

# VMware NSX-T Data Center 2.3 リリース ノート

VMware NSX-T Data Center 2.3 | 2018 年 9 月 18 日 | ビルド 10085361

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](#)
- [互換性とシステム要件](#)
- [全般的な動作変更](#)
- [API リファレンス情報](#)
- [解決した問題](#)
- [既知の問題](#)

## 新機能

NSX-T Data Center 2.3 は、クラウドとコンテナに新しいマルチハイパーバイザー プラットフォームを提供するアップデートリリースです。

NSX-T Data Center 2.3 リリースでは、次の新機能および機能拡張が提供されます。

### ベアメタル ホストでの NSX-T Data Center サポートの導入

ベアメタルのサポートには、ベアメタル サーバで実行する Linux ベースのワークロードや、ハイパーバイザーを使用せずにベアメタル サーバで実行するコンテナが含まれます。NSX-T Data Center は Open vSwitch を利用して、Linux ホストを NSX-T Data Center トランスポート ノードとして使用できるようにします。

- **ベアメタル サーバのサポート**：RHEL 7.4、CentOS 7.4、Ubuntu 16.0.4 オペレーション システムを実行するネイティブ コンピュート ワークロードが含まれます。これにより、ユーザーは VLAN やオーバーレイ バックিং接続を介してベアメタル コンピュート ワークロードを接続できるほか、仮想から物理への通信フローや物理から物理への通信フローに対してマイクロセグメンテーション ポリシーを適用（ステートフル レイヤー 4 を適用）することができます。
- **ベアメタルの Linux コンテナのサポート**：RHEL 7.4 または RHEL 7.5 を搭載したベアメタルの Linux ホスト上で、RedHat OpenShift Container Platform を使用して Docker Containers を実行します。

### NSX Cloud の機能強化

- **AWS 環境のサポート**：AWS 環境での NSX Cloud のサポート。
- **Azure VNET での NSX Agent の自動プロビジョニング**
- **オンプレミスとパブリック クラウド間の VPN サポート**：NSX Cloud Public Cloud Gateway 内部に、API を使用する組み込みの VPN 機能が含まれています。VPN 機能を使用して、以下の間に IPsec リンクを作成することができます。
  - 管理対象のコンピュート Amazon VPC/Azure VNET と、トランジット Amazon VPC/Azure VNET のサードパーティ製サービスの仮想マシン

- 管理対象の Amazon VPC/Azure VNET と、オンプレミス VPN デバイス
- NSX Cloud エージェントの OS サポートの拡張：NSX Cloud は、パブリック クラウドで RHEL 7.5 オペレーティング システムをサポートしています。

## セキュリティ サービスのサポート

### ルーティング ティアでのサービス挿入の導入

- Tier-0 および Tier-1 ルーターでのサービス挿入のサポート：サードパーティ製セキュリティ ソリューションのオンボーディング、Tier-0、Tier-1、および両方での High Availability のサードパーティ製セキュリティ ソリューションの展開、リダイレクト ポリシーを経由したサードパーティ製セキュリティ ソリューションの挿入などの機能があります。  
NSX-T Data Center でのサードパーティ製ソリューションの最新の認定状態については、「VMware Compatibility Guide – Network and Security」を参照してください。

### 分散ファイアウォールの強化

- NSX Edge ファイアウォールで複数セクションをサポート：管理を簡素化するため、NSX Edge ファイアウォールに複数セクションを追加します。
- ファイアウォールのルール ヒット数およびルール ポピュラリティ 指数：ルールの使用を監視し、未使用ルールを迅速に特定してクリーンアップします。
- ファイアウォール セクションのロック：複数のセキュリティ管理者がファイアウォールを同時に操作できます。
- グループ オブジェクト：指定された 5 つのタグがすべて一致した場合にオブジェクトをグループに追加します（以前は 2 つのタグで追加）。
- タグの長さ：タグの長さの値を 65 から 256 に、タグ範囲を 20 から 128 に拡大します。
- アプリケーションの検出：ゲスト仮想マシン内にインストールされているアプリケーションを検出し、分類します。ユーザーによるカスタム分類も可能です。アプリケーションの詳細には、実行可能ファイル、ハッシュ、発行元情報、インストール日時が含まれます。

## ネットワークおよび NSX Edge サービスのサポート

- N-VDS の拡張データ パス モード用のオーバーレイのサポート：vSphere 6.7 と連携することで、NSX-T Data Center 2.3 用の N-VDS の拡張データ パス モードでは、高パフォーマンスのデータ パスを必要とする NFV 型のワークロードがサポートされます。
- 中央集中型サービス ポートでのステートフル NAT およびファイアウォール サービスのサポート
- DNS フォワーダですべての DNS エントリをクリアする API のサポート：指定した DNS フォワーダで、単一の API 呼び出しですべての DNS キャッシュ エントリをクリアする機能を提供します。このコマンドは、DNS サーバの応答が誤っているときや、DNS サーバの修正後に DNS エントリのタイムアウトの待機を回避する際に有効です。
- ロード バランサの強化
  - 事前定義された暗号化リストのサポート：セキュリティ強化または高パフォーマンスのための HTTPS VIP の事前定義された SSL プロファイル
  - ロード バランサ ルールの強化：新しいロード バランサ ルール、ヘッダーの削除アクション、SSL 一致条件、条件一致での変数割り当ての追加。
  - スタンドアローン サービス ルーターでのロード バランサのサポート：ルーター ポートのないサービス ルーターにロード バランシング サービスを展開する機能を提供します。

## ユーザー インターフェイスの強化

- 新しい言語のサポート：ユーザー インターフェイスは、英語、ドイツ語、フランス語、日本語、韓国語、簡体字中国語、繁体字中国語、スペイン語で利用できるようになりました。
- ナビゲーションおよびホーム画面の強化：新しいホーム画面の主な変更点は、検索と、一目で分かるシステム機能です。
- 検索の強化：検索では、ホーム画面から利用できる予測入力機能を追加しました。

- ネットワーク トポロジの可視化：NSX Policy Manager は、グループ間、仮想マシン間、プロセス間の通信を監視する機能を提供します。論理スイッチ、ポート、ルーター、NSX Edge などのネットワーク オブジェクト間の関係を可視化できます。

## 操作とトラブルシューティングのサポート

- インストールとアップグレードの強化
  - ステートレスな vSphere 環境での NSX-T Data Center：vSphere Auto Deploy とホスト プロファイルを使用するステートレスな ESXi ホストのサポートにより、追加の展開オプションを可能にします。この機能のサポートには、vSphere 6.7 U1 以降が必要です。
  - 同一の NSX Edge クラスタにおいて NSX Edge 仮想マシンおよびベアメタルの共存をサポート：NSX Edge ノード仮想マシンとベアメタルを同一の NSX Edge クラスタに共存させることが可能になり、NSX Edge ノードでホストされている、ロード バランサなどのサービスのスケーリングが簡素化されました。
  - NSX-T Data Center のモジュラー アップグレード：Upgrade Coordinator でモジュラー アップグレードがサポートされます。新しいリリース バージョンで変更があった NSX-T Data Center コンポーネントのみをアップグレードすることができます。この機能が追加されたことにより、NSX-T Data Center バージョンのパッチ適用による運用上のオーバーヘッドが低減されます。
- 監視とトラブルシューティング
  - KVM ハイパーバイザー用 ERSPAN：KVM 上でポート ミラーリングがサポートされます（ERSPAN Type II および III）。
  - Tier-0 論理ルーター アップリンクで送受信するトレースフローの使用：Tier-0 論理ルーター アップリンクからトレースフロー トラフィックを生成し、Tier-0 論理ルーター アップリンクでのトレースフロー パケットの受信を報告する機能により、トレースフロー レポートに NSX Edge ノードのアップリンク先のインターフェイスを含めることで、トラブルシューティング操作を簡素化しました。
  - ベアメタル Edge ノードの DPDK ポートをシャットダウンする CLI のサポート：ベアメタル NSX Edge ノードで DPDK が要求するポートをシャットダウンする機能により、インストールおよびトラブルシューティング時のポートの分離を簡素化しました。

## OpenStack Neutron プラグインのサポート

OpenStack Upstream Queens リリース以降では、以下の機能がサポートされています。

- Neutron プラグインによって拡張データパスがバックリングするオーバーレイ論理スイッチをプロビジョニングする機能：NSX Neutron プラグインで、オーバーレイに拡張データパス モードを利用する機能を提供します。以前、この機能は VLAN のみに提供されていました。このサポートにより、OpenStack 環境の他に、NFV 関連のワークロードなどの拡張データパス パフォーマンスを利用することができます。
- NSX 製品と OpenStack の共存をサポート：NSX Neutron プラグインにより、OpenStack 実装環境での NSX Data Center for vSphere と NSX-T Data Center の同時管理をサポートするようになりました。
- OpenStack での VPN as a Service (VPNaaS) 機能：VPN 機能セットを導入した OpenStack の Neutron 拡張機能で、OpenStack VPNaaS がサポートされます。

## NSX Container Plug-in (NCP) のサポート

- NSX-T Data Center をインストールする Concourse のパイプライン
- ロード バランサの SNAT IP のアノテーション：ロード バランサの SNAT IP は、Kubernetes サービス タイプ LoadBalancer に、アノテーション `ncp/internal_ip_for_policy: <SNAT IP>` が付加され、サービス状態：`status.loadbalancer.ingress.ip: [<SNAT IP>, <Virtual IP>]` に追加されます。この IP アドレスは、この IP CIDR を許可するネットワーク ポリシーの作成に使用できます。
- Kubernetes ネットワーク ポリシーの強化：Kubernetes ネットワーク ポリシー ルールを使用して異なるネームスペースからポッドを選択する機能が提供されます。
- Kubernetes Load Balancer/SNAT アノテーションの強化
  - NCP でサービスにロード バランサを設定できなかった場合、サービスにはアノテーション `ncp/error.loadbalancer` が付加されます。
  - NCP でサービスに SNAT IP を設定できなかった場合、サービスにはアノテーション

ncp/error.snat が付加されます。

- NSX-T Data Center Load Balancer for Kubernetes Ingress と OpenShift Route のセッション パーシステンス
- スクリプトのクリーンアップの強化

## 互換性とシステム要件

互換性とシステム要件の詳細については、『[NSX-T Data Center インストール ガイド](#)』を参照してください。

ステートレスな vSphere 環境での NSX-T Data Center : vSphere Auto Deploy とホスト プロファイルを使用するステートレスな ESXi ホストの場合、vSphere 6.7 U1 以降が必要です。

NCP 互換性の要件：

製品	バージョン
NCP / NSX-T Data Center Tile for PAS	2.3.0
NSX-T Data Center	2.2、2.3
Kubernetes	1.10、1.11
OpenShift	3.9、3.10
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、RHEL 7.5
PAS (PCF)	OpsManager 2.1.x + PAS 2.1.x (PAS 2.1.0 を除く) OpsManager 2.2.0 + PAS 2.2.0

## 全般的な動作変更

Tier-1 論理ルーターのデフォルトの HA モードがプリエンプティブから非プリエンプティブに変更

Tier-1 論理ルーターの作成時に、デフォルトの HA モードはプリエンプティブで、優先 NSX Edge ノードがオンラインに復帰した際のトラフィック低速化の原因となっていました。新しいデフォルト HA モードが非プリエンプティブになったことで、このトラフィック低速化は新規に作成した Tier-1 論理ルーターで発生しなくなりました。既存の Tier-1 論理ルーターはこの変更の影響を受けません。

トランスポート ノードから NSX Controller への通信の変更

トランスポート ノードから NSX Controller への通信が変更されたため、NSX-T 2.2 以降では TCP ポート 1235 を開く必要があります。『[NSX-T Data Center インストール ガイド](#)』を参照してください。

NSX-T 2.1 から上位のバージョンにアップデートする場合は、TCP ポート 1234 と 1235 を開く必要があります。アップデートが完了すると、TCP ポート 1235 が使用されます。

## API リファレンス情報

「[NSX-T Data Center and NSX Policy deprecated API calls and properties](#)」を参照してください。

最新の API リファレンスは、[NSX-T Data Center 製品情報](#)でご確認ください。

## 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。

- [解決した一般的な問題](#)
- [インストールに関する解決した問題](#)
- [NSX Manager に関する解決した問題](#)
- [NSX Edge に関する解決した問題](#)
- [論理ネットワークに関する解決した問題](#)
- [セキュリティ サービスに関する解決した問題](#)
- [ロード バランサに関する解決した問題](#)
- [ソリューションの相互運用性に関する解決した問題](#)
- [運用および監視サービスに関する解決した問題](#)
- [アップグレードに関する解決した問題](#)
- [API に関する解決した問題](#)
- [NSX Container Plug-in \(NCP\) に関する解決した問題](#)

## 解決した一般的な問題

- **問題 1775315**：Postman クライアントを Web ブラウザから開くと、CSRF 攻撃が発生する  
Postman、CURL、またはその他の REST クライアントを使用する API 呼び出しでは、XSRF-TOKEN ヘッダーとその値を明示的に指定する必要があります。リモート認証または /api/session/create（ローカル認証）の呼び出しを使用する最初の API 呼び出しでは、XSRF-Token が応答オブジェクトに格納されて伝達されます。以降の API 呼び出しでは、要求の一部として XSRF-TOKEN ヘッダー内にトークン値が保持されます。
- **問題 1989412**：NSX Manager に接続できないときに行ったドメイン削除が、接続復旧後に反映されない  
NSX Manager に接続できない状態でドメインをポリシーから削除した場合、NSX Manager への接続が復旧した後も、削除したドメインに対するファイアウォールおよびルールが残ったままになります。
- **問題 2018478**：ダッシュボードからウィジェットを削除すると、スタック トレース エラーによってクラッシュする  
複数のウィジェットのうち 1 つを削除するなど、カスタム ダッシュボード ユーザー インターフェイスの変更を行うと、スタック トレース エラーによってユーザー インターフェイスがクラッシュします。
- **問題 1959647**：データベース サーバ エイリアス名を使用して DSN を作成すると、vCenter Server のインストールに失敗することがある  
データベース サーバ エイリアス名を使用して DSN を作成すると、外部 Microsoft SQL データベースを使用する vCenter Server のインストールに失敗します。インベントリ サービスのインストール中に次のエラーが表示されます：invsvc の起動中にエラーが発生しました。

## インストールに関する解決した問題

- **問題 1739120**：管理プレーン、または管理プレーン内の Proton サービスの再起動後、ファブリック ノードの展開状態が停止する  
ファブリック ページで新しいサポート対象ホストをホストの認証情報と共に追加すると、状態が[インストールが進行中です]へと変わります。管理プレーン、または管理プレーン内の Proton サービスの再起動後、ホストの展開状態は[インストールが進行中です]または[アンインストールが進行中です]のまま変わりなくなります。
- **問題 1944669**：KVM に NSX-T Data Center アプライアンスを展開する際に正確なメモリ サイズの指定が必要になる  
NSX-TData Center アプライアンスは、さまざまな RAM 設定を使用して、小、中、大のサイズで ESX に展開できます。しかし、NSX-TData Center アプライアンスを KVM に展開する際には、RAM の割り当ては明示的に設定する必要があります。
- **問題 1944678**：NSX-T 統合アプライアンスを展開する際に有効なロール タイプが必要になる  
NSX-T 統合アプライアンスをロール指定なしで、または無効なロール タイプを指定して KVM に展開すると、すべてのロールが有効になったサポート対象外の設定で展開されます。

- 問題 1958308：ホストがロックダウン モードの場合、ホストの準備またはトランスポート ノードの作成に失敗する  
ホストがロックダウン モードの場合、ホストの準備またはトランスポート ノードの作成に失敗します。次のエラー メッセージが表示されます。この操作の実行権限は拒否されました。

## NSX Manager に関する解決した問題

- 問題 1954923：管理プレーンのアップグレード中に、論理スイッチに接続した仮想マシンの vMotion に失敗する  
管理プレーンのアップグレード中に、論理スイッチに接続した仮想マシンに対して vMotion を実行すると、移行に失敗します。
- 問題 1954927：NSX Manager をリストアした後、vCenter Server で管理されていない新しい ESX ホストを NSX Manager に登録し、その仮想マシンが既存の論理スイッチに接続した場合、ESX ホストの管理対象オブジェクト ブラウザ (MOB) で仮想マシンの MAC アドレスが空白になる  
NSX Manager をリストアした後、vCenter Server で管理されていない新しい ESX ホストを NSX Manager に登録し、その仮想マシンが既存の論理スイッチに接続した場合、ESX ホストの管理対象オブジェクト ブラウザ (MOB) で仮想マシンの MAC アドレスが空白になります。
- 問題 1978104：Internet Explorer 11 で NSX Manager ユーザー インターフェイスの一部のページにアクセスできない  
Windows マシンで Internet Explorer を使用している場合は、ダッシュボード、[はじめに] ワークフロー、NSX Manager ユーザー インターフェイスのロード バランサ ページにアクセスできません。

- 問題 1954986：ライセンス キーがユーザー インターフェイスから削除されても、キーがログに表示される

NSX のライセンス キーは /var/log/syslog では次のように表示されます。

```
<182>1 2017-03-24T05:03:47.008Z bb-mgr-221 NSX - SYSTEM [nsx@6876 audit="true"
comp="nsx-manager" reqId="3d146f2b-fa34-460f-8ac3-56e3c7326015"
subcomp="manager"] UserName:'admin', ModuleName:'License',
Operation:'DeleteLicense, Operation status:'success', New value: ["
<license_key>"] <182>1 2017-03-24T05:03:47.009Z bb-mgr-221 NSX - - [nsx@6876
audit="true" comp="nsx-manager" subcomp="manager"] UserName:'admin',
ModuleName:'Batch', Operation:'RegisterBatchRequest, Operation status:'success',
New value: [{"atomic":false} {"request":
[{"method":"DELETE","uri":"/v1/licenses/<license_key>"}]}}
```

ログを外部のログ コレクタに送信するようにアプライアンスが設定されている場合、外部のログ コレクタで認証されているユーザーにもキーの値が表示されます。

- 問題 1956055：管理プレーンのデータストアが停止していると、ローカル管理ユーザーがユーザー インターフェイスからテクニカル サポート バンドルにアクセスできない  
管理プレーンのデータストアが停止していると、ローカル管理ユーザーがユーザー インターフェイスからテクニカル サポート バンドルにアクセスできない
- 問題 1957165：10,040 件以上のレコードを含む検索結果セットの最後のページを読み込むとエラーが発生する  
検索クエリで 10,040 以上のオブジェクトを返す可能性がある大規模環境では、結果セットの最後の数件のレコードを読み込むときに、エラーが発生する場合があります。

## NSX Edge に関する解決した問題

- 問題 1762064：NSX Edge の再起動直後に、NSX Edge の VTEP IP アドレス プールとアップリンク プロファイルを設定すると、VTEP BFD フォワーディング検出セッションがアクセス不能になる  
NSX Edge の再起動後、ブローカによる NSX Edge 接続のリセットに時間がかかります。

## 論理ネットワークに関する解決した問題

- **問題 1966641**：ホストを追加してトランスポート ノードとして設定した場合、そのノードが論理スイッチの一部でなければノードの状態が「停止」と表示される  
新しいホストを追加してトランスポート ノードとして設定した場合、または NSX-T 2.1 へのアップグレード プランを設定する際、トランスポート ノードが論理スイッチの一部でなければ、ユーザー インターフェイスにトランスポート ノードの状態が「停止」と表示されます。
- **問題 2015445**：アクティブなサービス ルーター上のファイアウォールの状態が、新しくアクティブになったサービス ルーター上で複製されない場合がある  
テナント論理ルーター (TLR) では、NSX Edge1 から NSX Edge2 へのフェイルオーバー、および NSX Edge2 から NSX Edge1 へのフェイルオーバーが複数発生してしまうことがあります。ファイアウォールまたは NAT フローの状態は、アクティブおよびスタンバイ TLR サービス ルーターの間で同期されます。TLR がノン プリエンプティブ フェイルオーバー モードで設定されていると、同期は 1 番目のフェイルオーバーの前に実行されますが、2 番目のフェイルオーバーの前には実行されません。このため、2 番目のフェイルオーバーでは TCP トラフィックがタイムアウトになることがあります。この問題はプリエンプティブ モードで設定された TLR では発生しません。
- **問題 2016629**：RSPAN\_SRC ミラー セッションが仮想マシン移行後に停止する  
RSPAN\_SRC ミラー セッション用に割り当てられたポートに仮想マシンを接続し、この仮想マシンを別のハイパーバイザーに移行する際、必要な物理 NIC が移行先のハイパーバイザーのネットワークに存在しないと、そのポートに RSPAN\_SRC ミラー セッションが設定されません。そのため、ポートに接続障害が発生しますが、vMotion の移行プロセスは正常に完了します。
- **問題 1620144**：トランスポート ノードが削除されたあとでも、NSX-T Data Center CLI で **get logical-switches** を実行すると、状態が「稼動中」の論理スイッチが表示される  
この CLI の表示によって、ユーザーが、機能している論理スイッチがあると誤って判断する可能性があります。論理スイッチが表示されても、それらは機能していません。トランスポート ノードが削除されると不透明スイッチは無効になるため、トラフィックは通過しません。
- **問題 1590888**：「イーサネット セクションで選択された論理ポートは、同じ L2 ネットワーク内にのみ適用する必要がある」という警告が表示される  
分散ファイアウォールの場合、イーサネット セクションで、ソースまたはターゲット セクションに論理ポートまたは MAC アドレスが入力されると、「MAC アドレスまたは論理ポートは、同じ論理スイッチに接続されている同じ L2 ネットワーク内の仮想マシン ポートに属している必要がある」という警告が表示されます。現在、警告メッセージは表示されません。
- **問題 1763576**：NSX-T Data Center ネットワーク上に仮想マシンがあっても、ハイパーバイザーをトランスポート ノードとして削除できる  
NSX-T Data Center ネットワークに属するトランスポート ノードに仮想マシンがあっても、そのトランスポート ノードを削除できてしまいます。トランスポート ノードが削除されると、仮想マシンに接続することはできません。
- **問題 1780798**：大規模な環境で、一部のホストがエラー状態になる場合がある  
200 台以上のホスト ノードを抱える大規模環境をしばらく運用した後、一部のホストが NSX Manager と接続できなくなる場合があり、ログに次のエラー メッセージが表示されます。  
2016-12-09T00:57:58Z mpa: [nsx@6876 comp="nsx-esx" subcomp="mpa" level="WARN"]  
Unknown routing key: com.vmware.nsx.tz.\*
- **問題 1954997**：トランスポート ノード上の仮想マシンが論理スイッチに接続していると、トランスポート ノードの削除に失敗する
  1. ファブリック ノードとトランスポート ノードを作成します。
  2. VIF を論理スイッチに接続します。
  3. この状態で、VIF の論理スイッチへの接続を解除せずにトランスポート ノードを削除することはできません。

きません。

- **問題 1958041**：ESX ハイパーバイザーに複数のアップリンクがあると、物理レイヤー 2 セグメント全体のレイヤー 3 フローで BUM トラフィックが正常に処理されない場合がある  
次のすべての条件を満たしている場合、ハイパーバイザーから論理ルーター経由で送信される BUM トラフィックが宛先のハイパーバイザーに到達しません。

- ESX に複数のアップリンクがある
- 送信元と宛先の仮想マシンが論理ルーター経由で接続している
- 送信元と宛先のハイパーバイザーが異なる物理セグメントにある
- 宛先の論理ネットワークが MTEP レプリケーションを使用している

この問題は、BFD モジュールがセッションを作成できない場合、つまり、宛先の論理ネットワークの MTEP が選択されない場合に発生します。

## セキュリティ サービスに関する解決した問題

- **問題 1520694**：RHEL 7.1 カーネル 3.10.0-229 以前では、FTP ALG はデータチャネルでネゴシエーション ポートを開くことができない  
同じハイパーバイザー上の仮想マシンにクライアントとサーバ両方が存在する FTP セッションでは、FTP アプリケーション レベル ゲートウェイ (ALG) はデータ チャネルに対してネゴシエーション ポートを開きません。この問題は Red Hat 固有であり、RHEL 7.1 カーネル 3.10.0-229 で発生します。これより新しいバージョンの RHEL カーネルには影響しません。
- **問題 2008882**：アプリケーション検出を適切に動作させるには、複数のホストにまたがるセキュリティ グループを作成しないようにする  
複数のホストにまたがる仮想マシンが 1 つのセキュリティ グループに属していると、アプリケーション検出セッションが機能しない場合があります。

## ロード バランサに関する解決した問題

- **問題 1995228**：重み付きラウンドロビンおよび重み付き最小接続数のアルゴリズムで、設定を変更して再ロードした後、分散トラフィックが適切に機能しない場合がある  
重み付きラウンドロビンまたは重み付き最小接続数の設定が変更されて再ロードされると、サーバへの接続が失われます。接続が失われた後、トラフィック分散の履歴情報は保存されないため、トラフィックの分散が適切に行われなくなります。
- **問題 2018629**：健全性チェック テーブルに NS グループ プールの更新された監視タイプが表示されない  
同じ監視タイプを持つメンバーで静的な NS グループ プールと動的な NS グループ プールを作成し、動的プールの監視タイプを変更すると、動的プールの健全性チェックが健全性チェック テーブルに表示されなくなります。
- **問題 2020372**：パッシブ健全性チェックで、「失敗」の回数が最大値に達しても、プール メンバーが停止していると見なされない  
パッシブ健全性チェックで、プール メンバーが停止していると見なされるには、設定された値よりも多くの失敗回数が必要となります。

## ソリューションの相互運用性に関する解決した問題

- **問題：2025624**：Splunk ダッシュボードがロード時に停止する、またはダッシュボードのグラフが空白になる  
HTML テンプレートが誤って以前のクエリ スクリプトのパスを参照しているため、Splunk は古いバージョンの nsx\_splunk\_app を取得してしまいます。そのため、ダッシュボードは、vmw\_nsxt\_comp、vmw\_nsxt\_subcomp、vmw\_nsxt\_errorcode などのフィールドを含む古いクエリを実行しますが、これらのフィールド名は、新しいバージョンのクエリ スクリプトとは異なります。このため、クエリは空の結果を返し、ダッシュボードが空白になってしまいます。

## 運用および監視サービスに関する解決した問題



- 問題 1957092 : Docker イメージのロード中にエラーが発生すると、NSX Controller クラスタの初期化に失敗する

initialize control-cluster コマンドが失敗し、次のエラー メッセージが表示されます。Control cluster activation timed out.Please try again.Syslog にも次のログ情報が記録されます。  
<30>1 2017-08-03T22:52:41.258925+00:00 localhost load-zookeeper-image 1183 - -  
grpc: the connection is unavailable.

## アップグレードに関する解決した問題

- 問題 1847884 : 管理プレーンのアップグレード処理が完了するまで NSX-T Data Center に関連する変更を実行できない  
トランスポート ゾーン、トランスポート ノード、または論理スイッチの作成、更新、削除など、何らかの変更を管理プレーンのアップグレード中に行うと、管理プレーンが破損し、NSX Edge、ホスト、およびデータ パスの接続エラーが発生する場合があります。
- 問題 2005709 : NSX Manager の完全修飾ドメイン名 (FQDN) を使用すると、Upgrade Coordinator のページにアクセスできなくなる  
NSX Manager の FQDN を使用して NSX Manager ユーザー インターフェイスを開くと、Upgrade Coordinator のページに「このページは、Upgrade Coordinator が実行されている NSX Manager でのみ使用可能です。」というエラー メッセージが表示されます。サービスを有効にするには、NSX Manager でコマンド「set service install-upgrade enabled」を実行します。install-upgrade サービスがすでに有効な場合は、「clear service install-upgrade enabled」を使用してサービスを無効にしてから再度有効にします。」
- 問題 2022609 : Upgrade Coordinator で、管理対象ホストが管理対象ではないホストとして扱われる  
管理対象ホストが 128 台を超える環境では、アップグレード プロセスで、クラスタに属しているホストが管理対象ではない ESXi グループとして表示されます。
- 問題 1944731 : 最初にアップグレードされた NSX Edge が 2 番目の NSX Edge のアップグレード中に多数の要求を処理すると、DHCP リースのレコードが競合する  
最初にアップグレードされた NSX Edge が 2 番目の NSX Edge のアップグレード中に多数の要求を処理した場合、DHCP リースのレコードが競合することがあります。

## API に関する解決した問題

- 問題 1619450 : ポーリング頻度設定 API GET /api/v1/hpm/features によって test vertical が返される  
GET /api/v1/hpm/features は、ポーリング頻度を設定できるすべての機能のリストを返します。この API は、内部でのテストを目的とした機能を返します。ユーザーには不要な情報であり、機能的な影響はありません。
- 問題 1781225 : API GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules が Ubuntu で機能しない  
API GET https://<NSX-Manager>/api/v1/fabric/nodes/<node-id>/modules は ESXi と RHEL では機能しますが、Ubuntu では機能しません。
- 問題 1954990 : Realization API が正しくない状態を返す  
バリアーの前に実行されたすべての API の状況を確認するために Realization API を使用すると、Realization API が返す状態が実際の状態と異なる場合があります。管理プレーン内での分散ファイアウォールの実行は複雑であるため、本来追従すべきバリアーの後に分散ファイアウォール API がスリップすることがあります。これにより、不正確なステータスが表示されることがあります。

## NSX Container Plug-in (NCP) に関する解決した問題

- 問題 2167491 : NSX-T ロード バランサの仮想サーバが最大数に達すると、NCP の開始に失敗する

NCP の ConfigMap では、NSX-T ロード バランサのサイズを小、中、大に設定することができます。仮想サーバの最大数は、小規模のロード バランサの場合は 10、中規模の場合は 100、大規模の場合は 1000 です。ロード バランサに最大数の仮想サーバがある場合、NCP は開始されません。ロード バランサに最大数の仮想サーバがあるかどうかを確認するには、NSX-T Manager GUI でこのクラスタ名のタグを含むロード バランサを検索し、仮想サーバの数を数えます。

- **問題 2160806：NCP が実行されていないときのアクティブな Ingress の TLS 仕様の更新がサポートされていない**

NCP が Ingress リソースに外部 IP アドレスを割り当てており、NCP が実行されていないときに Ingress の TLS 仕様を更新した場合（たとえば、パラメータ secretName を削除または変更した場合など）、NCP は変更を認識しません。NCP が再度実行されると、古いシークレットに対応する証明書はまだ存在しており、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。

- [一般的な既知の問題](#)
- [インストールに関する既知の問題](#)
- [NSX Manager に関する既知の問題](#)
- [NSX Edge に関する既知の問題](#)
- [論理ネットワークに関する既知の問題](#)
- [セキュリティ サービスに関する既知の問題](#)
- [KVM ネットワークに関する既知の問題](#)
- [ロード バランサに関する既知の問題](#)
- [ソリューションの相互運用性に関する既知の問題](#)
- [運用および監視サービスに関する既知の問題](#)
- [アップグレードに関する既知の問題](#)
- [API に関する既知の問題](#)
- [NSX Policy Manager に関する既知の問題](#)
- [NSX Cloud に関する既知の問題](#)
- [NSX Container Plug-in \(NCP\) に関する既知の問題](#)
- [ドキュメントの修正と追加情報](#)

### 一般的な既知の問題

- **問題 1842511：マルチホップ BFD (Bidirectional Forwarding Detection) がスタティック ルートでサポートされない**

NSX-T 2.0 では、マルチホップ BGP (MH-BGP) ネイバーに対して BFD を有効にできます。NSX-T 2.0 で BFD を設定できるのは BGP に対してのみで、マルチホップ スタティック ルートに対しては設定できません。マルチホップ BGP ネイバーに BFD を設定してから、同じネクストホップを BGP ネイバーとするマルチホップ スタティック ルートを設定すると、BFD セッションの状態が BGP セッションとスタティック ルートの両方に影響します。

回避策：なし。

- **問題 1931707：自動トランスポート ノード機能を利用するには、クラスタ内のすべてのホストで物理 NIC (pnic) を同じ構成にする必要がある**

クラスタで自動トランスポート ノード機能を有効にすると、トランスポート ノード テンプレートが、クラスタ内のすべてのホストに適応されるように作成されます。テンプレートにあるすべての物理 NIC は、トランスポート ノード用にすべてのホストで未使用にする必要があります。ホストの物理 NIC が存在しないか、すでに使用済みの場合、トランスポート ノードの設定に失敗する場合があります。

回避策：トランスポート ノードの設定に失敗した場合は、トランスポート ノードを個別に再度設定してください。

- **問題 1909703** : NSX 管理者は、OpenStack によってバックエンドから直接作成されたルーターで、スタティック ルート、NAT ルール、およびポートを新しく作成できる  
NSX-T 2.0 の RBAC 機能では、OpenStack プラグインによって作成されたスイッチ、ルーター、セキュリティ グループなどのリソースは、NSX のユーザー インターフェイスまたは API を利用して、NSX 管理者に直接削除または変更することはできません。これらのリソースを変更または削除するには、OpenStack プラグインを介して送信される API を利用する必要があります。この機能には制限があります。現時点では、NSX 管理者は OpenStack で作成されたリソースの削除と変更を行うことはできませんが、OpenStack で作成された既存のリソース内でスタティック ルートや NAT ルールなどのリソースを新規に作成することはできます。

回避策：なし。

- **問題 1957072** : ブリッジ ノードのアップリンク プロファイルでは、複数のアップリンクに対して常に LAG を使用する必要がある

LAG (リンク アグリゲーション グループ) を設定していない複数のアップリンクを使用すると、トラフィックのロード バランシングが行われず、正常に動作しない場合があります。

回避策：ブリッジ ノード上の複数のアップリンクには、LAG を使用します。

- **問題 1970750** : 高速タイマーの LACP を使用したトランスポート ノード N-VDS プロファイルが vSphere ESXi ホストに適用されない

高速タイマーの LACP アップリンク プロファイルを NSX Manager 上の vSphere ESXi トランスポート ノードに適用すると、NSX Manager にはプロファイルが正しく適用されたと表示されますが、vSphere ESXi ホストではデフォルトの LACP 低速タイマーが使用されています。

vSphere のハイパーバイザーでは、LACP NSX が管理する分散スイッチ (N-VDS) プロファイルが NSX Manager のトランスポート ノードで使用されていても、lacp-timeout 値 (SLOW/FAST) の結果を確認できません。

回避策：なし。

- **問題 1989407** : Enterprise Administrator ロールを持つ vIDM ユーザーがオブジェクト保護を上書きできない

Enterprise Administrator ロールを持つ vIDM ユーザーが、オブジェクト保護を上書きできず、プリンシパル ID の作成も削除も実行できません。

回避策：管理者権限でログインします。

- **問題 2030784** : 非 ASCII の文字を含むリモート ユーザー名を使用して NSX Manager にログインできない

非 ASCII の文字を含むユーザー名を使用して、リモート ユーザーとして NSX Manager アプライアンスにログインすることはできません。

回避策：NSX Manager アプライアンスにログインする場合、リモート ユーザー名には ASCII 文字が含まれている必要があります。

非 ASCII の文字を使用できるのは、Active Directory サーバで非 ASCII の文字を含むリモート ユーザー名が設定されている場合に限られます。

- **問題 2111047** : NSX-T 2.2 リリースを使用した VMware vSphere 6.7 ホストでアプリケーション検出がサポートされない

セキュリティ グループ内の vSphere 6.7 ホストで仮想マシンが実行されている場合に、セキュリティ グループでアプリケーション検出を実行すると、検出セッションが失敗します。

回避策：なし

- **問題 2157370** : L3 SPAN (Switched Port Analyzer) にパケットの切り捨てを設定すると、特定の物

理スイッチでミラーリングされたパケットがドロップする

GRE/ERSPAN などの L3 SPAN でパケットの切り捨てを設定すると、ミラーリングされ、切り捨てられたパケットは物理スイッチ ポリシーが原因でドロップします。この問題の原因として、ポートが受信しているパケットで、ペイロードのバイト数が type-length フィールドと等しくないことが考えられます。

回避策：L3 SPAN の切り捨て設定を削除します。

- 問題 216992：宛先 MAC アドレス 02:50:56:56:44:52 を含む他のホストからのミラーリングされたパケットが vSphere ESXi アップリンクでドロップする  
ホストが宛先 MAC アドレス 02:50:56:56:44:52 を含むミラーリングされたパケットを他のホストから受信すると、vSphere ESXi アップリンクではこれらのミラーリングされたパケットをドロップします。

回避策：なし

- 問題 2174583：[はじめに] ウィザードで [トランスポート ノードのセットアップ] ボタンが Microsoft Edge ブラウザで正常に動作しない  
[はじめに] ウィザードで [トランスポート ノードのセットアップ] ボタンをクリックすると、Microsoft Edge Web ブラウザが JavaScript エラーを表示して停止します。

回避策：ブラウザは Firefox または Google Chrome を使用します。

## インストールに関する既知の問題

- 問題 1617459：Ubuntu のホスト設定で、インターフェイス構成ファイルのソーシングがサポートされない  
物理 NIC (pnic) インターフェイスが /etc/network/interfaces ファイルに含まれていない場合、MTU がネットワーク構成ファイルで正しく設定されません。このため、再起動するたびに転送ブリッジの MTU 設定が失われます。

回避策：物理 NIC インターフェイス構成を /etc/network/interfaces に移動します。

- 問題 1906410：最初にトランスポート ノードを削除せずにホストをユーザー インターフェイスから削除すると、ホストが不整合な状態になる  
最初にトランスポート ノードを削除せずにホストをユーザー インターフェイスから削除すると、そのホストは不整合な状態になります。ホストが不整合な状態でトランスポート ノードを削除した場合、ユーザー インターフェイスでこのホストを削除できなくなります。

回避策：

1. トランスポート ノードを削除する前に、トランスポート ノードに展開されているすべてのテナント仮想マシンをパワーオフします。
2. トランスポート ノードからトランスポート ゾーンを削除します。
3. トランスポート ノードを削除します。
4. トランスポート ノードの削除に成功してから、ホストを削除します。

トランスポート ノードの削除に失敗する場合は、ナレッジベースの記事

<https://kb.vmware.com/s/article/52068> に掲載されている手順を実行します。

- 問題 1957059：unprep の実行時に VIB が存在するホストをクラスタに追加すると、ホストの unprep に失敗する  
クラスタにホストを追加する前に VIB が完全に削除されていないと、ホストの unprep 操作が失敗します。

回避策：ホストの VIB を完全に削除してからホストを再起動します。

- 問題 2106956：同じクラスタに属する 2 つの NSX Controller を 2 台の異なる NSX Manager に参加させると、データパスが定義されなくなる  
同じ NSX Controller クラスタに属する 2 つの NSX Controller を 2 台の異なる NSX Manager に参加させると、データパスが定義されなくなります。

回避策：NSX Manager で detach CLI コマンドを使用して、NSX Controller クラスタから NSX Controller を削除します。クラスタ内のすべての NSX Controller が同じ NSX Manager に登録されるように、NSX Controller クラスタを再設定します。

次のドキュメント内の「NSX Controller のインストールとクラスタリング」に関するセクションを参照してください：『NSX-TData Centerインストール ガイド』。

- **問題 2106973**：すべての NSX Controller で NSX Controller クラスタを初期化すると、それぞれの NSX Controller が 1 台のノードで構成される NSX Controller クラスタとなり、データパス接続が定義されなくなる

すべての NSX Controller で NSX Controller クラスタを初期化しないでください。それぞれの NSX Controller が 1 台のノードで構成される NSX Controller クラスタとなり、データパス接続が定義されなくなります。1 つ目の NSX Controller でのみ NSX Controller クラスタを初期化し、その NSX Controller で `join control-cluster` CLI コマンドを実行して他の NSX Controller をそのクラスタに参加させます。

回避策：次のドキュメント内の「NSX Controller のインストールとクラスタリング」に関するセクションの手順に沿って、NSX Controller クラスタを再設定します：『NSX-TData Centerインストール ガイド』。

- **問題 2114756**：NSX-T Data Center で作成したクラスタからホストを削除するときに、VIB が削除されないことがある

ホストを NSX-TData Centerで作成したクラスタから削除すると、一部の VIB がホストに残ることがあります。

回避策：ホストから VIB を手動でアンインストールします。

- **問題 2059414**：python-gevent RPM の古いバージョンが原因で RHEL LCP バンドルのインストールが失敗する

RHEL ホストに新しいバージョンの python-gevent RPM が含まれていると、NSX-T Data Center RPM に古いバージョンの python-gevent RPM が含まれているために RHEL LCP バンドルのインストールが失敗します。

回避策：ホストに最新バージョンの python-gevent RPM が含まれている場合、RHEL ホストの LCP バンドルは手動でインストールします。

次の手順を実行してください。

1. RHEL LCP バンドルを抽出します。
2. LCP バンドル フォルダに移動します。
3. LCP フォルダから libev、python-greenlet、python-gevent RPM を削除します。
4. 他の RPM をインストールします。『NSX-T Data Center インストール ガイド』を参照してください。

- **問題 2142755**：OVS カーネル モジュールのインストールが、動作している RHEL 7.4 カーネルのマイナー バージョンによって失敗する

OVS カーネル モジュールのインストールが、カーネルのマイナー バージョン 17.1 以降が動作する RHEL 7.4 ホストで失敗します。インストールの失敗により、カーネルのデータ パスは動作を停止し、アプライアンス管理コンソールは使用できなくなります。

回避策：RHEL 7.4 のカーネル バージョンをアップグレードします。管理者権限で、ホストでスクリプト `/usr/share/openvswitch/scripts/ovs-kmod-manage.sh` を実行し、OVS カーネル モジュールを再ロードします。

## NSX Manager に関する既知の問題

- **問題 1950583**：システムを NSX-T 2.0.0 にアップグレードした後、NSX Manager のスケジュール設定されたバックアップが失敗することがある

一部の NSX-T 環境では、NSX-T をバージョン 2.0.0 にアップグレードした後で、スケジュール設定されたバックアップに失敗する場合があります。この問題は、SSH フィンガープリントの形式が以前のバージョンから変更されたことが原因で発生します。

回避策：バックアップのスケジュールを再設定します。

- 問題 1576112：KVM ハイパーバイザーが異なるレイヤー 2 セグメントに配置されている場合、ゲートウェイを手動で設定する必要がある

NSX Manager に IP アドレス プールを設定し、その IP アドレス プールをトランスポート ノードの作成に使用する場合、IP アドレス プールで設定されたゲートウェイのルートが、Ubuntu KVM ボックスに表示されません。その結果、異なる L2 セグメントにあるハイパーバイザー上の仮想マシン間のオーバーレイトラフィックでエラーが発生します。これは、基盤となるファブリック ホストが、リモート セグメント内のファブリック ノードにアクセスする方法を認識していないためです。

回避策：異なるセグメントにある別のハイパーバイザーにトラフィックをルーティングできるように、ルートをゲートウェイに追加します。この設定を手動で行わないと、オーバーレイトラフィックでエラーが発生します。これは、ファブリック ノードがリモート ファブリック ノードへのアクセス方法を認識しないためです。

- 問題 1710152：互換性モードでは、Internet Explorer 11 で NSX Manager GUI が機能しない

回避策：[ツール] > [互換表示設定] の順に移動し、Internet Explorer が NSX Manager GUI を互換性モードで表示していないことを確認します。

- 問題 2128476：ホスト 500 台、仮想マシン 1,000 台、および仮想ネットワーク インターフェイス (VIF) 10,000 個を超えるインベントリを持つ大規模環境で、ハード リブートを行うと、完全同期するまでに約 30 分かかることがある

NSX Manager を再起動すると、各ホストが NSX Manager と同期され、NSX Manager はホストの最新データを受け取ります。このデータには、ホスト上の仮想マシンや仮想マシン上の VIF に関する情報が含まれています。500 台を超えるホスト、1,000 台の仮想マシン、および 10,000 個の VIF を含むインベントリを持つ大規模環境では、完全に同期するまでに約 30 分かかります。

回避策：ハード リブートを行った後、NSX Manager に最新情報が表示されるまで待機します。

API `api/v1/fabric/nodes/<nodeid>/status` を使用して、特定のノードの最新同期時刻を示す `last_sync_time` プロパティを確認します。

- 問題 1928376：NSX Manager をリストアした後、コントローラ クラスタのメンバー ノードの状態が悪化する

メンバー ノードをクラスタから切断する前に作成されたバックアップ イメージから NSX Manager をリストアすると、Controller クラスタのメンバー ノードが不安定になったり、健全性状態が悪化することがあります。

回避策：クラスタのメンバーシップに変更があった場合、NSX Manager のバックアップを新しく作成するようにしてください。

- 問題 1956088：ユーザー インターフェイスのファイアウォール ビューでルール セットにフィルタが適用されている場合、フィルタをキャンセルすると、ファイアウォール ビューの変更が Manager に保存される前に失われることがある

ユーザー インターフェイスのファイアウォール ビューでルール セットにフィルタが適用されている場合、フィルタをキャンセルすると、ファイアウォール ビューの変更が Manager に保存される前に失われることがある

回避策：なし。

- 問題 1928447：重複する仮想トンネル エンドポイント IP アドレスを持つハイパーバイザーが管理

プレーン ノードの Syslog に記録されない

重複する仮想トンネル エンドポイント IP アドレスを持つハイパーバイザーが、管理プレーン ノードの Syslog に記録されません。ハイパーバイザーの仮想エンドポイントと NSX Edge ノードのアップリンク インターフェイスに一意的 IP アドレスを割り当ててください。

回避策： なし。

- 問題 2125725：大規模なトポロジ環境をリストアすると、検索データが同期されず、複数の NSX Manager ページが応答しなくなる  
大規模なトポロジ環境で NSX Manager をリストアすると、検索データが同期されず、複数の NSX Manager ページに「リカバリできないエラーが発生しました」というエラー メッセージが表示されます。

回避策：次の手順を実行してください。

1. NSX Manager の CLI に管理者としてログインします。
2. 検索サービスを再起動します。

```
restart service search
```

検索サービスによってデータの不一致がバックグラウンドで修正されます。完了するまで 15 分以上待機します。

- 問題 2128361：NSX Manager のログ レベルをデバッグ モードに設定する CLI コマンドが適切に機能しない  
CLI コマンド `set service manager logging-level debug` を使用して NSX Manager のログ レベルをデバッグ モードに設定しても、デバッグ ログ情報が収集されません。

回避策：次の手順を実行してください。

1. NSX Manager の CLI に管理者としてログインします。
2. コマンド `st e` を実行して root ユーザーに切り替えます。
3. `log4j2.xml.default` および `log4j2.xml` ファイルをコピーします。

```
cp /opt/vmware/proton-tomcat/conf/log4j2.xml.default /opt/vmware/proton-tomcat/conf/log4j2.xml
```

4. `log4j2.xml` ファイルの所有権を変更します。

```
chown uproton:uproton /opt/vmware/proton-tomcat/conf/log4j2.xml
```

- 問題 1964681：Manager ユーザー インターフェイスの [ホスト] タブで、トランスポート ノードホストを削除した後もホストの状態が「削除中」と表示される  
Manager ユーザー インターフェイスの [ファブリック] > [ノード] > [トランスポート ノード] タブで、トランスポート ノード ホストを正常に削除した後でも、[ホスト] タブにはホストの状態が「削除中」と表示されます。

回避策：ブラウザを更新します。

- 問題 2169998：Chrome ブラウザで、NSX Manager にログインする際に閲覧履歴データをクリアすると、Manager のユーザー インターフェイスが動作を停止する  
Chrome ブラウザを使用して NSX Manager にログイン後、ブラウザ設定に移動して閲覧履歴データをクリアすると、基本または詳細設定のいずれかの場合でも、ブラウザは NSX Manager への接続を失います。

回避策：NSX Manager へのログイン中には閲覧履歴データを削除しないでください。

## NSX Edge に関する既知の問題

- **問題 1765087**：データパスから Linux カーネルにパケットを転送するために NSX Edge が作成するカーネル インターフェイスでは、MTU が 1600 までしかサポートされない  
データパスとカーネル間のカーネル インターフェイスでは、ジャンボ フレームをサポートしません。1600 を超える BGP プロトコルのパケット サイズは、BGP プロトコル デモンによって切り捨てられ、ドロップされます。1600 を超える SPAN パケット サイズは切り捨てられ、パケット キャプチャ ユーティリティが警告を表示します。ペイロードは切り捨てられず、有効なままです。

回避策：なし。

- **問題 1738960**：DHCP サーバ プロファイルの NSX Edge ノードが別のクラスタの NSX Edge ノードに置き換えられると、DHCP サーバから仮想マシンに提供された IP アドレスが変更される  
この問題は、元のノードと置き換えられた新しいノードが連携していないために発生します。

回避策：なし。

- **問題 1629542**：単一の NSX Edge ノードで転送遅延を設定すると、誤ったルーティング ステータスが表示される  
高可用性を設定していない単一の NSX Edge を実行するとき、転送遅延を設定すると、ルーティング ステータスが正しく報告されない場合があります。転送遅延が設定されると、転送タイマーが期限切れになるまで、誤ったルーティング 状態 **停止** が表示されます。ルーターのコンバージェンスは完了したが、転送遅延タイマーの期限が切れていない場合、ルーティング 状態が **停止** と報告されますが、アップリンク元からアップリンク先への South-North のデータパス フローは問題なく継続されます。この警告は無視しても問題ありません。

- **問題 1601425**：NSX Manager クラスタに登録されている NSX Edge 仮想マシンのクローンを作成できない  
NSX Manager クラスタ登録されている NSX Edge 仮想マシンのクローン作成は、サポートされていません。代わりに、新しいイメージをデプロイする必要があります。

回避策：なし。

- **問題 1585575**：Tier-0 ルーターに接続されている Tier-1 ルーターで NSX Edge クラスタの詳細情報を編集できない  
Tier-1 の論理ルーター上で NAT を有効にした場合、NSX Edge ノードまたは NSX Edge クラスタを指定してから、Tier-1 のルーターを Tier-0 のルーターに接続する必要があります。NSX では、Tier-0 ルーターに接続されている Tier-1 ルーターで、NSX Edge クラスタの詳細情報を編集することはできません。

回避策：Tier-0 ルーターに接続されている Tier-1 ルーターで NSX Edge クラスタの詳細設定を編集するには、Tier-1 ルーターを Tier-0 ルーターから切断し、情報を変更してから、再度接続します。

- **問題 1955830**：NSX Edge クラスタ名に拡張 ASCII 文字または ASCII 以外の文字が含まれていると、NSX-T 1.1 から NSX-T 2.0 へのアップグレードに失敗する  
NSX-T 1.1 の NSX Edge クラスタ名に拡張 ASCII 文字または ASCII 以外の文字が含まれていると、無限ループ エラーが発生し、NSX-T 1.1 から NSX-T 2.0 へのアップグレードに失敗します。

回避策：アップグレードを開始する前に、NSX-T 1.1 インスタンスの NSX Edge クラスタ名から拡張 ASCII 文字または ASCII 以外の文字を削除し、名前を変更します。

- **問題 2122332**：ベアメタル Edge への SSH ログインができない場合がある  
ベアメタル Edge への SSH ログインができないことがあります。

回避策：コマンド プロンプトを開いて iLO ドライバに移動します。Edge SSH サービスを再起動します。

- **問題 2187888**：NSX Manager ユーザー インターフェイスから自動で展開した NSX Edge が無制限



に「登録保留中」のままになる

NSX Manager ユーザー インターフェイスから自動で展開した NSX Edge が無制限に「登録保留中」のままになります。この状態が原因で、NSX Edge で以降の設定ができなくなります。

回避策：CLI を使用し、NSX Edge を NSX Manager に手動で登録します。

## 論理ネットワークに関する既知の問題

- **問題 1769922**：vSphere Client で、NSX Controller クラスタのプレーンに実際の IP アドレスではなく内部 IP アドレス 172.17.0.1 が表示される場合がある

vSphere Client で、NSX Controller の IP アドレスが、実際の IP アドレスではなく 172.17.0.1 と誤って表示されます。NSX Manager の IP アドレスは正しく表示されます。

回避策：なし。これは表示のみの問題で、機能に影響はありません。

- **問題 1771626**：NSX Controller ノードの IP アドレスの変更がサポートされない

回避策：NSX Controller クラスタを再デプロイします。

- **問題 1940046**：複数の Tier-1 論理ルーターに同じスタティック ルートが追加され、アドバタイズされると、East-West トラフィックが遮断される

複数の Tier-1 論理ルーターに同じスタティック ルートが追加され、アドバタイズされた場合、East-West トラフィックが遮断されます。

回避策：スタティック ルートのアドバタイズは、プレフィックスが Tier-1 分散ルーターの接続ネットワークの後ろにある場合、起点となる Tier-1 論理ルーターからのみ行ってください。

- **問題 1753468**：ブリッジ VLAN で Spanning Tree Protocol (STP) を有効にすると、ブリッジ クラスタの状態が [停止] と表示される

LACP チーミングでのブリッジに使用される VLAN で STP が有効になっている場合、物理スイッチのポートチャンネルがブロックされ、ESX ホストのブリッジ クラスタが [停止] と表示されます。

回避策：STP を無効にするか、BPDU フィルタおよび BPDU ガードを有効にします。

- **問題 1753468**：Tier-0 の論理ルーターがルートを集約せず、代わりにルートを個別に再配付する  
Tier-0 の論理ルーターは、接続されているサブプレフィックスのすべてに対応しないプレフィックスに対しては、ルート集約を実行しません。代わりにルートを個別に再配付します。

回避策：なし。

- **問題 1536251**：ESX ホストの仮想マシンを、同じ論理スイッチに接続されている別の ESX ホストにコピーできない

ESX ホストから仮想マシンをコピーし、別の ESX ホストに登録すると、レイヤー 2 のネットワークでエラーが発生します。

回避策：vCenter Server を使用して ESX ホストを管理している場合は、仮想マシンのクローン作成機能を使用します。

ESX ホスト間の仮想マシンのコピーで、レイヤー 2 ネットワークを機能させるには、仮想マシンの .vmx ファイル内で一意の外部 ID を設定する必要があります。

- **問題 1747485**：LAG インターフェイスからアップリンクを削除すると、すべての BFD プロトコルが停止し、BGP ルートでフラッピングが発生する

設定された LAG インターフェイスから任意のインターフェイスが削除されると、すべての BFD プロトコルが停止し、BGP ルートでフラッピングが発生するため、トラフィック フローに影響します。

回避策：なし。

- 問題 1741929：KVM 環境でポートのミラーリングが設定され、パケットの切り捨てが有効になっている場合、ジャンボ パケットはソースから断片的に送信され、ミラーリング先で再集約される

回避策：再集約は、ターゲット仮想マシンの vNIC ドライバで実行されるため、回避策は必要ありません。

- 問題 1619838：論理ルーターのトランスポート ゾーン接続を別の論理スイッチ セットに変更すると、不一致エラーになる

論理ルーターでは、ダウンリンク ポートに対して単一のオーバーレイ トランスポート ゾーンのみをサポートしています。したがって、既存のダウンリンクまたはルーターリンク ポートを削除せずに、トランスポート ゾーン接続を別の論理スイッチ セットに変更することはできません。

回避策：次の手順を実行してください。

1. 既存のダウンリンクまたはルーターリンク ポートをすべて削除します。
2. システムが更新されるまで少し待機します。
3. 再度、トランスポート ゾーン接続を異なる論理スイッチに変更します。

- 問題 1625360：論理スイッチを作成しても、NSX Controller に新しく作成された論理スイッチの情報が表示されない場合がある

回避策：論理スイッチの作成後、60 秒経過してから、NSX Controller で論理スイッチの情報を確認してください。

- 問題 1581649：論理スイッチの作成および削除後、VNI プール範囲を縮小できない

論理スイッチを削除しても、VNI は直ちに解放されないため、範囲を縮小できません。VNI は 6 時間後に解放されます。これは、別の論理スイッチ作成時の VNI の再利用を回避するためです。そのため、論理スイッチの削除後 6 時間が経過するまで、範囲を縮小または変更できません。

回避策：論理スイッチに割り当てられている VNI の範囲を変更するには、論理スイッチの削除後、6 時間待機してください。または、VNI プールの別の範囲を使用するか、範囲を縮小または削除せずに、同じ範囲を再利用します。

- 問題 1516253：Intel 82599 NIC には Queue Bytes Received Counter (QBRC) に関するハードウェア制限があるため、合計受信バイト数が 0xFFFFFFFF を超えるとオーバーフローが発生する  
ハードウェアの制限が原因でオーバーフローが発生した場合、`get dataplane physical-port stats` の CLI 出力と実際の値が一致しません。

回避策：カウンタがリセットされるように、一度 CLI を実行し、時間を空けずに再度 CLI を実行します。

- 問題 2075246：Tier-1 論理ルーターを Tier-0 論理ルーター間で移動できない。

Tier-1 論理ルーターを Tier-0 論理ルーター間で移動すると、Tier-1 論理ルーターのダウンリンク ポートのルート接続が切断されます。

回避策：次の手順を実行してください。

1. Tier-1 論理ルーターを Tier-0 論理ルーターから切断します。
2. Tier-1 論理ルーターが Tier-0 論理ルーターから完全に切断されるまで約 20 分間待機します。
3. Tier-1 論理ルーターを Tier-0 論理ルーターに接続します。  
ダウンリンク ポートのルート接続がリストアされます。

- 問題 2077145：トランスポート ノードを強制的に削除すると、「トランスポート ノードが見当たらない」状態となる

ハードウェア障害が発生してホストを回復できない場合などに、API 呼び出しを使用してトランスポート ノードを強制的に削除すると、「トランスポート ノードが見当たらない」状態になります。

回避策：「見当たらない」トランスポート ノードを含むファブリック ノードを削除します。

- **問題 2099530**：ブリッジ ノードの VTEP IP アドレスを変更すると、トラフィックが停止する  
ブリッジ ノードの VTEP の IP アドレスを変更すると、VLAN からオーバーレイへの MAC アドレス テーブルがリモート ハイパーバイザー上で更新されなくなるため、最大 10 分間トラフィックが停止します。

回避策：VLAN からトラフィックの変更を開始して、ハイパーバイザー上のオーバーレイ MAC アドレス テーブルが更新されるようにします。

- **問題 2106176**：インストールの登録待機の手順で、NSX Controller の自動インストールが停止する  
NSX Manager API またはユーザー インターフェイスを使用して NSX Controller を自動インストールする際、進行中のいずれかの NSX Controller の状態が停止し「登録待機中」と表示されたまま変わらなくなります。

回避策：次の手順を実行してください。

1. 停止した NSX Controller に関連付けられた仮想マシン ID を特定する API 要求を送信します。

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments
```

2. 停止した NSX Controller を削除する API 要求を送信します。

```
https://<nsx-mgr>/api/v1/cluster/nodes/deployments/<Controller id>?action=delete
```

- **問題 2112459**：ブリッジ クラスタ内の単一ノードを置き換えるとトラフィックがドロップする  
ブリッジ クラスタ内の単一ノードを置き換えると、ブリッジ トラフィックが古いノードに流れるため、リモート ハイパーバイザーの転送エントリが更新されるか期限切れになるまで、トラフィックはドロップします。

回避策：次の手順を実行してください。

1. ブリッジ クラスタ内に代替ノードを配置します。
2. HA の設定を許可します。
3. 古いノードを削除します。

- **問題 216992**：カスタム論理ポートの MTU 設定を使用すると、パケットがドロップすることがある

論理ルーター アップリンク ポートなどの論理ポート上でカスタム MTU 設定を使用する際、適切でない値を指定するか、または Tier-0 および Tier-1 論理ルーターに特定の設定を適用すると、パケットがドロップすることがあります。デフォルトの MTU 設定は 1,500 です。

回避策：デフォルトの MTU 設定を使用します。

デフォルトの MTU 設定を使用しない場合は、それぞれの論理ポートに適用されている MTU を次のような関係に設定する必要があります。

1. Tier-0 論理ルーター アップリンクの MTU を 8,900 に設定します。
2. NSX Edge VTEP の MTU を 9,000 に設定します。
3. 仮想マシンの MTU を 8,900 に設定します。

Tier-0 論理ルーターおよび Tier-0 論理ルーターに接続されているすべての Tier-1 論理ルーターは、同じ NSX Edge ノード上に配置する必要があります。

- **問題 2125514**：レイヤー 2 ブリッジのフェイルオーバー後、MAC アドレスが再取得されるまで、一部の NSX Edge 仮想マシン上の論理スイッチがすべてのパケットで BUM レプリケーションを行う可能性がある

レイヤー 2 ブリッジのフェイルオーバー後、エンドポイントの MAC アドレスを再取得するまで、一部の NSX Edge 仮想マシン上の論理スイッチがすべてのパケットの BUM レプリケーションを 10 分間ほど行う可能性があります。エンドポイントが次の ARP を生成すると、システムは自動的にリカバリします。

回避策：なし

- **問題 2113769：NSX Edge VLAN レイヤー 2 ブリッジで DHCP リレーがサポートされない**  
NSX Edge のレイヤー 2 ブリッジ ポートを介して VLAN ホストを論理スイッチ VNI に接続すると、論理ルーター ポートの DHCP リレー エージェントが VLAN ホストに IP アドレスを提供しなくなります。

回避策：次の手順を実行してください。

1. VLAN ホストを手動で設定します。
2. レイヤー 2 ブリッジ ポートを ESXi ホストに移動します。

- **問題 2183549：中央集中型サービス ポートの編集時、新規作成した VLAN 論理スイッチを表示できない**  
Manager ユーザー インターフェイスで、中央集中型サービス ポートと VLAN 論理スイッチを作成すると、新規作成した VLAN 論理スイッチを表示できません。

回避策：ポートの編集に API を使用します。

- **問題 2160634：ループバックの IP アドレスを変更すると、アップリンクのルーター ID の IP アドレスも変更される可能性がある**  
ループバックの IP アドレスを変更すると、NSX Edge はアップリンクの IP アドレスをルーター ID として選択します。ルーター ID として割り当てられたアップリンクの IP アドレスは変更できません。

\*ユーザーへの影響\*：1.Router-ID に想定される副作用として、すべての BGP セッションでフラッピングが発生することがあります。  
2.Router-ID の変更による深刻な影響としては、BGP のデバッグが困難であるため、錯綜状態に陥る可能性があることです。

回避策：BGP 構成を無効にし、ループバックの IP アドレスを変更します。

- **問題 2186040：トランスポート ノードがシステムの上位 250 アップリンク プロファイル内にな**  
**い場合、ユーザーインターフェイスで物理 NIC のアップリンクのドロップダウンが無効になる**  
トランスポート ノードがシステムの上位 250 アップリンク プロファイル内にない場合、ユーザーインターフェイスで物理 NIC のアップリンクのドロップダウンが無効になります。トランスポート ノードを保存すると、トランスポート ノードからアップリンク名が削除されます。

回避策：トランスポート ノードにアップリンク プロファイルとアップリンク名を再選択します。

- **問題 2106635：スタティック ルートの作成中、NULL ルートのアドミニストレーティブ ディスタ**  
**ンスを変更すると、ネクスト ホップの NULL 設定がユーザー インターフェイスに表示されなくな**  
**ります。**  
スタティック ルートの作成中、[ネクスト ホップ] を NULL に設定し、NULL ルートのアドミニストレーティブ ディスタンスを変更すると、ネクスト ホップの NULL 設定がユーザー インターフェイスに表示されなくなります。

回避策：ネクスト ホップを再選択します。

## セキュリティ サービスに関する既知の問題

- **問題 1680128：クライアントとサーバ間の DHCP 通信が暗号化されない**

回避策：通信の安全性を高めるには、IPSEC を使用します。

- **問題 1711221：IPFIX データが、プレーンテキストでネットワーク送信される**  
デフォルトで、IPFIX フローを収集するオプションが無効になっています。

回避策：なし。

- 問題 1726081 : Geneve のトンネル トラフィック (UDP) が KVM で拒否される

回避策：次の手順を実行してください。

KVM で firewalld を使用している場合は、次のコマンドを使用してポートを開き、ファイアウォールを通過させます。

```
# firewall-cmd --zone=public --permanent --add-port=6081/udp
```

KVM で IPtables を直接使用している場合は、次のコマンドを使用してポートを開きます。

```
# iptables -A INPUT -p udp --dport 6081 -j ACCEPT
```

KVM で UFW を使用している場合は、次のコマンドを使用してポートを開きます。

```
# ufw allow 6081/udp
```

- クライアントが異なるネットワーク上にあり、ルーティング サービスがゲスト仮想マシンから提供されている場合、DHCP のリリース/再取得パケットが DHCP サーバに到達しない

NSX-T は、仮想マシンがルーターとして機能しているかどうか区別できません。このため、パケットの CHADDR フィールドが送信元 MAC アドレスと一致しない場合、ルーター仮想マシンによってルーティングされるユニキャスト DHCP パケットがドロップされる可能性があります。CHADDR に DHCP クライアント仮想マシンの MAC アドレスが設定され、送信元の MAC アドレスはルーター インターフェイスの MAC アドレスになります。

回避策：仮想マシンがルーターとして機能している場合には、ルーター仮想マシンのすべての VIF に適用されるスイッチ セキュリティ プロファイルで、DHCP サーバ ブロックを無効にします。

- 問題 2108290 : トランスポート ノードに設定されているベアメタル サーバには、NSX-T Data Center のセキュリティ機能が提供されない

新しいタイプのトランスポート ノードのベアメタル サーバでは、マイクロ セグメンテーションなど、他のハイパーバイザー ワークロードと同じレベルのセキュリティは確保されません。これは、アプリケーション ワークロードと NSX エージェントとの間に信頼性の高い信頼境界が適用されていないためです。

回避策：セキュリティ上の理由から、テナント仮想マシンにはベアメタル サーバへの root 権限を割り当てないでください。また、アプリケーションを root で実行しないでください。テナント仮想マシンにこのアクセス権があると、セキュリティの侵害されたテナント アカウントやアプリケーションがベアメタル サーバ上で悪意のあるアクティビティを実行し、NSX-T Data Center ネットワークに問題を引き起こす可能性があります。

- 問題 2162722 : DROP または REJECT ルールおよびステートレスなルールにポピュラリティ指数を適用できない

「session」はステートフルな ALLOW ルールにのみ適用可能であるため、トラフィックが DROP/REJECT アクションを伴うルールまたはステートレスなルールに該当する場合、ルールのセッション数はインクリメントされません。ポピュラリティ指数はセッション数をキー パラメータとして使用しているため、これらのルールでは変化しません。

回避策：なし

- 問題 2170512 : インターフェイスに 1,000 個を超えるルールがあると、ファイアウォール ルールを取得する CLI コマンドが失敗する

インターフェイスに 1,000 個を超えるルールがあると、CLI コマンド `get firewall <VIF_ID> ruleset rules` は空白の文字列を返します。

回避策：次の 2 つの回避策があります。

- 上記のコマンドの代わりに「`nsxcli -c get firewall <VIF_ID> ruleset rules | json`」コマンドを実行します。

- 次の raw CLI コマンドを実行します。結果を含むファイルの名前が表示されます。

```
ovs-appctl -t /var/run/vmware/nsx-agent/nsxa-ctl dfw/rules
```

## KVM ネットワークに関する既知の問題

- 問題 1775916 : RHEL KVM ホストのファブリックへの追加に失敗したあと、リゾルバ API **POST** **/api/v1/error-resolver?action=resolve\_error** でエラーが解決されない

RHEL KVM ホストのファブリックへの追加に失敗し、NSX Manager ユーザー インターフェイスに「インストール失敗」のようなステータスが表示された場合、リゾルバ API **POST /api/v1/error-resolver?action=resolve\_error** を実行してエラーを解決します。しかしホストを再度ファブリックに追加すると、次のようなエラー メッセージが表示されます。

「ホストにソフトウェアをインストールできませんでした。対象外の展開プラグインの実行アクションです。  
インストール コマンドが失敗しました。」

回避策：次の手順を実行してください。

1. 次のパッケージを手動で削除します。

```
rpm -e glog-0.3.1-1nn5.x86_64
rpm -e json_spirit-v4.06-1.el6.x86_64
rpm -e kmod-openvswitch-2.6.0.4557686-1.el7.x86_64
rpm -e nicira-ovs-hypervisor-node-2.6.0.4557686-1.x86_64
rpm -e nsx-agent-1.1.0.0.0.4690847-1.el7.x86_64
rpm -e nsx-aggservice-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-cli-1.1.0.0.0.4690892-1.el6.x86_64
rpm -e nsx-da-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-host-1.1.0.0.0.4690932-1.x86_64 rpm -e nsx-
host_node_status_reporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-lldp-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-logical_exporter-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-mpa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-netcpa-1.1.0.0.0.4690924-1.el7.x86_64 rpm -e nsx-sfhc-
1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-support-bundle-client-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsx-transport_node_status-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e nsxa-1.1.0.0.0.4690845-1.el7.x86_64
rpm -e openvswitch-2.6.0.4557686-1.x86_64
rpm -e openvswitch-selinux-policy-2.6.0.4557686-1.noarch
rpm -e python-simplejson-3.3.3-1.el7.x86_64
rpm -e コマンドの実行中にエラーが発生する場合は、--noscripts フラグをコマンドに追加し
ます。
```

2. リゾルバ API **POST /api/v1/error-resolver?action=resolve\_error** を実行します。
3. KVM ホストを再度ファブリックに追加します。

- 問題 1602470 : KVM でロード バランシングのチーミングがサポートされていない

- **問題 1611154** : KVM トランスポート ノードにある仮想マシンが、別のトランスポート ノードの仮想マシンにアクセスできない

複数の異なるネットワークに属する VTEP に複数の IP アドレス プールが使用されている環境では、KVM ホスト上の仮想マシンから、異なる IP アドレス プールの VTEP IP アドレスを持つホスト上の仮想マシンにアクセスできない場合があります。

回避策：ルートを追加して、KVM トランスポート ノードが、他のトランスポート ノード上の VTEP で使用されるすべてのネットワークにアクセスできるようにします。

たとえば、2 つのネットワーク 25.10.10.0/24 と 35.10.10.0/24 があり、ローカル VTEP に IP アドレス 25.10.10.20、ゲートウェイ 25.10.10.1 が設定されている場合、次のコマンドを使用して別のネットワーク用のルートを追加できます。

```
ip route add dev nsx-vtep0.0 35.10.10.0/24 via 25.10.10.1
```

- **問題 1654999** : アンダーレイ トラフィックの接続追跡により利用可能なメモリが減少する  
仮想マシン間に大規模な接続を確立すると、次の症状が発生する場合があります。

/var/log/syslog または /var/log/messages ファイルに、次のようなエントリが含まれます。

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950872] net_ratelimit: 239 callbacks suppressed
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.950875] nf_conntrack: table full, dropping packet
```

```
Apr 26 11:45:44 prmh-nsx-perf-server149 kernel: [1625289.958436] nf_conntrack: table full, dropping packet
```

この問題は、デフォルトのファイアウォール ルールが設定されている場合に発生する可能性があります。ファイアウォール ルールが設定されていなければ発生しません（例：論理スイッチがファイアウォール除外リストに含まれている）。

注：上記のログはあくまで一例です。日付、時間、環境変数は、お使いの環境によって変わる場合があります。

回避策：アンダーレイ デバイスのポート 6081 で、UDP に対する接続追跡を無効にするファイアウォール ルールを追加します。

次はコマンドの一例です。

```
# iptables -A PREROUTING -t raw -p udp --dport 6081 -j CT --notrack
```

これはブート中に実行されるように設定する必要があります。プラットフォームでファイアウォール マネージャが有効になっている場合（Ubuntu：UFW、RHEL：firewalld）は、ファイアウォール マネージャを使用して同等のルールを設定する必要があります。関連するナレッジベースの記事 [KB 2145463](#) を参照してください。

- **問題 2002353** : Linux の Network Manager を使用した KVM ホストのアップリンクの管理がサポートされない

NSX-TData Centerは、N-VDS で使用される KVM ホスト上のすべての NIC を管理します。これらのアップリンクで Network Manager が有効になっていると、構成エラーが発生します。

回避策：Ubuntu ホストでは、NSX-TData Centerで使用される NIC を Network Manager から除外します。

Red Hat ホストでは、NSX-TData Center を有効にする前に、/etc/sysconfig/network-scripts の NIC 設定スクリプトを NM\_CONTROLLED="no" に変更します。ホストで NSX-TData Center が有効になっている場合は、同じようにスクリプトを変更し、ホストのネットワークを再起動します。

- **問題 2186045** : KVM では、logrotate がデフォルトで毎分でなく 1 日に 1 回のみ実行される  
KVM では、ログ ファイルのサイズがサイズベースのローテーション ポリシーで定義されたサイズ制限を 1 日で超えてしまうと、その日の終わりに logrotate が実行されるまでローテーションされません。そのため、ログ ファイルのサイズが定義されたサイズ制限を超える可能性があります。

回避策：次の手順を実行してください。

1. /etc/cron.minutes という新しいディレクトリを作成します。
2. 次の内容を持つ /etc/cron.minutes/logrotate というスクリプトを作成します。

```
#!/bin/sh

/usr/sbin/logrotate /etc/logrotate.conf
```
3. /etc/cron.minutes/logrotate の権限を次のように変更します。

```
chmod 755 /etc/cron.minutes/logrotate
```
4. 次のように、cron.minutes を /etc/crontab のエントリとして付加します。

```
echo "* * * * * root cd / && run-parts --report /etc/cron.minutes"
>>/etc/crontab
```

## ロード バランサに関する既知の問題

- **問題 2010428：ロード バランサ ルールの作成と適用に関する制限事項**

ユーザー インターフェイスでは、仮想サーバからのみロード バランサ ルールを作成できます。ユーザー インターフェイスでは、REST API を使用して作成されたロード バランサ ルールを仮想サーバに適用できません。

回避策：REST API を使用するロード バランサ ルールを作成した場合は、REST API を使用して仮想サーバに適用します。これで、REST API を使用して作成されたルールが、ユーザー インターフェイスの仮想サーバで表示されるようになります。

- **問題 2016489：SNI (Server Name Indication) が選択されていると LCP でデフォルト証明書を設定できない**

SNI (Server Name Indication) で複数の証明書 ID が使用される場合は、LCP でデフォルト証明書が無視されないように、証明書リストでデフォルト証明書 ID を設定する必要があります。

回避策：デフォルトの証明書を SNI 証明書リストの先頭に設定してください。

- **問題 2115545：ロード バランサの健全性チェックが有効な場合、バックエンド サーバのプールメンバーに直接接続できないことがある**

ロード バランサが論理ルーターに接続しており、論理ルーターのアップリンクを使用してプール メンバーにアクセス可能なときは、健全性チェックと同じプロトコルを使用して、論理ルーターのダウンリンクに接続されているクライアントからプール メンバーにアクセスできません。

たとえば、ロード バランサが論理ルーター LR1 に接続されていて、LR1 アップリンクを介してアクセス可能なプール メンバーへの ICMP 健全性チェックが有効な場合、LR1 ダウンリンク上のクライアントはこれらのプール メンバーに直接 ping を送信できません。ただし、同じクライアントが、SSH や HTTP などの他のプロトコルを使用してサーバと通信することはできます。

回避策：ロード バランサで、異なるタイプの健全性チェックを使用します。たとえば、バックエンドサーバに ping を送信するには、従来の ICMP 健全性チェックではなく、TCP または UDP 健全性チェックを使用します。

- **問題 2128560：ロード バランサの SNAT 自動マップと健全性チェックを両方設定すると、健全性チェックまたは接続に失敗することがある**

同じサーバ ポートに対してロードバランサの SNAT 自動マップと健全性チェック（TCP、HTTP、HTTPS、または UDP など）を両方設定すると、サーバ プールの健全性チェックまたは接続が失敗することがあります。

回避策：SNAT 自動マップでなく、SNAT IP アドレス リストを使用します。

注：SNAT IP アドレス リスト モードで指定された SNAT IP アドレスに、論理ルーター アップリンクの IP アドレスを含めないようにしてください。



たとえば、ロード バランサが Tier-1 論理ルーター LR1 に接続されている場合は、SNAT IP アドレス範囲の設定で、LR1 アップリンクの IP アドレスを含めないようにします。

## ソリューションの相互運用性に関する既知の問題

- **問題 1588682** : ESXi ホストをロックダウン モードにすると、ユーザー `nsx-user` が無効になる  
ESXi ホストがロックダウン モードになると、ユーザー `vpxuser` がホストへのアクセス権を持ち、コマンドを実行できる唯一のユーザーになります。NSX-TData Centerは、ホスト上の NSX-TData Centerの関連タスクを実行するときは必ず、別のユーザー `nsx-user` を必要とします。

回避策：ロックダウン モードを使用しないでください。vSphere ドキュメントの [ロックダウン モード](#) を参照してください。

## 運用および監視サービスに関する既知の問題

- **問題 1749078** : ESXi ホストのテナント仮想マシンと、対応するホストのトランスポート ノードを削除したあとに、ESXi ホストを削除できない  
ホスト ノードの削除では、さまざまなオブジェクトの再設定も行われるため、数分以上の時間がかかる場合があります。

回避策：数分待機し、削除操作を再度実行します。必要に応じて、操作を繰り返します。

- **問題 1761955** : 仮想マシンの登録後に、仮想マシンの vNIC を NSX-T Data Center 論理スイッチに接続できない

既存の vmx ファイルを使用して ESXi ホストに仮想マシンを登録する場合、次の vNIC 固有のエラーは無視されます。

- vNIC が無効なネットワーク バックリングを使用して設定されている。
- NSX-T 論理スイッチに接続されている vNIC で、VIF 接続に失敗する。

回避策：次の手順を実行してください。

1. 標準の vSwitch に一時的なポート グループを作成します。
2. 切断状態の vNIC を新しいポート グループに接続し、接続済みとしてマークします。
3. vNIC を有効な NSX-TData Center論理スイッチに接続します。

- **問題 1774858** : NSX Controller クラスタが何日間か実行された後、まれに非アクティブになる  
NSX Controller クラスタが非アクティブになると、すべてのトランスポート ノードと NSX Edge ノードは NSX Controller への接続を失い、設定を変更できなくなります。ただし、データ トラフィックは影響を受けません。

回避策：次の手順を実行してください。

- ディスク遅延の問題がある場合は修正します。
- すべての NSX Controller でクラスタ管理サービスを再起動します。

- **問題 1576304** : ドロップされたバイト数が、ポートのステータスと統計レポートに表示されない  
`/api/v1/logical-ports/<port-id>/statistics` または NSX Manager を使用して、論理ポートの状態と統計情報を表示すると、ドロップされたパケット数が 0 で表示されます。この値は正確ではありません。パケットがいくつドロップされても、レポートには空白で表示されます。

回避策：なし。

- **問題 1955822** : ライセンス使用のレポート機能で、csv ファイルに実際の使用状況のみが含まれ、CPU や仮想マシンの使用資格が含まれていない

API またはユーザー インターフェイスからライセンス使用レポートのクエリを実行すると、現在の使用状況のみが返されます。

回避策：ユーザー インターフェイスまたは REST API を使用して、現在のライセンスで許可される使用制限を返すクエリを実行します。

メソッド：GET; URL: /api/v1/licenses

- **問題 2081979**：トランスポート ノード ホストがどのコントローラにも接続できない  
NSX プロキシ ログに、以下の内容が記録されます。「Certificate validation (証明書の確認)」というメッセージが想定されますが、記録されません。

```
TCP connection started: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757:1234
Doing SSL handshake
TCP connection established: 10.171.0.73:0::3a4de8a2-3bc1-41ea-a94d-c1427d8cd757,
local addr: 10.171.0.59:36048, remote addr: 10.171.0.73
```

回避策：コントローラに管理者としてログインし、次のコマンドを実行します。

```
set debug
get mediator forcesync
```

## アップグレードに関する既知の問題

- **問題 1930705**：管理プレーンのアップグレード中に、論理スイッチに接続した仮想マシンの vMotion に失敗する  
管理プレーンのアップグレード中に、論理スイッチに接続した仮想マシンの vMotion に失敗します。

回避策：管理プレーンのアップグレードが完了してから、vMotion プロセスを再試行します。

- **問題 2005423**：以前の NSX-T バージョンからアップグレードした KVM ノードが balance-tcp を使用するように自動変更されない  
NSX-T は、アップグレードされた KVM ホストのアップリンクの結合モードを active-backup から balance-tcp に自動変更しません。

回避策：適切なモードを設定するには、設定の変更がなくても、トランスポート ノードを編集します。

- **問題 2101728**：NSX Edge グループのアップグレードに成功した後で、NSX Edge アップグレードプロセスが一時的に停止することがある  
NSX Edge グループのアップグレードに成功しても、別の NSX Edge グループのアップグレード中にプロセスが一時的に停止します。

回避策：[続行] をクリックして、NSX Edge グループのアップグレードを続行します。

- **問題 2106257**：NSX-T 2.1 から NSX-T 2.2 へのアップデートで EULA API の承認ワークフローが変更されている  
EULA API の承認は、Upgrade Coordinator を更新してから既存のホストをアップグレードするまでの間に呼び出す必要があります。

回避策：なし

- **問題 2108649**：アップグレードを行うパーティション内でファイルまたはディレクトリが開いていると、アップグレードに失敗する  
NSX Manager や NSX Controller など、アップグレード対象となっているパーティション内で、ファイルやディレクトリを開いたままにしないでください。これらが開いたままだと、アップグレード プロセスに失敗します。

回避策：障害が発生したアプライアンスを再起動して、アップグレード プロセスを再開します。

- 問題 2116020：NSX-T 2.1 から NSX-T 2.2 へのアップデート後、一部の廃止された Ubuntu KVM パッケージが削除されない

NSX-T 2.1 から NSX-T 2.2 へのアップデート後、以下の廃止された Ubuntu KVM パッケージが削除されません。

- nsx-host-node-status-reporter
- nsx-lldp
- nsx-logical-exporter
- nsx-netcpa
- nsx-support-bundle-client
- nsx-transport-node-status-reporter
- nsxa

回避策：次の手順を実行してください。

1. /etc/vmware/nsxa/ ディレクトリに一時ファイルを作成します。  

```
cd /etc/vmware/nsxa  
touch temp.txt
```
2. すべての nsxa パッケージ ディレクトリおよびファイルをリストします。  

```
dpkg -L nsxa  
/etc/vmware/nsxa# ls
```
3. 次のパッケージを削除します。
  - a) `dpkg --purge nsx-lldp`
  - b) `dpkg --purge nsx-support-bundle-client`
  - c) `dpkg --purge nsx-transport-node-status-reporter`
  - d) `dpkg --purge nsx-logical-exporter`
  - e) `dpkg --purge nsx-netcpa`
  - f) `dpkg --purge nsxa`
  - g) `dpkg --purge nsx-host-node-status-reporter`
4. 次のディレクトリが使用可能なことを確認します。  

```
/etc/vmware/nsxa/
```
5. /etc/vmware/nsxa/ ディレクトリから temp.txt ファイルを削除します。  

```
rm -f temp.txt
```

- 問題 2164930：空白のホスト アップグレード ユニット グループがある場合、管理プレーンのアップグレードが完了すると状態が一時停止と表示される

空白のホスト アップグレード ユニット グループがある場合、管理プレーン全体のアップグレード状態が一時停止と表示され、ホストのアップグレード状態は 100% とマークされません。

**\*ユーザーへの影響\***：アップグレード中に空白のホスト グループがある場合、管理プレーンのアップグレード完了後にアップグレード状態が PAUSED と表示されます。

回避策：管理プレーンをアップグレードする前に、空白のホスト アップグレード ユニット グループを削除します。

管理プレーンをアップグレードする際は、空白のホスト アップグレード ユニット グループを削除し、CLI を使用して `install-upgrade service` を再起動します。

- 問題 2097094：アップロードの途中でアップグレード バンドルのアップロードをキャンセルできない

アップグレード バンドルの .mub ファイルがアップロードされているときにアップロード処理をキャンセルすることはできません。

回避策：アップグレード バンドルの .mub ファイルのアップロードが完了するまで待ちます。

- 問題 2122242 : Ubuntu KVM ホストを NSX-T 2.1 から 2.2 または NSX-T Data Center 2.3 にアップデートしても、nsx-support-bundle-client パッケージが削除されない  
Ubuntu KVM ホストを NSX-T 2.1 リリースから新しいリリース (NSX-T 2.2 または NSX-T Data Center 2.3) にアップデートしても、使用されなくなった nsx-support-bundle-client パッケージはインストールされたままとなります。/usr/bin/dpkg -l などのコマンドを実行すると、このパッケージがインストールされていることを確認できます。

回避策 : root としてログインし、次のコマンドを実行してパッケージを手動で削除します。

```
# /usr/bin/dpkg --purge nsx-support-bundle-client
```

- 問題 2186957 : アップグレード後に ESXi ホストのメンテナンス モードが終了しない  
クラスタ内のホストが 1 台だけで、Upgrade Coordinator がそのホストをメンテナンス モードにする前回の試行が失敗している場合、アップグレード後に ESXi ホストのメンテナンス モードが終了しません。

回避策 : ホストのメンテナンス モードを手動で終了するか、ホストが確実にメンテナンス モードになるようにします (クラスタあたり 2 台以上のホストが必要です) 。

- 問題 2166207 : 500 台のハイパーバイザーがある環境で NSX-T Data Center 2.2 から NSX-T Data Center 2.3 にアップデートすると、アップデート処理全体がいつまでも IN\_PROGRESS 状態のままになることがある  
500 台のハイパーバイザーがある環境で NSX-T Data Center 2.2 から NSX-T Data Center 2.3 にアップデートすると、[一時停止] をクリックしてから Web ブラウザの表示を何回か更新しても、アップデート処理全体がいつまでも IN\_PROGRESS 状態のままであることがあります。

回避策 : NSX Manager で NSX-T Data Center の CLI にログインします。install-upgrade コマンドを入力してサービスを再起動します。

- 問題 2113681 : NSX Edge のアップグレード後に KVM ホストがアクセス不能になり障害が発生すると、Upgrade Coordinator は NSX Controller ノードのアップグレードには進まず、障害が発生したホストのアップグレードを試行する  
KVM ホストと NSX Edge をアップグレードした後、新しい RPM をアンインストールして以前の RPM をホストにインストールすると、そのホストは Upgrade Coordinator から使用できなくなります。そのため、Upgrade Coordinator は NSX Controllers ノードのアップグレードに進まず、KVM ホストのアップグレードを試行します。

回避策 : Upgrade Coordinator のユーザー インターフェイスの表示を更新し、[ホスト] タブをクリックして、KVM ホストのアップグレードを行います。

KVM ホストのアップグレードはスキップすることもできます。それには、コマンド プロンプトを起動し、curl -i -k -u admin -X POST https://<nsx-manager-ip-address>/api/v1/upgrade/plan?action=continue&skip=true というコマンドを入力します。

## API に関する既知の問題

- 問題 1605461 : Syslog に記録される NSX-T API のログにシステム内部の API 呼び出しが含まれる  
NSX-T は、ユーザーによる API 呼び出しとシステムによる API 呼び出しの両方を Syslog に記録します。  
API 呼び出しイベントが Syslog に記録されていても、ユーザーが NSX-T API を直接呼び出しているわけではありません。ログには NSX Controller と NSX Edge API 呼び出しが記録されていますが、これらの NSX-T アプライアンスでは一般に公開されている API サービスは使用されません。これらのプライベート API サービスは、NSX-T CLI などの他の NSX-T サービスによって使用されます。

回避策 : なし。

- 問題 1641035 : `POST/hpm/features/<feature-stack-name>`

`action=reset_collection_frequency` への REST 呼び出しで、`collection_frequency` が復旧せず統計が上書きされない

この REST 呼び出しを使用して収集頻度をデフォルトにリセットしようとしても、リセットされません。

回避策 : `PUT /hpm/features/<feature-stack-name>` を使用して、`collection_frequency` を新しい値に設定します。

- 問題 1648571 : ステータスと統計のオンデマンド要求が断続的に失敗する HTTP エラー コードが一貫していない

特定の状況で、オンデマンド要求が失敗します。これらの要求は、再試行時に API 呼び出しが成功しても、HTTP 503 エラーではなく HTTP 500 エラーで失敗します。

統計 API では、タイムアウト条件によっては深刻なメッセージ ルーティング エラー ログが発生する場合があります。これらのエラーは、タイムアウトになったあとに応答が返されるために発生します。

たとえば、次のようなエラーが発生します。`java.lang.IllegalArgumentException: Unknown message handler for type`

`com.vmware.nsx.management.aggr.messaging.AggService$OnDemandStatsResponseMsg.`

ステータス API の場合、タイムアウト後の応答を設定するタイムアウト条件によっては、通常より早くキャッシュが更新される可能性があります。

回避策 : API 要求を再試行します。

- 問題 1963850 : GET API によって表示される項目が大文字と小文字を区別してソートされる

GET API を実行すると表示名によってソートされた項目が返され、大文字と小文字を区別してソートされます。

回避策 : なし。

- 問題 2070136 : 分散ファイアウォール API で大量のデータを処理すると障害が発生する

分散ファイアウォール API で作成または更新するデータが 100 MB を超えると障害が発生し、エラーコード 500 とトランザクションの失敗を示すメッセージが生成されます。通常、API は 1,000 個を超えるルールを含むセクションを参照し、それぞれのルールは多くの送信元、宛先、および適用先オブジェクトを参照しています。

回避策 : 少しずつ数を増やしながらルールの作成または更新を行います。

- 問題 1895497 : ロード バランサの SRCDESTMACIPPORT アルゴリズムが API で機能しない

API を呼び出してトランスポート ノードのアップリンク プロファイルを作成する際に、プロファイル中に送信元および宛先の MAC アドレス、IP アドレス、および TCP/UDP ポートが指定された LAG が含まれていると、呼び出しは失敗します。

回避策 : なし

## NSX Policy Manager に関する既知の問題

- 問題 2057616 : NSX Policy Manager を NSX-T 2.1 から NSX-T 2.2 にアップデートするときに、サポート対象外の NSService および NSGroup が転送されない

NSX Policy Manager を NSX-T 2.1 から NSX-T 2.2 にアップデートするとき、Ether タイプが指定されたサポート対象外の NSService と、MAC セットおよび論理ポートメンバーシップ基準が指定された サポート対象外の NSGroup が転送されません。

回避策 : 次の手順を実行してください。

1. NSX-T 2.1 で、通信エントリで使用する、Ether タイプが指定された NSService を削除して、変更します。
2. 通信エントリで使用する、MAC セットおよび論理ポートメンバーシップ基準が指定された NSGroup を削除して、変更します。

3. NSX Manager を NSX-T 2.1 から NSX-T 2.2 にアップデートします。
  4. CLI を使用して NSX Policy Manager をアップデートします。
- 問題 2116117：ユーザー インターフェイスの NSX Policy Manager のトポロジ タブにデータ接続が失敗したと表示される  
ユーザー インターフェイスの NSX Policy Manager のトポロジ タブで、ポリシー ドメイン内のグループに、サポート対象外の ESXi 6.7 がホストする仮想マシンが含まれていると、データ接続に失敗したと表示されます。

回避策：なし

- 問題 2126647：NSX Policy Manager 分散ファイアウォールの更新を同時に行うと、設定が上書きされる  
2 名のユーザーが NSX Policy Manager 分散ファイアウォール セクションを同時に編集した場合、最後にユーザーが加えた変更が、それ以前に他のユーザーが加えた編集内容を上書きします。

回避策：最初のユーザーが分散ファイアウォールに加えた変更を回復させます。変更を保存してから、2 番目のユーザーが変更を加えます。

## NSX Cloud に関する既知の問題

- 問題 2112947：Cloud Service Manager (CSM) で NSX Agent をアップグレードするとき、一部のインスタンスに失敗と表示される  
CSM で NSX Agent をアップグレードするとき、ユーザー インターフェイスが応答せず、一部のインスタンスに「失敗」と表示されることがあります。

回避策：ユーザー インターフェイスを更新します。

- 問題 2111262：PCG の展開時に次のエラーが表示される：「Gateway deployment failed: [Errorcode: 60609] Async operation failed with provisioning state: Failed.」または「Failed to create gateway virtual machine with name nsx-gw, Gateway deployment failed.」  
これは、Microsoft Azure インフラストラクチャが原因でまれに発生します。

回避策：失敗した Public Cloud Gateway (PCG) を再度展開します。

- 問題 2110728：HA を使用している場合で、--gateway オプションを使用して 1 つの PCG の DNS 名のみを指定して NSX エージェントを仮想マシンにインストールしてあると、2 番目の PCG へのフェイルオーバーが機能しない  
フェイルオーバー後にワークロード仮想マシンを PCG に接続できなくなるため、PCG は仮想マシンの論理ステータスを適用/認識できません。

回避策：ワークロード仮想マシンにエージェントをインストールするときに、--gateway オプションを使用しないでください。VPC または VNet の [ゲートウェイ] 画面に示される値を使用します。詳細については、『NSX-T Data Center Administration Guide』の「Installing NSX Agent」を参照してください。

- 問題 2071374：特定の Linux 仮想マシン インスタンスに NSX Agent をインストールすると、「nscd」に関する無害なエラー メッセージが表示されることがある  
説明：仮想マシンで「nscd」が実行されている場合、NSX Agent のインストールで次のエラー メッセージが表示されることがあります。「sent invalidate(passwd) request, exiting」これは、Ubuntu 14.04、16.04 などを実行している仮想マシンで発生します。

回避策：このメッセージが表示される原因は、Linux ディストリビューションの既知のバグです。このメッセージは無害であり、NSX Agent のインストールに影響しません。

- 問題 2010739：2 台の Public Cloud Gateway (PCG) がスタンバイと表示される

ゲートウェイのオンボーディング中、プライマリ PCG をコントローラに接続できない場合は、コントローラとゲートウェイ間の接続が回復するまで、プライマリとセカンダリの両方のゲートウェイがスタンバイモードになります。

- 問題 2121686 : Cloud Service Manager (CSM) に、「Server failed to authenticate the request.」という例外が表示される

このエラーは、CSM アプライアンスの時刻が Microsoft Azure Storage サーバまたは NTP と同期していないために、CSM に表示されることがあります。この場合、Microsoft Azure は「サーバが要求の認証に失敗しました (Server failed to authenticate the request.)」というあいまいな例外を生成し、これと同じエラーが CSM に表示されます。

回避策 : CSM アプライアンスの時刻と NTP または Microsoft Azure Storage サーバの時刻を同期します。

- 問題 2092378 : HA モードで Public Cloud Gateway (PCG) を展開すると、両方の PCG がスタンバイモードで表示され、クラウドの同期ではプライマリ PCG がアクティブと表示される

Cloud Service Manager (CSM) を使用して、プライベート ネットワーク内で PCG に高可用性を展開すると、最大 1 時間にわたり、PCG がスタンバイ/スタンバイまたはアクティブ/アクティブ状態であると表示されます。この間、PCG に何らかの問題があり、状態も不明であるため、使用を継続できないように見えます。

回避策 : 次の手順を実行します。

1. PCG の展開後にユーザー インターフェイスでアカウントを再同期することにより、CSM が最新データを取得および表示できるようにします。
2. 再同期後も CSM に PCG が誤った状態で表示される場合は、NSX Manager で PCG の接続状態を確認してください。
3. 接続が起動中と表示されているにも関わらず、正しい状態が表示されない場合は、PCG のデバッグに進んでください。

- 問題 2119726 : Microsoft Azure VNet に Public Cloud Gateway (PCG) を展開している場合、以前は仮想マシンに関連付けられていたパブリック IP が、使用可能な IP のリストに誤って表示されることがある

パブリック IP が以前に割り当てられていた仮想マシンをパワーオフすると、仮想マシンとパブリック IP の関連付けが解除されてしまいます。これは、仮想マシンが一定期間パワーオフ状態になった場合、仮想マシンに関連付けられているパブリック IP の関連付けを Microsoft Azure が解除するためです。解除するまでの期間は、具体的に Microsoft Azure で定義されているわけではありません。

回避策 : VNet 内で PCG をパワーオフしなければ、パブリック IP とプライマリ PCG のアップリンク インターフェイスとの関連付けは解除されません。PCG をパワーオフする必要がある場合は、該当の PCG に関連付けられている PIP が再利用されないように、PCG が再びパワーオンしたらすぐに同じ PIP を取得するようにしてください。

- 問題 2165915 : kmod.x86\_64 0:20-15.el7\_4.6 を使用した Red Hat Enterprise Linux 7.4 に対する NSX Cloud のサポート

NSX Cloud は、kmod-20-15.el7\_4.6 を使用した Red Hat Enterprise Linux 7.4 を実行する仮想マシン インスタンスをサポートしません。これは、Red Hat 社が報告されたバグが原因です。[https://bugzilla.redhat.com/show\\_bug.cgi?id=1522994](https://bugzilla.redhat.com/show_bug.cgi?id=1522994) を参照してください。

回避策 : NSX Agent をインストールするには、このバグが修正されている kmod バージョンにアップデートします。

- 問題 2102828 : Microsoft Azure の展開で、NSX-T 2.2 から NSX-T Data Center 2.3 へのアップデートの進行中および終了後に、Public Cloud Gateway (PCG) が機能しないことがある

Microsoft Azure の展開でシステムが NSX-T 2.2 から NSX-T Data Center 2.3 にアップデートされると、Public Cloud Gateway (PCG) のインターフェイスで IP アドレスを取得できない状況がまれに発生します。これは、PCG のアップデート手順で発生することがあり、PCG のアップデート処理がハングしたように見えます。この問題は、管理者が Microsoft Azure portal から PCG アプライアンスを再起動したときに PCG が操作できないという形で現れることもあります。この問題は、NSX-T Data Center 2.3 を新しいシステムに初めてインストールする場合には発生しません。

回避策： アップデート対象の PCG を Microsoft Azure ポータルから再起動してから、Cloud Service Manager (CSM) で、PCG と仮想マシン インスタンスの状態が正常であることを確認します。

- **問題 2180531：Ubuntu 16.04 仮想マシン インスタンスでの NSX Agent のサポートがカーネル 4.14 以前に制限される**

Ubuntu 16.04 仮想マシン インスタンスでは、NSX Agent のサポートはカーネル 4.14 以前に制限されます。NSX Agent は、カーネル 4.15 以降の Ubuntu 16.04 仮想マシン インスタンスでは機能しません。

この問題の回避策はありません。

- **問題 2170445：PCG を NSX-T Data Center 2.2 から NSX-T Data Center 2.3 にアップデートすると、PCG の HA 状態が Microsoft Azure の PCG に適切に設定されない**

Microsoft Azure PCG を NSX-T 2.2 から NSX-TData Center2.3 にアップデートした後、PCG の HA 状態が予想されるとおりのアクティブ/スタンバイになりません。PCG HA の望ましい状態は SYNC、望ましくない状態は Active と表示されます。そのため、アップデート後に HA のフェイルオーバーが発生した場合は、1 つの PCG のみが有効な状態になります。

回避策： NSX-TData Center2.3.

これは、NSX Manager ユーザー インターフェイスまたは NSX Manager REST API を使用して行います。

ユーザー インターフェイスからは、次のようにします。

1. [ファブリック] > [プロファイル] の順に移動します。
2. 名前が「PCG-Uplink-HostSwitch-Profile」、説明が「PublicCloudGateway Uplink HostSwitch Profile」のプロファイルを選択します。
3. [編集] をクリックし、MTU 値を 1,500 に変更して、[保存] をクリックします。
4. NSX-T 2.2 から NSX-TData Center2.3.

REST API では、次のようにします。

- 1.次のコマンドで、すべてのホスト スイッチ プロファイルを取得します。

```
curl -X GET \  
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles \  
  -H 'authorization: Basic <AUTH ID>' \  
  -H 'content-type: application/json'
```

- 2.名前が「PCG-Uplink-HostSwitch-Profile」、説明が「PublicCloudGateway Uplink HostSwitch Profile」のホスト スイッチ プロファイルを見つけ、そのプロファイルの ID を取得します。

```
curl -X PUT \  
  https://<NSX-Manager-URL>/api/v1/host-switch-profiles/<host-switch-profile-id> \  
  -H 'authorization: Basic <AUTH ID>' \  
  -H 'content-type: application/json' \  
  -d '{
```



```

"resource_type": "UplinkHostSwitchProfile",
"description": "PublicCloudGateway Uplink HostSwitch Profile",
"id": "<host-switch-profile-id>",
"display_name": "PCG-Uplink-HostSwitch-Profile",
"tags": [
  {
    "scope": "CrossCloud",
    "tag": "public-cloud-manager"
  },
  {
    "scope": "PcmId",
    "tag": "<Existing PCM ID>"
  },
  {
    "scope": "EntityType",
    "tag": "default"
  },
  {
    "scope": "CloudScope",
    "tag": "<Existing VPC/VNET name>"
  },
  {
    "scope": "CloudType",
    "tag": "<Existing cloud type>"
  },
  {
    "scope": "CloudVpcId",
    "tag": "<Existing Vpc/Vnet id>"
  }
],
"transport_vlan": 0,
"teaming": {
  "active_list": [
    {
      "uplink_type": "PNIC",
      "uplink_name": "uplink-1"
    }
  ],
  "policy": "FAILOVER_ORDER"
},
"overlay_encap": "GENEVE",
"mtu": 1500,
"_revision": 1
}'

```

- 問題 2174725 : Public Cloud Gateway (PCG) が展開されている管理対象の VPC/VNet が、Cloud Service Manager (CSM) で管理対象外と表示される  
PCG が展開されている管理対象の Amazon VPC または Microsoft Azure VNet が、CSM で管理対象外と表示されます。

回避策： この問題は、CSM を再起動すると解消されます。

- 問題 2162856 : Azure PCG の HA 状態がいずれもアクティブ、またはいずれもスタンバイなど無効

になる

1 組の Public Cloud Gateway (PCG) を AWS に展開し、もう 1 組のペアを Azure に展開すると、Azure PCG の HA 状態が両方ともアクティブ、または両方ともスタンバイになるなどして、無効になります。

回避策：クロス クラウドを NSX-T Data Center 2.3 にアップグレードする前に、PCM で作成した PCG のアップリンク ホスト スイッチ プロファイルで MTU を 1,500 に更新します。マネージャのユーザー インターフェイスで、次の手順を実行します。

- [ファブリック] > [プロファイル] の順に移動します。
- 名前が「PCG-Uplink-HostSwitch-Profile」、説明が「PublicCloudGateway Uplink HostSwitch Profile」のプロファイルを選択します。
- [編集] をクリックし、「MTU」値を 1,500 に変更して、[保存] をクリックします。
- アップグレード ワークフローを開始します。

- 問題 2102321：Microsoft Azure における NSX Cloud の処理の速度が、トラフィックが増加したときに低下することがある

NSX Cloud は、仮想マシンを管理するとき、NSX の管理対象から仮想マシンを除外するとき、仮想マシンに対して検疫アクションを実施するときなど、一部の処理で Microsoft Azure ARM API を利用します。負荷が高い状況では、特定のサブスクリプションについて Microsoft Azure が API の上限に達することがあり、その場合は、そのサブスクリプションに関するすべての API リクエストに対してスロットリングが開始されます。これにより、上記の NSX 処理が時間内に終了しない可能性があります。これらの処理は、Microsoft Azure がリクエストのスロットリングを停止すれば、最終的に完了します。Public Cloud Gateway の PCM ログには、現在スロットリングが発生していることを示す次のようなログが記録されます。

[Azure Resource Manager read/write per hour limit reached.Will retry in: x seconds]

回避策： Microsoft Azure によるスロットリングが停止するまで待ちます。

- 問題 2189738：オンボーディングした Virtual Private Cloud (VPC) で、以前有効だった検疫ポリシーを無効にすると AWS ワークロード仮想マシンにアクセスできなくなる

検疫ポリシーを有効にして Public Cloud Gateway (PCG) を展開してから検疫モードを無効にすると、この VPC にある NSX 管理対象の AWS ワークロード仮想マシンの一部は、PCG と通信できなくなります。

回避策：AWS VPC で、NSX Cloud セキュリティ グループに対して 受信ルール gw-mgmt-sg を追加します。

注：検疫ポリシーを再度有効にするときは、セキュリティ上の理由から、これらのルールを削除してください。

タイプ	プロトコル	ポート	送信元
CUSTOM-TCP	TCP	8080	VPC-CIDR
CUSTOM-TCP	TCP	5555	VPC-CIDR

- 問題 2188950：API を使用して PCG のリストを取得するときに、「No VNet found for specified ID.」というエラーが表示される

このエラーは、展開された PCG に関連付けられたアカウントが CSM から削除されると発生します。

回避策：PCG を展開した CSM で、Microsoft Azure アカウントを追加します。

- 問題 2191571：PCG の展開は、PCG 展開の SSH パブリック キーの末尾が E メール ID でない場合、開始されません。

SSH パブリック キーの末尾は、E メール ID にする必要があります。そうでない場合、PCG 展開は開始されず、エラーが表示されます。

回避策：SSH キーの末尾を E メール ID にします。

- 問題 2092073：Windows ワークロード仮想マシンで、IPFIX テンプレートが正しく受信されない

IPFIX コレクタが仮想マシンと同じサブネットに構成されている場合、Windows ワークロード仮想マシンでは、論理スイッチとファイアウォールの IPFIX テンプレートはすぐには送信されません。これは、Windows ソケットで UDP パケットを送信する際に、IPFIX コレクタの IP アドレスに ARP エントリがあることが前提にされているためです。ARP エントリがない場合、最後のパケットを除くすべての UDP パケットはメッセージなしでドロップします。その結果、IPFIX コレクタでは、データ パケットがテンプレート情報なしで受信されます。

**回避策：**次のいずれかを実行します。

- 次のコマンドを使用して、IPFIX コレクタに固定 ARP エントリを追加します。

```
netsh interface ipv4 add neighbors "<Interface name>" <collector IP> <physical address of collector>
```

次はその例です。

```
netsh interface ipv4 add neighbors "Ethernet 3" 172.26.15.7 12-34-56-78-9a-bc
```

- IPFIX コレクタをワークロード仮想マシンとは別のサブネットに構成します。

- **問題 2210490：**CSM でプロキシ プロファイルを追加すると、以下のいずれかのロールが割り当てられているすべての CSM API ユーザーにパスワードが表示された状態になる： クラウド サービス監査者またはクラウド サービス管理者

CSM でプロキシ プロファイルを作成し、ユーザー名とパスワードを指定すると、パスワードが CSM ユーザー インターフェイスでは表示されていなくても、次の API への応答で表示されてしまいます。

- /csm/proxy-server-profiles
- /csm/proxy-server-profiles/<profile-id>

- **問題 2039804：**PCG の展開が失敗しても PCG インスタンスが AWS で終了しない  
PCG の展開中に展開が失敗しても、Amazon VPC 内の PCG インスタンスと、自動作成された NSX Manager 内の論理エンティティは表示され続けます。

**回避策：**自動作成された NSX Manager のエンティティを手動で削除し、Amazon VPC 内の PCG インスタンスを手動で終了させます。

## NSX Container Plug-in (NCP) に関する既知の問題

- **PAS 2.1.0 CNI の変更点**

PAS 2.1.0 での CNI プラグインの変更により、すべてのバージョンの NSX-T タイルが PAS 2.1.0 で動作しないこの問題は、PAS 2.1.1 で修正されました。

- **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。

- 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 `resove.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：NSX-T タイルが独自のルーターを展開する PAS 分離セグメントで機能しない

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。

- **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

## ドキュメントの修正と追加情報

- **問題 1372211：同じサブネット上の 2 つのインターフェイス**  
トンネルのエンドポイントが管理インターフェイスと同じサブネット上にある場合、トンネル トラフィックが管理インターフェイスに漏出する可能性があります。これは、トンネル パケットが管理インターフェイスを通るために発生します。管理インターフェイスをトンネル エンドポイントのインターフェイスとは異なるサブネット上に配置するようにしてください。