Utiliser l'authentification unique (SSO)

StorageGRID software

NetApp
December 03, 2025

Sommaire

Utiliser l’authentification unique (SSO)

Configurer l’authentification unique

Lorsque l’authentification unique (SSO) est activée, les utilisateurs ne peuvent accéder au gestionnaire de grille, au gestionnaire de locataires, à l’API de gestion de grille ou à l’API de gestion de locataires que si leurs informations d’identification sont autorisées à l’aide du processus de connexion SSO mis en œuvre par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Comment fonctionne l’authentification unique

Le système StorageGRID prend en charge l’authentification unique (SSO) à l’aide de la norme Security Assertion Markup Language 2.0 (SAML 2.0).

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

Sign in lorsque SSO est activé

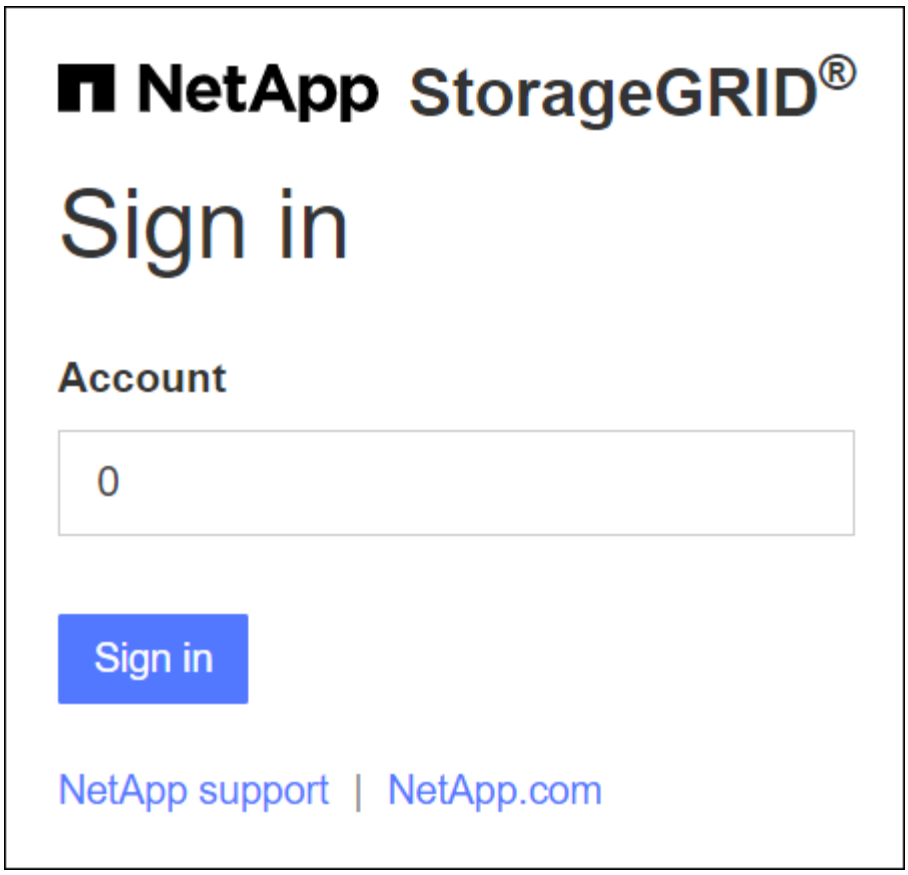
Lorsque SSO est activé et que vous vous connectez à StorageGRID, vous êtes redirigé vers la page SSO de votre organisation pour valider vos informations d’identification.

Étapes

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

   La page de Sign in StorageGRID s’affiche.

   - Si c’est la première fois que vous accédez à l’URL sur ce navigateur, vous êtes invité à saisir un identifiant de compte :

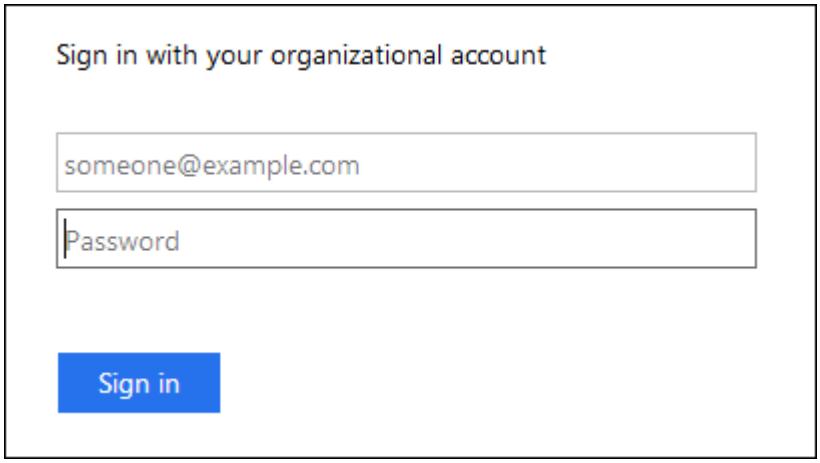


- Si vous avez déjà accédé au Grid Manager ou au Tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un ID de compte :

La page de Sign in StorageGRID ne s'affiche pas lorsque vous saisissez l'URL complète d'un compte 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 organisation, où vous pouvezconnectez-vous avec vos identifiants SSO .

2. Indiquez si vous souhaitez accéder au Grid Manager ou au Tenant Manager :
   - Pour accéder au Gestionnaire de grille, laissez le champ **ID de compte** vide, saisissez **0** comme ID de compte ou sélectionnez **Gestionnaire de grille** s'il apparaît dans la liste des comptes récents.
   - Pour accéder au gestionnaire de locataires, saisissez l'ID de compte locataire à 20 chiffres ou sélectionnez un locataire par son nom s'il apparaît dans la liste des comptes récents.
3. Sélectionner * Sign in*

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



4. Sign in avec vos identifiants SSO.

   Si vos informations d'identification SSO sont correctes :

   a. Le fournisseur d'identité (IdP) 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 avec des autorisations d'accès StorageGRID , vous êtes connecté au Grid Manager ou au Tenant Manager, selon le compte que vous avez sélectionné.

   Si le compte de service est inaccessible, vous pouvez toujours vous connecter, à condition que vous soyez un utilisateur existant appartenant à un groupe fédéré avec des autorisations d'accès StorageGRID .

5. Vous pouvez également accéder à d'autres nœuds d'administration ou accéder au gestionnaire de grille ou au gestionnaire de locataires, si vous disposez des autorisations adéquates.

   Vous n'avez pas besoin de ressaisir vos identifiants SSO.

Déconnectez-vous lorsque SSO est activé

Lorsque SSO est activé pour StorageGRID, ce qui se passe lorsque vous vous déconnectez dépend de ce à quoi vous êtes connecté et de l'endroit d'où vous vous déconnectez.

Étapes

1. Localisez le lien **Déconnexion** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Déconnexion**.

   La page de Sign in 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 à ces interfaces utilisateur plus rapidement à l'avenir.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté de…
Gestionnaire de grille sur un ou plusieurs nœuds d'administration	Gestionnaire de grille sur n'importe quel nœud d'administration	Gestionnaire de grille sur tous les nœuds d'administration **Remarque :** si vous utilisez Azure pour l'authentification unique, la déconnexion de tous les nœuds d'administration peut prendre quelques minutes.
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
Gestionnaire de réseau et gestionnaire de locataires	Gestionnaire de grille	Le gestionnaire de grille uniquement. Vous devez également vous déconnecter du gestionnaire de locataires 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 sur plusieurs sessions de navigateur, vous devez vous déconnecter de toutes les sessions de navigateur séparément.

Exigences et considérations relatives à l'authentification unique

Avant d'activer l'authentification unique (SSO) pour un système StorageGRID , examinez les exigences et les considérations.

Exigences relatives aux fournisseurs d'identité

StorageGRID prend en charge les fournisseurs d'identité SSO (IdP) suivants :

- Service de fédération Active Directory (AD FS)

- Azure Active Directory (Azure AD)
- PingFédéré

Vous devez configurer la fédération d'identité pour votre système StorageGRID avant de pouvoir configurer un fournisseur d'identité SSO. Le type de service LDAP que vous utilisez pour la fédération d'identité contrôle le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

Exigences AD FS

Vous pouvez utiliser l'une des versions suivantes d'AD FS :

- Windows Server 2022 AD FS
- Windows Server 2019 AD FS
- Windows Server 2016 AD FS

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

Exigences supplémentaires

- Sécurité de la couche transport (TLS) 1.2 ou 1.3
- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations pour Azure

Si vous utilisez Azure comme type SSO et que les utilisateurs ont des noms d'utilisateur principaux qui n'utilisent pas sAMAccountName comme préfixe, des problèmes de connexion peuvent survenir si StorageGRID perd sa connexion avec le serveur LDAP. Pour permettre aux utilisateurs de se connecter, vous devez restaurer la connexion au serveur LDAP.

Exigences relatives aux certificats de serveur

Par défaut, StorageGRID utilise un certificat d'interface de gestion sur chaque nœud d'administration pour sécuriser l'accès au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Lorsque vous configurez des approbations de parties de confiance (AD FS), des applications d'entreprise (Azure) ou des connexions de fournisseurs de services (PingFederate) pour StorageGRID, vous utilisez le certificat du serveur comme certificat de signature pour les demandes StorageGRID .

Si vous ne l'avez pas déjà fait"configuré un certificat personnalisé pour l'interface de gestion" , tu devrais 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 parties de confiance StorageGRID , les applications d'entreprise ou les connexions SP .

L'utilisation du certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, une application d'entreprise ou un SP n'est pas recommandée. 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 récupéré, vous devez mettre à jour l'approbation de la partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

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

Exigences portuaires

L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique. Voir "Contrôler l'accès au pare-feu externe" .

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 gestionnaire de grille et au gestionnaire de locataires pour tous les comptes de locataires existants.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous avez déjà configuré la fédération d'identité.

Étapes

1. S'il existe des comptes locataires existants, confirmez qu'aucun des locataires n'utilise sa propre source d'identité.

   Lorsque vous activez SSO, une source d'identité configurée dans le gestionnaire de locataires est remplacée par la source d'identité configurée dans le gestionnaire de grille. Les utilisateurs appartenant à la source d'identité du locataire ne pourront plus se connecter à moins qu'ils ne disposent d'un compte auprès de la source d'identité Grid Manager.

   a. Sign in au gestionnaire de locataires pour chaque compte locataire.
   b. Sélectionnez **GESTION DES ACCÈS** > **Fédération d'identité**.
   c. Vérifiez que la case à cocher **Activer la fédération d'identité** n'est pas sélectionnée.
   d. Si tel est le cas, confirmez que tous les groupes fédérés susceptibles d'être utilisés pour ce compte locataire ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.

2. Confirmer qu'un utilisateur fédéré peut accéder au gestionnaire de grille :
   a. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Groupes d'administrateurs**.
   b. Assurez-vous qu'au moins un groupe fédéré a été importé à partir de la source d'identité Active Directory et que l'autorisation d'accès racine lui a été attribuée.

c. Se déconnecter.

d. Confirmez que vous pouvez vous reconnecter au gestionnaire de grille en tant qu'utilisateur du groupe fédéré.

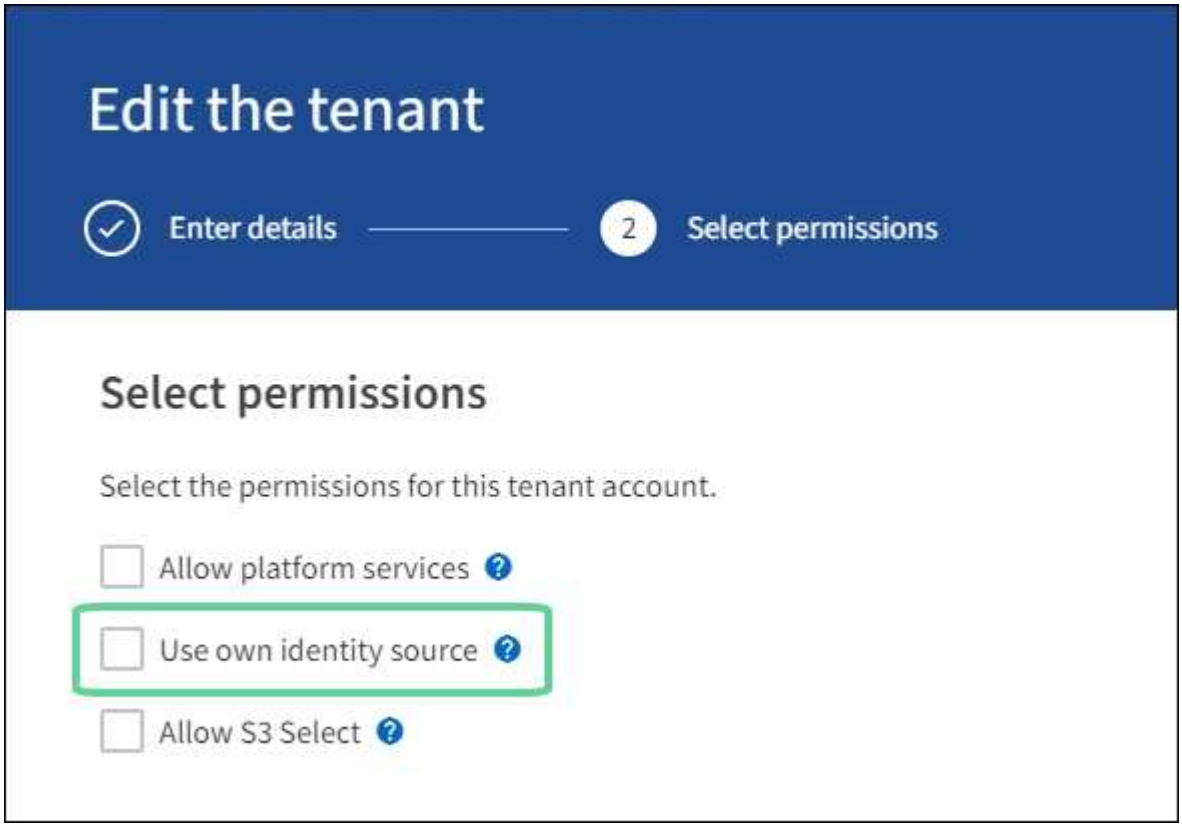
3. S'il existe des comptes locataires existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès root peut se connecter :

a. Depuis le gestionnaire de grille, sélectionnez **LOCATAIRES**.

b. Sélectionnez le compte locataire, puis sélectionnez **Actions** > **Modifier**.

c. Dans l'onglet Entrer les détails, sélectionnez **Continuer**.

d. Si la case à cocher **Utiliser sa propre source d'identité** est sélectionnée, décochez la case et sélectionnez **Enregistrer**.



La page Locataire apparaît.

a. Sélectionnez le compte locataire, sélectionnez * Sign in* et connectez-vous au compte locataire en tant qu'utilisateur root local.

b. Depuis le gestionnaire de locataires, sélectionnez **GESTION DES ACCÈS** > **Groupes**.

c. Assurez-vous qu'au moins un groupe fédéré du gestionnaire de grille s'est vu attribuer l'autorisation d'accès racine pour ce locataire.

d. Se déconnecter.

e. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur du groupe fédéré.

Informations connexes

- "Exigences et considérations relatives à l'authentification unique"
- "Gérer les groupes d'administrateurs"

- "Utiliser un compte locataire"

Utiliser le mode sandbox

Vous pouvez utiliser le mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs StorageGRID . Une fois l'authentification unique activée, vous pouvez revenir au mode sandbox chaque fois que vous devez modifier ou retester la configuration.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .
- Vous avez configuré la fédération d'identité pour votre système StorageGRID .
- Pour le type de service LDAP de fédération d'identité, vous avez sélectionné Active Directory ou Azure, en fonction du fournisseur d'identité SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Azuré • PingFédéré
Azuré	Azuré

À propos de cette tâche

Lorsque SSO est activé et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une demande d'authentification au fournisseur d'identité SSO. À son tour, le fournisseur d'identité SSO renvoie une réponse d'authentification à StorageGRID, indiquant si la demande d'authentification a réussi. Pour des demandes réussies :

- La réponse d'Active Directory ou de PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Azure inclut un nom d'utilisateur principal (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer en toute sécurité sur les demandes d'authentification des utilisateurs, vous devez configurer certains paramètres dans StorageGRID. Ensuite, vous devez utiliser le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Azure) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration. Enfin, vous devez revenir à StorageGRID pour activer SSO.

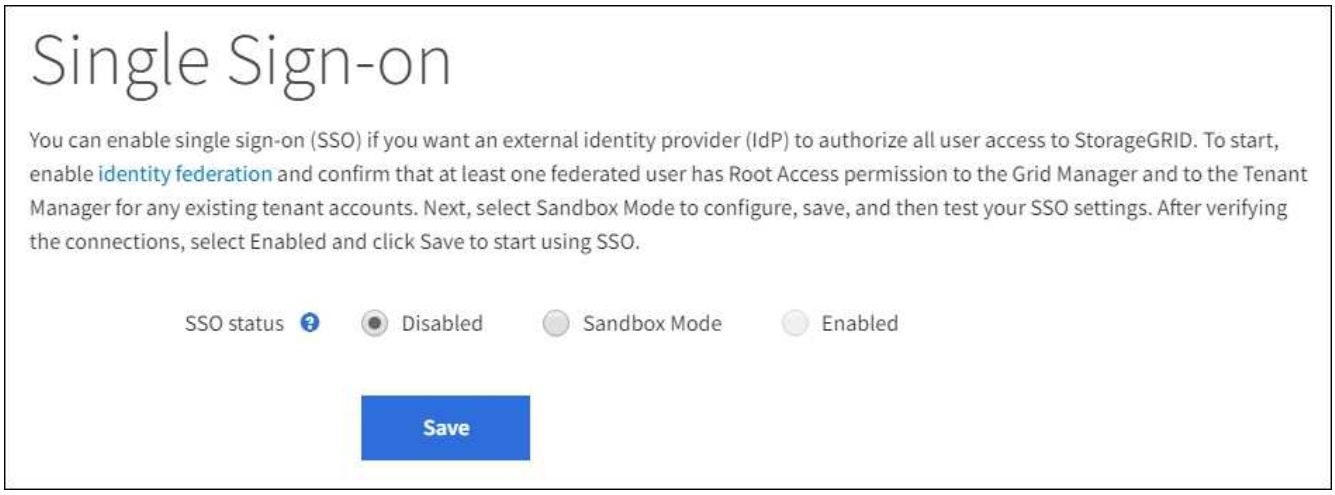
Le mode Sandbox facilite l'exécution de cette configuration aller-retour et permet de tester tous vos paramètres avant d'activer SSO. Lorsque vous utilisez le mode sandbox, les utilisateurs ne peuvent pas se connecter à l'aide de SSO.

Accéder au mode sandbox

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   La page d'authentification unique s'affiche, avec l'option **Désactivé** sélectionnée.



> Si les options d'état SSO n'apparaissent pas, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. Voir "Exigences et considérations relatives à l'authentification unique" .

2. Sélectionnez **Mode Sandbox**.

   La section Fournisseur d'identité apparaît.

Entrez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type SSO** dans la liste déroulante.
2. Remplissez les champs de la section Fournisseur d'identité en fonction du type SSO que vous avez sélectionné.

Active Directory

a. Saisissez le **Nom du service de fédération** pour le fournisseur d'identité, exactement tel qu'il apparaît dans Active Directory Federation Service (AD FS).

> Pour localiser le nom du service de fédération, accédez au Gestionnaire de serveur Windows. Sélectionnez **Outils** > **Gestion AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération est affiché dans le deuxième champ.

b. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

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

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

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

> Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

c. Dans la section Partie de confiance, spécifiez l'**identifiant de la partie de confiance** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque approbation de partie de confiance dans AD FS.

- Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

> Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

d. Sélectionnez **Enregistrer**.

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

Azuré

a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

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

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

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

   > Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

b. Dans la section Application d'entreprise, spécifiez le **Nom de l'application d'entreprise** pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque application d'entreprise dans Azure AD.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche un nom d'application d'entreprise pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   > Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

c. Suivez les étapes dans"Créer des applications d'entreprise dans Azure AD" pour créer une application d'entreprise pour chaque nœud d'administration répertorié dans le tableau.

d. Depuis Azure AD, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ **URL des métadonnées de la fédération** correspondant dans StorageGRID.

e. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer**.

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

PingFédéré

a. Spécifiez quel certificat TLS sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux demandes StorageGRID .

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

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

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

   > Si vous modifiez le certificat CA, immédiatement"redémarrer le service mgmt-api sur les nœuds d'administration" et tester une connexion SSO réussie dans le Grid Manager.

b. Dans la section Fournisseur de services (SP), spécifiez l'*ID de connexion SP * pour StorageGRID. Cette valeur contrôle le nom que vous utilisez pour chaque connexion SP dans PingFederate.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'ajouter d'autres nœuds d'administration à l'avenir, entrez `SG` ou `StorageGRID` .
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple : `SG-[HOSTNAME]` . Cela génère un tableau qui affiche l'ID de connexion SP pour chaque nœud d'administration de votre système, en fonction du nom d'hôte du nœud.

   > Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une connexion SP pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

c. Spécifiez l'URL des métadonnées de la fédération pour chaque nœud d'administration dans le champ **URL des métadonnées de la fédération**.

   Utilisez le format suivant :

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

d. Sélectionnez **Enregistrer**.

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

Configurer les approbations des parties de confiance, les applications d'entreprise ou les connexions SP

Lorsque la configuration est enregistrée, l'avis de confirmation du mode Sandbox apparaît. Cet avis confirme que le mode sandbox est désormais activé et fournit des instructions générales.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, lorsque le **Mode Sandbox** est sélectionné sur la page d'authentification unique, l'authentification unique est désactivée pour tous les utilisateurs de StorageGRID . Seuls les utilisateurs locaux peuvent se connecter.

Suivez ces étapes pour configurer les approbations des parties de confiance (Active Directory), compléter les applications d'entreprise (Azure) ou configurer les connexions SP (PingFederate).

Active Directory

Étapes

1. Accédez aux services de fédération Active Directory (AD FS).
2. Créez une ou plusieurs approbations de partie de confiance pour StorageGRID, en utilisant chaque identifiant de partie de confiance indiqué dans le tableau de la page d'authentification unique StorageGRID .

   Vous devez créer une approbation pour chaque nœud d'administration affiché dans le tableau.

   Pour obtenir des instructions, rendez-vous sur"Créer des approbations de parties de confiance dans AD FS" .

Azuré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
   a. Sign in au nœud.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes dans"Créer des applications d'entreprise dans Azure AD" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Azure correspondante.

PingFédéré

Étapes

1. Depuis la page d'authentification unique du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tous les autres nœuds d'administration de votre grille, répétez ces étapes :
   a. Sign in au nœud.
   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML pour ce nœud.
3. Accédez à PingFederate.
4. "Créer une ou plusieurs connexions de fournisseur de services (SP) pour StorageGRID" . Utilisez l'ID de connexion SP pour chaque nœud d'administration (affiché dans le tableau de la page d'authentification unique StorageGRID) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

   Vous devez créer une connexion SP pour chaque nœud d'administration indiqué dans le tableau.

Tester les connexions SSO

Avant d'appliquer l'utilisation de l'authentification unique pour l'ensemble de votre système StorageGRID ,

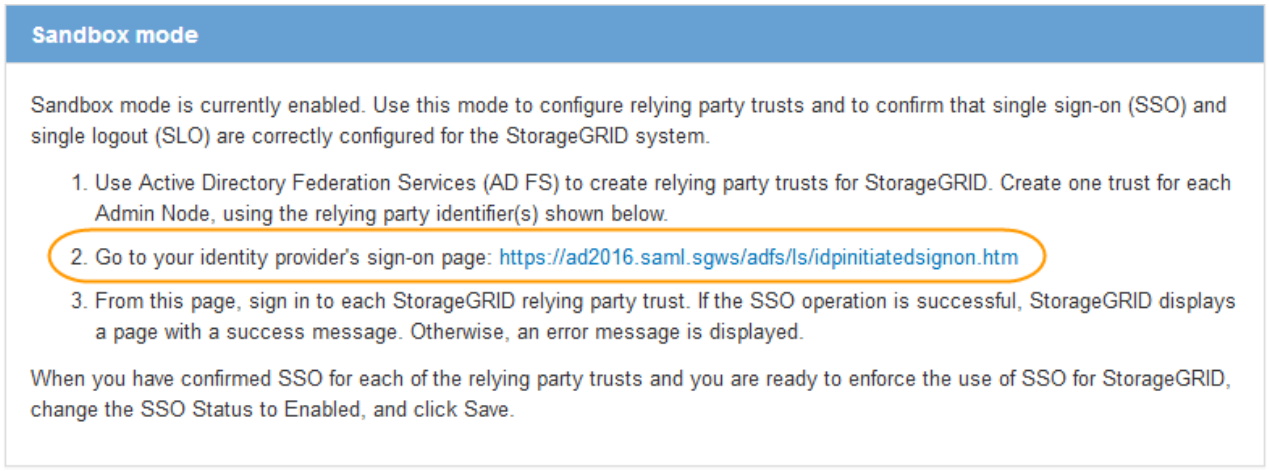
vous devez confirmer que l’authentification unique et la déconnexion unique sont correctement configurées pour chaque nœud d’administration.

Active Directory

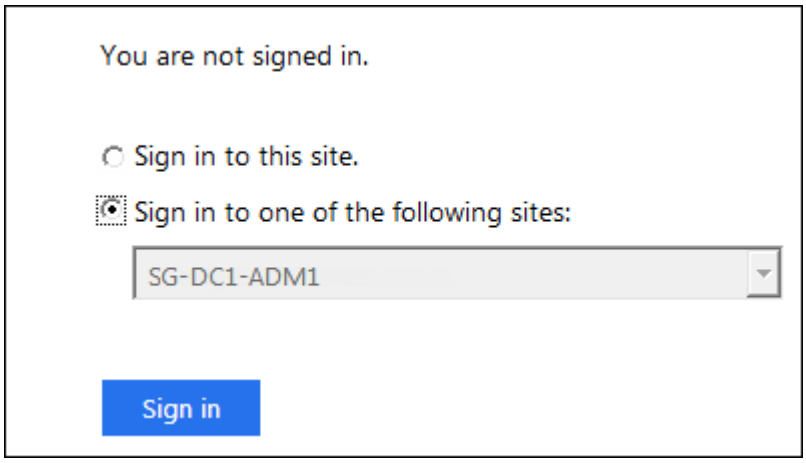
Étapes

1. À partir de la page d'authentification unique StorageGRID , recherchez le lien dans le message du mode Sandbox.

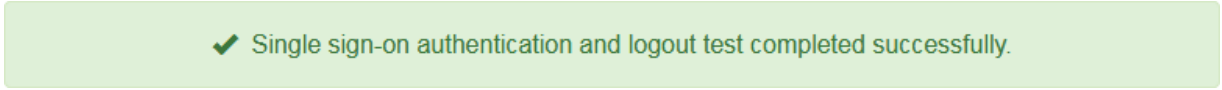
   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Nom du service de fédération**.



2. Sélectionnez le lien ou copiez et collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identité.
3. Pour confirmer que vous pouvez utiliser SSO pour vous connecter à StorageGRID, sélectionnez * Sign in à l'un des sites suivants*, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal et sélectionnez * Sign in*.



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



   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre

grille.

Azuré

Étapes

1. Accédez à la page d'authentification unique dans le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de réussite s'affiche.

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

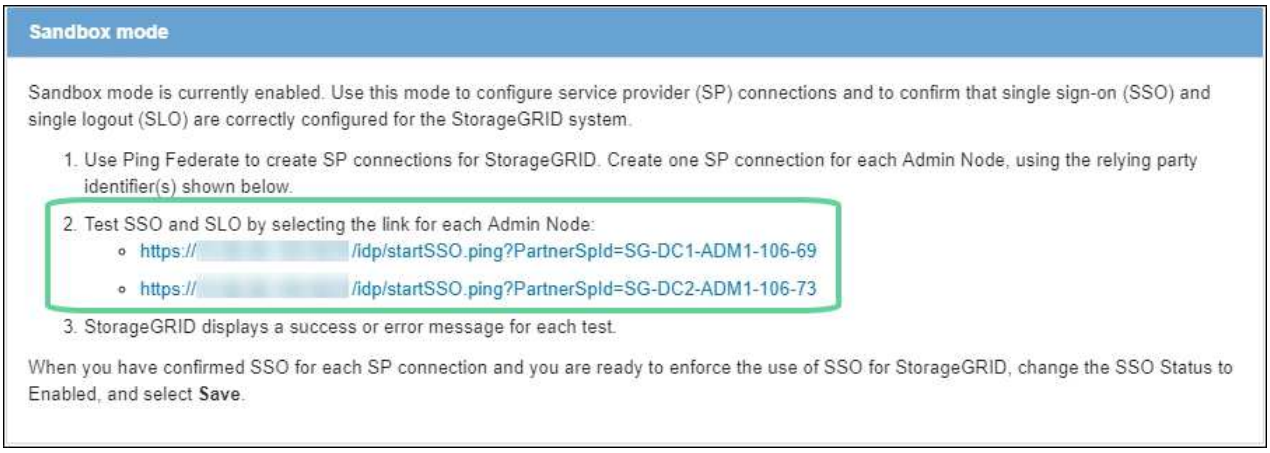
   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFédéré

Étapes

1. À partir de la page d'authentification unique StorageGRID , sélectionnez le premier lien dans le message du mode Sandbox.

   Sélectionnez et testez un lien à la fois.



2. Saisissez les informations d'identification d'un utilisateur fédéré.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de réussite s'affiche.

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

   - Si l'opération SSO échoue, un message d'erreur s'affiche. Résolvez le problème, effacez les cookies du navigateur et réessayez.
3. Sélectionnez le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si vous voyez un message indiquant que la page a expiré, sélectionnez le bouton **Retour** dans votre navigateur et soumettez à nouveau vos informations d'identification.

Activer l'authentification unique

Une fois que vous avez confirmé que vous pouvez utiliser SSO pour vous connecter à chaque nœud d'administration, vous pouvez activer SSO pour l'ensemble de votre système StorageGRID .

Lorsque SSO est activé, tous les utilisateurs doivent utiliser SSO pour accéder au gestionnaire de grille, au gestionnaire de locataires, à l'API de gestion de grille et à l'API de gestion de locataires. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
2. Modifiez le statut SSO sur **Activé**.
3. Sélectionnez **Enregistrer**.
4. Lisez le message d'avertissement et sélectionnez **OK**.

   L'authentification unique est désormais activée.

Si vous utilisez le portail Azure et que vous accédez à StorageGRID à partir du même ordinateur que celui que vous utilisez pour accéder à Azure, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (un utilisateur d'un groupe fédéré qui a été importé dans StorageGRID) ou déconnectez-vous du portail Azure avant de tenter de vous connecter à StorageGRID.

Créer des approbations de parties de confiance dans AD FS

Vous devez utiliser les services de fédération Active Directory (AD FS) pour créer une approbation de partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez créer des approbations de parties de confiance à l'aide de commandes PowerShell, en important des métadonnées SAML à partir de StorageGRID ou en saisissant les données manuellement.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **AD FS** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous connaissez le nom de domaine complet (ou l'adresse IP) et l'identifiant de la partie de confiance pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .

Vous devez créer une approbation de partie de confiance pour chaque nœud d'administration de votre système StorageGRID . Le fait de disposer d'une partie de confiance pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'approbations de parties de confiance dans AD FS ou vous avez accès à la documentation Microsoft AD FS.
- Vous utilisez le composant logiciel enfichable Gestion AD FS et vous appartenez au groupe Administrateurs.
- Si vous créez manuellement l'approbation de partie de confiance, vous disposez du certificat personnalisé qui a été téléchargé pour l'interface de gestion StorageGRID ou vous savez comment vous connecter à un nœud d'administration à partir de l'interpréteur de commandes.

À propos de cette tâche

Ces instructions s'appliquent à Windows Server 2016 AD FS. Si vous utilisez une version différente d'AD FS, vous remarquerez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

Créer une approbation de partie de confiance à l'aide de Windows PowerShell

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

Étapes

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

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

   - Pour `Admin_Node_Identifier` , saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : `SG-DC1-ADM1` .
   - Pour `Admin_Node_FQDN` , entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **Gestion AD FS**.

   L'outil de gestion AD FS apparaît.
4. Sélectionnez **AD FS** > **Approbations de parties de confiance**.

   La liste des fiducies de parties utilisatrices s'affiche.
5. Ajoutez une politique de contrôle d'accès à la nouvelle approbation de partie de confiance créée :
   a. Localisez la fiducie de partie de confiance que vous venez de créer.
   b. Cliquez avec le bouton droit sur l'approbation et sélectionnez **Modifier la politique de contrôle d'accès**.

c. Sélectionnez une politique de contrôle d'accès.

d. Sélectionnez **Appliquer**, puis **OK**

6. Ajoutez une politique d'émission de réclamation à la fiducie de partie utilisatrice nouvellement créée :

a. Localisez la fiducie de partie de confiance que vous venez de créer.

b. Cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

c. Sélectionnez **Ajouter une règle**.

d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.

e. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

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

g. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

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

i. Sélectionnez **Terminer**, puis **OK**.

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

a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.

b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

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

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

9. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode Sandbox" pour les instructions.

Créer une approbation de partie de confiance en important des métadonnées de fédération

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

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.

2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.

3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.

4. Sélectionnez **Importer des données sur la partie utilisatrice publiées en ligne ou sur un réseau local**.

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

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

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

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

> Lors de la saisie du nom d'affichage, utilisez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. Par exemple : `SG-DC1-ADM1`.

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

      Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

   e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
   f. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
   g. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.
   h. Sélectionnez **Terminer**, puis **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
   b. Confirmez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

      Si les métadonnées sont manquantes, confirmez que l'adresse des métadonnées de la Fédération est correcte ou saisissez les valeurs manuellement.
9. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
10. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode Sandbox" pour les instructions.

Créer manuellement une fiducie de partie utilisatrice

Si vous choisissez de ne pas importer les données des approbations de partie de confiance, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **Gestion AD FS**.
2. Sous Actions, sélectionnez **Ajouter une approbation de partie de confiance**.
3. Sur la page d'accueil, choisissez **Réclamations prises en compte**, puis sélectionnez **Démarrer**.
4. Sélectionnez **Saisir manuellement les données sur la partie de confiance**, puis sélectionnez **Suivant**.
5. Complétez l'assistant d'approbation de partie de confiance :

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

      Par souci de cohérence, utilisez l'identifiant de partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique dans le gestionnaire de grille. 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 point de terminaison du service SAML pour le nœud 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. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

   e. Sur la page Configurer les identifiants, spécifiez l'identifiant de la partie de confiance pour le même nœud d'administration :

      `Admin_Node_Identifier`

      Pour *`Admin_Node_Identifier`* , saisissez l'identifiant de la partie de confiance pour le nœud d'administration, exactement tel qu'il apparaît sur la page d'authentification unique. Par exemple : `SG-DC1-ADM1` .

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

      La boîte de dialogue Modifier la politique d'émission de réclamation s'affiche.

      > Si la boîte de dialogue n'apparaît pas, cliquez avec le bouton droit sur la fiducie et sélectionnez **Modifier la politique d'émission de réclamation**.

6. Pour démarrer l'assistant de règle de revendication, sélectionnez **Ajouter une règle** :

   a. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer les attributs LDAP en tant que revendications** dans la liste, puis sélectionnez **Suivant**.

   b. Sur la page Configurer la règle, entrez un nom d'affichage pour cette règle.

      Par exemple, **ObjectGUID vers Name ID** ou **UPN vers Name ID**.

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

d. Dans la colonne Attribut LDAP de la table de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

e. Dans la colonne Type de réclamation sortante de la table de mappage, sélectionnez **ID de nom** dans la liste déroulante.

f. Sélectionnez **Terminer**, puis **OK**.

7. Cliquez avec le bouton droit sur l'approbation de la partie de confiance pour ouvrir ses propriétés.
8. Dans l'onglet **Points de terminaison**, configurez le point de terminaison pour la déconnexion unique (SLO) :

a. Sélectionnez **Ajouter SAML**.

b. Sélectionnez **Type de point de terminaison** > **Déconnexion SAML**.

c. Sélectionnez **Liaison** > **Redirection**.

d. Dans le champ **URL de confiance**, saisissez l'URL utilisée pour la déconnexion unique (SLO) de ce nœud 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. Cependant, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP change un jour.)

a. Sélectionnez **OK**.

9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour cette approbation de partie de confiance :

a. Ajoutez le certificat personnalisé :

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

> Utilisation du certificat par défaut du nœud d'administration(`server.crt`) n'est pas recommandé. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lorsque vous récupérerez le nœud et vous devrez mettre à jour l'approbation de la partie de confiance.

b. Sélectionnez **Appliquer**, puis **OK**.

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

10. Répétez ces étapes pour configurer une approbation de partie de confiance pour tous les nœuds d'administration de votre système StorageGRID .
11. Une fois que vous avez terminé, revenez à StorageGRID et testez toutes les approbations des parties de confiance pour confirmer qu'elles sont correctement configurées. Voir"Utiliser le mode sandbox" pour les instructions.

Créer des applications d'entreprise dans Azure AD

Vous utilisez Azure AD pour créer une application d'entreprise pour chaque nœud d'administration de votre système.

Avant de commencer

- Vous avez commencé à configurer l'authentification unique pour StorageGRID et vous avez sélectionné **Azure** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID .

> Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID . Disposer d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité de n'importe quel nœud d'administration.

- Vous avez de l'expérience dans la création d'applications d'entreprise dans Azure Active Directory.
- Vous disposez d'un compte Azure avec un abonnement actif.
- Vous disposez de l'un des rôles suivants dans le compte Azure : administrateur général, administrateur d'applications cloud, administrateur d'applications ou propriétaire du principal du service.

Accéder à Azure AD

Étapes

1. Connectez-vous à la "Portail Azure" .
2. Accéder à "Azure Active Directory" .
3. Sélectionner "Applications d'entreprise" .

Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID

Pour enregistrer la configuration SSO pour Azure dans StorageGRID, vous devez utiliser Azure pour créer une application d'entreprise pour chaque nœud d'administration. Vous copierez les URL de métadonnées de fédération depuis Azure et les collerez dans les champs **URL de métadonnées de fédération** correspondants sur la page d'authentification unique StorageGRID .

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet Applications Azure Enterprise, sélectionnez **Nouvelle application**.
   b. Sélectionnez **Créer votre propre application**.
   c. Pour le nom, saisissez le **Nom de l'application d'entreprise** que vous avez copié à partir du tableau des détails du nœud d'administration sur la page d'authentification unique StorageGRID .
   d. Laissez le bouton radio **Intégrer toute autre application que vous ne trouvez pas dans la galerie (Hors galerie)** sélectionné.

e. Sélectionnez **Créer**.

f. Sélectionnez le lien **Commencer** dans le **2. Configurer l'authentification unique** ou sélectionner le lien **Authentification unique** dans la marge de gauche.

g. Sélectionnez la case **SAML**.

h. Copiez l'**URL des métadonnées de la fédération d'applications**, que vous pouvez trouver sous **Étape 3 Certificat de signature SAML**.

i. Accédez à la page d'authentification unique StorageGRID et collez l'URL dans le champ **URL des métadonnées de la fédération** qui correspond au **nom de l'application d'entreprise** que vous avez utilisé.

2. Après avoir collé une URL de métadonnées de fédération pour chaque nœud d'administration et apporté toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page d'authentification unique StorageGRID .

Téléchargez les métadonnées SAML pour chaque nœud d'administration

Une fois la configuration SSO enregistrée, vous pouvez télécharger un fichier de métadonnées SAML pour chaque nœud d'administration de votre système StorageGRID .

Étapes

1. Répétez ces étapes pour chaque nœud d'administration.

   a. Sign in à StorageGRID à partir du nœud d'administration.

   b. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   c. Sélectionnez le bouton pour télécharger les métadonnées SAML pour ce nœud d'administration.

   d. Enregistrez le fichier que vous téléchargerez dans Azure AD.

Télécharger les métadonnées SAML vers chaque application d'entreprise

Après avoir téléchargé un fichier de métadonnées SAML pour chaque nœud d'administration StorageGRID , effectuez les étapes suivantes dans Azure AD :

Étapes

1. Revenez au portail Azure.
2. Répétez ces étapes pour chaque application d'entreprise :

   > Vous devrez peut-être actualiser la page Applications d'entreprise pour voir les applications que vous avez précédemment ajoutées dans la liste.

   a. Accédez à la page Propriétés de l'application d'entreprise.

   b. Définissez **Affectation requise** sur **Non** (sauf si vous souhaitez configurer les affectations séparément).

   c. Accédez à la page d'authentification unique.

   d. Terminez la configuration SAML.

   e. Sélectionnez le bouton **Télécharger le fichier de métadonnées** et sélectionnez le fichier de métadonnées SAML que vous avez téléchargé pour le nœud d'administration correspondant.

   f. Une fois le fichier chargé, sélectionnez **Enregistrer** puis sélectionnez **X** pour fermer le volet. Vous êtes redirigé vers la page Configurer l'authentification unique avec SAML.

3. Suivez les étapes dans"Utiliser le mode sandbox" pour tester chaque application.

Créer des connexions de fournisseur de services (SP) dans PingFederate

Vous utilisez PingFederate pour créer une connexion de fournisseur de services (SP) pour chaque nœud d'administration de votre système. Pour accélérer le processus, vous importerez les métadonnées SAML depuis StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type d'authentification unique.
- Le **mode Sandbox** est sélectionné sur la page d'authentification unique dans Grid Manager. Voir "Utiliser le mode sandbox" .
- Vous disposez de l'*ID de connexion SP * pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau détaillé des nœuds d'administration sur la page d'authentification unique StorageGRID .
- Vous avez téléchargé les **métadonnées SAML** pour chaque nœud d'administration de votre système.
- Vous avez de l'expérience dans la création de connexions SP dans PingFederate Server.
- Vous avez lehttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Guide de référence de l'administrateur"^] pour le serveur PingFederate. La documentation de PingFederate fournit des instructions et des explications détaillées étape par étape.
- Vous avez le"Autorisation d'administrateur" pour le serveur PingFederate.

À propos de cette tâche

Ces instructions résument comment configurer PingFederate Server version 10.3 en tant que fournisseur SSO pour StorageGRID. Si vous utilisez une autre version de PingFederate, vous devrez peut-être adapter ces instructions. Reportez-vous à la documentation du serveur PingFederate pour obtenir des instructions détaillées pour votre version.

Prérequis complets dans PingFederate

Avant de pouvoir créer les connexions SP que vous utiliserez pour StorageGRID, vous devez effectuer les tâches préalables dans PingFederate. Vous utiliserez les informations de ces prérequis lorsque vous configurerez les connexions SP .

Créer un magasin de données

Si vous ne l'avez pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées lorsque"configuration de la fédération d'identité" dans StorageGRID.

- **Type** : Répertoire (LDAP)
- **Type LDAP** : Active Directory
- **Nom de l'attribut binaire** : saisissez **objectGUID** dans l'onglet Attributs binaires LDAP exactement comme indiqué.

Créer un validateur d'informations d'identification de mot de passe

Si vous ne l'avez pas déjà fait, créez un validateur d'informations d'identification de mot de passe.

- **Type** : Validateur d'informations d'identification de mot de passe de nom d'utilisateur LDAP
- **Magasin de données** : sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : saisissez les informations de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche** : sAMAccountName=${username}
- **Portée** : Sous-arbre

Créer une instance d'adaptateur IdP

Si vous ne l'avez pas déjà fait, créez une instance d'adaptateur IdP.

Étapes

1. Accédez à **Authentification** > **Intégration** > **Adaptateurs IdP**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **Adaptateur IdP de formulaire HTML**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à « Validateurs d'informations d'identification »**.
5. Sélectionnez levalidateur d'informations d'identification de mot de passe tu as créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si vous ne l'avez pas déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **Sécurité** > **Clés et certificats de signature et de déchiffrement**.
2. Créez ou importez le certificat de signature.

Créer une connexion SP dans PingFederate

Lorsque vous créez une connexion SP dans PingFederate, vous importez les métadonnées SAML que vous avez téléchargées à partir de StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient de nombreuses valeurs spécifiques dont vous avez besoin.

> Vous devez créer une connexion SP pour chaque nœud d'administration de votre système StorageGRID , afin que les utilisateurs puissent se connecter et se déconnecter en toute sécurité de n'importe quel nœud. Utilisez ces instructions pour créer la première connexion SP . Ensuite, allez àCréer des connexions SP supplémentaires pour créer toutes les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **Applications** > **Intégration** > *Connexions SP *.

2. Sélectionnez **Créer une connexion**.
3. Sélectionnez **Ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Profils SSO du navigateur** et **SAML 2.0** comme protocole.

Importer les métadonnées SP

Étapes

1. Dans l'onglet Importer des métadonnées, sélectionnez **Fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page d'authentification unique StorageGRID pour le nœud d'administration.
3. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

   L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion StorageGRID SP . (par exemple, 10.96.105.200-DC1-ADM1-105-200). L'URL de base est l'IP du nœud d'administration StorageGRID .

4. Sélectionnez **Suivant**.

Configurer l'authentification unique du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** et **IdP-initiated SLO**.
3. Sélectionnez **Suivant**.
4. Dans l'onglet Durée de vie de l'assertion, n'apportez aucune modification.
5. Dans l'onglet Création d'assertion, sélectionnez **Configurer la création d'assertion**.
   a. Dans l'onglet Mappage d'identité, sélectionnez **Standard**.
   b. Dans l'onglet Contrat d'attribut, utilisez **SAML_SUBJECT** comme contrat d'attribut et le format de nom non spécifié qui a été importé.
6. Pour prolonger le contrat, sélectionnez **Supprimer** pour supprimer le `urn:oid` , qui n'est pas utilisé.

Instance d'adaptateur de carte

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance de l'adaptateur, sélectionnez l'instance d'adaptateur tu as créé.
3. Dans l'onglet Méthode de mappage, sélectionnez **Récupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attribut et recherche d'utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Magasin de données, fournissez une description et sélectionnez l'optionmagasin de données tu as ajouté.
6. Dans l'onglet Recherche d'annuaire LDAP :
   - Saisissez le **DN de base**, qui doit correspondre exactement à la valeur que vous avez saisie dans StorageGRID pour le serveur LDAP.

- Pour la portée de la recherche, sélectionnez **Sous-arbre**.
- Pour la classe d'objet racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.

7. Dans l'onglet Types de codage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet Filtre LDAP, saisissez **sAMAccountName=${username}**.
9. Dans l'onglet Exécution du contrat d'attribut, sélectionnez **LDAP (attribut)** dans la liste déroulante Source et sélectionnez **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source de l'attribut.
11. Dans l'onglet Source d'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Consultez le résumé et sélectionnez **Terminé**.
13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet * Connexion SP * > * SSO du navigateur* > * Paramètres du protocole*, sélectionnez * Configurer les paramètres du protocole*.
2. Dans l'onglet URL du service consommateur d'assertions, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**POST** pour la liaison et `/api/saml-response` pour l'URL du point de terminaison).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées SAML StorageGRID (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du point de terminaison.
4. Dans l'onglet Liaisons SAML autorisées, décochez **ARTIFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont obligatoires.
5. Dans l'onglet Politique de signature, laissez les cases à cocher **Exiger que les demandes d'authentification soient signées** et **Toujours signer l'assertion** sélectionnées.
6. Dans l'onglet Politique de chiffrement, sélectionnez **Aucun**.
7. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Terminé** pour enregistrer les paramètres SSO du navigateur.

Configurer les informations d'identification

Étapes

1. Dans l'onglet Connexion SP , sélectionnez **Informations d'identification**.
2. Dans l'onglet Informations d'identification, sélectionnez **Configurer les informations d'identification**.
3. Sélectionnez lecertificat de signature vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **Gérer les paramètres de vérification de signature**.
   a. Dans l'onglet Modèle de confiance, sélectionnez **Non ancré**.
   b. Dans l'onglet Certificat de vérification de signature, vérifiez les informations du certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID .
5. Consultez les écrans récapitulatifs et sélectionnez **Enregistrer** pour enregistrer la connexion SP .

Créer des connexions SP supplémentaires

Vous pouvez copier la première connexion SP pour créer les connexions SP dont vous avez besoin pour chaque nœud d'administration de votre grille. Vous téléchargez de nouvelles métadonnées pour chaque copie.

> Les connexions SP pour différents nœuds d'administration utilisent des paramètres identiques, à l'exception de l'ID d'entité du partenaire, de l'URL de base, de l'ID de connexion, du nom de connexion, de la vérification de la signature et de l'URL de réponse SLO.

Étapes

1. Sélectionnez **Action** > **Copier** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Saisissez l'ID de connexion et le nom de connexion pour la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :
   a. Sélectionnez **Action** > **Mettre à jour avec les métadonnées**.
   b. Sélectionnez **Choisir un fichier** et téléchargez les métadonnées.
   c. Sélectionnez **Suivant**.
   d. Sélectionnez **Enregistrer**.
4. Résoudre l'erreur due à l'attribut inutilisé :
   a. Sélectionnez la nouvelle connexion.
   b. Sélectionnez **Configurer l'authentification unique du navigateur > Configurer la création d'assertions > Contrat d'attribut**.
   c. Supprimez l'entrée pour **urn:oid**.
   d. Sélectionnez **Enregistrer**.

Désactiver l'authentification 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 d'identité.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .

Étapes

1. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.

   La page d'authentification unique s'affiche.

2. Sélectionnez l'option **Désactivé**.
3. Sélectionnez **Enregistrer**.

   Un message d'avertissement apparaît indiquant que les utilisateurs locaux pourront désormais se connecter.

4. Sélectionnez **OK**.

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

Désactiver et réactiver temporairement l'authentification unique pour un nœud d'administration

Vous ne pourrez peut-être pas vous connecter au Grid Manager si le système d'authentification unique (SSO) tombe en panne. Dans ce cas, vous pouvez désactiver et réactiver temporairement SSO pour un nœud d'administration. Pour désactiver puis réactiver SSO, vous devez accéder à l'interpréteur de commandes du nœud.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous avez le `Passwords.txt` déposer.
- Vous connaissez le mot de passe de l'utilisateur root local.

À propos de cette tâche

Après avoir désactivé SSO pour un nœud d'administration, vous pouvez vous connecter au gestionnaire de grille en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID , vous devez utiliser l'interpréteur de commandes 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 des autres nœuds d'administration de la grille. La case à cocher **Activer SSO** sur la page Authentification unique dans le Gestionnaire de grille reste sélectionnée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

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

      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 SSO.

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

4. À partir d'un navigateur Web, accédez au gestionnaire de grille sur le même nœud d'administration.

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

5. Sign in avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.
6. Si vous avez désactivé temporairement SSO parce que vous deviez corriger la configuration SSO :
   a. Sélectionnez **CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**.
   b. Modifiez les paramètres SSO incorrects ou obsolètes.
   c. Sélectionnez **Enregistrer**.

      La sélection de **Enregistrer** sur la page d'authentification unique réactive automatiquement l'authentification unique pour l'ensemble de la grille.

7. Si vous avez désactivé temporairement SSO parce que vous aviez besoin d'accéder au Grid Manager pour une autre raison :

   a. Effectuez la ou les tâches que vous devez effectuer.
   b. Sélectionnez **Déconnexion** et fermez le gestionnaire de grille.
   c. Réactiver SSO sur le nœud d'administration. Vous pouvez effectuer l'une des étapes 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 SSO.

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

      - Redémarrer le nœud de grille : `reboot`

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

Informations sur le copyright

Informations sur les marques commerciales