

NSX Container Plugin 2.4.1 リリース ノート

VMware NSX Container Plugin 2.4.1 | 2019 年 5 月 9 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

NSX Container Plugin (NCP) 2.4.1 には、以下の新しい機能が導入されています。

- 健全性チェックで単一の分散ファイアウォール セクションを使用
クラスタごとに 1 つの分散ファイアウォール セクションを使用し、稼動状態と準備状態の検証が設定されているポッドに必要なすべてのファイアウォール ルールを追加します。分散ファイアウォール セクションには最大 1,000 個までのルールを記述できるため、1 つのクラスタ内で稼動状態または準備状態の検証を設定できるポッド数は 1,000 に制限されます。
- NSX Node Agent で `privsep` デーモンの予期しない終了を処理
予期しない `privsep` デーモンの終了を処理し、リカバリするように NSX Node Agent の機能が拡張されました。
- Kubernetes サービスのオートスケーリングに最大数を定義
新しい NCP configMap オプションの `max_allowed_virtual_servers` を使用して、クラスタ内で作成できる仮想サーバの最大数を定義できます。
- Kubernetes Ingress への特定の IP アドレスの割り当て
NCP configMap の `http_and_https_ingress_ip` オプションを使用して、Ingress に IP アドレスを割り当てることができます。
- Kubernetes ingress への X-Forwarded-For の設定
- Kubernetes Ingress へのパーシステンス タイムアウトの設定
NCP configMap に `l7_persistence_timeout` オプションが追加されました。これにより、Kubernetes Ingress をバックエンドレイヤー 7 仮想サーバのパーシステンス プロファイルで、タイムアウトを制御できるようになりました。
- NodePort タイプの Kubernetes サービスのサポート
NodePort を使用すると、クラスタの外部から Kubernetes サービスにアクセスできます。kube-proxy は、ポッドへのトラフィックをリレーするように仮想マシンのホストを自動的に構成します。転送を行うには、仮想マシンのホストに適切な iptables ルールを設定する必要があります (例: `iptables -I FORWARD -m conntrack --ctstate RELATED,ESTABLISHED -j ACCEPT`)。ターゲット ポッドが Kubernetes ネットワーク ポリシーで隔離されている場合、管理者は、ホスト IP CIDR からのトラフィックがポッドのサービスにアクセスできるようにネットワーク ポリシーを構成する必要があります。これにより、NCP が必要なファイアウォール ルールを自動的に追加して、トラフィックの通過を許可します。

互換性の要件

製品	バージョン
PAS 用 NCP/NSX-T タイル	2.4.1
NSX-T	2.3.1、2.4.0.1、2.4.1
Kubernetes	1.13、1.14
OpenShift	3.11
Kubernetes ホスト仮想マシン OS	Ubuntu 16.04、CentOS 7.5、CentOS 7.6
OpenShift ホスト仮想マシン OS	RHEL 7.6
OpenShift BMC	RHEL 7.6
PAS (PCF)	OpsManager 2.5 + PAS 2.5 OpsManager 2.4 + PAS 2.4

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、クラスの変更後に 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 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 2330811：NCP の停止中に LoadBalancer タイプの Kubernetes サービスを作成すると、NCP の再起動後にサービスが作成できないことがある

LoadBalancer タイプの Kubernetes サービスで使用可能な NSX-T リソースがなくなった場合、既存のサービスの一部を削除すると、新しいサービスを作成できます。ただし、NCP の停止中にサービスを削除して作成すると、NCP は新しいサービスを作成できなくなります。

回避策：LoadBalancer タイプの Kubernetes サービスで使用可能な NSX-T リソースがなくなった場合、NCP の停止中に削除と作成の両方を行わないでください。

- 問題 2317608：複数の CNI プラグインはサポートされていない

Kubernetes は、プラグインの構成リストを含む .conflist タイプの CNI 構成ファイルを想定しています。

Kubelet は、この conflist ファイルで定義されているプラグインをその定義順に 1 つずつ呼び出します。現在、nsx-cf-cni bosh リリースでは、1 つの CNI プラグイン構成のみがサポートされています。追加の CNI プラグインが存在すると、指定された cni_config_dir にある CNI 構成ファイル 10-nsx.conf が上書きされます。

回避策：なし。この問題は、NCP 2.5 で修正されました。