



Configurez les paramètres de sécurité

StorageGRID 11.7

NetApp
April 12, 2024

Sommaire

- Configurez les paramètres de sécurité 1
 - Gestion des règles TLS et SSH 1
 - Configurer la sécurité du réseau et des objets 3
 - Modifier le délai d'inactivité du navigateur 5

Configurez les paramètres de sécurité

Gestion des règles TLS et SSH

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

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la règle 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 le chiffrement inclus dans ces règles.

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 racine"](#).

Sélectionnez une stratégie de sécurité

Étapes

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

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



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

Politique	Description
Compatibilité moderne (par défaut)	Utilisez la stratégie par défaut si vous avez besoin d'un cryptage fort et si vous ne disposez pas d'exigences particulières. Cette règle est compatible avec la plupart des clients TLS et SSH.
Compatibilité avec les systèmes existants	Utilisez cette stratégie si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette politique pourraient la rendre moins sécurisée que la politique de compatibilité moderne.

Politique	Description
Critères communs	Utilisez cette règle si vous avez besoin de la certification critères communs.
Norme FIPS stricte	Utilisez cette règle si vous avez besoin de la certification critères communs et que vous devez utiliser NetApp Cryptographic Security module 3.0.0 pour les connexions de clients externes vers les terminaux d'équilibrage de charge, le gestionnaire de locataires et Grid Manager. L'utilisation de cette règle peut réduire les performances.
Personnalisées	Créez une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

3. Pour afficher des détails sur les chiffrements, les protocoles et les algorithmes de chaque stratégie, sélectionnez **Afficher les détails**.
4. Pour modifier la stratégie actuelle, sélectionnez **utiliser la stratégie**.

Une coche verte apparaît en regard de **police actuelle** sur la mosaïque de police.

Créez une stratégie de sécurité personnalisée

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

Étapes

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



3. Dans la mosaïque **Personnaliser la stratégie**, sélectionnez **configurer et utiliser**.
4. Collez le fichier JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **utiliser la stratégie**.

Une coche verte apparaît en regard de **politique actuelle** sur la mosaïque de stratégie personnalisée.

6. Si vous le souhaitez, sélectionnez **Modifier la configuration** pour apporter d'autres modifications à la nouvelle stratégie personnalisée.

Rétablir temporairement la stratégie de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, il se peut que vous ne puissiez pas vous connecter au gestionnaire de grille si la stratégie TLS configurée est incompatible avec le "[certificat de serveur configuré](#)".

Vous pouvez rétablir temporairement la stratégie de sécurité par défaut.

Étapes

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

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

3. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.
4. Suivez les étapes de la section [Sélectionnez une stratégie de sécurité](#) pour reconfigurer la stratégie.

Configurer la sécurité du réseau et des objets

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

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données d'objet 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 cryptage AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets récemment acquis 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 objets nouvellement 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 de l'objet.

Pour plus d'informations sur les méthodes de cryptage StorageGRID, reportez-vous à la section "[Étudiez les méthodes de cryptage StorageGRID](#)".

Empêcher toute 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.

L'API REST S3

- Supprimer les demandes de compartiment
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3

API REST Swift

- Supprimer les demandes de conteneur
- Demande de modifier tout objet existant. Par exemple, les opérations suivantes sont refusées : remplacement, suppression, mise à jour des métadonnées, etc.

Activez HTTP pour les connexions de nœud 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 autre que la production.

Utilisez HTTP pour les connexions de nœuds de stockage uniquement si les clients S3 et Swift 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 (parce que vous le pouvez) "[configurez chaque point d'extrémité de l'équilibreur de charge](#)" Pour utiliser HTTP ou HTTPS).

Voir "[Résumé : adresses IP et ports pour les connexions client](#)" Pour savoir quels ports les clients S3 et Swift 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 racine.

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 **None** (par défaut) si vous ne souhaitez pas que les objets stockés soient cryptés, ou sélectionnez **AES-128** ou **AES-256** pour crypter les objets stockés.
4. Vous pouvez également sélectionner **empêcher la modification du client** si vous souhaitez empêcher les clients S3 et Swift de faire des demandes spécifiques.



Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

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



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

6. Sélectionnez **Enregistrer**.

Modifier le délai d'inactivité du navigateur

Vous pouvez contrôler si les utilisateurs de Grid Manager et de tenant Manager sont déconnectés s'ils sont inactifs pendant plus d'un certain temps.

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 racine.

Description de la tâche

Par défaut, le délai d'inactivité du navigateur est de 15 minutes. Si le navigateur d'un utilisateur n'est pas actif pendant cette période, l'utilisateur est déconnecté.

Si nécessaire, vous pouvez augmenter ou diminuer le délai d'expiration en définissant l'option **déconnecter les utilisateurs inactifs après**.

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

- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Par défaut, 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) est activée pour StorageGRID.

Si la fonction SSO est activée et que le navigateur d'un utilisateur arrive à expiration, l'utilisateur doit saisir à nouveau ses informations d'identification SSO pour accéder à StorageGRID à nouveau. Voir ["Configurer l'authentification unique"](#).

Étapes

1. Sélectionnez **CONFIGURATION > sécurité > Paramètres de sécurité**.
2. Sélectionnez l'onglet **délai d'inactivité du navigateur**.
3. Dans le champ **déconnecter les utilisateurs inactifs après**, spécifiez un délai d'expiration du navigateur compris entre 60 secondes et 7 jours.

Vous pouvez spécifier le délai d'expiration du navigateur en secondes, minutes, heures ou jours.

4. Sélectionnez **Enregistrer**. Si un navigateur est inactif pendant la durée spécifiée, l'utilisateur est déconnecté du Gestionnaire de grille ou du Gestionnaire de locataires.

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.

Informations sur le copyright

Copyright © 2024 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 DÉLICTEUELLE (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.