Configurez les paramètres de sécurité

StorageGRID 11.9

NetApp
November 08, 2024

Sommaire

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 Gestionnaire de grille 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 le module de sécurité cryptographique NetApp 3.0.8 pour les connexions de clients externes aux terminaux d'équilibrage de charge, au gestionnaire de locataires et au gestionnaire de grille. L'utilisation de cette règle peut réduire les performances. **Remarque** : après avoir sélectionné cette stratégie, tous les nœuds doivent être "redémarrés de manière mobile" pour activer le module de sécurité cryptographique NetApp. Utilisez **Maintenance** > **redémarrage en roulant** pour lancer et surveiller les redémarrages.
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 à Grid Manager si la stratégie TLS configurée est incompatible avec "certificat de serveur configuré".

Vous pouvez rétablir temporairement la stratégie de sécurité par défaut.

Étapes

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

   ```
   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 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 "Étudiez les méthodes de cryptage StorageGRID"la section .

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

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

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 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 (parce que vous pouvez "configurez chaque point d'extrémité de l'équilibreur de charge"utiliser HTTP ou HTTPS).

Reportez-vous à la section "Résumé : adresses IP et ports pour les connexions client" pour connaître les ports utilisés par les clients S3 lors de la connexion 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 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 sélectionner **empêcher la modification du client** si vous voulez empêcher les clients S3 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 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 temps que spécifié 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 racine".

Description de la tâche

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

Délai d'inactivité du navigateur dépassé

Indique la durée pendant laquelle le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est 15 minutes.

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. 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".

Trace de la 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 pouvez 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 logiciels internes en cas d'erreurs d'API.

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 la période de temporisation, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai par défaut est de 15 minutes.

c. Pour désactiver cette fonction, décochez la case.

d. Sélectionnez **Enregistrer**.

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

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

a. Développez l’accordéon.

b. Cochez cette 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 logiciels internes en cas d’erreur d’API.

c. Sélectionnez **Enregistrer**.

Informations sur le copyright

Informations sur les marques commerciales