# Configurer les paramètres de sécurité

StorageGRID software

NetApp
December 03, 2025

# Sommaire


Configurer les paramètres de sécurité . . . 1
- Gérer la politique TLS et SSH . . . 1
  - Sélectionnez une politique de sécurité . . . 1
  - Créer une politique de sécurité personnalisée . . . 2
  - Revenir temporairement à la politique de sécurité par défaut . . . 3
- Configurer la sécurité du réseau et des objets . . . 3
  - Chiffrement des objets stockés . . . 3
  - Empêcher la modification du client . . . 4
  - Activer HTTP pour les connexions aux nœuds de stockage . . . 4
  - Sélectionnez les options . . . 4
- Modifier les paramètres de sécurité de l’interface . . . 5

# Configurer les paramètres de sécurité

## Gérer la politique TLS et SSH

La politique TLS et SSH détermine les protocoles et chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications clientes et des connexions SSH sécurisées aux services StorageGRID internes.

La politique de sécurité contrôle la manière dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la politique de compatibilité moderne (par défaut), sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

Certains services StorageGRID n'ont pas été mis à jour pour utiliser les chiffrements dans ces politiques.

**Avant de commencer**

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

### Sélectionnez une politique de sécurité

**Étapes**

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité**.

   L'onglet **Politiques TLS et SSH** affiche les politiques disponibles. La politique actuellement active est indiquée par une coche verte sur la vignette de la politique.


2. Consultez les tuiles pour en savoir plus sur les politiques disponibles.

| Politique | Description |
|---|---|
| Compatibilité moderne (par défaut) | Utilisez la politique par défaut si vous avez besoin d'un cryptage fort et à moins que vous n'ayez des exigences particulières. Cette politique est compatible avec la plupart des clients TLS et SSH. |
| Compatibilité héritée | Utilisez cette politique si vous avez besoin d'options de compatibilité supplémentaires pour les clients plus anciens. Les options supplémentaires de cette politique peuvent la rendre moins sécurisée que la politique de compatibilité moderne. |

| Politique | Description |
| --- | --- |
| Critères communs | Utilisez cette politique si vous avez besoin d'une certification Critères communs. |
| FIPS strict | Utilisez cette politique si vous avez besoin d'une certification Common Criteria et devez utiliser le module de sécurité cryptographique NetApp 3.0.8 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au gestionnaire de locataires et au gestionnaire de grille. L'utilisation de cette politique peut réduire les performances.<br><br>**Remarque** : après avoir sélectionné cette politique, tous les nœuds doivent être"redémarré de manière continue" pour activer le module de sécurité cryptographique NetApp . Utilisez **Maintenance** > **Redémarrage progressif** pour lancer et surveiller les redémarrages. |
| Coutume | Créez une politique personnalisée si vous devez appliquer vos propres chiffrements. |

3. Pour voir les détails sur les chiffrements, les protocoles et les algorithmes de chaque politique, sélectionnez **Afficher les détails**.
4. Pour modifier la politique actuelle, sélectionnez **Utiliser la politique**.

   Une coche verte apparaît à côté de **Politique actuelle** sur la vignette de la politique.

## Créer une politique de sécurité personnalisée

Vous pouvez créer une politique personnalisée si vous devez appliquer vos propres chiffrements.

**Étapes**

1. À partir de la vignette de la politique la plus similaire à la politique personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.

3. Dans la mosaïque **Politique personnalisée**, sélectionnez **Configurer et utiliser**.
4. Collez le JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **Utiliser la politique**.

   Une coche verte apparaît à côté de **Politique actuelle** sur la mosaïque Politique personnalisée.

6. Vous pouvez également sélectionner **Modifier la configuration** pour apporter d'autres modifications à la nouvelle politique personnalisée.

### Revenir temporairement à la politique de sécurité par défaut

Si vous avez configuré une politique de sécurité personnalisée, vous ne pourrez peut-être pas vous connecter au Grid Manager si la politique TLS configurée est incompatible avec la"certificat de serveur configuré" .

Vous pouvez revenir temporairement à la politique de sécurité par défaut.

**Étapes**

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

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

2. Exécutez la commande suivante :

   ```
   restore-default-cipher-configurations
   ```

3. À partir d'un navigateur Web, accédez au gestionnaire de grille sur le même nœud d'administration.
4. Suivez les étapes dansSélectionnez une politique de sécurité pour configurer à nouveau la politique.

# Configurer la sécurité du réseau et des objets

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, pour empêcher certaines requêtes S3 ou pour autoriser les connexions client aux nœuds de stockage à utiliser HTTP au lieu de HTTPS.

### Chiffrement des objets stockés

Le chiffrement des objets stockés permet le chiffrement de toutes les données d'objets lorsqu'elles sont ingérées via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de crypter les objets à l'aide de l'algorithme de chiffrement AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets nouvellement ingérés sont chiffrés, mais aucune modification n'est apportée aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les objets nouvellement ingérés ne sont pas chiffrés.

Le paramètre de chiffrement d'objet stocké s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par un chiffrement au niveau du bucket ou au niveau de l'objet.

Pour plus de détails sur les méthodes de chiffrement StorageGRID , voir"Examiner les méthodes de chiffrement StorageGRID" .

## Empêcher la modification du client

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option **Empêcher la modification du client** est sélectionnée, les demandes suivantes sont refusées.

#### API REST S3

- Requêtes DeleteBucket
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'un objet S3

## Activer HTTP pour les connexions aux nœuds de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions directes aux nœuds de stockage. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille non productive.

Utilisez HTTP pour les connexions aux nœuds de stockage uniquement si les clients S3 doivent établir des connexions HTTP directement aux nœuds de stockage. Vous n'avez pas besoin d'utiliser cette option pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service Load Balancer (car vous pouvez"configurer chaque point de terminaison de l'équilibreur de charge" (utiliser soit HTTP soit HTTPS).

Voir"Résumé : Adresses IP et ports pour les connexions client" pour savoir quels ports les clients S3 utilisent lors de la connexion aux nœuds de stockage via HTTP ou HTTPS.

## Sélectionnez les options

#### Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous disposez de l'autorisation d'accès root.

#### Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **Aucun** (par défaut) si vous ne souhaitez pas que les objets stockés soient chiffrés, ou sélectionnez **AES-128** ou **AES-256** pour chiffrer les objets stockés.
4. Sélectionnez éventuellement **Empêcher la modification du client** si vous souhaitez empêcher les clients S3 d'effectuer des demandes spécifiques.

   Si vous modifiez ce paramètre, l'application du nouveau paramètre prendra environ une minute. La valeur configurée est mise en cache pour les performances et la mise à l'échelle.

5. Sélectionnez éventuellement **Activer HTTP pour les connexions aux nœuds de stockage** si les clients se connectent directement aux nœuds de stockage et que vous souhaitez utiliser des connexions HTTP.

Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées non chiffrées.

6. Sélectionnez **Enregistrer**.

# Modifier les paramètres de sécurité de l'interface

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant plus de la durée spécifiée et si une trace de pile est incluse dans les réponses d'erreur d'API.

**Avant de commencer**

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

**À propos de cette tâche**

La page **Paramètres de sécurité** inclut les paramètres **Délai d'inactivité du navigateur** et **Trace de la pile de l'API de gestion**.

**Délai d'inactivité du navigateur**

Indique combien de temps le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est de 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID distinct et non configurable, inclus pour la sécurité du système. Le jeton d'authentification de chaque utilisateur expire 16 heures après la connexion de l'utilisateur. Lorsque l'authentification d'un utilisateur expire, cet utilisateur est automatiquement déconnecté, même si le délai d'inactivité du navigateur est désactivé ou si la valeur du délai d'expiration du navigateur n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai d'expiration pour le fournisseur d'identité, en supposant que l'authentification unique (SSO) est activée pour StorageGRID.

  Si SSO est activé et que le navigateur d'un utilisateur expire, l'utilisateur doit ressaisir ses informations d'identification SSO pour accéder à nouveau à StorageGRID . Voir "Configurer l'authentification unique" .

**Trace de pile de l'API de gestion**

Contrôle si une trace de pile est renvoyée dans les réponses d'erreur de l'API Grid Manager et Tenant Manager.

Cette option est désactivée par défaut, mais vous souhaiterez peut-être activer cette fonctionnalité pour un environnement de test. En général, vous devez laisser la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails internes du logiciel lorsque des erreurs d'API se produisent.

**Étapes**

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :

a. Développez l’accordéon.

b. Pour modifier le délai d’expiration, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai d’expiration par défaut est de 15 minutes.

c. Pour désactiver cette fonctionnalité, décochez la case.

d. Sélectionnez **Enregistrer**.

Le nouveau paramètre n’affecte pas les utilisateurs actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d’expiration prenne effet.

4. Pour modifier le paramètre de la trace de la pile de l’API de gestion :

a. Développez l’accordéon.

b. Cochez la case pour renvoyer une trace de pile dans les réponses d’erreur de l’API Grid Manager et Tenant Manager.

Laissez la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails internes du logiciel lorsque des erreurs d’API se produisent.

c. Sélectionnez **Enregistrer**.

## Informations sur le copyright



## Informations sur les marques commerciales