Gérer les paramètres de sécurité

StorageGRID

NetApp
October 03, 2025

Sommaire

Gérer les paramètres de sécurité . . . 1
- Gérer les certificats . . . 1
  - À propos des certificats de sécurité . . . 1
  - Configurer les certificats de serveur . . . 12
  - Configurer les certificats client . . . 23
- Configurer les serveurs de gestion des clés . . . 32
  - Configurer les serveurs de gestion des clés : présentation . . . 32
  - Étudiez les méthodes de cryptage StorageGRID . . . 32
  - Présentation de la configuration des appliances et KMS . . . 35
  - Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés . . . 38
  - Considérations relatives à la modification du KMS pour un site . . . 41
  - Configurer StorageGRID en tant que client dans le KMS . . . 44
  - Ajout d'un serveur de gestion des clés (KMS) . . . 45
  - Afficher les détails du KMS . . . 53
  - Afficher les nœuds chiffrés . . . 55
  - Modification d'un serveur de gestion des clés (KMS) . . . 57
  - Suppression d'un serveur de gestion des clés (KMS) . . . 60
- Gérer les paramètres proxy . . . 61
  - Configurez les paramètres du proxy de stockage . . . 61
  - Configurez les paramètres du proxy d'administration . . . 62
- Gérer les réseaux clients non fiables . . . 64
  - Gérer les réseaux clients non approuvés : présentation . . . 64
  - Le réseau client du nœud spécifié n'est pas fiable . . . 64

Gérer les paramètres de sécurité

Gérer les certificats

À propos des certificats de sécurité

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

StorageGRID utilise deux types de certificats de sécurité :

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

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant 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 (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Certificat CA grille par défaut

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

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

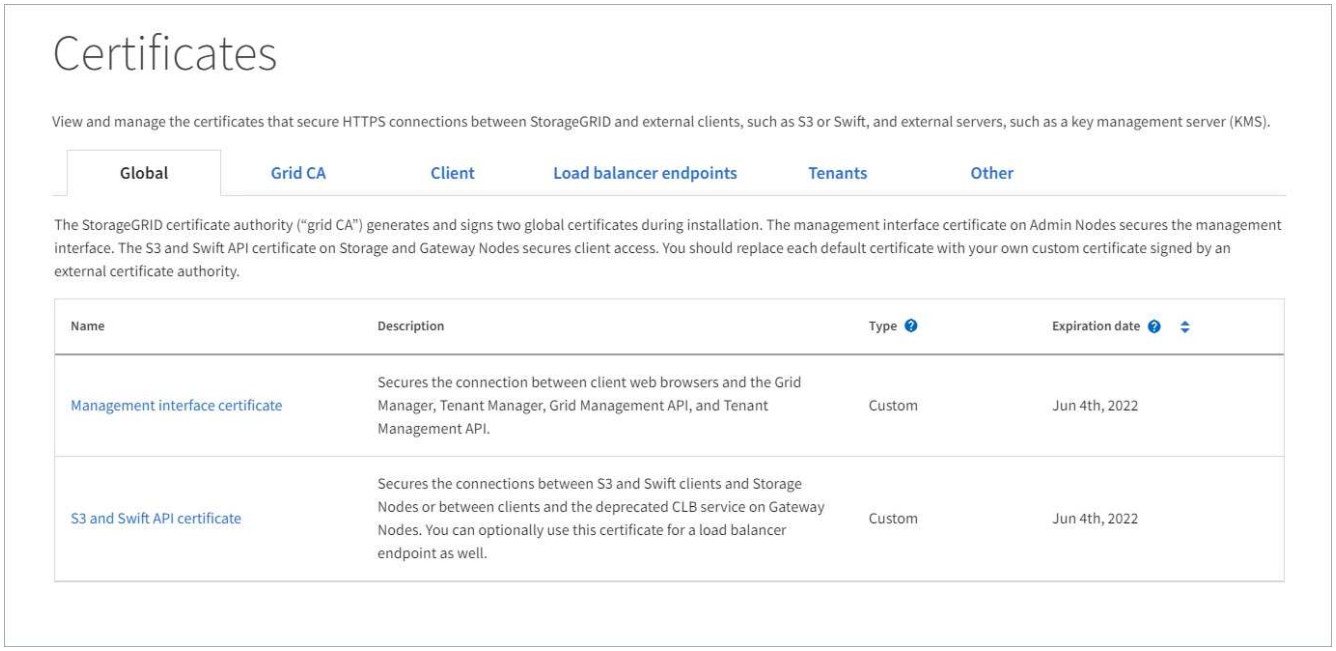
> StorageGRID inclut également des certificats CA du système d'exploitation identiques sur toutes les grilles. Dans les environnements de production, assurez-vous de spécifier un certificat personnalisé signé par une autorité de certification externe à la place du certificat d'autorité de certification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

Les variantes du serveur et des types de certificats client sont mises en œuvre de plusieurs façons. Avant de configurer le système, tous les certificats nécessaires à votre configuration StorageGRID spécifique doivent être prêts.

Accéder aux certificats de sécurité

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

1. Dans Grid Manager, sélectionnez **CONFIGURATION sécurité certificats**.



2. Sélectionnez un onglet sur la page certificats pour obtenir des informations sur chaque catégorie de certificat et pour accéder aux paramètres du certificat. Vous ne pouvez accéder à un onglet que si vous disposez de l'autorisation appropriée.

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

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

Mondial

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

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

Les informations sur les 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 améliorer la sécurité de la grille :
  - Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID Utilisé pour les connexions Grid Manager et tenant Manager.
  - Remplacez le certificat API S3 et Swift Utilisé pour les connexions nœud de stockage, service CLB (obsolète) et point final de l'équilibreur de charge (facultatif).
- Restaurez le certificat de l'interface de gestion par défaut.
- Restaurez le certificat API S3 et Swift par défaut.
- Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé.
- Copiez ou téléchargez le certificat de l'interface de gestion ou Certificat API S3 et Swift.

CA grille

Le Certificat CA de la grille, Généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic StorageGRID interne.

Les informations sur le certificat comprennent la date d'expiration du certificat et son contenu.

C'est possible Copiez ou téléchargez le certificat de l'autorité de certification Grid, mais vous ne pouvez pas le changer.

Client

Certificats client, Généré par une autorité de certification externe, sécurisez les connexions entre les outils de contrôle externes et la base de données StorageGRID Prometheus.

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

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 l'autorisation d'accès Prometheus.
  - Téléchargez et remplacez le certificat client.
  - Copiez ou téléchargez le certificat client.
  - Supprimez le certificat client.
- Sélectionnez **actions** pour accélérer modifier, attacher, ou déposer un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats client et les supprimer en une seule fois en utilisant **actions Supprimer**.

Terminaux d'équilibrage de charge

Certificats de noeud final de l'équilibreur de charge, Que vous téléchargez ou générez, sécurisez les connexions entre les clients S3 et Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des noeuds finaux de l'équilibreur de charge comporte une ligne pour chaque noeud final de l'équilibreur de charge configuré et indique si le certificat API S3 et Swift global ou un certificat de point final d'équilibreur de charge personnalisé est utilisé pour le noeud final. La date d'expiration de chaque certificat s'affiche également.

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

Vous pouvez :

- Sélectionnez un nom de noeud final pour ouvrir un onglet de navigateur contenant des informations sur le noeud final de l'équilibreur de charge, y compris ses détails de certificat.
- Spécifiez un certificat de noeud final de l'équilibreur de charge pour FabricPool.
- Utilisez le certificat global d'API S3 et Swift au lieu de générer un nouveau certificat de terminal de l'équilibreur de charge.

Locataires

Les locataires peuvent utiliser certificats de serveur de fédération des identités ou certificats de terminal du service de plate-forme Pour sécuriser leurs connexions avec StorageGRID.

La table de tenant dispose d'une ligne pour chaque locataire et indique si chaque locataire a l'autorisation d'utiliser ses propres services de référentiel d'identité ou de plate-forme.

Vous pouvez :

- Sélectionnez un nom de locataire pour vous connecter au Gestionnaire de tenant
- Sélectionnez un nom de locataire pour afficher les détails de la fédération des identités du locataire
- Sélectionnez un nom de locataire pour afficher les détails des services de plateforme du locataire
- Spécifiez un certificat de noeud final du service de plate-forme pendant la création du noeud final

Autre

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

- Certificats de fédération des identités
- Certificats de pool de stockage cloud
- Certificats de serveur de gestion des clés (KMS)
- Certificats d'authentification unique
- Certificats de notification d'alerte par e-mail
- Certificats de serveur syslog externe

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

> Vous ne pouvez afficher et accéder aux informations d'autres certificats que si vous disposez de l'autorisation appropriée.

Vous pouvez :

- Afficher et modifier un certificat de fédération d'identités
- Télécharger les certificats du serveur de gestion des clés (KMS) et du client
- Spécification d'un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure
- Spécifiez manuellement un certificat SSO pour la confiance de la partie utilisatrices
- Spécifiez un certificat pour les notifications par e-mail d'alerte
- Spécifiez un certificat de serveur syslog externe

Détails du certificat de sécurité

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

Certificat de l'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de 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 **certificat d'interface de gestion**	Configurer les certificats d'interface de gestion

Certificat API S3 et Swift

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 ou Swift sécurisées vers un nœud de stockage, vers le service CLB (Connection Load Balancer) obsolète sur un nœud de passerelle et les terminaux de l'équilibreur de charge (facultatif).	**CONFIGURATION sécurité certificats**, sélectionnez l'onglet **Global**, puis **S3 et Swift API certificates**	Configurez les certificats API S3 et Swift

Certificat CA de la grille

Voir la Description du certificat CA de la grille par défaut.

Certificat du client administrateur

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

Certificat de terminal de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 ou Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un noeud final d'équilibreur de charge. Les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée de Global Certificat API S3 et Swift Certificat permettant d'authentifier les connexions au service Load Balancer. Si le certificat global est utilisé pour authentifier les connexions de l'équilibreur de charge, il n'est pas nécessaire de télécharger ou de générer un certificat distinct pour chaque noeud final de l'équilibreur de charge. **Remarque :** le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de l'StorageGRID.	**CONFIGURATION réseau points de terminaison de l'équilibreur de charge**	• Configurer les terminaux de l'équilibreur de charge • Créez un noeud final d'équilibrage de charge pour FabricPool

Certificat de fédération des identités

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 des identités, ce qui permet de gérer les groupes et les utilisateurs d'administration par un système externe.	**CONFIGURATION contrôle d'accès fédération des identités**	Utiliser la fédération des identités

Certificat de terminal des services de plate-forme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentification de la connexion depuis le service de la plateforme StorageGRID vers une ressource de stockage S3	**Tenant Manager STOCKAGE (S3) noeuds finaux des services de plate-forme**	Créer un terminal de services de plate-forme Modifier le point final des services de plate-forme

Certificat de terminal Cloud Storage Pool

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

Certificat de serveur de gestion des clés (KMS)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre StorageGRID et un serveur de gestion des clés (KMS) externe qui fournit les clés de chiffrement aux nœuds d'appliance StorageGRID.	**CONFIGURATION sécurité serveur de gestion des clés**	Ajout d'un serveur de gestion des clés (KMS)

Certificat SSO (Single Sign-on)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identités, tels que Active Directory Federation Services (AD FS) et StorageGRID utilisés pour les demandes SSO (Single Sign-on).	**CONFIGURATION contrôle d'accès Single Sign-on**	Configurer l'authentification unique

Certificat de notification d'alerte par e-mail

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.	**ALERTES Configuration de la messagerie**	Configurez 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 consigne les événements dans StorageGRID. **Remarque :** un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	**CONFIGURATION surveillance serveur d'audit et syslog**, puis sélectionnez **configurer serveur syslog externe**	Configurer un serveur syslog externe

Exemples de certificats

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un noeud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.

2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : serveur de gestion externe des clés (KMS)

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le 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 les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Configurer les certificats de serveur

Types de certificat de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (algorithme de signature numérique de courbe elliptique).

Pour plus d'informations sur la sécurisation des connexions clients par StorageGRID pour l'API REST, reportez-vous à la section Utilisation de S3 ou Utiliser Swift.

Configurer les certificats d'interface de gestion

Vous pouvez remplacer le certificat de l'interface de gestion par défaut par un certificat personnalisé unique qui permet aux utilisateurs d'accéder à Grid Manager et au Gestionnaire de locataires sans rencontrer d'avertissement de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

Description de la tâche

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

Étant donné qu'un seul certificat d'interface de gestion personnalisée est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients

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

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

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration du certificat de serveur pour l'interface de gestion** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION sécurité certificats** et en consultant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

> Si vous accédez à Grid Manager 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 option de contournement si l'un des cas suivants se produit :
>
> - Votre certificat d'interface de gestion personnalisée expire.
> - Vous restaurez le certificat de serveur par défaut à partir d'un certificat d'interface de gestion personnalisée.

Ajoutez un certificat d'interface de gestion personnalisée

Pour ajouter un certificat d'interface de gestion personnalisée, 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 **Management interface certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

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

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

- **Paquet CA** : un fichier facultatif unique contenant les certificats de chaque autorité de certification intermédiaire (AC). Le fichier doit contenir chacun des fichiers de certificat d'autorité de certification codés au 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 téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

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

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

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

Générez un certificat

Générez les fichiers de certificat du serveur.

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

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

- **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
- **IP** : une ou plusieurs adresses IP à inclure dans le certificat.
- **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
- **Jours valides**: Nombre de jours après la création que le certificat expire.

c. Sélectionnez **generate**.

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 l'emplacement de téléchargement. Enregistrez le fichier avec l'extension `.pem`.

  Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**. + le certificat d'interface de gestion personnalisée est utilisé pour toutes les nouvelles connexions ultérieures à Grid Manager, tenant Manager, l'API Grid Manager ou l'API tenant Manager.

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

> Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

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

Restaurez le certificat de l'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 **Management interface certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de 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 suivantes.

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

Ce dont vous avez besoin

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

Description de la tâche

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

Étapes

1. Obtenez le nom de domaine complet (FQDN) de chaque nœud d'administration.
2. Connectez-vous au nœud d'administration principal :
   a. Saisissez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.
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`.
   - Réglez `--type` à `management` Pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et tenant Manager.
   - Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par défaut.

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

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

   Le résultat contient le certificat public requis par votre client de l'API de gestion.
4. Sélectionnez et copiez le certificat.

   Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.
5. Déconnectez-vous du shell de commande. `$ 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 **Management interface certificate**.

7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

Téléchargez ou copiez le certificat de l'interface de gestion

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

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

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

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA 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`

Configurez les certificats API S3 et Swift

Vous pouvez remplacer ou restaurer le certificat de serveur utilisé pour les connexions client S3 ou Swift vers les nœuds de stockage, le service CLB (Connection Load Balancer) obsolète sur les nœuds de passerelle ou pour charger les noeuds finaux de l'équilibreur. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Description de la tâche

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

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

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

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration du certificat de serveur global pour S3 et l'API Swift** est déclenchée lorsque le certificat de serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez afficher quand le certificat en cours expire en sélectionnant **CONFIGURATION sécurité certificats** et en regardant la date d'expiration du certificat API S3 et Swift dans l'onglet Global.

Vous pouvez charger ou générer un certificat API S3 et Swift personnalisé.

Ajoutez un certificat S3 et Swift personnalisé

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

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

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2048 bits ou plus.

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

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

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

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

  Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copy certificate PEM** ou **Copy CA bundle PEM** pour copier le contenu du certificat pour le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 et Swift suivantes.

Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

- **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
- **IP** : une ou plusieurs adresses IP à inclure dans le certificat.
- **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
- **Jours valides**: Nombre de jours après la création que le certificat expire.

c. Sélectionnez **generate**.

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

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

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

  Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 et Swift suivantes.

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

   Après avoir téléchargé ou généré un nouveau certificat, autorisez jusqu'à un jour l'effacement des alertes d'expiration de certificat associées.

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

Restaurez le certificat API S3 et Swift par défaut

Vous pouvez revenir à l'utilisation du certificat d'API S3 et Swift par défaut pour les connexions des clients S3 et Swift vers les nœuds de stockage et du service CLB obsolète sur les nœuds de passerelle. Cependant, vous ne pouvez pas utiliser le certificat API S3 et Swift par défaut pour un noeud final d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez la version par défaut du certificat de l'API globale S3 et Swift, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat API S3 et Swift par défaut sera utilisé pour les nouvelles connexions clients S3 et Swift ultérieures aux nœuds de stockage et pour le service CLB obsolète sur les nœuds de passerelle.

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

   Si vous disposez de l'autorisation d'accès racine et que le certificat d'API S3 et Swift personnalisé a été utilisé pour les connexions de terminal de l'équilibreur de charge, une liste de terminaux d'équilibreur de charge qui ne seront plus accessibles via le certificat d'API S3 et Swift par défaut s'affiche. Accédez à Configurer les terminaux de l'équilibreur de charge pour modifier ou supprimer les points finaux affectés.

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

Téléchargez ou copiez le certificat API S3 et Swift

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 et certificat API Swift**.
3. Sélectionnez l'onglet **Server** ou **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

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

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

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont téléchargés en un seul fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un bundle CA facultatif, chaque certificat du bundle s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copy Certificate PEM** ou **Copy CA bundle PEM**.

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA 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 associées

- Utilisation de S3
- Utiliser Swift
- Configurez les noms de domaine de terminaux API S3

Copiez le certificat de l'autorité de certification Grid

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

Ce dont vous avez besoin

- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Vous disposez d'autorisations d'accès spécifiques.

Description de la tâche

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificate PEM**, téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

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

   Par exemple : `storagegrid_certificate.pem`

Configurez les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et qui ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP utilisant FabricPool, vous pouvez générer ou charger un certificat de serveur lors de la configuration du point de terminaison de l'équilibreur de charge.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.

Description de la tâche

Lorsque vous créez un noeud final d'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées

parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

Les étapes suivantes fournissent des instructions d'ordre général pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures, reportez-vous à la section Configuration de StorageGRID pour FabricPool.

> Le service distinct Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète et n'est pas recommandé pour une utilisation avec FabricPool.

Étapes

1. Configurez également un groupe haute disponibilité (HA) pour FabricPool à utiliser.
2. Créez un terminal d'équilibrage de charge S3 pour FabricPool.

   Lorsque vous créez un noeud final d'équilibreur de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre bundle CA facultatif.

3. Association de StorageGRID en tant que Tier cloud dans ONTAP

   Spécifiez le port de point final de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat de l'autorité de certification que vous avez téléchargé. Ensuite, indiquez le certificat de l'autorité de certification.

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

Configurer les certificats client

Les certificats client permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, ce qui fournit un moyen sécurisé aux outils externes de surveillance 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 de certificat dans l'outil externe.

Voir les informations sur utilisation du certificat de sécurité général et configuration des certificats de serveur personnalisés.

> Pour garantir que les opérations ne sont pas interrompues par un certificat de serveur ayant échoué, l'alerte **expiration des certificats client configurés sur la page certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le moment où le certificat en cours expire en sélectionnant **CONFIGURATION sécurité certificats** et en consultant la date d'expiration du certificat client dans l'onglet client.

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

Ce dont vous avez besoin

- Vous disposez de l'autorisation d'accès racine.
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Pour configurer un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
  - Si vous avez configuré le certificat de l'interface de gestion StorageGRID, l'autorité de certification, le certificat client et la clé privée sont 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 enregistrée ou enregistrée au moment de sa création. Si vous ne disposez pas de la clé privée d'origine, vous devez en créer une nouvelle.
- Pour modifier un certificat client :
  - Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
  - Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Suivez la procédure de votre scénario pour ajouter un certificat client :

- Certificat d'interface de gestion déjà configuré
- CERTIFICAT client émis
- Certificat généré par Grid Manager

Certificat d'interface de gestion déjà configuré

Utilisez cette procédure pour ajouter un certificat client si un certificat d'interface de gestion est déjà configuré à l'aide d'une autorité de certification 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 **Ajouter**.
3. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Dans la section **Type de certificat**, téléchargez le certificat de l'interface de gestion `.pem` fichier.
   a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
   b. Téléchargez le fichier de certificat de l'interface de gestion (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît sur l'onglet client.

6. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

   a. **Nom** : saisissez un nom pour la connexion.

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

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

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

   c. Activez **TLS client Auth** et **avec CA Cert**.

   d. Sous TLS/SSL Auth Details, copiez et collez :

      - Le certificat CA de l'interface de gestion à **CA Cert**
      - Le certificat client à **Cert client**
      - La clé privée pour **clé client**

   e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

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

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

      Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section Instructions de surveillance de StorageGRID.

CERTIFICAT client émis

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

Étapes

1. Effectuez les étapes à configurez un certificat d'interface de gestion.
2. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.
3. Sélectionnez **Ajouter**.
4. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Dans la section **Type de certificat**, téléchargez le certificat client, la clé privée et le bundle CA `.pem` fichiers :

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

b. Téléchargez des fichiers de certificat client, de clé privée et de bundle CA (`.pem`).

   - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.

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

   Les nouveaux certificats apparaissent sur l'onglet client.

7. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

   a. **Nom** : saisissez un nom pour la connexion.

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

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

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

   c. Activez **TLS client Auth** et **avec CA Cert**.

   d. Sous TLS/SSL Auth Details, copiez et collez :

      - Le certificat CA de l'interface de gestion à **CA Cert**
      - Le certificat client à **Cert client**
      - La clé privée pour **clé client**

   e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

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

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

      Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section Instructions de surveillance de StorageGRID.

Certificat généré par Grid Manager

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

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez **Ajouter**.

3. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Dans la section **Type de certificat**, sélectionnez **générer certificat**.
6. Spécifiez les informations de certificat :
   - **Nom de domaine** : un ou plusieurs noms de domaine complets du noeud d'administration à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
   - **IP** : une ou plusieurs adresses IP de noeud d'administration à inclure dans le certificat.
   - **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
7. Sélectionnez **generate**.
8. sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

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

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

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

   Par exemple : `storagegrid_certificate.pem`

   - Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
   - Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

     Spécifiez le nom du fichier de clé privée et l'emplacement de téléchargement.
9. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

   Le nouveau certificat apparaît sur l'onglet client.
10. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **Global**.
11. Sélectionnez **certificat d'interface de gestion**.
12. Sélectionnez **utiliser le certificat personnalisé**.
13. Téléchargez les fichiers Certificate.pem et private_key.pem à partir du détails du certificat client étape. Il n'est pas nécessaire de télécharger le pack CA.
    a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
    b. Téléchargez chaque fichier de certificat (`.pem`).
    c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

       Le nouveau certificat apparaît sur l'onglet client.
14. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

a. **Nom** : saisissez un nom pour la connexion.

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

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

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

c. Activez **TLS client Auth** et **avec CA Cert**.

d. Sous TLS/SSL Auth Details, copiez et collez :

   - Le certificat client de l'interface de gestion à la fois **CA Cert** et **client Cert**
   - La clé privée pour **clé client**

e. **NomServeur** : saisissez le nom de domaine du noeud d'administration.

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

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

   Vous avez désormais accès aux metrics Prometheus à partir de StorageGRID grâce à votre outil de surveillance externe.

Pour plus d'informations sur les mesures, reportez-vous à la section Instructions de surveillance de StorageGRID.

Modifier les certificats client

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.

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

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**
4. Saisissez un nom de certificat contenant au moins 1 et 32 caractères.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans 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 celui actuel a expiré.

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.

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

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis sélectionnez une option d'édition.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **Télécharger 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 certificat PEM.

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

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

   Par exemple : `storagegrid_certificate.pem`

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

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

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

Générez un certificat

Générez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

   - **Nom de domaine** : un ou plusieurs noms de domaine pleinement qualifiés à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
   - **IP** : une ou plusieurs adresses IP à inclure dans le certificat.
   - **Sujet**: X.509 sujet ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides**: Nombre de jours après la création que le certificat expire.

c. Sélectionnez **generate**.

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

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

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

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

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier la clé privée** pour copier la clé privée de certificat pour coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée en tant que fichier.

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

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

Le nouveau certificat apparaît sur l'onglet client.

Téléchargez ou copiez les certificats client

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat que vous souhaitez copier ou télécharger.
3. Téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

a. Sélectionnez **Télécharger le certificat**.

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

Par exemple : `storagegrid_certificate.pem`

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 client

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez le certificat à supprimer.

3. Sélectionnez **Supprimer**, puis confirmez.

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

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

Configurer les serveurs de gestion des clés

Configurer les serveurs de gestion des clés : présentation

Vous pouvez configurer un ou plusieurs serveurs de gestion externe des clés (KMS) afin de protéger les données sur les nœuds d'appliance spécialement configurés.

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

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

Vous pouvez utiliser un ou plusieurs serveurs de gestion des clés pour gérer les clés de cryptage de nœud pour tous les nœuds d'appliance StorageGRID dont le paramètre **Node Encryption** est activé pendant l'installation. L'utilisation de serveurs de gestion des clés avec ces nœuds de dispositif permet de protéger vos données même en cas de retrait d'une appliance du data Center. Une fois les volumes de l'appliance chiffrés, vous ne pouvez accéder à aucune donnée sur l'appliance à moins que le nœud ne puisse communiquer avec le KMS.

> StorageGRID ne crée ni ne gère pas les clés externes utilisées pour chiffrer et décrypter les nœuds des systèmes. Si vous prévoyez d'utiliser un serveur de gestion externe des clés pour protéger les données StorageGRID, vous devez comprendre comment configurer ce serveur et savoir comment gérer les clés de cryptage. Ces instructions ne sont pas uniquement destinées à effectuer des tâches de gestion clés. Si vous avez besoin d'aide, consultez la documentation de votre serveur de gestion des clés ou contactez le support technique.

Étudiez les méthodes de cryptage StorageGRID

StorageGRID fournit plusieurs options pour le chiffrement des données. Consultez les méthodes disponibles pour identifier les méthodes qui répondent à vos exigences en matière de protection des données.

Le tableau fournit un récapitulatif détaillé des méthodes de cryptage disponibles dans StorageGRID.

Option de chiffrement	Comment cela fonctionne	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous configurez un serveur de gestion des clés pour le site StorageGRID (**CONFIGURATION sécurité serveur de gestion des clés**) et activez le cryptage des noeuds pour l'appliance. Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et décrypte la clé de chiffrement des données (DEK) sur chaque volume.	Nœuds d'appliance sur lesquels **Node Encryption** est activé pendant l'installation. Toutes les données de l'appliance sont protégées contre les pertes ou les suppressions physiques du data Center. 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.
Sécurité des disques dans SANtricity System Manager	Si la fonction sécurité des disques est activée pour une appliance de stockage, vous pouvez utiliser SANtricity System Manager pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données sur les disques sécurisés.	Appliances de stockage dotées de disques FDE (Full Disk Encryption) ou FIPS (Federal information Processing Standard). Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Ne peut pas être utilisé avec certains dispositifs de stockage ni avec des appliances de service. • Dispositifs de stockage SG6000 • Appliances de stockage SG5700 • Appliances de stockage SG5600
Option de grille de chiffrement d'objet stocké	L'option **Inenregistré Object Encryption** peut être activée dans Grid Manager (**CONFIGURATION System Grid options**). Lorsqu'il est activé, tout nouvel objet qui n'est pas chiffré au niveau du compartiment ou au niveau de l'objet est chiffré lors de l'ingestion.	Ingestion récente des données d'objet S3 et Swift. Les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. • Configurez le chiffrement des objets stockés

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement de compartiment S3	Vous émettez une demande de chiffrement Put bucket pour activer le chiffrement du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. • Utilisation de S3
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une demande S3 pour stocker un objet et inclure le `x-amz-server-side-encryption` en-tête de demande.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. • Utilisation de S3
Chiffrement côté serveur objet S3 avec clés fournies par le client (SSE-C)	Vous émettez une demande 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 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors du StorageGRID. • Utilisation de S3
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement autres que StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, de métadonnées et de configuration du système, en supposant que chaque volume ou datastore est chiffré. Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées.

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées. • "Amazon simple Storage Service - Guide des développeurs : 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 à la fois. Par exemple :

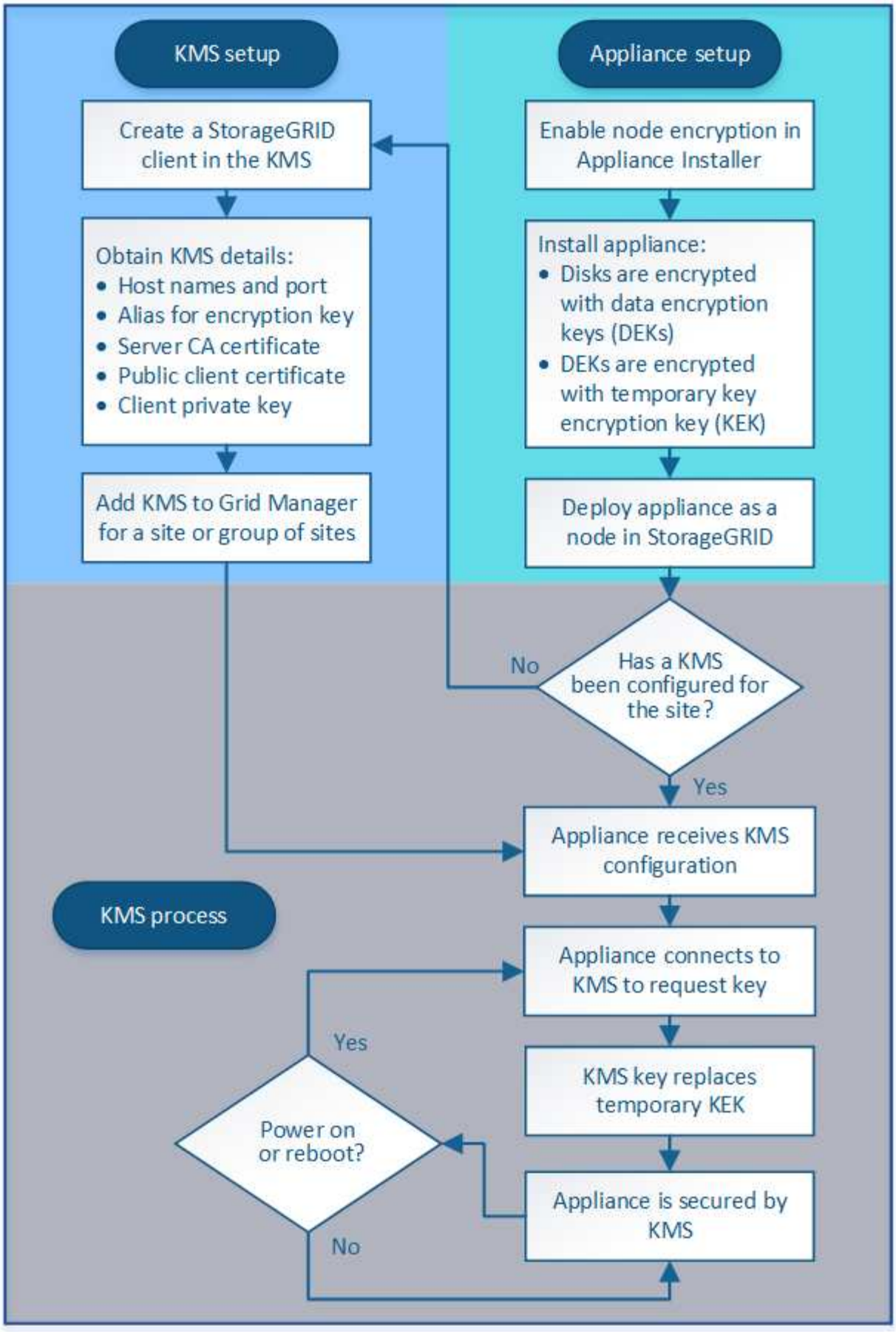
- Vous pouvez utiliser un KMS pour protéger les nœuds d'appliance et utiliser également la fonctionnalité de sécurité des disques de SANtricity System Manager pour « déchiffrer » les données présentes sur les disques à autocryptage des mêmes dispositifs.
- Vous pouvez utiliser un KMS pour sécuriser les données sur les nœuds d'appliance et utiliser l'option GRID de chiffrement d'objet stocké pour chiffrer tous les objets à l'ingestion.

Si seule une petite partie de vos objets doit être cryptée, pensez à contrôler le chiffrement au niveau du compartiment ou de l'objet au niveau individuel. L'activation de plusieurs niveaux de chiffrement a un coût supplémentaire en termes de performance.

Présentation de la configuration des appliances et KMS

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

L'organigramme présente les étapes générales permettant d'utiliser un KMS pour sécuriser les données StorageGRID sur les nœuds du dispositif.



L’organigramme présente la configuration du KMS et l’appliance en parallèle. Toutefois, vous pouvez

configurer les serveurs de gestion des clés avant ou après avoir activé le chiffrement des nœuds pour les nouveaux nœuds d'appliance, selon vos besoins.

Configuration du serveur de gestion des clés (KMS)

La configuration d'un serveur de gestion des clés comprend les étapes générales suivantes.

Étape	Reportez-vous à la section
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque cluster KMS ou KMS.	Configurer StorageGRID en tant que client dans le KMS
Obtenir les informations requises pour le client StorageGRID sur le KMS.	Configurer StorageGRID en tant que client dans le KMS
Ajoutez le KMS à Grid Manager, attribuez-le à un seul site ou à un groupe de sites par défaut, téléchargez les certificats requis et enregistrez la configuration KMS.	Ajout d'un serveur de gestion des clés (KMS)

Configurez l'appareil

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

1. Pendant l'étape de configuration matérielle de l'installation de l'appliance, utilisez le programme d'installation de l'appliance StorageGRID pour activer le paramètre **Node Encryption** pour l'appliance.

   > Vous ne pouvez pas activer le paramètre **Node Encryption** après l'ajout d'une appliance à la grille et vous ne pouvez pas utiliser la gestion externe des clés pour les appliances dont le cryptage de nœud n'est pas activé.

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

Pour plus de détails, reportez-vous aux sections suivantes :

- Appareils de services SG100 et SG1000
- Dispositifs de stockage SG6000
- Appliances de stockage SG5700
- Appliances de stockage SG5600

Processus de chiffrement de la gestion des clés (automatique)

Le chiffrement de la gestion des clés inclut les étapes générales suivantes qui sont automatiquement effectuées.

1. Lorsque vous installez une appliance sur laquelle le chiffrement de nœud est activé dans le grid, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
   - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.
   - Si un KMS n'a pas encore été configuré pour le site, les données de l'appliance continuent d'être cryptées par le KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.
2. L'appliance utilise la configuration KMS pour vous connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé du KMS remplace la KEK temporaire et est maintenant utilisée pour crypter et décrypter les clés de fin de séjour des volumes d'appliance.

   > Toutes les données qui existent avant que le nœud d'appliance chiffré ne se connecte 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 de leur retrait du data Center tant que la clé temporaire n'est pas remplacée par la clé de cryptage KMS.

4. Si l'appliance est sous tension ou redémarrée, elle se reconnecte au KMS pour demander la clé. La clé, qui est enregistrée dans la mémoire volatile, ne peut pas survivre à une perte de puissance ou à un redémarrage.

Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés

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

Quelles sont les exigences du protocole KMIP ?

StorageGRID prend en charge KMIP version 1.4.

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

Les communications entre les nœuds d'appliance et le KMS configuré utilisent des connexions TLS sécurisées. StorageGRID prend en charge le chiffrement TLS v1.2 suivant pour KMIP :

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

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

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

Quels dispositifs sont pris en charge ?

Vous pouvez utiliser un serveur de gestion des clés (KMS) pour gérer les clés de cryptage de n'importe quelle appliance StorageGRID de la grille dont le paramètre **Node Encryption** est activé. Ce paramètre ne peut être activé que lors de l'étape de configuration matérielle de l'installation de l'appliance à l'aide du programme d'installation de l'appliance StorageGRID.

> Vous ne pouvez pas activer le chiffrement de nœud après l'ajout d'une appliance à la grille et ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement de nœud n'est pas activé.

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

Appliance	Type de nœud
Appareil de services SG1000	Nœud d'administration ou nœud de passerelle
Appareil de services SG100	Nœud d'administration ou nœud de passerelle
Dispositif de stockage SG6000	Nœud de stockage
Appliance de stockage SG5700	Nœud de stockage
Appliance de stockage SG5600	Nœud de stockage

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds Software-based (non appliance), notamment :

- Nœuds déployés en tant que machines virtuelles
- Nœuds déployés dans les moteurs de mise en conteneurs sur les hôtes Linux

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

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

Dans le cadre d'une nouvelle installation, vous devez généralement configurer un ou plusieurs serveurs de gestion des clés dans Grid Manager avant de créer des locataires. Cette commande garantit que les nœuds sont protégés avant que des données d'objet ne soient stockées sur ces nœuds.

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

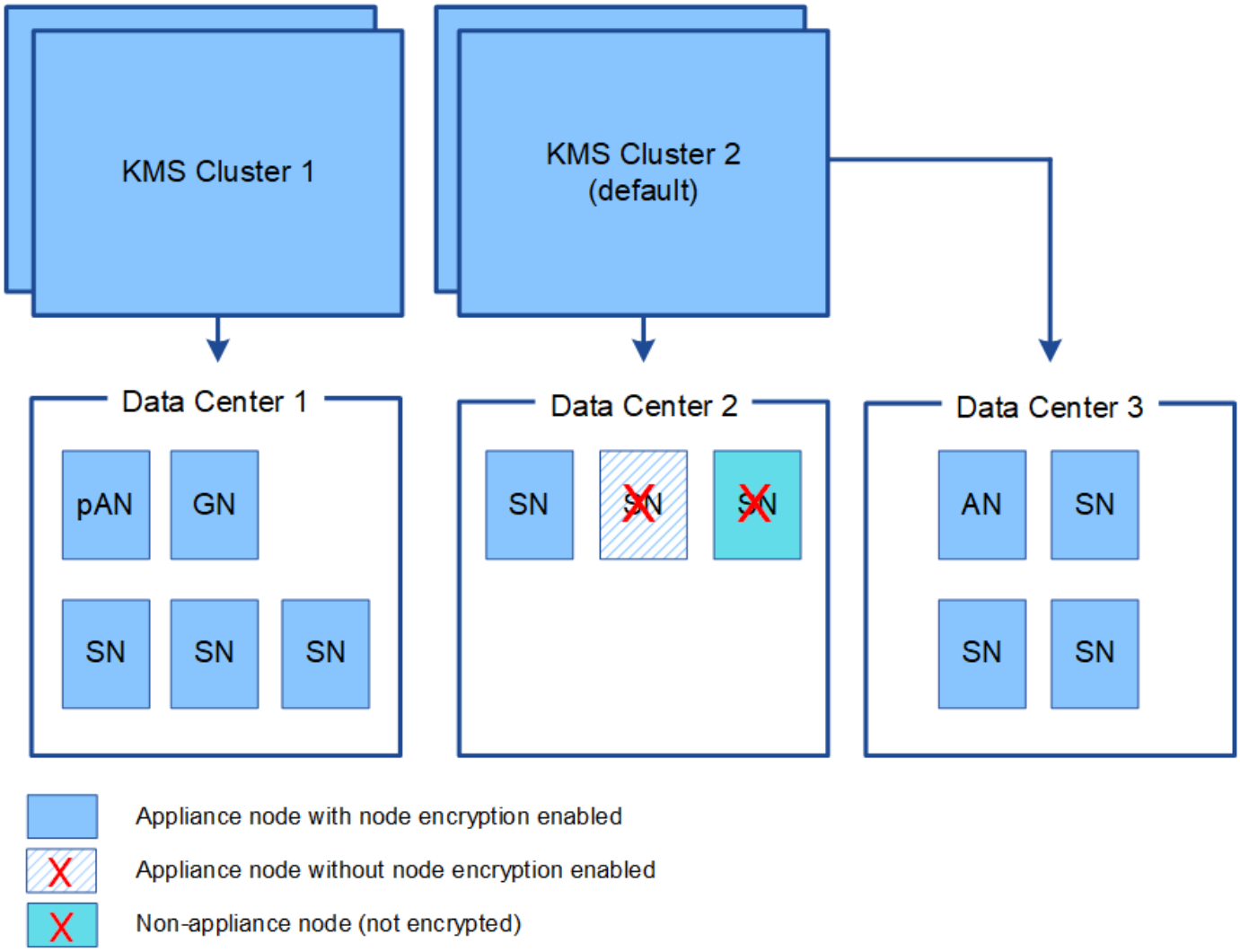
Combien de serveurs de gestion des clés ai-je besoin ?

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

StorageGRID prend en charge l'utilisation des clusters KMS. Chaque cluster KMS contient plusieurs serveurs de gestion des 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 il améliore les fonctionnalités de basculement d'une configuration haute disponibilité.

Supposons par exemple que votre système StorageGRID possède trois sites de data Center. Vous pouvez configurer un cluster KMS pour que tous les nœuds d'appliance soient essentiels dans le Data Center 1 et un second cluster KMS pour que ces derniers soient essentiels pour que tous les nœuds d'appliance soient disponibles sur 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 de KMS pour les nœuds non-appliance ou pour les nœuds d'appliance dont le paramètre **Node Encryption** n'est pas activé au cours de l'installation.



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

Dans le cadre de nos meilleures pratiques en matière de sécurité, vous devez régulièrement faire tourner la clé de chiffrement utilisée par chaque KMS configuré.

Lors de la rotation de la clé de chiffrement, utilisez le logiciel KMS pour faire pivoter la dernière version utilisée de la clé vers une nouvelle version de la même clé. Ne pas tourner sur une clé totalement différente.

Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS dans Grid Manager. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. Utilisez le même alias de clé pour les nouvelles clés que celles utilisées pour les touches précédentes. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données.

Lorsque la nouvelle version de clé est disponible :

- Elle est automatiquement distribuée aux nœuds d'appliance chiffrés sur le site ou les sites associés au KMS. La distribution doit se produire dans une heure après la rotation de la clé.
- Si le nœud d'appliance chiffré est hors ligne lorsque la nouvelle version de clé est distribuée, le nœud reçoit la nouvelle clé dès le redémarrage.
- Si la nouvelle version de la clé ne peut pas être utilisée pour crypter les volumes de l'appliance, l'alerte **KMS échec de rotation de la clé de chiffrement** 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 chiffrement ?

Si vous devez installer une appliance chiffrée dans un autre système StorageGRID, vous devez d'abord désactiver le nœud de grille pour déplacer les données d'objet vers un autre nœud. Ensuite, vous pouvez utiliser le programme d'installation de l'appliance StorageGRID pour effacer la configuration KMS. L'effacement de la configuration KMS désactive le paramètre **Node Encryption** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID.

Étant donnée l'accès à la clé de chiffrement KMS, toutes les données conservées sur l'appliance ne sont plus accessibles et sont verrouillées en permanence.

Informations associées

- Appareils de services SG100 et SG1000
- Dispositifs de stockage SG6000
- Appliances de stockage SG5700
- Appliances de stockage SG5600

Considérations relatives à la modification du KMS pour un site

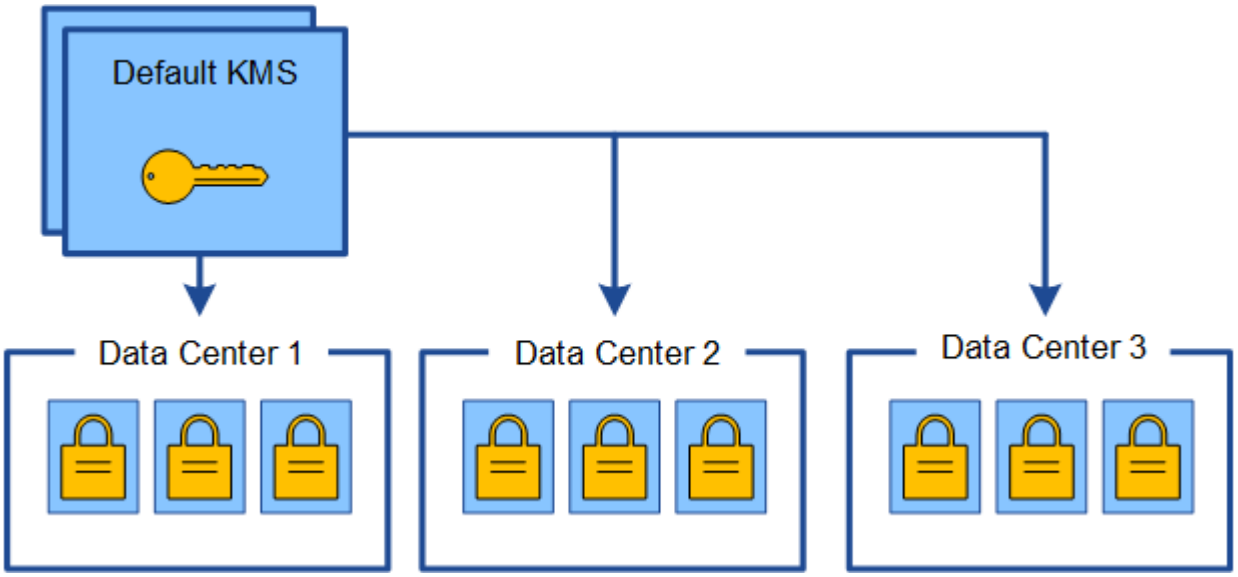
Chaque cluster de serveur de gestion des clés (KMS) ou KMS fournit une clé de chiffrement à tous les nœuds d'appliance sur un site unique ou dans un groupe de sites. Si vous devez modifier le KMS utilisé pour un site, vous devrez peut-être copier la clé de chiffrement d'un KMS vers un autre.

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

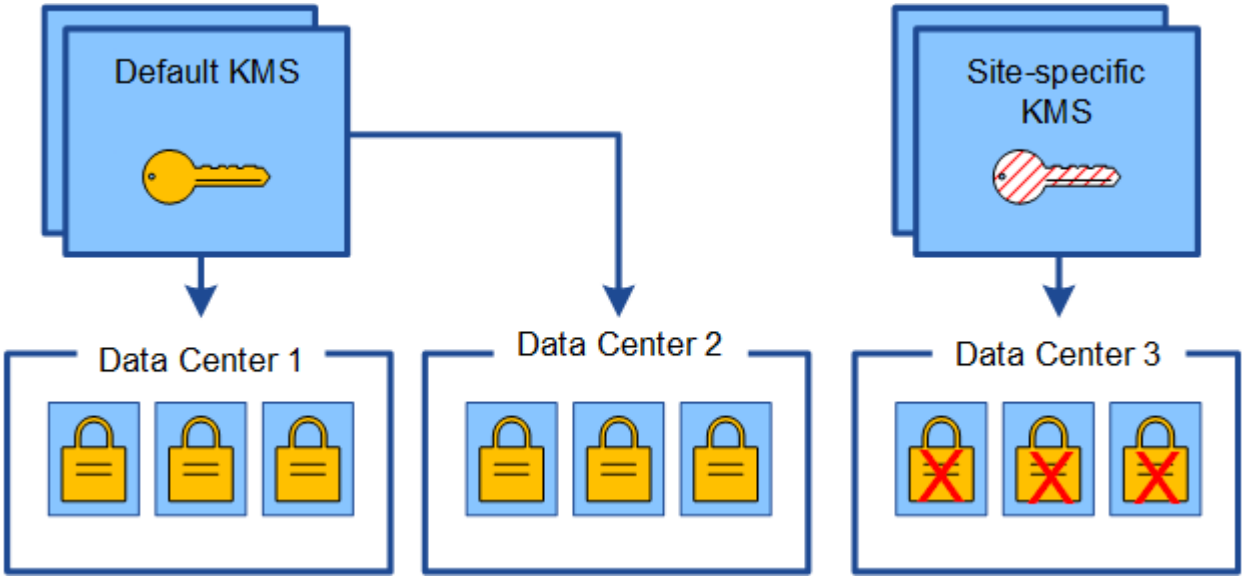
Par exemple :

1. Vous configurez au départ un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.

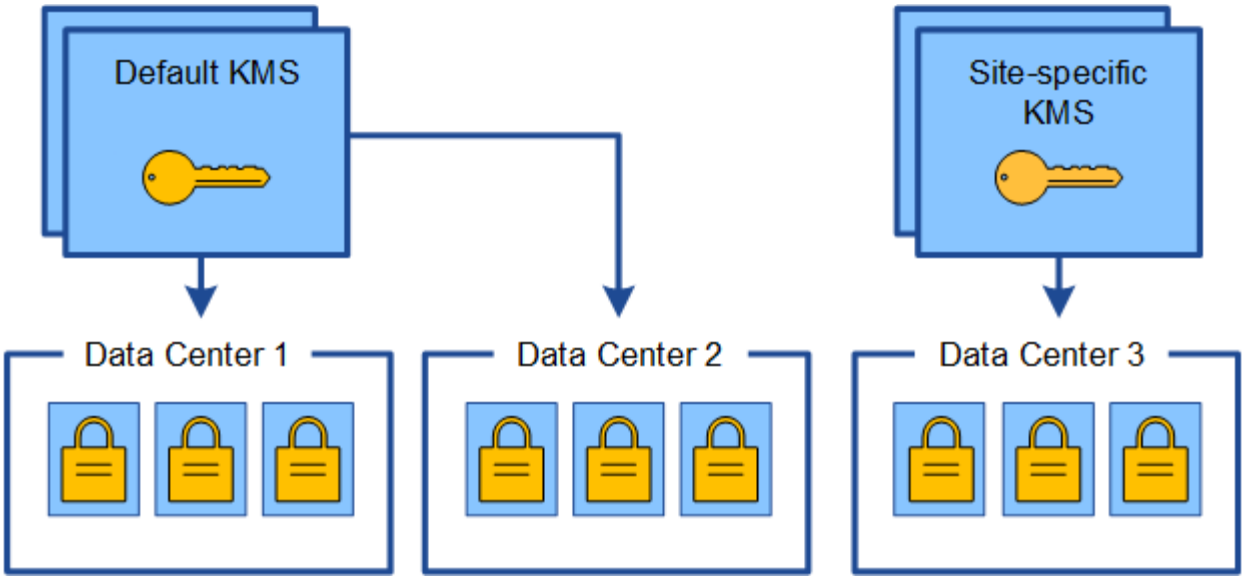
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée pour chiffrer les nœuds de l'appliance sur tous les sites. Cette même clé doit également être utilisée pour décrypter ces dispositifs.



3. Vous décidez d'ajouter un KMS spécifique au site pour un site (Data Center 3 dans la figure). Toutefois, les nœuds d'appliance sont déjà chiffrés. Une erreur de validation se produit lorsque vous tentez d'enregistrer la configuration du KMS spécifique au site. L'erreur se produit car le KMS spécifique au site ne dispose pas de la clé correcte pour décrypter les nœuds de ce site.



4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement à partir du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine dans 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 décrypter les nœuds d'appliance sur Data Center 3, afin qu'ils puissent être sauvegardés sur StorageGRID.



Cas d'utilisation pour changer quel KMS est utilisé pour un site

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

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous avez une ou plusieurs entrées KMS spécifiques au site, et vous souhaitez utiliser l'une d'entre elles comme étant le KMS par défaut.	Modifiez le KMS spécifique au site. Dans le champ **gère clés pour**, sélectionnez **sites non gérés par un autre KMS (KMS par défaut)**. Le KMS spécifique au site sera maintenant utilisé comme KMS par défaut. Il s'appliquera à tous les sites qui n'ont pas de KMS dédié. Modification d'un serveur de gestion des clés (KMS)
Vous avez un KMS par défaut et vous ajoutez un nouveau site dans une extension. Vous ne souhaitez pas utiliser le KMS par défaut pour le nouveau site.	1. Si les nœuds d'appliance du 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 à partir du KMS par défaut vers un nouveau KMS. 2. À l'aide de Grid Manager, ajoutez le nouveau KMS et sélectionnez le site. Ajout d'un serveur de gestion des clés (KMS)

Cas d'utilisation lors de la modification du KMS d'un site	Étapes requises
Vous souhaitez que le KMS pour un site utilise un serveur différent.	1. Si les nœuds d'appliance du site ont déjà été chiffrés par le KMS existant, utilisez le logiciel KMS pour copier la version actuelle de la clé de chiffrement à partir du KMS existant vers le nouveau KMS. 2. À l'aide de Grid Manager, modifiez la configuration KMS existante et entrez le nouveau nom d'hôte ou l'adresse IP. Ajout d'un serveur de gestion des clés (KMS)

Configurer StorageGRID en tant que client dans le KMS

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

Description de la tâche

Ces instructions s'appliquent à Thales CipherTrust Manager k170v, versions 2.0, 2.1 et 2.2. Pour toute question concernant l'utilisation d'un autre serveur de gestion des clés avec StorageGRID, contactez le support technique.

"Thales CipherTrust Manager"

Étapes

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

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

2. Depuis le logiciel KMS, créez une clé de chiffrement AES pour chaque cluster KMS ou KMS.

   La clé de cryptage doit être exportable.

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

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

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

   > La clé de chiffrement doit déjà exister dans le KMS. StorageGRID ne crée ni ne gère pas de clés KMS.

4. Pour chaque cluster KMS ou KMS, procurez-vous un certificat de serveur signé par une autorité de certification (CA) ou un bundle de certificats contenant chacun des fichiers de certificat d'autorité de certification codés au 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 au format PEM (Privacy Enhanced Mail) Base-64.
- Le champ Subject alternative Name (SAN) de chaque certificat de serveur doit inclure le nom de domaine complet (FQDN) ou l'adresse IP à laquelle StorageGRID se connectera.

> Lorsque vous configurez le KMS dans StorageGRID, vous devez entrer 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. Obtenir le certificat du client public délivré à StorageGRID par le KMS externe et la clé privée du certificat du client.

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

Ajout d'un serveur de gestion des clés (KMS)

L'assistant de serveur de gestion des clés StorageGRID vous permet d'ajouter chaque cluster KMS ou KMS.

Ce dont vous avez besoin

- Vous avez passé en revue le considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés.
- Vous avez Configuration de StorageGRID en tant que client dans le KMS, Et vous disposez des informations requises pour chaque cluster KMS ou KMS.
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Vous disposez de l'autorisation d'accès racine.

Description de la tâche

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

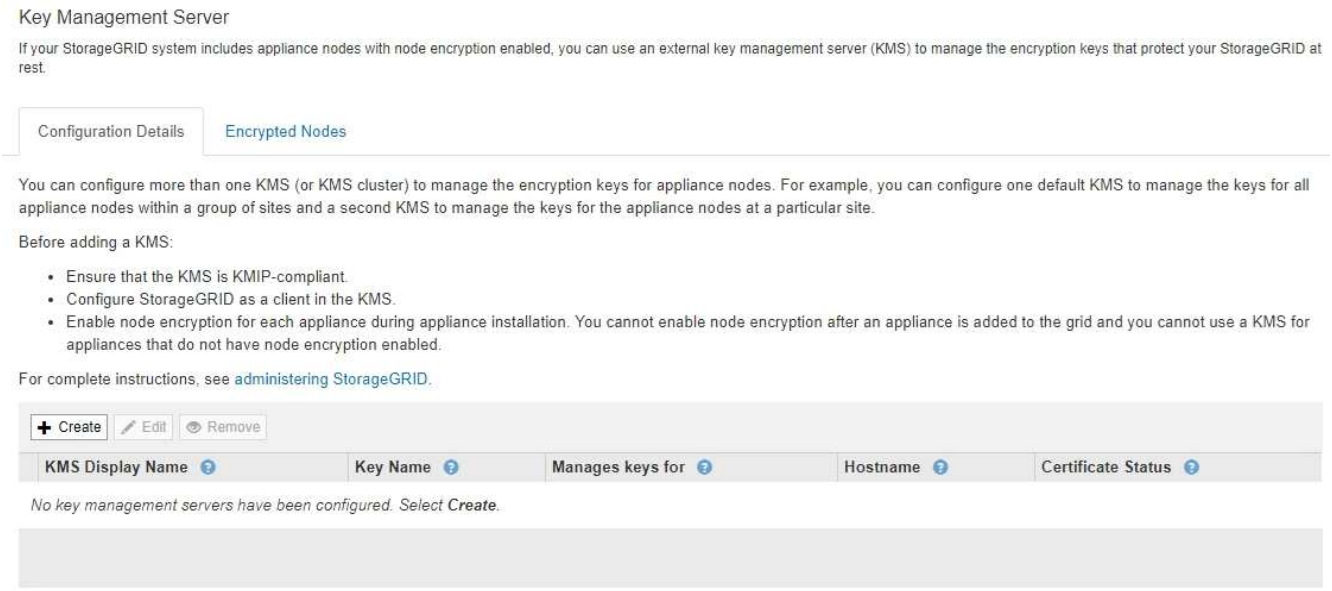
Étape 1 : saisissez les détails du KMS

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

Étapes

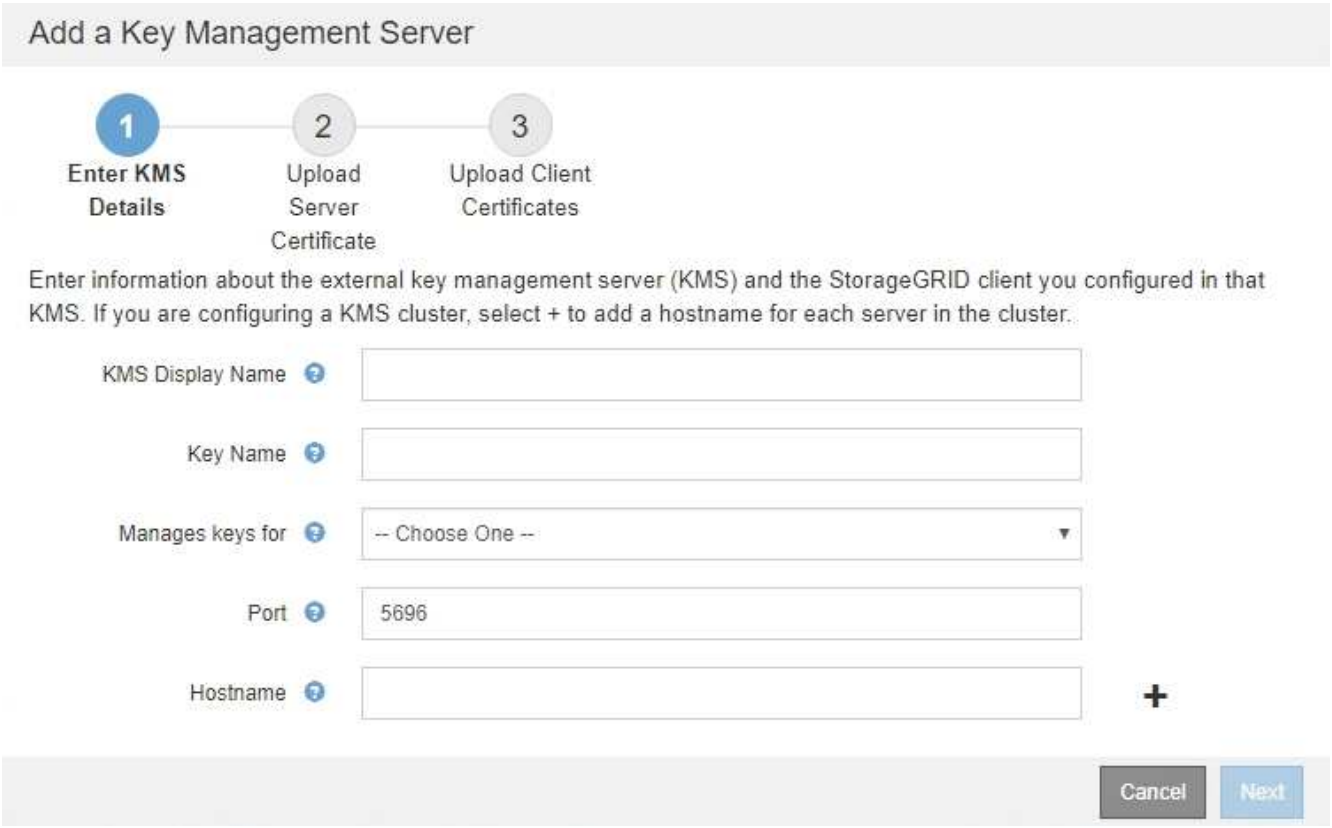
1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

   La page Key Management Server s'affiche avec l'onglet Configuration Details (Détails de la configuration) sélectionné.



2. Sélectionnez **Créer**.

   L'étape 1 (entrer les détails KMS) de l'assistant Ajout d'un serveur de gestion de clés s'affiche.



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

Champ	Description
Nom d'affichage DES KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.

Champ	Description
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer des serveurs de gestion de clés spécifiques au site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS. • Sélectionnez un site si ce KMS gère les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez **sites non gérés par un autre KMS (KMS par défaut)** pour configurer un KMS par défaut qui s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. **Remarque :** Une erreur de validation se produit lorsque vous enregistrez la configuration KMS si vous sélectionnez un site qui a été précédemment crypté par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de cryptage d'origine au nouveau KMS.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ SAN du certificat de serveur doit inclure le FQDN ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous utilisez un cluster KMS, sélectionnez le signe plus ➕ pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Suivant**.

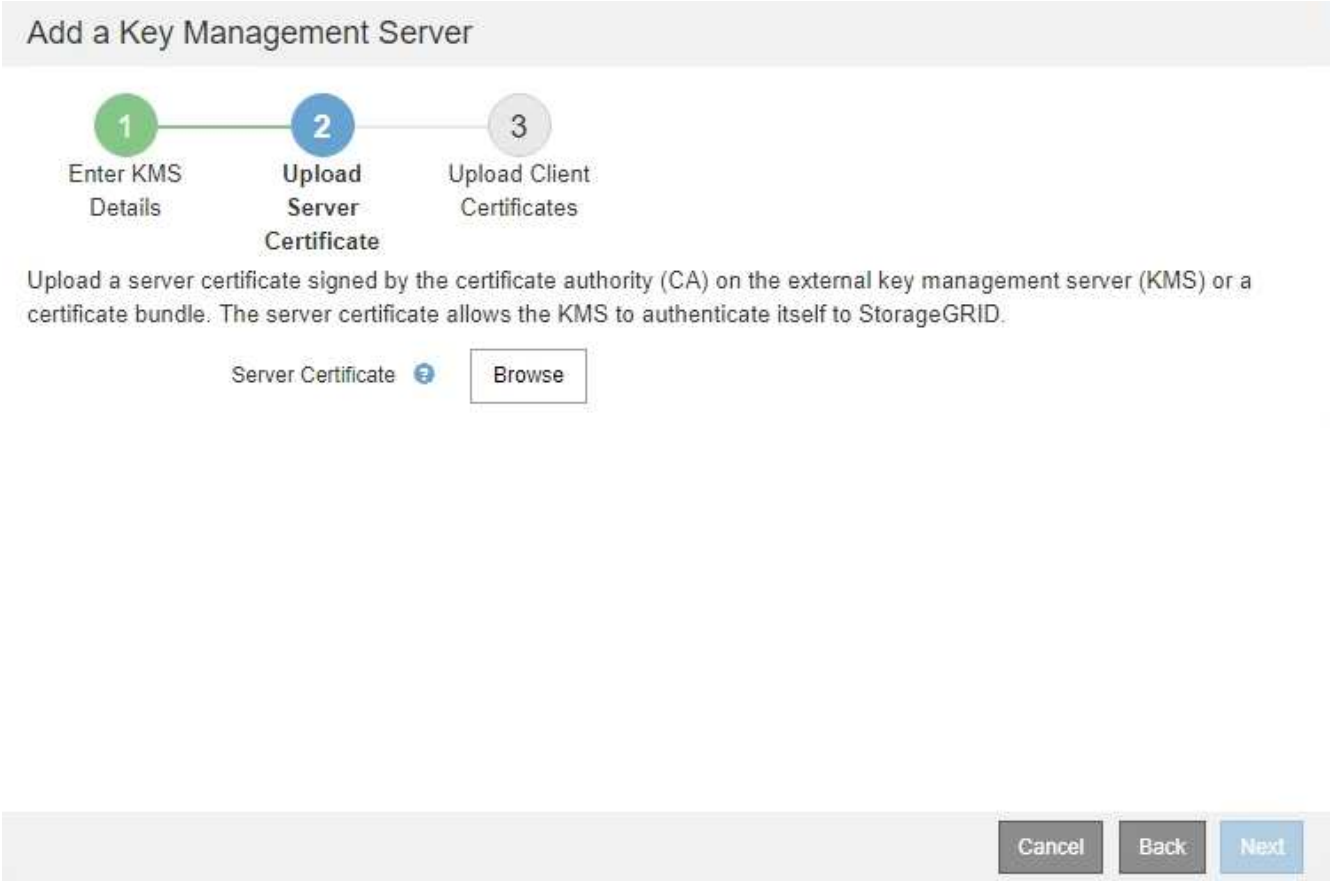
Étape 2 : télécharger le certificat du serveur

À l'étape 2 (Télécharger le certificat de serveur) de l'assistant Ajout d'un serveur de gestion de clés, vous téléchargez le certificat de serveur (ou le paquet de certificats) pour le KMS. Le certificat du serveur permet au

KMS externe de s’authentifier auprès de StorageGRID.

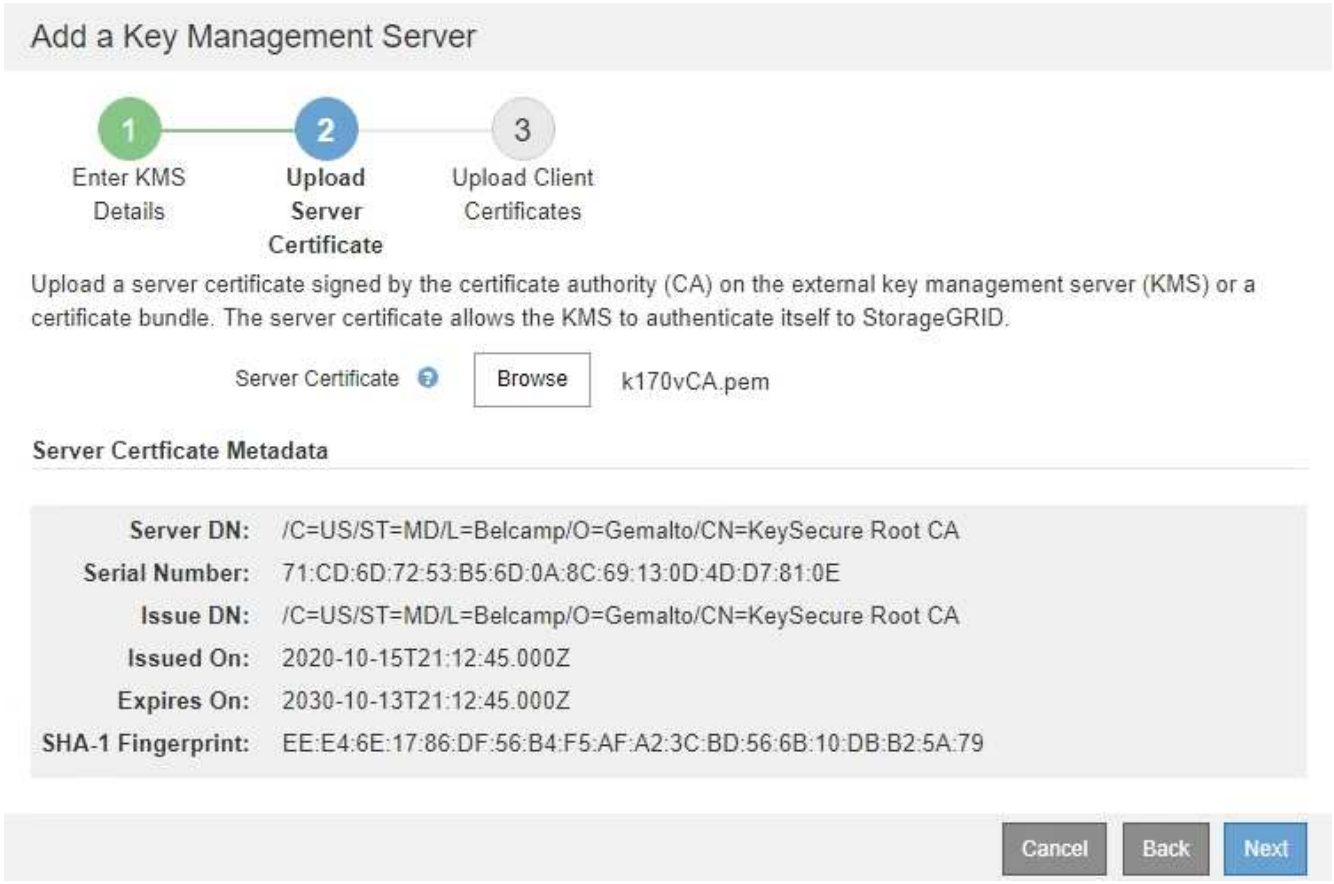
Étapes

1. À partir de **Etape 2 (Télécharger le certificat du serveur)**, accédez à l’emplacement du certificat du serveur enregistré ou du groupe de certificats.



2. Téléchargez le fichier de certificat.

   Les métadonnées du certificat de serveur s’affichent.



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

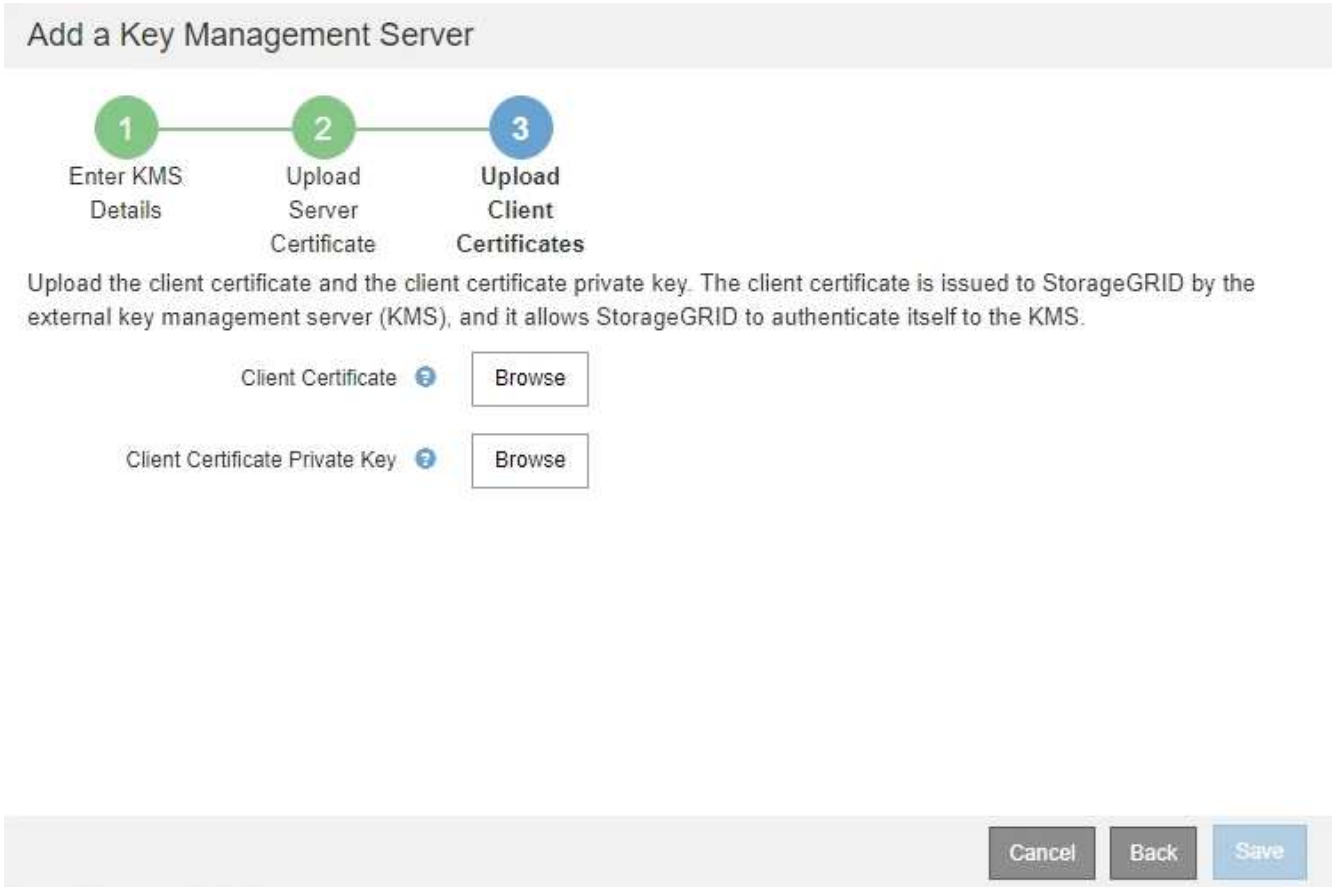
3. Sélectionnez **Suivant**.

Étape 3 : télécharger des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajout d'un serveur de gestion des 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 **Etape 3 (Téléchargement de certificats client)**, accédez à l'emplacement du certificat client.

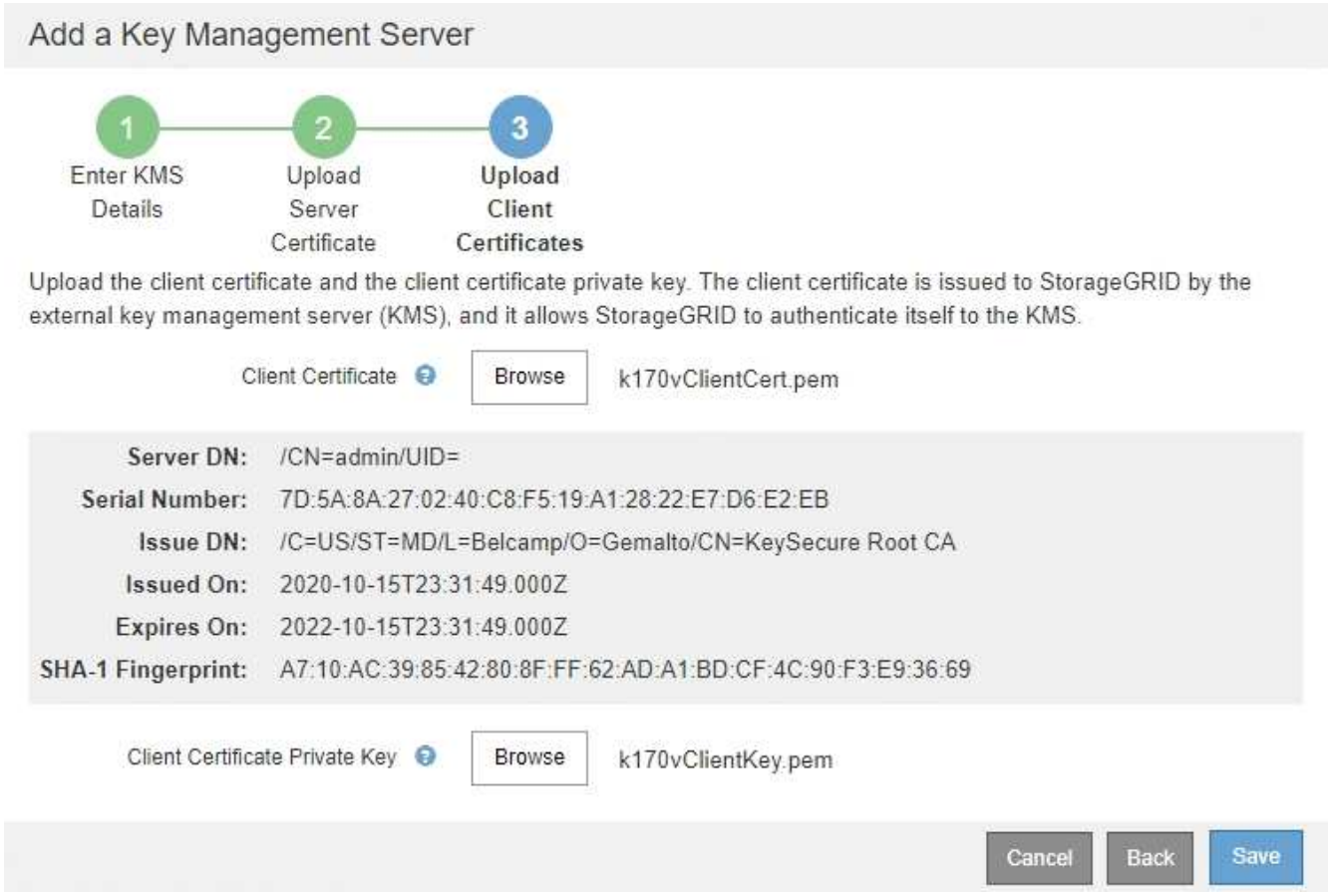


2. Téléchargez le fichier de certificat client.

   Les métadonnées du certificat client s’affichent.

3. Accédez à l’emplacement de la clé privée pour le certificat client.
4. Téléchargez le fichier de clé privée.

   Les métadonnées du certificat client et de la clé privée du certificat client s’affichent.



5. Sélectionnez **Enregistrer**.

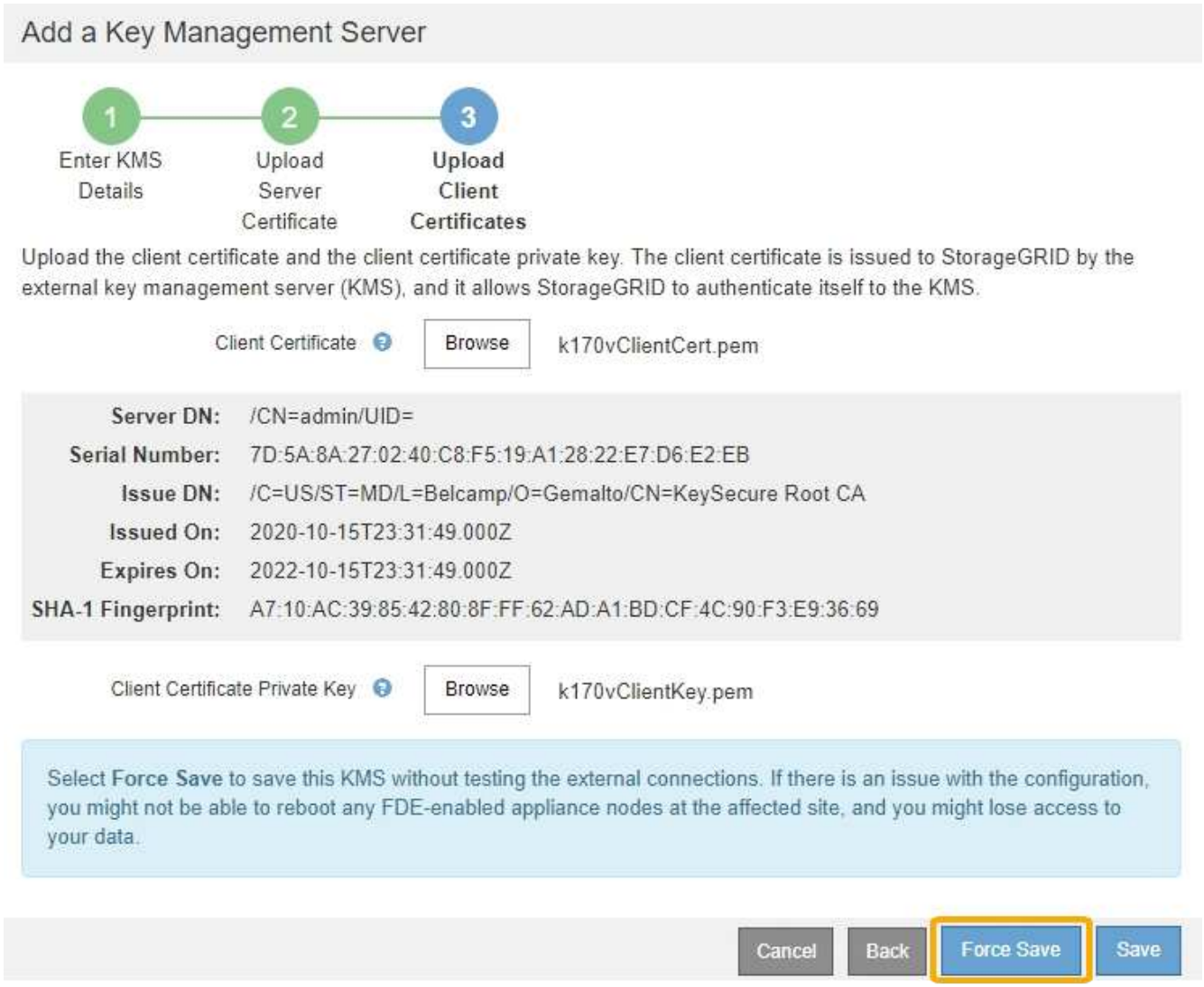
   Les connexions entre le serveur de gestion des clés et les nœuds de dispositif sont testées. Si toutes les connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté à la table de la page serveur de gestion des clés.

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

6. Si un message d'erreur apparaît lorsque vous sélectionnez **Enregistrer**, vérifiez les détails du message, puis sélectionnez **OK**.

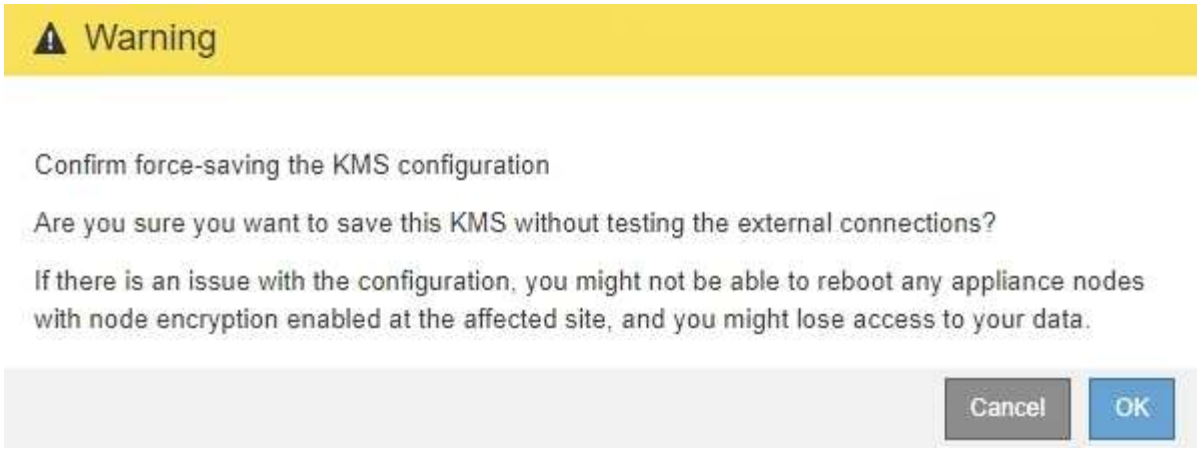
   Par exemple, vous pourriez recevoir une erreur 422 : entité impossible à traiter si un test de connexion a échoué.

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



Si vous sélectionnez **forcer l'enregistrement**, la configuration KMS est enregistrée, mais il ne teste pas la connexion externe de chaque appliance vers ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

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



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

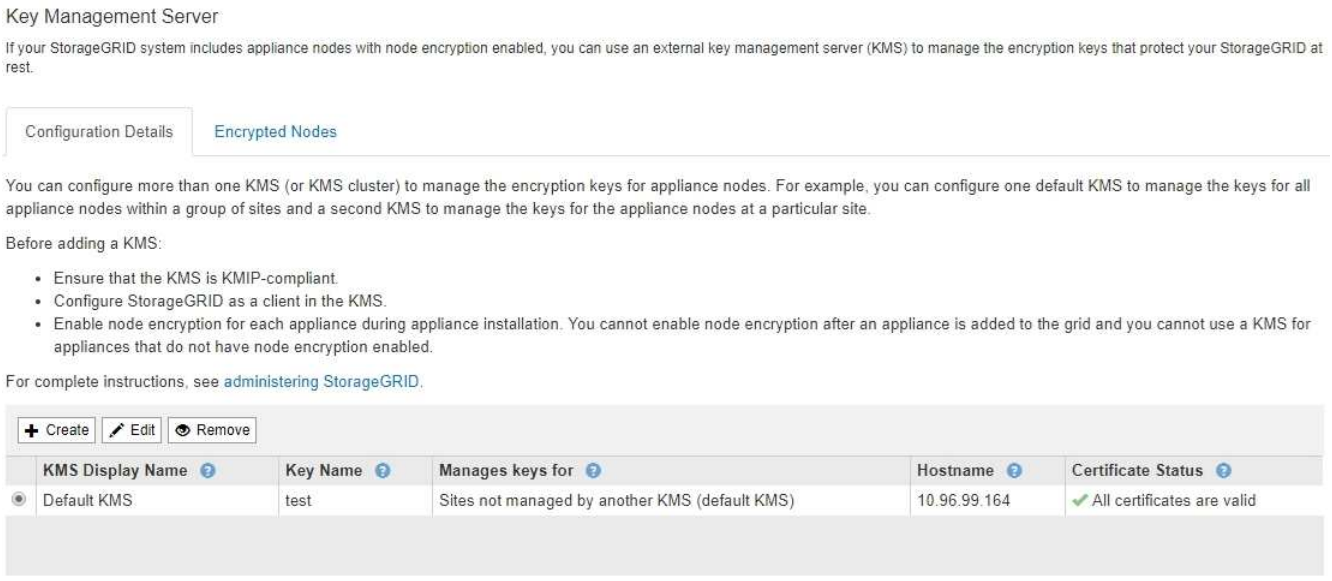
Afficher les détails du KMS

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

   La page Key Management Server s'affiche. L'onglet Détails de la configuration affiche tous les serveurs de gestion des clés configurés.



2. Examinez les informations du tableau pour chaque KMS.

Champ	Description
Nom d'affichage DES KMS	Nom descriptif du KMS.

Champ	Description
Nom de clé	Alias de clé pour le client StorageGRID dans le KMS.
Gère les clés pour	Site StorageGRID associé au KMS Ce champ affiche le nom d'un site StorageGRID spécifique ou **sites non gérés par un autre KMS (KMS par défaut).**
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. S'il existe un cluster de deux serveurs de gestion des clés, le nom de domaine complet ou l'adresse IP des deux serveurs sont répertoriés. S'il y a plus de deux serveurs de gestion des clés dans un cluster, le nom de domaine complet ou l'adresse IP du premier KMS est répertorié avec le nombre de serveurs de gestion des 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, puis sélectionnez **Modifier**.
État du certificat	État actuel du certificat de serveur, du certificat d'autorité de certification facultatif et du certificat client : valide, expiré, proche de l'expiration ou inconnu. **Remarque :** StorageGRID peut prendre 30 minutes pour obtenir des mises à jour de l'état du certificat. Vous devez actualiser votre navigateur Web pour voir les valeurs actuelles.

3. Si l'état du certificat est inconnu, attendez jusqu'à 30 minutes, puis actualisez votre navigateur Web.

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

4. Si la colonne État du certificat indique qu'un certificat a expiré ou qu'il arrive à expiration, traitez le problème dès que possible.

   Consultez les actions recommandées pour les alertes d'expiration du certificat CA **KMS**, **expiration du certificat client KMS** et **expiration du certificat serveur KMS** dans les instructions pour Contrôle et dépannage de StorageGRID.

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

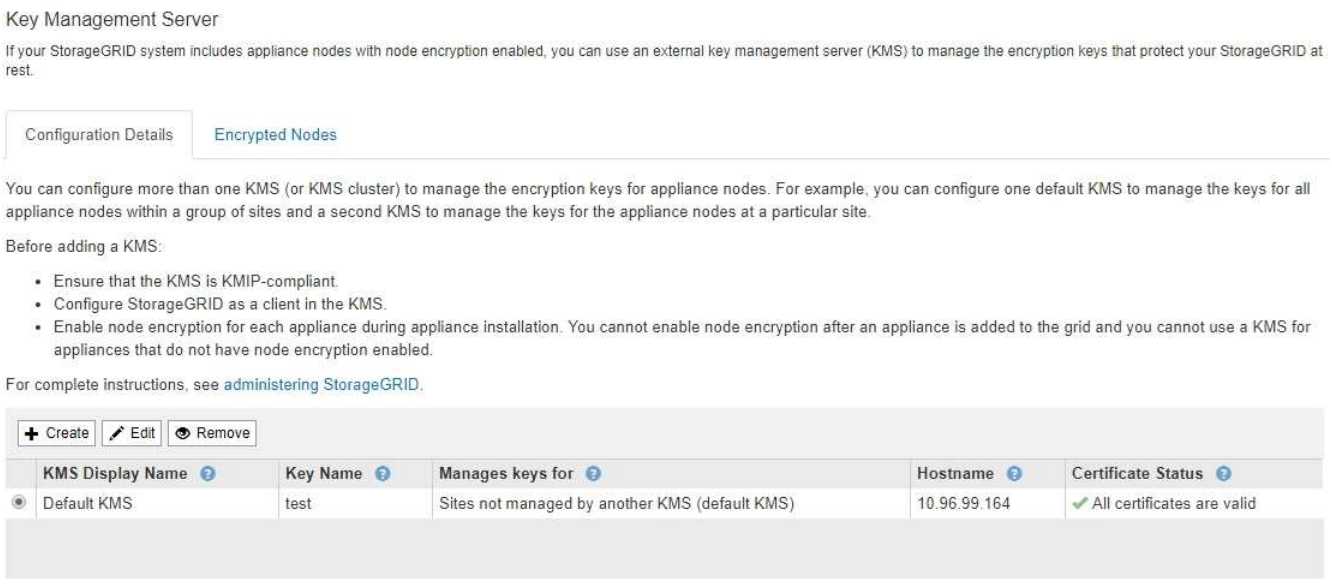
Afficher les nœuds chiffrés

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

Étapes

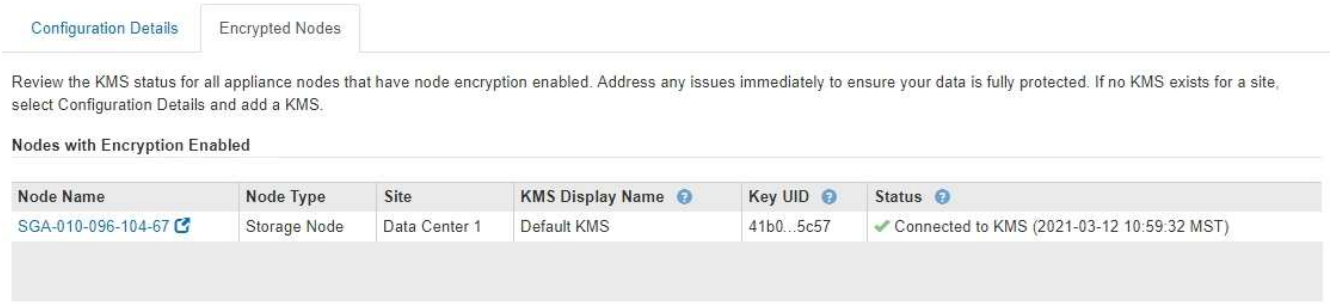
1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

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



2. En haut de la page, sélectionnez l'onglet **Nodes cryptés**.

   L'onglet nœuds cryptés répertorie les nœuds d'appliance de votre système StorageGRID dont le paramètre **Node Encryption** est activé.



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

Colonne	Description
Nom du nœud	Nom du nœud d'appliance.
Type de nœud	Le type de nœud : stockage, Administrateur ou passerelle.
Le site	Nom du site StorageGRID sur lequel le nœud est installé.
Nom d'affichage DES KMS	Nom descriptif du KMS utilisé pour le nœud. Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de la configuration pour ajouter un KMS. Ajout d'un serveur de gestion des clés (KMS)
UID de clé	ID unique de la clé de cryptage utilisée pour crypter et décrypter les données sur le nœud de l'appliance. Pour afficher l'intégralité d'un UID de clé, placez le curseur sur la cellule. Un tiret (--) indique que l'UID de clé est inconnu, peut-être en raison d'un problème de connexion entre le nœud de l'appliance et le KMS.
État	L'état de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de connexion peut prendre plusieurs minutes après la modification de la configuration KMS. **Remarque :** vous devez actualiser votre navigateur Web pour voir les nouvelles valeurs.

4. Si la colonne État indique un problème KMS, répondez immédiatement au problème.

   Pendant les opérations KMS normales, l'état sera **connecté à KMS**. Si un nœud est déconnecté de la grille, l'état de connexion du nœud est affiché (administrativement arrêté ou inconnu).

   Les autres messages d'état correspondent aux alertes StorageGRID portant le même nom :

   - Echec du chargement de la configuration DES KMS
   - Erreur de connectivité KMS

- Nom de la clé de cryptage KMS introuvable
- Echec de la rotation de la clé de chiffrement KMS
- La clé KMS n'a pas réussi à décrypter un volume d'appliance
- LES KMS ne sont pas configurés

Reportez-vous aux actions recommandées pour ces alertes dans les instructions pour Contrôle et dépannage de StorageGRID.

> Vous devez immédiatement résoudre tout problème pour assurer la protection intégrale de vos données.

Modification d'un serveur de gestion des clés (KMS)

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

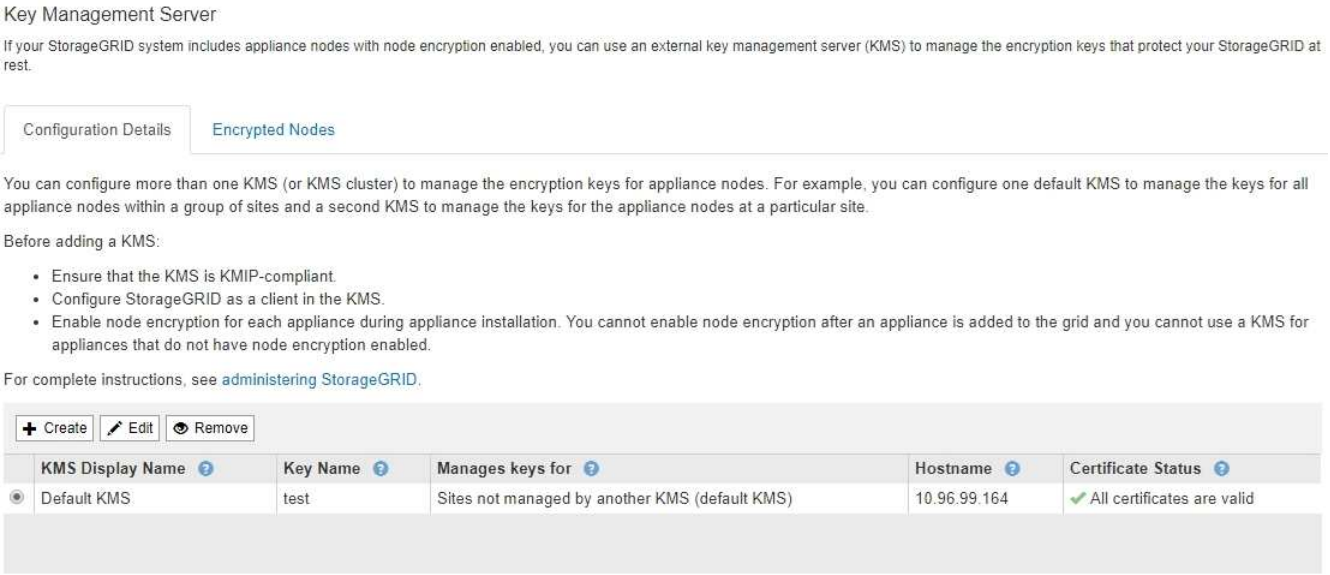
Ce dont vous avez besoin

- Vous avez passé en revue le considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés.
- Si vous prévoyez de mettre à jour le site sélectionné pour un KMS, vous avez examiné le Considérations relatives à la modification du KMS pour un site.
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

   La page Key Management Server s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.



2. Sélectionnez le KMS à modifier et sélectionnez **Modifier**.
3. Vous pouvez également mettre à jour les détails dans **étape 1 (entrer les détails KMS)** de l'assistant

Modifier un serveur de gestion de clés.

Champ	Description
Nom d'affichage DES KMS	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. Il vous suffit de modifier le nom de la clé dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de la clé précédente ont été copiées dans l'historique des versions du nouvel alias. Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du KMS. Faites plutôt pivoter la clé en mettant à jour la version de clé dans le logiciel KMS. StorageGRID nécessite que toutes les versions de clés déjà utilisées (ainsi que toutes les versions à venir) soient accessibles depuis le KMS avec le même alias de clé. Si vous modifiez l'alias de clé pour un KMS configuré, StorageGRID risque de ne pas être en mesure de décrypter vos données. Considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés
Gère les clés pour	Si vous modifiez un KMS spécifique au site et que vous n'avez pas déjà un KMS par défaut, vous pouvez sélectionner **sites non gérés par un autre KMS (par défaut KMS)**. Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. **Remarque :** si vous modifiez un KMS spécifique au site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications KMIP (Key Management Interoperability Protocol). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ SAN du certificat de serveur doit inclure le FQDN ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

4. Si vous configurez un cluster KMS, sélectionnez le signe plus ➕ pour ajouter un nom d'hôte pour chaque serveur du cluster.
5. Sélectionnez **Suivant**.

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

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

   L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion de clés s'affiche.

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

   Les connexions entre le serveur de gestion des clés et tous les nœuds d'appliance chiffrés sur les sites affectés 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 à la table de la page Key Management Server.

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

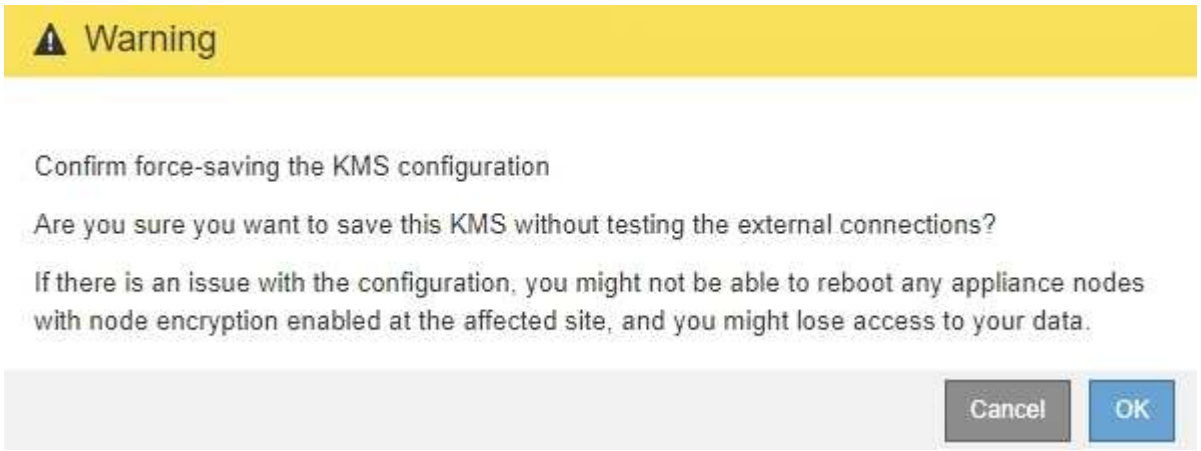
    Par exemple, vous pouvez recevoir une erreur 422 : entité impossible à traiter si le site que vous avez sélectionné pour ce KMS est déjà géré par un autre KMS, ou si un test de connexion a échoué.

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

    > Si vous sélectionnez **forcer l'enregistrement**, la configuration KMS est enregistrée, mais il ne teste pas la connexion externe de chaque appliance vers ce KMS. En cas de problème avec la configuration, vous ne pouvez pas redémarrer les nœuds d'appliance pour lesquels le chiffrement de nœud est activé sur le site affecté. L'accès à vos données risque d'être perdu jusqu'à la résolution des problèmes.

    La configuration KMS est enregistrée.

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



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

Suppression d’un serveur de gestion des clés (KMS)

Dans certains cas, vous pouvez supprimer un serveur de gestion des clés. Par exemple, vous pouvez vouloir supprimer un KMS spécifique au site si vous avez désactivé le site.

Ce dont vous avez besoin

- Vous avez passé en revue le considérations et conditions requises pour l’utilisation d’un serveur de gestion des clés.
- Vous êtes connecté au Grid Manager à l’aide d’un navigateur web pris en charge.
- Vous disposez de l’autorisation d’accès racine.

Description de la tâche

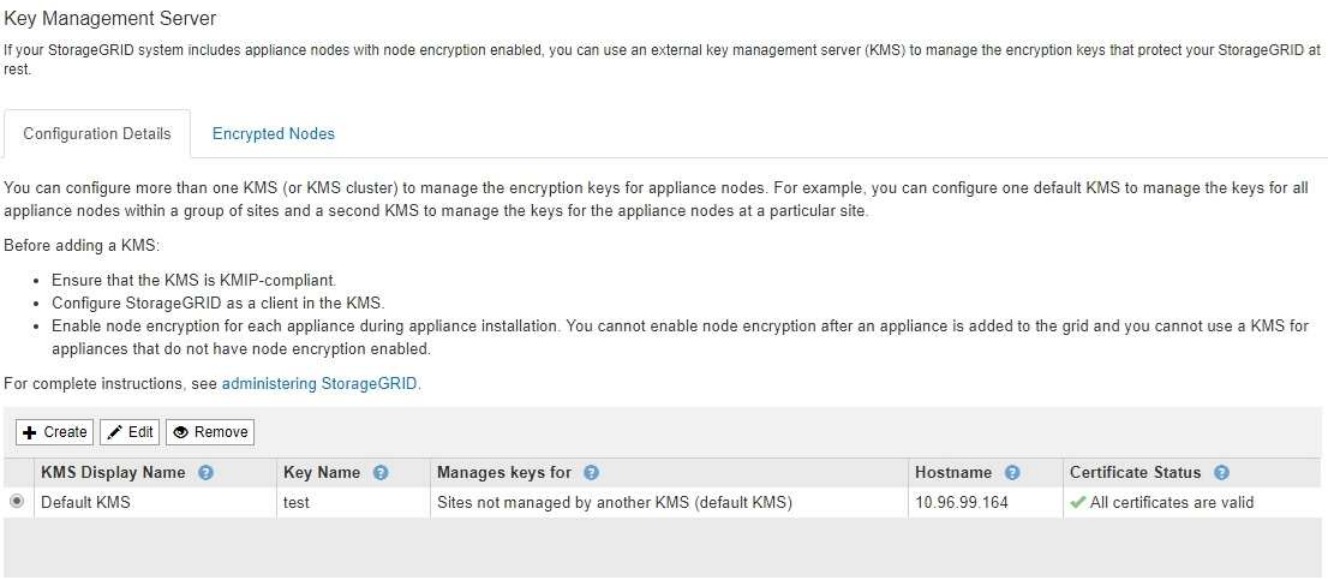
Vous pouvez supprimer un KMS dans les cas suivants :

- Vous pouvez supprimer un KMS spécifique au site si le site a été désactivé ou si le site ne contient aucun nœud d’appliance lorsque le chiffrement de nœud est activé.
- Vous pouvez supprimer le KMS par défaut si un KMS spécifique au site existe déjà pour chaque site sur lequel des nœuds d’appliance sont activés pour que le chiffrement des nœuds soit activé.

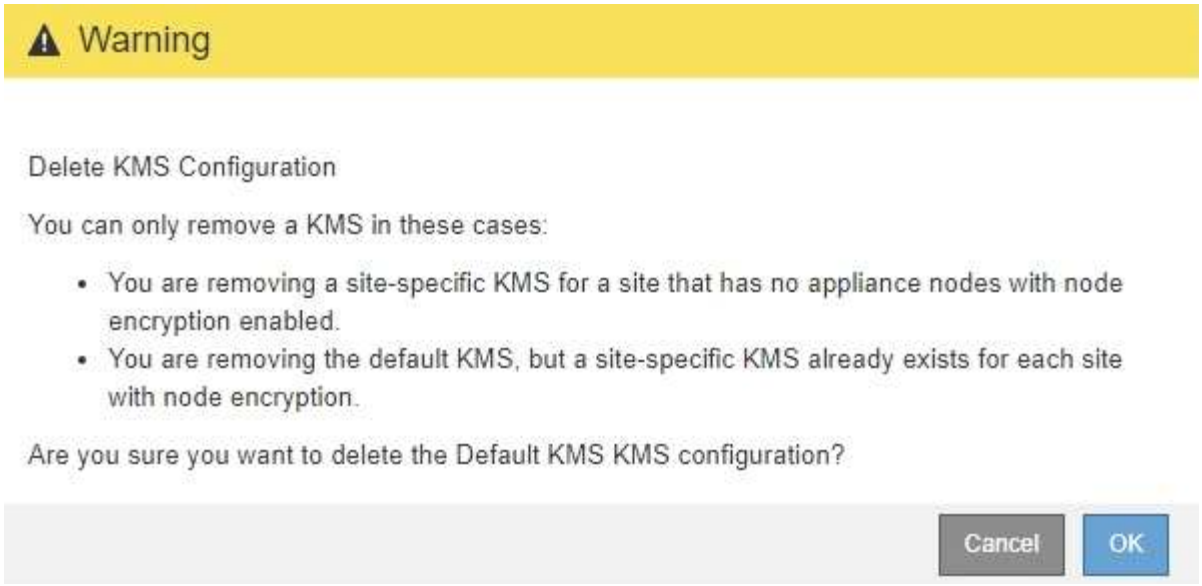
Étapes

1. Sélectionnez **CONFIGURATION sécurité serveur de gestion des clés**.

   La page Key Management Server s’affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.



2. Sélectionnez le bouton radio du KMS que vous souhaitez supprimer, puis sélectionnez **Supprimer**.
3. Passez en revue les éléments à prendre en compte dans la boîte de dialogue d’avertissement.



4. Sélectionnez **OK**.

   La configuration KMS est supprimée.

Gérer les paramètres proxy

Configurez les paramètres du proxy de stockage

Si vous utilisez des services de plateforme ou des pools de stockage cloud, vous pouvez configurer un proxy non transparent entre les nœuds de stockage et les terminaux S3 externes. Par exemple, vous aurez peut-être besoin d'un proxy non transparent pour permettre l'envoi de messages de services de plate-forme vers des noeuds finaux externes, tels qu'un noeud final sur Internet.

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.

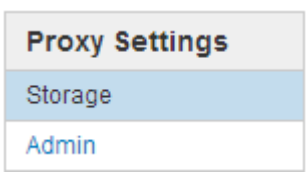
Description de la tâche

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

Étapes

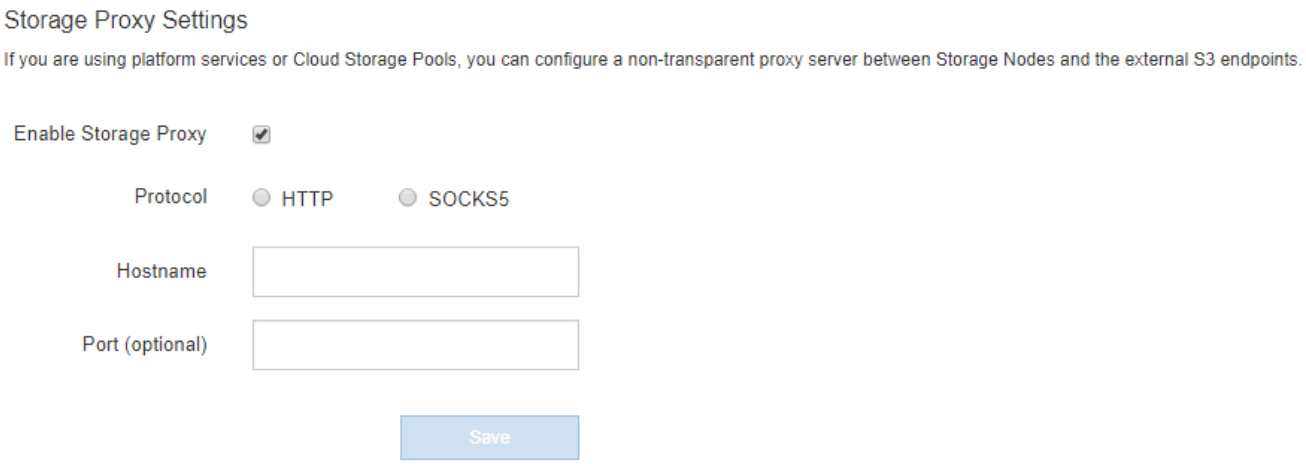
1. Sélectionnez **CONFIGURATION sécurité Paramètres proxy**.

   La page Paramètres du proxy de stockage s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.



2. Cochez la case **Activer le proxy de stockage**.

   Les champs de configuration d'un proxy de stockage s'affichent.



3. Sélectionnez le protocole du proxy de stockage non transparent.
4. Entrez 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.

   Vous pouvez laisser ce champ vide si vous utilisez le port par défaut pour le protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

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

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

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme de StorageGRID ne seront pas bloqués.

Une fois que vous avez terminé

Si vous devez désactiver un proxy de stockage, décochez la case **Activer le proxy de stockage** et sélectionnez **Enregistrer**.

Informations associées

- Réseau et ports pour les services de plate-forme
- Gestion des objets avec ILM

Configurez les paramètres du proxy d'administration

Si vous envoyez des messages AutoSupport via HTTP ou HTTPS (reportez-vous à la section Configurez AutoSupport), vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Ce dont vous avez besoin

- Vous disposez d'autorisations d'accès spécifiques.
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.

Description de la tâche

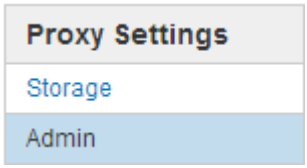
Vous pouvez configurer les paramètres d'un proxy d'administration unique.

Étapes

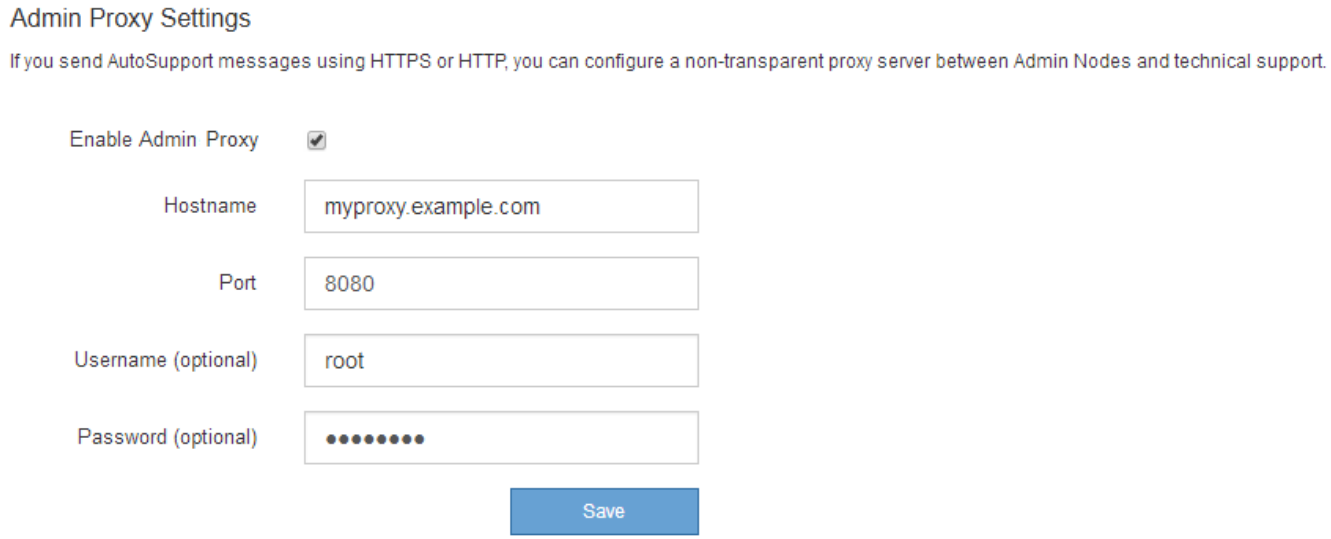
1. Sélectionnez **CONFIGURATION sécurité Paramètres proxy**.

   La page Paramètres du proxy administrateur s'affiche. Par défaut, **Storage** est sélectionné dans le menu de la barre latérale.

2. Dans le menu barre latérale, sélectionnez **Admin**.



3. Cochez la case **Activer le proxy d'administration**.



4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir le nom d'utilisateur du proxy.

   Laissez ce champ vide si votre serveur proxy ne nécessite pas de nom d'utilisateur.

7. Vous pouvez également saisir le mot de passe du proxy.

   Laissez ce champ vide si votre serveur proxy ne nécessite pas de mot de passe.

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.

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

Gérer les réseaux clients non fiables

Gérer les réseaux clients non approuvés : présentation

Si vous utilisez un réseau client, vous pouvez protéger StorageGRID des attaques hostiles en acceptant le trafic client entrant uniquement sur les noeuds finaux configurés explicitement.

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. Par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de la grille sur tous les ports externes disponibles (voir les informations sur les communications externes dans le Instructions de mise en réseau).

Vous pouvez réduire la menace d'attaques hostiles sur votre système StorageGRID en spécifiant que le réseau client sur chaque nœud est *non fiable*. Si le réseau client d'un nœud n'est pas fiable, le nœud accepte uniquement les connexions entrantes sur les ports explicitement configurés en tant que points finaux d'équilibreur de charge. Voir Configurer les terminaux de l'équilibreur de charge.

Exemple 1 : le nœud de passerelle n'accepte que les requêtes HTTPS S3

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

1. À partir de la page des noeuds finaux Load Balancer, configurez un noeud final Load Balancer pour S3 sur HTTPS sur le port 443.
2. Dans la page réseaux clients non approuvés, spécifiez que le réseau client sur le nœud de passerelle n'est pas fiable.

Après avoir enregistré votre configuration, tout le trafic entrant sur le réseau client du nœud passerelle est supprimé, sauf pour les requêtes HTTPS S3 sur le port 443 et les requêtes ICMP Echo (ping).

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

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

- Dans la page réseaux clients non approuvés, indiquez que le réseau client sur le nœud de stockage n'est pas fiable.

Après avoir enregistré votre configuration, le nœud de stockage n'accepte plus de trafic entrant sur le réseau client, mais continue d'autoriser les requêtes sortantes vers Amazon Web Services.

Le réseau client du nœud spécifié n'est pas fiable

Si vous utilisez un réseau client, vous pouvez spécifier si le réseau client de chaque nœud est fiable ou non fiable. Vous pouvez également spécifier le paramètre par défaut

pour les nouveaux nœuds ajoutés dans une extension.

Ce dont vous avez besoin

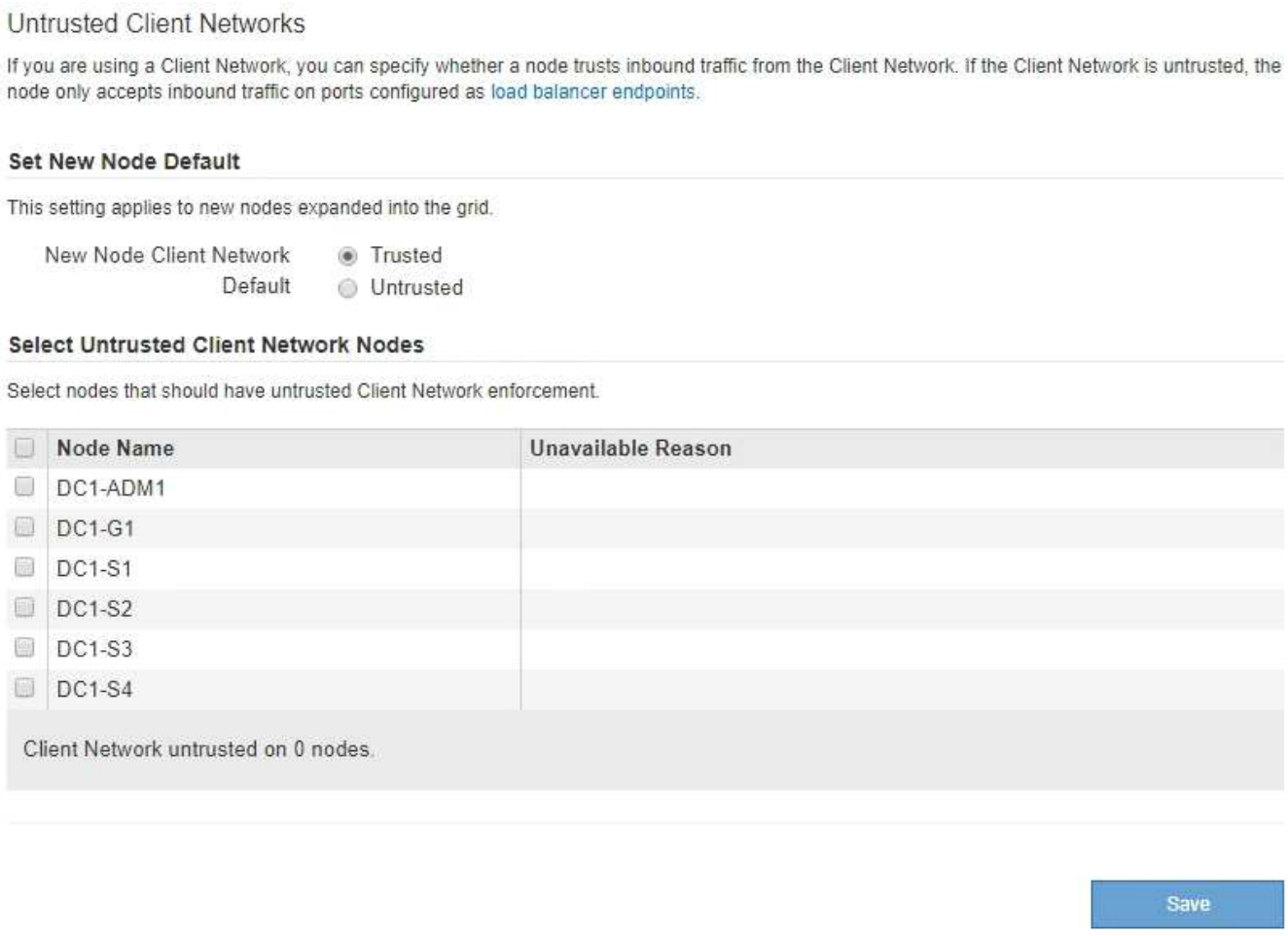
- Vous êtes connecté au Grid Manager à l'aide d'un navigateur web pris en charge.
- Vous disposez de l'autorisation d'accès racine.
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des noeuds finaux configurés explicitement, vous avez défini les noeuds finaux de l'équilibreur de charge.

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

Étapes

1. Sélectionnez **CONFIGURATION sécurité réseaux client non fiables**.

   La page réseaux clients non fiables répertorie tous les nœuds de votre système StorageGRID. La colonne motif indisponible comprend une entrée si le réseau client du nœud doit être approuvé.



2. Dans la section **Set New Node Default** (définir nouveau nœud par défaut*), indiquez le paramètre par défaut à utiliser lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.

   - **Trusted**: Lorsqu'un noeud est ajouté dans une extension, son réseau client est fiable.
   - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable. Si

nécessaire, vous pouvez revenir à cette page pour modifier le paramètre d'un nouveau nœud spécifique.

> Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.

3. Dans la section **Sélectionner des nœuds réseau client non approuvés**, sélectionnez les nœuds qui doivent autoriser les connexions client uniquement sur les noeuds finaux de l'équilibreur de charge configurés explicitement.

   Vous pouvez sélectionner ou désélectionner la case à cocher du titre pour sélectionner ou désélectionner tous les nœuds.

4. Sélectionnez **Enregistrer**.

   Les nouvelles règles de pare-feu sont immédiatement ajoutées et appliquées. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.