Configurer les paramètres de sécurité

StorageGRID software

NetApp
July 23, 2026

Sommaire

Configurer les paramètres de sécurité

Gérez la politique TLS et SSH dans StorageGRID

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

La politique de sécurité détermine la façon dont TLS et SSH chiffrent les données en transit. En général, utilisez la politique Modern compatibility (par défaut), sauf si votre système doit être conforme aux Common Criteria ou si vous devez utiliser d'autres algorithmes de chiffrement.

> Certains services StorageGRID n'ont pas été mis à jour pour utiliser les algorithmes de chiffrement définis dans ces politiques.

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".

Sélectionnez une politique de sécurité

Étapes

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

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

   

2. Consultez les onglets pour en savoir plus sur les stratégies disponibles.

Compatibilité moderne (par défaut)

Utilisez la stratégie par défaut si vous avez besoin d'un chiffrement fort et que vous n'avez pas d'exigences particulières. Cette stratégie est compatible avec la plupart des clients TLS et SSH.

Compatibilité héritée

Utilisez la stratégie de compatibilité héritée si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette stratégie peuvent la rendre moins sécurisée que la stratégie de compatibilité moderne.

Critères communs

Utilisez la politique Common Criteria si vous avez besoin d'une certification Common Criteria.

FIPS strict

Utilisez la politique FIPS stricte si vous avez besoin de la certification Critères communs et devez utiliser le NetApp Cryptographic Security Module (NCSM) 3.0.8 ou le module NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 pour les connexions client externes aux points de terminaison de l'équilibreur de charge, au Tenant Manager et au Grid Manager. L'utilisation de cette politique peut réduire les performances.

Les modules NCSM 3.0.8 et NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 sont utilisés dans les opérations suivantes :

- NCSM
  - Connexions TLS entre les services suivants : ADC, AMS, CMN, DDS, LDR, SSM, NMS, mgmt-api, nginx, nginx-gw et cache-svc
  - Connexions TLS entre les clients et le service nginx-gw (points de terminaison de l'équilibreur de charge)
  - Connexions TLS entre les clients et le service LDR
  - Chiffrement du contenu des objets pour SSE-S3, SSE-C et le paramètre de chiffrement des objets stockés
  - connexions SSH

  Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "Certificat n° 4838".

- NetApp StorageGRID module API de chiffrement du noyau

  Le module API de chiffrement du noyau NetApp StorageGRID est présent uniquement sur les plateformes VM et les appliances StorageGRID.

  - Collecte d'entropie
  - Chiffrement du nœud

  Pour plus d'informations, consultez le programme de validation des algorithmes cryptographiques du NIST "Certificats n° A6242 à A6257" et "Certificat d'entropie n° E223".

Remarque : Après avoir sélectionné cette stratégie, "effectuer un redémarrage progressif" pour activer le NCSM sur tous les nœuds. Utilisez **Maintenance** > **Redémarrage progressif** pour lancer et surveiller les redémarrages.

Personnalisé

Créez une politique personnalisée si vous devez appliquer vos propres chiffrements.

Si votre StorageGRID est soumis à des exigences de cryptographie FIPS 140, vous pouvez activer la fonctionnalité de mode FIPS pour utiliser le module NCSM 3.0.8 et le module NetApp StorageGRID Kernel Crypto API 6.1.129-1-ntap1-amd64 :

a. Définissez le `fipsMode` paramètre sur `true`.

b. Lorsque vous y êtes invité, "effectuer un redémarrage progressif" pour activer les modules de cryptographie sur tous les nœuds. Utilisez **Maintenance** > **Rolling reboot** pour lancer et surveiller les redémarrages.

c. Sélectionnez **Support** > **Diagnostics** pour afficher les versions actives du module FIPS.

3. Pour consulter les détails des chiffrements, protocoles et 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 **Current policy** 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 vignette **Stratégie personnalisée**, sélectionnez **Configurer et utiliser**.
4. Collez le JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **Utiliser la stratégie**.

   Une coche verte apparaît à côté de **Police actuelle** sur la vignette **Police personnalisée**.

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

Rétablir temporairement la politique de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, vous pourriez ne pas être en mesure de vous connecter au Grid Manager si la stratégie TLS configurée est incompatible avec le "certificat de serveur configuré".

Vous pouvez temporairement rétablir la politique de sécurité par défaut.

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 :

   ```
   restore-default-cipher-configurations
   ```
3. Depuis un navigateur Web, accédez au Grid Manager sur le même nœud d'administration.
4. Suivez les étapes décrites dans Sélectionnez une politique de sécurité pour configurer à nouveau la politique.

Configurer la sécurité du réseau et des objets StorageGRID

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

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données des objets lors de leur ingestion via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de chiffrer les objets à l'aide de l'algorithme de chiffrement AES-128 ou AES-256. Lorsque vous activez ce paramètre, tous les nouveaux objets ingérés sont chiffrés, mais aucun changement n'est apporté aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les nouveaux objets ingérés ne sont pas chiffrés.

Le paramètre de chiffrement des objets stockés s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou au niveau de l'objet.

Pour plus de détails sur les méthodes de chiffrement StorageGRID, voir "Passez en revue les méthodes de chiffrement de StorageGRID".

Empêcher la modification du client

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

API REST S3

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

Activer HTTP pour les connexions au nœud de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toute connexion directe aux Storage Nodes. Vous pouvez activer le protocole HTTP pour ces connexions, par exemple lors du test d'une grille hors production.

Utilisez HTTP pour les connexions aux nœuds de stockage uniquement si les clients S3 doivent établir des connexions HTTP directes avec ces nœuds. 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 d'équilibrage de charge" utiliser HTTP ou HTTPS).

Consultez "Résumé : adresses IP et ports pour les connexions client" pour savoir quels ports les clients S3 utilisent lorsqu'ils se connectent aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous disposez des droits 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. Vous pouvez également sélectionner **Empêcher la modification du client** si vous souhaitez empêcher les clients S3 d'effectuer des requêtes spécifiques.

   Si vous modifiez ce paramètre, il faudra environ une minute pour que le nouveau paramètre soit appliqué. La valeur configurée est mise en cache pour optimiser les performances et la mise à l'échelle.

5. Vous pouvez également sélectionner **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 le protocole HTTP pour une grille de production, car les requêtes seront envoyées sans chiffrement.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface StorageGRID

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

Avant de commencer

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

À propos de cette tâche

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

Délai d'inactivité du navigateur

Indique la durée pendant laquelle le navigateur d'un utilisateur peut rester 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 est 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'inactivité 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) soit activée pour StorageGRID.

  Si l'authentification unique (SSO) est activée et que la session du navigateur d'un utilisateur expire, ce dernier doit saisir à nouveau ses identifiants SSO pour accéder de nouveau à StorageGRID. Voir "Fonctionnement de l'authentification unique (SSO)".

Trace de pile de l'API de gestion

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

Cette option est désactivée par défaut, mais vous pouvez activer cette fonctionnalité pour un environnement de test. En règle générale, vous devez laisser la trace de pile désactivée dans les environnements de production afin d'éviter de révéler des 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. Déployez 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**.

Ce nouveau paramètre n'affecte pas les utilisateurs déjà connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau délai d'expiration prenne effet.

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

a. Déployez l'accordéon.

b. Cochez la case pour afficher 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 afin d'éviter de révéler des détails internes du logiciel en cas d'erreurs d'API.

c. Sélectionnez **Enregistrer**.

Gérer l'accès SSH externe dans StorageGRID

Gérez l'accès SSH au trafic entrant dans la grille en bloquant ou en autorisant l'accès externe. La gestion de l'accès SSH externe n'a aucun impact sur le trafic entre les nœuds de la grille.

Avant de commencer

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

À propos de cette tâche

Pour renforcer la sécurité du système, l'accès SSH externe est bloqué par défaut. Si vous devez effectuer des tâches nécessitant un accès SSH entrant, comme le dépannage, autorisez temporairement l'accès externe. Lorsque vous avez terminé la tâche, bloquez l'accès externe.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Bloquer SSH**.
3. Utilisez l'option **Bloquer l'accès SSH entrant** pour gérer l'accès SSH externe :

a. Cochez la case pour bloquer l'accès (par défaut).

b. Décochez la case pour autoriser l'accès.

Nécessite un accès au port 22 entre l'ordinateur portable de service et tous les autres nœuds du grid. Supprimez l'accès au port 22 une fois la tâche de maintenance terminée.

4. Sélectionnez **Enregistrer**.

Informations sur le copyright

Informations sur les marques commerciales