Utilisez l'authentification unique (SSO)

StorageGRID software

NetApp
July 23, 2026

Sommaire

Utilisez l'authentification unique (SSO)

Découvrez l'authentification unique StorageGRID

Lorsque l'authentification unique (SSO) est activée, les utilisateurs peuvent accéder à Grid Manager, Tenant Manager, à l'API de gestion de Grid ou à l'API de gestion de locataires uniquement si leurs identifiants sont autorisés via le processus de connexion SSO mis en place par votre organisation. Les utilisateurs locaux ne peuvent pas se connecter à StorageGRID.

Le système StorageGRID prend en charge l'authentification unique (SSO) utilisant la norme Security Assertion Markup Language 2.0 (SAML 2.0).

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

Connectez-vous lorsque l'authentification unique est activée

Lorsque l'authentification unique (SSO) est activée 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 connexion StorageGRID s'affiche.

   - Si c'est la première fois que vous accédez à l'URL sur ce navigateur, un identifiant de compte vous sera demandé.
   - Si vous avez déjà accédé au Grid Manager ou au Tenant Manager, vous êtes invité à sélectionner un compte récent ou à saisir un identifiant de compte.

   > La page de connexion StorageGRID ne s'affiche pas lorsque vous saisissez l'URL complète d'un compte locataire (c'est-à-dire un domaine complet ou une adresse IP suivis de `/?accountId=20-digit-account-id`). Vous êtes immédiatement redirigé vers la page de connexion SSO de votre organisation, où vous pouvez Connectez-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 du compte** vide, saisissez **0** comme ID du compte ou sélectionnez **Grid Manager** s'il apparaît dans la liste des comptes récents.
   - Pour accéder au Gestionnaire de locataires, saisissez l'identifiant du compte locataire à 20 chiffres ou sélectionnez un locataire par son nom s'il apparaît dans la liste des comptes récents.
3. Sélectionnez **Sign in**

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

4. Connectez-vous avec vos identifiants SSO.

Si vos identifiants SSO sont corrects :

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 disposant des autorisations d'accès à 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 d'être un utilisateur existant appartenant à un groupe fédéré disposant des autorisations d'accès à StorageGRID.

5. Vous pouvez également accéder à d'autres Admin Nodes, ou au Grid Manager ou au Tenant Manager, si vous disposez des autorisations nécessaires.

   Vous n'avez pas besoin de saisir à nouveau vos identifiants SSO.

Déconnectez-vous lorsque l'authentification unique est activée

Lorsque l'authentification unique (SSO) est activée 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. Repérez le lien **Se déconnecter** dans le coin supérieur droit de l'interface utilisateur.
2. Sélectionnez **Se déconnecter**.

   La page de connexion StorageGRID s'affiche. Le menu déroulant **Comptes récents** est mis 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.

> Le tableau récapitule ce qui se passe lorsque vous vous déconnectez si vous utilisez une seule session de navigateur. Si vous êtes connecté à StorageGRID dans plusieurs sessions de navigateur, vous devez vous déconnecter de chaque session séparément.

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté(e) 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 Entra ID pour l'authentification unique (SSO), il peut s'écouler quelques minutes avant que vous ne soyez déconnecté de 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

Si vous êtes connecté à…	Et vous vous déconnectez de…	Vous êtes déconnecté(e) de…
Grid Manager et Tenant Manager	Gestionnaire de grille	Uniquement le Grid Manager. Vous devez également vous déconnecter du Tenant Manager pour vous déconnecter de l'authentification unique (SSO).

Exigences et considérations relatives à l'authentification unique StorageGRID

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

Exigences du fournisseur d'identité

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

- Service de fédération Active Directory (AD FS)
- Microsoft Entra ID
- PingFederate

Vous devez configurer la fédération d'identités 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'identités détermine le type de SSO que vous pouvez implémenter.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

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 doit utiliser la "Mise à jour KB3201845", ou une version supérieure.

Exigences supplémentaires

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

Considérations relatives à Entra ID

Si vous utilisez Entra ID comme type d'authentification unique (SSO) et que les utilisateurs ont des noms principaux d'utilisateur 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 rétablir 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 Grid Manager, au Tenant Manager, à l'API de gestion du Grid et à l'API de gestion des locataires. Lorsque vous configurez des approbations de parties de confiance (AD FS), des applications d'entreprise (Entra ID) ou des connexions de fournisseur de services (PingFederate) pour StorageGRID, vous utilisez le certificat du serveur comme certificat de signature pour les requêtes StorageGRID.

Si vous ne l'avez pas déjà "configuré un certificat personnalisé pour l'interface de gestion"fait, vous devriez le faire maintenant. Lorsque vous installez un certificat 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.

> Il est déconseillé d'utiliser le certificat serveur par défaut d'un nœud d'administration dans une approbation de partie de confiance, une application d'entreprise ou une connexion SP. En cas de défaillance du nœud et de sa récupération, un nouveau certificat serveur par défaut est généré. Avant de pouvoir vous connecter au nœud récupéré, vous devez mettre à jour l'approbation de partie de confiance, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

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

Exigences relatives aux ports

L'authentification unique (SSO) n'est pas disponible sur les ports restreints de Grid Manager ou de 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 niveau du pare-feu externe".

Confirmez que les utilisateurs fédérés peuvent se connecter à StorageGRID

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 tous les comptes locataires existants.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez déjà configuré la fédération d'identité.

Étapes

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

   Lorsque vous activez l'authentification unique (SSO), la source d'identité configurée dans le Tenant Manager est remplacée par la source d'identité configurée dans le Grid Manager. 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 du Grid Manager.

   a. Connectez-vous au Tenant Manager pour chaque compte locataire.
   b. Sélectionnez **Gestion des accès** > **Fédération d'identités**.
   c. Vérifiez que la case **Activer la fédération d'identités** n'est pas cochée.
   d. Si c'est le cas, vérifiez que les groupes fédérés éventuellement utilisés pour ce compte locataire ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.

2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
   a. Dans Grid Manager, 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 qu'il dispose de l'autorisation d'accès racine.
   c. Déconnexion.
   d. Vérifiez que vous pouvez vous reconnecter à Grid Manager en tant qu'utilisateur du groupe fédéré.

3. S'il existe des comptes locataires, vérifiez qu'un utilisateur fédéré disposant de l'autorisation d'accès Root peut se connecter :
   a. Dans le Gestionnaire de grille, sélectionnez **Locataires**.
   b. Sélectionnez le compte du locataire, puis sélectionnez **Actions** > **Modifier**.
   c. Dans l'onglet Saisir les détails, sélectionnez **Continuer**.
   d. Si la case **Utiliser votre propre source d'identité** est cochée, décochez-la et sélectionnez **Enregistrer**.

      La page du locataire s'affiche.

   e. Sélectionnez le compte locataire, sélectionnez **Se connecter**, puis connectez-vous au compte locataire en tant qu'utilisateur racine local.
   f. Dans le Gestionnaire de locataires, sélectionnez **Gestion des accès** > **Groupes**.
   g. Assurez-vous qu'au moins un groupe fédéré du Grid Manager s'est vu attribuer l'autorisation d'accès racine pour ce locataire.
   h. Déconnexion.
   i. Vérifiez 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"

- "Utilisez un compte locataire"

Configurer l'authentification unique (SSO) dans StorageGRID

Vous pouvez suivre l'assistant de configuration SSO et accéder au mode sandbox pour configurer et tester l'authentification unique (SSO) avant de l'activer pour tous les utilisateurs de StorageGRID. Une fois l'authentification unique (SSO) activée, vous pouvez revenir au mode sandbox si nécessaire pour modifier ou tester à nouveau la configuration.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".
- Vous avez configuré la fédération d'identités pour votre système StorageGRID.
- Pour le **type de service LDAP** de la fédération d'identités, vous avez sélectionné soit Active Directory, soit Entra ID, en fonction du fournisseur d'identités SSO que vous prévoyez d'utiliser.

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Service de fédération Active Directory (AD FS)	• Active Directory • Entra ID • PingFederate
Entra ID	Entra ID

À propos de cette tâche

Lorsque l'authentification unique (SSO) est activée et qu'un utilisateur tente de se connecter à un nœud d'administration, StorageGRID envoie une requête 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 requête d'authentification a réussi. Pour les requêtes réussies :

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Entra ID inclut un User Principal Name (UPN).

Pour permettre à StorageGRID (le fournisseur de services) et au fournisseur d'identité SSO de communiquer de manière sécurisée au sujet des demandes d'authentification des utilisateurs, vous devrez effectuer les tâches suivantes :

1. Configurez les paramètres dans StorageGRID.
2. Utilisez le logiciel du fournisseur d'identité SSO pour créer une approbation de partie de confiance (AD FS), une application d'entreprise (Entra ID) ou un fournisseur de services (PingFederate) pour chaque nœud d'administration.
3. Retournez à StorageGRID pour activer SSO.

Le mode bac à sable facilite les allers-retours de configuration et permet de tester tous vos paramètres avant d'activer l'authentification unique (SSO). Lorsque vous utilisez le mode bac à sable, les utilisateurs ne peuvent pas se connecter avec SSO.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**. La page d'authentification unique s'affiche.

   Si le bouton Configurer les paramètres SSO est désactivé, vérifiez que vous avez bien configuré le fournisseur d'identité comme source d'identité fédérée. Consultez "Exigences et considérations relatives à l'authentification unique".

2. Sélectionnez **Configurer les paramètres SSO**. La page « Fournir les détails du fournisseur d'identité » s'affiche.

Fournissez les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **type d'authentification unique** dans la liste déroulante.
2. Si vous avez sélectionné Active Directory comme type SSO, saisissez le **nom du service de fédération** pour le fournisseur d'identité, exactement comme il apparaît dans Active Directory Federation Service (AD FS).

   Pour trouver le nom du service de fédération, ouvrez le Gestionnaire de serveur Windows. Sélectionnez **Outils** > **Gestion d'AD FS**. Dans le menu Action, sélectionnez **Modifier les propriétés du service de fédération**. Le nom du service de fédération s'affiche dans le deuxième champ.

3. Spécifiez le certificat TLS qui sera utilisé pour sécuriser la connexion lorsque le fournisseur d'identité envoie des informations de configuration SSO en réponse aux requêtes 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 **CA Certificate**.

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

     Si vous modifiez le certificat d'autorité de certification, "Redémarrez le service mgmt-api sur les nœuds d'administration" effectuez immédiatement cette opération et testez la réussite de l'authentification unique (SSO) dans Grid Manager.

4. Sélectionnez **Continuer**. La page « Fournir l'identifiant de la partie de confiance » s'affiche.

Fournissez l’identifiant de la partie de confiance

1. Remplissez les champs de la page « Fournir l’identifiant de la partie de confiance » en fonction du type d’authentification unique (SSO) que vous avez sélectionné.

Active Directory

a. Spécifiez l'**identificateur de la partie de confiance** pour StorageGRID. Cette valeur détermine 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'en ajouter d'autres à l'avenir, saisissez `SG` ou `StorageGRID`.
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple, `SG-[HOSTNAME]`. Inclure cette chaîne génère un tableau affichant l'identifiant de la partie de confiance pour chaque nœud d'administration de la grille, en fonction du nom d'hôte du nœud.

   > Vous devez créer une relation de confiance avec une partie de confiance pour chaque nœud d'administration dans votre système StorageGRID. Le fait d'avoir une relation de confiance avec 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.

b. Sélectionnez **Enregistrer et passer en mode bac à sable**.

Entra ID

a. Dans la section Application d'entreprise, spécifiez le **nom de l'application d'entreprise** pour StorageGRID. Cette valeur détermine le nom que vous utilisez pour chaque application d'entreprise dans Entra ID.

   - Par exemple, si votre grille ne comporte qu'un seul nœud d'administration et que vous ne prévoyez pas d'en ajouter d'autres à l'avenir, saisissez `SG` ou `StorageGRID`.
   - Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple, `SG-[HOSTNAME]`. Inclure cette chaîne permet d'afficher un tableau présentant le nom de l'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. Le fait de 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.

b. Suivez les étapes décrites dans "Créez des applications d'entreprise dans Entra ID" pour créer une application d'entreprise pour chaque Admin Node répertorié dans le tableau.

c. À partir de Entra ID, copiez l'URL des métadonnées de fédération pour chaque application d'entreprise. Collez ensuite cette URL dans le champ **URL des métadonnées de fédération** correspondant dans StorageGRID.

d. Après avoir copié et collé une URL de métadonnées de fédération pour tous les Admin Nodes, sélectionnez **Enregistrer et entrer en mode sandbox**.

PingFederate

a. Dans la section Fournisseur de services (SP), spécifiez l'**ID de connexion SP** pour StorageGRID. Cette valeur détermine 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'en ajouter d'autres à l'avenir, saisissez `SG` ou `StorageGRID`.

- Si votre grille comprend plusieurs nœuds d'administration, incluez la chaîne `[HOSTNAME]` dans l'identifiant. Par exemple, `SG-[HOSTNAME]`. Inclure cette chaîne génère un tableau affichant 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 dans votre système StorageGRID. Le fait d'avoir 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.

b. Spécifiez l'URL des métadonnées de fédération pour chaque nœud d'administration dans le champ **Federation metadata URL**.

Utilisez le format suivant :

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

c. Sélectionnez **Enregistrer et passer en mode bac à sable**.

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

Après avoir enregistré la configuration et activé le mode sandbox, vous pouvez finaliser et tester la configuration pour le type de SSO que vous avez sélectionné.

StorageGRID peut rester en mode sandbox aussi longtemps que nécessaire. Cependant, seuls les utilisateurs fédérés et les utilisateurs locaux peuvent se connecter.

Active Directory

Étapes

1. Accédez à Active Directory Federation Services (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 Configurer SSO.

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

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

Entra ID

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. Connectez-vous au nœud.
   b. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML de ce nœud.
3. Accédez au portail Azure.
4. Suivez les étapes décrites "Créez des applications d'entreprise dans Entra ID" pour télécharger le fichier de métadonnées SAML pour chaque nœud d'administration dans son application d'entreprise Entra ID correspondante.

PingFederate

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. Connectez-vous au nœud.
   b. Sélectionnez **Configuration** > **Contrôle d'accès** > **Authentification unique**.
   c. Téléchargez et enregistrez les métadonnées SAML de ce nœud.
3. Accédez à PingFederate.
4. "Créez une ou plusieurs connexions de fournisseur de services (SP) pour StorageGRID". Utilisez l'ID de connexion SP pour chaque nœud d'administration (indiqué dans le tableau de la page Configurer l'authentification unique) 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 la configuration

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

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

Active Directory

Étapes

1. Sur la page Configurer SSO, repérez le lien à l'étape Tester la configuration de l'assistant.

   L'URL est dérivée de la valeur que vous avez saisie dans le champ **Federation service name**.

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 l'authentification unique (SSO) pour vous connecter à StorageGRID, sélectionnez **Se connecter à l'un des sites suivants**, sélectionnez l'identifiant de la partie de confiance pour votre nœud d'administration principal, puis sélectionnez **Se connecter**.
4. Saisissez votre nom d'utilisateur et votre mot de passe fédérés.
   - Si les opérations de connexion et de déconnexion SSO réussissent, un message de confirmation s'affiche.
   - En cas d'échec de l'authentification unique, 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.

Entra ID

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 confirmation s'affiche.
   - En cas d'échec de l'authentification unique, 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.

PingFederate

Étapes

1. Sur la page Configurer l'authentification unique (SSO), sélectionnez le premier lien du message relatif au 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 confirmation s'affiche.
   - En cas d'échec de l'authentification unique, 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 de chaque nœud d'administration de votre grille.

Si vous voyez un message « Page expirée », sélectionnez le bouton **Retour** de votre navigateur et soumettez à nouveau vos identifiants.

Activer l'authentification unique

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

Lorsque l'authentification unique (SSO) est activée, tous les utilisateurs doivent utiliser SSO pour accéder au Grid Manager, au Tenant Manager, 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. À l'étape de configuration de test de l'assistant de configuration SSO, sélectionnez **Activer SSO**.
2. Examinez le message d'avertissement et sélectionnez **Activer SSO**.

   L'authentification unique est désormais activée. La page d'authentification unique s'affiche et contient désormais les informations relatives à l'authentification unique que vous venez de configurer.

3. Pour modifier la configuration, sélectionnez **Modifier**.
4. Pour désactiver l'authentification unique, sélectionnez **Désactiver SSO**.

Si vous utilisez le portail Azure et que vous accédez à StorageGRID depuis le même ordinateur que celui utilisé pour accéder à Entra ID, assurez-vous que l'utilisateur du portail Azure est également un utilisateur StorageGRID autorisé (un utilisateur appartenant à 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 pour StorageGRID

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 partie de confiance à l'aide de commandes PowerShell, en important les métadonnées SAML depuis 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 de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous connaissez le 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 des détails des nœuds d'administration sur la page Configurer SSO de StorageGRID.

Vous devez créer une relation de confiance avec une partie de confiance pour chaque nœud d'administration dans votre système StorageGRID. Le fait d'avoir une relation de confiance avec 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 Administrators.
- Si vous créez manuellement la relation de confiance avec la 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'invite de commandes.

À propos de cette tâche

Ces instructions concernent Windows Server 2016 AD FS. Si vous utilisez une autre version d'AD FS, vous constaterez de légères différences dans la procédure. Consultez la documentation Microsoft AD FS si vous avez des questions.

Créer une relation d'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, cliquez avec le bouton droit sur l'icône PowerShell et sélectionnez **Exécuter en tant qu'administrateur**.
2. À l'invite de commandes PowerShell, saisissez 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 comme il apparaît sur la page d'authentification unique. Par exemple, `SG-DC1-ADM1`.
   - Pour *Admin_Node_FQDN*, saisissez le 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 devrez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP venait à changer.)
3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils** > **Gestion d'AD FS**.

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

   La liste des relations d'approbation de parties approuvées apparaît.
5. Ajoutez une stratégie de contrôle d'accès à l'approbation de partie de confiance nouvellement créée :
   a. Localisez la relation d'approbation de partie utilisatrice que vous venez de créer.
   b. Cliquez avec le bouton droit sur l'approbation, puis sélectionnez **Modifier la stratégie de contrôle**

d'accès.

c. Sélectionnez une politique de contrôle d'accès.

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

6. Ajoutez une politique d'émission de revendications à la nouvelle relation de confiance de partie utilisatrice :

a. Localisez la relation d'approbation de partie utilisatrice que vous venez de créer.

b. Cliquez avec le bouton droit sur la fiducie, puis sélectionnez **Modifier la politique d'émission des revendications**.

c. Sélectionnez **Ajouter une règle**.

d. Sur la page Sélectionner le 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, saisissez 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 du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

h. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.

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

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

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

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

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

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

9. Une fois que vous avez terminé, retournez sur StorageGRID "tester toutes les relations d'approbation des parties dépendantes" pour confirmer qu'ils sont correctement configurés.

Créez une relation de confiance de partie utilisatrice en important les métadonnées de fédération

Vous pouvez importer les valeurs de chaque approbation de partie de confiance en accédant aux métadonnées SAML de chaque Admin Node.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis sélectionnez **Gestion d'AD FS**.
2. Sous Actions, sélectionnez **Ajouter une fiducie de partie de confiance**.
3. Sur la page d'accueil, choisissez **Claims aware**, puis sélectionnez **Start**.
4. Sélectionnez **Importer les données relatives à la partie de confiance publiées en ligne ou sur un réseau local**.

5. Dans **Adresse des métadonnées de la fédération (nom de l'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour cet Admin Node :

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

   Pour *Admin_Node_FQDN*, saisissez le 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 devrez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP venait à changer.)

6. Terminez l'assistant de création de la fiducie de partie de confiance, enregistrez la fiducie 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 Grid Manager. Par exemple, `SG-DC1-ADM1`.

7. Ajouter une règle de revendication :
   a. Cliquez avec le bouton droit sur la fiducie, puis sélectionnez **Modifier la politique d'émission des revendications**.
   b. Sélectionnez **Ajouter une règle** :
   c. Sur la page Sélectionner le 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, saisissez 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 du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.
   g. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.
   h. Sélectionnez **Terminer**, puis sélectionnez **OK**.
8. Confirmez que les métadonnées ont été importées avec succès.
   a. Cliquez avec le bouton droit sur l'entité de confiance pour ouvrir ses propriétés.
   b. Vérifiez que les champs des onglets **Points de terminaison**, **Identifiants** et **Signature** sont renseignés.

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

9. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
10. Une fois que vous avez terminé, retournez sur StorageGRID et "tester toutes les relations d'approbation des parties dépendantes" pour confirmer qu'ils sont correctement configurés.

Créer manuellement une relation de confiance avec une partie utilisatrice

Si vous choisissez de ne pas importer les données pour les approbations de la partie dépendante, vous pouvez saisir les valeurs manuellement.

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis sélectionnez **Gestion d'AD FS**.
2. Sous Actions, sélectionnez **Ajouter une fiducie de partie de confiance**.
3. Sur la page d'accueil, choisissez **Claims aware**, puis sélectionnez **Start**.
4. Sélectionnez **Saisir manuellement les données relatives à la partie de confiance**, puis sélectionnez **Suivant**.
5. Terminez l'assistant de création de fiducie de partie de confiance :

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

      Par souci de cohérence, 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 Grid Manager. Par exemple, `SG-DC1-ADM1`.

   b. Ignorez l'étape de configuration d'un certificat de chiffrement de jeton facultatif.

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

   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`*, saisissez le nom de domaine complet pour le 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 devrez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP venait à changer.)

   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 comme 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 des réclamations 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 des revendications**.

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

   a. Sur la page Sélectionner le 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, saisissez 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 du tableau de mappage, saisissez **objectGUID** ou sélectionnez **User-Principal-Name**.

e. Dans la colonne Outgoing Claim Type du tableau de mappage, sélectionnez **Name ID** dans la liste déroulante.

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

7. Cliquez avec le bouton droit sur l'entité 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) à partir de ce Admin Node :

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

   Pour *`Admin_Node_FQDN`*, saisissez le 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 devrez mettre à jour ou recréer cette approbation de partie de confiance si cette adresse IP venait à changer.)

   a. Sélectionnez **OK**.

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

   a. Ajouter le certificat personnalisé :

      - Si vous avez téléchargé le certificat de gestion personnalisé sur StorageGRID, sélectionnez ce certificat.
      - Si vous ne possédez pas le 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.

      > L'utilisation du certificat par défaut du nœud d'administration (`server.crt` n'est pas recommandée. Si le nœud d'administration échoue, le certificat par défaut sera régénéré lors de la restauration du nœud, et vous devrez mettre à jour la relation de confiance de la partie dépendante.

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

      Les propriétés de la partie utilisatrice sont enregistrées et fermées.

10. Répétez ces étapes pour configurer une relation de confiance de partie utilisatrice pour tous les nœuds d'administration de votre système StorageGRID.
11. Une fois que vous avez terminé, retournez sur StorageGRID et "tester toutes les relations d'approbation

des parties dépendantes" pour confirmer qu'ils sont correctement configurés.

Créez des applications d'entreprise dans Entra ID pour StorageGRID

Vous utilisez Entra ID 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 **Entra ID** comme type de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous disposez du **nom de l'application d'entreprise** pour chaque nœud d'administration de votre système. Vous pouvez copier ces valeurs depuis le tableau des détails du nœud d'administration sur la page Configurer SSO.

> ⓘ Vous devez créer une application d'entreprise pour chaque nœud d'administration de votre système StorageGRID. Le fait de 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 Entra ID.
- Vous possédez un compte Entra ID avec un abonnement actif.
- Vous possédez l'un des rôles suivants dans le compte Entra ID : Global Administrator, Cloud Application Administrator, Application Administrator ou owner of the service principal.

Accéder à Entra ID

Étapes

1. Connectez-vous à l' "Portail Azure".
2. Accédez à "Entra ID".
3. Sélectionnez "Applications d'entreprise".

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

Pour enregistrer la configuration SSO d'Entra ID dans StorageGRID, vous devez utiliser Entra ID pour créer une application d'entreprise pour chaque Admin Node. Vous copierez les URL des métadonnées de fédération depuis Entra ID et les collerez dans les champs correspondants **Federation metadata URL** sur la page Configurer SSO.

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
   a. Dans le volet Applications d'entreprise d'Entra ID, 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 du tableau des détails du nœud d'administration sur la page Configurer SSO.

d. Laissez l'option **Intégrer toute autre application que vous ne trouvez pas dans la galerie (Hors galerie)** sélectionnée.

e. Sélectionnez **Create**.

f. Sélectionnez le lien **Get started** dans la **2. Set up single sign on** box, ou sélectionnez le lien **Single sign-on** dans la marge de gauche.

g. Sélectionnez la case **SAML**.

h. Copiez l'**App Federation Metadata Url**, que vous trouverez sous **Step 3 SAML Signing Certificate**.

i. Accédez à la page Configurer SSO, puis collez l'URL dans le champ **Federation metadata URL** qui correspond au **Enterprise application name** que vous avez utilisé.

2. Après avoir collé une URL de métadonnées de fédération pour chaque Admin Node et effectué toutes les autres modifications nécessaires à la configuration SSO, sélectionnez **Enregistrer** sur la page Configurer SSO.

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. Connectez-vous à StorageGRID depuis le nœud d'administration.

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

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

   d. Enregistrez le fichier, que vous téléchargerez ensuite dans Entra ID.

Téléversez les métadonnées SAML dans chaque application d'entreprise

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

Étapes

1. Retournez 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 à la liste.

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

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

   c. Accédez à la page d'authentification unique.

   d. Finalisez la configuration SAML.

   e. Sélectionnez le bouton **Téléverser un 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 **X** pour fermer le volet. Vous êtes renvoyé à la page Configurer l'authentification unique avec SAML.

3. "Tester chaque application".

Créez des connexions de fournisseur de services dans PingFederate pour StorageGRID

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 allez importer les métadonnées SAML depuis StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et vous avez sélectionné **Ping Federate** comme type de SSO.
- Vous avez "mode bac à sable activé" dans Grid Manager.
- Vous disposez de l'**ID de connexion SP** pour chaque nœud d'administration de votre système. Vous pouvez trouver ces valeurs dans le tableau des détails des nœuds d'administration sur la page Configurer le SSO.
- 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 le serveur PingFederate.
- Vous disposez du "Guide de référence de l'administrateur" pour le serveur PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous disposez du "Autorisation d'administrateur" pour le serveur PingFederate.

À propos de cette tâche

Ces instructions résument comment configurer le serveur PingFederate 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. Consultez la documentation du serveur PingFederate pour obtenir des instructions détaillées concernant votre version.

Effectuez les prérequis 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 issues de ces prérequis lors de la configuration des connexions SP.

Créer un magasin de données

Si ce n'est pas déjà fait, créez un magasin de données pour connecter PingFederate au serveur LDAP AD FS. Utilisez les valeurs que vous avez utilisées lors de "configuration de la fédération d'identités" dans StorageGRID.

- **Type** : Annuaire (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'identifiants de mot de passe

Si ce n'est pas déjà fait, créez un validateur d'identifiants de mot de passe.

- **Type** : Validateur d'identifiant nom d'utilisateur/mot de passe LDAP
- **Magasin de données** : Sélectionnez le magasin de données que vous avez créé.
- **Base de recherche** : Saisissez les informations provenant 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 **HTML Form IdP Adapter**.
4. Dans l'onglet Adaptateur IdP, sélectionnez **Ajouter une nouvelle ligne à 'Credential Validators'**.
5. Sélectionnez validateur d'identifiants de mot de passe que vous avez créé.
6. Dans l'onglet Attributs de l'adaptateur, sélectionnez l'attribut **username** pour **Pseudonym**.
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 **Security** > **Signing & Decryption Keys & Certificates**.
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 depuis 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 à Créer des connexions SP supplémentaires pour créer les connexions supplémentaires dont vous avez besoin.

Choisissez le type de connexion SP

Étapes

1. Accédez à **Applications** > **Integration** > **SP Connections**.
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 Import Metadata, sélectionnez **File**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé depuis la page Configure SSO pour le nœud d'administration.
3. Consultez le résumé des métadonnées et les informations fournies dans l'onglet Informations générales.

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

4. Sélectionnez **Next**.

Configurer l'authentification unique (SSO) du navigateur IdP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **Configurer le SSO du navigateur**.
2. Dans l'onglet Profils SAML, sélectionnez les options **SSO initié par le SP**, **SLO initié par le SP**, **SSO initié par l'IdP** et **SLO initié par l'IdP**.
3. Sélectionnez **Next**.
4. Dans l'onglet Durée de vie de l'assertion, ne modifiez rien.
5. Dans l'onglet Création d'assertions, sélectionnez **Configurer la création d'assertions**.
   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 retirer la `urn:oid`, qui n'est pas utilisée.

Mapper l'instance d'adaptateur

Étapes

1. Dans l'onglet Mappage de la source d'authentification, sélectionnez **Mapper une nouvelle instance d'adaptateur**.
2. Dans l'onglet Instance d'adaptateur, sélectionnez instance d'adaptateur que vous avez créée.
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'attributs et recherche d'utilisateurs, sélectionnez **Ajouter une source d'attributs**.
5. Dans l'onglet « Stockage de données », saisissez une description et sélectionnez l'élément magasin de données que vous avez ajouté.
6. Dans l'onglet Recherche dans l'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 l'étendue 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 d'encodage des attributs binaires 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 soit **objectGUID** ou **userPrincipalName** dans la liste déroulante Valeur.
10. Vérifiez puis enregistrez la source des attributs.
11. Dans l'onglet Source de l'attribut Failsave, sélectionnez **Annuler la transaction SSO**.
12. Vérifiez le récapitulatif et sélectionnez **Terminé**.
13. Sélectionnez **Terminé**.

Configurer les paramètres du protocole

Étapes

1. Dans l'onglet **SP Connection** > **Browser SSO** > **Protocol Settings**, sélectionnez **Configure Protocol Settings**.
2. Sur l'onglet URL du service de consommation d'assertion, acceptez les valeurs par défaut, qui ont été importées des métadonnées SAML de 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 des métadonnées SAML de 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 requis.
5. Dans l'onglet Signature Policy, laissez les cases à cocher **Require Authn Requests to be Signed** et **Always Sign Assertion** sélectionnées.
6. Dans l'onglet Encryption Policy, sélectionnez **None**.
7. Vérifiez le récapitulatif et sélectionnez **Terminé** pour enregistrer les paramètres du protocole.
8. Vérifiez le récapitulatif et sélectionnez **Terminé** pour enregistrer les paramètres Browser SSO.

Configurer les identifiants

Étapes

1. Dans l'onglet Connexion SP, sélectionnez **Informations d'identification**.
2. Dans l'onglet Identifiants, sélectionnez **Configurer les identifiants**.
3. Sélectionnez l'certificat de signature que vous avez créé ou importé.
4. Sélectionnez **Suivant** pour accéder à **Manage Signature Verification Settings**.
   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 de 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 nécessaires 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 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 la 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 **Next**.
   d. Sélectionnez **Enregistrer**.
4. Résolvez 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'attributs**.
   c. Supprimez l'entrée pour **urn:oid**.
   d. Sélectionnez **Enregistrer**.

Désactiver SSO dans StorageGRID

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'identités.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

Étapes

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

   La page d'authentification unique s'affiche.

2. Sélectionnez **Désactiver l'authentification unique**.
3. Sélectionnez **Oui**.

   Un message d'avertissement s'affiche, indiquant que les utilisateurs locaux pourront désormais se connecter.

La prochaine fois que vous vous connecterez à StorageGRID, la page de connexion StorageGRID s'affichera et vous devrez saisir le nom d'utilisateur et le mot de passe d'un utilisateur StorageGRID local ou fédéré.

Désactivez et réactivez temporairement l'authentification unique (SSO) pour un nœud d'administration StorageGRID

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

Avant de commencer

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

À propos de cette tâche

Après avoir désactivé l'authentification unique (SSO) pour un nœud d'administration, vous pouvez vous connecter au Grid Manager en tant qu'utilisateur root local. Pour sécuriser votre système StorageGRID, vous devez utiliser le shell de commande du nœud pour réactiver l'authentification unique (SSO) sur le nœud d'administration dès que vous vous déconnectez.

> La désactivation de l'authentification unique (SSO) pour un nœud d'administration n'affecte pas les paramètres SSO des autres nœuds d'administration de la grille. La case à cocher **Enable SSO** sur la page Single Sign-on dans le Grid Manager 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. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

   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. Depuis un navigateur Web, accédez au Grid Manager sur le même nœud d'administration.

   La page de connexion de Grid Manager s'affiche désormais 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 temporairement l'authentification unique (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 (SSO) pour l'ensemble de la grille.

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

a. Effectuez la ou les tâches que vous devez accomplir.
b. Sélectionnez **Se déconnecter**, puis fermez le Grid Manager.
c. Réactivez l'authentification unique (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 l'authentification unique (SSO).

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

- Redémarrez le nœud de grille : `reboot`

8. Depuis un navigateur Web, accédez au Grid Manager depuis le même nœud d'administration.
9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos identifiants SSO pour accéder au Grid Manager.