



Utilizzo di SSO (Single Sign-on) per StorageGRID

StorageGRID 11.5

NetApp
April 11, 2024

Sommario

- Utilizzo di SSO (Single Sign-on) per StorageGRID 1
 - Come funziona il single sign-on 1
 - Requisiti per l'utilizzo del single sign-on 3
 - Configurazione del single sign-on 4

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

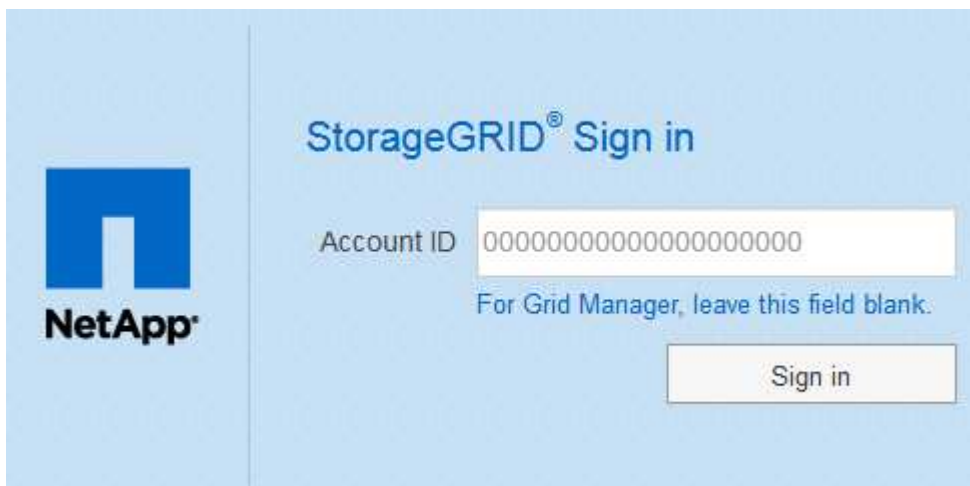
Quando SSO è attivato e si accede a StorageGRID, si viene reindirizzati alla pagina SSO dell'organizzazione per convalidare le credenziali.

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:



The image shows the StorageGRID Sign in interface. On the left is the NetApp logo. The main area has the title 'StorageGRID® Sign in'. Below the title, there is a 'Recent' dropdown menu with 'S3 tenant' selected. Underneath is the 'Account ID' field containing the value '27469746059057031822'. A note below the field says 'For Grid Manager, leave this field blank.' At the bottom right is a 'Sign in' button.



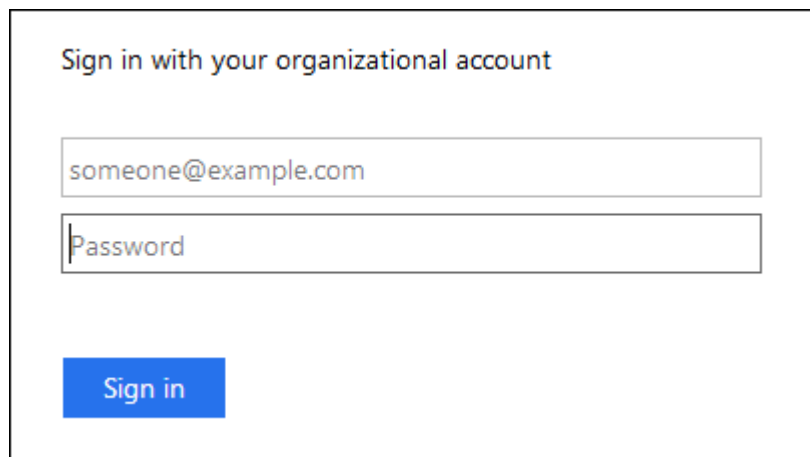
La pagina di accesso a StorageGRID non viene visualizzata quando si inserisce l'URL completo di un account tenant (ovvero un nome di dominio completo o un indirizzo IP seguito da) `/?accountId=20-digit-account-id`. Al contrario, si viene immediatamente reindirizzati alla pagina di accesso SSO dell'organizzazione,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



The image shows a 'Sign in with your organizational account' form. It has two input fields: the first contains 'someone@example.com' and the second is labeled 'Password'. Below the fields is a blue 'Sign in' button.

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
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. Assicurarsi che almeno un gruppo federated sia stato importato dall'origine dell'identità di Active Directory e che sia stata assegnata l'autorizzazione di accesso root.
 - c. Disconnettersi.
 - d. Confermare che è possibile accedere nuovamente a Grid Manager come utente nel gruppo federated.
 3. Se sono presenti account tenant, verificare che un utente 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)

Cancel

Save

Viene visualizzata la pagina account tenant.

- Selezionare l'account tenant, fare clic su **Accedi** e accedere all'account tenant come utente root locale.
- Da Tenant Manager, fare clic su **Access Control Groups**.
- Assicurarsi che almeno un gruppo federated di Grid Manager sia stato assegnato all'autorizzazione di accesso root per questo tenant.
- Disconnettersi.
- 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**.

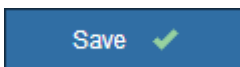
- **Non utilizzare TLS:** Non utilizzare un certificato TLS per proteggere la connessione.

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**.

You are not signed in.

Sign in to this site.

Sign in to one of the following sites:

SG-DC1-ADM1

Sign in

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.

Warning

Disable single sign-on

After you disable SSO or switch to sandbox mode, local users will be able to sign in. Are you sure you want to proceed?

Cancel

OK

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"](#)

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.