Gérer la sécurité

StorageGRID software

NetApp
July 23, 2026

Sommaire

Gérer la sécurité

Gérer la sécurité dans StorageGRID

Vous pouvez configurer différents paramètres de sécurité depuis le Grid Manager pour contribuer à la sécurité de votre système StorageGRID.

Gérer le chiffrement

StorageGRID propose plusieurs options de chiffrement des données. Il vous appartient "examiner les méthodes de chiffrement disponibles" de déterminer celles qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

Vous pouvez "configurer et gérer les certificats du serveur" utiliser 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 des clés

L'utilisation d'une "serveur de gestion des clés" vous permet de protéger les données StorageGRID même si un dispositif est retiré du centre de données. Une fois les volumes du dispositif chiffrés, vous ne pouvez accéder à aucune donnée sur le dispositif à moins que le nœud puisse communiquer avec le KMS.

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

Gérer les paramètres du proxy

Si vous utilisez les services de la plateforme S3 ou des Cloud Storage Pools, vous pouvez configurer une "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.

Contrôlez les pare-feu

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

Passez en revue les méthodes de chiffrement de StorageGRID

StorageGRID propose plusieurs options de chiffrement des données. Vous devez examiner les méthodes disponibles afin de déterminer celles qui répondent à vos exigences en matière de protection des données.

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

Option de chiffrement	Comment ça marche	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous "configurer un serveur de gestion de clés" pour le site StorageGRID et "activer le chiffrement pour l'appliance". Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et déchiffre la clé de chiffrement (DEK) sur chaque volume.	Les nœuds d'appliance dont la fonction **Node Encryption** est activée lors de l'installation. Toutes les données sur l'appliance sont protégées contre toute perte physique ou tout retrait du centre de données. **Remarque** : La gestion des clés de chiffrement avec un KMS n'est prise en charge que pour les nœuds de stockage et les appliances de services.
Page de chiffrement du disque dans l'installateur de l'appliance StorageGRID	Si l'appliance contient des disques prenant en charge le chiffrement matériel, vous pouvez définir une phrase secrète de disque lors de l'installation. Lorsque vous définissez une phrase secrète de disque, il est impossible pour quiconque de récupérer des données valides à partir de disques retirés du système, à moins de connaître la phrase secrète. Avant de commencer l'installation, allez dans **Configure Hardware** > **Drive Encryption** pour définir une phrase secrète de disque qui s'appliquera à tous les disques à chiffrement automatique gérés par StorageGRID dans un nœud.	Les appareils équipés de disques à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre la perte physique ou le retrait du centre de données. Le chiffrement des disques ne s'applique pas aux disques gérés par SANtricity. Si vous disposez d'un système de stockage avec des disques à chiffrement automatique et des contrôleurs SANtricity, vous pouvez activer la sécurité des disques dans SANtricity.
Sécurité des disques dans SANtricity System Manager	Si la fonction de sécurité des disques est activée pour votre StorageGRID appliance, vous pouvez utiliser "SANtricity System Manager" pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données des disques sécurisés.	Les appliances de stockage équipées de disques à chiffrement intégral (FDE) ou de disques à chiffrement automatique. Toutes les données sur les disques sécurisés sont protégées contre la perte physique ou le retrait du centre de données. Ne peut pas être utilisé avec certains appliances de stockage ni avec aucune appliance de services.

Option de chiffrement	Comment ça marche	S'applique à
Chiffrement des objets stockés	Vous activez l'option "Chiffrement des objets stockés" dans le Gestionnaire de grille. Une fois activée, tous les nouveaux objets qui ne sont pas chiffrés au niveau du compartiment 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 envoyez une requête PutBucketEncryption pour activer le chiffrement du compartiment. Tous les nouveaux objets qui ne sont pas chiffrés au niveau de l'objet sont chiffrés lors de leur ingestion.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets existants du compartiment ne sont pas chiffrés. Les métadonnées des objets et autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"
Chiffrement côté serveur des objets S3 (SSE)	Vous envoyez une requête S3 pour stocker un objet et incluez l `x-amz-server-side-encryption` en-tête de la requête.	Données d'objet S3 nouvellement ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées de l'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le chiffrement côté serveur"
Chiffrement côté serveur S3 des objets avec des clés fournies par le client (SSE-C)	Vous envoyez 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 chiffrement doit être spécifié pour l'objet. Les métadonnées de l'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors de StorageGRID. "Utilisez le chiffrement côté serveur"

Option de chiffrement	Comment ça marche	S'applique à
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement externe à StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, les métadonnées et les données de configuration système, en supposant que chaque volume ou banque de données soit chiffré. Une méthode de chiffrement externe offre un contrôle plus strict sur les algorithmes de chiffrement et les clés de chiffrement. Elle peut être combinée avec les autres méthodes mentionnées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement externe à StorageGRID pour chiffrer les données et les métadonnées des objets avant leur ingestion dans StorageGRID.	Données et métadonnées de l'objet uniquement (les données de configuration système ne sont pas chiffrées). Une méthode de chiffrement externe offre un contrôle plus strict sur les algorithmes de chiffrement et les clés de chiffrement. Elle peut être combinée avec les autres méthodes mentionnées. "Amazon Simple Storage Service - Guide de l'utilisateur : Protection des données à l'aide du chiffrement côté client"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement simultanément. Par exemple :

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et également utiliser la fonction de sécurité des disques dans SANtricity System Manager pour « double chiffrer » les données sur les disques à chiffrement automatique des 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 lors de leur ingestion.

Si seule une petite partie de vos objets nécessite un chiffrement, envisagez de contrôler le chiffrement au niveau du compartiment ou de chaque objet à la place. L'activation de plusieurs niveaux de chiffrement engendre un coût supplémentaire en termes de performances.

Informations connexes

"Découvrez les options de chiffrement certifiées FIPS"

Gérer les certificats

Gérer les certificats de sécurité dans StorageGRID

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 chiffrent 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 compare 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 CA Grid par défaut

StorageGRID intègre une autorité de certification (CA) qui génère un certificat Grid CA interne lors de l'installation du système. Le certificat Grid CA est utilisé par défaut pour sécuriser le trafic interne de StorageGRID. Une autorité de certification (CA) externe peut émettre des certificats personnalisés, entièrement conformes aux politiques de sécurité informatique de votre organisation.

Utilisez le certificat de l'autorité de certification Grid pour les environnements hors production. Pour la production, utilisez des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont prises en charge, mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne remplacent pas les certificats internes ; toutefois, ce sont les certificats personnalisés qui doivent être spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent respecter les "Recommandations de renforcement du système pour les certificats de serveur".
- StorageGRID prend en charge le regroupement des certificats d'une autorité de certification dans un seul fichier (appelé ensemble de certificats d'une autorité de certification).

> ⓘ StorageGRID inclut également des certificats d'autorité de certification (CA) du système d'exploitation, identiques sur toutes les grilles. En environnement de production, veillez à spécifier un certificat personnalisé signé par une autorité de certification externe, en remplacement du certificat CA du système d'exploitation.

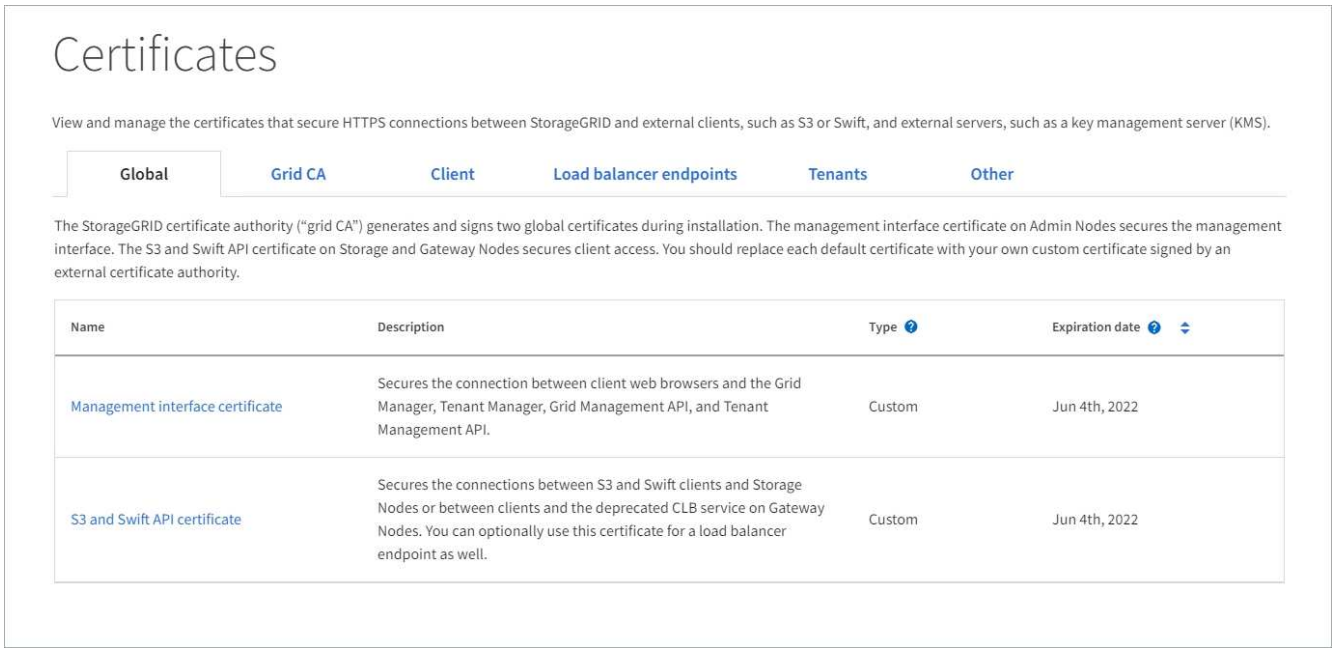
Les différents types de certificats serveur et client sont implémentés de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID avant de configurer le système.

Certificats de sécurité d'accès

Vous pouvez accéder aux informations concernant tous les certificats StorageGRID en un seul endroit, ainsi qu'aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Dans Grid Manager, sélectionnez **Configuration** > **Security** > **Certificates**.



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

   - **Global** : Sécurise l'accès à StorageGRID depuis les navigateurs web et les clients API externes.
   - **Autorité de certification Grid** : Sécurise le trafic interne de StorageGRID.
   - **Client** : Sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
   - **Points de terminaison de l'équilibreur de charge** : Sécurisent les connexions entre les clients S3 et l'équilibreur de charge StorageGRID.
   - **Locataires** : Sécurise les connexions aux serveurs de fédération d'identité ou depuis les points de terminaison de service de la plateforme vers les 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 supplémentaires sur le certificat.

Global

Les certificats globaux sécurisent l'accès à StorageGRID depuis les navigateurs web et les clients API S3 externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La bonne 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 des navigateurs web clients 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 clientes S3 utilisent pour charger et télécharger des données d'objet.

Les informations relatives aux certificats globaux installés comprennent :

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

Vous pouvez :

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour une sécurité renforcée de la grille :
  - "Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID" Utilisé pour les connexions de Grid Manager et de Tenant Manager.
  - "Remplacez le certificat de l'API S3"utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (optionnel).
- "Restaurez le certificat d'interface de gestion par défaut".
- "Restaurez le certificat d'API S3 par défaut".
- "Utilisez 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".

Grid CA

Le Certificat d'autorité de certification Grid généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic interne de StorageGRID.

Les informations relatives au certificat comprennent la date d'expiration du certificat et le contenu du certificat.

Vous pouvez "Copiez ou téléchargez le certificat Grid CA", mais vous ne pouvez pas le changer.

Client

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

Le tableau 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 sa date d'expiration.

Vous pouvez :

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

points de terminaison de l'équilibreur de charge

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

Le tableau des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison configuré et indique si le certificat d'API S3 global ou un certificat personnalisé de point de terminaison d'équilibreur de charge 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.

Vous pouvez :

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

locataires

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

Le tableau 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.

Vous pouvez :

- "Sélectionnez un nom de locataire pour vous connecter au Tenant Manager"
- "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 du locataire"
- "Spécifiez 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. Les autres certificats de sécurité incluent :

- Certificats du pool de stockage cloud
- Certificats de notification d'alerte par e-mail
- Certificats de serveur syslog externe
- Certificats de connexion à la fédération de grille
- Certificats de fédération d'identité
- Certificats de serveur de gestion de clés (KMS)
- Certificats d'authentification unique

Les informations indiquent le type de certificat qu'une fonction utilise ainsi que les dates d'expiration de ses certificats serveur et client, le cas échéant. Sélectionner un nom de fonction ouvre un onglet du navigateur où vous pouvez consulter et modifier les détails du certificat.

> Vous ne pouvez consulter et accéder aux informations des autres certificats que si vous disposez du "autorisation appropriée".

Vous pouvez :

- "Spécifiez un certificat de Cloud Storage Pool pour S3, C2S S3 ou Azure"
- "Spécifiez un certificat pour les notifications par e-mail d'alerte"
- "Utilisez un certificat pour un serveur syslog externe"
- "Faites pivoter les certificats de connexion à la fédération de grille"
- "Afficher et modifier un certificat de fédération d'identité"
- "Téléversez les certificats serveur et client du serveur de gestion des clés (KMS)"
- "Spécifiez manuellement un certificat SSO pour une relation d'approbation de partie utilisatrice"

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 au Grid Manager et au Tenant Manager sans avertissement de sécurité. Ce certificat authentifie également les connexions à l'API de gestion de la grille et à l'API de gestion des locataires. 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 **S3 API certificate**	"Configurer les certificats de l'API S3"

Certificat d'autorité de certification Grid

Voir la Description du certificat d'autorité de certification Default Grid.

Certificat client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, il permet à StorageGRID d'authentifier l'accès des clients externes. • Permet aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID. • 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'équilibrage de charge lors de la configuration d'un point de terminaison d'équilibrage de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer des données d'objets. Vous pouvez également utiliser une version personnalisée du Certificat API S3 certificat global pour authentifier les connexions au service de Load Balancer. Si le certificat global est utilisé pour authentifier les connexions au Load Balancer, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque point de terminaison du Load Balancer. **Remarque :** Le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus fréquemment utilisé lors du 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 Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un StorageGRID Cloud Storage Pool à un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob storage. 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 courriel

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID qui est 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 (CA) du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP exige des certificats clients pour l'authentification.	**Alertes** > **Configuration des e-mails**	"Configurer les 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 de syslog**	"Utilisez un serveur syslog externe"

Certificat de connexion à la fédération Grid

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et chiffrez les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grilles.	**Configuration** > **Système** > **Fédération de grilles**	• "Créer des connexions de fédération de grille" • "Rotation des 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, ce qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	**Configuration** > **Contrôle d'accès** > **Fédération d'identité**	"Utilisez la fédération d'identités"

certificat de 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 des 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.	**Tenant Manager** > **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**	"Créer un point de terminaison de services de plateforme" "Modifier le point de terminaison des services de 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 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 fait office de 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 téléversez 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 via 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 compare la signature du serveur à celle figurant sur sa copie du certificat. Si les signatures correspondent, le client établit 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 fait office de client.

1. À l'aide d'un logiciel Key Management Server externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat serveur signé par une autorité de certification (CA), un certificat client public et la clé privée du certificat client.
2. À l'aide de Grid Manager, 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 requête au serveur KMS qui inclut des 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 serveur pris en charge dans StorageGRID

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 "rétablir temporairement 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".

Configurez les certificats d'interface de gestion dans StorageGRID

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un certificat personnalisé unique permettant aux utilisateurs d'accéder au Grid Manager et au Tenant Manager sans rencontrer d'avertissements de sécurité. Vous pouvez également rétablir le 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 la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat d'interface de gestion personnalisé commun 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 un certificat générique ou multidomaine si les clients

doivent vérifier le nom d'hôte lors de la connexion au Grid Manager et au Tenant Manager. Définissez le certificat personnalisé de manière à ce qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez effectuer la configuration sur le serveur et, selon l'autorité de certification racine (CA) que vous utilisez, les utilisateurs devront peut-être également installer le certificat de l'autorité de certification Grid dans le navigateur web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.

> Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration du certificat serveur pour l'interface de gestion** est déclenchée lorsque ce certificat est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en vérifiant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

> Si vous accédez au Gestionnaire de grille ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans possibilité de contournement si l'une des situations suivantes se produit :
>
> - Votre certificat d'interface de gestion personnalisée expire.
> - Vousrevenir d'un certificat d'interface de gestion personnalisé au certificat du 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 de Grid Manager.

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

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

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

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

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

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez importé. Si vous avez importé un ensemble CA optionnel, chaque certificat s'affiche dans 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 son 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

Générez les fichiers de certificat du serveur.

> La bonne 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 complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : Laissez cette case cochée, 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 du certificat généré.

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

     Spécifiez le nom du fichier de certificat et son 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 une journée pour que les alertes d'expiration de certificat associées disparaissent.

6. Après avoir ajouté un certificat d'interface de gestion personnalisé, la page du certificat d'interface de gestion affiche des informations détaillées sur les certificats utilisés. Vous pouvez télécharger ou copier le PEM du certificat si nécessaire.

Restaurez 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 serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés 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.

Utilisez 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

- Vous avez "autorisations d'accès spécifiques".
- Vous avez le `Passwords.txt` fichier.

À propos de cette tâche

La bonne 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. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

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

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`.
   - Définissez `--type` sur `management` pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et Tenant Manager.
   - Par défaut, les certificats générés sont valides pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser l'argument `--days` pour remplacer la période de validité par défaut.

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

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

Le résultat obtenu 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'invite de commandes. `$ exit`
6. Vérifiez que le certificat a été configuré :
   a. Accédez au Grid Manager.
   b. Sélectionnez **Configuration** > **Sécurité** > **Certificats**
   c. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
7. Configurez votre client de gestion pour qu'il utilise le certificat public que vous avez copié. Incluez les balises BEGIN et END.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat d'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 **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le fichier du bundle CA `.pem`. Si vous utilisez un bundle CA optionnel, chaque certificat du bundle s'affiche dans son propre sous-onglet.

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

   Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble CA optionnel, 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 ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble 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 d'API S3 dans StorageGRID

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

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

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat serveur X.509 signé par la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat serveur personnalisé unique et la clé privée correspondante.

Un seul certificat serveur personnalisé est utilisé pour tous les nœuds de stockage, donc vous devez spécifier le certificat comme un 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 du 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 éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte « Expiration du certificat serveur global pour l'API S3 » est déclenchée lorsque le certificat racine du serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en consultant la date d'expiration du certificat de l'API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat d'API S3 personnalisé.

Ajouter un certificat d'API S3 personnalisé

Étapes

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

Télécharger le certificat

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

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

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **Ensemble d'autorités de certification (CA bundle)** : Fichier optionnel unique contenant les certificats de chaque autorité de certification intermédiaire. Le fichier doit contenir chaque fichier de certificat d'autorité de certification au format PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM de chaque certificat d'API S3 personnalisé que vous avez chargé. Si vous avez chargé un bundle CA optionnel, chaque certificat s'affiche dans 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 son 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 serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

Générer un certificat

Générez 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 complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : Laissez cette case cochée, 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 d'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 son 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 serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat 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 une journée 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 d'API S3 personnalisé, la page du certificat d'API S3 affiche des informations détaillées sur le certificat d'API S3 personnalisé actuellement utilisé. Vous pouvez télécharger ou copier le PEM du certificat selon vos besoins.

Restaurez le certificat d'API S3 par défaut

Vous pouvez rétablir l'utilisation du certificat d'API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat d'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 **S3 API certificate**.
3. Sélectionnez **Utiliser le certificat par défaut**.

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

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

   Si vous disposez des droits d'accès root 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 avec le certificat API S3 par défaut s'affiche. Accédez à "Configurer les points de terminaison de l'équilibreur de charge" pour modifier ou supprimer les points de terminaison concernés.

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

Téléchargez ou copiez le certificat de l'API S3

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

Étapes

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

Téléchargez le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le fichier du bundle CA `.pem`. Si vous utilisez un bundle CA optionnel, chaque certificat du bundle s'affiche dans son propre sous-onglet.

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

   Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble CA optionnel, 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 ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble 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

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

Copiez le certificat d'autorité de certification (CA) StorageGRID Grid

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

Avant de commencer

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

À propos de cette tâche

Si un certificat serveur personnalisé a été configuré, les applications clientes doivent vérifier le serveur à l'aide de ce certificat serveur personnalisé. Elles ne doivent pas copier le certificat d'autorité de certification du système StorageGRID.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le 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 cette validation stricte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lors de la configuration du point de terminaison de l'équilibreur de charge.

Avant de commencer

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

À propos de cette tâche

Lors de la création d'un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat serveur auto-signé ou importer un certificat signé par une autorité de certification (CA) reconnue. Dans les environnements de production, vous devez utiliser un certificat signé par une CA reconnue. Les certificats signés par une CA peuvent être renouvelés sans interruption de service. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type homme du milieu.

Les étapes suivantes fournissent des instructions générales pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures détaillées, consultez "Configurer StorageGRID pour FabricPool".

Étapes

1. Vous pouvez éventuellement configurer un groupe à haute disponibilité (HA) pour que FabricPool puisse l'utiliser.
2. Créez un point de terminaison d'équilibrage de charge S3 pour que FabricPool puisse l'utiliser.

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, éventuellement, le bundle d'autorité de certification.

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

   Veuillez indiquer le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat d'autorité de certification que vous avez importé. Ensuite, fournissez le certificat d'autorité de certification.

> ⓘ Si le certificat StorageGRID a été émis par une autorité de certification intermédiaire, 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.

Configurez les certificats clients dans StorageGRID

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID, offrant ainsi un moyen sécurisé pour les 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 de Grid Manager et copier les informations du certificat dans l'outil externe.

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

> ⓘ Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat serveur est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel 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 concernant "téléchargement d'un certificat client KMS".

Avant de commencer

- Vous disposez des droits d'accès root.
- Vous êtes connecté au Gestionnaire de grille 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 de l'interface de gestion StorageGRID, vous disposez de l'autorité de certification, du certificat client et de la clé privée utilisés pour configurer le certificat de l'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 lors de sa création. Si vous ne possédez pas 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 (le cas échéant) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

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

- Le certificat d'interface de gestion est déjà configuré
- Certificat client délivré par CA
- Certificat généré par Grid Manager

Le certificat d'interface de gestion est 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 fournie par le client, d'un certificat client et d'une clé privée.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **Configuration** > **Sécurité** > **Certificats**, puis sélectionnez l'onglet **Client**.
2. Sélectionnez **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre les certificats**, téléversez le certificat de l'interface de gestion.
   a. Sélectionnez **Téléverser 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 Grid Manager.

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

Certificat client délivré par CA

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 et une clé privée émis par une autorité de certification (CA).

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 **Add**.
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continue**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle d'autorité de certification :
   a. Sélectionnez **Téléverser le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez les fichiers du certificat client, de la clé privée et du bundle CA (`.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 Grid Manager.

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

Certificat généré par 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 **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre des certificats**, sélectionnez **Générer un certificat**.
7. Spécifiez les informations du certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom unique (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

     Ces extensions définissent la finalité de la clé contenue dans le certificat.

Laissez cette case cochée 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 plus consulter 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 son 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 dans un fichier.

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

10. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

    Le nouveau certificat apparaît dans l'onglet Client.

11. Dans le Grid Manager, sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Global**.
12. Sélectionnez **certificat d'interface de gestion**.
13. Sélectionnez **Utiliser un certificat personnalisé**.
14. Téléversez les fichiers certificate.pem et private_key.pem de l'Détails du certificat clientétape. Il n'est pas nécessaire de téléverser le bundle CA.
    a. Sélectionnez **Téléverser le certificat** puis **Continuer**.
    b. Téléchargez chaque fichier de certificat (`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans le Grid Manager.

       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 n'a pas besoin de 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 **l'authentification client TLS** et **Avec certificat d'autorité de certification (CA)**.

d. Sous Détails d'authentification TLS/SSL, copiez et collez :
   - Le certificat CA de l'interface de gestion à **CA Cert**
   - Le certificat client à **Client Cert**
   - La clé privée de **Client Key**

e. **ServerName** : Entrez 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 depuis StorageGRID ou un fichier local.

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

   Pour plus d'informations sur les indicateurs, consultez le "Instructions pour la surveillance StorageGRID".

Modifier les certificats clients

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

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

   Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis **Modifier le nom et les permissions**
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le Grid Manager.

   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** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

   Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche 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 **Téléverser le certificat** puis **Continuer**.

b. Téléchargez 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 son 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 Grid Manager.

   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 unique (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

     Ces extensions définissent la finalité de la clé contenue dans le certificat.

     Laissez cette case cochée 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 plus consulter 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 son 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 dans un fichier.

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

e. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

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** > **Security** > **Certificates** 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

Téléchargez le fichier de certificat `.pem`.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le 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** > **Security** > **Certificates** 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** > **Delete**.

Après la suppression d'un certificat, les clients qui utilisaient ce certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Configurer les paramètres de sécurité

Gérez la politique TLS et SSH dans StorageGRID

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

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

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

Avant de commencer

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

Sélectionnez une politique de sécurité

Étapes

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

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

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

Compatibilité moderne (par défaut)

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

Compatibilité héritée

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

Critères communs

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

FIPS strict

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

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

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

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

- NetApp StorageGRID module API de chiffrement du noyau

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

  - Collecte d'entropie
  - Chiffrement du nœud

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

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

Personnalisé

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

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

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

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

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

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

   Une coche verte apparaît à côté de **Current policy** sur la vignette de la politique.

Créer une politique de sécurité personnalisée

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

Étapes

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

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

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

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

Rétablir temporairement la politique de sécurité par défaut

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

Vous pouvez temporairement rétablir la politique de sécurité par défaut.

Étapes

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

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

2. Exécutez la commande suivante :

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

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

Configurer la sécurité du réseau et des objets StorageGRID

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

Chiffrement des objets stockés

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

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

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

Empêcher la modification du client

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

API REST S3

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

Activer HTTP pour les connexions au nœud de stockage

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

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

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

Sélectionnez les options

Avant de commencer

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

Étapes

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

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

5. Vous pouvez également sélectionner **Activer HTTP pour les connexions aux nœuds de stockage** si les clients se connectent directement aux nœuds de stockage et que vous souhaitez utiliser des connexions HTTP.

   Soyez prudent lorsque vous activez le protocole HTTP pour une grille de production, car les requêtes seront envoyées sans chiffrement.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface StorageGRID

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

Avant de commencer

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

À propos de cette tâche

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

Délai d'inactivité du navigateur

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

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

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

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

Trace de pile de l'API de gestion

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

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

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **Interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :
   a. Déployez l'accordéon.
   b. Pour modifier le délai d'expiration, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai d'expiration par défaut est de 15 minutes.

c. Pour désactiver cette fonctionnalité, décochez la case.

d. Sélectionnez **Enregistrer**.

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

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

a. Déployez l'accordéon.

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

Laissez la trace de pile désactivée dans les environnements de production afin d'éviter de révéler des détails internes du logiciel en cas d'erreurs d'API.

c. Sélectionnez **Enregistrer**.

Gérer l'accès SSH externe dans StorageGRID

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

Avant de commencer

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

À propos de cette tâche

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

Étapes

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

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

b. Décochez la case pour autoriser l'accès.

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

4. Sélectionnez **Enregistrer**.

Configurer les serveurs de gestion des clés

Découvrez les serveurs de gestion des clés dans StorageGRID

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 en utilisant le protocole d'interopérabilité de gestion de clés (KMIP).

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

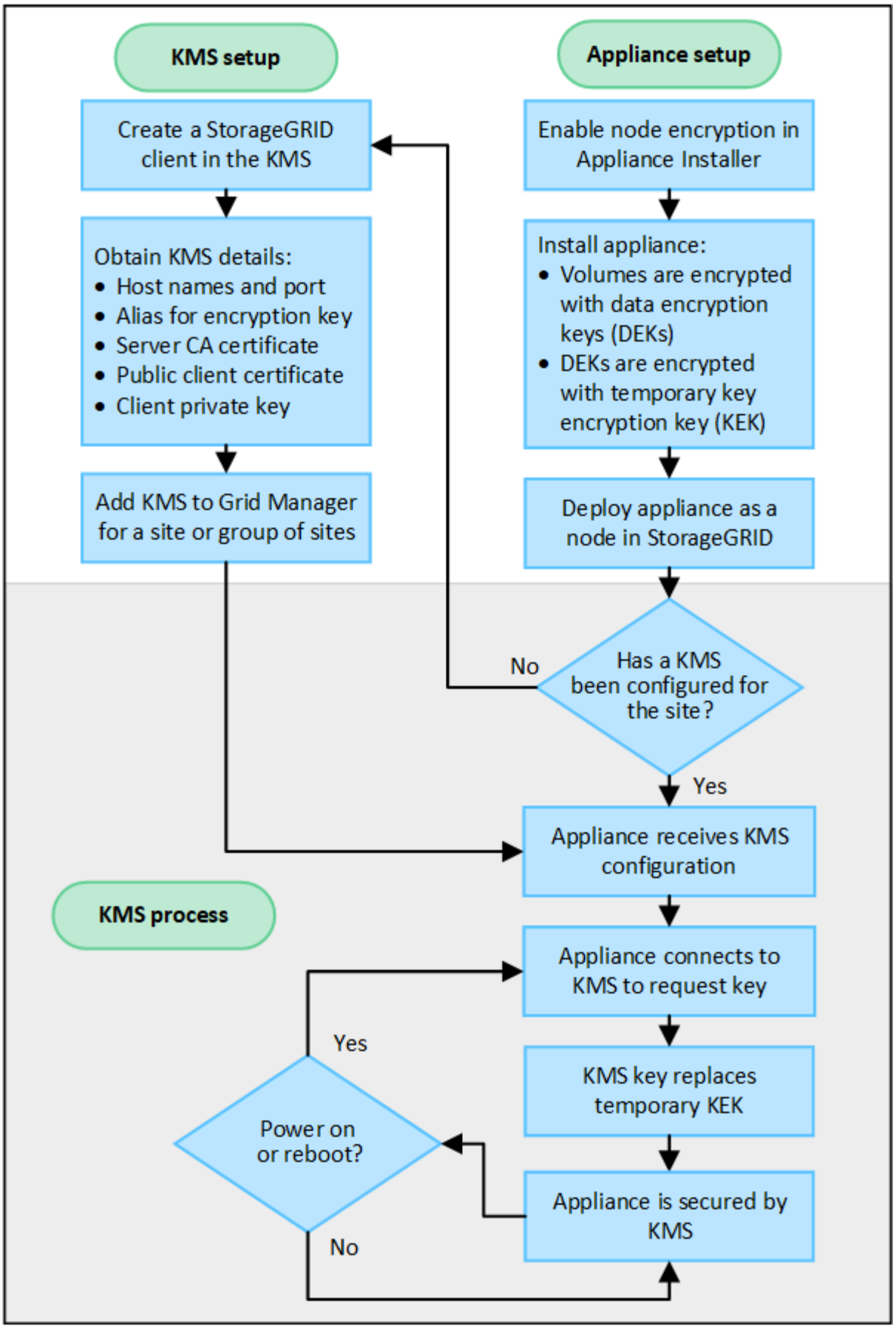
Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement des nœuds StorageGRID dont l'option **Chiffrement des nœuds** est activée lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds StorageGRID vous permet de protéger vos données même si un dispositif est retiré du centre de données. Une fois les volumes du dispositif chiffrés, vous ne pouvez accéder à aucune donnée sur le dispositif, 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 du serveur de gestion des clés et de l'appliance StorageGRID

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 de l'appliance. Une fois ces deux tâches de configuration terminées, le processus de gestion des clés s'effectue automatiquement.

Le diagramme illustre les grandes étapes de l'utilisation d'un KMS pour sécuriser les données StorageGRID sur les nœuds de l'appliance.



Le diagramme montre que la configuration du KMS et celle de l'appliance se déroulent en parallèle ;

cependant, vous pouvez configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement pour les nouveaux nœuds de l'appliance, en fonction de vos besoins.

Configurer le serveur de gestion des clés (KMS)

La mise en place d'un serveur de gestion de clés comprend les étapes générales suivantes.

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

Configurez l'appareil

La configuration d'un nœud d'appliance pour une utilisation KMS comprend les étapes générales suivantes.

1. Lors de la phase de configuration matérielle de l'installation de l'appliance, utilisez le StorageGRID Appliance Installer pour activer le paramètre **Chiffrement de nœud** pour l'appliance.

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

2. Exécutez le programme d'installation de l'appliance StorageGRID. Lors de l'installation, une clé de chiffrement de données (DEK) aléatoire est attribuée à chaque volume de l'appliance, comme suit :
   - Les clés DEK servent à chiffrer les données de 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 principale (KEK). La KEK initiale est une clé temporaire qui chiffre les DEK jusqu'à ce que l'appliance puisse se connecter au KMS.
3. Ajoutez le nœud de l'appliance à StorageGRID.

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

Processus de chiffrement de la gestion des clés (effectué automatiquement)

Le chiffrement avec gestion des clés comprend les étapes générales suivantes, qui sont exécutées automatiquement.

1. Lorsque vous installez dans la grille un appareil dont le chiffrement des nœuds est activé, 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 aucun KMS n'a encore été configuré pour le site, les données sur l'appliance continuent d'être chiffrées par la 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'appliance. La nouvelle clé provenant du KMS remplace la clé KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les clés DEK des volumes de l'appliance.

> Toutes les données existantes avant la connexion du nœud de l'appliance chiffrée au KMS configuré sont chiffrées à l'aide d'une clé temporaire. Cependant, les volumes de l'appliance ne doivent pas être considérés comme protégés contre leur suppression du centre de données tant que la clé temporaire n'est pas remplacée par la clé de chiffrement KMS.

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

Exigences et considérations relatives au serveur de gestion des clés StorageGRID

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 autoriser chaque nœud de l'appliance à communiquer via le port utilisé pour le protocole Key Management Interoperability Protocol (KMIP). Le port KMIP par défaut est 5696.

Vous devez vous assurer que chaque nœud d'appliance utilisant le chiffrement 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 soit le protocole TLS 1.2, soit le protocole TLS 1.3 lors des connexions KMIP à un KMS ou un cluster KMS, en fonction de ce que le KMS prend en charge et de celui que "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 lors de l'établissement de la connexion. Pour connaître les versions de protocole et les chiffrements/suites de chiffrement disponibles, consultez la `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 appareil StorageGRID de votre grille dont l'option **Chiffrement des nœuds** est activée. Cette option ne peut être activée que lors de l'étape de configuration matérielle de l'installation de l'appareil, à l'aide de l'outil

StorageGRID Appliance Installer.

> Vous ne pouvez pas activer le chiffrement du nœud après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion externe des clés pour les appareils qui n'ont pas le chiffrement du nœud 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 logiciels (non-appliance), notamment les suivants :

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

Les nœuds déployés sur ces autres plateformes peuvent utiliser le chiffrement en dehors de StorageGRID au niveau du datastore ou du disque.

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

Lors d'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'objets ne soient stockées dessus.

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

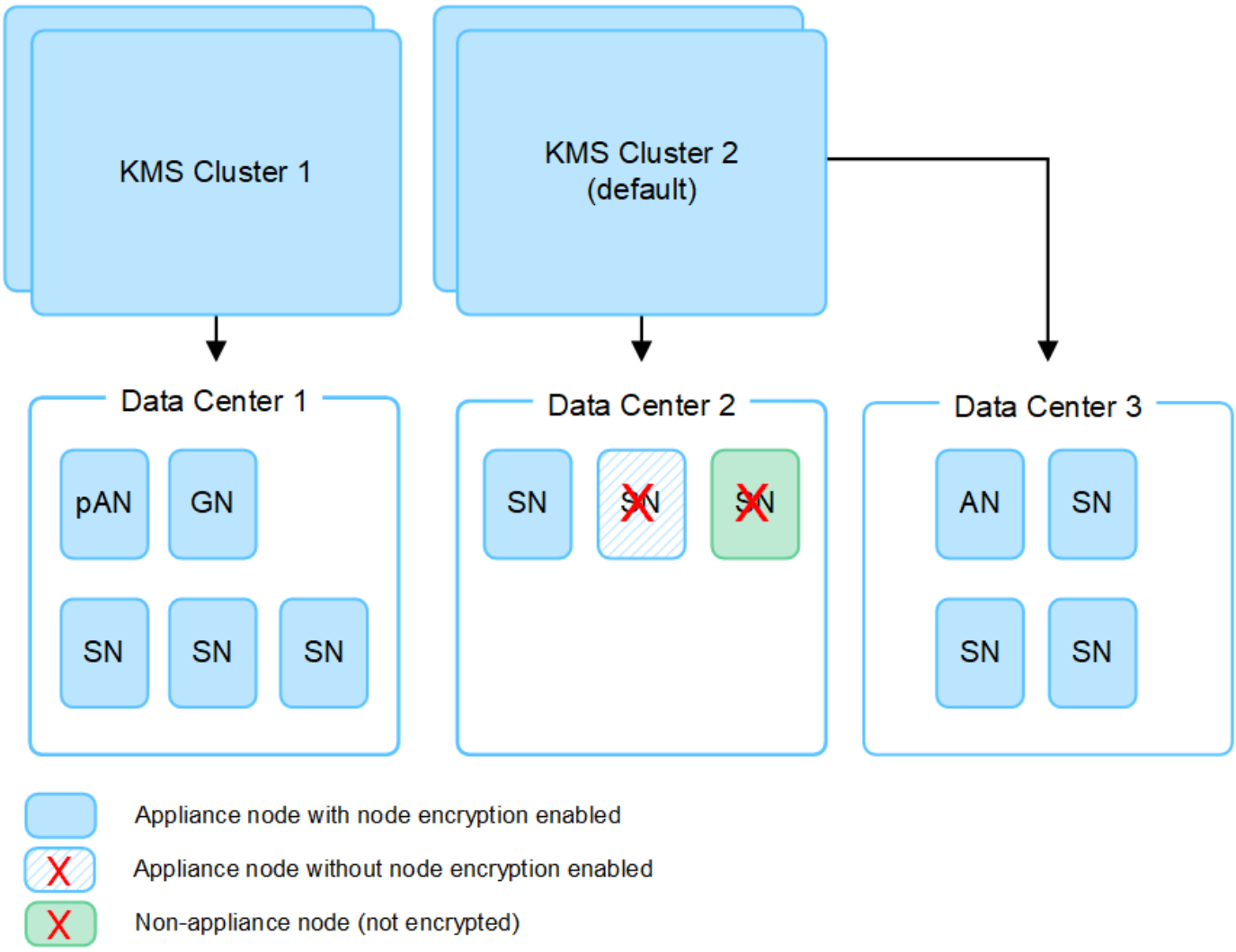
De combien de serveurs de gestion de clés avez-vous besoin ?

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 seule clé de chiffrement aux nœuds d'appliance StorageGRID d'un site ou d'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 à haute disponibilité.

Par exemple, supposons que votre système StorageGRID comporte trois centres de données. Vous pouvez configurer un cluster KMS pour fournir une clé à tous les nœuds d'appliance du Data Center 1 et un second cluster KMS pour fournir une clé à tous les nœuds d'appliance de tous les autres sites. Lorsque vous ajoutez le second 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 **Node Encryption** 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 "faites pivoter la clé de chiffrement" utilisée par chaque KMS configuré.

Lorsque la nouvelle version de la clé sera disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés du ou des sites associés au KMS. La distribution doit avoir lieu dans l'heure suivant la rotation de la clé.
- Si le nœud de l'appliance chiffrée est hors ligne lors de la distribution de la nouvelle version de la clé, il recevra la nouvelle clé dès son redémarrage.
- Si la nouvelle version de la clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour quelque raison que ce soit, l'alerte **KMS encryption key rotation failed** est déclenchée pour le nœud de l'appliance. Vous devrez peut-être contacter le support technique pour obtenir de l'aide afin de résoudre cette alerte.

Puis-je réutiliser un nœud d'appliance après son chiffrement ?

Si vous devez installer un dispositif chiffré dans un autre système StorageGRID, vous devez d'abord mettre hors service le nœud de la grille afin de déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le StorageGRID Appliance Installer "effacer la configuration KMS". La suppression de la

configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud du dispositif et la configuration KMS pour le site StorageGRID.

> Sans accès à la clé de chiffrement KMS, toutes les données restant sur l'appareil ne peuvent plus être accessibles et sont définitivement verrouillées.

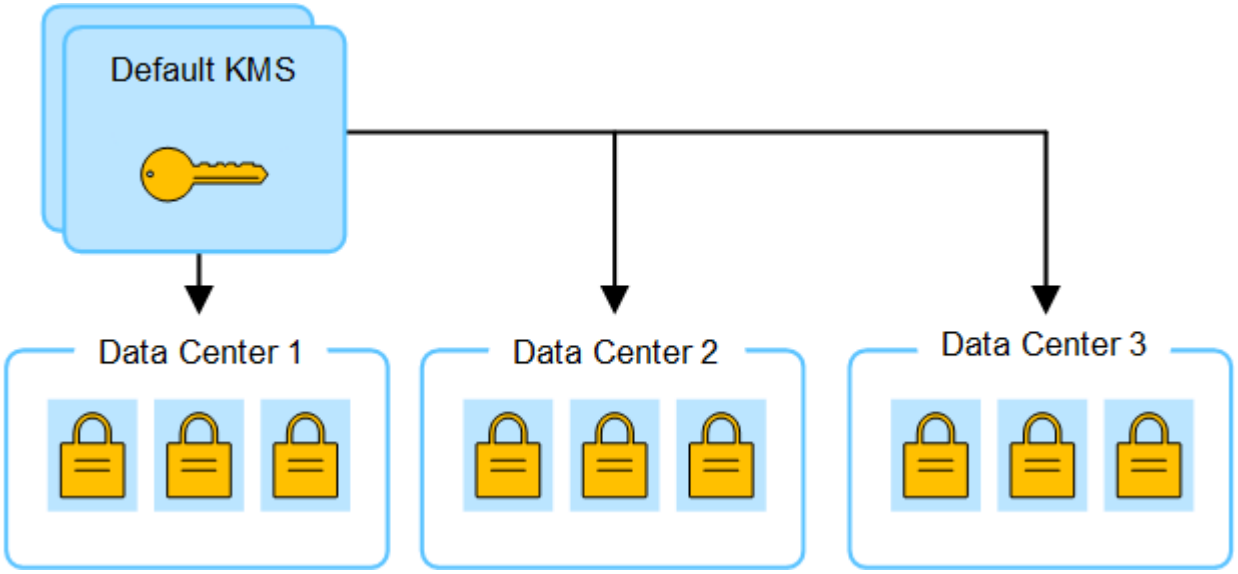
Considérations relatives à la modification du KMS pour un site StorageGRID

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

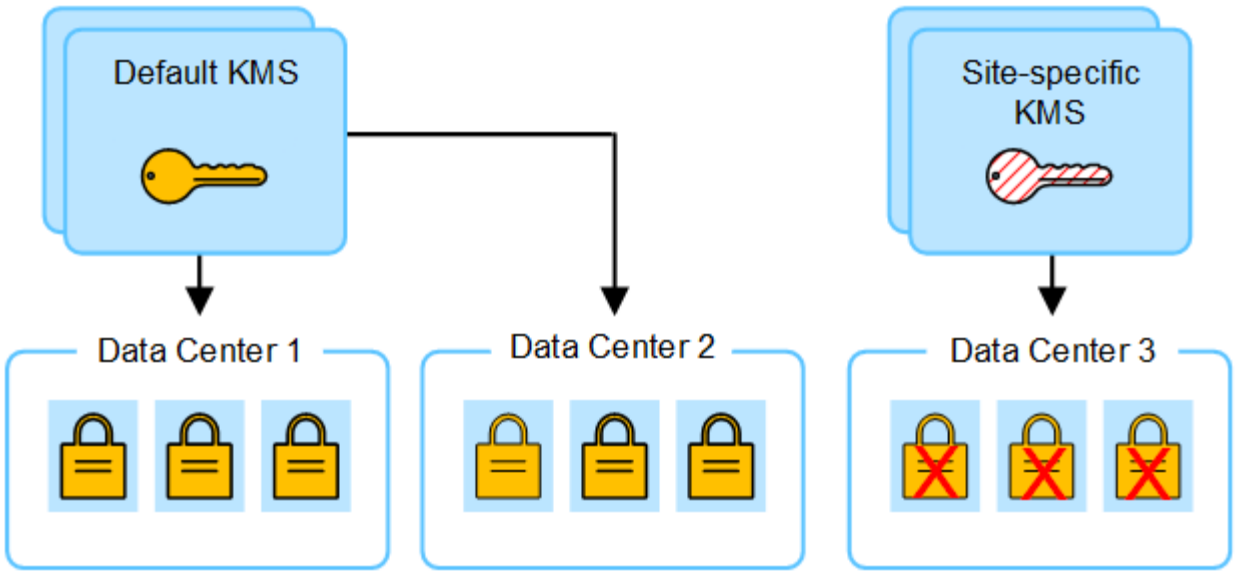
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous pourriez avoir besoin de copier la version actuelle de la clé de chiffrement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

Par exemple :

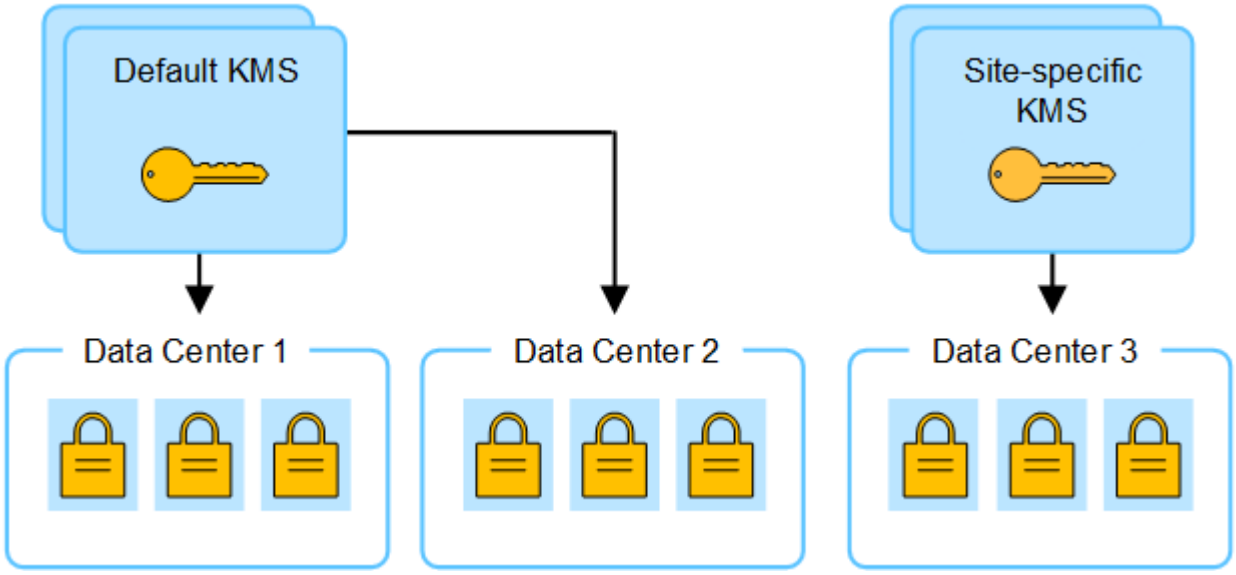
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites ne disposant pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement des nœuds** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée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



3. Vous décidez d'ajouter un KMS spécifique au site (Data Center 3 sur la figure). Cependant, comme 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 parce que le KMS spécifique au site ne possède pas la clé correcte pour déchiffrer les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine vers 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 du Data Center 3, elle peut donc être enregistrée dans StorageGRID.



Cas d'utilisation pour la modification du KMS utilisé pour un site

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

Cas d'utilisation pour la modification du KMS d'un site	Étapes requises
Vous disposez d'une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez en utiliser une comme KMS par défaut.	Modifiez 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. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. "Modifier un serveur de gestion de clés (KMS)"
Vous disposez d'un KMS par défaut et vous ajoutez un nouveau site lors d'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 Grid Manager, 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 de l'appliance sur le 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 Grid Manager, modifiez la configuration KMS existante et saisissez le nouveau nom de l'hôte ou la nouvelle adresse IP. "Ajouter un serveur de gestion de clés (KMS)"

Configurez 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 compatibles, utilisez le "Outil de matrice d'interopérabilité (IMT) NetApp".

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 seule clé de chiffrement pour les nœuds des 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 comporter au moins 2 048 bits et être exportable.

   - Laissez StorageGRID créer la clé. Vous serez invité à le faire lors du test et de l'enregistrement après

"téléversement des certificats clients".

3. Enregistrez les informations suivantes pour chaque KMS ou cluster KMS.

   Vous aurez besoin de ces informations lorsque vous ajouterez le KMS à StorageGRID :

   - Nom d'hôte ou adresse IP pour chaque serveur.
   - Port KMIP utilisé par le KMS.
   - Alias de la clé de chiffrement dans le KMS.

4. Pour chaque KMS ou cluster KMS, obtenez un certificat serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA encodés au format 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 encodé en Base-64 Privacy Enhanced Mail (PEM).
   - Le champ Subject Alternative Name (SAN) de chaque certificat de serveur doit inclure le domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.

     > Lorsque vous configurez le KMS dans StorageGRID, vous devez saisir les mêmes FQDN ou adresses IP dans le champ **Hostname**.

   - 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 délivré 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 dans StorageGRID

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".
- Vous avez "configuré StorageGRID comme client dans le KMS", et vous disposez des informations requises pour chaque KMS ou cluster KMS.
- Vous êtes connecté au Gestionnaire de grille 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 les serveurs de gestion de clés spécifiques à chaque site avant de configurer un KMS par défaut applicable à tous les sites non gérés par un autre KMS. Si vous créez d'abord le KMS par défaut, tous les équipements chiffrés au niveau des nœuds dans la grille seront chiffrés par le KMS par défaut. Si vous souhaitez créer un KMS spécifique à un site ultérieurement, 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 du 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** > **Security** > **Key management server**.

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

2. Sélectionnez **Create**.

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

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

Champ	Description
Nom KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	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.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer les serveurs de gestion de clés spécifiques à un 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 des 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 ne disposant pas d'un KMS dédié et à tous les sites que vous ajouterez lors d'extensions ultérieures. **Remarque :** Une erreur de validation se produira lors de l'enregistrement de 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 que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.

Champ	Description
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. **Remarque :** Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni 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 **Continue**.

Étape 2 : Télécharger le certificat du serveur

À l'étape 2 (Téléchargement du certificat serveur) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat serveur (ou le lot de certificats) pour le KMS. Le certificat 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 du serveur enregistré ou du bundle de certificats.
2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat du serveur apparaissent.

   > Si vous avez importé un ensemble de certificats, les métadonnées de chaque certificat apparaissent dans son propre onglet.

3. Sélectionnez **Continue**.

Étape 3 : Téléversez les certificats clients

À l'étape 3 (Téléchargement des certificats clients) de l'assistant Ajout d'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. Téléversez le fichier de clé privée.
5. Sélectionnez **Tester et enregistrer**.

   Si aucune clé n'existe, vous êtes invité à laisser StorageGRID 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 des

clés est ajouté au tableau de la page Serveur de gestion des clés.

> Immédiatement après l'ajout d'un KMS, l'état du certificat sur la page Key Management Server apparaît comme Inconnu. StorageGRID peut prendre jusqu'à 30 minutes pour obtenir l'état réel de chaque certificat. Vous devez actualiser votre navigateur web pour voir l'état actuel.

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

   Par exemple, vous pourriez 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**.

   > L'option **Forcer l'enregistrement** sauvegarde la configuration KMS, mais ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème de configuration, il se peut que vous ne puissiez pas redémarrer les nœuds d'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous pourriez perdre l'accès à vos données jusqu'à la résolution des problèmes.

8. Examinez 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 serveur de gestion de clés dans StorageGRID

La gestion d'un serveur de gestion de clés (KMS) implique la consultation ou la modification des détails, la gestion des certificats, la consultation des nœuds chiffrés et la suppression d'un KMS lorsqu'il n'est plus nécessaire.

Avant de commencer

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

Afficher les détails KMS

Vous pouvez consulter les informations relatives à chaque serveur de gestion de clés (KMS) dans votre système StorageGRID, notamment les détails des clés et l'état actuel des certificats du serveur et du client.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche et présente les informations suivantes :

   - L'onglet Détails de la configuration répertorie tous les serveurs de gestion des clés configurés.
   - L'onglet « Nœuds chiffrés » répertorie tous les nœuds dont le chiffrement de nœud est activé.

2. Pour consulter les détails d'un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le nom du KMS. La page de détails du KMS affiche 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 **des sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion de clés, le domaine complet ou l'adresse IP des deux serveurs est indiqué. S'il existe plus de deux serveurs de gestion de clés dans un cluster, le domaine complet ou l'adresse IP du premier KMS est indiqué, ainsi que 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'hôte d'un cluster, sélectionnez un KMS et sélectionnez **Modifier** ou **Actions** > **Modifier**.

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

Onglet	Champ	Description
Détails clés	Nom de la clé	L'alias de clé pour le client StorageGRID dans le KMS.
UID de la clé	L'identifiant unique de la dernière version de la clé.	Dernière modification
Date et heure de la dernière version de la clé.	Certificat serveur	Métadonnées
Les métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration, et le certificat PEM.	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 certificat PEM.

4. Aussi souvent que nécessaire selon 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 de la clé réussit, les champs Key UID 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 cette même clé. Ne faites pas pivoter vers une clé totalement différente.

Ne tentez jamais de faire tourner une clé en modifiant son nom (alias) auprès du KMS. StorageGRID exige que toutes les versions de clés précédemment utilisées (ainsi que les futures) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID pourrait ne pas être en mesure de déchiffrer vos données.

Gérer les certificats

Réglez rapidement tout problème lié aux certificats serveur ou client. Si possible, remplacez les certificats avant leur expiration.

Vous devez régler tout problème de certificat dès que possible afin de maintenir l'accès aux données.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.
2. Dans le tableau, consultez la valeur de l'expiration du certificat pour chaque KMS.
3. Si la date d'expiration du certificat de n'importe quel 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 de détails du KMS.
   a. Sélectionnez **Certificat 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 **KMS CA certificate expiration**, **KMS client certificate expiration** et **KMS server certificate expiration** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

   StorageGRID peut prendre jusqu'à 30 minutes pour mettre à jour la date d'expiration du certificat. Actualisez votre navigateur web pour voir les valeurs actuelles.

Si vous obtenez le statut **Statut du certificat serveur inconnu**, assurez-vous que votre KMS permette d'obtenir un certificat serveur sans exiger de certificat client.

Afficher les nœuds chiffrés

Vous pouvez consulter les informations relatives aux nœuds d'appliance de votre système StorageGRID dont le paramètre **Chiffrement des nœuds** est activé.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page Serveur de gestion des clés s'affiche. L'onglet Détails de la configuration présente les serveurs de gestion des clés 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 dont le paramètre **Chiffrement des nœuds** est activé.

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

Colonne	Description
Nom du nœud	Le nom du nœud de l'appliance.
Type de nœud	Le type de nœud : Storage, Admin ou Gateway.
Site	Le nom du site StorageGRID où le nœud est installé.
Nom KMS	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)"
UID de la clé	L'identifiant unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID complet de la clé, 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	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 peut prendre plusieurs minutes après une modification de la configuration du KMS. **Remarque :** Actualisez votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne « Status » indique un problème KMS, résolvez le problème immédiatement.

   Lors des opérations normales du KMS, le statut sera **Connecté au KMS**. Si un nœud est déconnecté du grid, l'état de connexion du nœud est affiché (Administrativement hors service ou Inconnu).

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

   - Échec du chargement de la configuration KMS
   - Erreur de connectivité KMS
   - Nom de clé de chiffrement KMS introuvable
   - La rotation de la clé de chiffrement KMS a échoué
   - La clé KMS n'a pas pu déchiffrer le volume de l'appliance.
   - KMS n'est pas configuré

Veuillez effectuer les actions recommandées pour ces alertes.

> Vous devez remédier immédiatement à tout problème afin de garantir la protection intégrale de vos données.

Modifier un KMS

Vous pourriez avoir besoin de 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 prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le "considérations relatives à la modification du KMS d'un site".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche et présente tous les serveurs de gestion des clés configurés.

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

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

3. Vous pouvez également mettre à jour les détails à l'étape 1 (détails KMS) de l'assistant Modifier un Key Management Server.

Champ	Description
Nom KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	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 l'ancienne clé ont été copiées dans l'historique des versions du nouvel alias.

Champ	Description
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous n'avez pas encore de KMS par défaut, vous pouvez sélectionner **Sites non gérés par un autre KMS (KMS par défaut)**. Cette sélection convertit un KMS spécifique à un 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 lors d'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 que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le domaine complet ou l'adresse IP du KMS. **Remarque :** Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni 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 **Continue**.

   L'étape 2 (Télécharger le certificat du serveur) de l'assistant Modifier un Key Management Server apparaît.

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

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

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

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

10. Si un message d'erreur apparaît, consultez les détails du message et sélectionnez **OK**.

    Par exemple, vous pourriez 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 **Force save**.

L'option **Forcer l'enregistrement** sauvegarde la configuration KMS, mais ne teste pas la connexion externe de chaque appliance à ce KMS. En cas de problème de configuration, il se peut que vous ne puissiez pas redémarrer les nœuds d'appliance dont le chiffrement de nœud est activé sur le site concerné. Vous pourriez perdre l'accès à vos données jusqu'à la résolution des problèmes.

La configuration KMS est enregistrée.

12. Examinez 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 pourriez vouloir supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous pourriez vouloir supprimer un KMS spécifique à un site si vous avez mis ce 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 Gestionnaire de grille 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 les cas suivants :

- Vous pouvez supprimer un KMS spécifique à un site si celui-ci a été mis hors service ou s'il ne comprend aucun nœud d'appliance avec chiffrement de nœud activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site comportant des nœuds d'appliance avec chiffrement de nœud activé.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Key management server**.

   La page du serveur de gestion des clés s'affiche et présente tous les serveurs de gestion des clés configurés.

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

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

3. Veuillez confirmer que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique à un site pour un site qui ne possède aucun nœud d'appliance avec 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 du proxy

Configurer un proxy de stockage StorageGRID

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 des services de plateforme vers 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

- Vous avez "autorisations d'accès spécifiques".
- Vous êtes connecté au Gestionnaire de grille 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 du proxy**.
2. Dans l'onglet **Stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole pour le proxy de stockage.
4. Saisissez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

   Laissez ce champ vide pour utiliser le port par défaut du 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 Cloud Storage Pools 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 relatifs 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**.

Configurez les paramètres du proxy d'administration dans StorageGRID

Si vous envoyez des packages AutoSupport en utilisant 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 "Configurez AutoSupport".

Avant de commencer

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

À propos de cette tâche

Vous pouvez configurer les paramètres d'un seul proxy d'administration.

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Paramètres du 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 d'administration**.
4. Saisissez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Saisissez le port utilisé pour vous connecter au serveur proxy.
6. Vous pouvez éventuellement saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

   Laissez ces champs vides si votre serveur proxy ne requiert ni nom d'utilisateur ni mot de passe.

7. Sélectionnez l'une des options suivantes :

   - Pour sécuriser la connexion au proxy d'administration, sélectionnez **Vérifier le certificat du proxy**. Chargez un bundle CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.

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

   Après que vous ayez téléchargé le paquet CA, ses métadonnées apparaissent.

   - 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**.

Contrôlez les pare-feu

Contrôlez l'accès à StorageGRID à un 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 pouvez 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 de 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 API de gestion peuvent accéder au Grid Manager, à l'API de gestion du Grid, au Tenant Manager et à l'API de gestion du Tenant. **Remarque :** Le port 443 est également utilisé pour une partie du trafic interne.
8443	Port restreint du Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Grid Manager et à l'API de gestion du Grid à l'aide de HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder au Tenant Manager ni à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port restreint du gestionnaire de locataires sur les nœuds d'administration	• Les navigateurs Web et les clients API de gestion peuvent accéder au Tenant Manager et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au Grid Manager ni à l'API de gestion du Grid. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports restreints de Grid Manager ou de 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

- "Connectez-vous au Grid Manager"
- "Créer un compte locataire"
- "Communications externes"

Gérez les contrôles de pare-feu internes dans StorageGRID

StorageGRID intègre un pare-feu interne sur chaque nœud, renforçant ainsi la sécurité de votre grid en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-

feu pour empêcher l'accès réseau sur tous les ports, sauf ceux nécessaires au déploiement spécifique de votre grid. 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 grid.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès à des ports fermés sélectionnés. Vous pouvez ajouter des adresses IP ou des sous-réseaux au format 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 fait confiance au trafic entrant provenant du réseau client.

  Les paramètres de cet onglet prévalent sur ceux de l'onglet Gérer l'accès externe.

  - Un nœud doté d'un Client Network non fiable n'acceptera que 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 liés au type de nœud).
  - Les ports des points 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 Manage external networks.
  - Une fois 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 dans un onglet peuvent affecter les modifications d'accès que vous effectuez dans un autre onglet. Assurez-vous de vérifier les paramètres de tous les onglets pour que votre réseau se comporte comme vous l'attendez.

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

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

Onglets Liste d'adresses privilégiées et Gérer l'accès externe

L'onglet « Liste des adresses privilégiées » vous permet d'enregistrer une ou plusieurs adresses IP autorisées à accéder à des ports de la grille fermés. L'onglet « Gérer l'accès externe » vous permet de fermer l'accès externe à certains ports externes ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut aux nœuds non-grille). Ces deux onglets peuvent souvent être utilisés conjointement pour personnaliser précisément l'accès réseau dont vous avez besoin pour votre grille.

> Les adresses IP privilégiées n'ont pas accès par défaut aux ports internes de la grille.

Exemple 1 : Utilisez un serveur de rebond pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un serveur de rebond (un hôte sécurisé) pour l'administration du réseau. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste des adresses privilégiées pour ajouter l'adresse IP de l'hôte de rebond.
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 à moins que leur adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Une fois votre configuration enregistrée, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception du jump host. Vous pouvez alors utiliser le jump host pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : Verrouillez les ports sensibles

Supposons que vous souhaitiez verrouiller les ports sensibles et le service sur ce port. Vous pouvez suivre les étapes générales suivantes :

1. Utilisez l'onglet Liste d'adresses privilégiées pour n'accorder l'accès qu'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 tout port attribué à l'accès à Grid Manager et Tenant Manager (les ports prédéfinis sont 443 et 8443). Tout utilisateur actuellement connecté à un port bloqué, y compris vous, perdra l'accès à Grid Manager à moins que son adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

Une fois votre configuration enregistrée, le port sensible et le service associé sont accessibles aux hôtes figurant dans la liste d'adresses privilégiées. L'accès au service est refusé à tous les autres hôtes, quelle que soit l'interface d'où provient la requête.

Exemple 3 : Désactivez 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 HTTP des clients S3, vous utiliseriez le bouton bascule de l'onglet Gérer l'accès externe pour bloquer le port 18084.

Onglet Réseaux clients non approuvés

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

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

Vous pouvez réduire le risque d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client de chaque nœud soit *non fiable*. Si le réseau client d'un nœud est non fiable, le nœud n'accepte les connexions entrantes que 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 passerelle accepte uniquement les requêtes HTTPS S3

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

1. À partir de la page "points de terminaison de l'équilibreur de charge", configurez un point de terminaison

d'équilibrage de charge pour S3 via HTTPS sur le port 443.

2. Sur la page de contrôle du pare-feu, sélectionnez Non approuvé pour indiquer que le réseau client sur le nœud de passerelle n'est pas approuvé.

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

Exemple 2 : Un nœud de stockage envoie des requêtes de services de plateforme S3

Supposons que vous souhaitiez autoriser le trafic sortant des services de la plateforme S3 depuis un nœud de stockage, mais empêcher toute connexion entrante vers ce nœud de stockage sur le réseau client. Vous effectueriez l'étape générale suivante :

- 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 requêtes sortantes vers les destinations des services de plateforme configurés.

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

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

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet Untrusted Client Network pour configurer le réseau client comme non approuvé.
3. Lorsque vous créez un point de terminaison d'équilibreur de charge d'interface de gestion, saisissez le port et sélectionnez l'interface de gestion à laquelle le port accédera.
4. Sélectionnez **Oui** pour 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 situés en dehors de ce sous-réseau).

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

Configurer le pare-feu interne de StorageGRID

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 Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez examiné les informations 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 n'accepte le trafic entrant que sur les 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 intègre un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer les ports qui sont ouverts par défaut sur le réseau de la grille, le réseau d'administration et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille qui sont fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud fait confiance au trafic entrant provenant du réseau client, et vous pouvez configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP extérieures à votre grid aux seuls ports strictement nécessaires renforce la sécurité de votre grid. 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 du 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 réseau, consultez "Contrôler l'accès au niveau du pare-feu externe".

Contrôler l'accès au pare-feu

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 un onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez dans un onglet n'empêchent pas ce que vous pouvez faire dans les autres onglets ; cependant, les modifications de configuration que vous effectuez dans un onglet peuvent modifier le comportement des ports configurés dans les 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 et les sous-réseaux privilégiés n'ont pas accès au grid interne par défaut. De plus, les points de terminaison de l'équilibreur de charge et les ports supplémentaires ouverts dans l'onglet Liste des adresses privilégiées sont accessibles même s'ils sont bloqués dans l'onglet Gérer l'accès externe.

Les paramètres de l'onglet « Liste des adresses privilégiées » ne peuvent pas remplacer les paramètres de l'onglet « Réseau client non approuvé ».

Étapes

1. Dans l'onglet Liste des adresses privilégiées, saisissez 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 sous-réseau au format CIDR** pour ajouter des clients privilégiés supplémentaires.

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

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes de StorageGRID**. Voir "Ports internes de StorageGRID".

   Cette option désactive certaines protections des services internes. Laissez-la désactivée si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

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

Les paramètres de l'onglet « Gérer l'accès externe » ne peuvent pas prévaloir sur ceux de l'onglet « Réseau client non fiable ». Par exemple, si un nœud est non fiable, 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 fiable » prévalent sur les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **Gérer l'accès externe**. L'onglet affiche un tableau répertoriant tous les ports externes (ports accessibles par défaut aux nœuds hors grille) des nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez le bouton à bascule situé 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 listés 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 à moins que leur adresse IP n'ait été ajoutée à la liste des adresses privilégiées.

     Utilisez la barre de défilement à droite 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 saisissez **2**, tous les ports dont le nom contient la chaîne « 2 » seront affichés.

3. Sélectionnez **Save**

Réseau de clients non fiables

Si le réseau client d'un nœud n'est pas approuvé, le nœud n'accepte le trafic entrant que sur les ports

configurés comme points de terminaison d'équilibrage de charge et, éventuellement, sur les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour définir le paramètre par défaut des nouveaux nœuds ajoutés lors d'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 des nouveaux nœuds, spécifiez le paramètre par défaut qui doit être appliqué lorsque de nouveaux nœuds sont ajoutés à la grille lors d'une procédure d'expansion.

   - **Fiable** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est fiable.
   - **Non fiable** : Lorsqu'un nœud est ajouté lors d'une extension, son réseau client est non fiable.

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

     > Ce paramètre n'affecte pas les nœuds existants de 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 supplémentaires sélectionnés :

   - Sélectionnez **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste Untrusted Client Network.
   - Sélectionnez **Faire confiance aux nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste Untrusted Client Network.
   - Utilisez le bouton bascule situé à côté de chaque nœud pour définir le réseau client comme étant de confiance ou non de confiance pour le nœud sélectionné.

     Par exemple, vous pouvez sélectionner **Ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste Réseau client non fiable, puis utiliser le bouton bascule situé à côté d'un nœud individuel pour ajouter ce nœud à la liste Réseau client fiable.

     > Utilisez la barre de défilement à droite 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 saisissez **GW**, tous les nœuds dont le nom contient la chaîne "GW" seront affichés.

4. Sélectionnez **Enregistrer**.

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