Utilisation de l'authentification unique (SSO) pour StorageGRID

StorageGRID

NetApp
October 03, 2025

Sommaire

Utilisation de l’authentification unique (SSO) pour StorageGRID

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language). Lorsque l’authentification SSO est activée, tous les utilisateurs doivent être authentifiés par un fournisseur d’identités externe avant d’accéder au Grid Manager, au tenant Manager, à l’API Grid Management ou à l’API de gestion des locataires. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

- "Fonctionnement de l’authentification unique"
- "Conditions requises pour l’utilisation de l’authentification unique"
- "Configuration de l’authentification unique"

Fonctionnement de l’authentification unique

Avant d’activer l’authentification unique (SSO), vérifiez comment les processus de connexion et de déconnexion StorageGRID sont affectés lorsque l’authentification SSO est activée.

Connexion lorsque SSO est activé

Lorsque l’authentification SSO est activée et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre entreprise afin de valider vos identifiants.

Étapes

1. Entrez le nom de domaine complet ou l’adresse IP d’un nœud d’administration StorageGRID dans un navigateur Web.

   La page de connexion StorageGRID s’affiche.

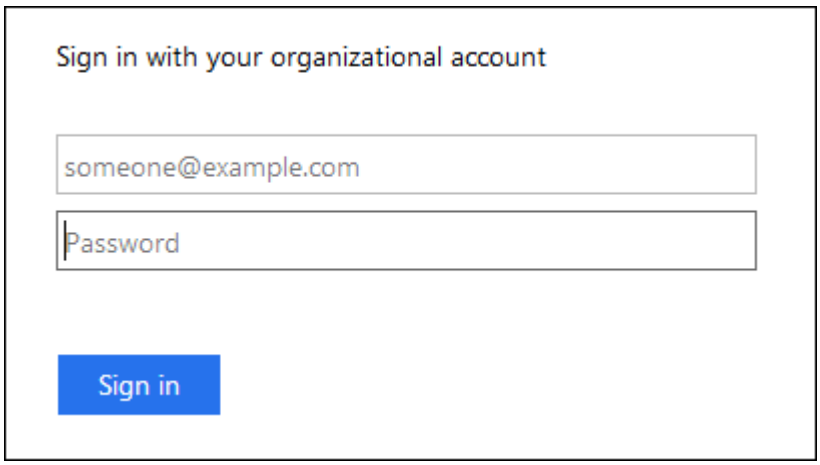
   - S’il s’agit de la première fois que vous accédez à l’URL sur ce navigateur, vous êtes invité à entrer un ID de compte :

- Si vous avez déjà accédé au Grid Manager ou au tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

> La page de connexion StorageGRID n'apparaît pas lorsque vous saisissez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivi de `/?accountId=20-digit-account-id`). Au lieu de cela, vous êtes immédiatement redirigé vers la page de connexion SSO de votre entreprise, où vous pouvez Connectez-vous à l'aide de vos identifiants SSO.

2. Indiquez si vous souhaitez accéder au Grid Manager ou au tenant Manager :
   - Pour accéder au Grid Manager, laissez le champ Identifiant de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Grid Manager** si celui-ci apparaît dans la liste des comptes récents.
   - Pour accéder au Gestionnaire de locataires, entrez l'ID de compte de tenant à 20 chiffres ou sélectionnez un locataire par nom s'il apparaît dans la liste des comptes récents.
3. Cliquez sur **connexion**

   StorageGRID vous redirige vers la page de connexion SSO de votre entreprise. Par exemple :



4. Connectez-vous à l'aide de vos identifiants SSO.

   Si vos informations d'identification SSO sont correctes :

   a. Le fournisseur d'identités fournit une réponse d'authentification à StorageGRID.

b. StorageGRID valide la réponse d'authentification.

c. Si la réponse est valide et que vous appartenez à un groupe fédéré disposant d'une autorisation d'accès adéquate, vous êtes connecté au Grid Manager ou au tenant Manager, selon le compte que vous avez sélectionné.

5. Accédez éventuellement à d'autres nœuds d'administration ou à Grid Manager ou au tenant Manager, si vous disposez des autorisations adéquates.

   Il n'est pas nécessaire de saisir à nouveau vos identifiants SSO.

Déconnexion lorsque SSO est activé

Lorsque l'authentification SSO est activée pour StorageGRID, le processus de déconnexion dépend de ce que vous êtes connecté et de l'endroit où vous vous déconnectez.

Étapes

1. Repérez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Cliquez sur **Déconnexion**.

   La page de connexion StorageGRID s'affiche. La liste déroulante **comptes récents** est mise à jour pour inclure **Grid Manager** ou le nom du locataire, afin que vous puissiez accéder plus rapidement à ces interfaces utilisateur à l'avenir.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration
Gestionnaire de locataires sur un ou plusieurs nœuds d'administration	Gestionnaire de locataires sur n'importe quel nœud d'administration	Gestionnaire de locataires sur tous les nœuds d'administration
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.

Le tableau résume ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID à travers plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Conditions requises pour l'utilisation de l'authentification unique

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises dans cette section.

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Exigences du fournisseur d'identités

Le fournisseur d'identités (IDP) pour SSO doit satisfaire aux exigences suivantes :

- L'une des versions suivantes d'Active Directory Federation Service (AD FS) :
  - AD FS 4.0, inclus dans Windows Server 2016

    Windows Server 2016 doit utiliser le "Mise à jour KB3201845", ou supérieur.

  - AD FS 3.0, inclus avec la mise à jour Windows Server 2012 R2, ou une version ultérieure.
- TLS (transport Layer Security) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Configuration requise pour le certificat de serveur

StorageGRID utilise un certificat de serveur d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès à Grid Manager, au gestionnaire de locataires, à l'API de gestion du grid et à l'API de gestion des locataires. Lorsque vous configurez les approbations de tiers basés SSO pour StorageGRID dans AD FS, vous utilisez le certificat de serveur comme certificat de signature pour les requêtes StorageGRID à AD FS.

Si vous n'avez pas encore installé de certificat de serveur personnalisé pour l'interface de gestion, vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID.

Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans la confiance de l'intervenant de confiance AD FS. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrice dans AD FS avec le nouveau certificat.

Vous pouvez accéder au certificat de serveur d'un nœud d'administration en vous connectant au shell de commande du nœud et en allant à `/var/local/mgmt-api` répertoire. Un certificat de serveur personnalisé est nommé `custom-server.crt`. Le certificat de serveur par défaut du nœud est nommé `server.crt`.

Informations associées

"Contrôle de l'accès par pare-feu"

"Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager"

Configuration de l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs n'ont accès qu'au Grid Manager, au tenant Manager, à l'API Grid Management ou à l'API de gestion des locataires si leurs identifiants sont autorisés à l'aide du processus de connexion SSO mis en œuvre par votre entreprise.

- "Confirmer que les utilisateurs fédérés peuvent se connecter"
- "Utilisation du mode sandbox"
- "Création de fiducies de tiers de confiance dans AD FS"
- "Confiance de la partie qui fait confiance aux essais"
- "Activation de l'authentification unique"
- "Désactivation de la connexion unique"
- "Désactivation et réactivation temporaire de l'authentification unique pour un nœud d'administration"

Confirmer que les utilisateurs fédérés peuvent se connecter

Avant d'activer l'authentification unique (SSO), vous devez confirmer qu'au moins un utilisateur fédéré peut se connecter au Grid Manager et au tenant Manager pour tout compte de tenant existant.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous utilisez Active Directory en tant que source d'identité fédérée et AD FS en tant que fournisseur d'identité.

  "Conditions requises pour l'utilisation de l'authentification unique"

Étapes

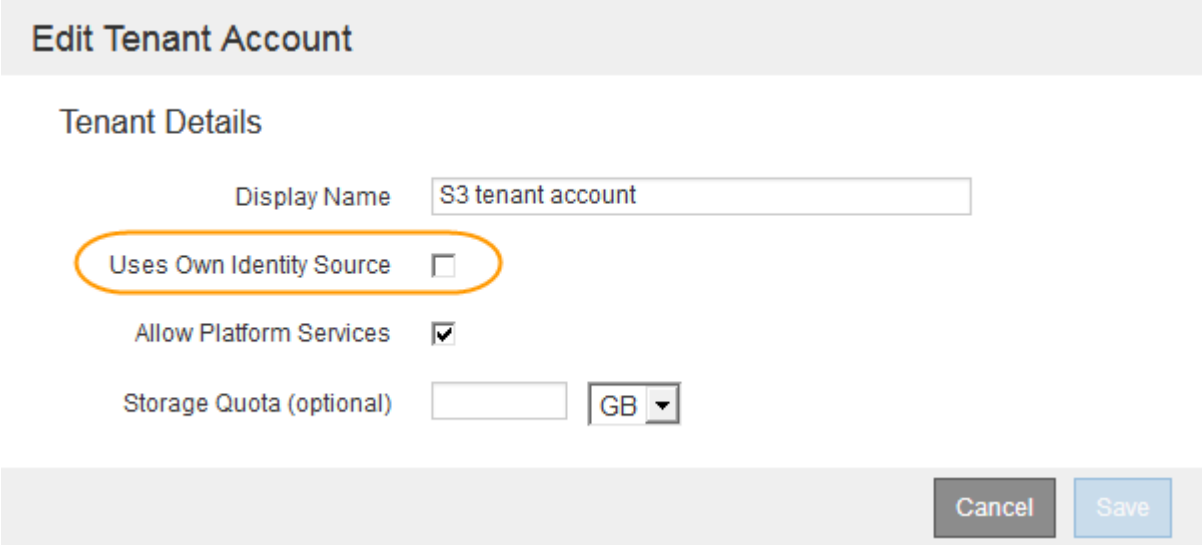
1. S'il existe des comptes de tenant existants, vérifiez qu'aucun des locataires n'utilise son propre référentiel d'identité.

   > Lorsque vous activez SSO, un référentiel d'identité configuré dans le Gestionnaire de locataires est remplacé par le référentiel d'identité configuré dans le Gestionnaire de grille. Les utilisateurs appartenant au référentiel d'identité du locataire ne pourront plus se connecter à moins qu'ils aient un compte avec le référentiel d'identité Grid Manager.

   a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
   b. Sélectionnez **contrôle d'accès** > **fédération d'identités**.
   c. Vérifiez que la case à cocher **Activer la fédération d'identités** n'est pas cochée.
   d. Si c'est le cas, vérifiez que les groupes fédérés qui pourraient être utilisés pour ce compte de locataire ne sont plus nécessaires, désélectionnez la case à cocher et cliquez sur **Enregistrer**.
2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
   a. Dans Grid Manager, sélectionnez **Configuration** > **contrôle d'accès** > **groupes d'administration**.
   b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation accès racine.
   c. Se déconnecter.
   d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
3. S'il existe déjà des comptes de tenant, confirmez qu'un utilisateur fédéré disposant d'une autorisation

accès racine peut se connecter :

a. Dans Grid Manager, sélectionnez **tenants**.
b. Sélectionnez le compte de tenant, puis cliquez sur **Modifier le compte**.
c. Si la case **utilise son propre référentiel d'identité** est cochée, décochez la case et cliquez sur **Enregistrer**.



La page comptes de tenant s'affiche.

a. Sélectionnez le compte de tenant, cliquez sur **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.
b. Dans le Gestionnaire de locataires, cliquez sur **contrôle d'accès** > **groupes**.
c. Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation accès racine pour ce locataire.
d. Se déconnecter.
e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur dans le groupe fédéré.

Informations associées

"Conditions requises pour l'utilisation de l'authentification unique"

"Gestion des groupes d'administration"

"Utilisez un compte de locataire"

Utilisation du mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester les approbations de parties utilisatrices Active Directory Federation Services (AD FS) avant d'appliquer l'authentification unique (SSO) pour les utilisateurs StorageGRID. Une fois l'authentification SSO activée, vous pouvez réactiver le mode sandbox pour configurer ou tester les approbations nouvelles et existantes. La réactivation du mode sandbox désactive temporairement l'authentification SSO pour les utilisateurs StorageGRID.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

Description de la tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification à AD FS. À son tour, AD FS renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'autorisation a réussi. Pour les requêtes réussies, la réponse inclut un identificateur unique universel (UUID) pour l'utilisateur.

Pour permettre à StorageGRID (le fournisseur de services) et à AD FS (le fournisseur d'identité) de communiquer en toute sécurité au sujet des demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser AD FS pour créer une confiance de partie de confiance pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer le SSO.

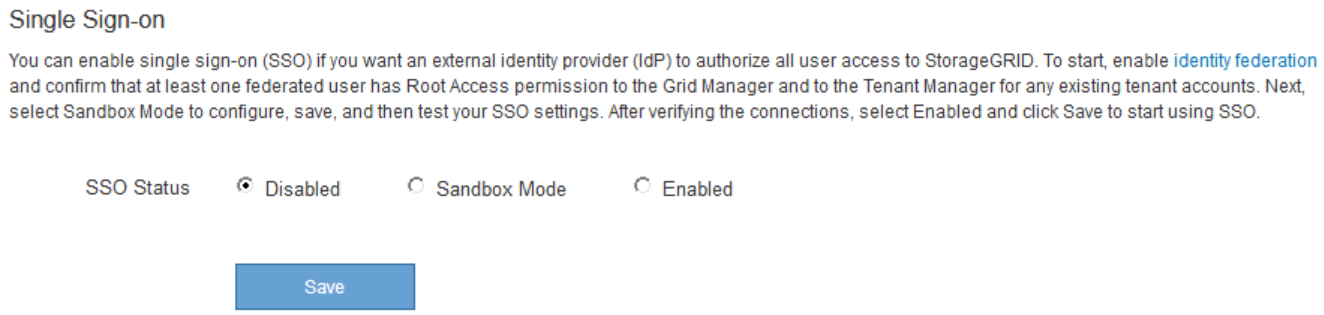
Le mode sandbox facilite l'exécution de cette configuration et le test de tous vos paramètres avant l'activation de SSO.

> L'utilisation du mode sandbox est fortement recommandée, mais pas strictement nécessaire. Si vous êtes prêt à créer des approbations de tiers AD FS immédiatement après avoir configuré SSO dans StorageGRID, Vous n'avez pas besoin de tester les processus SSO et SLO (Single logout) pour chaque noeud d'administration, cliquez sur **Enabled**, saisissez les paramètres StorageGRID, créez une confiance de partie de confiance pour chaque noeud d'administration dans AD FS, puis cliquez sur **Save** pour activer SSO.

Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **connexion unique**.

   La page connexion unique s'affiche, avec l'option **Disabled** sélectionnée.



> Si les options d'état SSO ne s'affichent pas, confirmez que vous avez configuré Active Directory en tant que référentiel d'identité fédéré. Voir « exigences relatives à l'utilisation d'un seul signe ».

2. Sélectionnez l'option **Sandbox mode**.

   Les paramètres fournisseur d'identité et partie de confiance s'affichent. Dans la section Identity Provider, le champ **Service Type** est en lecture seule. Elle indique le type de service de fédération d'identités que vous utilisez (par exemple, Active Directory).

3. Dans la section Identity Provider :

   a. Entrez le nom du service de fédération, exactement tel qu'il apparaît dans AD FS.

Pour localiser le nom du service de fédération, accédez à Windows Server Manager. Sélectionnez **Outils** > **AD FS Management**. Dans le menu action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est indiqué dans le second champ.

b. Indiquez si vous souhaitez utiliser TLS (transport Layer Security) pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes StorageGRID.

   - **Utilisez le certificat CA du système d'exploitation** : utilisez le certificat CA par défaut installé sur le système d'exploitation pour sécuriser la connexion.
   - **Utilisez un certificat d'autorité de certification personnalisé** : utilisez un certificat d'autorité de certification personnalisé pour sécuriser la connexion.

     Si vous sélectionnez ce paramètre, copiez et collez le certificat dans la zone de texte **certificat CA**.

   - **N'utilisez pas TLS**: N'utilisez pas de certificat TLS pour sécuriser la connexion.

4. Dans la section partie utilisatrice, spécifiez l'identifiant de partie utilisatrice que vous utiliserez pour les nœuds Admin StorageGRID lorsque vous configurez des approbations de partie utilisatrice.

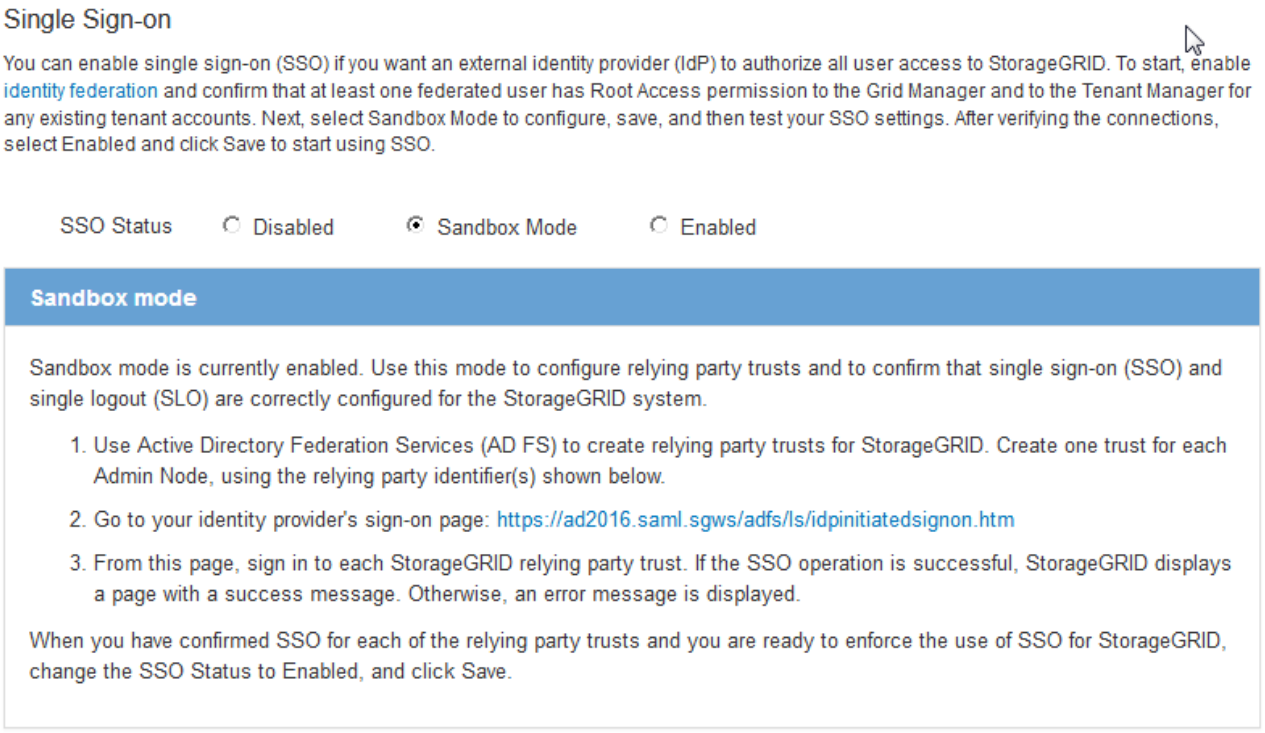
   - Par exemple, si votre grid ne comporte qu'un seul nœud d'administration et que vous n'prévoyez pas d'ajouter de nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID`.
   - Si votre grid inclut plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identificateur. Par exemple : `SG-[HOSTNAME]`. Cela génère une table qui inclut un identifiant de partie de confiance pour chaque nœud d'administration, en fonction du nom d'hôte du nœud. + REMARQUE : vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

5. Cliquez sur **Enregistrer**.

   - Une coche verte apparaît sur le bouton **Save** pendant quelques secondes.

   - L'avis de confirmation du mode Sandbox s'affiche, confirmant que le mode sandbox est à présent activé. Vous pouvez utiliser ce mode pendant que vous utilisez AD FS pour configurer une confiance de tiers de confiance pour chaque nœud d'administration et tester les processus d'ouverture de session unique (SSO) et de déconnexion unique (SLO).



Informations associées

"Conditions requises pour l'utilisation de l'authentification unique"

Création de fiducies de tiers de confiance dans AD FS

Vous devez utiliser Active Directory Federation Services (AD FS) pour créer une confiance de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations tierces via les commandes PowerShell, en important les métadonnées SAML depuis StorageGRID ou en saisissant manuellement les données.

Création d'une confiance de confiance avec Windows PowerShell

Vous pouvez utiliser Windows PowerShell pour créer rapidement une ou plusieurs approbations de parties qui font confiance.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque noeud d'administration de votre système.

> Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.

- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le menu Démarrer de Windows, cliquez avec le bouton droit de la souris sur l'icône PowerShell et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commande PowerShell, saisissez la commande suivante :

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

   - Pour *Admin_Node_Identifier*, Entrez l'identifiant de partie de confiance du noeud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : `SG-DC1-ADM1`.
   - Pour *Admin_Node_FQDN*, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **AD FS Management**.

   L'outil de gestion AD FS s'affiche.
4. Sélectionnez **AD FS** > **confiance de la partie de confiance**.

   La liste des fiducies de tiers de confiance s'affiche.
5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :
   a. Recherchez la confiance de la partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
   c. Sélectionnez une stratégie de contrôle d'accès.
   d. Cliquez sur **appliquer**, puis sur **OK**
6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiducie de compte comptant :
   a. Recherchez la confiance de la partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
   c. Cliquez sur **Ajouter règle**.
   d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.
   e. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **objectGUID to Name ID**.

f. Pour le magasin d'attributs, sélectionnez **Active Directory**.

g. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.

h. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

i. Cliquez sur **Terminer**, puis sur **OK**.

7. Confirmez que les métadonnées ont été importées avec succès.

   a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.

   b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la fédération est correcte ou entrez simplement les valeurs manuellement.

8. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.

9. Lorsque vous avez terminé, revenez à StorageGRID et "tester toutes les fiducies de la partie qui repose" pour confirmer qu'ils sont correctement configurés.

Création d'une confiance de tiers de confiance en important des métadonnées de fédération

Vous pouvez importer les valeurs de chaque confiance de fournisseur en accédant aux métadonnées SAML de chaque nœud d'administration.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque noeud d'administration de votre système.

> Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le Gestionnaire de serveur Windows, cliquez sur **Outils**, puis sélectionnez **AD FS Management**.
2. Sous actions, cliquez sur **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware**, puis cliquez sur **Démarrer**.
4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un**

réseau local.

5. Dans **adresse de métadonnées de fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce noeud d'administration :

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

   Pour *`Admin_Node_FQDN`*, Entrez le nom de domaine complet du même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

6. Terminez l'assistant confiance de la partie de confiance, enregistrez la confiance de la partie de confiance et fermez l'assistant.

   Lors de la saisie du nom d'affichage, utilisez l'identificateur de partie comptant pour le noeud d'administration, exactement comme il apparaît sur la page d'ouverture de session unique dans le Gestionnaire de grille. Par exemple : `SG-DC1-ADM1`.

7. Ajouter une règle de sinistre :
   a. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
   b. Cliquez sur **Ajouter règle** :
   c. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.
   d. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **objectGUID to Name ID**.

   e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   f. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
   g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
   h. Cliquez sur **Terminer**, puis sur **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
   b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la fédération est correcte ou entrez simplement les valeurs manuellement.

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
10. Lorsque vous avez terminé, revenez à StorageGRID et "tester toutes les fiducies de la partie qui repose" pour confirmer qu'ils sont correctement configurés.

Création manuelle d'une confiance de partie de confiance

Si vous choisissez de ne pas importer les données pour les approbations de pièces de confiance, vous pouvez entrer les valeurs manuellement.

Ce dont vous avez besoin

- Vous avez configuré l'authentification unique dans StorageGRID et vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de partie utilisatrice pour chaque noeud d'administration de votre système.

> Vous devez créer une confiance en tiers pour chaque nœud d'administration de votre système StorageGRID. Le fait d'avoir une confiance de partie de confiance pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- Vous disposez du certificat personnalisé chargé pour l'interface de gestion StorageGRID, ou vous savez comment vous connecter à un nœud d'administration à partir du shell de commande.
- Vous avez l'expérience de créer des approbations de tiers de confiance dans AD FS, ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable AD FS Management et vous appartenez au groupe administrateurs.

Description de la tâche

Ces instructions s'appliquent à AD FS 4.0, qui est inclus dans Windows Server 2016. Si vous utilisez AD FS 3.0, qui est inclus dans Windows 2012 R2, vous remarquerez de légères différences dans la procédure. Pour toute question, consultez la documentation Microsoft AD FS.

Étapes

1. Dans le Gestionnaire de serveur Windows, cliquez sur **Outils**, puis sélectionnez **AD FS Management**.
2. Sous actions, cliquez sur **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware**, puis cliquez sur **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement**, puis cliquez sur **Suivant**.
5. Suivez l'assistant confiance de la partie de confiance :

   a. Entrez un nom d'affichage pour ce nœud d'administration.

      Pour plus de cohérence, utilisez l'identifiant de partie utilisatrices du nœud d'administration, exactement comme il apparaît sur la page Single Sign-On du Grid Manager. Par exemple : `SG-DC1-ADM1`.

   b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.

   c. Sur la page configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.

   d. Saisissez l'URL du noeud final du service SAML pour le noeud d'administration :

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

      Pour *`Admin_Node_FQDN`*, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une

adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

e. Sur la page configurer les identificateurs, spécifiez l'identificateur de partie de confiance pour le même noeud d'administration :

`Admin_Node_Identifier`

Pour `Admin_Node_Identifier`, Entrez l'identifiant de partie de confiance du noeud d'administration, exactement comme il apparaît sur la page Single Sign-On. Par exemple : `SG-DC1-ADM1`.

f. Vérifiez les paramètres, enregistrez la confiance de la partie utilisatrices et fermez l'assistant.

La boîte de dialogue Modifier la politique d'émission des demandes de remboursement s'affiche.

Si la boîte de dialogue ne s'affiche pas, cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.

6. Pour démarrer l'assistant règle de sinistre, cliquez sur **Ajouter règle** :
   a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste, puis cliquez sur **Suivant**.
   b. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **objectGUID to Name ID**.

   c. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   d. Dans la colonne attribut LDAP de la table mappage, saisissez **objectGUID**.
   e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
   f. Cliquez sur **Terminer**, puis sur **OK**.
7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :
   a. Cliquez sur **Ajouter SAML**.
   b. Sélectionnez **Endpoint Type** > **SAML Logout**.
   c. Sélectionnez **Redirect** > **Redirect**.
   d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud d'administration :

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

   Pour `Admin_Node_FQDN`, Entrez le nom de domaine complet du nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

   a. Cliquez sur **OK**.
9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour la fiducie de cette partie de confiance :

a. Ajouter le certificat personnalisé :

   - Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé vers StorageGRID, sélectionnez ce certificat.
   - Si vous ne disposez pas du certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` Répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.

     Remarque : utilisation du certificat par défaut du noeud d'administration (`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous restaurez le nœud et vous devrez mettre à jour la confiance de l'organisme de confiance.

b. Cliquez sur **appliquer**, puis sur **OK**.

   Les propriétés de la partie de confiance sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
11. Lorsque vous avez terminé, revenez à StorageGRID et "tester toutes les fiducies de la partie qui repose" pour confirmer qu'ils sont correctement configurés.

Confiance de la partie qui fait confiance aux essais

Avant d'appliquer l'utilisation de l'authentification unique (SSO) pour StorageGRID, vérifiez que l'authentification unique et la déconnexion unique (SLO) sont correctement configurées. Si vous avez créé une confiance en tiers pour chaque nœud d'administration, confirmez que vous pouvez utiliser SSO et SLO pour chaque nœud d'administration.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous avez configuré une ou plusieurs fiducies de tiers de confiance dans AD FS.

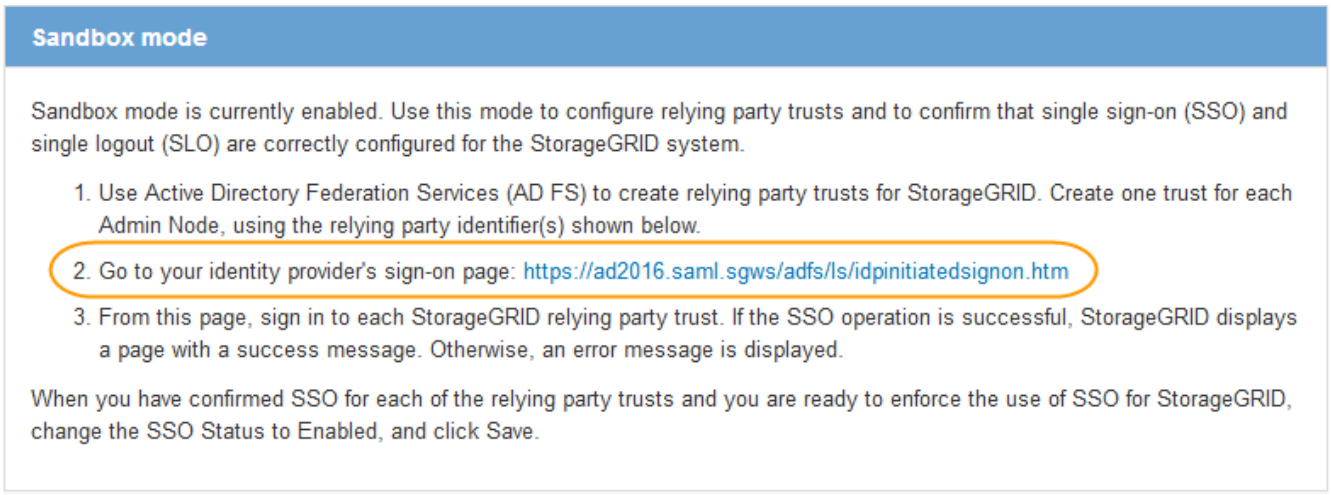
Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **connexion unique**.

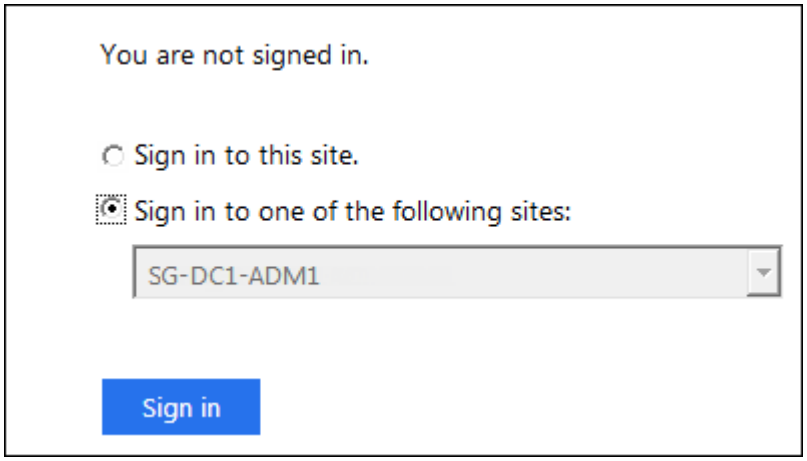
   La page connexion unique s'affiche, avec l'option **Sandbox mode** sélectionnée.

2. Dans les instructions pour le mode sandbox, recherchez le lien vers la page de connexion de votre fournisseur d'identités.

   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service fédéré**.

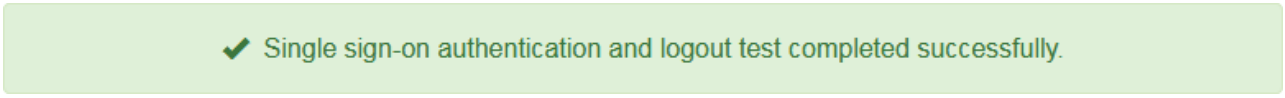


3. Cliquez sur le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identités.
4. Pour confirmer que vous pouvez utiliser l'authentification SSO pour vous connecter à StorageGRID, sélectionnez **connexion à l'un des sites suivants**, sélectionnez l'identifiant de partie de confiance pour votre nœud d'administration principal, puis cliquez sur **connexion**.



Vous devez entrer votre nom d'utilisateur et votre mot de passe.

5. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
   - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.



   - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
6. Répétez les étapes précédentes pour confirmer que vous pouvez vous connecter à n'importe quel autre nœud d'administration.

Si toutes les opérations de connexion SSO et de déconnexion ont réussi, vous êtes prêt à activer SSO.

Activation de l’authentification unique

Après avoir utilisé le mode sandbox pour tester toutes vos approbations StorageGRID, vous êtes prêt à activer l’authentification unique (SSO).

Ce dont vous avez besoin

- Vous devez avoir importé au moins un groupe fédéré du référentiel d’identité et affecté des autorisations de gestion de l’accès racine au groupe. Vous devez confirmer qu’au moins un utilisateur fédéré dispose d’une autorisation d’accès racine au gestionnaire de grille et au gestionnaire de locataires pour tout compte de locataire existant.
- Vous devez avoir testé toutes les approbations de parties utilisatrices à l’aide du mode sandbox.

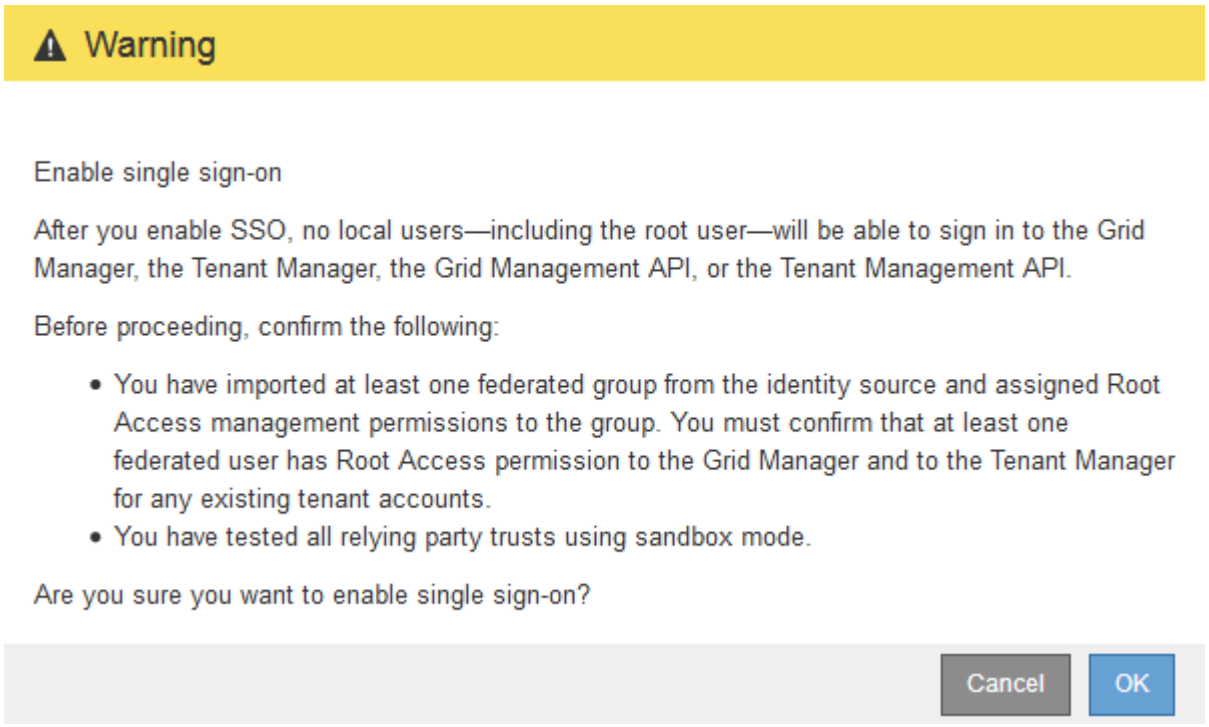
Étapes

1. Sélectionnez **Configuration** > **contrôle d’accès** > **connexion unique**.

   La page Single Sign-On s’affiche avec **Sandbox mode** sélectionné.

2. Définissez l’état SSO sur **activé**.
3. Cliquez sur **Enregistrer**.

   Un message d’avertissement s’affiche.



4. Vérifiez l’avertissement et cliquez sur **OK**.

   L’authentification unique est désormais activée.

> Tous les utilisateurs doivent utiliser l’authentification SSO pour accéder au Grid Manager, au Gestionnaire de locataires, à l’API de gestion Grid et à l’API de gestion des locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Désactivation de la connexion unique

Vous pouvez désactiver l'authentification unique (SSO) si vous ne souhaitez plus utiliser cette fonctionnalité. Vous devez désactiver l'authentification unique avant de pouvoir désactiver la fédération des identités.

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

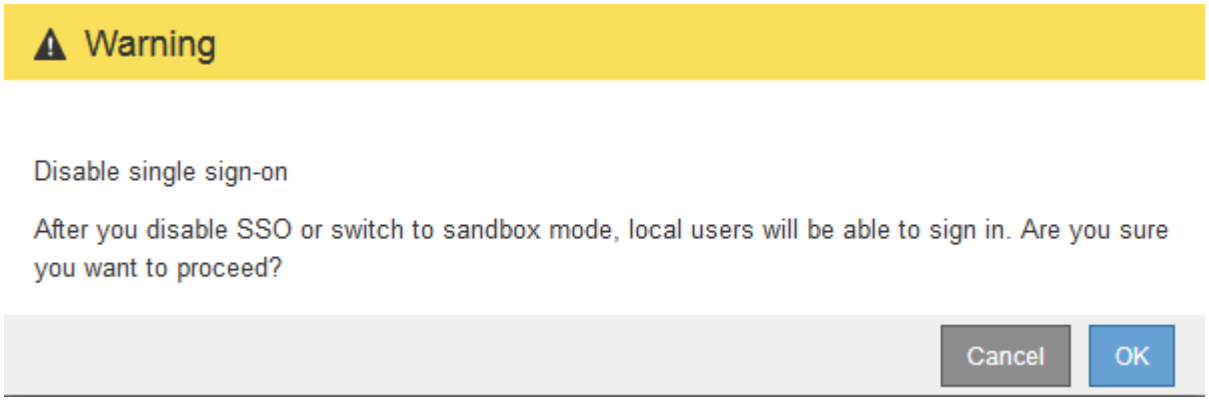
Étapes

1. Sélectionnez **Configuration** > **contrôle d'accès** > **connexion unique**.

   La page authentification unique s'affiche.

2. Sélectionnez l'option **Disabled**.
3. Cliquez sur **Enregistrer**.

   Un message d'avertissement s'affiche pour indiquer que les utilisateurs locaux pourront maintenant se connecter.



4. Cliquez sur **OK**.

   La prochaine fois que vous vous connectez à StorageGRID, la page de connexion StorageGRID s'affiche et vous devez entrer le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivation et réactivation temporaire de l'authentification unique pour un nœud d'administration

Il se peut que vous ne puissiez pas vous connecter à Grid Manager si le système d'authentification unique (SSO) est en panne. Dans ce cas, vous pouvez temporairement désactiver et réactiver SSO pour un noeud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder au shell de commande du nœud.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

- Vous devez connaître le mot de passe de l'utilisateur root local.

Description de la tâche

Après avoir désactivé SSO pour un noeud d'administration, vous pouvez vous connecter à Grid Manager en tant qu'utilisateur racine local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver SSO sur le nœud d'administration dès que vous vous déconnectez.

> La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO pour les autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page d'ouverture de session unique dans Grid Manager reste sélectionnée et tous les paramètres SSO existants sont conservés à moins que vous ne les mettrez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez la commande suivante :`disable-saml`

   Un message indique que la commande s'applique uniquement à ce nœud d'administration.

3. Confirmez que vous souhaitez désactiver l'authentification SSO.

   Un message indique que l'authentification unique est désactivée sur le nœud.

4. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.

   La page de connexion à Grid Manager s'affiche car SSO a été désactivé.

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :
   a. Sélectionnez **Configuration** > **contrôle d'accès** > **connexion unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Cliquez sur **Enregistrer**.

      Si vous cliquez sur **Enregistrer** à partir de la page connexion unique, l'option SSO est automatiquement réactivée pour l'ensemble de la grille.

7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :
   a. Effectuez les tâches que vous souhaitez effectuer.
   b. Cliquez sur **Déconnexion** et fermez le gestionnaire de grille.

c. Réactivez SSO sur le nœud d'administration. Vous pouvez effectuer l'une des opérations suivantes :

   - Exécutez la commande suivante : `enable-saml`

     Un message indique que la commande s'applique uniquement à ce nœud d'administration.

     Confirmez que vous souhaitez activer le SSO.

   Un message indique que l'authentification unique est activée sur le nœud.

   - Redémarrez le nœud grid : `reboot`

8. À partir d'un navigateur Web, accédez à Grid Manager à partir du même nœud d'administration.
9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Gestionnaire de grille.

Informations associées

"Configuration de l'authentification unique"