

VMware NSX-T Data Center 2.4 リリース ノート

VMware NSX-T Data Center 2.4 | 2019 年 2 月 28 日 | ビルド 12456646

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](#)
- [API および CLI リソース](#)
- [改訂履歴](#)
- [解決した問題](#)
- [既知の問題](#)

新機能

NSX-T Data Center 2.4 では、プライベート、パブリック、およびハイブリッド クラウドの仮想ネットワークとセキュリティに関連するさまざまな新機能が追加されています。主な新機能には、新しいインテント ベースのネットワーク ユーザー インターフェイス、コンテキスト認識ファイアウォール、ゲストおよびネットワーク イントロスペクション機能、IPv6、高可用性クラスタ化管理、vSphere コンピュート クラスタ用のプロファイル ベースの NSX インストール、NSX for vSphere コンピュートの再起動なしのメンテナンス アップグレード モード、vSphere コンピュート用の新しいインプレース アップグレード モード、NSX Data Center for vSphere から NSX-T Data Center に移行するための Migration Coordinator などがあります。

NSX-T Data Center 2.4 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。

管理クラスタ

NSX-T Data Center 2.4 では、ユーザー インターフェイスと API の高可用性を実現するために、マネージャのクラスタを作成する機能がサポートされるようになりました。このクラスタリングでは、外部バランサを使用した冗長性および負荷分散と、NSX が提供する仮想 IP アドレスを使用した冗長性の両方がサポートされます。また、NSX 管理を通じて展開と管理が必要になる仮想アプライアンスの数を減らすため、この新しい管理クラスタには、管理プレーン機能と中央制御プレーン機能が統合されています。さまざまな展開シナリオに対応できるように、3 つの異なるサイズの NSX Manager アプライアンスが提供されています。Small アプライアンスは、ラボや事前検証の展開に適しています。Medium アプライアンスは、64 台までのホストの展開に適し、Large アプライアンスは、大規模環境に展開するお客様に適しています。最大構成の詳細については、次のリンクから VMware 最大構成ツールを参照してください。 <https://configmax.vmware.com>

単一クラスタ設計のサポート

1 台の物理ホストにある単一の N-VDS で、Edge、管理、コンピューティング用のすべての仮想マシンが提供される単一クラスタ設計がサポートされます。VCF SP ユーザー向けの標準のリファレンス設計では、4 x 10G 物理 NIC で 2 台のホスト スイッチを使用し、1 台のスイッチを Edge と管理用、もう 1 台をコンピューティング仮想マシン用に使用しています。これにより、Edge 仮想マシンとコンピューティング仮想マシン間の通信が実質的に分離され、トラフィックをホストに戻すことができます。ただし、25G NIC がトレンドのため、VCF SP のユーザーは 2 x 25G NIC ホストで標準化を行っています。この設計を使用することで、2 つの物理 NIC を持つホストを提供する単一の N-VDS に移行できます。この設計では、ホストのアップリンクを離れて再びホストに戻るトラフィックがなくても、同じサブネットに属する Edge 仮想マシンとコンピューティング仮想マシンは通信を行うことができます。

ポリシーとユーザー インターフェイス

NSX 管理と自動化

- **宣言型ポリシー管理** - 結果主導型のポリシー ステートメントを使用して、ネットワークとセキュリティの構成を簡素化および自動化できます。この新しい宣言型ポリシー API は、ユーザーが目指す最終目標を記述できるようにすることで構成手順の数を減らし、それを達成するための最良の方法をシステムに判断させます。ネットワーク トポロジ全体を定義し、順序に依存しない規範的な方法でトポロジ全体を一括で展開できます。

ユーザー インターフェイスの強化

- **強化されたナビゲーションとページ レイアウト**：重要な情報にアクセスするためのクリック数を減らすために、ナビゲーション バーとページ レイアウトが強化されました。
- **利用可能な言語**：日付/時刻形式、数値形式、タイムゾーンなど、ロケール固有の項目の処理が強化されました。

注：バージョン 2.3 で導入された NSX Policy Manager のネットワーク トポロジ可視化機能は、今回のリリースで廃止されました。

ファイアウォール

NSX-T Data Center 2.4 以降では、分散ファイアウォールとゲートウェイ ファイアウォールで、IPv6 トラフィックのフィルタリングがサポートされます。また、以下の操作機能が製品に追加されています。

[発行][元に戻す] ボタン

1 個の [発行] ボタンで、ファイアウォール テーブル全体に対応できるようになりました。この機能は、分散ファイアウォールとゲートウェイ ファイアウォールの両方に対して使用できます。NSX-T Data Center 2.4 より前のバージョンでは、セクションごとに [発行] ボタンが存在していました。この機能は API を介して使用することもできます。また、変更を元に戻すオプションも追加されました。さらに、変更が更新されたときにセクションをロックするオプションも追加されました。

ルールの統計情報

各ルールで、ヒット数、パケット数、セッション数、バイト数、およびポピュラリティ指数を指定できるようになりました。また、観測された最大値と現在のヒット数の比率も表示されるようになりました。この統計情報は、ボタンでリセットできます。

グループ分けの強化

仮想マシンのオペレーティング システムや Active Directory グループに基づく新しいグループ分け条件が追加されました。

仮想マシンごとのルールの表示

仮想マシンごとの論理スイッチ ポートの関連付けを調べることで、特定の仮想マシンに適用されているファイアウォール ルールのリストを確認できるようになりました。

仮想マシンの IP アドレス検出

既定の IP アドレス検出プロファイルが更新され、ARP スヌーピングと DHCP スヌーピングに加えて、VMware Tools ベースの IP アドレス検出も含まれるようになりました。以前のリリースからアップグレードするお客様は、VMware Tools ベースの検出を有効にするために、IP アドレス検出プロファイルを更新する必要があります。さらに、NSX-T 2.4 では、グローバル IP アドレス検出プロファイルの作成がサポートされています。また、以下の変更も行われています。

1. DHCPv6 に基づく IPv6 IP アドレス検出および近隣探索メカニズムを利用できるようになりました。
2. デフォルトでは、IPv6 検出は無効になっています。
3. 自動検出された IP バインドをホワイトリストまたは除外リストに手動で追加できるようになりました。
4. デフォルトでは、ローカル リンク IPv4 アドレスは無視されます。

Identity Firewall

NSX-T Data Center 2.4 では、分散ファイアウォール用に、ID (ユーザー ID) ベースのルールが導入されています。ファイアウォール管理者は、Active Directory ベースのグループに基づいて仮想マシンに分散ルールを設定できるようになりました。この機能を使用すると、ファイアウォール管理者は、仮想マシンにログインするユーザーごとにファイアウォール ルールを設定できます。NSX はログイン/ログオフしたユーザーを自動検出し、そのユーザーに固有のルールを有効にします。ID ベースのファイアウォールでは、仮想マシンにログインしている各ユーザーを検出して、そのユーザーに固有のルールを適用できます。また、同じ仮想マシン内で特定のセッションを実行している複数のユーザーを追跡することもできます。ファイアウォール管理者は、Active Directory グループを条件として使用して、NSX-T グループを作成します。NSX-T Manager は、指定されたドメイン コントローラから自動的に Active Directory グループのリストを取得します。ファイアウォール管理者は、仮想デスクトップ環境や、ターミナル サービスが有効になっているリモート デスクトップ セッションにおけるユーザーの East-West アクセスを制御できます。

コンテキスト認識分散ファイアウォールの L7 アプリケーション署名

NSX-T Data Center 2.4 では、分散ファイアウォール ルールの L7 ベース アプリケーション署名がサポートされています。ユーザーは、L3/L4 ルールと L7 アプリケーション署名を組み合わせて使用することも、L7 アプリケーション署名ベースのルールのみを作成することもできます。従来、各種のサブ属性を含むアプリケーション署名は、サーバ間通信およびクライアント/サーバ間通信に対してのみサポートされていました。NSX-T Data Center 2.4 では、ESXi ベースのトランスポート ノードに対してのみ、この機能がサポートされます。

コンテキスト認識分散ファイアウォールの FQDN/URL ホワイトリスト

NSX-T Data Center 2.4 では、分散ファイアウォールに URL/FQDN ホワイトリスト ベースのルールが導入されています。NSX-T Data Center では、分散 DNS スヌーピングを使用して各仮想マシンからの接続ごとに URL/FQDN を解決する革新的な手法が導入されています。ファイアウォール管理者は、事前に準備された URL ドメインを分散ファイアウォールのルールに適用することができます。SaaS サービスまたはクラウド ベースのサービスにアクセスするハイブリッドな性質を持つアプリケーションは、アクセスする URL を基準としてマイクロセグメンテーションを実行できます。SaaS アプリケーションにアクセスするクライアント アプリケーションやブラウザには、きめ細かく設定したアクセス許可を付与できます。NSX-T Data Center 2.4 では、ESXi ベースのトランスポート ノードに対してのみ、この機能がサポートされます。

サービス挿入

NSX-T Data Center 2.4 では、レイヤー 7 アプリケーション ID、FQDN ホワイトリスト、Identity Firewall など、さらに細かいマイクロセグメンテーションを可能にする、幅広いネイティブ セキュリティ機能が導入されています。分散ファイアウォールおよびゲートウェイ ファイアウォールによって提供されるネイティブ セキュリティ制御に加え、NSX サービス挿入フレームワークを使用すると、IDS/IPS、NGFW、ネットワーク監視ソリューションなど、さまざまなタイプのパートナー サービスをデータ パスに透過的に挿入し、トポロジの変更なしで NSX 内からそれらのサービスを使用できます。

NSX-T Data Center 2.4 では、サービス挿入で East-West トラフィック（データセンターの仮想マシン間のトラフィック）がサポートされるようになりました。データセンター内の仮想マシン間のすべてのトラフィックは、パートナー サービスの動的なチェーンにリダイレクトできます。

E-W サービス プレーンは、サービスのチェーンに沿ってトラフィックをポリシー ベースでリダイレクトできる独自の転送メカニズムを備えています。サービス プレーンに沿った転送はプラットフォームによって完全に自動化されます（自動的にエラーが検出され、既存または新規のフローが適切にリダイレクトされ、ステートフルサービスをサポートするためにフローが固定化されます）。また、スループット/遅延または集約度を最適化できるように、複数のパス選択ポリシーが用意されています。

ゲスト イントロスペクション

NSX-T Data Center 2.4 では、VMware パートナー向けにゲスト イントロスペクション サービス プラットフォームが導入されています。これにより、vSphere ESXi ハイパーバイザー上の Windows ベースのゲスト仮想マシン ワークロードに対して、ポリシー ベースのエージェントレス アンチウイルス機能やアンチマルウェア オフロード機能を提供することができます。

NSX-T Data Center 2.4 のゲスト イントロスペクション プラットフォームには、以下の特徴があります。

- ゲスト イントロスペクション展開が NSX Agent ホスト準備インストールに統合され、ゲスト イントロスペクション ユニバーサル サービス仮想マシンを各 ESXi ハイパーバイザーに展開する必要がなくなったため、展開とライフサイクル管理が簡素化されました。
- 複数の vCenter Server 間で一貫したポリシー ベースのサービスが提供されます。
- パートナー SVM のサイズ（「小規模」、「中規模」、「大規模」パートナー アプライアンス）を選択できるようになったことで、VMware パートナーの選択の幅が広がりました。

L2 ネットワーク

ホストごとに複数の N-VDS

各ホストで複数の N-VDS をサポートできるようになったため、仮想マシン トラフィックを柔軟に整理だけでなく、仮想マシン トラフィックを厳密に分離することを義務付けている PCI 規制への準拠が容易になりました。

この機能の追加により、ENS アップリンクを非 ENS アップリンクから分離できるようになりました。現在のところ、ENS と N-VDS の機能に等価性はなく、ENS を使用したワークロードは高速になるものの、機能が少なくなるため、この分離機能は便利です。

N-VDS の可視化

この機能を使用すると、N-VDS をスタンドアロン オブジェクトとして管理し、接続されているホストなどをドリル ダウンして確認できます。特定のホストを選択すると、N-VDS への接続状態がユーザー インターフェイスのグリッドに表示されます。また、仮想マシン カーネル インターフェイスなどの論理インターフェイスも、N-VDS の一部として表示されます。このように、すべての物理 NIC、仮想マシン カーネル インターフェイス、OVS ポートを含むインターフェイスのリストが 1 つのビューに表示されるようになったことで、ホスト ビューの利便性が大幅に向上しています。

物理 NIC での LLDP のサポート

この機能は、NSX の LLDP 実装におけるギャップを埋めるのに役立ちます。この機能を使用することで、物理スイッチ接続のデバッグが可能になります。どの物理ポートがホスト上のどのインターフェイスに接続されているかを確認できるため、ケーブル配線の問題を簡単に解決できます。この機能は、NSX データプレーンに参加するすべての物理ホスト（ESXi、KVM、Baremetal Linux ホスト、および Baremetal Edge）に適用されます。

Edge ノードでのプロキシ ARP のサポート

外部クライアントが同じサブネット アドレスで LB や IKE などのサービスにアクセスすると、デバイス ルーティングが発生します。外部クライアントはループバック ポートにバインドされているアドレスに対して ARP クエリを送信しますが、LR ループバック ポートには MAC アドレスがないため、これらの ARP クエリには応答しません。そのため、アクセスの問題が生じます。

現時点での回避策は、ループバック IP/32 → アップリンク/CSP のように、これらのクライアントで /32 ルーティングを設定し、トラフィックをアップリンク/CSP ポートに転送して、最終的に正しいループバック ポートに転送されるようにすることです。ARP プロキシを使用すれば、この問題を正しく解決できます。

L3 ネットワーク

MTU 設定の機能強化

NSX-T 2.4 では、次の 2 つの MTU グローバル パラメータが追加されています。

- グローバル物理アップリンク MTU。NSX ドメイン内のすべての N-VDS インスタンスの MTU を構成します。これは、GENEVE カプセル化フレームまたは TEP MTU の最大フレーム サイズに変換できます。
 - アップリンク プロファイル MTU は、特定のホストのグローバル物理アップリンク パラメータよりも優先させることができます。
- グローバル論理インターフェイス MTU。すべての論理ルーター インターフェイスの MTU を構成します。
 - 論理ルーター アップリンク MTU および CSP ポート MTU は、必要に応じ、特定のポートでグローバル論理インターフェイス MTU よりも優先させることができます。

これにより、East-West および North-South トラフィックの MTU が 1,500 バイトより大きく設定された仮想マシンのエンドツーエンド通信が可能になります。

サービス ルーター間ルーティング

アクティブ/アクティブ モードの Tier-0 論理ルーターが、特定の Tier-0 論理ルーターのサービス ルーター (SR) 部分全体にわたり、フル メッシュの iBGP ピアリングを自動的に確立できるようになりました。これにより、SR に複数のアップリンクが設定されていて、そのうちの 1 つのみに障害が発生した場合に、トラフィックのドロップが発生しなくなります。この障害シナリオにおいて、特定の SR が自身のアップリンクを通じて宛先に到達できないときは、他の SR にトラフィックが転送されます。

DNS フォワーダの機能強化

- 現在の設定を失うことなく、DNS フォワーダ機能を有効または無効にできるようになりました。
- DNS フォワーダ機能は、API およびユーザー インターフェイスを通じて、統計情報、イベント、およびアラームも公開します。

アップリンクからアップリンクへの SNAT のサポート

NSX-T 2.4 では、アップリンクを介して Tier-0 論理ルーターに入り、別のアップリンクを介して同じ論理ルーターから出て行くトラフィックに対する SNAT（送信元アドレス変換）がサポートされるようになりました。この機能は、複数の Tier-0 論理ルーターが相互接続されている場合に役立ちます。

Tier-0 論理ルーターでのプロキシ ARP のサポート

NSX-T 2.4 では、Tier-0 論理ルーター アップリンクでプロキシ ARP がサポートされるようになりました。これにより、Tier-0 論理ルーターの North バウンド ルーターでルーティングを設定できない環境でも、NSX-T の展開が可能になります。この機能を使用すれば、Tier-0 アップリンクのネットワークに属する IP アドレスを、NAT、LB、または任意のステートフル サービスで設定できます。

Edge ノードの機能強化

- NSX-T 2.4 では、高速パス NIC での管理をサポートするために、ベア メタル Edge ノードのオプションが導入され、専用の管理 NIC が不要になりました。
- ベア メタル Edge ノードでは、25 Gbps の Intel NIC XXV710 もサポートされます。
- Edge ノードでは、複数の GENEVE トンネル エンドポイント (TEP) がサポートされます。これにより、オーバーレイ トラフィックの高可用性を実現するために Edge ノードで LAG の使用を強制する必要がなくなります。

BGP の機能強化

- NSX-T 2.4 以降では、Tier-0 論理ルーターにより、North バウンド物理ルーターとの iBGP ピアリングがサポートされます。
- NSX-T 2.4 では、異なる ASN の eBGP ピア間で ECMP を有効にするオプション (as-path multipath relax) が導入されています。また、Tier-0 論理ルーターが AS パス上で独自の ASN を許可するオプション (allow-as in) も導入されています。

IPv6

NSX-T 2.4 では、IPv6 ルーティング/転送とセキュリティが導入されています。これには以下のサポートが含まれます。

- IPv6 スタティック ルーティング
- IPv6 近隣探索
- DHCPv6 リレー
- IPv6 分散ファイアウォール (DFW)
- IPv6 Edge ファイアウォール
- MP-BGP および関連するプレフィックス リスト/ルートマップの IPv6 アドレス ファミリ
- IPv6 スイッチ セキュリティ
- IPv6 アドレス検出
- IPv6 運用ツール

運用

トレースフローの機能強化

トレースフローに、新しいトラブルシューティング機能と可視化機能が追加されました。NSX-T 2.4 のトレースフローでは、Edge ファイアウォール、ロード バランサ、NAT、ルート ベース VPN などの統合サービスを観測することができます。

インストールの機能強化

- vSphere コンピュート クラスタ用に NSX コンポーネントをインストールする際、プロファイル ベースの新しいインストール機能を使用することで、NSX の展開が簡素化されました。この機能を使用すると、迅速な展開が可能になるだけでなく、設定の一貫性が向上し、手動設定によるエラーを回避でき、1 度定義すれば何度でも再利用できるようになります。
- ユーザー インターフェイスからの NSX Manager ノードのインストールとクラスタリングを自動化できるようになりました。
- 新しい展開設定が追加され、プロファイルを介して複数の N-VDS スイッチを作成し、VMKernel ポートおよび物理アダプタを移行できるようになりました。

アップグレードの機能強化

- ホストの再起動が必要となるデフォルトのメンテナンス モード NSX アップグレードを使用せずに、環境全体で ESXi ホストのアップグレードを完全に調整できるようになりました。
- 「インプレース アップグレード」と呼ばれる新しい NSX アップグレード モードが導入されました。この機能により、運用が簡素化され、迅速なアップグレードが可能になります。このモードを使用すると、ワークロードをパワーオフしたり、別のハイパーバイザーに移行したりすることなく、ESXi ホスト上の NSX コンポーネントをアップグレードできます。
- 新しいフレームワークが導入され、NSX をアップグレードする際に、特別な設定を行うことなく、事前チェック テスト/事後チェック テストを実行できるようになりました。これにより、アップグレードの実行前や実行直後に潜在的な問題を明らかにすることができます。

変更検出時の NSX のバックアップ

構成の変更を検出し、万が一に備えて安全なストレージにバックアップする機能が NSX のディザスタ リカバリソリューションに追加されました。この機能を使用すると、不要なファイルをストレージ サーバにバックアップする必要がなくなるため、構成バックアップの SLA（サービス レベル アグリーメント）を強化できます。

NFV

N-VDS スイッチの EDP モードで次の機能が強化されました。

- 分散ファイアウォール
- IP アドレス検出
- SpoofGuard
- IPFIX
- IPv6
- Edge 仮想マシンのパフォーマンスが強化され、EDP モードのスループットが最大で 5 倍になりました。
- マルチホーム構成アプリケーションのパス冗長性。仮想マシンを特定のアップリンクに固定できるようになり、VTEP を含む NSX でマルチホーム構成の冗長パスを構築できるようになりました。

運用 - AAA/RBAC およびプラットフォーム セキュリティ

運用

- **プリンシパル ID の機能強化**：プリンシパル ID ユーザーが NSX コンポーネントの登録とインストールを行えるようになりました。また、ユーザー インターフェイスからプリンシパル ID ユーザーの作成とロールの割り当てを行えるようになりました。
- **パスワード ポリシーの機能強化**：デフォルトのパスワードの最小長が 12 文字になりました。パスワードの有効期限を設定し、期限が近づくとアラームを生成する機能が導入されました。デフォルトでは、パスワードは 90 日で有効期限が切れます。パスワードをリセットしてパスワードの有効期限を調整する手順については、ナレッジベースの記事 [KB70691](#) を参照してください。
- **証明書の管理**：証明書の失効状態をチェックする機能が追加されました。

VPN

NSX-T 2.4 では、VPN サービスに次の機能が追加されています。

- L3 VPN サービスおよび L2 VPN サービスの両方に対して、ポリシー API と GUI を利用できるようになりました。
- L3 VPN サービスで証明書ベースの認証がサポートされ、セキュリティ管理が強化されました。
- NSX-T の SDDC から NSX-T の SDDC への L2 エクステンションをサポートする L2 VPN クライアント モードを利用できるようになりました。
- DH グループ 19、20、21 を利用して高度なセキュリティ要件を満たせるようになりました。

ロード バランシング

NSX-T 2.4 では、ロード バランシング サービスに次の機能が追加されています。

- ポリシー API と新しい GUI を利用できるようになりました。ロード バランサ GUI は、従来どおり、[ネットワークとセキュリティの詳細設定] タブで利用できます。
- スタンドアロン SR の仮想 IP アドレスを中央のサービス ポート (CSP) と同じサブネットに所属させることができるようになりました。本リリース以前は、CSP ネットワークと同じサブネット内に仮想 IP アドレスを作成する場合、CSP の IP アドレスを仮想 IP アドレスとして使用する必要がありました。あるいは、別のネットワーク上で仮想 IP アドレスを作成する必要がありました。
- 同じ Tier-1 ゲートウェイ上のロード バランサ トラフィック フローに対して、DNAT および Edge ファイアウォールがサポートされるようになりました。本リリース以前は、ロード バランサ トラフィック フローは、Edge ファイアウォールを経由していませんでした。
- LB ルールで、「」から始まる HTTP ヘッダーがサポートされるようになりました。この機能拡張により、vIDM および AirWatch に NSX ロード バランサを展開できるようになりました。
- LB SNAT の送信元 IP アドレスとして、仮想 IP アドレスを使用できるようになりました。
- HTTP 応答ヘッダーの最大サイズを 64 KB まで設定できるようになりました。デフォルトのサイズは、以前のリリースと同じく 4 KB のままです。
- 大規模な Edge 仮想マシンで大規模な LB インスタンスがサポートされるようになりました。本リリース以前は、大規模な Edge 仮想マシンで中規模の LB インスタンスまでしかサポートできませんでした。

NSX Data Center for vSphere から NSX-T Data Center への移行

NSX-T 2.4 に Migration Coordinator が追加され、NSX Data Center for vSphere から NSX-T Data Center への移行が容易になりました。この機能は、vMotion を使用せずに既存のホストを移行することを目的としています。

Migration Coordinator は、レイヤー 2 ネットワーク、レイヤー 3 ネットワーク、ファイアウォール、ロード バランシング、および VPN の移行をサポートしています。このツールの詳細については、『*NSX-T Data Center Migration Coordinator ガイド*』を参照してください。

移行は NSX-T Manager および Edge ノードを導入するだけで完了し、その他のコンピューティング リソースを追加する必要はありません。移行が完了した後は、NSX for vSphere、および関連する Manager、Controller、Edge をアンインストールできます。この移行は、データ プレーン トラフィックに影響を与えます。また、この移行は、1 つの変更ウィンドウ内で完了するように設計されています。

自動化、OpenStack、その他の CMP

Neutron プラグインを介して OpenStack を利用できるように、NSX-T 2.4 では、次の機能が導入されています。

- Rocky および Queens のサポート
- 管理プレーン クラスタリングのサポート
OpenStack Neutron プラグインでは、Manager のクラスタを作成する新しい機能が利用されます。このプラグインでは、パフォーマンスと可用性を強化するために、外部の仮想 IP アドレスなしで、3 つの Manager の REST API エンドポイントを使用できます。
- Barbican のサポート
OpenStack Neutron プラグインで、Barbican がサポートされるようになりました。Barbican は、ストレージのセキュリティを確保し、パスワード、暗号化キー、X.509 証明書などの秘密データのプロビジョニングと管理を行うために設計された REST API です。この機能を使用すると、ロード バランサ サービスが HTTPS ターミネーションを行うために使用する証明書を管理できます。この機能は、現在、VIO 環境のみでサポートされます。

NSX-T 2.4 では、既存の機能（論理スイッチ、ルーター、ファイアウォール ルールの作成など）に加えて、次の機能が NSX-T の Terraform プロバイダに追加されています。

- ロード バランサの CRUD およびロード バランサの構成（監視、プールなど）をサポートする機能
- DHCP サーバで CRUD をサポートする機能

- NSX-T の IP アドレス管理 (IP アドレス ブロック、IP アドレス プール) で CRUD をサポートする機能

NSX Cloud

NSX-T 2.4 for NSX Cloud では、お客様による採用および導入の円滑化、サービス挿入方法に関するオプションの拡充、VPN の終端、VDI 環境の管理とそれによるマルチリージョンかつマルチクラウドのハイブリッド環境の管理のためのさまざまな新機能が追加されています。

以下は、NSX-T 2.4 により実現する NSX Cloud の主な機能の一部です。

- トランジット VPC/VNET でゲートウェイを共有することによるオンボーディングと統合の簡素化および迅速化
- オンプレミス DC に戻るバックホール トラフィックのための VPN
- 選択的 North-South サービス挿入とパートナー統合
- Horizon Cloud for Azure でのマイクロセグメンテーション
- ハイブリッド ワークロード用のインテントベース ポリシー

トランジット VPC/VNET のアーキテクチャ簡素化：2.4 以降では、1 つの NSX Cloud ゲートウェイをトランジット VPC/VNet にインストールし、最大 10 個までのコンピュート VPC/VNet を管理できます。これにより、ハブアンドスポークのトランジット/コンピュート アーキテクチャが簡素化され、ピアリング接続がない場合でも、コンピュート VPC 間のトランジット ルーティングが可能になります。NSX オーバーレイ トンネルを使用して、VPC 間のトラフィックをオーバーレイ トンネルで送信できるようになりました。転送ポリシーを仮想マシン レベルで設定し、トラフィックが Geneve でカプセル化されてオーバーレイで送信されるのか、パブリック クラウド プロバイダのアンダーレイ ネットワークで送信されるのかを指定できます。これらの機能を使用すると、パブリック クラウド ネットワークの内外でのトラフィックのルーティング方法をより柔軟に設定できます。

バックホール トラフィックのための VPN：NSX Cloud で、パブリック クラウドからオンプレミスのデータセンターに向かうバックホール トラフィックのための VPN トンネルが、新たに組み込みでサポートされるようになりました。オンプレミスのデータセンターを起点とする VPN については、パブリック クラウドの NSX Cloud Gateway を直接終端とすることができるようになりました。パブリック クラウド ベンダーが提供する VGW が必要なくなるため、コストを削減できます。このほか、NSX Cloud Gateway により BGP に基づく経路が自動で指定されるので、管理業務の負担も軽減できます。BW の観点では、NSX Cloud の利用にはキャパシティが大きく増大するというメリットもあります。VPC 間のトラフィック フローは、VGW では 1 Gbps なのに対し、ピアリングを施した VPC では 5 Gbps にもなります。

選択的 North-South サービス挿入とパートナー統合：共有サービス/トランジット アーキテクチャでは、パブリック クラウド マーケットプレイスから直接パートナー サービスを展開できるようになりました。プログラミングにより、トランジット VPC/VNET に配置されている NSX Cloud Gateway に対して、NSX ポリシーに応じてパートナー サービス アプライアンスにトラフィックを選択的にルーティングするような設定が可能です。この設定により、一部のトラフィックは、パブリック クラウド用に購入した仮想 L7 ファイアウォール アプライアンスを経由する必要がなくなります。このアプライアンスは経由したトラフィック量に基づいて課金されるため、コストを大きく削減できます。さらに、NSX Cloud によるサービス挿入ではコンピュート VPC/VNET への VPN が不要になります。これにより、コストと手間をさらに削減できます。

Horizon Cloud for Azure でのマイクロセグメンテーション：NSX Cloud に、Horizon Cloud for Azure との連携に対応したソリューションを新たに追加しました。NSX Cloud では、Azure に Horizon VDI 環境を構築するお客様向けに、マイクロセグメンテーションと VDI 環境のセキュリティ保護の機能を提供しています。

ハイブリッド ワークロード用のインテントベース ポリシー：Cloud Service Manager (CSM) を NSX Manager に統合しました。これにより、ワークロードの展開場所や、将来的にワークロードを移行する場所を気にすることなく、Policy Manager からインテントベースのポリシーを定義できるようになりました。NSX Cloud では、このポリシーをオンプレミス データセンター、Azure、AWS にわたり一貫した方法で反映します。

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。

API および CLI リソース

NSX-T Data Center の API または CLI を自動化に使用する場合には、code.vmware.com を参照してください。

API ドキュメントは、[API Reference (API リファレンス)] タブから利用できます。CLI ドキュメントは、ドキュメント タブから利用できます。

ドキュメントの改訂履歴

2019 年 2 月 28 日初版。

2019 年 4 月 2 日第 2 版。既知の問題に追加した問題：2273651、2279326、2281095、2296888。解決した問題に追加した問題：2199785。

2019 年 4 月 10 日第 3 版。既知の問題に追加した問題：2203863、2248186、2252738、2277543、2276398、2279326、2281537、2287124、2290688、2294178、2295592、2296430、2297157、2297918、2298499。「新機能」セクションを更新し、単一クラスタ設計のサポートを追加しました。

2019 年 6 月 20 日第 4 版。既知の問題 2261818 について記載しました。解決した問題 2182745 について記載しました。

2019 年 8 月 23 日第 5 版。既知の問題 2362688、2395334、2392093 について記載しました。

解決した問題

- 解決した問題 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。
- 解決した問題 2279326：4 個を超える IP アドレスとポートの組み合わせを持つ IPFIX L2 コレクタを作成してもエラーが表示されない
IP アドレスとポートの組み合わせの最大数を超えても、エラー メッセージが表示されません。最大数の制限を超えると、UI でタグの作成が制限されるため、問題はありません。
- 解決した問題 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 (pnict) 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。
- 解決した問題 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。

- **解決した問題 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。
- **解決した問題 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。
- **解決した問題 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。
- **解決した問題 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。
- **解決した問題 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。
- **解決した問題 2114756**：NSX-T 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
NSX-T で作成したクラスタからホストを削除するときに、一部の VIB がホストに残ることがあります。
- **解決した問題 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。
- **解決した問題 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。
- **解決した問題 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。
- **解決した問題 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。

- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 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、中央のサービス ポートと VLAN 論理スイッチを作成すると、中央のサービス ポートを編集する場合に、新規作成した VLAN 論理スイッチを表示できません。
- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 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場合があります。
- 解決した問題 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。

- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 2199785：健全性モニター（ポート番号なし）をダイナミック プール（ポート番号あり）に追加すると NGINX Core が発生する
動的メンバー（ポート番号あり）を持つサーバ プールでロード バランシングを構成した後、監視ポートが設定されていない健全性モニターを関連付けようとする、nginx がクラッシュすることがあります。
- 解決した問題 2182745：再配分ルールの le/ge がマネージャで検証されず、正常に機能しない
再配分ルールで、プレフィックス リスト内の le/ge がサポートされます。

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](#)

一般的な既知の問題

- 問題 2239365：「承認されていない」というエラーが表示される
ユーザーが種類の同じブラウザで認証セッションを複数開こうとすると、このエラーが発生することがあります。このエラーが発生すると、ログインに失敗して認証できません。ログの場所：`/var/log/proxy/reverse-proxy.log` `/var/log/syslog`

回避策：認証のウィンドウやタブをすべて閉じてから、認証をもう一度やり直してください。

- 問題 2287482：自動検出されたバインド テーブルに、現在検出されたものではないバインドが含まれていることがある
自動検出されたバインド テーブルで「重複」しているものとしてマークされているバインドが、検出されなくなることがあります。

回避策：なし。

- 問題 2278142：スイッチの IPFIX グローバル プロファイルを編集できない

システムにグローバル プロファイルがあると、グローバル プロファイルに対応するワークフローがないため、インターフェイスを使用して編集や削除ができません。

回避策：API を使用して問題のグローバル プロファイルを削除してください。

- **問題 2292222**：サムプリントが正しくない場合に、[エラーの解決] 画面で通知が表示されない
ホストの準備の処理に失敗した場合には、[NSX インストール失敗] をクリックして問題を解決できます。その際、ユーザー名、パスワード、およびホストのサムプリントを指定する必要があります。ユーザーが指定したサムプリントが正しくなかった場合でも、ユーザーに通知されることがないため、問題が解決されずに残ってしまいます。

サムプリントが正しくないことを確認できる確実な方法はありません。この `ThumbPrintValidationFailedException` が記録されているログを確認してください。

回避策：正しいサムプリントを指定してください。

- **問題 2252487**：複数のトランスポート ノードが並行して追加されると、BM エッジ トランスポート ノードのトランスポート ノードの状態が保存されない
管理プレーンのユーザー インターフェイスで、トランスポート ノードの状態が正しく表示されません。

回避策：

1. Proton を再起動すると、トランスポート ノードの状態がすべて正常に更新されます。
2. このほか、API (<https://<nsx-manager>/api/v1/transport-nodes/<node-id>/status?source=realtime>) を使用してトランスポート ノードの状態を照会することもできます。

- **問題 2285117**：NSX の管理対象仮想マシンでカーネルのアップグレードがサポートされない
一部の Linux Ubuntu マーケットプレイス イメージでは、仮想マシンの再起動時にカーネル自体が自動的にアップグレードされます。その結果、NSX Agent が想定どおりに機能しなくなります。NSX Agent が機能しているように見えても、一部のネットワーク ポリシーが認識されていないため、NSX Agent に影響が発生します。エージェントはこれらのポリシーの認識を繰り返し試行するため、CPU 使用率が増大します。

回避策：カーネルのアップグレードが必要であれば、新しいカーネルの適切な Linux ヘッダーをダウンロードしたうえで、`openvswitch-datapath-dkms` パッケージを再コンパイルする必要があります。

- **問題 2285544**：`ssh_fingerprint` の値の指定が必要な NSX API を呼び出す際に、MD5 ハッシュがサポートされていない
NSX-T 2.4 では、FIPS に準拠していない暗号化アルゴリズム、ハッシュなどがサポートされなくなりました。これには、バックアップリストア、ファイルストア、およびサポート バンドル NSX API の呼び出しや、`ssh_fingerprint` の値への MD5 ハッシュの指定が含まれます。このため、MD5 ハッシュはサポートされなくなりました。

回避策：SHA256 など、別のハッシュ アルゴリズムを使用して計算したハッシュ値を指定してください。

- **問題 2256709**：vMotion の実行中に、インスタント クローン仮想マシン（スナップショットから復元した仮想マシン）で一時的に AV 保護が失われる
スナップショットから仮想マシンを復元し、その仮想マシンを別のホストに移行した際に発生します。移行後のインスタント クローン仮想マシンについて、パートナー コンソールに AV 保護の情報が表示されません。AV 保護が一時的に失われます。

回避策：なし。

- **問題 2261431**：他の展開のパラメータによっては、フィルタ適用後のデータストア一覧が必要になる
選択したオプションが正しくない場合には、それに応じたエラーがユーザー インターフェイスに表示されます。エラーが発生した展開を削除して新しい展開を作成すると、エラーが表示されなくなります。

回避策：クラスタ化された展開を作成する場合には、共有データストアを選択してください。

- 問題 2266553：NSX アプライアンスで、サービスを初めて起動したときに初期化に失敗することがある

展開されたノードが要求を処理できないか、クラスタを形成できません。

回避策：エラーが発生したサービスを再起動してください。

- 問題 2267632：GI 保護の設定が失われる

ポリシー ユーザー インターフェイスに公開したゲスト保護ルールに「成功」の文字が表示されます。ゲスト仮想マシンには、対応する動作の変更が反映されていません。同じ時点の OpsAgent ログでは、再起動したという記録があります。ゲスト仮想マシンの保護が失われています。

回避策：設定の変更を手動でもう一度行ってください。

- 問題 2269901：パケット キャプチャ CLI に vmk インターフェイスが含まれていない

このコマンドは実行できません。

回避策：パケット キャプチャ uw を使用してください。

- 問題 2274988：サービス チェーンで同じサービスの連続するサービス プロファイルがサポートされない

サービス チェーンに同じサービスに属するサービス プロファイルが 2 つ連続して存在していると、トラフィックはサービス チェーンを経由しないため、トラフィックがドロップします。

回避策：所属するサービスが同じサービス プロファイルが 2 つ連続しないように、別のサービスのサービス プロファイルを追加してください。このほか、連続する元の 2 つと同じ処理を実行する第 3 のサービス プロファイルを定義して、サービス チェーンでそのプロファイルを単独で使用方法も有効です。

- 問題 2275285：ノードがクラスタに参加するための要求を実行した場合に、その要求が完了してクラスタが安定するよりも前に、同じクラスタを対象とする 2 回目の参加要求が実行される

クラスタが正しく機能しなくなり、CLI コマンド (get cluster status または get cluster config) を実行したときにエラーが返されることがあります。

回避策：最初に参加要求を出してから 10 分間は、同じクラスタに参加するための join コマンドを新たに実行しないようにしてください。

- 問題 2275388：ルートを拒否するフィルタが追加される前に、ループバック インターフェイス/接続済みインターフェイスのルートが再配分されることがある

不要なルート更新により、トラフィックの分散に数秒から数分程度かかるようになることがあります。

回避策：なし。

- 問題 2275708：プライベート キーにパスフレーズが設定されていると、証明書と一緒にプライベート キーをインポートできない

返されるメッセージは「証明書の無効な PEM データを受け取りました。(エラー コード: 2002)」です。新しい証明書とプライベート キーと一緒にインポートすることができません。

回避策：

1. 証明書とプライベート キーを作成します。新しいパスフレーズの設定を求めるメッセージが表示されたら、パスフレーズを入力せずに Enter キーを押してください。

2. [証明書をインポート] を選択して、証明書ファイルとプライベート キーファイルを選択します。

確認のため、キーファイルを開きます。キーの生成時にパスフレーズを入力していると、ファイルの 2 行目に「Proc-Type: 4,ENCRYPTED」のような文言があります。

キーファイルの生成時にパスフレーズを指定しなかった場合には、この行がありません。

- 問題 2275985：論理スイッチに接続されていない vNIC が、NSGroup の直接メンバーのオプション

として表示されない

この問題は、論理スイッチに接続されていない vNIC を NSGroup の直接メンバーとして追加した際に発生します。操作は成功しますが、そのグループに対して適用されるポリシーが vNIC に適用されません。

回避策：なし。

vNIC を NSGroup の直接メンバーとして追加する前に、その vNIC が論理スイッチに接続されているかどうかを確認してください。

- 問題 2277742：NSX-T Manager アプライアンスにホスト名ではなく完全修飾ドメイン名 (FQDN) が設定されていると、要求の本文で `publish_fqdns` を `true` に設定した PUT `https://<MGR_IP>/api/v1/configs/management` が失敗することがある
FQDN が設定されている状態では、PUT `https://<MGR_IP>/api/v1/configs/management` を呼び出すことはできません。

回避策：NSX Manager の展開にあたっては、FQDN ではなくホスト名を使用してください。

- 問題 2279249：vMotion の実行中に、インスタント クローン仮想マシンで一時的に AV 保護が失われる
この問題は、インスタント クローン仮想マシンをあるホストから別のホストに移行すると発生します。移行直後に EICAR ファイルが仮想マシンに残された状態になります。そのため、AV 保護が一時的に失われます。

回避策：なし。

- 問題 2290669：仮想サーバの数が増えるにつれて、それぞれの設定にかかる時間が増える
仮想サーバの数が増えると、それに従って検証の件数が増え、それぞれの設定にかかる時間が増大します。最初の 100 台については、平均応答時間は 1 秒前後です。250 台目以降は、平均応答時間が 5 ～ 10 秒になります。450 台以降は、応答時間が約 30 秒にまで増大します。

回避策：なし。トポロジによっては、仮想サーバを複数の LbService として設定することができます。この方法が使えない場合には、仮想サーバを備えた大規模環境の設定では応答時間が長くなることを想定しておいてください。

- 問題 2292116：IPFIX L2 の画面でグループを作成するときに、IPFIX L2 の [適用先] に CIDR ベースの IP アドレス グループが一覧表示されない
[適用先] ダイアログから IP アドレスのグループを作成し、[メンバーの設定] ダイアログ ボックスで正しくない IP アドレスまたは CIDR を入力すると、このメンバーはグループに表示されません。再度グループを編集し、正しい IP アドレスを入力する必要があります。

回避策：グループの表示画面に移動し、このグループに IP アドレスを追加します。これで、[適用先] ダイアログでグループが入力されます。

- 問題 2294821：NSX アプライアンスの情報がクラスタ監視ダッシュボードでエラー「ノードを削除できません」とともに表示され、この状況の対処方法も表示されない
この問題は、自動展開されたノードをユーザーがインターフェイスから削除し、そのノードのパワーオフに失敗した後に確認されています。クラスタでノードが失われた場合、新しいノードを手動で追加し、以下の回避策を実行して構成の状態をクリーンアップする必要があります。

回避策：API/ユーザー インターフェイスでアプライアンスの削除に失敗したら、以下のように `force-delete` API を使用して、アプライアンスを手動で削除します。

```
POST api/v1/cluster/nodes/deployments/467a102d-472f-4f43-a93c-08b992b9f471?  
action=delete&force_delete=true
```

その後、vCenter Server から仮想マシンを破棄します。

- 問題 2281095：SVM が展開されているホストが同じクラスタに再度追加されると、EAM からコー

ルバックがトリガされない

すべてのゲスト仮想マシンの保護が解除されている可能性があります。NSX のユーザー インターフェイスが進行中状態のまま変わりなくなります。

回避策：SVM をホストから削除した後、クラスタに追加します。

- **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 2261818：eBGP ネイバーから学習したルートが同じネイバーにアドバタイズされる**
bgp デバッグ ログを有効にすると、返信されるパケットとドロップされたパケットがエラー メッセージに表示されます。BGP プロセスは、追加の CPU リソースを使用して、ピアに送信された更新メッセージを破棄します。ルートとピアの数が非常に多い場合、ルートのコンバージェンスに影響する可能性があります。

回避策：なし。

インストールに関する既知の問題

- **問題 2238093：NSX パッケージが強制的に削除された場合、リゾルバがサポートされない**
ホストから NSX をアンインストールする際に、NSX パッケージは強制的に削除されます。これにより、NSX パッケージが破損状態となることがあります。NSX パッケージが、リゾルバより前に強制的に削除された場合、NSX パッケージ インストールのリゾルバは正常に機能しないことがあります。ログの場所：`/var/log/proton/nsxapi.log`

回避策：なし。

NSX パッケージは強制的に削除しないでください。NSX ドキュメントに記載されている通常の手順を実行して、NSX コンポーネントをアンインストールします。

- **問題 2288872：インストールの状態が「ノードの準備ができていません」と表示される**
Edge ノードがオンボーディングされません。トランスポート ノードの設定状態が保留のため、Edge クラスタに追加することができません。ログの場所：`/var/log/proton/nsxapi.log`

回避策：Edge ノードの登録を再試行します。または、Edge ノードをパワーオフします。起動すると、MP-MPA チャンネルを確立します。

- **問題 2252776：ホスト上で以前に発生した検証エラーを解決したにもかかわらず、トランスポート ノード プロファイルをクラスタ メンバー ホストの 1 台で適用できない**
トランスポート ノード プロファイル (TNP) はクラスタ上で適用されます。しかし、ホストで仮想マシンがパワーオンされていたなど、いずれかの検証がエラーであった場合、クラスタ メンバー ホストのいずれかで TNP を適用することはできません。問題を解決しても、ユーザー インターフェイス上には依然として検証が表示され、TNP はこのホストで自動的に適用されません。

回避策：ホストをクラスタの外部に移動した後で、再びクラスタに追加します。これにより、ホスト上でのトランスポート ノード プロファイルの適用アクティビティをトリガします。

- 問題 2284683：登録済みのコンピュート マネージャを削除し、再び追加すると、自動展開されたアプライアンスを削除できない
アプライアンスの削除が、エラー「パワーオフに失敗しました」とともに失敗し、該当するコンピュート マネージャが見つかりません。

回避策：API/ユーザー インターフェイスでアプライアンスの削除に失敗したら、以下のように force-delete API を使用して、アプライアンスを手動で削除します。POST api/v1/cluster/nodes/deployments/<node-id>?action=delete&force_delete=true .vCenter Server から仮想マシンを破棄します。

- 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 2296888：トランスポート ノード (TN)/トランスポート ノード プロファイル (TNP) の構成で、両方の「物理 NIC のみ移行」フラグを true に設定すると、インストール用の VMK マッピングをホスト スイッチ全体で更新できない
CREATE の実行時に、構成の不一致（両方の「物理 NIC のみ移行」フラグを true に設定し、ホスト スイッチ全体でインストール用の VMK マッピングを更新する）が見つかったと、次の例外が発生します。

```
VMK migration for host b17afc36-bbdc-491a-b944-21f73cf91585 failed with error
[com.vmware.nsx.management.switching.common.exceptions.SwitchingException: TransportNode
[TransportNode/b17afc36-bbdc-491a-b944-21f73cf91585] can not be updated or deleted while migrating ESX
vmk interface null to [null]].(エラー コード: 9418)
```

更新中に構成の不一致が見つかったと、次の例外が発生します。
一般的な（エラー コード: 400）

両方の「物理 NIC のみ移行」フラグが true に設定され、VMK 移行マッピングが含まれている TN/TNP 構成を適用すると、例外が発生します。

回避策：ホストに送信される各構成で、「物理 NIC のみ移行」フラグを設定するか、インストール用の VMK マッピングの更新を有効にしてください。両方を設定することはできません。

1. 「物理 NIC のみ移行」を true に設定する必要があるホスト スイッチを含む TN 構成を送信します。
2. すべての「物理 NIC のみ移行」フラグを false に設定し、必要に応じてインストール用 VMK マッピングを更新するように TN 構成を変更します。つまり、TN に送信される構成では、「物理 NIC のみ移行」フラグを true にするか、すべてのホスト スイッチ全体でインストール用の VMK マッピングを設定するか、いずれかにする必要があります。両方を必要とする構成の場合は、呼び出しを個別に行う必要があります。

- 問題 2273651：トランスポート ノードの削除後、ユーザーがホストに SSH 接続できない
この問題は、KVM の実装で確認されています。ユーザーがトランスポート ノードを削除し、削除の成功を知らせるメッセージを受け取りますが、その後、ユーザーは SSH 経由で同じホストにアクセスできなくなります。この問題は、NSX-T で管理されていない Open Virtual Switch (OVS) が存在し、このスイッチが KVM テンプレートの一部として事前にインストールされているために発生する可能性があります。

回避策：トランスポート ノードを削除する前に、問題のある OVS を特定します。

1. ovs-vsctl を実行して、OVS を特定します。
2. OVS から Linux ブリッジにワークロード仮想マシンのインターフェイスを移行します。
3. 次のように、トランスポート ノードを削除します。

```
DELETE api/v1/transport-nodes/<uuid>
```

- 問題 2281537：移行後、マルチ VTEP の ESXi トランスポート ノードが BFD セッションを開始できない
NSX-V ノードを NSX-T に移行した後、マルチ VTEP の ESXi トランスポート ノードが、Edge ノードのすべての VTEP で BFD セッションを開始できません。

回避策：netcpa サービスを再起動します。

NSX Manager に関する既知の問題

- 問題 2285306：ゲスト イントロスペクション サービスのサービス展開状態が、サービス仮想マシンがパワーオンされるまで、「不明」のままとなることがある
サービス展開を作成し、これがサービス展開グリッドに表示されると、状態はただちに「進行中」とは表示されず、グリッドが更新されるまで「不明」のままとなることがあります。

回避策：なし。10 秒後に画面を更新します。状態が更新されます。

- 問題 2292526：ホストを追加する際に「ホストにアクセスできません」というメッセージが表示される
ESXi ホストを追加する際に、「ホストにアクセスできません」というメッセージが表示されますが、原因は特定されません。正しくない認証情報が原因と考えられます。

回避策：ホストの構成を確認し、認証情報を再入力して、ホストの追加を再試行します。

- 問題 2292701：割り当てマップでシーケンス番号を更新できない
シーケンス番号を更新して、エンティティに適用されるプロファイルの順序や優先順位を変えることができません。

回避策：割り当てマップを削除し、新しい適切なシーケンス番号を使用して再作成します。

- 問題 2294345：ESXi ホストの仮想マシンおよび KVM ホストの仮想マシンが両方混在するグループでアプリケーション検出分類を実行すると失敗することがある
アプリケーション検出機能は、ESXi ハイパーバイザーでのみサポートされます。サポート対象外のホストが含まれる混在ホスト上に仮想マシンのグループがある場合、アプリケーション検出分類の結果は正しいとは限りません。

回避策：なし。

NSX Edge に関する既知の問題

- 問題 2248345：NSX-T Edge をインストールすると、マシンが空のブラック スクリーンで起動する
HPE ProLiant DL380 Gen9 マシンでは、NSX-T Edge をインストールできません。

回避策：別のマシンを使用するか、ハイパーバイザーで NSX-T Edge を仮想マシンとして展開します。

- 問題 2283559：Edge で RIB に 65,000 以上のルート、FIB に 100,000 以上のルートがある場合、
/routing-table および /forwarding-table 管理プレーン API がエラーを返す
Edge で RIB に 65,000 以上のルート、FIB に 100,000 以上のルートがある場合、管理プレーンから Edge への要求に 10 秒以上かかり、この結果タイムアウトになります。これは読み取り専用 API であり、API/ユーザー インターフェイスを使用して、RIB の 65,000 以上のルートおよび FIB の 100,000 以上のルートをダウンロードする必要がある場合にのみ影響を受けます。

回避策：RIB/FIB を取得するには、2 つのオプションがあります。

- これらの API では、ネットワーク プレフィックスまたはルートのタイプに基づくフィルタリング オプションをサポートしています。これらのオプションを使用して、目的とするルートをダウンロードします。
- RIB/FIB テーブル全体が必要な場合は CLI でサポートします。これによるタイムアウトはありません。

論理ネットワークに関する既知の問題

- **問題 2243415**：論理スイッチを管理ネットワークとして使用して NXGI サービスを展開できない
NXGI 展開画面で、ネットワーク選択コントロールで論理スイッチが表示されません。論理スイッチを管理ネットワークとして記述して API を直接使用すると、次のエラーが表示されます。「サービス展開用に指定されたネットワークにアクセスできません」

回避策：ローカル、分散など、別のタイプのスイッチを使用して展開します。

- **問題 2264386**：トランスポート ノードが NS Group に含まれている場合でも、トランスポート ノードが削除される
トランスポート ノードが NS Group に含まれていても、このノードを削除することができます。削除は回避する必要があります。この問題が発生したら、NS Group を再作成し、トランスポート ノードとの関係を再構築する必要があります。

回避策：この問題を回避するには、トランスポート ノードが NS Group のいずれかと関連付けられているかどうかを手動で確認します。管理プレーン インターフェイスで、[ネットワークとセキュリティの詳細設定] > [インベントリ] > [グループ] または [システム] > [ノード] > [トランスポート ノード] > [関連] > [NSGroup] の順に移動します。

- **問題 2292997**：Linux ネットワーク スタックでの特定の論理ルーター インターフェイスの作成で失敗することがある

Linux ネットワーク スタックでの特定の論理ルーター インターフェイスの作成で失敗し、
「errorCode="EDG0100002", Operation failed creating sub-interface: max sub-interface exceeded」 というエラーが返されることがあります。この結果、Tier-0 サービス ルーター (T-0 SR) により転送されるトラフィックは、ルートが見つからずにドロップすることがあります。

回避策：影響を受ける Edge ノードを再起動してください。

- **問題 228688**：BGP が VTI 上で設定されている場合に、IPsec ルート ベース セッションを削除中に、BGP ネイバーを削除する必要がある
BGP が VTI 上で設定されており、IPsec セッションを削除する場合、サービス ルーター (SR) はいずれも、停止状態となり、トラフィックをブロックします。トラフィックを再開するには、VTI に設定された BGP ネイバーを削除する必要があります。このシナリオでは、VTI 上で BGP のみが設定されます。

回避策：IPsec セッションを削除する前に BGP ネイバーを削除してください。

- **問題 2288509**：MTU プロパティが Tier-0/Tier-1 サービス インターフェイス（統合サービス ポート）でサポートされない
MTU プロパティが Tier-0/Tier-1 サービス インターフェイス（統合サービス ポート）でサポートされません。

回避策：CSP ポートがポリシー ワークフローで作成されていても、管理プレーン API を使用して MTU を構成します。

- **問題 2288774**：タグが誤って 30 個を超えていることが原因で、セグメンテーション ポートで認識エラーが発生する
ユーザーの誤った入力により、30 個を超えるタグの適用を試行します。しかし、ポリシー ワークフローでは、ユーザーの入力を適切に検証/拒否しないため、設定が許可されてしまいます。そして、30 個を超えるタグは使用できないという内容の適切なエラー メッセージとともに、ポリシーにアラームが表示されます。この時点で、ユーザーは問題を解決できます。

回避策：エラー メッセージが表示されたら、設定を訂正します。

- **問題 2275412**：複数のトランスポート ゾーン (TZ) でポート接続が機能しない
ポート接続は単一の TZ でのみ使用できます。

回避策：なし。

- **問題 2290083：VLAN ベース セグメントの作成時に検証が見つからない**
VLAN ID プロパティを持つ VLAN トランスポート ゾーンを指定する際に、システムは検証およびエラーの特定に失敗します。この結果、認識中にインテントが失敗し、エラーが発生します。

回避策：入力の修正手順については、認識アラーム エラー詳細を参照してください。

- **問題 2292096：CLI コマンド「get service router config route-maps」が空の出力を返す**
CLI コマンド「get service router config route-maps」は、ルートマップが設定されている場合でも、空の出力を返します。これは表示のみの問題です。

回避策：CLI コマンド `get service router config` を使用します。これにより、ルートマップ設定を出力全体のサブセットとして返します。

- **問題 2994002：DNS フォワーダ作成で選択する Tier-0/Tier-1 ゲートウェイ ドロップダウン リストで Tier-1 が表示されない**
レコード数が数千ある大規模展開では、DNS フォワーダ作成ワークフローで選択する Tier-0/Tier-1 ゲートウェイ ドロップダウン リストに Tier-1 が表示されません。この結果、DNS フォワーダ作成を構成するには、API を使用する必要があります。

回避策：API を使用して設定を行います。

- **問題 2298499：ゲートウェイがパブリック IP アドレスで展開されていない場合、Public Cloud Gateway とピア ホストの間で VPN が失敗する**
Public Cloud Gateway (PCG) がパブリック IP アドレスなしでアップリンクに展開されている場合、PCG とピア ホスト間で VPN トンネルを確立できません。PCG は、デフォルトで VPN トラフィックに SNAT を実行しているためです。

回避策：Public Cloud Gateway を展開するときに、アップリンク インターフェイスのパブリック IP アドレスを有効にします。

- **問題 2392093：RPF チェックが原因でトラフィックがドロップする**
Tier-0 と Tier-1 ルーターが同じ Edge ノードにあり、トラフィックで Tier-0 ダウンリンクを経由したヘアピン通信が発生すると、RPF チェックでトラフィックがドロップする場合があります。

回避策：なし。

セキュリティ サービスに関する既知の問題

- **問題 2288523：NSX ゲスト イントロスペクション ドライバをアンロードすると、セキュリティ問題が発生することがある**
IDFW は、NSX ゲスト イントロスペクション ドライバのユーザー ID 情報を使用します。ドライバをアンロードすると、特定のゲストからログインしているユーザーにセキュリティ上の問題が発生することがあります。これは以下の兆候を示します。

- ゲスト イントロスペクション ドライバがアンロードされている特定のゲスト仮想マシンからログインしたユーザーに対してファイアウォール ルールが適用されない。
- ゲスト イントロスペクション ドライバがアンロードされている特定のゲスト仮想マシンからログインしているユーザーに対して、IDFW コンポーネントがユーザー詳細をログ収集していない。
- IDFW がホストで有効であるにもかかわらず、MUX ログにゲスト仮想マシンからの接続が表示されない。
- IDFW がホストで有効であるにもかかわらず、MUX ログにゲスト仮想マシンからのネットワーク イベントが表示されない。

この結果として、デフォルトですべて拒否ルールでは、ゲスト イントロスペクション ドライバがアンロードされたゲスト仮想マシンからログインしたユーザーのアクセスをブロックできます。

回避策：なし。IT 管理者は、セキュリティ ベスト プラクティスを実行し、ゲスト仮想マシン内のゲスト イントロスペクション ドライバをアンロードする権限をユーザーに付与しないようにしてください。

- **問題 2288773：以前の TLS プロトコル API が依然として使用でき、上書きされる**
NSX-T では NSX TLS プロトコル バージョンおよび暗号スイートを設定する新しい API を導入しています。これにより、NSX-T クラスターのすべてのノードが更新されます。しかし、以前の API も引き続き使用可能な状態です。これは使用できますが、グローバル設定により、新しい設定が上書きされます。

回避策：新しい API を使用します。

- **問題 2291872：TFTP サービスがファイアウォール ルールで使用されている場合、ログ メッセージに警告メッセージが表示される**
TFTP サービスが ESXi ノードのファイアウォール rule.Log の場所で使用されている場合、ログ メッセージに無関係な警告メッセージが表示されます。/var/log/cfgAgent.log.

回避策：TFTP 用に新しいサービスを L4PortSet サービスとして作成し、ファイアウォール ルールで使います。

- **問題 2203863：UDP および ICMP トラフィックに Identity Firewall ルールが機能しない**
Identity Firewall ルールが ping テストで機能しません。現在の機能は、TCP トラフィックでのみ使用できます。

回避策：Identity Firewall ルールのテストに TCP を使用します。Identity Firewall を設定するときに、[サービス] 列に ANY/UDP/ICMP を設定しないでください。

- **問題 2296430：NSX-T Manager API が証明書の生成中にサブジェクトの代替名を提供しない**
NSX-T Manager API が証明書の発行でサブジェクト代替名を提供しません。この問題は特に、CSR 生成中に発生します。

回避策：拡張機能をサポートする外部ツールを使用して CSR を作成します。認証局から署名付きの証明書を受信したら、CSR からのキーを使用して、この証明書を NSX-T Manager にインポートします。

- **問題 2252738：完全修飾ドメイン名 (FQDN) ルールで、ルールに一致しないパケットが宛先に到達する**
特定の FQDN ルールを作成すると、IP アドレスに関連付けられたドメイン名がファイアウォール データベースに追加され、一致ルールとの照合に使用されます。このため、そのドメイン名に送信されたパケットがサーバに到達できるようになります。ただし、ユーザーがドメイン ネームサーバの IP アドレスに関連付けられたドメイン名を変更した場合、ファイアウォール データベースでドメイン名エントリは更新されません（新しいドメイン名に一致する別の FQDN ルールが存在しない場合）。このため、FQDN ルールでドロップする必要があるパケットが新しいドメイン名に送信されます。

回避策：なし。

- **問題 2395334：(Windows) ステートレス ファイアウォール ルールの conntrack エントリが原因で、パケットが誤ってドロップされる**
Windows 仮想マシンでは、ステートレス ファイアウォール ルールが完全にサポートされていません。

回避策：ステートフル ファイアウォール ルールを追加します。

- **問題 2458384：NSX-T Manager インターフェイスのページの読み込みに失敗し、403 エラーが発生する**
これは、リリース バージョン 2.4.0 と 2.4.1 で発生します。この問題は、admin と Identity Manager の両方のログインに影響します。NSX-T Manager の FQDN は *.SLD.TLD の形式です。次はその例です。*.co.uk、*.co.il、*.com.au など。

回避策：FQDN ではなく、省略名または IP を使用して NSX-T Manager UI にアクセスします。<https://kb.vmware.com/s/article/71217> を参照してください。

KVM ネットワークに関する既知の問題

- 問題 2292995：すべての設定済みルールが OVS でプログラミングされているにもかかわらず、認識状態がエラーに設定される
分散ファイアウォール (DFW) ルールがデータ プレーンでプログラミングされている場合であっても、API により誤検出される場合があります。

回避策：任意の DFW ルールを更新すると、エラーが解消します。たとえば、ルールのログ収集を切り替えるだけで、KVM DFW モジュールのエラーが解消します。

ロード バランサに関する既知の問題

- 問題 2290899：IPsec VPN が動作せず、IPsec の制御プレーンの認識が失敗する
同じ Edge ノードで Tier-0 の IPsec サービスと 62 台を超える LbServer が有効な場合、IPsec VPN（または L2VPN）の起動に失敗する

回避策：LbServer の数を 62 台以下に減らします。

- 問題 2297157：ロード バランシングの HTTPS パフォーマンスが FIPS モードの影響を受ける
デフォルトの FIPS モードが有効になっていると、ロード バランシングのパフォーマンスに悪影響を与える可能性があります。

回避策：回避策については、ナレッジベースの記事 KB67400、[NSX-T 2.4.0 Load Balance Service may observe low performance on HTTPS](#) を参照してください。

- 問題 2362688：ロード バランサ サービスで一部のプール メンバーが停止しているときに、ユーザー インターフェイスで統合の状態が「稼動中」と表示される
プール メンバーが停止しているときに、その状態がポリシー ユーザー インターフェイスに表示されません。プールの状態は緑で、「稼動中」と表示されます。

回避策：なし。

ソリューションの相互運用性に関する既知の問題

- 問題 2289150：AWS 開始の PCM 呼び出しに失敗する
CSM で AWS アカウントの PCG ロールを *old-pcg-role* から *new-pcg-role* に更新すると、CSM では、AWS の PCG インスタンスのロールを *new-pcg-role* に更新します。しかし、PCM では PCG のロールが更新されたことを認識していないため、この結果、引き続き *old-pcg-role* を使用して作成された、以前の AWS クライアントを使用します。これにより、PCM AWS クラウド インベントリ スキャンが発生し、他の AWS クラウドの呼び出しは失敗します。

回避策：この問題が発生した場合、新しいロールに変更してから 6.5 時間以上は、以前の PCG ロールを変更/削除しないでください。PCG を再起動すると、新しいロールの認証情報を使用してすべての AWS クライアントが再初期化されます。

運用および監視サービスに関する既知の問題

- 問題 2275869：ESXi ホスト上のルールに 31 文字より長いタグがあると、このホスト上で `cfgAgent` ログのロールオーバーが 1 分以内に発生する
頻繁にログのローリングを行うと、ホストのデバッグやトラブルシューティングに役立つ `cfgAgent.log` 内の情報が失われることがあります。ESXi ホストのログの場所：`/var/log/cfgAgent.log`

回避策：なし。

- 問題 2289984：`nsx-context-mux` サービスをホストで停止したあとも、`mux_connectivity_status` に `CONNECTED` と表示される

nsx-context-mux または nsx-opsagent がホストで実行されていない場合、システム（NSX インターフェイスまたはサービス インスタンス API）では、時刻が正しく反映されないタイムスタンプとともに、ソリューションの状態および GI エージェントの状態が実行中と誤って表示されます。この結果、ゲスト仮想マシンはウイルス対策保護を失うことがあります。

回避策：mux および opsagent が実行されていない場合、これらをホストで手動で起動します。

1. ホストに root としてログインし、以下のコマンドを実行します。

```
/etc/init.d/nsx-opsagent start  
/etc/init.d/nsx-context-mux start
```
2. エージェントを起動したら、数分ほど待機し、ユーザー インターフェイスの健全性状態タイムスタンプが更新されていることを確認します。

アップグレードに関する既知の問題

- **問題 2273737**：NSX-T 2.3 から 2.4 へアップデートすると、vIDM サーバの詳細が見つからなくなる
vIDM を使用し、vIDM サーバが NSX ポリシー アプライアンス上でのみ構成されている場合、アップデートで vIDM サーバは移行されますが、統合アプライアンスでは vIDM サーバが見つかりません。

回避策：この問題が発生したタイミングに応じて、次の 2 つの方法があります。

- バージョン 2.3 から 2.4 にアップデートする前：
NSX ポリシー アプライアンスと NSX Manager 仮想マシンの両方で同じ vIDM サーバの詳細を構成します。
- バージョン 2.3 から 2.4 にアップデートした後：
統合アプライアンスで同じ vIDM サーバの詳細を再設定します。

- **問題 2288549**：RepoSync がマニフェスト ファイルでチェックサム エラーとともに失敗する
この問題は、2.4 にアップグレードされたばかりの展開で確認されました。アップグレードした設定のバックアップを実行し、新しく展開したマネージャにリストアした場合、データベースにあるリポジトリマニフェスト チェックサムと実際のマニフェスト ファイルのチェックサムが一致しません。これにより、バックアップのリストア後に RepoSync が失敗とマークされます。

回避策：この問題を回避するには、次の手順を実行します。

1. CLI コマンド `get service install-upgrade` を実行します。
結果で「Enabled on」の IP アドレスをメモしておきます。
2. 上記のコマンドで返った「Enabled on」に表示されている NSX Manager の IP アドレスにログインします。
3. [システム] > [概要] の順に移動し、戻りが「Enabled on」と同じ IP アドレスを持つノードを探します。
4. このノードで [解決] をクリックします。
5. 上記の解決処理が正常に実行されたら、同じインターフェイスのすべてのノードで [解決] をクリックします。
3 台のノードすべてで、RepoSync の状態が [完了] と表示されます。

- **問題 2279973**：空のグループを作成し、アップグレードを行うと、管理プレーンのアップグレード後に、空のグループが開始前と表示される
この問題は、空のグループを作成してアップグレードを行うと発生します。

回避策：空のグループを作成しないでください。

次の手順のいずれかを実行します。

- 空のグループを削除する
- [再開] ボタンをクリックしてアップグレードを完了する

。プランをリセットする

- **問題 2282389**：ESX をクラスタ間で移動した場合、Upgrade Coordinator のアップグレード プランが vCenter Server のクラスタ メンバーシップと同期されない
ESX を vCenter Server の 1 つのクラスタから別のクラスタへ移動した場合、この変更が Upgrade Coordinator (UC) のアップグレード プランに反映されません。これにより、ユーザーが複数のグループで「並行アップグレード」を選択した場合、複数のホストが同時にメンテナンス モードに切り替わる可能性があります。

回避策：ホスト アップグレード画面で、[リセット] オプションをクリックして、プランを再構築し、UC アップグレード プランが vCenter Server のクラスタと同期するようにします。

- **問題 2288921**：以前のバージョンの Edge ノードが追加されると、アップグレード状態が同期されなくなる
Edge アップグレード後に以前のバージョンの Edge ノードを追加すると、アップグレード状態が同期されなくなります。この問題は、アップグレード呼び出しを繰り返し発生させます。

回避策：まず、以前のバージョンの Edge ノードは追加しないようにします。この問題が発生した場合は、UC サービスを再起動してください。

- **問題 2291625**：アップグレード プランが同期されると、PCG アップグレードの状態が SUCCESS から NOT_STARTED に変更される
この問題は、PCG をアップグレードしてから、その後さらにエージェント/PCG をアップグレードする際に発生します。
推奨されるワークフローでは、PCG のアップグレード後は、UC インターフェイスを介してクロスクラウド コンポーネントはアップグレードしません。

これによる機能面への影響はありません。以前正常に完了した PCG アップグレードの状態がアップグレード ユーザー インターフェイス上で「なし」と表示される

回避策：なし。機能面への影響はありません。

- **問題 2293227**：2.4 にアップグレードすると、VMware Tools 10.3.5 を実行する仮想マシンに IDFW ルールが適用されない
NSX-T ライブ アップグレードを実行すると、VMware Tools 10.3.5 を実行する仮想マシンに IDFW ルールが適用されません。これにより、この仮想マシンのウイルス対策保護が失われる可能性があります。

回避策：影響を受ける仮想マシンを再起動します。

- **問題 2295564**：2.3 から 2.4 にアップデートすると、Edge ノード コントローラの接続がダウンすることがある
これは、断続的に発生し、一部の North-South トラフィックに影響を与える問題です。

回避策：該当する Edge ノードでメンテナンス モードを有効にしてから無効にします。

- **問題 2294178**：2.3.1 から 2.4 にアップグレードするとホスト VIB の更新に失敗する
バージョン 2.3.1 から 2.4 へのアップグレード中にエラーが発生し、ホストにオフライン バンドルがインストールできない場合があります。具体的には、スイッチのセキュリティ モジュールのアンロードに失敗するため、ホスト VIB の更新に失敗します。この問題は、スイッチング プロファイルで IP アドレス検出機能が有効になっていて、ESXi-6.7EP06 (ビルド 11675023) が実行されているホストで NSX-T 2.3.1 から NSX-T 2.4 にインプレース アップグレードを実行すると発生します。

回避策：回避策については、ナレッジベースの記事 KB67445、[With IP Discovery enabled, host VIB update may fail when upgrading from NSX-T 2.3.1 to NSX-T 2.4](#) を参照してください。

- **問題 2277543**：インプレース アップグレードの実行中に、ホストへのオフライン バンドルのインストールでエラーが発生し、ホスト VIB の更新に失敗する

NSX-T 2.3.x から 2.4 にインプレース アップグレードを行う前のホストと ESXi-6.5P03 (ビルド 10884925) を実行しているホストで Storage vMotion を実行すると、このエラーが発生する場合があります。ホストのアップグレード直前に Storage vMotion を実行すると、2.3.x のスイッチ セキュリティ モジュールが削除されません。Storage vMotion によってメモリ リークが発生し、スイッチ セキュリティ モジュールのアンロードに失敗します。

回避策：ナレッジベースの記事 KB67444、[Host VIB update may fail when upgrading from NSX-T 2.3.x to NSX-T 2.4.0 if VMs are storage vMotioned before host upgrade](#) を参照してください。

- **問題 2276398**：NSX を使用して AV パートナー サービス仮想マシンをアップグレードすると、最大で 20 分ほど、保護されていない状態が継続する
パートナー サービス仮想マシンをアップグレードすると、新しいサービス仮想マシンがデプロイされ、古いサービス仮想マシンが削除されます。ホストの Syslog に SolutionHandler の接続エラーが記録されることがあります。

回避策：アップグレード後にホストの ARP キャッシュ エントリを削除し、ホストのパートナー制御 IP アドレスに ping を送信して、この問題を解決します。

- **問題 2297918**：2.3.1 から 2.4 へのアップグレード後、クラスタから NSX を削除できない
クラスタを 2.3.1 から 2.4 にアップグレードした後に NSX-T の削除に失敗し、次のメッセージが表示されます。「クラスタ上の NSX の削除に失敗：このファブリック テンプレートに関連するトランスポート ノード テンプレートまたはトランスポート ノードのコレクションがあります。このファブリック テンプレートを削除/無効にする前に、トランスポート ノード テンプレートまたはトランスポート ノードのコレクションを削除する必要があります」

回避策：影響を受けたクラスタからトランスポート ノード プロファイルを分離してから、「NSX の削除」ワークフローを使用します。

- **問題 2286030**：NSX-T 2.3.x 以前から 2.4.x にアップグレードすると、トランスポート ノードの構成状態が「失敗」と表示される
NSX-T 2.3.x 以前から 2.4.x にアップグレードすると、null ポインタ例外が発生し、トランスポート ノードの構成状態が「失敗」になります。vmkernel アダプタを含む ESXi トランスポート ノードを N-VDS VLAN 論理スイッチに移行して、NSX-T 2.3.x から NSX-T 2.4.x にアップグレードすると、競合条件が発生し、ESXi トランスポート ノードの構成状態が「失敗」と表示されることがあります。ただし、ノードの構成状態が「失敗」と表示された後でも、アップグレード中は NSX Manager およびコントローラと ESXi トランスポート ノードとの接続が維持されます。

回避策：トランスポート ノードを更新または再送信して、構成状態を「成功」にリセットします。

1. NSX Manager で、「失敗」と表示されている ESXi トランスポート ノードを編集します。
2. ESXi トランスポート ノードの構成ポップアップで、[保存] をクリックします。
この操作により、状態がリセットされます。構成を変更する必要はありません。

API に関する既知の問題

NSX Policy Manager に関する既知の問題

- **問題 2291267**：PCM により作成されたデフォルトのゲートウェイ ポリシー セクションにシーケンス番号が割り当てられず、ポリシーがデフォルトで 0 と設定される
シーケンス番号または insert_top オプションを指定せずにゲートウェイ ポリシーを作成するとポリシーの競合が発生します。ログの場所：/var/log/policy/policy.log

回避策：この問題を回避するには、適切な sequence_numbers または URL パラメータ action=revise&operation=insert_top を使用してポリシーを作成します。

- **問題 2289278**：ポリシー API でエラーが発生するにもかかわらず、異なるパーシステンス プロファイルを持ち、同じプールにある複数の仮想サーバを設定することができる

システムでは、異なる LbVirtualServer で同じプールにある場合に、競合しているパーシステンス タイプの設定をサポートしません。しかし、ポリシーでは、競合する入力を適切に検証/拒否できず、設定が許可されてしまいます。この結果、ポリシーではエラー メッセージとともにアラームが表示されます。

回避策：この問題が発生した場合、LbVirtualServer のグループ設定を変更して、修正することができます。

- **問題 2248186**：BGP ルーターが、独自のインターフェイスを持つネイバーからネクスト ホップとして IPV6 ルートをインストールする
その結果、インストールされたルートの IPV6 転送が失敗し、転送ループが発生することがあります。

回避策：この問題を回避するには、BGP の更新で IPv6 接続のアドレスをネクスト ホップとしてフィルタリングするようにルート マップを構成します。

NSX Cloud に関する既知の問題

- **問題 2287884**：NSX Cloud で特定の CentOS マーケットプレイス イメージがサポートされない
NSX Cloud でサポートされる CentOS マーケットプレイス イメージは、想定されるマイナー カーネル バージョンと一致する配布バージョンのもののみです。
たとえば、配布バージョンと対応するカーネル バージョンは次のように想定されます。

- RHEL 7.5 3.10.0-862
- RHEL 7.4 3.10.0-693
- RHEL 7.3 3.10.0-514

回避策：ドキュメントで推奨される CentOS 配布のみを使用します。

- **問題 2275232**：分散ファイアウォールの Connectivity_statregy が BLACKLIST から WHITELIST に変更されると、クラウドの仮想マシンで DHCP が動作しなくなる
新しい DHCP リースを要求する仮想マシンはすべて、IP アドレスを失います。分散ファイアウォール (DFW) でクラウド仮想マシンの DHCP を明示的に許可する必要があります。

回避策：DFW でクラウド仮想マシンの DHCP を明示的に許可します。

- **問題 2277814**：仮想マシンが nsx.network タグの無効な値で vm-overlay-sg に移動する
nsx.network タグでタグ付けされた仮想マシンが、vm-overlay-sg に移動します。

回避策：無効なタグを削除します。

- **問題 2280663**：複数の VPC を並行してオフボーディングすると、まれに失敗する
コンピュート VPC のいずれかをオフボーディングすると失敗します。

回避策：手動で VPC およびポリシー上の対応するグループを削除します。

- **解決した問題 2287124**：Microsoft Azure VNet に PCG を展開した後、CSM の VNet のタイルに誤って警告が表示される

Microsoft Azure VNet に PCG を展開した後、CSM で警告サイン（感嘆符付きの黄色の三角形）が表示されます。警告アイコンの上にカーソルを置くと、MP（管理プレーン）と CCP（制御プレーン）の状態が不明と表示されます。ただし、接続に問題がなくても警告が表示される場合があります。

- **問題 2290688**：AWS で Windows 2016 仮想マシンのアップグレードに失敗する
AWS で、複数の Windows ワークロード仮想マシンのアップグレードが失敗します。AWS ポータルで、仮想マシンのアップグレード 状態が「1/2 Check」と表示されます。再試行も失敗します。この問題は、同じバージョンの NSX-T のアップグレードでのみ発生します。

回避策：この問題を回避するには、次の手順を実行します。

1. 仮想マシンが最新のホスト コンポーネントをダウンロードできるように、影響を受けるホストで PCG がアップグレードされていることを確認します。

2. 仮想マシンを再起動して、正常な状態にします。
3. `uninstall cmd` を手動で実行します。
4. `install cmd` を手動で実行します。