Gérer les certificats

StorageGRID software

NetApp
December 03, 2025

Sommaire

Gérer les certificats

Gérer les certificats de sécurité

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 sont utilisés pour établir des connexions sécurisées entre les clients et les serveurs, authentifiant l'identité d'un serveur auprès de ses clients et fournissant un chemin de communication sécurisé pour les données. Le serveur et le client disposent chacun d'une copie du certificat.
- Les **certificats clients** authentifient l'identité d'un client ou d'un utilisateur auprès du serveur, offrant une authentification plus sécurisée que les mots de passe seuls. Les certificats clients ne cryptent 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 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 (comme le point de terminaison de l'équilibreur de charge) ou comme client pour d'autres connexions (comme le service de réplication CloudMirror).

Certificat Grid CA par défaut

StorageGRID inclut une autorité de certification (CA) intégrée qui génère un certificat CA Grid interne lors de l'installation du système. Le certificat Grid CA est utilisé, par défaut, pour sécuriser le trafic StorageGRID interne. Une autorité de certification (CA) externe peut émettre des certificats personnalisés entièrement conformes aux politiques de sécurité des informations de votre organisation. Bien que vous puissiez utiliser le certificat Grid CA pour un environnement hors production, 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 CA personnalisés 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 répondre aux"directives 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 regroupement de certificats d'autorité de certification).

> ⓘ StorageGRID inclut également des certificats d'autorité de certification du système d'exploitation qui sont les mêmes 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 CA du système d'exploitation.

Les variantes des types de certificats serveur et client sont implémentées de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID spécifique avant de configurer

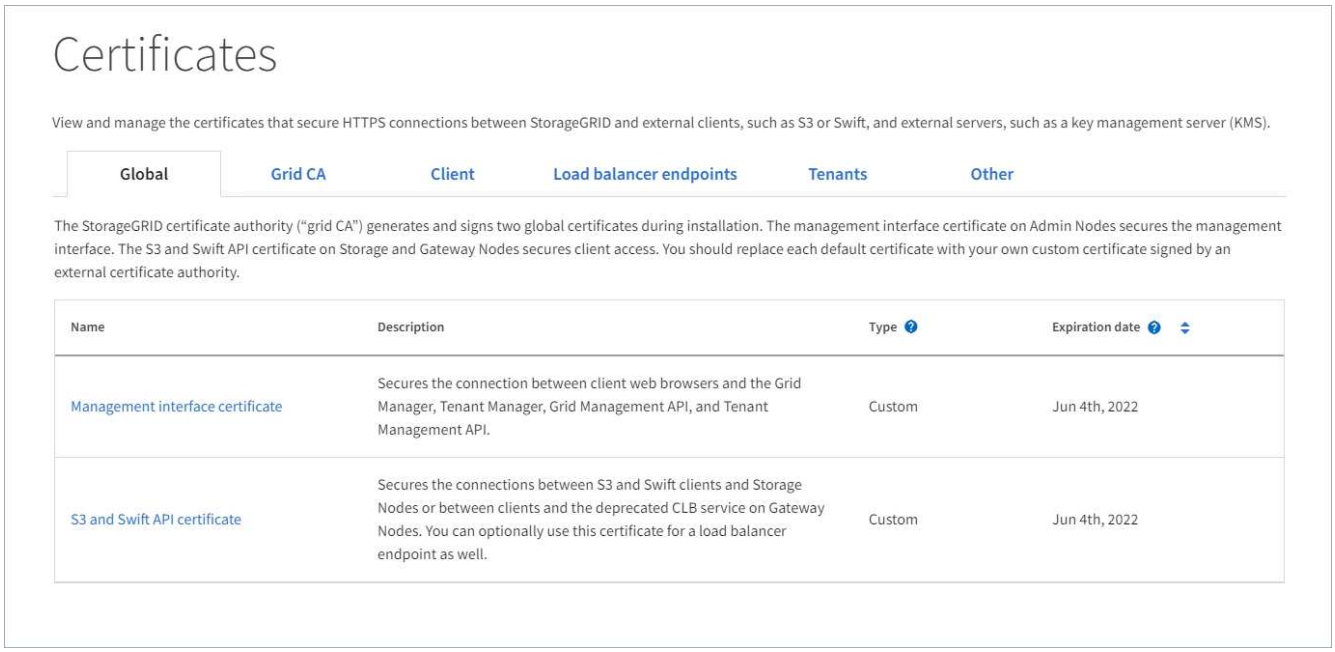
le système.

Accéder aux certificats de sécurité

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

Étapes

1. Depuis le Gestionnaire de grille, 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 des navigateurs Web et des 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 de terminaison de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et l'équilibreur de charge StorageGRID .
   - * Locataires * : sécurise les connexions aux serveurs de fédération d'identité ou des points de terminaison de service de la plateforme 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 à StorageGRID à partir des navigateurs Web et des clients API S3 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 d'interface de gestion: Sécurise les connexions du navigateur Web client aux interfaces de gestion StorageGRID .
- Certificat API S3:Sécurise les connexions API client aux nœuds de stockage, aux nœuds d'administration et aux nœuds de passerelle, que les applications client S3 utilisent pour télécharger et charger des données d'objet.

Les informations sur les certificats globaux installés incluent :

- **Nom** : Nom du certificat avec lien pour gérer le certificat.
- **Description**
- **Type** : Personnalisé ou par défaut. + Vous devez toujours utiliser un certificat personnalisé pour améliorer la sécurité du réseau.
- **Date d'expiration** : Si vous utilisez le certificat par défaut, aucune date d'expiration n'est affichée.

Tu peux:

- Remplacez les certificats par défaut par des certificats personnalisés signés par une autorité de certification externe pour améliorer la sécurité de la grille :
  - "Remplacer le certificat d'interface de gestion généré par StorageGRID par défaut"utilisé pour les connexions Grid Manager et Tenant Manager.
  - "Remplacer le certificat API S3"utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (facultatif).
- "Restaurer le certificat d'interface de gestion par défaut" .
- "Restaurer le certificat API S3 par défaut" .
- "Utiliser un script pour générer un nouveau certificat d'interface de gestion auto-signé" .
- Copiez ou téléchargez le"certificat d'interface de gestion" ou"Certificat API S3" .

Grille CA

LeCertificat Grid CA , généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID , sécurise tout le trafic interne de StorageGRID .

Les informations du certificat incluent la date d'expiration du certificat et le contenu du certificat.

Tu peux"copier ou télécharger le certificat Grid CA" , mais tu ne peux pas le changer.

Client

Certificats clients, généré par une autorité de certification externe, sécurise les connexions entre les outils de surveillance externes et la base de données StorageGRID Prometheus.

La table des certificats comporte 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.

Tu peux:

- "Téléchargez ou générez un nouveau certificat client."
- Sélectionnez un nom de certificat pour afficher les détails du certificat où vous pouvez :
  - "Modifier le nom du certificat client."
  - "Définissez l'autorisation d'accès Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimer le certificat client."
- Sélectionnez **Actions** pour rapidement"modifier" ,"attacher" , ou"retirer" un certificat client. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément en utilisant **Actions** > **Supprimer**.

Points de terminaison de l'équilibreur de charge

Certificats de point de terminaison d'équilibrage de chargesécurisez les connexions entre les clients S3 et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration.

La table des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison de l'équilibreur de charge configuré et indique si le certificat API S3 global ou un certificat de point de terminaison de l'équilibreur de charge personnalisé est utilisé pour le point de terminaison. La date d'expiration de chaque certificat est également affichée.

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

Tu peux:

- "Afficher un point de terminaison d'équilibrage de charge", y compris les détails de son certificat.
- "Spécifiez un certificat de point de terminaison d'équilibrage de charge pour FabricPool."
- "Utiliser le certificat API S3 global"au lieu de générer un nouveau certificat de point de terminaison d'équilibrage de charge.

Locataires

Les locataires peuvent utilisercertificats de serveur de fédération d'identité oucertificats de point de terminaison de service de plateforme pour sécuriser leurs connexions avec StorageGRID.

La table des locataires comporte une ligne pour chaque locataire et indique si chaque locataire est autorisé à utiliser sa propre source d'identité ou ses propres services de plateforme.

Tu peux:

- "Sélectionnez un nom de locataire pour vous connecter au gestionnaire de locataires"
- "Sélectionnez un nom de locataire pour afficher les détails de la fédération d'identité du locataire"
- "Sélectionnez un nom de locataire pour afficher les détails des services de la plateforme locataire"
- "Spécifier un certificat de point de terminaison de service de plateforme lors de la création du point de terminaison"

Autre

StorageGRID utilise d'autres certificats de sécurité à des fins spécifiques. Ces certificats sont répertoriés par leur nom fonctionnel. D'autres certificats de sécurité incluent :

- Certificats Cloud Storage Pool
- Certificats de notification d'alerte par courrier électronique
- Certificats de serveur syslog externes
- Certificats de connexion à la fédération de réseau
- Certificats de fédération d'identité
- Certificats du serveur de gestion de clés (KMS)
- Certificats d'authentification unique

Les informations indiquent le type de certificat utilisé par une fonction ainsi que les dates d'expiration de ses certificats serveur et 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 des autres certificats que si vous disposez des droits d'accès."autorisation appropriée" .

Tu peux:

- "Spécifier un certificat de pool de stockage cloud pour S3, C2S S3 ou Azure"
- "Spécifier un certificat pour les notifications d'alerte par e-mail"
- "Utiliser un certificat pour un serveur syslog externe"
- "Faire pivoter les certificats de connexion à la fédération de réseau"
- "Afficher et modifier un certificat de fédération d'identité"
- "Télécharger les certificats du serveur de gestion des clés (KMS) et du client"
- "Spécifier manuellement un certificat SSO pour une approbation de partie de confiance"

Détails du certificat de sécurité

Chaque type de certificat de sécurité est décrit ci-dessous, avec des liens vers les instructions de mise en œuvre.

Certificat d'interface de gestion

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les navigateurs Web clients et l'interface de gestion StorageGRID , permettant aux utilisateurs d'accéder à Grid Manager et Tenant Manager sans avertissements de sécurité. Ce certificat authentifie également les connexions à l'API Grid Management et à l'API Tenant Management. 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 sélectionnez **Certificat d'interface de gestion**	"Configurer les certificats de l'interface de gestion"

Certificat API S3

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie les connexions client S3 sécurisées à un nœud de stockage et aux points de terminaison de l'équilibreur de charge (facultatif).	**CONFIGURATION** > **Sécurité** > **Certificats**, sélectionnez l'onglet **Global**, puis sélectionnez **Certificat API S3**	"Configurer les certificats API S3"

Certificat Grid CA

Voir leDescription du certificat Grid CA par défaut .

Certificat 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. • Permet une surveillance sécurisée de StorageGRID à l'aide d'outils externes.	**CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Client**	"Configurer les certificats clients"

Certificat de point de terminaison de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les clients S3 et le service d'équilibrage de charge StorageGRID 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 point de terminaison d'équilibreur de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet. Vous pouvez également utiliser une version personnalisée du globalCertificat API S3 certificat pour 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 point de terminaison 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 StorageGRID .	**CONFIGURATION** > **Réseau** > **Points de terminaison de l'équilibreur de charge**	• "Configurer les points de terminaison de l'équilibreur de charge" • "Créer un point de terminaison d'équilibrage de charge pour FabricPool"

Certificat de point de terminaison du pool de stockage cloud

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

Certificat de notification d'alerte par courrier électronique

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 Transport Layer Security (TLS), vous devez spécifier le certificat d'autorité de certification du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP requiert des certificats clients pour l'authentification.	**ALERTES** > **Configuration de la messagerie électronique**	"Configurer des 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 enregistre 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 à la fédération de réseau

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et cryptez 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 tourner les certificats de connexion"

Certificat de fédération d'identité

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 d'identité, qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	**CONFIGURATION** > **Contrôle d'accès** > **Fédération d'identité**	"Utiliser la fédération d'identité"

Certificat du serveur de gestion de clés (KMS)

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

Certificat de point de terminaison des services de plateforme

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion du service de plateforme StorageGRID à une ressource de stockage S3.	**Gestionnaire de locataires** > **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**	"Créer un point de terminaison des services de plateforme" "Modifier le point de terminaison des services de la plateforme"

Certificat d'authentification unique (SSO)

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion entre les services de fédération d'identité, tels que les services de fédération Active Directory (AD FS) et StorageGRID qui sont utilisés pour les demandes d'authentification unique (SSO).	**CONFIGURATION** > **Contrôle d'accès** > **Authentification unique**	"Configurer l'authentification unique"

Exemples de certificats

Exemple 1 : service d'équilibrage de charge

Dans cet exemple, StorageGRID agit comme serveur.

1. Vous configurez un point de terminaison d'équilibrage de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 au point de terminaison de l'équilibreur de charge et téléchargez le même certificat sur le 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 avec une signature basée sur la clé privée.
5. Le client vérifie ce certificat en comparant la signature du serveur à la signature sur sa copie du certificat. Si les signatures correspondent, le client démarre une session en utilisant la même clé publique.
6. Le client envoie des données d'objet à StorageGRID.

Exemple 2 : Serveur de gestion de clés externe (KMS)

Dans cet exemple, StorageGRID agit en tant que client.

1. À l'aide d'un logiciel de gestion de clés externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat de serveur signé par une autorité de certification, un certificat client public et la clé privée du certificat client.
2. À l'aide du gestionnaire de grille, 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 demande 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 en utilisant la connexion validée.

Types de certificats de serveur pris en charge

Le système StorageGRID prend en charge les certificats personnalisés chiffrés avec RSA ou ECDSA (Elliptic Curve Digital Signature Algorithm).

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

Pour plus d'informations sur la manière dont StorageGRID sécurise les connexions client, consultez"Sécurité pour les clients S3" .

Configurer les certificats de l'interface de gestion

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un seul certificat personnalisé qui permet aux utilisateurs d'accéder au gestionnaire de grille et au gestionnaire de locataires sans rencontrer d'avertissements de sécurité. Vous pouvez également revenir au certificat d'interface de gestion par défaut ou en générer un nouveau.

À propos de cette tâche

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

Étant donné qu'un seul certificat d'interface de gestion personnalisé est utilisé pour tous les nœuds d'administration, vous devez spécifier le certificat comme certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au gestionnaire de grille et au gestionnaire de locataires. 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 (CA) que vous utilisez, les utilisateurs peuvent également avoir besoin d'installer le certificat Grid CA dans le navigateur Web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.

> Pour garantir que les opérations ne sont pas perturbées 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 voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

> Si vous accédez au Grid Manager ou au Tenant Manager 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'une des situations suivantes se produit :
>
> - Votre certificat d'interface de gestion personnalisée expire.
> - Toirevenir d'un certificat d'interface de gestion personnalisé au certificat de serveur par défaut .

Ajouter un certificat d'interface de gestion personnalisé

Pour ajouter un certificat d'interface de gestion personnalisé, vous pouvez fournir votre propre certificat ou en générer un à l'aide du gestionnaire de grille.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez 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** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

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

c. Développez **Détails du certificat** pour voir 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 bundle CA** pour enregistrer le bundle 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 **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

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

Générer un certificat

Générer les fichiers de certificat du serveur.

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

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

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

Champ	Description
propriété intellectuelle	Une ou plusieurs adresses IP à inclure dans le certificat.
Sujet (facultatif)	Sujet 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 adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour voir 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 afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**. + Le certificat d'interface de gestion personnalisé est utilisé pour toutes les nouvelles connexions ultérieures au Grid Manager, au Tenant Manager, à l'API Grid Manager ou à l'API Tenant Manager.

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

> Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

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

Restaurer le certificat d'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 **Certificat d'interface de gestion**.
3. Sélectionnez **Utiliser le certificat par défaut**.

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

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

Utiliser 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

- Tu as"autorisations d'accès spécifiques" .
- Vous avez le `Passwords.txt` déposer.

À propos de cette 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. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
   b. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.
   c. Entrez la commande suivante pour passer en root : `su -`
   d. Entrez le mot de passe indiqué dans le `Passwords.txt` déposer.

      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` .
   - Ensemble `--type` à `management` pour configurer le certificat d'interface de gestion, qui est utilisé par Grid Manager et Tenant Manager.

◦ Par défaut, les certificats générés sont valables 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 lorsque `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 risque de rejeter le certificat.

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

La sortie résultante contient le certificat public nécessaire à votre client API de gestion.

4. Sélectionnez et copiez le certificat.

   Incluez les balises BEGIN et END dans votre sélection.

5. Déconnectez-vous de l'interpréteur de commandes. `$ exit`
6. Confirmer que le certificat a été configuré :
   a. Accéder au gestionnaire de grille.
   b. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**
   c. Dans l'onglet **Global**, sélectionnez **Certificat d'interface de gestion**.
7. Configurez votre client de gestion pour utiliser le certificat public que vous avez copié. Inclure les balises BEGIN et END.

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 **Certificat d'interface de gestion**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

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

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

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 ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification 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`

Configurer les certificats API S3

Vous pouvez remplacer ou restaurer le certificat de serveur utilisé pour les connexions client S3 aux nœuds de stockage ou aux points de terminaison de l'équilibreur de charge. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Les détails Swift ont été supprimés de cette version du site de documentation. Voir "StorageGRID 11.8 : Configurer les certificats API S3 et Swift" .

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat de serveur X.509 signé par l'autorité de certification de la grille. Ces certificats signés par une 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 certificat générique ou multi-domaine si les clients doivent vérifier le nom d'hôte lors de la connexion au point de terminaison de stockage. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds de stockage de la grille.

Une fois la configuration sur le serveur terminée, vous devrez peut-être également installer le certificat Grid CA dans le client API S3 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 perturbées par un certificat de serveur défaillant, l'alerte **Expiration du certificat de serveur global pour l'API S3** est déclenchée lorsque le certificat du serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat API S3 personnalisé.

Ajouter un certificat API S3 personnalisé

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez 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** : Le fichier de certificat de serveur personnalisé (codé PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat du serveur personnalisé(`.key`).

> Les clés privées EC doivent être de 224 bits ou plus. Les clés privées RSA doivent être de 2 048 bits ou plus.

- **CA bundle** : un fichier facultatif unique contenant les certificats de chaque autorité de certification émettrice intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA codés 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 personnalisé qui a été 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 bundle CA** pour enregistrer le bundle 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 **Copier le certificat PEM** ou **Copier le bundle CA PEM** pour copier le contenu du certificat afin de le coller ailleurs.

d. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

Générer un certificat

Générer les fichiers de certificat du serveur.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

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

Champ	Description
Sujet (facultatif)	Sujet 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 adresse IP comme nom commun du sujet (CN).
Jours de validité	Nombre de jours après la création pendant lesquels le certificat expire.
Ajouter des extensions d'utilisation de clés	Si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent l'objectif de la clé contenue dans le certificat. **Remarque** : laissez cette case à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat API S3 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 afin de le coller ailleurs.

e. Sélectionnez **Enregistrer**.

Le certificat de serveur personnalisé est utilisé pour les nouvelles connexions client S3 ultérieures.

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

> Après avoir téléchargé ou généré un nouveau certificat, prévoyez jusqu'à un jour pour que les alertes d'expiration de certificat associées disparaissent.

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

Restaurer le certificat API S3 par défaut

Vous pouvez revenir à l'utilisation du certificat API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat API S3 par défaut pour un point de terminaison d'équilibreur de charge.

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez **Utiliser le certificat par défaut**.

   Lorsque vous restaurez la version par défaut du certificat API S3 global, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés à partir du système. Le certificat API S3 par défaut sera utilisé pour les nouvelles connexions client S3 ultérieures aux nœuds de stockage.

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

   Si vous disposez de l'autorisation d'accès racine et que le certificat API S3 personnalisé a été utilisé pour les connexions aux points de terminaison de l'équilibreur de charge, une liste des points de terminaison de l'équilibreur de charge qui ne seront plus accessibles à l'aide du certificat API S3 par défaut s'affiche. Aller à"Configurer les points de terminaison de l'équilibreur de charge" pour modifier ou supprimer les points de terminaison affectés.

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

Téléchargez ou copiez le certificat API S3

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **Certificat API S3**.
3. Sélectionnez l'onglet **Serveur** ou **Pack CA**, puis téléchargez ou copiez le certificat.

Télécharger le fichier de certificat ou le bundle CA

Téléchargez le certificat ou le bundle CA `.pem` déposer. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

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

   Si vous téléchargez un bundle CA, tous les certificats des onglets secondaires du bundle CA sont téléchargés sous forme de fichier unique.

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 ou le bundle CA PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble d'autorités de certification facultatif, chaque certificat de l'ensemble s'affiche dans son propre sous-onglet.

a. Sélectionnez **Copier le certificat PEM** ou **Copier le bundle CA PEM**.

   Si vous copiez un bundle d'autorités de certification, tous les certificats des onglets secondaires du bundle d'autorités de certification 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 connexes

- "Utiliser l'API REST S3"
- "Configurer les noms de domaine des points de terminaison S3"

Copier le certificat Grid CA

StorageGRID utilise une autorité de certification interne (CA) 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" .
- Tu as"autorisations d'accès spécifiques" .

À propos de cette tâche

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l'onglet **Grid CA**.

2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

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`

Configurer les certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lorsque vous configurez le point de terminaison de l'équilibreur de charge.

Avant de commencer

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

À propos de cette tâche

Lorsque vous créez un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat de serveur auto-signé ou télécharger un certificat signé par une autorité de certification (CA) 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 renouvelés sans interruption. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type « man-in-the-middle ».

Les étapes suivantes fournissent des directives générales pour les clients S3 qui utilisent FabricPool. Pour des informations et des procédures plus détaillées, voir"Configurer StorageGRID pour FabricPool" .

Étapes

1. Vous pouvez également configurer un groupe de haute disponibilité (HA) à utiliser par FabricPool .
2. Créez un point de terminaison d'équilibrage de charge S3 à utiliser par FabricPool .

Lorsque vous créez un point de terminaison d'équilibrage de charge HTTPS, vous êtes invité à télécharger votre certificat de serveur, votre clé privée de certificat et votre ensemble d'autorités de certification facultatif.

3. Attachez StorageGRID en tant que niveau cloud dans ONTAP.

   Spécifiez le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat CA que vous avez téléchargé. Ensuite, fournissez le certificat CA.

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

Configurer les certificats clients

Les certificats clients permettent aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus, offrant ainsi un moyen sécurisé aux outils externes de surveiller 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 du Grid Manager et copier les informations du certificat sur l'outil externe.

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

> Pour garantir que les opérations ne sont pas perturbées par un certificat de serveur défaillant, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **CONFIGURATION** > **Sécurité** > **Certificats** et en regardant la date d'expiration du certificat client dans l'onglet Client.

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

Avant de commencer

- Vous disposez de l'autorisation d'accès root.
- 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 d'interface de gestion StorageGRID , vous disposez de l'autorité de certification, du certificat client et de la clé privée utilisés pour configurer le certificat d'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 sauvegardée ou enregistrée au moment de sa création. Si vous ne disposez pas de 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 clients

Pour ajouter le certificat client, utilisez l'une de ces procédures :

- Certificat d'interface de gestion déjà configuré
- Certificat client émis par l'AC
- Certificat généré à partir de 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, d'un certificat client et d'une clé privée fournis par le client.

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 métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
5. Sélectionnez **Continuer**.
6. Pour l'étape **Joindre les certificats**, téléchargez le certificat de l'interface de gestion.
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Parcourir** 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 PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Le nouveau certificat apparaît dans l'onglet Client.
7. Configurer un outil de surveillance externe, comme Grafana.

Certificat client émis par l'AC

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

Étapes

1. Effectuez les étapes pour"configurer 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 métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle CA :
   a. Sélectionnez **Télécharger le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez le certificat client, la clé privée et les fichiers groupés de l'autorité de certification(`.pem`).
      - Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.
      - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de le coller ailleurs.
   c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

      Les nouveaux certificats apparaissent dans l'onglet Client.
8. Configurer un outil de surveillance externe, comme Grafana.

Certificat généré à partir de Grid Manager

Utilisez cette procédure pour ajouter un certificat client administrateur si aucun certificat d'interface de gestion n'a été configuré et que vous prévoyez d'ajouter un certificat client pour Prometheus qui utilise la fonction de génération de 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 métriques 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 du certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et 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 à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

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

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

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de 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 du certificat afin de la coller ailleurs.
   - Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de 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 dans 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 un certificat personnalisé**.
14. Téléchargez les fichiers certificate.pem et private_key.pem depuis ledétails du certificat client étape. Il n'est pas nécessaire de télécharger le bundle CA.
    a. Sélectionnez **Télécharger le certificat** puis sélectionnez **Continuer**.
    b. Téléchargez chaque fichier de certificat(`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans le gestionnaire de grille.

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

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

Configurer un outil de surveillance externe

Étapes

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

      StorageGRID ne nécessite 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 nœud d'administration. Spécifiez HTTPS et le port 9091.

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

c. Activez **TLS Client Auth** et **Avec certificat CA**.

d. Sous Détails d'authentification TLS/SSL, copiez et collez :
   - L'interface de gestion du certificat CA vers **CA Cert**
   - Le certificat client de **Client Cert**
   - La clé privée de **Clé client**

e. **ServerName**: saisissez le nom de domaine du nœud d'administration.

   ServerName 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 pouvez désormais accéder aux métriques Prometheus depuis StorageGRID avec votre outil de surveillance externe.

   Pour plus d'informations sur les mesures, consultez le"instructions pour la surveillance de StorageGRID" .

Modifier les certificats clients

Vous pouvez modifier un certificat client administrateur pour changer son nom, activer ou désactiver l'accès à 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 que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez **Modifier le nom et l'autorisation**
4. Entrez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser Prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le gestionnaire de grille.

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

Joindre un nouveau certificat client

Vous pouvez 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 que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis sélectionnez une option de modification.

Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

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

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

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

   - 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 afin de 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.

Générer un certificat

Générez le texte du certificat à coller ailleurs.

a. Sélectionnez **Générer un certificat**.

b. Spécifiez les informations du certificat :

   - **Sujet** (facultatif) : sujet X.509 ou nom distinctif (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à compter du moment où il est généré.
   - **Ajouter des extensions d'utilisation de clé** : si cette option est sélectionnée (par défaut et recommandé), les extensions d'utilisation de clé et 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 à cocher sélectionnée, sauf si vous rencontrez des problèmes de connexion avec des clients plus anciens lorsque les certificats incluent ces extensions.

c. Sélectionnez **Générer**.

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

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

   - Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat afin de 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 du certificat afin de la coller ailleurs.
- Sélectionnez **Télécharger la clé privée** pour enregistrer la clé privée sous forme de 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 dans l'onglet Client.

Télécharger ou copier les certificats clients

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.

Télécharger le fichier de certificat

Télécharger le certificat `.pem` déposer.

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

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 clients

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

Étapes

1. Sélectionnez **CONFIGURATION** > **Sécurité** > **Certificats** puis sélectionnez l’onglet **Client**.
2. Sélectionnez le certificat que vous souhaitez 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**.

Une fois un certificat supprimé, les clients qui ont utilisé le certificat doivent spécifier un nouveau certificat client pour accéder à la base de données StorageGRID Prometheus.

Informations sur le copyright

Informations sur les marques commerciales