Notes de mise à jour de NSX Container Plugin 2.4

VMware NSX Container Plugin 2.4 | 7 mars 2019

Vérifiez régulièrement les ajouts et les mises à jour apportées à ce document.

Contenu des notes de mise à jour

Les notes de mise à jour couvrent les sujets suivants :

- Nouveautés
- Conditions de compatibilité
- Problèmes résolus
- Problèmes connus

Nouveautés

Nouveautés

NSX Container Plugin (NCP) 2.4 comprend les nouvelles fonctionnalités suivantes :

- Le nom de fondation de la vignette VMware NSX-T est désormais facultatif. Si vous n'en spécifiez aucun, le nom du déploiement PAS est utilisé.
- La fonctionnalité HA de NCP est activée par défaut sur Kubernetes.
- NCP/nsx_node_agent s'arrête en cas d'échec de connexion au serveur principal.
  Ajout de l'option de configuration connect_retry_timeout. Vous pouvez l'utiliser pour configurer le délai en secondes pris par NCP/nsx_node_agent pour récupérer la connexion à NSX Manager, à l'adaptateur orchestrateur de conteneur ou à Hyperbus avant de se fermer.
- Prise en charge de l'affinité de session pour un service de type LoadBalancer.
  Outre l'option configMap l4_persistence, NCP prend désormais en charge la configuration sessionAffinity dans la spécification de service pour les services de type LoadBalancer. Si l4_persistence est défini sur Aucun, la configuration sessionAffinity dans la spécification de service détermine uniquement l'effet de la persistance. Dans le cas contraire, l'affinité de session est activée pour tous les services de type LoadBalancer, et les utilisateurs peuvent utiliser la configuration sessionAffinity dans la spécification de service pour contrôler le délai d'expiration de la persistance.
- Si une adresse IP est fournie dans la spécification loadBalancerIP d'un service Kubernetes de type LoadBalancer, le service est exposé en externe sur cette adresse IP.
- Prise en charge pour le cluster NSX Manager.

Remarque : NCP ignore les routes OpenShift avec des relais et des terminaisons de rechiffrement SSL.

Conditions de compatibilité

Produit	Version
Mosaïque NCP/NSX-T pour PAS	2.4
NSX-T	2.3, 2.3.1, 2.4

Kubernetes	1.12, 1.13
OpenShift	3.10, 3.11
Système d'exploitation de VM sur hôte Kubernetes	Ubuntu 16.04, RHEL 7.5, 7.6, CentOS 7.4, 7.5
Système d'exploitation de VM sur hôte OpenShift	RHEL 7.4, 7.5, 7.6, CentOS 7.4, 7.5
PAS (PCF)	OpsManager 2.3.x + PAS 2.3.x OpsManager 2.4.x (à l'exception de la version 2.4.0) + PAS 2.4.x (à l'exception de la version 2.4.0)

Problèmes connus

- **Problème 2118515 : Dans une configuration à grande échelle, la création de pare-feu par sur NSX-T est assez longue**
  Dans une configuration à grande échelle (par exemple, 250 nœuds Kubernetes, 5 000 espaces, 2 500 stratégies réseau), NCP peut prendre quelques minutes pour créer les sections de pare-feu et les règles dans NSX-T.

  Solution : aucune. Une fois les sections de pare-feu et les règles créées, les performances doivent revenir à la normale.

- **Problème 2125755 : un StatefullSet peut perdre la connectivité réseau lors de l'exécution des mises à jour de Canary et des mises à jour continues par phase**
  Si un StatefulSet a été créé avant la mise à niveau de NCP vers la version actuelle, le StatefullSet peut perdre la connectivité réseau lors de l'exécution des mises à jour de Canary et des mises à jour continues par phase.

  Solution : Créez le StatefulSet après la mise à niveau de NCP vers la version actuelle.

- **Problème 2131494 : NGINX Kubernetes Ingress fonctionne toujours après la redéfinition de la classe Ingress nginx sur nsx**
  Lorsque vous créez un objet NGINX Kubernetes Ingress, NGINX crée des règles de transfert du trafic. Si vous redéfinissez la classe Ingress sur une autre valeur, NGINX ne supprime pas les règles et continue à les appliquer, même si vous supprimez l'objet Kubernetes Ingress après la modification de la classe. Il s'agit d'une limitation de NGINX.

  Solution : pour supprimer les règles créées par NGINX, supprimez l'objet Kubernetes Ingress lorsque la valeur de classe est nginx. Recréez ensuite l'objet Kubernetes Ingress.

- **Pour un service Kubernetes de type ClusterIP, l'affinité de session basée sur l'adresse IP du client n'est pas prise en charge**
  NCP ne prend pas en charge l'affinité de session basée sur l'adresse IP du client pour un service Kubernetes de type ClusterIP.

  Solution : aucune

- **Pour un service Kubernetes de type ClusterIP, l'indicateur de mode épingle n'est pas pris en charge**
  NCP ne prend pas en charge l'indicateur de mode épingle pour un service Kubernetes de type ClusterIP.

  Solution : aucune

- **Problème 2193901 : l'utilisation de plusieurs PodSelectors ou de plusieurs NsSelectors pour une**

seule règle de stratégie réseau Kubernetes n'est pas prise en charge
L'application de plusieurs sélecteurs permet uniquement le trafic entrant depuis des espaces spécifiques.

Solution : utilisez plutôt matchLabels avec matchExpressions dans un seul PodSelector ou NsSelector.

- Problème 2194646 : la mise à jour des stratégies réseau lorsque NCP est hors service n'est pas prise en charge
  Si vous mettez à jour une stratégie réseau lorsque NCP est hors service, l'ensemble d'adresses IP de destination pour la stratégie réseau sera incorrect lorsque NCP est rétabli.

  Solution : recréez la stratégie réseau lorsque NCP est en service.

- Problème 2192489 : après la désactivation de « BOSH DNS server » dans PAS director config, le serveur DNS Bosh (169.254.0.2) figure toujours dans le fichier resolve.conf du conteneur.
  Dans un environnement PAS exécutant PAS 2.2, après que vous désactivez « BOSH DNS server » dans PAS director config, le serveur DNS Bosh (169.254.0.2) figure toujours dans le fichier resove.conf du conteneur. Dans ce cas, l'exécution d'une commande ping avec un nom de domaine complet est très longue. Ce problème n'existe pas avec PAS 2.1.

  Solution : aucune. Il s'agit d'un problème PAS.

- Problème 2194367 : la vignette NSX-T ne prend actuellement pas en charge les segments d'isolation PAS qui déploient leurs propre routeurs
  La vignette NSX-T ne fonctionne pas avec des segments d'isolation PAS (Pivotal Application Service) qui déploient leurs propres routeurs GoRouters et routeurs TCP. En effet, NCP ne peut pas obtenir les adresses IP des machines virtuelles de routeur ni créer des règles de pare-feu NSX pour autoriser le trafic allant des routeurs aux conteneurs d'applications PAS.

  Solution : aucune.

- Problème 2199504 : le nom complet des ressources NSX-T créées par NCP est limité à 80 caractères
  Quand NCP crée une ressource NSX-T pour une ressource dans l'environnement du conteneur, il génère le nom complet de la ressource NSX-T en combinant le nom du cluster, un espace de noms ou nom de projet, et le nom de la ressource dans l'environnement du conteneur. Si le nom complet contient plus de 80 caractères, il est tronqué à 80 caractères.

  Solution : aucune

- Problème 2199778 : avec NSX-T 2.2, Ingress, Service et Secrets portant des noms d'une longueur supérieure à 65 caractères ne sont pas pris en charge
  Avec NSX-T 2.2, lorsque `use_native_loadbalancer` est défini sur `True`, les noms Ingresses, Secrets et Services référencés par Ingress et les services de type LoadBalancer, doivent compter un nombre maximal de 65 caractères. Dans le cas contraire, Ingress ou Service ne fonctionne pas correctement.

  Solution : lors de la configuration d'Ingress, Secret ou Service, spécifiez un nom comportant 65 caractères ou moins.

- Problème 2065750 : l'installation du module NSX-T CNI échoue avec un conflit de fichier
  Dans un environnement RHEL où Kubernetes est installé, si vous installez le module NSX-T CNI à l'aide de `yum localinstall` ou `rpm -i`, vous obtenez une erreur indiquant un conflit avec un fichier du module kubernetes-cni.

  Solution : installez le module NSX-T CNI à l'aide de la commande `rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm`.

- Problème 2224218 : après la suppression d'un service ou d'une application, la libération de l'adresse IP SNAT pour le pool IP dure 2 minutes

Si vous supprimez un service ou une application et que vous le/la recréez en moins de 2 minutes, il/elle obtiendra une nouvelle IP SNAT du pool IP.

Solution : après la suppression d'un service ou d'une application, patientez 2 minutes avant de le/la recréer si vous souhaitez réutiliser la même adresse IP.

- **Problème 2218008 : la configuration de différents clusters Kubernetes afin d'utiliser le même bloc d'IP entraîne des problèmes de connectivité**
  Si vous configurez différents clusters Kubernetes pour utiliser le même bloc d'IP, certains espaces ne seront pas en mesure de communiquer avec d'autres espaces ou des réseaux externes.

  Solution : ne configurez pas différents clusters Kubernetes afin d'utiliser le même bloc d'IP.

- **Problème 2263536 : le service Kubernetes de type NodePort ne parvient pas à transférer le trafic**
  Avec un service de type NodePort, un nœud Kubernetes est utilisé en tant que routeur pour le transfert du trafic depuis l'extérieur du cluster vers les espaces. Lorsque vous configurez ce nœud, les règles des iptables ne sont parfois pas configurées correctement pour autoriser le trafic.

  Solution : exécutez la commande suivante pour ajouter manuellement une règle aux iptables :

  ```
  iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT
  ```

  Notez que cette commande fonctionne uniquement pour un service NodePort avec « externalTrafficPolicy: Cluster ». Elle ne fonctionne pas pour « externalTrafficPolicy: Local ».