



# Mise en grappe pour Threat Defense Virtual dans un nuage public

La mise en grappe vous permet de regrouper plusieurs Défense contre les menaces virtuelles en un seul périphérique logique. Une grappe offre toute la commodité d'un seul appareil (gestion, intégration dans un réseau), tout en offrant le débit accru et la redondance de plusieurs périphériques. Vous pouvez déployer des grappes Défense contre les menaces virtuelles dans un nuage public en utilisant les plateformes de nuage public suivantes :

- Amazon Web Services (AWS)
- Microsoft Azure
- Google Cloud Platform (GCP)

Actuellement, seul le mode pare-feu routé est pris en charge.



**Remarque** Certaines fonctionnalités ne sont pas prises en charge lors de l'utilisation de la mise en grappe. Consultez [Fonctionnalités et mise en grappe non prises en charge](#), à la page 71.

- [À propos de la mise en grappe de Threat Defense Virtual dans un nuage public](#), à la page 2
- [Licences pour la mise en grappe Threat Defense Virtual](#), à la page 4
- [Exigences et conditions préalables pour la mise en grappe Threat Defense Virtual](#), à la page 5
- [Lignes directrices pour la mise en grappe virtuelle Threat Defense](#), à la page 7
- [Déployer la grappe dans AWS](#), à la page 8
- [Déployer la grappe dans Azure](#), à la page 22
- [Déployer la grappe dans GCP](#), à la page 42
- [Ajouter la grappe au centre de gestion \(déploiement manuel\)](#), à la page 50
- [Configurer les paramètres de surveillance de l'intégrité de la grappe](#), à la page 57
- [Gérer les nœuds de la grappe](#), à la page 61
- [Surveillance de la grappe](#), à la page 64
- [Mise à niveau de la grappe](#), à la page 70
- [Référence pour la mise en grappe](#), à la page 71
- [Historique des mises en grappe Threat Defense Virtual dans le nuage public](#), à la page 83

# À propos de la mise en grappe de Threat Defense Virtual dans un nuage public

Cette section décrit l'architecture de mise en grappe et son fonctionnement.

## Intégration de la grappe dans votre réseau

La grappe se compose de plusieurs pare-feu agissant comme un seul périphérique. Pour agir comme une grappe, les pare-feu ont besoin de l'infrastructure suivante :

- Réseau isolé pour la communication intra-grappe, appelé *liaison de commande de grappe*, qui utilise des interfaces VXLAN. Les VXLAN, qui agissent comme des réseaux virtuels de couche 2 sur des réseaux physiques de couche 3, permettent au Défense contre les menaces virtuelles d'envoyer des messages en diffusion ou en multidiffusion sur la liaison de commande de grappe.
- Équilibreur(s) de charge : pour l'équilibrage de charge externe, vous avez les options suivantes en fonction de votre nuage public :

- Équilibreur de charge de passerelle AWS

L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Le Défense contre les menaces virtuelles prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point terminal de l'équilibreur de charge de passerelle) à l'aide d'un serveur mandataire à un seul bras d'interface de Geneve.

- Équilibreur de charge de la passerelle Azure

Dans une chaîne de service Azure, les Défense contre les menaces virtuelles agissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. Le Défense contre les menaces virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant les segments VXLAN dans un serveur mandataire apparié.

- Équilibreurs de charge GCP natifs, internes et externes

- Routage à chemins multiples à coût égal (ECMP) utilisant des routeurs internes et externes comme le routeur des services en nuage de Cisco

Le routage ECMP peut transférer des paquets sur plusieurs « meilleurs chemins » qui se partagent la première place dans la mesure du routage. Comme pour l'EtherChannel, un hachage des adresses IP source et de destination ou des ports source et de destination peut être utilisé pour envoyer un paquet vers l'un des sauts suivants. Si vous utilisez des routes statiques pour le routage ECMP, la défaillance de Défense contre les menaces peut provoquer des problèmes. Le routage continue d'être utilisé et le trafic vers le Défense contre les menaces défaillant sera perdu. Si vous utilisez des routes statiques, veillez à utiliser une fonctionnalité de surveillance de routage statique telle que le suivi d'objets. Nous recommandons d'utiliser des protocoles de routage dynamique pour ajouter et supprimer des routes, auquel cas vous devez configurer chaque Défense contre les menaces pour qu'il participe au routage dynamique.




---

**Remarque** Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge pour l'équilibrage de la charge.

---

## Interfaces individuelles

Vous pouvez configurer les interfaces de grappe en tant *qu'interfaces individuelles*.

Les interfaces individuelles sont des interfaces de routage normales, chacune avec sa propre adresse IP locale. La configuration d'interface doit être configurée uniquement sur le nœud de contrôle et chaque interface utilise DHCP.




---

**Remarque** Les canaux EtherChannels étendus de couche 2 ne sont pas pris en charge.

---

## Rôles des nœuds de contrôle et de données

Un membre de la grappe est le nœud de contrôle. Si plusieurs nœuds de la grappe sont mis en ligne en même temps, le nœud de contrôle est déterminé par le paramètre de priorité. La priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée. Tous les autres membres sont des nœuds de données. Lorsque vous créez la grappe pour la première fois, vous spécifiez le nœud que vous souhaitez utiliser comme nœud de contrôle. Il deviendra le nœud de contrôle simplement parce qu'il s'agit du premier nœud ajouté à la grappe.

Tous les nœuds de la grappe partagent la même configuration. Le nœud que vous avez initialement spécifié comme nœud de contrôle remplacera la configuration sur les nœuds de données lorsqu'ils rejoindront la grappe. Vous n'avez donc qu'à effectuer la configuration initiale sur le nœud de contrôle avant de former la grappe.

Certaines fonctionnalités ne sont pas évolutives en grappe, et le nœud de contrôle gère tout le trafic pour ces fonctionnalités.

## Liaison de commande de grappe

Chaque nœud doit dédier une interface en tant qu'interface VXLAN (VTEP) pour la liaison de commande de grappe. Pour en savoir plus sur VXLAN, consultez [Configurer les interfaces VXLAN](#).

### Point terminal du tunnel VXLAN

Les périphériques de point terminal de tunnel VXLAN (VTEP) effectuent l'encapsulation et la désencapsulation VXLAN. Chaque VTEP comporte deux types d'interface : une ou plusieurs interfaces virtuelles appelées interfaces VNI (VXLAN Network Identifier), et une interface normale appelée interface source du VTEP qui canalise les interfaces VNI entre les VTEP. L'interface source du VTEP est connectée au réseau IP de transport pour la communication de VTEP à VTEP.

### Interface de la source VTEP

L'interface source du VTEP est une interface défense contre les menaces virtuelles classique à laquelle vous prévoyez associer l'interface VNI. Vous pouvez configurer une interface source de VTEP pour qu'elle agisse

en tant que liaison de commande de grappe. L'interface source est réservée à une utilisation avec la liaison de commande de grappe uniquement. Chaque interface source de VTEP possède une adresse IP sur le même sous-réseau. Ce sous-réseau doit être isolé de tout autre trafic et ne doit inclure que les interfaces de liaison de commande de grappe.

### Interface VNI

Une interface VNI est semblable à une interface VLAN : il s'agit d'une interface virtuelle qui sépare le trafic réseau sur une interface physique donnée au moyen de balisage. Vous ne pouvez configurer qu'une seule interface VNI. Chaque interface VNI possède une adresse IP sur le même sous-réseau.

### VTEP homologues

Contrairement au VXLAN habituel pour les interfaces de données, qui autorise un seul homologue VTEP, la mise en grappe défense contre les menaces virtuelles vous permet de configurer plusieurs homologues.

## Présentation du trafic de liaison de commande de grappe

Le trafic de liaison de commande de grappe comprend à la fois un trafic de contrôle et un trafic de données.

Le trafic de contrôle comprend :

- Choix du nœud de contrôle.
- Duplication de la configuration.
- Surveillance de l'intégrité

Le trafic de données comprend :

- Duplication de l'état.
- Requêtes de propriété de connexion et transfert de paquets de données.

## Réplication de la configuration

Tous les nœuds de la grappe partagent une configuration unique. Vous pouvez uniquement apporter des modifications à la configuration sur le nœud de contrôle (à l'exception de la configuration de démarrage) et les modifications sont automatiquement synchronisées avec tous les autres nœuds de la grappe.

## le réseau de gestion

Vous devez gérer chaque nœud à l'aide de l'interface de gestion; la gestion à partir d'une interface de données n'est pas prise en charge avec la mise en grappe.

## Licences pour la mise en grappe Threat Defense Virtual

Chaque nœud de grappe défense contre les menaces virtuelles nécessite la même licence de niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les membres, sinon les performances seront limitées sur tous les nœuds pour correspondre au membre le moins

capable. Le niveau de débit sera répliqué du nœud de contrôle à chaque nœud de données afin qu'ils correspondent.

Vous attribuez des licences de fonctionnalités à la grappe dans son ensemble, et non à des nœuds individuels. Cependant, chaque nœud de la grappe consomme une licence distincte pour chaque fonctionnalité. La fonctionnalité de mise en grappe elle-même ne nécessite aucune licence.

Lorsque vous ajoutez le nœud de contrôle au Centre de gestion, vous pouvez préciser les licences de fonctionnalités que vous souhaitez utiliser pour la grappe. Vous pouvez modifier les licences de la grappe dans la zone **Devices > Device Management > Cluster > License** (Périphériques > Gestion des périphériques > Grappe > Licence).



**Remarque**

Si vous ajoutez la grappe avant que le Centre de gestion ne soit sous licence (et s'exécute en mode d'évaluation), alors, lorsque vous obtenez la licence pour le Centre de gestion, vous pouvez rencontrer des perturbations de trafic lorsque vous déployez des modifications de politique sur la grappe. Lors du passage en mode sous licence, toutes les unités de données quittent la grappe, puis la rejoignent.

## Exigences et conditions préalables pour la mise en grappe Threat Defense Virtual

### Exigences du modèle

- FTDv5, FTDv10, FTDv20, FTDv30, FTDv50, FTDv100



**Remarque**

FTDv5 et FTDv10 ne prennent pas en charge l'équilibreur de charge de passerelle (GWL) d'Amazon Web Services (AWS) et Azure GWLB.

- Les services infonuagiques publics suivants :
  - Amazon Web Services (AWS)
  - Microsoft Azure
  - Google Cloud Platform (GCP)
- Maximum de 16 nœuds

Consultez également les exigences générales pour Défense contre les menaces virtuelles dans la section [Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual](#).

### Rôles utilisateur

- Admin
- Administrateur d'accès
- Administrateur de réseau

### Configuration matérielle et logicielle requise

Pour toutes les unités d'une grappe :

- Doit être dans le même niveau de performance. Nous vous recommandons d'utiliser le même nombre de CPU et de mémoire pour tous les nœuds, sinon les performances seront limitées sur tous les nœuds pour correspondre au nœud le moins performant.
- L'accès au Centre de gestion doit provenir de l'interface de gestion; la gestion de l'interface de données n'est pas prise en charge.
- Doit exécuter le logiciel identique, sauf lors d'une mise à niveau d'image. La mise à niveau rapide est prise en charge.
- Toutes les unités d'une grappe doivent être déployées dans la même zone de disponibilité.
- Les interfaces de liaison de commande de grappe de toutes les unités doivent se trouver dans le même sous-réseau.

### MTU

Assurez-vous que les ports connectés à la liaison de commande de grappe ont une MTU correcte (plus élevée) configurée. En cas de non-concordance MTU, la formation de la grappe échouera. La MTU de la liaison de commande de grappe doit être 154 octets supérieure aux interfaces de données. Étant donné que le trafic de la liaison de commande de grappe comprend la transmission de paquets de données, celle-ci doit prendre en charge la taille totale d'un paquet de données, plus les surcharges de trafic de la grappe (100 octets) et les surcharges VXLAN (54 octets).

Pour AWS avec GWLB, l'interface de données utilise l'encapsulation de Geneve. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Vous devez définir la MTU de l'interface source comme étant la MTU du réseau + 306 octets. Ainsi, pour le chemin réseau standard de 1 500 MTU, la MTU de l'interface source doit être de 1 806 et la MTU de la liaison de commande de grappe doit être de +154, 1 960.

Pour Azure avec GWLB, l'interface de données utilise l'encapsulation VXLAN. Dans ce cas, le datagramme Ethernet entier est encapsulé, de sorte que le nouveau paquet est plus volumineux et nécessite une MTU plus grande. Vous devez définir la MTU de liaison de commande de grappe pour qu'elle corresponde à la MTU de l'interface source + 80 octets.

Le tableau suivant présente les valeurs par défaut pour la MTU de la liaison de commande de grappe et la MTU de l'interface de données.

**Tableau 1 : MTU par défaut**

Nuage public	Liaison de commande de grappe	MTU de l'interface de données
AWS avec GWLB	1960	1806
AWS	1654	1 500
Azure avec GWLB	1554	1454
Azure	1554	1400
GCP	1554	1400

# Lignes directrices pour la mise en grappe virtuelle Threat Defense

## Haute disponibilité

La haute disponibilité n'est pas prise en charge par la mise en grappe.

## IPv6

La liaison de commande de grappe est uniquement prise en charge avec IPv4.

## Directives supplémentaires

- Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur Défense contre les menaces ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec toutes les unités, vous pouvez réactiver le contrôle d'intégrité.
- lors de l'ajout d'un nœud à une grappe existante ou lors du rechargement d'un nœud, il se produit une perte temporaire et limitée de paquets ou de connexion; c'est un comportement attendu. Dans certains cas, les paquets abandonnés peuvent bloquer votre connexion; Par exemple, la suppression d'un paquet FIN/ACK pour une connexion FTP entraînera le blocage du client FTP. Dans ce cas, vous devez rétablir la connexion FTP.
- Ne mettez pas un nœud hors tension sans désactiver d'abord la mise en grappe sur le nœud.
- Pour les connexions TLS/SSL déchiffrées, les états de déchiffrement ne sont pas synchronisés, et si le propriétaire de la connexion échoue, les connexions déchiffrées sont réinitialisées. De nouvelles connexions devront être établies vers un nouveau nœud. Les connexions qui ne sont pas déchiffrées (elles correspondent à une règle « ne pas déchiffrer ») ne sont pas affectées et sont répliquées correctement.
- L'évolutivité dynamique n'est pas prise en charge.
- le basculement avec état de la cible n'est pas pris en charge lorsque vous déployez la grappe sur AWS.
- Effectuer un déploiement global à la fin de chaque fenêtre de maintenance.
- Assurez-vous de ne pas supprimer plusieurs périphériques à la fois du groupe d'évolutivité automatique (AWS)/du groupe d'instances (GCP) ou de l'ensemble d'évolutivité (Azure). Nous vous recommandons également d'exécuter la commande **cluster disable** sur le périphérique avant de retirer ce périphérique du groupe d'évolutivité (AWS)/du groupe d'instances (GCP) /de l'ensemble d'évolutivité (Azure).
- Si vous souhaitez désactiver les nœuds de données et le nœud de contrôle dans une grappe, nous vous recommandons de désactiver les nœuds de données avant de désactiver le nœud de contrôle. Si un nœud de contrôle est désactivé alors qu'il y a d'autres nœuds de données dans la grappe, l'un d'eux doit être promu au rang de nœud de contrôle. Notez que le changement de rôle pourrait perturber la grappe.
- Dans les scripts de configuration personnalisés du jour 0 présentés dans ce guide, vous pouvez modifier les adresses IP selon vos besoins, fournir des noms d'interface personnalisés et modifier la séquence de l'interface CCL-Link.

- Si vous rencontrez des problèmes d'instabilité CCL, comme des défaillances de commande ping intermittentes, après le déploiement d'une grappe virtuelle de défense contre les menaces sur une plateforme infonuagique, nous vous recommandons de déterminer les raisons qui causent l'instabilité CCL. En outre, vous pouvez augmenter le temps d'attente à titre de solution de contournement temporaire pour atténuer les problèmes d'instabilité CCL dans une certaine mesure. Pour plus d'informations sur la modification du délai d'attente, consultez [Modifier les paramètres du moniteur d'intégrité de la grappe](#).
- Lorsque vous configurez votre règle de pare-feu ou votre groupe de sécurité pour le centre de gestion virtuel, vous devez inclure les adresses IP privée et publique de Défense contre les menaces virtuelles dans la plage d'adresses IP source. Assurez-vous également de spécifier les adresses IP privée et publique du Centre de gestion virtuel dans la règle ou le groupe de sécurité du pare-feu de Défense contre les menaces virtuelles. Cela est important pour assurer l'enregistrement correct des nœuds lors du déploiement de la mise en grappe.

### Valeurs par défaut pour la mise en grappe

- L'ID du système cLACP est généré automatiquement et la priorité du système est 1 par défaut.
- La fonction de vérification de l'intégrité de la grappe est activée par défaut avec un délai d'attente de 3 secondes. La surveillance de l'intégrité des interfaces est activée sur toutes les interfaces par défaut.
- La fonction de jonction automatique de la grappe en cas d'échec de la liaison de commande de grappe offre des tentatives illimitées toutes les 5 minutes.
- La fonction de jonction automatique de la grappe pour une interface de données défaillante effectue 3 essais toutes les 5 minutes, l'intervalle croissant étant fixé à 2.
- Un délai de duplication de connexion de 5 secondes est activé par défaut pour le trafic HTTP.

## Déployer la grappe dans AWS

Pour déployer une grappe dans AWS, vous pouvez soit la déployer manuellement, soit utiliser des modèles CloudFormation pour déployer une pile. Vous pouvez utiliser la grappe avec l'équilibreur de charge de passerelle AWS ou avec un équilibreur de charge non natif comme le routeur des services en nuage de Cisco.

## Équilibreur de charge de passerelle AWS et serveur mandataire à un seul volet de Geneve



### Remarque

Ce scénario est le seul actuellement pris en charge pour les interfaces de Geneve.

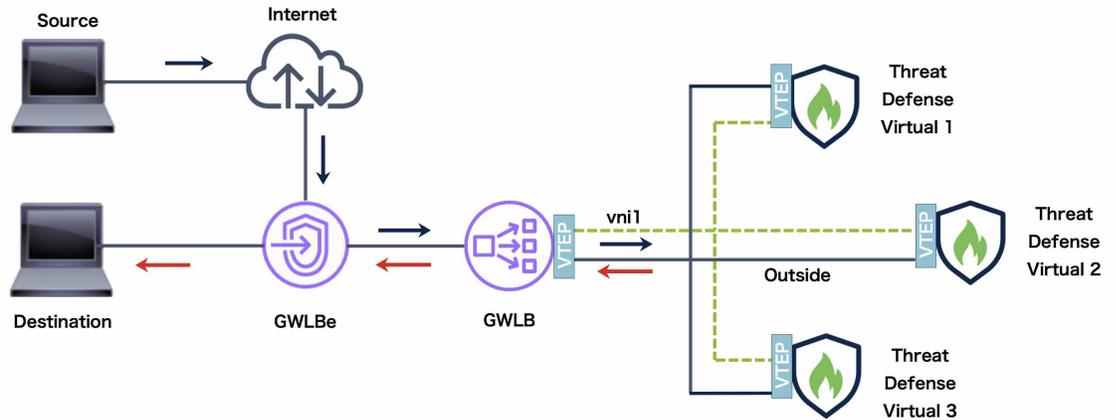
L'équilibreur de charge de passerelle AWS combine une passerelle de réseau transparente et un équilibreur de charge qui répartit le trafic et fait évoluer les périphériques virtuels à la demande. Threat Defense Virtual prend en charge le plan de contrôle centralisé de l'équilibreur de charge de passerelle avec un plan de données distribué (point de terminaison de l'équilibreur de charge de passerelle). La figure suivante montre le trafic acheminé vers l'équilibreur de charge de passerelle à partir du point terminal de l'équilibreur de charge de passerelle. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs Threat Defense virtuels, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle (trafic

en demi-tour). L'équilibreur de charge de passerelle renvoie ensuite le trafic au point terminal de l'équilibreur de charge de passerelle et à la destination.



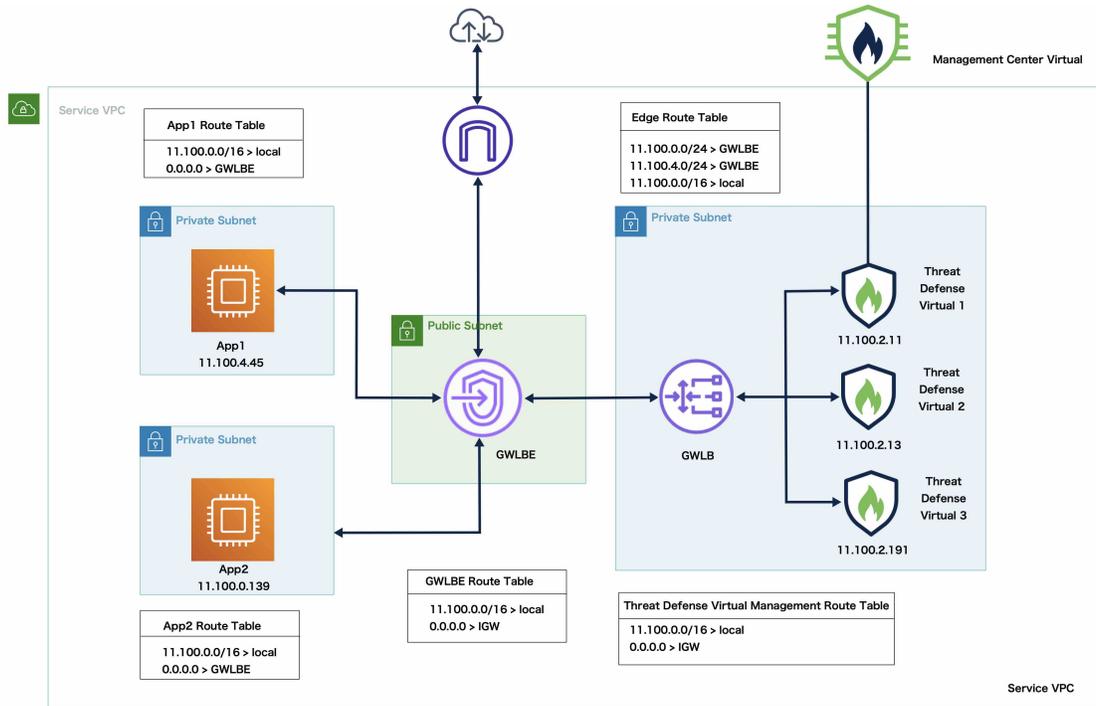
**Remarque** La découverte de l'identité du serveur TLS ( Transport Layer Security ) n'est pas prise en charge avec la configuration à Bras unique de Geneve sur AWS.

*Illustration 1 : Serveur mandataire à un seul volet Geneve*



## Exemple de topologie

La topologie indiquée ci-dessous décrit le flux de trafic entrant et sortant. Il y a trois instances virtuelles de défense contre les menaces dans la grappe qui est connectée à une GWLB. Une instance virtuelle du centre de gestion est utilisée pour gérer la grappe.



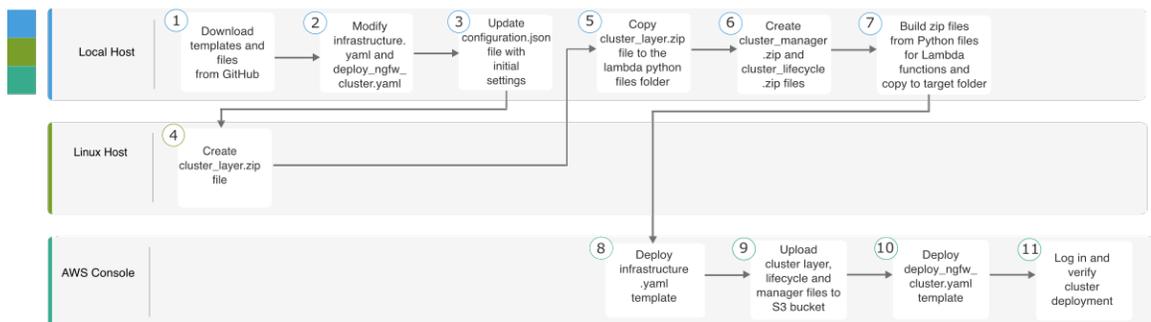
Le trafic entrant provenant d’Internet est dirigé vers le point terminal de la GWLB, qui le transmet ensuite à la GWLB. Le trafic est ensuite acheminé vers la grappe virtuelle Threat Defense. Une fois que le trafic a été inspecté par une instance virtuelle de Threat Defense dans la grappe, il est transféré à la machine virtuelle de l’application, App1 /App2.

Le trafic sortant d’App1/App2 est transmis au point terminal de la GWLB, qui l’envoie ensuite vers Internet.

## Processus de bout en bout pour le déploiement des grappes virtuelles de défense contre les menaces sur AWS

### Déploiement basé sur un modèle

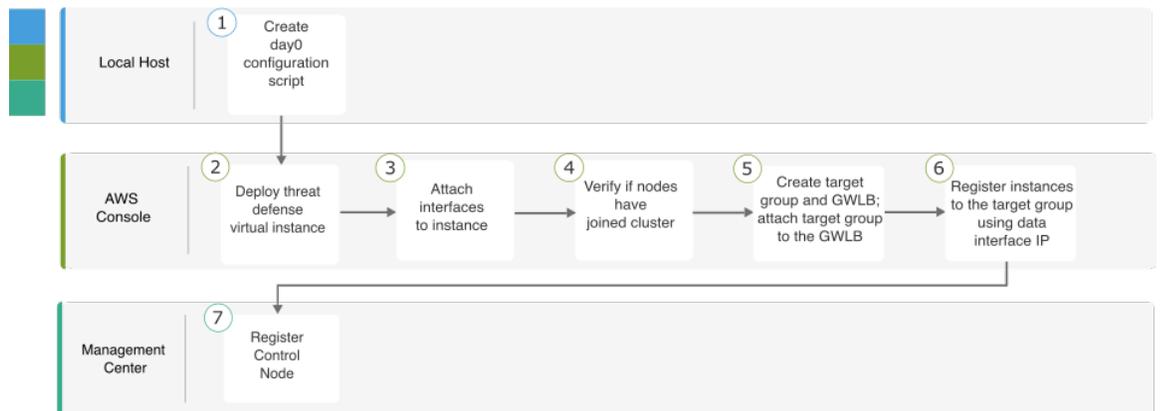
Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe virtuelle Threat Defense sur AWS.



	Espace de travail	Étapes
①	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
②	Hôte local	Modifiez les modèles <i>infrastructure.yaml</i> et <i>deploy_ngfw_cluster.yaml</i> .
③	Hôte local	Mettez à jour le fichier <i>Configuration.json</i> avec les paramètres initiaux.
④	Hôte Linux	Créez le fichier <i>cluster_layer.zip</i> .
⑤	Hôte local	Copiez le fichier <i>cluster_layer.zip</i> dans le dossier des fichiers Python Lambda.
⑥	Hôte local	Créez les fichiers <i>cluster_manager.zip</i> et <i>cluster_lifecycle.zip</i> .
⑦	Hôte local	Créer des fichiers compressés à partir des fichiers Python pour les fonctions Lambda et les copier dans le dossier cible.
⑧	Console AWS	Déployez le modèle <i>infrastructure.yaml</i> .
⑨	Console AWS	Chargez <i>cluster_layer.zip</i> , <i>cluster_lifecycle.zip</i> et <i>cluster_manager.zip</i> dans le compartiment S3.
⑩	Console AWS	Déployez le modèle <i>déploie_ngfw_cluster.yaml</i> .
⑪	Console AWS	Connectez-vous et vérifiez le déploiement de la grappe.

### Déploiement manuel

Le diagramme suivant illustre le flux de travail pour le déploiement manuel de la grappe virtuelle Threat Defense sur AWS.



	Espace de travail	Étapes
①	Hôte local	Créer la configuration Day0 pour AWS
②	Console AWS	Déployer une instance Threat Defense Virtual.
③	Console AWS	Associez des interfaces à l'instance.
④	Console AWS	Vérifier si les nœuds ont rejoint la grappe.
⑤	Console AWS	Créer le groupe cible et la GWLB; associer un groupe cible à la GWLB.
⑥	Console AWS	Enregistrez les instances avec le groupe cible à l'aide de l'adresse IP de l'interface de données.
⑦	Centre de gestion	Nœud de contrôle d'enregistrement.

## Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms des paramètres, les valeurs par défaut, les valeurs autorisées et la description sont donnés dans le modèle.

- [infrastructure.yaml](#) : modèle pour le déploiement de l'infrastructure
- [deploy\\_ngfw\\_cluster.yaml](#) : modèle pour le déploiement en grappe.



### Remarque

Assurez-vous de consulter la liste des types d'instances AWS pris en charge avant de déployer les nœuds de la grappe. Cette liste se trouve dans le modèle *deploy\_ngfw\_cluster.yaml*, sous les valeurs autorisées pour le paramètre InstanceType (Type d'instance).

## Déployer la pile dans AWS à l'aide d'un modèle CloudFormation

Déployez la pile dans AWS à l'aide du modèle personnalisé Cloud Formation.

### Avant de commencer

- Vous avez besoin d'un ordinateur Linux avec Python 3.
- Pour permettre à la grappe de s'enregistrer automatiquement auprès de centre de gestion, vous devez créer un utilisateur avec des privilèges d'administration sur centre de gestion qui peut utiliser l'API REST. Consultez la section [Guide d'administration Cisco Secure Firewall Management Center](#).
- Ajoutez une politique d'accès dans le centre de gestion qui correspond au nom de la politique que vous avez spécifié dans Configuration.JSON.

## Procédure

### Étape 1

Préparez le modèle.

- a) Copiez le référentiel github dans votre dossier local. Consultez <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/aws>.
- b) Modifiez **infrastructure.yaml** et **déploie\_ngfw\_cluster.yaml** avec les paramètres requis.
- c) Modifiez **cloud-clustering/ftdv-cluster/lambda-python-files/Configuration.json** avec les paramètres initiaux.

Par exemple :

```
{
  "licenseCaps": ["BASE", "MALWARE", "THREAT"],
  "performanceTier": "FTDv50",
  "fmcIpforDeviceReg": "DONTRESOLVE",
  "RegistrationId": "cisco",
  "NatId": "cisco",
  "fmcAccessPolicyName": "AWS-ACL"
}
```

- Conservez le paramètre `fmcIpforDeviceReg` DONTRESOLVE.
- Le nom `fmcAccessPlicyName` doit correspondre à une politique d'accès sur centre de gestion.

**Remarque** Les niveaux FTDv5 et FTDv10 ne sont pas pris en charge.

- d) Créez un fichier nommé **cluster\_layer.zip** pour fournir les bibliothèques Python essentielles aux fonctions Lambda.

Vous pouvez créer le fichier `cluster_layer.zip` dans un environnement Linux - Ubuntu 18.04 sur lequel Python 3.9 est installé.

Exécutez le script Shell suivant pour créer `cluster_layer.zip` :

```
#!/bin/bash
mkdir -p layer
virtualenv -p /usr/bin/python3.9 ./layer/
source ./layer/bin/activate
pip3 install pycryptodome==3.17.0
pip3 install paramiko==2.7.1
pip3 install requests==2.23.0
pip3 install scp==0.13.2
pip3 install jsonschema==3.2.0
pip3 install cffi==1.15.1
pip3 install zipp==3.1.0
pip3 install importlib-metadata==1.6.0
echo "Copy from ./layer directory to ./python\n"
mkdir -p ./python/
cp -r ./layer/lib/python3.9/site-packages/* ./python/
zip -r cluster_layer.zip ./python
deactivate
```

- e) Copiez le fichier `cluster_layer.zip` résultant dans le dossier des fichiers lambda python.
- f) Créez les fichiers **cluster\_manager.zip** et **cluster\_lifecycle.zip**.

Un fichier **make.py** se trouve dans le référentiel cloné. Cela compressera les fichiers python dans un fichier compressé et les copiera dans un dossier cible.

**python3 make.py build**

**Étape 2**

Déployez **infrastructure.yaml** et notez les valeurs de sortie pour le déploiement en grappe.

- Sur la console AWS, accédez à **CloudFormation** et cliquez sur **Create stack** (créer une pile). sélectionnez **Avec de nouvelles ressources (standard)**.
- Sélectionnez **Charger un fichier modèle**, cliquez sur **Choisir un fichier** et sélectionnez **infrastructure.yaml** dans le dossier cible.
- Cliquez sur **Next** (suivant) et fournissez les informations requises.
- Cliquez sur **Next** (suivant), puis sur **Create stack** (créer une pile).
- Une fois le déploiement terminé, accédez aux **résultats** et notez le nom de **compartiment S3**.

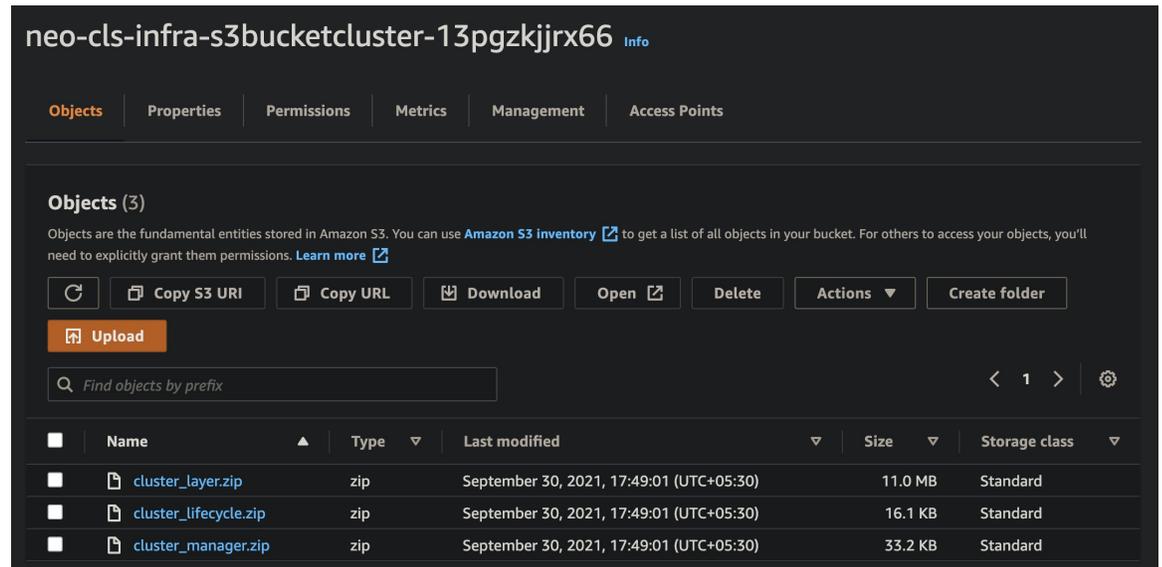
*Illustration 2 : Sortie de infrastructure.yaml*

Outputs (16)				
<input type="text" value="Search outputs"/>				
Key	Value	Description	Export name	
AZ	me-south-1a	Availability zone	-	
AppInstanceSGId	sg-02b07af19c3e746d9	Security Group ID for Application Instances	-	
ApplicationSubnetIds	subnet-03217efc6049e5fee	Application subnet ID	-	
BucketName	neo-cls-infra-s3bucketcluster-13pgzkjrx66	Name of the sample Amazon S3 bucket with Private Static Web hosting Configuration	-	
BucketUrl	<a href="http://neo-cls-infra-s3bucketcluster-13pgzkjrx66.s3-website.me-south-1.amazonaws.com">http://neo-cls-infra-s3bucketcluster-13pgzkjrx66.s3-website.me-south-1.amazonaws.com</a>	URL of S3 Bucket Static Website	-	
CCLSubnetId	subnet-0caf6c4801922d8b1	CCL subnet ID	-	
EIPforNATgw	15.184.208.231	EIP reserved for NAT GW	-	
FmcInstanceSGID	sg-0a0d3797b04370aa3	Security Group ID for FMC if user would like to launch in this VPC itself	-	
InInterfaceSGId	sg-0522ebe5acb8a2827	Security Group ID for Instances Inside Interface	-	
InsideSubnetIds	subnet-056fdc9fe5389bf88	Inside subnet ID	-	
InstanceSGId	sg-0be5b62647eb53dec	Security Group ID for Instances Management Interface	-	
LambdaSecurityGroupId	sg-0347d191d724b2574	Security Group ID for Lambda Functions	-	
LambdaSubnetIds	subnet-0989fbaeb522a906c,subnet-0c7a9b649d506f930	List of lambda subnet IDs (comma seperated)	-	
MgmtSubnetIds	subnet-08c386d4b06890532	Mangement subnet ID	-	
UseGWLB	Yes	Use Gateway Load Balancer	-	
VpcName	vpc-0d94d3eaaa1f1354d	Name of the VPC created	-	

**Étape 3**

Chargez **cluster\_layer.zip**, **cluster\_lifecycle.zip** et **cluster\_manager.zip** dans le compartiment S3 créé par **infrastructure.yaml**.

Illustration 3 : Compartiment S3



#### Étape 4 Déployez `déploy_ngfw_cluster.yaml`.

- Allez sur **CloudFormation** et cliquez sur **Create stack** (Créer une pile); sélectionnez **Avec de nouvelles ressources (standard)**.
- Sélectionnez **Charger un fichier modèle**, cliquez sur **Choisir un fichier** et sélectionnez **déploie\_ngfw\_cluster.yaml** dans le dossier cible.
- Cliquez sur **Next** (suivant) et fournissez les informations requises.
- Cliquez sur **Next** (suivant), puis sur **Create stack** (créer une pile).

Les fonctions Lambda gèrent le reste du processus et les défenses contre les menaces virtuelles s'enregistrent automatiquement auprès du centre de gestion.

Illustration 4 : Ressources déployées

Logical ID	Physical ID	Type	Status
ASmanagerTopic	arn:aws:sns:me-south-1:797661843114:neo-cls-1-1-autoscale-manager-topic	AWS::SNS::Topic	CREATE_COMPLETE
ClusterManager	neo-cls-1-1-manager-lambda	AWS::Lambda::Function	CREATE_COMPLETE
ClusterManagerLogGrp	/aws/lambda/neo-cls-1-1-manager-lambda	AWS::Logs::LogGroup	CREATE_COMPLETE
ClusterManagerSNS1	arn:aws:sns:me-south-1:797661843114:neo-cls-1-1-autoscale-manager-topicae9962ae-de5a-4274-afa1-b38fb815e6dc	AWS::SNS::Subscription	CREATE_COMPLETE
ClusterManagerSNS1Permission	neo-cls-stack-ClusterManagerSNS1Permission-1QUGG6QPBYAMM	AWS::Lambda::Permission	CREATE_COMPLETE
FTDGroup	neo-cls-1-1	AWS::AutoScaling::AutoScalingGroup	CREATE_COMPLETE
FTDLaunchTemplate	lt-073774ba8e52a7e70	AWS::EC2::LaunchTemplate	CREATE_COMPLETE
InstanceEvent	neo-cls-1-1-notify-instance-event	AWS::Events::Rule	CREATE_COMPLETE
InstanceEventInvokeLambdaPermission	neo-cls-stack-InstanceEventInvokeLambdaPermission-1HIW8J9L356E2	AWS::Lambda::Permission	CREATE_COMPLETE
LambdaLayer	arn:aws:lambda:me-south-1:797661843114:layer:neo-cls-1-1-lambda-layer:1	AWS::Lambda::LayerVersion	CREATE_COMPLETE
LambdaPolicy	neo-c-Lamb-JNZARJ36KVKQ	AWS::IAM::Policy	CREATE_COMPLETE
LambdaRole	neo-cls-1-1-Role	AWS::IAM::Role	CREATE_COMPLETE
LifeCycleEvent	neo-cls-1-1-lifecycle-action	AWS::Events::Rule	CREATE_COMPLETE
LifeCycleEventInvokeLambdaPermission	neo-cls-stack-LifeCycleEventInvokeLambdaPermission-7036X3FAVFF7	AWS::Lambda::Permission	CREATE_COMPLETE
LifeCycleLambda	neo-cls-1-1-lifecycle-lambda	AWS::Lambda::Function	CREATE_COMPLETE
LifeCycleLambdaLogGrp	/aws/lambda/neo-cls-1-1-lifecycle-lambda	AWS::Logs::LogGroup	CREATE_COMPLETE
gwlb	arn:aws:elasticloadbalancing:me-south-1:797661843114:loadbalancer/gwy/neo-cls-1-1-GWLB/186e8004d09d30c5	AWS::ElasticLoadBalancingV2::LoadBalancer	CREATE_COMPLETE
listener	arn:aws:elasticloadbalancing:me-south-1:797661843114:listener/gwy/neo-cls-1-1-GWLB/186e8004d09d30c5//8F58F3F92fcd13	AWS::ElasticLoadBalancingV2::Listener	CREATE_COMPLETE
tg	arn:aws:elasticloadbalancing:me-south-1:797661843114:targetgroup/neo-cls-1-1-GWLB-tg/0091e49395247f9355	AWS::ElasticLoadBalancingV2::TargetGroup	CREATE_COMPLETE

Étape 5

Vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en utilisant la commande **show cluster info**.

Illustration 5 : Nœuds de la grappe

Instance ID	Lifecycle	Instance ty...	Weighted capacity	Launch template/configuration
i-0a8a98d3bda571dc9	InService	c5.xlarge	-	neo-cls-1-1-ftd-launch-template
i-0f6c3f8ea3ba2b044	InService	c5.xlarge	-	neo-cls-1-1-ftd-launch-template

Illustration 6 : afficher l'information sur grappe

```

Copyright 2004-2022, Cisco and/or its affiliates. All rights reserved.
Cisco is a registered trademark of Cisco Systems, Inc.
All other trademarks are property of their respective owners.

Cisco Firepower Extensible Operating System (FX-OS) v2.13.0 (build 198)
Cisco Firepower Threat Defense for AWS v7.3.0 (build 69)

>
>
> show cluster info
Cluster res-cluster: On
  Interface mode: individual
Cluster Member Limit : 16
  This is "123" in state CONTROL_NODE
    ID       : 0
    Version  : 9.19(1)
    Serial No.: 9AWDHS75AGV
    CCL IP   : 1.1.1.123
    CCL MAC  : 0642.3261.a1d0
    Module   : NGFWv
    Resource : 4 cores / 7680 MB RAM
    Last join : 05:50:46 UTC May 18 2023
    Last leave: N/A
Other members in the cluster:
  Unit "208" in state DATA_NODE
    ID       : 1
    Version  : 9.19(1)
    Serial No.: 9AX02RCE9NM
    CCL IP   : 1.1.1.208
    CCL MAC  : 0687.a4e4.4442
    Module   : NGFWv
    Resource : 4 cores / 7680 MB RAM
    Last join : 05:50:47 UTC May 18 2023
    Last leave: N/A
>

```

## Déployer manuellement la grappe dans AWS

Pour déployer la grappe manuellement, préparez la configuration du jour 0, déployez chaque nœud, puis ajoutez le nœud de contrôle à centre de gestion.

### Créer la configuration Day0 pour AWS

Vous pouvez utiliser une configuration fixe ou une configuration personnalisée. Nous vous recommandons d'utiliser la configuration fixe.

#### Créer la configuration Day0 avec une configuration fixe pour AWS

La configuration fixe générera automatiquement la configuration de démarrage de grappe.

```

{
  "AdminPassword": "password",
  "Hostname": "hostname",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "Cluster": {
    "CclSubnetRange": "ip_address_start ip_address_end",
    "ClusterGroupName": "cluster_name",

```

Créer la configuration Day0 avec une configuration personnalisée pour AWS

```

        [For Gateway Load Balancer] "Geneve": "{Yes | No}",
        [For Gateway Load Balancer] "HealthProbePort": "port"
    }
}

```

Par exemple :

```

{
  "AdminPassword": "Sup3rnatural",
  "Hostname": "ciscoftdv",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "Cluster": {
    "CclSubnetRange": "10.10.55.4 10.10.55.30", //mandatory user input
    "ClusterGroupName": "ftdv-cluster", //mandatory user input
    "Geneve": "Yes",
    "HealthProbePort": "7777"
  }
}

```



**Remarque** Si vous copiez et collez la configuration donnée ci-dessus, veuillez à supprimer //entrée utilisateur obligatoire de la configuration.

Pour la variable **CclSubnetRange**, spécifiez une plage d'adresses IP à partir de xxx4. Assurez-vous d'avoir au moins 16 adresses IP disponibles pour la mise en grappe. Quelques exemples d'adresses IP de début (*ip\_address\_start*) et de fin (*ip\_address\_end*) sont donnés ci-dessous.

**Tableau 2 : Exemples d'adresses IP de début et de fin**

CIDR	Adresse IP de début	Adresse IP de fin
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254
10.1.1.0/24	10.1.1.4	10.1.1.254

Créer la configuration Day0 avec une configuration personnalisée pour AWS

Vous pouvez saisir la configuration complète de démarrage de grappe à l'aide des commandes.

```

{
  "AdminPassword": "password",

```

```

    "Hostname": "hostname",
    "FirewallMode": "Routed",
    "ManageLocally": "No",
    "run_config": [comma_separated_threat_defense_configuration]
}

```

### Exemple d'équilibreur de charge de passerelle

Dans l'exemple suivant, une configuration est créée pour un équilibreur de charge de passerelle avec une interface Geneve pour le trafic en demi-tour et une interface VXLAN pour la liaison de commande de grappe. Notez les valeurs en gras qui doivent être uniques par nœud.

Un exemple de configuration de jour 0 pour les **versions 7.4 et ultérieures** est donné ci-dessous.

```

{
  "AdminPassword": "Sam&Dean",
  "Hostname": "ftdvl",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "run_config": [
    "cluster interface-mode individual force",
    "interface TenGigabitEthernet0/0",
    "nameif geneve-vtep-ifc",
    "ip address dhcp",
    "no shutdown",
    "interface TenGigabitEthernet0/1",
    "nve-only cluster",
    "nameif ccl_link",
    "ip address dhcp",
    "no shutdown",
    "interface vni1",
    "description Clustering Interface",
    "segment-id 1",
    "vtep-nve 1",
    "interface vni2",
    "proxy single-arm",
    "nameif uturn-ifc",
    "vtep-nve 2",
    "object network ccl#link",
    "range 10.1.90.4 10.1.90.19",
    "object-group network cluster#group",
    "network-object object ccl#link",
    "nve 2",
    "encapsulation geneve",
    "source-interface geneve-vtep-ifc",
    "nve 1",
    "encapsulation vxlan",
    "source-interface ccl_link",
    "peer-group cluster#group",
    "jumbo-frame reservation",
    "mtu geneve-vtep-ifc 1826",
    "mtu ccl_link 1980",
    "cluster group ftdv-cluster",
    "local-unit 1",
    "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
    "priority 1",
    "enable",
    "aaa authentication listener http geneve-vtep-ifc port 7777"
  ]
}

```

Un exemple de configuration de jour 0 pour les **versions 7.3 et antérieures** est donné ci-dessous.

```

{
  "AdminPassword": "Sam&Dean",
  "Hostname": "ftdvl",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "run_config": [
    "cluster interface-mode individual force",
    "interface TenGigabitEthernet0/0",
    "nameif geneve-vtep-ifc",
    "ip address dhcp",
    "no shutdown",
    "interface TenGigabitEthernet0/1",
    "nve-only cluster",
    "nameif ccl_link",
    "ip address dhcp",
    "no shutdown",
    "interface vni1",
    "description Clustering Interface",
    "segment-id 1",
    "vtep-nve 1",
    "interface vni2",
    "proxy single-arm",
    "nameif uturn-ifc",
    "vtep-nve 2",
    "object network ccl#link",
    "range 10.1.90.4 10.1.90.19",
    "object-group network cluster#group",
    "network-object object ccl#link",
    "nve 2",
    "encapsulation geneve",
    "source-interface geneve-vtep-ifc",
    "nve 1",
    "encapsulation vxlan",
    "source-interface ccl_link",
    "peer-group cluster#group",
    "jumbo-frame reservation",
    "mtu geneve-vtep-ifc 1806",
    "mtu ccl_link 1960",
    "cluster group ftdv-cluster",
    "local-unit 1",
    "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
    "priority 1",
    "enable",
    "aaa authentication listener http geneve-vtep-ifc port 7777"
  ]
}
    
```


**Remarque**

Pour la plage de sous-réseau CCL, spécifiez les adresses IP du CIDR de sous-réseau CCL, à l'exception des adresses IP réservées. Consultez le [Tableau 2 : Exemples d'adresses IP de début et de fin](#) ci-dessus pour obtenir des exemples.

Pour les paramètres de vérification de l'intégrité d'AWS, assurez-vous de préciser le port **aaa authentication listener http** que vous avez défini ici.

### Exemple d'équilibreur de charge non natif

Dans l'exemple suivant, une configuration à utiliser avec des équilibreurs de charge non natifs avec des interfaces Management, Inside et Outside est créée, ainsi qu'une interface VXLAN pour la liaison de commande de grappe. Notez les valeurs en gras qui doivent être uniques par nœud.

```
{
  "AdminPassword": "W1nch3sterBr0s",
  "Hostname": "ftdv1",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "run_config": [
    "cluster interface-mode individual force",
    "interface Management0/0",
    "management-only",
    "nameif management",
    "ip address dhcp",
    "interface GigabitEthernet0/0",
    "no shutdown",
    "nameif outside",
    "ip address dhcp",
    "interface GigabitEthernet0/1",
    "no shutdown",
    "nameif inside",
    "ip address dhcp",
    "interface GigabitEthernet0/2",
    "nve-only cluster",
    "nameif ccl_link",
    "ip address dhcp",
    "no shutdown",
    "interface vni1",
    "description Clustering Interface",
    "segment-id 1",
    "vtep-nve 1",
    "jumbo-frame reservation",
    "mtu ccl_link 1654",
    "object network ccl#link",
    "range 10.1.90.4 10.1.90.19", //mandatory user input
    "object-group network cluster#group",
    "network-object object ccl#link",
    "nve 1",
    "encapsulation vxlan",
    "source-interface ccl_link",
    "peer-group cluster#group",
    "cluster group ftdv-cluster", //mandatory user input
    "local-unit 1",
    "cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
    "priority 1",
    "enable"
  ]
}
```

Pour l'objet de réseau de liaison de commande de grappe, indiquez uniquement le nombre d'adresses dont vous avez besoin (jusqu'à 16). Une plage plus importante peut nuire aux performances.



**Remarque** Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **la //entrée utilisateur obligatoire** de la configuration.

## Déployer les nœuds de la grappe

Déployez les nœuds de la grappe pour qu'ils forment une grappe.

### Procédure

**Étape 1** Déployez l'instance virtuelle de Threat Defense en utilisant la configuration de jour 0 de la grappe avec le nombre d'interfaces requis (quatre interfaces si vous utilisez l'équilibreur de charge de passerelle (GWLB) ou cinq interfaces si vous utilisez un équilibreur de charge non natif). Pour ce faire, dans la section **Configurer Instance Details** (Configurer les détails de l'instance) > Advanced Details (détails avancés), collez la configuration du jour 0 de la grappe.

**Remarque** Assurez-vous d'associer des interfaces aux instances dans l'ordre indiqué ci-dessous.

- Équilibreur de charge de passerelle AWS : quatre interfaces : liaison de gestion, de dépistage, interne et de commande de grappe.
- Équilibreurs de charge non natifs : cinq interfaces – liaison de gestion, de dépistage, interne, externe et de commande de grappe.

Pour en savoir plus sur le déploiement de Threat Defense Virtual sur AWS, consultez [Déployer Threat Defense Virtual sur AWS](#).

**Étape 2** Répétez l'étape 1 pour déployer le nombre requis de nœuds supplémentaires.

**Étape 3** Utilisez la commande **show cluster info** de la console virtuelle Threat Defense pour vérifier si tous les nœuds ont bien rejoint la grappe.

**Étape 4** Configurez l'équilibreur de charge de passerelle AWS

- a) Créez un groupe cible et un GWLB.
- b) Associez le groupe cible au GWLB.

**Remarque** Assurez-vous de configurer le GWLB pour utiliser les paramètres de groupe de sécurité, de configuration d'écouteur et de vérification de l'intégrité adéquats.

- c) Enregistrez l'interface de données (interface interne) avec le groupe cible à l'aide des adresses IP.

Pour en savoir plus, consultez [Créer un équilibreur de charge de passerelle](#).

**Étape 5** Ajoutez le nœud de contrôle au centre de gestion. Consultez [Ajouter la grappe au centre de gestion \(déploiement manuel\)](#), à la page 50.

## Déployer la grappe dans Azure

Vous pouvez utiliser la grappe avec Azure Gateway Load Balancer (GWLB) ou avec un équilibreur de charge non natif. Pour déployer une grappe dans Azure, utiliser des modèles du gestionnaire de ressources Azure (ARM) pour déployer un ensemble de machines virtuelles identiques.

# Exemple de topologie pour un déploiement en grappes basé sur GWLB

Illustration 7 : Scénario et topologie du trafic entrant avec GWLB

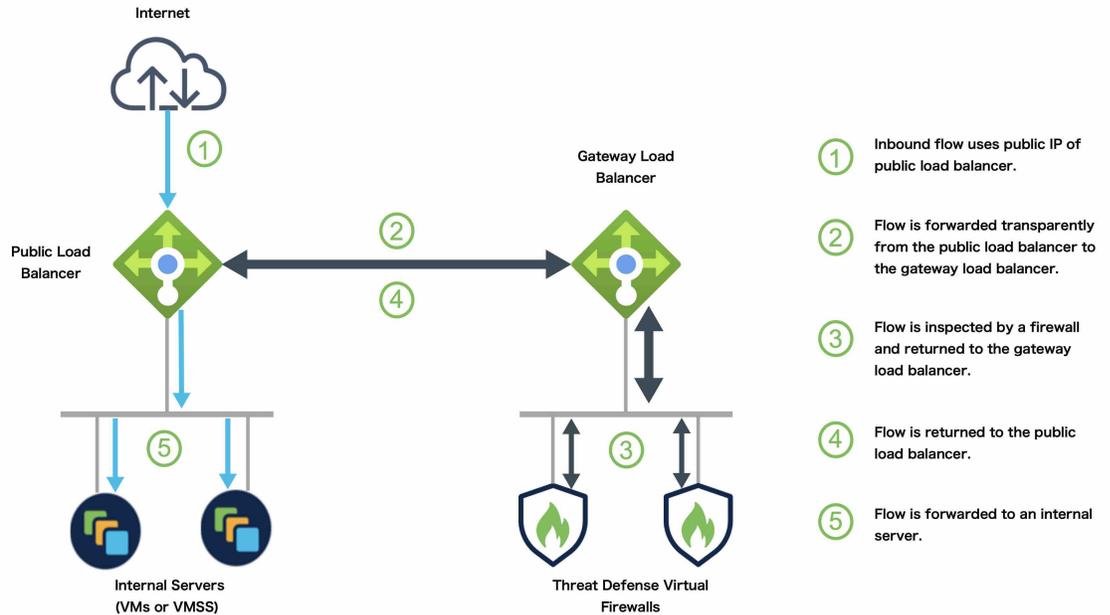
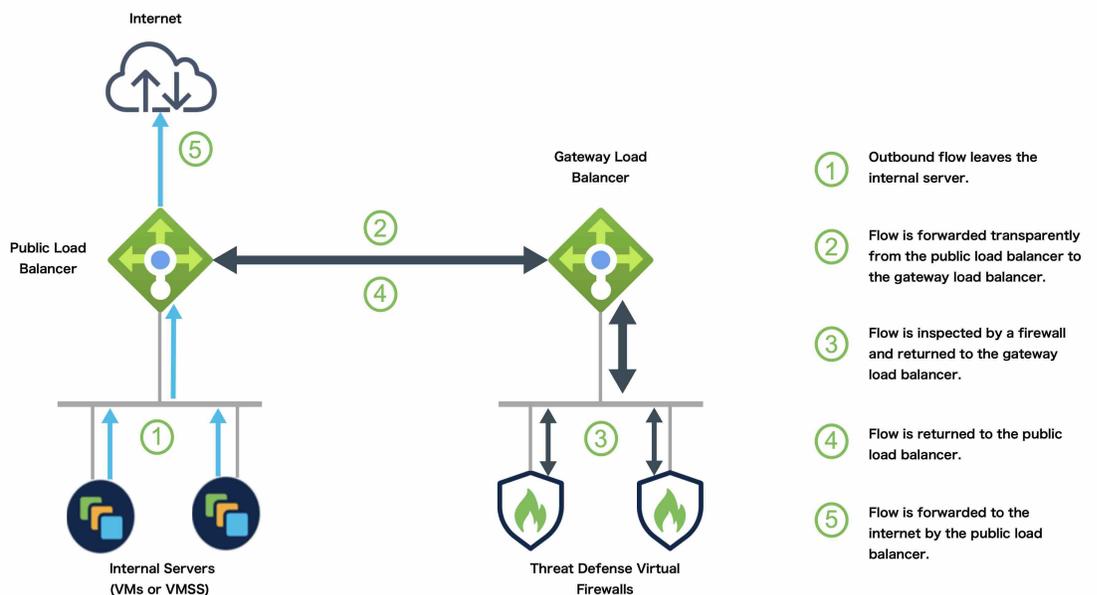


Illustration 8 : Scénario et topologie du trafic sortant avec GWLB

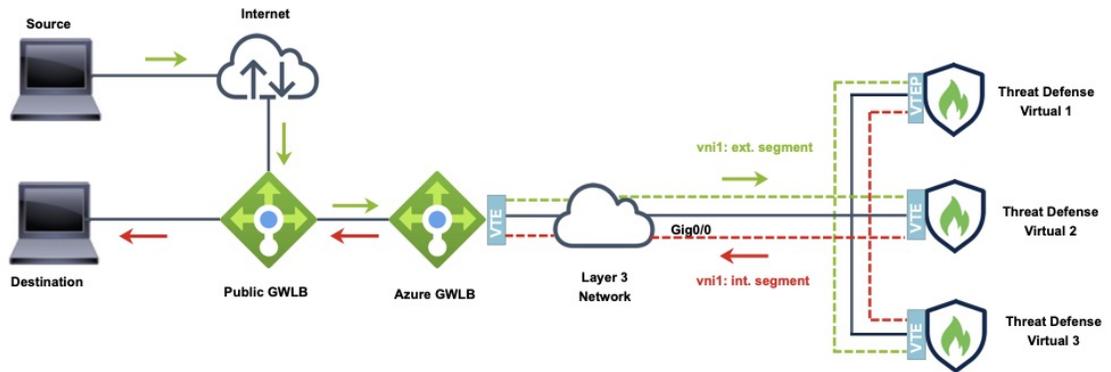


## Équilibreur de charge de passerelle Azure et serveur mandataire jumelé

Dans une chaîne de service Azure, les solutions virtuelles de défense contre les menaces agissent comme une passerelle transparente qui peut intercepter les paquets entre Internet et le service client. La défense contre les menaces virtuelles définit une interface externe et une interface interne sur une seule carte réseau en utilisant des segments VXLAN dans un proxy apparié.

La figure suivante montre le trafic transféré vers l'équilibreur de charge de passerelle Azure à partir de l'équilibreur de charge de passerelle publique sur le segment VXLAN externe. L'équilibreur de charge de passerelle équilibre le trafic entre plusieurs virtuels Threat Defense, qui inspectent le trafic avant de l'abandonner ou de le renvoyer à l'équilibreur de charge de passerelle sur le segment VXLAN interne. L'équilibreur de charge de passerelle Azure renvoie ensuite le trafic vers l'équilibreur de charge de passerelle publique et vers la destination.

Illustration 9 : Équilibreur de charge de passerelle Azure avec mandataire jumelé

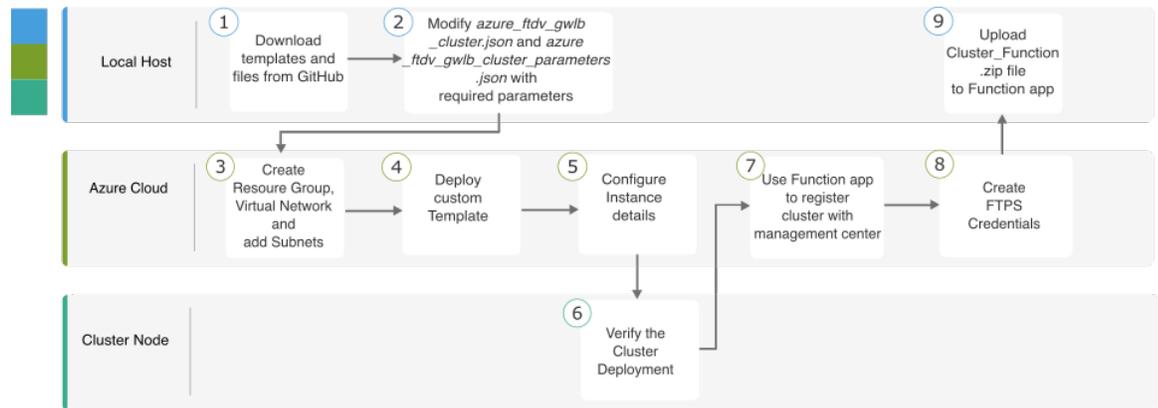


Traffic flow between GWLBs to GWLB (Geneve Single-Arm Proxy) in Azure

## Processus de bout en bout pour le déploiement de grappe Threat Defense Virtual dans Azure avec GWLB

### Déploiement basé sur un modèle

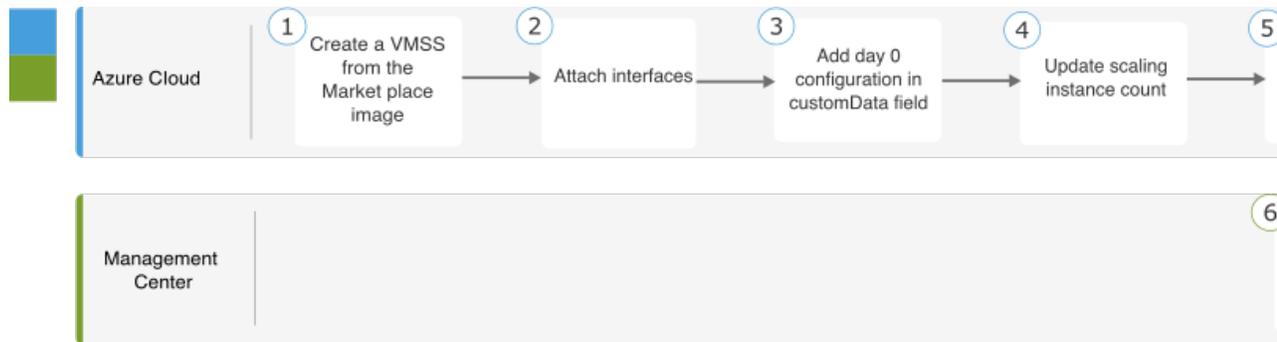
Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe virtuelle Threat Defense dans Azure avec GWLB.



	Espace de travail	Étapes
1	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
2	Hôte local	Modifiez <code>azure_ftdv_gwlb_cluster.json</code> et <code>azure_ftdv_gwlb_cluster_parameters.json</code> avec les paramètres requis.
3	Nuage Azure	Créez le groupe de ressources, le réseau virtuel et les sous-réseaux.
4	Nuage Azure	Déployer un modèle personnalisé.
5	Nuage Azure	Configurer les détails de l'instance.
6	Nom de la grappe	Vérifier le déploiement de la grappe.
7	Nuage Azure	Utilisez l'application de fonction pour enregistrer la grappe auprès du centre de gestion.
8	Nuage Azure	Créer des informations d'authentification FTPS
9	Hôte local	Téléversez le fichier <code>Cluster_Function.zip</code> dans l'application de fonction.

### Déploiement manuel

Le diagramme suivant illustre le flux de travail du déploiement manuel de la grappe virtuelle Threat Defense dans Azure avec GWLB.



	Espace de travail	Étapes
①	Hôte local	Créez un VMSS à partir de l'image du Marché.
②	Hôte local	Associer des interfaces.
③	Hôte local	Ajouter la configuration de jour 0 dans le champ customData.
④	Hôte local	Mettre à jour le nombre d'instances évolutives.
⑤	Hôte local	Configurer GWLB.
⑥	Centre de gestion	Ajouter un nœud de contrôle

## Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms et les valeurs des paramètres sont indiqués dans le modèle.

- [azure\\_ftdv\\_gwlb\\_cluster\\_parameters.json](#) : Modèle pour la saisie des paramètres pour la grappe Threat Defense Virtual avec GWLB
- [azure\\_ftdv\\_gwlb\\_cluster.json](#) : Modèle de déploiement de grappe Threat Defense Virtual avec GWLB

## Prérequis

- Pour permettre à la grappe de s'enregistrer automatiquement auprès du centre de gestion, créez un utilisateur avec les privilèges d'administrateur et de maintenance réseau sur le centre de gestion. Les utilisateurs disposant de ces privilèges peuvent utiliser l'API REST. Reportez-vous au [Guide d'administration de Cisco Secure Firewall Management Center](#).
- Ajoutez dans le centre de gestion une politique d'accès qui correspond au nom de la politique que vous spécifierez lors du déploiement du modèle.
- Vérifier que la licence du centre de gestion virtuel est approprié.

- Effectuez les étapes ci-dessous après avoir ajouté la grappe au centre de gestion virtuel :
  1. Configurez les paramètres de la plateforme avec le numéro de port de vérification de l'intégrité dans le centre de gestion. Pour en savoir plus sur cette configuration, consultez les [paramètres de la plateforme](#).
  2. Créez une route statique pour le trafic de données. Pour en savoir plus sur la création d'une route statique, consultez [Ajouter une route statique](#).

Exemple de configuration d'une route statique:

```
Network: any-ipv4
Interface: vxlan_tunnel
Leaked from Virtual Router: Global
Gateway: vxlan_tunnel_gw
Tunneled: false
Metric: 2
```



**Remarque** `vxlan_tunnel_gw` est l'adresse IP de la passerelle du sous-réseau de données.

## Déployer une grappe sur Azure avec GWLB à l'aide d'un modèle Azure Resource Manager

Déployer l'ensemble de machines virtuelles identiques pour Azure GWLB à l'aide du modèle personnalisé Azure Resource Manager (ARM).

### Procédure

- 
- Étape 1** Préparez le modèle.
- a) Copiez le référentiel github dans votre dossier local. Consultez <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure>.
  - b) Modifiez `azure_ftdv_gwlb_cluster.json` et `azure_ftdv_gwlb_cluster_parameters.json` avec les paramètres requis.
- Étape 2** Connectez-vous au portail Azure : <https://portal.azure.com>.
- Étape 3** Créez un groupe de ressources.
- a) Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.
  - b) Choisissez la **région** requise.
- Étape 4** Créez un réseau virtuel avec quatre sous-réseaux : de gestion, de dépistage, externe et Cluster Control Link (CCL, lien contrôlé par la grappe).
- a) Créer le réseau virtuel.
    1. Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.
    2. Choisissez la **région** requise. Cliquez sur **Next: IP Addresses** (prochaines adresses IP).

Dans l'onglet **IP Addresses** (adresses IP), cliquez sur **Add subnet** (ajouter un sous-réseau) et ajoutez les sous-réseaux suivants : Management, Diagnostic, Data et Cluster Control Link.

b) Ajoutez les sous-réseaux.

**Étape 5**

Déployez le modèle personnalisé.

- a) Cliquez sur **Créer > Déploiement à l'aide de modèles (déployer à l'aide de modèles personnalisés)**.
- b) Cliquez sur **Créer votre propre modèle dans l'éditeur**.
- c) Cliquez sur **Load File**( téléverser le fichier) et chargez **azure\_ftdv\_gwlb\_cluster.json**.
- d) Cliquez sur **Save** (enregistrer).

**Étape 6**

Configurer les détails de l'instance

- a) Saisissez les valeurs requises, puis cliquez sur **Vérifier + créer**.
- b) Cliquez sur **Create** (créer) une fois la validation réussie.

**Étape 7**

Une fois l'instance en cours d'exécution, vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en saisissant la commande **show cluster info**.

*Illustration 10 : afficher l'information sur grappe*

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
Interface mode: individual
Cluster Member Limit : 16
This is "12" in state CONTROL_NODE
ID : 0
Version : 99.19(1)180
Serial No.: 9AKGFV8VH4G
CCL IP : 10.1.1.12
CCL MAC : 000d.3a55.5470
Module : NGFWv
Resource : 8 cores / 28160 MB RAM
Last join : 11:13:24 UTC Sep 5 2022
Last leave: N/A
```

**Étape 8**

Dans le portail Azure, cliquez sur l'application Function pour enregistrer la grappe auprès de Centre de gestion.

**Remarque** Si vous ne souhaitez pas utiliser l'application Fonction, vous pouvez également enregistrer le nœud de contrôle auprès de centre de gestion directement en utilisant **Add > Device** (et non **Add > Cluster**). Les autres nœuds de la grappe s'enregistreront automatiquement.

**Étape 9**

Créez les informations d'authentification FTPS en cliquant sur **Centre de déploiement > Informations d'identification FTPS > Portée de l'utilisateur > Configurer le nom d'utilisateur et le mot de passe**, puis cliquez sur **Enregistrer**.

**Étape 10**

Chargez le fichier Cluster\_Function.zip dans l'application Function en exécutant la commande **curl** suivante sur le terminal local.

```
curl -X POST -u username --data-binary @"Cluster_Function.zip" https://
Function_App_Name.scm.azurewebsites.net/api/zipdeploy
```

**Remarque** La commande **curl** peut prendre quelques minutes (environ 2 à 3 minutes) pour achever de s'exécuter.

La fonction sera chargée dans l'application Fonction. La fonction démarrera et vous pourrez voir les journaux dans la file d'attente de sortie du compte de stockage. L'enregistrement du périphérique auprès du centre de gestion sera lancé.

Illustration 11 : Fonctions

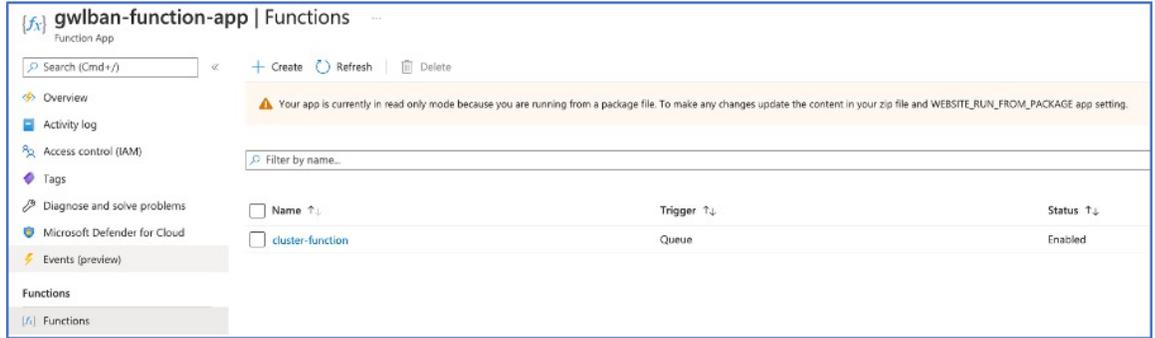


Illustration 12 : Files d'attente

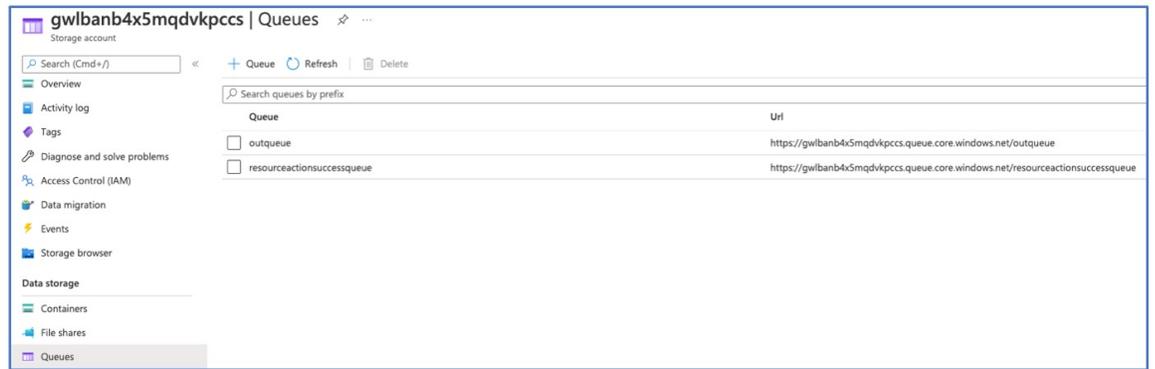
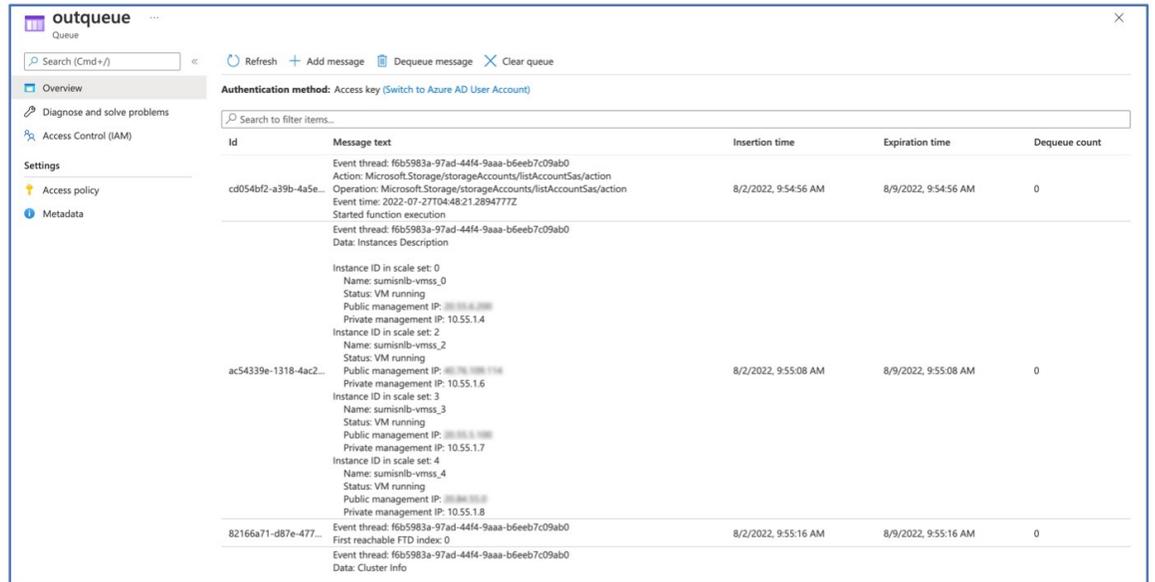
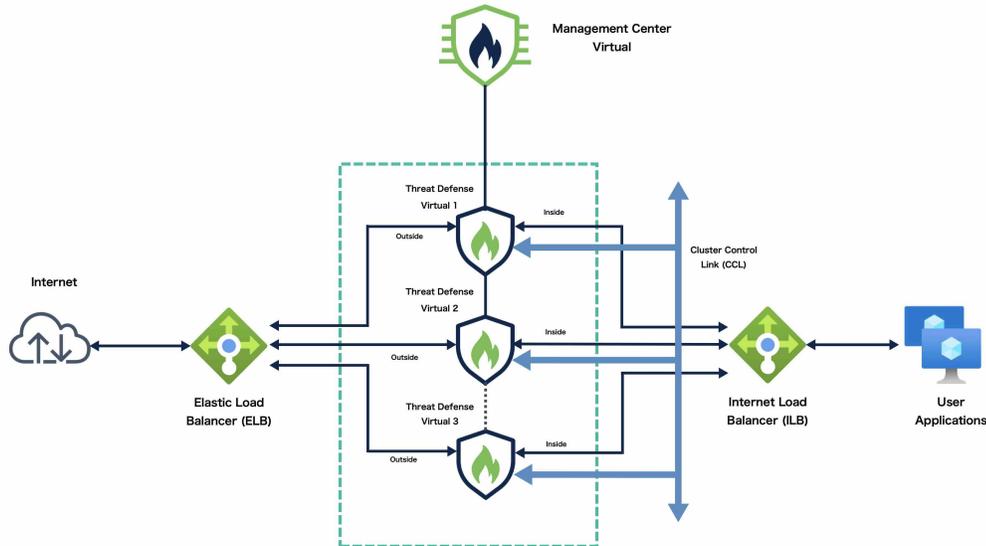


Illustration 13 : Outqueue



## Exemple de topologie pour le déploiement de grappes selon l'équilibrage de la charge de réseau



Cette topologie décrit le flux de trafic entrant et sortant. La grappe virtuelle Threat Defense est comprise entre les équilibreurs de charge interne et externe. Une instance virtuelle du centre de gestion est utilisée pour gérer la grappe.

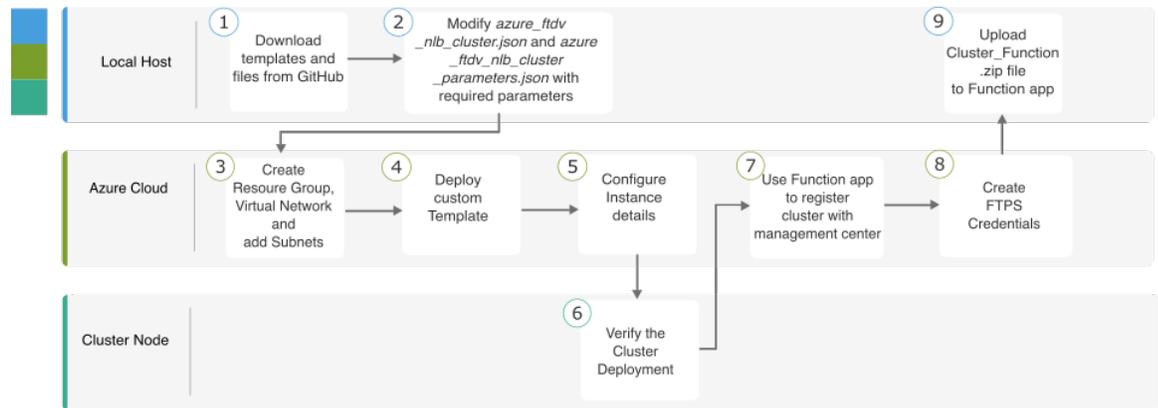
Le trafic entrant provenant d'Internet est dirigé vers l'équilibreur de charge externe, qui le transmet ensuite à la grappe virtuelle Threat Defense. Une fois que le trafic a été inspecté par une instance virtuelle de Threat Defense dans la grappe, il est transféré à la machine virtuelle de l'application.

Le trafic sortant de la machine virtuelle d'application est transmis à l'équilibreur de charge interne. Le trafic est ensuite acheminé vers la grappe virtuelle Threat Defense, puis envoyé à Internet.

## Processus de bout en bout pour le déploiement de grappe Threat Defense Virtual dans Azure avec équilibrage de la charge de réseau

### Déploiement basé sur un modèle

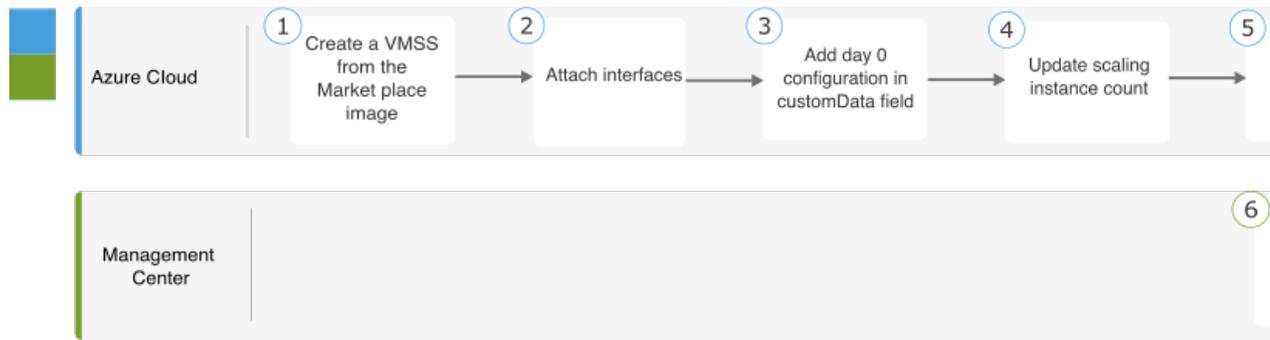
Le schéma dynamique suivant illustre le flux de travail du déploiement basé sur un modèle de la grappe virtuelle Threat Defense dans Azure avec l'équilibrage de la charge réseau (TLB).



	Espace de travail	Étapes
①	Hôte local	Téléchargez des modèles et des fichiers à partir de GitHub.
②	Hôte local	Modifiez <i>azure_ftdv_nlb_cluster.json</i> et <i>azure_ftdv_nlb_cluster_parameters.json</i> avec les paramètres requis.
③	Nuage Azure	Créez le groupe de ressources, le réseau virtuel et les sous-réseaux.
④	Nuage Azure	Déployer un modèle personnalisé.
⑤	Nuage Azure	Configurer les détails de l'instance.
⑥	Nom de la grappe	Vérifier le déploiement de la grappe.
⑦	Nuage Azure	Utilisez l'application de fonction pour enregistrer la grappe auprès du centre de gestion.
⑧	Nuage Azure	Créer des informations d'authentification FTPS
⑨	Hôte local	Téléversez le fichier <i>Cluster_Function.zip</i> dans l'application de fonction.

**Déploiement manuel**

Le diagramme suivant illustre le flux de travail du déploiement manuel de la grappe virtuelle Threat Defense dans Azure avec équilibrage de la charge réseau.



	Espace de travail	Étapes
①	Hôte local	Créez un VMSS à partir de l’image du Marché.
②	Hôte local	Associer des interfaces.
③	Hôte local	Ajouter la configuration de jour 0 dans le champ customData.
④	Hôte local	Mettre à jour le nombre d’instances évolutives.
⑤	Hôte local	Configurer NLB.
⑥	Centre de gestion	Ajouter un nœud de contrôle

## Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms et les valeurs des paramètres sont indiqués dans le modèle.

- [azure\\_ftdv\\_nlb\\_cluster\\_parameters.json](#) : modèle pour saisir les paramètres de la grappe virtuelle Threat Defense avec équilibrage de la charge réseau.
- [azure\\_ftdv\\_nlb\\_cluster.json](#) – Modèle pour déployer une grappe virtuelle Threat Defense avec équilibrage de la charge réseau.

## Prérequis

- Pour permettre à la grappe de s’enregistrer automatiquement auprès du centre de gestion, créez un utilisateur avec les privilèges d’administrateur et de maintenance réseau sur le centre de gestion. Les utilisateurs disposant de ces privilèges peuvent utiliser l’API REST. Reportez-vous au [Guide d’administration de Cisco Secure Firewall Management Center](#).
- Ajoutez une politique d’accès dans le centre de gestion qui correspond au nom de la politique que vous spécifierez lors du déploiement du modèle.
- Vérifier que la licence du centre de gestion virtuel est approprié.

- Une fois la grappe ajoutée au centre de gestion virtuel :
  1. Configurez les paramètres de la plateforme avec le numéro de port de vérification de l'intégrité dans le centre de gestion. Pour en savoir plus sur cette configuration, consultez les [paramètres de la plateforme](#).
  2. Créez des routes statiques pour le trafic provenant des interfaces externes et internes. Pour en savoir plus sur la création d'une route statique, consultez [Ajouter une route statique](#).

Exemple de configuration de routage statique pour l'interface externe :

```
Network: any-ipv4
Interface: outside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-outside
Tunneled: false
Metric: 10
```



**Remarque** *ftdv-cluster-outside* est l'adresse IP de la passerelle du sous-réseau externe.

Exemple de configuration de routage statique pour l'interface interne :

```
Network: any-ipv4
Interface: inside
Leaked from Virtual Router: Global
Gateway: ftdv-cluster-inside-gw
Tunneled: false
Metric: 11
```



**Remarque** *ftdv-cluster-inside-gw* est l'adresse IP de la passerelle du sous-réseau interne.

3. Configurez la règle NAT pour le trafic de données. Pour en savoir plus sur la configuration des règles NAT, consultez [Traduction d'adresses réseau](#)

## Déployer une grappe sur Azure avec équilibrage de la charge de réseau à l'aide d'un modèle Azure Resource Manager

Déployez la grappe pour l'équilibrage de la charge (TLB) Azure à l'aide du modèle personnalisé Azure Resource Manager (ARM).

### Procédure

#### Étape 1

Préparez le modèle.

- a) Copiez le référentiel github dans votre dossier local. Consultez <https://github.com/CiscoDevNet/cisco-ftdv/tree/master/cluster/azure>.
- b) Modifiez *azure\_ftdv\_nlb\_cluster.json* et *azure\_ftdv\_nlb\_cluster\_parameters.json* avec les paramètres requis.

- Étape 2** Connectez-vous au portail Azure : <https://portal.azure.com>.
- Étape 3** Créez un groupe de ressources.
- Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.
  - Choisissez la **région** requise.
- Étape 4** Créer un réseau virtuel avec cinq sous-réseaux : de gestion, de dépiage, interne, externe et de liaison de commande de grappe.
- Créer le réseau virtuel.
    - Dans l'onglet **Basics** (Base), choisissez **Subscription** (Abonnement) et **Resource Group** (Groupe de ressources) dans les listes déroulantes.
    - Choisissez la **région** requise. Cliquez sur **Next: IP Addresses** (prochaines adresses IP).
  - Ajoutez les sous-réseaux.
 

Dans l'onglet **IP Addresses** (adresses IP), cliquez sur **Add subnet** (ajouter un sous-réseau) et ajoutez les sous-réseaux suivants : Gestion, Dépiage, interne, Externe et Liaison de commande de grappe.
- Étape 5** Déployez le modèle personnalisé.
- Cliquez sur **Créer > Déploiement à l'aide de modèles (déployer à l'aide de modèles personnalisés)**.
  - Cliquez sur **Créer votre propre modèle dans l'éditeur**.
  - Cliquez sur **Load File** (téléverser le fichier) et chargez **azure\_ftdv\_nlb\_cluster.json**.
  - Cliquez sur **Save** (enregistrer).
- Étape 6** Configurer les détails de l'instance
- Saisissez les valeurs requises, puis cliquez sur **Vérifier + créer**.
 

**Remarque** Pour les adresses de début et de fin de la liaison de commande de grappe, indiquez uniquement le nombre d'adresses dont vous avez besoin (jusqu'à 16). Une plage plus importante peut nuire aux performances.
  - Cliquez sur **Create** (créer) une fois la validation réussie.
- Étape 7** Une fois l'instance en cours d'exécution, vérifiez le déploiement de la grappe en vous connectant à l'un des nœuds et en utilisant la commande **show cluster info**.

**Illustration 14 : afficher l'information sur grappe**

```
> show cluster info
Cluster gwlb-cluster-template-with-AN: On
Interface mode: individual
Cluster Member Limit : 16
This is "12" in state CONTROL_NODE
ID : 0
Version : 99.19(1)180
Serial No.: 9AKGFV8VH4G
CCL IP : 10.1.1.12
CCL MAC : 000d.3a55.5470
Module : NGFWv
Resource : 8 cores / 28160 MB RAM
Last join : 11:13:24 UTC Sep 5 2022
Last leave: N/A
```

- Étape 8** Dans le portail Azure, cliquez sur l'application Function pour enregistrer la grappe dans centre de gestion.

**Remarque** Si vous ne souhaitez pas utiliser l'application Fonction, vous pouvez également enregistrer le nœud de contrôle avec le centre de gestion directement en utilisant **Ajouter > Périphérique** (et non **Ajouter > Grappe**). Les autres nœuds de la grappe s'enregistreront automatiquement.

**Étape 9** Créez les informations d'authentification FTPS en cliquant sur **Centre de déploiement > Informations d'identification FTPS > Portée de l'utilisateur > Configurer le nom d'utilisateur et le mot de passe**, puis cliquez sur **Enregistrer**.

**Étape 10** Chargez le fichier Cluster\_Function.zip dans l'application Fonction en exécutant la commande **curl** suivante sur le terminal local.

```
curl -X POST -u username --data-binary @"Cluster_Function.zip" https://Function_App_Name.scm.azurewebsites.net/api/zipdeploy
```

**Remarque** La commande **curl** peut nécessiter quelques minutes (environ 2 à 3 minutes) pour terminer l'exécution de la commande.

La fonction sera chargée dans l'application Fonction. La fonction démarrera et vous pourrez voir les journaux dans la file d'attente de sortie du compte de stockage. L'enregistrement du périphérique auprès du centre de gestion sera lancé.

## Déployer manuellement la grappe dans Azure

Pour déployer la grappe manuellement, préparez la configuration de day0, déployez chaque nœud, puis ajoutez le nœud de contrôle à centre de gestion.

### Créer la configuration Day0 pour Azure

Vous pouvez utiliser une configuration fixe ou une configuration personnalisée.

#### Créer la configuration Day0 avec une configuration fixe pour Azure

La configuration fixe générera automatiquement la configuration de démarrage de grappe.

```
{
  "AdminPassword": "password",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "FmcIp": "<FMC_IP>",
  "FmcRegKey": "<REGISTRATION_KEY>",
  "FmcNatId": "<NAT_ID>",
  "Cluster": {
    "CclSubnetRange": "ip_address_start ip_address_end",
    "ClusterGroupName": "cluster_name",
    "HealthProbePort": "port_number",
    "GatewayLoadBalancerIP": "ip_address",
    "EncapsulationType": "vxlan",
    "InternalPort": "internal_port_number",
    "ExternalPort": "external_port_number",
    "InternalSegId": "internal_segment_id",
    "ExternalSegId": "external_segment_id"
  }
}
```

### Exemple

Un exemple de configuration du jour 0 est donné ci-dessous.

```
{
  "AdminPassword": "password",
  "FirewallMode": "routed",
  "ManageLocally": "No",
  "FmcIp": "<FMC_IP>",
  "FmcRegKey": "<REGISTRATION_KEY>",
  "FmcNatId": "<NAT_ID>",
  "Cluster": {
    "CclSubnetRange": "10.45.3.4 10.45.3.30", //mandatory user input
    "ClusterGroupName": "ngfwv-cluster", //mandatory user input
    "HealthProbePort": "7777", //mandatory user input
    "GatewayLoadBalanceIP": "10.45.2.4", //mandatory user input
    "EncapsulationType": "vxlan",
    "InternalPort": "2000",
    "ExternalPort": "2001",
    "InternalSegId": "800",
    "ExternalSegId": "801"
  }
}
```



**Remarque** Si vous copiez et collez la configuration donnée ci-dessus, veuillez à supprimer la //saisie utilisateur obligatoire de la configuration

Pour les paramètres de vérification de l'intégrité d'Azure, assurez-vous de spécifier le **HealthProbePort** que vous définissez ici.

Pour la variable **CclSubnetRange**, spécifiez une plage d'adresses IP à partir de xxx4. Assurez-vous d'avoir au moins 16 adresses IP disponibles pour la mise en grappe. Quelques exemples d'adresses IP de début et de fin sont donnés ci-dessous.

**Tableau 3 : Exemples d'adresses IP de début et de fin**

CIDR	Adresse IP de début	Adresse IP de fin
10.1.1.0/27	10.1.1.4	10.1.1.30
10.1.1.32/27	10.1.1.36	10.1.1.62
10.1.1.64/27	10.1.1.68	10.1.1.94
10.1.1.96/27	10.1.1.100	10.1.1.126
10.1.1.128/27	10.1.1.132	10.1.1.158
10.1.1.160/27	10.1.1.164	10.1.1.190
10.1.1.192/27	10.1.1.196	10.1.1.222
10.1.1.224/27	10.1.1.228	10.1.1.254

### Créer la configuration Day0 avec une configuration personnalisée pour Azure

Vous pouvez saisir la configuration complète de démarrage de grappe à l'aide des commandes.

```
{
  "AdminPassword": "password",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "FmcIp": "<FMC_IP>",
  "FmcRegKey": "<REGISTRATION_KEY>",
  "FmcNatId": "<NAT_ID>",
  "Cluster": {
    "CclSubnetRange": "ip_address_start ip_address_end",
    "ClusterGroupName": "cluster_name",
    "HealthProbePort": "port_number",
    "GatewayLoadBalancerIP": "ip_address",
    "EncapsulationType": "vxlan",
    "InternalPort": "internal_port_number",
    "ExternalPort": "external_port_number",
    "InternalSegId": "internal_segment_id",
    "ExternalSegId": "external_segment_id"
  }
}
```

### Exemple

Un exemple de configuration de jour 0 pour les **versions 7.4 et ultérieures** est donné ci-dessous.

```
{
  "AdminPassword": "Sup3rnatural",
  "Hostname": "clusterftdv",
  "FirewallMode": "routed",
  "ManageLocally": "No",
  "FmcIp": "<FMC_IP>",
  "FmcRegKey": "<REGISTRATION_KEY>",
  "FmcNatId": "<NAT_ID>",
  "run_config": [
    "cluster interface-mode individual force",
    "policy-map global_policy",
    "class inspection_default",
    "no inspect h323 h225",
    "no inspect h323 ras",
    "no inspect rtsp",
    "no inspect skinny",
    "interface Management0/0",
    "management-only",
    "nameif management",
    "security-level 0",
    "ip address dhcp",
    "interface GigabitEthernet0/0",
    "no shutdown",
    "nameif vxlan_tunnel",
    "security-level 0",
    "ip address dhcp",
    "interface GigabitEthernet0/1",
    "no shutdown",
    "nve-only cluster",
    "nameif ccl_link",
    "security-level 0",
    "ip address dhcp",
    "interface vni1",
    "description Clustering Interface",
    "segment-id 1",
    "vtep-nve 1",
    "interface vni2",
    "proxy paired",
  ]
}
```

```

"nameif GWLB-backend-pool",
"internal-segment-id 800",
"external-segment-id 801",
"internal-port 2000",
"external-port 2001",
"security-level 0",
"vtep-nve 2",
"object network ccl#link",
"range 10.45.3.4 10.45.3.30",
"object-group network cluster#group",
"network-object object ccl#link",
"nve 1 ",
"encapsulation vxlan",
"source-interface ccl_link",
"peer-group cluster#group",
"nve 2 ",
"encapsulation vxlan",
"source-interface vxlan_tunnel",
"peer ip <GatewayLoadbalancerIP>",
"cluster group ftdv-cluster",
"local-unit 1",
"cluster-interface vnil ip 1.1.1.1 255.255.255.0",
"priority 1",
"enable",
"mtu vxlan_tunnel 1454",
"mtu ccl_link 1454"
]
}

```

Un exemple de configuration de jour 0 pour les versions 7.3 et antérieures est donné ci-dessous.

```

{
"AdminPassword": "Sup3rnatural",
"Hostname": "clusterftdv",
"FirewallMode": "routed",
"ManageLocally": "No",
"FmcIp": "<FMC_IP>",
"FmcRegKey": "<REGISTRATION_KEY>",
"FmcNatId": "<NAT_ID>",
"run_config": [
"cluster interface-mode individual force",
"policy-map global_policy",
"class inspection_default",
"no inspect h323 h225",
"no inspect h323 ras",
"no inspect rtsp",
"no inspect skinny",
"interface Management0/0",
"management-only",
"nameif management",
"security-level 0",
"ip address dhcp",
"interface GigabitEthernet0/0",
"no shutdown",
"nameif vxlan_tunnel",
"security-level 0",
"ip address dhcp",
"interface GigabitEthernet0/1",
"no shutdown",
"nve-only cluster",
"nameif ccl_link",
"security-level 0",
"ip address dhcp",
"interface vnil",

```

```

"description Clustering Interface",
"segment-id 1",
"vtep-nve 1",
"interface vni2",
"proxy paired",
"nameif GWLB-backend-pool",
"internal-segment-id 800",
"external-segment-id 801",
"internal-port 2000",
"external-port 2001",
"security-level 0",
"vtep-nve 2",
"object network ccl#link",
"range 10.45.3.4 10.45.3.30", //mandatory user input
"object-group network cluster#group",
"network-object object ccl#link",
"nve 1 ",
"encapsulation vxlan",
"source-interface ccl_link",
"peer-group cluster#group",
"nve 2 ",
"encapsulation vxlan",
"source-interface vxlan_tunnel",
"peer ip <GatewayLoadbalancerIP>",
"cluster group ftdv-cluster", //mandatory user input
"local-unit 1",
"cluster-interface vni1 ip 1.1.1.1 255.255.255.0",
"priority 1",
"enable",
"mtu vxlan_tunnel 1454",
"mtu ccl_link 1554"
]
}

```



**Remarque** Si vous copiez et collez la configuration donnée ci-dessus, veuillez à supprimer //entrée utilisateur obligatoire de la configuration.

## Déployer manuellement les nœuds de la grappe : Déploiement basé sur GWLB

Déployez les nœuds de la grappe pour qu'ils forment une grappe.

### Procédure

- Étape 1** Créez un ensemble de machines virtuelles évolutives à partir de l'image de la place de marché avec 0 nombre d'instances à l'aide de la CLI **az vmss create**.
- ```

az vmss create --resource-group <ResourceGroupName> --name <VMSSName> --vm-sku <InstanceSize> --image <FTDvImage> --instance-count 0 --admin-username <AdminUserName> --admin-password <AdminPassword> --plan-name <ftdv-azure-byol/ftdv-azure-payg> --plan-publisher cisco --plan-product cisco-ftdv --plan-promotion-code <ftdv-azure-byol/ftdv-azure-payg> --vnet-name <VirtualNetworkName> --subnet <MgmtSubnetName>

```
- Étape 2** Connectez trois interfaces : dépistage, données et liaison de commande de grappe.
- Étape 3** Accédez à l'ensemble de machines virtuelles évolutives que vous avez créé et effectuez les étapes suivantes :

- a) Dans la section **Operating system** (système d'exploitation), ajoutez la configuration du jour 0 dans le champ **personData**.
- b) Cliquez sur **Save** (enregistrer).
- c) Dans la section **Scaling** (évolutivité), mettez à jour le nombre d'instances avec le nœud de grappe requis. Vous pouvez définir la plage du nombre d'instances : au minimum 1 et au maximum 16.

**Étape 4** Configurez l'équilibreur de charge de la passerelle Azure. Consultez [le scénario de mise à l'échelle automatique avec l'équilibreur de charge de passerelle Azure](#) pour en savoir plus.

**Étape 5** Ajoutez le nœud de contrôle à centre de gestion. Consultez [Ajouter la grappe au centre de gestion \(déploiement manuel\)](#), à la page 50.

## Déployer manuellement les nœuds de la grappe : Déploiement basé sur l'équilibrage de la charge de réseau (TLB)

Déployez les nœuds de la grappe pour qu'ils forment une grappe.

### Procédure

**Étape 1** Créez un ensemble de machines virtuelles évolutives à partir de l'image de la place de marché avec 0 nombre d'instances à l'aide de la CLI **az vmss create**.

```
az vmss create --resource-group <ResourceGroupName> --name <VMSSName> --vm-sku <InstanceSize>
--image <FTDvImage> --instance-count 0 --admin-username <AdminUserName> --admin-password
<AdminPassword> --plan-name <ftdv-azure-byol/ftdv-azure-payg> --plan-publisher cisco --plan-product
cisco-ftdv --plan-promotion-code <ftdv-azure-byol/ftdv-azure-payg> --vnet-name <VirtualNetworkName>
--subnet <MgmtSubnetName>
```

**Étape 2** Connectez quatre interfaces : dépistage, interne, externe et liaison de commande de grappe.

**Étape 3** Accédez à l'ensemble de machines virtuelles identiques que vous avez créé et procédez comme suit :

- a) Dans la section **Operating system** (système d'exploitation), ajoutez la configuration **day0** dans le champ personnaliser les données.
- b) Cliquez sur **Save** (enregistrer).
- c) Dans la section **Scaling** (évolutivité), mettez à jour le nombre d'instances avec le nœud de grappe requis. Vous pouvez définir la plage du nombre d'instances : au minimum 1 et au maximum 16.

**Étape 4** Ajoutez le nœud de contrôle au centre de gestion. Consultez [Ajouter la grappe au centre de gestion \(déploiement manuel\)](#), à la page 50.

## Dépannage du déploiement de grappes dans Azure

- Problème : aucun flux de trafic

Dépannage :

- Vérifiez si l'état de la sonde d'intégrité des instances virtuelles de défense contre les menaces déployées avec une GWLB est intègre.

- Si l'état de la sonde d'intégrité de l'instance virtuelle de défense contre les menaces est non intègre,
  - Vérifiez si la voie de routage statique est configurée dans Management Center Virtual.
  - Vérifiez si la passerelle par défaut correspond à l'adresse IP de la passerelle du sous-réseau de données.
  - Vérifiez si l'instance virtuelle de défense contre les menaces reçoit le trafic de la sonde d'intégrité.
  - Vérifiez si la liste d'accès configurée dans le centre de gestion virtuel autorise le trafic des sondes d'intégrité.

- Problème : la grappe n'est pas formée

Dépannage :

- Vérifiez l'adresse IP de l'interface de grappe nve uniquement. Assurez-vous de pouvoir envoyer un message ping à l'interface de grappe nve uniquement des autres nœuds.
  - Vérifiez que l'adresse IP des interfaces de grappe nve uniquement fait partie du groupe d'objets.
  - Assurez-vous que l'interface NVE est configurée avec le groupe d'objets .
  - Assurez-vous que l'interface de grappe dans le groupe de grappes possède la bonne interface VNI. Cette interface VNI a la NVE avec le groupe d'objets correspondant.
  - Assurez-vous que les nœuds peuvent être envoyés à l'aide d'un ping les uns des autres. Étant donné que chaque nœud a sa propre adresse IP d'interface de grappe, ils devraient pouvoir être interrogés les uns des autres.
  - Vérifiez si l'adresse de début et de fin du sous-réseau CCL mentionnée lors du déploiement du modèle est correcte. L'adresse de début doit commencer par la première adresse IP disponible dans le sous-réseau. Par exemple, si le sous-réseau est 192.168.1.0/24. L'adresse de début doit être 192.168.1.4 (les trois adresses IP de début sont réservées par Azure).
  - Vérifiez si le Management Center virtuel dispose d'une licence valide.
- Problème : erreur liée au rôle lors du déploiement de ressources dans le même groupe de ressources.

Dépannage : supprimez les rôles donnés ci-dessous en utilisant les commandes suivantes sur le terminal.

Message d'erreur :

```
"error": {
  "code": "RoleAssignmentUpdateNotPermitted",
  "message": "Tenant ID, application ID, principal ID, and scope are not allowed to be updated."}
```

- **az role assignment delete --resource-group <Nom du groupe de ressources> --role "Storage Queue Data Contributor"**
- **az role assignment delete --resource-group <Nom du groupe de ressources> --role "Contributor"**

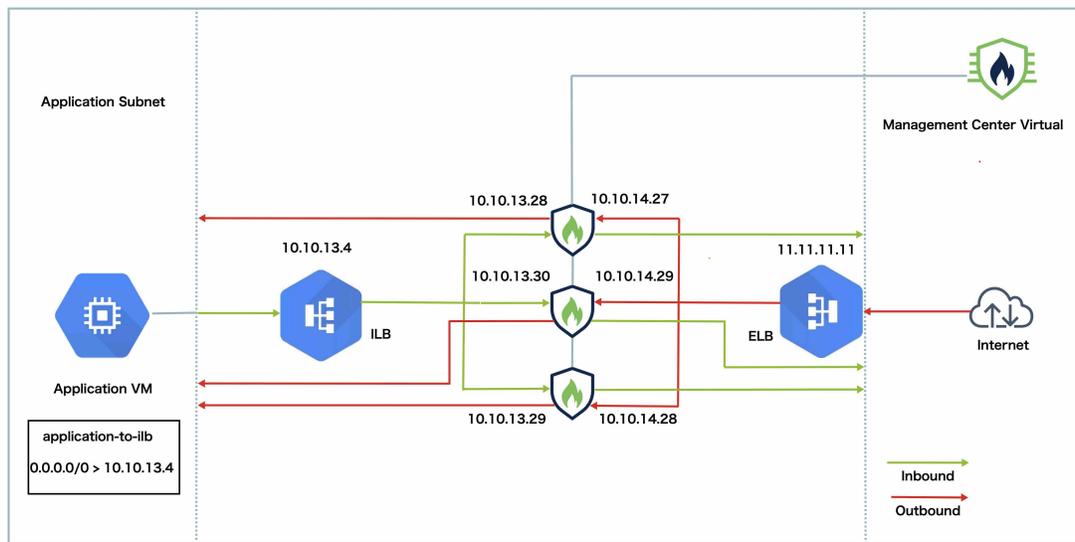
# Déployer la grappe dans GCP

Pour déployer une grappe dans GCP, vous pouvez soit déployer manuellement, soit utiliser un modèle d'instance pour déployer un groupe d'instances. Vous pouvez utiliser la grappe avec des équilibreurs de charge GCP natifs ou des équilibreurs de charge non natifs tels que le routeur de services infonuagiques Cisco.



**Remarque** Le trafic sortant nécessite une NAT d'interface et est limité à 64 000 connexions.

## Exemple de topologie



Cette topologie décrit le flux de trafic entrant et sortant. La grappe virtuelle Threat Defense est comprise entre les équilibreurs de charge interne et externe. Une instance virtuelle du centre de gestion est utilisée pour gérer la grappe.

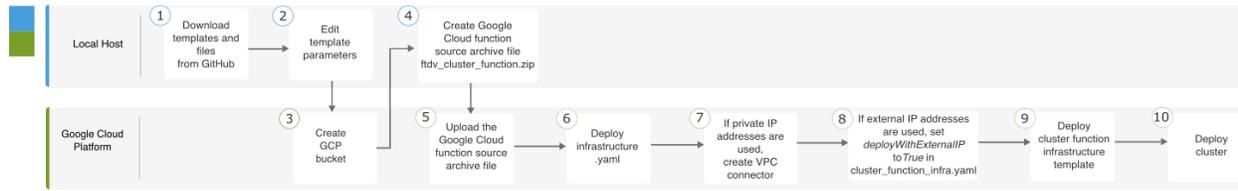
Le trafic entrant provenant d'Internet est dirigé vers l'équilibreur de charge externe, qui le transmet ensuite à la grappe virtuelle Threat Defense. Une fois que le trafic a été inspecté par une instance virtuelle de Threat Defense dans la grappe, il est transféré à la machine virtuelle de l'application.

Le trafic sortant de la machine virtuelle d'application est transmis à l'équilibreur de charge interne. Le trafic est ensuite acheminé vers la grappe virtuelle Threat Defense, puis envoyé à Internet.

## Processus de bout en bout pour le déploiement de Virtual Threat Defense Cluster dans GCP

### Déploiement basé sur un modèle

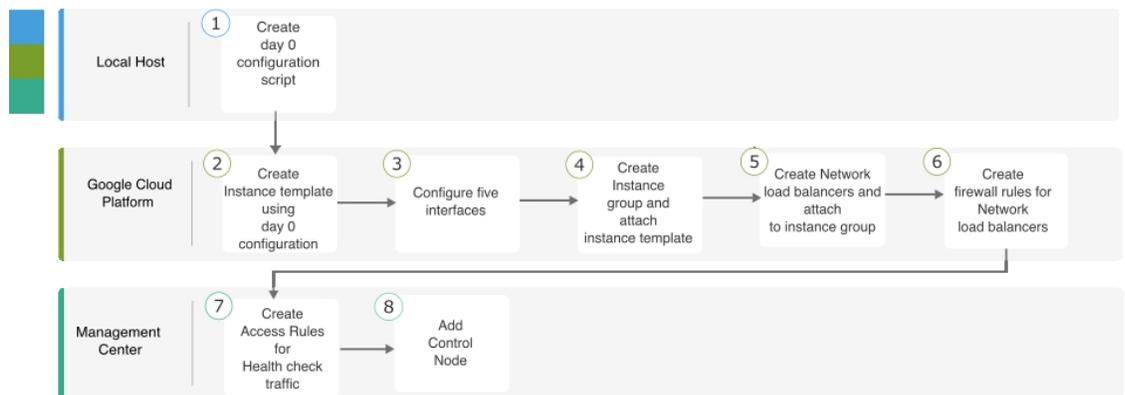
Le diagramme suivant illustre le flux de travail pour le déploiement basé sur le modèle de la grappe virtuelle Threat Defense sur GCP.



|    | Espace de travail   | Étapes                                                                                                                                       |
|----|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 1  | Hôte local          | Téléchargez des modèles et des fichiers à partir de GitHub.                                                                                  |
| 2  | Hôte local          | Modifiez les paramètres du modèle.                                                                                                           |
| 3  | Plateforme en nuage | Créez un compartiment GCP.                                                                                                                   |
| 4  | Hôte local          | Créez le fichier archive source de la fonction Google Cloud <i>ftdv_cluster_fonction.zip</i> .                                               |
| 5  | Plateforme en nuage | Chargez le fichier archive source de la fonction Google.                                                                                     |
| 6  | Plateforme en nuage | Déployez <i>infrastructure.yaml</i> .                                                                                                        |
| 7  | Plateforme en nuage | Si des adresses IP privées sont utilisées, créez un connecteur VPC.                                                                          |
| 8  | Plateforme en nuage | Si des adresses IP externes sont utilisées, définissez <i>deployWithExternalIP</i> sur <i>True</i> dans <i>cluster_fonction_infra.yaml</i> . |
| 9  | Plateforme en nuage | Déployer le modèle d'infrastructure de fonction de grappe.                                                                                   |
| 10 | Plateforme en nuage | Déployer la grappe                                                                                                                           |

### Déploiement manuel

Le diagramme suivant illustre le flux de travail pour le déploiement manuel de la grappe virtuelle Threat Defense sur GCP.



|   | Espace de travail   | Étapes                                                                                 |
|---|---------------------|----------------------------------------------------------------------------------------|
| ① | Hôte local          | Créer la configuration Day0 pour GCP                                                   |
| ② | Plateforme en nuage | Créer un modèle d'instance en utilisant la configuration de jour 0.                    |
| ③ | Plateforme en nuage | Configurer les interfaces.                                                             |
| ④ | Plateforme en nuage | Créer un groupe d'instances et attachez-y un modèle d'instance.                        |
| ⑤ | Plateforme en nuage | Créer l'équilibrage de la charge de réseau (BLB) et associez-la au groupe d'instances. |
| ⑥ | Plateforme en nuage | Créer des règles de pare-feu pour l'équilibrage de la charge réseau (TLB).             |
| ⑦ | Centre de gestion   | Créer des règles d'accès pour le trafic de vérification de l'intégrité.                |
| ⑧ | Centre de gestion   | Ajouter un nœud de contrôle                                                            |

## Modèles

Les modèles fournis ci-dessous sont disponibles dans GitHub. Les valeurs des paramètres sont explicites et les noms et les valeurs des paramètres sont indiqués dans le modèle.

- Modèle de déploiement de grappe pour le trafic est-ouest — [deploy\\_ngfw\\_cluster.yaml](#)
- Modèle de déploiement de grappe pour le trafic nord-sud : [deploy\\_ngfw\\_cluster.yaml](#)

## Déployer le groupe d'instances dans GCP à l'aide d'un modèle d'instance

Déployez le groupe d'instances dans GCP à l'aide d'un modèle d'instance.

### Avant de commencer

- Utiliser Google Cloud Shell pour le déploiement Vous pouvez également utiliser le SDK Google sur n'importe quel ordinateur macOS, Linux et Windows.
- Pour permettre à la grappe de s'enregistrer automatiquement auprès du centre de gestion, vous devez créer un utilisateur avec des privilèges d'administration sur le centre de gestion qui peut utiliser l'API REST. Consultez la section [Guide d'administration Cisco Secure Firewall Management Center](#).
- Ajoutez une politique d'accès dans le centre de gestion qui correspond au nom de la politique que vous avez spécifiée dans *cluster\_function\_infra.yaml*.

## Procédure

- Étape 1** Téléchargez les modèles à partir de [GitHub](#) dans votre dossier local.
- Étape 2** Modifiez **infrastructure.yaml**, **cluster\_fonction\_infra.yaml** et **deploy\_ngfw\_cluster.yaml** avec le paramètre *resourceNamePrefix* requis (par exemple, ngfwvcls) et les autres entrées utilisateur requises.
- Notez qu'il existe un fichier **deploy\_ngfw\_cluster.yaml** dans les dossiers **est-ouest** et **nord-sud** de GitHub. Téléchargez le modèle approprié selon vos exigences de flux de trafic.
- Étape 3** Créez un compartiment à l'aide de Google Cloud Shell pour téléverser le fichier d'archive source de la fonction nuage Google *ftdv\_cluster\_function.zip*.
- gsutil mb --pap enforced gs://resourceNamePrefix-ftdv-cluster-bucket/**
- Assurez-vous que la variable *resourceNamePrefix* correspond à la variable *resourceNamePrefix* que vous avez spécifiée dans **cluster\_fonction\_infra.yaml**.
- Étape 4** Créez un fichier d'archive pour l'infrastructure de grappe.
- Exemple :**
- ```
zip -j ftdv_cluster_function.zip ./cluster-function/*
```
- Étape 5** Téléversez l'archive source Google que vous avez créée précédemment.
- gsutil cp ftdv\_cluster\_function.zip gs://resourceNamePrefix-ftdv-cluster-bucket/**
- Étape 6** Déployer l'infrastructure pour la grappe.
- gcloud deployment-manager deployments create cluster\_name --config infrastructure.yaml**
- Étape 7** Si vous utilisez des adresses IP privées, procédez comme suit :
- Lancez et configurez le centre de gestion virtuel avec un VPC de gestion virtuel Threat Defense.
  - Créez un connecteur VPC pour connecter les fonctions Google Cloud avec le VPC de gestion virtuelle Threat Defense.
- gcloud compute networks vpc-access connectors create vpc-connector-name --region us-central1 --subnet resourceNamePrefix-ftdv-mgmt-subnet28**
- Étape 8** Si le centre de gestion est distant de la solution virtuelle Threat Defense et que cette dernière a besoin d'une adresse IP externe, veillez à définir **deployWithExternalIP** sur **True** (vrai) dans **cluster\_fonction\_infra.yaml**.
- Étape 9** Déployer l'infrastructure de la fonction de grappe.
- gcloud deployment-manager deployments create cluster\_name --config cluster\_fonction\_infra.yaml**
- Étape 10** Déployez la grappe.
- Pour le déploiement de la topologie nord-sud :
 

**gcloud deployment-manager deployments create cluster\_name --config north-south/deploy\_ngfw\_cluster.yaml**
  - Pour un déploiement de la topologie est-ouest :

```
gcloud deployment-manager deployments create cluster_name --config
east-west/deploy_ngfw_cluster.yaml
```

## Déployer la grappe manuellement dans GCP

Pour déployer la grappe manuellement, préparez la configuration de day0, déployez chaque nœud, puis ajoutez le nœud de contrôle à centre de gestion.

### Créer la configuration Day0 pour GCP

Vous pouvez utiliser une configuration fixe ou une configuration personnalisée.

#### Créer la configuration Day0 avec une configuration fixe pour GCP

La configuration fixe générera automatiquement la configuration de démarrage de grappe.

```
{
  "AdminPassword": "password",
  "Hostname": "hostname",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "Diagnostic": "OFF",
  "Cluster": {
    "CclSubnetRange": "ip_address_start ip_address_end",
    "ClusterGroupName": "cluster_name"
  }
}
```

Par exemple :

```
{
  "AdminPassword": "DeanWlnche$ter",
  "Hostname": "ciscoftdv",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "Cluster": {
    "CclSubnetRange": "10.10.55.2 10.10.55.253", //mandatory user input
    "ClusterGroupName": "ftdv-cluster" //mandatory user input
  }
}
```



**Remarque** Si vous copiez et collez la configuration donnée ci-dessus, veillez à supprimer **//entrée utilisateur obligatoire** de la configuration.

Pour la variable **CclSubnetRange**, notez que vous ne pouvez pas utiliser les deux premières adresses IP et les deux dernières adresses IP du sous-réseau. Consultez la section [Adresses IP réservées dans les sous-réseaux IPv4](#) pour en savoir plus. Assurez-vous d'avoir au moins 16 adresses IP disponibles pour la mise en grappe. Quelques exemples d'adresses IP de début et de fin sont donnés ci-dessous.

Tableau 4 : Exemples d'adresses IP de début et de fin

CIDR	Adresse IP de début	Adresse IP de fin
10.1.1.0/27	10.1.1.2	10.1.1.29
10.1.1.32/27	10.1.1.34	10.1.1.61
10.1.1.64/27	10.1.1.66	10.1.1.93
10.1.1.96/27	10.1.1.98	10.1.1.125
10.1.1.128/27	10.1.1.130	10.1.1.157
10.1.1.160/27	10.1.1.162	10.1.1.189
10.1.1.192/27	10.1.1.194	10.1.1.221
10.1.1.224/27	10.1.1.226	10.1.1.253
10.1.1.0/24	10.1.1.2	10.1.1.253

### Créer la configuration Day0 avec une configuration personnalisée pour GCP

Vous pouvez saisir la configuration complète de démarrage de grappe à l'aide des commandes.

```
{
  "AdminPassword": "password",
  "Hostname": "hostname",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "run_config": [comma_separated_threat_defense_configuration]
}
```

Dans l'exemple suivant, une configuration est créée avec des interfaces de gestion, interne et externe, et une interface VXLAN pour la liaison de commande de grappe. Notez les valeurs en gras qui doivent être uniques par nœud.

```
{
  "AdminPassword": "Wlnch3sterBr0s",
  "Hostname": "ftdvl",
  "FirewallMode": "Routed",
  "ManageLocally": "No",
  "run_config": [
    "cluster interface-mode individual force",
    "interface Management0/0",
    "management-only",
    "nameif management",
    "ip address dhcp",
    "interface GigabitEthernet0/0",
    "no shutdown",
    "nameif outside",
    "ip address dhcp",
    "interface GigabitEthernet0/1",
    "no shutdown",
    "nameif inside",
    "ip address dhcp",
    "interface GigabitEthernet0/2",
    "nve-only cluster",
    "nameif ccl_link",
    "ip address dhcp",
    "no shutdown",
  ]
}
```

```

"interface vni1",
"description Clustering Interface",
"segment-id 1",
"vtep-nve 1",
"object network ccl#link",
"range 10.1.90.2 10.1.90.17",
"object-group network cluster#group",
"network-object object ccl#link",
"nve 1",
"encapsulation vxlan",
"source-interface ccl_link",
"peer-group cluster#group",
"cluster group ftdv-cluster",
"local-unit 1",
"cluster-interface vni1 ip 10.1.1.1 255.255.255.0",
"priority 1",
"enable",
"mtu outside 1400",
"mtu inside 1400"
]
}
    
```



**Remarque** Pour l'objet de réseau de liaison de commande de grappe, indiquez uniquement le nombre d'adresses dont vous avez besoin (jusqu'à 16). Une plage plus importante peut nuire aux performances.

## Déployer manuellement les nœuds de la grappe

Déployez les nœuds de la grappe pour qu'ils forment une grappe. Pour la mise en grappe sur GCP, vous ne pouvez pas utiliser le type de machine à 4 vCPU. Le type de machine à 4 vCPU ne prend en charge que quatre interfaces, et cinq interfaces sont nécessaires. Utilisez un type de machine qui prend en charge cinq interfaces, par exemple, c2-standard-8.

### Procédure

- 
- Étape 1** Créer un modèle d'instance en utilisant la configuration de jour 0 (dans la section **Métadonnées > Script de démarrage**) avec cinq interfaces : externe, interne, liaison de gestion, de dépiage et de commande de grappe. Consultez [Guide de démarrage de Cisco Secure Firewall Threat Defense Virtual](#).
  - Étape 2** Créez un groupe d'instances et attachez le modèle d'instance.
  - Étape 3** Créez des équilibreurs de charge réseau GCP (internes et externes) et reliez-les au groupe d'instances.
  - Étape 4** Pour les équilibreurs de charge réseau GCP, autorisez les vérifications de l'intégrité dans votre politique de sécurité dans le centre de gestion. Consultez [Autoriser les vérifications de l'intégrité pour les équilibreurs de charge réseau GCP](#), à la page 49.
  - Étape 5** Ajoutez le nœud de contrôle au centre de gestion. Consultez [Ajouter la grappe au centre de gestion \(déploiement manuel\)](#), à la page 50.
-

# Autoriser les vérifications de l'intégrité pour les équilibreurs de charge réseau GCP

Google Cloud effectue des vérifications de l'intégrité pour déterminer si les serveurs principaux répondent au trafic.

Consultez <https://cloud.google.com/load-balancing/docs/health-checks> pour créer des règles de pare-feu pour les équilibreurs de charge réseau. Ensuite, dans centre de gestion, créez des règles d'accès pour autoriser le trafic de vérification de l'intégrité. Consultez <https://cloud.google.com/load-balancing/docs/health-check-concepts> pour connaître les plages réseau requises. Consultez [Règles de contrôle d'accès](#).

Vous devez également configurer des règles NAT manuelles dynamiques pour rediriger le trafic de vérification de l'intégrité vers le serveur de métadonnées de Google à l'adresse 169.254.169.254. Consultez [Configurer la NAT manuelle dynamique](#).

## Exemple de configuration de règles de NAT nord-sud

```

nat (inside,outside) source dynamic GCP-HC ILB-SOUTH destination static ILB-SOUTH METADATA
nat (outside,outside) source dynamic GCP-HC ELB-NORTH destination static ELB-NORTH METADATA

nat (outside,inside) source static any interface destination static ELB-NORTH Ubuntu-App-VM
nat (inside,outside) source dynamic any interface destination static obj-any obj-any

object network Metadata
  host 169.254.169.254

object network ILB-SOUTH
  host <ILB_IP>
object network ELB-NORTH
  host <ELB_IP>

object-group network GCP-HC
  network-object 35.191.0.0 255.255.0.0
  network-object 130.211.0.0 255.255.252.0
  network-object 209.85.204.0 255.255.252.0
  network-object 209.85.152.0 255.255.252.0
    
```

The screenshot shows the configuration page for a NAT rule named 'nat-ngfw-cis'. The 'Rules' tab is active, and the rule is expanded to show its configuration. The rule is a dynamic NAT rule with the following settings:

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	Options
1	↔	Dyn...	inside	outside	GCP-HC	ILB-SOUTH	ILB Health Check NAT rule	ILB-SOUTH	METADATA		Disc: false
2	↔	Dyn...	outside	outside	GCP-HC	ELB-NORTH		ELB-NORTH	METADATA		Disc: false
3	↔	Static	outside	inside	any	ELB-NORTH		Interface	Ubuntu-App-VM		Disc: false
4	↔	Dyn...	inside	outside	any	obj-any	Inbound/Outbound traffic NAT rule	Interface	obj-any		Disc: false

## Exemple de configuration de règles de NAT est-ouest

```

nat (inside,outside) source dynamic GCP-HC ILB-East destination static ILB-East Metadata
nat (outside,outside) source dynamic GCP-HC ILB-West destination static ILB-West Metadata

object network Metadata
  host 169.254.169.254

object network ILB-East
  host <ILB_East_IP>
object network ILB-West
    
```

**Ajouter la grappe au centre de gestion (déploiement manuel)**

```

host <ILB_West_IP>

object-group network GCP-HC
network-object 35.191.0.0 255.255.0.0
network-object 130.211.0.0 255.255.252.0
network-object 209.85.204.0 255.255.252.0
network-object 209.85.152.0 255.255.252.0
    
```

The screenshot shows the configuration page for a NAT rule named 'nat-ftdv-cluster'. The 'Rules' tab is active, and the rule is expanded to show its configuration. The rule is named 'NAT Rules Before' and has two entries. The first entry is for 'LB Health Check NAT rule' with a direction of 'X' (inside to outside). The second entry is for 'LB Health Check NAT rule' with a direction of 'X' (outside to outside). Both entries have 'GCP-HC' as the source and 'ILB-East' and 'ILB-West' as destinations. The 'Translated Sources' are 'ILB-East' and 'ILB-West', and the 'Translated Destinations' are 'Metadata'. The 'Options' column shows 'Dns:false' for both entries.

#	Direction	Type	Source Interface Objects	Destination Interface Objects	Original Packet			Translated Packet			Options
					Original Sources	Original Destinations	Original Services	Translated Sources	Translated Destinations	Translated Services	
1	X	Dyn...	inside	outside	GCP-HC	ILB-East	LB Health Check NAT rule	ILB-East	Metadata		Dns:false
2	X	Dyn...	outside	outside	GCP-HC	ILB-West	LB Health Check NAT rule	ILB-West	Metadata		Dns:false

## Ajouter la grappe au centre de gestion (déploiement manuel)

Utilisez cette procédure pour ajouter la grappe à centre de gestion si vous l'avez déployée manuellement. Si vous avez utilisé un modèle, la grappe s'enregistrera automatiquement sur centre de gestion.

Ajoutez l'une des unités de grappe en tant que nouveau périphérique à centre de gestion; le centre de gestion détecte automatiquement tous les autres membres de la grappe.

### Avant de commencer

- Toutes les unités de grappe doivent faire partie d'une grappe formée avec succès avant d'être ajoutée à la grappe centre de gestion. Vous devez également vérifier quelle unité est l'unité de contrôle. Utilisez la commande défense contre les menaces **show cluster info**.

### Procédure

#### Étape 1

Dans centre de gestion, choisissez **Périphériques > Gestion des périphériques**, puis choisissez **Ajouter > Ajouter un périphérique** pour ajouter l'unité de contrôle en utilisant l'adresse IP de gestion de l'unité.

**Illustration 15 : Ajouter un appareil**

Add Device
?

---

CDO Managed Device

Host:†

Display Name:

Registration Key: \*

Group:

Access Control Policy: \*

**Smart Licensing**  
 Note: All virtual Firewall Threat Defense devices require a performance tier license. Make sure your Smart Licensing account contains the available licenses you need. It's important to choose the tier that matches the license you have in your account. Click [here](#) for information about the Firewall Threat Defense performance-tiered licensing. Until you choose a tier, your Firewall Threat Defense virtual defaults to the FTDv50 selection.

Performance Tier (only for Firewall Threat Defense virtual 7.0 and above):

Malware  
 Threat  
 URL Filtering

Advanced

Unique NAT ID: †

Transfer Packets

- a) Dans le champ **Host** (Hôte), saisissez l'adresse IP ou le nom d'hôte de l'unité de contrôle.  
 Nous vous recommandons d'ajouter l'unité de contrôle pour obtenir les meilleures performances, mais vous pouvez ajouter n'importe quelle unité de la grappe.  
 Si vous avez utilisé un ID NAT lors de la configuration du périphérique, vous n'aurez peut-être pas besoin de remplir ce champ.
- b) **Display Name**(Nom d'affichage) : saisissez le nom de l'unité de contrôle comme vous souhaitez qu'il apparaisse dans centre de gestion.  
 Ce nom d'affichage n'est pas pour la grappe; elle concerne uniquement l'unité de contrôle que vous ajoutez. Vous pouvez ultérieurement modifier le nom d'autres membres de la grappe et le nom d'affichage de la grappe.

- c) Dans le champ **Registration Key**, saisissez la clé d'enregistrement que vous avez utilisée lors de la configuration du périphérique. La clé d'enregistrement est un code secret partagé à usage unique.
- d) Dans un déploiement multidomaine, quel que soit votre domaine actuel, affectez le périphérique à un **domaine descendant**.

Si votre domaine actuel est un domaine descendant, le périphérique est automatiquement ajouté au domaine actuel. Si votre domaine actuel n'est pas un domaine descendant, après l'enregistrement, vous devez passer au domaine descendant pour configurer le périphérique.

- e) (Facultatif) Ajouter le périphérique à un **groupe** de périphériques .
- f) Choisissez une **politique de contrôle d'accès** initiale à déployer sur le périphérique lors de l'inscription ou créez une nouvelle politique.

Si vous créez une nouvelle politique, vous créez seulement une politique de base. Vous pourrez personnaliser la politique ultérieurement selon vos besoins.

The screenshot shows a 'New Policy' configuration window. It contains the following elements:

- Name:** A text input field containing the word 'basic'.
- Description:** An empty text input field with a blue border.
- Select Base Policy:** A dropdown menu currently showing 'None'.
- Default Action:** Three radio button options: 'Block all traffic' (which is selected), 'Intrusion Prevention', and 'Network Discovery'.
- Snort3:** A checkbox that is currently unchecked.

- g) Choisissez la licence à appliquer au périphérique.
- h) Si vous avez utilisé un ID NAT lors de la configuration du périphérique , développez la section **Advanced** (Avancé) et saisissez le même ID NAT dans le champ **Unique NAT ID** (ID NAT unique).
- i) Cochez la case **Transfer Packets** (Transférer les paquets) pour permettre au périphérique de transférer des paquets vers le centre de gestion.

Par défaut, cette option est activée. Lorsque des événements comme IPS ou Snort sont déclenchés avec cette option activée, l'appareil envoie des informations sur les métadonnées d'événement et des données de paquets vers centre de gestion pour l'inspection. Si vous la décochez, seules les informations d'événement seront envoyées vers centre de gestion, mais les données de paquets ne sont pas envoyées.

- j) Cliquez sur **Register** (Inscrire).

Le centre de gestion identifie et enregistre l'unité de contrôle, puis enregistre toutes les unités de données. Si l'unité de contrôle ne s'enregistre pas avec succès, la grappe n'est pas ajoutée. Un échec de l'enregistrement peut se produire si la grappe n'était pas opérationnelle ou en raison d'autres problèmes de connectivité. Dans ce cas, nous vous recommandons d'essayer d'ajouter à nouveau l'unité de grappe.

Le nom de la grappe s'affiche sur la page **Devices (Périphériques) > Device Management** (gestion des périphériques); développez la grappe pour voir les unités de la grappe.

**Illustration 16 : Gestion des grappes**

IP Address	Role	Version	Status	Policies
172.16.0.50 (Control) 172.16.0.50 - Routed	FTDv for VMware	7.2.0	Manage	Base, Threat (2 more...) Default AC Policy
172.16.0.51 (Snort 3) 172.16.0.51 - Routed	FTDv for VMware	7.2.0	N/A	Base, Threat (2 more...) Default AC Policy

Une unité en cours d'enregistrement affiche l'icône de chargement.

**Illustration 17 : Inscription des nœuds**

IP Address	Role	Status
172.16.0.50 (Control) 172.16.0.50 - Routed	Snort 3	Success
172.16.0.51 172.16.0.51 - Routed	Snort 3	Loading

Vous pouvez surveiller l'enregistrement des unités de grappe en cliquant sur l'icône **Notifications** et en sélectionnant **Tasks** (Tâches). Le centre de gestion met à jour la tâche d'enregistrement de grappe à chaque enregistrement d'unité. Si des unités ne s'enregistrent pas, voir [Rapprocher les nœuds de la grappe](#), à la page 62.

Task ID	Description	Completion Time
10.10.1.12	Deployment to device successful.	1m 54s
10.10.1.13	Deployment to device successful.	1m 3s
TD_Cluster	Deployment to device successful.	35s

**Étape 2** Configurez les paramètres spécifiques au périphérique en cliquant sur le **Edit** (✎) de la grappe.

La majeure partie de la configuration peut être appliquée à la grappe dans son ensemble, et non aux nœuds de la grappe. Par exemple, vous pouvez modifier le nom d'affichage par nœud, mais vous ne pouvez configurer que des interfaces pour l'ensemble de la grappe.

**Étape 3** Sur l'écran **Devices (Périphériques) > Device Management (Gestion des périphériques) > Cluster (Grappe)**, vous voyez les paramètres **General** (Général), **License** (Licence), **System** (système), et **Health** (Intégrité).

TD Native Cluster  
Cisco Firepower Threat Defense for VMware

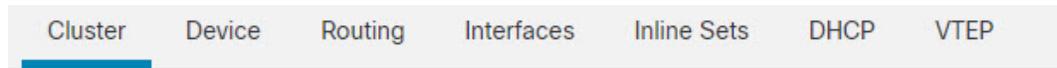
Cluster | **Device** | Routing | Interfaces | Inline Sets | DHCP | VTEP

10.10.1.13  
10.10.1.13

General [Edit] System [Edit]

Consultez les éléments suivants, propres à la grappe :

- **General > Name** (Général > Nom) : modifiez le nom d'affichage de la grappe en cliquant sur le **Edit** (✎).



General
✎

Name: <span style="color: blue;">?</span>	TD_Cluster
Transfer Packets:	Yes
Status:	<span style="color: green;">✔</span>
Control:	10.10.1.13
Cluster Live Status:	<a href="#">View</a>

Définissez ensuite le champ **Name** (Nom).

General
?

---

Name:

Transfer Packets:

Compliance Mode:

Performance Profile:

TLS Crypto Acceleration:

Force Deploy: →

- **General > Cluster Live Status**(Général > État de la grappe en direct) : cliquez sur le lien **View** (afficher) pour ouvrir la boîte de dialogue **Cluster Status** (état de la grappe).

Cluster    Device    Routing    Interfaces    Inline Sets    DHCP    VTEP

---

**General** 

Name:  TD Native Cluster

Transfer Packets: Yes

Status: 

Control: 10.10.1.13

Cluster Live Status: 

La boîte de dialogue **Cluster Status** (état de la grappe) vous permet également de réessayer l'enregistrement de l'unité de données en cliquant sur **Reconcile** (Rapprocher).

Cluster Status 

---

Overall Status:  Cluster has all nodes in sync

Nodes details (1)  

Status	Device Name	Unit Name	Chassis URL	
> In Sync.	10.10.1.13 	10.10.1.13	N/A	

---

Dated: 11:22:40 | 30 Aug 2022 

- **License** (Licence) : cliquez sur **Edit**  pour définir les droits de licence.

**Étape 4**

Sur la page **Devices (Périphériques) > Device Management (Gestion des périphériques) > Devices (Périphériques)**, vous pouvez choisir chaque membre de la grappe dans le menu déroulant supérieur droit et configurer les paramètres suivants.

- **General > Name** (Général > Nom) : modifiez le nom d'affichage du membre de la grappe en cliquant sur le **Edit** (✎).

General	
Name:	10.89.5.21
Transfer Packets:	Yes
Mode:	routed
Compliance Mode:	None
TLS Crypto Acceleration:	Enabled

Définissez ensuite le champ **Name** (Nom).

General ?

---

Name:

Transfer Packets:

Mode: routed

Compliance Mode: None

Performance Profile: Default

TLS Crypto Acceleration: Disabled

Force Deploy: →

- **Management > Host** (Gestion > Hôte) : si vous modifiez l'adresse IP de gestion dans la configuration du périphérique, votre modification doit correspondre à la nouvelle adresse dans centre de gestion pour qu'elle puisse atteindre le périphérique sur le réseau; Modifiez l'adresse de l' **hôte** dans la zone **Management** (Gestion).

Management	
Host:	10.89.5.20
Status:	✓

# Configurer les paramètres de surveillance de l'intégrité de la grappe

La section **Paramètres du moniteur d'intégrité de la grappe** de la page **Cluster** (Grappe) affiche les paramètres décrits dans le tableau ci-dessous.

*Illustration 18 : Paramètres de surveillance de l'intégrité de la grappe*

Cluster Health Monitor Settings			
<b>Timeouts</b>			
Hold Time			3 s
Interface Debounce Time			9000 ms
<b>Monitored Interfaces</b>			
Service Application			Enabled
Unmonitored Interfaces			None
<b>Auto-Rejoin Settings</b>			
	Attempts	Interval Between Attempts	Interval Variation
Cluster Interface	-1	5	1
Data Interface	3	5	2
System	3	5	2

*Tableau 5 : Champs de la table Paramètres de surveillance de l'intégrité de la grappe*

Champ	Description
<b>Délai d'expiration</b>	
Temps de retenue	Pour déterminer l'état de santé du système, les nœuds de la grappe envoient aux autres nœuds des messages de pulsation sur la liaison de commande de la grappe. Si un nœud ne reçoit aucun message de pulsation d'un nœud homologue au cours de la période de rétention, le nœud homologue est considéré comme ne répondant pas ou comme étant inactif.
Délai de l'antirebond de l'interface	L'heure de l'antirebond de l'interface est le délai avant que le nœud considère une interface comme défaillante et que le nœud ne soit retiré de la grappe.
<b>Interfaces surveillées</b>	La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe.
Application de service	Indique si Snort et les processus de disque plein sont surveillés.

Champ	Description
Interfaces non surveillées	Affiche les interfaces non surveillées.
<b>Paramètres de la jonction automatique</b>	
Interface de la grappe	Affiche les paramètres de jonction automatique en cas d'échec de la liaison de commande de grappe.
Interfaces de données	Affiche les paramètres de jonction automatique en cas de défaillance de l'interface de données.
Système	Affiche les paramètres de jonction automatique pour les erreurs internes. Les défaillances internes comprennent : des états d'applications non uniformes; et ainsi de suite.



**Remarque** Si vous désactivez la vérification de l'intégrité du système, les champs qui ne s'appliquent pas lorsque la vérification de l'intégrité du système est désactivée ne s'afficheront pas.

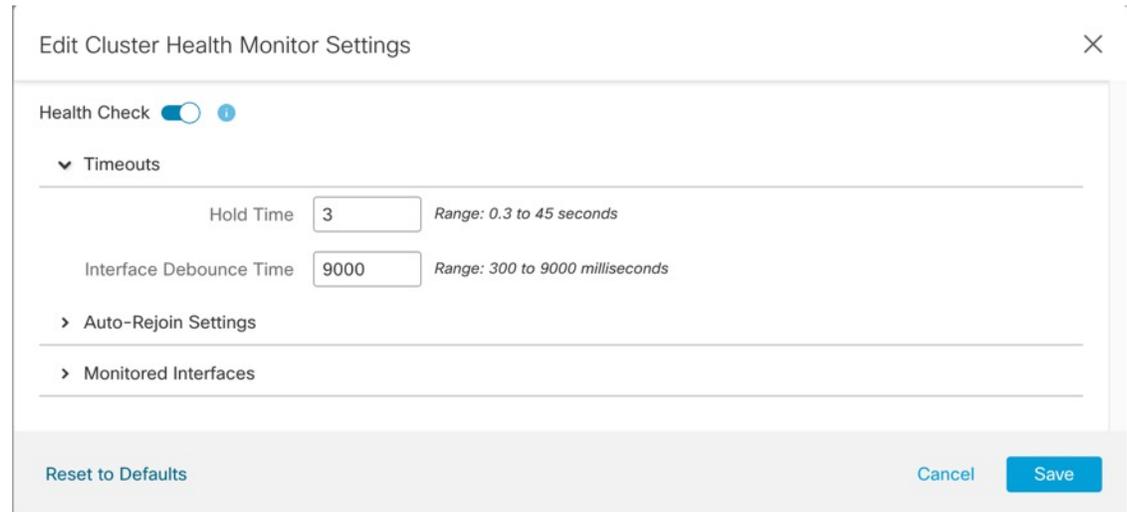
Vous pouvez utiliser ces paramètres dans cette section.

Vous pouvez surveiller n'importe quel ID de canal de port, tout ID d'interface physique unique, ainsi que les processus Snort et de disque plein. La surveillance de l'intégrité n'est pas effectuée sur les sous-interfaces VLAN ou les interfaces virtuelles telles que les VNI ou les BVI. Vous ne pouvez pas configurer la surveillance pour la liaison de commande de grappe; elle est toujours surveillée.

### Procédure

- Étape 1** Choisissez **Devices (appareils) > Device Management (gestion des appareils)**.
- Étape 2** À côté de la grappe que vous souhaitez modifier, cliquez sur **Edit** (✎).  
Dans un déploiement multidomaine, si vous n'êtes pas dans un domaine enfant, le système vous invite à basculer.
- Étape 3** Cliquez sur **Cluster** (Grappe).
- Étape 4** Dans la section **Cluster Health Monitor Settings** (paramètres de surveillance d'intégrité de la grappe), cliquez sur **Edit** (✎).
- Étape 5** Désactivez la fonction de vérification de l'intégrité du système en cliquant sur le curseur **Vérification de l'intégrité**.

Illustration 19 : Désactiver la vérification de l'intégrité du système



Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

### Étape 6

Configurez le temps d'attente et le temps d'antirebond de l'interface.

- **Hold Time** (Temps d'attente) : permet de définir le délai d'attente pour déterminer l'intervalle de temps entre les messages d'état de pulsation du nœud, entre 0,3 et 45 secondes; La valeur par défaut est de 3 secondes.
- **Interface Debounce Time** (Temps d'antirebond de l'interface) : définit le temps d'antirebond entre 300 et 9000 ms. La valeur par défaut est 500ms. Des valeurs inférieures permettent une détection plus rapide des défaillances d'interface. Notez que la configuration d'un délai antirebond inférieur augmente les risques de faux positifs. Lorsqu'une mise à jour d'état d'interface se produit, le nœud attend le nombre de millisecondes spécifié avant de marquer l'interface comme en échec, et le nœud est supprimé de la grappe. Dans le cas d'un EtherChannel qui passe de l'état inactif à un état opérationnel (par exemple, le commutateur a rechargé ou le commutateur a activé un EtherChannel), un temps d'antirebond plus long peut empêcher l'interface de sembler être défaillante sur un nœud de la grappe juste, car un autre nœud de la grappe a été plus rapide à regrouper les ports.

### Étape 7

Personnalisez les paramètres de grappe de la jonction automatique après l'échec de la vérification de l'intégrité.

Illustration 20 : Configurer les paramètres de jonction automatique

▼ Auto-Rejoin Settings

---

Cluster Interface

Attempts  Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts  Range: 2-60 minutes between rejoin attempts

Interval Variation  Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

Data Interface

Attempts  Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts  Range: 2-60 minutes between rejoin attempts

Interval Variation  Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

System

Attempts  Range: 0-65535 (-1 for unlimited number of attempts)

Interval Between Attempts  Range: 2-60 minutes between rejoin attempts

Interval Variation  Range: 1-3. Defines if the interval duration increases. 1 (no change); 2 (2 x the previous duration), or 3 (3 x the previous duration).

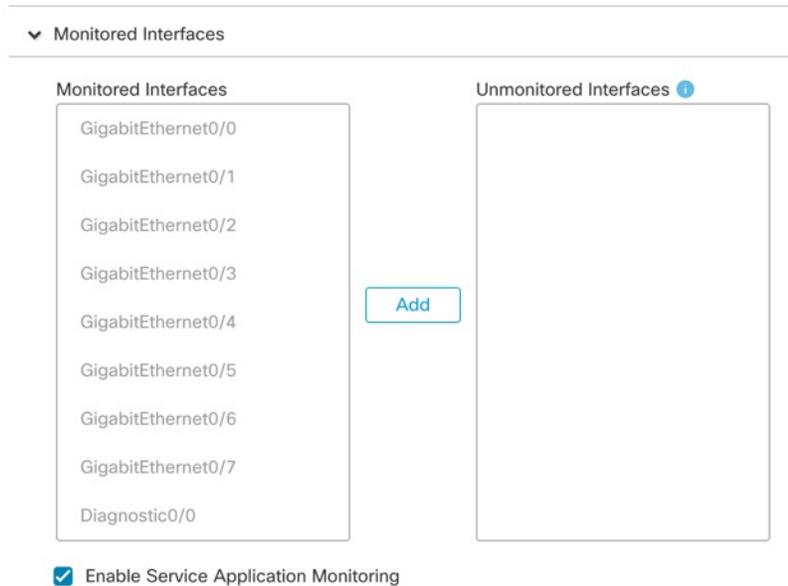
Définissez les valeurs suivantes pour l'**interface de grappe**, l'**interface de données** et le **système** (les défaillances internes comprennent : l'expiration du délai de synchronisation des applications, des états d'applications incohérents, etc.) :

- **Tentatives** – Définit le nombre de tentatives de jonction, entre -1 et 65 535. **0** désactive la jonction automatique. La valeur par défaut pour l' **interface de la grappe** est -1 (illimité). La valeur par défaut pour l'**interface de données** et le **système** est 3.
- **Interval Between Attempts** (intervalle entre les tentatives) : Permet de définir la durée de l'intervalle en minutes entre les tentatives de jonction en sélectionnant un intervalle entre 2 et 60. La valeur par défaut est 5 minutes. Le temps total maximum pendant lequel le nœud tente de rejoindre la grappe est limité à 14400 minutes (10 jours) à partir du moment de la dernière défaillance.
- **Interval Variation** (Variation de l'intervalle) : définit si la durée de l'intervalle augmente. définissez la valeur entre 1 et 3 : **1** (pas de changement); **2** (2 x la durée précédente), ou **3** (3 x la durée précédente). Par exemple, si vous définissez la durée de l'intervalle à 5 minutes et la variation à 2, la première tentative survient après 5 minutes; la deuxième tentative, après 10 minutes (2 x 5); la troisième tentative, après 20 minutes (2 x 10), etc. La valeur par défaut est **1** pour l' **interface de grappe** et **2** pour l' **interface de données** et le **système**.

**Étape 8**

Configurez les interfaces surveillées en les déplaçant dans la fenêtre **Interfaces surveillées** ou **interfaces non surveillées**. Vous pouvez également cocher ou décocher la case **Enable Service Application Monitoring** (activer la surveillance des applications de service) pour activer ou désactiver la surveillance Snort et des processus de surveillance de disque plein.

Illustration 21 : configurer les interfaces surveillées



La vérification de l'intégrité de l'interface surveille les défaillances de liaison. Si tous les ports physiques d'une interface logique donnée tombent en panne sur un nœud particulier, mais qu'il y a des ports actifs sous la même interface logique sur d'autres nœuds, le nœud est supprimé de la grappe. Le délai avant que le nœud ne supprime un membre de la grappe dépend du type d'interface et du fait que le nœud soit établi ou en voie de se joindre à la grappe. Le contrôle de l'intégrité est activé par défaut pour toutes les interfaces et pour les processus Snort et de détection du disque plein.

Vous pouvez souhaiter désactiver la surveillance de l'état des interfaces non essentielles, par exemple l'interface de diagnostic.

Lorsque des modifications de topologie surviennent (par exemple, ajout ou suppression d'une interface de données, activation ou désactivation d'une interface sur le nœud ou le commutateur, ajout d'un commutateur supplémentaire pour former un VSS ou un vPC), vous devez désactiver le contrôle d'intégrité et désactiver la surveillance d'interface pour les interfaces désactivées. Lorsque la modification de la topologie est terminée et que la modification de la configuration est synchronisée avec tous les nœuds, vous pouvez réactiver la fonction de contrôle d'intégrité du système et les interfaces surveillées.

**Étape 9** Cliquez sur **Save** (enregistrer).

**Étape 10** Déployer les changements de configuration.

## Gérer les nœuds de la grappe

## Désactiver la mise en grappe

Vous pouvez désactiver un nœud en préparation de sa suppression, ou temporairement pour la maintenance. Cette procédure vise à désactiver temporairement un nœud; le nœud continuera de s'afficher dans la liste des périphériques centre de gestion. Lorsqu'un nœud devient inactif, toutes les interfaces de données sont fermées.



**Remarque** Ne mettez pas le nœud hors tension sans avoir d'abord désactivé la mise en grappe.

### Procédure

- Étape 1** Pour l'unité que vous souhaitez désactiver, choisissez **Devices > Device Management** (Périphériques > Gestion des périphériques), cliquez sur **Plus** (⋮) et sélectionnez **Disable Node Clustering** (désactiver le regroupement de nœuds).
- Étape 2** Confirmez que vous souhaitez désactiver la mise en grappe sur le nœud.  
Le nœud affichera (**Désactivé**) à côté de son nom dans la liste **Device > Management** (gestion des périphériques).
- Étape 3** Pour réactiver la mise en grappe, consultez [Rejoindre la grappe, à la page 62](#).

## Rejoindre la grappe

Si un nœud a été supprimé de la grappe, par exemple pour une interface défectueuse ou si vous avez désactivé manuellement la mise en grappe, vous devez rejoindre manuellement la grappe. Assurez-vous que le problème est résolu avant d'essayer de rejoindre la grappe.

### Procédure

- Étape 1** Pour l'unité que vous souhaitez réactiver, sélectionnez **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮) et choisissez **Enable Node Clustering** (activer la mise en grappe de nœuds).
- Étape 2** Confirmez que vous souhaitez activer la mise en grappe sur le nœud.

## Rapprocher les nœuds de la grappe

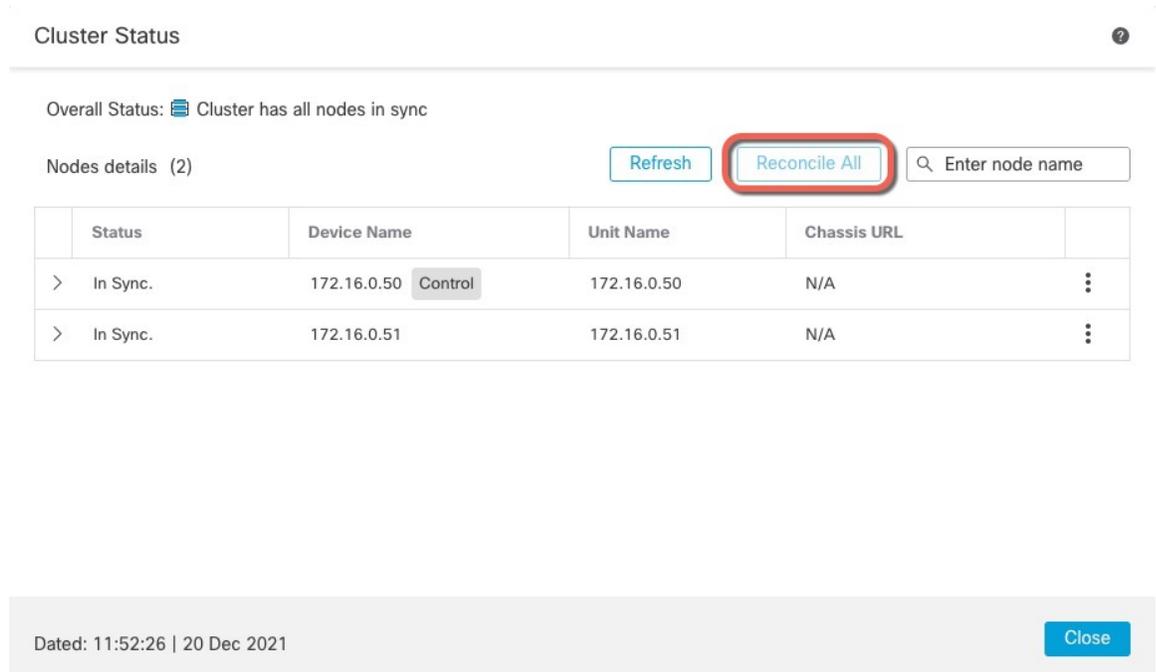
Si un nœud de grappe ne s'enregistre pas, vous pouvez rapprocher les membres de la grappe du périphérique avec centre de gestion. Par exemple, un nœud de données peut ne pas s'enregistrer si centre de gestion est occupé par certains processus ou en cas de problème de réseau.

## Procédure

**Étape 1** Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques) > Plus (+)** pour la grappe, puis choisissez **Cluster Live Status (État en direct de la grappe)** pour ouvrir la boîte de dialogue **Cluster Status (État de la grappe)**.

**Étape 2** Cliquez sur **Reconcile All (Tout faire concorder)**.

*Illustration 22 : Tout faire concorder*



Pour plus d'informations sur l'état de la grappe, consultez [Surveillance de la grappe, à la page 64](#).

## Supprimer la grappe ou les nœuds et enregistrer dans un nouveau Centre de gestion

Vous pouvez annuler l'enregistrement de la grappe à partir de centre de gestion, ce qui conserve la grappe inchangée. Vous souhaitez peut-être annuler l'enregistrement de la grappe si vous souhaitez l'ajouter à un nouveau centre de gestion.

Vous pouvez également désinscrire un nœud du centre de gestion sans le dissocier de la grappe. Bien que le nœud ne soit pas visible dans le centre de gestion, il fait tout de même partie de la grappe et continuera de transmettre le trafic et pourrait même devenir le nœud de contrôle. Vous ne pouvez pas annuler l'enregistrement du nœud de contrôle actuel. Il se peut que vous souhaitiez désenregistrer le nœud s'il n'est plus accessible depuis le centre de gestion, mais que vous souhaitiez le conserver dans la grappe pendant que vous dépannez la connectivité de gestion.

Désinscription d'une grappe :

- Rompt toutes les communications entre le centre de gestion et la grappe.
- Supprime la grappe de la page **Device Management** (gestion des périphériques).
- Renvoie la grappe à la gestion locale de l'heure si la politique de paramétrage de la plateforme de la grappe est configurée pour recevoir l'heure à partir du centre de gestion utilisent le protocole NTP.
- Laisse la configuration telle quelle, de sorte que la grappe continue de traiter le trafic.

Les politiques, telles que la NAT et le VPN, les listes de contrôle d'accès et les configurations d'interface, demeurent inchangées.

Si vous enregistrez de nouveau la grappe sur le même centre de gestion, ou sur un autre fichier, la configuration sera supprimée, de sorte que la grappe cessera de traiter le trafic à ce moment-là; la configuration de la grappe demeure inchangée, vous pouvez donc ajouter la grappe dans son ensemble. Vous pouvez choisir une politique de contrôle d'accès lors de l'inscription, mais vous devrez réappliquer les autres politiques après l'inscription, puis déployer la configuration avant de traiter à nouveau le trafic.

### Avant de commencer

Cette procédure nécessite un accès de l'interface de ligne de commande à l'un des nœuds.

### Procédure

- 
- Étape 1** Choisissez **Devices (Périphériques) > Device Management (Gestion des périphériques)**, cliquez sur **Plus** (⋮) pour la grappe ou le nœud, et choisissez **Delete**(annuler l'enregistrement).
- Étape 2** Vous êtes invité à l'enregistrement et à supprimer la grappe ou le nœud; cliquez sur **Yes**(oui).
- Étape 3** Vous pouvez enregistrer la grappe sur un nouveau (ou le même) centre de gestion en ajoutant l'un des membres de la grappe en tant que nouveau périphérique.
- Il vous suffit d'ajouter un des nœuds de la grappe en tant que périphérique et les autres nœuds de la grappe seront détectés.
- Étape 4** Pour rajouter un nœud supprimé, consultez [Rapprocher les nœuds de la grappe](#), à la page 62.
- 

## Surveillance de la grappe

Vous pouvez surveiller la grappe dans centre de gestion et l'interface de ligne de commande défense contre les menaces .

- Boîte de dialogue **Cluster Status** (État de la grappe) accessible à partir de l'icône **Devices > Device Management (Gestion des périphériques) > Plus** (⋮) ou de la page **Devices > Device Management > Cluster**, zone **> Générale > lien Cluster Live Status** (État de la grappe en direct).

**Illustration 23 : État de la grappe (cluster)**

Cluster Status ?

---

Overall Status:  Cluster has all nodes in sync

Nodes details (2)

	Status	Device Name	Unit Name	Chassis URL	
>	In Sync.	172.16.0.50 <span style="background-color: #ccc; padding: 2px;">Control</span>	172.16.0.50	N/A	⋮
>	In Sync.	172.16.0.51	172.16.0.51	N/A	⋮

Dated: 11:52:26 | 20 Dec 2021

Le nœud de contrôle est doté d'un indicateur graphique identifiant son rôle.

Les **états** des membres de la grappe comprennent les états suivants :

- En synchronisation : le nœud est enregistré auprès de centre de gestion.
- En attente d'enregistrement : le nœud fait partie de la grappe, mais ne s'est pas encore enregistré auprès de centre de gestion. Si un nœud ne s'enregistre pas, vous pouvez réessayer l'enregistrement en cliquant sur **Reconcile All** (Rapprocher tout).
- La mise en grappe est désactivée : le nœud est enregistré auprès de centre de gestion, mais est un membre inactif de la grappe. La configuration de la mise en grappe reste inchangée si vous avez l'intention de la réactiver ultérieurement, ou vous pouvez supprimer le nœud de la grappe.
- Grappe en cours de jonction... : le nœud se joint à la grappe sur le châssis, mais n'a pas terminé la jonction. Après s'être joint, elle s'enregistrera auprès de centre de gestion.

Pour chaque nœud, vous pouvez afficher le **résumé** ou l'**historique**.

Illustration 24 : Résumé du nœud

Status	Device Name	Unit Name	Chassis URL
In Sync.	172.16.0.50 <b>Control</b>	172.16.0.50	N/A

Summary
History

ID:	0	CCL IP:	10.10.10.1
Site ID:	N/A	CCL MAC:	6c13.d509.4d9a
Serial No:	FJZ2512139M	Module:	N/A
Last join:	05:41:26 UTC Dec 17 2021	Resource:	N/A
Last leave:	N/A		

Illustration 25 : Historique du nœud

Status	Device Name	Unit Name	Chassis URL
In Sync.	172.16.0.50 <b>Control</b>	172.16.0.50	N/A

Summary
History

Timestamp	From State	To State	Event
05:56:31 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment hold for app 1 is relea...
05:56:31 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment hold for app 1 is relea...
05:56:29 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment is on hold for app 1 fo...
05:56:29 UTC Dec 17 2021	MASTER	MASTER	Event: Cluster new slave enrollment is on hold for app 1 fo...

- **System** (⚙️) > page **Tâches** (Tâches).

La page **Tasks** (Tâches) affiche les mises à jour de la tâche d'enregistrement de la grappe à chaque fois que chaque nœud s'enregistre.

- **Devices (Périphériques)** > **Device Management (Gestion des périphériques)** > *cluster\_name* (Nom de la grappe).

Lorsque vous développez la grappe sur la page de liste des périphériques, vous pouvez voir tous les nœuds membres, y compris le nœud de contrôle affiché avec son rôle à côté de l'adresse IP. L'icône de chargement s'affiche pour les nœuds en cours d'enregistrement.

- **show cluster** {*access-list* [*acl\_name*] | *conn* [*count*] | *cpu* [*usage*] | *history* | *interface-mode* | *memory* | *resource usage* | *service-policy* | *traffic* | *xlate count*}

Pour afficher les données agrégées pour l'ensemble de la grappe ou d'autres informations, utilisez la commande **show cluster**.

- **show cluster info** [*auto-join* | *clients* | *conn-distribution* | *flow-mobility counters* | *goid* [*options*] | *health* | *incompatible-config* | *loadbalance* | *old-members* | *packet-distribution* | *trace* [*options*] | *transport* { *asp* | *cp*}]

Pour afficher les informations sur la grappe, utilisez la commande **show cluster info**.

# Tableau de bord de surveillance de l'intégrité de la grappe

## Moniteur d'intégrité de la grappe

Lorsque défense contre les menaces est le nœud de contrôle d'une grappe, centre de gestion recueille régulièrement diverses métriques à partir du collecteur de données des métriques du périphérique. Le moniteur d'intégrité de la grappe comprend les composants suivants :

- Tableau de bord de présentation : affiche des informations sur la topologie de la grappe, les statistiques de la grappe et les tableaux de mesures :
  - La section de topologie affiche l'état actuel d'une grappe, l'intégrité de la défense contre les menaces individuelles, le type de nœud de défense contre les menaces (nœud de contrôle ou nœud de données) et l'état du périphérique. L'état du périphérique peut être *Désactivé* (lorsque le périphérique quitte la grappe), *Ajouté prêt à l'emploi* (dans une grappe de nuage public, les nœuds supplémentaires qui n'appartiennent pas à centre de gestion) ou *Normal* (état idéal du nœud) .
  - La section des statistiques de la grappe affiche les métriques actuelles de la grappe en ce qui concerne l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.



**Remarque**

Les mesures de CPU et de mémoire affichent la moyenne individuelle de l'utilisation du plan de données et Snort.

- Les tableaux de mesures, à savoir l'utilisation de la CPU, l'utilisation de la mémoire, le débit et les connexions, affichent sous forme de diagramme les statistiques de la grappe sur la période de temps spécifiée.
- Tableau de bord de répartition de la charge : affiche la répartition de la charge sur les nœuds de la grappe dans deux gadgets :
  - Le gadget Distribution affiche la distribution moyenne des paquets et de la connexion sur la plage temporelle sur les nœuds de la grappe. Ces données décrivent comment la charge est répartie par les nœuds. Ce gadget vous permet de repérer facilement toute anomalie dans la répartition de la charge et d'y remédier.
  - Le gadget Statistiques de nœud affiche les mesures au niveau du nœud sous forme de tableau. Il affiche des données de métriques sur l'utilisation du processeur, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions de NAT sur les nœuds de la grappe. Cette vue du tableau vous permet de corréler les données et d'identifier facilement les écarts.
- Tableau de bord des performances des membres : affiche les mesures actuelles des nœuds de la grappe. Vous pouvez utiliser le sélecteur pour filtrer les nœuds et afficher les détails d'un nœud en particulier. Les données de la métrique comprennent l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, les connexions actives et les traductions NAT.
- Tableau de bord CCL : affiche sous forme graphique les données de liaison de commande de grappe, à savoir le débit d'entrée et de sortie.
- Dépannage et liens : contient des liens pratiques vers des rubriques et des procédures de dépannage fréquemment utilisées.

- Plage de temps : une fenêtre temporelle réglable permet de limiter les informations qui s'affichent dans les divers tableaux de bord et gadgets de métriques de grappe.
- Tableau de bord personnalisé : affiche des données sur les mesures à l'échelle de la grappe et au niveau des nœuds. Cependant, la sélection du nœud s'applique uniquement aux mesures de défense contre les menaces et non à l'ensemble de la grappe à laquelle le nœud appartient.

## Affichage de l'intégrité de la grappe

Vous devez être un utilisateur administrateur, de maintenance ou analyste de sécurité pour effectuer cette procédure.

Le moniteur d'intégrité de grappe fournit une vue détaillée de l'état d'intégrité d'une grappe et de ses nœuds. Ce moniteur d'intégrité de grappe fournit l'état d'intégrité et les tendances de la grappe dans un tableau de bord.

### Avant de commencer

- Assurez-vous d'avoir créé une grappe à partir d'un ou de plusieurs périphériques du centre de gestion.

### Procédure

**Étape 1** Choisissez **System** (⚙) > **Moniteur** > **d'intégrité**.

Utilisez le volet de navigation Monitoring (surveillance) pour accéder aux moniteurs d'intégrité spécifiques au nœud.

**Étape 2** Dans la liste des périphériques, cliquez sur **Développer** (>) et **Réduire** (∨) pour développer ou réduire la liste des périphériques de grappe gérés.

**Étape 3** Pour afficher les statistiques d'intégrité de la grappe, cliquez sur le nom de la grappe. Le moniteur de grappe signale par défaut les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis. Les tableaux de bord des mesures comprennent :

- **Présentation** : met en évidence les mesures clés d'autres tableaux de bord prédéfinis, y compris les nœuds, le processeur, la mémoire, les débits d'entrée et de sortie, les statistiques de connexion et les informations de traduction NAT.
- **Répartition de la charge** : répartition du trafic et des paquets sur les nœuds de la grappe.
- **Rendement des membres** : statistiques au niveau du nœud sur l'utilisation de la CPU, l'utilisation de la mémoire, le débit d'entrée, le débit de sortie, la connexion active et la traduction NAT.
- **CCL** : État de l'interface et statistiques de trafic agrégé.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Pour obtenir une liste complète des mesures de grappe prises en charge, consultez les [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#).

**Étape 4** Vous pouvez configurer la plage temporelle à partir de la liste déroulante dans le coin supérieur droit. La plage de temporelle peut refléter une période aussi courte que la dernière heure (par défaut) ou aussi longue que deux semaines. Sélectionnez **Custom** (Personnalisé) dans la liste déroulante pour configurer des dates de début et de fin personnalisées.

Cliquez sur l'icône d'actualisation pour définir l'actualisation automatique à 5 minutes ou pour la désactiver.

**Étape 5** Cliquez sur l'icône de déploiement pour une superposition de déploiement sur le graphique de tendance, par rapport à la plage temporelle sélectionnée.

L'icône de déploiement indique le nombre de déploiements au cours de la plage temporelle sélectionnée. Une bande verticale indique les heures de début et de fin de déploiement. Pour les déploiements multiples, plusieurs bandes/lignes s'affichent. Cliquez sur l'icône en haut de la ligne en pointillé pour afficher les détails du déploiement.

**Étape 6** (Pour la surveillance de l'intégrité spécifique au nœud) Affichez les **alertes d'intégrité** du nœud dans la notification d'alerte en haut de la page, directement à droite du nom du périphérique.

Passer votre pointeur sur les **alertes d'intégrité** pour afficher le résumé de l'intégrité du nœud. La fenêtre contextuelle affiche un résumé tronqué des cinq principales alertes d'intégrité. Cliquez sur dans la fenêtre contextuelle pour ouvrir une vue détaillée du résumé de l'alerte d'intégrité.

**Étape 7** (Pour le moniteur d'intégrité propre à un nœud) Le moniteur de périphérique signale les mesures d'intégrité et de performance dans plusieurs tableaux de bord prédéfinis par défaut. Les tableaux de bord des mesures comprennent :

- Aperçu : met en évidence les mesures clés des autres tableaux de bord prédéfinis, y compris les statistiques du processeur, de la mémoire, des interfaces et de la connexion; ainsi que l'utilisation du disque et des informations sur les processus critiques.
- CPU : utilisation de la CPU, y compris l'utilisation de la CPU par processus et par cœurs physiques.
- Mémoire : utilisation de la mémoire du périphérique, y compris l'utilisation du plan de données et de la mémoire Snort.
- Interfaces : état de l'interface et statistiques de trafic agrégées.
- Connexions : statistiques de connexion (comme les flux d'éléphants, les connexions actives, les connexions de pointe, etc.) et le nombre de traductions NAT.
- Snort : Statistiques liées au processus Snort.
- Abandons ASP : Statistiques sur les paquets abandonnés pour diverses raisons.

Vous pouvez naviguer dans les différents tableaux de bord des mesures en cliquant sur les étiquettes. Reportez-vous à la section [Indicateurs d'intégrité de Cisco Secure Firewall Threat Defense](#) pour obtenir une liste complète des indicateurs pris en charge.

**Étape 8** Cliquez sur le signe plus (+) dans le coin supérieur droit du moniteur d'intégrité pour créer un tableau de bord personnalisé en concevant votre propre ensemble de variables à partir des groupes de mesures disponibles.

Pour le tableau de bord à l'échelle de la grappe, choisissez Groupe de mesures de la grappe, puis choisissez la métrique.

## Mesures de la grappe

Le moniteur d'intégrité des grappes suit les statistiques liées à une grappe et à ses nœuds, ainsi que les statistiques agrégées de la répartition de la charge, des performances et du trafic CCL.

Tableau 6 : Mesures de la grappe

Unité	Description	Format
UC	Moyenne des mesures de CPU sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Mémoire	Moyenne des mesures de mémoire sur les nœuds d'une grappe (individuellement pour le plan de données et Snort).	pourcentage
Débit de données	Statistiques de trafic de données entrant et sortant pour une grappe.	octets
Débit du CCL	Statistiques de trafic CCL entrant et sortant pour une grappe.	octets
Connexions	Nombre de connexions actives dans une grappe.	number
Traductions NAT	Nombre de traductions NAT pour une grappe.	number
Distribution	Nombre de distributions de connexion dans la grappe à chaque seconde.	number
Paquets	Nombre de distributions de paquets dans la grappe à chaque seconde.	number

## Mise à niveau de la grappe

Effectuez les étapes suivantes pour mettre à niveau une grappe défense contre les menaces virtuelles :

### Procédure

- 
- Étape 1** Téléversez la version de l'image cible sur le stockage d'image en nuage.
- Étape 2** Mettez à jour le modèle d'instance de nuage de la grappe avec la version de l'image cible mise à jour.
- Créez une copie du modèle d'instance avec la version de l'image cible.
  - Associez le modèle nouvellement créé au groupe d'instances de la grappe.
- Étape 3** Téléversez le paquet de mise à niveau de la version de l'image cible dans centre de gestion.
- Étape 4** Effectuez la vérification de la disponibilité sur la grappe que vous souhaitez mettre à niveau.
- Étape 5** Une fois la vérification de l'état de préparation réussie, lancez l'installation du paquet de mise à niveau.
- Étape 6** Le centre de gestion met à niveau les nœuds de la grappe un à la fois.
- Étape 7** Le centre de gestion affiche une notification après la mise à niveau réussie de la grappe.
- Il n'y a aucun changement dans le numéro de série et l'UUID de l'instance après la mise à niveau.

- Remarque**
- Si vous lancez la mise à niveau de la grappe à partir du centre de gestion, assurez-vous qu'aucun périphérique virtuel de défense contre les menaces n'est accidentellement arrêté ou remplacé par le groupe auto Scaling au cours du processus de redémarrage après la mise à niveau. Pour éviter cela, accédez à la console AWS, cliquez sur **Auto scaling group-gt; Advanced configurations** et suspendez les processus - Health Check and Replace UnHealthy. Une fois la mise à niveau terminée, accédez de nouveau à **Advanced configuration** (configurations avancées) et supprimez tous les processus interrompus pour détecter les instances non intègres.
  - Si vous mettez à niveau une grappe déployée sur AWS d'une version majeure à une version de correctif, puis que vous faites évoluer la grappe, les nouveaux nœuds produiront la version principale au lieu de la version de correctif. Vous devez ensuite mettre à niveau manuellement chaque nœud vers la version du correctif à partir du centre de gestion.

Vous pouvez également créer une Amazon Machine Image (AMI) à partir d'un instantané d'une instance virtuelle autonome de défense contre les menaces sur laquelle le correctif a été appliqué et qui n'a pas de configuration de jour 0. Utilisez cette AMI dans le modèle de déploiement en grappe. Tous les nouveaux nœuds qui se présenteront lorsque vous augmenterez la grappe auront la version du correctif.

## Référence pour la mise en grappe

Cette section comprend des renseignements supplémentaires sur le fonctionnement de la mise en grappe.

### Fonctionnalités de défense contre les menaces et mise en grappe

Certaines fonctions défense contre les menaces ne sont pas prises en charge avec la mise en grappe et d'autres le sont uniquement sur l'unité de contrôle. Pour une utilisation correcte, d'autres fonctionnalités peuvent comporter des mises en garde.

### Fonctionnalités et mise en grappe non prises en charge

Ces fonctionnalités ne peuvent pas être configurées lorsque la mise en grappe est activée, et les commandes seront rejetées.



**Remarque** Pour afficher les fonctionnalités FlexConfig qui ne sont pas non plus prises en charge avec la mise en grappe, par exemple l'inspection WCCP, consultez le [guide de configuration des opérations générales ASA](#). FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir [Politiques FlexConfig](#).

- VPN d'accès à distance (VPN SSL et VPN IPsec)
- Client DHCP, serveur et serveur mandataire. Le relais DHCP est pris en charge.
- Interfaces de tunnel virtuel (VTI)
- Haute disponibilité

- Routage et pont intégrés
- Mode FMC UCAPL/CC

## Fonctionnalités centralisées pour la mise en grappe

Les fonctionnalités suivantes ne sont prises en charge que sur le nœud de contrôle et ne sont pas adaptées à la grappe.



### Remarque

Le trafic pour les fonctionnalités centralisées est acheminé des nœuds membres vers le nœud de contrôle par la liaison de commande de grappe.

Si vous utilisez la fonctionnalité de rééquilibrage, le trafic des fonctionnalités centralisées peut être rééquilibré vers des nœuds sans contrôle avant que le trafic ne soit classé comme fonctionnalité centralisée. Si cela se produit, le trafic est renvoyé au nœud de contrôle.

Pour les fonctionnalités centralisées, si le nœud de contrôle tombe en panne, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.



### Remarque

Pour afficher les fonctionnalités FlexConfig qui sont également centralisées avec la mise en grappe, par exemple l'inspection RADIUS, consultez le [guide de configuration des opérations générales ASA](#). FlexConfig vous permet de configurer de nombreuses fonctionnalités ASA qui ne sont pas présentes dans l'interface graphique centre de gestion. Voir [Politiques FlexConfig](#).

- Les inspections d'application suivantes :
  - DCERPC
  - ESMTTP
  - NetBIOS
  - PPTP
  - RSH
  - SQLNET
  - SunRPC
  - TFTP
  - XDMCP
- Surveillance du routage statique

## Cisco Trustsec et mise en grappe

Seul le nœud de contrôle reçoit les informations des balises de groupe de sécurité (SGT). Le nœud de contrôle remplit ensuite la balise SGT pour les nœuds de données, et les nœuds de données peuvent prendre une décision de correspondance pour la balise SGT en fonction de la politique de sécurité.

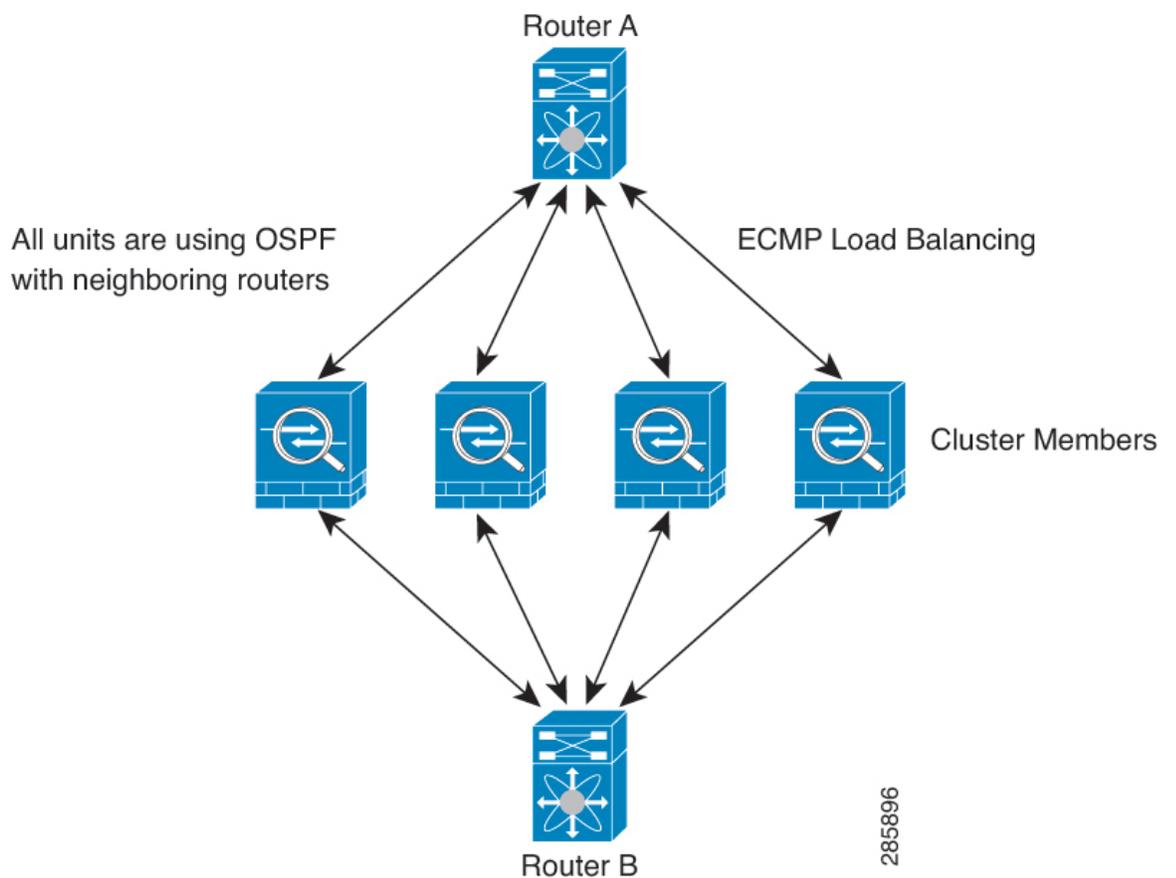
## Paramètres de connexion et mise en grappe

Les limites de connexion s'appliquent à l'ensemble de la grappe. Chaque nœud dispose d'une estimation des valeurs de compteur à l'échelle de la grappe en fonction des messages de diffusion. Pour des raisons d'efficacité, la limite de connexion configurée dans la grappe pourrait ne pas être appliquée exactement au nombre limite. Chaque nœud peut surévaluer ou sous-évaluer la valeur du compteur à l'échelle de la grappe à tout moment. Cependant, les informations seront mises à jour au fil du temps dans une grappe à charge équilibrée.

## Routage et mise en grappe dynamiques

En mode d'interface individuel, chaque nœud exécute le protocole de routage en tant que routeur autonome, et les routes sont apprises par chaque nœud indépendamment.

*Illustration 26 : Routage dynamique en mode d'interface individuelle*



Dans le diagramme ci-dessus, le routeur A détecte qu'il existe quatre chemins à coûts égaux vers le routeur B, chacun passant par un nœud. ECMP est utilisé pour équilibrer la charge du trafic entre les quatre chemins. Chaque nœud choisit un ID de routeur différent lorsqu'il communique avec des routeurs externes.

Vous devez configurer un groupement de grappes pour l'ID de routeur afin que chaque nœud ait un ID de routeur distinct.

## FTP et mise en grappe

- Si le canal de données et les flux du canal de contrôle FTP appartiennent à différents membres de la grappe, le propriétaire du canal de données enverra périodiquement des mises à jour du délai d'inactivité au propriétaire du canal de contrôle et mettra à jour la valeur du délai d'inactivité. Cependant, si le propriétaire du flux de contrôle est rechargé et que le flux de contrôle est réhébergé, la relation de flux parent/enfant ne sera plus maintenue; le délai d'inactivité du flux de contrôle ne sera pas mis à jour.

## NAT et mise en grappe

Pour l'utilisation de la NAT, consultez les limites suivantes.

La NAT peut affecter le débit global de la grappe. Les paquets NAT entrants et sortants peuvent être envoyés à différents défense contre les menaces dans la grappe, car l'algorithme d'équilibrage de charge repose sur les adresses IP et les ports, et la NAT fait en sorte que les paquets entrants et sortants aient des adresses IP ou des ports différents. Lorsqu'un paquet arrive à défense contre les menaces qui n'est pas le propriétaire NAT, il est transféré sur la liaison de commande de grappe vers le propriétaire, ce qui entraîne un trafic important sur la liaison de commande de grappe. Notez que le nœud de réception ne crée pas de flux de transfert vers le propriétaire, car le propriétaire de la NAT peut ne pas créer de connexion pour le paquet en fonction des résultats des vérifications de sécurité et des politiques.

Si vous souhaitez toujours utiliser la NAT en grappe, tenez compte des directives suivantes :

- No Proxy ARP (Pas de serveur mandataire ARP) : Pour les interfaces individuelles, une réponse de serveur mandataire ARP n'est jamais envoyée pour les adresses mappées. Cela empêche le routeur adjacent de maintenir une relation d'homologue avec un ASA qui ne fait plus partie de la grappe. Le routeur en amont a besoin d'une route statique ou d'un PBR avec suivi d'objets pour les adresses mappées qui pointe vers l'adresse IP de la grappe principale.
- PAT avec attribution de bloc de ports : Consultez les consignes suivantes pour cette fonctionnalité :
  - La limite maximale par hôte n'est pas une limite à l'échelle de la grappe et s'applique à chaque nœud individuellement. Ainsi, dans une grappe à 3 nœuds avec la limite maximale par hôte configurée à 1, si le trafic d'un hôte est équilibré en charge sur les 3 nœuds, 3 blocs avec 1 dans chaque nœud peuvent lui être alloués.
  - Les blocs de ports créés sur le nœud de sauvegarde à partir des pools de sauvegarde ne sont pas pris en compte lors de l'application de la limite maximale par hôte.
  - Les modifications des règles PAT à la volée, où l'ensemble PAT est modifié avec une toute nouvelle plage d'adresses IP, entraînera des échecs de création de sauvegarde xlate pour les demandes de sauvegarde xlate qui étaient encore en transit lorsque le nouveau ensemble est entré en vigueur. Ce comportement n'est pas spécifique à la fonctionnalité d'attribution de bloc de ports et il s'agit d'un problème transitoire d'ensemble PAT que l'on observe uniquement dans les déploiements en grappe où l'ensemble est distribué et le trafic est équilibré en charge sur les nœuds de la grappe.
  - Lorsque vous utilisez une grappe, vous ne pouvez pas simplement modifier la taille de l'allocation de bloc. La nouvelle taille n'est en vigueur qu'après le rechargement de chaque périphérique de la grappe. Pour éviter d'avoir à téléverser chaque périphérique, nous vous recommandons de supprimer toutes les règles d'attribution de blocage et d'effacer tous les xlates associés à ces règles. Vous pouvez ensuite modifier la taille du bloc et recréer les règles d'attribution des blocs.
- Distribution des adresses de l'ensemble NAT pour la PAT dynamique : lorsque vous configurez un ensemble PAT, le cluster divise chaque adresse IP de l'ensemble en blocs de ports. Par défaut, chaque

bloc comporte 512 ports, mais si vous configurez des règles d'attribution de bloc de ports, votre paramètre de blocage est utilisé à la place. Ces blocs sont répartis uniformément entre les nœuds de la grappe, de sorte que chaque nœud ait un ou plusieurs blocs pour chaque adresse IP dans l'ensemble PAT. Ainsi, vous pourriez avoir aussi peu qu'une adresse IP dans un ensemble PAT pour une grappe, si cela est suffisant pour le nombre de connexions PAT que vous attendez. Les blocs de ports couvrent la plage de ports 1 024 à 65535, sauf si vous configurez l'option pour inclure les ports réservés, 1 à 1023, dans la règle NAT de l'ensemble PAT.

- Reusing a PAT pool in multiple Rules (réutiliser un pool PAT dans plusieurs règles) : Pour utiliser le même pool PAT dans plusieurs règles, vous devez faire attention à la sélection d'interface dans les règles. Vous devez soit utiliser des interfaces spécifiques dans toutes les règles, soit utiliser « any » dans toutes les règles. Vous ne pouvez pas combiner des interfaces spécifiques et « any » dans les règles, sans quoi le système pourrait ne pas être en mesure de faire correspondre le trafic de retour vers le bon nœud dans la grappe. L'option la plus fiable est l'utilisation d'ensembles de PAT uniques par règle.
- Pas de tourniquet (Round robin) : le tourniquet pour un ensemble PAT n'est pas pris en charge avec la mise en grappe.
- Pas de PAT étendue : la PAT étendue n'est pas prise en charge avec la mise en grappe.
- Tableaux xlates dynamiques de NAT gérés par le nœud de contrôle : Le nœud de contrôle conserve et reproduit le tableau xlate sur les nœuds de données. Lorsqu'un nœud de données reçoit une connexion qui nécessite une NAT dynamique et que le xlate n'est pas dans le tableau, il le demande au nœud de contrôle. Le nœud de données est propriétaire de la connexion.
- Disques xlates périmés : le temps d'inactivité xlate sur le propriétaire de la connexion n'est pas mis à jour. Ainsi, le temps d'inactivité peut dépasser le délai d'inactivité. Une valeur de minuteur d'inactivité supérieure au délai d'expiration configuré avec un contrôle de référence de 0 est une indication d'un xlate périmé.
- Pas de PAT statique pour les inspections suivantes :
  - FTP
  - RSH
  - SQLNET
  - TFTP
  - XDMCP
  - SIP
- Si vous avez un nombre extrêmement important de règles NAT, plus de dix mille, vous devez activer le modèle de validation transactionnelle à l'aide de la commande **asp rule-engine transactional-commit nat** dans l'interface de ligne de commande du périphérique. Sinon, le nœud pourrait ne pas être en mesure de rejoindre la grappe.

## Inspection SIP et mise en grappes

Un flux de contrôle peut être créé sur n'importe quel nœud (en raison de l'équilibrage de la charge); ses flux de données enfants doivent résider sur le même nœud.

## SNMP et mise en grappe

Un agent SNMP interroge chaque défense contre les menaces en fonction de l'adresse IP locale de son interface Diagnostic. Vous ne pouvez pas interroger les données consolidées de la grappe.

Vous devez toujours utiliser l'adresse locale, et non l'adresse IP de la grappe principale pour l'interrogation SNMP. Si l'agent SNMP interroge l'adresse IP de la grappe principale, si un nouveau nœud de contrôle est choisi, l'interrogation du nouveau nœud de contrôle échouera.

Lorsque vous utilisez SNMPv3 avec la mise en grappe et que vous ajoutez un nouveau nœud de grappe après la formation initiale de la grappe, les utilisateurs SNMPv3 ne seront pas répliqués sur le nouveau nœud. Vous devez supprimer les utilisateurs, les rajouter, puis redéployer votre configuration pour forcer les utilisateurs à se reproduire sur le nouveau nœud.

## Syslog et mise en grappe

- Chaque nœud de la grappe génère ses propres messages syslog. Vous pouvez configurer la journalisation de sorte que chaque nœud utilise le même ID d'appareil ou un ID d'appareil différent dans le champ d'en-tête du message syslog. Par exemple, la configuration du nom d'hôte est répliquée et partagée par tous les nœuds de la grappe. Si vous configurez la journalisation pour utiliser le nom d'hôte comme ID d'appareil, les messages syslog générés par tous les nœuds semblent provenir d'un seul nœud. Si vous configurez la journalisation pour utiliser le nom de nœud local attribué dans la configuration de démarrage de la grappe comme ID d'appareil, les messages du journal système semblent provenir de nœuds différents.

## VPN et mise en grappe

Le VPN de site à site est une fonctionnalité centralisée; seul le nœud de contrôle prend en charge les connexions VPN.



**Remarque** L'accès VPN à distance n'est pas pris en charge avec la mise en grappe.

La fonctionnalité VPN est limitée au nœud de contrôle et ne tire pas parti des capacités de haute disponibilité de la grappe. Si le nœud de contrôle tombe en panne, toutes les connexions VPN existantes sont perdues, et les utilisateurs de VPN verront une perturbation de service. Lorsqu'un nouveau nœud de contrôle est choisi, vous devez rétablir les connexions VPN.

Pour les connexions à une interface individuelle lors de l'utilisation de PBR ou d'ECMP, vous devez toujours vous connecter à l'adresse IP de la grappe principale, et non à une adresse locale.

Les clés et les certificats liés au VPN sont répliqués sur tous les nœuds.

## Facteur d'évolutivité de rendement

Lorsque vous combinez plusieurs unités dans une grappe, vous pouvez vous attendre à ce que les performances totales de la grappe atteignent environ 80 % du débit combiné maximal.

Par exemple, si votre modèle peut gérer environ 10 Gbit/s de trafic lorsqu'il est exécuté seul, pour une grappe de 8 unités, le débit combiné maximal sera d'environ 80 % de 80 Gbit/s (8 unités x 10 Gbit/s) : 64 Gbit/s.

## Choix du nœud de contrôle

Les nœuds de la grappe communiquent sur la liaison de commande de grappe pour élire un nœud de contrôle comme suit :

1. Lorsque vous activez la mise en grappe pour un nœud (ou lorsqu'il démarre avec la mise en grappe déjà activée), il diffuse une demande de sélection toutes les 3 secondes.
2. Tous les autres nœuds ayant une priorité plus élevée répondent à la demande de sélection; la priorité est réglée entre 1 et 100, 1 étant la priorité la plus élevée.
3. Si, après 45 secondes, un nœud ne reçoit pas de réponse d'un autre nœud de priorité plus élevée, il devient le nœud de contrôle.



### Remarque

Si plusieurs nœuds sont à égalité pour la priorité la plus élevée, le nom du nœud de la grappe, suivi du numéro de série, est utilisé pour déterminer le nœud de contrôle.

4. Si un nœud se joint ultérieurement à la grappe avec une priorité plus élevée, il ne devient pas automatiquement le nœud de contrôle; le nœud de contrôle existant demeure toujours le nœud de contrôle, sauf s'il s'arrête de répondre, moment auquel un nouveau nœud de contrôle est sélectionné.
5. Dans un scénario de « discernement partagé », où il y a temporairement plusieurs nœuds de contrôle, le nœud ayant la priorité la plus élevée conserve le rôle tandis que les autres nœuds retournent aux rôles de nœud de données.



### Remarque

Vous pouvez forcer manuellement un nœud à devenir le nœud de contrôle. Pour les fonctionnalités centralisées, si vous forcez un changement de nœud de contrôle, toutes les connexions sont abandonnées et vous devez rétablir les connexions sur le nouveau nœud de contrôle.

## Haute disponibilité au sein de la grappe

La mise en grappe assure une disponibilité élevée en surveillant l'intégrité des nœuds et de l'interface et en reproduisant les états de la connexion entre les nœuds.

### Surveillance de l'intégrité du nœud

Chaque nœud envoie périodiquement un paquet de diffusion heartbeat sur la liaison de commande de grappe. Si le nœud de contrôle ne reçoit aucun paquet heartbeat ou autre paquet d'un nœud de données au cours du délai d'expiration configurable, le nœud de contrôle supprime le nœud de données de la grappe. Si les nœuds de données ne reçoivent pas de paquets du nœud de contrôle, un nouveau nœud de contrôle est élu parmi les nœuds restants.

Si les nœuds ne peuvent pas se joindre sur le lien de commande de grappe en raison d'une défaillance du réseau et non parce qu'un nœud est réellement défaillant, la grappe peut entrer dans un scénario de « scission du cœur » où les nœuds de données isolés éliront leurs propres nœuds de contrôle. Par exemple, si un routeur tombe en panne entre deux emplacements de grappe, le nœud de contrôle d'origine à l'emplacement 1 supprimera les nœuds de données de l'emplacement 2 de la grappe. Pendant ce temps, les nœuds de l'emplacement 2 éliront leur propre nœud de contrôle et formeront leur propre grappe. Notez que le trafic

symétrique peut échouer dans ce scénario. Une fois la liaison de commande de grappe restauré, le nœud de contrôle qui a la priorité la plus élevée conservera le rôle de nœud de contrôle.

## Surveillance d'interfaces

Chaque nœud surveille l'état de la liaison de toutes les interfaces matérielles désignées utilisées et signale les modifications d'état au nœud de contrôle.

Toutes les interfaces physiques sont surveillées; seules les interfaces nommées peuvent être surveillées. Vous pouvez éventuellement désactiver la surveillance par interface.

Un nœud est supprimé de la grappe en cas de défaillance de ses interfaces surveillées. Le nœud est supprimé après 500 ms.

## État après l'échec

Si le nœud de contrôle échoue, un autre membre de la grappe ayant la priorité la plus élevée (numéro le plus bas) devient le nœud de contrôle.

défense contre les menaces tente automatiquement de rejoindre la grappe, en fonction de l'événement d'échec.



### Remarque

Lorsque défense contre les menaces devient inactif et ne parvient pas à rejoindre automatiquement la grappe, toutes les interfaces de données sont fermées; Seule l'interface de gestion/dépistage de gestion peut envoyer et recevoir du trafic.

## Rejoindre la grappe

Après le retrait d'un membre de la grappe, la façon dont il peut rejoindre la grappe dépend de la raison de sa suppression :

- Échec de la liaison de commande de grappe lors de la jonction : après avoir résolu le problème avec la liaison de commande de grappe, vous devez rejoindre manuellement la grappe en réactivant la mise en grappe.
- Échec de la liaison de commande de la grappe après avoir rejoint la grappe : FTD essaie automatiquement de la rejoindre toutes les 5 minutes, indéfiniment.
- Échec de l'interface de données : défense contre les menaces tente automatiquement de rejoindre à 5 minutes, puis à 10 minutes et enfin à 20 minutes. Si la jonction échoue après 20 minutes, l'application défense contre les menaces désactive la mise en grappe. Après avoir résolu le problème de l'interface de données, vous devez activer manuellement la mise en grappe.
- Nœud en échec : si le nœud a été supprimé de la grappe en raison d'un échec de vérification de l'intégrité du nœud, la jonction avec la grappe dépend de la source de la défaillance. Par exemple, une panne de courant temporaire signifie que le nœud rejoindra la grappe au redémarrage, à condition que le lien de commande de grappe soit actif. L'application défense contre les menaces tente de rejoindre la grappe toutes les 5 secondes.
- Erreur interne : les défaillances internes comprennent : le dépassement du délai de synchronisation de l'application, les statuts incohérents de l'application, etc.
- Échec du déploiement de la configuration : si vous déployez une nouvelle configuration à partir de FMC et que le déploiement échoue sur certains membres de la grappe mais réussit sur d'autres, les nœuds qui

ont échoué sont supprimés de la grappe. Vous devez rejoindre manuellement la grappe en réactivant la mise en grappe. Si le déploiement échoue sur le nœud de contrôle, le déploiement est annulé et aucun membre n'est supprimé. Si le déploiement échoue sur tous les nœuds de données, le déploiement est restauré et aucun membre n'est supprimé.

## Réplication de l'état de la connexion du chemin de données

Chaque connexion a un propriétaire et au moins un propriétaire secondaire dans la grappe. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec; au lieu de cela, il stocke les informations d'état TCP/UDP, de sorte que la connexion puisse être transférée de manière transparente à un nouveau propriétaire en cas de défaillance. Le propriétaire de la sauvegarde est généralement aussi le directeur.

Certains trafics nécessitent des informations d'état au-dessus de la couche TCP ou UDP. Consultez le tableau suivant pour connaître la prise en charge ou l'absence de prise en charge de ce type de trafic.

**Tableau 7 : Fonctionnalités répliquées dans la grappe**

Trafic	Soutien relatif à l'état	Notes
Temps de disponibilité	Oui	Assure le suivi de la disponibilité du système.
Table ARP	Oui	—
tableau d'adresses MAC	Oui	—
Identité de l'utilisateur	Oui	—
Base de données du voisin IPv6	Oui	—
Routage dynamique	Oui	—
ID du moteur SNMP	<b>Non</b>	—

## Gestion des connexions par la grappe

Les connexions peuvent être équilibrées vers plusieurs nœuds de la grappe. Les rôles de connexion déterminent la façon dont les connexions sont gérées, à la fois en fonctionnement normal et en situation de disponibilité élevée.

### Rôles de connexion

Consultez les rôles suivants, définis pour chaque connexion :

- Propriétaire : généralement, le nœud qui reçoit initialement la connexion. Le propriétaire gère l'état TCP et traite les paquets. Une connexion n'a qu'un seul propriétaire. Si le propriétaire d'origine échoue, lorsque les nouveaux nœuds reçoivent des paquets de la connexion, le directeur choisit un nouveau propriétaire dans ces nœuds.
- Propriétaire du sauvegarde : Nœud qui stocke les informations d'état TCP/UDP reçues du propriétaire, de sorte que la connexion puisse être transférée en toute transparence à un nouveau propriétaire en cas de défaillance. Le propriétaire de secours ne prend pas en charge la connexion en cas d'échec. Si le propriétaire devient indisponible, le premier nœud à recevoir les paquets de la connexion (selon

l'équilibrage de la charge) contacte le propriétaire de secours pour obtenir les informations d'état pertinentes, afin qu'il puisse devenir le nouveau propriétaire.

Tant que le directeur (voir ci-dessous) n'est pas le même nœud que le propriétaire, le directeur est également le propriétaire secondaire. Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

Pour la mise en grappe sur le périphérique Firepower 9300, qui peut inclure jusqu'à 3 nœuds de grappe dans un châssis, si le propriétaire de secours se trouve sur le même châssis que le propriétaire, un propriétaire de secours supplémentaire sera choisi dans un autre châssis pour protéger les flux d'une défaillance du châssis .

- **Directeur** : nœud qui gère les demandes de recherche de propriétaire provenant des transitaires. Lorsque le propriétaire reçoit une nouvelle connexion, il choisit un directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports (voir ci-dessous pour les détails du hachage ICMP) et envoie un message au directeur pour enregistrer la nouvelle connexion. Si les paquets arrivent à un nœud autre que le propriétaire, le nœud interroge le directeur sur quel nœud est le propriétaire afin qu'il puisse transférer les paquets. Une connexion n'a qu'un seul directeur. En cas de défaillance d'un directeur, le propriétaire en choisit un nouveau.

Tant que le directeur ne se trouve pas sur le même nœud que le propriétaire, le directeur est également le propriétaire suppléant (voir ci-dessus). Si le propriétaire se choisit lui-même directeur, un propriétaire de secours distinct est choisi.

Détails du hachage ICMP/ICMPv6 :

- Pour les paquets Echo, le port source correspond à l'identifiant ICMP et le port de destination est 0.
  - Pour les paquets de réponse, le port source est 0 et le port de destination est l'identifiant ICMP.
  - Pour les autres paquets, les ports source et de destination sont à 0.
- **Forwarder (transitaire)** : nœud qui transfère les paquets au propriétaire. Si un transitaire reçoit un paquet pour une connexion qu'il ne possède pas, il interroge le directeur à propos du propriétaire, puis établit un flux vers le propriétaire pour tout autre paquet qu'il reçoit pour cette connexion. Le directeur peut également être un transitaire. Notez que si un transitaire reçoit le paquet SYN-ACK, il peut en dériver le propriétaire directement d'un témoin SYN dans le paquet, donc il n'a pas besoin d'interroger le directeur. (Si vous désactivez la répartition aléatoire de la séquence TCP, le témoin SYN n'est pas utilisé; une requête au directeur est requise.) Pour les flux de courte durée tels que DNS et ICMP, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire. Une connexion peut avoir plusieurs redirecteurs; le débit le plus efficace est obtenu par une bonne méthode d'équilibrage de la charge où il n'y a pas de redirecteurs et où tous les paquets d'une connexion sont reçus par le propriétaire.




---

**Remarque** Nous vous déconseillons de désactiver la répartition aléatoire de la séquence TCP lors de l'utilisation de la mise en grappe. Il y a un faible risque que certaines sessions TCP ne soient pas établies, car le paquet SYN/ACK sera abandonné.

---

- **Propriétaire de fragment** : Pour les paquets fragmentés, les nœuds de la grappe qui reçoivent un fragment déterminent le propriétaire du fragment à l'aide d'un hachage de l'adresse IP source du fragment, de l'adresse IP de destination et de l'ID de paquet. Tous les fragments sont ensuite transférés au propriétaire du fragment sur la liaison de commande de grappe. Les fragments peuvent être équilibrés en charge vers

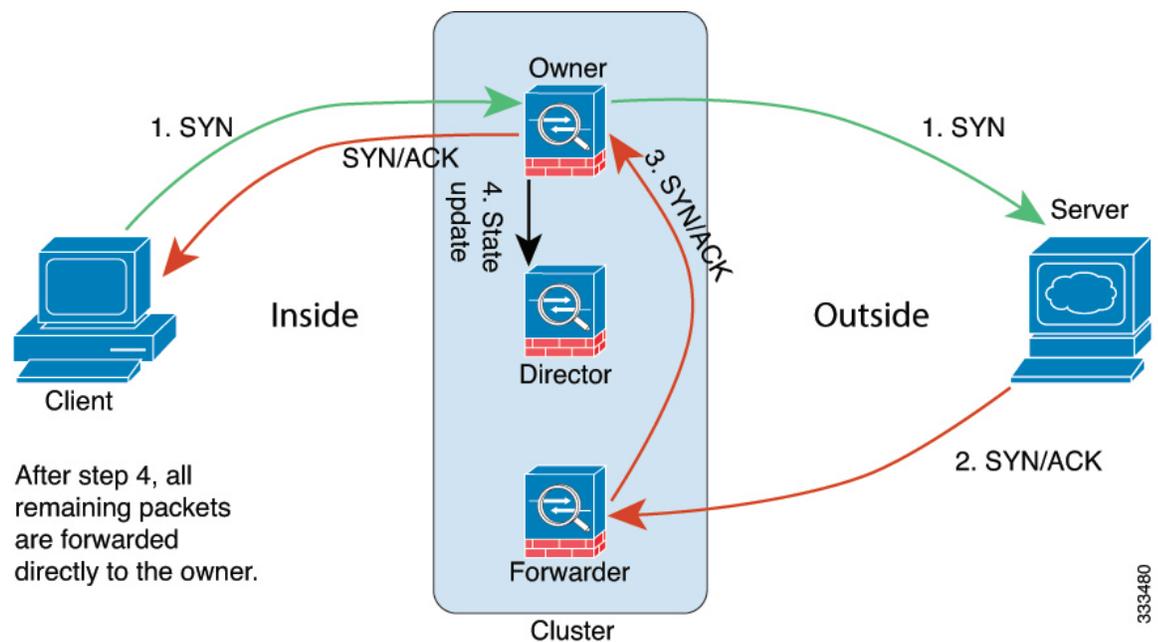
différents nœuds de grappe, car seul le premier fragment comprend le quintuple utilisé dans le hachage d'équilibrage de charge du commutateur. Les autres fragments ne contiennent pas les ports source et de destination et peuvent être répartis en charge vers d'autres nœuds de la grappe. Le propriétaire du fragment rassemble temporairement le paquet afin de pouvoir déterminer le directeur en fonction d'un hachage de l'adresse IP source/de destination et des ports. S'il s'agit d'une nouvelle connexion, le propriétaire du fragment s'enregistre en tant que propriétaire de la connexion. S'il s'agit d'une connexion existante, le propriétaire du fragment transfère tous les fragments au propriétaire de la connexion fourni par la liaison de commande de grappe. Le propriétaire de la connexion rassemblera ensuite tous les fragments.

## Nouvelle propriété de connexion

Lorsqu'une nouvelle connexion est acheminée vers un nœud de la grappe par l'équilibrage de la charge, ce nœud possède les deux sens de connexion. Si des paquets de connexion arrivent à un nœud différent, ils sont acheminés au nœud propriétaire sur la liaison de commande de grappe. Si un flux inverse arrive sur un autre nœud, il est redirigé vers le nœud d'origine.

## Exemple de flux de données pour TCP

L'exemple suivant montre l'établissement d'une nouvelle connexion.



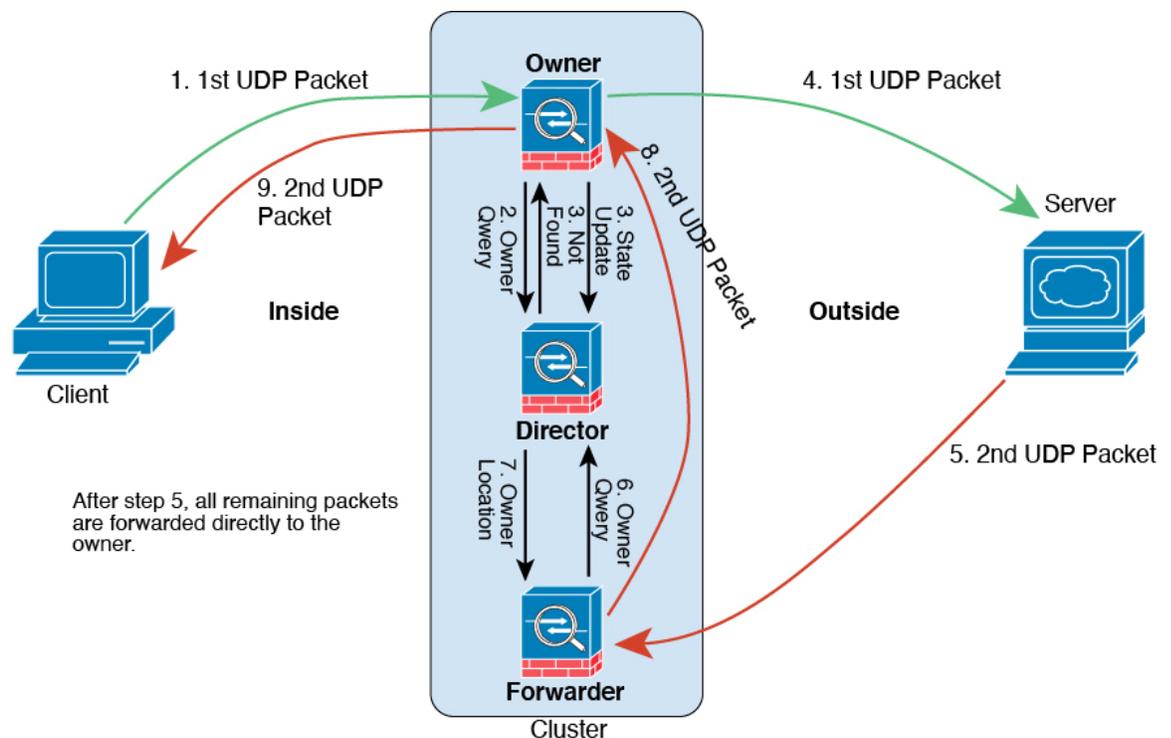
1. Le paquet SYN provient du client et est livré à un défense contre les menaces (selon la méthode d'équilibrage de la charge), qui devient le propriétaire. Le propriétaire crée un flux, code les renseignements sur le propriétaire dans un témoin SYN et transfère le paquet au serveur.
2. Le paquet SYN-ACK provient du serveur et est livré à un défense contre les menaces différent (selon la méthode d'équilibrage de la charge). Ce défense contre les menaces est le transitaire.
3. Comme le transitaire n'est pas propriétaire de la connexion, il decode les informations sur le propriétaire à partir du témoin SYN, crée un flux de transfert vers le propriétaire et transmet le SYN-ACK au propriétaire.
4. Le propriétaire envoie une mise à jour de l'état au directeur et transmet le SYN-ACK au client.

5. Le directeur reçoit la mise à jour d'état du propriétaire, crée un flux à destination du propriétaire et enregistre les informations d'état TCP ainsi que le propriétaire. Le directeur agit en tant que propriétaire secondaire pour la connexion.
6. Tous les paquets suivants livrés au transitaire seront transférés au propriétaire.
7. Si des paquets sont livrés à d'autres nœuds, il interrogera le directeur à propos du propriétaire et établira un flux.
8. Tout changement d'état du flux entraîne une mise à jour d'état du propriétaire au directeur.

## Exemple de flux de données pour ICMP et UDP

L'exemple suivant montre l'établissement d'une nouvelle connexion.

1. *Illustration 27 : Flux de données ICMP et UDP*



Le premier paquet UDP provient du client et est remis à un défenseur contre les menaces (selon la méthode d'équilibrage de la charge).

2. Le nœud qui a reçu le premier paquet interroge le nœud directeur qui est choisi en fonction d'un hachage de l'adresse IP et des ports source/de destination.
3. Le directeur ne trouve aucun flux existant, crée un flux de directeur et renvoie le paquet au nœud précédent. Autrement dit, le directeur a choisi un propriétaire pour ce flux.
4. Le propriétaire crée le flux, envoie une mise à jour d'état au directeur et transfère le paquet au serveur.
5. Le deuxième paquet UDP provient du serveur et est livré au redirecteur.

6. Le transitaire interroge le directeur pour fournir les renseignements sur la propriété. Pour les flux de courte durée tels que le DNS, au lieu d'interroger, le redirecteur envoie immédiatement le paquet au directeur, qui l'envoie ensuite au propriétaire.
7. Le directeur répond au transitaire avec les renseignements de propriété.
8. Le transitaire crée un flux de transfert pour enregistrer les informations sur le propriétaire et transfère le paquet au propriétaire.
9. Le propriétaire transfère le paquet au client.

## Historique des mises en grappe Threat Defense Virtual dans le nuage public

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
Paramètres de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	<p>Vous pouvez désormais modifier les paramètres de surveillance de l'intégrité de la grappe.</p> <p>Écrans nouveaux ou modifiés : <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Cluster (Grappe) &gt; Cluster Health Monitor Settings (Paramètres d'intégrité de la grappe)</b></p> <p><b>Remarque</b> Si vous avez déjà configuré ces paramètres à l'aide de FlexConfig, veuillez à supprimer la configuration FlexConfig avant de procéder au déploiement. Sinon, la configuration FlexConfig remplacera la configuration du centre de gestion.</p>
Tableau de bord de surveillance de l'intégrité de la grappe	20221213	N'importe lequel	<p>Vous pouvez maintenant afficher l'intégrité de la grappe sur le tableau de bord du moniteur d'intégrité des grappes.</p> <p>Écrans nouveaux ou modifiés : <b>System (⚙️) &gt; Moniteur &gt; d'intégrité</b></p>
Mise en grappe pour défense contre les menaces virtuelles dans Azure	20221213	7.3.0	<p>Vous pouvez désormais configurer la mise en grappe pour un maximum de 16 nœuds défense contre les menaces virtuelles dans Azure pour l'équilibreur de charge de passerelle Azure ou pour des équilibreurs de charge externes.</p> <p>Écrans nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Add Cluster (Ajouter une grappe)</b></li> <li>• <b>Périphériques &gt; Gestion des périphériques &gt; Plus</b></li> <li>• <b>Devices(Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Cluster (Grappe)</b></li> </ul> <p>Plateformes prises en charge : Défense contre les menaces virtuelles dans Azure</p>

Fonctionnalités	Centre de gestion Minimum	Défense contre les menaces Minimum	Détails
<p>Mise en grappe pour Défense contre les menaces virtuelles dans le nuage public (Amazon Web Services et Google Cloud Platform)</p>	<p>N'importe lequel</p>	<p>7.2.0</p>	<p>défense contre les menaces virtuelles prend en charge la mise en grappe d'interfaces individuelles pour un maximum de 16 nœuds dans le nuage public (AWS et GCP).</p> <p>Écrans Nouveaux ou modifiés :</p> <ul style="list-style-type: none"> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Add Device (Ajouter un périphérique)</b></li> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques), menu &gt; More (Plus)</b></li> <li>• <b>Devices (Périphériques) &gt; Device Management (Gestion des périphériques) &gt; Cluster (Grappe)</b></li> </ul> <p>Plateformes prises en charge : Défense contre les menaces virtuelles dans AWS et GCP</p>

## À propos de la traduction

Cisco peut fournir des traductions du présent contenu dans la langue locale pour certains endroits. Veuillez noter que des traductions sont fournies à titre informatif seulement et, en cas d'incohérence, la version anglaise du présent contenu prévaudra.