



VMware NSX-T Data Center 2.3.1 および NSX Container Plug-in 2.3.1 リリース ノート

VMware NSX-T Data Center 2.3.1 | 2018 年 12 月 20 日

VMware NSX Container Plug-in 2.3.1 | 2018 年 11 月 8 日

本リリース ノー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-T Data Center 2.3.1 の新機能

NSX-T Data Center 2.3.1 は、これまでのリリースで見つかった問題を数多くを解決したメンテナンス リリースです。NSX-T Data Center 2.3 の新機能と、NSX-T Data Center 2.3.1 の既知の問題および解決した問題については、[NSX-T Data Center 2.3 リリース ノート](#)を参照してください。

NSX Container Plug-in 2.3.1 の新機能

NSX Container Plug-in (NCP) 2.3.1 は、これまでのリリースで見つかった問題を数多く解決したメンテナンス リリースであり、次の新機能を利用できます。

- Kubernetes LoadBalancer サービスに対応した NSX-T ロード バランサの自動スケーリング。Kubernetes LoadBalancer サービスに仮想サーバを追加する場合、新しい NSX-T ロード バランサが作成されます。

NSX-T Data Center 2.3.1 で推奨される ESXi バージョン

- ESXi 6.5 P03 ビルド 10884925
- ESXi 6.7 U1 ビルド 10302608

NCP 2.3.1 の互換性要件

製品	バージョン
PAS 用 NCP/NSX-T タイル	2.3.1
NSX-T	2.2、2.3、2.3.1
Kubernetes	1.11、1.12
OpenShift	3.10、3.11
Kubernetes ホスト仮想マシン OS	Ubuntu 16.04、RHEL 7.4、7.5
OpenShift ホスト仮想マシン OS	RHEL 7.4、7.5
PAS (PCF)	OpsManager 2.2.0 + PAS 2.2.0 OpsManager 2.3.x + PAS 2.3.x

解決した問題

解決した問題には、次のトピックが含まれます。

- [NSX-T Data Center 2.3.1 で解決された問題](#)
- [NCP 2.3.1 で解決された問題](#)

NSX-T Data Center 2.3.1 で解決された問題

- 問題 2238957：ESXi ホストを再起動した後でも、古いハイパーバス ポートがクリーンアップされない
ホストで実行中のコンテナ仮想マシンをパワーオフせずに ESXi ホストを再起動すると、ハイパーバス ポートが、想定どおりにクリーンアップされません。
- 問題 2226523：CLI コマンド「get debug bgp」が機能しない
CLI コマンド「get debug bgp」を実行しても、出力されません。
- 問題 2241365：NSX-T Data Center 2.2 から 2.3 へのアップデート中に、ALG（アプリケーション レベル ゲートウェイ）トラフィックを使用し、ファイアウォールで保護された仮想マシンのネットワーク接続が失われる
NSX-T Data Center 2.2 から 2.3 へのアップデート中、仮想マシンは、NSX-T Data Center 2.2 を実行するホストから NSX-T Data Center 2.3 を実行するホストへと移行します。仮想マシンがファイアウォールで保護され、ALG トラフィックを使用する場合、移行後にネットワーク接続が失われます。
- 問題 2241378：VPN トンネルでフラッピングが行われ、トラフィックがドロップする
VPN トンネルで、ファイアウォール ルールにドロップが設定され、トラフィックが断片化されている場合、フラッピングが行なわれ、トラフィックがドロップします。
- 問題 2232034：MAC アドレスの数が 1,024 個を超える分散論理ルーター ブリッジがホストに設定されている場合、サポート バンドルの作成中に ESXi ホストがクラッシュする
vm-support またはコマンド「net-bridge --mac-address-table \$bridgeName」を実行すると、エントリを転送するブリッジが多数の場合、バッファ オーバーフローが発生します。
- 問題 2216746：vMotion または仮想マシンのパワーオン時に、仮想マシンの NIC が切断され、仮想マシンのネットワーク接続が失われる
多数の仮想マシンでパワーオンまたは vMontion を同時に実行すると、一部の仮想マシンの NIC が切断され、ネットワーク接続が失われます。
- Issue 2216747：仮想マシンの vMotion を実行すると、ポートが切断する

NFS にストレージがある仮想マシンで vMotion を実行すると、仮想マシンのネットワーク接続が失われます。これは HA によって発生する場合があります。

- **問題 2229210： 論理スイッチ ポートの作成と削除を繰り返し行くと、NSX Controller でメモリリークが発生する**
この問題は、論理スイッチ ポートが削除される際に、SpoofGuard ドメイン オブジェクトが削除されないことが原因で発生します。
- **問題 2220560： metricRegistry に多数のイベント ログが生成されると、NSX Controller でメモリリークが発生する**
NSX Controller で多数のトランザクションが処理されると、多量のログが生成され、メモリ リークが発生します。
- **問題 2221286： 仮想マシンの接続が停止してすぐに、ARP エントリが期限切れとなる**
この問題により、仮想マシンは一定の時間、アクセス不能になります。
- **問題 2227882： ポリシー ベース VPN が「No active IPsec SA, deleting childless IKE Sa (アクティブな IPsec SA がありません。子 SA がない IKE SA を削除しています)」というエラーとともに停止する**
このエラーとともに、再ネゴシエーションとトラフィック ドロップが発生します。
- **問題 2227885 および 2227879： 特定のトラフィック パターンを持つ Edge ノード上の IPsec VPN で、メモリ リークが発生する**
この現象は、宛先 IP アドレスが Edge 所有で、UDP がカプセル化された ESP トラフィック（宛先ポートが 4500 のパケット）を次の期間に受信した場合に発生します。
 - リダイレクト IP アドレスからループバック ポートへの転送情報ベース (FIB) プログラミング後、HCX で使用する PBR リダイレクト ルールがプログラミングされる
 - VPN トンネルの送信元アドレスが見つからない場合 (iked が誤った動作をする、コアダンプが発生したなど)
- **問題 2227890： 論理ポート設定でトンネル ID を変更したにもかかわらず、VLAN ID が変更されない**
API 呼び出しを行って論理ポートのトンネル ID を変更しても、VLAN ID が変更されません。
- **問題 2230277： vMotion 実行中にポートのランタイム データがフラッシュされない**
Storage vMotion の実行中、ESXi 6.5 では、vMotion フレームワークがデータを保存する前に、ポート上のフラッシュされるべきランタイム データに問題が発生します。
- **問題 2236206： メモリ リークが原因で、ESXi トランスポート ノードがネットワーク接続を失うことがある**
この問題により、PKS 環境の ESXi トランスポート ノードでネットワーク接続が失われる場合があります。

NCP 2.3.1 で解決された問題

- **問題 2216781： タグの値が NCP 2.2.x では 65 文字、NCP 2.3.0 では 256 文字に制限されている**
NCP 2.3.1 では、以下のロード バランサに関連する Kubernetes リソースで、タグの最大値を超える名前をサポートしています。
 - LoadBalancer サービス
 - 入力方向 (Ingress)
 - Ingress の仕様で指定される Secret
 - Ingress の仕様で指定される Service
- **問題： 2217051： LoadBalancer サービスの loadBalancerIP が変更された後でも仮想サーバの IP アドレスが更新されない**

LoadBalancer サービスの作成後、サービスの loadBalancerIP の値を変更しても、NSX-T ロード バランサの仮想サーバの IP アドレスに変更が反映されません。

- **問題 2216085**：ネームスペースの削除後、NSX-T ロード バランサのルールとプールが削除されない
Ingress リソースと NSX-T ロード バランシングを設定すると、NSX-T の仮想サーバ、プール、およびルールが作成されます。Ingress リソースを含んでいるネームスペースを削除すると、一部のルールとプールは NSX-T から削除されません。

既知の問題

既知の問題には次の項目が含まれます。

- [NSX-T Data Center 2.3.1 の既知の問題](#)
- [NCP 2.3.1 の既知の問題](#)

NSX-T Data Center 2.3.1 の既知の問題

- **問題 2235834**：flow-cache が有効な場合の RDP および HTTPS トラフィックの問題
flow-cache が有効な場合、RDP および HTTPS トラフィックに問題が発生する場合があります。

回避策：Edge ノードで、次のコマンドを実行して flow-cache を無効にします。
 - set dataplane flow-cache disabled
 - restart service dataplane
- **問題 2227975**：Edge ノードを経由する TCP トラフィックが断続的にドロップする
Edge ノードを経由する TCP トラフィックが断続的にドロップします。ICMP トラフィックに影響はありません。

回避策：Edge ノードで、次のコマンドを実行して flow-cache を無効にします。
 - set dataplane flow-cache disabled
 - restart service dataplane

NCP 2.3.1 の既知の問題

- **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、クラスの色が 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 2194845：PAS Cloud Foundry V3 API の機能「multiple processes per app」がサポートされない**
PAS Cloud Foundry V3 API の `v3-push` を使用して複数のプロセスを持つアプリケーションをプッシュしても、NSX Container Plug-in (NCP) はこれらのプロセスに対して、デフォルトの 1 つ以外に論理スイッチポートを作成しません。この問題は、NCP 2.3.0 およびそれ以前のリリースで発生します。

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**
複数のセレクトラを適用することは、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。