



VMware NSX for vSphere 6.2.9 リリース ノート

VMware NSX for vSphere 6.2.9 | 2017 年 10 月 26 日リリース | ビルド 6926419

このドキュメントの[改訂履歴](#)を参照してください。

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](#)
- [バージョン、システム要件、およびインストール](#)
- [廃止および提供を中止する機能](#)
- [アップグレードに関する注意事項](#)
- [改訂履歴](#)
- [解決した問題](#)
- [既知の問題](#)

新機能

重要度の高いバグの修正：このリリースには、複数の重要なバグ修正とセキュリティ アップデートが含まれています。詳細については、「[解決した問題](#)」セクションを参照してください。

NSX の各バージョンの新機能と変更点について

は、[6.2.8](#)、[6.2.7](#)、[6.2.6](#)、[6.2.5](#)、[6.2.4](#)、[6.2.3](#)、[6.2.2](#)、[6.2.1](#)、[6.2.0](#) を参照してください。

バージョン、システム要件、およびインストール

注：

- 次の表は、推奨される VMware ソフトウェアのバージョンです。ここで推奨されるバージョンは一般的なものであり、環境に固有の推奨に優先するものではありません。
- これは、本ドキュメントが公開された時点で最新の情報です。
- NSX とその他の VMware 製品を併用する場合にサポートされる最小バージョンについては、[VMware 製品の相互運用性マトリクス](#)を参照してください。VMware はテスト結果に基づいて、サポートされる最小バージョンを定めています。

製品またはコンポーネント	推奨されるバージョン
--------------	------------

新しく導入する場合には、最新の NSX for vSphere リリースをお勧めします。

既存の環境をアップグレードする場合は、アップグレード プランを策定する前に、NSX リリース ノートを参照して、特定の問題に関する情報を確認してください。あるいは、VMware テクニカル サポートの担当者に詳細をお問い合わせください。

NSX for vSphere

- NSX for vSphere 6.2.4 では、SSL VPN の既知の問題が解決されています。詳細については、CVE-2016-2079 を参照してください。6.2.2 以前のバージョンを実行している場合、アップグレードをお勧めします。
- NSX for vSphere 6.2.4 と vSphere 6.0 Update 3 を併用することで、vCenter Server の再起動後に ESXi ホストの VTEP が重複するという問題が解決されます。詳細については、[VMware のナレッジベースの記事 KB2144605](#) を参照してください。

NSX 環境では、vSphere 5.5U3 および 6.0U3 以降を使用することをお勧めします。また、[VMware 製品の相互運用性マトリクス](#)で相互運用性の情報を確認してください。

注：

vSphere

- NSX 6.2.x には、vSphere 6.5 との互換性がありません。
- NSX for vSphere 6.2.4 と vSphere 6.0 Update 3 を併用すると、vCenter Server の再起動後に ESXi ホストの VTEP が重複するという問題が解決されます。詳細については、[VMware のナレッジベースの記事 KB2144605](#) を参照してください。
- 分散サービス挿入を行う場合は、ESXi 5.5 パッチ 10 および ESXi 6.0U3 以降を使用することをお勧めします。詳細については、[VMware のナレッジベースの記事 KB2149704](#) を参照してください。

ゲスト イントロスペクション

ゲスト イントロスペクション ベースの NSX の機能は、特定の VMware Tools のバージョンと互換性があります。VMware Tools に含まれるオプションの Thin Agent Network Introspection Driver コンポーネントを利用するには、VMware Tools を次のいずれかにアップグレードする必要があります。

- VMware Tools 10.0.8 以降。NSX または vCloud Networking and Security で VMware Tools をアップグレードした後に、仮想マシンの処理速度が低下する問題を解決します。[VMware ナレッジベースの記事 KB2144236](#) を参照してください。
- VMware Tools 10.0.9 以降。このバージョンは Windows 10 をサポートします

vRealize Orchestrator

vRealize Orchestrator Plugin for NSX 1.0.3 以降

VMware Integrated Openstack (VIO)

VIO 2.5.1 以降

- vCloud Director 8.0 (vCNS から NSX に移行する場合)
- vCloud Director 8.10.1 (NSX 上で稼動している場合)

システム要件とインストール

NSX のインストールの前提条件については、『NSX 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。

インストール手順については、『[NSX インストール ガイド](#)』または『[Cross-vCenter NSX インストール ガイド](#)』を参照してください。

廃止および提供を中止する機能

販売およびサポートの終了に関するご注意

ただちにアップグレードが必要な NSX およびその他の VMware 製品については、[VMware Lifecycle Product Matrix](#) (英語) を参照してください。今後サポートの終了が予定されている製品は次のとおりです。

- vCloud Networking and Security は、2016 年 9 月 19 日に提供終了日 (EOA) およびジェネラル サポートの終了日 (EOGS) を迎えました。(VMware ナレッジベースの記事 [KB2144733](#) を参照してください)
(VMware ナレッジベースの記事 [KB2144620](#) を参照してください)
- NSX for vSphere 6.1.x は、2017 年 1 月 15 日に提供終了日 (EOA) およびジェネラル サポートの終了日 (EOGS) を迎えました。(VMware ナレッジベースの記事 [KB2144769](#) を参照してください)
- NSX Data Security は、NSX 6.2.3 のリリースでは推奨されない機能です。NSX 6.2.3 では、ユーザーの判断でこの機能を引き続き使用できます。ただし、この機能は NSX の今後のリリースでは削除されることにご注意ください。
- Web Access Terminal (WAT) は廃止される予定の機能です。この機能は、今後のメンテナンス リリースには含まれません。セキュリティを強化するには、SSL VPN 環境への完全なアクセス権を持つクライアントの利用をお勧めします。
- vCloud Network and Security Edge のサポートが終了しました。NSX 6.2.9 以降にアップグレードするには、まず NSX Edge にアップグレードする必要があります。

サポートされていないコントローラ コマンドが表示されない

サポートされるコマンドの一覧については、CLI ガイドを参照してください。このガイドに記載されているコマンドのみを使用してください。join control-cluster コマンドは NSX for vSphere ではサポートされません。[VMware ナレッジベースの記事 KB2135280](#) を参照してください。

NSX 6.2.3 で TLS 1.0 のサポートが廃止に

NSX 6.2.3 では、NSX VPN、IPsec およびロード バランサ暗号化スイートでの TLS 1.0 のサポートが廃止になっています。暗号化サポートの変更については、[VMware ナレッジベースの記事 KB2147293](#) を参照してください。

アップグレードに関する注意事項

- ダウングレードはサポートされない:
 - アップグレードの前に、必ず NSX Manager をバックアップしてください。
 - NSX を正常にアップグレードしたあとは、ダウングレードすることはできません。
- NSX 6.2.4 以降にアップグレードするには、ホスト クラスタのアップグレード (ホストの VIB を 6.2.4

にアップグレード)を含む完全な NSX アップグレードを実行する必要があります。手順については、『[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](#)」のセクションを参照してください。

- 8GB 以上のメモリ要件：メモリが 8 GB 未満の場合、ホストでの NSX 6.2.3 以降へのアップグレードに失敗します。
- Edge Services Gateway (ESG) のアップグレード：

6.2.5 以降、リソース予約は NSX Edge のアップグレード時に実行されるようになりました。十分なリソースのないクラスタで vSphere HA が有効になっている場合、vSphere HA の制約に違反するためアップグレードに失敗することがあります。

そのようなアップグレードの失敗を回避するには、ESG をアップグレードする前に次の手順を実行します。

1. インストール環境が vSphere HA 向けのベスト プラクティスに従っていることを常に確認します。[ナレッジベースの記事 KB1002080](#) を参照してください。

2. NSX チューニング設定 API を使用します。

PUT <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration>

edgeVCpuReservationPercentage と edgeMemoryReservationPercentage の値が、フォーム ファクタで使用可能なリソースを超えていないことを確認します（デフォルト値は以下の表を参照）。

インストール時またはアップグレード時に値を明示的に設定していない場合は、次のリソース予約が NSX Manager で使用されます。

NSX Edge フォーム ファクタ	CPU 予約	メモリの予約
Compact	1000 MHz	512 MB
Large	2000 MHz	1024 MB
Quad Large	4000 MHz	2048 MB
X-Large	6000 MHz	8192 MB

- vSphere HA が有効で Edge を展開している環境では、vSphere の [仮想マシンの起動] オプションを無効にする：vSphere HA が有効で Edge が展開されているクラスタでは、NSX Edge の 6.2.4 以前のバージョンを 6.2.5 以降にアップグレードした後、vSphere の [仮想マシンの起動] オプションを無効にする必要があります。無効にするには、vSphere Web Client を開いて、NSX Edge 仮想マシンが配置されている ESXi ホストを検索し、[管理] をクリックします。[設定] > [仮想マシン] の順にクリックして、[仮想マシンの起動/シャットダウン] を選択します。[編集] をクリックし、仮想マシンが手動モードになっていること、すなわち、自動起動/シャットダウン リストに含まれていないことを確認します。

- NSX 6.2.5 以降にアップグレードする前に、ロード バランサの暗号化リストがコロン区切りであることを確認します。暗号化リストにカンマなど別の区切り文字が使用されている場合は、https://nsxmgr_ip/api/4.0/edges/EdgeID/loadbalancer/config/applicationprofiles への PUT 呼び出しを実行し、<clientSsl> および <serverSsl> の各 <ciphers> リストをコロン区切りのリストに置換します。たとえば、要求本文の関連セグメントは次のようになります。すべてのアプリケーション プロファイルに対して次の手順を繰り返します。

```
<applicationProfile>
```

```
  <name>https-profile</name>
```

```
  <insertXForwardedFor>>false</insertXForwardedFor>
```

```
  <sslPassthrough>>false</sslPassthrough>
```

```

<template>HTTPS</template>
<serverSslEnabled>true</serverSslEnabled>
<clientSsl>
  <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
  <clientAuth>ignore</clientAuth>
  <serviceCertificate>certificate-4</serviceCertificate>
</clientSsl>
<serverSsl>
  <ciphers>AES128-SHA:AES256-SHA:ECDHE-ECDSA-AES256-SHA</ciphers>
  <serviceCertificate>certificate-4</serviceCertificate>
</serverSsl>
...
</applicationProfile>

```

- **コントローラ ディスクのレイアウト**：NSX 6.2.3 以降の新規インストールでデプロイされる NSX Controller アプライアンスでは、ディスク パーティションを更新することにより、クラスタの回復性がさらに強化されます。以前のリリースでは、コントローラ ディスクでのログのオーバーフローがコントローラの安定性に影響する場合があります。NSX Controller アプライアンスは、オーバーフローを防止するためのログ管理機能の強化に加え、データとログに個別のディスク パーティションを使用することで、このような問題の発生を防ぎます。NSX 6.2.3 以降にアップグレードする場合、NSX Controller アプライアンスは元のディスク レイアウトを保持します。
- **アップグレード パス**：
 - NSX 6.x からのアップデート：VMware NSX のアップグレードの詳細については、[VMware 製品の相互運用性マトリクス](#)を参照してください。Cross-vCenter NSX のアップグレードについては、『[NSX アップグレード ガイド](#)』を参照してください。
 - VMware vCloud Network and Security (vCNS) 5.5.x からのアップグレード：
 - NSX アップグレード バンドルを使用すると、VMware vCloud Networking and Security (vCNS) 5.5.x から NSX 6.2.x 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 から NSX へのアップグレード](#)」を参照してください。このセクションでは、vCloud Director 環境における vCNS 5.5.x から NSX へのアップグレードの手順についても説明しています。また、『[NSX for vShield Endpoint アップグレード ガイド](#)』では、vShield Endpoint をアンチウイルス保護にのみ使用する場合の vCNS 5.5.x から NSX 6.2.x へのアップグレードの手順を説明しています。
 - 環境内で仮想ワイヤーを使用している場合は、ホスト クラスタをアップデートする必要があります。アップデートが完了すると、仮想ワイヤーが論理スイッチになります。「[ホスト クラスタのアップグレード](#)」のセクションを参照してください。
- NSX 6.2.x へのアップデートが成功したことを確認するには、[ナレッジベースの記事 KB2134525](#) を参照してください。
- **パートナー サービスとの互換性**：ゲスト イントロスペクションまたはネットワーク イントロスペクション用に VMware のパートナー サービスをサイトで使用している場合、アップグレード前に [VMware 互換性ガイド](#)を参照して、このリリースの NSX とベンダーのサービスに互換性があることを確認してください。
- **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 Manager のインストールとアップグレードに必要なメモリと CPU の要件については、NSX 6.2 ドキュメントの「[NSX のシステム要件](#)」セクションを参照してください。
- **TLS 1.0 を使用するロード バランシングされたクライアントに正しい暗号化バージョンを設定**：これは、TLS バージョン 1.0 を使用する vRealize Operations プール メンバーに影響します。トラフィックのロード バランシングを行っているサーバが本バージョンを使用する場合、NSX ロード バランサの設定で監視の拡張機能を編集し、「ssl-version=10」と明示的に指定する必要があります。『[NSX 管理ガイド](#)』を

参照してください。

```
{  
  
    "expected" : null,  
    "extension" : "ssl-version=10",  
    "send" : null,  
    "maxRetries" : 2,  
    "name" : "sm_vrops",  
    "url" : "/suite-api/api/deployment/node/status",  
    "timeout" : 5,  
    "type" : "https",  
    "receive" : null,  
    "interval" : 60,  
    "method" : "GET"  
}
```

- **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.x にアップグレードする前に、環境内のどのトンネルでも、VXLAN トンネル ID 4094 を使用していないことを確認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。ブラウザのキャッシュと履歴の消去が必要な場合もあります。
- **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。
- **ドラフトの自動保存と Service Composer** : NSX 6.2.3 以降では、`autoDraftDisabled` を `true` に設定すると、ドラフトの自動保存機能を無効にできます。アップグレードした場合、手動で行った設定は引き継がれます。ファイアウォール ルールに多数の変更を加える前にドラフトの自動保存機能を無効にすると、パフォーマンスが向上する可能性があります。また、すでに保存されているドラフトが上書きされないようにすることができます。次の API 呼び出しを使用して、`autoDraftDisabled` プロパティを `true` にグローバル構成できます。

1. ファイアウォールの既存のグローバル構成 (GlobalConfiguration) の取得

```
GET https://NSX-Manager-IP-  
Address/api/4.0/firewall/config/globalconfiguration  
GET メソッドでは、autoDraftDisabled フィールドは表示されません。
```

2. PUT API を使用してグローバル構成で `autoDraftDisabled` プロパティを `true` に設定

```
PUT https://NSX-Manager-IP-  
Address/api/4.0/firewall/config/globalconfiguration  
要求の本文に次が含まれる：
```

```
<globalConfiguration>  
  <layer3RuleOptimize>...</layer3RuleOptimize>  
  <layer2RuleOptimize>...</layer2RuleOptimize>  
  <tcpStrictOption>...</tcpStrictOption>  
  <autoDraftDisabled>true</autoDraftDisabled>  
</globalConfiguration>
```

- **ホストがインストール状態のままになることがある** : 大規模な NSX 環境のアップグレードを実行中に、ホストが長時間にわたってインストール状態のままになることがあります。これは、以前の NSX VIB のアンインストール関連の問題が原因で発生する可能性があります。このような場合、このホストに関連づけられている ESX Agent Manager (EAM) スレッドが vSphere Web Client のタスク リストにスタック状態としてレポートされます。

回避策 : vSphere Web Client を使用して vCenter Server にログインします。スタックしている EAM タスクを右クリックして、キャンセルします。vSphere Web Client から、クラスタ上で [解決] を発行します。スタックしたホストの表示が InProgress になります。ホストにログインして再起動し、ホストのアップグレードを強制的に実行します。

ドキュメントの改訂履歴

2017 年 10 月 26 日 : 初版。

2017 年 11 月 20 日 : 第 2 版。解決した問題に追加した問題 : 1486403、1944599既知の問題に追加した問題 : 1934416、1960172、1971595

2017 年 11 月 27 日 : 第 3 版。問題 1726953 を削除しました。

解決した問題

- **問題 1486403** : NSX Manager はスペース区切りのある DNS 検索文字列を受け付け
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。この問題は NSX 6.2.9 で修正されました。
- **問題 1713669** : NSX Manager のディスクが IDFW データでいっぱいになる
IDFW ルールが使用されているかどうかにかかわらず、ゲスト イントロスペクションおよびイベント ログサーバによって検出されたログイン イベントは、NSX Manager データベースに格納され、期限切れ後 30 日間にわたってデータベースに保持されます。大量のログイン アクティビティが発生する環境では、データベースのサイズが拡大し、NSX Manager のディスク容量に影響する可能性があります。この問題は NSX 6.2.9 で修正されました。
- **問題 1765744** : [適用先] フィールドにセキュリティ グループが設定されている分散ファイアウォール (DFW) ルールが新しいクラスタのホストに適用されない
環境に新しいクラスタを追加する際、NSX Manager のキャッシュが、新しいクラスタが含まれるように更新されません。[適用先] フィールドにセキュリティ グループが設定されているルールの変更が、クラスタのホストにプッシュされません。これが原因で、これらのホストにファイアウォールを適用できません。NSX Manager サービスを再起動するとキャッシュがクリアされ、以降の更新は既存のすべてのクラスタにプッシュされます。この問題は NSX 6.2.9 で修正されました。

回避策 :

既存の環境を NSX 6.2.4 以降のリリースにアップグレードする場合は次の手順を実行します。

1. NSX Manager サービスを再起動します。
2. ファイアウォールのユーザー インターフェイスで、2 つの異なるセクションにある 1 つのルールを変更し、発行します。不明になっているすべてのルールが ESXi ホストにプッシュされます。

この回避策は、NSX for vSphere 6.2.4 以降のリリースにアップグレードする場合に適用できます。この回避策を適用するまで、新しいクラスタを追加したときに同じ問題が発生します。

- **問題 1770436** : 重複する IP アドレスが存在していない場合でもアラートが生成される
`arping` コマンドを実行すると、実際には重複していないにもかかわらず、ネットワーク内で NSX Manager の IP アドレスが重複しているとレポートされることがあります。これにより、誤検知のイベントが生成されます。この問題は NSX 6.2.9 で修正されました。
- **問題 1806368** : Cross-vCenter Server フェイルオーバー環境で、以前に障害が発生し、フェイルオーバー後に再度プライマリに昇格した NSX Manager が古いコントローラを再利用していると、一部のホストに分散論理ルーターの設定がプッシュされない
Cross-vCenter Server 環境では、プライマリ NSX Manager に障害が発生すると、セカンダリ NSX Manager がプライマリに昇格し、新しいプライマリ NSX Manager で使用するための新しいコントローラ クラスタがデプロイされます。障害の起きたプライマリ NSX Manager がオンラインに戻ると、現在のプライマリ NSX Manager がセカンダリに降格し、元のプライマリ NSX Manager がリストアされます。このとき、リストアされたプライマリ NSX Manager で、フェイルオーバー前にデプロイされていたコントローラを使用すると、一部のホストに分散論理ルーターの設定がプッシュされません。リストアされた NSX Manager 用に新しいコントローラ クラスタを作成する場合、この問題は発生しません。

回避策 : リストアしたプライマリ NSX Manager に新しいコントローラ クラスタをデプロイします。

- **問題 1826225** : パートナー サービス仮想マシンのサービス ステータスが、NSX Manager に「不明」としてレポートされる
パートナー サービス仮想マシンのサービス ステータスが、NSX Manager に「不明」としてレポートされます。この問題は、パートナー仮想マシンに関する古いデータベース エントリがあると発生します。この問題は NSX 6.2.9 で修正されました。
- **問題 1851833** : バックエンドで、NULL と設定されたオブジェクト名が渡される

バックエンドで、NULL と設定されたオブジェクト名が渡されます。ユーザー インターフェイスで NULL が確認され、NULL ではなく、その時点の最新のオブジェクトが表示されます。この問題は NSX 6.2.9 で修正されました。

- **問題 1874735:** クラスタにアラームがあると「アップグレードを利用可能」リンクが表示されない
リンクが表示されない場合は、新しいサービスの仕様を ESX Agent Manager にプッシュできないため、サービスをアップグレードすることはできません。この問題は NSX 6.2.9 で修正されました。
- **問題 1882534:** ESG システム イベントの更新で最初の 1,024 個のイベントが表示され、新しいイベントは表示されない
Edge をダブルクリックした後、[監視] > [システム イベント] の順に選択すると、1,024 個のレコードしか表示されません。この問題は NSX 6.2.9 で修正されました。
- **問題 1886469:** コントローラとの接続の問題
コントローラが SSL ハンドシェイク応答を返さず、非アクティブな状態であるかを確認する NSX Manager のスレッドが無期限に待機する場合があります。これが原因でコントローラとの接続が失われます。この問題は NSX 6.2.9 で修正されました。
- **問題 1891756:** OpenSSH 7.x を使用したバックアップ/リストアのサポート
OpenSSH 7.2 SFTP サーバを使用したバックアップに失敗し、エラーが発生します。この問題は NSX 6.2.9 で修正されました。
- **問題 1894906:** ホストがメモリ不足になるため、フィルタを 1,000 個まで作成できない
dvfilter の上限設定を 2048 に増やしたにも関わらず、実際はフィルタを 1,000 個まで作成できません。この問題は NSX 6.2.9 で修正されました。
- **問題 1901448:** ESXi ホストに完全な VNI の VTEP リストがないため、East-West 接続で問題が発生する
コントローラ クラスタにシャーディングの変更があり、新しいコントローラ ノードでステータスが同期されたあとに表示されるセッション メッセージよりもレガシーのマスター コントローラのメッセージ処理が遅い場合にのみ、競合状態が発生します。これが原因で、該当する VNI のコントローラ間で変更が同期されません。この問題は NSX 6.2.9 で修正されました。
- **問題 1904842:** NSX Manager が vCenter Server または Platform Service Controller に登録されない
NSX Manager がユーザー インターフェイスに表示されず、NSX Manager への REST 呼び出しが失敗します。この問題は NSX 6.2.9 で修正されました。
- **問題 1913609:** SSLVPN サービス ログ レベルがデバッグに設定されていると、Web ベースのクライアント認証の際、NSX Edge ログに SSLVPN ユーザー パスワードがプレーン テキストで表示される
ユーザーが Web クライアント経由で SSLVPN サーバの認証を行うと、Active Directory/LDAP ユーザー認証情報が NSX Edge ログにプレーン テキストで保存されます。この問題は NSX 6.2.9 で修正されました。
- **問題 1915246:** Edge から送信され VPN トンネルを通過するトラフィックの ping/Syslog が機能しない
トラフィックが Edge から送信され、ピア サブネットの VPN トンネルを通過する場合、トラフィックが送信されません。Syslog サーバが VPN 経由のピア サブネットに配置されていると、Syslog に影響します。この問題は NSX 6.2.9 で修正されました。
- **問題 1920343:** プライベート キーなしでサーバ証明書が作成される
証明書のコンテンツにプライベート キーのデータが含まれていても、そのプライベート キーが無視されます。この問題は NSX 6.2.9 で修正されました。
- **問題 1920863:** vRealize Operations が誤って Edge 高可用性サービスの停止をレポートする
Edge 高可用性サービスが実行中でも、Edge が NSX Manager に誤ったステータス（高可用性サービスの停止）をレポートします。同じ内容が vRealize Operations にもレポートされ、アラートがトリガされます。この問題は NSX 6.2.9 で修正されました。

- **問題 1926668**：分散ファイアウォール フィルタで、分散ファイアウォール ルールが部分的に処理される場合がある
トラフィックを許可またはブロックするファイアウォール ルールが想定どおりに機能しない場合があります。この問題は NSX 6.2.9 で修正されました。
- **問題 1927739**：監査ロールのユーザーがクラスタ レベルで分散ファイアウォールを無効または有効にできてしまう
分散ファイアウォールを有効または無効にする権限は、監査ロールのユーザーに付与されるべきではありません。この問題は NSX 6.2.9 で修正されました。
- **問題 1928916**：コンマ区切りを使用して複数のドメインを追加すると DNS 検索の設定に失敗する
NSX Manager に複数のドメイン検索サフィックスを追加する場合、NSX Manager のユーザー インターフェイスでは、コンマを使用してドメインを区切る必要があります。しかし、この操作を行ってもドメインが検索できず、すべての接続で IP アドレスまたは FQDN を使用する必要があります。これは、`/etc/resolv.conf` 内の形式の問題です。この問題は NSX 6.2.9 で修正されました。
- **問題 1931552**：分散論理ルーターで ARP の解決に 1 秒～ 1.5 秒かかる
ARP 抑制に失敗すると、ローカルの分散論理ルーターによるリモート ホストの仮想マシンの ARP 解決に 1 秒～ 1.5 秒かかります。この問題は NSX 6.2.9 で修正されました。

詳細については、[VMware のナレッジベースの記事 KB2151374](#) を参照してください。
- **問題 1934088**：ESXi の `hostd` プロセスが停止すると、NSX Manager の CPU 使用率が高くなる
ESXi の `hostd` プロセスが停止すると、NSX Manager の `VirtualMachineDvFilterMonitor` スレッドがホストへの仮想マシン フィルタ リストの送信を繰り返します。これにより、作業キュー内のタスクが増加し、CPU の使用率が高くなります。この問題は NSX 6.2.9 で修正されました。
- **問題 1934354**：ARP 要求を送信して ARP エントリを更新するときに、GARP を有効な応答として受け入れない
一部の古いデバイスは、ARP 要求の応答として GARP を送信します。今後 GARP は、有効な応答として受け入れられるようになります。この問題は NSX 6.2.9 で修正されました。
- **問題 1941004**：ポートの VNI の無効な更新により ESXi ホストで PSOD（パープル スクリーン）が発生する
ポートの VNI の無効な更新により ESXi ホストで PSOD（パープル スクリーン）が発生します。この問題は NSX 6.2.9 で修正されました。
- **問題 1944599**：変換された IP アドレスが vNIC フィルタに追加されないため、分散ファイアウォールがトラフィックをドロップする
新しい仮想マシンをデプロイする際、vNIC フィルタが正しい IP アドレスで更新されないため、分散ファイアウォールがトラフィックをブロックします。この問題は NSX 6.2.9 で修正されました。
- **問題 1950663**：仮想マシンを NSX 6.0.x から移行すると、ホストで PSOD（パープル スクリーン）が発生する場合がある
クラスタを NSX 6.0.x から 6.2.3 ～6.2.8 にアップデートすると、エクスポートした仮想マシンが破損し、受信側のホストで PSOD（パープル スクリーン）が発生する場合があります。この問題は NSX 6.2.9 で修正されました。
- **問題 1956165**：NSX GUI ですべてのハードウェア VTEP が停止と表示される
ハードウェア VTEP が停止とマークされ、ハードウェア VTEP を使用するトラフィックがすべて切断されます。この問題は NSX 6.2.9 で修正されました。
- **問題 1966308**：ピア エンドの IP アドレスが繰り返し変更されると、Edge IPsec VPN が停止する

この問題は、VPN ピアの IP アドレスが繰り返し変更される環境（3G ドングル/動的 WAN IP アドレス）で発生します。ピア IP アドレスが変更されると、トンネルが停止し、ピア サブネットのルートが正しくフラッシュされません。このため、トンネルの再ネゴシエーション時に Edge で IPsec SA のインストールに失敗します。この問題は NSX 6.2.9 で修正されました。

- **問題 1981372**：SSL VPN クライアントが IP アドレス プールから IP アドレスを取得できない
IP アドレスが IP アドレス プールから 割り当てられていないため、クライアントはプライベート ネットワークに接続できません。IP アドレス プールの IP アドレスは自動再接続によって使用されます。この問題は NSX 6.2.9 で修正されました。

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](#)
- [ソリューションの相互運用性に関する既知の問題](#)
- [NSX Controller に関する既知の問題](#)

一般的な既知の問題

- **問題 1659043**：NSX Manager からユニバーサル サービス仮想マシン（USVM）への通信がタイムアウトすると、ゲスト イントロスペクションのサービス ステータスに「Not Ready」と表示される
内部のメッセージ バス (rabbit MQ) 上で NSX Manager によるパスワードの変更プロセスが正常に完了しなかった場合、ゲスト イントロスペクション USVM に対して、「PLAIN login refused: user 'usvm-admin-host-14' - invalid credentials」のようなエラー メッセージが表示される場合があります。

回避策：USVM と NSX Manager を再接続するには、USVM を再起動するか、手動で削除してから、Service Composer のユーザー インターフェイスで [解決] ボタンを選択して、影響を受けたホストにのみ USVM を再デプロイするプロンプトを表示します。

- **問題 1558285**：ゲスト イントロスペクションを利用しているクラスタを vCenter Server で削除すると、Null ポインタ例外が発生する
vCenter Server からクラスタを削除する前に、ゲスト イントロスペクションなどのサービスを削除する必要があります。
回避策：クラスタに関連付けられていないサービスの EAM エージェントを削除します。
- **問題 1629030**：パケット キャプチャのセントラル CLI（パケット キャプチャのデバッグと表示用コマンド）は vSphere 5.5U3 以降でサポートされる
これらのコマンドは、vSphere 5.5 より前のバージョンではサポートされません。
回避策：NSX をご利用になる場合は、vSphere 5.5U3 以降を導入することをお勧めします。

- **問題 1568180**：vCenter Server Appliance (vCSA) 5.5 を使用する場合、NSX の機能リストが正しく表示されない
vSphere Web Client のライセンスの機能を表示するには、ライセンスを選択して [操作] > [機能の表示] の順にクリックします。NSX 6.2.3 にアップグレードする場合、Enterprise ライセンスにアップグレードされ、すべての機能が有効になります。しかし、NSX Manager が vCenter Server Appliance (vCSA) 5.5 に登録されている場合、[機能の表示] を選択すると、新しい Enterprise ライセンスではなく、アップグレード前に使用されていたライセンスの機能が一覧表示されます。
回避策：vSphere Web Client に正しく表示されない場合でも、すべての Enterprise ライセンスでは同じ機能を利用できます。詳細については、[NSX ライセンス ページ](#)を参照してください。

- **問題 1477280**：コントローラがデプロイされていない場合、ハードウェア ゲートウェイ インスタンスを作成できない

ハードウェア ゲートウェイ インスタンスを設定する前に、コントローラをデプロイする必要があります。コントローラを先にデプロイしない場合には、「コントローラ上での操作に失敗しました」というメッセージが表示されます。

回避策：なし。

- **問題 1971684**：1 台の ESX ホストで VTEP の作成に失敗する
一度に 250 台のハイパーバイザーのホストの準備を行うと、1 ～2 台のホストで VTEP の作成に失敗します。

回避策：

1. 該当する ESXi ホストをメンテナンス モードに切り替えます。
2. NSX を使用するクラスタから ESXi ホストを削除します。
3. ホストを再起動します。
4. 再起動後も ESXi ホストに VTEP VMkernel インターフェイスが残っている場合は、ホスト ネットワークの VMkernel インターフェイス構成から手動で削除します。
5. ESXi ホストを NSX クラスタに戻し、NSX を準備します。

- **問題 1960172**：タグ付きの分散ファイアウォール ルールが Edge (ESG) に適用されない
ルール タグ付きのルールを作成し、すべての Edge または個別の Edge に適用すると、「ルール タグは、分散ファイアウォールに適用されるルールにのみ使用できます」というエラーが発生し、発行操作が失敗します。分散ファイアウォール/セキュリティ グループ/個別の Edge などの複数のオブジェクトがあるときに、適用先に「個別の Edge のみ」または「すべての Edge」を設定すると、Edge でルール タグが使用されていなくても、ルールの発行に成功します。

回避策：回避策はありません。Edge に適用されるルールにルール タグを使用しないでください。

インストールとアップグレードに関する既知の問題

- **問題 1905064**：ホストのアップグレードにおいて、クラスタ内の一部のホストで NSX Manager およびコントローラへの TCP 接続が失われる
アップグレードで、ESXi ホスト上での NSX Manager への TCP 接続が失われると、コントローラの情報取得できなくなります。これにより、コントローラが NSX 関連の設定をこのホストにプッシュできなくなり、このホスト上のすべての仮想マシンの接続が失われます。

回避策：問題のあるホストを再起動します。

- **問題 1910593**：API を使用して NSX Manager をアップグレードするときに、応答パラメータで大文字と小文字が区別される
NSX Manager のアップグレードに NSX API を使用した場合、SSH を有効にする際、または VMware のカスタマー エクスペリエンス向上プログラムに参加する際に、パラメータとして「YES」ではなく「Yes」を指定しなければなりません。

回避策：API を使用してアップグレードを行う場合の詳細については、『NSX API ガイド』を参照してください。

- **問題 1838229**：NSX 6.1.5 以降にアップグレードした後、NSX ロード バランサで HTTP/HTTPS トランザクションが失敗する
NSX 6.1.5 以降で x-forwarded-for を有効にすると、HTTP 接続モードがパッシブ クローズ (option httpclose) からデフォルトの HTTP サーバクローズ (option http-server-close) に変わり、サーバから応答を受信した後でサーバ方向の接続を閉じて、クライアント方向の接続が開いたままになります。NSX 6.1.5 より前のバージョンでは、ロード バランサが接続をプロアクティブに終了せず、両方に

"Connection:close" ヘッダーを挿入してクライアントまたはサーバに接続の終了を示すため、一部のアプリケーションで問題が発生しています。

回避策：option httpclose スクリプトを含むアプリケーション ルールを追加して、仮想サーバに関連付けてください。

- **問題 1820723**: NSX 6.2.x から 6.2.7 へのアップグレード後にホストへ接続できなくなり、ESXi でフィルタが表示されなくなる

NSX 6.2.x から 6.2.7 へアップグレードし、クラスタ VIB を 6.2.7 へアップグレードすると、インストールステータスが「成功」と表示されます。しかし、ファイアウォールが有効と表示されている場合でも、[通信チャネルの健全性]を確認すると、NSX Manager からファイアウォール エージェントへの接続と NSX Manager から制御プレーン エージェントへの接続がダウンしている则表示されます。このため、ファイアウォール ルールとセキュリティ ポリシーの発行に失敗し、VXLAN 設定がホストに送信されなくなります。

回避策：API の POST `https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize` を使用して、クラスタに対し、メッセージ バス同期 API 呼び出しを実行します。

API の本文：

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>{Cluster-MOId}</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

- **問題 1435504**: NSX 6.0.x または 6.1.x から 6.2.x にアップグレードした後、HTTP または HTTPS の健全性チェックが DOWN となり、その理由として「Return code of 127 is out of bounds - plugin may be missing」と表示される

NSX 6.0.x および 6.1.x リリースでは、二重引用符 (") を付けずに URL を設定すると、健全性チェックが失敗して次のエラーが発生していました。「Return code of 127 is out of bounds - plugin may be missing」この問題の回避策は、URL の入力値に二重引用符 (") を追加することでした（送信、受信、期待値のフィールドでは不要）。この問題は NSX 6.2.0 で解決されました。その結果、6.0.x または 6.1.x から 6.2.x にアップグレードすると、URL に二重引用符が追加されていた場合、健全性チェックでプール メンバーが DOWN として表示されます。

回避策：アップグレード後に、健全性チェックに関するすべての設定で、URL のフィールドから二重引用符 (") を削除します。

- **問題 1768144**：以前のバージョンの NSX Edge アプライアンスで設定されたリソース予約が新しい上限を上回ると、アップグレードまたは再デプロイに失敗することがある

NSX 6.2.4 以前では、1 台の NSX Edge アプライアンスに任意の大きなリソース予約を設定でき、NSX には最大値の設定がありませんでした。NSX Manager を 6.2.5 以降にアップグレードすると、フォーム ファクタごとに最大値が新しく設定されます。既存の Edge にその最大値を上回るリソース予約（特にメモリ）が設定されていると、Edge のアップグレードまたは再デプロイ（アップグレードをトリガする）に失敗します。たとえば、NSX 6.2.5 以前の「Large」サイズの Edge にユーザーが 1,000 MB のメモリ予約を設定した場合、NSX 6.2.5 以降にアップグレードしてからアプライアンスのサイズを「Compact」に変更すると、ユーザーが指定したメモリ予約が新しく設定される最大値（「Compact」サイズでは 512 MB）を上回るため、アップグレードまたは再デプロイに失敗します。

NSX 6.2.5 以降で推奨されるリソース割り当てについては、「[Edge Service Gateway \(ESG\) のアップグレード](#)」を参照してください。

回避策：NSX Edge アプライアンスの REST API：PUT

`https://<NSXManager>/api/4.0/edges/<edge-Id>/appliances/` を使用して、フォーム ファクタごとに指定される最大値を上回らないようにメモリ予約を再設定します。アプライアンスにその他の変更を加える必要はありません。この操作が完了したら、アプライアンスのサイズを変更します。

- **問題 1730017**：NSX 6.2.3 から 6.2.7 にアップグレードすると、ゲスト イントロスペクションのバージョンが変更されたことが表示されない

NSX 6.2.3 のゲスト イントロスペクション モジュールには最新バージョンが使用されますが、6.2.7 へアップグレードしてもバージョンは変更されません。以前の NSX リリースからのアップグレードでは、NSX 6.2.7 へのバージョン変更が示される場合があります。

回避策：これは機能には影響しません。

- **問題 1683879**：メモリが 8 GB 未満の場合、NSX 6.2.3 以降へのホストのアップグレードに失敗する

NSX 6.2.3 以降では、ネットワークとセキュリティのサービスを実行するホストに 8 GB 以上のメモリが必要です。ESXi 6.0 のメモリの最小要件は 4 GB ですが、これは NSX を実行するには十分ではありません。

回避策：なし。

- **問題 1673626**：vCloud Networking and Security を NSX にアップグレードした後、`/api/3.0/edges` 経由の `tcpLoose` の変更が許可されない

vCloud Networking and Security を NSX にアップグレードしたあとで、API リクエスト `/api/3.0/edges` で `tcpLoose` 設定を変更しようとすると、エラーが表示されます。

回避策：代わりに、API リクエスト `/api/4.0/firewall/config` の `globalConfig` セクションの `tcpPickOngoingConnections` 設定を使用します。

- **問題 1658720**：vCloud Networking and Security (vCNS) から NSX へのアップグレードの際、vCNS 環境のクラスタに VXLAN がインストールされており、vShield App がインストールされていない（またはアップグレード前に削除されている）場合は、クラスタで分散ファイアウォール (DFW) を有効にしようとすると失敗する

この問題は、ホストのアップグレード時にクラスタの同期ステータスが呼び出されないために発生します。

回避策：NSX Manager を再起動します。

- **問題 1569010/1645525**：vCenter Server 5.5 に接続したシステムで、NSX for vSphere 6.1.x から 6.2.3 へアップデートすると、[ライセンス キーの割り当て] ウィンドウの [製品] フィールドに、「NSX for vSphere - Enterprise」などの具体的な NSX ライセンス名ではなく、総称の「NSX for vSphere」と表示される

回避策：なし。

- **問題 1465249**：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。

- **問題 1660355**：NSX 6.1.5 から 6.2.3 に移行した仮想マシンで TFTP ALG がサポートされない
ホストで TFTP ALG が有効な場合でも、6.1.5 から 6.2.3 に移行した仮想マシンでは TFTP ALG がサポートされません。

回避策：仮想マシンを除外リストに一度追加して削除するか、または仮想マシンを再起動します。これによって、新しい 6.2.3 フィルタが作成され、TFTP ALG がサポートされるようになります。

- **問題 1394287**：仮想ワイヤーから仮想マシンを追加または削除しても、vShield App ルールに設定

された IP アドレスが更新されない

拡張モードにおいて、既存の vCNS vShield App ファイアウォールを NSX 分散ファイアウォールにアップグレードしない場合、仮想ワイヤー ベースのファイアウォール ルールを使用する新しい仮想マシンの IP アドレスは更新されません。このため、仮想マシンは NSX ファイアウォールで保護されません。この問題が発生するのは、

- vCNS から NSX Manager にアップグレードした後に、分散ファイアウォール (DFW) 拡張モードに切り替えていない場合のみです。
- vShield App ルールを使用する VirtualWire に新しい仮想マシンを追加して、これらの VirtualWire を使用している場合、vShield App ルールに新しい仮想マシン用の新しい IP アドレスが設定されません。

このため、新しい仮想マシンは vShield App で保護されません。

回避策： ルールをもう一度発行すると、新しいアドレスが設定されます。

● 問題 1386874：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。

● 問題 1375794: 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。

● 問題 1112628: 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、仮想マシンのクローン作成や再設定などの進行中のタスクが表示されない
- 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
```

- 問題 1288506：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。
- 問題 1263858: 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。
- 問題 1402307：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。
- 問題 1491820：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。
- 問題 1284735：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。
- 問題 1495969：vCloud Networking and Security 5.5.4 から NSX 6.2.x へとアップグレードした後、[ホストの準備] タブで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.x へアップグレードし、すべてのクラスタをアップグレードした後、[ホストの準備] タブで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に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。
- 問題 1474066：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。

- **問題 1434909：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。

- **問題 1459032：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。

- **問題 1463767：Cross-vCenter Server 環境で、ユニバーサル ファイアウォール構成セクションが**

ローカル構成セクションの下位に（従属的に）置かれる場合がある

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。

- **問題 1289348**： 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 イントロセクション 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。
- **問題 1462319**： 「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。
NSX 6.2.3 以降では、esx-vsip および esx-vxlan の NSX VIB とともに、3 つめの VIB として esx-vmtoolsd が提供されます。インストールに成功すると 3 つすべての VIB が表示されます。
回避策： なし。
- **問題 1481083**： 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。
- **問題 1485862**： 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]）。
- **問題 1411275**： NSX for vSphere 6.2 でのバックアップとリストア後、vSphere Web Client で [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。
- **問題 1393889**： 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働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。

- [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。

- 問題 1764460：ホストの準備の完了後、クラスタのすべてのメンバーが [準備完了] 状態と表示されるが、クラスタ レベルが [無効] と誤って表示される

ホストの準備が完了すると、クラスタのすべてのメンバーの状態が [準備完了] と正しく表示されますが、クラスタ レベルは [無効] と表示されます。その理由として、ホストの再起動が必要だと表示されますが、ホストはすでに再起動されています。

回避策：赤い警告アイコンをクリックして、[解決済み] を選択します。

- 問題 1967503：Edge/分散論理ルーターのアップグレード中に vShield Manager サービスを再起動すると、Edge/分散論理ルーターの情報が正しく同期されない場合がある

Edge/分散論理ルーターのアップグレード中に vShield Manager サービスを再起動すると、アップグレードが再開されません。このため、アップグレードが部分的に完了し、Edge/分散論理ルーターの情報が正しく同期されません。

回避策：Edge/分散論理ルーターのアップグレード中に vShield Manager サービスを再起動した場合は、Edge/分散論理ルーターを再デプロイし、コントローラのアップデートを行います。必要であれば、Edge/分散論理ルーターのステータスと情報を再度同期します。

NSX Manager に関する既知の問題

- 問題 1831131: LocalOS ユーザーで認証を行うと、NSX Manager から SSO への接続が失敗する
LocalOS ユーザーで認証を行うと、次のエラーが発生し、NSX Manager から SSO への接続に失敗します。
「NSX Manager との通信を確立できませんでした。管理者に連絡してください。」

回避策：エンタープライズ管理者ロールを nsxmanager@localos と nsxmanager@domain に追加してください。

- 問題 1772911：NSX Manager のディスク容量が急速に増え、タスクおよびジョブ テーブルのサイズが大きくなり CPU 使用率が高くなる

NSX Manager CPU は常に 100% になるか、頻繁に 100% にまで急増します。NSX Manager コマンドライン インターフェイス (CLI) で show process monitor コマンドを実行すると、Java プロセスが最も高い CPU サイクルを使用しています。ディスク容量が急速に増えて DB のサイズが大きくなり、NSX Manager のパフォーマンスが低下します。

回避策：VMware テクニカル サポートにお問い合わせください。

- 問題 1441874：リンク モードで vCenter Server を使用している環境で単一の NSX Manager をアップグレードするとエラー メッセージが表示される

複数の NSX Manager を含む複数の VMware vCenter Server がある環境で、[vSphere Web Client] > [Networking and Security] > [インストール手順] > [ホストの準備] の順にクリックし、1 台以上の NSX Manager を選択すると、次のエラーが表示されます。

「NSX Manager との通信を確立できませんでした。管理者に連絡してください。」

回避策：詳細については、[VMware のナレッジベースの記事 KB2127061](#) を参照してください。

- 問題 1696750 : PUT API を介して NSX Manager に割り当てた IPv6 アドレスを有効にするには、再起動が必要となる

NSX Manager のネットワーク設定を `https://{NSX Manager IP address}/api/1.0/appliance-management/system/network` を介して変更する場合、変更を有効にするにはシステムの再起動が必要です。再起動するまでは変更前の設定が表示されます。

回避策 : なし。

- 問題 1671067 : NSX プラグインと ESXTOP プラグインと一緒にインストールされている場合、vCenter Web Client に NSX プラグインが表示されない

NSX をデプロイして vCenter Server に登録した後、NSX プラグインが vCenter Web Client に表示されません。この問題は、NSX プラグインと ESXTOP プラグイン間の競合が原因で発生します。

回避策 : 次の手順で ESXTOP プラグインを削除します。

1. vCenter Server 仮想マシンのスナップショット（休止なし）の最新のバックアップがあることを確認します。
2. 次のように指定して、`/usr/lib/vmware-vmware-client/plugin-packages/esxtop-plugin` を削除します。
`rm -R /usr/lib/vmware-vmware-client/plugin-packages/esxtop-plugin`
3. 次のように指定して、`/usr/lib/vmware-vmware-client/server/work` を削除します。
`rm -R /usr/lib/vmware-vmware-client/server/work`
4. Web Client を再起動します。
`service vmware-client restart`
5. （オプション）`tail -f /var/log/vmware/vsphere-client/logs/eventlog.log | grep esx` コマンドからの出力がないことを確認します。
6. ロールバック オプションとして vCenter Server スナップショットの統合を選択する場合は、これを実行します。

- 問題 1529178 : 共通名を含まないサーバ証明書をアップロードすると、「内部サーバエラー」のメッセージが返される

共通名を含まないサーバ証明書をアップロードすると、「内部サーバエラー」のメッセージが表示されます。

回避策 : サブジェクト代替名と共通名の両方、または少なくとも共通名を含むサーバ証明書を使用します。

- 問題 1655388 : 日本語、中国語、およびドイツ語版 Windows 10 OS 上で IE11/Edge ブラウザを使用すると、NSX Manager 6.2.3 のユーザー インターフェイスがローカル言語ではなく英語で表示される

日本語、中国語、およびドイツ語版 Windows 10 OS 上で IE11/Edge ブラウザを使用して NSX Manager 6.2.3 を起動すると、英語で表示されます。

回避策 :

次の手順を実行してください。

1. Microsoft のレジストリ エディター (`regedit.exe`) を起動して、[コンピューター] > [HKEY_CURRENT_USER] > [SOFTWARE] > [Microsoft] > [Internet Explorer] > [International] の順に移動します。
2. `AcceptLanguage` ファイルの値をネイティブ言語に変更します。たとえば、言語をドイツ語で表示する場合、値を `DE` に変更して最初に表示されるようにします。
3. ブラウザを再起動し、NSX Manager にもう一度ログインします。これで、言語が正しく表示されるようになります。

- 問題 1435996 : 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 CSV 形式でログファイルを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ます。

回避策： なし。

- **問題 1644297：プライマリ NSX で分散ファイアウォール (DFW) セクションの追加/削除操作を実行すると、セカンダリ NSX に 2 つの分散ファイアウォール設定が保存される**
Cross-vCenter のセットアップで、ユニバーサルまたはローカルの分散ファイアウォール (DFW) セクションがプライマリ NSX Manager に追加されると、2 つの分散ファイアウォール設定がセカンダリ NSX Manager に保存されます。この問題によって影響を受ける機能はありませんが、想定より早く保存可能な設定数の上限に達してしまい、重要な設定が上書きされてしまう可能性があります。
回避策： なし。
- **問題 1534606：[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。
- **問題 1386874：[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。
- **問題：1027066: NSX Manager の vMotion 時に「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とがある**
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。
- **問題 1477041：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。
- **問題 1460766: 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 インターフェイスを自動的にログアウトしない**
NSX Manager へのログイン中に、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ることがあります。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。
- **問題 1467382: 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。

- 問題 1436953：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。

- 問題 1489768：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。

- 問題 1971595: Cross-vCenter 環境で、セカンダリ NSX Manager でユニバーサル論理スイッチの作成が 30 秒ほど遅延する場合がある

セカンダリ NSX Manager で、新規に作成したユニバーサル論理スイッチに仮想マシンを接続しようとする
と、「ユニバーサル論理スイッチが存在しません」というエラーが発生し、接続に失敗する場合があります。

回避策：セカンダリ NSX Manager の論理スイッチを使用する前に、30 秒ほど待機してください。

論理ネットワークと NSX Edge に関する既知の問題

- 問題 1878081：Edge Services Gateway のフォワーディング テーブルから一部のルーターがフラッシュされる

まれに、一部のルーターがフォワーディング テーブルからフラッシュされる場合があります。これがトラフィック障害につながります。

回避策：Edge ノードを再起動してください。

- 問題 1798847：Cross-vCenter Server NSX 環境で VXLAN UDP ポートの更新が完了しないことがある

プライマリ NSX Manager にセカンダリ NSX Manager が設定されていないと、VXLAN UDP ポートの更新が完了しません。

回避策：NSX Manager API を使用して、プライマリ NSX Manager 上でポート更新のワークフローを再開します。

- 問題 1698286: Cross-vCenter NSX 環境では、ハードウェア VTEP はプライマリ NSX Manager でのみサポートされる

Cross-vCenter NSX 環境では、ハードウェア ゲートウェイ スイッチの設定と運用はプライマリ NSX Manager でのみサポートされます。ハードウェア ゲートウェイ スイッチは、論理スイッチにバインドしている必

要があります。ハードウェア ゲートウェイ設定は、セカンダリ NSX Manager でサポートされていません。

回避策：Cross-vCenter NSX 環境では、NSX Edge による L2 プリッジを使用して論理スイッチを物理ネットワークに接続することをお勧めします。

- **問題 1844966: NSX Edge ファイル システムが読み取り専用になる**

Edge が配置されている場所にストレージ接続の問題があると、OS ファイル システムを保護するために Edge ファイル システムが読み取り専用モードになる場合があります。これは、Linux サーバでは想定される動作です。詳細については、[VMware のナレッジベースの記事 KB2146870](#) を参照してください。

回避策：次の手順を実行します。

1. Edge を再デプロイします。
2. 高可用性構成の 2 台の Edge を再起動します。
3. Edge を強制的に同期します。

- **問題 1799261: NSX Edge が、アップグレードまたは再デプロイ後にスプリット ブレイン状態になることがある**

スタンバイ NSX Edge で、show service highavailability CLI コマンドを使用すると高可用性のステータスが「Standby」と表示されますが、構成エンジンのステータスは「Active」と表示されます。

回避策：スタンバイ NSX Edge を再起動してください。

- **問題 1777792：「ANY」として設定されたピア エンドポイントによって IPsec 接続が失敗する**
NSX Edge の IPsec 設定がリモートのピア エンドポイントを「ANY」に設定すると、Edge は IPsec の「サーバ」として動作し、リモート ピアが接続の開始するまで待機します。ただし、イニシエータが PSK と XAUTH を使用した認証要求を送信すると、Edge に「最初のメイン モード メッセージを XXX.XXX.XX.XX:500 で受信しましたが、接続が policy=PSK+XAUTH で認証されていません」というエラーメッセージが表示され、IPsec を確立することができません。

回避策：IPsec VPN 設定で ANY ではなく、特定のピア エンドポイント IP アドレスまたは完全修飾ドメイン名 (FQDN) を使用してください。

- **問題 1741158：未設定の新しい NSX Edge を作成して設定を適用すると、準備ができていない Edge サービスが有効になることがある**

NSX API を使用して新しい未設定の NSX Edge を作成し、API 呼び出しによってその Edge の Edge サービスの 1 つを無効にした（たとえば dhcp-enabled を「false」に変更した）場合、無効にした Edge サービスの設定を変更すると、そのサービスがただちに有効になります。

回避策：無効のままにしておきたい Edge サービスの設定を変更したら、すぐに PUT API を使用してそのサービスの有効フラグを「false」に設定します。

- **問題 1758500：複数のネクスト ホップがあるスタティック ルートは、設定されているネクスト ホップの 1 つ以上が Edge の vNIC の IP アドレスである場合、NSX Edge のルーティング テーブルとフォワーディング テーブルに含まれない**

ECMP が有効で、ネクスト ホップのアドレスが複数ある場合、少なくとも 1 つのネクスト ホップ IP アドレスが有効であれば、NSX は Edge の vNIC の IP アドレスをネクスト ホップとして設定することを許可してしまいます。このように設定してもエラーや警告は発生しませんが、そのネットワークのルートは Edge のルーティング テーブルとフォワーディング テーブルから削除されます。

回避策：ECMP を使用する場合、Edge 自身の vNIC の IP アドレスをスタティック ルートのネクスト ホップとして設定しないでください。

- **問題 1733165：IPsec によって、NSX Edge のフォワーディング テーブルから動的ルーティングが削除されることがある**

動的ルーティングでアクセスできるサブネットが IPsec 設定のリモート サブネットとして使用されている場合、NSX Edge はそのサブネットをフォワーディング テーブルから削除します。また、そのサブネット

が IPsec 設定から削除されても、フォワーディング テーブルに再度追加されることはありません。

回避策：ルーティング プロトコルをいったん有効にして無効にするか、ルーティングの隣接関係を消去します。

- **問題 1675659：**OSPF ダイナミック ルートよりフローティング スタティック ルートが選択される
OSPF ルートが使用可能な場合でもルート再配分が有効な場合、バックアップ フローティング スタティック ルートが Edge のルーティング テーブルに誤って入力されます。

回避策：この問題を回避するには、OSPF へのスタティックのルート再配分を無効にします。

注：この問題は、データ パスに影響しません。[VMware ナレッジベースの記事 KB2147998](#) を参照してください。

- **問題 1716464：**NSX ロード バランサがセキュリティ タグで新規にタグ付けされた仮想マシンにルーティングしない
2 台の仮想マシンを指定タグで展開し、ロード バランサがそのタグにルーティングするように設定すると、ロード バランサはこれらの 2 台の仮想マシンに正常にルーティングします。しかし、そのタグで 3 台目の仮想マシンを展開すると、ロード バランサは最初の 2 台の仮想マシンにのみルーティングします。**回避策：**ロード バランサ プールで [保存] をクリックします。これにより仮想マシンが再スキャンされ、新規にタグ付けされた仮想マシンへのルーティングを開始します。
- **問題 1776073：**プライベート ローカル AS を含む Edge が EBGP ピアへのルートを送信すると、送信された BGP ルーティング更新からすべてのプライベート AS パスが削除される
NSX には現在、AS パスにプライベート AS パスのみが含まれている場合にフル AS パスが eBGP ネイバーと共有されないようにする制限が含まれています。これは期待される動作ですが、管理者がプライベート AS パスを eBGP ネイバーと共有したい場合には問題となります。

回避策：Edge に BGP 更新のすべての AS パスを通達させるための回避策はありません。

- **問題 1716545：**Edge のアプライアンス サイズを変更しても、スタンバイ Edge の CPU とメモリの予約が変更されない
予約設定は、高可用性構成の 2 台の Edge 仮想マシンのうち、最初に作成された仮想マシンにのみ割り当てられます。
両方の Edge 仮想マシンに同じ CPU/メモリ予約（以下、予約）を構成するには、次のいずれかの手順を実行します。
 - PUT API <https://<NSXManager>/api/4.0/edgePublish/tuningConfiguration> を使用して、両方の Edge 仮想マシンに値を明示的に設定します。
 - または
 - Edge の高可用性を一度無効にして再び有効にします。これで、2 番目の Edge 仮想マシンが削除され、デフォルトの予約が設定された新しい Edge 仮想マシンが展開されます。

回避策：なし。

- **問題 1510724：**新しいユニバーサル分散論理ルーター (UDLR) を作成した後にデフォルトのルートがホストにポピュレートされない
NSX for vSphere 6.2.x で、Cross-vCenter を構成するために NSX Manager をスタンドアロンからプライマリモードに変更した後、次の問題が発生することがあります。
 - 新しい UDLR を作成するときに、ホスト インスタンスにデフォルトのルートがポピュレートされない。
 - ルートがホスト インスタンスではなくユニバーサル分散論理ルーター制御仮想マシンにポピュレートされる。
 - `show logical-router host host-ID dlr Edge-ID route` コマンドを実行すると、デフォルトのルートが追加されない。

回避策：この問題を解決するには、[VMware ナレッジベースの記事 KB2145959](#) を参照してください。

- 問題 1492547：一番大きい数字の IP アドレスを持つ NSX の OSPF エリア境界ルーター (ABR) をシャットダウンまたは再起動すると、コンバージェンスに時間がかかる

一番大きい数字の IP アドレスを持っていない Not-So-Stubby Area (NSSA) ABR をシャットダウンまたは再起動した場合、トラフィックは別のパスにただちに収束されます。一番大きい数字の IP アドレスを持つ NSSA ABR をシャットダウンまたは再起動すると、再コンバージェンスに時間が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。

回避策：VMware ナレッジベースの記事 KB2127369 を参照してください。
- 問題 1542416：サブ インターフェイスを使用して Edge の再デプロイや高可用性フェイルオーバーを行った後、データ パスが 5 分間動作しない

サブ インターフェイスを使用して再デプロイまたは高可用性フェイルオーバーの処理を行うと、データパスが 5 分間停止します。この問題は通常のインターフェイスでは発生しません。

回避策：回避策はありません。
- 問題 1706429：分散論理ルーターの展開後に高可用性機能を有効にすると、通信の問題が発生し、両方の分散論理ルーター アプライアンスがアクティブになる場合がある

高可用性なしの分散論理ルーターをデプロイした後で、新しい分散論理ルーター アプライアンスをデプロイして高可用性機能を有効にするか、高可用性機能を無効にしてから再度有効にすると、分散論理ルーター アプライアンスの 1 台が高可用性インターフェイスへの接続ルートを失うことがあります。このため、両方のアプライアンスがアクティブな状態になります。

回避策：高可用性インターフェイスへの接続ルートを失っている分散論理ルーター アプライアンスの vNIC への接続を解除してから再接続するか、または分散論理ルーター アプライアンスを再起動します。
- 問題 1461421：NSX Edge の「show ip bgp neighbor」コマンドの出力で、以前接続を確立したカウンタが維持される

「show ip bgp neighbor」コマンドは、任意のピアに対して BGP ステート マシンが Established に遷移した回数を表示します。MD5 認証で使用するパスワードを変更すると、ピア接続が破棄されて再作成されるため、カウンタがクリアされます。この問題は、Edge 分散論理ルーター (DLR) では発生しません。

回避策：カウンタをクリアするには、「clear ip bgp neighbor」コマンドを実行します。
- 問題 1676085：リソースの予約に失敗すると、Edge の高可用性機能の有効化に失敗する

NSX for vSphere 6.2.3 以降、高可用性構成の 2 台目の Edge 仮想マシン アプライアンス用に十分なリソースを予約できない場合、既存の Edge で高可用性機能を有効にすると失敗します。その場合、直近の正常な設定にロール バックします。以前のリリースでは、Edge の展開後に高可用性機能を有効にした場合、リソースの予約に失敗しても Edge 仮想マシンは作成されました。

回避策：これは、機能変更で想定される正常な動作です。
- 問題 1656713：HA フェイルオーバー後 NSX Edge に IPsec セキュリティ ポリシー (SP) が存在せず、トラフィックがトンネルを通過できない

IPsec トンネルを通過するトラフィックに対する、スタンバイ から アクティブへの切り替えが動作しません。

回避策：NSX Edge の切り替え後、IPsec を一度無効にしてから有効にします。
- 問題 1624663：[詳細デバッグの設定] をクリックすると、vCenter Server ユーザー インターフェイスが更新され、変更が維持されない

特定の Edge ID > [設定] > [アクション] > [詳細デバッグの設定] の順にクリックすると、vCenter Server のユーザー インターフェイスが更新され、変更が維持されません。

回避策：Edge のリスト メニューに直接移動して Edge をハイライト表示し、[アクション] > [詳細デバッグの設定] の順にクリックして、変更を行います。
- 問題 1354824：Edge 仮想マシンが破損したり、電源障害などの理由によりアクセスできなくなると、NSX Manager からの健全性チェックが失敗した場合にシステム イベントが表示される

[システム イベント] タブには、「Edge にアクセスできない」ことを示すイベントが通知されます。NSX Edge のリストでは、「デプロイ済み」のステータスが引き続き表示される場合があります。

回避策： <https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status> API with *detailedStatus=true* を使用します。

- 問題 1647657：ESXi ホストで分散論理ルーターを有効にしている場合に show コマンドを使用すると、分散論理ルーター インスタンスごとのルートが最大 2,000 個しか表示されない

ESXi ホストで分散論理ルーターを有効にしている場合に show コマンドを使用すると、分散論理ルーター インスタンスごとに表示されるルートの最大数が 2,000 個となり、この数を超えるルートを実行していても表示されません。これは表示の問題であり、データ パスはすべてのルートで正しく動作します。

回避策： 回避策はありません。

- 問題 1634215：OSPF CLI コマンド出力に、ルーティングが無効になっているかどうかが表示されない

OSPF が無効になっている場合でも、ルーティングの CLI コマンドの出力に「OSPF が無効」であることを示すメッセージが表示されません。出力は空白です。

回避策： `show ip ospf` コマンドを使用すると、正しいステータスが表示されます。

- 問題 1663902：NSX Edge 仮想マシンの名前を変更すると、Edge からのトラフィックが中断する

- 問題 1647739：vMotion の操作後に Edge 仮想マシンを再デプロイすると、Edge または分散論理ルーター仮想マシンの配置場所が元のクラスタに戻る

回避策： Edge 仮想マシンを異なるリソース プールまたはクラスタに配置するには、NSX Manager ユーザー インターフェイスを使用して希望の場所を構成します。

- 問題 1463856：NSX Edge ファイアウォールが有効になっていると、既存の TCP 接続がブロックされる

Edge のステートフル ファイアウォールで、最初の 3 ウェイ ハンドシェイクが認識されないために、TCP 接続がブロックされます。

回避策：このような既存のフローを処理するには、次の操作を実行します。NSX REST API を使用して、ファイアウォールのグローバル構成で `[tcpPickOngoingConnections]` フラグを有効にします。これにより、ファイアウォールが Strict モードから Lenient モードに切り替わります。次に、ファイアウォールを有効にします。ファイアウォールを有効にしてから数分後に、既存の接続が検出されたら、`[tcpPickOngoingConnections]` フラグを `false` に戻して、ファイアウォールを Strict モードに戻します。この設定は維持されます。

```
PUT /api/4.0/edges/{edgeId}/firewall/config/global
```

```
<globalConfig>
```

```
<tcpPickOngoingConnections>true</tcpPickOngoingConnections>
```

```
</globalConfig>
```

- 問題 1374523：esxcli を使用した VXLAN コマンドを利用するには、VXLAN VIB のインストール後に、ESXi を再起動するか、`services.sh restart` を実行する必要がある

VXLAN VIB のインストール後、esxcli を使用した VXLAN コマンドを利用するには、ESXi を再起動するか `services.sh restart` コマンドを実行する必要があります。

回避策： esxcli の代わりに localcli を使用します。

- 問題 1642087：IPsec VPN 拡張で `securelocaltrafficbyip` のパラメータ値を変更すると、宛先ネットワークへの転送に失敗する

NSX Edge Services Gateway を使用すると、次の問題が発生します。

- NSX ユーザー インターフェイスの [IPsec VPN の編集] 画面で、securelocaltrafficbyip の値を 0 に変更すると、IPsec VPN トンネルのリモート サブネットへの転送が動作しなくなる
- このパラメータを変更すると、IP ルーティング テーブルでリモート サブネットの情報が正しく表示されなくなる

回避策： IPsec VPN サービスを一度無効にしてから、再び有効にします。次に、正しいルーティング情報が CLI とユーザー インターフェイスに表示されることを確認します。

- 問題 1525003：誤ったパスフレーズを使用して NSX Manager のバックアップをリストアしようとすると、クリティカルなルート フォルダにアクセスできないため、警告なしで操作に失敗する
回避策： なし。

- 問題 1637639：Windows 8 SSL VPN PHAT クライアントを使用する場合、IP アドレス プールから仮想 IP アドレスが割り当てられない

Windows 8 では、Edge Services Gateway が新しい IP アドレスが割り当てられる場合、または異なる IP アドレス範囲を使用するように IP アドレス プールを変更した場合、IP アドレス プールから仮想 IP アドレスが割り当てられません。

回避策： この問題は Windows 8 でのみ発生します。別の Windows OS を使用することで、この問題の発生を回避できます。

- 問題 1483426: IPsec および L2 VPN サービスが有効にでない場合でも、サービスのステータスが停止中と表示される

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。ユーザー インターフェイス ページを更新しない限り、[設定] タブの L2 VPN および IPsec サービスは、常に停止中と表示されます。

回避策： 画面を更新します。

- 問題 1446327：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>

- 問題 1534602：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。

- 問題 1498243：BGP ネイバー フィルタを「拒否、任意、送信」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「拒否、任意、送信」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。

- 操作：拒否

- ネットワーク：任意
- 方向：送信

回避策： なし。

- **問題 1471561：直接接続されているルーターでは、BGP/OSPF の隣接関係が確立されない**
ECMP ルートが直接接続されたネットワークに存在する場合、直接接続されたルーターでは動的ルーティングが期待したとおりに動作しません。
回避策： Edge を再起動します。または、関連付けられている vNIC インターフェイスを削除してから再作成します。
- **問題 1089238: 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。
- **問題 1499978: Edge の Syslog メッセージがリモートの Syslog サーバに到達しない**
デプロイの直後は、Edge の Syslog サーバは構成済みのリモート Syslog サーバの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。
- **問題 1489829: 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。
- **問題 1243112：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。
- **問題 1281425: 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?vmoid=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 c
onnected-->
</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。

- 問題 1637939：ハードウェア ゲートウェイのデプロイ中に MD5 証明書がサポートされない
論理 L2 VLAN から VXLAN へのブリッジ用 VTEP としてハードウェア ゲートウェイ スイッチをデプロイしている間、NSX Controller と OVSDB スイッチ間の OVSDB コネクション用に、物理スイッチは最低でも SHA1 SSL 証明書をサポートします。

回避策：なし。

- 問題 1637943：ハードウェア ゲートウェイ バインドを含む VNI で、ハイブリッドまたはマルチキャスト レプリケーション モードがサポートされない
L2 VXLAN から VLAN へのブリッジ用 VTEP として使用されるハードウェア ゲートウェイ スイッチは、ユニキャスト レプリケーション モードのみをサポートします。

回避策：ユニキャスト レプリケーション モードのみを使用します。

- 問題 1934416: TCP 最適化モードが有効になっていると、SSLVPN プロセスが停止する
SSLVPN プロセスが停止し、ユーザー インターフェイスで SSLVPN 設定のデータが更新されません。
SSLVPN show コマンドを実行しても、CLI に出力が表示されません。

回避策：Edge を再デプロイするか、SSLVPN プロセスを再起動します。

セキュリティ サービスに関する既知の問題

- 問題 1474650：NetX を使用している場合、ESXi 5.5.x または 6.x ホストで「**ALERT: NMI: 709: NMI IPI received**」というパープル スクリーンが表示される
サービス仮想マシンが大量のパケットを送信または受信すると、DVFilter が CPU を占有し続けるため、ハートビートが失われ、パープル スクリーンが表示されます。詳細については、[VMware のナレッジベースの記事 KB2149704](#) を参照してください。
- 問題 1741844：複数の IP アドレスを持つ vNIC のアドレスを検出するために ARP スヌーピングを使用すると、CPU 使用率が 100% になる
この問題は、仮想マシンの vNIC に複数の IP アドレスが設定されており、ARP スヌーピングで IP アドレス検出が有効になっている場合に発生します。IP アドレス検出モジュールは vNIC-IP アドレスの更新を NSX Manager に継続的に送信し続け、これにより、複数の IP アドレスを使用して構成されたすべての仮想マシン

ンの vNIC-IP アドレス マッピングを変更しようとします。

回避策：回避策はありません。現在 ARP スヌーピング機能では、vNIC ごとに 1 つの IP アドレスのみがサポートされています。詳細については、『NSX 管理ガイド』の「[仮想マシンの IP アドレス検出](#)」セクションを参照してください。

- **問題 1689159：**フロー モニタリングのルールの追加機能が ICMP フローに対して適切に動作しない
フロー モニタリングでルールを追加する際、[サービス] フィールドに明示的に ICMP に設定せずに空白のままにすると、サービス タイプが「任意」のルールが追加されます。

回避策：[サービス] フィールドを更新して ICMP トラフィックを反映します。

- **問題 1620460:** NSX は、Service Composer のルール セクションにユーザーがルールを作成することを許可してしまう
vSphere Web Client の [Networking and Security] のファイアウォールの設定を使用して、ユーザーは Service Composer のルール セクションにルールを作成できてしまいます。ユーザーは Service Composer のセクションの上部または下部にルールを追加することは許可されていますが、Service Composer のセクション内にルールを追加することは許可されていません。

回避策：Service Composer のルール セクションにルールを追加する場合は、グローバル ルール レベルで [+] ボタンを使用しないようにします。

- **問題 1682552：**分散ファイアウォール (DFW) の CPU、メモリ、1 秒あたりの接続数 (CPS) のしきい値イベントがレポートされない
分散ファイアウォールの CPU、メモリ、および CPS のしきい値イベントをレポートするように設定してあっても、しきい値を超えた際にレポートされません。

回避策：

- 各 ESXi ホストにログインして、次のコマンドを実行して分散ファイアウォールの制御プレーン プロセスを再起動します。
`/etc/init.d/vShield_Stateful_Firewall restart`
- 次のコマンドを実行して状態を確認します。
`/etc/init.d/vShield_Stateful_Firewall status`
- 次のような結果が表示されます。
`"vShield-Stateful-Firewall is running"`

注：この操作は慎重に行ってください。分散ファイアウォールのすべてのルールがすべてのフィルタに再度プッシュされます。多数のルールがある場合、すべてのフィルタにルールを適用するまでに時間がかかる場合があります。

- **問題 1717635:** 環境内にクラスタが複数あり、変更が同時に行われた場合、ファイアウォールの設定操作に失敗する

クラスタが複数ある環境で、2 人以上のユーザーがセクションやルールを追加または変更するなど、ファイアウォール構成を何度も続けて変更した場合、一部の操作に失敗して、次のような API 応答がユーザーに表示されます。

```
<?xml version="1.0" encoding="UTF-8"? >
```

```
neutron-server.log.1:70282:2016-08-23 17:58:23.429 30787 ERROR vmware_nsx.plugins.nsx_v.plugin
```

```
<error>
```

```
<details> org.hibernate.exception.GenericJDBCException: Could not execute JDBC batch update; nested exception is  
javax.persistence.PersistenceException: org.hibernate.exception.GenericJDBCException: Could not execute JDBC  
batch update </details>
```

```
<errorCode>258
```

```
</errorCode>
```

```
</error>
```

回避策： ファイアウォール構成を同時に変更しないようにします。

- **問題 1717994：分散ファイアウォール (DFW) のステータス API のクエリによって、「500 internal server error」 が断続的に発生する**

ホストを準備済みのクラスタに新しいホストを追加している間に分散ファイアウォールのステータス API のクエリが発行されると、「500 internal server error」が発生して、クエリの試行が何度か失敗します。その後、ホストに VIB がインストールされると、適切な応答が返されるようになります。

回避策：新しいホストの準備が正常に完了するまで分散ファイアウォールのステータス API のクエリを使用しないようにします。

- **問題 1686036：デフォルトのセクションが削除されると、ファイアウォール ルールを追加、編集、削除できなくなる**

レイヤー 2 またはレイヤー 3 のデフォルトのセクションを削除すると、ファイアウォール ルールの発行に失敗する場合があります。

回避策：デフォルトのルールは削除しないでください。デフォルトのルールを使用した設定をドラフトに保存している場合、次の手順を実行します。

1. 次の DELETE API 呼び出しを使用して、ファイアウォール構成全体を削除します。
<https://<NSX Manager IP>/api/4.0/firewall/globalroot-0/config>
これによって、ファイアウォールのデフォルトのセクションがリストアされます。
2. デフォルトのセクションを含むファイアウォール ルールの保存されたドラフトをファイアウォールにロードします。

- **問題 1628220：受信側で分散ファイアウォールまたは NetX の監視が表示されない**

宛先 vNIC に関連付けられているスイッチ ポートが変更された場合、レシーバ側でトレースフローが分散ファイアウォール (DFW) および NetX の監視を表示しないことがあります。この問題は、vSphere 5.5 のリリースでは修正されていません。vSphere 6.0 以降では、このような問題は発生しません。

回避策：vNIC を無効にしないでください。仮想マシンを再起動してください。

- **問題 1626233：NetX サービス仮想マシン (SVM) がパケットをドロップする際に、トレースフローでドロップが検出されない**

トレースフロー セッションは、パケットが NetX サービス仮想マシン (SVM) に送信された後に終了します。SVM がパケットをドロップしても、トレースフローはドロップを検出しません。

回避策：回避策はありません。SVM から送信されたパケットにトレースフロー パケットが挿入されていない場合、SVM がパケットをドロップしたと考えられます。

- **問題 1632235：ゲスト イントロスペクションのインストール中、ネットワークのドロップダウンリストに「ホストで指定済み」のみが表示される**

アンチウイルスのみの NSX のライセンスおよび vSphere Essential または Standard ライセンスを使用してゲスト イントロスペクションをインストールする場合、ネットワークのドロップダウン リストには既存の分散仮想ポート グループのみが表示されます。このライセンスは分散仮想スイッチの作成をサポートしていません。

回避策：これらのライセンスのいずれかを使用して vSphere ホストにゲスト イントロスペクションをインストールする前に、まず [エージェント仮想マシン設定] ウィンドウでネットワークを指定します。

- **問題 1652155：REST API を使用してファイアウォール ルールを作成または移行しようとする、特定の状況で失敗して、HTTP 404 エラーが発生する**

次の状況では、REST API を使用したファイアウォール ルールの追加または移行はサポートされません。

- autoSaveDraft=true に設定されている場合の一括処理でのファイアウォール ルールの作成
- 複数のセクションへのファイアウォール ルールの同時追加

回避策：ファイアウォール ルールの作成または移行を一括で実行する場合、API 呼び出しで autoSaveDraft パラメータを false に設定します。

- **問題 1509687：一度の API 呼び出しで 1 つのセキュリティ タグを多数の仮想マシンに割り当てる**

場合、サポートされる URL は最長 16,000 文字である

URL の長さが 16,000 文字を超える場合、単一の API で 1 つのセキュリティ タグを多数の仮想マシンに同時に割り当てることはできません。

回避策：パフォーマンスを最大にするには、一度の呼び出しでタグを指定する仮想マシン数を最大 500 台にしてください。

- 問題 1662020：分散ファイアウォールのユーザー インターフェイスの [全般] および [パートナーセキュリティ サービス] セクションに、「前回の発行操作はホスト <ホストの番号> で失敗しました」という内容のエラー メッセージが表示され、発行操作に失敗する場合がある
任意のファイアウォール ルールを変更した後、ユーザー インターフェイスに「前回の発行操作はホスト <ホストの番号> で失敗しました」というエラー メッセージが表示されます。ユーザー インターフェイスに表示されるホストは、正しいバージョンのファイアウォール ルールを使用していない可能性があり、そのためにセキュリティ上の不備や、ネットワークの中断が発生します。

この問題は、通常次の状況で発生します。

- NSX を最新のバージョンにアップグレードした後
- ホストをクラスタの外部に移動した後で、再びクラスタに戻した場合
- クラスタ内のホストを別のクラスタに移動した場合

回避策：リカバリを行うには、影響を受けるクラスタで強制同期を行う必要があります（ファイアウォールのみ）。

- 問題 1481522：6.1.x から 6.2.3 へのファイアウォール ルール ドラフトの移行は、これらのリリース間でドラフトの互換性がないためにサポートされない

回避策：なし。

- 問題 1491046：VMware NSX for vSphere 6.2.x で SpoofGuard ポリシーが「Trust On First Use (TOFU)」に設定されていると、IPv4 IP アドレスが自動承認されない

回避策：[VMware ナレッジベースの記事 KB2144649](#) を参照してください。

- 問題 1628679：ID ベースのファイアウォールを使用すると、削除されたユーザーの仮想マシンが Security Group の一部であり続ける

Active Directory サーバで、ユーザーをグループから削除しても、ユーザーがログインしている仮想マシンはセキュリティ グループにそのまま所属し続けます。これにより、ハイパーバイザーの仮想マシン vNIC でファイアウォール ポリシーが保持され、サービスへの完全なアクセス権限がユーザーに付与されます。

回避策：なし。これは、設計上想定される正常な動作です。

- 問題 1462027：Cross-vCenter NSX のデプロイ環境で、保存されている複数のバージョンのファイアウォール構成がセカンダリ 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 が同じ名前で同じ時刻に作成されているため、重複と判断できます。同様に、ドラフト 127 と 128 も同じ名前で 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す。


```

<firewallDrafts>
  <firewallDraft id="144" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 P
M 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 P
M 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>

```

- **問題 1449611** : 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 インターフェー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 インターフェースで、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。
- **問題 1557880** : 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、送信元または宛先フィールドのいずれかを [任意] に設定します。
- **問題 1496273** : 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。

- **問題 1557924：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。

- **問題 1559971：1 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。

- **問題 1407920：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。

- **問題 1534585：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。

- **問題 1494718：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。

- **問題 1442379：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。

- **問題 1066277：229 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。

- **問題 1443344：サードパーティの VM-Series の特定のバージョンがデフォルト設定で NSX Manager と連携しない**

NSX 6.1.4 以降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。

- 問題 1660718 : Service Composer のポリシーのステータスが、ユーザー インターフェイスには「処理中」と表示され、API の出力には「保留」と表示される

回避策 : なし。

- 問題 1620491 : Service Composer のポリシー レベルの同期のステータスで、ポリシー内のルール の発行状態が表示されない

ポリシーが作成または変更されると、処理が正常に完了したことが Service Composer に表示されますが、そこで示されるのはポリシーのセッション維持状態の情報のみであり、ルールがホストに正常に発行されたかどうかの情報は示されません。

回避策 : ファイアウォールのユーザー インターフェイスを使用して、発行のステータスを表示します。

- 問題 1317814 : Service Manager の 1 つがダウンしている間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

複数の Service Manager の 1 つがダウンしているときにポリシーの変更を行うと、変更に失敗し、Service Composer が同期されなくなります。

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。

- 問題 1070905 : ゲスト イントロスペクション 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 イントロ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。

- 問題 1648578 : 新しい NetX ホストベースのサービス インスタンスの作成時に、NSX でクラスタ/ネットワーク/ストレージの追加が強制される

vSphere Web Client からファイアウォール、IDS、IPS などの NetX ホストベース サービス用に新しいサービス インスタンスを作成する際に、クラスタ/ネットワーク/ストレージの追加が不要な場合でも強制されます。

回避策 : 新しいサービス インスタンスの作成時に、クラスタ/ネットワーク/ストレージに関する情報を追加し、フィールドに入力します。これにより、サービス インスタンスの作成が許可され、操作を続行できるようになります。

- 問題 1772504 : Service Composer では MAC セットを含む Security Group がサポートされない

Service Composer では、ポリシー設定での Security Group の使用が許可されています。Service Composer は MAC セットを含むセキュリティ グループを受け入れますが、その場合、個々の MAC セットのルールは適用されません。これは、Service Composer がレイヤー 3 で動作し、レイヤー 2 構造をサポートしないためです。Security Group に IP セットと MAC セットの両方がある場合、IP セットは有効になりますが、MAC セットは無視されます。MAC セットを含むセキュリティ グループを参照しても問題ありませんが、MAC セットが無視されることに注意する必要があります。

回避策 : MAC セットを使用してファイアウォール ルールを作成する場合、Service Composer ではなく分散ファイアウォール レイヤー 2/イーサネット設定を使用する必要があります。

- 問題 1718726: ユーザーが分散ファイアウォール (DFW) の REST API を使用して Service Composer のポリシー セクションを手動で削除した後、Service Composer を強制同期できない

Cross-vCenter NSX 環境で、Service Composer が管理するポリシー セクションが 1 つだけあり、このポリシー セクションが REST API 呼び出しを使用して削除された場合、ユーザーが NSX Service Composer の設定を強制同期しようすると失敗します。

回避策： Service Composer が管理するポリシー セクションは、REST API 呼び出しを使用して削除しないでください。ユーザー インターフェイスでは、このセクションを削除することはできません。

監視サービスに関する既知の問題

- **問題 1655593：** 監査ロールまたはセキュリティ管理者ロールでログインしているときに、NSX ダッシュボードにステータスが表示されない
監査担当者またはセキュリティ管理者として NSX ダッシュボードを表示すると、「ユーザーは、オブジェクト ... および機能 ... にアクセスする権限がありません。このユーザーのオブジェクト アクセス範囲および機能の使用権限を確認してください。」というエラーメッセージが表示されます。たとえば、ダッシュボードから [論理スイッチのステータス] が監査ロールでは表示されないことがあります。

回避策： なし。

- **問題 1466790：** 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。

ソリューションの相互運用性に関する既知の問題

- **問題 1840744:** 仮想マシンが再起動ループに入ると、VMware ESXi 6.0.0 ホストにパープル スクリーンが表示される
この問題は、再起動ループに入った仮想マシンが生成する dvfilter の作成/破棄イベントの競合状態が原因で発生します。詳細については、[VMware ナレッジベースの記事 KB2149782](#) を参照してください。

回避策：この問題は、VMware のダウンロード ページで公開されている VMware ESXi 6.0 パッチ 03 以降のリリースで解決されています。

アップグレードせずにこの問題を回避するには、問題のある仮想マシンをパワーオフしてください。

- **問題 1568861：** vCenter Server リスナーを所有しない vCloud Director のセルから NSX Edge をデプロイすると、デプロイに失敗する

vCenter Server リスナーを所有しない vCloud Director のセルから NSX Edge をデプロイすると、デプロイに失敗します。また、vCloud Director から再デプロイを含む NSX Edge のアクションを実行すると、失敗します。

回避策： vCenter Server リスナーを所有する vCloud Director セルから NSX Edge をデプロイします。

- **問題 1530360：** NSX Manager 仮想マシンのフェイルオーバー後に、Site Recovery Manager (SRM) が誤ってタイムアウト エラーをレポートする

NSX Manager 仮想マシンのフェイルオーバー後、VMware Tools の待機中にタイムアウトが発生したというエラーを SRM が誤ってレポートします。実際には、タイムアウトする前（300 秒以内）に、VMware Tools が起動して実行中となります。

回避策： なし。

NSX Controller に関する既知の問題

- **問題 1845087:** ディスク遅延が非常に大きくなると、NSX Controller API に影響する
NSX Controller が使用するストレージの I/O 遅延が非常に大きくなると、NSX Manager の制限時間内に NSX Controller API が応答しない場合があります。これにより、NSX Controller のアップグレードや他の機能に

影響が及ぶ可能性があります。遅延の程度が上限を超えた場合、vSphere Web Client の Network and Security プラグインに、コントローラーのディスク遅延が大きいことを示すエラーが表示されます。

回避策：この問題を解決するには、専用のローカル ハード ドライブと SSD を使用することをお勧めします。

- **問題 1765354：**<deployType> は必須プロパティだが使用されない
<deployType> は必須プロパティですが、使用されない、意味のないものです。
- **問題 1760102：**ストレージ障害からリカバリするため、NSX Controller が削除され再デプロイされると、仮想マシンの通信が失われることがある
vSphere 6.2.x の NSX Controller では、ストレージに障害が発生すると、読み取り専用モードになることがあります。コントローラを削除して再デプロイし、その状態からリカバリした場合、一部の仮想マシンの通信が失われることがあります。ストレージ障害が発生した際、通常は再起動するとコントローラの読み取り専用モードが解除します。しかし、現在の NSX ではそのように動作しません。

回避策：NSX 管理サービスを再起動します。

- **問題 1516207：**NSX Controller クラスタで IPsec 通信を再度有効にすると、コントローラが隔離されることがある
NSX Controller クラスタが、IPsec を無効にした暗号化なしのコントローラ間通信を許可するように設定され、後から IPsec 通信を再び有効にした場合、PSK （事前共有鍵） の不一致が原因で、クラスタ マジョリティから 1 個以上のコントローラが隔離されることがあります。この問題が発生すると、NSX API はコントローラの IPsec 設定を変更できなくなる場合があります。

回避策：

この問題を解決するには、次の手順を実行します。

1. NSX API を使用して、IPsec を無効にします。

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>false</ipSecEnabled>
</controllerNodeConfig>
```

2. NSX API を使用して、IPsec を再び有効にします。

```
PUT /2.0/vdn/controller/node

<controllerNodeConfig>
  <ipSecEnabled>true</ipSecEnabled>
</controllerNodeConfig>
```

この問題を回避するには、次のベスト プラクティスを実行することをお勧めします。

- NSX API を常に使用して、IPsec を無効にします。NSX Controller の CLI を使用して IPsec を無効にする操作はサポートされていません。
- API を使用して IPsec 設定を変更する前に、すべてのコントローラがアクティブであることを必ず確認します。

- **問題 1306408：**NSX Controller のログを同時にダウンロードできない
NSX Controller のログは、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。

- **問題 1937015：NSX Controller クラスターが一時的に停止する**

NSX Controller 仮想マシンの e1000 ドライバがハングし、一時的に停止します。本番環境のネットワークトラフィックに影響はありません。

回避策：詳細については、VMware のナレッジベース（英語版）の記事 [KB2150747](#) を参照してください。