# Déployer l'ASA virtuel sur Google Cloud Platform

Vous pouvez déployer l'ASA virtuel sur Google Cloud Platform (GCP).



# Aperçu

GCP vous permet de créer, de déployer et de faire évoluer des applications, des sites Web et des services sur la même infrastructure que Google.

L'ASA virtuel exécute le même logiciel que les ASA physiques pour fournir des fonctionnalités de sécurité éprouvées dans un format virtuel. L'ASA virtuel peut être déployé dans le GCP public. Il peut ensuite être configuré pour protéger les charges de travail des centres de données virtuels et physiques qui se développent, se contractent ou changent d'emplacement au fil du temps.

### Prise en charge des types de machines GCP

Sélectionnez le type et la taille de machine virtuelle Google qui répondent à vos besoins ASA virtuel.

L'ASA virtuel prend en charge les types de machines GCP *à usage général N1, N2* et *C2 optimisées pour le calcul* :

***Tableau 1 : Types de machines optimisées pour le calcul prises en charge***

| Types de machines optimisées pour le calcul | Attributs | |
|---|---|---|
| | vCPU | Mémoire (Go) |
| c2-standard-4 | 4 | 16 |
| c2-standard-8 | 8 | 32 |
| c2-standard-16 | 16 | 64 |

*Tableau 2 : Types de machines générales prises en charge*

| Type de machine | Attributs | |
|---|---|---|
| | vCPU | Mémoire (Go) |
| n1-standard-4 | 4 | 15 |
| n1-standard-8 | 8 | 30 |
| n1-standard-16 | 16 | 60 |
| n2-standard-4 | 4 | 16 |
| n2-standard-8 | 8 | 32 |
| n2-standard-16 | 16 | 64 |
| n2-highmem-4 | 4 | 32 |
| n2-highmem-8 | 8 | 64 |

- L'ASA virtuel nécessite un minimum de 3 interfaces.
- Le maximum de vCPU pris en charge est de 16.
- Le type de machine à mémoire optimisée n'est pas pris en charge.

Vous créez un compte sur GCP, lancez une instance ASA virtuel à l'aide de l'offre du pare-feu virtuel ASA (ASA virtuel) sur le Marché GCP et choisissez un type de machine GCP.

### Limites du type de machine C2 optimisée pour le calcul

Les types de machines C2 optimisées pour le calcul ont les restrictions suivantes :

- Vous ne pouvez pas utiliser de disques persistants régionaux avec des types de machines optimisées pour le calcul. Pour en savoir plus, consultez la documentation de Google Ajout ou redimensionnement de disques persistants régionaux.
- Sous réserve de limites de disque différentes de celles des types de machines à usage général et à mémoire optimisée. Pour en savoir plus, consultez la documentation de Google Bloquer la performance du stockage.
- Disponible uniquement dans certaines zones et régions. Pour plus d'informations, consultez la documentation de Google Régions et zones disponibles.
- Disponible uniquement sur certaines plateformes CPU. Pour plus d'informations, consultez la documentation de Google Plateformes CPU.

### Niveaux de performance pour ASA virtuel

L'ASA virtuel prend en charge les licences par niveau de performance qui fournissent différents niveaux de débit et limites de connexion VPN en fonction des exigences de déploiement.

| Niveau de performance | Type d'instance (cœur/RAM) | Limite du débit | Limite de session RA VPN |
|---|---|---|---|
| ASAv5 | c2-standard-4<br>4 cœurs/16 Go | 100 Mbit/sec | 50 |
| ASAv10 | c2-standard-4<br>4 cœurs/16 Go | 1 Gbit/sec | 250 |
| ASAv30 | c2-standard-4<br>4 cœurs/16 Go | 2 Gbit/s | 750 |
| ASAv50 | c2-standard-8<br>8 cœurs/32 Go | 7,6 Gbit/s | 10 000 |
| ASAv100 | c2-standard-16<br>16 cœurs/64 Go | 16 Gbit/s | 20 000 |

# Prérequis

- Créez un compte GCP à l'adresse https://cloud.google.com.
- Créez votre projet GCP. Consultez la documentation de Google, Création de votre projet.
- Obtenez une licence pour l'ASA virtuel. Jusqu'à ce que vous obteniez une licence pour l'ASA virtuel, il fonctionnera en mode dégradé, ce qui n'autorisera que 100 connexions et un débit de 100 kbit/s. Consultez Licences : gestion des licences Smart Software.
- Exigences d'interface :
  - Interface de gestion : utilisée pour connecter l'ASA virtuel à ASDM; ne peut pas être utilisée pour le trafic traversant.
  - Interface interne : utilisée pour connecter l'ASA virtuel aux hôtes internes.
  - Interface externe : utilisée pour connecter l'ASA virtuel au réseau public.
- Chemins de communication :
  - Adresses IP publiques pour l'accès à l'ASA virtuel.
- Pour les exigences du système ASA virtuel, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

# Lignes directrices et limites relatives à la licence

### Fonctionnalités prises en charge

L'ASA virtuel sur GCP prend en charge les fonctionnalités suivantes :

- Déploiement dans le cloud privé virtuel (VPC) de GCP
- Maximum de 16 vCPU par instance
- Mode avec routeur (par défaut)
- Licences : Seul le protocole BYOL est pris en charge

### Fonctionnalités non prises en charge

L'ASA virtuel sur GCP ne prend pas en charge les éléments suivants :

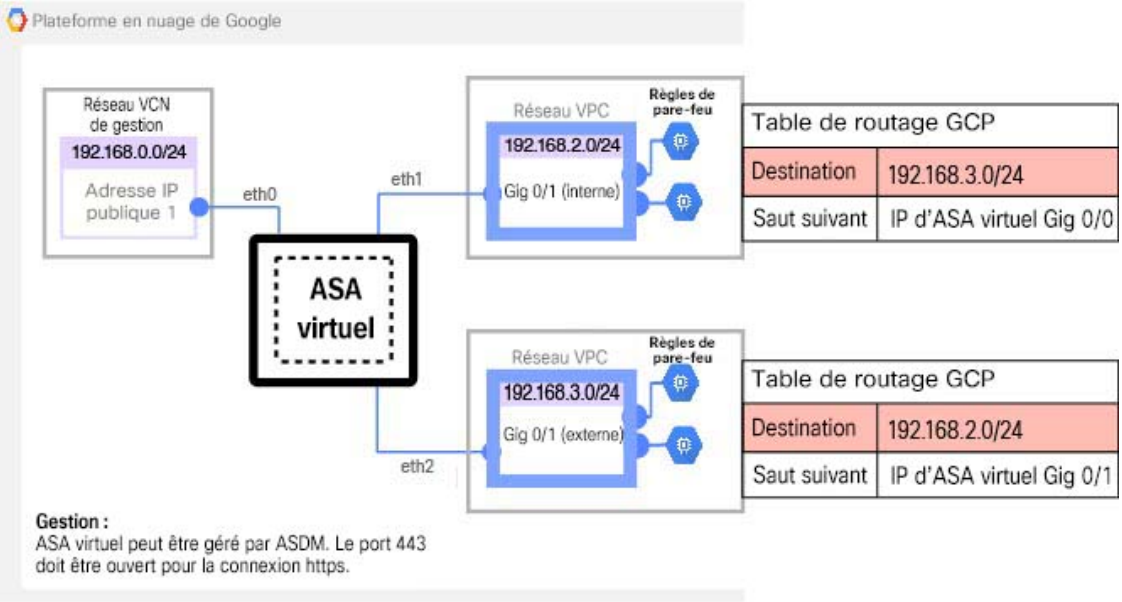
- IPv6
  - Le paramètre IPv6 au niveau de l'instance n'est pas pris en charge sur le GCP
  - Seul l'équilibreur de charges peut accepter les connexions IPv6 et les transmettre sur IPv4 aux instances de GCP
- Cadres jumbo
- Haute disponibilité en natif ASA virtuel
- Évolutivité automatique
- Modes transparent/en ligne/passif

# Exemple de topologie de réseau

La figure suivante montre la topologie de réseau recommandée pour l'ASA virtuel en mode pare-feu routé avec trois sous-réseaux configurés dans GCP pour l'ASA virtuel (gestion, interne et externe).

Déployer l'ASA virtuel sur Google Cloud Platform

*Illustration 1 : Exemple d'ASA virtuel sur le déploiement GCP*




# Déployer l'ASA virtuel sur Google Cloud Platform

Vous pouvez déployer l'ASA virtuel sur Google Cloud Platform (GCP).

## Créer des réseaux vPC

### Avant de commencer

Le déploiement de ASA virtuel nécessite trois réseaux que vous devez créer avant de déployer l'ASA virtuel. Les réseaux sont les suivants :

- VPC de gestion pour le sous-réseau de gestion.
- VPC interne pour le sous-réseau interne.
- VPC externe pour le sous-réseau externe.

En outre, vous configurez des tableaux de routage et des règles de pare-feu de GCP pour permettre au trafic de circuler dans l'ASA virtuel. Les tableaux de routage et les règles de pare-feu sont distincts de ceux configurés sur l'ASA virtuel lui-même. Nommez les tableaux de routage et les règles de pare-feu de GCP en fonction du réseau et des fonctionnalités associés. Consultez Exemple de topologie de réseau, à la page 4.

### Procédure

**Étape 1** Dans la console GCP, choisissez **Networking (réseautage)** > **VPC network (réseau VPC)** > **VPC networks (réseaux VPC)**, puis cliquez sur **Create VPC Network** (créer un réseau VPC).

**Étape 2** Dans le champ **Name** (nom), saisissez le nom descriptif de votre réseau VPC, par exemple, *vpc-asiasouth-mgmt*.

**Étape 3** Dans le **Subnet creation mode** (mode de création de sous-réseau), cliquez sur **Custom** (personnalisé).

**Étape 4** Dans le champ **Name** (nom) sous **New subnet** (nouveau sous-réseau), saisissez le nom souhaité, par xemple, *vpc-asiasouth-mgmt*.

**Étape 5** Dans la liste déroulante **Region** (région), sélectionnez la région appropriée pour votre déploiement. Les trois réseaux doivent se trouver dans la même région.

**Étape 6** Dans le champ **IP address range** (plage d'adresses IP), saisissez le sous-réseau du premier réseau au format CIDR, par exemple 10.10.0.0/24.

**Étape 7** Acceptez les valeurs par défaut de tous les autres paramètres, puis cliquez sur **Create** (Créer).

**Étape 8** Répétez les étapes 1 à 7 pour créer les deux autres réseaux VPC.

# Créer les règles de pare-feu

Vous appliquez les règles de pare-feu de l'interface de gestion (pour autoriser les connexions SSH et HTTPS) lors du déploiement de l'instance ASA virtuel, consultez Créer l'instance ASA virtuel sur GCP, à la page 6. Selon vos besoins, vous pouvez également créer des règles de pare-feu pour les interfaces interne et externe.

### Procédure

**Étape 1** Dans la console GCP, choisissez **Networking (réseautage)** > **VPC network (réseau VPC)** > **Firewall (pare-feu)**, puis cliquez sur **Create Firewall Rule** (créer une règle de pare-feu).

**Étape 2** Dans le champ **Name** (nom), saisissez un nom descriptif pour votre règle de pare-feu, par exemple, *vpc-asiasouth-inside-fwrule*.

**Étape 3** Dans la liste déroulante **Network** (réseau), sélectionnez le nom du réseau VPC pour lequel vous créez la règle de pare-feu, par exemple, *asav-south-inside*.

**Étape 4** Dans la liste déroulante **Targets** (cibles), sélectionnez l'option applicable à votre règle de pare-feu, par exemple, **All instances in the network** (toutes les instances du réseau).

**Étape 5** Dans le champ **Source IP ranges** (plages IP sources), saisissez les plages d'adresses IP sources au format CIDR, par exemple, 0.0.0.0/0.

Le trafic n'est autorisé que par des sources comprises dans ces plages d'adresses IP.

**Étape 6** Sous **Protocols and ports** (protocoles et ports), sélectionnez **Specified protocols and ports** (protocoles et ports spécifiés).

**Étape 7** Ajoutez vos règles de sécurité.

**Étape 8** Cliquez sur **Create** (créer).

# Créer l'instance ASA virtuel sur GCP

Effectuez les étapes suivantes pour déployer une instance ASA virtuel en utilisant l'offre de pare-feu virtuel Cisco ASA (ASA virtuel) du Marché GCP.

## Procédure

**Étape 1** Connectez-vous à la console GCP.

**Étape 2** Cliquez sur **Navigation menu (Menu de navigation)** > **Marketplace (Marché)**.

**Étape 3** Effectuez une recherche sur le Marché pour « Cisco ASA virtual firewall (ASAv) » (Pare-feu virtuel Cisco ASA (ASAv)) et choisissez l'offre.

**Étape 4** Cliquez sur **Launch** (Lancer).

**Étape 5** Ajoutez un **Deployment name** (Nom de déploiement) unique pour l'instance.

**Étape 6** Sélectionnez la **Zone** dans laquelle vous souhaitez déployer l'ASA virtuel.

**Étape 7** Sélectionnez le **Machine type** (Type de machine) approprié. Pour obtenir la liste des types de machines prises en charge, consultez Aperçu, à la page 1.

**Étape 8** (Facultatif) Collez la clé publique de la paire de clés SSH sous **SSH key (optional)** (Clé SSH (facultatif)).

La paire de clés se compose d'une clé publique que GCP stocke et d'un fichier de clé privée que l'utilisateur stocke. Ensemble, ils vous permettent de vous connecter à votre instance en toute sécurité. Assurez-vous d'enregistrer la paire de clés à un emplacement connu, car elle devra se connecter à l'instance.

**Étape 9** Choisissez d'autoriser ou de bloquer les clés SSH à l'échelle du projet pour l'accès à cette instance. Consultez la documentation de Google Autoriser ou bloquer les clés SSH publiques à l'échelle du projet à partir d'une instance Linux.

**Étape 10** (Facultatif) Sous **Startup script** (Script de démarrage), fournissez la configuration day0 (jour0) pour votre ASA virtuel. La configuration day0 (jour0) est appliquée lors du premier démarrage d'ASA virtuel.

L'exemple suivant montre une configuration day0 (jour0) que vous pouvez copier et coller dans le champ **Startup script** (Script de démarrage) :

Consultez les Guides de configuration ASA et la Référence sur les commandes ASA pour en savoir plus sur les commandes ASA.

**Important**
Lorsque vous copiez du texte à partir de cet exemple, vous devez valider le script dans un éditeur de texte ou un moteur de validation tiers pour éviter les erreurs de format et supprimer les caractères Unicode non valides.

```
!ASA Version 9.15.1

interface management0/0

management-only
nameif management
security-level 100
ip address dhcp setroute
no shut
!
same-security-traffic permit inter-interface
same-security-traffic permit intra-interface
!
crypto key generate rsa modulus 2048
ssh 0 0 management
ssh timeout 60
ssh version 2
username admin password cisco123 privilege 15
username admin attributes
```

```
service-type admin
! required config end
dns domain-lookup management
dns server-group DefaultDNS
name-server 8.8.8.8
```

**Étape 11** Conservez le **Boot disk type** (Type de disque de démarrage) par défaut et la **Boot disk size in GB** (Taille de disque de démarrage en Go) pour l'espace disque provisionné.

**Étape 12** Configurez les interfaces sous **Network interfaces** (Interfaces réseau).

- gestion
- interne
- externe

**Remarque**
Vous ne pouvez pas ajouter des interfaces à une instance après l'avoir créée. Si vous créez l'instance avec une configuration d'interface incorrecte, vous devez supprimer l'instance et la recréer avec la configuration d'interface appropriée.

a) Dans la liste déroulante **Network** (Réseau), sélectionnez un réseau VPC, par exemple, *vpc-asiasouth-mgmt*.
b) Dans la liste déroulante **External IP** (Adresse IP externe), sélectionnez l'option appropriée.

Pour l'interface de gestion, sélectionnez **External IP** (Adresse IP externe) à **Ephemeral** (Éphémère). Cette opération est facultative pour les interfaces interne et externe.

c) Cliquez sur **Done (Terminé)**.

**Étape 13** Appliquez les règles de pare-feu sous **Firewall** (Pare-feu).

- Cochez la case **Allow TCP port 22 traffic from the Internet (SSH access)** (Autoriser le trafic du port TCP 22 de l'Internet (accès SSH)) pour autoriser SSH.
- Cochez la case **Allow HTTPS traffic from the Internet (ASDM access)** (Autoriser le trafic HTTPS de l'Internet (accès ASDM)) pour autoriser les connexions HTTPS.

**Étape 14** Cliquez sur **More** (Plus) pour développer l'affichage et assurez-vous que **IP Forwarding** (Transfert IP) est défini sur **On** (Activé).

**Étape 15** Cliquez sur **Deploy** (Déployer).

Affichez les détails de l'instance dans la page d'instance de VM de la console GCP. Vous trouverez l'adresse IP interne, l'adresse IP externe et les contrôles pour arrêter et démarrer l'instance. Vous devez arrêter l'instance si vous devez la modifier.

# Accéder à l'instance ASA virtuel sur GCP

Assurez-vous d'avoir déjà activé une règle de pare-feu pour autoriser les connexions SSH (TCP par le port 22) pendant le déploiement. Consultez Créer l'instance ASA virtuel sur GCP, à la page 6 pour de plus amples renseignements.

Cette règle de pare-feu active l'accès à l'instance ASA virtuel et vous permet de vous connecter à l'instance en utilisant les méthodes suivantes.

- External IP (IP externe)
  - Tout autre outil client SSH ou tiers
- Console de série
- Ligne de commande Gcloud

Consultez la documentation de Google, Connexion aux instances pour en savoir plus.

**Remarque** Vous pouvez vous connecter à l'instance ASA virtuel en utilisant les renseignements d'authentification spécifiés dans la configuration day0 (jour0) ou en utilisant la paire de clés SSH que vous avez créée lors du lancement de l'instance.

# Se connecter à l'instance ASA virtuel à l'aide d'une adresse IP externe

L'instance ASA virtuel se voit attribuer une adresse IP interne et une adresse IP externe. Vous pouvez utiliser l'adresse IP externe pour accéder à l'instance ASA virtuel.

### Procédure

**Étape 1** Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

**Étape 2** Cliquez sur le nom de l'instance ASA virtuel pour ouvrir la page **VM instance details** (Détails de l'instance de VM).

**Étape 3** Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

**Étape 4** Sélectionnez l'option souhaitée dans le menu déroulant **SSH**.

Vous pouvez vous connecter à l'instance ASA virtuel en utilisant la méthode suivante.

- Tout autre outil client SSH ou tiers : consultez l'information sur la connexion à l'aide d'outils tiers de la documentation de Google pour en savoir plus.

**Remarque**
Vous pouvez vous connecter à l'instance ASA virtuel en utilisant les renseignements d'authentification spécifiés dans la configuration day0 (jour0) ou en utilisant la paire de clés SSH que vous avez créée lors du lancement de l'instance.

## Se connecter à l'instance ASA virtuel à l'aide de SSH

Pour vous connecter à l'instance ASA virtuel à partir d'un système de type Unix, connectez-vous à l'instance à l'aide de SSH.

**Procédure**

**Étape 1** Utilisez la commande suivante pour définir les autorisations de fichier afin que seul vous puissiez lire le fichier :

```
$ chmod 400 <private_key>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

**Étape 2** Utilisez la commande SSH suivante pour accéder à l'instance.

```
$ ssh –i <private_key> <username>@<public-ip-address>
```

Lieu :

`<private_key>` est le chemin d'accès complet et le nom du fichier qui contient la clé privée associée à l'instance à laquelle vous souhaitez accéder.

`<username>` correspond au nom d'utilisateur pour l'instance ASA virtuel.

`<public-ip-address>` correspond à l'adresse IP publique de votre instance que vous avez extraite de la console.

# Se connecter à l'instance ASA virtuel à l'aide de la console de série

**Procédure**

**Étape 1** Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

**Étape 2** Cliquez sur le nom de l'instance ASA virtuel pour ouvrir la page **VM instance details** (Détails de l'instance de VM).

**Étape 3** Sous l'onglet **Details** (Détails), cliquez sur **Connect to serial console** (Se connecter à la console série).

Consultez la documentation de Google, Interagir avec la console série pour en savoir plus.

# Se connecter à l'instance ASA virtuel à l'aide de GCloud

**Procédure**

**Étape 1** Dans la console GCP, choisissez **Compute Engine (Moteur de calcul)** > **VM instances (Instances de VM)**.

**Étape 2** Cliquez sur le nom de l'instance ASA virtuel pour ouvrir la page **VM instance details** (Détails de l'instance de VM).

**Étape 3** Sous l'onglet **Details** (Détails), cliquez sur le menu déroulant du champ **SSH**.

**Étape 4** Cliquez sur **View gcloud command (Voir la commande gcloud)** > **Run in Cloud Shell (Exécuter dans Cloud Shell)**.

La fenêtre de terminal Cloud Shell s'ouvre. Consultez la documentation de Google, Présentation de l'outil de ligne de commande gcloudet Calcul gcloud ssh pour en savoir plus.

# Utilisation et rapport d'utilisation du processeur (CPU)

Le rapport d'utilisation du processeur résume le pourcentage du processeur utilisé pendant la période précisée. En règle générale, le cœur fonctionne sur environ 30 à 40 % de la capacité totale du processeur en dehors des heures de pointe et sur environ 60 à 70 % de capacité pendant les heures de pointe.

## Utilisation de vCPU dans ASA virtuel

L'utilisation du vCPU ASA virtuel affiche la quantité de vCPU utilisée pour le chemin de données, le point de contrôle et les processus externes.

L'utilisation du vCPU signalé par GCP comprend l'utilisation de l'ASA virtuel, comme décrit :

- Délai d'inactivité d'ASA virtuel
- %SYS surdébit utilisé pour la machine ASA virtuel
- Surdébit du déplacement des paquets entre les vSwitches, les vNIC et les pNIC. Ce surdébit peut être assez important.

## Exemple d'utilisation du processeur

La commande **show cpu usage** (afficher l'utilisation du processeur) peut être utilisée pour afficher les statistiques d'utilisation du processeur.

**Exemple**

```
Ciscoasa#show cpu usage

Utilisation du processeur pendant 5 secondes = 1 %; 1 minute : 2 %; 5 minutes : 1 %
```

Voici un exemple dans lequel l'utilisation de vCPU signalée est sensiblement différente :

- Rapports ASA virtuel : 40 %
- DP : 35 %
- Processus externes : 5 %
- ASA (comme les rapports ASA virtuel) : 40 %
- Interrogation ASA inactive : 10 %
- Frais généraux : 45 %

Le surdébit est utilisé pour effectuer des fonctions d'hyperviseur et pour déplacer des paquets entre les NIC et les vNIC à l'aide du vSwitch.

# Rapport d'utilisation du processeur (CPU) de GCP

Cliquez sur le nom de l'instance sur la console GCP, puis sur l'onglet **Monitoring (**supervision). Vous pourrez voir le pourcentage d'utilisation du processeur (CPU).

Compute Engine vous permet d'exporter des rapports détaillés de votre utilisation de Compute Engine vers un compartiment de stockage Google Cloud à l'aide de la fonctionnalité d'exportation de l'utilisation. Les rapports d'utilisation fournissent des renseignements sur la durée de vie de vos ressources. Par exemple, vous pouvez voir le nombre d'instances de machine virtuelle de votre projet qui exécutent un type de machine `n2-standard-4` et la durée de l'exécution de chaque instance. Vous pouvez également passer en revue l'espace de stockage d'un disque persistant et des informations sur d'autres fonctionnalités de Compute Engine.

# Graphiques ASA virtuel et GCP

Il existe des différences dans les numéros de % du CPU entre l'ASA virtuel et le GCP :

- Les numéros de graphique GCP sont toujours supérieurs aux numéros d'ASA virtuel.
- GCP l'appelle « %CPU usage »; l'ASA virtuel l'appelle « %CPU utilization ».

Les termes « %CPU utilization » et « %CPU usage » signifient des choses différentes :

- L'utilisation du CPU fournit des statistiques sur les processeurs (CPU) physiques.
- L'usage du CPU fournit des statistiques pour les processeurs (CPU) logiques, qui sont basées sur l'hyperthreading du CPU. Comme un seul processeur virtuel (vCPU) est utilisé, l'hyperthreading n'est pas activé.

GCP calcule le pourcentage d'usage du CPU comme suit :

Nombre de CPU virtuels utilisés activement, spécifié en pourcentage du nombre total de CPU disponibles

Ce calcul est la vue de l'hôte de l'utilisation du CPU, et non la vue du système d'exploitation invité, et est l'utilisation moyenne du CPU sur tous les CPU virtuels disponibles dans la machine virtuelle.

Par exemple, si une machine virtuelle avec un CPU virtuel fonctionne sur un hôte qui a quatre CPU physiques et que l'usage des CPU est de 100 %, la machine virtuelle utilise complètement un CPU physique. Le calcul de l'usage du CPU virtuel est l'usage en MHz/nombre de CPU virtuels x fréquence du cœur

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.