Introduction à Cisco Secure Firewall ASA Virtual

L'appliance virtuelle de sécurité adaptative (ASA virtuel) offre des fonctionnalités complètes de pare-feu aux environnements virtualisés afin de sécuriser le trafic des centres de données et les environnements multilocataires.

Vous pouvez gérer et surveiller l'ASA virtuel à l'aide d'ASDM ou de l'interface de ligne de commande. D'autres options de gestion peuvent être disponibles.

Prise en charge des hyperviseurs

Pour la prise en charge des hyperviseurs, consultez Compatibilité Cisco Cisco Secure Firewall ASA.

Gestion des licences pour l'ASA virtuel

L'ASA virtuel utilise les licences logicielles Cisco Smart. Pour des renseignements complets, consultez Gestion des licences logicielles Smart.

Remarque Vous devez installer une licence Smart sur l'ASA virtuel. Jusqu'à ce que vous installiez une licence, le débit est limité à 100 kbit/s. Vous pouvez donc effectuer des tests de connectivité préalables. Une licence Smart est requise pour le fonctionnement normal.

À partir de la version 9.13(1), toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge. Cela vous permet de déployer un ASA virtuel sur une grande variété de profils de ressources VM. Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée plutôt que par une limite de plateforme liée à un type de modèle.

Consultez les sections suivantes pour obtenir des renseignements sur les droits de licence d'ASA virtuel et les spécifications de ressources pour les cibles de déploiement privées et publiques prises en charge.

À propos des droits de licence Smart

Toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuelprise en charge. Cela vous permet d'exécuter l'ASA virtuel sur une grande variété de profils de ressources VM. Cela augmente également le nombre d'instances AWS et Azure prises en charge. Lors de la configuration de la machine ASA virtuel, le nombre maximal de vCPU pris en charge est 16 (ASAv100); et la mémoire maximale prise en charge est de 64 Go pour l'ASA virtuel déployé sur toutes les plateformes autres que AWS et OCI. Pour l'ASA virtuel déployé sur AWS et OCI, la mémoire maximum prise en charge est de 128 Go.

Important Il n'est pas possible de modifier l'allocation des ressources (mémoire, CPU, espace disque) d'une instance ASA virtuel une fois qu'elle est déployée. Si vous devez augmenter vos allocations de ressources pour quelque raison que ce soit, par exemple pour modifier vos droits sous licence d'ASAv30/2 Gbit/s à ASAv50/10 Gbit/s, vous devez créer une nouvelle instance avec les ressources nécessaires.

- vCPU : l'ASA virtuel prend en charge de 1 à 16 vCPU.
- Mémoire : l'ASA virtuel prend en charge de 2 Go à 64 Go de RAM pour l'ASA virtuel déployé sur toutes les plateformes à l'exception d'AWS et d'OCI. Pour l'ASA virtuel déployé sur AWS et OCI, la mémoire maximum prise en charge est de 128 Go.
- Stockage sur disque : l'ASA virtuel prend en charge un disque virtuel minimum de 8 Go par défaut. Selon le type de plateforme, la prise en charge du disque virtuel varie entre 8 Go et 10 Go. Gardez cela à l'esprit lorsque vous provisionnez vos ressources de VM.

Important La mémoire minimale requise pour l'ASA virtuel est de 2 Go. Si votre ASA virtuel actuel fonctionne avec moins de 2 Go de mémoire, vous ne pouvez pas effectuer de mise à niveau vers la version 9.13(1) ou une version ultérieure à partir d'une version antérieure sans augmenter la mémoire de votre machine ASA virtuel. Vous pouvez également redéployer une nouvelle machine ASA virtuel avec la dernière version.

La mémoire minimale requise pour le déploiement d'ASA virtuel avec plus d'un vCPU est de 4 Go.

Pour la mise à niveau d'ASA virtuel version 9.14 ou ultérieure vers une dernière version, la machine virtuelle ASA nécessite une mémoire minimale de 4 Go et de 2 vCPU.

Limites de session pour les fonctions sous licence

Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité et du limiteur de débit.

Tableau 1 : Limites de session d'ASA virtuel par droit

Autorisation	Paires Secure Client (services client sécurisés) Premium	Nombre total de sessions de mandataire TLS	Limiteur de débit
Niveau standard, 100 M	50	500	150 Mbit/s

Autorisation	Paires Secure Client (services client sécurisés) Premium	Nombre total de sessions de mandataire TLS	Limiteur de débit
Niveau standard, 1 G	250	500	1 Gbit/sec
Niveau standard, 2 G	750	1 000	2 Gbit/s
Niveau standard, 10 G	10 000	10 000	10 Gbit/s
Niveau standard, 20 G	20 000	20 000	20 Gbit/s

Les limites de session accordées par un droit, comme indiqué dans le tableau précédent, ne peuvent pas dépasser les limites de session de la plateforme. Les limites de session de la plateforme sont basées sur la quantité de mémoire provisionnée pour l'ASA virtuel.

Tableau 2 : Limites de session d'ASA virtuel par exigence de mémoire

Mémoire provisionnée	Paires Secure Client (services client sécurisés) Premium	Nombre total de sessions de mandataire TLS
De 2 Go à 7,9 Go	250	500
De 8 Go à 15,9 Go	750	1 000
De 16 Go à 31,9 Go	10 000	10 000
De 32 Go à 64 Go	20 000	20 000
De 64 Go à 128 Go	20 000	20 000

Limites de la plateforme

Les connexions de pare-feu, les connexions simultanées et les VLAN sont des limites de plateforme basées sur la mémoire ASA virtuel.

Remarque Nous limitons les connexions de pare-feu à 100 lorsque l'ASA virtuel est dans un état sans licence. Une fois une licence avec n'importe quel droit, les connexions sont acheminées à la limite de la plateforme. La mémoire minimale requise pour l'ASA virtuel est de 2 Go.

Tableau 3 : Limites de la plateforme

Mémoire ASA virtuel	Connexions de pare-feu, simultanées	Réseaux VLAN
De 2 Go à 7,9 Go	100 000	50
De 8 Go à 15,9 Go	500 000	200
De 16 Go à 31,9 Go	2 000 000	1024
De 32 Go à 64 Go	4 000 000	1024

Droits relatifs au cloud privé ASA virtuel (VMware, KVM, Hyper-V)

Étant donné que toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge, vous disposez d'une plus grande flexibilité lorsque vous déployez l'ASA virtuel dans un environnement de cloud privé (VMware, KVM, Hyper-V).

Remarque ASAv50 et ASAv100 ne sont pas pris en charge sur HyperV.

Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit. Le tableau suivant récapitule les limites de session en fonction du niveau d'admissibilité de l'ASA virtueldéployé dans un environnement de cloud privé, avec le limiteur de débit appliqué.

Remarque Les limites de session d'ASA virtuel sont basées sur la quantité de mémoire provisionnée pour l'ASA virtuel; voir Tableau 2 : Limites de session d'ASA virtuel par exigence de mémoire, à la page 3.

Tableau 4 : ASA virtuel sur le cloud privé VMware/KVM/HyperV — Limites de fonctionnalités sous licence en fonction des droits

RAM (Go)		Prise en charge des droits*				
Min	**Max**	**Niveau standard, 100 M**	**Niveau standard, 1 G**	**Niveau standard, 2 G**	**Niveau standard, 10 G**	**Niveau standard, 20 G**
2	7.9	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500/20 G
8	15.9	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
16	31.9	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
32	64	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	20 K/20 K/20 G
*Sessions Secure Client (services client sécurisés)/Sessions de mandataire TLS/Limiteur de débit par droit/instance.						

Droits pour le nuage public ASA virtuel (AWS)

Comme toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge, vous pouvez déployer l'ASA virtuel sur de nombreux types d'instances AWS. Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit.

Le tableau suivant récapitule les limites de session et le limiteur de débit en fonction du niveau d'admissibilité pour les types d'instance AWS. Consultez « À propos du déploiement d'ASA virtuel sur le nuage AWS » pour obtenir une ventilation des dimensions de la VM AWS (vCPU et mémoire) pour les instances prises en charge.

Tableau 5 : ASA virtuel sur AWS – Limites des fonctionnalités sous licence en fonction des droits

Instance	Prise en charge des droits BYOL*				PAYG**
	Niveau standard, 100 M	Niveau standard, 1 G	Niveau standard, 2 G	Niveau standard, 10 G	
c5.xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000
c5.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K
c4.large	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c4.xlarge	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c4.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	750/1 000
c3.large	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c3.xlarge	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
c3.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	750/1 000
m4.large	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500
m4.xlarge	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	10 K/10 K
m4.2xlarge	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K

*Sessions Secure Client (services client sécurisés)/Sessions de mandataire TLS/Limiteur de débit par droit/instance.

**Sessions Secure Client (services client sécurisés)/Sessions de mandataire TLS. Le limiteur de débit n'est pas utilisé en mode PAYG.

Mode Pay-As-You-Go (PAYG)

Le tableau suivant résume les droits de licence Smart pour chaque niveau du mode de facturation à l'heure (PAYG), qui est basé sur la mémoire allouée.

Tableau 6 : ASA virtuel sur AWS – droits de licence Smart pour PAYG

RAM (Go)	Droit pour le mode de facturation à l'heure
< 2 Go	Niveau standard, 100 M (ASAv5)
2 Go à < 8 Go	Niveau standard, 1 G (ASAv10)
8 Go à < 16 Go	Niveau standard, 2 G (ASAv30)
16 Go à < 32 Go	Niveau standard, 10 G (ASAv50)
30 Go et plus	Niveau standard, 20 G (ASAv100)

Droits pour le nuage public ASA virtuel (Azure)

Comme toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuel prise en charge, vous pouvez déployer l'ASA virtuel sur de nombreux types d'instances Azure. Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS sont déterminées par le niveau d'autorisation de la plateforme ASA virtuel installée et appliquées par l'intermédiaire d'un limiteur de débit.

Le tableau suivant récapitule les limites de session et le limiteur de débit en fonction du niveau d'admissibilité pour les types d'instance Azure. Consultez « À propos du déploiement d'ASA virtuel sur le nuage Microsoft Azure » pour obtenir une ventilation des dimensions de la VM Azure (vCPU et mémoire) pour les instances prises en charge.

Remarque Actuellement, le mode Pay-As-You-Go (PAYG) n'est pas pris en charge pour l'ASA virtuel sur Azure.

Tableau 7 : ASA virtuel sur Azure – Limites des fonctionnalités sous licence en fonction des droits

Instance	Prise en charge des droits BYOL*				
	Niveau standard, 100 M	**Niveau standard, 1 G**	**Niveau standard, 2 G**	**Niveau standard, 10 G**	**Niveau standard, 20 G**
D1, D1_v2DS1, DS1_v2	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500/20 G
D2, D2_v2, DS2, DS2_v2	50/500/100 M	250/500/1 G	250/500/2 G	250/500/10 G	250/500/20 G
D3, D3_v2, DS3, DS3_v2	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
D4, D4_v2, DS4, DS4_v2	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
D5, D5_v2, DS5, DS5_v2	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/20 K/20 G
D2_v3	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
D4_v3	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
D8_v3	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/10 K/20 G
F4, F4s	50/500/100 M	250/500/1 G	750/1 000/2 G	750/1 000/10 G	750/1 000/20 G
F8, F8s	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/20 K/20 G
F16, F16s	50/500/100 M	250/500/1 G	750/1 000/2 G	10 K/10 K/10 G	10 K/20 K/20 G
*Sessions Secure Client (services client sécurisés)/Sessions de mandataire TLS/Limiteur de débit par droit/instance.					

Lignes directrices et limites relatives à la licence

La fonctionnalité de pare-feu ASA virtuel est très similaire aux pare-feu matériel ASA, mais avec les lignes directrices et les limites suivantes.

Lignes directrices et limites pour l'ASA virtuel (tous les droits)

Lignes directrices relatives aux licences Smart

- Le nombre maximum de vCPU pris en charge est de 16. La mémoire maximum prise en charge est de 64 Go pour l'ASA virtuel déployé sur toutes les plateformes à l'exception d'AWS et d'OCI. Pour l'ASA virtuel déployé sur AWS et OCI, la mémoire maximum prise en charge est de 128 Go. Toute licence ASA virtuel peut être utilisée sur n'importe quelle configuration vCPU/mémoire ASA virtuelprise en charge.
- Les limites de session pour les fonctionnalités sous licence et les capacités de plateforme sans licence sont définies en fonction de la quantité de mémoire de VM
- Les limites de session pour Secure Client (services client sécurisés) et le mandataire TLS sont déterminées par les droits de plateforme d'ASA virtuel; les limites de session ne sont plus associées à un type de modèle ASA virtuel (ASAv5/10/30/50/100).
- Les limites de session ont une exigence de mémoire minimum; dans les cas où la mémoire de VM est inférieure au minimum d'exigence, les limites de session seront définies pour le nombre maximum pris en charge par la quantité de mémoire.
- Il n'y a aucune modification des droits existants; l'UGS de droit et le nom d'affichage continueront d'inclure le numéro de modèle (ASAv5/10/30/50/100).
- Le droit définit le débit maximum par l'intermédiaire d'un limiteur de débit.
- Il n'y a aucune modification du processus de commande des clients.

Stockage sur disque

L'ASA virtuel prend en charge un disque virtuel maximum de 8 Go par défaut. Vous ne pouvez pas augmenter la taille du disque au-delà de 8 Go. Gardez cela à l'esprit lorsque vous provisionnez vos ressources de VM.

Directives relatives au mode contextuel

Pris en charge en mode contexte unique uniquement Ne prend pas en charge le mode contexte multiple.

Lignes directrices relatives au basculement pour la haute disponibilité

Pour les déploiements de basculement, assurez-vous que l'unité de secours a les mêmes droits de licence; par exemple, les deux unités doivent avoir le droit de 2 Gbit/s.

Important Lors de la création d'une paire à haute accessibilité à l'aide d'ASA virtuel, il est nécessaire d'ajouter les interfaces de données à chaque ASA virtuel dans le même ordre. Si exactement les mêmes interfaces sont ajoutées à chaque ASA virtuel, mais dans un ordre différent, des erreurs peuvent s'afficher à la console ASA virtuel. La fonctionnalité de basculement peut également être affectée.

Fonctionnalités ASA non prises en charge

L'ASA virtuel ne prend pas en charge les fonctionnalités ASA suivantes :

- Mise en grappe (pour tous les droits, sauf AWS, KVM et VMware)
- Mode contexte multiple
- Basculement actif/actif
- EtherChannels
- Licences partagées AnyConnect Premium

Restrictions

- L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)

Lignes directrices et limites pour le droit de 1 Go

Lignes directrices relatives aux performances

- La réservation de bâtis grand format sur plateforme de 1 Go avec 9 interfaces e1000 configurées ou plus peut entraîner le rechargement de l'appareil. Si la **jumbo-frame reservation** (réservation de bâtis grand format) est activée, réduisez le nombre d'interfaces à 8 ou moins. Le nombre exact d'interfaces dépendra de la quantité de mémoire nécessaire pour le fonctionnement des autres fonctionnalités configurées. Il pourrait être inférieur à 8.

Lignes directrices et limites pour le droit de 10 Go

Lignes directrices relatives aux performances

- Prend en charge 10 Gbit/s de trafic agrégé.
- Prend en charge les pratiques suivantes pour améliorer les performances d'ASA virtuel :
  - Nombre de nœuds
  - Plusieurs files d'attente RX
  - Provisionnement SR-IOV
  - Reportez-vous à Réglage de la performance et à Réglage de la performance pour en savoir davantage.

- L'épinglage du CPU est recommandé pour atteindre des débits maximum; voir Amélioration de la performance pour les configurations ESXi et Amélioration des performances pour les configurations KVM.
- La réservation de bâtis grand format avec un ensemble d'interfaces e1000 et i40e-vf peut faire en sorte que les interfaces i40e-vf restent inactives. Si **jumbo-frame reservation** (réservation bâtis grand format) est activé, ne mélangez pas les types d'interface qui utilisent les pilotes e1000 et i40e-vf.

Restrictions

- Le mode transparent n'est pas pris en charge.
- L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)
- Non pris en charge sur Hyper-V.

Lignes directrices et limites relatives au droit à 20 GO

Lignes directrices relatives aux performances

- Prend en charge 20 Gbit/s de trafic agrégé.
- Prend en charge les pratiques suivantes pour améliorer les performances d'ASA virtuel :
  - Nombre de nœuds
  - Plusieurs files d'attente RX
  - Provisionnement SR-IOV
  - Reportez-vous à Réglage de la performance et à Réglage de la performance pour en savoir davantage.
- L'épinglage du CPU est recommandé pour atteindre des débits maximum; voir Amélioration de la performance pour les configurations ESXi et Amélioration des performances pour les configurations KVM.

Restrictions

- L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)
- Le mode transparent n'est pas pris en charge.
- Non pris en charge sur Amazon Web Services (AWS) et Hyper-V.

Interfaces et cartes réseau virtuelles d'ASA virtuel

En tant qu'invité sur une plateforme virtualisée, l'ASA virtuel utilise les interfaces réseau de la plateforme physique sous-jacente. Chaque interface ASA virtuel est mappée à une carte réseau virtuelle (vNIC).

- Interfaces ASA virtuel

- vNIC prises en charge

Interfaces ASA virtuel

L'ASA virtuel comprend les interfaces Gigabit Ethernet suivantes :

- Management 0/0

  Pour AWS et Azure, Management 0/0 peut être une interface « externe » d'acheminement du trafic.

- GigabitEthernet 0/0 jusqu'à 0/8. Notez que le GigabitEthernet 0/8 est utilisé pour la liaison de basculement lorsque vous déployez l'ASA virtuel dans le cadre d'une paire de basculement.

Remarque Pour simplifier la migration de la configuration, dix interfaces GigabitEthernet, comme celles disponibles sur le pilote VMXNET3, portent la mention GigabitEthernet. Cela n'a aucune incidence sur la vitesse d'interface réelle et est uniquement cosmétique.

L'ASA virtuel définit les interfaces GigabitEthernet à l'aide du pilote E1000 comme des liens de 1 Gbit/s. Notez que VMware ne recommande plus d'utiliser le pilote E1000.

- Hyper-V prend en charge jusqu'à huit interfaces. Management 0/0 et GigabitEthernet 0/0 jusqu'à 0/6. Vous pouvez utiliser GigabitEthernet 0/6 comme liaison de basculement.

vNIC prises en charge

L'ASA virtuel prend en charge les vNIC suivantes. Le mélange de vNIC, tels que e1000 et vmxnet3, sur le même ASA virtuel n'est pas pris en charge.

Tableau 8 : vNIC prises en charge

Type de vNIC	Prise en charge des hyperviseurs		ASA virtuelVersion	Notes
	VMware	KVM		
vmxnet3	Oui	Non	Version 9.9(2) ou ultérieure	VMware par défaut Lorsque vous utilisez vmxnet3, vous devez désactiver le Large Receive Offload (LRO, grand déchargement de réception) pour éviter de mauvaises performances TCP. Consultez Désactiver LRO pour VMware et VMXNET3, à la page 11.
e1000	Oui	Oui	version 9.2(1) ou ultérieure	Non recommandé par VMware.

Type de vNIC	Prise en charge des hyperviseurs		ASA virtuelVersion	Notes
	VMware	KVM		
virtio	Non	Oui	Version 9.3(2.200) ou ultérieure	KVM par défaut
ixgbe-vf	Oui	Oui	Version 9.8(1) ou ultérieure	Par défaut AWS; ESXi et KVM pour la prise en charge de SR-IOV.
i40e-vf	Non	Oui	version 9.10(1) ou ultérieure	KVM pour la prise en charge de SR-IOV.

Désactiver LRO pour VMware et VMXNET3

Large Receive Offload (LRO) est une technique pour augmenter le débit entrant des connexions réseau à bande passante élevée en réduisant le surdébit du processeur. Elle fonctionne par agrégation de plusieurs paquets entrants d'un seul flux dans un tampon plus grand avant qu'ils ne soient transmis au niveau supérieur de la pile de réseau, réduisant ainsi le nombre de paquets qui doivent être traités. Cependant, la technique LRO peut entraîner des problèmes de performance TCP dans lesquels la livraison des paquets réseau peut ne pas circuler de manière uniforme et pourrait être « en rafale » dans les réseaux congestionnés.

Important VMware active LRO par défaut pour augmenter le débit global. Il est donc nécessaire de désactiver LRO pour les déploiements ASA virtuel sur cette plateforme.

Vous pouvez désactiver LRO directement sur la machine ASA virtuel. Éteignez la machine virtuelle avant d'apporter des modifications à la configuration.

1. Recherchez la machine ASA virtuel dans l'inventaire du client Web vSphere.
    1. Pour trouver une machine virtuelle, sélectionnez un centre de données, un dossier, une grappe, un ensemble de ressources ou un hôte.
    2. Cliquez sur l'onglet **Related Objects** (objets associés), puis sur **Virtual Machines** (machines virtuelles).
2. Faites un clic droit sur la machine virtuelle et sélectionnez **Edit Settings** (modifier les paramètres).
3. Cliquez sur **VM Options** (options de machine virtuelle).
4. Développez **Advanced** (avancé).
5. Sous Configuration Parameters (paramètres de configuration), cliquez sur le bouton **Edit Configuration** (modifier la configuration).
6. Cliquez sur **Add Parameter** (ajouter un paramètre) et saisissez un nom et une valeur pour les paramètres LRO :
    - Net.VmxnetSwLROSL | 0
    - Net.Vmxnet3SwLRO | 0
    - Net.Vmxnet3HwLRO | 0

- Net.Vmxnet2SwLRO | 0
- Net.Vmxnet2HwLRO | 0

Remarque En option, si les paramètres LRO existent, vous pouvez également examiner les valeurs et les modifier au besoin. Si un paramètre est égal à 1, LRO est activé. S'il est égal à 0, LRO est désactivé.

7. Cliquez sur **OK** pour enregistrer vos modifications et quitter la boîte de dialogue **Configuration Parameters** (paramètres de configuration).
8. Cliquez sur **Save** (enregistrer).

Consultez les articles d'assistance de VMware suivants pour plus d'informations :

- VMware KB 1027511
- VMware KB 2055140

ASA virtuel et provisionnement de l'interface SR-IOV

La virtualisation des E/S à racine unique (SR-IOV) permet à plusieurs machines virtuelles exécutant divers systèmes d'exploitation invités de partager un seul adaptateur de réseau PCIe dans un serveur d'hôte. SR-IOV permet à une machine virtuelle de déplacer des données directement vers et à partir de l'adaptateur réseau, en contournant l'hyperviseur pour augmenter le débit du réseau et réduire la charge CPU du serveur. Les processeurs de serveur x86 récents comprennent des améliorations de jetons, comme la technologie Intel VT-d, qui facilitent les transferts directs de mémoire et d'autres opérations requises par SR-IOV.

La spécification SR-IOV définit deux types d'appareils :

- Fonction physique (PF) : essentiellement un NIC statique, un PF est un périphérique PCIe complet qui comprend des fonctionnalités SR-IOV. Les PF sont détectés, gérés et configurés comme des périphériques PCIe normaux. Un seul PF peut assurer la gestion et la configuration d'un ensemble de fonctions virtuelles (VF).
- Fonction virtuelle (VF) : comme pour une vNIC dynamique, un VF est un périphérique PCIe virtuel complet ou allégé qui fournit au moins les ressources nécessaires pour les déplacements de données. Un VF n'est pas géré directement, mais il est dérivé et géré par un PF. Un ou plusieurs VF peuvent être attribués à une machine virtuelle.

Le protocole SR-IOV est défini et géré par le groupe d'intérêts spécial pour l'interconnexion des composants périphériques (PCI SIG), une organisation du secteur qui est agréée pour développer et gérer la norme PCI. Pour en savoir plus sur SR-IOV, consultez Introduction à PCI-SIG SR-IOV : Introduction à la technologie SR-IOV.

Le provisionnement des interfaces SR-IOV sur l'ASA virtuel nécessite une certaine planification, qui commence par le niveau de système d'exploitation, le matériel et le processeur (CPU), les types et les paramètres d'adaptateur appropriés.

Lignes directrices et limites des interfaces SR-IOV

Le matériel spécifique utilisé pour le déploiement ASA virtuel peut varier, selon la taille et les exigences d'utilisation. Gestion des licences pour l'ASA virtuel, à la page 1 explique les scénarios de ressources conformes qui correspondent aux droits de licence pour les différentes plateformes ASA virtuel. En outre, les fonctions virtuelles SR-IOV nécessitent des ressources système spécifiques.

Prise en charge du système d'exploitation de l'hôte et de l'hyperviseur

La prise en charge de SR-IOV et les pilotes VF sont disponibles pour :

- le noyau Linux 2.6.30 ou une version ultérieure

L'ASA virtuel avec les interfaces SR-IOV est actuellement pris en charge sur les hyperviseurs suivants :

- VMware vSphere/ESXi
- QEMU/KVM
- AWS

Prise en charge pour la plateforme matérielle

Remarque Vous devez déployer l'ASA virtuel sur n'importe quel périphérique CPU *de classe de serveur* x86 compatible avec les plateformes de virtualisation prises en charge.

Cette section décrit les lignes directrices matérielles pour les interfaces SR-IOV. Bien qu'il s'agisse de lignes directrices et non d'exigences, l'utilisation de matériel qui ne respecte pas ces lignes directrices peut entraîner des problèmes de fonctionnalité ou de mauvaises performances.

Un serveur prenant en charge SR-IOV et équipé d'un adaptateur PCIe compatible avec SR-IOV est requis. Vous devez être conscient des considérations matérielles suivantes :

- Les capacités des cartes réseau SR-IOV, y compris le nombre de VF disponibles, varient selon les fournisseurs et les périphériques.
- Tous les logements PCIe ne prennent pas en charge SR-IOV.
- Les logements PCIe compatibles avec SR-IOV peuvent avoir des capacités différentes.

Remarque Consultez la documentation de votre fabricant pour connaître la prise en charge de SR-IOV sur votre système.

- Pour les jetons, les cartes-mères et les processeurs compatibles avec VT-d, vous pouvez trouver des renseignements sur cette page de matériel prenant en charge IOMMU compatible avec la virtualisation. VT-d est un paramètre BIOS requis pour les systèmes SR-IOV.
- Pour VMware, vous pouvez effectuer des recherches dans le Guide de compatibilité en ligne pour la prise en charge de SR-IOV.

- Pour KVM, vous pouvez vérifier la compatibilité du processeur. Notez que pour l'ASA virtuel sur KVM, nous prenons uniquement en charge le matériel x86.

Remarque Nous avons testé l'ASA virtuel avec le serveur rack série C Cisco UCS. Notez que le serveur Cisco UCS-B ne prend pas en charge le vNIC ixgbe-vf.

Cartes réseau (NIC) prises en charge pour SR-IOV

- Adaptateur réseau Ethernet Intel X710

Attention L'ASA virtuel n'est pas compatible avec le pilote d'hôte i40en de 1.9.5 pour la carte réseau x710. Les versions de pilote plus anciennes ou plus récentes fonctionneront. (VMware uniquement)

- Adaptateur pour serveur Ethernet Intel X520, DA2

CPU

- CPU multicœur x86_64

  Pont Intel Sandy ou version ultérieure (recommandé).

Remarque Nous avons testé l'ASA virtuel sur le processeur Broadwell d'Intel (E5-2699-v4) à 2,3 GHz.

- Cœurs
  - Au moins 8 cœurs physiques par socket de CPU
  - Les 8 cœurs doivent se trouver sur un seul connecteur.

Remarque L'épinglage de CPU est recommandé pour atteindre le débit maximal sur ASAv50 et ASAv100; consultez Amélioration de la performance pour les configurations ESXi et Amélioration des performances pour les configurations KVM.

Paramètres BIOS

SR-IOV nécessite une prise en charge dans le BIOS ainsi que dans l'instance de système d'exploitation ou l'hyperviseur qui s'exécute sur le matériel. Vérifiez le BIOS de votre système pour identifier les paramètres suivants :

- SR-IOV est activé
- VT-x (Technologie de virtualisation) est activée

- VT-d est activée
- (Facultatif) Hyperthreading est désactivé

Nous vous recommandons de vérifier le processus avec la documentation du fournisseur, car différents systèmes ont des méthodes différentes pour accéder aux paramètres BIOS et les modifier.

Restrictions

Gardez à l'esprit des limites suivantes lors de l'utilisation des interfaces ixgbe-vf :

- La machine virtuelle invitée n'est pas autorisée à définir le VF en mode promiscuité. Pour cette raison, le mode transparent n'est pas pris en charge lors de l'utilisation de ixgbe-vf.
- La machine virtuelle invitée n'est pas autorisée à définir l'adresse MAC sur le VF. C'est pourquoi l'adresse MAC n'est pas transférée pendant la haute accessibilité, comme cela se fait sur d'autres plateformes ASA et avec d'autres types d'interfaces. Le basculement à haute accessibilité fonctionne par le transfert de l'adresse IP de l'active à la veille.

Remarque Cette limite s'applique également aux interfaces i40e-vf.

- Le serveur Cisco UCS-B ne prend pas en charge la vNIC ixgbe-vf.
- Dans une configuration de basculement, en cas de défaillance d'un ASA virtuel (unité principale) jumelé, l'unité en veille ASA virtuel prend le rôle d'unité principale et l'adresse IP de son interface est mise à jour avec une nouvelle adresse MAC de l'unité en veille ASA virtuel. Ensuite, l'ASA virtuel envoie une mise à jour Gratuitous ARP (Address Resolution Protocol) pour annoncer le changement d'adresse MAC de l'adresse IP de l'interface aux autres périphériques du même réseau. Cependant, en raison d'une incompatibilité avec ces types d'interfaces, la mise à jour Gratuitous ARP n'est pas envoyée à l'adresse IP globale qui est définie dans les instructions NAT ou PAT pour traduire l'adresse IP de l'interface en adresses IP globales.

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.