Configuration des certificats de serveur

StorageGRID 11.5

NetApp
April 11, 2024

Sommaire

Configuration des certificats de serveur

Vous pouvez personnaliser les certificats de serveur utilisés par le système StorageGRID.

Le système StorageGRID utilise des certificats de sécurité à diverses fins :

- Certificats de serveur de l'interface de gestion : utilisés pour sécuriser l'accès à Grid Manager, au tenant Manager, à l'API de gestion du grid et à l'API de gestion des locataires.
- Certificats de serveur d'API de stockage : utilisés pour sécuriser l'accès aux nœuds de stockage et aux nœuds de passerelle, que les applications client d'API utilisent pour charger et télécharger les données d'objet.

Vous pouvez utiliser les certificats par défaut créés lors de l'installation ou remplacer l'un ou l'autre de ces types de certificats par défaut par vos propres certificats personnalisés.

Types pris en charge de certificat de serveur personnalisé

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

Pour plus d'informations sur la sécurisation des connexions clients par StorageGRID pour l'API REST, consultez les guides d'implémentation S3 ou Swift.

Certificats pour les noeuds finaux de l'équilibreur de charge

StorageGRID gère séparément les certificats utilisés pour les terminaux de l'équilibreur de charge. Pour configurer des certificats d'équilibreur de charge, reportez-vous aux instructions de configuration des noeuds finaux d'équilibreur de charge.

Informations associées

"Utilisation de S3"

"Utiliser Swift"

"Configuration des terminaux d'équilibrage de charge"

Configuration d'un certificat de serveur personnalisé pour le Grid Manager et le tenant Manager

Vous pouvez remplacer le certificat de serveur StorageGRID par défaut par un seul certificat de serveur personnalisé qui permet aux utilisateurs d'accéder au Gestionnaire de grille et au Gestionnaire de locataires sans rencontrer d'avertissements de sécurité.

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 de serveur personnalisé commun et une clé privée correspondante.

Comme un seul certificat de serveur personnalisé 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 Gestionnaire de locataires. Définissez le certificat personnalisé de sorte qu'il corresponde à tous les nœuds d'administration de la grille.

Vous devez terminer la configuration sur le serveur et, selon l'autorité de certification racine (AC) que vous utilisez, les utilisateurs devront peut-être aussi installer le certificat d'autorité de certification racine dans le navigateur Web qu'ils utiliseront pour accéder au gestionnaire de grille et au gestionnaire de tenant.

> 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** et l'alarme expiration du certificat de l'interface de gestion héritée (MCEP) sont toutes deux déclenchées lorsque ce certificat de serveur est sur le point d'expirer. Si nécessaire, vous pouvez afficher le nombre de jours jusqu'à l'expiration du certificat de service en cours en sélectionnant **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***primary Admin Node*** > **CMN** > **Resources**.

> 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 de serveur de l'interface de gestion personnalisée expire.
> - Vous restaurez un certificat de serveur d'interface de gestion personnalisée vers le certificat de serveur par défaut.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section certificat du serveur de l'interface de gestion, cliquez sur **installer le certificat personnalisé**.
3. Téléchargez les fichiers de certificat de serveur requis :
   - **Certificat de serveur** : fichier de certificat de serveur personnalisé (`.crt`).
   - **Clé privée de certificat de serveur** : 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 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.
4. Cliquez sur **Enregistrer**.

   Les certificats de serveur personnalisés sont utilisés pour toutes les nouvelles connexions client suivantes.

   Sélectionnez un onglet pour afficher des informations détaillées sur le certificat de serveur StorageGRID par défaut ou sur un certificat signé par l'autorité de certification qui a été téléchargé.

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

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

Restauration des certificats de serveur par défaut pour le Grid Manager et le tenant Manager

Vous pouvez revenir à l'utilisation des certificats de serveur par défaut pour le Grid Manager et le tenant Manager.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section gérer le certificat du serveur d'interface, cliquez sur **utiliser les certificats par défaut**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

   Lorsque vous restaurez les certificats de serveur par défaut, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Les certificats de serveur par défaut sont utilisés pour toutes les nouvelles connexions client suivantes.

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

Configuration d'un certificat de serveur personnalisé pour les connexions au nœud de stockage ou au service CLB

Vous pouvez remplacer le certificat de serveur utilisé pour les connexions des clients S3 ou Swift vers le nœud de stockage ou vers le service CLB (obsolète) sur le nœud de passerelle. Le certificat de serveur personnalisé de remplacement est spécifique à votre organisation.

Description de la tâche

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

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

Une fois la configuration terminée sur le serveur, les utilisateurs peuvent également avoir besoin d'installer le certificat d'autorité de certification racine dans le client API S3 ou Swift qu'ils utiliseront pour accéder au système, selon l'autorité de certification racine que vous utilisez.

> Pour garantir que les opérations ne sont pas interrompues par un échec du certificat de serveur, l'alerte **expiration du certificat de serveur pour les noeuds finaux de l'API de stockage** et l'alarme expiration du certificat de noeuds finaux du service de l'API de stockage héritée sont toutes deux déclenchées lorsque le certificat de serveur racine est sur le point d'expirer. Si nécessaire, vous pouvez afficher le nombre de jours jusqu'à l'expiration du certificat de service en cours en sélectionnant **support** > **Outils** > **topologie de grille**. Sélectionnez ensuite ***primary Admin Node*** > **CMN** > **Resources**.

Les certificats personnalisés sont utilisés uniquement si les clients se connectent à StorageGRID à l'aide du service CLB obsolète sur les nœuds de passerelle ou s'ils se connectent directement aux nœuds de stockage.

Les clients S3 ou Swift qui se connectent à StorageGRID via le service Load Balancer sur les nœuds d'administration ou les nœuds de passerelle utilisent le certificat configuré pour le terminal de l'équilibreur de charge.

> L'alerte **expiration du certificat de point final de l'équilibreur de charge** est déclenchée pour les noeuds finaux de l'équilibreur de charge qui expirent bientôt.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section certificat de serveur de noeuds finaux du service API de stockage d'objets, cliquez sur **installer le certificat personnalisé**.
3. Téléchargez les fichiers de certificat de serveur requis :
   - **Certificat de serveur** : fichier de certificat de serveur personnalisé (`.crt`).
   - **Clé privée de certificat de serveur** : 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 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.
4. Cliquez sur **Enregistrer**.

   Le certificat de serveur personnalisé est utilisé pour toutes les nouvelles connexions client API suivantes.

   Sélectionnez un onglet pour afficher des informations détaillées sur le certificat de serveur StorageGRID par défaut ou sur un certificat signé par l'autorité de certification qui a été téléchargé.

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

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

Informations associées

"Utilisation de S3"

"Utiliser Swift"

"Configuration des noms de domaine de terminaux API S3"

Restauration des certificats de serveur par défaut pour les terminaux API REST S3 et Swift

Vous pouvez revenir à l'utilisation des certificats de serveur par défaut pour les terminaux API REST S3 et Swift.

Étapes

1. Sélectionnez **Configuration** > **Paramètres réseau** > **certificats serveur**.

2. Dans la section certificat de serveur de noeuds finaux du service API de stockage d'objets, cliquez sur **utiliser les certificats par défaut**.
3. Cliquez sur **OK** dans la boîte de dialogue de confirmation.

   Lorsque vous restaurez les certificats de serveur par défaut pour les noeuds finaux de l'API de stockage d'objets, les fichiers de certificat de serveur personnalisés que vous avez configurés sont supprimés et ne peuvent pas être récupérés du système. Les certificats de serveur par défaut sont utilisés pour toutes les nouvelles connexions client API suivantes.

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

Copie du certificat de l'autorité de certification du système StorageGRID

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

Ce dont vous avez besoin

- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.
- Vous devez disposer d'autorisations d'accès spécifiques.

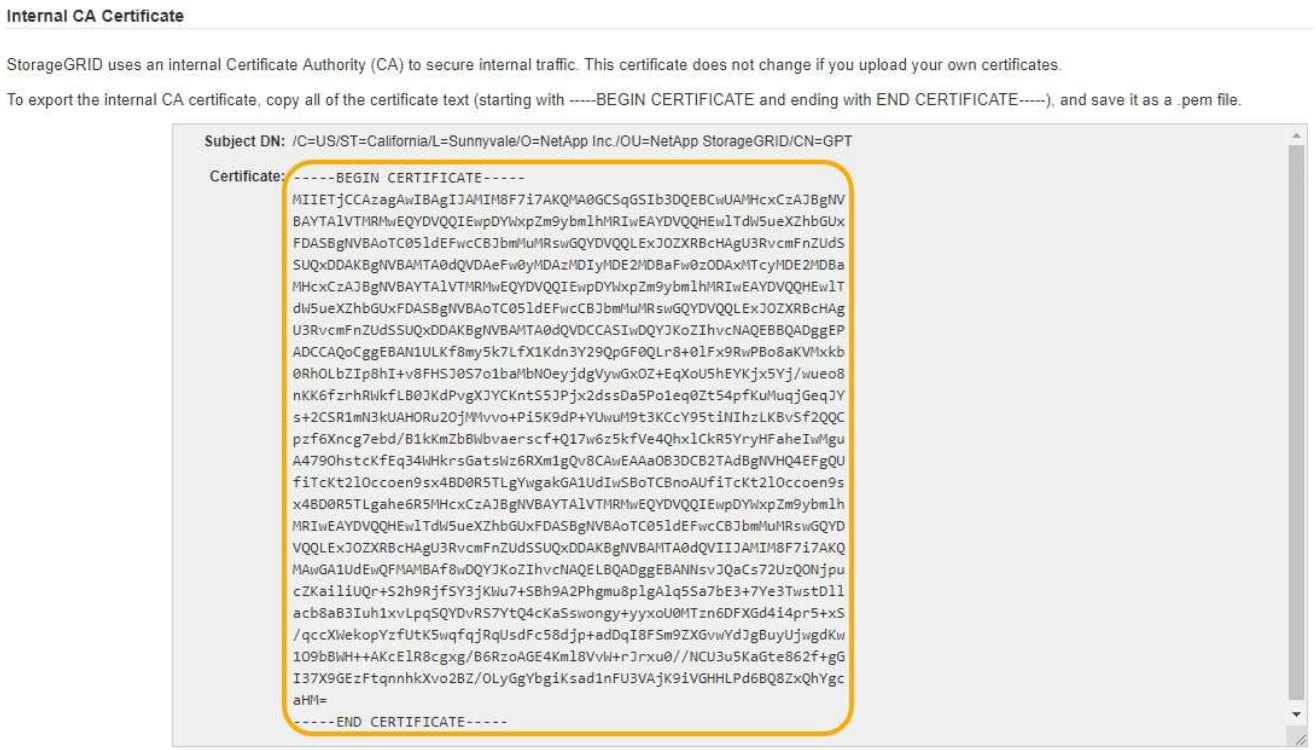
Description de la tâche

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** > **Paramètres réseau** > **certificats serveur**.
2. Dans la section **certificat CA interne**, sélectionnez tout le texte du certificat.

   Vous devez inclure `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----` dans votre sélection.



3. Cliquez avec le bouton droit de la souris sur le texte sélectionné et sélectionnez **Copier**.
4. Collez le certificat copié dans un éditeur de texte.
5. Enregistrez le fichier avec l'extension `.pem`.

   Par exemple : `storagegrid_certificate.pem`

Configuration des certificats StorageGRID pour FabricPool

Pour les clients S3 qui effectuent une validation stricte du nom d'hôte et qui ne prennent pas en charge la désactivation de la validation stricte du nom d'hôte, comme les clients ONTAP utilisant FabricPool, vous pouvez générer ou charger un certificat de serveur lors de la configuration du point de terminaison de l'équilibreur de charge.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez être connecté à Grid Manager à l'aide d'un navigateur pris en charge.

Description de la tâche

Lorsque vous créez un noeud final de l'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 aux instructions de configuration de StorageGRID pour FabricPool.

> Le service distinct Connection Load Balancer (CLB) sur les nœuds de passerelle est obsolète et n'est plus recommandé pour une utilisation avec 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.

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.

Informations associées

"Configuration de StorageGRID pour FabricPool"

Génération d'un certificat de serveur auto-signé pour l'interface de gestion

Vous pouvez utiliser un script pour générer un certificat de serveur auto-signé pour les clients de l'API de gestion nécessitant une validation stricte du nom d'hôte.

Ce dont vous avez besoin

- Vous devez disposer d'autorisations d'accès spécifiques.
- Vous devez avoir le `Passwords.txt` fichier.

Description de la tâche

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.

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 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 l'API de gestion est synchronisé avec la même source que StorageGRID ; sinon, le client peut rejeter le certificat.

```
$ sudo make-certificate --domains *.ui.storagegrid.example.com --type
management --days 365
```

   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** > **certificats de serveur** > **certificat de serveur d'interface de gestion**.
7. Configurez votre client de l'API de gestion pour utiliser le certificat public que vous avez copié. Incluez les balises DE DÉBUT et DE FIN.