore IdP

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

#### Fasi

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

### Creare o importare un certificato di firma

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

## Fasi

1. Accedere a **sicurezza > chiavi e certificati di firma e decrittografia**.
2. Creare o importare il certificato di firma.

## Creare una connessione SP in PingFederate

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

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

## Scegliere il tipo di connessione SP

### Fasi

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

## Importare metadati SP

### Fasi

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

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

4. Selezionare **Avanti**.

## Configurare IdP browser SSO

### Fasi

1. Dalla scheda SSO del browser, selezionare **Configure browser SSO** (Configura SSO browser).
2. Nella scheda SAML profiles (profili SAML), selezionare le opzioni **SP-initiated SSO**, **SP-initial SLO**, **IdP-initiated SSO** e **IdP-initiated SLO**.
3. Selezionare **Avanti**.
4. Nella scheda Assertion Lifetime (durata asserzione), non apportare modifiche.
5. Nella scheda Assertion Creation (creazione asserzione), selezionare **Configure Assertion Creation (Configura creazione asserzione)**.
  - a. Nella scheda Identity Mapping (mappatura identità), selezionare **Standard**.

- b. Nella scheda Contratto attributo, utilizzare **SAML SUBJECT** come Contratto attributo e il formato del nome non specificato importato.
6. Per estendere il contratto, selezionare **Elimina** per rimuovere il `urn:oid`, non utilizzato.

## Istanza dell'adattatore di mappatura

### Fasi

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

## Configurare le impostazioni del protocollo

### Fasi

1. Nella scheda **connessione SP > SSO browser > Impostazioni protocollo**, selezionare **Configura impostazioni protocollo**.
2. Nella scheda URL servizio clienti asserzione, accettare i valori predefiniti, importati dai metadati SAML di StorageGRID (**POST** per l'associazione e `/api/saml-response` per l'URL dell'endpoint).
3. Nella scheda URL servizio SLO, accettare i valori predefiniti, importati dai metadati SAML di StorageGRID (**REDIRECT** per l'associazione e `/api/saml-logout` per l'URL dell'endpoint).
4. Nella scheda Allowable SAML Bindings (Binding SAML autorizzati), deselectare **ARTEFACTO** e **SOAP**. Sono richiesti solo **POST** e **REDIRECT**.
5. Nella scheda Firma Policy, lasciare selezionate le caselle di controllo **Richiedi la firma delle richieste Authn** e **Firma sempre asserzione**.

6. Nella scheda Encryption Policy (Criteri di crittografia), selezionare **None** (Nessuno).
7. Esaminare il riepilogo e selezionare **Done** (fine) per salvare le impostazioni del protocollo.
8. Esaminare il riepilogo e selezionare **fine** per salvare le impostazioni SSO del browser.

## Configurare le credenziali

### Fasi

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

## Creare ulteriori connessioni SP

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



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

### Fasi

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

## Disabilitare SSO

È possibile disattivare SSO (Single Sign-on) se non si desidera più utilizzare questa

funzionalità. È necessario disattivare il Single Sign-on prima di poter disattivare la federazione delle identità.

#### Prima di iniziare

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

#### Fasi

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

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

2. Seleziona **Disabilita SSO**.

3. Selezionare **Sì**.

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

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

## Disabilitare e riabilitare temporaneamente SSO per un nodo di amministrazione

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

#### Prima di iniziare

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

#### A proposito di questa attività

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

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

#### Fasi

1. Accedere a un nodo amministratore:

- a. Immettere il seguente comando: `ssh admin@Admin_Node_IP`
- b. Immettere la password elencata nel `Passwords.txt` file.

- c. Immettere il seguente comando per passare alla directory principale: `su` –
- d. Immettere la password elencata nel `Passwords.txt` file.

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

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

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

## 3. Confermare che si desidera disattivare SSO.

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

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

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

## 5. Accedere con il nome utente root e la password dell'utente root locale.

## 6. Se SSO è stato disattivato temporaneamente perché era necessario correggere la configurazione SSO:

- a. Selezionare **Configurazione > Controllo accessi > Single sign-on**.
- b. Modificare le impostazioni SSO non corrette o non aggiornate.
- c. Selezionare **Salva**.

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

## 7. Se l'SSO è stato disattivato temporaneamente perché era necessario accedere a Grid Manager per un altro motivo:

- a. Eseguire qualsiasi attività o attività da eseguire.
- b. Selezionare **Disconnetti** e chiudere Grid Manager.
- c. Riabilitare SSO sul nodo di amministrazione. È possibile eseguire una delle seguenti operazioni:
  - Eseguire il seguente comando: `enable-saml`

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

Confermare che si desidera attivare SSO.

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

- Riavviare il nodo della griglia: `reboot`

## 8. Da un browser Web, accedere a Grid Manager dallo stesso nodo di amministrazione.

## 9. Verificare che venga visualizzata la pagina di accesso a StorageGRID e che sia necessario immettere le credenziali SSO per accedere a Grid Manager.

## Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

## Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.