# Configurer les serveurs de gestion des clés

StorageGRID software

NetApp
July 23, 2026

# Sommaire

# Configurer les serveurs de gestion des clés

## Découvrez les serveurs de gestion des clés dans StorageGRID

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

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

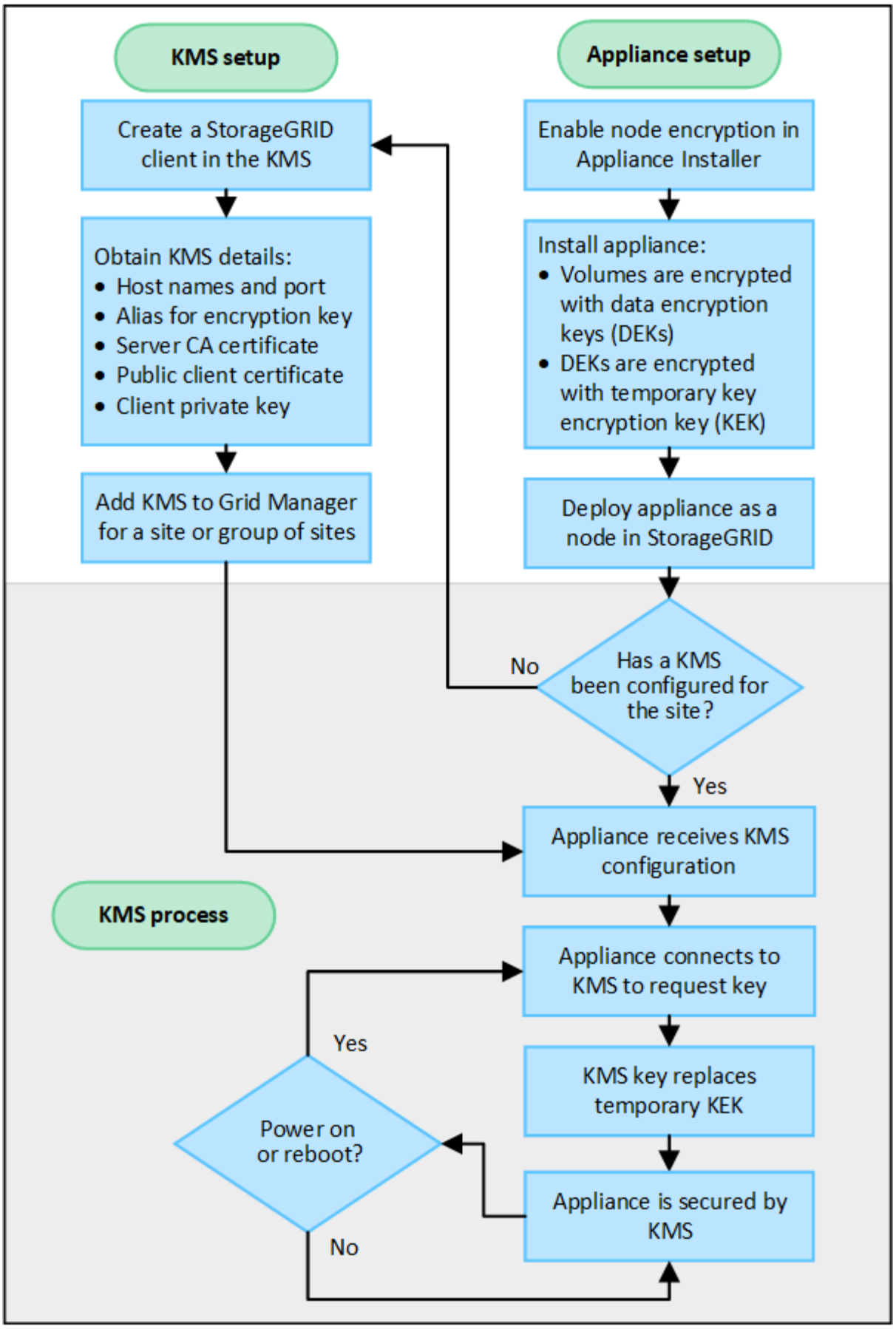
Vous pouvez utiliser un ou plusieurs serveurs de gestion de clés pour gérer les clés de chiffrement des nœuds StorageGRID dont l'option **Chiffrement des nœuds** est activée lors de l'installation. L'utilisation de serveurs de gestion de clés avec ces nœuds StorageGRID vous permet de protéger vos données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

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

## Configuration du serveur de gestion des clés et de l'appliance StorageGRID

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

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




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

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

## Configurer le serveur de gestion des clés (KMS)

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

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

## Configurez l'appareil

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

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

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

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

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

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

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

1. Lorsque vous installez dans la grille un appareil dont le chiffrement des nœuds est activé, StorageGRID détermine si une configuration KMS existe pour le site qui contient le nouveau nœud.
   - Si un KMS a déjà été configuré pour le site, l'appliance reçoit la configuration KMS.

- Si aucun KMS n'a encore été configuré pour le site, les données sur l'appliance continuent d'être chiffrées par la KEK temporaire jusqu'à ce que vous configuriez un KMS pour le site et que l'appliance reçoive la configuration KMS.

2. L'appareil utilise la configuration KMS pour se connecter au KMS et demander une clé de chiffrement.
3. Le KMS envoie une clé de chiffrement à l'appliance. La nouvelle clé provenant du KMS remplace la clé KEK temporaire et est désormais utilisée pour chiffrer et déchiffrer les clés DEK des volumes de l'appliance.

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

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

# Exigences et considérations relatives au serveur de gestion des clés StorageGRID

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

## Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

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

## Quelles sont les considérations relatives au réseau ?

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

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

## Quelles versions de TLS sont prises en charge ?

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

StorageGRID négocie le protocole et le chiffrement (TLS 1.2) ou la suite de chiffrement (TLS 1.3) avec le KMS lors de l'établissement de la connexion. Pour connaître les versions de protocole et les chiffrements/suites de chiffrement disponibles, consultez la `tlsOutbound` section de la politique TLS et SSH active de la grille (**Configuration** > **Sécurité Paramètres de sécurité**).

## Quels appareils sont pris en charge ?

Vous pouvez utiliser un serveur de gestion de clés (KMS) pour gérer les clés de chiffrement de tout appareil StorageGRID de votre grille dont l'option **Chiffrement des nœuds** est activée. Cette option ne peut être activée que lors de l'étape de configuration matérielle de l'installation de l'appareil, à l'aide de l'outil StorageGRID Appliance Installer.

> Vous ne pouvez pas activer le chiffrement du nœud après l'ajout d'un appareil à la grille, et vous ne pouvez pas utiliser la gestion externe des clés pour les appareils qui n'ont pas le chiffrement du nœud activé.

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

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

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

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

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

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

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

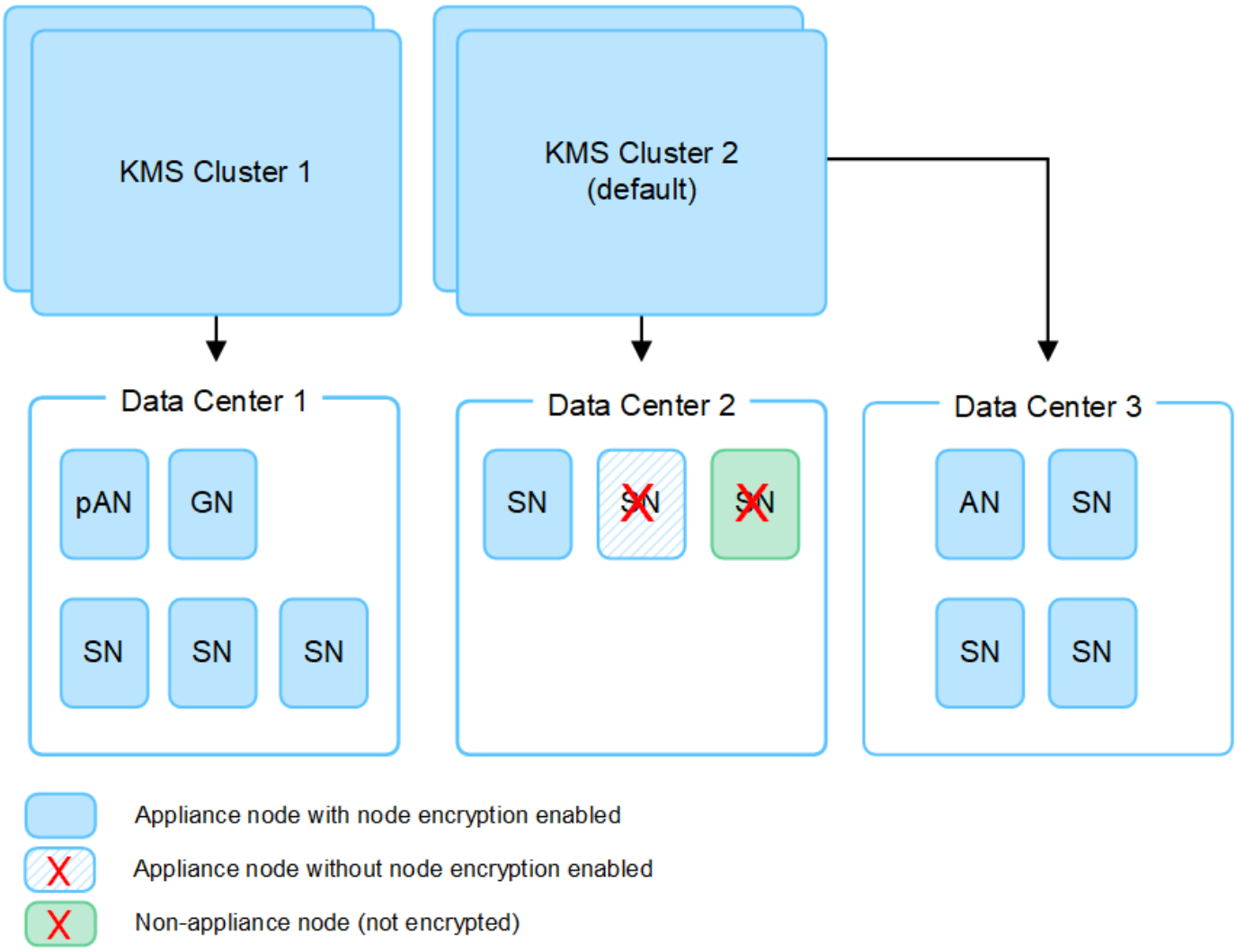
## De combien de serveurs de gestion de clés avez-vous besoin ?

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

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

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

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




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

En tant que bonne pratique de sécurité, vous devez périodiquement "faites pivoter la clé de chiffrement" utilisée par chaque KMS configuré.

Lorsque la nouvelle version de la clé sera disponible :

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

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

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

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

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

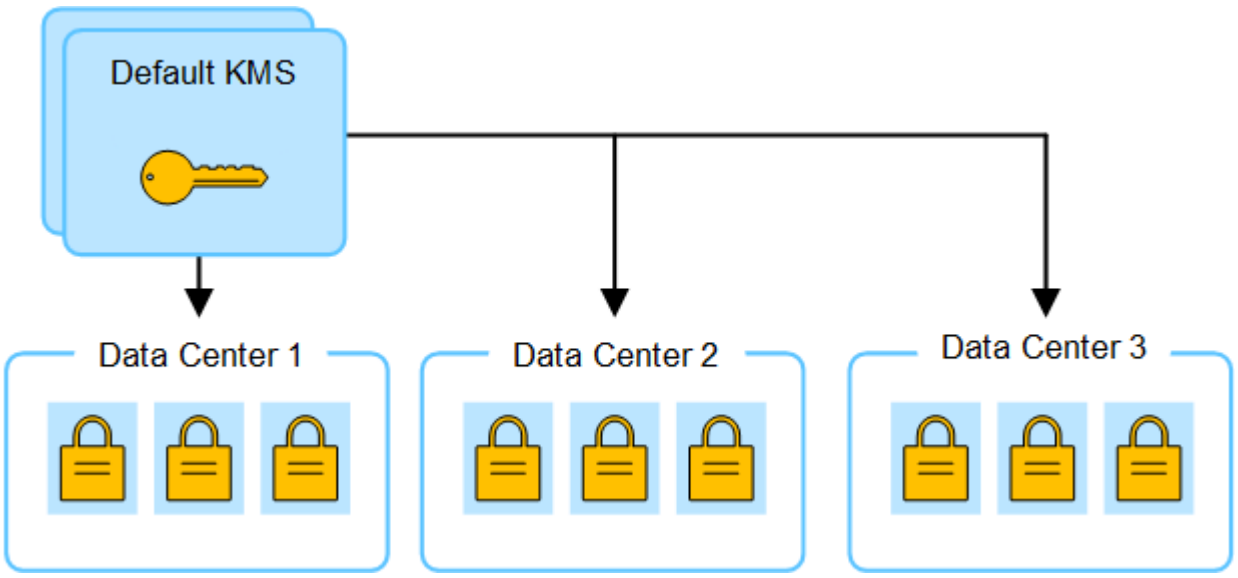
# Considérations relatives à la modification du KMS pour un site StorageGRID

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

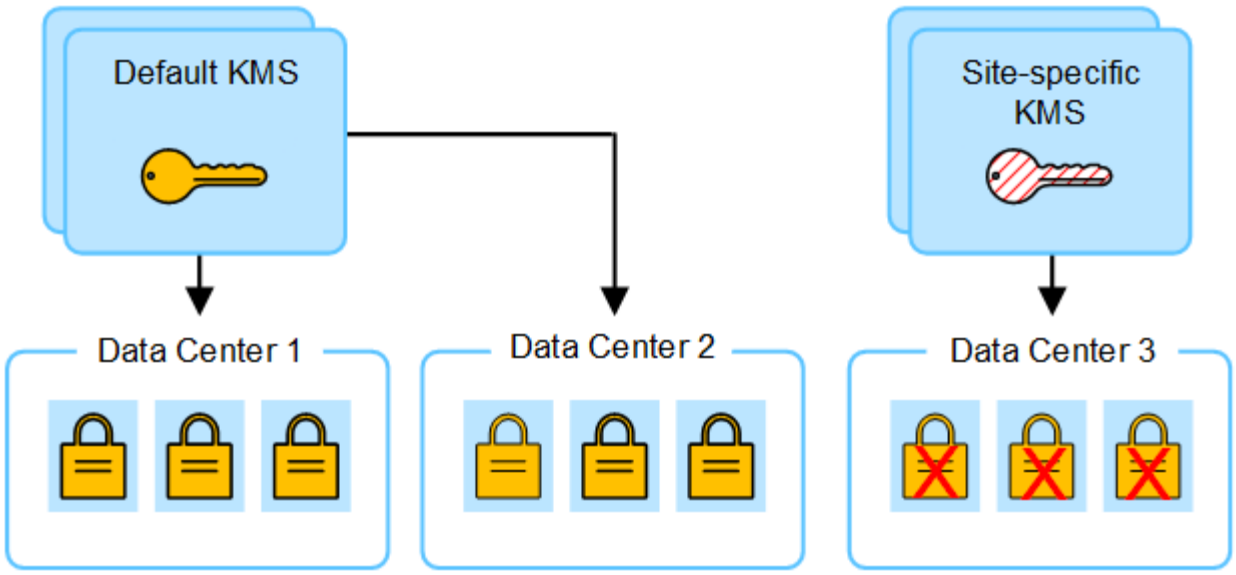
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous pourriez avoir besoin de copier la version actuelle de la clé de chiffrement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

Par exemple :

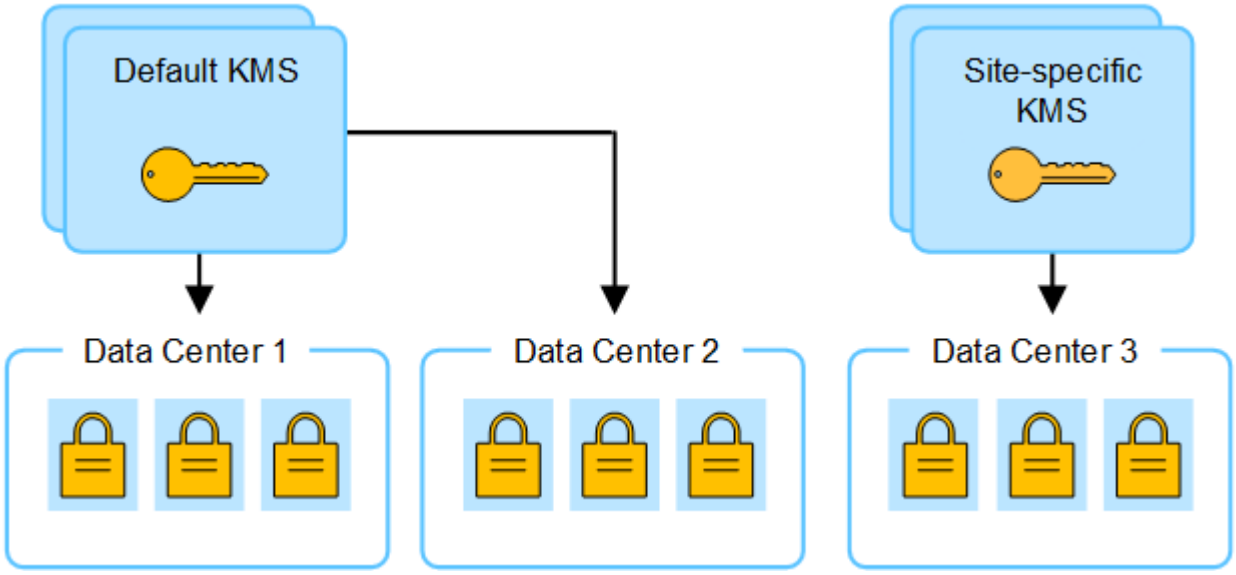
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites ne disposant pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement des nœuds** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est utilisée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




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




4. Pour résoudre ce problème, vous copiez la version actuelle de la clé de chiffrement du KMS par défaut vers le nouveau KMS. (Techniquement, vous copiez la clé d'origine vers une nouvelle clé avec le même alias. La clé d'origine devient une version antérieure de la nouvelle clé.) Le KMS spécifique au site dispose désormais de la clé correcte pour déchiffrer les nœuds de l'appliance du Data Center 3, elle peut donc être enregistrée dans StorageGRID.




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

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

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

# Configurez StorageGRID en tant que client dans le KMS

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

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

**Étapes**

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

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

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

     La clé de chiffrement doit comporter au moins 2 048 bits et être exportable.

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

"téléversement des certificats clients".

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

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

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

4. Pour chaque KMS ou cluster KMS, obtenez un certificat serveur signé par une autorité de certification (CA) ou un ensemble de certificats contenant chacun des fichiers de certificat CA encodés au format PEM, concaténés dans l'ordre de la chaîne de certificats.

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

   - Le certificat doit utiliser le format X.509 encodé en Base-64 Privacy Enhanced Mail (PEM).
   - Le champ Subject Alternative Name (SAN) de chaque certificat de serveur doit inclure le domaine complet (FQDN) ou l'adresse IP auquel StorageGRID se connectera.

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

   - Le certificat du serveur doit correspondre au certificat utilisé par l'interface KMIP du KMS, qui utilise généralement le port 5696.

5. Obtenez le certificat client public délivré à StorageGRID par le KMS externe et la clé privée du certificat client.

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

# Ajouter un serveur de gestion de clés dans StorageGRID

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

**Avant de commencer**

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

**À propos de cette tâche**

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

## Étape 1 : Détails du KMS

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

**Étapes**

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

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

2. Sélectionnez **Create**.

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

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

| Champ | Description |
|---|---|
| Nom KMS | Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères. |
| Nom de la clé | Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.<br><br>**Remarque** : Si vous n'avez pas créé de clé à l'aide de votre produit KMS, vous serez invité à demander à StorageGRID de créer la clé. |
| Gère les clés pour | Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer les serveurs de gestion de clés spécifiques à un site avant de configurer un KMS par défaut qui s'applique à tous les sites non gérés par un autre KMS.<br><br>• Sélectionnez un site si ce KMS doit gérer les clés de chiffrement des nœuds d'appliance sur un site spécifique.<br>• Sélectionnez **Sites non gérés par un autre KMS (KMS par défaut)** pour configurer un KMS par défaut qui s'appliquera à tous les sites ne disposant pas d'un KMS dédié et à tous les sites que vous ajouterez lors d'extensions ultérieures.<br><br>**Remarque :** Une erreur de validation se produira lors de l'enregistrement de la configuration KMS si vous sélectionnez un site qui était précédemment chiffré par le KMS par défaut, mais que vous n'avez pas fourni la version actuelle de la clé de chiffrement d'origine au nouveau KMS. |
| Port | Le port que le serveur KMS utilise pour les communications Key Management Interoperability Protocol (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP. |

| Champ | Description |
| --- | --- |
| Nom d'hôte | Le domaine complet ou l'adresse IP du KMS.<br><br>**Remarque :** Le champ Nom alternatif du sujet (SAN) du certificat serveur doit inclure le domaine complet (FQDN) ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ni à tous les serveurs d'un cluster KMS. |

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

## Étape 2 : Télécharger le certificat du serveur

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

**Étapes**

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

   Les métadonnées du certificat du serveur apparaissent.

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

3. Sélectionnez **Continue**.

## Étape 3 : Téléversez les certificats clients

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

**Étapes**

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

   Les métadonnées du certificat client apparaissent.

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

   Si aucune clé n'existe, vous êtes invité à laisser StorageGRID en créer une.

   Les connexions entre le serveur de gestion des clés et les nœuds de l'appliance sont testées. Si toutes les

connexions sont valides et que la clé correcte est trouvée sur le KMS, le nouveau serveur de gestion des clés est ajouté au tableau de la page Serveur de gestion des clés.

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

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

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

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

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

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

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

# Gérer un serveur de gestion de clés dans StorageGRID

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

**Avant de commencer**

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

## Afficher les détails KMS

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

**Étapes**

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

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

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

2. Pour consulter les détails d'un KMS spécifique et effectuer des opérations sur ce KMS, sélectionnez le

nom du KMS. La page de détails du KMS affiche les informations suivantes :

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

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

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

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

   Lorsque la rotation de la clé réussit, les champs Key UID et Dernière modification sont mis à jour.

Si vous faites pivoter la clé de chiffrement à l'aide du logiciel KMS, faites-la pivoter de la dernière version utilisée de la clé vers une nouvelle version de cette même clé. Ne faites pas pivoter vers une clé totalement différente.

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

## Gérer les certificats

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

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

**Étapes**

1. Sélectionnez **Configuration** > **Security** > **Key management server**.
2. Dans le tableau, consultez la valeur de l'expiration du certificat pour chaque KMS.
3. Si la date d'expiration du certificat de n'importe quel KMS est inconnue, attendez jusqu'à 30 minutes, puis actualisez votre navigateur web.
4. Si la colonne « Expiration du certificat » indique qu'un certificat a expiré ou est sur le point d'expirer, sélectionnez le KMS pour accéder à la page de détails du KMS.
   a. Sélectionnez **Certificat serveur** et vérifiez la valeur du champ « Expire le ».
   b. Pour remplacer le certificat, sélectionnez **Modifier le certificat** pour télécharger un nouveau certificat.
   c. Répétez ces sous-étapes et sélectionnez **Certificat client** au lieu de **Certificat serveur**.
5. Lorsque les alertes **KMS CA certificate expiration**, **KMS client certificate expiration** et **KMS server certificate expiration** sont déclenchées, notez la description de chaque alerte et effectuez les actions recommandées.

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

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

## Afficher les nœuds chiffrés

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

**Étapes**

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

   La page Serveur de gestion des clés s'affiche. L'onglet Détails de la configuration présente les serveurs de gestion des clés configurés.

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

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

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

| Colonne | Description |
|---|---|
| Nom du nœud | Le nom du nœud de l'appliance. |
| Type de nœud | Le type de nœud : Storage, Admin ou Gateway. |
| Site | Le nom du site StorageGRID où le nœud est installé. |
| Nom KMS | Nom descriptif du KMS utilisé pour le nœud.<br><br>Si aucun KMS n'est répertorié, sélectionnez l'onglet Détails de configuration pour ajouter un KMS.<br><br>"Ajouter un serveur de gestion de clés (KMS)" |
| UID de la clé | L'identifiant unique de la clé de chiffrement utilisée pour chiffrer et déchiffrer les données sur le nœud de l'appliance. Pour afficher l'UID complet de la clé, sélectionnez le texte.<br><br>Un tiret (--) indique que l'UID de la clé est inconnu, probablement en raison d'un problème de connexion entre le nœud de l'appliance et le KMS. |
| Statut | État de la connexion entre le KMS et le nœud de l'appliance. Si le nœud est connecté, l'horodatage est mis à jour toutes les 30 minutes. La mise à jour de l'état de la connexion peut prendre plusieurs minutes après une modification de la configuration du KMS.<br><br>**Remarque :** Actualisez votre navigateur Web pour voir les nouvelles valeurs. |

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

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

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

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

Veuillez effectuer les actions recommandées pour ces alertes.

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

## Modifier un KMS

Vous pourriez avoir besoin de modifier la configuration d'un serveur de gestion de clés, par exemple si un certificat est sur le point d'expirer.

**Avant de commencer**

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

**Étapes**

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

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

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

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

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

| Champ | Description |
| --- | --- |
| Nom KMS | Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères. |
| Nom de la clé | Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.<br><br>Vous n'avez besoin de modifier le nom de la clé que dans de rares cas. Par exemple, vous devez modifier le nom de la clé si l'alias est renommé dans le KMS ou si toutes les versions de l'ancienne clé ont été copiées dans l'historique des versions du nouvel alias. |

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

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

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

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

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

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

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

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

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

11. Si vous devez enregistrer la configuration actuelle avant de résoudre les erreurs de connexion, sélectionnez **Force save**.

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

La configuration KMS est enregistrée.

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

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

## Supprimer un serveur de gestion de clés (KMS)

Vous pourriez vouloir supprimer un serveur de gestion de clés dans certains cas. Par exemple, vous pourriez vouloir supprimer un KMS spécifique à un site si vous avez mis ce site hors service.

**Avant de commencer**

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

**À propos de cette tâche**

Vous pouvez supprimer un KMS dans les cas suivants :

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

**Étapes**

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

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

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

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

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

   La configuration KMS est supprimée.