Gérer la sécurité

StorageGRID software

NetApp
December 03, 2025

Sommaire

Gérer la sécurité

Gérer la sécurité

Vous pouvez configurer divers paramètres de sécurité à partir du Grid Manager pour contribuer à sécuriser votre système StorageGRID .

Gérer le cryptage

StorageGRID fournit plusieurs options pour crypter les données. Tu devrais"examiner les méthodes de cryptage disponibles" pour déterminer ceux qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

Tu peux"configurer et gérer les certificats du serveur" utilisé pour les connexions HTTP ou les certificats clients utilisés pour authentifier l'identité d'un client ou d'un utilisateur auprès du serveur.

Configurer les serveurs de gestion de clés

En utilisant un"serveur de gestion de clés" vous permet de protéger les données StorageGRID même si un appareil est retiré du centre de données. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance, sauf si le nœud peut communiquer avec le KMS.

> Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Chiffrement de nœud** pour chaque appliance lors de l'installation, avant que l'appliance ne soit ajoutée à la grille.

Gérer les paramètres de proxy

Si vous utilisez des services de plateforme S3 ou des pools de stockage cloud, vous pouvez configurer un"serveur proxy de stockage" entre les nœuds de stockage et les points de terminaison S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un"serveur proxy d'administration" entre les nœuds d'administration et le support technique.

Contrôler les pare-feu

Pour améliorer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du"pare-feu externe" . Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son"pare-feu interne" . Vous pouvez empêcher l'accès sur tous les ports, sauf ceux nécessaires à votre déploiement.

Examiner les méthodes de chiffrement StorageGRID

StorageGRID fournit plusieurs options pour crypter les données. Vous devez examiner les méthodes disponibles pour déterminer celles qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un résumé de haut niveau des méthodes de chiffrement disponibles dans StorageGRID.

Option de cryptage	Comment ça marche	S'applique à
Serveur de gestion de clés (KMS) dans Grid Manager	Toi"configurer un serveur de gestion de clés" pour le site StorageGRID et "activer le chiffrement des nœuds pour l'appliance" . Ensuite, un nœud d'appareil se connecte au KMS pour demander une clé de chiffrement de clé (KEK). Cette clé crypte et décrypte la clé de cryptage des données (DEK) sur chaque volume.	Nœuds d'appareils pour lesquels le **chiffrement de nœud** est activé lors de l'installation. Toutes les données de l'appareil sont protégées contre toute perte physique ou suppression du centre de données. **Remarque** : la gestion des clés de chiffrement avec un KMS est uniquement prise en charge pour les nœuds de stockage et les appliances de services.
Page de chiffrement de lecteur dans le programme d'installation de l'appliance StorageGRID	Si l'appareil contient des lecteurs prenant en charge le chiffrement matériel, vous pouvez définir une phrase secrète de lecteur lors de l'installation. Lorsque vous définissez une phrase secrète de lecteur, il est impossible pour quiconque de récupérer des données valides à partir de lecteurs qui ont été supprimés du système, à moins de connaître la phrase secrète. Avant de commencer l'installation, accédez à **Configurer le matériel** > **Chiffrement de lecteur** pour définir une phrase secrète de lecteur qui s'applique à tous les lecteurs à chiffrement automatique gérés par StorageGRID dans un nœud.	Appareils contenant des lecteurs à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre toute perte physique ou suppression du centre de données. Le chiffrement des lecteurs ne s'applique pas aux lecteurs gérés par SANtricity. Si vous disposez d'un dispositif de stockage avec des lecteurs à chiffrement automatique et des contrôleurs SANtricity , vous pouvez activer la sécurité des lecteurs dans SANtricity.
Pilotez la sécurité dans SANtricity System Manager	Si la fonctionnalité Drive Security est activée pour votre appliance StorageGRID , vous pouvez utiliser "Gestionnaire de système SANtricity" pour créer et gérer la clé de sécurité. La clé est nécessaire pour accéder aux données sur les lecteurs sécurisés.	Appareils de stockage dotés de lecteurs à chiffrement complet du disque (FDE) ou de lecteurs à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre toute perte physique ou suppression du centre de données. Ne peut pas être utilisé avec certains appareils de stockage ou avec des appareils de service.

Option de cryptage	Comment ça marche	S'applique à
Chiffrement des objets stockés	Vous activez le"Chiffrement des objets stockés" option dans le gestionnaire de grille. Lorsque cette option est activée, tous les nouveaux objets qui ne sont pas chiffrés au niveau du bucket ou au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées. Les objets stockés existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées.
Chiffrement du compartiment S3	Vous émettez une demande PutBucketEncryption pour activer le chiffrement du bucket. Tous les nouveaux objets qui ne sont pas chiffrés au niveau de l'objet sont chiffrés lors de l'ingestion.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour le bucket. Les objets de bucket existants ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. "Opérations sur les godets"
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une requête S3 pour stocker un objet et incluez le `x-amz-server-side-encryption` en-tête de requête.	Données d'objet S3 nouvellement ingérées uniquement. Le cryptage doit être spécifié pour l'objet. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utiliser le cryptage côté serveur"
Chiffrement côté serveur d'objets S3 avec clés fournies par le client (SSE-C)	Vous émettez une requête S3 pour stocker un objet et incluez trois en-têtes de requête. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Données d'objet S3 nouvellement ingérées uniquement. Le cryptage doit être spécifié pour l'objet. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors de StorageGRID. "Utiliser le cryptage côté serveur"

Option de cryptage	Comment ça marche	S'applique à
Chiffrement de volume externe ou de banque de données	Vous utilisez une méthode de chiffrement en dehors de StorageGRID pour chiffrer un volume ou une banque de données entière, si votre plate-forme de déploiement la prend en charge.	Toutes les données d'objet, métadonnées et données de configuration système, en supposant que chaque volume ou banque de données soit chiffré. Une méthode de cryptage externe permet un contrôle plus strict des algorithmes et des clés de cryptage. Peut être combiné avec les autres méthodes répertoriées.
Chiffrement d'objets en dehors de StorageGRID	Vous utilisez une méthode de chiffrement en dehors de StorageGRID pour chiffrer les données et les métadonnées des objets avant qu'elles ne soient ingérées dans StorageGRID.	Données d'objet et métadonnées uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de cryptage externe permet un contrôle plus strict des algorithmes et des clés de cryptage. Peut être combiné avec les autres méthodes répertoriées. "Amazon Simple Storage Service - Guide de l'utilisateur : Protection des données à l'aide du chiffrement côté client"

Utiliser plusieurs méthodes de cryptage

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de cryptage à la fois. Par exemple:

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et également utiliser la fonction de sécurité du lecteur dans SANtricity System Manager pour « doublement crypter » les données sur les lecteurs à chiffrement automatique dans les mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds de l'appliance et également utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lorsqu'ils sont ingérés.

Si seule une petite partie de vos objets nécessite un chiffrement, envisagez plutôt de contrôler le chiffrement au niveau du bucket ou de l'objet individuel. L'activation de plusieurs niveaux de cryptage entraîne un coût supplémentaire en termes de performances.

Gérer les certificats

Gérer les certificats de sécurité

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

- **Les certificats de serveur** sont requis lorsque vous utilisez des connexions HTTPS. Les certificats de serveur sont utilisés pour établir des connexions sécurisées entre les clients et les serveurs, authentifiant l'identité d'un serveur auprès de ses clients et fournissant un chemin de communication sécurisé pour les données. Le serveur et le client disposent chacun d'une copie du certificat.
- Les **certificats clients** authentifient l'identité d'un client ou d'un utilisateur auprès du serveur, offrant une authentification plus sécurisée que les mots de passe seuls. Les certificats clients ne cryptent pas les données.

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (comme le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (comme le service de réplication CloudMirror).

Certificat Grid CA par défaut

StorageGRID inclut une autorité de certification (CA) intégrée qui génère un certificat CA Grid interne lors de l'installation du système. Le certificat Grid CA est utilisé, par défaut, pour sécuriser le trafic StorageGRID interne. Une autorité de certification (CA) externe peut émettre des certificats personnalisés entièrement conformes aux politiques de sécurité des informations de votre organisation. Bien que vous puissiez utiliser le certificat Grid CA pour un environnement hors production, la meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont également prises en charge mais ne sont pas recommandées.

- Les certificats CA personnalisés ne suppriment pas les certificats internes ; cependant, les certificats personnalisés doivent être ceux spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent répondre aux"directives de renforcement du système pour les certificats de serveur" .
- StorageGRID prend en charge le regroupement de certificats d'une autorité de certification dans un seul fichier (appelé regroupement de certificats d'autorité de certification).

> ⓘ StorageGRID inclut également des certificats d'autorité de certification du système d'exploitation qui sont les mêmes sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat CA du système d'exploitation.

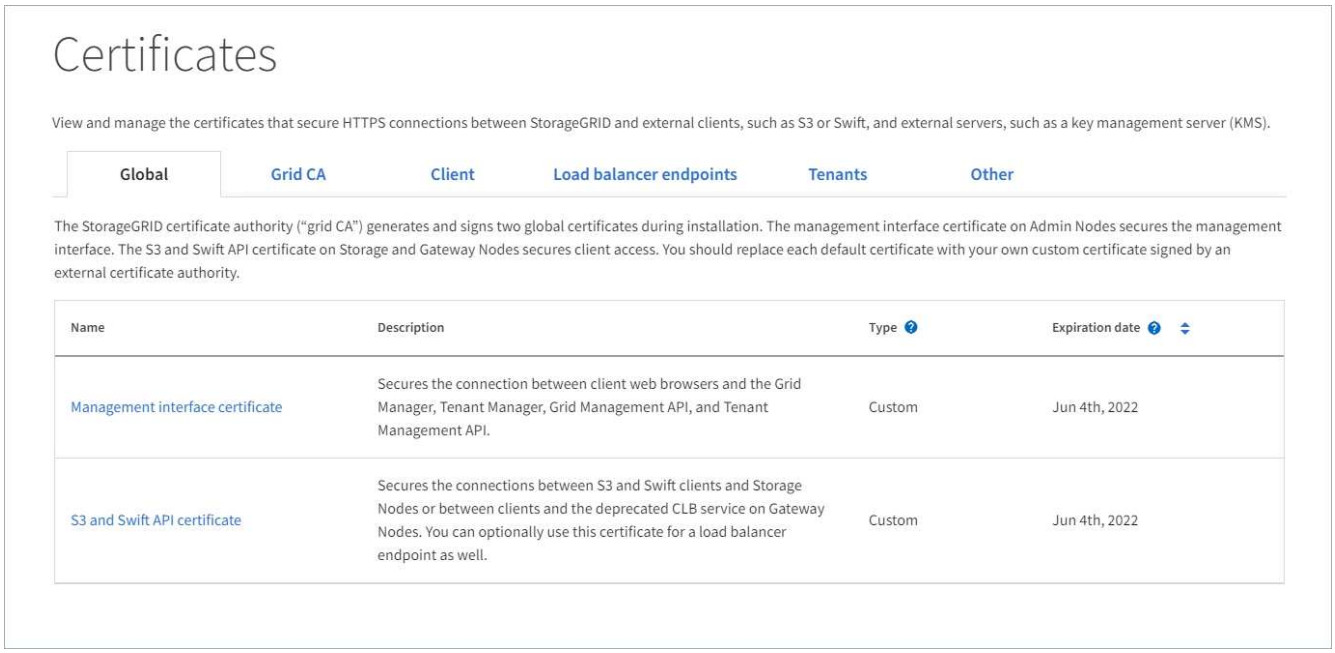
Les variantes des types de certificats serveur et client sont implémentées de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID spécifique avant de configurer le système.

Accéder aux certificats de sécurité

Vous pouvez accéder aux informations sur tous les certificats StorageGRID dans un seul emplacement, ainsi qu'aux liens vers le flux de travail de configuration pour chaque certificat.

Étapes

1. Depuis le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.



2. Sélectionnez un onglet sur la page Certificats pour obtenir des informations sur chaque catégorie de certificat et pour accéder aux paramètres du certificat. Vous pouvez accéder à un onglet si vous avez le"autorisation appropriée" .

   - **Global** : Sécurise l'accès à StorageGRID à partir des navigateurs Web et des clients API externes.
   - **Grid CA** : sécurise le trafic StorageGRID interne.
   - **Client** : sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
   - **Points de terminaison de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et l'équilibreur de charge StorageGRID .
   - * Locataires * : sécurise les connexions aux serveurs de fédération d'identité ou des points de terminaison de service de la plateforme aux ressources de stockage S3.
   - **Autre** : Sécurise les connexions StorageGRID nécessitant des certificats spécifiques.

     Chaque onglet est décrit ci-dessous avec des liens vers des détails de certificat supplémentaires.

Mondial

Les certificats globaux sécurisent l'accès à StorageGRID à partir des navigateurs Web et des clients API S3 externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La meilleure pratique pour un environnement de production consiste à utiliser des certificats personnalisés signés par une autorité de certification externe.

- Certificat d'interface de gestion: Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID .
- Certificat API S3:Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications client S3 utilisent pour télécharger et charger des données d'objet.

Les informations sur les certificats globaux installés incluent :

- **Nom** : Nom du certificat avec lien pour gérer le certificat.
- **Description**
- **Type** : Personnalisé ou par défaut. + Vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité du réseau.
- **Date d'expiration** : Si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Tu peux:

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
  - "Remplacer le certificat d'interface de gestion généré par StorageGRID par défaut"utilisé pour les connexions Grid Manager et Tenant Manager.
  - "Remplacer le certificat API S3"utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (facultatif).
- "Restaurer le certificat d'interface de gestion par défaut" .
- "Restaurer le certificat API S3 par défaut" .
- "Utiliser un script pour générer un nouveau certificat d'interface de gestion auto-signé" .
- Copiez ou téléchargez le"certificat d'interface de gestion" ou"Certificat API S3" .

Grille CA

LeCertificat Grid CA , généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID , sécurise tout le trafic interne de StorageGRID .

Les informations du certificat incluent la date d'expiration du certificat et le contenu du certificat.

Tu peux"copier ou télécharger le certificat Grid CA" , mais tu ne peux pas le changer.

Client

Certificats clients, généré par une autorité de certification externe, sécurise les connexions entre les outils de surveillance externes et la base de données StorageGRID Prometheus.

La table des certificats comporte une ligne pour chaque certificat client configuré et indique si le certificat peut être utilisé pour l'accès à la base de données Prometheus, ainsi que la date d'expiration du certificat.

Tu peux:

- "Téléchargez ou générez un nouveau certificat client."
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
  - "Modifier le nom du certificat client."
  - "Définissez l'autorisation d'accès Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimer le certificat client."
- Sélectionnez **Actions** pour rapidement"modifier" ,"attacher" , ou"retirer" un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément en utilisant **Actions** > **Supprimer**.

Points de terminaison de l'équilibreur de charge

Certificats de point de terminaison d'équilibrage de chargesécurisez les connexions entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison de l'équilibreur de charge configuré et indique si le certificat API S3 global ou un certificat de point de terminaison de l'équilibreur de charge personnalisé est utilisé pour le point de terminaison. La date d'expiration de chaque certificat est également affichée.

> Les modifications apportées à un certificat de point de terminaison peuvent prendre jusqu'à 15 minutes pour être appliquées à tous les nœuds.

Tu peux:

- "Afficher un point de terminaison d'équilibrage de charge", y compris les détails de son certificat.
- "Spécifiez un certificat de point de terminaison d'équilibrage de charge pour FabricPool."
- "Utiliser le certificat API S3 global"au lieu de générer un nouveau certificat de point de terminaison d'équilibrage de charge.

Locataires

Les locataires peuvent utilisercertificats de serveur de fédération d'identité oucertificats de point de terminaison de service de plateforme pour sécuriser leurs connexions avec StorageGRID.

La table des locataires comporte une ligne pour chaque locataire et indique si chaque locataire est autorisé à utiliser sa propre source d'identité ou ses propres services de plateforme.

Tu peux:

- "Sélectionnez un nom de locataire pour vous connecter au gestionnaire de locataires"
- "Sélectionnez un nom de locataire pour afficher les détails de la fédération d'identité du locataire"
- "Sélectionnez un nom de locataire pour afficher les détails des services de la plateforme locataire"
- "Spécifier un certificat de point de terminaison de service de plateforme lors de la création du point de terminaison"

Autre

StorageGRID utilise d'autres certificats de sécurité à des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. D'autres certificats de sécurité incluent :

- Certificats Cloud Storage Pool
- Certificats de notification d'alerte par courrier électronique
- Certificats de serveur syslog externes
- Certificats de connexion à la fédération de réseau
- Certificats de fédération d'identité
- Certificats du serveur de gestion de clés (KMS)
- Certificats d'authentification unique

Les informations indiquent le type de certificat utilisé par une fonction ainsi que les dates d'expiration de ses certificats serveur et client, le cas échéant. La sélection d'un nom de fonction ouvre un onglet de navigateur dans lequel vous pouvez afficher et modifier les détails du certificat.

> Vous ne pouvez afficher et accéder aux informations des autres certificats que si vous disposez des droits d'accès."autorisation appropriée" .

Tu peux:

- "Spécifier un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"
- "Spécifier un certificat pour les notifications d'alerte par e-mail"
- "Utiliser un certificat pour un serveur syslog externe"
- "Faire pivoter les certificats de connexion à la fédération de réseau"
- "Afficher et modifier un certificat de fédération d'identité"
- "Télécharger les certificats du serveur de gestion des clés (KMS) et du client"
- "Spécifier manuellement un certificat SSO pour une approbation de partie de confiance"

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions de mise en œuvre.

Certificat d'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web clients et l'interface de gestion StorageGRID , permettant aux utilisateurs d'accéder à Grid Manager et Tenant Manager sans avertissements de sécurité. Ce certificat authentifie également les connexions à l'API Grid Management et à l'API Tenant Management. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	**CONFIGURATION** > **Sécurité** > **Certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **Certificat d'interface de gestion**	"Configurer les certificats de l'interface de gestion"

Certificat API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées à un nœud de stockage et aux points de terminaison de l'équilibreur de charge (facultatif).	**CONFIGURATION** > **Sécurité** > **Certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **Certificat API S3**	"Configurer les certificats API S3"

Certificat Grid CA

Voir leDescription du certificat Grid CA par défaut .

Certificat client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe. • Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus. • Permet une surveillance sécurisée de StorageGRID à l'aide d'outils externes.	**CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**	"Configurer les certificats clients"

Certificat de point de terminaison de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service d'équilibrage de charge StorageGRID sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un point de terminaison d'équilibreur de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée du globalCertificat API S3 certificat pour authentifier les connexions au service Load Balancer. Si le certificat global est utilisé pour authentifier les connexions de l'équilibreur de charge, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque point de terminaison de l'équilibreur de charge. **Remarque :** le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de StorageGRID .	**CONFIGURATION** > **Réseau** > **Points de terminaison de l'équilibreur de charge**	• "Configurer les points de terminaison de l'équilibreur de charge" • "Créer un point de terminaison d'équilibrage de charge pour FabricPool"

Certificat de point de terminaison du pool de stockage cloud

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un pool de stockage cloud StorageGRID vers un emplacement de stockage externe, tel que S3 Glacier ou le stockage Microsoft Azure Blob. Un certificat différent est requis pour chaque type de fournisseur de cloud.	**ILM** > **Pools de stockage**	"Créer un pool de stockage cloud"

Certificat de notification d'alerte par courrier électronique

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent Transport Layer Security (TLS), vous devez spécifier le certificat d'autorité de certification du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP requiert des certificats clients pour l'authentification.	**ALERTES** > **Configuration de la messagerie électronique**	"Configurer des notifications par e-mail pour les alertes"

Certificat de serveur syslog externe

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion TLS ou RELP/TLS entre un serveur syslog externe qui enregistre les événements dans StorageGRID. **Remarque :** un certificat de serveur Syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur Syslog externe.	**CONFIGURATION** > **Surveillance** > **Serveur d'audit et syslog**	"Utiliser un serveur syslog externe"

Certificat de connexion à la fédération de réseau

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et cryptez les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grille.	**CONFIGURATION** > **Système** > **Fédération de grille**	• "Créer des connexions de fédération de grille" • "Faire tourner les certificats de connexion"

Certificat de fédération d'identité

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération d'identité, qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	**CONFIGURATION** > **Contrôle d'accès** > **Fédération d'identité**	"Utiliser la fédération d'identité"

Certificat du serveur de gestion de clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion de clés externe (KMS), qui fournit des clés de chiffrement aux nœuds de l'appliance StorageGRID .	**CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**	"Ajouter un serveur de gestion de clés (KMS)"

Certificat de point de terminaison des services de plateforme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion du service de plateforme StorageGRID à une ressource de stockage S3.	**Gestionnaire de locataires** > **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**	"Créer un point de terminaison des services de plateforme" "Modifier le point de terminaison des services de la plateforme"

Certificat d'authentification unique (SSO)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identité, tels que les services de fédération Active Directory (AD FS) et StorageGRID qui sont utilisés pour les demandes d'authentification unique (SSO).	**CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service d'équilibrage de charge

Dans cet exemple, StorageGRID agit comme serveur.

1. Vous configurez un point de terminaison d'équilibrage de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 au point de terminaison de l'équilibreur de charge et téléchargez le même certificat sur le client.

3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et avec une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature sur sa copie du certificat. Si les signatures correspondent, le client démarre une session en utilisant la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : Serveur de gestion de clés externe (KMS)

Dans cet exemple, StorageGRID agit en tant que client.

1. À l'aide d'un logiciel de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par une autorité de certification, un certificat client public et la clé privée du certificat client.
2. À l'aide du gestionnaire de grille, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une demande au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond en utilisant la connexion validée.

Types de certificats de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm).

> Le type de chiffrement de la politique de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA nécessitent des certificats ECDSA. Voir "Gérer les certificats de sécurité" . Si vous configurez une politique de sécurité personnalisée qui n'est pas compatible avec le certificat du serveur, vous pouvez"revenir temporairement à la politique de sécurité par défaut" .

Pour plus d'informations sur la manière dont StorageGRID sécurise les connexions client, consultez"Sécurité pour les clients S3" .

Configurer les certificats de l'interface de gestion

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un seul certificat personnalisé qui permet aux utilisateurs d'accéder au gestionnaire de grille et au gestionnaire de locataires sans rencontrer d'avertissements de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

À propos de cette tâche

Par défaut, chaque nœud d'administration reçoit un certificat signé par l'autorité de certification de la grille. Ces certificats signés par une autorité de certification peuvent être remplacés par un seul certificat d'interface de gestion personnalisée commune et la clé privée correspondante.

Étant donné qu'un seul certificat d'interface de gestion personnalisé est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat comme certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au gestionnaire de grille et au gestionnaire de locataires. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, en fonction de l'autorité de certification racine (CA) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat Grid CA dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.

Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

Si vous accédez au Grid Manager ou au Tenant Manager à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Toirevenir d'un certificat d'interface de gestion personnalisé au certificat de serveur par défaut .

Ajouter un certificat d'interface de gestion personnalisé

Pour ajouter un certificat d'interface de gestion personnalisé, vous pouvez fournir votre propre certificat ou en générer un à l'aide du gestionnaire de grille.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire (CA). Le fichier doit contenir chacun des fichiers de certificat CA codés en PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Développez **Détails du certificat** pour voir les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

Générer un certificat

Générer les fichiers de certificat du serveur.

> La meilleure pratique pour un environnement de production consiste à utiliser un certificat d'interface de gestion personnalisé signé par une autorité de certification externe.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour voir les métadonnées du certificat généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

5. Actualisez la page pour vous assurer que le navigateur Web est à jour.

> Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page Certificat d'interface de gestion affiche des informations détaillées sur les certificats en cours d'utilisation. + Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat d'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid

Manager et Tenant Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client ultérieures.

4. Actualisez la page pour vous assurer que le navigateur Web est à jour.

Utiliser un script pour générer un nouveau certificat d'interface de gestion auto-signé

Si une validation stricte du nom d'hôte est requise, vous pouvez utiliser un script pour générer le certificat de l'interface de gestion.

Avant de commencer

- Tu as"autorisations d'accès spécifiques" .
- Vous avez le `Passwords.txt` déposer.

À propos de cette tâche

La meilleure pratique pour un environnement de production consiste à utiliser un certificat signé par une autorité de certification externe.

Étapes

1. Obtenez le nom de domaine complet (FQDN) de chaque nœud d'administration.
2. Connectez-vous au nœud d'administration principal :
   a. Entrez la commande suivante : `ssh admin@primary_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 `#` .

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Pour `--domains` , utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple, `*.ui.storagegrid.example.com` utilise le caractère générique * pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com` .
   - Ensemble `--type` à `management` pour configurer le certificat d'interface de gestion, qui est utilisé par Grid Manager et Tenant Manager.
   - Par défaut, les certificats générés sont valables un an (365 jours) et doivent être recréés avant leur

expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par défaut.

> La période de validité d'un certificat commence lorsque `make-certificate` est exécuté. Vous devez vous assurer que le client de gestion est synchronisé avec la même source horaire que StorageGRID; sinon, le client risque de rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 720
```

La sortie résultante contient le certificat public nécessaire à votre client API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les balises BEGIN et END dans votre sélection.

5. Déconnectez-vous de l'interpréteur de commandes. `$ exit`
6. Confirmer que le certificat a été configuré :
   a. Accéder au gestionnaire de grille.
   b. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**
   c. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Inclure les balises BEGIN et END.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat de l'interface de gestion pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Configurer les certificats API S3

Vous pouvez remplacer ou restaurer le certificat de serveur utilisé pour les connexions client S3 aux nœuds de stockage ou aux points de terminaison de l'équilibreur de charge. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Les détails Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Configurer les certificats API S3 et Swift" .

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par une autorité de certification peuvent être remplacés par un seul certificat de serveur personnalisé commun et une clé privée correspondante.

Un seul certificat de serveur personnalisé est utilisé pour tous les nœuds de stockage. Vous devez donc spécifier le certificat comme certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au point de terminaison de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration sur le serveur terminée, vous devrez peut-être également installer le certificat Grid CA dans le client API S3 que vous utiliserez pour accéder au système, en fonction de l'autorité de certification racine (CA) que vous utilisez.

> Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration du certificat de serveur global pour l'API S3** est déclenchée lorsque le certificat du serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat API S3 personnalisé.

Ajouter un certificat API S3 personnalisé

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

- **Certificat de serveur** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA codés PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM pour chaque certificat API S3 personnalisé qui a été téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat ou sélectionnez **Télécharger le bundle CA** pour enregistrer le bundle de certificats.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

Générer un certificat

Générer les fichiers de certificat du serveur.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine entièrement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat API S3 personnalisé qui a été généré.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat de serveur StorageGRID par défaut, d'un certificat signé par une autorité de certification qui a été téléchargé ou d'un certificat personnalisé qui a été généré.

> Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

6. Actualisez la page pour vous assurer que le navigateur Web est à jour.
7. Après avoir ajouté un certificat API S3 personnalisé, la page de certificat API S3 affiche des informations détaillées sur le certificat API S3 personnalisé en cours d'utilisation. + Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

Restaurer le certificat API S3 par défaut

Vous pouvez revenir à l'utilisation du certificat API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat API S3 par défaut pour un point de terminaison d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser le certificat par défaut**.

   Lorsque vous restaurez la version par défaut du certificat API S3 global, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat API S3 par défaut sera utilisé pour les nouvelles connexions client S3 ultérieures aux nœuds de stockage.

4. Sélectionnez **OK** pour confirmer l'avertissement et restaurer le certificat API S3 par défaut.

   Si vous disposez de l'autorisation d'accès racine et que le certificat API S3 personnalisé a été utilisé pour les connexions aux points de terminaison de l'équilibreur de charge, une liste des points de terminaison de l'équilibreur de charge qui ne seront plus accessibles à l'aide du certificat API S3 par défaut s'affiche. Aller à"Configurer les points de terminaison de l'équilibreur de charge" pour modifier ou supprimer les points de terminaison affectés.

5. Actualisez la page pour vous assurer que le navigateur Web est à jour.

Téléchargez ou copiez le certificat API S3

Vous pouvez enregistrer ou copier le contenu du certificat API S3 pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Télécharger le certificat** ou **Télécharger le bundle CA**.

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Informations connexes

- "Utiliser l'API REST S3"
- "Configurer les noms de domaine des points de terminaison S3"

Copier le certificat Grid CA

StorageGRID utilise une autorité de certification interne (CA) pour sécuriser le trafic interne. Ce certificat ne change pas si vous téléchargez vos propres certificats.

Avant de commencer

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

À propos de cette tâche

Si un certificat de serveur personnalisé a été configuré, les applications clientes doivent vérifier le serveur à l'aide du certificat de serveur personnalisé. Ils ne doivent pas copier le certificat CA du système StorageGRID .

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Grid CA**.

2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

a. Sélectionnez **Télécharger le certificat**.

b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem` .

Par exemple : `storagegrid_certificate.pem`

Configurer les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le point de terminaison de l'équilibreur de charge.

Avant de commencer

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

À propos de cette tâche

Lorsque vous créez un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification (CA) connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être renouvelés sans interruption. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type « man-in-the-middle ».

Les étapes suivantes fournissent des directives générales pour les clients S3 qui utilisent FabricPool. Pour des informations et des procédures plus détaillées, voir"Configurer StorageGRID pour FabricPool" .

Étapes

1. Vous pouvez également configurer un groupe de haute disponibilité (HA) à utiliser par FabricPool .
2. Créez un point de terminaison d'équilibrage de charge S3 à utiliser par FabricPool .

Lorsque vous créez un point de terminaison d'équilibrage de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre ensemble d'autorités de certification facultatif.

3. Attachez StorageGRID en tant que niveau cloud dans ONTAP.

   Spécifiez le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat CA que vous avez téléchargé. Ensuite, fournissez le certificat CA.

   > Si une autorité de certification intermédiaire a émis le certificat StorageGRID , vous devez fournir le certificat de l'autorité de certification intermédiaire. Si le certificat StorageGRID a été émis directement par l'autorité de certification racine, vous devez fournir le certificat de l'autorité de certification racine.

Configurer les certificats clients

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, offrant ainsi un moyen sécurisé aux outils externes de surveiller StorageGRID.

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide du Grid Manager et copier les informations du certificat sur l'outil externe.

Voir"Gérer les certificats de sécurité" et"Configurer des certificats de serveur personnalisés" .

> Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat client dans l'onglet Client.

> Si vous utilisez un serveur de gestion de clés (KMS) pour protéger les données sur des nœuds d'appliance spécialement configurés, consultez les informations spécifiques sur"téléchargement d'un certificat client KMS" .

Avant de commencer

- Vous disposez de l'autorisation d'accès root.
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Pour configurer un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
  - Si vous avez configuré le certificat d'interface de gestion StorageGRID , vous disposez de l'autorité de certification, du certificat client et de la clé privée utilisés pour configurer le certificat d'interface de gestion.
  - Pour télécharger votre propre certificat, la clé privée du certificat est disponible sur votre ordinateur local.
  - La clé privée doit avoir été sauvegardée ou enregistrée au moment de sa création. Si vous ne disposez pas de la clé privée d'origine, vous devez en créer une nouvelle.
- Pour modifier un certificat client :

- Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
- Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats clients

Pour ajouter le certificat client, utilisez l'une de ces procédures :

- Certificat d'interface de gestion déjà configuré
- Certificat client émis par l'AC
- Certificat généré à partir de Grid Manager

Certificat d'interface de gestion déjà configuré

Utilisez cette procédure pour ajouter un certificat client si un certificat d'interface de gestion est déjà configuré à l'aide d'une autorité de certification, d'un certificat client et d'une clé privée fournis par le client.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Joindre les certificats**, téléchargez le certificat de l'interface de gestion.
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez le fichier de certificat de l'interface de gestion(`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît dans l'onglet Client.
7. Configurer un outil de surveillance externe, comme Grafana.

Certificat client émis par l'AC

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise un certificat client émis par une autorité de certification et une clé privée.

Étapes

1. Effectuez les étapes pour"configurer un certificat d'interface de gestion" .
2. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

3. Sélectionnez **Ajouter**.
4. Entrez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle CA :
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez le certificat client, la clé privée et les fichiers groupés de l'autorité de certification(`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Les nouveaux certificats apparaissent dans l'onglet Client.
8. Configurer un outil de surveillance externe, comme Grafana.

Certificat généré à partir de Grid Manager

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction de génération de certificat dans Grid Manager.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Joindre des certificats**, sélectionnez **Générer un certificat**.
7. Spécifiez les informations du certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

Laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **Générer**.
9. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

     Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
   - Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de fichier.

     Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

10. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

    Le nouveau certificat apparaît dans l'onglet Client.

11. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Global**.
12. Sélectionnez **Certificat d'interface de gestion**.
13. Sélectionnez **Utiliser un certificat personnalisé**.
14. Téléchargez les fichiers certificate.pem et private_key.pem depuis ledétails du certificat client étape. Il n'est pas nécessaire de télécharger le bundle CA.
    a. Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.
    b. Téléchargez chaque fichier de certificat(`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans le gestionnaire de grille.

       Le nouveau certificat apparaît sur la page des certificats de l'interface de gestion.

15. Configurer un outil de surveillance externe, comme Grafana.

Configurer un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tel que Grafana.
   a. **Nom**: Saisissez un nom pour la connexion.

      StorageGRID ne nécessite pas ces informations, mais vous devez fournir un nom pour tester la connexion.

b. **URL**: Saisissez le nom de domaine ou l'adresse IP du nœud d'administration. Spécifiez HTTPS et le port 9091.

   Par exemple : `https://admin-node.example.com:9091`

c. Activez **TLS Client Auth** et **Avec certificat CA**.

d. Sous Détails d'authentification TLS/SSL, copiez et collez :

   - L'interface de gestion du certificat CA vers **CA Cert**
   - Le certificat client de **Client Cert**
   - La clé privée de **Clé client**

e. **ServerName**: saisissez le nom de domaine du nœud d'administration.

   ServerName doit correspondre au nom de domaine tel qu'il apparaît dans le certificat de l'interface de gestion.

2. Enregistrez et testez le certificat et la clé privée que vous avez copiés à partir de StorageGRID ou d'un fichier local.

   Vous pouvez désormais accéder aux métriques Prometheus depuis StorageGRID avec votre outil de surveillance externe.

   Pour plus d'informations sur les mesures, consultez le"instructions pour la surveillance de StorageGRID" .

Modifier les certificats clients

Vous pouvez modifier un certificat client administrateur pour changer son nom, activer ou désactiver l'accès à Prometheus ou télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

   Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez **Modifier le nom et l'autorisation**
4. Entrez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le gestionnaire de grille.

   Le certificat mis à jour s'affiche dans l'onglet Client.

Joindre un nouveau certificat client

Vous pouvez télécharger un nouveau certificat lorsque le certificat actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.

   Les dates d'expiration des certificats et les autorisations d'accès Prometheus sont répertoriées dans le tableau. Si un certificat expire bientôt ou est déjà expiré, un message apparaît dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez une option de modification.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.

b. Télécharger le nom du certificat client(`.pem`).

   Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   - Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

     Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.

c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

   Le certificat mis à jour s'affiche dans l'onglet Client.

Générer un certificat

Générez le texte du certificat à coller ailleurs.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

     Laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

   Vous ne pourrez pas afficher la clé privée du certificat après avoir fermé la boîte de dialogue. Copiez ou téléchargez la clé dans un emplacement sûr.

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller

ailleurs.

- Sélectionnez **Télécharger le certificat** pour enregistrer le fichier de certificat.

  Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de fichier.

  Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.

e. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

Le nouveau certificat apparaît dans l'onglet Client.

Télécharger ou copier les certificats clients

Vous pouvez télécharger ou copier un certificat client pour l'utiliser ailleurs.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

a. Sélectionnez **Télécharger le certificat**.
b. Spécifiez le nom du fichier de certificat et l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Copier le certificat PEM**.
b. Collez le certificat copié dans un éditeur de texte.
c. Enregistrez le fichier texte avec l'extension `.pem` .

   Par exemple : `storagegrid_certificate.pem`

Supprimer les certificats clients

Si vous n'avez plus besoin d'un certificat client administrateur, vous pouvez le supprimer.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez supprimer.
3. Sélectionnez **Supprimer** puis confirmez.

> Pour supprimer jusqu'à 10 certificats, sélectionnez chaque certificat à supprimer dans l'onglet Client, puis sélectionnez **Actions** > **Supprimer**.

Une fois un certificat supprimé, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

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.
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. **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**.

Configurer les serveurs de gestion de clés

Qu'est-ce qu'un serveur de gestion de clés (KMS) ?

Un serveur de gestion de clés (KMS) est un système externe tiers qui fournit des clés de chiffrement aux nœuds d'appliance StorageGRID sur le site StorageGRID associé à l'aide du protocole d'interopérabilité de gestion de clés (KMIP).

StorageGRID prend en charge uniquement certains serveurs de gestion de clés. Pour obtenir la liste des produits et versions pris en charge, utilisez le "Outil de matrice d'interopérabilité NetApp (IMT)" .

Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Chiffrement de nœud** est activé lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds d'appliance vous permet de protéger vos données même si une appliance est supprimée du centre de données. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance, sauf si le nœud peut communiquer avec le KMS.

> StorageGRID ne crée ni ne gère les clés externes utilisées pour chiffrer et déchiffrer les nœuds de l'appliance. Si vous prévoyez d'utiliser un serveur de gestion de clés externe pour protéger les données StorageGRID , vous devez comprendre comment configurer ce serveur et comment gérer les clés de chiffrement. L'exécution des tâches de gestion des clés dépasse le cadre de ces instructions. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion de clés ou contactez le support technique.

Configuration KMS et appliance

Avant de pouvoir utiliser un serveur de gestion de clés (KMS) pour sécuriser les données StorageGRID sur les nœuds de l'appliance, vous devez effectuer deux tâches de configuration : configurer un ou plusieurs serveurs KMS et activer le chiffrement des nœuds pour les nœuds de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés se déroule automatiquement.

L'organigramme montre les étapes de haut niveau pour utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds de l'appliance.

L'organigramme montre la configuration de KMS et la configuration de l'appliance se déroulant en parallèle ; cependant, vous pouvez configurer les serveurs de gestion de clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds de l'appliance, en fonction de vos besoins.

Configurer le serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion de clés comprend les étapes de haut niveau suivantes.

Étape	Se référer à
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque KMS ou cluster KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Obtenez les informations requises pour le client StorageGRID sur le KMS.	"Configurer StorageGRID en tant que client dans le KMS"
Ajoutez le KMS au Grid Manager, attribuez-le à un site unique ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	"Ajouter un serveur de gestion de clés (KMS)"

Installer l'appareil

La configuration d'un nœud d'appareil pour l'utilisation de KMS comprend les étapes de haut niveau suivantes.

1. Au cours de l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Chiffrement de nœud** pour l'appliance.

   > Vous ne pouvez pas activer le paramètre **Chiffrement de nœud** après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion des clés externes pour les appareils sur lesquels le chiffrement de nœud n'est pas activé.

2. Exécutez le programme d'installation de l'appliance StorageGRID . Lors de l'installation, une clé de chiffrement de données aléatoire (DEK) est attribuée à chaque volume d'appareil, comme suit :
   - Les DEK sont utilisés pour crypter les données sur chaque volume. Ces clés sont générées à l'aide du chiffrement de disque Linux Unified Key Setup (LUKS) dans le système d'exploitation de l'appliance et ne peuvent pas être modifiées.
   - Chaque DEK individuel est chiffré par une clé de chiffrement à clé principale (KEK). La KEK initiale est une clé temporaire qui crypte les DEK jusqu'à ce que l'appareil puisse se connecter au KMS.
3. Ajoutez le nœud de l'appliance à StorageGRID.

Voir "Activer le cryptage des nœuds" pour plus de détails.

Processus de cryptage de gestion des clés (se produit automatiquement)

Le chiffrement de gestion des clés comprend les étapes de haut niveau suivantes qui sont exécutées automatiquement.

1. Lorsque vous installez un dispositif sur lequel le chiffrement de nœud est activé dans la grille, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
   - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.
   - Si un KMS n'a pas encore été configuré pour le site, les données sur l'appliance continuent d'être chiffrées par le KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.
2. L'appareil utilise la configuration KMS pour se connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appareil. La nouvelle clé du KMS remplace la KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les DEK pour les volumes de l'appliance.

   > Toutes les données qui existent avant que le nœud de l'appareil chiffré ne se connecte au KMS configuré sont chiffrées avec une clé temporaire. Toutefois, les volumes de l'appareil ne doivent pas être considérés comme protégés contre le retrait du centre de données tant que la clé temporaire n'est pas remplacée par la clé de chiffrement KMS.

4. Si l'appareil est sous tension ou redémarré, il se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée dans la mémoire volatile, ne peut pas survivre à une panne de courant ou à un redémarrage.

Considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés

Avant de configurer un serveur de gestion de clés externe (KMS), vous devez comprendre les considérations et les exigences.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

"Spécification du protocole d'interopérabilité de gestion des clés version 1.4"

Quelles sont les considérations relatives au réseau ?

Les paramètres du pare-feu réseau doivent permettre à chaque nœud d'appareil de communiquer via le port utilisé pour les communications du protocole KMIP (Key Management Interoperability Protocol). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'appliance qui utilise le chiffrement de nœud dispose d'un accès réseau au KMS ou au cluster KMS que vous avez configuré pour le site.

Quelles versions de TLS sont prises en charge ?

Les communications entre les nœuds de l'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID peut prendre en charge le protocole TLS 1.2 ou TLS 1.3 lorsqu'il établit des connexions KMIP à un cluster KMS ou KMS, en fonction de ce que le KMS prend en charge et de ce qu'il prend en charge."Politique TLS et SSH" vous utilisez.

StorageGRID négocie le protocole et le chiffrement (TLS 1.2) ou la suite de chiffrement (TLS 1.3) avec le KMS lorsqu'il établit la connexion. Pour voir quelles versions de protocole et quels chiffrements/suites de chiffrement sont disponibles, consultez le `tlsOutbound` section de la politique TLS et SSH active de la grille (**CONFIGURATION** > **Sécurité Paramètres de sécurité**).

Quels appareils sont pris en charge ?

Vous pouvez utiliser un serveur de gestion de clés (KMS) pour gérer les clés de chiffrement de tout dispositif StorageGRID de votre grille sur lequel le paramètre **Chiffrement de nœud** est activé. Ce paramètre ne peut être activé que pendant l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID .

> Vous ne pouvez pas activer le chiffrement des nœuds après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion des clés externes pour les appareils sur lesquels le chiffrement des nœuds n'est pas activé.

Vous pouvez utiliser le KMS configuré pour les appliances StorageGRID et les nœuds d'appliance.

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds basés sur des logiciels (non-appliances), y compris les suivants :

- Nœuds déployés en tant que machines virtuelles (VM)
- Nœuds déployés dans des moteurs de conteneurs sur des hôtes Linux

Les nœuds déployés sur ces autres plates-formes peuvent utiliser le chiffrement en dehors de StorageGRID au niveau de la banque de données ou du disque.

Quand dois-je configurer les serveurs de gestion de clés ?

Pour une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion de clés dans Grid Manager avant de créer des locataires. Cet ordre garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur eux.

Vous pouvez configurer les serveurs de gestion de clés dans Grid Manager avant ou après l'installation des nœuds de l'appliance.

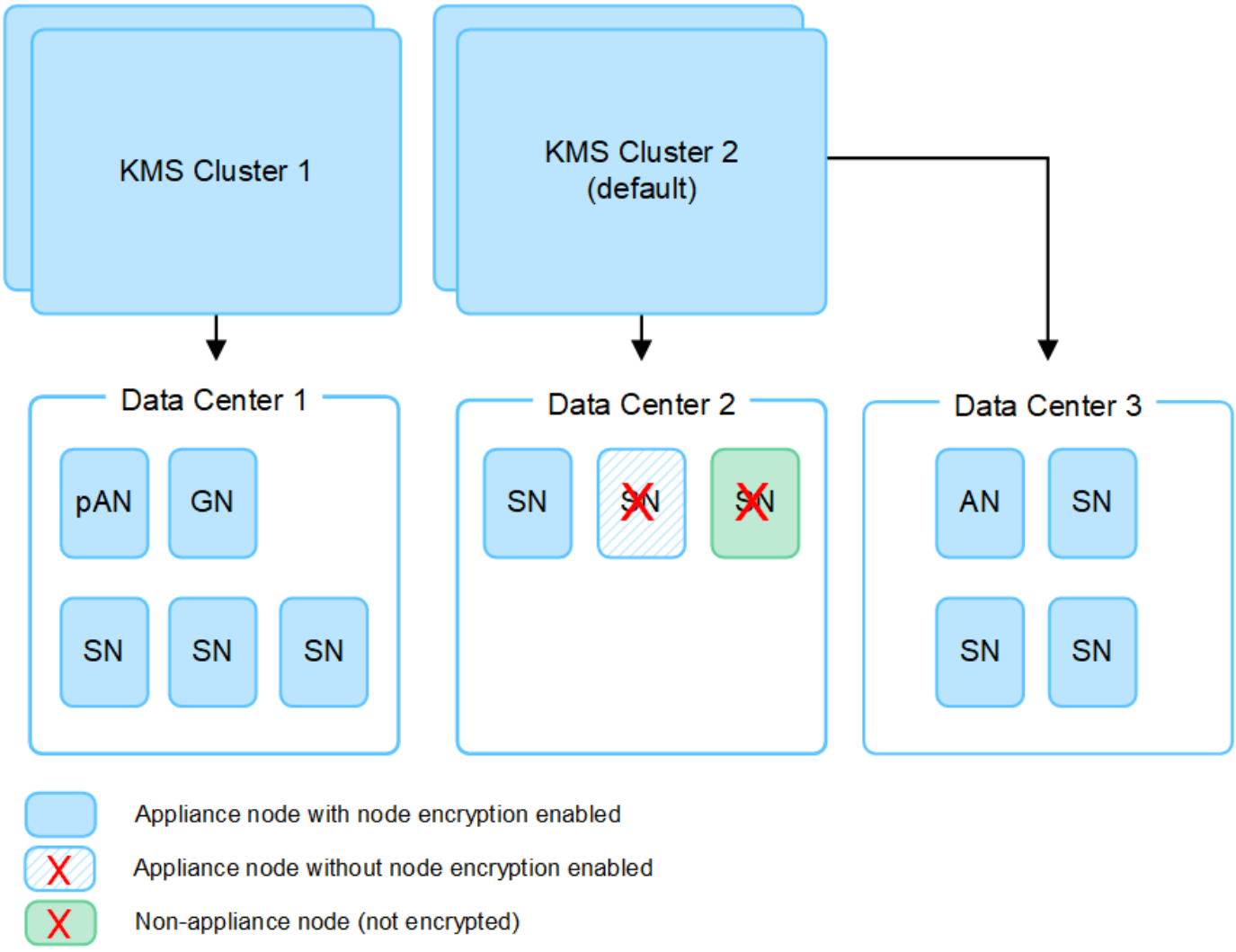
De combien de serveurs de gestion de clés ai-je besoin ?

Vous pouvez configurer un ou plusieurs serveurs de gestion de clés externes pour fournir des clés de chiffrement aux nœuds d'appliance de votre système StorageGRID . Chaque KMS fournit une clé de chiffrement unique aux nœuds de l'appliance StorageGRID sur un site unique ou sur un groupe de sites.

StorageGRID prend en charge l'utilisation de clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion de clés répliqués qui partagent les paramètres de configuration et les clés de chiffrement. L'utilisation de clusters KMS pour la gestion des clés est recommandée car elle améliore les capacités de basculement d'une configuration haute disponibilité.

Par exemple, supposons que votre système StorageGRID dispose de trois sites de centre de données. Vous pouvez configurer un cluster KMS pour fournir une clé à tous les nœuds d'appliance du centre de données 1 et un deuxième cluster KMS pour fournir une clé à tous les nœuds d'appliance de tous les autres sites. Lorsque vous ajoutez le deuxième cluster KMS, vous pouvez configurer un KMS par défaut pour Data Center 2 et Data Center 3.

Notez que vous ne pouvez pas utiliser un KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont le paramètre **Chiffrement de nœud** n'a pas été activé lors de l'installation.



Que se passe-t-il lorsqu'une clé est tournée ?

En tant que bonne pratique de sécurité, vous devez périodiquement"faire pivoter la clé de cryptage" utilisé par chaque KMS configuré.

Lorsque la nouvelle version de clé sera disponible :

- Il est automatiquement distribué aux nœuds d'appareils chiffrés sur le ou les sites associés au KMS. La distribution devrait avoir lieu dans l'heure qui suit la rotation de la clé.
- Si le nœud de l'appareil chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud recevra la nouvelle clé dès son redémarrage.
- Si la nouvelle version de clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour une raison quelconque, l'alerte **Échec de la rotation de la clé de chiffrement KMS** est déclenchée pour le nœud de l'appliance. Vous devrez peut-être contacter le support technique pour obtenir de l'aide pour résoudre cette alerte.

Puis-je réutiliser un nœud d'appareil après l'avoir chiffré ?

Si vous devez installer un dispositif chiffré dans un autre système StorageGRID , vous devez d'abord mettre hors service le nœud de grille pour déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le programme d'installation de l'appliance StorageGRID pour "effacer la configuration KMS" . La suppression de la configuration KMS désactive le paramètre **Chiffrement de nœud** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID .

> ⓘ Sans accès à la clé de cryptage KMS, toutes les données restantes sur l'appareil ne sont plus accessibles et sont verrouillées de manière permanente.

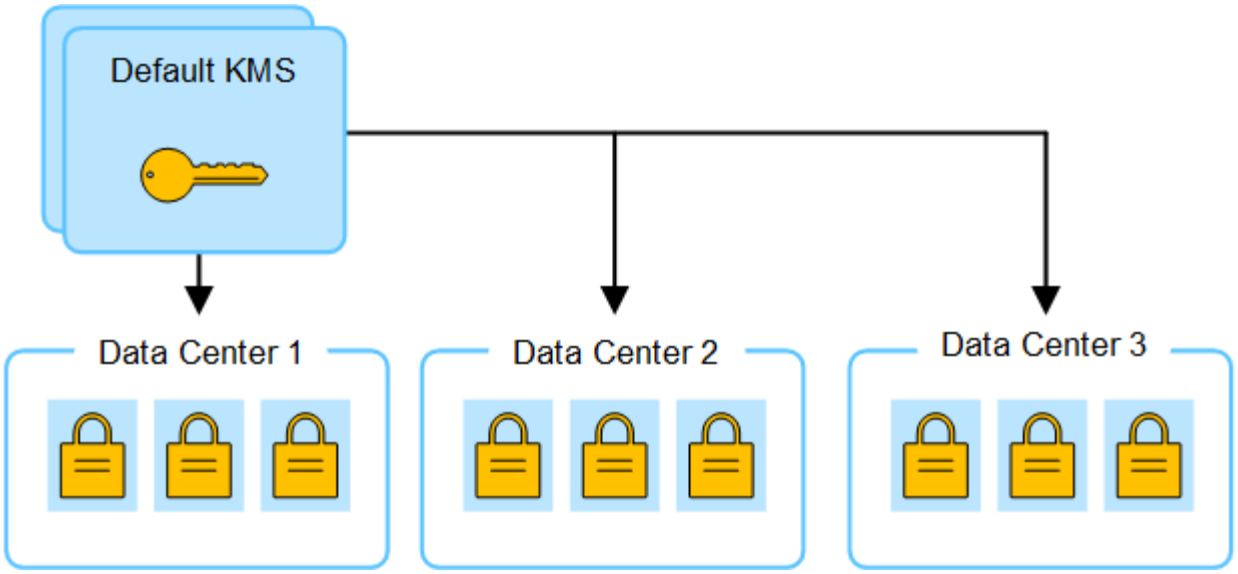
Considérations relatives à la modification du KMS d'un site

Chaque serveur de gestion de clés (KMS) ou cluster KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou sur un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS à un autre.

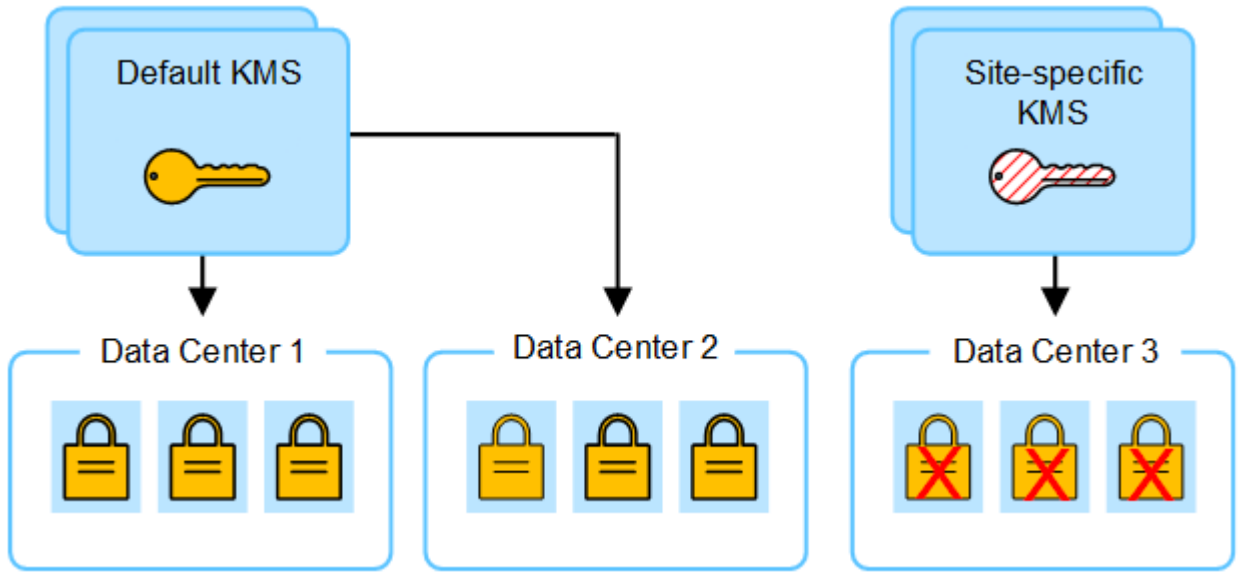
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement du KMS d'origine vers le nouveau KMS. Vous devez vous assurer que le KMS dispose de la clé correcte pour déchiffrer les nœuds d'appliance chiffrés sur le site.

Par exemple:

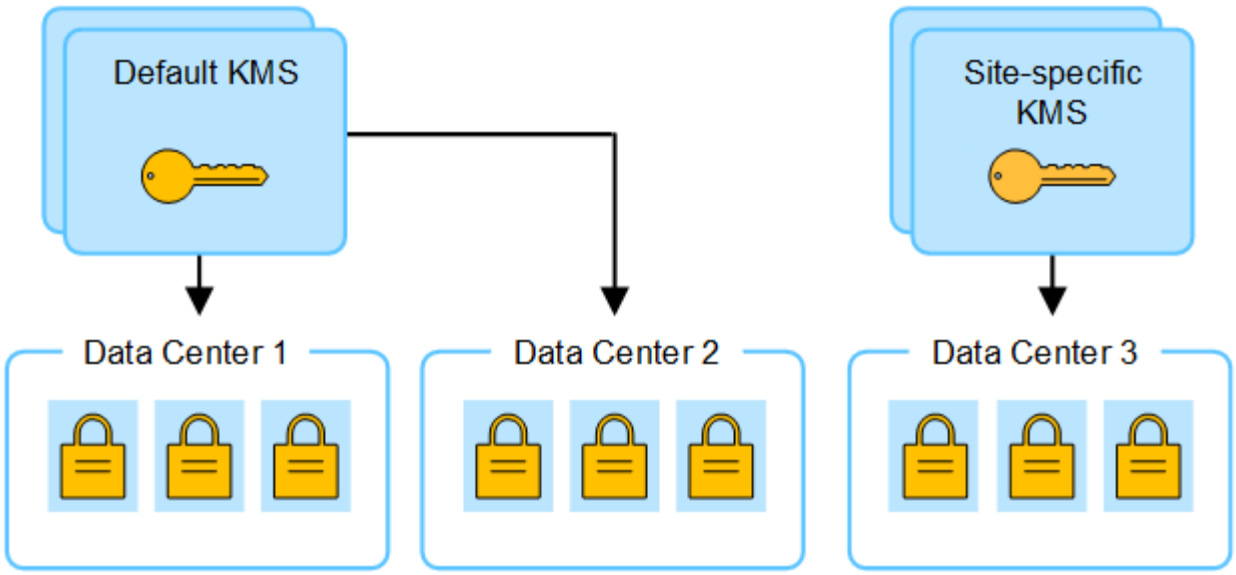
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement de nœud** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour crypter les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces appareils.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 sur la figure). Cependant, étant donné que les nœuds de l'appliance sont déjà chiffrés, une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour déchiffrer les nœuds de ce site.



4. Pour résoudre le problème, copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine sur une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour déchiffrer les nœuds de l'appliance dans le centre de données 3, afin qu'il puisse être enregistré dans StorageGRID.



Cas d'utilisation pour modifier le KMS utilisé pour un site

Le tableau résume les étapes requises pour les cas les plus courants de modification du KMS d'un site.

Cas d'utilisation pour modifier le KMS d'un site	Étapes requises
Vous disposez d'une ou plusieurs entrées KMS spécifiques au site et vous souhaitez utiliser l'une d'entre elles comme KMS par défaut.	Modifier le KMS spécifique au site. Dans le champ **Gère les clés pour**, sélectionnez **Sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera désormais utilisé comme KMS par défaut. Cela s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié. "Modifier un serveur de gestion de clés (KMS)"
Vous disposez d'un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds de l'appliance sur le nouveau site ont déjà été chiffrés par le KMS par défaut, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS par défaut vers un nouveau KMS. 2. À l'aide du gestionnaire de grille, ajoutez le nouveau KMS et sélectionnez le site. "Ajouter un serveur de gestion de clés (KMS)"
Vous souhaitez que le KMS d'un site utilise un serveur différent.	1. Si les nœuds d'appareils du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement du KMS existant vers le nouveau KMS. 2. À l'aide du gestionnaire de grille, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou la nouvelle adresse IP. "Ajouter un serveur de gestion de clés (KMS)"

Configurer StorageGRID en tant que client dans le KMS

Vous devez configurer StorageGRID en tant que client pour chaque serveur de gestion de clés externe ou cluster KMS avant de pouvoir ajouter le KMS à StorageGRID.

> Ces instructions s'appliquent à Thales CipherTrust Manager et Hashicorp Vault. Pour obtenir la liste des produits et versions pris en charge, utilisez le "Outil de matrice d'interopérabilité NetApp (IMT)" .

Étapes

1. À partir du logiciel KMS, créez un client StorageGRID pour chaque KMS ou cluster KMS que vous prévoyez d'utiliser.

   Chaque KMS gère une clé de chiffrement unique pour les nœuds d'appliances StorageGRID sur un seul site ou sur un groupe de sites.

2. Créez une clé en utilisant l'une des deux méthodes suivantes :
   - Utilisez la page de gestion des clés de votre produit KMS. Créez une clé de chiffrement AES pour chaque KMS ou cluster KMS.

     La clé de chiffrement doit être de 2 048 bits ou plus et doit être exportable.

   - Demandez à StorageGRID de créer la clé. Vous serez invité à tester et à enregistrer après"téléchargement de certificats clients" .
3. Enregistrez les informations suivantes pour chaque KMS ou cluster KMS.

   Vous avez besoin de ces informations lorsque vous ajoutez le KMS à StorageGRID:

   - Nom d'hôte ou adresse IP pour chaque serveur.
   - Port KMIP utilisé par le KMS.
   - Alias de clé pour la clé de chiffrement dans le KMS.
4. Pour chaque KMS ou cluster KMS, obtenez un certificat de serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA codés PEM, concaténés dans l'ordre de la chaîne de certificats.

   Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

   - Le certificat doit utiliser le format X.509 codé en base 64 (Privacy Enhanced Mail) PEM.
   - Le champ Nom alternatif du sujet (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.

     > Lorsque vous configurez le KMS dans StorageGRID, vous devez saisir les mêmes noms de domaine complets ou adresses IP dans le champ **Nom d'hôte**.

   - Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.
5. Obtenez le certificat client public émis à StorageGRID par le KMS externe et la clé privée du certificat client.

   Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Ajouter un serveur de gestion de clés (KMS)

Vous utilisez l'assistant du serveur de gestion de clés StorageGRID pour ajouter chaque KMS ou cluster KMS.

Avant de commencer

- Vous avez examiné le"considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés" .
- Tu as"configuré StorageGRID en tant que client dans le KMS" , et vous disposez des informations requises pour chaque KMS ou cluster KMS.
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

À propos de cette tâche

Si possible, configurez tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, tous les appareils chiffrés par nœud dans la grille seront chiffrés par le KMS par défaut. Si vous souhaitez créer ultérieurement un KMS spécifique au site, vous devez d'abord copier la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. Voir"Considérations relatives à la modification du KMS d'un site" pour plus de détails.

Étape 1 : Détails KMS

À l'étape 1 (Détails KMS) de l'assistant Ajouter un serveur de gestion de clés, vous fournissez des détails sur le KMS ou le cluster KMS.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page du serveur de gestion des clés s'affiche avec l'onglet Détails de configuration sélectionné.

2. Sélectionnez **Créer**.

   L'étape 1 (détails KMS) de l'assistant Ajouter un serveur de gestion de clés s'affiche.

3. Saisissez les informations suivantes pour le KMS et le client StorageGRID que vous avez configuré dans ce KMS.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	L'alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. **Remarque** : si vous n'avez pas créé de clé à l'aide de votre produit KMS, vous serez invité à demander à StorageGRID de créer la clé.

Champ	Description
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer tous les serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS doit gérer les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez **Sites non gérés par un autre KMS (KMS par défaut)** pour configurer un KMS par défaut qui s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié et à tous les sites que vous ajouterez dans les extensions ultérieures. **Remarque :** une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui était précédemment chiffré par le KMS par défaut mais que vous n'avez pas fourni la version actuelle de la clé de chiffrement d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications du protocole d'interopérabilité de gestion de clés (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Continuer**.

Étape 2 : Télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat du serveur) de l'assistant Ajouter un serveur de gestion de clés, vous téléchargez le certificat du serveur (ou le groupe de certificats) pour le KMS. Le certificat du serveur permet au KMS externe de s'authentifier auprès de StorageGRID.

Étapes

1. À partir de l'**Étape 2 (Télécharger le certificat du serveur)**, accédez à l'emplacement du certificat de serveur ou du groupe de certificats enregistré.
2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat du serveur apparaissent.

   Si vous avez téléchargé un ensemble de certificats, les métadonnées de chaque certificat apparaissent sur son propre onglet.

3. Sélectionnez **Continuer**.

Étape 3 : Télécharger les certificats clients

À l'étape 3 (Télécharger les certificats clients) de l'assistant Ajouter un serveur de gestion de clés, vous téléchargez le certificat client et la clé privée du certificat client. Le certificat client permet à StorageGRID de s'authentifier auprès du KMS.

Étapes

1. À partir de l'**Étape 3 (Télécharger les certificats clients)**, accédez à l'emplacement du certificat client.
2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client apparaissent.

3. Accédez à l'emplacement de la clé privée du certificat client.
4. Téléchargez le fichier de clé privée.
5. Sélectionnez **Tester et enregistrer**.

   Si une clé n'existe pas, vous êtes invité à demander à StorageGRID d'en créer une.

   Les connexions entre le serveur de gestion des clés et les nœuds de l'appliance sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion de clés est ajouté au tableau sur la page Serveur de gestion de clés.

   > Immédiatement après avoir ajouté un KMS, l'état du certificat sur la page Serveur de gestion des clés apparaît comme Inconnu. Il faudra peut-être jusqu'à 30 minutes à StorageGRID pour obtenir le statut réel de chaque certificat. Vous devez actualiser votre navigateur Web pour voir l'état actuel.

6. Si un message d'erreur s'affiche lorsque vous sélectionnez **Tester et enregistrer**, vérifiez les détails du message, puis sélectionnez **OK**.

   Par exemple, vous pouvez recevoir une erreur 422 : Entité non traitable si un test de connexion a échoué.

7. Si vous devez enregistrer la configuration actuelle sans tester la connexion externe, sélectionnez **Forcer l'enregistrement**.

   > La sélection de **Forcer l'enregistrement** enregistre la configuration KMS, mais ne teste pas la connexion externe de chaque appareil à ce KMS. En cas de problème avec la configuration, vous ne pourrez peut-être pas redémarrer les nœuds de l'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous risquez de perdre l'accès à vos données jusqu'à ce que les problèmes soient résolus.

8. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

   La configuration KMS est enregistrée mais la connexion au KMS n'est pas testée.

Gérer un KMS

La gestion d'un serveur de gestion de clés (KMS) implique l'affichage ou la modification

des détails, la gestion des certificats, l'affichage des nœuds chiffrés et la suppression d'un KMS lorsqu'il n'est plus nécessaire.

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 requise" .

Afficher les détails du KMS

Vous pouvez afficher des informations sur chaque serveur de gestion de clés (KMS) dans votre système StorageGRID , y compris les détails des clés et l'état actuel des certificats serveur et client.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page du serveur de gestion des clés apparaît et affiche les informations suivantes :

   - L'onglet Détails de configuration répertorie tous les serveurs de gestion de clés configurés.
   - L'onglet Nœuds chiffrés répertorie tous les nœuds pour lesquels le chiffrement de nœud est activé.

2. Pour afficher les détails d'un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le nom du KMS. La page de détails du KMS répertorie les informations suivantes :

Champ	Description
Gère les clés pour	Le site StorageGRID associé au KMS. Ce champ affiche le nom d'un site StorageGRID spécifique ou **Sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion de clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il existe plus de deux serveurs de gestion de clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion de clés supplémentaires dans le cluster. Par exemple: `10.10.10.10 and 10.10.10.11` ou `10.10.10.10 and 2 others` . Pour afficher tous les noms d'hôtes d'un cluster, sélectionnez un KMS et sélectionnez **Modifier** ou **Actions** > **Modifier**.

3. Sélectionnez un onglet sur la page des détails du KMS pour afficher les informations suivantes :

Languette	Champ	Description
Détails clés	Nom de la clé	L'alias de clé pour le client StorageGRID dans le KMS.

Languette	Champ	Description
Clé UID	L'identifiant unique de la dernière version de la clé.	Dernière modification
La date et l'heure de la dernière version de la clé.	Certificat de serveur	Métadonnées
Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.	Certificat PEM	Le contenu du fichier PEM (privacy enhanced mail) pour le certificat.
Certificat client	Métadonnées	Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.

4. Aussi souvent que l'exigent les pratiques de sécurité de votre organisation, sélectionnez **Rotate key** ou utilisez le logiciel KMS pour créer une nouvelle version de la clé.

   Lorsque la rotation des clés est réussie, les champs UID de la clé et Dernière modification sont mis à jour.

> Si vous faites pivoter la clé de chiffrement à l'aide du logiciel KMS, faites-la pivoter de la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne tournez pas vers une clé entièrement différente.
>
> N'essayez jamais de faire pivoter une clé en modifiant le nom de la clé (alias) pour le KMS. StorageGRID exige que toutes les versions de clés précédemment utilisées (ainsi que toutes les futures) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé d'un KMS configuré, StorageGRID risque de ne pas être en mesure de déchiffrer vos données.

Gérer les certificats

Résolvez rapidement tout problème de certificat de serveur ou de client. Si possible, remplacez les certificats avant leur expiration.

> Vous devez résoudre tout problème de certificat dès que possible pour maintenir l'accès aux données.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.
2. Dans le tableau, regardez la valeur d'expiration du certificat pour chaque KMS.
3. Si l'expiration du certificat pour un KMS est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.

4. Si la colonne Expiration du certificat indique qu'un certificat a expiré ou est sur le point d'expirer, sélectionnez le KMS pour accéder à la page des détails du KMS.
   a. Sélectionnez **Certificat de serveur** et vérifiez la valeur du champ « Expire le ».
   b. Pour remplacer le certificat, sélectionnez **Modifier le certificat** pour télécharger un nouveau certificat.
   c. Répétez ces sous-étapes et sélectionnez **Certificat client** au lieu de Certificat serveur.
5. Lorsque les alertes **Expiration du certificat KMS CA**, **Expiration du certificat client KMS** et **Expiration du certificat serveur KMS** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

   Il faudra peut-être jusqu'à 30 minutes à StorageGRID pour obtenir les mises à jour concernant l'expiration du certificat. Actualisez votre navigateur Web pour voir les valeurs actuelles.

> Si vous obtenez le statut **L'état du certificat du serveur est inconnu**, assurez-vous que votre KMS permet d'obtenir un certificat de serveur sans nécessiter de certificat client.

Afficher les nœuds chiffrés

Vous pouvez afficher des informations sur les nœuds d'appliance de votre système StorageGRID sur lesquels le paramètre **Chiffrement de nœud** est activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page Serveur de gestion des clés s'affiche. L'onglet Détails de configuration affiche tous les serveurs de gestion de clés qui ont été configurés.

2. En haut de la page, sélectionnez l'onglet **Nœuds chiffrés**.

   L'onglet Nœuds chiffrés répertorie les nœuds d'appliance de votre système StorageGRID pour lesquels le paramètre **Chiffrement de nœud** est activé.

3. Consultez les informations du tableau pour chaque nœud d'appareil.

Colonne	Description
Nom du nœud	Le nom du nœud de l'appareil.
Type de nœud	Le type de nœud : Stockage, Admin ou Passerelle.
Site	Le nom du site StorageGRID sur lequel le nœud est installé.
Nom du KMS	Le nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de configuration pour ajouter un KMS. "Ajouter un serveur de gestion de clés (KMS)"

Colonne	Description
Clé UID	L'ID unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID d'une clé entière, sélectionnez le texte. Un tiret (--) indique que l'UID de la clé est inconnu, probablement en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
Statut	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de la connexion après les modifications de la configuration KMS peut prendre plusieurs minutes. **Remarque :** actualisez votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne Statut indique un problème KMS, résolvez le problème immédiatement.

   Pendant les opérations KMS normales, le statut sera **Connecté à KMS**. Si un nœud est déconnecté du réseau, l'état de connexion du nœud est affiché (Administrativement hors service ou Inconnu).

   D'autres messages d'état correspondent aux alertes StorageGRID portant les mêmes noms :

   - Échec du chargement de la configuration KMS
   - Erreur de connectivité KMS
   - Nom de la clé de chiffrement KMS introuvable
   - Échec de la rotation de la clé de chiffrement KMS
   - La clé KMS n'a pas réussi à déchiffrer un volume d'appareil
   - KMS n'est pas configuré

   Effectuez les actions recommandées pour ces alertes.

> Vous devez résoudre tout problème immédiatement pour garantir que vos données sont entièrement protégées.

Modifier un KMS

Vous devrez peut-être modifier la configuration d'un serveur de gestion de clés, par exemple, si un certificat est sur le point d'expirer.

Avant de commencer

- Si vous envisagez de mettre à jour le site sélectionné pour un KMS, vous avez examiné les"considérations pour modifier le KMS d'un site" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

La page Serveur de gestion des clés apparaît et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS que vous souhaitez modifier, puis sélectionnez **Actions** > **Modifier**.

   Vous pouvez également modifier un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Modifier** sur la page des détails du KMS.

3. Vous pouvez également mettre à jour les détails de l'**Étape 1 (Détails KMS)** de l'assistant Modifier un serveur de gestion de clés.

Champ	Description
Nom du KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	L'alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Vous n'avez besoin de modifier le nom de la clé que dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l'historique des versions du nouvel alias.
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous ne disposez pas déjà d'un KMS par défaut, sélectionnez éventuellement **Sites non gérés par un autre KMS (KMS par défaut)**. Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. **Remarque :** si vous modifiez un KMS spécifique à un site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications du protocole d'interopérabilité de gestion de clés (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez **Ajouter un autre nom d'hôte** pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Continuer**.

   L'étape 2 (Télécharger le certificat du serveur) de l'assistant Modifier un serveur de gestion de clés s'affiche.

6. Si vous devez remplacer le certificat du serveur, sélectionnez **Parcourir** et téléchargez le nouveau fichier.
7. Sélectionnez **Continuer**.

   L'étape 3 (Télécharger les certificats clients) de l'assistant Modifier un serveur de gestion de clés s'affiche.

8. Si vous devez remplacer le certificat client et la clé privée du certificat client, sélectionnez **Parcourir** et téléchargez les nouveaux fichiers.
9. Sélectionnez **Tester et enregistrer**.

   Les connexions entre le serveur de gestion des clés et tous les nœuds d'appareil chiffrés sur les sites concernés sont testées. Si toutes les connexions de nœuds sont valides et que la clé correcte est trouvée sur le KMS, le serveur de gestion de clés est ajouté au tableau sur la page Serveur de gestion de clés.

10. Si un message d'erreur s'affiche, vérifiez les détails du message et sélectionnez **OK**.

    Par exemple, vous pouvez recevoir une erreur 422 : Entité non traitable si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS ou si un test de connexion a échoué.

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **Forcer l'enregistrement**.

    > La sélection de **Forcer l'enregistrement** enregistre la configuration KMS, mais ne teste pas la connexion externe de chaque appareil à ce KMS. En cas de problème avec la configuration, vous ne pourrez peut-être pas redémarrer les nœuds de l'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous risquez de perdre l'accès à vos données jusqu'à ce que les problèmes soient résolus.

    La configuration KMS est enregistrée.

12. Vérifiez l'avertissement de confirmation et sélectionnez **OK** si vous êtes sûr de vouloir forcer l'enregistrement de la configuration.

    La configuration KMS est enregistrée, mais la connexion au KMS n'est pas testée.

Supprimer un serveur de gestion de clés (KMS)

Vous souhaiterez peut-être supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous souhaiterez peut-être supprimer un KMS spécifique à un site si vous avez mis le site hors service.

Avant de commencer

- Vous avez examiné le"considérations et exigences relatives à l'utilisation d'un serveur de gestion de clés" .
- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Vous avez le"Autorisation d'accès root" .

À propos de cette tâche

Vous pouvez supprimer un KMS dans ces cas :

- Vous pouvez supprimer un KMS spécifique à un site si le site a été mis hors service ou si le site n'inclut aucun nœud d'appliance avec le chiffrement de nœud activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site disposant de nœuds d'appliance avec chiffrement de nœud activé.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Serveur de gestion des clés**.

   La page Serveur de gestion des clés apparaît et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS que vous souhaitez supprimer, puis sélectionnez **Actions** > **Supprimer**.

   Vous pouvez également supprimer un KMS en sélectionnant le nom du KMS dans le tableau et en sélectionnant **Supprimer** sur la page des détails du KMS.

3. Confirmez que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique au site pour un site qui ne possède aucun nœud d'appliance avec le chiffrement de nœud activé.
   - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement de nœud.
4. Sélectionnez **Oui**.

   La configuration KMS est supprimée.

Gérer les paramètres de proxy

Configurer le proxy de stockage

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les points de terminaison S3 externes. Par exemple, vous pourriez avoir besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plateforme à des points de terminaison externes, tels qu'un point de terminaison sur Internet.

> Les paramètres de proxy de stockage configurés ne s'appliquent pas aux points de terminaison des services de la plateforme Kafka.

Avant de commencer

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

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy de stockage.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres proxy**.
2. Dans l'onglet **Stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole pour le proxy de stockage.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Si vous le souhaitez, saisissez le port utilisé pour vous connecter au serveur proxy.

Laissez ce champ vide pour utiliser le port par défaut pour le protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

   Une fois le proxy de stockage enregistré, de nouveaux points de terminaison pour les services de plateforme ou les pools de stockage cloud peuvent être configurés et testés.

   > Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages liés au service de la plateforme provenant de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Configurer les paramètres du proxy d'administration

Si vous envoyez des packages AutoSupport via HTTP ou HTTPS, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Pour plus d'informations sur AutoSupport, voir"Configurer AutoSupport" .

Avant de commencer

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

À propos de cette tâche

Vous pouvez configurer les paramètres pour un seul proxy administrateur.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Paramètres proxy**.

   La page Paramètres du proxy s'affiche. Par défaut, Stockage est sélectionné dans le menu des onglets.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy administrateur**.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

   Laissez ces champs vides si votre serveur proxy ne nécessite pas de nom d'utilisateur ou de mot de passe.

7. Sélectionnez l'une des options suivantes :

   - Si vous souhaitez sécuriser la connexion au proxy administrateur, sélectionnez **Vérifier le certificat proxy**. Téléchargez un bundle CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.

AutoSupport à la demande, AutoSupport de la série E via StorageGRID et la détermination du chemin de mise à jour sur la page de mise à niveau de StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

Une fois le bundle CA téléchargé, ses métadonnées s'affichent.

- Si vous ne souhaitez pas valider les certificats lors de la communication avec le serveur proxy d'administration, sélectionnez **Ne pas vérifier le certificat proxy**.

8. Sélectionnez **Enregistrer**.

   Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.

   Les modifications de proxy peuvent prendre jusqu'à 10 minutes pour prendre effet.

9. Si vous devez désactiver le proxy d'administration, décochez la case **Activer le proxy d'administration**, puis sélectionnez **Enregistrer**.

Contrôler les pare-feu

Contrôler l'accès au pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API sur les nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au niveau du pare-feu externe. Par exemple, vous souhaiterez peut-être empêcher les locataires de se connecter au Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne StorageGRID , consultez"Configurer le pare-feu interne" .

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients de l'API de gestion peuvent accéder au gestionnaire de grille, à l'API de gestion de grille, au gestionnaire de locataires et à l'API de gestion de locataires. **Remarque :** le port 443 est également utilisé pour certains trafics internes.
8443	Port Grid Manager restreint sur les nœuds d'administration	• Les navigateurs Web et les clients de l'API de gestion peuvent accéder au Grid Manager et à l'API de gestion de grille à l'aide de HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.

Port	Description	Si le port est ouvert…
9443	Port du gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients de l'API de gestion peuvent accéder au gestionnaire de locataires et à l'API de gestion des locataires à l'aide de HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de grille ou à l'API de gestion de grille. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports restreints Grid Manager ou Tenant Manager. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec l'authentification unique.

Informations connexes

- "Sign in au gestionnaire de grille"
- "Créer un compte locataire"
- "Communications externes"

Gérer les contrôles du pare-feu interne

StorageGRID inclut un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grille spécifique. Les modifications de configuration que vous effectuez sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grille.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès sélectionné aux ports fermés. Vous pouvez ajouter des adresses IP ou des sous-réseaux en notation CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet Gérer l'accès externe.
- **Gérer l'accès externe** : utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : utilisez cet onglet pour spécifier si un nœud approuve le trafic entrant provenant du réseau client.

  Les paramètres de cet onglet remplacent les paramètres de l'onglet Gérer l'accès externe.

  - Un nœud avec un réseau client non approuvé acceptera uniquement les connexions sur les ports de point de terminaison de l'équilibreur de charge configurés sur ce nœud (points de terminaison globaux, d'interface de nœud et de type de nœud).
  - Les ports de point de terminaison de l'équilibreur de charge *sont les seuls ports ouverts* sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet Gérer les réseaux externes.

- Lorsqu'ils sont approuvés, tous les ports ouverts sous l'onglet Gérer l'accès externe sont accessibles, ainsi que tous les points de terminaison d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous définissez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous l'attendez.

Pour configurer les contrôles du pare-feu interne, voir"Configurer les contrôles du pare-feu" .

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez"Contrôler l'accès au pare-feu externe" .

Liste d'adresses privilégiées et onglets Gérer les accès externes

L'onglet Liste d'adresses privilégiées vous permet d'enregistrer une ou plusieurs adresses IP auxquelles l'accès aux ports de grille fermés est accordé. L'onglet Gérer l'accès externe vous permet de fermer l'accès externe aux ports externes sélectionnés ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut par les nœuds non-grille). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour autoriser votre grille.

> Les adresses IP privilégiées n'ont pas d'accès au port de grille interne par défaut.

Exemple 1 : Utiliser un hôte de saut pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de saut (un hôte renforcé en termes de sécurité) pour l'administration du réseau. Vous pouvez utiliser ces étapes générales :

1. Utilisez l'onglet Liste d'adresses privilégiées pour ajouter l'adresse IP de l'hôte de saut.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception de l'hôte de saut. Vous pouvez ensuite utiliser l'hôte de saut pour effectuer des tâches de maintenance sur votre réseau de manière plus sécurisée.

Exemple 2 : Verrouiller les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port (par exemple, SSH sur le port 22). Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet Liste d'adresses privilégiées pour accorder l'accès uniquement aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer l'accès à tous les ports attribués pour accéder à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 8443). Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, le port 22 et le service SSH seront disponibles pour les hôtes de la liste d'adresses privilégiées. Tous les autres hôtes se verront refuser l'accès au service, quelle que soit l'interface d'où provient la demande.

Exemple 3 : Désactiver l'accès aux services inutilisés

Au niveau du réseau, vous pouvez désactiver certains services que vous n'avez pas l'intention d'utiliser. Par exemple, pour bloquer le trafic client HTTP S3, vous utiliseriez le bouton bascule de l'onglet Gérer l'accès externe pour bloquer le port 18084.

Onglet Réseaux de clients non approuvés

Si vous utilisez un réseau client, vous pouvez contribuer à sécuriser StorageGRID contre les attaques hostiles en acceptant le trafic client entrant uniquement sur les points de terminaison explicitement configurés.

Par défaut, le réseau client sur chaque nœud de grille est *fiable*. Autrement dit, par défaut, StorageGRID approuve les connexions entrantes vers chaque nœud de grille sur tous les"ports externes disponibles" .

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud doit être *non fiable*. Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés comme points de terminaison d'équilibrage de charge. Voir"Configurer les points de terminaison de l'équilibreur de charge" et"Configurer les contrôles du pare-feu" .

Exemple 1 : le nœud de passerelle accepte uniquement les requêtes HTTPS S3

Supposons que vous souhaitiez qu'un nœud de passerelle refuse tout le trafic entrant sur le réseau client, à l'exception des requêtes HTTPS S3. Vous effectueriez ces étapes générales :

1. De la"Points de terminaison de l'équilibreur de charge" page, configurez un point de terminaison d'équilibrage de charge pour S3 via HTTPS sur le port 443.
2. Dans la page de contrôle du pare-feu, sélectionnez Non approuvé pour spécifier que le réseau client sur le nœud de passerelle n'est pas approuvé.

Une fois votre configuration enregistrée, tout le trafic entrant sur le réseau client du nœud de passerelle est supprimé, à l'exception des requêtes HTTPS S3 sur le port 443 et des requêtes d'écho ICMP (ping).

Exemple 2 : Le nœud de stockage envoie des demandes de services de la plateforme S3

Supposons que vous souhaitiez activer le trafic sortant des services de la plateforme S3 à partir d'un nœud de stockage, mais que vous souhaitiez empêcher toute connexion entrante vers ce nœud de stockage sur le réseau client. Vous effectueriez cette étape générale :

- Dans l'onglet Réseaux clients non approuvés de la page de contrôle du pare-feu, indiquez que le réseau client sur le nœud de stockage n'est pas approuvé.

Une fois votre configuration enregistrée, le nœud de stockage n'accepte plus aucun trafic entrant sur le réseau client, mais il continue d'autoriser les demandes sortantes vers les destinations des services de plate-forme configurées.

Exemple 3 : Limitation de l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès de Grid Manager uniquement sur un sous-réseau spécifique. Vous effectuerez les étapes suivantes :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet Réseau client non approuvé pour configurer le réseau client comme non approuvé.
3. Lorsque vous créez un point de terminaison d'équilibrage de charge d'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour le réseau client non approuvé.
5. Utilisez l'onglet Gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes en dehors de ce sous-réseau).

Une fois votre configuration enregistrée, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder au gestionnaire de grille. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne

Vous pouvez configurer le pare-feu StorageGRID pour contrôler l'accès réseau à des ports spécifiques sur vos nœuds StorageGRID .

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un"navigateur Web pris en charge" .
- Tu as"autorisations d'accès spécifiques" .
- Vous avez examiné les informations contenues dans"Gérer les contrôles du pare-feu" et"Directives de mise en réseau" .
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des points de terminaison explicitement configurés, vous avez défini les points de terminaison de l'équilibreur de charge.

> ⓘ Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

À propos de cette tâche

StorageGRID inclut un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains des ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer les ports ouverts par défaut sur le réseau de grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant provenant du réseau client et vous pouvez configurer l'accès de ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre réseau à ceux qui sont absolument nécessaires améliore la sécurité de votre réseau. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles de pare-feu, y compris des exemples, consultez"Gérer les contrôles du pare-feu" .

Pour plus d'informations sur les pare-feu externes et la sécurité du réseau, consultez"Contrôler l'accès au pare-feu externe" .

Contrôles du pare-feu d'accès

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans"Gérer les contrôles du pare-feu" .

2. Sélectionnez n'importe quel onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez sur un onglet ne limitent pas ce que vous pouvez faire sur les autres onglets ; cependant, les modifications de configuration que vous apportez sur un onglet peuvent modifier le comportement des ports configurés sur d'autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet Liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par les paramètres de l'onglet Gérer l'accès externe.

Les adresses IP privilégiées et les sous-réseaux n'ont pas d'accès au réseau interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste d'adresses privilégiées sont accessibles même s'ils sont bloqués dans l'onglet Gérer l'accès externe.

> Les paramètres de l'onglet Liste d'adresses privilégiées ne peuvent pas remplacer les paramètres de l'onglet Réseau client non approuvé.

Étapes

1. Dans l'onglet Liste d'adresses privilégiées, entrez l'adresse ou le sous-réseau IP auquel vous souhaitez accorder l'accès aux ports fermés.
2. Vous pouvez également sélectionner **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.

   > Ajoutez le moins d'adresses possible à la liste privilégiée.

3. Si vous le souhaitez, sélectionnez *Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID *. Voir "Ports internes StorageGRID" .

   > Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer les accès externes

Lorsqu'un port est fermé dans l'onglet Gérer l'accès externe, le port n'est pas accessible par une adresse IP non-grille, sauf si vous ajoutez l'adresse IP à la liste d'adresses privilégiées. Vous ne pouvez fermer que les ports ouverts par défaut et vous ne pouvez ouvrir que les ports que vous avez fermés.

Les paramètres de l'onglet Gérer l'accès externe ne peuvent pas remplacer les paramètres de l'onglet Réseau client non approuvé. Par exemple, si un nœud n'est pas approuvé, le port SSH/22 est bloqué sur le réseau client même s'il est ouvert dans l'onglet Gérer l'accès externe. Les paramètres de l'onglet Réseau client non approuvé remplacent les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **Gérer l'accès externe**. L'onglet affiche un tableau avec tous les ports externes (ports accessibles par défaut par les nœuds non-grille) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez le bouton bascule à côté de chaque port pour ouvrir ou fermer le port sélectionné.
   - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
   - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports répertoriés dans le tableau.

   Si vous fermez les ports 443 ou 8443 de Grid Manager, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

   Utilisez la barre de défilement sur le côté droit du tableau pour vous assurer d'avoir visualisé tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en saisissant un numéro de port. Vous pouvez saisir un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne « 2 » sont affichés.
3. Sélectionnez **Enregistrer**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points de terminaison d'équilibrage de charge et, éventuellement, les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour spécifier le paramètre par défaut des nouveaux nœuds ajoutés dans une extension.

Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Les modifications de configuration que vous effectuez dans l'onglet **Réseau client non approuvé** remplacent les paramètres de l'onglet **Gérer l'accès externe**.

Étapes

1. Sélectionnez **Réseau client non approuvé**.
2. Dans la section Définir la valeur par défaut du nouveau nœud, spécifiez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans le cadre d'une procédure d'extension.
   - **Fiable** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est approuvé.
   - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable.

     Si nécessaire, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.

Ce paramètre n’affecte pas les nœuds existants dans votre système StorageGRID .

3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les points de terminaison d’équilibrage de charge explicitement configurés ou sur des ports sélectionnés supplémentaires :

   - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste des réseaux clients non approuvés.
   - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Réseau client non approuvé.
   - Utilisez le bouton bascule à côté de chaque nœud pour définir le réseau client comme approuvé ou non approuvé pour le nœud sélectionné.

   Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste des réseaux clients non approuvés, puis utiliser le bouton bascule à côté d’un nœud individuel pour ajouter ce nœud unique à la liste des réseaux clients approuvés.

   Utilisez la barre de défilement sur le côté droit du tableau pour vous assurer d’avoir visualisé tous les nœuds disponibles. Utilisez le champ de recherche pour trouver les paramètres de n’importe quel nœud en saisissant le nom du nœud. Vous pouvez saisir un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds dont le nom contient la chaîne « GW » sont affichés.

4. Sélectionnez **Enregistrer**.

   Les nouveaux paramètres du pare-feu sont immédiatement appliqués et mis en œuvre. Les connexions client existantes peuvent échouer si les points de terminaison de l’équilibreur de charge n’ont pas été configurés.

Informations sur le copyright

Informations sur les marques commerciales