Préparez les hôtes (Ubuntu ou Debian)

StorageGRID software

NetApp
December 03, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/storagegrid-119/ubuntu/how-host-wide-settings-change.html on December 03, 2025. Always check docs.netapp.com for the latest.

Sommaire

Préparez les hôtes (Ubuntu ou Debian)

Comment les paramètres à l'échelle de l'hôte changent pendant l'installation

Sur les systèmes bare metal, StorageGRID apporte quelques modifications à l'échelle de l'hôte `sysctl` paramètres.

Les modifications suivantes sont apportées :

```
# Recommended Cassandra setting: CASSANDRA-3563, CASSANDRA-13008, DataStax
documentation
vm.max_map_count = 1048575

# core file customization
# Note: for cores generated by binaries running inside containers, this
# path is interpreted relative to the container filesystem namespace.
# External cores will go nowhere, unless /var/local/core also exists on
# the host.
kernel.core_pattern = /var/local/core/%e.core.%p

# Set the kernel minimum free memory to the greater of the current value
or
# 512MiB if the host has 48GiB or less of RAM or 1.83GiB if the host has
more than 48GiB of RTAM
vm.min_free_kbytes = 524288

# Enforce current default swappiness value to ensure the VM system has
some
# flexibility to garbage collect behind anonymous mappings. Bump
watermark_scale_factor
# to help avoid OOM conditions in the kernel during memory allocation
bursts. Bump
# dirty_ratio to 90 because we explicitly fsync data that needs to be
persistent, and
# so do not require the dirty_ratio safety net. A low dirty_ratio combined
with a large
# working set (nr_active_pages) can cause us to enter synchronous I/O mode
unnecessarily,
# with deleterious effects on performance.
vm.swappiness = 60
vm.watermark_scale_factor = 200
vm.dirty_ratio = 90

# Turn off slow start after idle
```

```
net.ipv4.tcp_slow_start_after_idle = 0

# Tune TCP window settings to improve throughput
net.core.rmem_max = 8388608
net.core.wmem_max = 8388608
net.ipv4.tcp_rmem = 4096 524288 8388608
net.ipv4.tcp_wmem = 4096 262144 8388608
net.core.netdev_max_backlog = 2500

# Turn on MTU probing
net.ipv4.tcp_mtu_probing = 1

# Be more liberal with firewall connection tracking
net.ipv4.netfilter.ip_conntrack_tcp_be_liberal = 1

# Reduce TCP keepalive time to reasonable levels to terminate dead
connections
net.ipv4.tcp_keepalive_time = 270
net.ipv4.tcp_keepalive_probes = 3
net.ipv4.tcp_keepalive_intvl = 30

# Increase the ARP cache size to tolerate being in a /16 subnet
net.ipv4.neigh.default.gc_thresh1 = 8192
net.ipv4.neigh.default.gc_thresh2 = 32768
net.ipv4.neigh.default.gc_thresh3 = 65536
net.ipv6.neigh.default.gc_thresh1 = 8192
net.ipv6.neigh.default.gc_thresh2 = 32768
net.ipv6.neigh.default.gc_thresh3 = 65536

# Disable IP forwarding, we are not a router
net.ipv4.ip_forward = 0

# Follow security best practices for ignoring broadcast ping requests
net.ipv4.icmp_echo_ignore_broadcasts = 1

# Increase the pending connection and accept backlog to handle larger
connection bursts.
net.core.somaxconn=4096
net.ipv4.tcp_max_syn_backlog=4096
```

Installer Linux

Vous devez installer StorageGRID sur tous les hôtes de grille Ubuntu ou Debian. Pour obtenir la liste des versions prises en charge, utilisez l'outil de matrice d'interopérabilité NetApp .

Avant de commencer

Assurez-vous que votre système d'exploitation répond aux exigences minimales de version du noyau de StorageGRID, comme indiqué ci-dessous. Utilisez la commande `uname -r` pour obtenir la version du noyau de votre système d'exploitation ou consultez le fournisseur de votre système d'exploitation.

Remarque : la prise en charge des versions Ubuntu 18.04 et 20.04 est obsolète et sera supprimée dans une prochaine version.

Version d'Ubuntu	Version minimale du noyau	Nom du paquet du noyau
18.04.6 (obsolète)	5.4.0-150-générique	linux-image-5.4.0-150-generic/bionic-updates,bionic-security,maintenant 5.4.0-150.167~18.04.1
20.04.5 (obsolète)	5.4.0-131-générique	linux-image-5.4.0-131-generic/focal-updates, maintenant 5.4.0-131.147
22.04.1	5.15.0-47-générique	linux-image-5.15.0-47-generic/jammy-updates,jammy-security,maintenant 5.15.0-47.51
24,04	6.8.0-31-générique	linux-image-6.8.0-31-generic/noble, maintenant 6.8.0-31.31

Remarque : la prise en charge de la version 11 de Debian est obsolète et sera supprimée dans une prochaine version.

Version Debian	Version minimale du noyau	Nom du paquet du noyau
11 (obsolète)	5.10.0-18-amd64	linux-image-5.10.0-18-amd64/stable, maintenant 5.10.150-1
12	6.1.0-9-amd64	linux-image-6.1.0-9-amd64/stable, maintenant 6.1.27-1

Étapes

1. Installez Linux sur tous les hôtes de grille physiques ou virtuels conformément aux instructions du distributeur ou à votre procédure standard.

   > N'installez aucun environnement de bureau graphique. Lors de l'installation d'Ubuntu, vous devez sélectionner les **utilitaires système standard**. Il est recommandé de sélectionner **Serveur OpenSSH** pour activer l'accès ssh à vos hôtes Ubuntu. Toutes les autres options peuvent rester désactivées.

2. Assurez-vous que tous les hôtes ont accès aux référentiels de packages Ubuntu ou Debian.
3. Si l'échange est activé :
   a. Exécutez la commande suivante : `$ sudo swapoff --all`
   b. Supprimer toutes les entrées d'échange de `/etc/fstab` pour conserver les paramètres.

Ne pas désactiver complètement l'échange peut réduire considérablement les performances.

Comprendre l'installation du profil AppArmor

Si vous travaillez dans un environnement Ubuntu auto-déployé et utilisez le système de contrôle d'accès obligatoire AppArmor, les profils AppArmor associés aux packages que vous installez sur le système de base peuvent être bloqués par les packages correspondants installés avec StorageGRID.

Par défaut, les profils AppArmor sont installés pour les packages que vous installez sur le système d'exploitation de base. Lorsque vous exécutez ces packages à partir du conteneur système StorageGRID , les profils AppArmor sont bloqués. Les packages de base DHCP, MySQL, NTP et tcdump sont en conflit avec AppArmor, et d'autres packages de base peuvent également être en conflit.

Vous avez deux choix pour gérer les profils AppArmor :

- Désactivez les profils individuels pour les packages installés sur le système de base qui chevauchent les packages du conteneur système StorageGRID . Lorsque vous désactivez des profils individuels, une entrée apparaît dans les fichiers journaux StorageGRID indiquant qu'AppArmor est activé.

  Utilisez les commandes suivantes :

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

  Exemple:

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- Désactivez complètement AppArmor. Pour Ubuntu 9.10 ou version ultérieure, suivez les instructions de la communauté en ligne Ubuntu : "Désactiver AppArmor" . La désactivation complète d'AppArmor peut ne pas être possible sur les versions plus récentes d'Ubuntu.

  Une fois AppArmor désactivé, aucune entrée indiquant qu'AppArmor est activé n'apparaîtra dans les fichiers journaux StorageGRID .

Configurer le réseau hôte (Ubuntu ou Debian)

Une fois l'installation de Linux terminée sur vos hôtes, vous devrez peut-être effectuer une configuration supplémentaire pour préparer un ensemble d'interfaces réseau sur chaque hôte adaptées au mappage dans les nœuds StorageGRID que vous déploierez ultérieurement.

Avant de commencer

- Vous avez examiné le"Directives de mise en réseau StorageGRID" .
- Vous avez examiné les informations sur"exigences de migration des conteneurs de nœuds" .
- Si vous utilisez des hôtes virtuels, vous avez lu leconsidérations et recommandations pour le clonage d'adresses MAC avant de configurer le réseau hôte.

> Si vous utilisez des machines virtuelles comme hôtes, vous devez sélectionner VMXNET 3 comme adaptateur réseau virtuel. L'adaptateur réseau VMware E1000 a provoqué des problèmes de connectivité avec les conteneurs StorageGRID déployés sur certaines distributions de Linux.

À propos de cette tâche

Les nœuds de grille doivent pouvoir accéder au réseau de grille et, éventuellement, aux réseaux d'administration et de client. Vous fournissez cet accès en créant des mappages qui associent l'interface physique de l'hôte aux interfaces virtuelles de chaque nœud de grille. Lors de la création d'interfaces d'hôte, utilisez des noms conviviaux pour faciliter le déploiement sur tous les hôtes et pour permettre la migration.

La même interface peut être partagée entre l'hôte et un ou plusieurs nœuds. Par exemple, vous pouvez utiliser la même interface pour l'accès à l'hôte et l'accès au réseau d'administration du nœud, afin de faciliter la maintenance de l'hôte et du nœud. Bien que la même interface puisse être partagée entre l'hôte et les nœuds individuels, tous doivent avoir des adresses IP différentes. Les adresses IP ne peuvent pas être partagées entre les nœuds ou entre l'hôte et un nœud.

Vous pouvez utiliser la même interface réseau hôte pour fournir l'interface réseau Grid pour tous les nœuds StorageGRID sur l'hôte ; vous pouvez utiliser une interface réseau hôte différente pour chaque nœud ; ou vous pouvez faire quelque chose entre les deux. Cependant, vous ne fournirez généralement pas la même interface réseau hôte que les interfaces réseau Grid et Admin pour un seul nœud, ou comme interface réseau Grid pour un nœud et comme interface réseau client pour un autre.

Vous pouvez réaliser cette tâche de plusieurs manières. Par exemple, si vos hôtes sont des machines virtuelles et que vous déployez un ou deux nœuds StorageGRID pour chaque hôte, vous pouvez créer le nombre correct d'interfaces réseau dans l'hyperviseur et utiliser un mappage 1 à 1. Si vous déployez plusieurs nœuds sur des hôtes bare metal pour une utilisation en production, vous pouvez tirer parti de la prise en charge de la pile réseau Linux pour VLAN et LACP pour la tolérance aux pannes et le partage de bande passante. Les sections suivantes fournissent des approches détaillées pour ces deux exemples. Vous n'avez pas besoin d'utiliser l'un ou l'autre de ces exemples ; vous pouvez utiliser n'importe quelle approche qui répond à vos besoins.

> N'utilisez pas de périphériques de liaison ou de pont directement comme interface réseau du conteneur. Cela pourrait empêcher le démarrage du nœud causé par un problème de noyau avec l'utilisation de MACVLAN avec des périphériques de liaison et de pont dans l'espace de noms du conteneur. Utilisez plutôt un périphérique non lié, tel qu'un VLAN ou une paire Ethernet virtuelle (veth). Spécifiez ce périphérique comme interface réseau dans le fichier de configuration du nœud.

Considérations et recommandations pour le clonage d'adresses MAC

Le clonage d'adresse MAC amène le conteneur à utiliser l'adresse MAC de l'hôte, et l'hôte à utiliser l'adresse MAC d'une adresse que vous spécifiez ou d'une adresse générée aléatoirement. Vous devez utiliser le clonage d'adresse MAC pour éviter l'utilisation de configurations réseau en mode promiscuité.

Activation du clonage MAC

Dans certains environnements, la sécurité peut être améliorée grâce au clonage d'adresse MAC, car cela vous permet d'utiliser une carte réseau virtuelle dédiée pour le réseau d'administration, le réseau de grille et le réseau client. Le fait que le conteneur utilise l'adresse MAC de la carte réseau dédiée sur l'hôte vous permet d'éviter d'utiliser des configurations réseau en mode promiscuité.

> Le clonage d'adresse MAC est destiné à être utilisé avec des installations de serveur virtuel et peut ne pas fonctionner correctement avec toutes les configurations d'appareils physiques.

> Si un nœud ne parvient pas à démarrer en raison d'une interface ciblée de clonage MAC occupée, vous devrez peut-être définir le lien sur « down » avant de démarrer le nœud. De plus, il est possible que l'environnement virtuel empêche le clonage MAC sur une interface réseau pendant que la liaison est active. Si un nœud ne parvient pas à définir l'adresse MAC et à démarrer en raison d'une interface occupée, définir le lien sur « down » avant de démarrer le nœud peut résoudre le problème.

Le clonage d'adresse MAC est désactivé par défaut et doit être défini par les clés de configuration du nœud. Vous devez l'activer lorsque vous installez StorageGRID.

Il existe une clé pour chaque réseau :

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

La définition de la clé sur « true » oblige le conteneur à utiliser l'adresse MAC de la carte réseau de l'hôte. De plus, l'hôte utilisera ensuite l'adresse MAC du réseau de conteneurs spécifié. Par défaut, l'adresse du conteneur est une adresse générée aléatoirement, mais si vous en avez défini une à l'aide de l'`_NETWORK_MAC` clé de configuration du nœud, cette adresse est utilisée à la place. L'hôte et le conteneur auront toujours des adresses MAC différentes.

> L'activation du clonage MAC sur un hôte virtuel sans activer également le mode promiscuité sur l'hyperviseur peut entraîner l'arrêt du fonctionnement du réseau hôte Linux utilisant l'interface de l'hôte.

Cas d'utilisation du clonage MAC

Il y a deux cas d'utilisation à prendre en compte avec le clonage MAC :

- Clonage MAC non activé : lorsque le `_CLONE_MAC` Si la clé dans le fichier de configuration du nœud n'est pas définie ou définie sur « false », l'hôte utilisera le MAC de la carte réseau de l'hôte et le conteneur aura un MAC généré par StorageGRID, sauf si un MAC est spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, le conteneur aura l'adresse spécifiée dans le `_NETWORK_MAC` clé. Cette configuration de clés nécessite l'utilisation du mode promiscuité.
- Clonage MAC activé : lorsque le `_CLONE_MAC` dans le fichier de configuration du nœud est définie sur « true », le conteneur utilise le MAC de la carte réseau de l'hôte et l'hôte utilise un MAC généré par StorageGRID, sauf si un MAC est spécifié dans le `_NETWORK_MAC` clé. Si une adresse est définie dans le `_NETWORK_MAC` clé, l'hôte utilise l'adresse spécifiée au lieu d'une adresse générée. Dans cette configuration de touches, vous ne devez pas utiliser le mode promiscuité.

Si vous ne souhaitez pas utiliser le clonage d'adresse MAC et préférez autoriser toutes les interfaces à recevoir et à transmettre des données pour des adresses MAC autres que celles attribuées par l'hyperviseur, assurez-vous que les propriétés de sécurité au niveau du commutateur virtuel et du groupe de ports sont définies sur **Accepter** pour le mode promiscuité, les modifications d'adresse MAC et les transmissions falsifiées. Les valeurs définies sur le commutateur virtuel peuvent être remplacées par les valeurs au niveau du groupe de ports. Assurez-vous donc que les paramètres sont les mêmes aux deux endroits.

Pour activer le clonage MAC, consultez le"instructions pour créer des fichiers de configuration de nœud" .

Exemple de clonage MAC

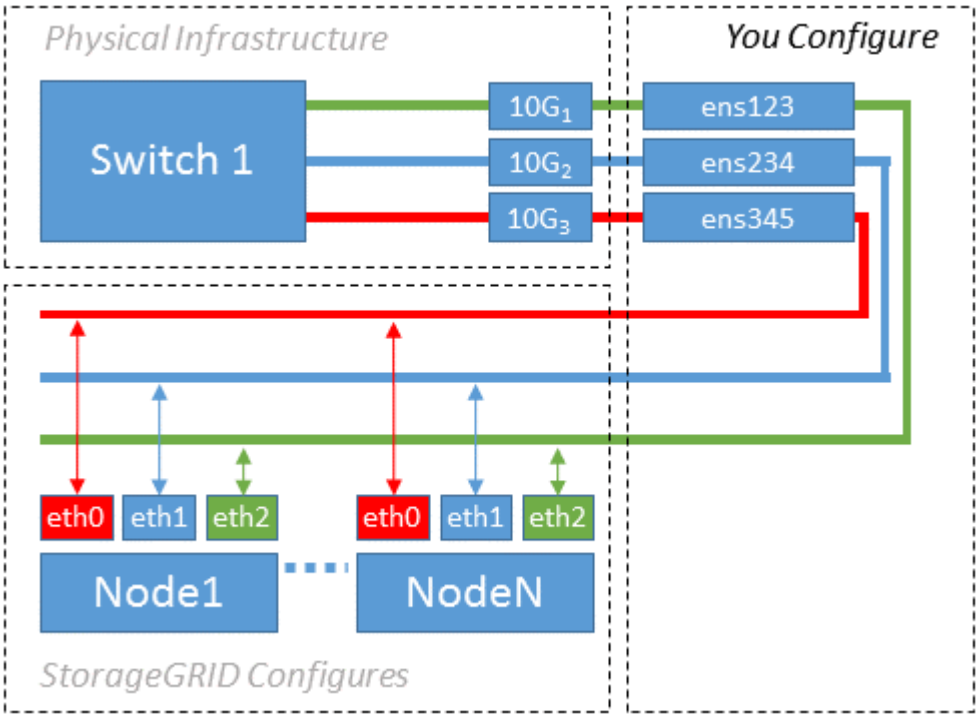
Exemple de clonage MAC activé avec un hôte ayant l'adresse MAC 11:22:33:44:55:66 pour l'interface ens256 et les clés suivantes dans le fichier de configuration du nœud :

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Résultat : l'adresse MAC de l'hôte pour ens256 est b2:9c:02:c2:27:10 et l'adresse MAC du réseau administrateur est 11:22:33:44:55:66

Exemple 1 : mappage 1 à 1 vers des cartes réseau physiques ou virtuelles

L'exemple 1 décrit un mappage d'interface physique simple qui nécessite peu ou pas de configuration côté hôte.



Le système d'exploitation Linux crée automatiquement les interfaces ensXYZ lors de l'installation ou du démarrage, ou lorsque les interfaces sont ajoutées à chaud. Aucune configuration n'est requise, si ce n'est de s'assurer que les interfaces sont configurées pour s'afficher automatiquement après le démarrage. Vous devez

déterminer quel ensXYZ correspond à quel réseau StorageGRID (Grid, Admin ou Client) afin de pouvoir fournir les mappages corrects plus tard dans le processus de configuration.

Notez que la figure montre plusieurs nœuds StorageGRID ; cependant, vous utiliseriez normalement cette configuration pour les machines virtuelles à nœud unique.

Si le commutateur 1 est un commutateur physique, vous devez configurer les ports connectés aux interfaces $10G_1$ à $10G_3$ pour le mode d'accès et les placer sur les VLAN appropriés.

Exemple 2 : liaison LACP transportant des VLAN

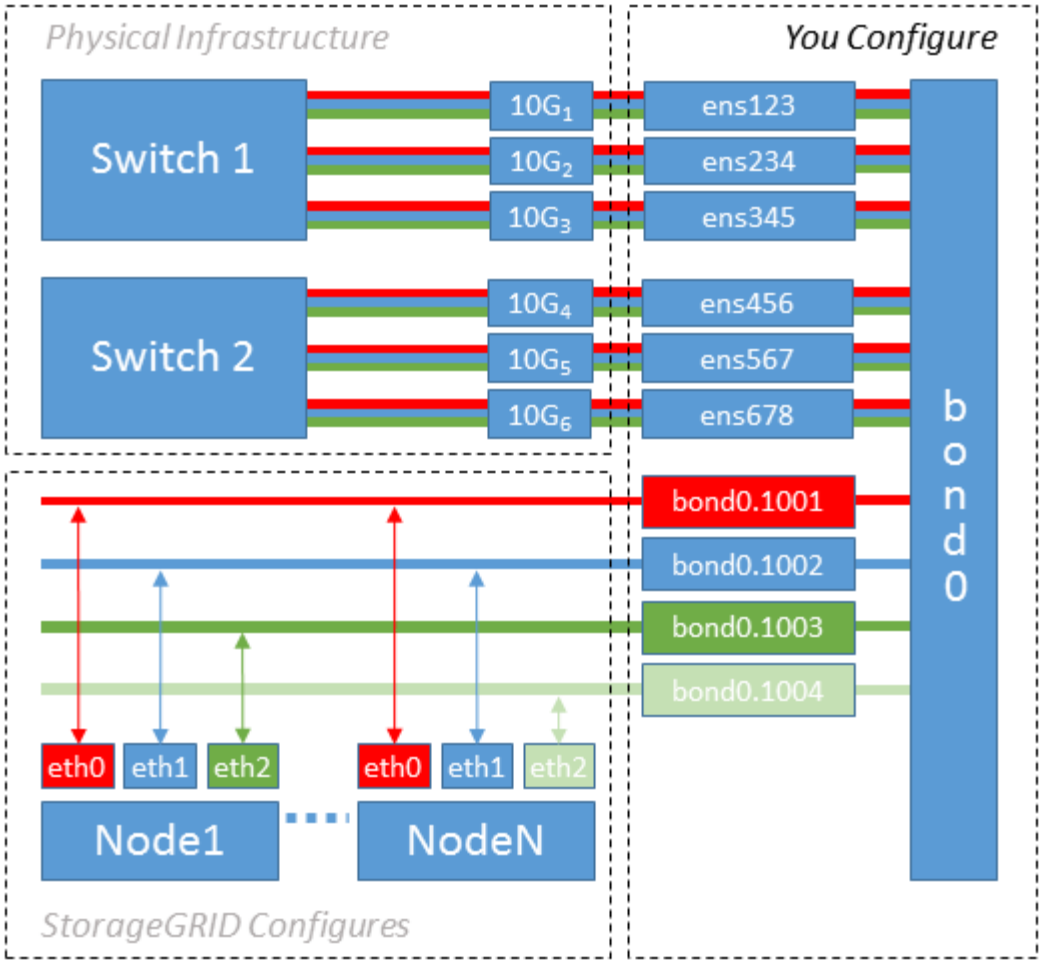
L'exemple 2 suppose que vous êtes familiarisé avec la liaison d'interfaces réseau et avec la création d'interfaces VLAN sur la distribution Linux que vous utilisez.

À propos de cette tâche

L'exemple 2 décrit un schéma générique, flexible et basé sur le VLAN qui facilite le partage de toute la bande passante réseau disponible sur tous les nœuds d'un seul hôte. Cet exemple est particulièrement applicable aux hôtes bare metal.

Pour comprendre cet exemple, supposons que vous disposez de trois sous-réseaux distincts pour les réseaux Grid, Admin et Client dans chaque centre de données. Les sous-réseaux se trouvent sur des VLAN distincts (1001, 1002 et 1003) et sont présentés à l'hôte sur un port de jonction lié LACP (bond0). Vous devez configurer trois interfaces VLAN sur la liaison : bond0.1001, bond0.1002 et bond0.1003.

Si vous avez besoin de VLAN et de sous-réseaux distincts pour les réseaux de nœuds sur le même hôte, vous pouvez ajouter des interfaces VLAN sur la liaison et les mapper dans l'hôte (affiché comme bond0.1004 dans l'illustration).



Étapes

1. Regroupez toutes les interfaces réseau physiques qui seront utilisées pour la connectivité réseau StorageGRID dans une seule liaison LACP.

   Utilisez le même nom pour la liaison sur chaque hôte, par exemple, bond0.

2. Créez des interfaces VLAN qui utilisent cette liaison comme « périphérique physique » associé, en utilisant la convention de dénomination d'interface VLAN standard `physdev-name.VLAN ID`.

   Notez que les étapes 1 et 2 nécessitent une configuration appropriée sur les commutateurs de périphérie terminant les autres extrémités des liaisons réseau. Les ports du commutateur périphérique doivent également être regroupés dans un canal de port LACP, configurés en tant que jonction et autorisés à transmettre tous les VLAN requis.

   Des exemples de fichiers de configuration d'interface pour ce schéma de configuration réseau par hôte sont fournis.

Informations connexes

"Exemple /etc/network/interfaces"

Configurer le stockage hôte

Vous devez allouer des volumes de stockage en blocs à chaque hôte.

Avant de commencer

Vous avez examiné les rubriques suivantes, qui fournissent les informations dont vous avez besoin pour accomplir cette tâche :

- "Exigences de stockage et de performances"
- "Exigences de migration des conteneurs de nœuds"

À propos de cette tâche

Lors de l'allocation de volumes de stockage en blocs (LUN) aux hôtes, utilisez les tableaux de la section « Exigences de stockage » pour déterminer les éléments suivants :

- Nombre de volumes requis pour chaque hôte (en fonction du nombre et des types de nœuds qui seront déployés sur cet hôte)
- Catégorie de stockage pour chaque volume (c'est-à-dire, données système ou données d'objet)
- Taille de chaque volume

Vous utiliserez ces informations ainsi que le nom persistant attribué par Linux à chaque volume physique lorsque vous déploierez des nœuds StorageGRID sur l'hôte.

Vous n'avez pas besoin de partitionner, de formater ou de monter l'un de ces volumes ; vous devez simplement vous assurer qu'ils sont visibles pour les hôtes.

Un seul LUN de données d'objet est requis pour les nœuds de stockage contenant uniquement des métadonnées.

Évitez d'utiliser des fichiers d'appareil spéciaux « bruts »(`/dev/sdb` , par exemple) lorsque vous composez votre liste de noms de volumes. Ces fichiers peuvent changer lors des redémarrages de l'hôte, ce qui aura un impact sur le bon fonctionnement du système. Si vous utilisez des LUN iSCSI et un mappeur de périphériques multi-chemins, pensez à utiliser des alias multi-chemins dans le `/dev/mapper` répertoire, en particulier si votre topologie SAN inclut des chemins réseau redondants vers le stockage partagé. Alternativement, vous pouvez utiliser les liens logiciels créés par le système sous `/dev/disk/by-path/` pour vos noms d'appareils persistants.

Par exemple:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Les résultats seront différents pour chaque installation.

Attribuez des noms conviviaux à chacun de ces volumes de stockage en blocs pour simplifier l'installation initiale de StorageGRID et les procédures de maintenance futures. Si vous utilisez le pilote multi-chemins du mappeur de périphériques pour un accès redondant aux volumes de stockage partagés, vous pouvez utiliser le `alias` champ dans votre `/etc/multipath.conf` déposer.

Par exemple:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

L'utilisation du champ alias de cette manière fait apparaître les alias comme des périphériques de bloc dans le `/dev/mapper` répertoire sur l'hôte, vous permettant de spécifier un nom convivial et facilement validé chaque fois qu'une opération de configuration ou de maintenance nécessite la spécification d'un volume de stockage en bloc.

Si vous configurez un stockage partagé pour prendre en charge la migration des nœuds StorageGRID et utilisez Device Mapper Multipathing, vous pouvez créer et installer un stockage partagé commun. `/etc/multipath.conf` sur tous les hôtes colocalisés. Assurez-vous simplement d'utiliser un volume de stockage Docker différent sur chaque hôte. L'utilisation d'alias et l'inclusion du nom d'hôte cible dans l'alias pour chaque LUN de volume de stockage Docker rendront cela facile à mémoriser et sont recommandées.

> La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

Informations connexes

- "Exigences de stockage et de performances"
- "Exigences de migration des conteneurs de nœuds"

Configurer le volume de stockage du moteur de conteneur

Avant d'installer le moteur de conteneur (Docker ou Podman), vous devrez peut-être formater le volume de stockage et le monter.

> La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

À propos de cette tâche

Vous pouvez ignorer ces étapes si vous prévoyez d'utiliser le stockage local pour le volume de stockage Docker et que vous disposez de suffisamment d'espace disponible sur la partition hôte contenant `/var/lib` .

Étapes

1. Créez un système de fichiers sur le volume de stockage Docker :

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Montez le volume de stockage Docker :

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Ajoutez une entrée pour docker-storage-volume-device à /etc/fstab.

   Cette étape garantit que le volume de stockage sera remonté automatiquement après le redémarrage de l'hôte.

Installer Docker

Le système StorageGRID fonctionne sous Linux en tant que collection de conteneurs Docker. Avant de pouvoir installer StorageGRID, vous devez installer Docker.

> La prise en charge de Docker comme moteur de conteneur pour les déploiements uniquement logiciels est obsolète. Docker sera remplacé par un autre moteur de conteneur dans une prochaine version.

Étapes

1. Installez Docker en suivant les instructions de votre distribution Linux.

   > Si Docker n'est pas inclus dans votre distribution Linux, vous pouvez le télécharger à partir du site Web de Docker.

2. Assurez-vous que Docker a été activé et démarré en exécutant les deux commandes suivantes :

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirmez que vous avez installé la version attendue de Docker en saisissant ce qui suit :

```
sudo docker version
```

Les versions Client et Serveur doivent être 1.11.0 ou ultérieures.

Informations connexes

"Configurer le stockage hôte"

Installer les services hôtes StorageGRID

Vous utilisez le package DEB StorageGRID pour installer les services hôtes StorageGRID .

À propos de cette tâche

Ces instructions décrivent comment installer les services hôtes à partir des packages DEB. Comme alternative, vous pouvez utiliser les métadonnées du référentiel APT incluses dans l'archive d'installation pour installer les packages DEB à distance. Consultez les instructions du référentiel APT pour votre système d'exploitation Linux.

Étapes

1. Copiez les packages DEB StorageGRID sur chacun de vos hôtes ou rendez-les disponibles sur un stockage partagé.

   Par exemple, placez-les dans le `/tmp` répertoire, vous pouvez donc utiliser l'exemple de commande à l'étape suivante.

2. Connectez-vous à chaque hôte en tant que root ou en utilisant un compte avec l'autorisation sudo et exécutez les commandes suivantes.

   Vous devez installer le `images` paquet d'abord, et le `service` paquet deuxième. Si vous avez placé les packages dans un répertoire autre que `/tmp` , modifiez la commande pour refléter le chemin que vous avez utilisé.

```
sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
```

```
sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
```

Python 2,7 doit déjà être installé avant que les packages StorageGRID puissent être installés. Le `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` la commande échouera jusqu'à ce que vous l'ayez fait.

Informations sur le copyright

Copyright © 2025 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 DÉLICTUELLE (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.