



## **Gérer les certificats**

StorageGRID 11.8

NetApp  
March 19, 2024

# Sommaire

- Gérer les certificats ..... 1
  - Gérer les certificats de sécurité : présentation ..... 1
  - Configurer les certificats de serveur ..... 12
  - Configurer les certificats client ..... 25

# Gérer les certificats

## Gérer les certificats de sécurité : présentation

Les certificats de sécurité sont de petits fichiers de données utilisés pour créer des connexions sécurisées et fiables entre les composants StorageGRID et entre les composants StorageGRID et les systèmes externes.

StorageGRID utilise deux types de certificats de sécurité :

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

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

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

### Certificat CA grille par défaut

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

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



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

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

être prêts.

## Accéder aux certificats de sécurité

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

### Étapes

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

Name	Description	Type	Expiration date
<a href="#">Management interface certificate</a>	Secures the connection between client web browsers and the Grid Manager, Tenant Manager, Grid Management API, and Tenant Management API.	Custom	Jun 4th, 2022
<a href="#">S3 and Swift API certificate</a>	Secures the connections between S3 and Swift clients and Storage Nodes or between clients and the deprecated CLB service on Gateway Nodes. You can optionally use this certificate for a load balancer endpoint as well.	Custom	Jun 4th, 2022

2. Sélectionnez un onglet sur la page certificats pour obtenir des informations sur chaque catégorie de certificat et pour accéder aux paramètres du certificat. Vous pouvez accéder à un onglet si vous avez le "autorisation appropriée".
  - **Global** : sécurise l'accès à StorageGRID à partir de navigateurs Web et de clients API externes.
  - **Grid CA** : sécurise le trafic StorageGRID interne.
  - **Client** : sécurise les connexions entre les clients externes et la base de données StorageGRID Prometheus.
  - **Points d'extrémité de l'équilibreur de charge** : sécurise les connexions entre les clients S3 et Swift et l'équilibreur de charge StorageGRID.
  - **Locataires** : sécurise les connexions aux serveurs de fédération d'identités ou des terminaux de service de plate-forme aux ressources de stockage S3.
  - **Autre** : sécurise les connexions StorageGRID nécessitant des certificats spécifiques.

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

## Mondial

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

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

Les informations sur les certificats globaux installés comprennent :

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

Vous pouvez :

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

## CA grille

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

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

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

## Client

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

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

Vous pouvez :

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

### Terminaux d'équilibrage de charge

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

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



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

Vous pouvez :

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

### Locataires

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

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

Vous pouvez :

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

### Autre

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

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

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

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



Vous ne pouvez afficher et accéder aux informations relatives aux autres certificats que si vous possédez le "[autorisation appropriée](#)".

Vous pouvez :

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

## Détails du certificat de sécurité

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

### Certificat de l'interface de gestion

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

#### Certificat API S3 et Swift

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

#### Certificat CA de la grille

Voir la [Description du certificat CA de la grille par défaut](#).

#### Certificat du client administrateur



Type de certificat	Description	Emplacement de navigation	Détails
Client	<p>Installé sur chaque client, permettant à StorageGRID d'authentifier l'accès client externe.</p> <ul style="list-style-type: none"> <li>• Permet aux clients externes autorisés d'accéder à la base de données StorageGRID Prometheus.</li> <li>• Contrôle sécurisé de StorageGRID à l'aide d'outils externes.</li> </ul>	<p><b>CONFIGURATION &gt; sécurité &gt; certificats</b>, puis sélectionnez l'onglet <b>client</b></p>	<p><a href="#">"Configurer les certificats client"</a></p>

### Certificat de terminal de l'équilibreur de charge

Type de certificat	Description	Emplacement de navigation	Détails
Serveur	<p>Authentifie la connexion entre les clients S3 ou Swift et le service StorageGRID Load Balancer sur les nœuds de passerelle et les nœuds d'administration. Vous pouvez télécharger ou générer un certificat d'équilibreur de charge lorsque vous configurez un nœud final d'équilibreur de charge. Les applications client utilisent le certificat d'équilibreur de charge lors de la connexion à StorageGRID pour enregistrer et récupérer les données d'objet.</p> <p>Vous pouvez également utiliser une version personnalisée de <a href="#">Global Certificat API S3 et Swift</a> Certificat permettant d'authentifier les connexions au service Load Balancer. Si le certificat global est utilisé pour authentifier les connexions de l'équilibreur de charge, vous n'avez pas besoin de télécharger ou de générer un certificat distinct pour chaque nœud final de l'équilibreur de charge.</p> <p><b>Remarque :</b> le certificat utilisé pour l'authentification de l'équilibreur de charge est le certificat le plus utilisé pendant le fonctionnement normal de l'StorageGRID.</p>	<b>CONFIGURATION &gt; réseau &gt; points d'extrémité de l'équilibreur de charge</b>	<ul style="list-style-type: none"> <li>• <a href="#">"Configurer les terminaux de l'équilibreur de charge"</a></li> <li>• <a href="#">"Créer un nœud final d'équilibrage de charge pour FabricPool"</a></li> </ul>

## Certificat de terminal Cloud Storage Pool

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

## Certificat de notification d'alerte par e-mail

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	<p>Authentifie la connexion entre un serveur de messagerie SMTP et StorageGRID utilisé pour les notifications d'alerte.</p> <ul style="list-style-type: none"><li>• Si les communications avec le serveur SMTP nécessitent TLS (transport Layer Security), vous devez spécifier le certificat AC du serveur de messagerie.</li><li>• Spécifiez un certificat client uniquement si le serveur de messagerie SMTP nécessite des certificats client pour l'authentification.</li></ul>	<b>ALERTE &gt; Configuration de la messagerie</b>	" <a href="#">Configurez les notifications par e-mail pour les alertes</a> "

## Certificat de serveur syslog externe

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

#### certificat de connexion de fédération de grille

Type de certificat	Description	Emplacement de navigation	Détails
Serveur et client	Authentifier et crypter les informations envoyées entre le système StorageGRID actuel et une autre grille dans une connexion de fédération de grille.	<b>CONFIGURATION &gt; système &gt; fédération de grille</b>	<ul style="list-style-type: none"> <li>"Créer des connexions de fédération de grille"</li> <li>"Faire pivoter les certificats de connexion"</li> </ul>

#### Certificat de fédération des identités

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

#### Certificat de serveur de gestion des clés (KMS)

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

### Certificat de terminal des services de plate-forme

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

### Certificat SSO (Single Sign-on)

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

## Exemples de certificats

### Exemple 1 : service Load Balancer

Dans cet exemple, StorageGRID sert de serveur.

1. Vous configurez un nœud final de l'équilibreur de charge et téléchargez ou générez un certificat de serveur dans StorageGRID.
2. Vous configurez une connexion client S3 ou Swift au point de terminaison de l'équilibreur de charge et téléchargez le même certificat au client.
3. Lorsque le client souhaite enregistrer ou récupérer des données, il se connecte au point de terminaison de l'équilibreur de charge à l'aide de HTTPS.

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

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

Dans cet exemple, StorageGRID agit comme client.

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

## Configurer les certificats de serveur

### Types de certificat de serveur pris en charge

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



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

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

### Configurer les certificats d'interface de gestion

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

#### Description de la tâche

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

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

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



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



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

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

## Ajoutez un certificat d'interface de gestion personnalisée

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

### Étapes

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

## Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

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



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

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

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

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

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

Par exemple : `storagegrid_certificate.pem`

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

d. Sélectionnez **Enregistrer**.

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

## Générez un certificat

Générez les fichiers de certificat du serveur.



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

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

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



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

c. Sélectionnez **generate**.

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

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

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

Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**.

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

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



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

6. Une fois que vous avez ajouté un certificat d'interface de gestion personnalisé, la page de certificat de l'interface de gestion affiche des informations détaillées sur le certificat pour les certificats en cours d'utilisation.

Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

## Restaurez le certificat de l'interface de gestion par défaut

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

### Étapes

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

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

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

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

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

### Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous avez le `Passwords.txt` fichier.

### Description de la tâche

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

### Étapes

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

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

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

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

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

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



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

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

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

4. Sélectionnez et copiez le certificat.

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

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

### Téléchargez ou copiez le certificat de l'interface de gestion

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

#### Étapes

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

### Téléchargez le fichier de certificat ou le bundle CA

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

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

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

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

Par exemple : `storagegrid_certificate.pem`

### Copie du certificat ou pack CA PEM

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

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

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

- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension .pem.

Par exemple : `storagegrid_certificate.pem`

## Configurez les certificats API S3 et Swift

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

### Description de la tâche

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

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

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



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

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

### Ajoutez un certificat S3 et Swift personnalisé

#### Étapes

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

## Télécharger le certificat

Téléchargez les fichiers de certificat de serveur requis.

a. Sélectionnez **Télécharger le certificat**.

b. Téléchargez les fichiers de certificat de serveur requis :

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



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

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

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

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

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

Par exemple : `storagegrid_certificate.pem`

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

d. Sélectionnez **Enregistrer**.

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

## Générez un certificat

Générez les fichiers de certificat du serveur.

a. Sélectionnez **générer certificat**.

b. Spécifiez les informations de certificat :

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

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

c. Sélectionnez **generate**.

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

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

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

Par exemple : `storagegrid_certificate.pem`

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

e. Sélectionnez **Enregistrer**.

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

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



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

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

7. Après avoir ajouté un certificat d'API S3 et Swift personnalisé, la page de certificats d'API S3 et Swift affiche des informations détaillées sur le certificat d'API S3 et Swift personnalisé utilisé.

Vous pouvez télécharger ou copier le certificat PEM selon vos besoins.

## Restaurez le certificat API S3 et Swift par défaut

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

### Étapes

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

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

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

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

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

## Téléchargez ou copiez le certificat API S3 et Swift

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

### Étapes

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



### Téléchargez le fichier de certificat ou le bundle CA

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

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

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

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

Par exemple : `storagegrid_certificate.pem`

### Copie du certificat ou pack CA PEM

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

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

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

- b. Collez le certificat copié dans un éditeur de texte.
- c. Enregistrez le fichier texte avec l'extension `.pem`.

Par exemple : `storagegrid_certificate.pem`

### Informations associées

- ["UTILISEZ L'API REST S3"](#)
- ["Utilisez l'API REST de Swift"](#)
- ["Configuration des noms de domaine de terminaux S3"](#)

### Copiez le certificat de l'autorité de certification Grid

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

### Avant de commencer

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

### Description de la tâche

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

### Étapes

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

#### **Téléchargez le fichier de certificat**

Téléchargez le certificat .pem fichier.

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

Par exemple : `storagegrid_certificate.pem`

#### **Copie du certificat PEM**

Copiez le texte du certificat pour le coller ailleurs.

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

Par exemple : `storagegrid_certificate.pem`

## **Configurez les certificats StorageGRID pour FabricPool**

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

### **Avant de commencer**

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

### **Description de la tâche**

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

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

### **Étapes**

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

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

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

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



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

## Configurer les certificats client

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

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

Voir "[Gérer les certificats de sécurité](#)" et "[Configurer des certificats de serveur personnalisés](#)".



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



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

### Avant de commencer

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

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

## Ajouter des certificats client

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

- [Certificat d'interface de gestion déjà configuré](#)
- [CERTIFICAT client émis](#)
- [Certificat généré par Grid Manager](#)

### Certificat d'interface de gestion déjà configuré

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

#### Étapes

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

Le nouveau certificat apparaît sur l'onglet client.

7. [Configurer un outil de surveillance externe](#), Comme Grafana.

### CERTIFICAT client émis

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

#### Étapes

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

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

Les nouveaux certificats apparaissent sur l'onglet client.

8. [Configurer un outil de surveillance externe](#), Comme Grafana.

### Certificat généré par Grid Manager

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

#### Étapes

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

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



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

8. Sélectionnez **generate**.

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



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

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

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

Par exemple : `storagegrid_certificate.pem`

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

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

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

Le nouveau certificat apparaît sur l'onglet client.

11. Dans le Gestionnaire de grille, sélectionnez **CONFIGURATION** > **sécurité** > **certificats**, puis sélectionnez l'onglet **Global**.

12. Sélectionnez **certificat d'interface de gestion**.

13. Sélectionnez **utiliser le certificat personnalisé**.

14. Téléchargez les fichiers `Certificate.pem` et `private_key.pem` à partir du [détails du certificat client](#) étape. Il n'est pas nécessaire de télécharger le pack CA.

- Sélectionnez **Télécharger le certificat**, puis **Continuer**.
- Téléchargez chaque fichier de certificat (`.pem`).
- Sélectionnez **Enregistrer** pour enregistrer le certificat dans Grid Manager.

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

15. [Configurer un outil de surveillance externe](#), Comme Grafana.

### configurez un outil de surveillance externe

#### Étapes

1. Configurez les paramètres suivants sur votre outil de surveillance externe, tels que Grafana.

- Nom** : saisissez un nom pour la connexion.

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

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

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

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

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

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

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

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

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

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

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

## Modifier les certificats client

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

### Étapes

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

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

2. Sélectionnez le certificat à modifier.

3. Sélectionnez **Modifier**, puis **Modifier le nom et l'autorisation**

4. Entrez un nom de certificat.

5. Pour accéder aux metrics Prometheus à l'aide de votre outil de surveillance externe, sélectionnez **Autoriser prometheus**.

6. Sélectionnez **Continuer** pour enregistrer le certificat dans Grid Manager.

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

## Joindre un nouveau certificat client

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

## Étapes

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

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

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



## Télécharger le certificat

Copiez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **Télécharger le certificat**, puis **Continuer**.
- b. Téléchargez le nom du certificat client (.pem).

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

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

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

Par exemple : `storagegrid_certificate.pem`

- Sélectionnez **Copier le certificat PEM** pour copier le contenu du certificat pour le coller ailleurs.
- c. Sélectionnez **Créer** pour enregistrer le certificat dans le gestionnaire de grille.

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

## Générez un certificat

Générez le texte du certificat pour le coller ailleurs.

- a. Sélectionnez **générer certificat**.
- b. Spécifiez les informations de certificat :

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

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



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

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



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

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

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

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

Par exemple : `storagegrid_certificate.pem`

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

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

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

Le nouveau certificat apparaît sur l'onglet client.

## Téléchargez ou copiez les certificats client

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

### Étapes

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

#### Téléchargez le fichier de certificat

Téléchargez le certificat `.pem` fichier.

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

Par exemple : `storagegrid_certificate.pem`

#### Copier le certificat

Copiez le texte du certificat pour le coller ailleurs.

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

Par exemple : `storagegrid_certificate.pem`

## Supprimer les certificats client

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

### Étapes

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



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

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

## Informations sur le copyright

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

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

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

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

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

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

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

## Informations sur les marques commerciales

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