

VMware NSX for vSphere 6.2.1 リリース ノート

ドキュメント更新日：2016 年 5 月 20 日

VMware NSX for vSphere 6.2.1 | 2015 年 12 月 17 日リリース | ビルド 3300239 |

リリース ノートの概要

本リリース ノートには、次のトピックが含まれています。

- [新機能](#)
- [推奨されるバージョン、システム要件、およびインストール](#)
- [アップグレードに関する注意事項](#)
- [既知の問題](#)
- [解決した問題](#)
- [ドキュメントの改訂履歴](#)

新機能

NSX [6.2.1](#) および [6.2.0](#) の新機能と変更点は次のとおりです。

6.2.1 の新機能

NSX 6.2.1 リリースでは多くのバグが修正されています。これらは「[解決した問題](#)」セクションに記載されています。

- **6.1.5 の修正**：このリリースには、NSX for vSphere 6.1.5 と同じ重要な修正が含まれます。
- **新しい show control-cluster network ipsec status コマンド**により、IPsec (Internet Protocol Security) の状態を確認できる
- **接続ステータス**：NSX Manager ユーザー インターフェイスで NSX Controller クラスタの接続ステータスを表示可能
- **vRealize Orchestrator Plug-in for NSX 1.0.3 のサポート**：NSX 6.2.1 リリースでは、vRealize Automation 7.0.0 用に vRealize Orchestrator Plugin for NSX 1.0.3 が追加されます。このプラグインには、vRealize Automation 7.0 がネットワークとセキュリティのエンドポイントとして NSX for vSphere 6.2.1 を使用する際に、パフォーマンスが向上する修正が含まれます。
- **6.2.1 より**、NSX Manager はクラスタ内の各コントローラ ノードでクエリを実行して、当該コントローラとクラスタ内の他のコントローラ間の接続情報を入手する
これは、NSX REST API (「GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller」コマンド) の出力として提供され、コントローラ ノード間のピア接続ステータスを表示します。NSX Manager が、任意の 2 台のコントローラ ノード間の接続が切断されていることを認識すると、システム イベントが生成され、ユーザーに警告します。

- Service Composer が公開する API により、ユーザーは Service Composer ワークフローのファイアウォール ドラフトの自動生成を設定できる
REST API を用いて、この設定を有効/無効に切り替えることができ、再起動後もその変更が維持されます。無効にすると、ポリシー ワークフロー用のドラフトは分散ファイアウォール内に生成されません。これにより、システム内で自動生成されるドラフトの数が抑えられ、パフォーマンスが向上します。

6.2.0 の新機能

NSX for vSphere 6.2.0 には次の新機能と変更された機能が含まれます。

- Cross-vCenter Networking and Security

- NSX 6.2 と vSphere 6.0 の併用による、Cross-vCenter NSX のサポート：これにより、論理スイッチ (LS)、分散論理ルーター (DLR)、分散ファイアウォール (DFW) を複数の vCenter Server にわたってデプロイできるようになるため、複数の vCenter Server や複数の物理的な場所にワークロード (仮想マシン) が分散しているアプリケーションに対し、論理ネットワークとセキュリティを提供できます。
- 複数の vCenter Server 間で一貫したファイアウォール ポリシー：NSX のファイアウォール ルールセクションを「ユニバーサル」としてマークし、このセクションで定義したルールが複数の NSX Manager に複製されるようになりました。これにより、複数の NSX 環境に一貫したファイアウォール ポリシーを定義するワークフローが簡素化されます。
- Cross-vCenter vMotion と分散ファイアウォール：「ユニバーサル」セクションでポリシーが定義されている仮想マシンは、異なる vCenter Server に属するホスト間を移動しても、一貫したセキュリティ ポリシーが適用されます。
- ユニバーサル Security Group：IP アドレス、IP セット、MAC アドレス、および MAC セットに基づく NSX 6.2 の Security Group をユニバーサル ルール内で使用して、グループとグループ メンバーシップを複数の NSX Manager 間で同期できるようになりました。また、複数の NSX Manager にまたがるオブジェクト グループ定義の一貫性が向上し、ポリシーを一貫して適用できます。
- ユニバーサル論理スイッチ (ULS)：Cross-vCenter NSX の一部として NSX 6.2 で追加された新機能です。複数の vCenter Server にまたがる論理スイッチの作成が可能になるため、ネットワーク管理者はアプリケーションまたはテナント用に連続する L2 ドメインを作成できます。
- ユニバーサル分散論理ルーター (UDLR)：Cross-vCenter NSX の一部として NSX 6.2 で追加された新機能で、複数の vCenter Server にまたがる分散論理ルーターが作成できるようになります。ユニバーサル分散論理ルーターを使用すると、前述のユニバーサル論理スイッチ間のルーティングが可能になります。さらに、NSX UDLR ではワークロードの物理的な場所に基づいて垂直方向のルーティングを最適化することができます。

- 操作とトラブルシューティングの機能強化

- 新しいトレースフロー トラブルシューティング ツール：トレースフローは、問題が仮想ネットワークまたは物理ネットワークのどちらで発生しているかを特定するのに役立つトラブルシューティング ツールです。ソースからターゲットまでパケットをトレースして、そのパケットが仮想ネットワーク内のさまざまなネットワーク機能をどのように通過するかを確認できます。
- フロー モニタリングと IPFIX の分離：NSX 6.1.x でも IPFIX レポートがサポートされていましたが、IPFIX レポートを有効にできるのは、NSX Manager への フロー モニタリング機能も有効にしている場合に限られていました。NSX 6.2.0 から、これらの機能が分離されます。NSX 6.2.0 以降では、NSX Manager での フロー モニタリング設定に関係なく IPFIX を有効にできます。
- 6.2 における監視およびトラブルシューティングの新しい CLI コマンド：詳細については、[ナレッジベースの記事 KB2129062](#) を参照してください。

- セントラル CLI：セントラル CLI は、分散ネットワーク機能のトラブルシューティング時間を縮小します。NSX Manager のコマンド ラインからコマンドを実行し、コントローラ、ホスト、および NSX Manager から情報を取得します。これによって、複数のソースにすばやくアクセスし、情報を比較することができます。セントラル CLI は、論理スイッチ、分散論理ルーター、分散ファイアウォール、および Edge に関する情報を提供します。
- ping CLI コマンドに設定可能なパケット サイズと do-not-fragment フラグを追加：NSX 6.2.0 から、NSX の「ping」CLI コマンドに、データ パケット サイズ (ICMP ヘッダを含まない) と do-not-fragment フラグを設定できるオプションが提供されます。詳細については、[NSX CLI リファレンス](#)を参照してください。
- 通信チャネルの健全性の表示：NSX 6.2.0 では、通信チャネルの健全性を監視する機能が追加されました。NSX Manager とファイアウォール エージェント間、NSX Manager と制御プレーン エージェント間、ホストと NSX Controller 間のチャネルの健全性ステータスを NSX Manager のユーザー インターフェイスで確認できます。さらに、ホスト コマンド チャネルが、より優れたフォルト トレランスを提供します。
- スタンドアロン Edge L2 VPN クライアント CLI：NSX 6.2 以前は、スタンドアロン NSX Edge L2 VPN クライアントを構成するには、vCenter Server に提供されている OVF 設定をデプロイするしか方法はありませんでした。このたび、スタンドアロン NSX Edge 専用のコマンドが追加され、コマンド ライン インターフェイスで設定することが可能になりました。

• 論理ネットワークとルーティング

- L2 ブリッジと分散論理ルーターの相互運用性：VMware NSX for vSphere 6.2 では、L2 ブリッジが分散論理ルーティングに参加できるようになりました。ブリッジ インスタンスに接続された VXLAN ネットワークが、ルーティング インスタンスとブリッジ インスタンスを接続するために使用されます。
- Edge Services Gateway (ESG) および分散論理ルーター インターフェイスでの RFC 3021 準拠の /31 プリフィックスのサポート
- ESG DHCP サーバ上でリレーされた DHCP 要求のサポートの強化
- NSX 仮想ネットワーク内で VLAN ID/ヘッダーを維持する機能
- 再分配フィルタにおける完全一致：再分配フィルタの一致アルゴリズムは ACL と同じです。したがって、デフォルトでは完全プリフィックス一致が実行されます（ただし、le または ge オプションが使用された場合を除く）。
- スタティック ルートのアドミニストレーティブ ディスタンスのサポート
- Edge のインターフェイスごとに uRPF チェックを有効、緩和、または無効にする機能
- CLI コマンド **show ip bgp** での AS パスの表示
- 分散論理ルーター制御仮想マシンでのルーティング プロトコルへの再分配から 高可用性インターフェイスを除外
- 分散論理ルーターの強制同期：分散論理ルーター間の East - West のルーティング トラフィックのデータ損失を回避します。North - South のルーティングとブリッジングでは引き続き中断が発生する場合があります。
- 高可用性構成の Edge アプライアンスが、アクティブかバックアップかを確認：NSX 6.2 Web クライアントでは、高可用性構成の 2 台の NSX Edge アプライアンスが、アクティブまたはバックアップのどちらであるかを確認できます。

- REST API が Edge でのリバース パス フィルタ (rp_filter) をサポート：システム制御 REST API を使用すると、ユーザー インターフェイスを使用して rp_filter sysctl を設定できます。また、これは vNIC インターフェイスおよびサブ インターフェイスの REST API にも発行されます。詳細については、[NSX API のドキュメント](#)を参照してください。
- IP プリフィックス **GE** および IP プリフィックス **LE** の BGP ルート フィルタの動作：NSX 6.2 では、BGP ルート フィルタが次のように機能強化されています。
 - LE/GE キーワードを使用できない：null ルート ネットワーク アドレス (ANY として定義または CIDR 形式 0.0.0.0/0 で定義) に対し、「以下 (LE)」と「以上 (GE)」のキーワードは使用できなくなりました。以前のリリースでは、これらのキーワードの使用は許可されていました。
 - LE と GE の値が 0 ～ 7 の場合、有効な値として処理されます。以前のリリースでは、この範囲は無効でした。
 - 所定のルート プリフィックスに対して、指定した LE 値よりも大きい GE 値を指定できなくなりました。

• ネットワークと Edge サービス

- 分散論理ルーターの管理インターフェイスの名称を高可用性インターフェイスに変更：高可用性のキープアライブがこのインターフェイスを経由すること、またインターフェイス上のトラフィックが中断するとスプリットブレイン状態になる場合があることから、これらを強調するわかりやすい名称に変更しました。
- ロード バランサの健全性監視の強化：障害に関する情報の報告、最新の健全性チェックとステータス変更の追跡、および障害原因の報告を行う詳細な健全性監視が可能になります。
- 仮想 IP アドレス (VIP) およびプール ポート範囲のサポート：ポート範囲の指定が必要なアプリケーションで、ロード バランサが利用できるようになります。
- 仮想 IP アドレスの最大数の増加：使用可能な仮想 IP アドレス数が増加し、最大 1024 までサポートされます。

• セキュリティ サービスの機能強化

- 仮想マシンの新しい IP アドレス検出メカニズム：仮想マシン名またはその他の vCenter Server ベースの属性に基づいてセキュリティ ポリシーを確実に適用するには、NSX が仮想マシンの IP アドレスを認識している必要があります。NSX 6.1 以前では、各仮想マシン上に VMware Tools (vmtools) をインストールするか、または各仮想マシンの IP アドレスを手動で認証することによって、特定の仮想マシンの IP アドレスを検出していました。NSX 6.2 では、ハイパーバイザーから検出を行うことで、仮想マシンの IP アドレスを検出するオプションが追加されています。これらの新しい検出メカニズムにより、VMware Tools がインストールされていない仮想マシンでも、NSX がオブジェクトベースの分散ファイアウォール ルールを適用できるようになりました。

• ソリューションの相互運用性

- vSphere 6.0 Platform Services Controller トポロジのサポート：すでにサポート対象となっている組み込みの Platform Services Controller (PSC) 構成に加えて、外部の PSC が NSX でサポートされます。
- vRealize Orchestrator Plug-in for NSX のサポート：NSX 6.2 は、NSX と vRealize Orchestrator を統合する [vRealize Orchestrator Plugin](#) をサポートしています。

システム要件とインストール

製品またはコンポーネント	推奨されるバージョン
NSX for vSphere	6.2.1
vSphere	5.5U3 または 6.0U1
ゲスト イントロスペクション	<p>ゲスト イントロスペクションとネットワーク イントロスペクション ベースの NSX の機能は、特定の VMware Tools (VMTools) バージョンとの互換性があります。VMware Tools に含まれるオプションの NSX ネットワーク イントロスペクション ドライバ コンポーネントを有効にするには、次のいずれかにアップグレードする必要があります。</p> <ul style="list-style-type: none"> • VMware Tools 5.1 P07 以降 • VMware Tools 5.5 P04 以降 • VMware Tools 6.0 P01 以降 • VMware Tools 10.0 以降
vRealize Orchestrator	vRealize Orchestrator Plugin for NSX 1.0.3

NSX インストールの前提条件の詳細については、『NSX 6.2 インストール ガイド』の「[NSX のシステム要件](#)」のセクションを参照してください。

アップグレードに関する注意事項

- アップグレード パス：
 - NSX 6.x からのアップデート：『[VMware 製品の相互運用性マトリクス](#)』を参照してください。[サポートされるアップグレード パス](#)。すべてのバージョンへのアップグレードがサポートされているわけではありません。対象の製品がアップグレード可能なバージョンかどうか、必ずご確認ください。
 - Cross-vCenter サイトのアップグレード：Cross-vCenter NSX 環境をアップグレードする場合は、このドキュメントの後半の「[Cross-vCenter のアップグレード](#)」を参照してください。
 - vCNS 5.x からのアップグレード：vCNS 5.x から NSX 6.2.1 への直接アップグレードはサポートされていません。ただし、2016 年 3 月 31 日以降に公開される NSX 6.2.2 アップグレード バンドルを使用すると、VMware vCloud Networking and Security (vCNS) 5.1.x または 5.5.x から NSX 6.2.2 へ直接アップグレードできます。手順については、『NSX アップグレード ガイド』の「[vCloud Networking and Security 5.5.x から NSX 6.2 へのアップグレード](#)」を参照してください。
 - NSX 6.1.6 からのアップデート：NSX 6.1.6 から NSX 6.2.0、6.2.1、または 6.2.2 へのアップデートはサポートされません。
 - NSX 6.1.5 からのアップデート：NSX 6.1.5 から NSX 6.2.0 へのアップデートはサポートされていません。NSX 6.1.5 から NSX 6.2.1 へのアップデートは推奨されません。代わりに、NSX 6.2.2 以降へアップデートすることで、最新のセキュリティ アップデートを取得できます。
- 6.2.x へのアップデートが成功したかどうか確認するには、この[ナレッジベースの記事 KB2134525](#)を参照してください。

- 他の VMware 製品との同時アップグレード：vCenter Server や ESXi などの他の VMware 製品とともに NSX をアップグレードする場合は、サポートされるアップグレード手順を実行する必要があります。アップグレード手順については、[ナレッジベースの記事 KB2109760](#) を参照してください。
- アップグレードに影響する既知の問題：アップグレードに関連する既知の問題については、このドキュメントの後半の「[インストールとアップグレードに関する既知の問題](#)」を参照してください。
- 新しいシステム要件：NSX 6.2.x では、NSX Manager をインストールおよびアップグレードするためのメモリと CPU の要件が NSX 6.1.x とは異なっています。『NSX 6.2 のインストール』または『NSX 6.2 のアップグレード』の「[NSX のシステム要件](#)」を参照してください。
- NAT ルールの最大数：NSX Edge 6.2 より前のバージョンでは、ユーザーは SNAT ルールと DNAT ルールをそれぞれ 2048 ずつ設定できたため、ルールの最大数は 4096 でした。NSX Edge 6.2 以降は、NSX Edge アプライアンスのサイズに基づいて、NAT ルールの最大数が制限されます。

「Compact」サイズでは SNAT ルールと DNAT ルールがそれぞれ 1024 ずつで、上限は合計で 2048 です。

「Large」および「Quad Large」サイズでは SNAT ルールと DNAT ルールがそれぞれ 2048 ずつで、上限は合計で 4096 です。

「X-Large」サイズでは SNAT ルールと DNAT ルールがそれぞれ 4096 ずつで、上限は合計で 8192 です。

NSX Edge を 6.2 にアップグレードする際に、既存の「Compact」Edge で NAT ルールの数（SNAT と DNAT の合計）が上限の 2048 を超えている場合、検証に失敗し、アップグレードできません。この場合、アプライアンス サイズを「Large」または「Quad Large」に変更し、アップグレードを再試行する必要があります。

- 分散論理ルーターおよび Edge Services Gateway 上の再分配フィルタの動作の変更：NSX 6.2 リリース以降、分散論理ルーターおよび Edge Services Gateway (ESG) の再分配ルールは ACL と同様に動作します。すなわち、ルールが完全に一致した場合、それぞれのアクションが実行されます。
- VXLAN トンネル ID：NSX 6.2.0 にアップグレードする前に、VXLAN トンネル ID 4094 をどのトンネルでも使用していないことを確認してからインストールする必要があります。VXLAN トンネル ID 4094 は使用できなくなりました。これに対処するには、以下の手順を実行してください。
 1. vCenter Server で [ホーム] > [Networking and Security] > [インストール手順] の順に移動し、[ホストの準備] タブを選択します。
 2. VXLAN 列の [設定] をクリックします。
 3. [VXLAN ネットワークの] ウィンドウで、VLAN ID を 1 ～ 4093 の値に設定します。
- vSphere Web Client のリセット：NSX Manager をアップグレードした後、vSphere Web Client サーバをリセットする必要があります（『[NSX アップグレード](#)』ドキュメントを参照）。これを行うまで [Networking and Security] タブが vSphere Web Client に表示されない場合があります。
- ステートレス環境：ステートレス ホスト環境での NSX のアップグレードでは、新しい VIB URL を使用します。ステートレス ホスト環境では、NSX アップグレード プロセスで、新しい VIB がホスト イメージ プロファイルに事前追加されます。ステートレス ホストで NSX のアップグレードを行う場合は、次の手順を実行してください。

1. NSX Manager で、固定 URL から最新の NSX VIB を手動でダウンロードします。
2. ホスト イメージ プロファイルに VIB を追加します。

NSX 6.2.0 より前のバージョンでは、NSX Manager 上に 1 つの URL があり、そこから特定バージョンの ESX ホストの VIB を見つけることができました。つまり、管理者は NSX バージョンに関係なく、1 つの URL を知っておくだけで済みました。NSX 6.2.0 以降では、新しい NSX VIB を異なる URL で利用できません。正しい VIB を見つけるには、以下の手順を実行する必要があります。

- 新しい VIB URL を `https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties` から見つけます。
 - 必要な ESX ホスト バージョンの VIB を、対応する URL から取得します。
 - 取得した VIB をホスト イメージ プロファイルに追加します。
- **Cross-vCenter のアップグレード**：『NSX アップグレード ガイド』には、Cross-vCenter NSX を実行するサイトのアップグレードに関する説明がありません。次の手順に従って、Cross-vCenter NSX 環境のアップグレードを行います。
 1. 『NSX アップグレード ガイド』の説明に従って、NSX Manager をアップグレードします。最初にプライマリの NSX Manager をアップグレードし、次にすべてのセカンダリ NSX Manager をアップグレードしてください。すべての NSX Manager を同じバージョンにアップグレードする必要があります。単一の Cross-vCenter NSX 環境で、複数バージョンの NSX Manager を使用することはサポートされていません。
 2. 『NSX アップグレード ガイド』の説明に従って、NSX Controller をアップグレードします。コントローラのアップグレードは、NSX Manager のアップグレードと同じメンテナンス期間中に実行することをお勧めします。
 3. 『NSX アップグレード ガイド』の「NSX 6.2 へのホスト クラスタのアップグレード」のセクションに記載の手順を実行し、アップグレードを完了します。
 - **VMware vCloud Network and Security (vCNS) のアップグレード**：VMware vCloud Network and Security 5.x を VMware NSX for vSphere 6.2 にアップグレードする場合、事前の確認が必要です。VMware vCloud Network and Security 5.5.x から VMware NSX for vSphere 6.2 にアップグレードする前に、次の REST API 呼び出しを使用して、アップリンク ポート名の情報がテーブルに含まれていることを確認します。

GET `https://<nsxmgr-IP>/api/2.0/vdn/switches`

出力で、`uplinkPortName` フィールドを探します。次はその例です。

```
<?xml version="1.0" encoding="UTF-8"?>
<vdsContexts>
  <vdsContext>
    <switch>
      <objectId>dvs-22</objectId>
      <objectTypeName>VmwareDistributedVirtualSwitch</objectTypeName>
      <nsxmgrUuid>4236F6CA-3B1A-56BE-4B55-1EF82B8CA12D</nsxmgrUuid>
      <revision>2</revision>
      <type>
        <typeName>VmwareDistributedVirtualSwitch</typeName>
      </type>
      <name>1-vds-20</name>
      <scope>
        <id>datacenter-3</id>
        <objectTypeName>Datacenter</objectTypeName>
        <name>datacenter-1</name>
      </scope>
      <clientHandle />
      <extendedAttributes />
    </switch>
```

```
<mtu>1600</mtu>
<teaming>FAILOVER_ORDER</teaming>
<uplinkPortName>uplink2</uplinkPortName>
<promiscuousMode>>false</promiscuousMode>
</vdsContext>
</vdsContexts>
```

このコマンドの出力に各 vSphere Distributed Switch の 1 つ以上のアップリンク ポート名が含まれる場合、アップグレードに進むことができます。出力にアップリンク ポート名が含まれていない場合は、[ナレッジベースの記事 KB2129200](#) を参照してください。

既知の問題

既知の問題には次の種類があります。

- [一般的な既知の問題](#)
- [インストールとアップグレードに関する既知の問題](#)
- [NSX Manager に関する既知の問題](#)
- [論理ネットワークと NSX Edge 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](#)
- [監視サービスに関する既知の問題](#)

一般的な既知の問題

一部の Log Insight レポートが NSX 6.2 でサポートされない

NSX 6.2 と NSX 用 vRealize コンテンツ パックは互換性がないため、NSX 6.2 では次の vRealize Log Insight のレポートがサポートされません。

- ダッシュボード内：NSX-vSphere-Infrastructure: ホスト - コントローラ：通信エラー、ウィジェットはサポートされません
- ダッシュボード内：論理スイッチ - 概要、次のウィジェットはサポートされません。
 - 論理スイッチ作成監査イベント
 - 論理スイッチ更新監査イベント
 - 論理スイッチ削除監査イベント
- ダッシュボード内：分散論理ルーター - 概要、次のウィジェットはサポートされません。
 - 分散論理ルーター作成監査イベント
 - 分散論理ルーター更新監査イベント

回避策： なし。最新情報については、[VMware ナレッジベースの記事 KB2143058](#) を参照してください。

ルールで使用する仮想マシンの MAC アドレスが変更されると、レイヤー 2 (L2) ルールが適用されない場合がある

L2 ルールの最適化はデフォルトでオンになっているため、送信元フィールドと宛先フィールドの両方が [任意] 以外に指定されている L2 ルールは、vNIC の MAC アドレスが送信元または宛先の MAC アドレス リストに一致する場合にのみ、vNIC (またはフィルタ) に適用されます。送信元または宛先 MAC アドレスと一致しない仮想マシンがあるホストには、これらの L2 ルールは適用されません。

回避策： すべての vNIC (またはフィルタ) に L2 ルールを適用するには、ソースまたはターゲット フィールドのいずれかを [任意] に設定する必要があります。

ユーザーが 1 回の API 呼び出しで、1 つのセキュリティ タグを複数の仮想マシンに一度に割り当てる場合、NSX では URL の長さが 16,000 文字に制限される

ユーザーが 1 回の API 呼び出しで、1 つのセキュリティ タグを複数台の仮想マシンに一度に割り当てようとしても、URL が 16,000 文字を超える場合は割り当てられません。利用可能な URL の文字数は、最大 16,000 文字です。

回避策：

1. URL の長さを 16,000 文字未満にする必要があります。
2. パフォーマンスが最適化されるのは、1 回の呼び出しで約 500 台の仮想マシンにタグ付けされている場合です。1 回の呼び出しで、それよりも多くの仮想マシンに タグ付けすると、パフォーマンスの低下を招く場合があります。

ユーザー インターフェイスと API で、レポートに表示されるサービスのステータスが一致しない
ユーザー インターフェイス の [設定] タブで、L2 サービスのステータスが停止中と表示されているにもかかわらず、API では稼働中と表示されます。

回避策： 画面を更新します。

ユーザー インターフェイスで、本来 Edge に適用できない、受信/送信の NSX ファイアウォール ルールを作成できる

Web クライアントでは、1 つ以上の NSX Edge に適用される NSX ファイアウォール ルールの作成が誤って許可されてしまいます。これは、ルール内に「受信」または「送信」方向に移動するトラフィックがあり、PacketType が IPV4 または IPV6 の場合に発生します。NSX は、このようなルールを NSX Edge に適用できないため、ユーザー インターフェイスからこのようなルールを作成できないようにすべきです。

回避策： なし。

ユーザーは NSX Controller のログを順次ダウンロードする必要がある

NSX Controller のログをダウンロードしてトラブルシューティングに使用できます。ただし、既知の問題があるため、複数のコントローラ ログを同時にダウンロードできません。複数のコントローラからダウンロードする場合でも、進行中のコントローラのダウンロードが終了するまで待ってから、次のコントローラのダウンロードを開始する必要があります。また、一度ログのダウンロードを開始すると、キャンセルすることはできません。

回避策： 進行中のコントローラ ログのダウンロードが終了するまで待ってから、次のログのダウンロードを開始します。

NSX Manager から CSV 形式でエクスポートしたログ ファイルのタイムスタンプが一般的な日時ではなくエポック時間である

vSphere Web Client を使用して NSX Manager からログファイルを CSV 形式でエクスポートした場合、ログ ファイルのタイムスタンプが、タイム ゾーンに基づく適切な時間ではなく、ミリ秒単位のエポック時間で記述されることがあります。

回避策： なし。

NSX トレースフロー ツールを使用してブリッジ ネットワーク上の仮想マシンを選択することができない
NSX トレースフロー ツールを使用して、論理スイッチに接続されていない仮想マシンを選択することはできません。つまり、L2 ブリッジ ネットワーク上の仮想マシンの場合、トレースフロー検査の送信元アドレスまたは宛先アドレスとして仮想マシン名を選択することはできません。

回避策： L2 ブリッジ ネットワークに接続された仮想マシンの場合、インターフェイスの IP アドレスまたは MAC アドレスを使用すれば、トレースフロー検査の宛先として指定できます。L2 ブリッジ ネットワークに接続された仮想マシンを送信元として選択することはできません。詳細については、[ナレッジベースの記事 KB2129191](#) を参照してください。

フロー モニタリングでは、5 分間で 200 万フローの制限を超えるとフローがドロップされる

NSX フロー モニタリングは最大 200 万件のフロー レコードを保持します。ホストが 5 分間に 200 万件を超えるレコードを生成すると、新しいフローはドロップされます。

NSX フロー モニタリングは本番稼動に対応していますが、スループットおよび 1 秒あたりの接続数の要件が低い場合にのみ適用できます。また、トラブルシューティングや、一時的なルール作成時にも使用できます。スループットが高い場合、NSX Manager での CPU 使用率の上昇、RabbitMQ メッセージ バスのオーバーフロー、ポリシー更新のデプロイの失敗といった問題が発生する可能性があります。また、大規模な UDP ワークロードでも問題が発生します。エンタープライズ規模での継続的なフロー情報収集には、IPFIX をお勧めします。フローモニタリングを一度無効にすると、データベース内のフロー データのパーティに 15 日間ほどかかる可能性があるため注意が必要です。

回避策： なし。

NSX API が特定の状況で XML ではなく JSON を返す

API 要求に対して、XML ではなく JSON がユーザーに返されることがあります。

回避策： 要求ヘッダに Accept: application/xml を追加します。

NSX Manager はスペース区切りのある DNS 検索文字列を受け付けない

NSX Manager はスペース区切りのある DNS 検索文字列を受け付けません。区切り文字としては、コンマのみを使用できます。たとえば、DHCP サーバが DNS 検索リストに eng.sample.com と sample.com を通知する場合、NSX Manager では eng.sample.com sample.com のようにコンマを使用して設定します。

回避策： コンマ区切りを使用します。NSX Manager が DNS 検索文字列として受け付ける区切り記号はコンマのみです。

Cross-vCenter NSX のデプロイで、保存されている複数のバージョンのがセカンダリ NSX Manager に複製される

ユニバーサル同期では、ユニバーサル設定の複数のコピーがセカンダリ NSX Manager に保存されます。保存されている設定リストには、同じ時刻または 1 秒違いで、NSX Manager 間の同期で作成された、同じ名前の複数のドラフトが含まれています。

回避策： API 呼び出しを実行して、重複しているドラフトを削除します。

DELETE : <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts/>

すべてのドラフトを表示して、削除するドラフトを見つけます。

GET: <https://<nsxmgr-ip>/api/4.0/firewall/config/drafts>

次のサンプル出力では、ドラフト 143 と 144 が同じ名前と同じ時刻に作成されているため、重複と判断できません。同様に、ドラフト 127 と 128 も同じ名前でも 1 秒違いで作成されているため、これらも重複と判断できません。

```
<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT
" timestamp="1438816120917">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT
" timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
```

```
<firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
timestamp="1438808882608">
  <description>Auto saved configuration</description>
  <preserve>false</preserve>
  <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
  <mode>autosaved</mode>
</firewallDraft>
<firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
timestamp="1438808881750">
  <description>Auto saved configuration</description>
  <preserve>false</preserve>
  <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
  <mode>autosaved</mode>
</firewallDraft>
</firewallDrafts>
```

Security Group の削除により Service Composer のファイアウォール ポリシーが同期しなくなると、ユーザー インターフェイスでファイアウォール ルールを修正できない

回避策： ユーザー インターフェイスで、無効なファイアウォール ルールを削除して、再度追加することができます。または、API で無効な Security Group を削除することでファイアウォール ルールを修正することもできます。その後、次の手順を実行して、ファイアウォール構成を同期します。[Service Composer] を選択します。[セキュリティ ポリシー] を選択し、ファイアウォール ルールに関連付けられている各セキュリティ ポリシーに対し[アクション] をクリックして[ファイアウォール構成の同期] を選択します。この問題を回避するには、Security Group を削除する前に、ファイアウォール ルールがその Security Group を参照しないようにルールを変更します。

ゲスト仮想マシンをパワーオンできない

ゲスト仮想マシンをパワーオンするときに、「All required agent virtual machines are not currently deployed」という内容のエラーが表示される場合があります。

回避策： 次の手順を実行してください。

1. vSphere Web Client で、[ホーム]>[管理]の順にクリックします。
2. [ソリューション]で、[vCenter Server の拡張機能]を選択します。
3. vSphere ESX Agent Manager > 管理 タブの順にクリックします。
4. [解決]をクリックします。

インストールとアップグレードに関する既知の問題

アップグレードの前に、このドキュメントの前半の「[アップグレードに関する注意事項](#)」を参照してください。

NSX 6.2 から 6.2.1 にアップデートした後で Cross vCenter のアップデート中に、NSX とプライマリ vCenter Server の接続が切断される

回避策： NSX のバンドルを消去し、vSphere Web Client を再起動します。

Windows：

1. C:\ProgramData\VMware\vCenterServer\cfg\vsphere-client\vc-packages\vsphere-client-serenity に移動します。
2. 「com.vmware.vShieldManagerxxxxxx」というフォルダを削除します（バックアップは不要です）。
3. vSphere Web Client を再起動します。

Unix：

1. /Etc/vmware/vsphere-client/vc-packages/vsphere-client-serenity に移動します。
2. 「com.vmware.vShieldManagerxxxxx」というフォルダを削除します（バックアップは不要です）。
3. vSphere Web Client を再起動します。

NSX Edge を 6.1.x から 6.2.x にアップデートすると、NSX Manager の vsm.log に「INVALID DHCP CONFIG」と表示される

インターフェイスに IPv6 サブネットを設定している場合、DHCP は空の共有サブネットを生成し、これを無効な操作として処理します。

回避策： DHCP サービスを無効にして、NSX Edge をアップデートします。アップデート後に、DHCP を有効にします。

ホストがオフラインであるにもかかわらず、ゲスト イントロスペクション のインストール ステータスが「成功しました」と表示される

オフラインのホスト 1 台を含むクラスタに ゲスト イントロスペクション をインストールした後、オフラインのホストのインストール ステータスが「成功しました」、ステータスが「不明」と表示されます。

回避策： なし。

Edge Services Gateway のアップグレードに失敗し、「Edge 仮想マシンの待機中にタイムアウトが発生しました」という内容のメッセージが表示される

NSX 管理インターフェイスに IPv6 アドレスを適用すると、NSX Manager はホスト名を使用するようになります。しかし、Edge 仮想マシンを NSX Manager に接続する vsfwd プロキシは FQDN を適切に処理できないため、「ERROR TaskFrameworkExecutor-6 AbstractEdgeApplianceManager:185 - Edge 仮想マシン {} の待機中にタイムアウトが発生しました。仮想マシンはブートおよび応答できませんでした。

com.vmware.vshield.edge.exception.VshieldEdgeException」という内容のエラーが返されます。

回避策： esxcfg-advcfg -q -s "10.20.233.160" /UserVars/RmqIpAddress のようなコマンドで設定を変更するか、インターフェイス管理設定で ipv6 アドレスを削除して IPv4 のみを使用します。

NSX Manager の証明書を置き換えた場合、NSX Manager の再起動が必要であり、場合によっては vSphere Web Client の再起動も必要になる

NSX Manager アプライアンスの証明書を置き換えた後は、常に NSX Manager アプライアンスを再起動する必要があります。状況によっては、証明書を置き換えた後、vSphere Web Client に [Networking and Security] タブが表示されないことがあります。この場合、次の回避策を実行します。

回避策： NSX Manager アプライアンスを再起動した後、vSphere Web Client を再起動します。

NSX Manager を再起動するには、次の手順を実行します。

1. NSX Manager の CLI にログインします。
2. 「en」と入力し、有効/特権モードに切り替えます。
3. 「no web-manager」と入力し、web-manager サービスを停止します。OK が表示されるまで待機し、サービスが停止したことを確認します。
4. 「web-manager」と入力し、NSX Manager を開始します。OK が表示されるまで待機し、サービスが再起動したことを確認します。
5. vSphere Web Client を再起動するには、vCenter Server 5.5 で https://{vcenter-ip}:5480 を開き、Web Client サーバを再起動します。
6. vCenter Server 6.0 アプライアンスで vCenter Server シェルに root ユーザーとしてログインし、次のコマンドを実行します。

```
shell.set --enabled True

shell

localhost:~ # cd /bin

localhost:~ # service-control --stop vsphere-client

localhost:~ # service-control --start vsphere-client
```

7. vCenter Server 6.0 で、次のコマンドを実行します。

```
cd C:\Program Files\VMware\vCenter Server\bin

service-control --stop vsphere-client

service-control --start vsphere-client
```

vCenter Server のアップグレード後に vCenter Server と NSX 間の接続が失われる場合がある

vCenter Server に組み込みの SSO を使用していて、vCenter Server 5.5 を vCenter Server 6.0 にアップグレードする場合、vCenter Server と NSX 間の接続が失われる場合があります。この状態は、vCenter Server 5.5 が root ユーザー名で NSX に登録されていた場合に発生します。NSX 6.2 では、root ユーザー名を使用した vCenter Server の登録は廃止されました。注：外部の SSO を使用している場合、変更は必要ありません。今までと同じユーザー名 (admin@mybusiness.mydomain など) をそのまま使用することができ、vCenter Server との接続は失われません。

回避策： root の代わりに ユーザー名 administrator@vsphere.local を使用して、vCenter Server を NSX に登録します。

パワーオフする前に、エージェント仮想マシン (SVA) のゲスト OS がシャットダウンする

ホストがメンテナンス モードになると、すべてのサービス アプライアンスが正常にシャットダウンされずに、パワーオフされます。これによりサードパーティ製のアプライアンスでエラーが発生する場合があります。

回避策： なし。

サービス デプロイ ビューを使用してデプロイしたサービス アプライアンスをパワーオンできない

回避策： 続行する前に、次を確認してください。

- 仮想マシンのデプロイが完了している。
- vCenter Server タスク ペインに表示されている仮想マシンに対し、クローン作成や再構成などのタスクが進行中になっている。
- 仮想マシンの vCenter Server のイベント ペインで、デプロイの開始後に次のイベントが表示される。

エージェント仮想マシン <仮想マシン名> がプロビジョニングされました。
エージェントを使用可能とマークして、エージェント ワークフローを進めます。

このような場合は、サービス仮想マシンを削除します。サービス デプロイ ユーザー インターフェイスで、デプロイが [失敗] と表示されます。赤いアイコンをクリックすると、ホストで利用できないエージェント仮想マシンに関するアラームが表示されます。アラームを解決すると、仮想マシンは再デプロイされ、パワーオン状態になります。

環境内のすべてのクラスタがネットワーク仮想化に対応していない場合、[インストール手順] 画面の [ホストの準備] タブに分散ファイアウォールのアップグレード メッセージが表示されない

ネットワーク仮想化を利用できるようにクラスタを準備すると、クラスタで分散ファイアウォールが有効になります。環境内のすべてのクラスタがネットワーク仮想化に対応していない場合、[ホストの準備] タブに分散ファイアウォールのアップグレード メッセージが表示されません。

回避策： 次の REST 呼び出しを使用して、分散ファイアウォールをアップグレードします。

```
PUT https://<nsxmgr-ip>/api/4.0/firewall/globalroot-0/state
```

アップグレード後、サービスの追加や削除などのサービス グループに加えた変更がファイアウォール テーブルに反映されない

ユーザーが作成したサービス グループが、アップグレード時に Edge ファイアウォール テーブルに展開されます。つまり、ファイアウォール テーブルの [サービス] 列にサービス グループ内のすべてのサービスが表示されます。アップグレード後に、サービスの追加や削除などの変更をサービス グループへ加えても、ファイアウォール テーブルに反映されません。

回避策： 別の名前で新しいサービス グループを作成し、ファイアウォール ルールで利用します。

[インストール手順] 画面の [サービス デプロイ] タブでデプロイされたサービス仮想マシンをパワーオンできない

回避策： 次の手順を実行してください。

1. クラスタの ESX Agents リソース プールからサービス仮想マシンを手動で削除します。
2. [Networking and Security] > [インストール手順] の順にクリックします。
3. [サービス デプロイ] タブをクリックします。
4. 該当するサービスを選択し、[解決] アイコンをクリックします。
サービス仮想マシンが再度デプロイされます。

vSphere Distributed Switch の MTU が更新されない

クラスタの準備時に vSphere Distributed Switch の MTU よりも小さい MTU 値を指定した場合、vSphere Distributed Switch はこの値に更新されません。これは、フレーム サイズがより大きい既存のトラフィックが誤ってドロップされないようにするためです。

回避策： クラスタの準備時に指定する MTU が vSphere Distributed Switch の現在の MTU 以上であることを確認します。VXLAN に必要な最小 MTU は 1550 です。

アップグレード後に SSO を再設定できない

NSX Manager 用に設定された SSO サーバが vCenter Server 上のネイティブなものである場合、vCenter Server をバージョン 6.0 へアップグレードし、NSX Manager をバージョン 6.x へアップグレードした後は、NSX Manager で SSO を再設定できません。

回避策： なし。

vCloud Networking and Security 5.5.3 を NSX for vSphere 6.0.5 以降にアップグレードした後、DSA-1024 のキーサイズを持つ SSL 証明書を使用すると、NSX Manager が開始されない

DSA-1024 のキーサイズを持つ SSL 証明書は、NSX for vSphere 6.0.5 以降ではサポートされないため、アップグレードは失敗します。

回避策： アップグレードの前に、サポートされているキーサイズを持つ新しい SSL 証明書をインポートします。

SSL VPN がアップグレード通知をリモート クライアントに送信しない

SSL VPN ゲートウェイはアップグレード通知をユーザーに送信しません。管理者は、SSL VPN ゲートウェイ (サーバ) が更新されたことと、リモート ユーザーが自分のクライアントを更新しなければならないことを、リモート ユーザーに手動で通知する必要があります。

回避策： ユーザーは旧バージョンのクライアントをアンインストールして、最新バージョンを手動でインストールする必要があります。

NSX をバージョン 6.0 から 6.0.x または 6.1 にアップデートした後、NSX Edge がユーザー インターフェイスにリスト表示されない

NSX 6.0 から NSX 6.0.x または 6.1 にアップデートした場合、vSphere Web Client プラグインが正しくアップデートされていない可能性があります。この場合、NSX Edge が見つからないなど、ユーザー インターフェイスの表示に問題が発生することがあります。

NSX 6.0.1 以降のバージョンからアップデートする場合、この問題は発生しません。

回避策： 次の手順を実行してください。

1. vCenter Managed Object Browser で、[content] をクリックします。
2. [VALUE] 列で、[ExtensionManager] をクリックします。
3. extensionList プロパティ値 (com.vmware.vShieldManager など) を検索し、その文字列をコピーします。
4. [メソッド] 領域で、[UnregisterExtension] をクリックします。
5. [VALUE] フィールドに、手順 3 でコピーした文字列を貼り付けます。
6. [Invoke Method] をクリックします。

これにより最新のプラグイン パッケージがデプロイされます。

L2 VPN が Edge で有効な場合、NSX Edge のアップグレードに失敗する

L2 VPN 構成の場合、5.x または 6.0.x から 6.1 へアップデートはサポートされていません。そのため、Edge で L2 VPN が設定されている場合はアップグレードに失敗します。

回避策： NSX Edge をアップグレードする前に L2 VPN 構成を削除します。アップグレード後、L2 VPN を再設定します。

NSX for vSphere のアップグレード プロセスで vCenter Server を再起動すると、クラスタのステータスが誤って表示される

NSX を展開した複数のクラスタを含む環境で、アップグレード中にホストの準備を行っている場合、1 つ以上のクラスタに NSX を展開した後 vCenter Server を再起動すると、他のクラスタの [クラスタのステータス] に [更新] リンクが表示されず、「準備ができていません」と表示されることがあります。vCenter Server 上のホストにも「再起動が必要です」と表示されます。

回避策： ホストの準備中には vCenter Server を再起動しないでください。

アップデート中にサードパーティ製アンチウイルスによる保護が一時的に失われる

NSX 6.0.x から NSX 6.1.x または 6.2.0 にアップデートするときに、仮想マシンのサードパーティ製アンチウイルスによる保護が一時的に失われることがあります。この問題によって、NSX 6.1.x から NSX 6.2 へのアップデートに影響が及ぶことはありません。

回避策： なし。

分散ファイアウォールの設定時にホストのエラーメッセージが表示される

分散ファイアウォールの設定時にホスト関連のエラー メッセージが表示された場合、ファブリック機能 com.vmware.vshield.nsxmgr.messagingInfra のステータスを確認します。ステータスが赤になっている場合、次の回避策を実行します。

回避策： 次の REST API 呼び出しを使用して、NSX Manager と個々のホストまたはクラスタ内のすべてのホスト間の通信をリセットします。

POST https://<NSX Manager IP>/api/2.0/nwfabric/configure?action=synchronize

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{HOST/CLUSTER MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

送信元/宛先の無効化オプションが有効になっているファイアウォール ルールをコピー アンド ペーストすると、コピーしたルールでは無効オプションが無効になる

送信元/宛先の無効化オプションが有効になっているファイアウォール ルールをコピー アンド ペーストすると、ペースト操作の後に新しいファイアウォール ルールが作成されますが、送信元/宛先の無効化オプションが無効になります。

回避策： なし。

NSX 6.2 へのアップデート後、NSX Manager ログに「**WARN messagingTaskExecutor-7**」というメッセージが記録される

NSX 6.1.x から NSX 6.2 へアップデートした後、NSX Manager ログに次のようなメッセージが大量に記録されます。「WARN messagingTaskExecutor-7 ControllerInfoHandler:48 - host is unknown: host-15 return empty list.」これにより、運用に影響が及ぶことはありません。

回避策： なし。

VMware vCloud Network and Security (vCNS) からのアップグレード後、アップグレードされたグループ オブジェクトに、新しいグループ オブジェクトを追加できない

vCNS 5.x では、GlobalRoot (NSX 全体のスコープ) より下の階層でのグループ オブジェクト作成がサポートされていました。たとえば、vCNS 5.x では、データセンター (DC) またはポート グループ (PG) レベルでのグループ オブジェクトの作成が可能でした。これに対して NSX 6.x のユーザー インターフェイスでは、グループ オブジェクトは GlobalRoot の直下に作成されます。アップグレード前の vCNS 環境でさらに下位の階層 (DC や PG) で作成された既存のグループ オブジェクトに、新たに作成されたグループ オブジェクトを追加することはできません。

回避策： [VMware ナレッジベースの記事 KB2117821](#) を参照してください。

vCloud Networking and Security 5.5.4 から NSX 6.2.0 へとアップグレードした後、[ホストの準備] タブのファイアウォールが無効のままになる

vCloud Networking and Security 5.5.x から NSX 6.2.0 へのアップグレード、およびすべてのクラスタのアップグレード後、[ホストの準備] タブのファイアウォールが無効のままになります。また、ファイアウォールをアップグレードするオプションがユーザー インターフェイスに表示されません。この問題は、NSX が展開された準備されたクラスタの一部で含まれないホストがデータセンターに存在するときのみ発生します。これはクラスタ外の、ホストには VIB がインストールされないためです。

回避策： この問題を解決するには、NSX 6.2 が展開されたクラスタにホストを移動します。

アップグレード中、L2 および L3 ファイアウォール ルールがホストに発行されない

分散ファイアウォール構成の変更を発行した後も、ステータスはユーザー インターフェイスと API の両方でいつまでも **処理中** のままになり、L2 または L3 ルールのログが vsfwd.log ファイルに書き込まれません。

回避策： NSX のアップグレード中、分散ファイアウォールへの変更は発行しないでください。[処理中] の状態を解除してこの問題を解決するには、NSX Manager 仮想アプライアンスを再起動します。

IP アドレスの検出を有効または無効にする NSX REST API 呼び出しが、機能していない可能性があるクラスタの展開が完了していない場合は、IP アドレス検出を有効または無効にする NSX REST API 呼び出し (<https://<nsxmgr-ip>/api/2.0/xvs/networks/universalwire-5/features>) は機能しません。

回避策： この API 呼び出しを実行する前に、ホスト クラスタの準備が完了していることを確認してください。

NSX 6.0.7 SSL VPN クライアントが NSX 6.2 SSL VPN ゲートウェイに接続できない

NSX 6.2 SSL VPN ゲートウェイでは、SSLv2 および SSLv3 プロトコルが無効になっています。つまり、SSL VPN ゲートウェイでは TLS プロトコルしか受け入れられません。SSL VPN 6.2 クライアントは、接続の確立時にデフォルトで TLS プロトコルを使用するようにアップグレードされています。NSX 6.0.7 では、SSL VPN クライアントは古いバージョンの OpenSSL ライブラリと SSLv3 プロトコルを使用して、接続を確立します。NSX 6.0.x クライアントが NSX 6.2 ゲートウェイへ接続しようとすると、SSL ハンドシェイク レベルで接続の確立に失敗します。

回避策： NSX 6.2 にアップグレードした後、お使いの SSL VPN クライアントを NSX 6.2 にアップグレードします。アップグレードの手順については、『[NSX のアップグレード](#)』ドキュメントを参照してください。

ESXi アップグレード時の PSOD

NSX を使用する vSphere 5.5U2 ホストを vSphere 6.0 にアップグレードする際、一部の ESXi ホストでパープル スクリーン（別名 PSOD）が表示され、アップグレードが停止する場合があります。

回避策： この問題が発生した場合、[ナレッジベースの記事 KB2137826](#) を参照してください。

新規またはアップグレードした分散論理ルーター用にセグメント ID プールを作成する必要がある

NSX 6.2 では、分散論理ルーターを 6.2 にアップグレードする際、または新しい 6.2 の分散論理ルーターを作成する際に、使用可能なセグメント ID を含むセグメント ID プールが必要です。これは、導入環境で NSX 論理スイッチを使用する予定がない場合でも必要となります。

回避策： NSX 分散論理ルーターのアップグレードまたはインストールを行う際の前提条件ですので、NSX 導入環境に論理セグメント ID プールがない場合は、プールを作成します。

VXLAN ゲートウェイの構成エラー

[Networking and Security] > [インストール手順] > [ホストの準備] > [VXLAN の構成] で、固定 IP アドレスプールを使用して VXLAN を構成し、ゲートウェイが適切に構成されていない、またはゲートウェイにアクセスできないなどの理由から VTEP 上に IP アドレス プール ゲートウェイ IP を構成できない場合、ホスト クラスタの VXLAN 構成ステータスがエラー（赤）状態になります。

エラー メッセージは「**ホスト上で VXLAN ゲートウェイを設定できません**」、エラー ステータスは VXLAN_GATEWAY_SETUP_FAILURE です。REST API 呼び出し GET `https://<nsxmgr-ip>/api/2.0/nwfabric/status?resource=<cluster-moid>` では、VXLAN のステータスが次のように表示されます。

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.nsxmgr.vxlan</featureId>
  <featureVersion>5.5</featureVersion>
  <updateAvailable>false</updateAvailable>
  <status>RED</status>
  <message>VXLAN Gateway cannot be set on host</message>
  <installed>true</installed>
  <enabled>true</enabled>
  <errorStatus>VXLAN_GATEWAY_SETUP_FAILURE</errorStatus>
</nwFabricFeatureStatus>
```

回避策： エラーを修正するには、次のいずれかの方法を使用します。

- オプション 1：ホスト クラスタの VXLAN 設定を削除します。次に、IP アドレス プール内で使用されているゲートウェイを適切に設定し、確実にアクセスできるようにした後、ホスト クラスタの VXLAN を再設定します。
- オプション 2：次の手順を実行してください。

1. IP アドレス プール内で使用されているゲートウェイを適切に設定し、ゲートウェイに確実にアクセスできるようにします。
2. ホストをメンテナンス モードにして、ホスト上でアクティブになっている仮想マシン トラフィックがないことを確認します。
3. VXLAN VTEP をホストから削除します。
4. ホストのメンテナンス モードを終了します。ホストのメンテナンス モードを終了すると、NSX Manager で VXLAN VTEP の作成プロセスがトリガされます。NSX Manager は、ホスト上で必要な VTEP の再作成を試みます。

Cross vCenter を環境で導入する際、ユニバーサル構成のセクションがローカル構成のセクションの下位に（従属的に）置かれる場合があります

セカンダリ NSX Manager をいったんスタンドアロン（移行）状態に移した後、再びセカンダリの状態に戻すと、プライマリ NSX Manager からの継承によってレプリケートされたユニバーサル設定のセクションよりも、一時的にスタンドアロンの状態であった間に加えられたローカル設定のすべての変更が、上位にリストされることがあります。これが原因で、「セカンダリ NSX Manager ではユニバーサル セクションを他のすべてのセクションより上位にする必要があります」というエラー状態が発生します。

回避策： ユーザー インターフェイスからオプションを使用して、ローカル セクションがユニバーサル セクションよりも下位になるように、各セクションを上下に移動します。

アップデートの後、ファイアウォール ルールとネットワーク イントロスペクション サービスが NSX Manager と同期しなくなることがある

NSX 6.0 から NSX 6.1 または 6.2 へアップデートした後、NSX ファイアウォール構成で、「同期が失敗しました/同期していません」というエラー メッセージが表示されます。[サービスの強制同期] を使用します。[ファイアウォール] アクションを使用しても問題は解決しません。

回避策： NSX 6.1.x および NSX 6.2 の場合、サービス プロファイルにバインドできるのは、Security Group または dvPortgroup のいずれか一方のみです。両方をバインドすることはできません。この問題を解決するには、サービス プロファイルを修正する必要があります。

「esxcli software vib list | grep esx」 コマンドの出力に、esx-dvfilter-switch-security VIB は今後表示されない

NSX 6.2 以降では、esx-dvfilter-switch-security モジュールが、esx-vxlan VIB の中に組み込まれています。6.2 でインストールされる NSX VIB は、esx-vsip と esx-vxlan のみです。NSX を 6.2 にアップグレードする間に、古い esx-dvfilter-switch-security VIB は ESXi ホストから削除されます。

回避策： なし。

アップグレード後、明示的フェイルオーバーのチーミングを設定した分散論理ルーターがパケットを正しく転送できないことがある

ホストで ESXi 5.5 が実行されている場合、明示的なフェイルオーバーである NSX 6.2 のチーミング ポリシーは、分散論理ルーター上での複数のアクティブ アップリンクをサポートしません。

回避策： アクティブ アップリンクを 1 つのみにして、その他のアップリンクがスタンバイ モードになるように明示的フェイルオーバーのチーミング ポリシーを変更します。

ホスト クラスタから NSX をアンインストールすると、エラーが発生することがある

[インストール手順]: [ホストの準備] タブでアンインストール アクションを実行すると、エラーになり、eam.issue.OrphanedAgency メッセージがホストの EAM ログに出力されることがあります。解決アクションを使用して、ホストを再起動した後、NSX VIB を正しくアンインストールしてもエラー状態は解決しません。

回避策： 実態のないエージェンシーを vSphere ESX Agent Manager から削除します（[管理] > [vCenter Server の拡張機能] > [vSphere ESX Agent Manager]）。

NSX 6.2 では SSLv2 と SSLv3 が廃止される

NSX 6.2 以降、SSL VPN ゲートウェイで許容されるのは、TLS プロトコルだけになります。NSX のアップグレード後、ユーザーが新規で作成する NSX 6.2 クライアントでは、接続を確立する間、自動的に TLS プロトコルが使用されます。NSX 6.0.x クライアントが NSX 6.2 ゲートウェイへ接続しようすると、SSL ハンドシェイクのステップで接続の確立に失敗します。

回避策： NSX 6.2 へのアップグレード後は、古い SSL VPN クライアントをアンインストールし、NSX 6.2 バージョンの SSL VPN クライアントをインストールしてください。

NSX for vSphere 6.2 でのバックアップとリストアの後、vSphere Web Client に [Networking and Security] タブが表示されない

NSX for vSphere 6.2 にアップグレードした後にバックアップとリストアの操作を実行すると、vSphere Web Client で [Networking and Security] タブが表示されません。

回避策： NSX Manager バックアップがリストアされると、NSX Manager の仮想アプライアンス管理ポータルからログアウトされます。数分間待機してから、vSphere Web Client にログインしてください。

NSX 6.2 へのアップグレード後、NSX Manager に割り当てられた物理メモリが 100% を超える

NSX 6.2 以降、NSX Manager では 16 GB の予約メモリが必要になります。以前のシステム要件では 12 GB でした。

回避策： NSX Manager 仮想アプライアンスの予約メモリを 16 GB に増やします。

IP アドレスの接続が確立されていない場合でも Data Security サービスのステータスが稼動中として表示される

Data Security アプライアンスが IP アドレスを DHCP から受け取っていないか、間違ったポート グループに接続されている可能性があります。

回避策： Data Security アプライアンスが DHCP/IP アドレス プールから IP アドレスを取得していて、管理ネットワークからアクセス可能であることを確認します。Data Security アプライアンスへの ping が NSX/ESX から正常に実行されるかチェックします。

NSX Manager に関する既知の問題

Firefox ブラウザの GUI 言語が日本語の場合、セカンダリ NSX Manager を追加できない

日本語、ドイツ語、韓国語、フランス語の Firefox ブラウザでセカンダリ NSX Manager を追加すると、サムプリントのダイアログが表示されません。このため、これらのロケールを使用しているユーザーは、セカンダリ NSX Manager を構成できません。

回避策： Internet Explorer を使用するか、ブラウザのロケールを英語に変更します。

ホスト名が 64 文字を超えている場合、NSX 管理サービスが起動しない

OpenSSL ライブラリで証明書を生成するには、ホスト名を 64 文字以下にする必要があります。

Web Client の画面で NSX Manager のリストが表示されるのが遅い

複数の NSX Manager を使用している vSphere 6.0 環境において、ログイン ユーザーが大規模な Active Directory グループで認証されている場合、vSphere Web Client の NSX Manager リストの表示に最大 2 分ほどかかる可能性があります。NSX Manager のリストを表示しようとすると、データ サービスのタイムアウト エラーが表示されることがあります。回避策はありません。リストがロードされるまで待つか、再ログインして NSX Manager リストを表示する必要があります。

NSX Controller が切断されていると表示される

NSX Manager ログに次のようなメッセージが表示され、コントローラが切断されたとレポートされます。

「ERROR http-nio-127.0.0.1-7441-exec-16908 BaseRestController:339 - Exception : 「I/O error: Read timed out; nested exception is java.net.SocketTimeoutException: Read timed out」これは、ネットワーク上のどこかのファイアウォールで TCP/IP FIN メッセージがアイドル タイムアウトでブロックされると発生します。この状況が発生すると、NSX Manager への接続数が増加します。

[ホストの準備] 画面をロードできない

リンク モードで vCenter Server を実行する際、各 vCenter Server は、同じバージョンの NSX Manager に接続する必要があります。NSX のバージョンが異なる場合、vSphere Web Client は、上位バージョンの NSX Manager としか通信できません。「NSX Manager との通信を確立できませんでした。管理者に問い合わせてください」という内容のエラーが、[ホストの準備] タブに表示されます。

回避策： すべての NSX Manager を同じバージョンにアップグレードします。

NSX Manager のユーザー インターフェイスで以前のバックアップが表示されない

また、バックアップ操作の実行後、NSX Manager のユーザー インターフェイスでバックアップの成功を示すメッセージが表示されません。ターゲット フォルダに保存されているバックアップ ファイルの数が多い場合、これらの問題のいずれかが発生する可能性があります。同じページでリストを表示する前に、各バックアップ ファイルをチェックして互換性を確認する必要があります。そのファイル リスト プロセスによって、ページがタイムアウトする場合があります。

回避策： ストレージ サーバを定期的に整理してバックアップ フォルダに保存されているファイルの数を減らすか、古いバックアップを別のフォルダに移動します。バックアップが成功したか確認するには、NSX Manager ログ ファイルで次のようなメッセージを探します。2015-07-01 22:10:55.869 GMT INFO http-nio-443-exec-250 VsmServiceBackupRestoreExecutor:236 - Run backup script - Start 2015-07-01 22:14:35.992 GMT INFO http-nio-443-exec-250 VsmServiceBackupRestoreExecutor:278 - Run backup script - Completed

Service Manager の 1 つがダウンしているときにポリシーに変更が加えられると、Service Composer が同期されなくなる

この問題は、複数のサービスおよび Service Manager が登録されたインスタンスと、これらのサービスを参照するように作成されたポリシーに関係します。Service Manager の 1 つがダウンしているときに、該当するポリシーに Service Composer で変更を加えると、ダウンしている Service Manager へのコールバックに失敗するため、変更は失敗します。したがって、Service Composer は同期されません。

回避策： Service Manager が応答していることを確認して、Service Composer から強制同期を発行します。

[Networking and Security] タブが vSphere Web Client に表示されない

vSphere 6.0 にアップグレードした後、vSphere Web Client に root ユーザーとしてログインすると [Networking and Security] タブが表示されません。

回避策： administrator@vsphere.local としてログインするか、アップグレード前に vCenter Server に存在し、NSX Manager でロールが定義されたその他の vCenter Server ユーザーとしてログインします。

NSX Manager のバックアップをリストアした後、REST 呼び出しでファブリック機能

com.vmware.vshield.nsxmgr.messagingInfra のステータスが赤で表示される

NSX Manager のバックアップをリストアし、REST API 呼び出しを使用してファブリック機能

com.vmware.vshield.nsxmgr.messagingInfra のステータスをチェックすると、ステータスは緑ではなく赤として表示されます。

回避策： 次の REST API 呼び出しを使用して、NSX Manager と個々のホストまたはクラスタ内のすべてのホスト間の通信をリセットします。

POST https://<NSX Manager IP>/api/2.0/nwfabric/configure?action=synchronize

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{HOST/CLUSTER MOID}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```


ゲスト イン트로スペクション およびサードパーティ製セキュリティ ソリューションで保護されたクラスタでは、ホストを削除して再追加できない

ゲスト イン트로スペクションおよびサードパーティ製セキュリティ ソリューションで保護されたクラスタからホストを削除する場合、vCenter Server からホストを切断して削除すると、同じホストを同じクラスタに再追加しようとしたときに問題が生じることがあります。

回避策： 保護されたクラスタからホストを削除するには、まず、ホストをメンテナンス モードにします。次に、保護されていないクラスタか、すべてのクラスタの外にホストを移動してから、ホストを切断して削除します。

NSX Manager の vMotion に「仮想イーサネット カード ネットワーク アダプタ 1 はサポートされていません」というエラー メッセージが表示される

このエラーは無視してかまいません。vMotion 後、ネットワークは適切に動作します。

バックアップ元の NSX Manager のホスト名が、リストア先 NSX Manager の Syslog に表示される

1 番目の NSX Manager のホスト名が A で、この NSX Manager のバックアップを作成したとします。2 番目の NSX Manager は、バックアップおよびリストアのドキュメントに従って、1 番目の NSX Manager と同じ IP アドレスを使用してインストールおよび設定されていますが、ホスト名は B となっています。リストアされた NSX Manager では、リストア直後はホスト名が A と表示され、再起動後に正しいホスト名 B と表示されます。

回避策： 2 番目の NSX Manager のホスト名とバックアップした NSX Manager のホスト名が同じ名前になるように設定する必要があります。

NSX Manager 仮想アプライアンスの [サマリ] 画面に DNS 名が表示されない

NSX Manager 仮想アプライアンスにログインすると、[サマリ] 画面に DNS 名のフィールドが表示されます。このフィールドは、仮に NSX Manager アプライアンスに DNS 名が定義されている場合でも、空白になっています。

回避策： NSX Manager のホスト名、および検索ドメインは、[Manage] > [Network] ページで確認できます。

NSX コマンドライン インターフェイスを使用してパスワードを変更した後、NSX Manager ユーザー インターフェイス上でユーザーを自動的にログアウトしない

NSX Manager にログインしている間に、コマンドライン インターフェイスを使用してパスワードを変更しても、旧パスワードを使用して NSX Manager ユーザー インターフェイスにログインしたままの状態が維持されます。通常、セッションが非アクティブ状態のままタイムアウトになると、NSX Manager はユーザーを自動的にログアウトします。

回避策： NSX Manager ユーザー インターフェイスからログアウトし、新しいパスワードを使用して再度ログインします。

スタンドアロンの NSX Manager で、ユニバーサル ファイアウォール構成のインポートが誤って許可される

通常、スタンドアロン ロールで動作している NSX Manager では、ローカル ファイアウォール ルールのインポートのみが許可されます。NSX 6.2 から、NSX Manager はスタンドアロン ロール（単一の vCenter Server のネットワークを管理するロール）または Cross-vCenter モードで実行できるようになったため、スタンドアロン ロールで実行されている NSX Manager 環境にユニバーサル ファイアウォール ルールを誤ってインポートすることが可能になります。ユニバーサル ファイアウォール ルールがいったんインポートされると、REST API または vSphere Web Client のいずれを使用しても、削除できません。NSX Manager がスタンドアロン ロールで実行されている場合、ユニバーサル セクションはローカル セクションと同様に処理されます。

回避策： NSX Manager をスタンドアロン ロールで実行しているときは、ユニバーサル ルールが含まれるファイアウォール構成のインポートは実行しないでください。ユニバーサル ファイアウォール ルールをスタンドアロンの NSX Manager にインポートしてしまった場合は、ユニバーサル ルールが含まれていない既存のファイアウォール構成ファイルをインポートし、ファイアウォール テーブルにロードすることで新しい構成ファイルを発行します。

次の手順を実行してください。

1. vSphere Web Client にログインします。
2. [Networking and Security] をクリックし、[ファイアウォール] をクリックします。
3. [ファイアウォール] タブをクリックします。
4. [保存した設定] タブをクリックします。
5. [構成のインポート] アイコンをクリックします。
6. [参照] をクリックして、インポートする設定が含まれているファイルを選択します。

ルールは、ルール名に基づいてインポートされます。インポート中、ファイアウォールは、ルールで参照されている各オブジェクトが環境に存在することを確認します。オブジェクトが見つからない場合、ルールは無効としてマークされます。ルールが動的 Security Group を参照している場合、インポート中にその動的 Security Group が NSX Manager で作成されます。

7. ノードをセカンダリ ノードとして追加し直します。NSX Manager 間で同期を行うと、ユニバーサル セクションが自動的に同期され、必要なクリーンアップが適切に実行されます。

構成ファイルが正常に発行されると、ルールがホストにプッシュ ダウンされ、データパスに反映されます。システムは正常に動作します。

ネットワーク ホスト名を編集できない

NSX Manager 仮想アプライアンスにログインし、[Manage Appliance Settings] に移動した後、[SETTING] > [Network] の順にクリックしてネットワーク ホスト名を編集すると、無効なドメイン名リスト エラーが発生することがあります。これは、[Search Domains] フィールドで指定したドメイン名が、コンマではなく空白文字で区切られている場合に発生するエラーです。NSX Manager ではコンマ区切りのドメイン名のみが使用できます。
回避策： 次の手順を実行してください。

1. NSX Manager 仮想アプライアンスにログインします。
2. [Appliance Management] で、[Manage Appliance Settings] をクリックします。
3. [SETTINGS] パネルで、[Network] をクリックします。
4. [DNS Servers] の横にある [Edit] をクリックします。
5. [ドメインの検索] フィールドで空白文字をすべてコンマに置き換えます。
6. [OK] をクリックして変更内容を保存します。

バックアップから NSX Manager を正しくリストアしても、False システム イベントが生成される
NSX Manager をバックアップから正常にリストアした後、vSphere Web Client で [Networking and Security] > [NSX Managers] > [監視] > [システム イベント] の順にクリックすると、次のシステム イベントが表示されます。

- バックアップからの NSX Manager のリストアに失敗しました(重要度 = 重大)。
- NSX Manager のリストアが正常に完了しました(重要度 = 情報)。

回避策： 最終的なシステム イベント メッセージに問題がなければ、生成されたイベント メッセージは無視してもかまいません。

データセンターに名前空間を追加するための NSX REST API 呼び出しの動作の変更

NSX 6.2 では、POST `https://<nsxmgr-ip>/api/2.0/namespace/datacenter/` REST API を呼び出すと、絶対パスで指定された URL が返されるようになりました。

例：`http://198.51.100.3/api/2.0/namespace/api/2.0/namespace/datacenter/datacenter-1628/2`以前の NSX リリースの API 呼び出しでは、相対パスの URL が返されていました。

例：`/api/2.0/namespace/datacenter/datacenter-1628/2`

回避策： なし。

論理ネットワークと NSX Edge に関する既知の問題

Arista EOS-4.12.7.1 ベースの一部の論理スイッチで、マルチキャスト トラフィックがドロップする NSX 環境が、Arista EOS-4.12 スイッチを含む物理ネットワークを使用している場合、マルチキャスト トラフィックがドロップする可能性があります。この問題は、2 台の ESX の VTEP が、該当する Arista スイッチを物理的な基盤として使用し、VXLAN ポート 8472 を使用して通信している場合に発生します。メジャー バージョンまたはメンテナンス バージョン EOS 4.12 のすべての Arista 7150 製品は、この問題の影響を受けます。

回避策： Arista スイッチを使用するユーザーがこの問題を回避する方法は、2 つあります。

1. Arista スイッチを EOS 4.13.0 以降にアップグレードします。
2. NSX REST API を使用して異なる UDP ポートを使用するように NSX を構成します。各 VXLAN 設定でポート 4789 を使用することをお勧めします。

NSX ロード バランサへの接続が遅くなると、複数の仮想 IP アドレスがある場合、一貫性のある接続が提供されない

ロード バランサが、送信元の IP ハッシュ値ベースでロード バランシングするように設定されている場合、接続中のクライアント セッションは、同じバックエンド サーバに接続されます。複数の仮想 IP アドレス (VIP) が同じサーバ プールに含まれている場合、ロード バランサは接続されたクライアントに対し、複数の VIP にわたって一貫性のある形で接続を提供する必要があります。つまり、1 台のバックエンド サーバから複数の仮想 IP アドレスが提供されており、あるクライアントが 1 つの仮想 IP アドレスに接続している場合、このクライアントが他の仮想 IP アドレスに接続する際は、同じバックエンド サーバから提供される仮想 IP アドレスに接続することを保証する必要があります。既知の問題によって、NSX のロード バランサは、このような複数の仮想 IP アドレスに一貫した接続方法を提供できません。

IP アドレスをインターフェイスに割り当てると、RIB や FIB への接続が遅くなる

IP アドレスをインターフェイスに割り当てようとすると、通常、そのインターフェイスの情報が即座にアップデートされます。しかし、ポーリング間隔が長くなると、IP アドレスの割り当てが遅くなる可能性があります。

一番大きい数字の IP アドレスを持つ OSPF エリア境界ルーター (ABR) をシャットダウンすると、コンバージェンスが遅くなる

一番大きい数字の IP アドレスを持つ NSX の OSPF ABR をシャットダウンまたはリブートすると、コンバージェンスに時間がかかります。それ以外の ABR をシャットダウンまたはリブートした場合、トラフィックは素早く別のパスに収束します。しかし、一番大きい数字の IP アドレスを持つ ABR をシャットダウンまたはリブートすると、再コンバージェンスに数分かかる場合があります。OSPF プロセスを手動でクリアして、コンバージェンスの時間を短縮できます。

DHCP Edge 上の静的バインドの合計数が 2048 以上にならない

2048 を超えると、「バインディングとプールの合計数は 2048 以下にする必要があります」というエラー メッセージが表示されます。

NSX Edge 経由で TCP ベースのアプリケーションを接続すると、タイムアウトになる場合がある

TCP で確立された接続における非アクティブ状態のタイムアウトは、デフォルトで 3600 秒です。NSX Edge は、非アクティブ タイムアウトを超過したアイドル状態の接続を削除し、接続をドロップします。

回避策：

1. 非アクティブな時間が比較的長いアプリケーションの場合は、ホストの TCP キープアライブを有効にし、keep_alive_interval を 3600 秒未満に設定します。
2. 次の NSX REST API を使用して、Edge の TCP 非アクティブ タイムアウトを 2 時間以上に増やします。たとえば、非アクティブ タイムアウトを 9000 秒に増やします。NSX API URL :

```
/api/4.0/edges/{edgeId}/systemcontrol/config PUT Method <systemControl>  
<property>sysctl.net.netfilter.nf_conntrack_tcp_timeout_established=9000</property> </systemControl>
```

ユーザー インターフェイスに Edge 管理プレーン モード (VIX/MSGBUS) が表示されず、VIX から MSGBUS に変更するオプションが提供されない

Edge アプライアンスが VIX モードである場合、分散ファイアウォールに含めることはできません。また、MSGBUS モードと比べて、コマンドの実行に時間がかかります。

回避策： Edge がデプロイされているクラスタが NSX に対応していて、「NSX Manager とファイアウォール エージェント間」が「接続中」であることを確認し、Edge を再デプロイします。

BGP ネイバー フィルタを「任意、送信、拒否」に設定している場合、分散論理ルーターがデフォルト ルートの誤ったネクスト ホップを通知する

NSX 分散論理ルーター (DLR) で [デフォルトの広告] が有効になっている場合、DLR で BGP ネイバー フィルタを「任意、送信、拒否」に設定すると、DLR は誤ったデフォルト ルートのネクスト ホップ アドレスを通知します。このエラーは、次の属性を使用して BGP ネイバー フィルタが追加されている場合にのみ発生します。

- 方向：送信
- 操作：拒否
- ネットワーク：任意

回避策： なし。

NSX Edge でルーティング プロトコルを無効にすると、データ トラフィックが一時的に失われる場合がある

NSX Edge でルーティング プロトコルを無効にしてもルート取り消し要求はピアに送信されません。そのため、ホールド ダウン タイマー/デッド インターバルの期限が切れるまでトラフィックがブラックホール状態になります。

回避策： なし。

分散論理ルーター OSPF が無効になっている場合でも、分散論理ルーター LIF のルートがアップストリーム Edge Services Gateway によってアドバタイズされる

分散論理ルーター OSPF が無効になっている場合でも、アップストリーム Edge Services Gateway は、分散論理ルーター接続インターフェイスから学習した OSPF 外部 LSA を引き続きアドバタイズします。

回避策： OSPF プロトコルを無効にする前に、OSPF への接続ルートの再配分を手動で無効にし、これを発行します。これにより、ルートは適切に廃止されます。

ESG Syslog がリモート サーバへ送信されない。「ホスト名を解決できない」というメッセージが表示されるが、DNS リゾルバは動作している

Edge をデプロイした直後、Syslog は、構成済みのどの Syslog サーバに対してもホスト名を解決できません。

回避策： リモートの Syslog サーバを IP アドレスを使用して設定するか、ユーザー インターフェイスから Edge の強制同期を行います。この問題は 6.2 で初めて確認されました。

REST Edge API で分散論理ルーターの DNS クライアントの設定 変更しても完全に適用されない

回避策： REST API を使用して DNS フォワーダ (リゾルバ) を設定する場合は、次の手順を実行します。

1. DNS フォワーダの設定と一致するように、DNS クライアントの XML サーバ設定を指定します。

2. DNS フォワーダを有効にして、フォワーダ設定が、XML 設定で指定された DNS クライアント サーバ設定と同じであることを確認します。

ECMP を有効にした場合、スタティック ルート内の無効なネクスト ホップに関する検証メッセージやエラー メッセージが表示されない

ECMP を有効にしてスタティック ルートの追加を試みると、ルーティング テーブルにデフォルト ルートの指定がない場合に、スタティック ルートの設定に到達不能のネクスト ホップが存在していても、エラー メッセージが表示されず、スタティック ルートも配置されません。

回避策： なし。

論理スイッチに接続されている 1 つのサブ インターフェイスを持つ NSX Edge 仮想マシンが vSphere Web Client ユーザー インターフェイスで削除されると、同じポートに接続する新しい仮想マシンのデータ パスが機能しないことがある

NSX Manager からではなく、vSphere Web Client を使用して Edge 仮想マシンを削除すると、不透明チャンネル上の dvPort に設定されている VXLAN トランクがリセットされません。これは、トランクの設定が NSX Manager で管理されているためです。

回避策： 次の手順を実行して、VXLAN のトランク設定を手動で削除します。

1. ブラウザ ウィンドウで次のように入力して、vCenter Server 管理対象オブジェクト ブラウザに移動します：

`https://<vc-ip>/mob?vmobl=1`

2. [Content] をクリックします。
3. 次の手順を実行して、dvsUuid 値を取得します。
 - a. [rootFolder] リンクをクリックします（例： group-d1(Datacenters)）。
 - b. データセンター名リンクをクリックします（例： datacenter-1）。
 - c. [networkFolder] リンクをクリックします（例： group-n6）。
 - d. 分散仮想スイッチ名のリンクをクリックします（例： dvs-1）。
 - e. uuid の値をコピーします。
4. [DVSManger] > [updateOpaqueDataEx] の順にクリックします。
5. [selectionSet] に次の XML を追加します。

```
<selectionSet xsi:type="DVPortSelection">
<dvsUuid>value</dvsUuid>
<portKey>value</portKey> <!--port number of the DVPG where trunk vnic got connected-->
</selectionSet>
```

6. [opaqueDataSpec] に次の XML を追加します。

```
<opaqueDataSpec>
  <operation>remove</operation>
  <opaqueData>
    <key>com.vmware.net.vxlan.trunkcfg</key>
    <opaqueData></opaqueData>
  </opaqueData>
</opaqueDataSpec>
```

7. isRuntime を [false] に設定します。
8. [Invoke Method] をクリックします。
9. 削除済みの Edge 仮想マシンに設定されたトランク ポートごとに手順 5～8 を繰り返します。

セキュリティ サービスに関する既知の問題

L2 VPN で VLAN ID 0 に接続できない

NSX の L2 VPN では、ユーザーが L2 VPN に VLAN ID 0 を設定できますが、これは不適切な設定です。この VPN 設定では、トラフィックが流れなくなります。

回避策： 回避策：1～4094 の有効な VLAN ID を使用してください。

SSLVPN-Plus で Cipher 3C (SHA-256) 暗号化アルゴリズムがサポートされない

ローカル分散ファイアウォール ルールの appliedTo フィールドでユニバーサル論理スイッチの使用が許可されてしまう

ユニバーサル論理スイッチがセキュリティ グループ メンバーとして使用されている場合、分散ファイアウォール ルールの AppliedTo フィールドでそのセキュリティ グループを指定できてしまいます。そのような DFW ルールはユニバーサル論理スイッチに間接的に適用されますが、それがどのように動作するかわからないため、本来は適用を許可するべきではありません。

回避策： なし。

NetX ルールで送信元/宛先として IPset を使用すると、[無効なコンテナ タイプ：IPSet] というエラーが表示される

回避策： NetX ルールの送信元/宛先として IPSet を使用する代わりに、セキュリティ グループを作成して、IPset をそのメンバーにします。

これは、6.2.1 における既知の問題です。

1 つのクラスタでファイアウォールが無効になっている場合、Cross-vCenter NSX ファイアウォール除外リストが発行されない

Cross-vCenter NSX で、クラスタの 1 つでファイアウォールが無効になっている場合、ファイアウォール除外リストがクラスタに発行されません。

回避策： 影響を受ける NSX Edge の強制同期を行います。

これは、6.2.1 における既知の問題です。

DELETE API が使用されると、ファイアウォール ルールの再発行に失敗する

DELETE API メソッドを使用してファイアウォール構成全体を削除してから、保存済みのファイアウォール ルール ドラフトからすべてのルールを再発行しようとする、ルールの発行に失敗します。

これは、6.1.5 および 6.2.1 の両方における既知の問題です。

VMware NSX for vSphere 6.1.x および 6.2.x でリファレンス オブジェクトの削除後、分散ファイアウォール (DFW) ルールの発行に失敗する

回避策： この問題が発生した場合、[ナレッジベースの記事 KB2126275](#) を参照してください。

新しいユニバーサル ルールを作成できず、既存のユニバーサル ルールを フロー モニタリングのユーザー インターフェイスで編集できない

回避策： フロー モニタリングのユーザー インターフェイスからユニバーサル ルールを追加または編集できません。EditRule は自動的に無効になります。

NSX のユーザー インターフェイスで、Security Group の作成時に Active Directory ユーザー/グループのロードに 3 分以上かかる

Security Group を設定し、「ディレクトリ グループ」を選択すると、NSX のユーザー インターフェイスで Active Directory ユーザー/グループのリストを取り込むまでに 3 分以上かかります。回避策はありません。

Service Composer のファイアウォール構成が同期していない

NSX Service Composer では、いずれかのファイアウォール ポリシーが無効になっている場合（ファイアウォール ルールで使用されている Security Group を削除した場合など）、別のファイアウォール ポリシーを削除または変更すると、「ファイアウォールの設定は同期されていません」というエラー メッセージが表示され、Service Composer が同期されなくなります。

回避策： 無効なファイアウォール ルールをすべて削除して、ファイアウォール構成を同期します。[Service Composer] を選択します。[セキュリティ ポリシー] を選択し、ファイアウォール ルールに関連付けられている各セキュリティ ポリシーに対し[アクション] をクリックして[ファイアウォール構成の同期] を選択します。この問題を回避するには、必ず無効なファイアウォールの設定を修正または削除してから、ファイアウォール構成の変更を行ってください。

229 文字を超えるセキュリティ ポリシー名が許容されない

Service Composer の [セキュリティ ポリシー] タブにあるセキュリティ ポリシー名のフィールドでは、229 文字まで許容されます。ポリシー名の先頭には内部でプリフィックスが付加されるためです。

回避策： なし。

Palo Alto Networks VM-Series の特定のバージョンがデフォルトの設定で NSX Manager と連携しない

NSX 6.1.4 のコンポーネントには、SSLv3 をデフォルトで無効にするものがあります。アップグレード前に、NSX デプロイと連携しているすべてのサードパーティのソリューションが SSLv3 通信に依存していないことを確認します。たとえば、Palo Alto Networks VM-series ソリューションのいくつかのバージョンには SSLv3 のサポートが必要です。そのため、ベンダーにバージョンの要件について確認する必要があります。

アップグレードされた NSX 環境でファイアウォール ルールを発行すると、Web Client で Null ポインタ例外になることがある

アップグレードされた NSX 環境でファイアウォール ルールを発行すると、ユーザー インターフェイスで Null ポインタ例外になることがあります。ルールの変更は保存されます。これは表示のみの問題です。

REST API 呼び出しを使用してファイアウォール構成を削除する場合、保存した設定をロードして発行することができない

ファイアウォールの設定を削除すると、新しいデフォルトのセクションが新しいセクション ID で作成されます。保存したドラフト（セクション名は同じでセクション ID が古い）をロードすると、セクション名が競合して次のようなエラーが表示されます。

重複するキーの値が一意性の制約「`firewall_section_name_key`」に違反しています

回避策： 次のいずれかの手順を実行します。

- 保存された設定をロードした後、現在のデフォルトのファイアウォール セクションの名前を変更します。
- ロードした保存済み設定で、発行前にデフォルトのセクションの名前を変更します。

監視サービスに関する既知の問題

分散論理ルーター（DLR）の展開で、vSphere Web Client を使用して 8 個を超えるアップリンク インターフェイスを追加できない

回避策： 分散論理ルーターがデプロイされてから、追加のインターフェイスを分散論理ルーターに追加します。

解決した問題

6.2.0 および 6.2.1 で解決した問題

解決した問題は次のカテゴリに分けられます。

- [インストールとアップグレードに関する解決した問題](#)

- [NSX Manager に関する解決した問題](#)
- [論理ネットワークに関する解決した問題と NSX Edge に関する解決した問題](#)
- [セキュリティ サービスに関する解決した問題](#)
- [監視サービスに関する解決した問題](#)
- [ソリューションの相互運用性に関する解決した問題](#)

解決した一般的な問題

- VMware NSX for vSphere 6.2.0 で IP アドレス検出を使用すると、ESXi 5.x および 6.x で紫色の診断画面が表示される (2134329)
VMware NSX for vSphere 6.2.0 の論理スイッチで IP アドレス検出を使用すると、ESXi 5.x および 6.x ホストで障害が発生し、パープル スクリーンが表示されます ([ナレッジベースの記事 KB2134329](#) で解説)。

NSX 6.2.1 で、この問題は修正されました。

- セキュリティ タグ ポートレットの [管理] オプションがデフォルトでグレースアウトされ、選択できない
仮想マシンのサマリ ページにあるセキュリティ タグ ポートレットの [管理] ハイパーリンクは、ユーザーが新しいセキュリティ タグを作成するまでグレースアウトされ、選択できません。

NSX 6.2.1 で、この問題は修正されました。

- 一部のコントローラ ログが、Syslog エクスポートに含まれない
Zookeeper クラスタリング ログを含むコントローラ ログは、Syslog のエクスポートに含まれません。

NSX 6.2.1 で、この問題は修正されました。

- 利用可能な MTU のサイズよりも大きなデータ サイズで ping すると、ESXi 6.0 の vdl2 で PSOD (パープル スクリーン) が発生する
NSX ホストのスイッチに接続された vmknix から ping を開始すると、データ サイズが MTU より大きい場合、ホストで PSOD が発生します。

NSX 6.2.1 で、この問題は修正されました。

- ユーザーは、TCP と UDP 双方のプロトコルに同じ IP アドレスとポート番号を設定する必要がある
このリリースでは、次の問題も解決されています。
 - プールが設定されていない UDP 仮想サーバの設定に失敗する
 - UDP 仮想サーバにプールが関連付けられていない場合、統計に誤ったデータが表示される

NSX 6.2.1 で、この問題は修正されました。6.2.1 リリースでは、プールが関連付けられているかどうかに関わらず、TCP と UDP 双方に同じ IP アドレスとポート番号を使用できます。

インストールとアップグレードに関する解決した問題

- Mac OS X Yosemite 以降に SSL VPN-Plus Client をインストールできない
Mac OS X は、Yosemite より前のバージョンのみがサポートされます。

NSX 6.2.1 で、この問題は修正されました。

- NSX for vSphere を 6.0.7 から 6.1.3 にアップデートした後、vSphere Web Client がログイン画面でクラッシュする
NSX Manager を 6.0.7 から 6.1.3 にアップデートした後に、vSphere Web Client ユーザー インターフェイスのログイン画面に例外が表示されます。ユーザーは、vCenter Server または NSX Manager でログインと操作ができなくなります。

NSX 6.2.0 で、この問題は修正されました。

- ゲスト イントロスペクションのインストールがエラーで失敗する
クラスタでゲスト イントロスペクションをインストールする場合、インストールが次のエラーで失敗します。

VIB モジュールの無効なフォーマット

NSX 6.2.0 で、この問題は修正されました。

- ホストの準備の問題により、DVPort に「Would block」というエラー メッセージが出力され、有効化に失敗する
NSX が有効な ESXi ホストで、ホストの準備の問題により「Would block」というエラーメッセージが出力され、DVPort の有効化に失敗します。この問題が発生した際に、最初に通知されるエラーメッセージはさまざまです。たとえば、VC/hostd.log では VTEP 作成失敗、vmkernel.log では DVPort 接続失敗、ゲストでは「SIOCSIFFLAGS」エラーと見なされる場合があります。この問題は、vSphere Distributed Switch (vDS) のプロパティが vCenter Server によってプッシュされた後に VIB がロードされると発生します。これはアップグレード中に発生する場合があります。[ナレッジベースの記事 KB2107951](#) を参照してください。

NSX 6.2.0 で、この問題は修正されました。

- NSX 6.1.4 にアップデートされた環境で、既存の NSX Edge Gateway の削除に失敗する
NSX インストール環境を 6.1.3 から 6.1.4 にアップデートすると、6.1.4 へのアップデート後に既存の NSX Edge Gateway を削除することができません。この問題は、アップデート後に作成された新しい Edge Gateway には影響しません。6.1.2 以前から直接アップデートされたインストール環境では、この問題の影響はありません。

NSX 6.2.0 で、この問題は修正されました。

- サードパーティのセキュアな FTP バックアップを使用して NSX バックアップを実行すると、AES 暗号化が使用できない

NSX 6.2.0 で、この問題は修正されました。

- ホストの再起動中、NSX Manager のユーザー インターフェイスでユーザーが理解できるエラーメッセージが表示されない
この 6.2 のリリースでは、NSX Manager のユーザー インターフェイスは詳細なエラー メッセージを表示するよう更新されました。メッセージは、ホストの再起動中に発生する可能性のある問題を説明し、可能なソリューションを提供します。

NSX 6.2.0 で、この問題は修正されました。

- NSX VIB をインストールすることができない
サードパーティのモジュールから ixgbe ドライバのロードに失敗した場合、NSX VIB のインストールが予期したとおりに完了しないことがあります。これは、ドライバがロックされ、インストールに使用されないためです。

NSX 6.2.0 で、この問題は修正されました。

- vCloud Networking and Security (vCNS) 5.5.3 からアップグレードすると、NSX Manager サービスを開始することができない
vCloud Networking and Security (vCNS) 5.5.3 から NSX 6.1.3 にアップグレードすると、NSX Manager サービスがハングし、開始に失敗します。

NSX 6.2.0 で、この問題は修正されました。

- NSX Edge の再起動後、メッセージ バスが開始されないことがある
Edge 仮想マシンの再起動後、パワーオンしてもメッセージ バスが開始されない場合があります。追加で再起動が必要になります。

NSX 6.2.0 で、この問題は修正されました。

NSX Manager に関する解決した問題

- 6.2.1 より、NSX Manager はクラスタ内の各コントローラ ノードでクエリを実行して、当該コントローラとクラスタ内の他のコントローラ間の接続情報を入手する
これは、NSX REST API（「GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller」 コマンド）の出力として提供され、コントローラ ノード間のピア接続ステータスを表示します。NSX Manager が、任意の 2 台のコントローラ ノード間の接続が切断されていることを認識すると、システム イベントが生成され、ユーザーに警告します。

NSX 6.2.1 で、この問題は修正されました。

- NSX Manager のバックアップ-リストアが別のアプライアンスで実施された場合、コントローラの強制同期が停止する
NSX Manager がバックアップからリストアされるか、バックアップからクローン作成された場合、NSX Controller クラスタへの強制同期が失敗します。この問題は、新規にデプロイされた NSX Manager では発生しません。

NSX 6.2.1 で、この問題は修正されました。

- NSX 環境に含まれないホストに対する、NSX のハートビートのログ作成が失敗する
NSX 準備済みホストを、NSX で準備解除せずに直接 vCenter Server のインベントリから削除すると、NSX は予期しない「ホスト接続」DCN を受け取り、ホストからメッセージング インフラストラクチャ コンポーネントが部分的に削除されます。結果として、削除されるはずの NSX/ホスト間のメッセージング リンクがアクティブのままになり、NSX はホストに関して誤った「アラート」システム イベントを通知する可能性があります。NSX 6.2.1 で、この問題は修正されました。

NSX 6.2.1 で、この問題は修正されました。

- NSX Manager が、**write erase** コマンドの実行後、機能しなくなる
write erase コマンドの実行後に NSX Manager を再起動すると、Linux シェルにアクセスするためのパスワードがリセットされる、セットアップ コマンドがないなど、NSX Manager が正しく動作しないことがあります。

NSX 6.2.0 で、この問題は修正されました。

- [ドメインの追加] で、LDAP オプションに **【ドメイン認証情報を使用】** エラーが表示される
NSX 6.1.x では、LDAP ドメインにユーザーを追加する場合、ユーザー名がユーザー インターフェイスに提供されていても、Web Client が「ユーザー名が指定されていませんでした」というエラーを表示しました。NSX 6.2.0 で、この問題は修正されました。

NSX 6.2.0 で、この問題は修正されました。

- CA 署名付き証明書のインポート後、NSX Manager を再起動しないと証明書が有効にならない
CA によって署名された NSX Manager 証明書をインポートするとき、NSX Manager を再起動するまで新たにインポートされた証明書が有効になりません。

NSX 6.2.0 で、この問題は修正されました。

- NSX Manager を LDAPS ドメインにインポートできない
NSX Manager を LDAPS ドメインにインポートしようとすると、次のエラー メッセージが表示されます。
ホスト <サーバ FQDN> に接続できません
エラー メッセージ: シンプル バインドに失敗しました:<サーバ FQDN: 番号>

NSX 6.2.0 で、この問題は修正されました。

論理ネットワークに関する解決した問題と NSX Edge に関する解決した問題

- NSX Edge で RADIUS 認証サーバの設定に失敗する

NSX 6.1.5 以前は、RADIUS サーバの秘密鍵には 32 文字の制限があり、文字列がこの上限を超えると、RADIUS サーバは NSX Edge との接続に失敗していました。現在は最大 64 文字です。

NSX 6.2.0 で、この問題は修正されました。

- VIO Heat スタックのデプロイが、次のようなエラーによって VMware NSX for vSphere 6.x Edge で断続的に失敗する：「メモリを割り当てることができません」

健全性監視のメモリ使用量は時間とともに増加し、最終的には Edge で障害が発生します。

NSX 6.2.1 で、この問題は修正されました。

- BGP フィルタが適用されるまでおよそ 40 秒かかる

この間、すべての再分配ポリシーはフィルタなしで適用されます。この遅延は、送信方向の NSX 分散論理ルーター (DLR) にのみ発生します。

NSX 6.2.0 で、この問題は修正されました。

- NSX Edge のサブインターフェイスで [ICMP リダイレクトの送信] オプションを無効にしても、ICMP リダイレクトが送信される

NSX Edge のサブインターフェイスでは、デフォルトで [ICMP リダイレクトの送信] が無効になっています。このオプションが無効になっていても、Edge のサブインターフェイスで ICMP リダイレクトが送信されます。

NSX 6.2.0 で、この問題は修正されました。

- 分散論理ルーターのブリッジまたはテナント名に非 ASCII 文字を追加できない

NSX Controller API は非 ASCII 文字に対応していません。

NSX 6.2.0 で、この問題は修正されました。

- BGP ネイバー フィルタ ルールが変更されると、既存のフィルタが最大 40 秒間適用されない可能性がある

BGP フィルタが IBGP を実行している NSX Edge に適用されると、IBGP セッションでフィルタが適用されるまで最大 40 秒かかる可能性があります。この時間に、NSX Edge が IBGP ピアの BGP フィルタで拒否されているルートを通知することがあります。

NSX 6.2.0 で、この問題は修正されました。

- NSX Controller のいずれかが、シャットダウン時に他のコントローラにマスター ロールを渡さない
通常は、マスター ロールを操作するコントローラがシャットダウンの準備をするときに、他のコントローラにマスター ロールを自動的に渡します。この場合、コントローラがロールを他のコントローラに渡すことに失敗し、ステータスは中断になり、切断モードに移行します。

NSX 6.2.0 で、この問題は修正されました。

- ホスト間の VXLAN トラフィックをユニキャストまたはマルチキャストで渡すことができない
複数の仮想マシンが同じホスト上にある場合、ユニキャストやマルチキャストで VXLAN から通信することができます。しかし、仮想マシンが違うホスト上にある場合は、通信できません。

NSX 6.2.0 で、この問題は修正されました。

- NSX Edge や分散論理ルーターで同時に複数の BGP ルールを削除すると Web Client のクラッシュが起こる

NSX 6.2.0 で、この問題は修正されました。一度に複数の BGP ルールを削除することが可能になりました。

- Border Gateway Protocol (BGP) 拒否ルールの追加後、プロトコル アドレスが一時的に表示される
NSX Edge Services Gateway に Border Gateway Protocol (BGP) 拒否ルールを追加した後、プロトコル アドレスが一時的に表示されることがあります。

NSX 6.2.0 で、この問題は修正されました。

- vMotion の間、仮想マシンの接続が切断される
vMotion の実行中に仮想マシンの接続が切断されたり、NIC が切断された仮想マシンに関するアラートを
受け取ったりすることがあります。

NSX 6.2.0 で、この問題は修正されました。

- コントローラのスナップショットをダウンロードできない
コントローラのスナップショットをダウンロードする場合、最後のコントローラのスナップショットをダ
ウンロードできないことがあります。たとえば、コントローラが 3 つあった場合、最初の 2 つのコント
ローラに関してはスナップショットのダウンロードに成功しますが、3 つ目のコントローラのスナップ
ショットがダウンロードできないことがあります。

NSX 6.2.0 で、この問題は修正されました。

- 仮想サーバの設定時に、以前に選択した IP アドレスが適用される
新しい仮想サーバを作成する際に、以前に選択した IP アドレス プールのリストから自動的に IP アドレス
が適用される場合があります。これは、以前に IP アドレス プールを選択して仮想サーバの IP アドレスを
獲得した場合に発生します。仮想サーバの IP アドレス プール情報を編集しようとする、ユーザー イン
ターフェイスからバックエンドに情報が自動送信されず、IP アドレスプールから獲得した以前の IP アド
レスが自動的に適用されます。

NSX 6.2.1 で、この問題は修正されました。

- Edge Services Gateway で HA が有効となっており、OSPF hello/dead 間隔がそれぞれ 30 秒または
120 秒以外の値に設定されていると、フェイルオーバー中にトラフィックが失われる場合がある
OSPF を実行し、HA が有効な状態でプライマリ NSX Edge に障害が発生すると、引き継ぎ待機に必要な時
間がグレースフル リスタートのタイムアウトを超過し、OSPF ネイバーで転送情報ベース (FIB) テーブル
から学習済みのルートが削除されます。その結果、OSPF が再収束するまで、データプレーンは停止した
ままになります。

NSX 6.2.0 で、この問題は修正されました。

- 仮想マシンが Edge DHCP サーバから ping を受信することができない
仮想マシンが Edge Gateway に ping を送信することはできますが、オーバーレイ ネットワークで Edge
Gateway トランクの DHCP の ping を受信できません。Edge DHCP サーバは、トランク ポートとしてセット
アップされ、すべてのトラフィックの送受信に失敗します。ただし、Edge Gateway および DHCP Edge が同
じホストにある場合、お互いに ping の送受信が可能です。DHCP Edge を別のホストに移動すると、DHCP
Edge は Edge Gateway から ping の受信ができなくなります。

NSX 6.2.0 で、この問題は修正されました。

- Edge ロード バランサの統計情報が vSphere Web Client に正しく表示されない
Edge ロード バランサで、vSphere Web Client ユーザー インターフェイスのチャートに同時接続統計の値が
表示されません。

NSX 6.2.0 で、この問題は修正されました。

- o IPsec VPN チャンネルのローカルおよびリモート サブネットにある直接集約ネットワークを削除すると、ピア Edge の間接的なサブネットへの集約ルートが表示されない
Edge にデフォルトのゲートウェイがなく、IPsec を設定しているときに、ローカルの子ブネットおよびリモート サブネットの一部にあるすべての直接接続の子ブネットを削除すると、残ったピアの子ブネットに IPsec VPN でアクセスできなくなります。

NSX 6.2.0 で、この問題は修正されました。

- NSX 6.1.2 以降にアップグレードした後、ロード バランサにトラフィックを渡すことができない
NSX Edge ロード バランサで [X-Forwarded-For の挿入] オプションを使用すると、トラフィックがロード バランサを通過しない場合があります。

NSX 6.2.0 で、この問題は修正されました。

- clear ip ospf neighbor command コマンドを実行すると、セグメント障害エラーを返す

NSX 6.2.0 で、この問題は修正されました。

- Kerberos の要求を処理することができない
特定の Kerberos の要求が、NSX Edge での分散処理中に失敗します。

NSX 6.2.0 で、この問題は修正されました。

セキュリティ サービスに関する解決した問題

- 既存のファイアウォール ドラフトの名前を変更すると、ユーザー インターフェイスに「内部サーバ エラー」が表示されて操作が失敗する

NSX 6.2.1 で、この問題は修正されました。

- 分散ファイアウォールのセントラル CLI で「ERROR output 100」が表示される場合がある
特定の状況下で、vNIC (Virtual Network Adapter) が切断されると、NSX Manager とホスト間で vNIC の状態の情報が一致なくなり、セントラル CLI で「ERROR output 100」が出力される場合があります。

NSX 6.2.1 で、この問題は修正されました。

- アプリケーション プロファイルのリストがソートされない
サービス挿入が有効になっている場合、NSX Edge 内のアプリケーション プロファイル名のリストが不規則な順番で表示されます。6.2.1 リリースでは、アプリケーション プロファイルのリストをソートして表示できるよう修正されました。

NSX 6.2.1 で、この問題は修正されました。

- 特定の ESXi ホストに対して実行されるセントラル CLI コマンドが、一部のセットアップでタイムアウトする

NSX 6.2.1 で、この問題は修正されました。

- 大量のコンテナ更新で vsfwd.log がすぐに上書きされる
SpoofGuard ポリシーが変更されると、NSX Manager は変更を速やかにホストに送りますが、ホストでの変更処理と仮想マシンの SpoofGuard 状態の更新に時間がかかります。

NSX 6.2.0 で、この問題は修正されました。

- グローバル スコープで定義された Security Group または他のグループ オブジェクトを使用して、NSX ファイアウォールを設定することができない
NSX Edge スコープで定義された管理者ユーザーは、グローバル スコープで定義されたオブジェクトにアクセスすることはできません。たとえば、ユーザー *abc* が Edge スコープで定義され、Security Group *sg-1* がグローバル スコープで定義された場合、*abc* は NSX Edge のファイアウォール構成で *sg-1* を使用することはできません。

NSX 6.2.0 で、この問題は修正されました。

- ファイアウォール ルールの表示中にマウスの動きが遅れる
vSphere Web Client の [Networking and Security] セクションで、ファイアウォール ルールの行の上にマウスを合わせると、表示が 3 秒遅れます。

NSX 6.2.0 で、この問題は修正されました。

- 発行が成功しているのに、ユーザー インターフェイスでエラー「ファイアウォールを発行できませんでした」が表示される
分散ファイアウォールが、環境内のクラスタのサブセットで有効になっていて、1 つ以上のアクティブなファイアウォール ルールで使用されているアプリケーション グループを更新すると、ユーザー インターフェイス上のすべての発行アクションにおいて、NSX ファイアウォールが有効でないクラスタに属しているホストの ID を含んだエラー メッセージが表示されます。
エラー メッセージに関わらず、ルールは正常に発行され、分散ファイアウォールが有効になっているホストに適用されます。

NSX 6.2.0 で、この問題は修正されました。

- REST を使用したセキュリティ ルールの削除でエラーが表示される
Service Composer によって作成されたセキュリティ ルールを削除するために REST API 呼び出しが使用されると、対応するルール セットは実際にはサービス プロファイル キャッシュで削除されず、結果として `ObjectNotFoundException` エラーが発生します。

NSX 6.2.0 で、この問題は修正されました。

- 新たに追加された仮想マシンにファイアウォール ルールが反映されない
新たに仮想マシンが論理スイッチに追加されると、ファイアウォール ルールが正しく更新されず、新規の仮想マシンが追加されません。ファイアウォールに変更を加えて変更を発行すると、新しいオブジェクトがポリシーに追加されます。

NSX 6.2.0 で、この問題は修正されました。

- Security Group の設定で Active Directory オブジェクトが選択できない
NSX 6.1.x では、Security Group オブジェクト選択画面で Active Directory ドメイン オブジェクトまたは LDAP ドメイン オブジェクトの応答に長い時間がかかります。

NSX 6.2.0 で、この問題は修正されました。

- IP アドレスが複数のコンマで区切られているため、ファイアウォールをソースやターゲットに追加することができない

NSX 6.2.0 で、この問題は修正されました。

- NSX 分散ファイアウォール (DFW) セクションをリストの最上位に移動できない
Service Composer で Security Group ポリシーを作成する場合、分散ファイアウォール テーブルで作成されたセクションをリストの最上位に追加することができません。分散ファイアウォール セクションは、上にも下にも動かすことができません。

NSX 6.2.0 で、この問題は修正されました。

- ポート範囲を使用して設定されたセキュリティ ポリシーにより、ファイアウォールが同期しない状態になる
ポート範囲（「5900-5964」など）としてセキュリティ ポリシーを設定すると
NumberFormatException エラーが発生してファイアウォールが同期しなくなります。

NSX 6.2.0 で、この問題は修正されました。

監視サービスに関する解決した問題

- フロー統計のレポート作成時に、インデックス 0（着信バイト）とインデックス 1（発信バイト）のカウントが逆転している場合がある
インデックス 0 は、元の方向のトラフィック カウントを示し、インデックス 1 は反対方向のトラフィック カウントを示します。

NSX 6.2.1 で、この問題は修正されました。

- **#show interface** コマンドで vNIC_0 インターフェイスのバンド幅や速度が表示されない
#show interface コマンドを実行すると、「全二重、速度 0M/秒」と表示されますが、正しい NSX Edge vNIC_0 インターフェイスのバンド幅や速度が表示されません。

NSX 6.2.0 で、この問題は修正されました。

- 分散ファイアウォールで IPFIX 構成を有効にすると、vSphere Distributed Switch の NetFlow または SNMP の ESXi 管理インターフェイスでファイアウォール ポートが削除されることがある
IPFIX 用にコレクタ IP アドレスおよびポートが定義されている場合、指定された UDP コレクタ ポートの送信方向に ESXi 管理インターフェイスのファイアウォールが開かれています。この操作により、事前に ESXi ホスト上で設定されていた場合、次のサービスの ESXi 管理インターフェイス ファイアウォール上の動的ルールセット設定が削除される可能性があります。
 - vSphere Distributed Switch 上の NetFlow コレクタ ポートの設定
 - SNMP ターゲット ポートの設定

NSX 6.2.0 で、この問題は修正されました。

- IPFIX プロトコルで拒否/ブロック イベントが処理できない
通常 vsfwd ユーザー プロセスはドロップや拒否などのフローを収集し、IPFIX 用に処理します。この問題は、IPFIX コレクタが拒否/ブロック イベントの認識に失敗すると発生します。これは、vSIP ドロップ パケット キューが狭すぎるか、非アクティブ フロー イベントによってラップ アラウンドされるためです。このリリースでは、拒否/ブロック イベントを IPFIX プロトコルで送信する機能が実装されました。

NSX 6.2.0 で、この問題は修正されました。

ソリューションの相互運用性に関する解決した問題

- 組織ネットワークをセットアップできない
組織規模のネットワークをセットアップしようとする、vCloud Director が失敗し、エラー メッセージが表示されます。

NSX 6.2.0 で、この問題は修正されました。

- VMware Integrated OpenStack (VIO) セットアップで複数の仮想マシンを起動できない
VMware Integrated OpenStack を使用している場合、短時間に大量の仮想マシンを起動したり、大量のファイアウォール ルールを発行することができませんでした。これによって、ログに「Error publishing ip for vnic」というメッセージが記録されます。

NSX 6.2.0 で、この問題は修正されました。

6.1.5 および 6.2.1 で解決した問題

解決した問題は次のカテゴリに分けられます。

- [インストールとアップグレードに関する解決した問題](#)
- [NSX Manager に関する解決した問題](#)
- [論理ネットワークに関する解決した問題](#)
- [ネットワークと Edge サービスに関する解決した問題](#)
- [セキュリティ サービスに関する解決した問題](#)
- [ソリューションの相互運用性に関する解決した問題](#)

解決した一般的な問題

- NSX Controller のいずれかが、シャットダウン時に他のコントローラにマスター ロールを渡さない
通常は、マスター ロールを操作する NSX Controller がシャットダウンの準備をするときに、他のコントローラにマスター ロールを自動的に渡します。この場合、コントローラがロールを他のコントローラに渡すことに失敗し、ステータスは中断になり、切断モードに移行します。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- NSX Controller の制御プレーン接続が失敗する
コントローラの制御プレーン接続が失敗し、`txInProgress` に関する `netcpa` にエラーが表示されず。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

インストールとアップグレードに関する解決した問題

- NSX のアップデート後、ゲスト イントロスペクション が NSX Manager と通信できなくなる
NSX 6.0.x から NSX 6.1.x、または NSX 6.0.x から NSX 6.2 へのアップデートを行った後、ゲスト イントロスペクション サービスをアップデートするまで、NSX Manager は、ゲスト イントロスペクション のユニバーサル サービス仮想マシン (USVM) との通信ができなくなります。NSX Manager と ゲスト イントロスペクション 間の通信が切断されると、仮想マシンに変更（たとえば仮想マシンの追加、vMotion、または削除）が生じた場合、NSX クラスタ内の仮想マシンが保護されなくなります。[NSX インストール] > [サービス デプロイ] タブに、ゲスト イントロスペクションの現在のバージョンが表示されます。この問題が生じると、[サービス ステータス] 列に警告が表示されます。警告メッセージには、影響を受けるホストの一覧と「ゲスト イントロスペクション の準備ができていません」というエラー メッセージが表示されます。

回避策：問題を解決するには、『[NSX のアップグレード](#)』ドキュメントの手順を実行してゲスト イントロスペクションをアップグレードします。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

NSX Manager に関する解決した問題

- Active Directory ドメインに追加した後、NSX Manager の CPU 使用率が高くなる
Active Directory ドメインに追加した後、NSX Manager の CPU 使用率が高くなります。NSX Manager のシステム ログでは、複数の Postgres スレッドが実行中として表示されます。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- vCenter Server で NSX Manager 6.1.4 を登録できず、「NSX 管理サービスの操作に失敗した」というエラーが表示される

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- NSX Manager の Web Client で、エラー「コード 301002」が表示される
説明：[NSX Manager] > [監視] > [システム イベント] の順に選択すると、次のエラーが表示されま
す。Filter config not applied to vnic.コード 301002。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

論理ネットワークに関する解決した問題

- 動的ルーティング環境で論理インターフェイス (LIF) を削除した後、接続が失われる
この問題は、NSX 分散論理ルーター (Edge および 分散論理ルーター) で発生していました。動的ルー
ティング (OSPF および BGP) を使用すると、LIF を削除した後にネットワーク接続が失われます。この問
題は、NSX バージョン 6.0.x から 6.1.4 で発生します。

動的ルーティングを使用している NSX 環境で、各 LIF それぞれに関連する再配分ルール インデックス ID が割り当てられます。このような環境で LIF を削除すると、アクティブな LIF に割り当てられたインデックス ID が変更される可能性があります。これにより、インデックス ID が変更された LIF のネットワーク接続が一時的に失われることがあります。LIF の削除が連続して行われる場合、個々の LIF を削除した後、影響を受ける LIF が 5 秒から 30 秒の間中断します。LIF の削除が一括で行われる場合、影響を受けた LIF の中断は合計で 5 秒から 30 秒になります。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

ネットワークと Edge サービスに関する解決した問題

- NSX Edge Services Gateway (ESG) に設定した OSPF ルートが分散論理ルーター (DLR) で受け入れられず、影響するパケットがドロップされる
この問題は、OSPF で IP_HDRINCL オプションを使用している場合に発生します。特定の Linux カーネルでは、このオプションが存在する場合、IP スタックでのパケットのフラグメント化が防止されます。このため、インターフェイスの MTU を上回るパケットはドロップされます。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

バックアップ元の NSX Manager のホスト名が、リストア先 NSX Manager の Syslog に表示される 1 番目の NSX Manager のホスト名が A で、この NSX Manager のバックアップを作成したとします。2 番目の NSX Manager は、バックアップおよびリストアのドキュメントに従って、1 番目の NSX Manager と同じ IP アドレスを使用してインストールおよび設定されていますが、ホスト名は B となっています。リストアされた NSX Manager では、リストア直後はホスト名が A と表示され、再起動後に正しいホスト名 B と表示されます。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- ESXi ホストのネットワーク接続が失われることがある
ESXi ホストのネットワーク接続が失われ、安定性に問題が生じることがあり、次のような複数のエラーメッセージがログに記録されます。
`WARNING: Heartbeat: 785: PCPU 63 didn't have a heartbeat for 7 seconds; *may* be locked up.`

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- vMotion の間、仮想マシンの接続が切断される
6.0.8 では vMotion の間、仮想マシンの接続が切断され、「VISP ヒープが枯渇しました」というメッセージが表示されます。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- CA 署名済み証明書を設定した L2 VPN サービスを利用する場合、NSX Edge を再デプロイできない
CA 署名済み証明書または自己署名済み証明書を設定した L2 VPN サービスでは、NSX Edge の再デプロイ
やサイズ変更を行うことができません。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- NSX Edge の再起動後、メッセージ バスが開始されないことがある
Edge 仮想マシンの再起動後、パワーオンしてもメッセージ バスが開始されない場合があります、追加で再起
動が必要になります。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

セキュリティ サービスに関する解決した問題

- NSX for vSphere 6.x Controller が断続的に切断される
6.1.4 以前のリリースで出荷されていた StrongSWAN パッケージ内の IPSEC バグにより、IPSEC の再キー化
後に、コントローラ間のトンネルが確立されませんでした。このためコントローラ間で部分的な接続障害
が発生し、さまざまな問題が生じていました。詳細については、[ナレッジベースの記事 KB2127655](#) を参
照してください。

NSX 6.1.5 および 6.2.1 で、この問題は修正されました。

- Security Group のオブジェクト選択画面で、LDAP ドメイン オブジェクトの応答に時間がかかるか、
応答がない場合がある

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- ファイアウォール ルールの表示中にマウスの動きが遅れる
vSphere Web Client の [Networking and Security] セクションで、ファイアウォール ルールの行の上でマウス
を動かすと、マウスの表示が 3 秒遅れます。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- NSX-v における一部の IP SpoofGuard ルールが正しく適用されません。
NSX-v における一部の IP SpoofGuard ルールが正しく適用されません。NSX-v の Security Group にはインス
タンスが存在せず、Security Group に手動で追加する必要があります。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- Service Composer のユーザー インターフェイスで一括削除を行うと、「0 ~ 0」というメッセー
ジが表示される
NSX Service Composer のユーザー インターフェイスでポリシーの一括削除（100 件以下）を行うと、「0
から 0 である必要があります」というメッセージが表示されます。このメッセージは無視しても問題あり
ません。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- ポリシー削除のバックグラウンド処理に時間がかかり、CPU 使用率が高くなる場合がある
ポリシーを削除すると、それ以外のすべてのポリシーがバックグラウンドで再評価されます。ポリシー、
Security Group、ポリシーごとのルールが多数あると、セットアップに 1 時間以上かかる場合があります。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- デフォルトのタイムアウトの 20 分が経過すると、キューに登録された発行可能なすべてのタスクに失敗のマークが付く
キューは NSX Edge ごとに保持され、異なる Edge に対して同時に発行できます。キューに登録された発行可能なタスクは、順次実行されます。その際、タスクごとに約 3 ～ 4 秒かかるため、20 分間で 300 ～ 400 件のタスクが完了します。Edge 向けの 400 件以上の発行タスクが短時間のうちにキューに登録され、待機中に発行タイムアウトの 20 分が経過すると、タスクには自動的に失敗のマークが付きます。NSX Manager は失敗を受けて、Edge への発行に成功した最後の正常なに戻します。Edge 設定のアップデートをバースト モードで NSX Manager に送信しているアプリケーションやプラグインでは、関連付けられているジョブ ID を使用して、タスクの成功/失敗のステータスを監視する必要があります。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

ソリューションの相互運用性に関する解決した問題

- NSX ロード バランサを通過するルートでは、vCloud Connector 経由の仮想マシンのコピーに失敗する

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- VMware Integrated OpenStack (VIO) のデプロイにおいて、新たに展開された仮想マシンで、有効なポートと IP アドレスが割り当てられているように表示されても、ネットワークにアクセスできない場合がある

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- Active Directory ベースの SSO で、vSphere Web Client の [NSX] タブにアクセスすると、ログインに時間がかかる

Active Directory 認証に SSO を使用する NSX for vSphere 環境では、ユーザーが初めて vSphere Web Client の [Networking and Security] セクションにログインする際に時間がかかります。

NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

ドキュメントの改訂履歴

2015 年 8 月 20 日：NSX 6.2.0 用初版。

2015 年 9 月 04 日：NSX 6.2.0 用第 2 版。不要なアップグレード警告を削除しました。

2015 年 12 月 17 日：NSX 6.2.1 用初版。

2016 年 2 月 27 日：NSX 6.2.1 用第 2 版。NSX と Log Insight との互換性について詳細を記載しました。

2016 年 5 月 20 日：NSX 6.2.2 用第 3 版。6.1.x のアップグレードにおける制限事項を追記。