



# **Controllo dell'accesso amministratore a StorageGRID**

StorageGRID 11.5

NetApp  
April 11, 2024

# Sommario

- Controllo dell'accesso amministratore a StorageGRID ..... 1
  - Controllo dell'accesso tramite firewall ..... 1
  - Utilizzo della federazione delle identità ..... 2
  - Gestione dei gruppi di amministratori ..... 8
  - Gestione degli utenti locali ..... 16
  - Utilizzo di SSO (Single Sign-on) per StorageGRID ..... 18
  - Configurazione dei certificati client dell'amministratore ..... 37

# Controllo dell'accesso amministratore a StorageGRID

È possibile controllare l'accesso dell'amministratore al sistema StorageGRID aprendo o chiudendo le porte del firewall, gestendo utenti e gruppi di amministratori, configurando SSO (Single Sign-on) e fornendo certificati client per consentire l'accesso esterno sicuro alle metriche StorageGRID.

- ["Controllo dell'accesso tramite firewall"](#)
- ["Utilizzo della federazione delle identità"](#)
- ["Gestione dei gruppi di amministratori"](#)
- ["Gestione degli utenti locali"](#)
- ["Utilizzo di SSO \(Single Sign-on\) per StorageGRID"](#)
- ["Configurazione dei certificati client dell'amministratore"](#)

## Controllo dell'accesso tramite firewall

Quando si desidera controllare l'accesso tramite firewall, aprire o chiudere porte specifiche sul firewall esterno.

### Controllo dell'accesso al firewall esterno

È possibile controllare l'accesso alle interfacce utente e alle API sui nodi di amministrazione StorageGRID aprendo o chiudendo porte specifiche sul firewall esterno. Ad esempio, è possibile impedire ai tenant di connettersi a Grid Manager dal firewall, oltre a utilizzare altri metodi per controllare l'accesso al sistema.

Porta	Descrizione	Se la porta è aperta...
443	Porta HTTPS predefinita per i nodi di amministrazione	I browser Web e i client API di gestione possono accedere a Grid Manager, Grid Management API, Tenant Manager e Tenant Management API.  <b>Nota:</b> la porta 443 viene utilizzata anche per il traffico interno.
8443	Porta Grid Manager limitata sui nodi di amministrazione	<ul style="list-style-type: none"><li>• I browser Web e i client API di gestione possono accedere a Grid Manager e all'API di Grid Management utilizzando HTTPS.</li><li>• I browser Web e i client API di gestione non possono accedere a tenant Manager o all'API di gestione tenant.</li><li>• Le richieste di contenuto interno verranno rifiutate.</li></ul>

Porta	Descrizione	Se la porta è aperta...
9443	Porta limitata di Tenant Manager sui nodi di amministrazione	<ul style="list-style-type: none"> <li>• I browser Web e i client API di gestione possono accedere a Tenant Manager e all'API di gestione tenant utilizzando HTTPS.</li> <li>• I browser Web e i client API di gestione non possono accedere a Grid Manager o all'API di Grid Management.</li> <li>• Le richieste di contenuto interno verranno rifiutate.</li> </ul>



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).

### Informazioni correlate

["Accesso a Grid Manager"](#)

["Creazione di un account tenant se StorageGRID non utilizza SSO"](#)

["Riepilogo: Indirizzi IP e porte per le connessioni client"](#)

["Gestione di reti client non attendibili"](#)

["Installare Ubuntu o Debian"](#)

["Installare VMware"](#)

["Installare Red Hat Enterprise Linux o CentOS"](#)

## Utilizzo della federazione delle identità

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

### Configurazione della federazione delle identità

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

#### Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si prevede di attivare SSO (Single Sign-on), è necessario utilizzare Active Directory come origine dell'identità federata e ad FS come provider di identità. Consulta "requisiti per l'utilizzo del Single Sign-on".
- È necessario utilizzare Active Directory, OpenLDAP o Oracle Directory Server come provider di identità.



Se si desidera utilizzare un servizio LDAP v3 non presente nell'elenco, contattare il supporto tecnico.

- Se si intende utilizzare TLS (Transport Layer Security) per le comunicazioni con il server LDAP, il provider di identità deve utilizzare TLS 1.2 o 1.3.

### A proposito di questa attività

È necessario configurare un'origine identità per Grid Manager se si desidera importare i seguenti tipi di gruppi federated:

- Gruppi di amministrazione. Gli utenti dei gruppi di amministrazione possono accedere a Grid Manager ed eseguire attività in base alle autorizzazioni di gestione assegnate al gruppo.
- Gruppi di utenti tenant per tenant che non utilizzano la propria origine di identità. Gli utenti dei gruppi di tenant possono accedere al tenant manager ed eseguire le attività in base alle autorizzazioni assegnate al gruppo nel tenant manager.

### Fasi

1. Selezionare **Configuration Access Control Identity Federation**.
2. Selezionare **Enable Identity Federation** (attiva federazione identità).

Vengono visualizzati i campi per la configurazione del server LDAP.

3. Nella sezione tipo di servizio LDAP, selezionare il tipo di servizio LDAP che si desidera configurare.

È possibile selezionare **Active Directory**, **OpenLDAP** o **Other**.



Se si seleziona **OpenLDAP**, è necessario configurare il server OpenLDAP. Consultare le linee guida per la configurazione di un server OpenLDAP.



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

4. Se si seleziona **Altro**, completare i campi nella sezione attributi LDAP.
  - **User Unique Name** (Nome univoco utente): Il nome dell'attributo che contiene l'identificatore univoco di un utente LDAP. Questo attributo è equivalente a `sAMAccountName` Per Active Directory e `uid` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `uid`.
  - **UUID utente**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un utente LDAP. Questo attributo è equivalente a `objectGUID` Per Active Directory e `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Ogni valore dell'utente per l'attributo specificato deve essere un numero esadecimale a 32 cifre in formato a 16 byte o stringa, dove i trattini vengono ignorati.
  - **Group unique name** (Nome univoco gruppo): Il nome dell'attributo che contiene l'identificatore univoco di un gruppo LDAP. Questo attributo è equivalente a `sAMAccountName` Per Active Directory e `cn` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `cn`.
  - **UUID gruppo**: Il nome dell'attributo che contiene l'identificatore univoco permanente di un gruppo LDAP. Questo attributo è equivalente a `objectGUID` Per Active Directory e `entryUUID` Per OpenLDAP. Se si sta configurando Oracle Directory Server, immettere `nsuniqueid`. Il valore di ciascun gruppo per l'attributo specificato deve essere un numero esadecimale a 32 cifre nel formato a 16 byte o stringa, dove i trattini vengono ignorati.
5. Nella sezione Configure LDAP server (Configura server LDAP), immettere le informazioni richieste per il server LDAP e la connessione di rete.
  - **Nome host**: Nome host del server o indirizzo IP del server LDAP.

- **Port** (porta): Porta utilizzata per la connessione al server LDAP.



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

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



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

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

- sAMAccountName oppure uid
- objectGUID, entryUUID, o. nsuniqueid
- cn
- memberOf oppure isMemberOf

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



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

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



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

6. Nella sezione **Transport Layer Security (TLS)**, selezionare un'impostazione di protezione.

- **Utilizzare STARTTLS (consigliato)**: Utilizzare STARTTLS per proteggere le comunicazioni con il server LDAP. Questa è l'opzione consigliata.
- **Usa LDAPS**: L'opzione LDAPS (LDAP su SSL) utilizza TLS per stabilire una connessione al server LDAP. Questa opzione è supportata per motivi di compatibilità.
- **Non utilizzare TLS**: Il traffico di rete tra il sistema StorageGRID e il server LDAP non sarà protetto.



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

7. Se si seleziona STARTTLS o LDAPS, scegliere il certificato utilizzato per proteggere la connessione.

- **Usa certificato CA del sistema operativo**: Utilizzare il certificato CA predefinito installato sul sistema operativo per proteggere le connessioni.

- **Usa certificato CA personalizzato:** Utilizza un certificato di protezione personalizzato.

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

8. Facoltativamente, selezionare **Test di connessione** per convalidare le impostazioni di connessione per il server LDAP.

Se la connessione è valida, nell'angolo superiore destro della pagina viene visualizzato un messaggio di conferma.

9. Se la connessione è valida, selezionare **Salva**.

La seguente schermata mostra valori di configurazione di esempio per un server LDAP che utilizza Active Directory.

## LDAP service type

Select the type of LDAP service you want to configure.

Active Directory OpenLDAP Other

### Configure LDAP server (All fields are required)

<b>Hostname</b>	<b>Port</b>
<input type="text" value="my-active-directory.example.com"/>	<input type="text" value="389"/>
<b>Username</b>	
<input type="text" value="MyDomain\Administrator"/>	
<b>Password</b>	
<input type="password" value="••••••••"/>	
<b>Group Base DN</b>	
<input type="text" value="DC=storagegrid,DC=example,DC=com"/>	
<b>User Base DN</b>	
<input type="text" value="DC=storagegrid,DC=example,DC=com"/>	

## Informazioni correlate

["Crittografia supportata per le connessioni TLS in uscita"](#)

["Requisiti per l'utilizzo del single sign-on"](#)

["Creazione di un account tenant"](#)

["Utilizzare un account tenant"](#)

## Linee guida per la configurazione di un server OpenLDAP

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

### MemberOf e refint overlay

Gli overlay memberof e refint devono essere attivati. Per ulteriori informazioni, consultare le istruzioni per la manutenzione inversa dell'appartenenza al gruppo nella Guida per l'amministratore di OpenLDAP.

### Indicizzazione

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

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

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

Consultare le informazioni sulla manutenzione inversa dell'appartenenza al gruppo nella Guida per l'amministratore di OpenLDAP.

## Informazioni correlate

["Documentazione di OpenLDAP: Guida per l'amministratore della versione 2.4"](#)

## Forzare la sincronizzazione con l'origine dell'identità

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

### Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- L'origine dell'identità deve essere attivata.

### Fasi

1. Selezionare **Configuration Access Control Identity Federation**.



Viene visualizzata la pagina Identity Federation. Il pulsante **Synchronize** si trova nella parte inferiore della pagina.

### Synchronize

---

StorageGRID periodically synchronizes federated groups and users from the configured LDAP server. Clicking the button below will immediately start the synchronization process against the saved LDAP server.

Synchronize

## 2. Fare clic su **Sincronizza**.

Un messaggio di conferma indica che la sincronizzazione è stata avviata correttamente. Il processo di sincronizzazione potrebbe richiedere del tempo a seconda dell'ambiente in uso.



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

## Disattivazione della federazione delle identità

È possibile disattivare temporaneamente o permanentemente la federazione di identità per gruppi e utenti. Quando la federazione delle identità è disattivata, non vi è alcuna comunicazione tra StorageGRID e l'origine delle identità. Tuttavia, tutte le impostazioni configurate vengono conservate, consentendo di riabilitare facilmente la federazione delle identità in futuro.

### Di cosa hai bisogno

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

### A proposito di questa attività

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

- Gli utenti federati non potranno accedere.
- Gli utenti federati che hanno effettuato l'accesso manterranno l'accesso al sistema StorageGRID fino alla scadenza della sessione, ma non potranno accedere dopo la scadenza della sessione.
- La sincronizzazione tra il sistema StorageGRID e l'origine dell'identità non viene eseguita e non vengono generati avvisi o allarmi per gli account che non sono stati sincronizzati.
- La casella di controllo **Enable Identity Federation** (Abilita federazione identità) è disattivata se Single Sign-on (SSO) è impostato su **Enabled** o **Sandbox Mode**. Lo stato SSO nella pagina Single Sign-on deve essere **Disabled** prima di poter disattivare la federazione delle identità.

### Fasi

1. Selezionare **Configuration Access Control Identity Federation**.
2. Deselezionare la casella di controllo **Enable Identity Federation** (attiva federazione identità).
3. Fare clic su **Save** (Salva).

### Informazioni correlate

["Disattivazione del single sign-on"](#)

# Gestione dei gruppi di amministratori

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

## Creazione di gruppi di amministratori

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

### Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Se si intende importare un gruppo federated, è necessario che la federazione delle identità sia configurata e che il gruppo federated esista già nell'origine delle identità configurata.

### Fasi

#### 1. Selezionare **Configuration Access Control Admin Groups**.

Viene visualizzata la pagina Admin Groups (gruppi di amministratori) che elenca i gruppi di amministratori esistenti.

#### Admin Groups

Add and manage local and federated user groups, allowing member users to sign in to the Grid Manager. Set group permissions to control access to specific pages and features.


<span>+ Add</span> <span>Clone</span> <span>Edit</span> <span>Remove</span>				
	Name	ID	Group Type	Access Mode
<input checked="" type="radio"/>	Flintstone	264083d0-23b5-3046-9bd4-88b7097731ab	Federated	Read-write
<input type="radio"/>	Simpson	cc8ad11f-68d0-f84a-af29-e7a6fcdc63a2	Federated	Read-only
<input type="radio"/>	ILM (read-only group)	88446141-9599-4543-b183-9c227ce7767a	Local	Read-only
<input type="radio"/>	API Developers	974b2faa-f9a1-4cfc-b364-914cdba2905f	Local	Read-write
<input type="radio"/>	ILM Admins (read-write)	a528c0c2-2417-4559-86ed-f0d2e31da820	Local	Read-write
<input type="radio"/>	Maintenance Users	7e3400ec-de8c-45a7-8bb8-e1496b362a8d	Local	Read-write
Group Type: <span>All</span> Show <span>20</span> rows per page				

#### 2. Selezionare **Aggiungi**.

Viene visualizzata la finestra di dialogo Add Group (Aggiungi gruppo).


## Add Group

Create a new local group or import a group from the external identity source.













Group Type   Local  Federated

Display Name

Unique Name 

Access Mode   Read-write  Read-only

### Management Permissions

- |  |   |
|--|---|
| <input type="checkbox"/> Root Access                  | <input type="checkbox"/> Manage Alerts                     |
| <input type="checkbox"/> Acknowledge Alarms           | <input type="checkbox"/> Grid Topology Page Configuration  |
| <input type="checkbox"/> Other Grid Configuration     | <input type="checkbox"/> Tenant Accounts                   |
| <input type="checkbox"/> Change Tenant Root Password  | <input type="checkbox"/> Maintenance                       |
| <input type="checkbox"/> Metrics Query                | <input type="checkbox"/> ILM                                 |
| <input type="checkbox"/> Object Metadata Lookup      | <input type="checkbox"/> Storage Appliance Administrator  |

Cancel

Save

3. Per tipo di gruppo, selezionare **locale** se si desidera creare un gruppo che verrà utilizzato solo all'interno di StorageGRID oppure selezionare **Federato** se si desidera importare un gruppo dall'origine dell'identità.
4. Se si seleziona **locale**, immettere un nome visualizzato per il gruppo. Il nome visualizzato è il nome visualizzato in Grid Manager. Ad esempio, "Maintenance Users" o "ILM Administrators."
5. Immettere un nome univoco per il gruppo.
  - **Locale**: Immettere il nome univoco desiderato. Ad esempio, "ILM Administrators."
  - **Federated**: Immettere il nome del gruppo esattamente come appare nell'origine dell'identità configurata.
6. Per **Access Mode**, selezionare se gli utenti del gruppo possono modificare le impostazioni ed eseguire operazioni in Grid Manager e nell'API Grid Management o se possono visualizzare solo impostazioni e funzionalità.
  - **Read-write** (valore predefinito): Gli utenti possono modificare le impostazioni ed eseguire le operazioni consentite dalle autorizzazioni di gestione.
  - **Sola lettura**: Gli utenti possono visualizzare solo le impostazioni e le funzionalità. Non possono apportare modifiche o eseguire operazioni nell'API Grid Manager o Grid Management. Gli utenti locali di sola lettura possono modificare le proprie password.



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

7. Selezionare una o più autorizzazioni di gestione.

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

8. Selezionare **Salva**.

Viene creato il nuovo gruppo. Se si tratta di un gruppo locale, è ora possibile aggiungere uno o più utenti. Se si tratta di un gruppo federated, l'origine identità gestisce gli utenti appartenenti al gruppo.

### Informazioni correlate

["Gestione degli utenti locali"](#)

## Autorizzazioni del gruppo di amministrazione

Quando si creano gruppi di utenti admin, si selezionano una o più autorizzazioni per controllare l'accesso a funzionalità specifiche di Grid Manager. È quindi possibile assegnare ciascun utente a uno o più di questi gruppi di amministratori per determinare quali attività possono essere eseguite dall'utente.

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

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

- Accedi a Grid Manager
- Visualizza la dashboard
- Visualizzare le pagine dei nodi
- Monitorare la topologia della griglia
- Visualizzare gli avvisi correnti e risolti
- Visualizzazione degli allarmi correnti e storici (sistema legacy)
- Modifica della propria password (solo utenti locali)
- Visualizzare alcune informazioni nelle pagine Configurazione e manutenzione

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

### Accesso root

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

### Gestire gli avvisi

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

### Riconoscere gli allarmi (sistema legacy)

Questa autorizzazione consente di riconoscere e rispondere agli allarmi (sistema legacy). Tutti gli utenti che hanno effettuato l'accesso possono visualizzare gli allarmi correnti e storici.

Se si desidera che un utente monitori la topologia della griglia e riconosca solo gli allarmi, è necessario assegnare questa autorizzazione.

### Configurazione della pagina Grid Topology (topologia griglia)

Questa autorizzazione consente di accedere alle seguenti opzioni di menu:

- Schede di configurazione disponibili nelle pagine di **supporto Strumenti topologia griglia**.
- Collegamento **Reset event count** (Ripristina conteggi eventi) nella scheda **Nodes Events** (nodi).

### Altra configurazione della griglia

Questa autorizzazione consente di accedere a ulteriori opzioni di configurazione della griglia.



Per visualizzare queste opzioni aggiuntive, gli utenti devono disporre anche dell'autorizzazione Grid Topology Page Configuration.

- **Allarmi** (sistema legacy):
  - Allarmi globali
  - Configurazione e-mail legacy
- **ILM:**
  - Pool di storage
  - Storage Grades (gradi di storage)
- **Configurazione Impostazioni di rete**
  - Costo del collegamento
- **Configurazione Impostazioni di sistema:**
  - Opzioni di visualizzazione
  - Opzioni griglia
  - Opzioni di storage
- **Configurazione monitoraggio:**
  - Eventi
- **Supporto:**
  - AutoSupport

### Account tenant

Questa autorizzazione consente di accedere alla pagina **tenant tenant account**.



La versione 1 dell'API Grid Management (obsoleta) utilizza questa autorizzazione per gestire i criteri di gruppo tenant, reimpostare le password di amministrazione di Swift e gestire le chiavi di accesso S3 dell'utente root.

### Modificare la password principale del tenant

Questa autorizzazione consente di accedere all'opzione **Change Root Password** (Modifica password root) nella pagina Tenant Accounts (account tenant), consentendo di controllare chi può modificare la password per

l'utente root locale del tenant. Gli utenti che non dispongono di questa autorizzazione non possono visualizzare l'opzione **Change Root Password** (Modifica password root).



Prima di poter assegnare questa autorizzazione, è necessario assegnare al gruppo l'autorizzazione account tenant.

## Manutenzione

Questa autorizzazione consente di accedere alle seguenti opzioni di menu:

- **Configurazione Impostazioni di sistema:**
  - Nomi di dominio\*
  - Certificati server\*
- **Configurazione monitoraggio:**
  - Audit\*
- **Configurazione controllo accessi:**
  - Password di rete
- **Manutenzione attività di manutenzione**
  - Decommissionare
  - Espansione
  - Recovery (recupero)
- **Manutenzione rete:**
  - Server DNS\*
  - Rete di rete\*
  - Server NTP\*
- **Manutenzione sistema:**
  - Licenza\*
  - Pacchetto di ripristino
  - Aggiornamento software
- **Supporto Strumenti:**
  - Registri
- Gli utenti che non dispongono dell'autorizzazione di manutenzione possono visualizzare, ma non modificare, le pagine contrassegnate da un asterisco.

## Query metriche

Questa autorizzazione consente di accedere alla pagina **Support Tools Metrics**. Questa autorizzazione consente inoltre di accedere alle query metriche Prometheus personalizzate utilizzando la sezione **metriche** dell'API Grid Management.

## ILM

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

- Erasure coding
- Regole
- Politiche
- Regioni



L'accesso alle opzioni di menu **ILM Storage Pools** e **ILM Storage Grades** è controllato dalle altre autorizzazioni Grid Configuration (Configurazione griglia) e Grid Topology Page Configuration (Configurazione pagina topologia griglia).

### Object Metadata Lookup (Ricerca metadati oggetto)

Questa autorizzazione consente di accedere all'opzione di menu **ILM Object Metadata Lookup**.

### Amministratore dell'appliance di storage

Questa autorizzazione consente di accedere al gestore di sistema e-Series SANtricity sulle appliance di storage tramite Grid Manager.

### Interazione tra permessi e modalità di accesso

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

### Disattivazione delle funzionalità dall'API Grid Management

È possibile utilizzare l'API di gestione griglia per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzione viene disattivata, non è possibile assegnare a nessuno le autorizzazioni per eseguire le attività correlate a tale funzione.

#### A proposito di questa attività

Il sistema Disattivato consente di impedire l'accesso a determinate funzioni del sistema StorageGRID. La disattivazione di una funzione è l'unico modo per impedire all'utente root o agli utenti appartenenti a gruppi di amministrazione con l'autorizzazione di accesso root di utilizzare tale funzione.

Per comprendere come questa funzionalità potrebbe essere utile, considerare il seguente scenario:

*L'azienda A è un provider di servizi che affitta la capacità di storage del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei titolari di leasing, la Società A desidera garantire che i propri dipendenti non possano mai accedere a alcun account tenant dopo l'implementazione dell'account.*

*L'azienda A è in grado di raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API Grid Management. Disattivando completamente la funzione **Change tenant Root Password** in Grid Manager (sia l'interfaccia utente che l'API), la società A può garantire che nessun utente Admin, incluso l'utente root e gli utenti appartenenti a gruppi con l'autorizzazione Root Access, possa modificare la password per qualsiasi utente root dell'account tenant.*

#### Riattivazione delle funzioni disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzione disattivata. Tuttavia, se si desidera evitare che le funzioni disattivate vengano riattivate, è possibile disattivare

la funzione **ActivateFeatures**.



Impossibile riattivare la funzione **ActivateFeatures**. Se decidi di disattivare questa funzione, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzione disattivata. È necessario contattare il supporto tecnico per ripristinare eventuali funzionalità perse.

Per ulteriori informazioni, consultare le istruzioni per l'implementazione delle applicazioni client S3 o Swift.

### Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia.
2. Individuare l'endpoint Deactivate Features.
3. Per disattivare una funzione, ad esempio **Change tenant Root Password**, inviare un corpo all'API come segue:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Al termine della richiesta, la funzione Cambia password principale tenant viene disattivata. L'autorizzazione per la gestione della password principale del tenant non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenta di modificare la password root per un tenant non riuscirà con "403 Forbidden".

4. Per riattivare tutte le funzioni, inviare un corpo all'API come segue:

```
{ "grid": null }
```

Una volta completata la richiesta, tutte le funzioni, inclusa la funzione Change tenant Root Password (Modifica password principale tenant), vengono riattivate. L'autorizzazione di gestione della password root del tenant viene ora visualizzata nell'interfaccia utente e tutte le richieste API che tentano di modificare la password root di un tenant avranno esito positivo, presupponendo che l'utente disponga dell'autorizzazione di gestione Root Access o Change tenant Root Password.



L'esempio precedente causa la riattivazione di *tutte* le funzioni disattivate. Se sono state disattivate altre funzioni che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzione Cambia password principale tenant e continuare a disattivare la funzione di conferma allarme, inviare la seguente richiesta PUT:

```
{ "grid": { "alarmAcknowledgment": true } }
```

### Informazioni correlate

["Utilizzando l'API Grid Management"](#)

## Modifica di un gruppo di amministratori

È possibile modificare un gruppo di amministratori per modificare le autorizzazioni associate al gruppo. Per i



gruppi di amministratori locali, è anche possibile aggiornare il nome visualizzato.

### Di cosa hai bisogno

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

### Fasi

1. Selezionare **Configuration Access Control Admin Groups**.
2. Selezionare il gruppo.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Edit** (Modifica).
4. Se si desidera, per i gruppi locali, inserire il nome del gruppo che verrà visualizzato agli utenti, ad esempio "Maintenance Users".

Non è possibile modificare il nome univoco, ovvero il nome del gruppo interno.

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



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

6. Facoltativamente, aggiungere o rimuovere le autorizzazioni di gruppo.

Vedere le informazioni sulle autorizzazioni del gruppo di amministrazione.

7. Selezionare **Salva**.

### Informazioni correlate

[Autorizzazioni del gruppo di amministrazione](#)

## Eliminazione di un gruppo di amministratori

È possibile eliminare un gruppo di amministratori quando si desidera rimuovere il gruppo dal sistema e rimuovere tutte le autorizzazioni associate al gruppo. L'eliminazione di un gruppo di amministratori comporta la rimozione di tutti gli utenti admin dal gruppo, ma non l'eliminazione degli utenti admin.

### Di cosa hai bisogno

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

### A proposito di questa attività

Quando elimini un gruppo, gli utenti assegnati a quel gruppo perderanno tutti i privilegi di accesso a Grid

Manager, a meno che non ricevano privilegi da un altro gruppo.

### Fasi

1. Selezionare **Configuration Access Control Admin Groups**.
2. Selezionare il nome del gruppo.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Selezionare **Rimuovi**.
4. Selezionare **OK**.

## Gestione degli utenti locali

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

Grid Manager include un utente locale predefinito, denominato "root". Sebbene sia possibile aggiungere e rimuovere utenti locali, non è possibile rimuovere l'utente root.



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

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

### Creazione di un utente locale

Se sono stati creati gruppi di amministratori locali, è possibile creare uno o più utenti locali e assegnare ciascun utente a uno o più gruppi. Le autorizzazioni del gruppo controllano le funzionalità di Grid Manager a cui l'utente può accedere.

#### A proposito di questa attività

È possibile creare solo utenti locali e assegnarli solo a gruppi di amministratori locali. Gli utenti federati e i gruppi federati vengono gestiti utilizzando l'origine dell'identità esterna.

### Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Fare clic su **Create** (Crea).
3. Immettere il nome visualizzato, il nome univoco e la password dell'utente.
4. Assegnare l'utente a uno o più gruppi che gestiscono le autorizzazioni di accesso.

L'elenco dei nomi dei gruppi viene generato dalla tabella Groups (gruppi).

5. Fare clic su **Save** (Salva).

### Informazioni correlate

["Gestione dei gruppi di amministratori"](#)

## Modifica dell'account di un utente locale

È possibile modificare l'account di un utente amministratore locale per aggiornare il nome visualizzato dell'utente o l'appartenenza al gruppo. È inoltre possibile impedire temporaneamente a un utente di accedere al sistema.

### A proposito di questa attività

È possibile modificare solo gli utenti locali. I dettagli dell'utente federato vengono sincronizzati automaticamente con l'origine dell'identità esterna.

### Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Selezionare l'utente che si desidera modificare.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Edit** (Modifica).
4. Facoltativamente, apportare modifiche al nome o all'appartenenza al gruppo.
5. Facoltativamente, per impedire all'utente di accedere temporaneamente al sistema, selezionare **Nega accesso**.
6. Fare clic su **Save** (Salva).

Le nuove impostazioni vengono applicate alla successiva disconnessione dell'utente e quindi all'accesso a Grid Manager.

## Eliminazione di un account utente locale

È possibile eliminare gli account degli utenti locali che non richiedono più l'accesso a Grid Manager.

### Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Selezionare l'utente locale che si desidera eliminare.



Non è possibile eliminare l'utente locale root predefinito.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Rimuovi**.
4. Fare clic su **OK**.

## Modifica della password di un utente locale

Gli utenti locali possono modificare le proprie password utilizzando l'opzione **Change Password** (Modifica password) nel banner Grid Manager. Inoltre, gli utenti che hanno accesso alla pagina Admin Users possono modificare le password per altri utenti locali.

## A proposito di questa attività

È possibile modificare le password solo per gli utenti locali. Gli utenti federati devono modificare le proprie password nell'origine dell'identità esterna.

### Fasi

1. Selezionare **Configuration Access Control Admin Users**.
2. Nella pagina utenti, selezionare l'utente.

Se il sistema include più di 20 elementi, è possibile specificare quante righe vengono visualizzate su ogni pagina contemporaneamente. È quindi possibile utilizzare la funzione trova del browser per cercare un elemento specifico nelle righe attualmente visualizzate.

3. Fare clic su **Change Password** (Modifica password).
4. Immettere e confermare la password, quindi fare clic su **Save** (Salva).

## Utilizzo di SSO (Single Sign-on) per StorageGRID

Il sistema StorageGRID supporta SSO (Single Sign-on) utilizzando lo standard SAML 2.0 (Security Assertion Markup Language 2.0). Quando SSO è attivato, tutti gli utenti devono essere autenticati da un provider di identità esterno prima di poter accedere a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API. Gli utenti locali non possono accedere a StorageGRID.

- ["Come funziona il single sign-on"](#)
- ["Requisiti per l'utilizzo del single sign-on"](#)
- ["Configurazione del single sign-on"](#)

### Come funziona il single sign-on

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.

#### 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 si accede per la prima volta all'URL del browser, viene richiesto di inserire un ID account:

- Se in precedenza hai effettuato l'accesso a Grid Manager o al Tenant Manager, ti verrà richiesto di selezionare un account recente o di inserire un ID account:



La pagina di accesso a StorageGRID non viene visualizzata quando si inserisce l'URL completo di un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da) `?accountId=20-digit-account-id`). Al contrario, si viene immediatamente reindirizzati alla pagina di accesso SSO dell'organizzazione, dove 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 **account ID**, 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. Fare clic su **Accedi**

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

Sign in with your organizational account

4. Accedi con le tue credenziali SSO.

Se le credenziali SSO sono corrette:

- a. Il provider di identità (IdP) fornisce una risposta di autenticazione a StorageGRID.
- b. StorageGRID convalida la risposta di autenticazione.
- c. Se la risposta è valida e l'utente appartiene a un gruppo federated con un'autorizzazione di accesso adeguata, l'utente ha effettuato l'accesso a Grid Manager o al tenant Manager, a seconda dell'account selezionato.

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

Non è necessario immettere nuovamente le credenziali SSO.

### Disconnessione quando SSO è attivato

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

#### Fasi

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

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
Tenant Manager su uno o più nodi di amministrazione	Tenant Manager su qualsiasi nodo di amministrazione	Tenant Manager su tutti i nodi di amministrazione

Se hai effettuato l'accesso a...	E ti disconnetterai da...	Sei disconnesso da...
Sia Grid Manager che tenant Manager	Grid Manager	Solo Grid Manager. Per disconnettersi da SSO, devi anche disconnetterti da Tenant Manager.



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.

## Requisiti per l'utilizzo del single sign-on

Prima di attivare il Single Sign-on (SSO) per un sistema StorageGRID, esaminare i requisiti di questa sezione.



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).

## Requisiti del provider di identità

Il provider di identità (IdP) per SSO deve soddisfare i seguenti requisiti:

- Una delle seguenti versioni di Active Directory Federation Service (ad FS):
  - AD FS 4.0, incluso in Windows Server 2016



Windows Server 2016 dovrebbe utilizzare "[Aggiornamento KB3201845](#)", o superiore.

- AD FS 3.0, incluso nell'aggiornamento di Windows Server 2012 R2 o superiore.
- Transport Layer Security (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versione 3.5.1 o successiva

## Requisiti dei certificati del server

StorageGRID utilizza un certificato del server di interfaccia di gestione su ciascun nodo di amministrazione per garantire l'accesso al gestore di griglia, al gestore del tenant, all'API di gestione del grid e all'API di gestione del tenant. Quando si configurano i trust delle parti di supporto SSO per StorageGRID in ad FS, il certificato del server viene utilizzato come certificato di firma per le richieste StorageGRID ad FS.

Se non è già stato installato un certificato server personalizzato per l'interfaccia di gestione, è necessario farlo ora. Quando si installa un certificato server personalizzato, viene utilizzato per tutti i nodi di amministrazione ed è possibile utilizzarlo in tutti i trust di StorageGRID.



Si sconsiglia di utilizzare il certificato server predefinito di un nodo di amministrazione nell'attendibilità della parte di base di ad FS. 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 in ad FS con il nuovo certificato.

È possibile accedere al certificato del server di un nodo amministratore accedendo alla shell dei comandi del nodo e accedendo a `/var/local/mgmt-api` directory. Viene assegnato un nome a un certificato server personalizzato `custom-server.crt`. Il certificato server predefinito del nodo viene denominato `server.crt`.

### Informazioni correlate

["Controllo dell'accesso tramite firewall"](#)

["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#)

## Configurazione del single sign-on

Quando è attivato il 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 utilizzando il processo di accesso SSO implementato dall'organizzazione.

- ["Conferma che gli utenti federati possono effettuare l'accesso"](#)
- ["Utilizzo della modalità sandbox"](#)
- ["Creazione di trust per la parte di base in ad FS"](#)
- ["Verifica dei trust della parte di base"](#)
- ["Abilitazione del single sign-on"](#)
- ["Disattivazione del single sign-on"](#)
- ["Disattivare e riabilitare temporaneamente il Single Sign-on per un nodo di amministrazione"](#)

### Conferma che gli utenti federati possono effettuare l'accesso

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.

#### Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Si utilizza Active Directory come origine dell'identità federata e ad FS come provider di identità.

["Requisiti per l'utilizzo del single sign-on"](#)

#### 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 **Access Control Identity Federation**.
  - c. Verificare che la casella di controllo **Enable Identity Federation** (Abilita federazione identità) non sia selezionata.
  - d. In tal caso, verificare che i gruppi federated che potrebbero essere in uso per questo account tenant non siano più necessari, deselegionare la casella di controllo e fare clic su **Salva**.
2. Verificare che un utente federated possa accedere a Grid Manager:
    - a. Da Grid Manager, selezionare **Configuration Access Control Admin Groups**.
    - b. Assicursi 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 federato che dispone dell'autorizzazione di accesso root possa effettuare l'accesso:
    - a. In Grid Manager, selezionare **tenant**.
    - b. Selezionare l'account tenant e fare clic su **Edit account** (Modifica account).
    - c. Se la casella di controllo **utilizza origine identità** è selezionata, deselegionare la casella e fare clic su **Salva**.

**Edit Tenant Account**

Tenant Details

Display Name

**Uses Own Identity Source**

Allow Platform Services

Storage Quota (optional)  **GB** ▼

Cancel Save

Viene visualizzata la pagina account tenant.

- a. Selezionare l'account tenant, fare clic su **Accedi** e accedere all'account tenant come utente root locale.
- b. Da Tenant Manager, fare clic su **Access Control Groups**.
- c. Assicursi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di accesso root per questo tenant.
- d. Disconnettersi.
- e. Confermare che è possibile accedere nuovamente al tenant come utente nel gruppo federated.

#### Informazioni correlate

["Requisiti per l'utilizzo del single sign-on"](#)

"Gestione dei gruppi di amministratori"

"Utilizzare un account tenant"

### Utilizzo della modalità sandbox

È possibile utilizzare la modalità sandbox per configurare e testare i trust delle parti di base di Active Directory Federation Services (ad FS) prima di applicare il single sign-on (SSO) per gli utenti StorageGRID. Una volta attivato SSO, è possibile riabilitare la modalità sandbox per configurare o testare i trust delle parti di base nuove ed esistenti. La riattivazione della modalità sandbox disattiva temporaneamente SSO per gli utenti StorageGRID.

#### Di cosa hai bisogno

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

#### 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 ad FS. A sua volta, ad FS invia una risposta di autenticazione a StorageGRID, indicando se la richiesta di autorizzazione ha avuto esito positivo. Per le richieste riuscite, la risposta include un UUID (Universally Unique Identifier) per l'utente.

Per consentire a StorageGRID (il provider di servizi) e ad FS (il provider di identità) di comunicare in modo sicuro sulle richieste di autenticazione dell'utente, è necessario configurare alcune impostazioni in StorageGRID. Quindi, è necessario utilizzare ad FS per creare un trust per la parte di base per ogni nodo di amministrazione. Infine, è necessario tornare a StorageGRID per attivare SSO.

La modalità sandbox semplifica l'esecuzione di questa configurazione e il test di tutte le impostazioni prima di attivare SSO.



L'utilizzo della modalità sandbox è altamente consigliato, ma non strettamente necessario. Se si è pronti a creare trust di ad FS contando subito dopo aver configurato SSO in StorageGRID, inoltre, non è necessario testare i processi SSO e di logout singolo (SLO) per ciascun nodo di amministrazione, fare clic su **Enabled**, immettere le impostazioni StorageGRID, creare un trust per ciascun nodo di amministrazione in ad FS, quindi fare clic su **Save** per attivare SSO.

#### Fasi

1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo), con l'opzione **Disabled** (Disattivato) selezionata.

## Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

Save



Se le opzioni di stato SSO non vengono visualizzate, verificare di aver configurato Active Directory come origine dell'identità federata. Consulta "requisiti per l'utilizzo del Single Sign-on".

### 2. Selezionare l'opzione **Sandbox Mode**.

Vengono visualizzate le impostazioni del provider di identità e della parte che si basa. Nella sezione Identity Provider, il campo **Service Type** è di sola lettura. Mostra il tipo di servizio di federazione delle identità in uso (ad esempio, Active Directory).

### 3. Nella sezione Identity Provider:

- a. Inserire il nome del servizio Federation, esattamente come appare in ad FS.



Per individuare il nome del servizio Federation, 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.

- b. Specificare se si desidera utilizzare TLS (Transport Layer Security) 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 e incollare il certificato nella casella di testo **certificato CA**.

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

### 4. Nella sezione parte che si basa, specificare l'identificativo della parte che si desidera utilizzare per i nodi di amministrazione StorageGRID quando si configurano i trust della parte che si basa.

- Ad esempio, se la griglia dispone di un solo nodo di amministrazione e non si prevede di aggiungere altri nodi di amministrazione in futuro, immettere `SG` oppure `StorageGRID`.
- Se la griglia include più di un nodo di amministrazione, includere la stringa `[HOSTNAME]` nell'identificatore. Ad esempio, `SG-[HOSTNAME]`. In questo modo viene generata una tabella che include un identificativo di parte di base per ciascun nodo di amministrazione, in base al nome host del nodo. + **NOTA:** È necessario creare un trust per ciascun nodo amministrativo 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.

## 5. Fare clic su **Save** (Salva).

- Sul pulsante **Save** viene visualizzato un segno di spunta verde per alcuni secondi.



- Viene visualizzato il messaggio di conferma della modalità Sandbox, che conferma l'attivazione della modalità sandbox. È possibile utilizzare questa modalità mentre si utilizza ad FS per configurare un trust di parte per ciascun nodo di amministrazione e testare i processi di accesso singolo (SSO) e di logout singolo (SLO).

### Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status    Disabled    Sandbox Mode    Enabled

#### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

### Informazioni correlate

["Requisiti per l'utilizzo del single sign-on"](#)

### Creazione di trust per la parte di base in ad FS

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

### Creazione di un trust di parte che si basa utilizzando Windows PowerShell

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

### Di cosa hai bisogno

- L'SSO è stato configurato in StorageGRID e si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo amministratore del sistema.



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.

### A proposito di questa attività

Queste istruzioni si applicano ad FS 4.0, incluso in Windows Server 2016. Se si utilizza ad FS 3.0, incluso in Windows 2012 R2, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

### Fasi

1. Dal menu Start di Windows, fare clic con il pulsante destro del mouse sull'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'identificativo della parte di base 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, 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 di base**.

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

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

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

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

- a. Individuare la fiducia della parte di base appena creata.
- b. Fare clic con il pulsante destro del mouse sull'attendibilità e selezionare **Edit claim issuance policy** (Modifica policy di emissione richiesta di rimborso).
- c. Fare clic su **Aggiungi regola**.
- d. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes**

**as Claims** (Invia attributi LDAP come richieste) dall'elenco e fare clic su **Next** (Avanti).

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

Ad esempio, da **objectGUID a ID nome**.

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

g. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.

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. Fare clic su **fine**, quindi su **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 o semplicemente 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. "[verificare tutti i trust delle parti di base](#)" per confermare che sono configurati correttamente.

### Creazione di un trust per la parte che si basa importando metadati di federazione

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

### Di cosa hai bisogno

- L'SSO è stato configurato in StorageGRID e si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo amministratore del sistema.



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.

### A proposito di questa attività

Queste istruzioni si applicano ad FS 4.0, incluso in Windows Server 2016. Se si utilizza ad FS 3.0, incluso in Windows 2012 R2, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

### Fasi

1. In Gestione server Windows, fare clic su **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, fare clic su **Aggiungi fiducia parte di base**.

3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e fare clic su **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 di amministrazione. (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. Fare clic su **Aggiungi regola**:
  - c. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste) dall'elenco e fare clic su **Next** (Avanti).
  - d. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.  
  
Ad esempio, da **objectGUID a ID nome**.
  - e. Per l'archivio attributi, selezionare **Active Directory**.
  - f. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.
  - 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. Fare clic su **fine**, quindi su **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 o semplicemente 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 **"verificare tutti i trust delle parti di base"** per confermare che sono configurati correttamente.

## Creazione manuale di 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.

### Di cosa hai bisogno

- L'SSO è stato configurato in StorageGRID e si conoscono il nome di dominio completo (o l'indirizzo IP) e l'identificativo della parte di base per ciascun nodo amministratore del sistema.



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 del certificato personalizzato caricato per l'interfaccia di gestione di StorageGRID oppure si sa come accedere a un nodo amministratore dalla shell dei comandi.
- 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.

### A proposito di questa attività

Queste istruzioni si applicano ad FS 4.0, incluso in Windows Server 2016. Se si utilizza ad FS 3.0, incluso in Windows 2012 R2, si noteranno lievi differenze nella procedura. In caso di domande, consultare la documentazione di Microsoft ad FS.

### Fasi

1. In Gestione server Windows, fare clic su **Strumenti**, quindi selezionare **Gestione di ad FS**.
2. In azioni, fare clic su **Aggiungi fiducia parte di base**.
3. Nella pagina di benvenuto, scegliere **Richieste di rimborso** e fare clic su **Avvia**.
4. Selezionare **inserire manualmente i dati relativi alla parte di base** e fare clic su **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 di amministrazione. (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'identificativo della parte di base per il nodo di amministrazione, esattamente come appare 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, fare clic su **Add Rule**:
  - a. Nella pagina Select Rule Template (Seleziona modello di regola), selezionare **Send LDAP Attributes as Claims** (Invia attributi LDAP come richieste) dall'elenco e fare clic su **Next** (Avanti).
  - b. Nella pagina Configure Rule (Configura regola), immettere un nome da visualizzare per questa regola.  
  
Ad esempio, da **objectGUID a ID nome**.
  - c. Per l'archivio attributi, selezionare **Active Directory**.
  - d. Nella colonna LDAP Attribute della tabella Mapping, digitare **objectGUID**.
  - 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. Fare clic su **fine**, quindi su **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. Fare clic su **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 di amministrazione. (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. Fare clic su **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 di amministrazione, quindi passare a `/var/local/mgmt-api` Della directory Admin Node e aggiungere `custom-server.crt` file di certificato.

**Nota:** utilizzando il certificato predefinito del nodo di amministrazione (`server.crt`) non è consigliato. 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. Fare clic su **Apply** (Applica), quindi su **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 "[verificare tutti i trust delle parti di base](#)" per confermare che sono configurati correttamente.

### Verifica dei trust della parte di base

Prima di imporre l'utilizzo del Single Sign-on (SSO) per StorageGRID, verificare che il Single Sign-on e il Single Logout (SLO) siano configurati correttamente. Se è stata creata un'attendibilità per ciascun nodo di amministrazione, confermare che è possibile utilizzare SSO e SLO per ciascun nodo di amministrazione.

#### Di cosa hai bisogno

- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario disporre di autorizzazioni di accesso specifiche.
- Sono stati configurati uno o più trust di parti di supporto in ad FS.

#### Fasi

1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo), con l'opzione **Sandbox Mode** (modalità sandbox) selezionata.

2. Nelle istruzioni per la modalità sandbox, individuare il collegamento alla pagina di accesso del provider di identità.

L'URL deriva dal valore immesso nel campo **Federated Service Name**.

#### Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

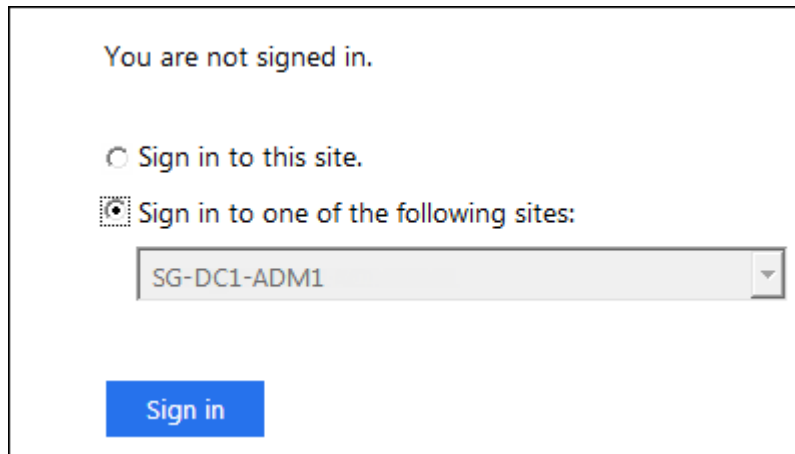
1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. Fare clic sul collegamento oppure copiare e incollare l'URL in un browser per accedere alla pagina di

accesso del provider di identità.

4. 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 fare clic su **Accedi**.



The screenshot shows a login page with the text "You are not signed in." at the top. Below it are two radio button options: "Sign in to this site." (which is unselected) and "Sign in to one of the following sites:" (which is selected). Under the second option is a dropdown menu with "SG-DC1-ADM1" selected. At the bottom left is a blue "Sign in" button.

Viene richiesto di inserire il nome utente e la password.

5. 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.

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

- Se l'operazione SSO non riesce, viene visualizzato un messaggio di errore. Risolvere il problema, eliminare i cookie del browser e riprovare.
6. Ripetere i passaggi precedenti per confermare che è possibile accedere a qualsiasi altro nodo Admin.

Se tutte le operazioni di accesso e disconnessione SSO hanno esito positivo, è possibile attivare SSO.

### Abilitazione del single sign-on

Dopo aver utilizzato la modalità sandbox per testare tutti i trust di StorageGRID, sei pronto per attivare il single sign-on (SSO).

#### Di cosa hai bisogno

- È necessario aver importato almeno un gruppo federated dall'origine dell'identità e aver assegnato al gruppo le autorizzazioni di gestione di accesso root. È necessario confermare che almeno un utente federato disponga dell'autorizzazione di accesso root per Grid Manager e per il tenant Manager per gli account tenant esistenti.
- È necessario aver testato tutti i trust delle parti di base utilizzando la modalità sandbox.

#### Fasi

1. Selezionare **Configuration Access Control Single Sign-on**.

Viene visualizzata la pagina Single Sign-on (accesso singolo) con l'opzione **Sandbox Mode** (modalità sandbox) selezionata.

2. Impostare lo stato SSO su **Enabled**.
3. Fare clic su **Save** (Salva).

Viene visualizzato un messaggio di avviso.

### Warning

#### Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Esaminare l'avviso e fare clic su **OK**.

Il Single Sign-on è ora 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.

### Disattivazione del single sign-on

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.

#### Di cosa hai bisogno

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

#### Fasi

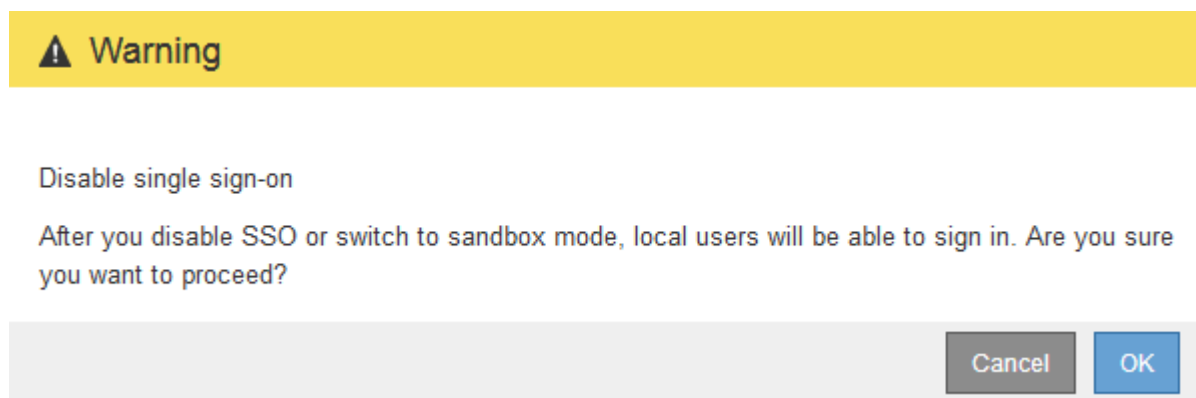
1. Selezionare **Configuration Access Control Single Sign-on**.

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

2. Selezionare l'opzione **Disabled**.

3. Fare clic su **Save** (Salva).

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



4. Fare clic su **OK**.

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.

### Disattivare e riabilitare temporaneamente il Single Sign-on 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.

#### Di cosa hai bisogno

- È necessario disporre di autorizzazioni di accesso specifiche.
- È necessario disporre di `Passwords.txt` file.
- È necessario conoscere 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 in `Passwords.txt` file.
  - c. Immettere il seguente comando per passare a root: `su -`

d. Immettere la password elencata in `Passwords.txt` file.

Una volta effettuato l'accesso 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 **Configuration Access Control Single Sign-on**.

b. Modificare le impostazioni SSO non corrette o non aggiornate.

c. Fare clic su **Save** (Salva).

Facendo clic su **Save** (Salva) dalla pagina Single Sign-on (accesso singolo), viene riattivata automaticamente l'SSO 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. Fare clic su **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 Grid: `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 correlate

["Configurazione del single sign-on"](#)

# Configurazione dei certificati client dell'amministratore

È possibile utilizzare i certificati client per consentire ai client esterni autorizzati di accedere al database StorageGRID Prometheus. I certificati client offrono un metodo sicuro per utilizzare strumenti esterni per monitorare StorageGRID.

Se si desidera accedere a StorageGRID utilizzando uno strumento di monitoraggio esterno, è necessario caricare o generare un certificato client utilizzando Grid Manager e copiare le informazioni del certificato nello strumento esterno.

## Aggiunta di certificati client amministratore

Per aggiungere un certificato client, è possibile fornire il proprio certificato o generarne uno utilizzando Grid Manager.

### Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario conoscere l'indirizzo IP o il nome di dominio del nodo di amministrazione.
- È necessario aver configurato il certificato del server dell'interfaccia di gestione StorageGRID e disporre del bundle CA corrispondente
- Se si desidera caricare il proprio certificato, la chiave pubblica e la chiave privata del certificato devono essere disponibili sul computer locale.

### Fasi

1. In Grid Manager, selezionare **Configuration Access Control Client Certificates**.

Viene visualizzata la pagina certificati client.

#### Client Certificates

You can upload or generate one or more client certificates to allow StorageGRID to authenticate external client access.


<b>+ Add</b> <b>Edit</b> <b>Remove</b>		
Name	Allow Prometheus	Expiration Date
<i>No client certificates configured.</i>		

2. Selezionare **Aggiungi**.

Viene visualizzata la pagina carica certificato.

## Upload Certificate

Name 

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Cancel

Save


3. Digitare un nome compreso tra 1 e 32 caratteri per il certificato.
4. Per accedere alle metriche Prometheus utilizzando lo strumento di monitoraggio esterno, selezionare la casella di controllo **Consenti Prometheus**.
5. Caricare o generare un certificato:
  - a. Per caricare un certificato, vai su [qui](#).
  - b. Per generare un certificato, andare [qui](#).
6. per caricare un certificato:
  - a. Selezionare **carica certificato client**.
  - b. Cercare la chiave pubblica per il certificato.

Dopo aver caricato la chiave pubblica per il certificato, i campi **metadati del certificato** e **PEM del certificato** vengono compilati.



## Upload Certificate

Name  test-certificate-upload

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Uploaded file name: client (1).crt

Certificate metadata 

```
Subject DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Serial Number: 0D:0E:FC:16:75:B8:BE:3E:7D:47:4D:05:49:08:F3:7B:E8:4A:71:90
Issuer DN: /C=US/ST=California/L=Sunnyvale/O=Example Co./OU=IT/CN=*.s3.example.com
Issued On: 2020-06-19T22:11:56.000Z
Expires On: 2021-06-19T22:11:56.000Z
SHA-1 Fingerprint: 13:AA:D6:06:2B:90:FE:B7:7B:EB:1A:83:BE:C3:62:39:B7:A6:E7:F0
SHA-256 Fingerprint: 5C:29:06:6B:CF:81:50:B8:4F:A9:56:F7:A7:AB:3C:36:FA:3D:B7:32:A4:C9:74:85:2C:8D:E6:67:37:C3:AC:60
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIIDmzCCAoQgAwIBAgIUUDQ78FnW4vj59R00FSQjze+hKcZAwDQYJKoZIhvcNAQEL
BQAwdDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbg1mb3JuaWEuXjAQBgNVBAcM
CVN1bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDby4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMB4XDTEwMDYxOTIyMTE1N1oXDTEwMDYx
OTIyMTE1N1owDELMAkGA1UEBhMCVVMxEzARBgNVBAgMCkNhbg1mb3JuaWEuXjAQBg
NVBAcMNVN1bm55dmFzZTEUMBIGA1UECgwLRXhhbXBsZSBDby4xCzAJBgNVBAsMAk1UMRkw
FwYDQDDDBAqLnMzLmV4YW1wbGUuY29tMIIIBIjANBgkqhkiG9w0BAQEF
AAOCAQ8AMIIBCgKCAQEAzVgq2MnjvVotLeStq1Co4coJmsQ2ygrhuwSza0bgMnjf
cwUgHNVPXGuGlzY/Tl37r3Dk5bu2fyGYAeJ6mqbQA6cE3yp0p5Hx7Cm/AWJknFw6
```

Copy certificate to clipboard

Cancel


Save

- a. Selezionare **Copia certificato negli Appunti** e incollare il certificato nello strumento di monitoraggio esterno.
  - b. Utilizzare uno strumento di modifica per copiare e incollare la chiave privata nello strumento di monitoraggio esterno.
  - c. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.
7. per generare un certificato:
- a. Selezionare **generate Client Certificate** (genera certificato client).
  - b. Immettere il nome di dominio o l'indirizzo IP del nodo di amministrazione.
  - c. Facoltativamente, immettere un oggetto X.509, denominato anche nome distinto (DN), per identificare l'amministratore proprietario del certificato.
  - d. Se si desidera, selezionare il numero di giorni in cui il certificato è valido. L'impostazione predefinita è 730 giorni.
  - e. Selezionare **generate**.

I campi **metadati del certificato**, **PEM del certificato** e **chiave privata del certificato** vengono compilati.

## Upload Certificate

Name  test-certificate-generate

Allow Prometheus 

### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate

Generate Client Certificate

Certificate metadata 

```
Subject DN: /CN=test.com
Serial Number: 08:F8:FB:76:B2:13:E4:DF:54:83:3D:35:56:6F:2A:03:53:B0:E2:0
A
Issuer DN: /CN=test.com
Issued On: 2020-11-20T22:44:46.000Z
Expires On: 2022-11-20T22:44:46.000Z
SHA-1 Fingerprint: 6E:DB:8C:F8:3E:20:88:E4:C6:42:52:5F:32:7E:E7:93:66:89:F3:3
D
SHA-256 Fingerprint: 73:D3:51:83:ED:D3:89:AD:7B:89:4C:AF:AE:34:76:B6:42:FE:0D:
EF:78:C0:A4:66:C2:EB:65:64:C3:D4:7A:B0
```

Certificate PEM 

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUUCFj7dxITSN9Ugs01Vm8qA1Ow4gowDQYJKoZIhvcNAQEL
BQAwEwERMA8GA1UEAwIgdGVudC5jb20wHhcNMjA1MTIwMjI0NDQ2WzBkMTIw
MjA1MTIwMjI0NDQ2WzATMREwDwYDVQQDDAh0ZXN0LmNvbTCCASAwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAR02dS9mx2jFrGuBb22Mjcidf/tTcKxLtB9m+4vIwt1gvrR
XgHZ31B9YIqn/Vo729R2mNKKyBwkyQTkGCO2Ixxv0STBLEIWFb8S+TgcIcMyt1V1F
OseBWy402xxjnR3/X+AX+6s2WZIsVe+3CDjGu4ie0V/uVQxx4yA1T9SoKnjBmOa
LCVjL6iVnkUGB8GbkYUPeOaoMjsL6TN1QsoFv9VEB0xBKCP4D7FDbaIy2f9Ng8rS
FEOQoLN=N+XCasLO4D7j2qFqOVUpFJ3M0ohlx0n5pQ78Z5KfYwV=DKg6v52P8UBM
1o6GeuoFaW+dbpLZKp09N1V=VhghXe9AxxN8s+kCAwEAAaMXXMBUwEwYDVR0RBBAw
```

Copy certificate to clipboard

Certificate private key 

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEArT20H2bHaM+sa4Fv2kyNyJ1/+1NwzEu0Eab7i8jC2KNC/BFe
AdneUH1ghCf9Wjvb1HaY0orIHCTJBOQYI5kjG+/RjMEb4h29sRx0Bw1gzK2VWUU7
OwF2jPg7bPFOorF9f4Bf7nL1ZkixV75IICMa7iJaRX+5VDPHjIDVP1KggelMGY5oe
JWmVqJWeRQYFI2uTJQ946qgyOwvpm2VDOgW/1UQHTEEoKngPfeUNtojL2/02DmtJ8
Q8Cg=202x0JrMe7gFuNmoWo5hS8kUncw6iHXHSfm1Dvxnkp9jBw0MqDm/nY/xQEwW
jw266h9pb51ukt2k703VW0WGCfD7GDPE2yyQIDAQABaoIBAQCfEUfY4pE0Hqcv
2uEL6De4yXMTwg/3Gn+W8mvdgQB4xWEGQrk1kEUG+HTYrFJen6XX0vACDYAC/
Hh1Q67xDVpWRjdpUK0cr1W8ervzEmpBx99MqH9Y2UGw6Yub3UBJaqfDvja4Nvaon
MxaYJRFBLvAR7f2z2xXV5b0zRPA+rn0YCs1Ler5Y0K73e0G8naTmwIdm2YM6EE
```

Copy private key to clipboard

 You will not be able to view the certificate private key after you close this dialog. To save the keys for future reference, copy and paste the values to another location.

Cancel Save

- Selezionare **Copia certificato negli Appunti** e incollare il certificato nello strumento di monitoraggio esterno.
- Selezionare **Copia chiave privata negli Appunti** e incollarla nello strumento di monitoraggio esterno.



Non sarà possibile visualizzare la chiave privata dopo aver chiuso la finestra di dialogo. Copiare la chiave in un luogo sicuro.

- Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.

8. Configurare le seguenti impostazioni sullo strumento di monitoraggio esterno, ad esempio Grafana.

Un esempio di Grafana viene mostrato nella seguente schermata:

The screenshot shows the configuration page for a data source named 'sg-prometheus'. The 'Name' field is 'sg-prometheus' and the 'Default' toggle is turned on. Under the 'HTTP' section, the 'URL' is 'https://admin-node.example.com:9091', 'Access' is 'Server (default)', and 'Whitelisted Cookies' is empty. Under the 'Auth' section, 'Basic auth' is off, 'With Credentials' is off, 'TLS Client Auth' is on, 'With CA Cert' is on, 'Skip TLS Verify' is off, and 'Forward OAuth Identity' is off. Under 'TLS/SSL Auth Details', 'CA Cert' is empty, 'ServerName' is 'admin-node.example.com', and 'Client Cert' is empty. The 'CA Cert' and 'Client Cert' fields have a placeholder text 'Begins with ---BEGIN CERTIFICATE---'.

a. **Nome:** Immettere un nome per la connessione.

StorageGRID non richiede queste informazioni, ma è necessario fornire un nome per verificare la connessione.

b. **URL:** Immettere il nome di dominio o l'indirizzo IP per il nodo di amministrazione. Specificare HTTPS e

la porta 9091.

Ad esempio: `https://admin-node.example.com:9091`

- c. Abilitare **TLS Client Authorization** e **with CA Certate**.
- d. Copiare e incollare il certificato del server dell'interfaccia di gestione o il bundle CA in **CA Certificate** in TLS/SSL Auth Details (Dettagli autorizzazione TLS/SSL).
- e. **ServerName**: Immettere il nome di dominio del nodo di amministrazione.

Il nome server deve corrispondere al nome di dominio così come appare nel certificato del server dell'interfaccia di gestione.

- f. Salvare e verificare il certificato e la chiave privata copiati da StorageGRID o da un file locale.

Ora puoi accedere alle metriche Prometheus da StorageGRID con il tuo tool di monitoraggio esterno.

Per informazioni sulle metriche, consultare le istruzioni per il monitoraggio e la risoluzione dei problemi di StorageGRID.

### Informazioni correlate

["Utilizzo dei certificati di sicurezza StorageGRID"](#)

["Configurazione di un certificato server personalizzato per Grid Manager e Tenant Manager"](#)

["Monitor risoluzione dei problemi"](#)

## Modifica dei certificati client amministratore

È possibile modificare un certificato per modificarne il nome, attivare o disattivare l'accesso Prometheus o caricare un nuovo certificato quando quello corrente è scaduto.

### Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.
- È necessario conoscere l'indirizzo IP o il nome di dominio del nodo di amministrazione.
- Se si desidera caricare un nuovo certificato e una nuova chiave privata, questi devono essere disponibili sul computer locale.

### Fasi

1. Selezionare **Configurazione controllo accessi certificati client**.

Viene visualizzata la pagina certificati client. Vengono elencati i certificati esistenti.

Le date di scadenza del certificato sono elencate nella tabella. Se un certificato scade presto o è già scaduto, viene visualizzato un messaggio nella tabella e viene attivato un avviso.

	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Selezionare il pulsante di opzione a sinistra del certificato che si desidera modificare.
3. Selezionare **Modifica**.

Viene visualizzata la finestra di dialogo Modifica certificato.

### Edit Certificate test-certificate-generate

Name

Allow Prometheus

---

#### Certificate Details

Upload the public key for the client certificate.

Upload Client Certificate
Generate Client Certificate

Certificate metadata

**Subject DN:** /CN=test.com  
**Serial Number:** 0C:11:87:6C:1E:FD:13:16:F3:F2:06:D9:DA:6D:BC:CE:2A:A9:C3:53  
**Issuer DN:** /CN=test.com  
**Issued On:** 2020-11-23T15:53:33.000Z  
**Expires On:** 2022-11-23T15:53:33.000Z  
**SHA-1 Fingerprint:** AE:E6:70:A7:D3:C3:39:7A:09:F9:62:9B:81:8A:87:CD:43:16:89:A7  
**SHA-256 Fingerprint:** 63:07:BF:FF:08:1E:84:F1:D4:67:C6:16:B0:35:26:00:C6:A3:13:11:7E:5E:90:EC:7A:7B:EF:23:14:55:3D:56

Certificate PEM

```
-----BEGIN CERTIFICATE-----
MIICyzCCAbOgAwIBAgIUDBGHbB79Exbz8gbZ2m28ziqpw1MwDQYJKoZIhvcNAQEL
BQAwEzERMA8GA1UEAwIdGVzdC5jb20wHhcNMjAxMTIzMTU1MzE1LjE1LjE1LjE1
MTU1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1MzE1
ggEPADCCAQoCggEBAKdGEdeneCDFDs1jvlnX9ow6oPrdU7m2EN6SS6xdVI155sCH+
hkwO5a2Mym7EhbNrfwOt2nMjQkcaKIrk8OAmutRgG6N1N12FIW0qYQouzFQ0QddLq
n7ymFw6w8a9zYSu7bLp84Yn0/LSDPk+h3Jio7Mrt2X70It52DRwFmbLNvEvYEtTS
h+FbNh885AIRO2eLxvC0IRi1j1bySe76wK+Wmc97HdxRSgyxIWk6BD47XC+d0rv55
wvtjc/41qc5xsE6Xm7s2yJg4VARx10y8Icwa9fz00+xPwIdC0NwXkpWJXeBnCoXx
YqQxbWzjz+iVLJqLTMxU8zTIT30zUgN00M82GJUCAwEAAaMKMBUwEwYDVR0RBAAw
```

Copy certificate to clipboard

Cancel Save

4. Apportare le modifiche desiderate al certificato.
5. Selezionare **Save** (Salva) per salvare il certificato in Grid Manager.
6. Se hai caricato un nuovo certificato:
  - a. Selezionare **Copia certificato negli Appunti** per incollare il certificato nello strumento di monitoraggio esterno.
  - b. Utilizzare uno strumento di modifica per copiare e incollare la nuova chiave privata nello strumento di monitoraggio esterno.

- c. Salvare e verificare il certificato e la chiave privata nello strumento di monitoraggio esterno.
7. Se è stato generato un nuovo certificato:
- a. Selezionare **Copia certificato negli Appunti** per incollare il certificato nello strumento di monitoraggio esterno.
  - b. Selezionare **Copia chiave privata negli Appunti** per incollare il certificato nello strumento di monitoraggio esterno.



Una volta chiusa la finestra di dialogo, non sarà possibile visualizzare o copiare la chiave privata. Copiare la chiave in un luogo sicuro.

- c. Salvare e verificare il certificato e la chiave privata nello strumento di monitoraggio esterno.

## Rimozione dei certificati del client amministratore

Se non hai più bisogno di un certificato, puoi rimuoverlo.

### Di cosa hai bisogno

- È necessario disporre dell'autorizzazione di accesso root.
- È necessario accedere a Grid Manager utilizzando un browser supportato.

### Fasi

1. Selezionare **Configurazione controllo accessi certificati client**.

Viene visualizzata la pagina certificati client. Vengono elencati i certificati esistenti.

<input type="button" value="+ Add"/> <input type="button" value="✎ Edit"/> <input type="button" value="✕ Remove"/>			
	Name	Allow Prometheus	Expiration Date
<input type="radio"/>	test-certificate-upload	✓	2021-06-19 16:11:56 MDT
<input checked="" type="radio"/>	test-certificate-generate	✓	2022-08-20 09:42:00 MDT

Displaying 2 certificates.

2. Selezionare il pulsante di opzione a sinistra del certificato che si desidera rimuovere.
3. Selezionare **Rimuovi**.

Viene visualizzata una finestra di dialogo di conferma.

**⚠ Warning**

Delete certificate

Are you sure you want to delete the certificate "test-certificate-generate"?

4. Selezionare **OK**.

Il certificato viene rimosso.



## Informazioni sul copyright

Copyright © 2024 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 COMMERCIALIZZABILITÀ 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.