Gérer la sécurité

StorageGRID 11.8

NetApp
March 19, 2024

Sommaire

Gérer la sécurité

Gérer la sécurité : présentation

Vous pouvez configurer différents paramètres de sécurité à partir du Gestionnaire de grille pour sécuriser votre système StorageGRID.

Gestion du chiffrement

StorageGRID propose plusieurs options pour le chiffrement des données. Vous devriez "consultez les méthodes de cryptage disponibles" afin d'identifier celles qui répondent à vos exigences en matière de protection des données.

Gérer les certificats

C'est possible "configurer et gérer les certificats de serveur" Utilisé pour les connexions HTTP ou les certificats client utilisés pour authentifier l'identité d'un client ou d'un utilisateur sur le serveur.

Configurer les serveurs de gestion des clés

À l'aide d'un "serveur de gestion des clés" Vous permet de protéger vos données StorageGRID même si une appliance est retirée 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.

> Pour utiliser la gestion des clés de chiffrement, vous devez activer le paramètre **Node Encryption** pour chaque appliance au cours de l'installation, avant d'ajouter l'appliance à la grille.

Gérer les paramètres proxy

Si vous utilisez les services de plateforme S3 ou les pools de stockage cloud, vous pouvez configurer un "serveur proxy de stockage" Entre les nœuds de stockage et les terminaux S3 externes. Si vous envoyez des packages AutoSupport via HTTPS ou HTTP, vous pouvez configurer un "serveur proxy d'administration" Entre les nœuds d'administration et le support technique.

Contrôle des pare-feu

Pour améliorer la sécurité de votre système, vous pouvez contrôler l'accès aux nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques sur le "pare-feu externe". Vous pouvez également contrôler l'accès réseau à chaque nœud en configurant son "pare-feu interne". Vous pouvez empêcher l'accès à tous les ports, à l'exception de ceux nécessaires à votre déploiement.

Étudiez les méthodes de cryptage StorageGRID

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

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

Option de chiffrement	Comment cela fonctionne	S'applique à
Serveur de gestion des clés (KMS) dans Grid Manager	Vous "configurer un serveur de gestion des clés" Pour le site StorageGRID et "activez le chiffrement des nœuds pour l'appliance". Ensuite, un nœud d'appliance se connecte au KMS pour demander une clé de chiffrement (KEK). Cette clé chiffre et décrypte la clé de chiffrement des données (DEK) sur chaque volume.	Nœuds d'appliance sur lesquels **Node Encryption** est activé pendant l'installation. Toutes les données de l'appliance sont protégées contre les pertes ou les suppressions physiques du data Center. **Remarque** : la gestion des clés de chiffrement avec un KMS n'est prise en charge que pour les nœuds de stockage et les appliances de services.
Page chiffrement de lecteur dans le programme d'installation de l'appliance StorageGRID	Si l'appliance contient des disques qui prennent en charge le chiffrement matériel, vous pouvez définir une phrase secrète de lecteur lors de l'installation. Lorsque vous définissez une phrase de passe pour un disque, il est impossible à quiconque de récupérer des données valides sur les disques qui ont été supprimés du système, sauf s'il connaît la phrase de passe. Avant de commencer l'installation, accédez à **Configure Hardware** > **Drive Encryption** pour définir une phrase de passe de lecteur qui s'applique à tous les disques à chiffrement automatique gérés par StorageGRID d'un nœud.	Les appliances contiennent des disques à chiffrement automatique. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Le chiffrement de disque ne s'applique pas aux disques gérés par SANtricity. Si vous disposez d'une appliance de stockage avec disques à chiffrement automatique et contrôleurs SANtricity, vous pouvez activer la sécurité des disques dans SANtricity.
Sécurité des disques dans SANtricity System Manager	Si la fonctionnalité Drive Security est activée pour une appliance de stockage SG5700 ou SG6000, vous pouvez utiliser "SANtricity System Manager" pour créer et gérer la clé de sécurité. La clé est requise pour accéder aux données sur les disques sécurisés.	Dispositifs de stockage équipés de disques Full Disk Encryption (FDE) ou de disques à autocryptage. Toutes les données des disques sécurisés sont protégées contre les pertes ou suppressions physiques du data Center. Utilisation avec certaines appliances de stockage ou avec des appliances de services impossible.

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement des objets stockés	Vous activez le "Chiffrement des objets stockés" Dans le Gestionnaire de grille. Lorsqu'il est activé, tout nouvel objet non chiffré au niveau du compartiment ou de l'objet est chiffré lors de l'ingestion.	Ingestion récente des données d'objet S3 et Swift. Les objets stockés existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées.
Chiffrement de compartiment S3	Vous lancez une demande PutBucketEncryption pour activer le cryptage du compartiment. Tout nouvel objet non chiffré au niveau de l'objet est chiffré lors de l'ingestion.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour le compartiment. Les objets de compartiment existants ne sont pas chiffrés. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. "Opérations sur les compartiments"
Chiffrement côté serveur d'objets S3 (SSE)	Vous émettez une demande S3 pour stocker un objet et inclure le `x-amz-server-side-encryption` en-tête de demande.	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. StorageGRID gère les clés. "Utilisez le cryptage côté serveur"
Chiffrement côté serveur objet S3 avec clés fournies par le client (SSE-C)	Vous émettez une demande S3 pour stocker un objet et incluez trois en-têtes de requête. • `x-amz-server-side-encryption-customer-algorithm` • `x-amz-server-side-encryption-customer-key` • `x-amz-server-side-encryption-customer-key-MD5`	Données d'objet S3 récemment ingérées uniquement. Le chiffrement doit être spécifié pour l'objet. Les métadonnées d'objet et les autres données sensibles ne sont pas chiffrées. Les clés sont gérées en dehors du StorageGRID. "Utilisez le cryptage côté serveur"

Option de chiffrement	Comment cela fonctionne	S'applique à
Chiffrement de volume ou de datastore externe	Vous utilisez une méthode de chiffrement autres que StorageGRID pour chiffrer un volume ou un datastore entier, si votre plateforme de déploiement le prend en charge.	Toutes les données d'objet, de métadonnées et de configuration du système, en supposant que chaque volume ou datastore est chiffré. Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées.
Chiffrement d'objet en dehors de StorageGRID	Vous utilisez une méthode de chiffrement à l'extérieur de StorageGRID pour chiffrer les données d'objet et les métadonnées avant leur ingestion dans StorageGRID.	Données et métadonnées d'objet uniquement (les données de configuration du système ne sont pas chiffrées). Une méthode de chiffrement externe permet un contrôle plus précis des clés et des algorithmes de chiffrement. Peut être combiné avec les autres méthodes répertoriées. "Amazon simple Storage Service - Guide des développeurs : protection des données à l'aide du chiffrement côté client"

Utilisez plusieurs méthodes de chiffrement

Selon vos besoins, vous pouvez utiliser plusieurs méthodes de chiffrement à la fois. Par exemple :

- Vous pouvez utiliser un KMS pour protéger les nœuds de l'appliance et utiliser la fonctionnalité de sécurité des disques de SANtricity System Manager pour « double chiffrement » des données sur les disques à chiffrement automatique des mêmes appliances.
- Vous pouvez utiliser un KMS pour sécuriser les données des nœuds de l'appliance et utiliser l'option de chiffrement des objets stockés pour chiffrer tous les objets lors de leur ingestion.

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

Gérer les certificats

Gérer les certificats de sécurité : présentation

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des

connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

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

Lorsqu'un client se connecte au serveur via HTTPS, le serveur répond avec le certificat du serveur, qui contient une clé publique. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client démarre une session avec le serveur en utilisant la même clé publique.

StorageGRID fonctionne comme serveur pour certaines connexions (par exemple, le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (par exemple, le service de réplication CloudMirror).

Certificat CA grille par défaut

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

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

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

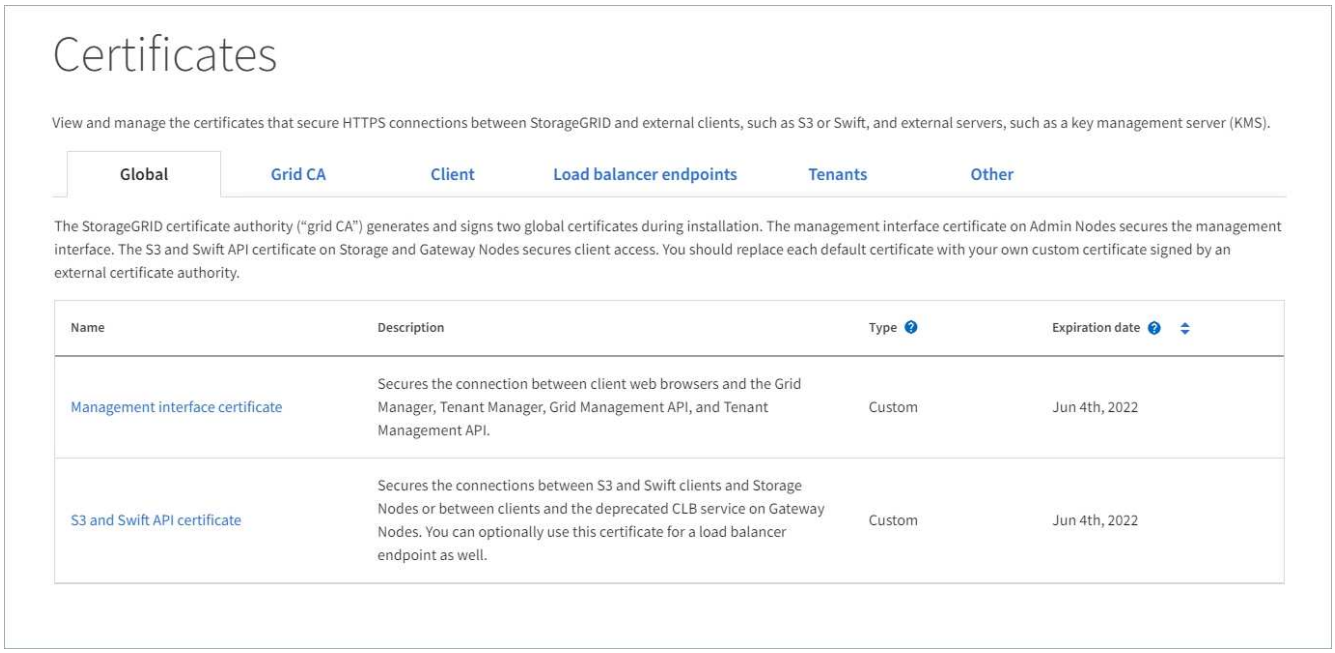
Les variantes du serveur et des types de certificats client sont mises en œuvre de plusieurs façons. Avant de configurer le système, tous les certificats nécessaires à votre configuration StorageGRID spécifique doivent être prêts.

Accéder aux certificats de sécurité

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

Étapes

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



2. Sélectionnez un onglet sur la page certificats pour obtenir des informations sur chaque catégorie de certificat et pour accéder aux paramètres du certificat. Vous pouvez accéder à un onglet si vous avez le "autorisation appropriée".

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

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

Mondial

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

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

Les informations sur les certificats globaux installés comprennent :

- **Nom** : nom du certificat avec lien vers la gestion du certificat.
- **Description**
- **Type** : personnalisé ou par défaut.
  Vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité de la grille.
- **Date d'expiration** : si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Vous pouvez :

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
  - "Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID" Utilisé pour les connexions Grid Manager et tenant Manager.
  - "Remplacez le certificat API S3 et Swift" Utilisé pour les connexions de nœuds de stockage et de terminaux d'équilibrage de la charge (en option).
- "Restaurez le certificat de l'interface de gestion par défaut."
- "Restaurez le certificat API S3 et Swift par défaut."
- "Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé."
- Copiez ou téléchargez le "certificat de l'interface de gestion" ou "Certificat API S3 et Swift".

CA grille

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

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

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

Client

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

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

Vous pouvez :

- "Téléchargez ou générez un nouveau certificat client."
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
  - "Modifiez le nom du certificat client."
  - "Définissez l'autorisation d'accès Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimez le certificat client."
- Sélectionnez **actions** pour accélérer "modifier", "attacher", ou "déposer" un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats client et les supprimer en une seule fois en utilisant **actions** > **Supprimer**.

Terminaux d'équilibrage de charge

Certificats de noeud final de l'équilibreur de charge Sécurisez les connexions entre les clients S3 et Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

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

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

Vous pouvez :

- "Afficher un point d'extrémité d'équilibreur de charge", y compris les détails de son certificat.
- "Spécifiez un certificat de noeud final de l'équilibreur de charge pour FabricPool."
- "Utilisez le certificat global d'API S3 et Swift" au lieu de générer un nouveau certificat de terminal de l'équilibreur de charge.

Locataires

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

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

Vous pouvez :

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

Autre

StorageGRID utilise d'autres certificats de sécurité pour des fins spécifiques. Ces certificats sont

répertoriés par leur nom fonctionnel. Voici d'autres certificats de sécurité :

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

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

> Vous ne pouvez afficher et accéder aux informations relatives aux autres certificats que si vous possédez le "autorisation appropriée".

Vous pouvez :

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

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions d'implémentation.

Certificat de l'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web client et l'interface de gestion StorageGRID, permettant aux utilisateurs d'accéder à Grid Manager et au gestionnaire de locataires sans avertissement de sécurité. Ce certificat authentifie également les connexions de l'API de gestion du grid et de l'API de gestion des locataires. Vous pouvez utiliser le certificat par défaut créé lors de l'installation ou télécharger un certificat personnalisé.	**CONFIGURATION** > **sécurité** > **certificats**, sélectionnez l'onglet **Global**, puis **certificat d'interface de gestion**	"Configurer les certificats d'interface de gestion"

Certificat API S3 et Swift

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 ou Swift sécurisées auprès d'un nœud de stockage et les terminaux d'équilibrage de la charge (facultatif).	**CONFIGURATION** > **sécurité** > **certificats**, sélectionnez l'onglet **Global**, puis **S3 et Swift API certificates**	"Configurez les certificats API S3 et Swift"

Certificat CA de la grille

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

Certificat du client administrateur

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

Certificat de terminal de l'équilibreur de charge

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

Certificat de terminal Cloud Storage Pool

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

Certificat de notification d'alerte par e-mail

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte. • Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.	**ALERTES** > **Configuration de la messagerie**	"Configurez les notifications par e-mail pour les alertes"

Certificat de serveur syslog externe

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion TLS ou RELP/TLS entre un serveur syslog externe qui consigne les événements dans StorageGRID. **Remarque :** un certificat de serveur syslog externe n'est pas requis pour les connexions TCP, RELP/TCP et UDP à un serveur syslog externe.	**CONFIGURATION** > **surveillance** > **serveur d'audit et syslog**	"Utiliser un serveur syslog externe"

certificat de connexion de fédération de grille

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifier et crypter les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grille.	**CONFIGURATION** > **système** > **fédération de grille**	• "Créer des connexions de fédération de grille" • "Faire pivoter les certificats de connexion"

Certificat de fédération des identités

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre StorageGRID et un fournisseur d'identité externe, tel qu'Active Directory, OpenLDAP ou Oracle Directory Server. Utilisé pour la fédération des identités, ce qui permet de gérer les groupes et les utilisateurs d'administration par un système externe.	**CONFIGURATION** > **contrôle d'accès** > **fédération d'identités**	"Utiliser la fédération des identités"

Certificat de serveur de gestion des clés (KMS)

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

Certificat de terminal des services de plate-forme

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

Certificat SSO (Single Sign-on)

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

Exemples de certificats

Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un noeud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.
4. StorageGRID répond avec le certificat du serveur, qui contient une clé publique, et une signature basée

sur la clé privée.

5. Le client vérifie ce certificat en comparant la signature du serveur à la signature figurant sur sa copie du certificat. Si les signatures correspondent, le client lance une session à l'aide de la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

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

Dans cet exemple, StorageGRID agit comme client.

1. À l'aide du logiciel serveur de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par l'autorité de certification, un certificat de client public et la clé privée pour le certificat client.
2. À l'aide de Grid Manager, vous configurez un serveur KMS et téléchargez les certificats du serveur et du client ainsi que la clé privée du client.
3. Lorsqu'un nœud StorageGRID a besoin d'une clé de chiffrement, il envoie une requête au serveur KMS qui inclut les données du certificat et une signature basée sur la clé privée.
4. Le serveur KMS valide la signature du certificat et décide qu'il peut faire confiance à StorageGRID.
5. Le serveur KMS répond à l'aide de la connexion validée.

Configurer les certificats de serveur

Types de certificat de serveur pris en charge

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

Le type de chiffrement de la stratégie de sécurité doit correspondre au type de certificat du serveur. Par exemple, les chiffrements RSA nécessitent des certificats RSA et les chiffrements ECDSA requièrent des certificats ECDSA. Voir "Gérer les certificats de sécurité". Si vous configurez une stratégie de sécurité personnalisée qui n'est pas compatible avec le certificat de serveur, vous pouvez le faire "rétablir temporairement la stratégie de sécurité par défaut".

Pour plus d'informations sur la façon dont StorageGRID sécurise les connexions client, reportez-vous à la section "Sécurité pour les clients S3 et Swift".

Configurer les certificats d'interface de gestion

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

Description de la tâche

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

Étant donné qu'un seul certificat d'interface de gestion personnalisée est utilisé pour tous les nœuds

d'administration, vous devez spécifier le certificat en tant que certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion à Grid Manager et au tenant Manager. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

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

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

Si vous accédez à Grid Manager ou au Gestionnaire de locataires à l'aide d'un nom de domaine au lieu d'une adresse IP, le navigateur affiche une erreur de certificat sans option de contournement si l'un des cas suivants se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vous restaurez le certificat de serveur par défaut à partir d'un certificat d'interface de gestion personnalisée.

Ajoutez un certificat d'interface de gestion personnalisée

Pour ajouter un certificat d'interface de gestion personnalisée, vous pouvez fournir votre propre certificat ou en générer un à l'aide de Grid Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat personnalisé**.
4. Chargez ou générez le certificat.

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

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

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

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

c. Développez **Détails du certificat** pour afficher les métadonnées de chaque certificat que vous avez téléchargé. Si vous avez téléchargé un bundle CA facultatif, chaque certificat s'affiche sur son propre onglet.

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

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

  Par exemple : `storagegrid_certificate.pem`

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

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

Générez un certificat

Générez les fichiers de certificat du serveur.

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

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.

Champ	Description
IP	Une ou plusieurs adresses IP à inclure dans le certificat.
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées du certificat généré.

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

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

  Par exemple : `storagegrid_certificate.pem`

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

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

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

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

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

Restaurez le certificat de l'interface de gestion par défaut

Vous pouvez revenir à l'utilisation du certificat d'interface de gestion par défaut pour les connexions Grid Manager et tenant Manager.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**.
2. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
3. Sélectionnez **utiliser le certificat par défaut**.

   Lorsque vous restaurez le certificat d'interface de gestion par défaut, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat d'interface de gestion par défaut est utilisé pour toutes les nouvelles connexions client suivantes.

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

Utilisez un script pour générer un nouveau certificat d'interface de gestion auto-signé

Si une validation stricte du nom d'hôte est requise, vous pouvez utiliser un script pour générer le certificat de l'interface de gestion.

Avant de commencer

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

Description de la tâche

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

Étapes

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

   Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

3. Configurez StorageGRID avec un nouveau certificat auto-signé.

   ```
   $ sudo make-certificate --domains wildcard-admin-node-fqdn --type management
   ```

   - Pour `--domains`, Utilisez des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration. Par exemple : `*.ui.storagegrid.example.com` utilise le caractère générique * pour représenter `admin1.ui.storagegrid.example.com` et `admin2.ui.storagegrid.example.com`.
   - Réglez `--type` à `management` Pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et tenant Manager.

- Par défaut, les certificats générés sont valables pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser le `--days` argument pour remplacer la période de validité par défaut.

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

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

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

4. Sélectionnez et copiez le certificat.

   Incluez les étiquettes DE DÉBUT et DE FIN dans votre sélection.

5. Déconnectez-vous du shell de commande. `$ exit`
6. Vérifiez que le certificat a été configuré :
   a. Accédez au Grid Manager.
   b. Sélectionnez **CONFIGURATION** > **sécurité** > **certificats**
   c. Dans l'onglet **Global**, sélectionnez **Management interface certificate**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.

Téléchargez ou copiez le certificat de l'interface de gestion

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

Étapes

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

Téléchargez le fichier de certificat ou le bundle CA

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

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

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

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

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

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

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

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Configurez les certificats API S3 et Swift

Vous pouvez remplacer ou restaurer le certificat du serveur utilisé pour les connexions des clients S3 ou Swift aux nœuds de stockage ou pour équilibreur de charge des terminaux. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Description de la tâche

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

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

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

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

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

Ajoutez un certificat S3 et Swift personnalisé

Étapes

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

Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

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

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

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

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

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

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

  Par exemple : `storagegrid_certificate.pem`

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

d. Sélectionnez **Enregistrer**.

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

Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

Champ	Description
Nom de domaine	Un ou plusieurs noms de domaine complets à inclure dans le certificat. Utilisez un * comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Objet (facultatif)	Objet X.509 ou nom distinctif (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou l'adresse IP comme nom commun de l'objet (CN).
Jours valides	Nombre de jours après la création, pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), l'utilisation des clés et les extensions d'utilisation des clés étendues sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : ne cochez pas cette case si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

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

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

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

  Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**.

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

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

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

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

Restaurez le certificat API S3 et Swift par défaut

Vous pouvez revenir à l'utilisation du certificat d'API S3 et Swift par défaut pour les connexions des clients S3 et Swift aux nœuds de stockage. Toutefois, vous ne pouvez pas utiliser le certificat par défaut des API S3 et Swift pour un terminal d'équilibrage des charges.

Étapes

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

   Lorsque vous restaurez la version par défaut du certificat d'API S3 et Swift global, les fichiers de certificat de serveur personnalisé que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Le certificat par défaut des API S3 et Swift sera utilisé pour les nouvelles connexions clientes S3 et Swift suivantes aux nœuds de stockage.

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

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

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

Téléchargez ou copiez le certificat API S3 et Swift

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

Étapes

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

Téléchargez le fichier de certificat ou le bundle CA

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

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

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

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

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat ou pack CA PEM

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

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

   Si vous copiez un bundle CA, tous les certificats des onglets secondaires de l'offre CA sont copiés ensemble.

b. Collez le certificat copié dans un éditeur de texte.

c. Enregistrez le fichier texte avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Informations associées

- "UTILISEZ L'API REST S3"
- "Utilisez l'API REST de Swift"
- "Configuration des noms de domaine de terminaux S3"

Copiez le certificat de l'autorité de certification Grid

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

Avant de commencer

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

Description de la tâche

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

Étapes

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

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copie du certificat PEM

Copiez le texte du certificat pour le coller ailleurs.

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

   Par exemple : `storagegrid_certificate.pem`

Configurez les certificats StorageGRID pour FabricPool

Pour les clients S3 qui valident rigoureusement le nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP qui utilisent FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le terminal de l'équilibreur de charge.

Avant de commencer

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

Description de la tâche

Lorsque vous créez un noeud final d'équilibreur de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification connue. Dans les environnements de production, vous devez utiliser un certificat signé par une autorité de certification connue. Les certificats signés par une autorité de certification peuvent être pivotés sans interruption. Elles sont également plus sécurisées parce qu'elles offrent une meilleure protection contre les attaques de l'homme au milieu.

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

Étapes

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

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

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

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

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

Configurer les certificats client

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

Si vous devez accéder à StorageGRID à l'aide d'un outil de surveillance externe, vous devez télécharger ou générer un certificat client à l'aide de Grid Manager et copier les informations de certificat dans l'outil externe.

Voir "Gérer les certificats de sécurité" et "Configurer des certificats de serveur personnalisés".

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

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

Avant de commencer

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

- Vous disposez de l'adresse IP ou du nom de domaine du nœud d'administration.
- Pour télécharger votre propre certificat ou un nouveau certificat, la clé privée, le certificat client et l'autorité de certification (si utilisée) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

Pour ajouter le certificat client, utilisez l'une des procédures suivantes :

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

Certificat d'interface de gestion déjà configuré

Utilisez cette procédure pour ajouter un certificat client si un certificat d'interface de gestion est déjà configuré à l'aide d'une autorité de certification fournie par le client, d'un certificat client et d'une clé privée.

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Attach certificates**, téléchargez le certificat de l'interface de gestion.
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Browse** et sélectionnez le fichier de certificat de l'interface de gestion (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît sur l'onglet client.
7. Configurer un outil de surveillance externe, Comme Grafana.

CERTIFICAT client émis

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

Étapes

1. Effectuez les étapes à "configurez un certificat d'interface de gestion".
2. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.

3. Sélectionnez **Ajouter**.
4. Entrez un nom de certificat.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **joindre des certificats**, téléchargez le certificat client, la clé privée et les fichiers de bundle CA :
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Browse** et sélectionnez le certificat client, la clé privée et les fichiers de bundle CA (`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Les nouveaux certificats apparaissent sur l'onglet client.
8. Configurer un outil de surveillance externe, Comme Grafana.

Certificat généré par Grid Manager

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

Étapes

1. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **client**.
2. Sélectionnez **Ajouter**.
3. Entrez un nom de certificat.
4. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **joindre des certificats**, sélectionnez **générer un certificat**.
7. Spécifiez les informations de certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

8. Sélectionnez **generate**.
9. sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le certificat PEM.

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

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

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

   Par exemple : `storagegrid_certificate.pem`

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

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

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

    Le nouveau certificat apparaît sur l'onglet client.

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

       Le nouveau certificat apparaît sur la page de certificat de l'interface de gestion.

15. Configurer un outil de surveillance externe, Comme Grafana.

configurez un outil de surveillance externe

Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.
   a. **Nom** : saisissez un nom pour la connexion.

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

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

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

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

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

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

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

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

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

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

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

Modifier les certificats client

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

Étapes

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

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

2. Sélectionnez le certificat à modifier.
3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**
4. Entrez un nom de certificat.
5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans Grid Manager.

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

Joindre un nouveau certificat client

Vous pouvez télécharger un nouveau certificat lorsque celui actuel a expiré.

Étapes

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

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

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

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

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

b. Téléchargez le nom du certificat client (`.pem`).

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

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

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

   Par exemple : `storagegrid_certificate.pem`

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

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

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

Générez un certificat

Générez le texte du certificat pour le coller ailleurs.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours valides** : nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandée), l'utilisation de clé et les extensions d'utilisation de clé étendue sont ajoutées au certificat généré.

     Ces extensions définissent l'objectif de la clé contenue dans le certificat.

     Laissez cette case cochée sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **generate**.

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

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

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

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

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

  Par exemple : `storagegrid_certificate.pem`

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

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

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

Le nouveau certificat apparaît sur l'onglet client.

Téléchargez ou copiez les certificats client

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

Étapes

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

Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat

Copiez le texte du certificat pour le coller ailleurs.

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

   Par exemple : `storagegrid_certificate.pem`

Supprimer les certificats client

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

Étapes

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

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

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

Configurez les paramètres de sécurité

Gestion des règles TLS et SSH

La règle TLS et SSH détermine les protocoles et les chiffrements utilisés pour établir des connexions TLS sécurisées avec les applications client et des connexions SSH sécurisées avec les services StorageGRID internes.

La règle de sécurité contrôle la façon dont TLS et SSH chiffrent les données en mouvement. En général, utilisez la règle de compatibilité moderne (par défaut), sauf si votre système doit être conforme aux critères communs ou si vous devez utiliser d'autres chiffrements.

> Certains services StorageGRID n'ont pas été mis à jour pour utiliser le chiffrement inclus dans ces règles.

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 racine".

Sélectionnez une stratégie de sécurité

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.

   L'onglet **TLS et SSH policies** affiche les stratégies disponibles. La règle actuellement active est indiquée par une coche verte sur la vignette de la police.

2. Consultez les vignettes pour en savoir plus sur les stratégies disponibles.

Politique	Description
Compatibilité moderne (par défaut)	Utilisez la stratégie par défaut si vous avez besoin d'un cryptage fort et si vous ne disposez pas d'exigences particulières. Cette règle est compatible avec la plupart des clients TLS et SSH.
Compatibilité avec les systèmes existants	Utilisez cette stratégie si vous avez besoin d'options de compatibilité supplémentaires pour les anciens clients. Les options supplémentaires de cette politique pourraient la rendre moins sécurisée que la politique de compatibilité moderne.
Critères communs	Utilisez cette règle si vous avez besoin de la certification critères communs.
Norme FIPS stricte	Utilisez cette règle si vous avez besoin de la certification critères communs et que vous devez utiliser le module de sécurité cryptographique NetApp 3.0.8 pour les connexions de clients externes aux terminaux d'équilibrage de charge, au gestionnaire de locataires et au gestionnaire de grille. L'utilisation de cette règle peut réduire les performances. **Remarque** : après avoir sélectionné cette stratégie, tous les nœuds doivent être "redémarrés de manière mobile" Pour activer le module de sécurité cryptographique NetApp. Utilisez **Maintenance** > **redémarrage en roulant** pour lancer et surveiller les redémarrages.
Personnalisées	Créez une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

3. Pour afficher des détails sur les chiffrements, les protocoles et les algorithmes de chaque stratégie, sélectionnez **Afficher les détails**.
4. Pour modifier la stratégie actuelle, sélectionnez **utiliser la stratégie**.

   Une coche verte apparaît en regard de **police actuelle** sur la mosaïque de police.

Créez une stratégie de sécurité personnalisée

Vous pouvez créer une stratégie personnalisée si vous devez appliquer vos propres chiffrements.

Étapes

1. Dans la mosaïque de la stratégie la plus similaire à la stratégie personnalisée que vous souhaitez créer, sélectionnez **Afficher les détails**.
2. Sélectionnez **Copier dans le presse-papiers**, puis sélectionnez **Annuler**.

3. Dans la mosaïque **Personnaliser la stratégie**, sélectionnez **configurer et utiliser**.
4. Collez le fichier JSON que vous avez copié et apportez les modifications nécessaires.
5. Sélectionnez **utiliser la stratégie**.

   Une coche verte apparaît en regard de **politique actuelle** sur la mosaïque de stratégie personnalisée.

6. Si vous le souhaitez, sélectionnez **Modifier la configuration** pour apporter d'autres modifications à la nouvelle stratégie personnalisée.

Rétablir temporairement la stratégie de sécurité par défaut

Si vous avez configuré une stratégie de sécurité personnalisée, il se peut que vous ne puissiez pas vous connecter au gestionnaire de grille si la stratégie TLS configurée est incompatible avec le "certificat de serveur configuré".

Vous pouvez rétablir temporairement la stratégie de sécurité par défaut.

Étapes

1. Connectez-vous à un nœud d'administration :
   a. Saisissez la commande suivante : `ssh admin@Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.
   c. Entrez la commande suivante pour passer à la racine : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` fichier.

      Lorsque vous êtes connecté en tant que root, l'invite passe de `$` à `#`.

2. Exécutez la commande suivante :

```
restore-default-cipher-configurations
```

3. À partir d'un navigateur Web, accédez à Grid Manager sur le même nœud d'administration.
4. Suivez les étapes de la section Sélectionnez une stratégie de sécurité pour reconfigurer la stratégie.

Configurer la sécurité du réseau et des objets

Vous pouvez configurer la sécurité du réseau et des objets pour chiffrer les objets stockés, empêcher certaines requêtes S3 et Swift, ou autoriser les connexions client aux nœuds de stockage à utiliser le protocole HTTP au lieu du protocole HTTPS.

Chiffrement des objets stockés

Le chiffrement des objets stockés permet de chiffrer toutes les données d'objet lors de leur ingestion via S3. Par défaut, les objets stockés ne sont pas chiffrés, mais vous pouvez choisir de chiffrer les objets à l'aide de l'algorithme de cryptage AES-128 ou AES-256. Lorsque vous activez le paramètre, tous les objets récemment acquis sont chiffrés, mais aucun changement n'est apporté aux objets stockés existants. Si vous désactivez le chiffrement, les objets actuellement chiffrés restent chiffrés, mais les objets nouvellement ingérés ne sont pas chiffrés.

Le paramètre de chiffrement des objets stockés s'applique uniquement aux objets S3 qui n'ont pas été chiffrés par chiffrement au niveau du compartiment ou de l'objet.

Pour plus d'informations sur les méthodes de cryptage StorageGRID, reportez-vous à la section "Étudiez les méthodes de cryptage StorageGRID".

Empêcher toute modification du client

Empêcher la modification du client est un paramètre à l'échelle du système. Lorsque l'option **empêcher la modification du client** est sélectionnée, les demandes suivantes sont refusées.

L'API REST S3

- Demandes DeleteBucket
- Toute demande de modification des données d'un objet existant, des métadonnées définies par l'utilisateur ou du balisage d'objets S3

API REST Swift

- Supprimer les demandes de conteneur
- Demande de modifier tout objet existant. Par exemple, les opérations suivantes sont refusées : remplacement, suppression, mise à jour des métadonnées, etc.

Activez HTTP pour les connexions de nœud de stockage

Par défaut, les applications clientes utilisent le protocole réseau HTTPS pour toutes les connexions directes aux nœuds de stockage. Vous pouvez éventuellement activer HTTP pour ces connexions, par exemple lors du test d'une grille autre que la production.

Utilisez HTTP pour les connexions de nœuds de stockage uniquement si les clients S3 et Swift doivent établir des connexions HTTP directement aux nœuds de stockage. Vous n'avez pas besoin d'utiliser cette option pour les clients qui utilisent uniquement des connexions HTTPS ou pour les clients qui se connectent au service

Load Balancer (parce que vous le pouvez) "configurez chaque point d'extrémité de l'équilibreur de charge" Pour utiliser HTTP ou HTTPS).

Voir "Résumé : adresses IP et ports pour les connexions client" Pour savoir quels ports les clients S3 et Swift utilisent lors de la connexion aux nœuds de stockage via HTTP ou HTTPS.

Sélectionnez les options

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous disposez de l'autorisation d'accès racine.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **réseau et objets**.
3. Pour le chiffrement des objets stockés, utilisez le paramètre **None** (par défaut) si vous ne souhaitez pas que les objets stockés soient cryptés, ou sélectionnez **AES-128** ou **AES-256** pour crypter les objets stockés.
4. Vous pouvez également sélectionner **empêcher la modification du client** si vous souhaitez empêcher les clients S3 et Swift de faire des demandes spécifiques.

   Si vous modifiez ce paramètre, il faudra environ une minute pour appliquer le nouveau paramètre. La valeur configurée est mise en cache pour les performances et l'évolutivité.

5. Sélectionnez **Activer HTTP pour les connexions de noeud de stockage** si les clients se connectent directement aux noeuds de stockage et que vous souhaitez utiliser les connexions HTTP.

   Soyez prudent lorsque vous activez HTTP pour une grille de production car les requêtes seront envoyées de manière non chiffrée.

6. Sélectionnez **Enregistrer**.

Modifier les paramètres de sécurité de l'interface

Les paramètres de sécurité de l'interface vous permettent de contrôler si les utilisateurs sont déconnectés s'ils sont inactifs pendant plus de temps que spécifié et si une trace de pile est incluse dans les réponses d'erreur de l'API.

Avant de commencer

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

Description de la tâche

La page **Paramètres de sécurité** inclut les paramètres **délai d'inactivité du navigateur** et **trace de pile de l'API de gestion**.

Délai d'inactivité du navigateur dépassé

Indique la durée pendant laquelle le navigateur d'un utilisateur peut être inactif avant que l'utilisateur ne soit déconnecté. La valeur par défaut est 15 minutes.

Le délai d'inactivité du navigateur est également contrôlé par les éléments suivants :

- Un minuteur StorageGRID séparé non configurable, inclus pour la sécurité du système. Le jeton d'authentification de chaque utilisateur expire 16 heures après la session de l'utilisateur. Lorsque l'authentification d'un utilisateur expire, cet utilisateur est automatiquement déconnecté, même si le délai d'inactivité du navigateur est désactivé ou si la valeur du délai d'inactivité du navigateur n'a pas été atteinte. Pour renouveler le jeton, l'utilisateur doit se reconnecter.
- Paramètres de délai d'expiration pour le fournisseur d'identité, en supposant que l'authentification unique (SSO) est activée pour StorageGRID.

  Si la fonction SSO est activée et que le navigateur d'un utilisateur arrive à expiration, l'utilisateur doit saisir à nouveau ses informations d'identification SSO pour accéder à StorageGRID à nouveau. Voir "Configurer l'authentification unique".

Trace de la pile de l'API de gestion

Contrôle si une trace de pile est renvoyée dans les réponses d'erreur de l'API Grid Manager et tenant Manager.

Cette option est désactivée par défaut, mais vous pouvez activer cette fonctionnalité pour un environnement de test. En général, vous devez laisser la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails logiciels internes en cas d'erreurs d'API.

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres de sécurité**.
2. Sélectionnez l'onglet **interface**.
3. Pour modifier le paramètre de délai d'inactivité du navigateur :
   a. Développez l'accordéon.
   b. Pour modifier la période de temporisation, spécifiez une valeur comprise entre 60 secondes et 7 jours. Le délai par défaut est de 15 minutes.
   c. Pour désactiver cette fonction, décochez la case.
   d. Sélectionnez **Enregistrer**.

      Le nouveau paramètre n'affecte pas les utilisateurs qui sont actuellement connectés. Les utilisateurs doivent se reconnecter ou actualiser leur navigateur pour que le nouveau paramètre de délai d'expiration prenne effet.
4. Pour modifier le paramètre de trace de pile de l'API de gestion :
   a. Développez l'accordéon.
   b. Cochez cette case pour renvoyer une trace de pile dans les réponses d'erreur de l'API Grid Manager et tenant Manager.

      Laissez la trace de pile désactivée dans les environnements de production pour éviter de révéler les détails logiciels internes en cas d'erreur d'API.

   c. Sélectionnez **Enregistrer**.

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.

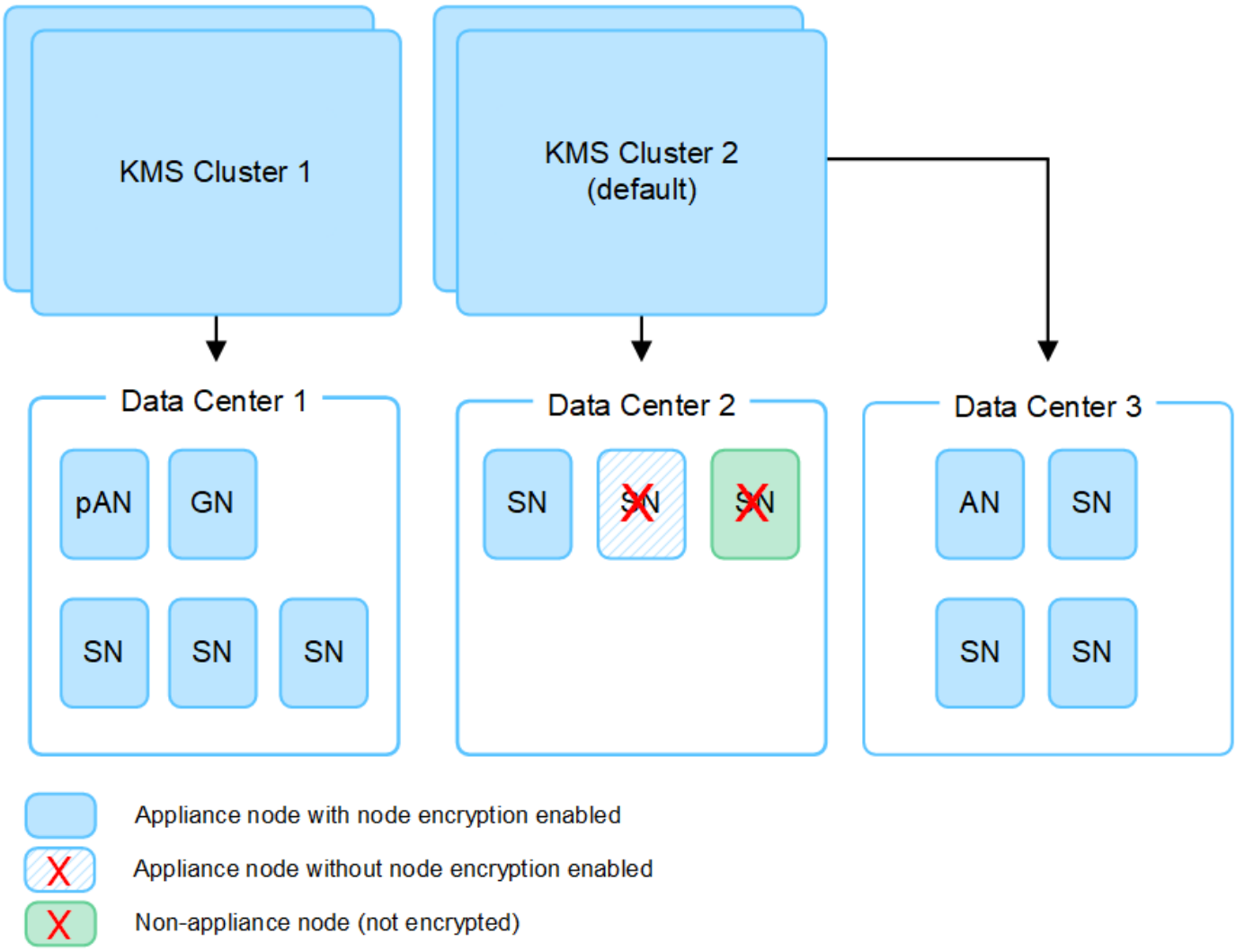
Combien de serveurs de gestion des clés ai-je besoin ?

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.

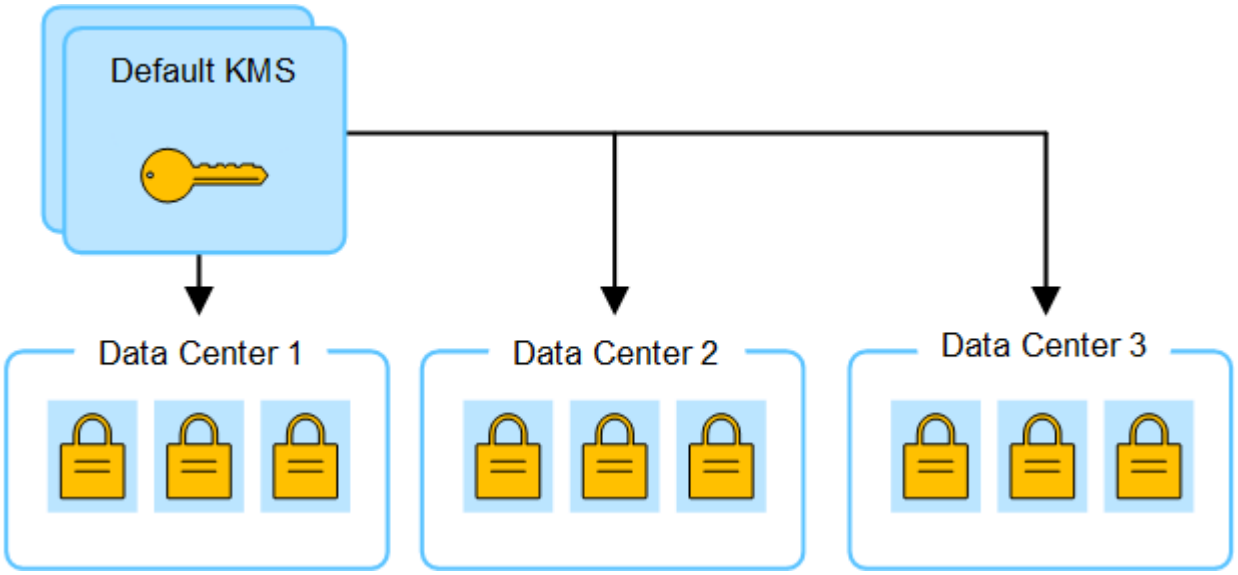
Considérations relatives à la modification du KMS pour un site

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.

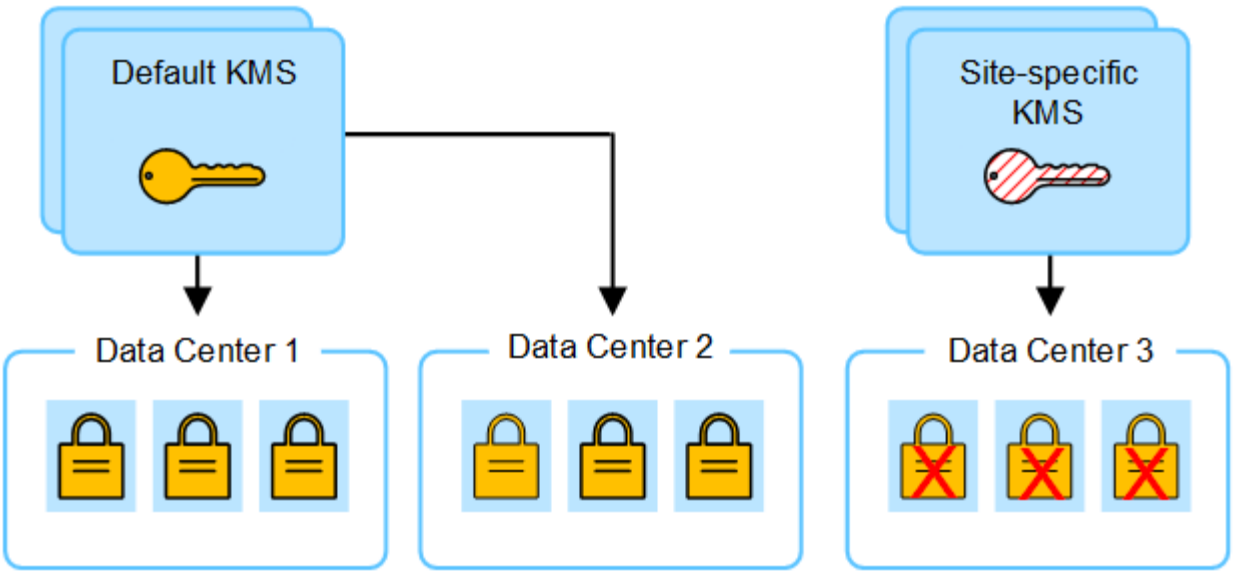
Si vous modifiez le KMS utilisé pour un site, vous devez vous assurer que les nœuds d'appliance précédemment cryptés de ce site peuvent être déchiffrés à l'aide de la clé stockée sur le nouveau KMS. Dans certains cas, vous devrez peut-être copier la version actuelle de la clé de chiffrement à partir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

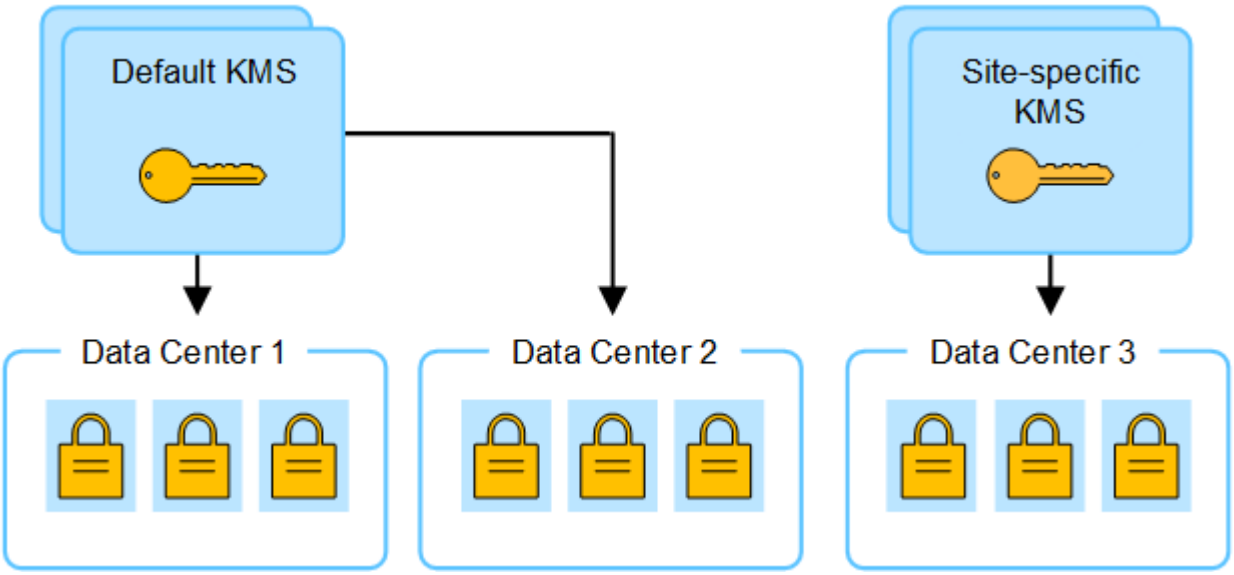
1. Vous configurez initialement un KMS par défaut qui s'applique à tous les sites qui ne disposent pas d'un KMS dédié.
2. Lorsque le KMS est enregistré, tous les nœuds de l'appliance dont le paramètre **Node Encryption** est activé se connectent au KMS et demandent la clé de chiffrement. Cette clé est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

Gérer les paramètres proxy

Configurer le proxy de stockage

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

> Les paramètres configurés du proxy de stockage ne s'appliquent pas aux terminaux des services de la plateforme Kafka.

Avant de commencer

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

Description de la tâche

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

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **Paramètres proxy**.
2. Dans l'onglet **stockage**, cochez la case **Activer le proxy de stockage**.
3. Sélectionnez le protocole du proxy de stockage.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Vous pouvez également saisir le port utilisé pour vous connecter au serveur proxy.

   Laissez ce champ vide pour utiliser le port par défaut du protocole : 80 pour HTTP ou 1080 pour SOCKS5.

6. Sélectionnez **Enregistrer**.

   Une fois le proxy de stockage enregistré, il est possible de configurer et de tester de nouveaux terminaux pour les services de plateforme ou les pools de stockage cloud.

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

7. Vérifiez les paramètres de votre serveur proxy pour vous assurer que les messages relatifs au service de la plate-forme de StorageGRID ne seront pas bloqués.
8. Si vous devez désactiver un proxy de stockage, décochez la case et sélectionnez **Enregistrer**.

Configurer les paramètres du proxy d'administration

Si vous envoyez des packages AutoSupport via HTTP ou HTTPS, vous pouvez configurer un serveur proxy non transparent entre les nœuds d'administration et le support technique (AutoSupport).

Pour plus d'informations sur AutoSupport, reportez-vous à la section "Configurez AutoSupport".

Avant de commencer

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

Description de la tâche

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

Étapes

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

   La page Paramètres proxy s'affiche. Par défaut, l'option stockage est sélectionnée dans le menu de l'onglet.

2. Sélectionnez l'onglet **Admin**.
3. Cochez la case **Activer le proxy Admin**.
4. Entrez le nom d'hôte ou l'adresse IP du serveur proxy.
5. Entrez le port utilisé pour se connecter au serveur proxy.
6. Vous pouvez également saisir un nom d'utilisateur et un mot de passe pour le serveur proxy.

   Laissez ces champs vides si votre serveur proxy ne requiert pas de nom d'utilisateur ou de mot de passe.

7. Sélectionnez l'une des options suivantes :

   - Si vous souhaitez sécuriser la connexion au proxy d'administration, sélectionnez **vérifier le certificat**. Téléchargez un paquet CA pour vérifier l'authenticité des certificats SSL présentés par le serveur proxy d'administration.

     > AutoSupport On Demand, E-Series AutoSupport via StorageGRID et la détermination du chemin de mise à jour sur la page mise à niveau StorageGRID ne fonctionneront pas si un certificat proxy est vérifié.

     Une fois le paquet CA téléchargé, ses métadonnées s'affichent.

   - Si vous ne souhaitez pas valider les certificats lors de la communication avec le serveur proxy d'administration, sélectionnez **ne pas vérifier le certificat**.

8. Sélectionnez **Enregistrer**.

   Une fois le proxy d'administration enregistré, le serveur proxy entre les nœuds d'administration et le support technique est configuré.

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

9. Si vous devez désactiver le proxy admin, décochez la case **Activer le proxy Admin**, puis sélectionnez **Enregistrer**.

Contrôle des pare-feu

Contrôler l'accès au niveau du pare-feu externe

Vous pouvez ouvrir ou fermer des ports spécifiques au niveau du pare-feu externe.

Vous pouvez contrôler l'accès aux interfaces utilisateur et aux API des nœuds d'administration StorageGRID en ouvrant ou en fermant des ports spécifiques au pare-feu externe. Par exemple, vous pouvez empêcher les locataires de se connecter à Grid Manager au niveau du pare-feu, en plus d'utiliser d'autres méthodes pour contrôler l'accès au système.

Si vous souhaitez configurer le pare-feu interne StorageGRID, reportez-vous à la section "Configurer le pare-feu interne".

Port	Description	Si le port est ouvert…
443	Port HTTPS par défaut pour les nœuds d'administration	Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager, à l'API de gestion du grid, au gestionnaire des locataires et à l'API de gestion des locataires. **Remarque :** le port 443 est également utilisé pour un trafic interne.
8443	Port restreint de Grid Manager sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder à Grid Manager et à l'API de gestion Grid via HTTPS. • Les navigateurs Web et les clients de l'API de gestion ne peuvent pas accéder au gestionnaire de locataires ou à l'API de gestion des locataires. • Les demandes de contenu interne seront rejetées.
9443	Port de gestionnaire de locataires restreint sur les nœuds d'administration	• Les navigateurs Web et les clients d'API de gestion peuvent accéder au Gestionnaire de locataires et à l'API de gestion des locataires via HTTPS. • Les navigateurs Web et les clients API de gestion ne peuvent pas accéder à Grid Manager ou à l'API Grid Management. • Les demandes de contenu interne seront rejetées.

L'authentification unique (SSO) n'est pas disponible sur les ports du gestionnaire de grille restreinte ou du gestionnaire de locataires. Vous devez utiliser le port HTTPS par défaut (443) si vous souhaitez que les utilisateurs s'authentifient avec une connexion unique.

Informations associées

- "Connectez-vous au Grid Manager"
- "Créer un compte de locataire"
- "Communications externes"

Gérer les contrôles de pare-feu internes

StorageGRID comprend un pare-feu interne sur chaque nœud qui améliore la sécurité de votre grille en vous permettant de contrôler l'accès réseau au nœud. Utilisez le pare-feu pour empêcher l'accès au réseau sur tous les ports, à l'exception de ceux nécessaires à votre déploiement de grille spécifique. Les modifications de configuration effectuées sur la page de contrôle du pare-feu sont déployées sur chaque nœud.

Utilisez les trois onglets de la page de contrôle du pare-feu pour personnaliser l'accès dont vous avez besoin pour votre grille.

- **Liste d'adresses privilégiées** : utilisez cet onglet pour autoriser l'accès sélectionné aux ports fermés. Vous pouvez ajouter des adresses IP ou des sous-réseaux en notation CIDR qui peuvent accéder aux ports fermés à l'aide de l'onglet gérer l'accès externe.
- **Gérer l'accès externe** : utilisez cet onglet pour fermer les ports ouverts par défaut ou rouvrir les ports précédemment fermés.
- **Réseau client non approuvé** : utilisez cet onglet pour indiquer si un nœud approuve le trafic entrant provenant du réseau client.

  Les paramètres de cet onglet remplacent les paramètres de l'onglet gérer l'accès externe.

  - Un nœud avec un réseau client non approuvé accepte uniquement les connexions sur les ports de point final de l'équilibreur de charge configurés sur ce nœud (points finaux globaux, liés à l'interface de nœud et au type de nœud).
  - Les ports de point final de l'équilibreur de charge sont les seuls ports ouverts_ sur les réseaux clients non approuvés, quels que soient les paramètres de l'onglet gérer les réseaux externes.
  - Une fois approuvés, tous les ports ouverts sous l'onglet gérer l'accès externe sont accessibles, ainsi que tous les noeuds finaux d'équilibrage de charge ouverts sur le réseau client.

> Les paramètres que vous effectuez sur un onglet peuvent affecter les modifications d'accès que vous effectuez sur un autre onglet. Vérifiez les paramètres de tous les onglets pour vous assurer que votre réseau se comporte comme vous le souhaitez.

Pour configurer les contrôles de pare-feu internes, reportez-vous à la section "Configurer les contrôles de pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section "Contrôler l'accès au niveau du pare-feu externe".

Liste d'adresses privilégiées et onglets gérer les accès externes

L'onglet liste d'adresses privilégiées vous permet d'enregistrer une ou plusieurs adresses IP qui ont accès aux ports de la grille fermés. L'onglet gérer l'accès externe vous permet de fermer l'accès externe aux ports externes sélectionnés ou à tous les ports externes ouverts (les ports externes sont des ports accessibles par défaut par les nœuds non-grid). Ces deux onglets peuvent souvent être utilisés ensemble pour personnaliser l'accès réseau exact dont vous avez besoin pour votre grille.

> Par défaut, les adresses IP privilégiées n'ont pas d'accès au port de la grille interne.

Exemple 1 : utilisez un hôte de secours pour les tâches de maintenance

Supposons que vous souhaitiez utiliser un hôte de secours (un hôte renforcé par la sécurité) pour l'administration du réseau. Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour ajouter l'adresse IP de l'hôte de saut.
2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer les ports 443 et 8443. Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, tous les ports externes du nœud d'administration de votre grille seront bloqués pour tous les hôtes, à l'exception de l'hôte de saut. Vous pouvez ensuite utiliser l'hôte de secours pour effectuer des tâches de maintenance sur votre grille de manière plus sécurisée.

Exemple 2 : limiter l'accès au gestionnaire de grille et au gestionnaire de locataires

Supposons que vous souhaitiez limiter l'accès au gestionnaire de grille et au gestionnaire de locataires (ports prédéfinis) pour des raisons de sécurité. Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez le bouton bascule de l'onglet gérer l'accès externe pour bloquer le port 443.
2. Utilisez la bascule de l'onglet gérer l'accès externe pour autoriser l'accès au port 8443.
3. Utilisez la bascule de l'onglet gérer l'accès externe pour autoriser l'accès au port 9443.

Une fois la configuration enregistrée, les hôtes ne pourront pas accéder au port 443, mais ils pourront toujours accéder au Grid Manager via le port 8443 et le tenant Manager via le port 9443.

> Les ports 443, 8443 et 9443 sont les ports prédéfinis pour Grid Manager et tenant Manager. Vous pouvez basculer n'importe quel port pour limiter l'accès à un gestionnaire de grille ou un gestionnaire de tenant spécifique.

Exemple 3 : verrouiller les ports sensibles

Supposons que vous souhaitez verrouiller les ports sensibles et le service sur ce port (par exemple, SSH sur le port 22). Vous pouvez utiliser les étapes générales suivantes :

1. Utilisez l'onglet liste d'adresses privilégiées pour accorder l'accès uniquement aux hôtes qui ont besoin d'accéder au service.
2. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports.

> Ajoutez l'adresse IP privilégiée avant de bloquer l'accès aux ports affectés à Grid Manager et au gestionnaire de locataires (les ports prédéfinis sont 443 et 8443). Tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager à moins que leur adresse IP n'ait été ajoutée à la liste d'adresses privilégiées.

Après avoir enregistré votre configuration, le port 22 et le service SSH seront disponibles pour les hôtes de la liste d'adresses privilégiées. Tous les autres hôtes se verront refuser l'accès au service, quelle que soit l'interface d'origine de la demande.

Exemple 4 : désactiver l'accès aux services inutilisés

Au niveau du réseau, vous pouvez désactiver certains services que vous n'avez pas l'intention d'utiliser. Par exemple, si vous ne souhaitez pas fournir l'accès Swift, vous devez effectuer les étapes générales suivantes :

1. Utilisez le bouton bascule de l'onglet gérer l'accès externe pour bloquer le port 18083.
2. Utilisez le bouton bascule de l'onglet gérer l'accès externe pour bloquer le port 18085.

Une fois la configuration enregistrée, le nœud de stockage n'autorise plus la connectivité Swift, mais continue d'autoriser l'accès à d'autres services sur les ports débloqués.

Onglet réseaux de clients non approuvés

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

Par défaut, le réseau client sur chaque nœud de la grille est *Trusted*. Par défaut, StorageGRID approuve les connexions entrantes à chaque nœud de grid sur tous "ports externes disponibles".

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

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

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

1. À partir du "Terminaux d'équilibrage de charge" Configurez un terminal d'équilibreur de charge pour S3 sur HTTPS sur le port 443.
2. Sur la page de contrôle du pare-feu, sélectionnez non approuvé pour indiquer que le réseau client sur le nœud passerelle n'est pas fiable.

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

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

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

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

Une fois la configuration enregistrée, le nœud de stockage n'accepte plus le trafic entrant sur le réseau client, mais continue à autoriser les requêtes sortantes vers les destinations de services de plate-forme configurées.

Exemple 3 : limitation de l'accès à Grid Manager à un sous-réseau

Supposons que vous souhaitiez autoriser l'accès à Grid Manager uniquement sur un sous-réseau spécifique. Procédez comme suit :

1. Connectez le réseau client de vos nœuds d'administration au sous-réseau.
2. Utilisez l'onglet réseau client non approuvé pour configurer le réseau client comme non fiable.
3. Lorsque vous créez un noeud final d'équilibreur de charge dans l'interface de gestion, entrez le port et sélectionnez l'interface de gestion à laquelle le port accérera.
4. Sélectionnez **Oui** pour réseau client non sécurisé.
5. Utilisez l'onglet gérer l'accès externe pour bloquer tous les ports externes (avec ou sans adresses IP privilégiées définies pour les hôtes situés en dehors de ce sous-réseau).

Après avoir enregistré votre configuration, seuls les hôtes du sous-réseau que vous avez spécifié peuvent accéder à Grid Manager. Tous les autres hôtes sont bloqués.

Configurer le pare-feu interne

Vous pouvez configurer le pare-feu StorageGRID pour contrôler l'accès réseau à des ports spécifiques sur vos nœuds StorageGRID.

Avant de commencer

- Vous êtes connecté au Grid Manager à l'aide d'un "navigateur web pris en charge".
- Vous avez "autorisations d'accès spécifiques".
- Vous avez examiné les informations dans "Gérer les contrôles de pare-feu" et "Instructions de mise en réseau".
- Si vous souhaitez qu'un nœud d'administration ou un nœud de passerelle accepte le trafic entrant uniquement sur des noeuds finaux configurés explicitement, vous avez défini les noeuds finaux de l'équilibreur de charge.

> Lors de la modification de la configuration du réseau client, les connexions client existantes peuvent échouer si les noeuds finaux de l'équilibreur de charge n'ont pas été configurés.

Description de la tâche

StorageGRID comprend un pare-feu interne sur chaque nœud qui vous permet d'ouvrir ou de fermer certains ports sur les nœuds de votre grille. Vous pouvez utiliser les onglets de contrôle du pare-feu pour ouvrir ou fermer des ports ouverts par défaut sur le réseau Grid, le réseau Admin et le réseau client. Vous pouvez également créer une liste d'adresses IP privilégiées pouvant accéder aux ports de la grille fermés. Si vous utilisez un réseau client, vous pouvez spécifier si un nœud approuve le trafic entrant à partir du réseau client et configurer l'accès à des ports spécifiques sur le réseau client.

Limiter le nombre de ports ouverts aux adresses IP en dehors de votre grille à ceux qui sont absolument nécessaires améliore la sécurité de votre grille. Vous utilisez les paramètres de chacun des trois onglets de contrôle du pare-feu pour vous assurer que seuls les ports nécessaires sont ouverts.

Pour plus d'informations sur l'utilisation des contrôles de pare-feu, notamment des exemples, reportez-vous à la section "Gérer les contrôles de pare-feu".

Pour plus d'informations sur les pare-feu externes et la sécurité réseau, reportez-vous à la section "Contrôler l'accès au niveau du pare-feu externe".

Accès aux contrôles de pare-feu

Étapes

1. Sélectionnez **CONFIGURATION** > **sécurité** > **contrôle du pare-feu**.

   Les trois onglets de cette page sont décrits dans "Gérer les contrôles de pare-feu".

2. Sélectionnez n'importe quel onglet pour configurer les contrôles du pare-feu.

   Vous pouvez utiliser ces onglets dans n'importe quel ordre. Les configurations que vous définissez sur un onglet ne limitent pas ce que vous pouvez faire sur les autres onglets. Cependant, les modifications de configuration effectuées sur un onglet peuvent modifier le comportement des ports configurés sur d'autres onglets.

Liste d'adresses privilégiées

Vous utilisez l'onglet liste d'adresses privilégiées pour accorder aux hôtes l'accès aux ports fermés par défaut ou fermés par des paramètres de l'onglet gérer l'accès externe.

Par défaut, les adresses IP privilégiées et les sous-réseaux ne disposent pas d'un accès au grid interne. En outre, les noeuds finaux d'équilibrage de charge et les ports supplémentaires ouverts dans l'onglet liste d'adresses privilégiées sont accessibles même si bloqués dans l'onglet gérer l'accès externe.

Les paramètres de l'onglet liste d'adresses privilégiées ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé.

Étapes

1. Dans l'onglet liste d'adresses privilégiées, entrez l'adresse ou le sous-réseau IP que vous souhaitez accorder à l'accès aux ports fermés.
2. Si vous le souhaitez, sélectionnez **Ajouter une autre adresse IP ou un autre sous-réseau en notation CIDR** pour ajouter des clients privilégiés supplémentaires.

   Ajoutez autant d'adresses que possible à la liste privilégiée.

3. Vous pouvez également sélectionner **Autoriser les adresses IP privilégiées à accéder aux ports internes StorageGRID**. Voir "Ports internes StorageGRID".

   Cette option supprime certaines protections pour les services internes. Laissez-le désactivé si possible.

4. Sélectionnez **Enregistrer**.

Gérer l'accès externe

Lorsqu'un port est fermé dans l'onglet gérer l'accès externe, il est impossible d'accéder au port par une adresse IP non grille à moins que vous n'ajoutiez l'adresse IP à la liste d'adresses privilégiées. Vous ne pouvez fermer que les ports ouverts par défaut et vous ne pouvez ouvrir que les ports que vous avez fermés.

Les paramètres de l'onglet gérer l'accès externe ne peuvent pas remplacer les paramètres de l'onglet réseau client non approuvé. Par exemple, si un nœud n'est pas approuvé, le port SSH/22 est bloqué sur le réseau client même s'il est ouvert dans l'onglet gérer l'accès externe. Les paramètres de l'onglet réseau client non approuvé remplacent les ports fermés (tels que 443, 8443, 9443) sur le réseau client.

Étapes

1. Sélectionnez **gérer l'accès externe**. L'onglet affiche un tableau contenant tous les ports externes (ports accessibles par défaut par les nœuds non GRID) pour les nœuds de votre grille.
2. Configurez les ports que vous souhaitez ouvrir et fermer à l'aide des options suivantes :
   - Utilisez la bascule située en regard de chaque port pour ouvrir ou fermer le port sélectionné.
   - Sélectionnez **Ouvrir tous les ports affichés** pour ouvrir tous les ports répertoriés dans le tableau.
   - Sélectionnez **Fermer tous les ports affichés** pour fermer tous les ports répertoriés dans le tableau.

   Si vous fermez les ports Grid Manager 443 ou 8443, tous les utilisateurs actuellement connectés sur un port bloqué, y compris vous, perdront l'accès à Grid Manager, sauf si leur adresse IP a été ajoutée à la liste d'adresses privilégiées.

   Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les ports disponibles. Utilisez le champ de recherche pour trouver les paramètres de n'importe quel port externe en entrant un numéro de port. Vous pouvez entrer un numéro de port partiel. Par exemple, si vous entrez un **2**, tous les ports dont le nom contient la chaîne "2" s'affichent.
3. Sélectionnez **Enregistrer**

Réseau client non fiable

Si le réseau client d'un nœud n'est pas approuvé, le nœud accepte uniquement le trafic entrant sur les ports configurés comme points finaux de l'équilibreur de charge et, éventuellement, les ports supplémentaires que vous sélectionnez dans cet onglet. Vous pouvez également utiliser cet onglet pour spécifier le paramètre par défaut pour les nouveaux nœuds ajoutés dans une extension.

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

Les modifications de configuration effectuées dans l'onglet **réseau client non approuvé** remplacent les paramètres de l'onglet **gérer l'accès externe**.

Étapes

1. Sélectionnez **réseau client non approuvé**.
2. Dans la section définir les nouveaux nœuds par défaut, spécifiez le paramètre par défaut lorsque de nouveaux nœuds sont ajoutés à la grille dans une procédure d'extension.
   - **Approuvé** (par défaut) : lorsqu'un nœud est ajouté dans une extension, son réseau client est approuvé.
   - **Non fiable** : lorsqu'un nœud est ajouté dans une extension, son réseau client n'est pas fiable.

     Si nécessaire, vous pouvez revenir à cet onglet pour modifier le paramètre d'un nouveau nœud spécifique.

     Ce paramètre n'affecte pas les nœuds existants du système StorageGRID.
3. Utilisez les options suivantes pour sélectionner les nœuds qui doivent autoriser les connexions client uniquement sur les terminaux d'équilibrage de charge configurés explicitement ou sur les ports sélectionnés supplémentaires :

- Sélectionnez **ne pas faire confiance aux nœuds affichés** pour ajouter tous les nœuds affichés dans le tableau à la liste réseau client non approuvé.
- Sélectionnez **confiance sur les nœuds affichés** pour supprimer tous les nœuds affichés dans le tableau de la liste réseau client non approuvé.
- Utilisez la bascule en regard de chaque nœud pour définir le réseau client comme approuvé ou non fiable pour le nœud sélectionné.

  Par exemple, vous pouvez sélectionner **ne plus faire confiance aux nœuds affichés** pour ajouter tous les nœuds à la liste réseau client non approuvé, puis utiliser la bascule à côté d'un nœud individuel pour ajouter ce nœud à la liste réseau client approuvé.

> Utilisez la barre de défilement située à droite du tableau pour vous assurer que vous avez affiché tous les nœuds disponibles. Utilisez le champ de recherche pour rechercher les paramètres d'un nœud en saisissant son nom. Vous pouvez entrer un nom partiel. Par exemple, si vous entrez un **GW**, tous les nœuds qui ont la chaîne "GW" comme partie de leur nom sont affichés.

4. Sélectionnez **Enregistrer**.

Les nouveaux paramètres de pare-feu sont immédiatement appliqués et appliqués. Les connexions client existantes peuvent échouer si les points de terminaison de l'équilibreur de charge n'ont pas été configurés.

Informations sur le copyright

Informations sur les marques commerciales