Gérer l'équilibrage de charge

StorageGRID software

NetApp
July 23, 2026

Sommaire

Gérer l’équilibrage de charge

Découvrez l’équilibrage de charge StorageGRID

Vous pouvez utiliser l’équilibrage de charge pour gérer les charges de travail d’ingestion et de récupération des clients S3.

Qu’est-ce que l’équilibrage de charge ?

Lorsqu’une application cliente enregistre ou récupère des données depuis un système StorageGRID, StorageGRID utilise un équilibreur de charge pour gérer la charge de travail d’ingestion et de récupération. L’équilibrage de charge optimise la vitesse et la capacité de connexion en répartissant la charge de travail sur plusieurs nœuds de stockage.

Le service d’équilibrage de charge StorageGRID est installé sur tous les nœuds d’administration et tous les nœuds de passerelle et assure l’équilibrage de charge de couche 7. Il effectue la terminaison TLS (Transport Layer Security) des requêtes client, les inspecte et établit de nouvelles connexions sécurisées avec les nœuds de stockage.

Le service d’équilibrage de charge de chaque nœud fonctionne indépendamment lors de la répartition du trafic client vers les nœuds de stockage. Grâce à un processus de pondération, le service d’équilibrage de charge achemine davantage de requêtes vers les nœuds de stockage disposant d’une plus grande disponibilité de processeur.

> Bien que le service StorageGRID Load Balancer soit le mécanisme d’équilibrage de charge recommandé, vous pouvez également intégrer un équilibreur de charge tiers. Pour plus d’informations, contactez votre représentant de compte NetApp ou consultez "Utilisez des équilibreurs de charge tiers avec StorageGRID".

De combien de nœuds d’équilibrage de charge avez-vous besoin ?

En bonne pratique, chaque site de votre système StorageGRID devrait comporter au moins deux nœuds avec le service d’équilibrage de charge. Par exemple, un site peut inclure deux nœuds de passerelle ou à la fois un nœud d’administration et un nœud de passerelle. Assurez-vous de disposer d’une infrastructure réseau, matérielle ou de virtualisation adéquate pour chaque nœud d’équilibrage de charge, que vous utilisiez des appliances de services, des nœuds bare metal ou des nœuds basés sur des machines virtuelles (VM).

Qu’est-ce qu’un point de terminaison d’équilibrage de charge ?

Un point de terminaison d’équilibrage de charge définit le port et le protocole réseau (HTTPS ou HTTP) que les requêtes entrantes et sortantes des applications clientes utiliseront pour accéder aux nœuds qui contiennent le service Load Balancer. Ce point de terminaison définit également le type de client (S3), le mode de liaison et, éventuellement, une liste de locataires autorisés ou bloqués.

Pour créer un point de terminaison d’équilibrage de charge, utilisez Grid Manager ou terminez la configuration S3 et les assistants FabricPool :

- "Configurer les points de terminaison de l’équilibreur de charge"
- "Utilisez l’assistant de configuration S3"
- "Utilisez l’assistant de configuration FabricPool"

Considérations relatives à la mise en cache de l'équilibreur de charge

La mise en cache améliore considérablement les performances lorsqu'une charge de travail traite un sous-ensemble de données et accède plusieurs fois aux objets. De plus, la mise en cache permet un accès distant au stockage d'objets sans déploiement complet de la grille. La mise en cache de l'équilibreur de charge est disponible uniquement pour les Gateway Nodes.

Lors de la création des points de terminaison de l'équilibreur de charge :

- N'activez la mise en cache que pour les charges de travail pouvant être mises en cache. Les charges de travail accédant plus fréquemment aux données non mises en cache qu'aux données mises en cache auront des performances inférieures à celles qui n'auraient pas été prises en charge par le cache. Dans certains cas, les charges de travail avec des taux élevés de réécriture et d'éviction peuvent également dépasser l'endurance d'écriture garantie du disque.
- Envisagez d'ajouter des points de terminaison ou des nœuds supplémentaires pour la mise en cache des charges de travail individuelles qui sont de bons candidats pour la mise en cache.
- Utilisez des points de terminaison distincts pour les charges de travail pouvant être mises en cache et celles qui ne le peuvent pas. Cette séparation garantit que les mécanismes de mise en cache sont appliqués correctement et n'interfèrent pas avec le traitement des données non mises en cache.
- Évaluez la pertinence d'une charge de travail pouvant être mise en cache en la dirigeant vers le point de terminaison compatible avec la mise en cache. Surveillez et vérifiez le taux d'accès au cache afin de déterminer si la charge de travail est adaptée à la mise en cache. Cette évaluation contribue à optimiser les performances et à garantir une utilisation efficace des ressources du cache.
- "Examiner les journaux d'audit" pour déterminer si une charge de travail existante serait un bon candidat pour la mise en cache. Pour une période donnée, déterminez quel pourcentage des requêtes GET concerne des objets uniques. Pour être adaptée à la mise en cache, cette valeur doit être inférieure à 50 %.

Exemples de charges de travail qui pourraient être de bons candidats pour la mise en cache

- lacs de données
- Calcul haute performance (HPC)
- Entraînement IA/ML
- Réseaux de distribution de contenu (CDN)
- gestion des ressources média
- Production vidéo

- Plusieurs versions d'un même objet peuvent être mises en cache.
- Les opérations de lecture de plage sont prises en charge.

Exemples de charges de travail qui ne sont pas de bons candidats pour la mise en cache

- FabricPool
- Applications de sauvegarde
- hiérarchisation du stockage

Si un contenu quelconque à servir par le cache nécessite un chiffrement au repos, "activer le chiffrement du nœud ou du disque" sur le nœud de cache.

Types d'objets et de requêtes qui ne seront pas mis en cache

- Le `response-content-encoding` paramètre de requête
- Le `partNumber` paramètre de requête
- En-têtes conditionnels
  - `If-Match`
  - `If-Modified-Since`
  - `If-None-Match`
  - `If-Unmodified-Since`
- Les requêtes qui ont été chiffrées au repos avec l'un des éléments suivants :
  - SSE (chiffrement côté serveur avec des clés gérées par StorageGRID)
  - SSE-C (chiffrement côté serveur avec clés fournies par le client)
  - Chiffrement des objets stockés

Toute requête qui n'est pas mise en cache est transmise à un LDR en amont comme si le cache n'était pas activé.

Informations connexes

- "Dépannez la mise en cache de l'équilibreur de charge"
- Pour plus d'informations sur la mise en cache de l'équilibreur de charge, contactez le support technique.

Considérations relatives au port

Le port d'un point de terminaison d'équilibrage de charge est par défaut 10433 pour le premier point de terminaison que vous créez, mais vous pouvez spécifier n'importe quel port externe inutilisé entre 1 et 65535. Si vous utilisez le port 80 ou 443, le point de terminaison utilisera le service Load Balancer uniquement sur les Gateway Nodes. Ces ports sont réservés sur les Admin Nodes. Si vous utilisez le même port pour plus d'un point de terminaison, vous devez spécifier un mode de liaison différent pour chaque point de terminaison.

Les ports utilisés par d'autres services de grid ne sont pas autorisés. Voir "Ports internes de StorageGRID".

Considérations relatives au protocole réseau

Dans la plupart des cas, les connexions entre les applications clientes et StorageGRID doivent utiliser le chiffrement Transport Layer Security (TLS). La connexion à StorageGRID sans chiffrement TLS est possible, mais déconseillée, notamment en environnement de production. Lorsque vous sélectionnez le protocole réseau pour le point de terminaison de l'équilibreur de charge StorageGRID, vous devez choisir **HTTPS**.

Considérations relatives aux certificats des points de terminaison de l'équilibreur de charge

Si vous sélectionnez **HTTPS** comme protocole réseau pour le point de terminaison de l'équilibreur de charge, vous devez fournir un certificat de sécurité. Vous pouvez utiliser l'une de ces trois options lors de la création du point de terminaison de l'équilibreur de charge :

- **Téléchargez un certificat signé (recommandé)**. Ce certificat peut être signé par une autorité de certification (CA) publique ou privée. Utiliser un certificat de serveur CA public pour sécuriser la connexion est la bonne pratique. Contrairement aux certificats générés, les certificats signés par une CA peuvent être renouvelés sans interruption, ce qui permet d'éviter les problèmes d'expiration.

Vous devez obtenir les fichiers suivants avant de créer le point de terminaison de l'équilibreur de charge :

  - Le fichier de certificat serveur personnalisé.
  - Le fichier de clé privée du certificat serveur personnalisé.
  - En option, un ensemble de certificats CA provenant de chaque autorité de certification émettrice intermédiaire.

- **Générez un certificat auto-signé**.
- **Utilisez le certificat S3 global StorageGRID**. Vous devez importer ou générer une version personnalisée de ce certificat avant de pouvoir le sélectionner pour le point de terminaison de l'équilibreur de charge. Voir "Configurer les certificats de l'API S3".

De quelles valeurs avez-vous besoin ?

Pour créer le certificat, vous devez connaître tous les noms de domaine et adresses IP que les applications clientes S3 utiliseront pour accéder au point de terminaison.

L'entrée **Subject DN** (Nom distinctif) du certificat doit inclure le nom de domaine complet que l'application cliente utilisera pour StorageGRID. Par exemple :

```
Subject DN:
/C=Country/ST=State/O=Company,Inc./CN=s3.storagegrid.example.com
```

Conformément aux exigences, le certificat peut utiliser des caractères génériques pour représenter les noms de domaine complets de tous les nœuds d'administration et les nœuds de passerelle exécutant le service Load Balancer. Par exemple, `*.storagegrid.example.com` utilise le caractère générique * pour représenter `adm1.storagegrid.example.com` et `gn1.storagegrid.example.com`.

Si vous prévoyez d'utiliser des requêtes de type hébergement virtuel S3, le certificat doit également inclure une entrée **Nom alternatif** pour chaque "nom de domaine du terminal S3" que vous avez configuré, y compris tout nom générique. Par exemple :

```
Alternative Name: DNS:*.s3.storagegrid.example.com
```

> ⓘ Si vous utilisez des caractères génériques pour les noms de domaine, consultez la "Recommandations pour le renforcement de la sécurité des certificats de serveur".

Vous devez également définir une entrée DNS pour chaque nom figurant dans le certificat de sécurité.

Comment gérer les certificats qui expirent ?

> ⚠ Si le certificat utilisé pour sécuriser la connexion entre l'application S3 et StorageGRID expire, l'application risque de perdre temporairement l'accès à StorageGRID.

Pour éviter les problèmes d'expiration de certificat, suivez ces bonnes pratiques :

- Surveillez attentivement toutes les alertes signalant l'approche des dates d'expiration des certificats, telles que les alertes **Expiration of load balancer endpoint certificate** et **Expiration of global server certificate for S3 API**.

- Veillez à toujours synchroniser les versions du certificat de StorageGRID et de l'application S3. Si vous remplacez ou renouvelez le certificat utilisé pour un point de terminaison d'équilibrage de charge, vous devez également remplacer ou renouveler le certificat équivalent utilisé par l'application S3.
- Utilisez un certificat signé par une autorité de certification (CA) publique. Si vous utilisez un certificat signé par une CA, vous pouvez remplacer les certificats arrivant bientôt à expiration sans interruption de service.
- Si vous avez généré un certificat StorageGRID auto-signé et que ce certificat est sur le point d'expirer, vous devez le remplacer manuellement à la fois dans StorageGRID et dans l'application S3 avant l'expiration du certificat existant.

Considérations relatives au mode de liaison

Le mode de liaison permet de contrôler les adresses IP qui peuvent être utilisées pour accéder à un point de terminaison d'équilibreur de charge. Si un point de terminaison utilise un mode de liaison, les applications clientes ne peuvent accéder au point de terminaison que si elles utilisent une adresse IP autorisée ou son domaine complet (FQDN) correspondant. Les applications clientes utilisant toute autre adresse IP ou tout autre FQDN ne peuvent pas accéder au point de terminaison.

Vous pouvez spécifier l'un des modes de liaison suivants :

- **Global** (par défaut) : les applications clientes peuvent accéder au point de terminaison via l'adresse IP de n'importe quel nœud de passerelle ou nœud d'administration, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un domaine complet (FQDN) correspondant. Utilisez ce paramètre sauf si vous devez restreindre l'accessibilité d'un point de terminaison.
- **Adresses IP virtuelles des groupes HA**. Les applications clientes doivent utiliser une adresse IP virtuelle (ou le nom de domaine complet correspondant) d'un groupe HA.
- **Interfaces de nœud**. Les clients doivent utiliser les adresses IP (ou les domaines complets correspondants) des interfaces de nœud sélectionnées.
- **Type de nœud**. En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le domaine complet correspondant) de n'importe quel nœud d'administration, soit l'adresse IP (ou le domaine complet correspondant) de n'importe quel nœud de passerelle.

Considérations relatives à l'accès des locataires

Le contrôle d'accès des locataires est une fonctionnalité de sécurité optionnelle qui vous permet de contrôler quels comptes locataires StorageGRID peuvent utiliser un point de terminaison d'équilibrage de charge pour accéder à leurs compartiments. Vous pouvez autoriser tous les locataires à accéder à un point de terminaison (par défaut), ou spécifier une liste de locataires autorisés ou bloqués pour chaque point de terminaison.

Vous pouvez utiliser cette fonctionnalité pour offrir une meilleure isolation de sécurité entre les locataires et leurs terminaux. Par exemple, vous pouvez utiliser cette fonctionnalité pour garantir que les documents ultra-confidentiels ou hautement classifiés appartenant à un locataire restent totalement inaccessibles aux autres locataires.

> Aux fins du contrôle d'accès, le locataire est déterminé à partir des clés d'accès utilisées dans la requête du client ; si aucune clé d'accès n'est fournie dans le cadre de la requête (comme dans le cas d'accès anonyme), le propriétaire du compartiment est utilisé pour déterminer le locataire.

Exemple d'accès locataire

Pour comprendre le fonctionnement de cette fonction de sécurité, considérez l'exemple suivant :

1. Vous avez créé deux points de terminaison d'équilibrage de charge, comme suit :

- Point de terminaison **public** : utilise le port 10443 et permet l'accès à tous les tenants.
- Point d'accès **Top secret** : utilise le port 10444 et autorise l'accès uniquement au locataire **Top secret**. Tous les autres locataires sont bloqués de l'accès à ce point d'accès.

2. Le `top-secret.pdf` se trouve dans un compartiment appartenant au locataire **Top secret**.

Pour accéder à `top-secret.pdf`, un utilisateur du locataire **Top secret** peut envoyer une requête GET à `https://w.x.y.z:10444/top-secret.pdf`. Ce locataire étant autorisé à utiliser le point de terminaison 10444, l'utilisateur peut accéder à l'objet. Cependant, si un utilisateur appartenant à un autre locataire envoie la même requête à la même URL, il reçoit immédiatement un message Accès refusé. L'accès est refusé même si les identifiants et la signature sont valides.

disponibilité du processeur

Le service d'équilibrage de charge sur chaque nœud d'administration et de passerelle fonctionne indépendamment lors de l'acheminement du trafic S3 vers les nœuds de stockage. Grâce à un processus de pondération, le service d'équilibrage de charge dirige davantage de requêtes vers les nœuds de stockage disposant d'une plus grande disponibilité CPU. Les informations sur la charge CPU des nœuds sont mises à jour toutes les quelques minutes, mais la pondération peut être actualisée plus fréquemment. Tous les nœuds de stockage se voient attribuer une valeur de poids minimale, même si un nœud signale une utilisation de 100 % ou ne parvient pas à signaler son utilisation.

Dans certains cas, les informations relatives à la disponibilité du processeur sont limitées au site où se trouve le service de Load Balancer.

Configurer les points de terminaison de l'équilibreur de charge StorageGRID

Les points de terminaison de l'équilibreur de charge déterminent les ports et les protocoles réseau que les clients S3 peuvent utiliser pour se connecter à l'équilibreur de charge StorageGRID sur les nœuds Gateway et Admin. Vous pouvez également utiliser ces points de terminaison pour accéder au Grid Manager, au Tenant Manager ou aux deux.

Avant de commencer

- Vous êtes connecté au Gestionnaire de grille à l'aide d'un "navigateur Web pris en charge".
- Vous avez le "Autorisation d'accès root".
- Vous avez examiné le "considérations relatives à l'équilibrage de charge".
- Si vous avez précédemment remappé un port que vous prévoyez d'utiliser pour le point de terminaison de l'équilibreur de charge, vous avez "suppression du remappage de port".
- Vous avez créé les groupes de haute disponibilité (HA) que vous prévoyez d'utiliser. Les groupes HA sont recommandés, mais non obligatoires. Voir "Gérer les groupes à haute disponibilité".
- Si le point de terminaison de l'équilibreur de charge sera utilisé par "Locataires S3 pour S3 Select", il ne doit pas utiliser les adresses IP ni les FQDN de nœuds bare-metal. Seuls les appliances de services et les nœuds logiciels basés sur VMware sont autorisés pour les points de terminaison de l'équilibreur de charge utilisés pour S3 Select.
- Vous avez configuré les interfaces VLAN que vous prévoyez d'utiliser. Voir "Configurer les interfaces VLAN".

- Si vous créez un point de terminaison HTTPS (recommandé), vous disposez des informations pour le certificat du serveur.

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

  - Pour télécharger un certificat, vous avez besoin du certificat serveur, de la clé privée du certificat et, éventuellement, d'un bundle d'autorité de certification (CA bundle).
  - Pour générer un certificat, vous avez besoin de tous les noms de domaine et adresses IP que les clients S3 utiliseront pour accéder au point de terminaison. Vous devez également connaître le sujet (Distinguished Name).
  - Si vous souhaitez utiliser le certificat de l'API StorageGRID S3 (qui peut également être utilisé pour les connexions directes aux nœuds de stockage), vous avez déjà remplacé le certificat par défaut par un certificat personnalisé signé par une autorité de certification externe. Voir "Configurer les certificats de l'API S3".

Créer un point de terminaison d'équilibrage de charge

Chaque point de terminaison d'équilibrage de charge client S3 spécifie un port, un type de client (S3) et un protocole réseau (HTTP ou HTTPS). Les points de terminaison d'équilibrage de charge de l'interface de gestion spécifient un port, un type d'interface et un réseau Client Network non approuvé.

Accédez à l'assistant

Étapes

1. Sélectionnez **Configuration** > **Réseau** > **Points de terminaison de l'équilibreur de charge**.
2. Pour créer un point de terminaison pour un client S3, sélectionnez l'onglet **S3 client**.
3. Pour créer un point de terminaison permettant d'accéder au Grid Manager, au Tenant Manager ou aux deux, sélectionnez l'onglet **Management interface**.
4. Sélectionnez **Create**.

Saisissez les détails du point de terminaison

Étapes

1. Sélectionnez les instructions appropriées pour saisir les détails du type de point de terminaison que vous souhaitez créer.

Client S3

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page des points de terminaison de l'équilibreur de charge.
Port	Le port StorageGRID que vous souhaitez utiliser pour l'équilibrage de charge. Ce champ est défini par défaut sur 10433 pour le premier point de terminaison que vous créez, mais vous pouvez saisir n'importe quel port externe inutilisé compris entre 1 et 65535. Si vous saisissez **80** ou **8443**, le point de terminaison est configuré uniquement sur les nœuds de passerelle, sauf si vous avez libéré le port 8443. Vous pouvez alors utiliser le port 8443 comme point de terminaison S3, et le port sera configuré à la fois sur les nœuds de passerelle et d'administration.
Type de client	Doit être **S3**.
Protocole réseau	Le protocole réseau que les clients utiliseront lorsqu'ils se connecteront à ce point de terminaison. • Sélectionnez **HTTPS** pour une communication sécurisée et chiffrée TLS (recommandé). Vous devez associer un certificat de sécurité avant de pouvoir enregistrer le point de terminaison. • Sélectionnez **HTTP** pour une communication moins sécurisée et non chiffrée. Utilisez HTTP uniquement pour une grille hors production.
Activer la mise en cache	Activer ou désactiver "mise en cache sur les nœuds de passerelle" pour ce point de terminaison d'équilibrage de charge. En cas de problème de mise en cache, veuillez vous référer à "Dépannez la mise en cache de l'équilibreur de charge".

Interface de gestion

Champ	Description
Nom	Un nom descriptif pour le point de terminaison, qui apparaîtra dans le tableau de la page des points de terminaison de l'équilibreur de charge.

Champ	Description
Port	Le port StorageGRID que vous souhaitez utiliser pour accéder au Grid Manager, au Tenant Manager ou aux deux. • Gestionnaire de grille : **8443** • Gestionnaire de locataires : **9443** • Gestionnaire de grille et gestionnaire de locataires : **443** **Remarque** : Vous pouvez utiliser ces ports prédéfinis ou d'autres ports disponibles.
Type d'interface	Sélectionnez le bouton radio pour l'interface StorageGRID à laquelle vous accéderez à l'aide de ce point de terminaison.
Réseau de clients non fiables	Sélectionnez **Oui** si ce point de terminaison doit être accessible aux réseaux clients non approuvés. Sinon, sélectionnez **Non**. Lorsque vous sélectionnez **Oui**, le port est ouvert sur tous les réseaux clients non approuvés. **Remarque** : Vous ne pouvez configurer un port pour qu'il soit ouvert ou fermé aux réseaux clients non approuvés que lors de la création du point de terminaison de l'équilibreur de charge.

1. Sélectionnez **Continue**.

Sélectionnez un mode de liaison

Étapes

1. Sélectionnez un mode de liaison pour le point de terminaison afin de contrôler la manière dont le point de terminaison est accessible en utilisant n'importe quelle adresse IP ou en utilisant des adresses IP et des interfaces réseau spécifiques.

   Certains modes de liaison sont disponibles pour les points de terminaison clients ou les points de terminaison d'interface de gestion. Tous les modes pour les deux types de points de terminaison sont répertoriés ici.

Mode	Description
Global (par défaut pour les points de terminaison clients)	Les clients peuvent accéder au point de terminaison en utilisant l'adresse IP de n'importe quel Gateway Node ou Admin Node, l'adresse IP virtuelle (VIP) de n'importe quel groupe HA sur n'importe quel réseau, ou un FQDN correspondant. Utilisez le paramètre **Global** sauf si vous devez restreindre l'accessibilité de ce point de terminaison.

Mode	Description
Adresses IP virtuelles des groupes HA	Les clients doivent utiliser une adresse IP virtuelle (ou un nom de domaine complet correspondant) d'un groupe HA pour accéder à ce point de terminaison. Les points de terminaison dotés de ce mode de liaison peuvent tous utiliser le même numéro de port, à condition que les groupes HA que vous sélectionnez pour les points de terminaison ne se chevauchent pas.
Interfaces de nœud	Les clients doivent utiliser les adresses IP (ou les noms de domaine complets correspondants) des interfaces de nœud sélectionnées pour accéder à ce point de terminaison.
Type de nœud (points de terminaison clients uniquement)	En fonction du type de nœud que vous sélectionnez, les clients doivent utiliser soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Admin Node, soit l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel Gateway Node pour accéder à ce point de terminaison.
Tous les nœuds d'administration (par défaut pour les points de terminaison de l'interface de gestion)	Les clients doivent utiliser l'adresse IP (ou le nom de domaine complet correspondant) de n'importe quel nœud d'administration pour accéder à ce point de terminaison.

Si plusieurs points de terminaison utilisent le même port, StorageGRID utilise cet ordre de priorité pour décider quel point de terminaison utiliser : **Virtual IPs of HA groups** > **Interfaces de nœud** > **Type de nœud** > **Global**.

Si vous créez des points de terminaison d'interface de gestion, seuls les nœuds d'administration sont autorisés.

2. Si vous avez sélectionné **Virtual IPs of HA groups**, sélectionnez un ou plusieurs groupes HA.

   Si vous créez des points de terminaison d'interface de gestion, sélectionnez les VIP associés uniquement aux Admin Nodes.

3. Si vous avez sélectionné **Interfaces de nœud**, sélectionnez une ou plusieurs interfaces de nœud pour chaque nœud d'administration ou nœud de passerelle que vous souhaitez associer à ce point de terminaison.
4. Si vous avez sélectionné **Type de nœud**, sélectionnez soit Admin Nodes, qui comprend à la fois le primary Admin Node et tous les non-primary Admin Nodes, soit Gateway Nodes.

Contrôler l'accès des locataires

Un point de terminaison d'interface de gestion ne peut contrôler l'accès des locataires que lorsque le point de terminaison possède le type d'interface de Tenant Manager.

Étapes

1. Pour l'étape **Accès locataire**, sélectionnez l'une des options suivantes :

Champ	Description
Autoriser tous les locataires (par défaut)	Tous les comptes locataires peuvent utiliser ce point de terminaison pour accéder à leurs compartiments. Vous devez sélectionner cette option si vous n'avez pas encore créé de comptes locataires. Après avoir ajouté des comptes locataires, vous pouvez modifier le point de terminaison de l'équilibreur de charge pour autoriser ou bloquer des comptes spécifiques.
Autoriser les locataires sélectionnés	Seuls les comptes locataires sélectionnés peuvent utiliser ce point de terminaison pour accéder à leurs compartiments.
Bloquer les locataires sélectionnés	Les comptes locataires sélectionnés ne peuvent pas utiliser ce point de terminaison pour accéder à leurs compartiments. Tous les autres locataires peuvent utiliser ce point de terminaison.

2. Si vous créez un point de terminaison **HTTP**, vous n'avez pas besoin d'associer un certificat. Sélectionnez **Créer** pour ajouter le nouveau point de terminaison d'équilibrage de charge. Ensuite, accédez à Après avoir terminé. Sinon, sélectionnez **Continuer** pour associer le certificat.

Joindre le certificat

Étapes

1. Si vous créez un point de terminaison **HTTPS**, sélectionnez le type de certificat de sécurité que vous souhaitez associer au point de terminaison.

   Le certificat sécurise les connexions entre les clients S3 et le service Load Balancer sur le nœud d'administration ou les nœuds de passerelle.

   - **Téléverser un certificat**. Sélectionnez cette option si vous avez des certificats personnalisés à téléverser.
   - **Générer un certificat**. Sélectionnez cette option si vous disposez des informations nécessaires pour générer un certificat personnalisé.
   - **Utiliser le certificat StorageGRID S3**. Sélectionnez cette option si vous souhaitez utiliser le certificat global de l'API S3, qui peut également être utilisé pour les connexions directes aux nœuds de stockage.

     Vous ne pouvez pas sélectionner cette option à moins d'avoir remplacé le certificat API S3 par défaut, qui est signé par l'AC du grid, par un certificat personnalisé signé par une autorité de certification externe. Voir "Configurer les certificats de l'API S3".

   - **Utiliser le certificat d'interface de gestion**. Sélectionnez cette option si vous souhaitez utiliser le certificat d'interface de gestion global, qui peut également être utilisé pour les connexions directes aux nœuds d'administration.
2. Si vous n'utilisez pas le certificat S3 StorageGRID, téléchargez-le ou générez-le.

Télécharger le certificat

a. Sélectionnez **Téléverser le certificat**.

b. Téléversez les fichiers de certificat serveur requis :

- **Certificat serveur** : Le fichier de certificat serveur personnalisé 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 **Créer**. + Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et le point de terminaison.

Générer un certificat

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.
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.

Champ	Description
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 **Create**.

Le point de terminaison de l'équilibreur de charge est créé. Le certificat personnalisé est utilisé pour toutes les nouvelles connexions ultérieures entre les clients S3 ou l'interface de gestion et ce point de terminaison.

Après avoir terminé

Étapes

1. Si vous utilisez un DNS, assurez-vous que celui-ci inclut un enregistrement permettant d'associer le nom de domaine complet (FQDN) de StorageGRID à chaque adresse IP que les clients utiliseront pour établir des connexions.

   L'adresse IP que vous saisissez dans l'enregistrement DNS dépend du fait que vous utilisiez ou non un groupe HA de nœuds d'équilibrage de charge :

   - Si vous avez configuré un groupe HA, les clients se connecteront aux adresses IP virtuelles de ce groupe HA.
   - Si vous n'utilisez pas de groupe HA, les clients se connecteront au service d'équilibrage de charge StorageGRID en utilisant l'adresse IP d'un nœud de passerelle ou d'un nœud d'administration.

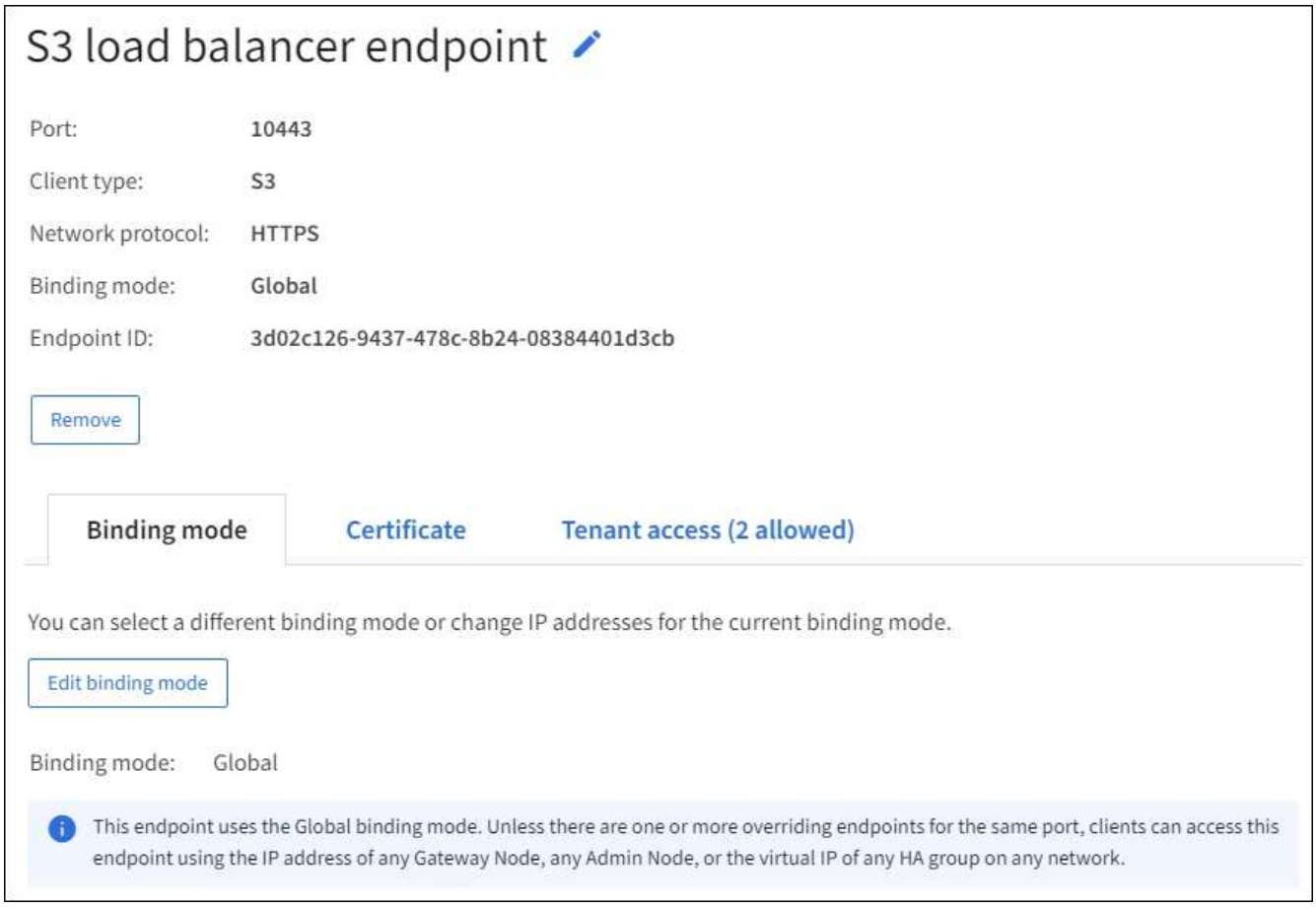
   Vous devez également vous assurer que l'enregistrement DNS référence tous les noms de domaine de point de terminaison requis, y compris les noms génériques.

2. Fournissez aux clients S3 les informations nécessaires pour se connecter au point de terminaison :
    - Numéro de port
    - nom de domaine complet ou adresse IP
    - Tous les détails de certificat requis

Afficher et modifier les points de terminaison de l'équilibreur de charge

Vous pouvez consulter les détails des points de terminaison d'équilibrage de charge existants, y compris les métadonnées du certificat d'un point de terminaison sécurisé. Vous pouvez modifier certains paramètres d'un point de terminaison.

- Pour consulter les informations de base de tous les points de terminaison de l'équilibreur de charge, consultez les tableaux de la page Points de terminaison de l'équilibreur de charge.
- Pour afficher tous les détails d'un point de terminaison spécifique, y compris les métadonnées du certificat, sélectionnez le nom du point de terminaison dans le tableau. Les informations affichées varient selon le type de point de terminaison et la façon dont il est configuré.



- Pour modifier un point de terminaison, utilisez le menu **Actions** sur la page des points de terminaison de l'équilibreur de charge.

> Si vous perdez l'accès à Grid Manager lors de la modification du port d'un point de terminaison d'interface de gestion, mettez à jour l'URL et le port pour rétablir l'accès.

Après avoir modifié un point de terminaison, vous devrez peut-être attendre jusqu'à 15 minutes pour que vos modifications soient appliquées à tous les nœuds.

Tâche	Menu Actions	Page de détails
Modifier le nom du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le nom du point de terminaison**. c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'icône de modification . c. Saisissez le nouveau nom. d. Sélectionnez **Enregistrer**.
Modifier le port du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le port du point de terminaison** c. Veuillez saisir un numéro de port valide. d. Sélectionnez **Enregistrer**.	*n/a*
Modifier le mode de liaison du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le mode de liaison du point de terminaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez **Modifier le mode de liaison**. c. Mettez à jour le mode de liaison si nécessaire. d. Sélectionnez **Save changes**.
Modifier le certificat du point de terminaison	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier le certificat du point de terminaison**. c. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon les besoins. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet **Certificat**. c. Sélectionnez **Modifier le certificat**. d. Téléchargez ou générez un nouveau certificat personnalisé ou commencez à utiliser le certificat S3 global, selon les besoins. e. Sélectionnez **Save changes**.

Tâche	Menu Actions	Page de détails
Modifier l'accès du locataire	a. Cochez la case correspondant au point de terminaison. b. Sélectionnez **Actions** > **Modifier l'accès du locataire**. c. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. d. Sélectionnez **Save changes**.	a. Sélectionnez le nom du point de terminaison pour afficher les détails. b. Sélectionnez l'onglet **Accès locataire**. c. Sélectionnez **Modifier l'accès du locataire**. d. Choisissez une autre option d'accès, sélectionnez ou supprimez des locataires de la liste, ou faites les deux. e. Sélectionnez **Save changes**.

Supprimez les points de terminaison de l'équilibreur de charge

Vous pouvez supprimer un ou plusieurs points de terminaison à l'aide du menu **Actions**, ou vous pouvez supprimer un seul point de terminaison à partir de la page de détails.

> Pour éviter toute interruption de service client, mettez à jour les applications clientes S3 concernées avant de supprimer un point de terminaison d'équilibreur de charge. Mettez à jour chaque client pour qu'il se connecte à l'aide d'un port attribué à un autre point de terminaison d'équilibreur de charge. Veillez également à mettre à jour les informations de certificat requises.

> Si vous perdez l'accès à Grid Manager lors de la suppression d'un point de terminaison d'interface de gestion, mettez à jour l'URL.

- Pour supprimer un ou plusieurs points de terminaison :
  a. Sur la page de l'équilibreur de charge, cochez la case correspondant à chaque point de terminaison que vous souhaitez supprimer.
  b. Sélectionnez **Actions** > **Supprimer**.
  c. Sélectionnez **OK**.
- Pour supprimer un point de terminaison de la page de détails :
  a. Sur la page de l'équilibreur de charge, sélectionnez le nom du point de terminaison.
  b. Sélectionnez **Supprimer** sur la page de détails.
  c. Sélectionnez **OK**.