Notes de mise à jour de NSX Container Plugin 2.4.1

VMware NSX Container Plugin 2.4.1 | 9 mai 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

NSX Container Plugin (NCP) 2.4.1 comprend les nouvelles fonctionnalités suivantes :

- Utilisation d'une section de pare-feu distribué unique pour le contrôle de santé
  Utilisez une section de pare-feu distribué unique par cluster pour inclure toutes les règles de pare-feu requises pour les espaces avec la sonde de réactivité et la sonde de disponibilité. La limite est un maximum de 1 000 espaces avec une sonde de réactivité ou une sonde de disponibilité dans un cluster, car il peut y avoir au maximum 1 000 règles dans une section de pare-feu distribué.
- Faire en sorte que l'agent de nœud NSX gère l'arrêt inattendu du démon `privsep`
  L'agent de nœud NSX a été amélioré pour traiter et récupérer à partir d'une interruption inattendue du démon `privsep`.
- Définition d'une limite maximale pour la mise à l'échelle automatique du service Kubernetes
  Avec une nouvelle option NCP configMap, `max_allowed_virtual_servers`, les utilisateurs peuvent définir le nombre maximal de serveurs virtuels autorisés à être créés dans le cluster.
- Possibilité d'attribuer une adresse IP spécifique pour l'entrée Kubernetes
  Les utilisateurs peuvent attribuer une adresse IP à des entrées à l'aide de l'option `http_and_https_ingress_ip` dans NCP configMap.
- Possibilité de définir X-Forwarded-for pour l'entrée Kubernetes
- Possibilité de définir le délai d'expiration de la persistance d'entrée Kubernetes
  Une option de NCP configMap, l7_persistence_timeout, a été ajoutée pour contrôler le délai d'expiration sur le profil de persistance pour les serveurs virtuels de couche 7 sauvegardant des entrées Kubernetes.
- Prise en charge du service Kubernetes de type NodePort
  NodePort permet d'accéder à un service Kubernetes depuis l'extérieur du cluster. kube-proxy configure automatiquement l'hôte de VM pour qu'il relaie le trafic vers l'espace. La règle iptables appropriée doit être configurée sur l'hôte de VM pour permettre le transfert (par exemple, `iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT`).
  Si des espaces cibles sont isolés par la stratégie réseau Kubernetes, l'administrateur doit configurer la stratégie réseau afin d'autoriser le trafic depuis le CIDR IP de l'hôte à accéder au service dans l'espace, puis NCP ajoute automatiquement les règles de pare-feu respectives pour autoriser le

trafic à passer.

Conditions de compatibilité

Produit	Version
Mosaïque NCP/NSX-T pour PAS	2.4.1
NSX-T	2.3.1, 2.4.0.1, 2.4.1
Kubernetes	1.13, 1.14
OpenShift	3.11
Système d'exploitation de machine virtuelle sur hôte Kubernetes	Ubuntu 16.04, CentOS 7.5, CentOS 7.6
Système d'exploitation de machine virtuelle sur hôte OpenShift	RHEL 7.6
OpenShift BMC	RHEL 7.6
PAS (PCF)	OpsManager 2.5 + PAS 2.5 OpsManager 2.4 + PAS 2.4

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 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 2330811 : lors de la création de services Kubernetes de type LoadBalancer alors que NCP est inactif, les services peuvent ne pas être créés lors du redémarrage de NCP
  Lorsque des ressources NSX-T sont épuisées pour les services Kubernetes de type LoadBalancer, vous pouvez créer des services après la suppression de certains services existants. Toutefois, si vous supprimez et créez les services alors que NCP est inactif, NCP ne parvient pas à créer les services.

  Solution : lorsque des ressources NSX-T sont épuisées pour les services Kubernetes de type LoadBalancer, n'effectuez pas les opérations de suppression et de création lorsque NCP est inactif.

- Problème 2317608 : plusieurs plug-ins CNI non pris en charge
  Kubernetes attend un fichier de configuration CNI de type .conflist contenant une liste de configurations de plug-in. Le kubelet appellera les plug-ins définis dans ce fichier conflist un par un dans l'ordre défini. Actuellement, la version nsx-cf-cni bosh ne prend en charge qu'une seule configuration de plug-in CNI. Tout plug-in CNI supplémentaire remplacera le fichier de configuration CNI existant 10-nsx.conf dans le répertoire cni_config_dir spécifié.

  Solution : aucune. Ce problème est résolu dans NCP 2.5.