



# VMware NSX-T Data Center 2.5 リリース ノート

VMware NSX-T Data Center 2.5 | 2019 年 9 月 19 日 | ビルド 14663974

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 の廃止と動作の変更](#)
- [使用可能な言語](#)
- [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 2.5 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。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 サポート、高可用性クラスタ管理、vSphere コンピュート クラスタ用のプロファイル ベースの NSX インストールが機能強化されています。また、NSX Data Center for vSphere から NSX-T Data Center に移行するための Migration Coordinator の機能も強化されています。

### NSX Intelligence

NSX-T Data Center 2.5 では、新しい NSX 分析コンポーネントとして NSX Intelligence v1.0 が導入されました。NSX Manager の 1 つの管理ペインから NSX Intelligence のユーザー インターフェイスにアクセスし、次の機能を使用できます。

- 環境内のワークロードのフロー情報がほぼリアルタイムで表示されます。
- NSX Intelligence は、ライブ フローまたは履歴フロー、ユーザー構成、ワークロード インベントリを関連付けて分析します。
- フロー、ユーザー構成、ワークロード インベントリに関する過去の情報を表示できます。
- ファイアウォール ルール、グループ、サービスを推奨し、マイクロセグメンテーションのプランニングを自動化します。

### コンテナ API のサポート

コンテナ インベントリで新しい API サポートを使用できます。API のドキュメントを参照してください。

### L2 ネットワーク

- **Edge ブリッジの機能強化** - Edge ブリッジで、同じセグメントを複数のブリッジ プロファイルに接続できるようになりました。これにより、物理インフラストラクチャの VLAN にセグメントを複数回ブリッジできます。この新機能は、以前のバージョンの NSX-T Data Center の元の ESXi ブリッジに置き換わります。これにより、元のブリッジは廃止されます。**注意**：この機能は、お客様の責任で使用してください。物理ネットワーク内の同じ L2 ドメインに同じセグメントを 2 回ブリッジすると、ブリッジ ループが生じる可能性があります。ループを回避するメカニズムはありません。
- **MTU/VLAN の健全性チェック** - 運用側から見ると、構成エラーによるネットワーク接続の問題は特定が難しい場合がほとんどです。一般的なシナリオでは、仮想ネットワークの管理者が NSX Manager を使用し、物理ネットワークの管理者が物理ネットワークのスイッチを管理しています。
  - **VLAN 健全性チェック** - N-VDS VLAN 設定が隣接する物理スイッチ ポートのトランク ポートの設定と一致するかどうかを確認できます。
  - **MTU 健全性チェック** - VLAN ごとの物理アクセス スイッチ ポートの MTU 設定が、N-VDS MTU 設定と一致するかどうかを確認できます。
- **ゲスト VLAN 間のタグ付け** - 拡張データパス N-VDS により、ゲスト VLAN タグをセグメントにマッピングできます。この機能により、仮想マシンごとに 10 個の vNIC の制限がなくなり、ゲスト VLAN のタグ付きトラフィック（別のセグメントにマッピングされたトラフィック）が NSX インフラストラクチャでルーティングされます。

## L3 ネットワーク

- **障害ドメインに基づいた Edge クラスタ内での Tier-1 の配置** - ユーザー定義の障害ドメインに基づいて、NSX-T が Tier-1 ゲートウェイを自動的に配置します。これにより、Tier-1 ゲートウェイが自動的に配置される場合でも、可用性ゾーン、ラック、またはホスト間での Tier-1 ゲートウェイの信頼性が向上します。
- **ECMP トポロジでルーター障害が発生した後の非対称ロード シェアリング** - アクティブ/アクティブの Tier-0 ゲートウェイでサービス ルーターが障害で停止し、別のルーターがそのトラフィックを引き継ぐと、サービス ルーターを通過するトラフィックが倍増します。ルーターの障害が発生してから 30 分が経過すると、障害の起きたルーターの IP アドレスがネクスト ホップのリストから削除され、特定のルーターへの追加トラフィックが回避されます。
- **API からピアごとに BGP アドバタイズ/受信ルートを取得** - CLI を使用せずに、BGP との間で送受信されるルートを検証できるため、BGP の処理が簡素化されます。
- **BGP ラージ コミュニティのサポート** - RFC8092 で定義されているように 4 バイトの ASN と一緒にコミュニティを使用できるようになりました。
- **ピアごとに設定できる BGP グレースフル リスタート ヘルパー モード オプション** - この Tier-0 ゲートウェイのオプションを使用すると、Tier-0 ルーター間のフェイルオーバー時間に影響せずに、冗長制御プレーンでノースパウンド物理ルーターのルーティングを管理できます。
- **複数の NAT ルールを一括で作成する API** - 多くの NAT ルールを 1 つの API 呼び出しにバンドルできるように、既存の NAT API が拡張されました。

## Edge プラットフォーム

- **ベアメタル Edge ノードでの Mellanox ConnectX-4 および ConnectX-4 LX のサポート** - ベアメタル Edge ノードで、10/25/40/50/100 Gbps の Mellanox ConnectX-4 および ConnectX-4 LX 物理 NIC がサポートされるようになりました。
- **ベアメタル Edge の物理 NIC の管理** - データプレーン NIC (fastpath) として使用する物理 NIC を選択できます。また、ベアメタル Edge ノードでサポートされる物理 NIC の数も 8 から 16 に増えました。

## IPv6 サポートの強化

NSX-T 2.5 では、引き続き IPv6 ルーティング/転送機能セットが機能強化されました。これには以下のサポートが含まれます。

- **IPv6 SLAAC (ステートレス アドレスの自動構成)**。IPv6 アドレスを仮想マシンに自動的に提供します。
- **IPv6 ルーターの通知**。NSX-T ゲートウェイは、ルーターの通知を介して IPv6 パラメータを提供します。

- IPv6 DAD。NSX-T ゲートウェイで重複する IPv6 アドレス割り当てが検出されます。

## ファイアウォールの向上

### レイヤー 7 での AppID のサポート

NSX-T 2.5 で、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レイヤー 7 機能が強化されました。これには以下のサポートが含まれます。

- KVM の分散ファイアウォールでのレイヤー 7 AppID サポート。
- ゲートウェイ ファイアウォールでのレイヤー 7 AppID サポート。
- 単一のファイアウォール ルールでの複数のレイヤー 7 AppID 構成。

### FQDN/URL フィルタリングの強化

NSX-T 2.5 では、FQDN フィルタリング サポートの機能が強化されています。

- DNS エントリの TTL タイマーの設定。
- KVM ハイパーバイザーで実行されているワークロードのサポート。

ファイアウォールの処理が強化され、次の機能が追加されました。

- **構成の自動保存とロールバック機能** - 構成を発行すると、構成のコピーが自動的に保存されます。保存された構成を再度展開し、元の状態にロールバックすることもできます。
- **手動ドラフト** - ルールセットを発行して適用する前に、ルールのドラフトを保存できるようになりました。手動ドラフトのルールはステージングが可能です。ロック メカニズムにより、複数のユーザーが同じドラフトで作業できるようになりました。この機能により、異なるユーザーによるルールのオーバーライドを無効にできます。
- **セッション タイマー** - TCP、UDP、ICMP セッションにセッション タイマーを設定できます。
- **フラッド防止** - 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で SynFlood 保護を使用できます。トラフィックにアラート、ログ、ドロップのしきい値を設定し、カスタム ワークフローで使用できます。
- **NSX LoadBalancer を作成して仮想サーバを展開すると、2 つのグループが自動的に生成されます。**1 つのグループにはサーバ プールが含まれ、もう 1 つのグループには仮想サーバの IP アドレスが含まれています。これらのグループは、ファイアウォール管理者が分散ファイアウォールまたはゲートウェイ ファイアウォールでトラフィックの許可または拒否に使用します。これらのグループは、NSX ロード バランサの構成に対する変更を追跡します。
- **仮想マシンごとに検出された IP アドレスの数。**vNIC の IP アドレスが 128 から 256 に増えました。

### Identity Firewall

- NSX-T 2.5 では、Windows 2016 に展開された Active Directory サーバがサポートされます。
- ターミナル サービスが有効になっていない Windows Server ワークロードで Identity Firewall がサポートされます。これにより、サーバ間での管理者の移動を厳密に制御できます。

## サービス挿入

- **パケット コピーのサポート** - サービス経由でのトラフィックのリダイレクトに加え、NSX-T でネットワーク監視の新しいユース ケースがサポートされます。元のパケットがネットワーク監視サービスを通過しない場合、パケットのコピーがパートナー サービス仮想マシン (SVM) に転送され、検査、モニタリング、統計情報の収集が行われます。
- **ホストベースのパートナー SVM の自動展開** - NSX-T 2.5 では、パートナー SVM の展開で 2 つのモードがサポートされます。クラスタ展開では、サービス仮想マシンが専用の vSphere (サービス) クラスタに展開されます。ホストベースでは、サービスごとに 1 台のサービス仮想マシンが特定のクラスタの各コンピュート ホストに展開されます。このモードでは、新しいコンピューティング ホストがクラスタに追加されると、適切な SVM が自動的に展開されます。

- North-South のサービス挿入に対する通知サポート - NSX-T 2.4 で East-West サービス挿入に対する通知フレームワークが導入され、パートナー サービスがグループの動的更新などに関連する変更通知を自動的に受信できるようになりました。NSX-T 2.5 では、この通知フレームワークが North-South のサービス挿入に拡張されました。パートナーは、このメカニズムを利用して、パートナー ポリシー（タグ、OS、仮想マシン名など）に基づいて動的 NSX グループの使用をユーザーに許可することができます。
- 追加のトラブルシューティング機能と表示機能 - NSX-T 2.5 では、サービス挿入に関連する問題のトラブルシューティングをより効率的に行えるように、いくつかのサービス機能が強化されました。たとえば、サービス インスタンスのランタイムの状態を確認できます。また、API を介して使用可能なサービスパスを取得したり、サービス挿入関連のログをサポート バンドルに追加したりできます。

## エンドポイント保護（ゲスト イントロスペクション）

- Linux のサポート - エンドポイント保護に Linux ベースのオペレーティング システムのサポートが追加されました。ゲスト イントロスペクションでサポートされている Linux オペレーティング システムについては、『NSX-T 管理ガイド』を参照してください。
- エンドポイント保護ダッシュボード - エンドポイント保護ダッシュボードでは、保護された仮想マシンと保護されていない仮想マシンの構成状態、ホスト エージェントとサービス仮想マシンの問題、VMware Tools とともにインストールされたファイル イントロスペクション ドライバが設定されている仮想マシンをモニタリングできます。
- ダッシュボードのモニタリング - システムのクラスタ全体で、パートナー サービスの展開状態をモニタリングできます。

## ロード バランシング

- ロード バランサの Edge キャパシティの状態を取得する API - ロード バランシング インスタンスの Edge キャパシティをモニタリングできる新しい API 呼び出しが追加されました。
- 健全性チェックの IP アドレスを自動的に選択 - SNAT IP リストが設定されている場合、Tier-1 ゲートウェイのアップリンク IP アドレスではなく、リストの先頭にある IP アドレスが健全性のモニタリングに使用されます。IP アドレスは、仮想サーバの IP アドレスと同じ場合もあります。この機能強化により、ロード バランサは、ソース NAT と健全性のモニタリングの両方で単一の IP アドレスを使用できます。
- ロード バランサ ログの機能強化 - この機能強化により、ロード バランサはモニタリング対象の仮想サーバごとに詳細なログ メッセージを生成できるようになりました。たとえば、仮想サーバのアクセスログには、クライアントの IP アドレスだけでなく、プール メンバーの IP アドレスも含まれます。
- LB ルールのパーシステンスの強化 - LB ルールに、「Persist」という新しいアクションが導入されました。このアクションを使用すると、ロード バランサはプール メンバーによって設定された Cookie に基づいてアプリケーションの永続性を提供できます。
- LB の適合 - 小規模な LB インスタンスは小規模 Edge 仮想マシンに適合できます。中規模の LB インスタンスは、中規模 Edge 仮想マシンに適合できます。以前は、Edge 仮想マシンのサイズを LB インスタンスのサイズよりも大きく設定する必要があったため、小規模 Edge 仮想マシンはロード バランシング サービスをサポートしていませんでした。
- VS/プール/メンバー統計 - 簡易インターフェイスで、すべての LB 関連の統計情報が利用できるようになりました。以前は、ネットワークとセキュリティの詳細設定インターフェイスでのみ、この情報を使用できました。
- SSL 終了での ECC（楕円曲線証明書）のサポート - SSL のパフォーマンスを向上させるため、EC 証明書の使用が可能になりました。
- FIPS 対応 - ロード バランサの FIPS コンプライアンス用に、API を介したグローバル設定があります。デフォルトでは、パフォーマンスを向上させるため、この設定はオフになっています。

## VPN

- Tier-1 ゲートウェイでの IPsec VPN のサポート - IPsec VPN を Tier-1 ゲートウェイに展開し、終了できるようになりました。これにより、テナントの隔離性とスケーラビリティが向上します。以前は、Tier-0 ゲートウェイでのみサポートされていました。
- NSX で管理する Edge でのレイヤー 2 VPN の VLAN サポート - この機能強化により、VLAN でバック

ングされたセグメントを拡張できます。以前は、レイヤー 2 の拡張機能で論理セグメントのみがサポートされていました。たとえば、VLAN トランク サポートにより、1 つの Edge インターフェイスとレイヤー 2 VPN セッションで複数の VLAN を拡張できます。

- IPsec VPN の TCP MSS クランプ - TCP MSS クランプにより、管理者はすべての TCP 接続の MSS 値を適用し、パケットの断片化を回避できます。
- IPsec VPN での ECC（楕円曲線証明書）のサポート - CNSA、UK Prime など、さまざまな IPsec コンプライアンススイートを有効にするには、EC 証明書が必要です。
- コンプライアンススイートの設定を簡単に実行できるボタン - UI のワンクリックまたは 1 回の API 呼び出しで CNSA、Suite-B-GCM、Suite-B-GMAC、Prime、Foundation、FIPS を設定できます。

## 自動化、OpenStack、その他の CMP

- OpenStack リリース サポートの拡張 - Stein と Rocky リリースが新たに追加されました。
- ポリシー API をサポートする OpenStack Neutron プラグイン - 管理 API をサポートする既存のプラグインに加え、新しい NSX-T ポリシー API を使用する OpenStack Neutron プラグインが追加されました。このプラグインは、レイヤー 2、L3、ファイアウォール、SLAAC の IPv6 をサポートします。
- OpenStack Neutron ルーターの最適化 - プラグインで、サービス ルーターの作成/削除を動的に管理し、OpenStack Neutron ルーターを最適化できるようになりました。これにより、サービスが構成されていない場合には分散ルーターのみを使用できます。追加されたサービスはすぐにプラグインによって管理されず。
- OpenStack Neutron プラグイン レイヤー 2 ブリッジ - OpenStack から設定されたレイヤー 2 ブリッジが ESXi クラスタではなく、Edge クラスタに設定されるようになりました。
- OpenStack Octavia のサポート - ロード バランシングの方法として LBaaSv2 に加え、Octavia が OpenStack Neutron プラグインでサポートされるようになりました。  
詳細については、『VMware NSX-T Data Center 2.5 Plugin for OpenStack Neutron リリース ノート』を参照してください。

## NSX Cloud

- 新しい操作モードの追加 - NSX Cloud に新しい 2 つの操作モードが追加されました。これにより、NSX Cloud はエージェントありとエージェントなしの両方の操作モードをサポートする唯一のハイブリッドクラウドソリューションになりました。
  - NSX 強制モード（エージェントあり） - オンプレミスとパブリッククラウドの間で一貫性のあるポリシーフレームワークを提供します。NSX のポリシー適用は、すべてのワークロードにインストールされている NSX Tools で実行されます。これにより、仮想マシンレベルの細分性が確保され、すべてのタグ付き仮想マシンが NSX によって管理されます。このモードでは、個々のパブリッククラウドプロバイダの相違点や制限事項を解消し、オンプレミスとパブリッククラウドのワークロードの間で一貫したポリシーフレームワークを利用できます。
  - ネイティブクラウド強制モード（エージェントなし） - オンプレミスとパブリッククラウドの間で共通のポリシーフレームワークを提供します。このモードでは、ワークロードに NSX Tools をインストールする必要はありません。NSX セキュリティポリシーは、ネイティブのクラウドプロバイダのセキュリティ要素に変換されます。このため、選択したパブリッククラウドの規模と機能の制限がすべて適用されます。制御単位は VPC/VPNET レベルになります。ホワイトリストに指定されていない限り、管理対象の VPC/VPNET 内のワークロードはすべて NSX によって管理されます。どちらのモードでも、動的なグループメンバーシップと、NSX グループメンバーシップ基準の豊富な抽象化セットが提供されます。
- NSX Cloud からのパブリッククラウドネイティブサービスの可視化とセキュリティのサポート - このリリースから、ローカルの VPC/VPNET エンドポイントとそれに関連付けられているセキュリティグループを持つ Azure および AWS で、ネイティブ SaaS サービスのセキュリティグループをプログラミングできるようになりました。これは、NSX ポリシーでユーザー指定のルールを使用して、クラウドネイティブサービスエンドポイントを検出し、セキュリティを確保することを主な目的としています。このリリースでは、次のサービスが AWS（ELB、RDS、DynamoDB）と Azure（Azure Storage、Azure LB、Azure SQL Server、CosmoDB）でサポートされます。今後の NSX-T リリースでは、サポートされるサービスがさらに追加される予定です。

- **新しい OS のサポート：**
  - Windows Server 2019 のサポート
  - Windows 10 v1809
  - Ubuntu 18.04 のサポート
- **検疫ポリシーと仮想マシン ホワイトリストの機能強化** - NSX 2.5 以降の NSX Cloud では、ユーザーが CSM インターフェイスから仮想マシンをホワイトリストに登録できます。ホワイトリストに登録すると、このような仮想マシンのクラウド セキュリティ グループは NSX によって管理されないため、ユーザーは仮想マシンを任意のクラウド セキュリティ グループに配置できます。
- **CSM インターフェイスでのエラー レポート機能の強化** - トラブルシューティングをより迅速に行うことができます。

## 運用

- **NSX Manager の vSphere HA サポート** - NSX 管理クラスタを vSphere HA で保護できるようになりました。これにより、実行中のホストで障害が発生したときに、NSX 管理クラスタの 1 台のノードをリカバリできます。また、サイト レベルの障害が発生した場合は、NSX 管理クラスタ全体を代替サイトにリカバリできます。サポートされているシナリオの詳細については、『NSX-T インストール ガイド』を参照してください。
- **キャパシティ ダッシュボードが向上** - キャパシティ ダッシュボードに新しいメトリックが追加され、既存のメトリックが向上しました。製品でサポートされる最大値と比較して、ユーザーが設定したオブジェクトの数が表示されます。NSX-T Data Center の設定の最大値については、VMware Configuration Maximums ツールで確認してください。
- **vSphere ロックダウン モードのサポート** - vSphere ロックダウン モード環境での NSX-T のインストール、アップグレード、操作が可能になり、より柔軟に展開オプションを選択できます。
- **ログの機能強化** - NSX コマンド ライン インターフェイスを介して NSX ユーザー空間エージェントのログレベルを動的に変更できるようになりました。これにより、トラブルシューティング中のサービスへの影響を軽減できます。
- **SNMPv3 のサポート** - NSX Edge および NSX Manager アプライアンス用に SNMPv3 構成のサポートを追加し、セキュリティ コンプライアンスを強化しました。
- **仮想マシンのアドレス解決のトラブルシューティングに使用する新しいトレースフロー機能** - トレースフローに ARP/NDP パケットの挿入サポートが追加されました。これにより、IP 宛先のアドレス解決を行いながら、接続の問題を検出できます。
- **アップグレード順序の変更** - NSX-T 2.5 にアップグレードするときのアップグレード順序が変わりました。Edge コンポーネントのアップグレードは、ホスト コンポーネントよりも前に行う必要があります。クラウド インフラストラクチャをアップグレードするときに、最適化によりメンテナンス全体の時間を短縮できます。
- **Log Insight コンテンツ パックの機能強化** - NSX-T 2.5 と互換性のある新しい NSX コンテンツ パックに、すぐに使えるアラートのサポートが追加されました。

## プラットフォームのセキュリティ

- **FIPS** - ユーザーが FIPS コンプライアンス レポートを生成できるようになりました。また、FIPS 準拠モードで NSX 環境を構成および管理することができます。暗号化モジュールが FIPS に認定されました。連邦規制に準拠する必要があるお客様や FIPS 標準に準拠した安全な方法で NSX を運用したいお客様に、保証されたセキュリティが提供されます。明記された例外を除き、NSX-T 2.5 のすべての暗号化モジュールが FIPS によって認証されています。FIPS 認定モジュールの証明書については、<https://www.vmware.com/security/certifications/fips.html> を参照してください。
- **パスワード管理の強化** - ユーザーがパスワードの有効期限を日単位で延長できるようになりました。アップグレード後でも、最後にパスワードを変更してからの日数を変更できます。パスワードが期限切れになる 30 日前から、警告と有効期限の通知がインターフェイス、CLI、Syslogs に表示されます。

## 単一クラスタ設計のサポート

Edge/管理/コンピュータ仮想マシンを備えた最小の単一クラスタ設計をサポート。4 台のホストから構成される 1 つのクラスタで 1 つの N-VDS を使用します。VxRail やその他のクラウド プロバイダのホスト ソリューションの標準的な設計では、2 台のホスト スイッチで 4 個の 10G pNIC を使用しています。1 台のスイッチは Edge と管理 (VDS) 専用で、もう 1 つはコンピュータ仮想マシン (N-VDS) 専用になります。2 台のホスト スイッチにより、管理トラフィックがコンピューティングトラフィックから効率的に分離されます。10G と 25G の経済性から、多くの小規模なデータセンターやクラウド プロバイダのユーザーは、2 台の pNIC ホストで標準化を行っています。このフォーム ファクタを使用すると、小規模なデータセンターやクラウド プロバイダのユーザーは、単一の VDS を備えた NSX-T ベースのソリューションを構築し、すべてのコンポーネントを 2 つの pNIC で管理することができます。

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

- **Migration Coordinator の機能強化** - Migration Coordinator の操作性が強化されました。NSX Data Center for vSphere から NSX-T Data Center への移行に必要なプロセスのワークフローが向上しました。移行中のユーザーがフィードバックを提供する機能も向上しています。

## 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。

## 全般的な動作変更

### NSX-T Data Center システム通信ポートの変更

NSX-T Data Center 2.5 以降では、すべてのトランスポート ノードおよび Edge ノードから NSX Manager への NSX メッセージング チャネルの TCP ポートがポート 5671 から TCP ポート 1234 に変更されました。この変更により、NSX-T Data Center 2.5 にアップグレードする前に、すべての NSX トランスポート ノードと Edge ノードが TCP ポート 1234 で NSX Manager に接続し、TCP ポート 1235 で NSX Controller に接続できることを確認してください。また、アップグレード プロセス中は、ポート 5671 を開いたままにしてください。

### L2 ネットワーク

レイヤー 2 ブリッジの機能強化により、ESXi ブリッジは廃止されました。NSX-T では当初、ESXi ホストをブリッジ専用にし、オーバーレイ セグメントを VLAN に拡張する機能を備えていました。新しい Edge ブリッジが機能的に優れ、専用の ESXi ホストが不要になることと、Edge ノードの最適化されたデータパスから得られるメリットのため、今回のリリースで以前のモデルは廃止されました。詳細については、「[新機能](#)」を参照してください。

## API の廃止と動作の変更

このリリースでは、トランスポート ノード テンプレート API が廃止されました。代わりにトランスポート ノード プロファイル API の使用を推奨します。廃止されたタイプとメソッドについては、[API 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](https://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。



# 使用可能な言語

NSX-T Data Center は英語、ドイツ語、フランス語、日本語、簡体字中国語、韓国語、繁体字中国語、スペイン語でご利用いただけます。NSX-T Data Center のローカライズではブラウザの言語設定が使用されるため、設定が目的の言語と一致することを確認してください。

## ドキュメントの改訂履歴

2019 年 9 月 19 日初版。

2019 年 9 月 23 日既知の問題 2424818 と 2419246 について記載しました。解決した問題 2364756、2406018、2383328 を追加しました。

2019 年 9 月 24 日「新機能」を更新しました。

2019 年 10 月 3 日解決した問題 2313673 について記載しました。

2019 年 11 月 12 日。既知の問題 2362688 と 2436302 について記載しました。問題 2282798 を解決し、解決した問題に移動しました。

2019 年 12 月 17 日。既知の問題 2444170 を追加しました。

2020 年 1 月 14 日。解決した問題 2399994 を追加しました。

2020 年 2 月 18 日。既知の問題 2436302 を更新し、ナレッジベースの記事へのリンクを追加しました。

2020 年 5 月 14 日。既知の問題 2467479 を追加しました。

2020 年 9 月 25 日。既知の問題 2586606 を追加しました。

2021 年 3 月 15 日。既知の問題 2730634 について記載しました。

## 解決した問題

- 解決した問題 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。
- 解決した問題 2334442：ユーザーが、管理者ユーザーの名前を変更した後に作成されたオブジェクトを編集または削除できない  
ユーザーが、管理者ユーザーの名前を変更した後に作成されたオブジェクトを編集または削除できません。管理者/監査者ユーザーの名前を変更できません。
- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 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。
- 解決した問題 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://<nsx-manager>/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://<nsx-manager>/api/v1/configs/management を呼び出すことはできません。

- 解決した問題 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。
- 解決した問題 2292116：IPFIX L2 の画面でグループを作成するときに、UI で 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。
- 解決した問題 2268406：追加されたタグが最大数に達すると、[タグ アンカー] ダイアログ ボックスに一部のタグが表示されない  
追加したタグが最大数に達すると、[タグ アンカー] ダイアログ ボックスに一部のタグが表示されず、ダイアログ ボックスのサイズ変更やスクロールができなくなります。[サマリ] 画面にはすべてのタグが表示されます。失われたデータはありません。
- 解決した問題 2282798：同時に多くの要求またはホストが NSX Manager への登録を試みると、ホストの登録に失敗することがある  
この問題により、ファブリック ノードが失敗状態になります。ファブリック ノードの状態 API の呼び出しで、「クライアントがハートビートに対してまだ応答していません」と表示されます。ホストの /etc/vmware/nsx-mpa/mpaconfig.json ファイルも空になります。
- 解決した問題 2383867：管理プレーン ノードの 1 つでログ バンドルの収集に失敗する  
サポート バンドルをリモート サーバにコピーするときに、ログ収集プロセスでエラーが発生します。
- 解決した問題 2332397：API を使用すると、存在しないドメインでも分散ファイアウォール ポリシーが作成される  
このようなポリシーを存在しないドメインに作成した後、分散ファイアウォールの [セキュリティ] タブを開くと、インターフェイスが応答しくなくなります。関連するログは /var/log/policy/policy.log です。
- 解決した問題 2410818：バージョン 2.4.2 にアップグレードした後に新しい仮想サーバを作成すると、NSX-T 2.3.x で作成された仮想サーバが停止することがある  
一部の環境では、バージョン 2.4.2 にアップグレードした後、新しい仮想サーバを作成すると、バージョン 2.3.x で作成された仮想サーバが停止します。
- 解決した問題 2310650：インターフェイスに「要求がタイムアウトしました」というエラー メッセージが表示される  
インターフェイスの複数ページに次のメッセージが表示されます。「要求がタイムアウトしました。システムの負荷が高いか、リソースが不足している可能性があります。」
- 解決した問題 2314537：vCenter Server の証明書とサムプリントが更新された後、接続状態が「停止」になる  
vCenter Server と NSX の同期で新しい情報に更新されないため、vCenter Server からデータを取得するオンデマンド クエリがすべて失敗します。ユーザーは新しい Edge またはサービス仮想マシンを展開できません。ユーザーは、vCenter Server に追加する新しいクラスタまたはホストを準備できません。ログの場所：NSX Manager ノードの /var/log/cm-inventory/cm-inventory.log と /var/log/proton/nsxapi.log
- 解決した問題 2316943：vMotion でワークロードの保護が一時的に解除される

vMotion 後、VMware Tools から仮想マシンの正しいコンピュータ名が報告されるまでに数秒かかります。  
vMotion 後の数秒間、コンピュータ名で NSGroups に追加された仮想マシンの保護が解除されます。

- **解決した問題 2318525：IPv6 ルートのネクスト ホップに設定されている eBGP ピアの IP アドレスが送信側の IP アドレスに変更される**  
eBGP IP4 セッションの場合、アドバタイズされる IPv4 ルートでネクスト ホップとして eBGP ピアが設定されている場合、このルートのネクスト ホップは送信者側の IP アドレスに変更されません。IPv6 の場合、これに起因する問題は発生しません。IPv6 セッションの場合、送信側でルートのネクスト ホップが自身の IP アドレスに変更されるため、ルートがループする場合があります。この動作によって、ルートのループが発生する可能性があります。
- **解決した問題 2320147：影響を受けるホストに VTEP がない**  
同じトランザクションで LogSwitchStateMsg の削除と追加を行い、管理プレーンが論理スイッチを送信する前にこの操作が中央の制御プレーンによって処理されると、論理スイッチの状態は更新されません。このため、VTEP が見つからず、トラフィックを送受信できません。
- **解決した問題 2320855：[追加/確認] ボタンをクリックしないと、新しい仮想マシンにセキュリティ タグが作成されない**  
インターフェイスの問題です。ユーザーが新しいセキュリティ タグをポリシー オブジェクトまたはインベントリに追加し、「タグ-範囲」ペア フィールドの横にある **追加/確認** ボタンをクリックせずに **保存** をクリックすると、新しいタグ ペアが作成されません。
- **解決した問題 2331683：詳細 UI の Add-Load-balancer フォームに、バージョン 2.4 の最新の容量が表示されない**  
add-load-balancer フォームを開くと、詳細 UI に form-factor-capacity が表示されますが、バージョン 2.4 の最新情報が反映されていません。以前のバージョンの容量が表示されています。
- **解決した問題 2295819：Edge 仮想マシンがアクティブで、物理 NIC が稼働している場合でも、L2 ブリッジが「停止」状態になる**  
Edge 仮想マシンがアクティブで、L2 ブリッジ ポートをバックアップする物理 NIC が稼働している場合でも、L2 ブリッジが「停止」状態になることがあります。Edge LCP がローカル キャッシュに保存された物理 NIC 状態の更新に失敗すると、物理 NIC が停止していると見なされるため、この問題が発生します。
- **解決した問題 2243415：論理スイッチを管理ネットワークとして使用して EPP サービスを展開できない**  
EPP 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」
- **解決した問題 2364756：優先順位が重複しているため、プロファイルの認識に失敗する**  
スケールの設定で、ユーザーが vRNI と NSX IPFIX を関連付けると、管理プレーンでプロファイルが認識されず、認識エラーが発生します。
- **解決した問題 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。
- **解決した問題 2307551：すべての物理 NIC を N-VDS に移行するときに、NSX-T ホストが管理ネットワーク接続を失うことがある**  
この問題は、ホストの移行が再試行され、N-VDS で vmk0 が設定されている物理 NIC がすべて削除されると発生します。最初のホストの移行では、すべての物理 NIC と vmk0 が N-VDS に移行されますが、以降は失敗します。移行を再試行すると、すべての物理 NIC が N-VDS から削除されます。その結果、ユーザーはネットワークを介してホストにアクセスできなくなります。ホスト内のすべての仮想マシンもネットワーク接続を失い、サービスにアクセスできなくなります。
- **解決した問題 2369792：CBM プロセス メモリが大量に使用され、CBM プロセスが繰り返しクラッ**

シュする

Cloud Service Manager アプライアンスの CSM プロセスと CBM プロセスで、データベースの圧縮に失敗します。その結果、CBM プロセスのメモリが大量に使用され、CBM プロセスが繰り返しクラッシュします。

- **解決した問題 2361892：NSX Edge アプライアンスでメモリ リークが発生し、プロセスがクラッシュまたは再起動する**  
NSX Edge アプライアンスでルールの検索が繰り返し実行され、プロセスのクラッシュと再起動が発生することがあります。これにより、長期間にわたってメモリ リークが発生することがあります。ルールの検索が実行されるたびに、メモリ リークが検出されます。 フロー キャッシュをクリアしても、VIF インターフェイスが削除されないため、メモリ リークが発生します。
- **解決した問題 2364529：再設定後にロード バランサでメモリ リークが発生する**  
NSX ロード バランサで設定イベントが連続または繰り返し発生すると、メモリ リークが発生し、nginx プロセス コア ダンプが生成されることがあります。
- **解決した問題 2378876：ESXi ホストで「Usage error in dlmalloc」と「PF Exception 14 in world 3916803:VSIP PF Purg IP」エラーが発生し、PSOD が生成される**  
トラフィックが数日間実行された後、ESXi がクラッシュ (PSOD) します。クラッシュが発生する前に、他の影響は見られません。ALG トラフィック (FTP、Sunrpc、Oracle、Dcerpc、tftp) で、原子化されていない増加カウンタが競合状態になり、ALG ツリー構造が破損すると、この問題が発生します。
- **解決した問題 2384922：Edge ノードで BGPD の CPU 使用率が 100% になる**  
VTYSH で複数のセッションが実行されると、NSX-T Edge の BGPD プロセスで CPU の使用率が 100% に達する場合があります。
- **解決した問題 2386738：リンク ポートを通過するトラフィックで NAT ルールが無視される**  
Tier-0 と Tier-1 の論理ルーターを接続しているリンク ルーター ポート タイプで NAT サービスが有効になっていません。
- **解決した問題 2363618：VMware Identity Manager ユーザーが NSX Manager ダッシュボードのポリシー画面にアクセスできない**  
VMware Identity Manager で、グループ権限を含むロールが付与されたユーザーが、NSX Manager ダッシュボードのポリシー画面にアクセスできません。グループ割り当ての権限は無視されます。
- **解決した問題 2298274：REST API で無効なドメイン名または部分的なドメイン名でポリシー グループが作成または更新されることがある**  
インターフェイスで、1 つの有効なコンテンツに対して、無効な Active Directory グループまたはグループ メンバーを含む ID 式を使用してグループを作成できます。ただし、ドメイン名に関連付けられている LDAP グループが 1 つだけの場合、メンバーが有効になります。以前のバージョンの NSX-T で作成されたグループでは、アップグレード プロセスでこのエラーにフラグが設定されないため、後続のリリースでも無効なグループが維持されます。この問題は NSX-T 2.5 で修正されました。
- **解決した問題 2317147：メンバーシップが IP アドレスまたは MAC アドレスに基づいているグループに、有効な仮想マシンが表示されない**  
ユーザーがグループ内に IP アドレスまたは MAC アドレスのみのグループを作成した場合、そのグループの有効なメンバーシップが API から呼び出されたときに仮想マシンが表示されません。これによる機能上の影響はありません。ポリシーでは、管理プレーンに NSGroup が適切に作成され、IP アドレスと MAC アドレスのリストが中央の制御プレーンに直接送信されます。
- **解決した問題 2327201：KVM ハイパーバイザー上の仮想マシンの更新がすぐに同期されない**  
KVM ハイパーバイザー上の仮想マシンの更新が NSX-T で同期されるまで数時間かかることがあります。このため、KVM ハイパーバイザーで作成された新しい仮想マシンを NSGroups に追加できません。また、これらの仮想マシンにファイアウォール ルールを適用することもできません。仮想マシンの電源状態が更新されないため、KVM ハイパーバイザーをアップグレードできません。
- **解決した問題 2329443：強制同期のタイムアウトで、制御クラスタが初期化されない**

0.0.0.0-1.1.1.20 のように、IP セットの IPV4 範囲が 0.0.0.0 で始まっている場合、強制同期のタイムアウトが原因で制御クラスが初期化されません。これは IPSetFullSyncMessageProvider の問題が原因で発生します。この問題が発生すると、無限ループに入り、停止します。中央の制御プレーンが初期化されていないため、新しいワークロードを展開することはできません。

- **解決した問題 2337839**：NSX-T バックアップ ウィジェットに正しいフィールド名が表示されない  
特に、NSX-T バックアップ ウィジェットに、正しいバックアップ エラー数が表示されません。バックアップ エラーの正確な数を確認するには、NSX Manager の [バックアップ] タブで確認する必要があります。
- **解決した問題 2341552**：システムでサポートされている NIC が多すぎると、Edge の起動に失敗する  
データパス サービスまたは接続が表示されません。データパス サービスの状態が「停止」で、Edge ノードの状態が「劣化」になっています。そのため、Edge との接続の一部またはすべてが切断されます。
- **解決した問題 2390374**：NSX Manager が非常に遅くなるか、応答不能になり、ログに大量の corfu 例外が記録される  
NSX が起動できない場合もあります。corfu 例外は、Active Directory メンバーのスケールが大きすぎて、テストされた制限を超えていることを示しています。
- **解決した問題 2371150**：ベアメタル Edge ノードでレイヤー 7 ファイアウォール ルールを設定できない  
NSX-T 2.5 では、ベアメタル Edge ノードでレイヤー 7 ファイアウォール ルールがサポートされていません。このサポートを有効にする内部コマンドがありますが、これは事前検証 (POC) でのみ使用できます。
- **解決した問題 2361238**：ダウンリンク ルーターがサービス ルーターとペアリングされない  
ダウンリンク ルーターとペアリングされているサービス ルーターを削除した後に再作成しても、NAT ルールがダウンリンク ルーターに影響を及ぼすことはありません。
- **解決した問題 2363248**：API 呼び出しの接続中でも、インターフェイスでサービス インスタンスの健全性状態が「停止」と表示される  
このような不整合により、誤ってアラームが表示することがあります。

この問題の詳細と解決方法については、ナレッジベースの記事 KB67165、[「Service Instance status displays as "Down" when there are no VMs up to be protected in NSX-T」](#)を参照してください。

- **解決した問題 2359936**：ESX ホストで cfgAgent ログが頻繁にローリングされる  
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。
- **解決した問題 2332938**：フラッド防止のセキュリティ プロファイルで SYN キャッシュが有効になっている場合、実際の TCP ハーフオープン接続の上限が、NSX Manager の設定値よりも大きくなる可能性がある  
NSX-T は、設定された制限に基づいて、最適な TCP ハーフオープン接続の制限を計算します。この計算値は、構成済みの制限よりも大きくなる場合があります。計算式は、制限 Limit = (PwrOf2 \* Depth) で、PwrOf2 は 64 未満の 2 の累乗で、Depth は 32 以下の整数を表します。
- **解決した問題 2376336**：ポリシーおよび Edge で、ルート再配分のアドレス ファミリがサポートされていない  
再配分のアドレス ファミリがアプリケーションで機能していないか、使用されていません。
- **解決した問題 2412842**：ramdisk でのホストをサポートするため、ESX でメトリック ログのサイズが 40 MB に制限されている  
この問題の詳細については、[ナレッジベースの記事 KB74574](#) を参照してください。
- **解決した問題 2385070**：IPv6 サブネットに対して、IP 検出と分散ファイアウォールが反対の操作を行う

IP 検出で 2001::1/64 をホスト IP と見なし、分散ファイアウォールではこれを IPv6 サブネットとみなします。

- **解決した問題 2394896**：ホストで NSX-T Data Center 2.4.x から 2.5 にアップグレードできない  
ホストで NSX-T Data Center 2.4.0、2.4.1、2.4.2 から 2.5 へのアップグレードに失敗します。KCP モジュールのアンロードの失敗が原因の可能性があります。

この問題の詳細については、[ナレッジベースの記事 KB74674](#) を参照してください。

- **解決した問題 2406018**：パスワードの有効期限が 30 日以内になると、イベント/アラームがトリガーされる  
パスワードの有効期限が 30 日以内になると、パスワードの有効期限が無効になっている場合でも、パスワードの有効期限に関するイベント/アラームがトリガーされます。
- **解決した問題 2383328**：ユーザーが判読可能な形式でメトリック データを生成するユーティリティを提供することを要求  
NSX-T Data Center は、収集したメトリック データをバイナリ形式で保存します。このデータをユーザーが判読可能な形式で表示したいという要求がありました。この問題は、この要求を追跡するものです。
- **解決した問題 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。
- **解決した問題 2313673**：仮想マシンベースの Edge トランスポート ノード：ユーザーが NSX-T 論理スイッチ/セグメントにアップリンクを接続できない  
仮想マシンベースの Edge トランスポート ノードの場合、ユーザーは Edge トランスポート ノードのアップリンクを NSX-T 論理スイッチ/セグメントに接続できません。これらは、vCenter Server の DVPG にのみ接続できます。仮想マシンベースの Edge トランスポート ノードの追加/編集フローの NSX の設定画面には、アップリンクを vCenter Server の DVPG にマッピングするオプションのみが表示されます。アップリンクを NSX-T 論理スイッチ/セグメントにマッピングするオプションはありません。
- **解決した問題 2424394**：NSX-T DR によって中継される DHCP パケットは、ホップ数が 10 を超えると送信されない  
DHCP サーバへのホップ数が 10 を超えている場合、中継された DHCP パケットがサーバに到達しません。
- **解決した問題 2399994**：再配布ルートが断続的に欠落する  
しばらくの間 Tier-1 へのルートが使用不能になり、ネットワーク トラフィックが影響を受ける可能性があります。

## 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](#)
- [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](#)
- [NSX Intelligence 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 Cloud に関する既知の問題](#)

## 一般的な既知の問題

- **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。

- **問題 2390624**：非アフィニティ ルールにより、ホストがメンテナンス モードのときにサービス仮想マシンの vMotion ができない  
2 台のホストから設定されるクラスタにサービス仮想マシンが展開されている場合、HA ペアに非アフィニティ ルールが設定されていると、メンテナンス モードのタスクの実行中に仮想マシンを他のホストに vMotion できません。これにより、ホストでメンテナンス モードへの切り替えが自動的に行われない可能性があります。

回避策：vCenter Server でメンテナンス モードのタスクが開始する前に、ホストのサービス仮想マシンをパワーオフします。

- **問題 2329273**：同じ Edge ノードで、同じセグメントにブリッジされている VLAN 間が接続されていない  
同じ Edge ノードでセグメントを 2 回ブリッジすることはできません。2 つの異なる Edge ノードの場合、同じセグメントに 2 つの VLAN をブリッジできます。

回避策：なし

- **問題 2239365**：「Unauthorized」エラーが発生する  
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 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 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 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则表示されますが、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 2320529**：新しく追加されたデータストアにサードパーティの仮想マシンを追加した後に「サービス展開用のストレージにアクセスできません」というエラーが発生する  
クラスタ内のすべてのホストからストレージにアクセスできる場合でも、新しく追加されたデータストアにサードパーティの仮想マシンを追加した後に「サービス展開用のストレージにアクセスできません」というエラーが発生します。このエラー状態は最大 30 分間続きます。

回避策：30 分後に再試行します。あるいは、次の API 呼び出しを行い、データストアのキャッシュ エントリを更新します。

`https://<nsx-manager>/api/v1/fabric/compute-collections/<CC Ext ID>/storage-resources?`

`uniform_cluster_access=true&source=realtime`

<nsx-manager> は、サービス展開 API が失敗した NSX Manager の IP アドレス、CC Ext ID は、展開が試行されているクラスタの NSX の ID です。

- **問題 2328126**：ベアメタルの問題：NSX アップリンク プロファイルで Linux OS のボンディング インターフェイスを使用するとエラーが返される  
Linux OS でボンディング インターフェイスを作成し、このインターフェイスを NSX アップリンク プロファイルで使用すると、「トランスポート ノードの作成に失敗する可能性があります」というエラーメッセージが表示されます。VMware が Linux OS のボンディングをサポートしていないため、この問題が発生します。VMware では、ベアメタル サーバのトランスポート ノードの Open vSwitch (OVS) ボンディングをサポートしています。

回避策：この問題が発生した場合は、ナレッジベースの記事 KB67835、[Bare Metal Server supports OVS bonding for Transport Node configuration in NSX-T](#)を参照してください。

- **問題 2370555**：特定のオブジェクトを詳細インターフェイスで削除できるが、簡易インターフェイス



スに反映されない

たとえば、詳細インターフェイスの分散ファイアウォール除外リストの設定で、分散ファイアウォールの除外リストの一部として追加されたグループを削除できます。このため、インターフェイスでの動作に一貫性がなくなります。

回避策：この問題を解決するには、次の手順を実行します。

- 簡易インターフェイスで、除外リストにオブジェクトを追加します。
- 詳細インターフェイスの分散ファイアウォール除外リストに表示されていることを確認します。
- 詳細インターフェイスの分散ファイアウォール除外リストからオブジェクトを削除します。
- 簡易インターフェイスに戻り、2 番目のオブジェクトを除外リストに戻して適用します。
- 新しいオブジェクトが詳細インターフェイスに表示されていることを確認します。

- **問題 2377217：KVM ホストの再起動後、仮想マシン間のトラフィック フローが原因で予期したとおり動作しないことがある**

KVM ホストを再起動すると、仮想マシン間で到達可能性の問題が発生する可能性があります。

回避策：ホストの再起動後、次のコマンドを使用して nsx-agent サービスを再起動します。

```
# systemctl restart nsx-agent.service
```

- **問題 2371251：[バックアップとリストア] 画面に戻ると、ダッシュボードのインターフェイスが点滅する**

この問題は、Firefox ブラウザでのみ確認されています。また、特定の環境でのみ発生しています。

回避策：手動でページを更新するか、サポートされている別のブラウザを使用します。

- **問題 2408453：NSX ゲスト イントロスペクション ドライバがインストールされていると、VMware Tools 10.3.5 がクラッシュする**

VMware Tools 10.3.5 が Windows 仮想マシンでクラッシュすることがあります。その場合、リモート セッションが切断されたり、ゲスト仮想マシンがシャットダウンしたりします。

回避策：詳細については、[ナレッジベースの記事 KB70543](#) を参照してください。

- **問題 2267964：vCenter Server を削除するとき、vCenter Server で実行されているサービスの切断に関する警告がユーザーに通知されない**

ゲスト イントロスペクションなどのサービスが展開されているコンピュータ マネージャ (vCenter Server) を削除すると、これらのサービスが切断される可能性についてユーザーに通知されません。

回避策：新しい vCenter Server をコンピュータ マネージャとして正しい手順で追加すると、この問題を回避できます。

- **問題 2444170：NSX CLI コマンドでデータパスをアンインストールできない**

`del nsx` コマンドを実行しても、NSX-T の構成とモジュールがホストからアンインストールされません。このため、NSX-T のインストールまたはアップグレードが失敗します。

回避策：なし。

- **問題 2467479：ファイアウォールが SNAT ルールのバイパスに設定されると、[バイパス] から [なし] に変更してもブロックされない**

ファイアウォールが SNAT ルールのバイパスに設定されると、[バイパス] から [なし] に変更してもブロックすることができません。

回避策：SNAT ルールを削除して再作成します。

- **問題 2586606：非常に多くの仮想サーバで送信元 IP のパーステンスが設定されていると、ロード バランサが機能しない**

ロード バランサ上の多数の仮想サーバで送信元 IP のパーシステンスが設定されていると、大量のメモリが消費され、NSX Edge でメモリ不足が発生する場合があります。ただし、仮想サーバをさらに追加すると、この問題が再発する可能性があります。

回避策：送信元 IP のパーシステンスを無効にするか、送信元 IP のパーシステンスを持つ VIP を別の LB サービスに移動します。

- 問題 2730634：ユニスケール アップグレードの後でネットワーク コンポーネントのページに「インデックスが同期していません」というエラーが表示される  
ユニスケール アップグレードの後でネットワーク コンポーネントのページに「インデックスが同期していません」というエラーが表示されます。

回避策：管理者認証情報を使用して NSX Manager にログインし、start search resync policy コマンドを実行します。ネットワーク コンポーネントのロードに数分かかります。

## インストールに関する既知の問題

- 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。

## NSX Manager に関する既知の問題

- 問題 2378970：分散ファイアウォールのクラスタ レベルの有効化/無効化の設定が誤って「無効」と表示される  
管理プレーンが有効になっていても、簡易 UI で IDFW のクラスタ レベルの有効化/無効化の設定が「無効」と表示されることがあります。2.4.x から 2.5 にアップデートした後、明示的に変更を行うまで、この不正確な情報が表示されます。  
回避策：簡易 UI で、管理プレーンと一致するように、IDFW の有効化/無効化の設定を手動で変更します。

## NSX Edge に関する既知の問題

- 問題 2283559：Edge に 65k 以上のルート（RIB の場合）または 100k 以上のルート（FIB の場合）が存在すると、<https://<nsx-manager>/api/v1/routing-table> と <https://<nsx-manager>/api/v1/forwarding-table> MP APIs でエラーが発生する  
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。
- 問題 2204932：BGP ピアリングを設定すると、HA フェイルオーバー リカバリが遅延することがある  
T0 Edge とピアリングしているルーターで Dynamic-BGP-Peering を設定し、Edge（アクティブ/スタンバイ モード）でフェイルオーバー イベントが発生すると、BGP ネイバーシップの確立に 120 秒ほどかかる場合があります。

回避策：遅延を回避するため、特定の BGP ピアを構成します。

- 問題 2285650：BGP ルート テーブルに不要なルートが追加される

BGP 構成で Allowas-in オプションが有効になっていると、Edge ノードにアドバタイズされたルートが BGP ルート テーブルに戻され、インストールされます。これにより、メモリが過剰に使用され、余分なルーティング計算が発生します。超過ルートにより高いローカル プリファレンスが使用されている場合、この転送ループにより、一部のルーターのルート テーブルに冗長ルートが追加される可能性があります。

たとえば、ルート X がルーター D から開始し、ルーター A と B にアドバタイズされているとします。Allowas-in が有効になっているルーター C がルーター B とピアリングしている場合、ルーター C がルート X を学習し、ルート テーブルにインストールします。これにより、ルーター C にアドバタイズされるルート X のパスが 2 つになり、この問題が発生します。

回避策：転送ループを防ぐには、アドバタイズされるルートをブロックするように問題のあるルーター（またはそのピア）を設定します。

- 問題 2343954：Edge L2 ブリッジ エンドポイント インターフェイスで、サポートされていない VLAN 範囲を設定できる

サポートされていない場合でも、Edge L2 ブリッジとポイントの設定インターフェイスで VLAN 範囲と複数の VLAN 範囲を設定できます。

回避策：Edge L2 ブリッジとポイントの構成で、このような VLAN 範囲を設定しないでください。

## 論理ネットワークに関する既知の問題

- 問題 2389993：ポリシー画面または API で再配分ルールを変更した後、ルート マップが削除される

管理プレーンのインターフェイスまたは API から再配分ルールにルート マップを追加し、ポリシー画面のインターフェイスまたは API を使用して同じ再配分ルールを変更すると、ルート マップが削除される場合があります。この問題は、ポリシー画面のインターフェイスまたは API がルート マップの追加をサポートしていないために発生します。これにより、BGP ピアに不要なプレフィックスがアドバタイズされることがあります。

回避策：ルート マップをリストアするには、管理プレーンのインターフェイスまたは API に戻り、同じルールに再度追加します。再配分ルールにルート マップを含める場合は、常に管理プレーンのインターフェイスまたは API を使用して、ルールの作成と変更を行うことをおすすめします。

- 問題 2275412：複数の 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 2327904：アップリンクとして事前に作成した Linux ボンディング インターフェイスを使用した後、トラフィックが不安定になる、または処理に失敗する

NSX-T は、アップリンクとして事前に作成された Linux ボンディング インターフェイスをサポートしていません。

回避策：アップリンクの場合は、アップリンク プロファイルから OVS ネイティブのボンディング設定を使用します。

- 問題 2304571：VDR を使用して L3 トラフィックを実行すると、重大なエラー (PSOD) が発生することがある

保留中の arp(ND) エントリが適切に保護されず、重大なエラー (PSOD) が発生する場合があります。

回避策：なし。

- 問題 2388158：Tier-0 論理ルーター構成で中継サブネットの設定を編集できない

Tier-0 の論理ルーターを作成した後、NSX Manager インターフェイスで中継サブネットの設定を変更できません。

回避策：なし。最適な方法は、論理ルーターを削除して、目的の中継サブネット構成で再作成することです。

## セキュリティ サービスに関する既知の問題

- **問題 2294410：L7 ファイアウォールで一部のアプリケーション ID が検出される**  
SAP、SUNRPC、SVN の L7 アプリケーション ID はアプリケーションではなく、ポートに基づいて検出されます。次の L7 アプリケーション ID はサポートされていません。AD\_BKUP、SKIP、および AD\_NSP。

回避策：なし。これによるユーザーへの影響はありません。

- **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 2366599：IPv6 アドレスが設定された仮想マシンにルールを適用できない**  
仮想マシンが IPv6 アドレスを使用しているにもかかわらず、IP アドレス検出プロファイルでその VIF に IPv6 スヌーピングが有効になっていない場合、データパスでその仮想マシンのルールに IPv6 アドレスが設定されません。このため、ルールが適用されません。

回避策：IPv6 アドレスを使用する場合は常に、VIF または論理スイッチのいずれかで、IPDiscovery プロファイルの IPv6 オプションが有効になっていることを確認します。

- **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 2379632：分類されたステージでレイヤー 7 ルールに一致すると、複数のパケットがログに記録される**

分類されたステージでレイヤー 7 ルールに一致すると、複数（2、3 個）のパケットがログ (dfwpktlogs) に記録されます。

回避策：なし。

- **問題 2368948：分散ファイアウォール ルール：各セクションの認識された状態が最新ではないことがある**

分散ファイアウォール ルール ビューを更新しても、そのビューの各セクションに表示される状態が更新されません。このため、最新の情報が表示されていない可能性があります。

回避策：これは、手動での更新にのみ影響を及ぼします。認識された状態は定期的にポーリングされるため、正確な更新情報が表示されます。正確な状態を確認するため、個々のセクションを更新することもできます。

- **問題 2380833：8,000 以上のルールを含むポリシーのドラフトを発行すると時間がかかる**  
8,000 以上のルールを含むポリシーのドラフトを発行すると、時間がかかる場合があります。たとえば、8,000 個のルールを含むポリシーのドラフトを発行するには 25 分ほどかかります。

回避策：なし。

- **問題 2424818：NSX Manager インターフェイスで、レイヤー 2 と分散ファイアウォールの状態が**

## 更新されない

ワークロード仮想マシンの論理エクスポートによって生成された状態情報が管理プレーンに転送されないことがあります。その結果、これらのコンポーネントの状態が正しく更新されません。

回避策：なし。正しい状態情報を確認するには、対応する仮想マシンの CLI を使用します。

## 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 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、UI に統合の状態が「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**：PCM から AWS への呼び出しが開始しない  
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 クラウドを使用します。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 クラウドが再初期化されます。

- **問題 2401715**：正しいサムプリントを提供していても、コンピュート マネージャの更新中にエラーが発生する  
この問題は、NSX-T Manager で vCenter Server v6.7U3 がコンピュート マネージャとして追加されると発生します。vSphere 6.7 は、FQDN または IP アドレスを変更可能な PNID の変更に対応しています。NSX-T 2.5 は、この機能をサポートしていないため、サムプリントの問題が発生します。

回避策：以前に追加した vCenter Server を削除し、新しく変更された FQDN を使用して vCenter Server を追加します。vCenter Server に以前の拡張機能が存在するため、登録の追加に失敗することがあります。登録エラーを解決して、正常に登録されたことを確認します。

## NSX Intelligence に関する既知の問題

- **問題 2410806**：500 個の上限を超えたことを示す例外が発生し、生成された推奨事項を発行できない  
推奨グループのメンバー（IP アドレスまたは仮想マシン）の合計が 500 を超えると、「IPAddressExpressions、MACAddressExpressions、PathExpression のパス、ExternalIDExpression の外部 ID の合計は 500 以下にする必要があります」という例外メッセージが表示され、生成された推奨事項をポリシー構成に発行できません。

回避策：500 を超えるクライアントがアプリケーション仮想マシンまたはロード バランサに接続している場合は、アプリケーション ロード バランサへのアクセスをマイクロセグメント化するルールを作成して、推奨事項の検出を開始するアプリケーション仮想マシンを選択します。あるいは、500 個を超えるメンバー グループを複数の小さなグループに分割します。

- **問題 2362865：デフォルト ルールでルール名によるフィルタを使用できない**

この問題は、[プランとトラブルシューティング] > [検出とアクションの実行] ページで発生します。接続方法で作成されたルールにのみ影響します。この問題は、指定された接続方法に基づくデフォルトポリシーが存在しないために発生します。デフォルト ルールが管理プレーンに作成されている場合がありますが、対応するデフォルト ポリシーがないと、デフォルト ルールでフィルタリングすることはできません。フロー表示フィルタで、ルール名を使用して、ルールに一致するフローをフィルタリングします。

回避策：ルール名フィルタを適用しないでください。代わりに、保護されていないフラグを確認してください。この設定では、デフォルト ルールと、送信元と宛先に「任意」が指定されたルールに一致するフローがフィルタリングされます。

- **問題 2368926：ジョブの実行中にアプライアンスを再起動すると、推奨ジョブが失敗する**

推奨ジョブの実行中にユーザーが NSX Intelligence アプライアンスを再起動すると、ジョブは失敗した状態になります。推奨ジョブは、一連のコンテキスト仮想マシンに対して実行されます。再起動を行うと、コンテキストが削除され、その結果としてジョブが失敗します。

回避策：再起動後、同じ仮想マシンのセットに対して推奨ジョブを繰り返します。

- **問題 2385599：NSX-T Intelligence の推奨で、静的 IP のグループがサポートされない**

NSX-T インベントリで認識されていない仮想マシンとワークロードにイントラネット IP アドレスが設定されている場合、これらの仮想マシンとワークロードは、静的 IP のグループとして推奨される可能性があります（これらのグループを含む推奨定義ルールを含む）。ただし、NSX Intelligence はこのようなグループをサポートしていないため、これらのグループに送信されたトラフィックが推奨グループではなく、「不明」として表示されます。

回避策：なし。ただし、推奨は正しく機能しています。これは表示の問題です。

- **問題 2374231：SCTP、GRE、ESP プロトコル フローで、サービスが不明、ポートが 0 として表示される**

NSX Intelligence は、GRE、ESP、SCTP プロトコル フローの送信元ポートまたは宛先ポートの解析をサポートしていません。NSX Intelligence は、TCP および UDP フローに対してヘッダー全体を解析し、フロー関連の統計情報を提供します。サポートされている他のプロトコル（GRE、ESP、SCTP など）の場合、NSX Intelligence は、プロトコル固有の送信元ポートまたは宛先ポートを除く IP 情報のみを提供します。これらのプロトコルの場合、送信元ポートまたは宛先ポートは 0 になります。

回避策：なし。

- **問題 2374229：NSX Intelligence アプライアンスのディスク容量が不足する**

NSX Intelligence アプライアンスには、デフォルトで 30 日間のデータ保持期間が設定されています。30 日以内にフロー データの量が想定量を超えると、アプライアンスのディスク容量が不足し、部分的または完全に動作しなくなる可能性があります。

回避策：NSX Intelligence アプライアンスのディスク使用量を監視することで、この問題を防止または軽減できます。ディスクの使用率が高く、容量不足が示されている場合は、データ保持期間を 2、3 日短くすることができます。

1. NSX Intelligence アプライアンスに SSH で接続し、`/opt/vmware/pace/druid-config/druid_data_retention.properties` ファイルにアクセスします。
2. `correlated_flow` 設定を検索して、30 日より小さい値に変更します。例：`correlated_flow=P14D`
3. 次のコマンドを実行して、ファイルを保存し、変更を適用します。

`/opt/vmware/pace/druid-config/druid-config-data-retention.sh`

注：データが物理的に削除されるまで、最大で 2 時間かかることがあります。

- **問題 2389691：「要求のペイロード サイズが上限を超えています。1 回の要求で許可されるオブジェクトの最大値は 2,000 です」というエラーが発生し、推奨ジョブの発行に失敗する**

2,000 個を超えるオブジェクトを含む単一の推奨ジョブを発行しようとする、「要求のペイロード サイズが上限を超えています。1 回の要求で許可されるオブジェクトの最大値は 2,000 です」というエラーが発生し、失敗します。

回避策：推奨ジョブのオブジェクト数を 2,000 個より少なくして、発行を再試行します。

- **問題 2376389：中規模環境の過去 24 時間のビューで、仮想マシンが誤って「削除済み」とマークされる**

コンピュータ マネージャからトランスポート ノードが切断または削除されると、NSX Intelligence で前の仮想マシンが「削除済み」となり、その場所に新しい仮想マシンが表示されます。この問題は、NSX Intelligence が NSX データベースでインベントリの更新を追跡することが原因であり、これにより、インベントリでのコンピュータ マネージャからトランスポート ノードの切断方法に影響します。NSX Intelligence が報告するライブ仮想マシンの合計数には影響しませんが、NSX Intelligence に、重複した仮想マシンが表示される場合があります。

回避策：操作は必要ありません。選択した間隔によって時間は異なりますが、重複する仮想マシンは最終的にインターフェイスから削除されます。

- **問題 2393240：仮想マシンから IP アドレスへの追加フローが表示される**

仮想マシンから IP-xxxx への追加フローが表示される場合があります。これは、フローが作成された後に、NSX Policy Manager の構成データ（グループ、仮想マシンおよびサービス）が NSX Intelligence アプライアンスに送信されるために発生します。フローの観点から見ると、以前のフローは存在しないため、この構成と関連付けることはできません。フローが関連付けられていないため、フロー検索のデフォルトでこの仮想マシンに IP-xxxx が表示されます。構成が同期されると、実際の仮想マシン フローが表示されます。

回避策：このフローが表示されないように、期間を変更します。

- **問題 2370660：NSX Intelligence で、特定の仮想マシンに対して矛盾したデータが表示される**  
データセンター内で同じ IP アドレスを持つ仮想マシンが存在している可能性があります。NSX-T 2.5 の NSX Intelligence では、この状況をサポートしていません。

回避策：なし。データセンター内の 2 台の仮想マシンに同じ IP アドレスを割り当てないようにします。

- **問題 2372657：VM-GROUP 関係と GROUP-GROUP フロー相関の一時的に正しく表示されない**  
データセンターで処理中のフローがあるときに NSX Intelligence アプライアンスを展開すると、VM-GROUP 関係と GROUP-GROUP フロー相関の一時的に正しく表示されないことがあります。たとえば、次のような状況が一時的に起きることがあります。

- 仮想マシンが誤って未分類グループに表示される
- 仮想マシンが誤って不明グループに表示される
- 2 つのグループ間の相関フローが誤って表示される

NSX Intelligence アプライアンスの展開後、ユーザーが選択した表示期間が経過すると、このエラーは解消されます。

回避策：なし。NSX Intelligence アプライアンスの展開中に表示期間が終了した場合、この問題は発生しません。

- **問題 2366630：NSX Intelligence アプライアンスの展開中に、トランスポート ノードの削除操作が失敗することがある**

NSX Intelligence アプライアンスの展開中にトランスポート ノードを削除しようとする、トランスポート ノードが NSX-INTELLIGENCE-GROUP NSGroup から参照されているため、削除に失敗することがあります。トランスポート ノードを削除するには、NSX Intelligence アプライアンスを展開するときに強制削除オプションを指定する必要があります。

回避策：強制オプションを使用して、トランスポート ノードを削除します。



- **問題 2357296**：特定のスケールおよび負荷条件で、一部の ESX ホストから NSX Intelligence にフローが報告されないことがある  
NSX Intelligence インターフェイスに、特定のホストの仮想マシンからのフローが表示されず、それらの仮想マシンに対するファイアウォール ルールの推奨が提供されないことがあります。その結果、一部のホストでファイアウォール セキュリティが適用されない可能性があります。これは、6.7U2 および 6.5U3 より前の vSphere バージョンの環境で発生します。この問題は、コア ESX ハイパーバイザー仮想マシンでフィルタの作成と削除の順序が正しくないことが原因で発生します。  
  
回避策：ホストのバージョンを vSphere 6.7U2 以降または vSphere 6.5U3 以降にアップグレードします。
- **問題 2393142**：vIDM 認証情報を使用して NSX Manager にログインすると、「403 unauthorized user」エラーが返されることがある  
これは、ローカル ユーザーではなく、NSX Manager で vIDM ユーザーとしてログインしているユーザーにのみ影響します。NSX-T 2.5 では、NSX Intelligence アプライアンスとのやり取りで vIDM ログインと統合がサポートされていません。  
  
回避策：NSX Manager IP/FQDN に login.jsp?local=true という文字列を追加して、ローカル ユーザーとしてログインします。
- **問題 2369802**：NSX Intelligence アプライアンスのバックアップで、イベント データストアのバックアップが除外される  
この機能は、NSX 2.5 でサポートされません。  
  
回避策：なし。
- **問題 2346545**：NSX Intelligence アプライアンスの証明書を置換すると、新しいフロー情報のレポートに影響する  
NSX Intelligence アプライアンスのプリンシパル ID 証明書を自己署名証明書に置き換えると、新しいフローの処理が影響を受け、アプライアンスにそれ以降の更新情報が表示されなくなります。  
  
回避策：なし。
- **問題 2407198**：NSX Intelligence のセキュリティ状態で、仮想マシンが未分類の仮想マシン グループに誤って表示される  
ESXi ホストが vCenter Server から切断されていると、実際には他のグループに属していても、そのホストの仮想マシンは「未分類の仮想マシン」グループに表示されることがあります。ESXi ホストが vCenter Server に再接続すると、仮想マシンは正しいグループに表示されます。  
  
回避策：ホストを vCenter Server に再接続します。
- **問題 2410224**：NSX Intelligence アプライアンスの登録が完了した後、ビューを更新すると、「403 Forbidden」エラーが返されることがある  
NSX Intelligence アプライアンスの登録が完了した後に、[表示を更新] をクリックすると、「403 Forbidden」エラーが返されることがあります。NSX Intelligence アプライアンスがインターフェイスにアクセスするまでに時間がかかる場合があります。これは一時的な状態です。  
  
回避策：このエラーが表示された場合は、しばらく待ってから再試行してください。
- **問題 2410096**：NSX Intelligence アプライアンスを再起動すると、再起動前の最後の 10 分間に収集されたフローが表示されないことがある  
これは、インデックスの問題が原因です。  
  
回避策：なし。
- **問題 2436302**：NSX-T 統合アプライアンス クラスタ証明書を置き換えた後、API またはマネージャ インターフェイスを介して NSX Intelligence にアクセスできない

NSX-T Manager インターフェイスで [プランとトラブルシューティング] タブに移動し、[検出とアクションの実行] または [推奨] をクリックすると、インターフェイスがロードされず、最終的に次のようなエラーが返されます。「要求されたアプリケーションのロードに失敗しました。再試行してください。問題が解決しない場合は、サポートにお問い合わせください。」

回避策：詳細と回避策については、[ナレッジベースの記事 KB76223](#) 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 2401164**：SFTP サーバ エラーが発生したにもかかわらず、バックアップが成功と報告される  
バックアップに使用する SFTP サーバのパスワードが期限切れになっている場合、NSX-T は「バックアップ処理で不明なエラーが発生しました」という一般エラーを報告します。

回避策：SFTP サーバにアクセスするための認証情報が最新であ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 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 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 2330417**：アップグレードされていないトランスポート ノードのアップグレードが実行できない

アップグレード時に、一部のトランスポート ノードがアップグレードされていない場合でも、アップグレード成功とマークされます。ログの場所：/var/log/upgrade-coordinator/upgrade-coordinator.log。

回避策：upgrade-coordinator サービスを再起動します。

- **問題 2348994**：ESXi 6.5 p03 トランスポート ノードの NSX VIB のアップグレード中に、一時的な障害が発生する

この問題は、2.4.x から 2.5 へのアップグレードで発生することがあります。ESXi 6.5 p03 トランスポート ノードの NSX VIB をアップグレードすると、次のエラーが発生し、アップグレードに失敗することがあります。「VI SDK invoke exception: Got no data from process: LANG=en\_US.UTF-8」

回避策：ESXi 5 p04 にアップグレードします。または、ホストをメンテナンス モードにして再起動します。アップグレードを再試行し、メンテナンス モードを終了します。

- **問題 2372653**：2.5 へのアップグレード後、以前の NSX-T バージョンで作成した LogicalPort と LogicalSwitch ベースのグループが見つからない

2.5 へのアップグレード後、以前の NSX-T バージョンのポリシーで作成した LogicalPort と LogicalSwitch ベースのグループがダッシュボード インターフェイスに表示されません。ただし、API では検索できます。この問題は、アップグレード プロセスで行われた名前の変更が原因で発生しています。2.5 では、LogicalPort と LogicalSwitch ベースのグループはセグメント ベースと SegmentPort ベースのグループとして表示されます。

回避策：アップグレード後、これらのポリシー グループにアクセスするには、API を使用します。

- **問題 2408972**：アップグレードで最後のホストの修正中に vSphere Update Manager でエラーが発生する

アップグレードで、NSX-T 論理スイッチによってバックアップされているワークロードを含む最後のホストを修正中に、vSphere Update Manager でエラーが発生します。

回避策：NSX-T でバックアップされているすべてのワークロード仮想マシンをアップグレード済みのホストに手動で移行してから、失敗したホストのアップグレードを再試行します。

- **問題 2400379**：[コンテキスト プロファイル] 画面に、サポートされていない APP\_ID エラー メッセージが表示される

[コンテキスト プロファイル] 画面に、次のエラーメッセージが表示されます。「このコンテキスト プロファイルは、サポートされていない APP\_ID - [<APP\_ID>] を使用しています。どのルールでも使用されていないことを確認してから、このコンテキスト プロファイルを手動で削除してください。」この問題は、データパスで機能しなくなった 6 つの非推奨 APP\_ID (AD\_BKUP、SKIP、AD\_NSP、SAP、SUNRPC、SVN) がアップグレード後に存在するために発生します。

回避策：使用されていないことを確認してから、6 つの APP\_ID コンテキスト プロファイルを手動で削除します。

- **問題 2419246**：Ubuntu KVM のアップグレードが失敗する

nsx-vdpi サービスが実行されていないため、Ubuntu KVM ノードのアップグレードに失敗することがあります。nsx-vdpi サービスは nsx-agent に依存しますが、アップグレードのこの時点で nsx-agent が設定されていません。vm-command-relay が正常に開始されていないため、nsx-agent が失敗します。

回避策：インストールが完了していない nsx-agent の設定を行います。次のコマンドを実行して、解凍または部分的に設定されたパッケージをすべて再設定します。

```
dpkg --configure -a
```

または、次のコマンドを使用して、nsx-agent と nsx-vdpi のみを再設定します。

```
dpkg --configure nsx-agent
```

```
dpkg --configure nsx-vdpi
```

- 問題 2260435：デフォルトで API によって作成されたステートレス リダイレクト ポリシーまたはルールが East-West 接続でサポートされない

デフォルトで API によって作成されたステートレス リダイレクト ポリシーまたはルールが East-West 接続でサポートされません。このため、トラフィックがパートナーにリダイレクトされません。

回避策：ポリシー API を使用してリダイレクト ポリシーを作成する場合は、ステートフル セクションを作成します。

- 問題 2200856：cloud-service-manager サービスを再起動できない

ユーザーが API サービスの初期起動を待たずにこの操作を行うと、cloud-service-manager サービスの再起動に失敗します。

回避策：数分待ってから再試行してください。

- 問題 2378752：API で、セグメントまたはポートに複数のバインド マップを作成できてしまう  
この問題は API でのみ発生します。セグメントまたはポートの下に複数のバインドマップを作成しても、エラーが報告されません。この問題は、ユーザーがセグメントまたはポート上の複数のプロファイルと同時に割り当てようとした場合に発生します。

回避策：この操作を実行する代わりに、NSX Manager インターフェイスを使用します。

## NSX Cloud に関する既知の問題

- 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 2355113：Microsoft Azure でネットワークの高速化が有効になっている場合、RedHat および CentOS ワークロード仮想マシンに NSX Tools をインストールできない

Microsoft Azure で、RedHat (7.4 以降) または CentOS (7.4 以降) ベースのオペレーティング システムを使用し、ネットワークの高速化が有効になっているときに、NSX Agent をインストールすると、イーサネット インターフェイスが IP アドレスを取得しません。

回避策：Microsoft Azure で RedHat または CentOS ベースの仮想マシンを起動した後、最新の Linux Integration Services ドライバをインストールします。このドライバは <https://www.microsoft.com/en-us/download/details.aspx?id=55106> にあります。ドライバのインストールが完了したら、NSX Tools をインストールします。

- 問題 2391231：Azure 仮想マシンに対する変更の検出が遅れることがある

クラウド上の Azure 仮想マシンに対する変更の検出が断続的に遅れることがあります。この遅延が仮想マシンのオンボーディングと NSX-T 内での論理エンティティが作成に影響を及ぼす可能性があります。確認された最大遅延時間は約 8 分です。

回避策：なし。遅延期間が経過すると、問題が自動的に解決されます。

- 問題 2424818：L2 と分散ファイアウォールの統計情報が NSX Manager UI で更新されない

ワークロード仮想マシンの論理エクスポートによって生成された統計情報の一部が管理プレーンに転送されていません。このため、NSX Manager UI に統計情報が表示されません。NSX Manager UI から分散ファイアウォールの統計情報は確認することはできません。論理スイッチ ポートの動作状態は「停止」と表示され、対応する統計情報が利用できません。この問題は、クラウド仮想マシンでのみ発生します。

回避策：なし。この統計情報は、対応する仮想マシンの CLI から確認できます。