

NSX Container Plugin 2.4 リリース ノート

VMware NSX Container Plugin 2.4 | 2019 年 2 月 7 日

本ドキュメントの追加情報およびアップデート情報を定期的に確認してください。

リリース ノートの概要

このリリース ノートには、次のトピックが含まれています。

- [新機能](#)
- [互換性の要件](#)
- [解決した問題](#)
- [既知の問題](#)

新機能

新機能

NSX Container Plugin (NCP) 2.4 には、以下の新しい機能が導入されています。

- VMware-NSX-T タイルのファンデーション名は、オプションとなりました。指定されない場合、PAS 展開の名前に設定されます。
- Kubernetes では、デフォルトで NCP HA が有効となります。
- NCP/nsx_node_agent は、バックエンドの接続エラーで終了します。
connect_retry_timeout 構成オプションが追加されました。これを使用して、NCP/nsx_node_agent が終了する前に NSX Manager、Container Orchestrator Adaptor、または Hyperbus への接続をリカバリする時間を秒単位で設定できます。
- LoadBalancer タイプ サービスのセッション アフィニティをサポートします。
configMap オプションの l4_persistence のほか、NCP では、LoadBalancer タイプ サービスのサービス仕様で SessionAffinity 設定をサポートするようになりました。l4_persistence が「なし」に設定されている場合、サービス仕様の sessionAffinity 設定のみにより、パーシステンスの効果を決定します。これを行わない場合、セッション アフィニティは、LoadBalancer タイプ サービスのすべてで有効になり、ユーザーはサービス仕様で sessionAffinity 設定を使用して、パーシステンス タイムアウトを制御できます。
- タイプが LoadBalancer である Kubernetes サービスの loadBalancerIP 仕様で IP アドレスが指定されている場合、サービスは、この IP アドレスで外部に公開されます。
- NSX Manager クラスターをサポートします。

注：NCP では、SSL パススルーが設定された OpenShift Route および再暗号化ターミネーションを無視します。

互換性の要件

製品	バージョン
PAS 用 NCP/NSX-T タイル	2.4
NSX-T	2.3、2.3.1、2.4

Kubernetes	1.12、1.13
OpenShift	3.10、3.11
Kubernetes ホスト仮想マシン OS	Ubuntu 16.04、RHEL 7.5、7.6、CentOS 7.4、7.5
OpenShift ホスト仮想マシン OS	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 (2.4.0 をのぞく) + PAS 2.4.x (2.4.0 をのぞく)

既知の問題

- 問題 2118515：大規模環境で、NCP による NSX-T のファイアウォール作成に時間がかかる
大規模環境（例：250 台の Kubernetes ノード、5,000 台のポッド、2,500 個のネットワーク ポリシー）で、NCP が NSX-T にファイアウォール セクションとルールを作成する際に数分間かかることがあります。

回避策：なし。ファイアウォール セクションとルールのを作成した後は、パフォーマンスが通常の状態に回復します。

- 問題 2125755：Canary のアップデートおよび段階的なローリング アップデートを実行すると StatefulSet の接続が失われることがある
NCP を現在のリリースにアップデートする前に StatefulSet が作成されている場合、Canary のアップデートおよび段階的なローリング アップデートを実行すると StatefulSet の接続が失われることがあります。

回避策：NCP を現在のリリースにアップグレードした後に StatefulSet を作成します。

- 問題 2131494：Ingress のクラスを nginx から nsx に変更しても NGINX Kubernetes Ingress が動作を続ける
NGINX Kubernetes Ingress の作成時、NGINX はトラフィック転送ルールを作成します。Ingress のクラスを他の値に変更すると、クラスの変更に Kubernetes Ingress を削除しても、NGINX はルールを削除せずにルールの適用を継続します。これは NGINX の制限の 1 つです。

回避策：NGINX が作成したルールを削除するには、クラスの値が nginx である Kubernetes Ingress を削除します。その後、再度 Kubernetes Ingress を作成します。

- タイプが ClusterIP の Kubernetes サービスの場合、クライアント IP アドレス ベースのセッション アフィニティがサポートされない
NSX Container Plug-in (NCP) ではタイプが ClusterIP の Kubernetes サービスの場合、クライアント IP アドレス ベースのセッション アフィニティがサポートされません。

回避策：なし

- タイプが ClusterIP の Kubernetes サービスの場合、ヘアピンモード フラグがサポートされない
NSX Container Plug-in (NCP) ではタイプが ClusterIP の Kubernetes サービスの場合、ヘアピンモード フラグがサポートされません。

回避策：なし

- 問題 2193901：1 つの Kubernetes ネットワーク ポリシー ルールに対して複数の PodSelector または複数の NsSelector を指定できない
複数のセレクトクを適用することは、特定のポッドからの受信トラフィックでのみ許可されます。

回避策：代わりに、単独の PodSelector または NsSelector で matchLabels と matchExpressions を組み合わせて使用します。

- **問題 2194646**：NCP が停止しているときはネットワーク ポリシーを更新できない
NCP が停止しているときにネットワーク ポリシーを更新すると、NCP が復帰したとき、そのネットワーク ポリシーの宛先 IPset が不正確になります。

回避策：NCP が動作しているときにネットワーク ポリシーを作成し直します。

- **問題 2192489**：PAS ディレクタ設定で「BOSH DNS server」を無効にした後でも、Bosh DNS サーバ (169.254.0.2) がコンテナの resolve.conf ファイルに表示される
PAS 2.2 を実行している PAS 環境の PAS ディレクタ設定で「BOSH DNS server」を無効にした後でも、Bosh DNS サーバ (169.254.0.2) がコンテナの resolve.conf ファイルに表示されます。これにより、完全修飾ドメイン名を指定した ping コマンドの実行にかかる時間が長くなります。この問題は、PAS 2.1 では発生しません。

回避策：なし。これは PAS の問題です。

- **問題 2194367**：独自のルーターを展開する PAS 分離セグメントが NSX-T タイルでサポートされない
NSX-T タイルが独自の GoRouters および TCP ルーターを展開する Pivotal Application Service (PAS) 分離セグメントでは機能しません。これは、NCP がルーター仮想マシンの IP アドレスを取得して、ルーターから PAS アプリケーション コンテナへのトラフィックを許可する NSX ファイアウォール ルールを作成できないためです。

回避策：なし。

- **問題 2199504**：NCP が作成する NSX-T リソースの表示名が 80 文字までに制限される
NCP がコンテナ環境のリソース用に NSX-T リソースを作成するとき、クラスタ名、ネームスペースまたはプロジェクトの名前、およびコンテナ環境内でのリソースの名前を結合して、その NSX-T リソースの表示名が生成されます。この表示名は、長さが 80 文字を超える場合、80 文字に切り詰められます。

回避策：なし

- **問題 2199778**：NSX-T 2.2 では、名前が 65 文字を超える Ingress、Service、Secret はサポートされない
NSX-T 2.2 で use_native_loadbalancer が True に設定されている場合、Ingress によって参照される Ingress、Secret、Service、およびタイプが LoadBalancer の Service の名前は、65 文字以内にする必要があります。これを守らない場合、Ingress または Service が正しく機能しません。

回避策：Ingress、Secret、または Service を設定するときは、65 文字以内の名前を指定します。

- **問題 2065750**：NSX-T CNI パッケージのインストールがファイルの競合で失敗する
kubernetes がインストールされている RHEL 環境で yum localinstall または rpm -i を使用して NSX-T CNI パッケージをインストールすると、kubernetes-cni パッケージのファイルとの競合を示すエラーが発生します。

回避策：rpm -i --replacefiles nsx-cni-2.3.0.xxxxxxxx-1.x86_64.rpm コマンドを使用して NSX-T CNI パッケージをインストールします。

- **問題 2224218**：サービスまたはアプリケーションの削除後、SNAT IP アドレスが IP アドレス プールに戻るのに 2 分かかる
サービスまたはアプリケーションを削除し、2 分以内に再作成すると、新しい SNAT IP アドレスが IP アドレス プールから取得されます。

回避策：同一の IP アドレスをもう一度使用する場合は、サービスまたはアプリケーションの削除後、2 分間待ってから再作成します。

- 問題 2218008：複数の Kubernetes クラスタで同一の IP アドレス ブロックを使用するように設定すると、接続の問題が発生する
複数の Kubernetes クラスタで同一の IP アドレス ブロックを使用するように設定すると、一部のポッドが他のポッドまたは外部ネットワークと通信できなくなります。

回避策：複数の Kubernetes クラスタで同一の IP アドレス ブロックを使用しないように設定します。

- 問題 2263536：タイプが NodePort の Kubernetes サービスでトラフィックが転送されない
タイプが NodePort のサービスでは、Kubernetes ノードがルーターとして動作し、トラフィックがクラスタ外部からポッドに転送されます。ルーターとして動作するノードをセットアップすると、トラフィックが通過できるように iptables 内のルールが正しく設定されない場合があります。

回避策：次のコマンドを実行して、iptables に手動でルールを追加します。

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

これは、「externalTrafficPolicy: Cluster」が設定された NodePort サービスのみで動作します。

「externalTrafficPolicy: Local」が設定されている場合は動作しません。