Configurer les serveurs de gestion de clés

StorageGRID software

NetApp
December 03, 2025

Sommaire

Configurer les serveurs de gestion de clés

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

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

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

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

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

Configuration KMS et appliance

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

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

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

Configurer le serveur de gestion des clés (KMS)

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

Étape	Se référer à
Accédez au logiciel KMS et ajoutez un client pour StorageGRID à chaque KMS ou cluster KMS.	"Configurer StorageGRID en tant que client dans le KMS"

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

Installer l'appareil

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

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

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

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

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

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

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

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

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

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

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

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

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge la version 1.4 de KMIP.

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

Quelles sont les considérations relatives au réseau ?

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

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

Quelles versions de TLS sont prises en charge ?

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

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

Quels appareils sont pris en charge ?

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

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

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

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

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

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

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

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

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

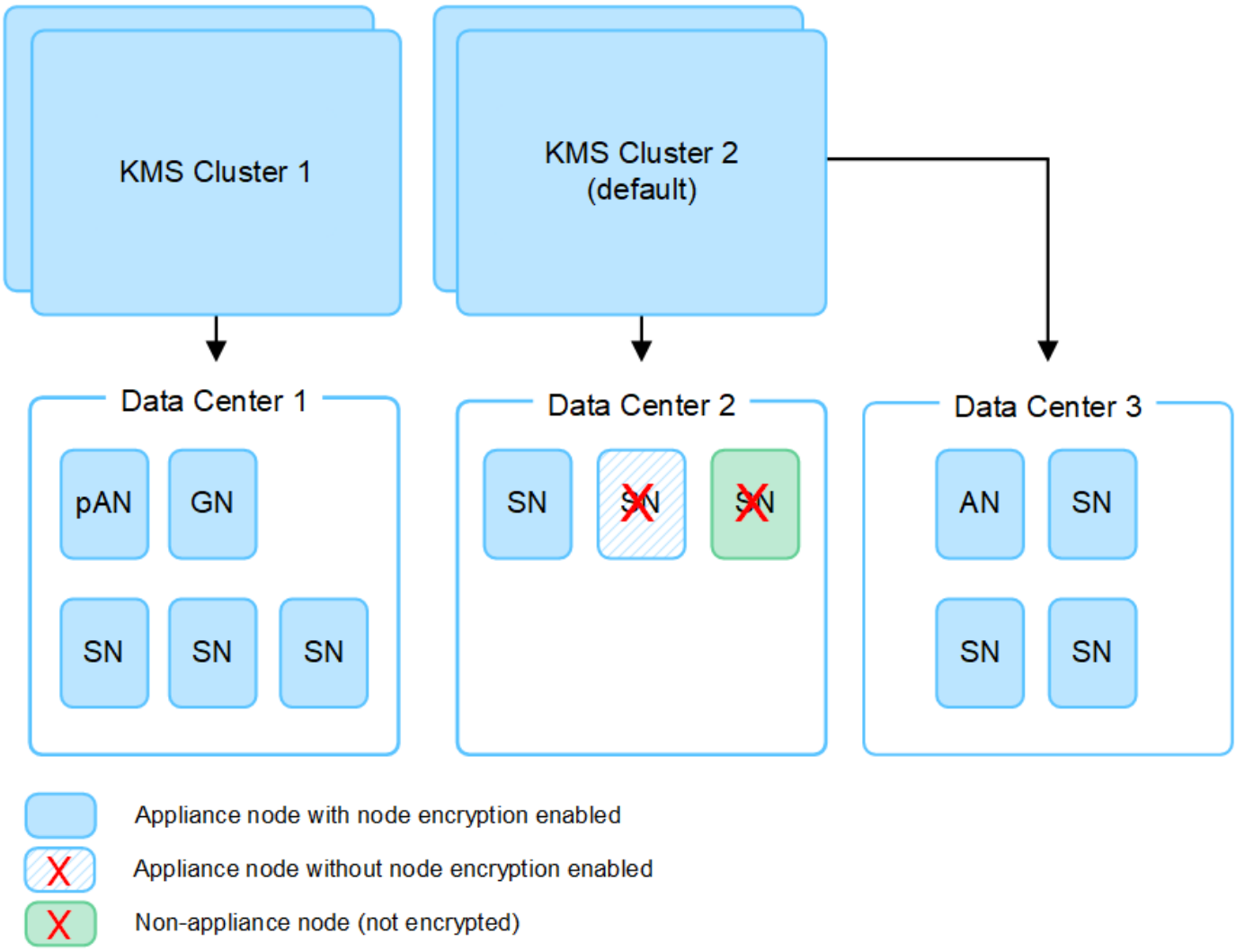
De combien de serveurs de gestion de clés ai-je besoin ?

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

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

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

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



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

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

Lorsque la nouvelle version de clé sera disponible :

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

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

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

suppression de la configuration KMS désactive le paramètre **Chiffrement de nœud** et supprime l'association entre le nœud de l'appliance et la configuration KMS pour le site StorageGRID .

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

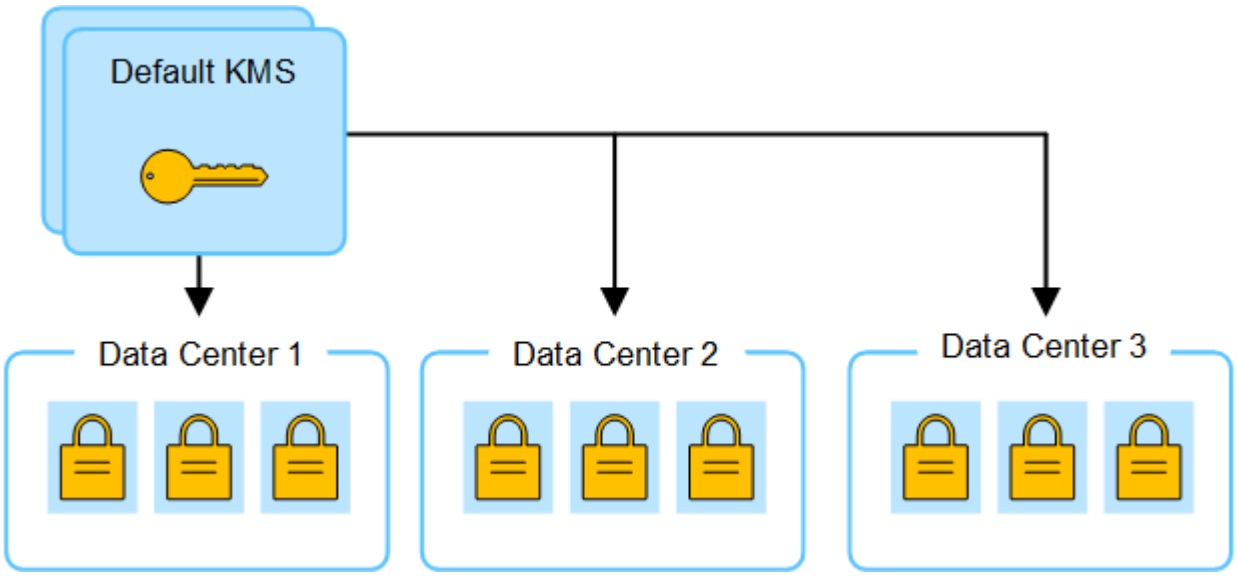
Considérations relatives à la modification du KMS d'un site

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

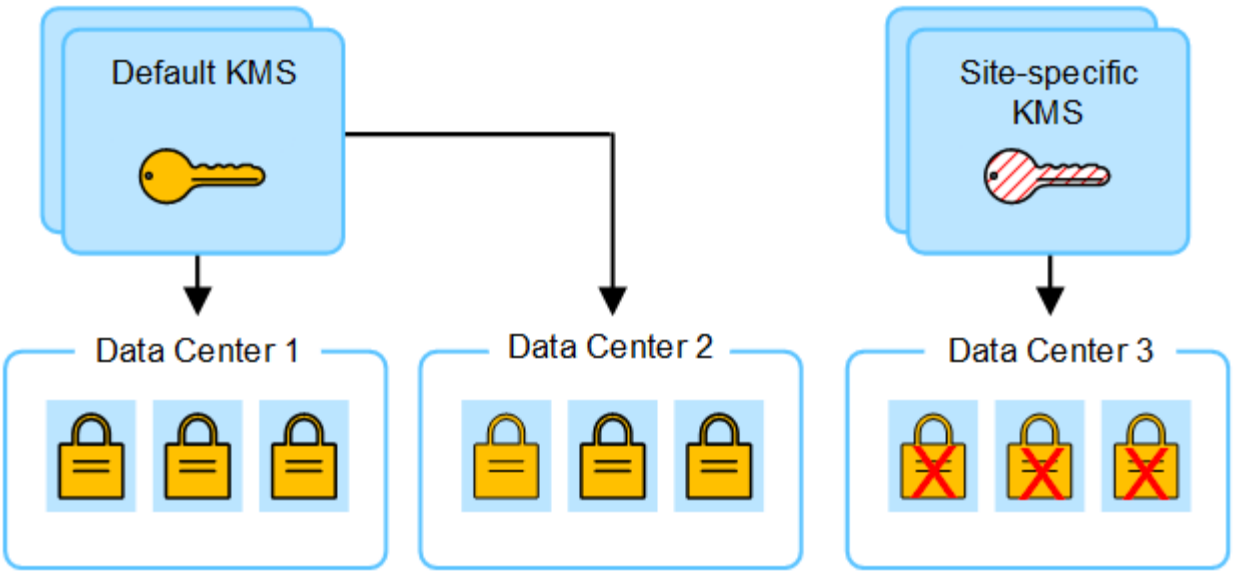
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment chiffrés sur ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement du KMS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

Par exemple:

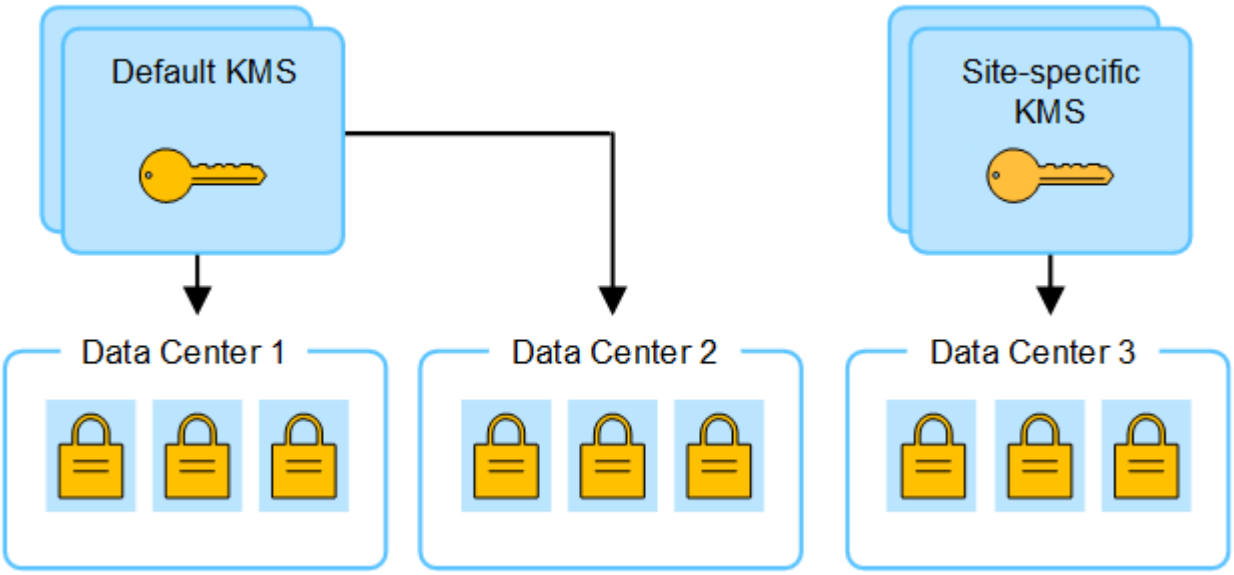
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Une fois le KMS enregistré, tous les nœuds d'appliance dont le paramètre **Chiffrement de nœud** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est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



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



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



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

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

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

Configurer StorageGRID en tant que client dans le KMS

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

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

Étapes

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

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

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

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

   - Demandez à StorageGRID de créer la clé. Vous serez invité à tester et à enregistrer

après"téléchargement de certificats clients" .

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

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

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

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

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

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

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

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

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

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

Ajouter un serveur de gestion de clés (KMS)

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

Avant de commencer

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

À propos de cette tâche

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

Étape 1 : Détails KMS

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

Étapes

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

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

2. Sélectionnez **Créer**.

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

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

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

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

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

Étape 2 : Télécharger le certificat du serveur

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

Étapes

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

   Les métadonnées du certificat du serveur apparaissent.

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

3. Sélectionnez **Continuer**.

Étape 3 : Télécharger les certificats clients

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

Étapes

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

   Les métadonnées du certificat client apparaissent.

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

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

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

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

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

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

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

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

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

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

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

Gérer un KMS

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

Avant de commencer

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

Afficher les détails du KMS

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

Étapes

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

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

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

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

du KMS. La page de détails du KMS répertorie les informations suivantes :

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

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

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

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

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

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

Gérer les certificats

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

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

Étapes

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

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

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

Afficher les nœuds chiffrés

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

Étapes

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

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

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

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

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

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

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

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

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

   - Échec du chargement de la configuration KMS
   - Erreur de connectivité KMS
   - Nom de la clé de chiffrement KMS introuvable
   - Échec de la rotation de la clé de chiffrement KMS

- La clé KMS n'a pas réussi à déchiffrer un volume d'appareil
- KMS n'est pas configuré

Effectuez les actions recommandées pour ces alertes.

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

Modifier un KMS

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

Avant de commencer

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

Étapes

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

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

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

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

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

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

Champ	Description
Gère les clés pour	Si vous modifiez un KMS spécifique à un site et que vous ne disposez pas déjà d'un KMS par défaut, sélectionnez éventuellement **Sites non gérés par un autre KMS (KMS par défaut)**. Cette sélection convertit un KMS spécifique au site en KMS par défaut, qui s'appliquera à tous les sites qui n'ont pas de KMS dédié et à tous les sites ajoutés dans une extension. **Remarque :** si vous modifiez un KMS spécifique à un site, vous ne pouvez pas sélectionner un autre site. Si vous modifiez le KMS par défaut, vous ne pouvez pas sélectionner un site spécifique.
Port	Le port utilisé par le serveur KMS pour les communications du protocole d'interopérabilité de gestion de clés (KMIP). La valeur par défaut est 5696, qui est le port standard KMIP.
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Nom alternatif du sujet (SAN) du certificat du serveur doit inclure le nom de domaine complet ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.

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

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

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

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

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

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

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

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

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

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

La configuration KMS est enregistrée.

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

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

Supprimer un serveur de gestion de clés (KMS)

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

Avant de commencer

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

À propos de cette tâche

Vous pouvez supprimer un KMS dans ces cas :

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

Étapes

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

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

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

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

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

   La configuration KMS est supprimée.

Informations sur le copyright

Informations sur les marques commerciales