



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

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

- Ajout d'un serveur de gestion des clés (KMS) 1
 - Étape 1 : saisissez les détails du KMS 1
 - Étape 2 : télécharger le certificat du serveur 4
 - Étape 3 : télécharger des certificats client 5

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

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

Ce dont vous avez besoin

- Vous devez avoir consulté le ["considérations et conditions requises pour l'utilisation d'un serveur de gestion des clés"](#).
- Vous devez avoir ["Configuration de StorageGRID en tant que client dans le KMS"](#), Et vous devez disposer des informations requises pour chaque cluster KMS ou KMS
- Vous devez disposer de l'autorisation accès racine.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

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.

["Considérations relatives à la modification du KMS pour un site"](#)

Étapes

1. ["Étape 1 : saisissez les détails du KMS"](#)
2. ["Étape 2 : télécharger le certificat du serveur"](#)
3. ["Étape 3 : télécharger des certificats client"](#)

Étape 1 : saisissez les détails du KMS

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

Étapes

1. Sélectionnez **Configuration > Paramètres système > serveur de gestion des clés**.

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

Key Management Server

If your StorageGRID system includes appliance nodes with node encryption enabled, you can use an external key management server (KMS) to manage the encryption keys that protect your StorageGRID at rest.

Configuration Details

Encrypted Nodes

You can configure more than one KMS (or KMS cluster) to manage the encryption keys for appliance nodes. For example, you can configure one default KMS to manage the keys for all appliance nodes within a group of sites and a second KMS to manage the keys for the appliance nodes at a particular site.

Before adding a KMS:

- Ensure that the KMS is KMIP-compliant.
- Configure StorageGRID as a client in the KMS.
- Enable node encryption for each appliance during appliance installation. You cannot enable node encryption after an appliance is added to the grid and you cannot use a KMS for appliances that do not have node encryption enabled.

For complete instructions, see [administering StorageGRID](#).

+ Create Edit Remove

KMS Display Name ?

Key Name ?

Manages keys for ?

Hostname ?

Certificate Status ?

No key management servers have been configured. Select **Create**.

2. Sélectionnez **Créer**.

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

Add a Key Management Server



Enter information about the external key management server (KMS) and the StorageGRID client you configured in that KMS. If you are configuring a KMS cluster, select + to add a hostname for each server in the cluster.

KMS Display Name ?	<input type="text"/>
Key Name ?	<input type="text"/>
Manages keys for ?	-- Choose One -- ▾
Port ?	<input type="text" value="5696"/>
Hostname ?	<input type="text"/>

+


Cancel

Next

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

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

Champ	Description
Nom de clé	Alias de clé exact pour le client StorageGRID dans le KMS. Doit comporter entre 1 et 255 caractères.
Gère les clés pour	<p>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.</p> <ul style="list-style-type: none"> • Sélectionnez un site si ce KMS gère les clés de chiffrement pour les nœuds d'appliance sur un site spécifique. • Sélectionnez sites non gérés par un autre KMS (KMS par défaut) pour configurer un KMS par défaut qui s'appliquera à tous les sites qui ne disposent pas d'un KMS dédié et à tous les sites que vous ajoutez dans les extensions suivantes. <p>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.</p>
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	<p>Le nom de domaine complet ou l'adresse IP du KMS.</p> <p>Remarque : le champ SAN du certificat de serveur doit inclure le FQDN ou l'adresse IP que vous saisissez ici. Dans le cas contraire, StorageGRID ne pourra pas se connecter au KMS ou à tous les serveurs d'un cluster KMS.</p>

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

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

Étape 2 : télécharger le certificat du serveur

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

Étapes

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

Add a Key Management Server

1

2

3

Enter KMS
Details

Upload
Server
Certificate

Upload Client
Certificates

Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate ⓘ

Cancel

Back

Next


2. Téléchargez le fichier de certificat.

Les métadonnées du certificat de serveur s'affichent.

Add a Key Management Server



Upload a server certificate signed by the certificate authority (CA) on the external key management server (KMS) or a certificate bundle. The server certificate allows the KMS to authenticate itself to StorageGRID.

Server Certificate  k170vCA.pem

Server Certificate Metadata

Server DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Serial Number: 71:CD:6D:72:53:B5:6D:0A:8C:69:13:0D:4D:D7:81:0E
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T21:12:45.000Z
Expires On: 2030-10-13T21:12:45.000Z
SHA-1 Fingerprint: EE:E4:6E:17:86:DF:56:B4:F5:AF:A2:3C:BD:56:6B:10:DB:B2:5A:79

Cancel

Back

Next



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

3. Sélectionnez **Suivant**.

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

Étape 3 : télécharger des certificats client

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

Étapes

1. À partir de **Etape 3 (Téléchargement de certificats client)**, accédez à l'emplacement du certificat client.

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

Client Certificate Private Key ?

Browse

Cancel

Back

Save

2. Téléchargez le fichier de certificat client.

Les métadonnées du certificat client s'affichent.

3. Accédez à l'emplacement de la clé privée pour le certificat client.

4. Téléchargez le fichier de clé privée.

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

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Cancel

Back

Save

5. Sélectionnez **Enregistrer**.

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



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

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

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

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

Add a Key Management Server



Upload the client certificate and the client certificate private key. The client certificate is issued to StorageGRID by the external key management server (KMS), and it allows StorageGRID to authenticate itself to the KMS.

Client Certificate ?

Browse

k170vClientCert.pem

Server DN: /CN=admin/UID=
Serial Number: 7D:5A:8A:27:02:40:C8:F5:19:A1:28:22:E7:D6:E2:EB
Issue DN: /C=US/ST=MD/L=Belcamp/O=Gemalto/CN=KeySecure Root CA
Issued On: 2020-10-15T23:31:49.000Z
Expires On: 2022-10-15T23:31:49.000Z
SHA-1 Fingerprint: A7:10:AC:39:85:42:80:8F:FF:62:AD:A1:BD:CF:4C:90:F3:E9:36:69

Client Certificate Private Key ?

Browse

k170vClientKey.pem

Select **Force Save** to save this KMS without testing the external connections. If there is an issue with the configuration, you might not be able to reboot any FDE-enabled appliance nodes at the affected site, and you might lose access to your data.

Cancel

Back

Force Save

Save



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

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

Warning

Confirm force-saving the KMS configuration

Are you sure you want to save this KMS without testing the external connections?

If there is an issue with the configuration, you might not be able to reboot any appliance nodes with node encryption enabled at the affected site, and you might lose access to your data.

Cancel

OK

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

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.