Configurer les serveurs de gestion des clés

StorageGRID 11.8

NetApp
March 19, 2024

Sommaire

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.

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

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 aux données de l'appliance que si le nœud peut 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.

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 de clés externe pour les appliances pour lesquelles 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 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 LUKS (Unified Key Setup) Linux 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.

Voir "Activez le chiffrement de nœud" pour plus d'informations.

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, 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.

Quelle version de KMIP est prise en charge ?

StorageGRID prend en charge KMIP version 1.4.

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

Quelles sont les considérations relatives au réseau ?

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.

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.

Quelles sont les versions de TLS prises en charge ?

Les communications entre les nœuds d'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 des éléments pris en charge par KMS et lesquels "Règles 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 la connexion. Pour connaître les versions de protocole et les suites de chiffrement/chiffrement disponibles, consultez le `tlsOutbound` Section de la stratégie TLS et SSH active de la grille (**CONFIGURATION** > **sécurité Paramètres de sécurité**).

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.

Le chiffrement des nœuds ne peut pas être activé après l'ajout d'une appliance à la grille. De plus, vous ne pouvez pas utiliser la gestion externe des clés pour les appliances pour lesquelles le chiffrement des nœuds n'est pas activé.

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

Vous ne pouvez pas utiliser le KMS configuré pour les nœuds logiciels (non liés à l'appliance) :

- 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.

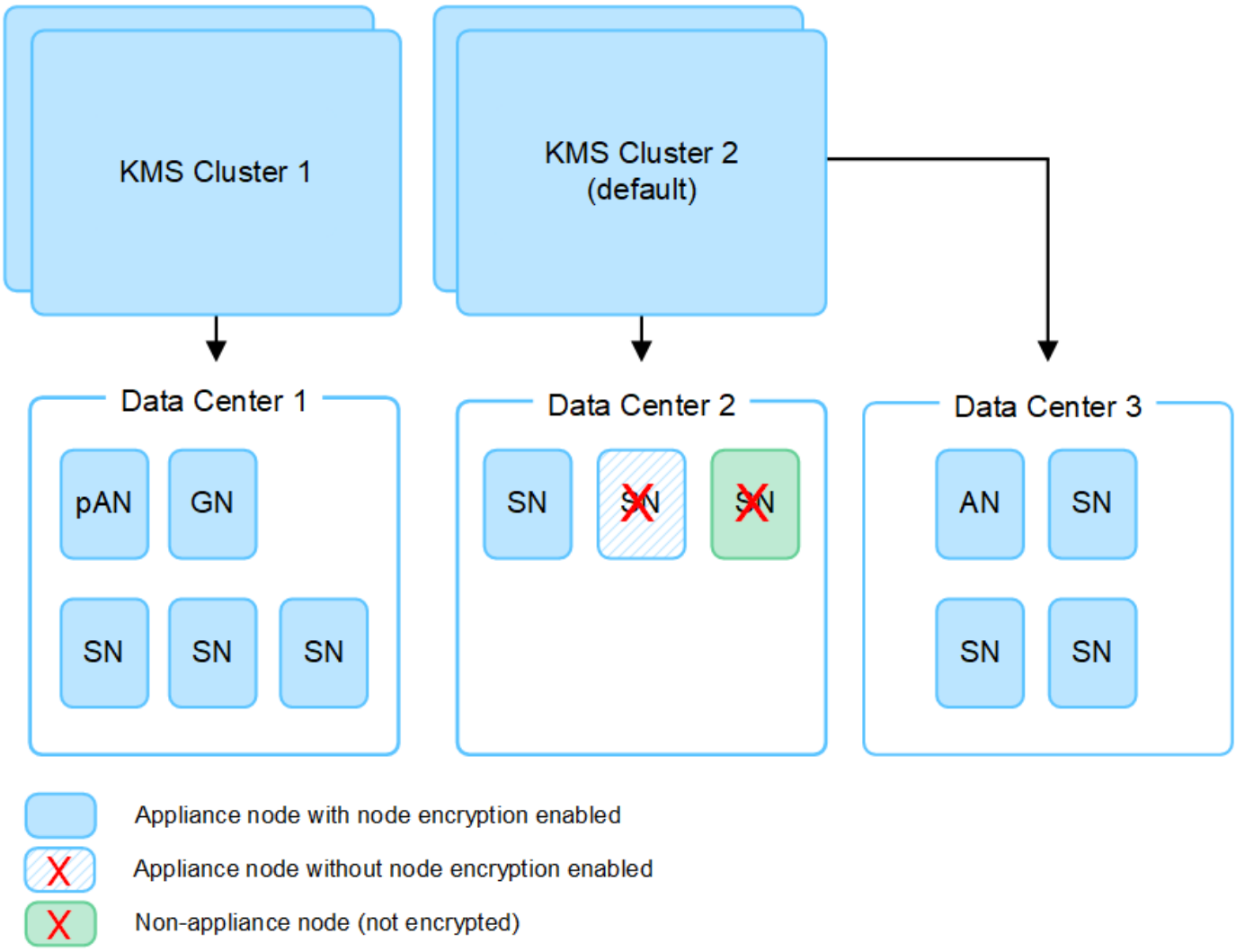
Combien de serveurs de gestion des clés ai-je besoin ?

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 liés à l'appliance ou pour les nœuds d'appliance sur lesquels 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 pratique exemplaire en matière de sécurité, vous devez régulièrement "faites pivoter la clé de cryptage" Utilisé par chaque KMS configuré.

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 clé ne peut pas être utilisée pour chiffrer les volumes de l'appliance pour une raison quelconque, l'alerte **Echec 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 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. Vous pouvez ensuite utiliser le programme d'installation de l'appliance StorageGRID pour "Effacez 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.

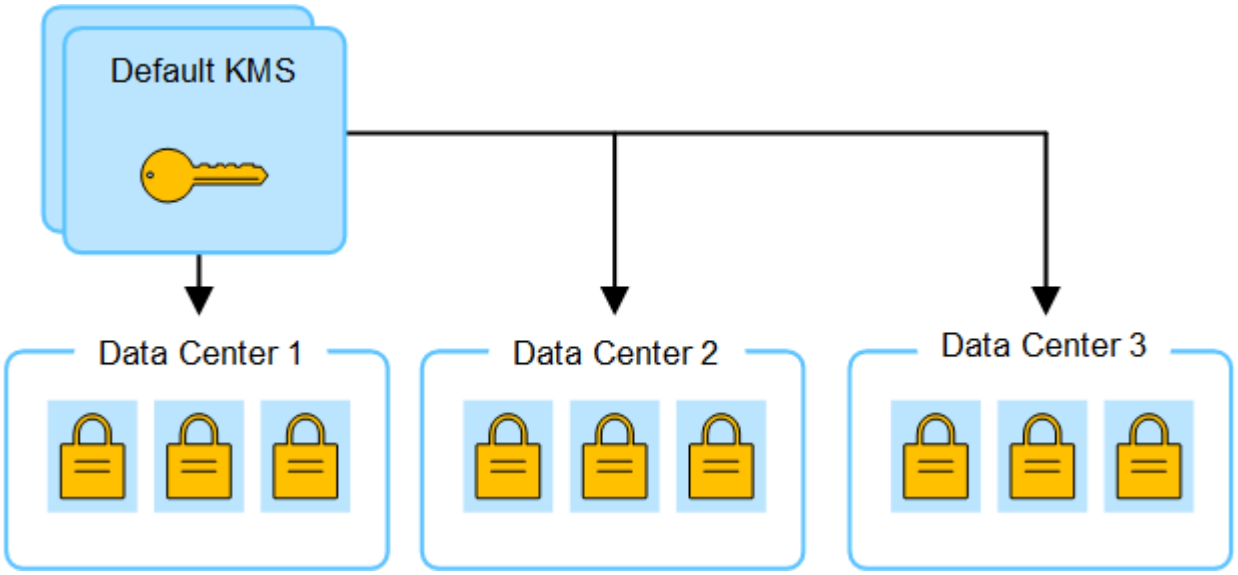
Considérations relatives à la modification du KMS pour un site

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.

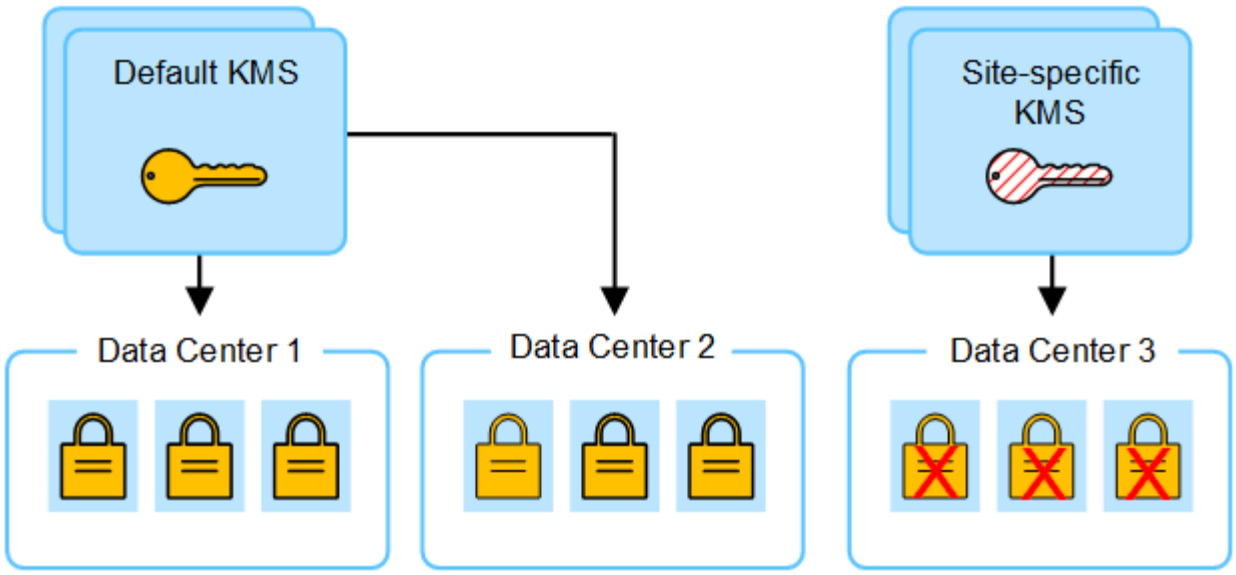
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir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

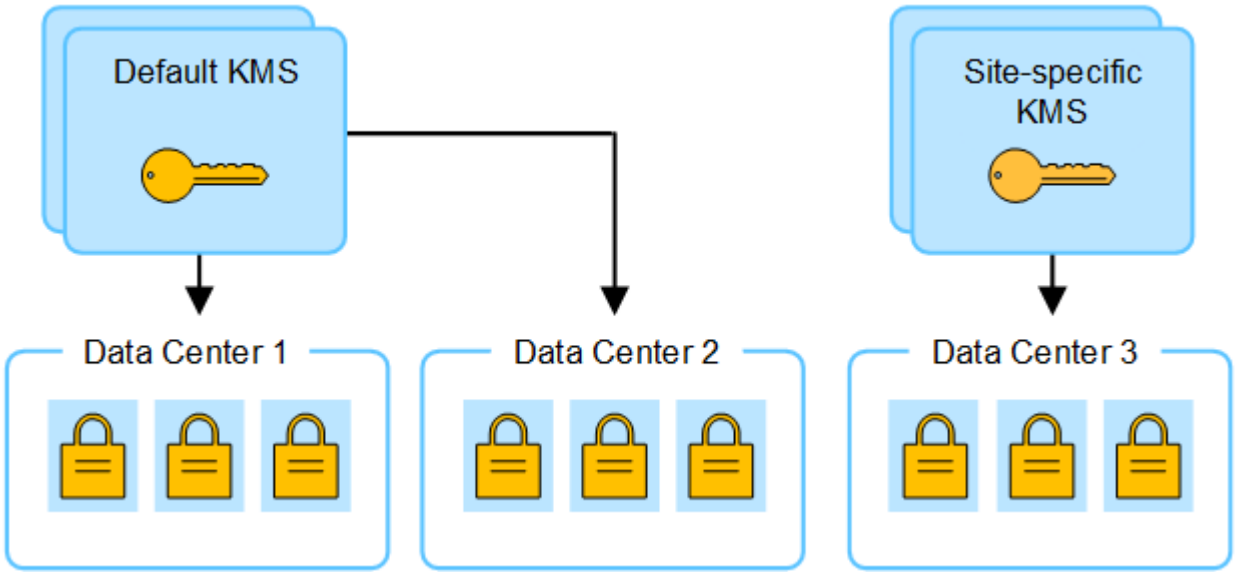
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est 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)"
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.

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

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. Créez une clé à l'aide de 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 cluster KMS ou 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 lorsque vous testez et enregistrez après

"téléchargement de certificats client".

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.

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.

Avant de commencer

- 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 avez le "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 : détails KM

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

Étapes

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

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

2. Sélectionnez **Créer**.

   L'étape 1 (détails KMS) de l'assistant Add a Key Management Server (Ajouter un serveur de gestion des 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 KM	Un nom descriptif pour vous aider à identifier ce KMS. Doit comporter entre 1 et 64 caractères.
Nom de la clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères. **Remarque** : si vous n'avez pas créé de clé à l'aide de votre produit KMS, vous serez invité à demander à StorageGRID de créer la clé.
Gère les clés pour	Le site StorageGRID qui sera associé à ce KMS. Si possible, vous devez configurer 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 n'ont pas de 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.

Champ	Description
Nom d'hôte	Le nom de domaine complet ou l'adresse IP du KMS. **Remarque :** le champ Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez 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 de serveur) de l'assistant Ajouter un serveur de gestion des 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. A partir de **Etape 2 (Télécharger le certificat de serveur)**, accédez à l'emplacement du certificat de serveur ou du paquet de certificats enregistré.
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 **Continuer**.

Étape 3 : téléchargement des certificats client

À l'étape 3 (Téléchargement de certificats client) de l'assistant Ajouter 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. A partir de **Etape 3 (Téléchargement de certificats client)**, naviguez jusqu'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.
5. Sélectionnez **Tester et enregistrer**.

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

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 s'affiche lorsque vous sélectionnez **Test and save**, 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**.

   > La sélection de **forcer l'enregistrement** enregistre la configuration KMS, mais elle ne teste pas la connexion externe de chaque appliance à 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.

Gérer un KMS

La gestion d'un serveur de gestion des 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 des clés (KMS) de votre système StorageGRID, y compris les détails des clés et l'état actuel des certificats du serveur et du client.

Étapes

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

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

   - L'onglet Détails de la configuration répertorie tous les serveurs de gestion des clés configurés.

◦ L'onglet nœuds cryptés répertorie tous les nœuds sur 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	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'une grappe, 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	Alias de clé pour le client StorageGRID dans le KMS.
UID de clé	Identifiant unique de la dernière version de la clé.	Dernière modification
Date et heure de la dernière version de la clé.	Certificat de serveur	Les métadonnées
Métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.	Certificat PEM	Contenu du fichier PEM (Privacy Enhanced mail) du certificat.
Certificat client	Les métadonnées	Métadonnées du certificat, telles que le numéro de série, la date et l'heure d'expiration et le PEM du certificat.

4. [[clé de rotation]]aussi souvent que requis par les pratiques de sécurité de votre organisation, sélectionnez

clé de rotation, ou utilisez le logiciel KMS, pour créer une nouvelle version de la clé.

Lorsque la rotation de la clé a réussi, 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 complètement différente.

Ne tentez jamais de faire pivoter une clé en modifiant le nom de clé (alias) du 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.

Gérer les certificats

Répondez rapidement à tous les problèmes de certificat de serveur ou de client. Si possible, remplacez les certificats avant qu'ils n'expirent.

Vous devez corriger 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, examinez 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 qu'il est sur le point d'expirer, sélectionnez KMS pour accéder à la page de détails 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 du 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 30 minutes pour obtenir les mises à jour de l'expiration du certificat. Actualisez votre navigateur Web pour afficher les valeurs actuelles.

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 **encrypted nodes**.

   L'onglet noeuds cryptés répertorie les noeuds de l'appliance de votre système StorageGRID sur lesquels le paramètre **chiffrement de noeud** 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 KM	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 un UID de clé entier, sélectionnez le texte. 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 :** Rafraîchir 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

Effectuez les actions recommandées pour ces alertes.

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

Modifier un 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.

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 pour un site".
- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez le "Autorisation d'accès racine".

Étapes

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

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

2. Sélectionnez le KMS à modifier, puis sélectionnez **actions** > **Modifier**.

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

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

Champ	Description
Nom KM	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. 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.

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 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 Subject alternative Name (SAN) du certificat de serveur doit inclure le nom de domaine complet ou l'adresse IP que vous entrez 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 de serveur) de l'assistant Modifier un serveur de gestion des clés s'affiche.

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

   L'étape 3 (Téléchargement de certificats client) de l'assistant Modifier un serveur de gestion des 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'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**.

La sélection de **forcer l'enregistrement** enregistre la configuration KMS, mais elle ne teste pas la connexion externe de chaque appliance à 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.

Avant de commencer

- 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 avez le "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 serveur de gestion des clés s'affiche et affiche tous les serveurs de gestion des clés qui ont été configurés.

2. Sélectionnez le KMS à supprimer, puis sélectionnez **actions** > **Supprimer**.

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

3. Vérifiez que ce qui suit est vrai :
   - Vous supprimez un KMS spécifique au site pour un site qui n'a aucun nœud d'appliance pour lequel le chiffrement des nœuds est activé.
   - Vous supprimez le KMS par défaut, mais un KMS spécifique au site existe déjà pour chaque site avec chiffrement des nœuds.
4. Sélectionnez **Oui**.

La configuration KMS est supprimée.