



Utilisation de la connexion unique (SSO)

StorageGRID software

NetApp

February 12, 2026

Sommaire

Utilisation de la connexion unique (SSO)	1
Comment fonctionne l'authentification unique	1
Connectez-vous lorsque SSO est activé	1
Déconnectez-vous lorsque SSO est activé	2
Exigences et considérations relatives à l'authentification unique (SSO)	3
Exigences du fournisseur d'identités	3
Configuration requise pour le certificat de serveur	4
Configuration requise pour les ports	4
Confirmez que les utilisateurs fédérés peuvent se connecter	4
Configurer SSO	6
Accéder à l'assistant	7
Fournir les détails du fournisseur d'identité	7
Fournir l'identifiant de la partie de confiance	7
Configurez les approbations des parties utilisatrices, les applications d'entreprise ou les connexions	
SP	9
Configuration de test	10
Activez l'authentification unique	12
Créer des fiducies de tiers de confiance dans AD FS	12
Créez une confiance en vous appuyant sur Windows PowerShell	13
Créez une confiance de partie de confiance en vous important des métadonnées de fédération	14
Créer une confiance de partie de confiance manuellement	15
Créer des applications d'entreprise dans Entra ID	17
Accès Entra ID	18
Créez des applications d'entreprise et enregistrez la configuration SSO de StorageGRID	18
Téléchargez les métadonnées SAML pour chaque nœud d'administration	19
Téléchargez les métadonnées SAML sur chaque application d'entreprise	19
Créer des connexions de fournisseur de services (SP) dans PingFederate	19
Remplir les conditions préalables dans PingFederate	20
Créer une connexion SP dans PingFederate	21
Désactiver SSO	24
Désactiver et réactiver temporairement SSO pour un nœud d'administration	24

Utilisation de la connexion unique (SSO)

Comment fonctionne l'authentification unique

Lorsque l'authentification unique (SSO) est activée, les utilisateurs peuvent accéder à Grid Manager, Tenant Manager, Grid Management API ou Tenant Management API uniquement 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.

Le système StorageGRID prend en charge la fonctionnalité SSO (Single Sign-on) en utilisant la 2.0 norme SAML 2.0 (Security assertion Markup Language).

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

Connectez-vous lorsque SSO est activé

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

Étapes

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

La page de connexion StorageGRID s'affiche.

- 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 gestionnaire de grille ou au gestionnaire de locataires, vous êtes invité à sélectionner un compte récent ou à saisir un identifiant de compte.



La page de connexion StorageGRID n'apparaît pas lorsque vous entrez l'URL complète d'un compte de locataire (c'est-à-dire un nom de domaine complet ou une adresse IP suivie 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 pouvez [Connectez-vous à l'aide de vos identifiants SSO](#).

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

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

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

Si vos informations d'identification SSO sont correctes :

- a. Le fournisseur d'identités fournit une réponse d'authentification à StorageGRID.
- b. StorageGRID valide la réponse d'authentification.
- c. Si la réponse est valide et que vous appartenez à un groupe fédéré avec des autorisations d'accès StorageGRID, vous êtes connecté au Gestionnaire de grille ou au Gestionnaire des locataires, selon le compte que vous avez sélectionné.



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

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

Il n'est pas nécessaire de saisir à nouveau vos informations d'identification SSO.

Déconnectez-vous lorsque SSO est activé

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

Étapes

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

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



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

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté de...
Grid Manager sur un ou plusieurs nœuds d'administration	Grid Manager sur n'importe quel nœud d'administration	Grid Manager sur tous les nœuds d'administration Remarque : si vous utilisez Entra ID pour l'authentification unique (SSO), 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

Si vous êtes connecté à...	Et vous vous déconnectez de...	Vous êtes déconnecté de...
Grid Manager et tenant Manager	Gestionnaire de grille	Le Grid Manager uniquement. Vous devez également vous déconnecter du tenant Manager pour vous déconnecter de SSO.

Exigences et considérations relatives à l'authentification unique (SSO)

Avant d'activer la signature unique (SSO) pour un système StorageGRID, consultez les conditions requises et les considérations à prendre en compte.

Exigences du fournisseur d'identités

StorageGRID prend en charge les fournisseurs d'identités SSO suivants :

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

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

Type de service LDAP configuré	Options pour le fournisseur d'identité SSO
Active Directory	<ul style="list-style-type: none"> • Active Directory • ID d'entrée • PingFederate
ID d'entrée	ID d'entrée

Exigences AD FS

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

- Système de fichiers AD Windows Server 2022
- Système de fichiers AD Windows Server 2019
- Système de fichiers AD Windows Server 2016



Windows Server 2016 doit utiliser le "[Mise à jour KB3201845](#)" ou une version ultérieure.

Supplémentaires requise

- TLS (transport Layer Security) 1.2 ou 1.3

- Microsoft .NET Framework, version 3.5.1 ou supérieure

Considérations pour Entra ID

Si vous utilisez Entra ID 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.

Configuration requise pour le certificat 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 (Entra ID) 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 ["configuré un certificat personnalisé pour l'interface de gestion"](#) fait, vous devriez le faire maintenant. Lorsque vous installez un certificat de serveur personnalisé, il est utilisé pour tous les nœuds d'administration et vous pouvez l'utiliser dans toutes les approbations de tiers StorageGRID, les applications d'entreprise ou les connexions SP.



Il n'est pas recommandé d'utiliser le certificat de serveur par défaut d'un nœud d'administration dans une connexion de confiance, d'une application d'entreprise ou d'un SP. Si le nœud échoue et que vous le récupérez, un nouveau certificat de serveur par défaut est généré. Avant de pouvoir vous connecter au nœud restauré, vous devez mettre à jour la confiance de la partie utilisatrices, l'application d'entreprise ou la connexion SP avec le nouveau certificat.

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

Configuration requise pour les ports

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique. Voir ["Contrôler l'accès au niveau du pare-feu externe"](#).

Confirmez que les utilisateurs fédérés peuvent se connecter

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

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 des identités.

Étapes

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



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

- a. Connectez-vous au Gestionnaire de locataires pour chaque compte de locataire.
 - b. Sélectionnez **Gestion des accès > Fédération d'identité**.
 - c. Vérifiez que la case **Activer la fédération d'identité** n'est pas cochée.
 - d. Si c'est le cas, vérifiez que tous les groupes fédérés pouvant être utilisés pour ce compte de tenant ne sont plus nécessaires, décochez la case et sélectionnez **Enregistrer**.
2. Vérifiez qu'un utilisateur fédéré peut accéder au Grid Manager :
 - a. Depuis Grid Manager, sélectionnez **Configuration > Contrôle d'accès > Groupes d'administrateurs**.
 - b. Assurez-vous qu'au moins un groupe fédéré a été importé du référentiel d'identité Active Directory et qu'il a reçu l'autorisation d'accès racine.
 - c. Se déconnecter.
 - d. Confirmez que vous pouvez vous reconnecter au Grid Manager en tant qu'utilisateur dans le groupe fédéré.
 3. S'il existe des comptes de tenant existants, confirmez qu'un utilisateur fédéré disposant d'une autorisation d'accès racine peut se connecter :
 - a. Dans 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 **utiliser le propre référentiel d'identité** est cochée, décochez la case et sélectionnez **Enregistrer**.

La page tenant s'affiche.

 - e. Sélectionnez le compte de tenant, sélectionnez **connexion** et connectez-vous au compte de tenant en tant qu'utilisateur racine local.
 - f. Depuis le gestionnaire de locataires, sélectionnez **Gestion des accès > Groupes**.
 - g. Assurez-vous qu'au moins un groupe fédéré du Grid Manager a reçu l'autorisation d'accès racine pour ce locataire.
 - h. Se déconnecter.
 - i. Confirmez que vous pouvez vous reconnecter au locataire en tant qu'utilisateur dans le groupe fédéré.

Informations associées

- ["Configuration requise et considérations pour l'authentification unique"](#)
- ["Gérez les groupes d'administration"](#)
- ["Utilisez un compte de locataire"](#)

Configurer SSO

Vous pouvez suivre l'assistant de configuration de l'authentification unique (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 activée, vous pouvez revenir au mode sandbox si nécessaire pour modifier ou retester 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 racine"](#).
- Vous avez configuré la fédération des identités pour votre système StorageGRID.
- Pour le type de service LDAP de fédération d'identité, vous avez sélectionné Active Directory ou Entra ID, en fonction du fournisseur d'identité 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)	<ul style="list-style-type: none">• Active Directory• ID d'entrée• PingFederate
ID d'entrée	ID d'entrée

Description de la tâche

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

- La réponse d'Active Directory ou PingFederate inclut un identifiant unique universel (UUID) pour l'utilisateur.
- La réponse d'Entra ID 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 effectuer ces tâches :

1. Configurer 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. Revenez 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 à l'assistant

Étapes

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



Si le bouton Configurer les paramètres SSO est désactivé, confirmez que vous avez configuré le fournisseur d'identité comme source d'identité fédérée. "[Configuration requise et considérations pour l'authentification unique](#)".

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

Fournir les détails du fournisseur d'identité

Étapes

1. Sélectionnez le **SSO type** 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 tel qu'il apparaît dans Active Directory Federation Service (AD FS).



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

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

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

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



Si vous modifiez le certificat de l'autorité de certification, testez immédiatement "[Redémarrez le service mgmt-api sur les nœuds d'administration](#)" et vérifiez si une authentification unique réussie est présente dans le gestionnaire de grille.

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

Fournir 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 SSO que vous avez sélectionné.

Active Directory

- a. 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 grid 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] . L'inclusion de cette chaîne génère un tableau qui affiche l'identifiant de la partie de confiance pour chaque nœud d'administration dans la grille, en fonction du nom d'hôte du nœud.



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

- b. Sélectionnez **Enregistrer et entrez en mode sandbox**.

ID d'entrée

- a. 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 Entra ID.
 - Par exemple, si votre grid 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] . L'inclusion de cette chaîne 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. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

- b. Suivez les étapes dans "[Créer des applications d'entreprise dans Entra ID](#)" pour créer une application d'entreprise pour chaque nœud d'administration répertorié dans le tableau.
- c. À partir d'Entra ID, copiez l'URL des métadonnées de la fédération pour chaque application d'entreprise. Ensuite, collez cette URL dans le champ **URL des métadonnées de la fédération** correspondant dans StorageGRID.
- d. Après avoir copié et collé une URL de métadonnées de fédération pour tous les nœuds d'administration, sélectionnez **Enregistrer et passer en mode sandbox**.

PingFederate

- a. Dans la section SP (Service Provider), 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 grid 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] . L'inclusion de cette chaîne 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. La présence d'une connexion SP pour chaque nœud d'administration permet aux utilisateurs de se connecter et de se déconnecter en toute sécurité à n'importe quel nœud d'administration.

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

Utilisez le format suivant :

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

- Sélectionnez **Enregistrer et entrez en mode sandbox**.

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

Après avoir enregistré la configuration et être entré en mode sandbox, vous pouvez terminer et tester la configuration pour le type 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 confiance pour chaque nœud d'administration indiqué dans le tableau.

Pour obtenir des instructions, rendez-vous sur "[Créer des fiducies de tiers de confiance dans AD FS](#)".

ID d'entrée

Étapes

1. Dans la page Single Sign-on du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
 - a. Connectez-vous 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 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. Dans la page Single Sign-on du nœud d'administration auquel vous êtes actuellement connecté, sélectionnez le bouton pour télécharger et enregistrer les métadonnées SAML.
2. Ensuite, pour tout autre nœud d'administration de votre grid, répétez la procédure suivante :
 - a. Connectez-vous 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. "[Créez une ou plusieurs connexions de fournisseur de services pour StorageGRID](#)". Utilisez l'ID de connexion SP pour chaque nœud d'administration (affiché dans le tableau de la page Configurer SSO) et les métadonnées SAML que vous avez téléchargées pour ce nœud d'administration.

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

Configuration de test

Avant d'appliquer 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. À partir de la page Configurer SSO, recherchez le lien à l'étape Configuration de test de l'assistant.

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-collez l'URL dans un navigateur pour accéder à la page de connexion de votre fournisseur d'identités.
3. Pour confirmer que vous pouvez utiliser l'authentification SSO pour vous connecter à StorageGRID, sélectionnez **connexion à l'un des sites suivants**, sélectionnez l'identifiant de partie de confiance pour votre nœud d'administration principal et sélectionnez **connexion**.
4. Entrez votre nom d'utilisateur et votre mot de passe fédérés.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
5. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

ID d'entrée

Étapes

1. Accédez à la page d'identification unique sur le portail Azure.
2. Sélectionnez **Tester cette application**.
3. Entrez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
4. Répétez ces étapes pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

PingFederate

Étapes

1. Depuis la page Configurer SSO, sélectionnez le premier lien dans le message du mode Sandbox.

Sélectionnez et testez un lien à la fois.

2. Entrez les informations d'identification d'un utilisateur fédéré.
 - Si les opérations de connexion SSO et de déconnexion ont réussi, un message de réussite s'affiche.
 - Si l'opération SSO échoue, un message d'erreur s'affiche. Corrigez le problème, effacez les cookies du navigateur et réessayez.
3. Cliquez sur le lien suivant pour vérifier la connexion SSO pour chaque nœud d'administration de votre grille.

Si un message page expirée s'affiche, sélectionnez le bouton **Retour** dans votre navigateur et

soumettez à nouveau vos informations d'identification.

Activez l'authentification unique

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



Lorsque l'authentification SSO est activée, tous les utilisateurs doivent utiliser l'authentification SSO pour accéder au Grid Manager, au tenant Manager, à l'API Grid Management et à l'API tenant Management. Les utilisateurs locaux ne peuvent plus accéder à StorageGRID.

Étapes

1. À partir de l'étape de configuration de test de l'assistant de configuration SSO, sélectionnez **Activer SSO**.
2. Consultez le message d'avertissement et sélectionnez **Activer SSO**.

L'authentification unique est désormais activée. La page d'authentification unique s'affiche et inclut désormais les détails du SSO que vous venez de configurer.

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



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 Entra ID, 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 fiducies de tiers de confiance dans AD FS

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

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **AD FS** comme type SSO.
- Tu as "[entré en mode bac à sable](#)" dans Grid Manager.
- 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 Configurer SSO de StorageGRID .



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

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

Description de la 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. Pour toute question, consultez la documentation Microsoft AD FS.

Créez une confiance en vous appuyant sur Windows PowerShell

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

Étapes

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

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

- Pour *Admin_Node_Identifier*, entrez l'identificateur de partie utilisatrice pour le nœud Admin, exactement comme il apparaît sur la page Single Sign-On. Par exemple SG-DC1-ADM1, .
- Pour *Admin_Node_FQDN*, entrez le nom de domaine complet pour le même nœud d'administration. (Si nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

3. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils > AD FS Management**.

L'outil de gestion AD FS s'affiche.

4. Sélectionnez **AD FS > confiance de la partie de confiance**.

La liste des fiduciaires de tiers de confiance s'affiche.

5. Ajouter une stratégie de contrôle d'accès à la confiance de la partie qui vient d'être créée :
 - a. Recherchez la confiance de la partie de confiance que vous venez de créer.
 - b. Cliquez avec le bouton droit de la souris sur la confiance et sélectionnez **Modifier la stratégie de contrôle d'accès**.
 - c. Sélectionnez une stratégie de contrôle d'accès.
 - d. Sélectionnez **appliquer**, puis **OK**
6. Ajouter une politique d'émission de demandes de remboursement à la nouvelle fiducie de compte comptant :

- a. Recherchez la confiance de la partie de confiance que vous venez de créer.
- b. Cliquez avec le bouton droit de la souris sur la fiducie et sélectionnez **Modifier la politique d'émission des sinistres**.
- c. Sélectionnez **Ajouter règle**.
- d. Sur la page Sélectionner un modèle de règle, sélectionnez **Envoyer attributs LDAP en tant que revendications** dans la liste et sélectionnez **Suivant**.
- e. Sur la page configurer la règle, entrez un nom d'affichage pour cette règle.

Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

- f. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - g. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.
 - h. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
 - i. Sélectionnez **Terminer** et sélectionnez **OK**.
7. Confirmez que les métadonnées ont été importées avec succès.
- a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
 - b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.
- Si les métadonnées sont manquantes, vérifiez que l'adresse des métadonnées de fédération est correcte ou entrez les valeurs manuellement.
8. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
9. Lorsque vous avez terminé, revenez à StorageGRID et "[tester toutes les fiducies des parties utilisatrices](#)" pour confirmer qu'ils sont correctement configurés.

Créez une confiance de partie de confiance en vous important des métadonnées de fédération

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

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.
3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Importer les données concernant la partie de confiance publiée en ligne ou sur un réseau local**.
5. Dans **adresse de métadonnées de fédération (nom d'hôte ou URL)**, saisissez l'emplacement des métadonnées SAML pour ce noeud d'administration :

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

Pour `Admin_Node_FQDN`, entrez le nom de domaine complet pour le même noeud d'administration. (Si

nécessaire, vous pouvez utiliser l'adresse IP du nœud à la place. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

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



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

7. Ajouter une règle de sinistre :

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

Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.

- e. Pour le magasin d'attributs, sélectionnez **Active Directory**.
- f. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.
- g. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.
- h. Sélectionnez **Terminer** et sélectionnez **OK**.

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

- a. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
- b. Vérifiez que les champs des onglets **Endpoints**, **identificateurs** et **Signature** sont renseignés.

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

9. Répétez ces étapes pour configurer une confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
10. Lorsque vous avez terminé, revenez à StorageGRID et "[tester toutes les fiducies des parties utilisatrices](#)" pour confirmer qu'ils sont correctement configurés.

Créer une confiance de partie de confiance manuellement

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

Étapes

1. Dans le Gestionnaire de serveur Windows, sélectionnez **Outils**, puis **AD FS Management**.
2. Sous actions, sélectionnez **Ajouter la confiance de la partie de confiance**.

3. Sur la page de bienvenue, choisissez **revendications Aware** et sélectionnez **Démarrer**.
4. Sélectionnez **Entrez les données relatives à la partie de confiance manuellement** et sélectionnez **Suivant**.
5. Suivez l'assistant confiance de la partie de confiance :

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

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

- b. Ignorez l'étape pour configurer un certificat de chiffrement de jeton facultatif.
- c. Sur la page configurer l'URL, cochez la case **Activer la prise en charge du protocole SAML 2.0 WebSSO**.
- d. Saisissez l'URL du nœud final 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. Toutefois, si vous saisissez une adresse IP ici, sachez que vous devez mettre à jour ou recréer cette confiance de partie de confiance si cette adresse IP change.)

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

Admin_Node_Identifier

Pour *Admin_Node_Identifier*, entrez l'identificateur de partie utilisatrice pour le nœud Admin, exactement comme il apparaît sur la page Single Sign-On. Par exemple SG-DC1-ADM1, .

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

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



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

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

Par exemple, **objectGUID à ID de nom** ou **UPN à ID de nom**.
 - c. Pour le magasin d'attributs, sélectionnez **Active Directory**.
 - d. Dans la colonne attribut LDAP de la table mappage, tapez **objectGUID** ou sélectionnez **User-principal-Name**.
 - e. Dans la colonne Type de demande sortante de la table mappage, sélectionnez **Nom ID** dans la liste déroulante.

- f. Sélectionnez **Terminer** et sélectionnez **OK**.
7. Cliquez avec le bouton droit de la souris sur la confiance de la partie utilisatrices pour ouvrir ses propriétés.
8. Dans l'onglet **Endpoints**, configurez le noeud final pour une déconnexion unique (SLO) :

- a. Sélectionnez **Ajouter SAML**.
- b. Sélectionnez **Endpoint Type > SAML Logout**.
- c. Sélectionnez **Redirect > Redirect**.
- d. Dans le champ **URL de confiance**, entrez l'URL utilisée pour la déconnexion unique (SLO) à partir de ce noeud d'administration :

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

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

- a. Sélectionnez **OK**.
9. Dans l'onglet **Signature**, spécifiez le certificat de signature pour la fiducie de cette partie de confiance :
 - a. Ajouter le certificat personnalisé :
 - Si vous disposez du certificat de gestion personnalisé que vous avez téléchargé vers StorageGRID, sélectionnez ce certificat.
 - Si vous ne disposez pas du certificat personnalisé, connectez-vous au nœud d'administration, accédez au `/var/local/mgmt-api` répertoire du nœud d'administration et ajoutez le `custom-server.crt` fichier de certificat.



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 lorsque vous restaurerez le nœud et vous devrez mettre à jour la confiance de l'organisme 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 confiance de tiers pour tous les nœuds d'administration de votre système StorageGRID.
11. Lorsque vous avez terminé, revenez à StorageGRID et "[tester toutes les fiducies des parties utilisatrices](#)" pour confirmer qu'ils sont correctement configurés.

Créer des applications d'entreprise dans Entra ID

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 d'authentification unique.

- Tu as "[entré en mode bac à sable](#)" 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 à partir du 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. La présence d'une application d'entreprise pour chaque nœud d'administration garantit que les utilisateurs peuvent se connecter et se déconnecter en toute sécurité à n'importe quel nœud d'administration.

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

Accès Entra ID

Étapes

1. Connectez-vous au "[Portail Azure](#)".
2. Accéder à "[ID d'entrée](#)".
3. Sélectionnez "[Les applications d'entreprise](#)".

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

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

Étapes

1. Répétez les étapes suivantes pour chaque nœud d'administration.
 - a. Dans le volet Applications Entra ID Enterprise, sélectionnez **Nouvelle application**.
 - b. Sélectionnez **Créez 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 Configurer SSO.
 - 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 **Get Started** dans **2. Configurez la case Single Sign On** ou sélectionnez le lien **Single Sign-on** dans la marge de gauche.
 - g. Sélectionnez la case **SAML**.
 - h. Copiez l'URL **App Federation Metadata URL**, que vous trouverez sous **étape 3 SAML Signing Certificate**.
 - i. Accédez à la page Configurer SSO 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 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 à partir du 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 dans Entra ID.

Téléchargez les métadonnées SAML sur 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. Revenez au portail Azure.
2. Répétez cette procédure 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 séparément les affectations).
 - c. Accédez à la page Single Sign-on.
 - 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 **X** pour fermer le volet. Vous revenez à la page configurer un Single Sign-on avec SAML.
3. "[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 importez les métadonnées SAML à partir de StorageGRID.

Avant de commencer

- Vous avez configuré l'authentification unique pour StorageGRID et sélectionné **Ping Federate** comme type SSO.
- Tu as ["entré en mode bac à sable"](#) 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 détaillé des nœuds d'administration sur la page Configurer SSO.
- Vous avez téléchargé les métadonnées **SAML** pour chaque nœud d'administration de votre système.
- Vous avez l'expérience de la création de connexions SP dans PingFederate Server.
- Vous avez le ["Guide de référence de l'administrateur"](#) serveur for PingFederate. La documentation PingFederate fournit des instructions détaillées étape par étape et des explications.
- Vous avez le ["Autorisation d'administrateur"](#) pour le serveur PingFederate.

Description de la 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 sur votre version.

Remplir les conditions préalables 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 lors de la configuration des connexions du processeur de service.

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 ["configuration de la fédération des identités"](#) dans StorageGRID.

- **Type:** Répertoire (LDAP)
- **Type LDAP :** Active Directory
- **Nom d'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 ce n'est pas déjà fait, créez un validateur pour les informations d'identification du mot de passe.

- **Type:** LDAP Nom d'utilisateur Mot de passe validateur des informations d'identification
- **Magasin de données :** sélectionnez le magasin de données que vous avez créé.
- **Base de recherche :** saisissez des informations à partir de LDAP (par exemple, DC=saml,DC=sgws).
- **Filtre de recherche :** sAMAccountName=\${username}
- **Portée :** sous-arbre

Créer une instance d'adaptateur IDP

Si ce n'est déjà fait, créez une instance de carte IDP.

Étapes

1. Accédez à **Authentication > Integration > IDP Adapters**.
2. Sélectionnez **Créer une nouvelle instance**.
3. Dans l'onglet Type, sélectionnez **HTML Form IDP adapter**.
4. Dans l'onglet carte IDP, sélectionnez **Ajouter une nouvelle ligne à 'Validators Credentials'**.
5. Sélectionnez le [validateur des informations d'identification du mot de passe](#) tu as créé.
6. Dans l'onglet attributs de l'adaptateur, sélectionnez l'attribut **nom d'utilisateur** pour **pseudonyme**.
7. Sélectionnez **Enregistrer**.

Créer ou importer un certificat de signature

Si ce n'est déjà fait, créez ou importez le certificat de signature.

Étapes

1. Accédez à **sécurité > clés 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 téléchargées depuis StorageGRID pour le nœud d'administration. Le fichier de métadonnées contient la plupart des 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 en toute sécurité à n'importe quel nœud et en dehors. Suivez ces instructions pour créer la première connexion du processeur de service. Ensuite, accédez 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 > intégration > connexions SP**.
2. Sélectionnez **Créer connexion**.
3. Sélectionnez **ne pas utiliser de modèle pour cette connexion**.
4. Sélectionnez **Browser SSO Profiles** et **SAML 2.0** comme protocole.

Importation des métadonnées SP

Étapes

1. Dans l'onglet Importer les métadonnées, sélectionnez **fichier**.
2. Choisissez le fichier de métadonnées SAML que vous avez téléchargé à partir de la page Configurer SSO pour le nœud d'administration.
3. Passez en revue le résumé des métadonnées et les informations fournies dans l'onglet Infos générales.

L'ID d'entité du partenaire et le nom de connexion sont définis sur l'ID de connexion SP 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 **Suivant**.

Configurer SSO du navigateur IDP

Étapes

1. Dans l'onglet SSO du navigateur, sélectionnez **configurer SSO du navigateur**.
2. Dans l'onglet des profils SAML, sélectionnez les options **SSO** initiée par le SP, **SLO initial du SP**, **SSO initié par l'IDP** et **SLO** lancé par l'IDP.
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.

Mapper l'instance de l'adaptateur

Étapes

1. Dans l'onglet mappage de la source d'authentification, sélectionnez **mappage d'une nouvelle instance de carte**.
2. Dans l'onglet instance d'adaptateur, sélectionnez le [instance d'adaptateur](#) que vous avez créé.
3. Dans l'onglet méthode de mappage, sélectionnez **recupérer des attributs supplémentaires à partir d'un magasin de données**.
4. Dans l'onglet Source d'attribut et recherche utilisateur, sélectionnez **Ajouter une source d'attribut**.
5. Dans l'onglet Data Store, indiquez une description et sélectionnez le [magasin de données](#) que vous avez ajouté.
6. Dans l'onglet LDAP Directory Search :
 - 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'objets racine, recherchez et ajoutez l'un de ces attributs : **objectGUID** ou **userPrincipalName**.
7. Dans l'onglet types d'encodage d'attribut binaire LDAP, sélectionnez **Base64** pour l'attribut **objectGUID**.
8. Dans l'onglet filtre LDAP, entrez **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 et enregistrez la source d'attribut.
11. Dans l'onglet Source de l'attribut FailSave, sélectionnez **abandonner la transaction SSO**.
12. Passez en revue le résumé et sélectionnez **Done**.
13. Sélectionnez **Done**.

Configurer les paramètres de protocole

Étapes

1. Dans l'onglet **connexion SP > connexion du navigateur SSO > Paramètres de protocole**, sélectionnez **configurer les paramètres de protocole**.
2. Dans l'onglet URL du service d'utilisateur d'assertion, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées StorageGRID SAML (**POST** pour la liaison et `/api/saml-response` pour l'URL du point final).
3. Dans l'onglet URL du service SLO, acceptez les valeurs par défaut, qui ont été importées à partir des métadonnées StorageGRID SAML (**REDIRECT** pour la liaison et `/api/saml-logout` pour l'URL du noeud final).
4. Dans l'onglet Allowable SAML Bindings, désactivez **ARTEFACT** et **SOAP**. Seuls **POST** et **REDIRECT** sont requis.
5. Dans l'onglet Signature Policy, laissez les cases **exiger la signature des requêtes Authn** et **toujours signer l'assertion** cochées.
6. Dans l'onglet Stratégie de cryptage, sélectionnez **aucun**.
7. Consultez le résumé et sélectionnez **Done** pour enregistrer les paramètres du protocole.
8. Consultez le résumé et sélectionnez **Done** 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 [signature du certificat](#) 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 de certificat de signature, qui ont été importées à partir des métadonnées SAML StorageGRID.
5. Passez en revue les écrans de résumé et sélectionnez **Enregistrer** pour enregistrer la connexion SP.

Créer des connexions SP supplémentaires

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



Les connexions SP des 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 l'URL de réponse SLO.

Étapes

1. Sélectionnez **action > copie** pour créer une copie de la connexion SP initiale pour chaque nœud d'administration supplémentaire.
2. Entrez l'ID de connexion et le nom de connexion de la copie, puis sélectionnez **Enregistrer**.
3. Choisissez le fichier de métadonnées correspondant au nœud d'administration :

- a. Sélectionnez **action > mettre à jour avec métadonnées**.
 - b. Sélectionnez **Choisissez fichier** et chargez les métadonnées.
 - c. Sélectionnez **Suivant**.
 - d. Sélectionnez **Enregistrer**.
4. Résoudre l'erreur en raison de l'attribut inutilisé :
- a. Sélectionnez la nouvelle connexion.
 - b. Sélectionnez **configurer le navigateur SSO > configurer la création d'assertion > Contrat d'attribut**.
 - c. Supprimez l'entrée pour **urn:oid**.
 - d. Sélectionnez **Enregistrer**.

Désactiver SSO

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

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 authentification unique s'affiche.

2. Sélectionnez **Désactiver SSO**.
3. Sélectionnez **Oui**.

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

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

Désactiver et réactiver temporairement SSO pour un nœud d'administration

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

Description de la tâche

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



La désactivation de SSO pour un nœud d'administration n'affecte pas les paramètres SSO pour les autres nœuds d'administration de la grille. La case **Activer SSO** de la page ouverture de session unique du gestionnaire de grille reste cochée et tous les paramètres SSO existants sont conservés, sauf si vous les mettez à jour.

Étapes

1. Connectez-vous à un nœud d'administration :

- Entrez la commande suivante : `ssh admin@Admin_Node_IP`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
- Entrez la commande suivante pour basculer en root : `su -`
- Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

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

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

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

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

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

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

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

5. Connectez-vous avec le nom d'utilisateur root et le mot de passe de l'utilisateur root local.

6. Si vous avez désactivé l'authentification SSO temporairement car vous avez besoin de corriger la configuration SSO :

- Sélectionnez **Configuration > Contrôle d'accès > Authentification unique**.
- Modifiez les paramètres SSO incorrects ou obsolètes.
- Sélectionnez **Enregistrer**.

La sélection de **Enregistrer** sur la page ouverture de session unique permet de réactiver automatiquement SSO pour l'ensemble de la grille.

7. Si vous avez désactivé l'authentification SSO temporairement car vous devez accéder au Grid Manager pour une autre raison :

- Effectuez les tâches que vous souhaitez effectuer.

b. Sélectionnez **se déconnecter** et fermez le Gestionnaire de grille.

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

- Exécutez la commande suivante : `enable-saml`

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

Confirmez que vous souhaitez activer le SSO.

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

- Redémarrer le nœud grid : `reboot`

8. À partir d'un navigateur Web, accédez à Grid Manager à partir du même nœud d'administration.

9. Vérifiez que la page de connexion StorageGRID s'affiche et que vous devez saisir vos informations d'identification SSO pour accéder au Gestionnaire de grille.

Informations sur le copyright

Copyright © 2026 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.