Gérer les certificats

StorageGRID software

NetApp
July 23, 2026

Sommaire

Gérer les certificats

Gérer les certificats de sécurité dans StorageGRID

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 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 compare 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 CA Grid par défaut

StorageGRID intègre une autorité de certification (CA) qui génère un certificat Grid CA interne lors de l'installation du système. Le certificat Grid CA est utilisé par défaut pour sécuriser le trafic interne de StorageGRID. Une autorité de certification (CA) externe peut émettre des certificats personnalisés, entièrement conformes aux politiques de sécurité informatique de votre organisation.

Utilisez le certificat de l'autorité de certification Grid pour les environnements hors production. Pour la production, utilisez des certificats personnalisés signés par une autorité de certification externe. Les connexions non sécurisées sans certificat sont prises en charge, mais ne sont pas recommandées.

- Les certificats d'autorité de certification personnalisés ne remplacent pas les certificats internes ; toutefois, ce sont les certificats personnalisés qui doivent être spécifiés pour vérifier les connexions au serveur.
- Tous les certificats personnalisés doivent respecter les "Recommandations de renforcement du système pour les certificats de serveur".
- StorageGRID prend en charge le regroupement des certificats d'une autorité de certification dans un seul fichier (appelé ensemble de certificats d'une autorité de certification).

> ⓘ StorageGRID inclut également des certificats d'autorité de certification (CA) du système d'exploitation, identiques sur toutes les grilles. En environnement de production, veillez à spécifier un certificat personnalisé signé par une autorité de certification externe, en remplacement du certificat CA du système d'exploitation.

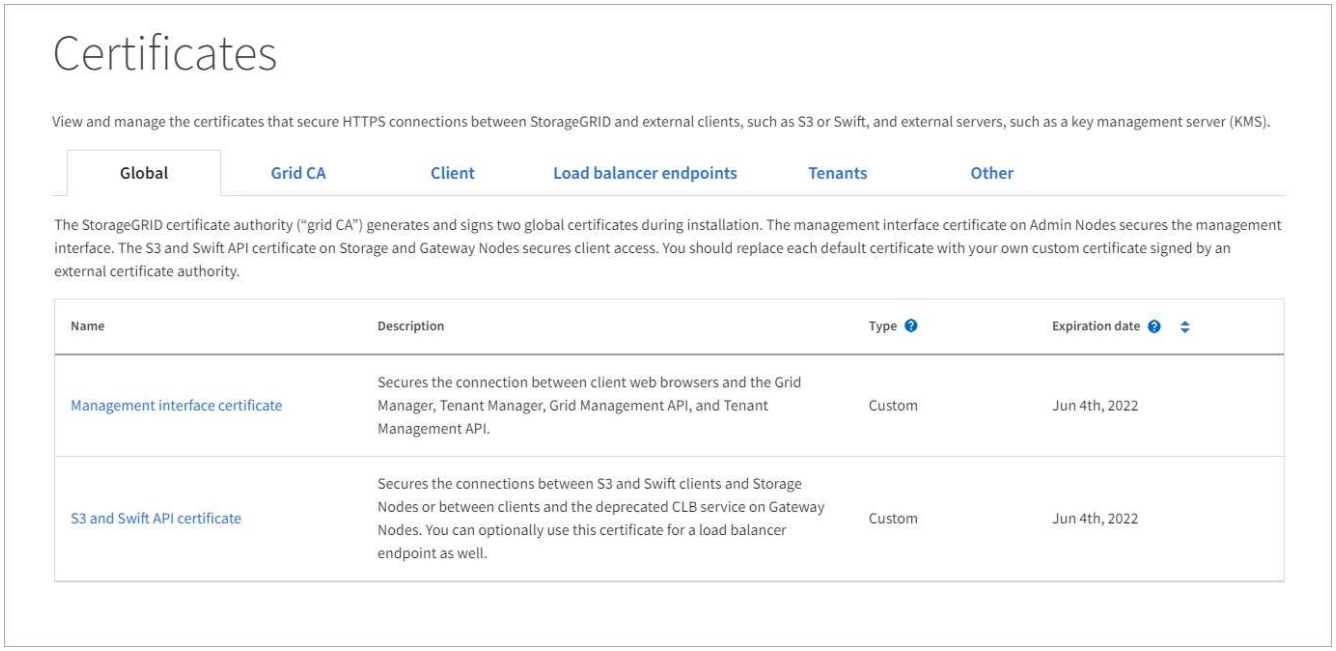
Les différents types de certificats serveur et client sont implémentés de plusieurs manières. Vous devez disposer de tous les certificats nécessaires à votre configuration StorageGRID avant de configurer le système.

Certificats de sécurité d’accès

Vous pouvez accéder aux informations concernant tous les certificats StorageGRID en un seul endroit, ainsi qu’aux liens vers le flux de travail de configuration de chaque certificat.

Étapes

1. Dans Grid Manager, sélectionnez **Configuration** > **Security** > **Certificates**.



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

   - **Global** : Sécurise l’accès à StorageGRID depuis les navigateurs web et les clients API externes.
   - **Autorité de certification Grid** : Sécurise le trafic interne de StorageGRID.
   - **Client** : Sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
   - **Points de terminaison de l’équilibreur de charge** : Sécurisent les connexions entre les clients S3 et l’équilibreur de charge StorageGRID.
   - **Locataires** : Sécurise les connexions aux serveurs de fédération d’identité ou depuis les points de terminaison de service de la plateforme vers les 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 supplémentaires sur le certificat.

Global

Les certificats globaux sécurisent l'accès à StorageGRID depuis les navigateurs web et les clients API S3 externes. Deux certificats globaux sont initialement générés par l'autorité de certification StorageGRID lors de l'installation. La bonne 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 des navigateurs web clients 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 clientes S3 utilisent pour charger et télécharger des données d'objet.

Les informations relatives aux 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 une sécurité renforcée de la grille :
  - "Remplacez le certificat d'interface de gestion généré par défaut par StorageGRID" Utilisé pour les connexions de Grid Manager et de Tenant Manager.
  - "Remplacez le certificat de l'API S3"utilisé pour les connexions au nœud de stockage et au point de terminaison de l'équilibreur de charge (optionnel).
- "Restaurez le certificat d'interface de gestion par défaut".
- "Restaurez le certificat d'API S3 par défaut".
- "Utilisez 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".

Grid CA

Le Certificat d'autorité de certification Grid généré par l'autorité de certification StorageGRID lors de l'installation de StorageGRID, sécurise tout le trafic interne de StorageGRID.

Les informations relatives au certificat comprennent la date d'expiration du certificat et le contenu du certificat.

Vous pouvez "Copiez ou téléchargez le certificat Grid CA", mais vous ne pouvez pas le changer.

Client

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

Le tableau 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 sa date d'expiration.

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 les autorisations d'accès à Prometheus."
  - "Téléchargez et remplacez le certificat client."
  - "Copiez ou téléchargez le certificat client."
  - "Supprimez le certificat client."
- Sélectionnez **Actions** pour "modifier", "attacher" ou "retirer" un certificat client rapidement. Vous pouvez sélectionner jusqu'à 10 certificats clients et les supprimer simultanément via **Actions** > **Supprimer**.

points de terminaison de l'équilibreur de charge

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

Le tableau des points de terminaison de l'équilibreur de charge comporte une ligne pour chaque point de terminaison configuré et indique si le certificat d'API S3 global ou un certificat personnalisé de point de terminaison d'équilibreur de charge 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.

Vous pouvez :

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

locataires

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

Le tableau 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.

Vous pouvez :

- "Sélectionnez un nom de locataire pour vous connecter au Tenant Manager"
- "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 du locataire"
- "Spécifiez 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. Les autres certificats de sécurité incluent :

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

Les informations indiquent le type de certificat qu'une fonction utilise ainsi que les dates d'expiration de ses certificats serveur et client, le cas échéant. Sélectionner un nom de fonction ouvre un onglet du navigateur où vous pouvez consulter et modifier les détails du certificat.

> Vous ne pouvez consulter et accéder aux informations des autres certificats que si vous disposez du "autorisation appropriée".

Vous pouvez :

- "Spécifiez un certificat de Cloud Storage Pool 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"
- "Faites pivoter les certificats de connexion à la fédération de grille"
- "Afficher et modifier un certificat de fédération d'identité"
- "Téléversez les certificats serveur et client du serveur de gestion des clés (KMS)"
- "Spécifiez manuellement un certificat SSO pour une relation d'approbation de partie utilisatrice"

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 au Grid Manager et au Tenant Manager sans avertissement de sécurité. Ce certificat authentifie également les connexions à l'API de gestion de la grille et à 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 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 **S3 API certificate**	"Configurer les certificats de l'API S3"

Certificat d'autorité de certification Grid

Voir la Description du certificat d'autorité de certification Default Grid.

Certificat client administrateur

Type de certificat	Description	Emplacement de navigation	Détails
Client	Installé sur chaque client, il permet à StorageGRID d'authentifier l'accès des clients externes. • Permet aux clients externes autorisés d'accéder à la base de données Prometheus de StorageGRID. • 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'équilibrage de charge lors de la configuration d'un point de terminaison d'équilibrage de charge. Les applications clientes utilisent le certificat d'équilibrage de charge lors de la connexion à StorageGRID pour enregistrer et récupérer des données d'objets. Vous pouvez également utiliser une version personnalisée du Certificat API S3 certificat global pour authentifier les connexions au service de Load Balancer. Si le certificat global est utilisé pour authentifier les connexions au Load Balancer, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque point de terminaison du Load Balancer. **Remarque :** Le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus fréquemment utilisé lors du 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 Cloud Storage Pool

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	Authentifie la connexion d'un StorageGRID Cloud Storage Pool à un emplacement de stockage externe, tel que S3 Glacier ou Microsoft Azure Blob storage. 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 courriel

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID qui est 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 (CA) du serveur de messagerie. • Spécifiez un certificat client uniquement si le serveur de messagerie SMTP exige des certificats clients pour l'authentification.	**Alertes** > **Configuration des e-mails**	"Configurer 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 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 de syslog**	"Utilisez un serveur syslog externe"

Certificat de connexion à la fédération Grid

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifiez et chiffrez les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grilles.	**Configuration** > **Système** > **Fédération de grilles**	• "Créer des connexions de fédération de grille" • "Rotation des 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, ce qui permet aux groupes d'administrateurs et aux utilisateurs d'être gérés par un système externe.	**Configuration** > **Contrôle d'accès** > **Fédération d'identité**	"Utilisez la fédération d'identités"

certificat de 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 des 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.	**Tenant Manager** > **STOCKAGE (S3)** > **Points de terminaison des services de plateforme**	"Créer un point de terminaison de services de plateforme" "Modifier le point de terminaison des services de 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 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 fait office de 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 téléversez 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 via 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 compare la signature du serveur à celle figurant sur sa copie du certificat. Si les signatures correspondent, le client établit 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 fait office de client.

1. À l'aide d'un logiciel Key Management Server externe, vous configurez StorageGRID en tant que client KMS et obtenez un certificat serveur signé par une autorité de certification (CA), un certificat client public et la clé privée du 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 des 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 serveur pris en charge dans StorageGRID

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 "rétablir temporairement 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".

Configurez les certificats d'interface de gestion dans StorageGRID

Vous pouvez remplacer le certificat d'interface de gestion par défaut par un certificat personnalisé unique permettant aux utilisateurs d'accéder au Grid Manager et au Tenant Manager sans rencontrer d'avertissements de sécurité. Vous pouvez également rétablir le 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 la CA du grid. Ces certificats signés par

la CA peuvent être remplacés par un certificat d'interface de gestion personnalisé commun 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 un certificat générique ou multidomaine si les clients doivent vérifier le nom d'hôte lors de la connexion au Grid Manager et au Tenant Manager. Définissez le certificat personnalisé de manière à ce qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez effectuer la configuration sur le serveur et, selon l'autorité de certification racine (CA) que vous utilisez, les utilisateurs devront peut-être également installer le certificat de l'autorité de certification Grid dans le navigateur web qu'ils utiliseront pour accéder au Grid Manager et au Tenant Manager.

Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration du certificat serveur pour l'interface de gestion** est déclenchée lorsque ce certificat est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en vérifiant la date d'expiration du certificat de l'interface de gestion dans l'onglet Global.

Si vous accédez au Gestionnaire de grille 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 possibilité de contournement si l'une des situations suivantes se produit :

- Votre certificat d'interface de gestion personnalisée expire.
- Vousrevenir d'un certificat d'interface de gestion personnalisé au certificat du 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 de Grid Manager.

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

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé (encodé au format PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **CA bundle** : Fichier optionnel unique contenant les certificats de chaque autorité de certification (CA) intermédiaire. Le fichier doit contenir chacun des fichiers de certificat CA encodés en 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 importé. Si vous avez importé un ensemble CA optionnel, chaque certificat s'affiche dans 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 son 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

Générez les fichiers de certificat du serveur.

> La bonne 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 complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : 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 **Générer**.

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 son 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 une journée pour que les alertes d'expiration de certificat associées disparaissent.

6. Après avoir ajouté un certificat d'interface de gestion personnalisé, la page du certificat d'interface de gestion affiche des informations détaillées sur les certificats utilisés. Vous pouvez télécharger ou copier le PEM du certificat si nécessaire.

Restaurez 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 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 ultérieures.

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

À propos de cette tâche

La bonne 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. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.
   c. Saisissez la commande suivante pour passer en mode superutilisateur : `su -`
   d. Saisissez le mot de passe indiqué dans le fichier `Passwords.txt`.

      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`.
   - Définissez `--type` sur `management` pour configurer le certificat de l'interface de gestion, utilisé par Grid Manager et Tenant Manager.
   - Par défaut, les certificats générés sont valides pendant un an (365 jours) et doivent être recréés avant leur expiration. Vous pouvez utiliser l'argument `--days` pour remplacer la période de validité par

défaut.

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

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

Le résultat obtenu 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'invite de commandes. `$ 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 **Certificat d'interface de gestion**.
7. Configurez votre client de gestion pour qu'il utilise le certificat public que vous avez copié. Incluez les balises BEGIN et END.

Téléchargez ou copiez le certificat de l'interface de gestion

Vous pouvez enregistrer ou copier le contenu du certificat d'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 **CA bundle**, puis téléchargez ou copiez le certificat.

Téléchargez le fichier de certificat ou le bundle CA

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

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

   Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble CA optionnel, 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 ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble 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 d'API S3 dans StorageGRID

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

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

À propos de cette tâche

Par défaut, chaque nœud de stockage reçoit un certificat serveur X.509 signé par la CA du grid. Ces certificats signés par la CA peuvent être remplacés par un certificat serveur personnalisé unique et la clé privée correspondante.

Un seul certificat serveur personnalisé est utilisé pour tous les nœuds de stockage, donc vous devez spécifier le certificat comme un 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 du 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 éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte « Expiration du certificat serveur global pour l'API S3 » est déclenchée lorsque le certificat racine du serveur est sur le point d'expirer. Si nécessaire, vous pouvez voir quand le certificat actuel expire en sélectionnant **Configuration** > **Sécurité** > **Certificats** et en consultant la date d'expiration du certificat de l'API S3 dans l'onglet Global.

Vous pouvez télécharger ou générer un certificat d'API S3 personnalisé.

Ajouter un certificat d'API S3 personnalisé

Étapes

1. Sélectionnez **Configuration** > **Sécurité** > **Certificats**.
2. Dans l'onglet **Global**, sélectionnez **S3 API certificate**.
3. Sélectionnez **Utiliser un certificat personnalisé**.
4. Téléchargez ou générez le certificat.

Télécharger le certificat

Téléversez les fichiers de certificat serveur requis.

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé (encodé au format PEM).
- **Clé privée du certificat** : Le fichier de clé privée du certificat de serveur personnalisé (`.key`).

> Les clés privées EC doivent comporter au moins 224 bits. Les clés privées RSA doivent comporter au moins 2048 bits.

- **Ensemble d'autorités de certification (CA bundle)** : Fichier optionnel unique contenant les certificats de chaque autorité de certification intermédiaire. Le fichier doit contenir chaque fichier de certificat d'autorité de certification au format PEM, concaténés dans l'ordre de la chaîne de certificats.

c. Sélectionnez les détails du certificat pour afficher les métadonnées et le PEM de chaque certificat d'API S3 personnalisé que vous avez chargé. Si vous avez chargé un bundle CA optionnel, chaque certificat s'affiche dans 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 son 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 serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

Générer un certificat

Générez 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 complet à inclure dans le certificat. Utilisez un astérisque (*) comme caractère générique pour représenter plusieurs noms de domaine.
IP	Une ou plusieurs adresses IP à inclure dans le certificat.

Champ	Description
Sujet (facultatif)	Sujet X.509 ou nom unique (DN) du propriétaire du certificat. Si aucune valeur n'est saisie dans ce champ, le certificat généré utilise le premier nom de domaine ou la première adresse IP comme nom commun (CN) du sujet.
Jours valides	Nombre de jours après la création du certificat avant son expiration.
Ajouter des extensions d'utilisation de clé	Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de clé et d'utilisation de clé étendue sont ajoutées au certificat généré. Ces extensions définissent la finalité de la clé contenue dans le certificat. **Remarque** : 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 **Générer**.

d. Sélectionnez **Détails du certificat** pour afficher les métadonnées et le PEM du certificat d'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 son 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 serveur personnalisé est utilisé pour les connexions client S3 ultérieures.

5. Sélectionnez un onglet pour afficher les métadonnées du certificat 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 une journée 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 d'API S3 personnalisé, la page du certificat d'API S3 affiche des informations détaillées sur le certificat d'API S3 personnalisé actuellement utilisé. Vous pouvez télécharger ou copier le PEM du certificat selon vos besoins.

Restaurez le certificat d'API S3 par défaut

Vous pouvez rétablir l'utilisation du certificat d'API S3 par défaut pour les connexions client S3 aux nœuds de stockage. Cependant, vous ne pouvez pas utiliser le certificat d'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 **S3 API certificate**.
3. Sélectionnez **Utiliser le certificat par défaut**.

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

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

   Si vous disposez des droits d'accès root 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 avec le certificat API S3 par défaut s'affiche. Accédez à "Configurer les points de terminaison de l'équilibreur de charge" pour modifier ou supprimer les points de terminaison concernés.

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

Téléchargez ou copiez le certificat de l'API S3

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

Étapes

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

Téléchargez le fichier de certificat ou le bundle CA

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

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

   Si vous téléchargez un ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble d'autorités de certification sont téléchargés sous forme d'un seul fichier.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le certificat ou le bundle d'autorités de certification PEM

Copiez le texte du certificat pour le coller ailleurs. Si vous utilisez un ensemble CA optionnel, 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 ensemble d'autorités de certification, tous les certificats des onglets secondaires de l'ensemble 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

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

Copiez le certificat d'autorité de certification (CA) StorageGRID Grid

StorageGRID utilise une autorité de certification interne (CA) pour sécuriser le trafic interne. Ce certificat ne change pas si vous importez vos propres certificats.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez "autorisations d'accès spécifiques".

À propos de cette tâche

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

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Grid CA**.
2. Dans la section **Certificat PEM**, téléchargez ou copiez le certificat.

Télécharger le fichier de certificat

Téléchargez le fichier de certificat `.pem`.

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

   Par exemple : `storagegrid_certificate.pem`

Copier le 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 cette validation stricte, tels que les clients ONTAP utilisant FabricPool, vous pouvez générer ou télécharger un certificat de serveur lors de la configuration du point de terminaison de l'équilibreur de charge.

Avant de commencer

- Vous avez "autorisations d'accès spécifiques".
- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".

À propos de cette tâche

Lors de la création d'un point de terminaison d'équilibrage de charge, vous pouvez générer un certificat serveur auto-signé ou importer un certificat signé par une autorité de certification (CA) reconnue. Dans les environnements de production, vous devez utiliser un certificat signé par une CA reconnue. Les certificats signés par une CA peuvent être renouvelés sans interruption de service. Ils sont également plus sécurisés car ils offrent une meilleure protection contre les attaques de type homme du milieu.

Les étapes suivantes fournissent des instructions générales pour les clients S3 qui utilisent FabricPool. Pour plus d'informations et de procédures détaillées, consultez "Configurer StorageGRID pour FabricPool".

Étapes

1. Vous pouvez éventuellement configurer un groupe à haute disponibilité (HA) pour que FabricPool puisse l'utiliser.

2. Créez un point de terminaison d'équilibrage de charge S3 pour que FabricPool puisse l'utiliser.

   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, éventuellement, le bundle d'autorité de certification.

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

   Veuillez indiquer le port du point de terminaison de l'équilibreur de charge et le nom de domaine complet utilisé dans le certificat d'autorité de certification que vous avez importé. Ensuite, fournissez le certificat d'autorité de certification.

> ⓘ Si le certificat StorageGRID a été émis par une autorité de certification intermédiaire, 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.

Configurez les certificats clients dans StorageGRID

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

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

> ⓘ Pour éviter toute interruption de service due à une défaillance du certificat serveur, l'alerte **Expiration des certificats clients configurés sur la page Certificats** est déclenchée lorsque ce certificat serveur est sur le point d'expirer. Au besoin, vous pouvez consulter la date d'expiration du certificat actuel 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 concernant "téléchargement d'un certificat client KMS".

Avant de commencer

- Vous disposez des droits d'accès root.
- Vous êtes connecté au Gestionnaire de grille 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, vous disposez de l'autorité de certification, du certificat client et de la clé privée 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 sauvegardée ou enregistrée lors 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 (le cas échéant) sont disponibles sur votre ordinateur local.

Ajouter des certificats client

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

- Le certificat d'interface de gestion est déjà configuré
- Certificat client délivré par CA
- Certificat généré par Grid Manager

Le certificat d'interface de gestion est 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 **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre les certificats**, téléversez le certificat de l'interface de gestion.
    a. Sélectionnez **Téléverser 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 Grid Manager.

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

Certificat client délivré par CA

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 et une clé privée émis par une autorité de certification (CA).

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 **Add**.
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continue**.
7. Pour l'étape **Joindre les certificats**, téléchargez le certificat client, la clé privée et les fichiers du bundle d'autorité de certification :
   a. Sélectionnez **Téléverser le certificat**.
   b. Sélectionnez **Parcourir** et sélectionnez les fichiers du certificat client, de la clé privée et du bundle CA (`.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 Grid Manager.

      Les nouveaux certificats apparaissent dans 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 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 **Add**.
3. Saisissez un nom de certificat.
4. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
5. Sélectionnez **Continue**.
6. Pour l'étape **Joindre des certificats**, sélectionnez **Générer un certificat**.
7. Spécifiez les informations du certificat :
   - **Sujet** (facultatif) : sujet X.509 ou nom unique (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

Ces extensions définissent la finalité 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 **Générer**.
9. Sélectionnez **Détails du certificat client** pour afficher les métadonnées du certificat et le PEM du certificat.

> Vous ne pourrez plus consulter 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 son 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 dans un fichier.

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

10. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

    Le nouveau certificat apparaît dans l'onglet Client.

11. Dans le Grid Manager, sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Global**.
12. Sélectionnez **certificat d'interface de gestion**.
13. Sélectionnez **Utiliser un certificat personnalisé**.
14. Téléversez les fichiers certificate.pem et private_key.pem de l'Détails du certificat clientétape. Il n'est pas nécessaire de téléverser le bundle CA.
    a. Sélectionnez **Téléverser le certificat** puis **Continuer**.
    b. Téléchargez chaque fichier de certificat (`.pem`).
    c. Sélectionnez **Enregistrer** pour enregistrer le certificat dans le Grid Manager.

       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 n'a pas besoin de 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 **l'authentification client TLS** et **Avec certificat d'autorité de certification (CA)**.

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

e. **ServerName** : Entrez 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 depuis StorageGRID ou un fichier local.

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

   Pour plus d'informations sur les indicateurs, consultez le "Instructions pour la surveillance StorageGRID".

Modifier les certificats clients

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

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

   Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche dans le tableau et une alerte est déclenchée.

2. Sélectionnez le certificat que vous souhaitez modifier.
3. Sélectionnez **Modifier** puis **Modifier le nom et les permissions**
4. Saisissez un nom de certificat.
5. Pour accéder aux métriques Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Allow prometheus**.
6. Sélectionnez **Continuer** pour enregistrer le certificat dans le 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 le certificat actuel a expiré.

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** puis sélectionnez l'onglet **Client**.

   Le tableau indique les dates d'expiration des certificats et les autorisations d'accès à Prometheus. Si un certificat expire bientôt ou a déjà expiré, un message s'affiche 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 **Téléverser 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 PEM du certificat.

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

     Spécifiez le nom du fichier de certificat et son 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 Grid Manager.

   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 unique (DN) du propriétaire du certificat.
   - **Jours de validité** : Le nombre de jours pendant lesquels le certificat généré est valide, à partir du moment où il est généré.
   - **Ajouter les extensions d'utilisation de la clé** : Si cette option est sélectionnée (par défaut et recommandée), les extensions d'utilisation de la clé et d'utilisation étendue de la clé sont ajoutées au certificat généré.

     Ces extensions définissent la finalité 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 **Générer**.

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

   Vous ne pourrez plus consulter 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 son 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 dans un fichier.

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

e. Sélectionnez **Créer** pour enregistrer le certificat dans le Grid Manager.

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** > **Security** > **Certificates** 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

Téléchargez le fichier de certificat `.pem`.

a. Sélectionnez **Télécharger le certificat**.
b. Spécifiez le nom du fichier de certificat et son 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 clients

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

Étapes

1. Sélectionnez **Configuration** > **Security** > **Certificates** 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** > **Delete**.

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