

VMware NSX for vSphere 6.3.0 リリース ノート

VMware NSX for vSphere 6.3.0 | 2017 年 2 月 2 日リリース | ビルド 5007049

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](#)
- [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 6.3.0 の新機能は次のカテゴリに分類することができます。

- [プラットフォームとコンプライアンス機能](#)
- [運用の機能拡張](#)
- [サービスとルーティングの機能拡張](#)
- [セキュリティの機能拡張](#)
- [CMP とパートナーとの連携](#)
- [インストールとアップグレード](#)
- [バックアップとリストア](#)

プラットフォームとコンプライアンス機能

- プラットフォーム側：
 - Cross-vCenter NSX のアクティブ/スタンバイ分散ファイアウォールの機能拡張：NSX 6.3.0 では、次の機能拡張が提供されます。
 - 複数のユニバーサル分散ファイアウォール セクションがサポートされます。ユニバーサル ルールとローカル ルールの両方で、Source、Destination および AppliedTo フィールドにユニバーサル セキュリティ グループを使用できます。
 - ユニバーサル セキュリティ グループ：ユニバーサル セキュリティ グループのメンバーシップを静的または動的な方法で定義することができます。静的メンバーシップでは、各仮想マシンにユニバーサル セキュリティ タグを手動で追加します。動的メンバーシップでは、仮想マシンを動的な基準（仮想マシン名）に基づいてメンバーとして追加します。
 - ユニバーサル セキュリティ タグ：プライマリ NSX Manager でユニバーサル セキュリティ タグを定義し、セカンダリ NSX Manager とユニバーサル同期を行うためにマークできるようになりました。一意の ID 選択に基づく静的な方法か、アンチウイルスまたは脆弱性スキャンによる、設定した基準に応じた動的な方法のいずれかを使用できます。

- 一意の ID 選択基準：NSX の以前のリリースでは、セキュリティ タグは NSX Manager に対してローカルであり、仮想マシンの管理対象オブジェクト ID を使用して仮想マシンにマッピングされていました。アクティブ/スタンバイ環境では、アクティブ データセンターとスタンバイ データセンターで、仮想マシンの管理対象オブジェクト ID が異なる場合があります。NSX 6.3.x では、プライマリ NSX Manager で一意の ID 選択基準を設定して、ユニバーサル セキュリティ タグを追加する仮想マシンの識別に使用できます。一意の ID 選択基準には、仮想マシン インスタンス UUID、仮想マシン BIOS UUID、仮想マシン名、またはこれらのオプションの組み合わせを利用できます。詳細については、『NSX 管理ガイド』の「一意の ID 選択」を参照してください。

- 制御プレーン エージェント (netcpa) の自動リカバリ：安定したデータ パス通信を維持するため、netcpa プロセスの自動リカバリ メカニズムが拡張されました。netcpa の自動監視プロセスはまた、問題が発生すると自動的に再起動し、Syslog サーバを介してアラートを提供します。この機能のメリットは次のとおりです。

- netcpa プロセスの自動監視
- システムのハングなどの問題が発生するとプロセスを自動的に再起動
- デバッグ用コア ファイルの自動生成
- 自動的に再起動イベントの Syslog を介したアラートの生成

- vSphere 6.5 との互換性：NSX 6.3.0 は vSphere 6.5a 以降をサポートします。NSX 6.3.0 は vSphere 5.5 および 6.0 との互換性があります。

- **技術プレビュー**：Controller Disconnected Operation (CDO) モード：Controller Disconnected Operation (CDO) モードが技術プレビューとして追加されました。このモードでは、ホストとコントローラの接続が失われてもデータ プレーンの接続に影響することはありません。『NSX 管理ガイド』の「[Controller Disconnected Operation \(CDO\) モード](#)」セクションを参照してください。また、問題 1803220 も参照してください。

- **コンプライアンス機能：**

- FIPS：NSX 6.3.0 には、FIPS に準拠する暗号スイートのみを使用する FIPS モードがあります。FIPS モードは、NSX Manager と NSX Edge で利用できます。これを有効にするには、vSphere Web Client または NSX REST API を使用します。FIPS モードの影響を受ける機能のリストについては、『NSX 管理ガイド』の「[FIPS モードと非 FIPS モードの機能の相違点](#)」を参照してください。

注：VMware の開発パートナーは、NSX で利用できる、FIPS に準拠した新しいパートナー ソリューション認定を受けています。NSX 6.3.0 の送信接続には TLS 1.1 以降が使用され、また FIPS 承認済みの暗号スイートのみが使用されます。これは、コールバックを受け取るパートナー アプライアンスが、より安全な暗号スイートへの安全な Web リスナーを設定する必要があることを意味します。デフォルト モードおよび FIPS モードで使用する暗号は次のとおりです。

- デフォルト モードの暗号：（FIPS モード OFF）[TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384, TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384, TLS_DHE_RSA_WITH_AES_256_CBC_SHA256, TLS_DHE_DSS_WITH_AES_256_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA, TLS_ECDH_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_RSA_WITH_AES_256_CBC_SHA, TLS_DHE_DSS_WITH_AES_256_CBC_SHA, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, TLS_DHE_DSS_WITH_AES_128_CBC_SHA256, TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDH_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_RSA_WITH_AES_128_CBC_SHA, TLS_DHE_DSS_WITH_AES_128_CBC_SHA, TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_RSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA, TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA, SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA, TLS_EMPTY_RENEGOTIATION_INFO_SCSV]
- FIPS モードの暗号：[TLS_RSA_WITH_AES_256_CBC_SHA256, TLS_RSA_WITH_AES_128_CBC_SHA256, TLS_RSA_WITH_AES_256_CBC_SHA, TLS_RSA_WITH_AES_128_CBC_SHA]

TLS 1.1 と TLS 1.2 プロトコルはデフォルト モードと FIPS モードの両方でサポートされます。パートナーのソリューションが FIPS モードの認定を受けているかどうかを確認するには、『[VMware 互換性ガイド](#)』を参照してください。

- **情報セキュリティ国際評価基準 (Common Criteria)**：Common Criteria に準拠するため、NSX では EAL2+ の評価保証レベルへのコンプライアンスがテストされています。Common Criteria に準拠する NSX 環境を実現するには、『NSX 管理ガイド』の「[Common Criteria のための NSX の設定](#)」の説明に従って NSX を設定する必要があります。
- **ICSA**：これは、業界で認められた標準認定機関で、アンチウイルス、ファイアウォール、IPSec VPN、暗号化、SSL VPN、ネットワーク IPS、アンチスパイウェア、および PC ファイアウォールなどの製品をテストおよび認定します。分散ファイアウォールと Edge ファイアウォールの両方で、ICSA の企業ファイアウォール基準への準拠が認定されています。
- **ICSA 認定の要件による分散ファイアウォール パケット ログ形式の変更**：NSX 6.3.0 では、分散ファイアウォール パケット ログが変更されています。NSX 6.3.0 以降は、ICSA 認定要件を満たすための ICMP のタイプとコードが含まれています。

次は、ICMP のコードとタイプを使用しない NSX 6.3.0 以前のログの例です。

```
2016-09-29T20:52:21.983Z 6673 INET6 match PASS domain-c27/1001 IN 96 ICMP
fe80:0:0:0:21d:b502:f984:c601->ff02:0:0:0:0:0:1
```

ICMP のコードとタイプを使用する NSX 6.3.0 以降では、次のようになります。この例では、8 がコードで 0 がタイプです。

```
2016-09-29T20:54:16.051Z 42991 INET match PASS domain-c27/1001 IN 84 ICMP 8
0 10.113.226.5->10.28.79.55
```

運用の機能拡張

- **トラブルシューティング ダッシュボード**：NSX 6.3.0 では NSX ダッシュボードが更新され、サービス デプロイ ステータス、NSX Manager バックアップ ステータスおよび Edge アプライアンス通知などの機能が追加されました。
- **セキュリティ タグ**：API 呼び出しを介して、特定の仮想マシンに複数のタグを割り当てたり、タグを消去できます。
- **Syslog の機能拡張**：ロード バランサ専用の新しい Syslog アップデートを利用できます。
- **Log Insight コンテンツ パック**：ロード バランサ向けに更新されており、集中管理ダッシュボード、End-to-End の監視、ユーザー インターフェイス (UI) を介したより効率的なキャパシティ プランニングを提供します。
- **ロールベースのアクセス コントロール**：この機能では、ユーザー管理が企業の管理者に制限され、NSX 管理者は、新規ユーザーの作成や新規ユーザーへのロールの割り当てを行うことはできません。これは、2 つの管理者ロールの間に、明確なセキュリティ上の境界を作成するのに役立ちます。
- **ロード バランサ プール メンバーのドレイン状態**：プール メンバーをドレイン状態にすることで、メンテナンス時にサーバを正常にシャットダウンするよう強制します。プール メンバーをドレイン状態にすると、バックエンド サーバはロード バランシングから削除されますが、サーバは引き続き新しいパーシステント コネクション (持続的接続) を受け入れることができます。

サービスとルーティングの機能拡張

- **BGP で 4 バイトの ASN をサポート**：BGP 構成が 4 バイト ASN に対応するようになりました。これには、既存の 2 バイト ASN BGP ピアとの後方互換性があります。
- **5-tuple 一致に対する NAT の機能拡張**：NAT ルールできめ細かい設定と柔軟性を実現するために、NSX 6.3.0 では 5-tuple 一致がサポートされます。
 - 一致基準はプロトコル、送信元 IP アドレス、送信元ポート、宛先 IP アドレス、および宛先ポートなど、5 つのパラメータに基づいています。
 - SNAT/DNAT 設定をより簡単に指定できるように、ユーザー インターフェイス (UI) の変更が行われました。以前の Edge バージョンで DNAT/SNAT の設定を変更する場合は、以前のスタイルのユーザー インターフェイスがペインに表示されます。
 - NSX REST API は、次のように新しいパラメータ フィールドを追加します。

```
<natRules>
  <natRule>
    {...}
  <!-- new fields applicable for DNAT -->
    <dnatMatchSourceAddress>any</dnatMatchSourceAddress>
    <dnatMatchSourcePort>any</dnatMatchSourcePort>
  </natRule>
```

```

<natRule>
  {...}
<!-- new fields applicable for SNAT -->
  <snatMatchDestinationAddress>any</snatMatchDestinationAddress>
  <snatMatchDestinationPort>any</snatMatchDestinationPort>
</natRule>
</natRules>

```

- **改善されたレイヤー 2 VPN のパフォーマンス：**レイヤー 2 VPN のパフォーマンスが改善されました。これにより、単一の Edge アプライアンスで 1.5 Gb/秒 までのスループットをサポートできるようになりました。これは、以前の 750 mb/秒に比べて大幅な向上です。
- **OSPF 構成機能の向上：**Edge Services Gateway (ESG) 上で OSPF を設定する際に、NSSA はすべての Type-7 LSA を Type-5 LSA に変換できるようになりました。

セキュリティの機能拡張

分散ファイアウォールではいくつかの拡張が加えられています。

- **分散ファイアウォール タイマー：**NSX 6.3.0 では、非アクティブ状態になったセッションをファイアウォールで保持する期間を定義するセッション タイマーが導入されました。プロトコルのセッションがタイムアウトになると、そのセッションは閉じられます。ファイアウォールで、TCP、UDP、および ICMP セッションのタイムアウトを定義し、それらを仮想マシンまたは vNIC のユーザー定義セットに適用することができます。『NSX 管理ガイド』の「[セッション タイマー](#)」を参照してください。
- **マイクロセグメンテーションをサポートする新しい機能：**視認性およびプランニング ツールでマイクロセグメンテーションをサポートするため、2 つの新しい機能が追加されました。
 - アプリケーション ルール マネージャは、既存のアプリケーション用にセキュリティ グループを作成し、ファイアウォール ルールのホワイトリストを作成する処理を簡素化します。
 - エンドポイントの監視は、アプリケーション所有者が自分のアプリケーションのプロファイルを作成し、ネットワーク接続を行うプロセスを特定できるようにします。
- **ゲスト イントロスペクションの Linux サポート：**NSX 6.3.0 では、Linux 仮想マシンのゲスト イントロスペクションが可能になります。NSX ゲスト イントロスペクション機能は、Linux ベースのゲスト仮想マシン上で、Linux カーネルによって提供される fanotify および inotify 機能を利用します。詳細については、『NSX 管理ガイド』の「[Linux 版ゲスト イントロスペクションのインストール](#)」を参照してください。NSX でサポートされる Linux のバージョンのリストについては、「[バージョン](#)」を参照してください。
- **Service Composer の発行ステータス：**ポリシーが同期しているかどうかを確認するため、Service Composer の発行ステータスを利用できます。これにより、ホスト上での分散ファイアウォール ルールへのセキュリティ ポリシー変換の視認性が向上します。

Cloud Management Platform (CMP) とパートナーの統合

- vCloud Director 8.20 と NSX 6.3.0 間の相互運用性の向上により、サービス プロバイダはテナントに対して高度なネットワークとセキュリティ サービスを提供できるようになります。NSX 6.3.0 と vCloud Director 8.20 を併用すると、ネイティブの NSX 機能を使用して、複数のテナントおよびテナントのセルフサービスをサポートします。
- NSX 6.3.0 では新しい vRO プラグイン バージョン 1.1 がサポートされています。このバージョンでは vRA がサポートされるほか、vRA 以外のアプリケーションもサポートできるようになります。

- NSX NetX 6.3.0 では、サービス挿入に関する拡張性とパフォーマンスが向上しています。

インストールとアップグレード

- NSX カーネル モジュールは ESXi のバージョンに依存しない：NSX 6.3.0 以降、NSX カーネル モジュールは一般公開された VMKAPI のみを使用しているため、リリースが変わってもインターフェイスは安定しています。この機能拡張によって、不正なカーネル モジュール バージョンが原因でホストのアップグレードが失敗する可能性が低減されます。以前のリリースでは、NSX 環境でそれぞれの ESXi アップグレードを行う場合、NSX 機能が継続して機能するためには少なくとも 2 回再起動する必要がありました（新しい ESXi バージョンごとに新しいカーネル モジュールをプッシュする必要があるため）。
- NSX 6.3.0 ではまた、ホストをメンテナンス モードから戻す前に NSX の準備ができているかをチェックします。これによって、DRS はワークロードを NSX の準備が整ったホストにのみ移動します。これにより、一部のワークロード仮想マシンのネットワークが失われるのを防ぎます。
- コンマ区切りの OVF パラメータ：次の OVF パラメータはスペース区切りからコンマ区切りに変更されました。
 - DNS サーバ リスト (vsm_dns1_0)
 - ドメイン検索リスト (vsm_domain_0)
 - NTP サーバ リスト (vsm_ntp_0)

バックアップとリストア

NSX 6.3.0 以降では、SFTP を使用したバックアップ用に次の暗号がサポートされています。

- 暗号：aes128-cbc、aes128-ctr、aes192-cbc、aes192-ctr、aes256-cbc、aes256-ctr
- メッセージ認証 (mac)：hmac-sha2-256
- 鍵交換：diffie-hellman-group-exchange-sha256

注：hmac-sha1 はサポートされず、hmac-sha2-256 のみがサポートされます。バックアップに SFTP を使用する場合は、6.3.0 以降へのアップグレード後に hmac-sha2-256 への変更が必要になります。詳細については、[VMware のナレッジベースの記事 KB2149282](#) 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や NSX 6.1.x からアップグレードする場合は、最新の NSX 6.3 リリースをお勧めします。

NSX for vSphere

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。

vSphere

- vSphere 5.5U3 以降。
- vSphere 6.0U3 以降。vSphere 6.0U3 では、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ています。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。
- vSphere 6.5U1 以降。vSphere 6.5U1 では、EAM がメモリ不足になる問題が解決されています。詳細については、[VMware のナレッジベースの記事 KB2135378](#) を参照してください。

VMware Tools のすべてのバージョンがサポートされます。一部のゲスト イン트로スペクション ベースの機能には、VMware Tools の最新バージョンが必要です。

ゲスト イン트로スペクション (Windows)

- VMware Tools に含まれるオプションの Thin Agent Network Introspection Driver コンポーネントを有効にするには VMware Tools 10.0.9 および 10.0.12 を使用します。
- NSX または vCloud Networking and Security 環境の VMware Tools をアップグレードした後に仮想マシンの動作が遅くなる問題を解決するには、VMware Tools 10.0.8 以降にアップグレードする必要があります。詳細については、[VMware のナレッジベースの記事 KB2144236](#) を参照してください。
- Windows 10 には VMware Tools 10.1.0 以降を使用します。

NSX の本バージョンは、次の Linux のバージョンをサポートします。

ゲスト イン트로スペクション (Linux)

- RHEL 7 GA (64 ビット)
- SLES 12 GA (64 ビット)
- Ubuntu 14.04 LTS (64 ビット)

vRealize Orchestrator

vRealize Orchestrator Plugin for NSX 1.1.0 以降。

注：VMware は、現在 vRealize Networking Insight 3.2 での NSX for vSphere 6.3.x をサポートしません。

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。

- NSX for vSphere 6.1.x : NSX for vSphere 6.1.x は、2017 年 1 月 15 日に提供終了 (EOA) およびジェネラルサポートの終了 (EOGS) となりました。 ([VMware ナレッジベースの記事 KB2144769](#) を参照してください)
- **新規**NSX Data Security を削除 : NSX 6.3.0 から、NSX Data Security 機能が削除されました。
- **新規**NSX アクティビティ モニタリング (SAM) を廃止 : NSX 6.3.0 から、アクティビティ モニタリングは NSX でサポートされません。代替機能として、エンドポイントの監視を使用してください。詳細については、『NSX 管理ガイド』の「[エンドポイントの監視](#)」を参照してください。
- **新規**Web Access Terminal を削除 : Web Access Terminal (WAT) は NSX 6.3.0 から削除されました。Web Access SSL VPN-Plus を設定して、NSX Edge を介してパブリック URL アクセスを有効にすることはできません。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。以前のリリースで WAT 機能を使用している場合は、6.3.0 にアップグレードする前に無効にする必要があります。
- **新規**IS-IS を NSX Edge から削除 : NSX 6.3.0 以降は、[ルーティング] タブから IS-IS プロトコルを設定することはできません。
- **新規**vCNS Edge のサポートが終了しました。NSX 6.3.x にアップグレードする前に、NSX Edge にアップグレードする必要があります。

API の削除と動作の変更

ファイアウォール構成またはデフォルト セクションの削除 :

- デフォルト セクションが指定されている場合、ファイアウォール セクションの削除の要求は拒否されます : `DELETE /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/sectionId`
- デフォルト設定を取得するための新しいメソッドが追加されました。このメソッドの出力を使用して、設定全体または任意のデフォルト セクションを置き換えます。
 - デフォルトの設定を取得する : `GET /api/4.0/firewall/globalroot-0/defaultconfig`
 - 設定全体を更新する : `PUT /api/4.0/firewall/globalroot-0/config`
 - 単一のセクションを更新する : `PUT /api/4.0/firewall/globalroot-0/config/layer2sections|layer3sections/{sectionId}`

次のメソッドから **defaultOriginate** パラメータが削除されました。これは分散論理ルーター NSX Edge アプライアンスの場合のみ適用されます。

- `GET/PUT /api/4.0/edges/{edge-id}/routing/config/ospf`
- `GET/PUT /api/4.0/edges/{edge-id}/routing/config/bgp`

- GET/PUT /api/4.0/edges/{edge-id}/routing/config

NSX 6.3.0 以降の分散論理ルーター Edge アプライアンスで defaultOriginate を true に設定すると失敗します。

すべての IS-IS メソッドを NSX Edge ルーティングから削除：

- GET/PUT/DELETE /4.0/edges/{edge-id}/routing/config/isis
- GET/PUT /4.0/edges/{edge-id}/routing/config

アップグレードに関する注意事項

- [NSX と vSphere に関連するアップグレードの注意事項](#)
- [NSX コンポーネントに関連するアップグレードの注意事項](#)
- [FIPS に関連するアップグレードの注意事項](#)

注：NSX バックアップに SFTP を使用する場合は、「[バックアップとリストア](#)」セクションで、6.3.x 以降でサポートされるセキュリティ アルゴリズムをご確認ください。

注：インストールとアップグレードに影響する既知の問題については、「[インストールとアップグレードに関する既知の問題](#)」セクションを参照してください。

NSX と vSphere に関連するアップグレードの注意事項

- NSX を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 のアップグレード）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「[ホスト クラスタのアップグレード](#)」セクションを参照してください。
- システム要件：NSX のインストールとアップグレードのシステム要件については、NSX 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。

NSX 6.3.0 では、NSX Edge アプライアンスのディスク サイズが変更されました。

- Compact、Large、Quad Large：584 MB のディスク 1 台 + 512 MB のディスク 1 台
- XLarge：584 MB のディスク 1 台 + 2 GB のディスク 1 台 + 256 MB のディスク 1 台
- 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。
- 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 6.3.x へのアップグレードが成功したかを確認するには、[ナレッジベースの記事 KB2134525](#) を参照してください。
- vCloud Networking and Security から NSX 6.3.0 へのアップグレードはサポートされません。まず、サポート対象の 6.2.x リリースにアップグレードする必要があります。
- vSphere 6.5a へのアップグレード：vSphere 5.5 または 6.0 から vSphere 6.5a にアップグレードする場合は、最初に NSX 6.3.0 にアップグレードする必要があります。『[NSX アップグレードガイド](#)』の「[NSX 環境での vSphere のアップグレード](#)」を参照してください。

注：NSX 6.2.x には、vSphere 6.5 との互換性がありません。

- **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、アップグレードする NSX のバージョン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。
- **ハードウェア ゲートウェイ（ハードウェア VTEP）を環境にインストールしている場合**、NSX 6.3.0 へのアップグレードはブロックされます。アップグレードを実行するには、VMware サポートにお問い合わせください。詳細については、[VMware のナレッジベースの記事 KB2148511](#) を参照してください。
- **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 で利用できます。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。

NSX コンポーネントに関連するアップグレードの注意事項

- **Edge Services Gateway (ESG) のアップグレード**：
NSX 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。十分なり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

- NSX Edge アプライアンスをアップグレードする前に NSX 用ホスト クラスタを準備する必要があります : NSX 6.3.0 以降では、NSX Manager と Edge 間で、VIX チャンネルを経由した管理プレーン通信はサポートされません。メッセージ バス チャンネル経由のみがサポートされます。NSX 6.2.x 以前から NSX 6.3.0 以降にアップグレードする場合、NSX Edge アプライアンスのデプロイ先のホスト クラスタが準備されていることと、メッセージング インフラストラクチャのステータスが正常であることを確認する必要があります。NSX 用ホスト クラスタが準備されていない場合、NSX Edge アプライアンスのアップグレードに失敗します。詳細については、『NSX アップグレード ガイド』の [NSX Edge のアップグレード](#) を参照してください。

NSX Edge のデプロイ先であるホストのメッセージング インフラストラクチャのステータスが正常であることを確認するには、次の操作を行います。

- API メソッド GET/api/2.0/nwfabric/status?resource={resourceId} を使用します。resourceId は、クラスタまたはホストの vCenter Server 管理対象オブジェクト ID です (domain-c33 や host-21 など)。クラスタおよびホストのリソース ID を検索する方法については、NSX API ガイドの「vCenter Server オブジェクト ID の検索」を参照してください。
- 応答本文の com.vmware.vshield.vsm.messagingInfra の featureId に対応する status を確認します。

```
<nwFabricFeatureStatus>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <updateAvailable>>false</updateAvailable>
  <status>GREEN</status>
  <installed>>true</installed>
  <enabled>>true</enabled>
  <allowConfiguration>>false</allowConfiguration>
</nwFabricFeatureStatus>
```

- 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。それには、vSphere Web Client を開き、NSX Edge 仮想マシンが常駐する ESXi ホストを見つけ、[管理] > [設定] の順にクリックし、[仮想マシン] で [仮想マシンの起動/シャットダウン] を選択して、[編集] をクリックします。次に、仮想マシンが手動モードにあることを確認します。[自動起動/シャットダウン] リストに追加されていないことを確認してください。
- コントローラ ディスクのレイアウト : NSX 6.2.2 以前のバージョンからアップグレードした場合は、NSX 6.2.3 で追加された新しいディスク レイアウトは使用できません。これは、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、コントローラの安定性を向上するものです。

- 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>
```

- vRealize Operations Manager (vROPs) 6.2.0 より前のバージョンでロード バランシングされたクライアントに正しい暗号バージョンを設定する：vROPs 6.2.0 より前のバージョンの vROPs プール メンバーは TLS バージョン 1.0 を使用しています。このため、NSX のロード 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。手順については、『NSX 管理ガイド』の「[サービス モニターの作成](#)」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"
}
```

- 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： 次の手順を実行します。

- 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。

FIPS に関連するアップグレードの注意事項

- NSX 6.3.0 より前のバージョンから NSX 6.3.0 以降のバージョンにアップグレードする場合は、アップグレードが完了するまで FIPS モードを有効にしないでください。アップグレードが完了する前に FIPS モードを有効にすると、アップグレード済みのコンポーネントとアップグレードされていないコンポーネント間の通信が中断されます。詳細については、『NSX アップグレード ガイド』の「[FIPS モードと NSX アップグレードの理解](#)」を参照してください。
- OS X Yosemite および OS X El Capitan でサポートされる暗号：OS X 10.11 (El Capitan) で SSL VPN クライアントを使用している場合は、AES128-GCM-SHA256、ECDHE-RSA-AES128-GCM-SHA256、ECDHE-RSA-AES256-GCM-SHA38、AES256-SHA、および AES128-SHA 暗号を使用して接続することができ、OS X 10.10 (Yosemite) を使用している場合は AES256-SHA および AES128-SHA 暗号のみを使用して接続することができます。
- NSX 6.3.0 へのアップグレードが完了するまでは FIPS を有効にしないでください。詳細については、『NSX アップグレード ガイド』の「[FIPS モードと NSX アップグレードの理解](#)」を参照してください。
- FIPS モードを有効にする前に、パートナーのソリューションが FIPS モードの認定を受けていることを確認してください。『[VMware 互換性ガイド](#)』と、関連するパートナーのドキュメント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](#)
- [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

新規問題 1740625/1749975：Mac OS での Firefox および Safari のユーザー インターフェイスの問題
Mac OS で Firefox または Safari を使用している場合、NSX Edge の [Networking and Security] ページの [戻る] ナビゲーション ボタンが vSphere 6.5 Web Client で動作せず、Firefox ではユーザー インターフェイスがフリーズする場合があります。

回避策：Mac OS で Google Chrome を使用するか、ホーム ボタンをクリックして操作を続行します。

問題 1700980：セキュリティの脆弱性 CVE-2016-2775 に対応するセキュリティパッチで、クエリ名が長過ぎると lwresd でセグメント障害が発生する場合がある

NSX 6.2.4 には BIND 9.10.4 がインストールされていますが、*named.conf* で lwres を使用しないように設定されているので、製品に脆弱性は発生しません。

回避策：問題による製品への影響はないので、パッチを適用する必要はありません。

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。

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。

新規問題 1734245：Data Security が原因で、6.3.0 へのアップグレードに失敗する

Data Security がサービス ポリシーの一部として設定されている場合、6.3.0 へのアップグレードに失敗します。アップグレードを行う前に、サービス ポリシーから Data Security を削除する必要があります。

新規問題 1801685：6.2.x から 6.3.0 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 6.3.0 へアップグレードし、クラスタ VIB を 6.3.0 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、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および 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と表示されます。そのため、ファイアウォール ルールの発行およびセキュリティ 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>
```

新規問題 1808478：NSX 6.2.x から NSX 6.3.0 へのアップグレード後に vmvisor のメモリを割り当てられない場合、vsfwd サービスの開始に失敗する

NSX 6.2.x から NSX 6.3.0 へのアップグレード後に vmvisor のメモリを割り当てられない場合、vsfwd サービスの開始に失敗します。詳細については、[VMware のナレッジベースの記事 KB2148974](#) を参照してください。

回避策：VMware サポートにお問い合わせください。

新規問題 1818257: VXLAN に拡張 LACP を使用している場合、ESXi 6.0 で NSX 6.2.x から NSX 6.3.0 にホストをアップグレードした後、VTEP 情報がコントローラにレポートされない
拡張 LACP を使用している場合、ESXi 6.0 で NSX 6.2.x から 6.3.0 にアップグレードする際、ホストのアップグレード後に VTEP 情報がコントローラにレポートされません。詳細については、[VMware のナレッジベースの記事 KB2149210](#) を参照してください。

回避策：VMware サポートにお問い合わせください。

新規問題 1791371：ESXi ホストを vSphere 6.5a にアップグレードするとき、ゲスト イントロスペクションと VXLAN の VIB を並行してアップグレードするとアラームが発生する
vSphere 6.5a では、ゲスト イントロスペクションと VXLAN の VIB は別のものです。これらを並行してアップグレードすると、VXLAN VIB のアップグレードでホストの再起動を求めるアラームが発生します。

回避策：vSphere 6.5a にアップグレードするときは、VXLAN VIB を先にインストールしてからゲスト イントロスペクション VIB をインストールします。

新規問題 1805983：NSX 6.2.5、NSX 6.2.6、または NSX 6.3.0 にアップグレードすると、サーバ プールを持たない仮想サーバが動作しなくなる
サーバ プールを持たない仮想サーバでは、HTTP/HTTPS のリダイレクトのみを実行できます。他の機能は動作しません。

回避策：メンバーが含まれないダミーのプールを作成して、仮想サーバに割り当てます。

新規問題 1797307：アップグレードまたは再デプロイ後に、NSX Edge でスプリット ブレインが発生する
場合がある

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。

新規問題 1789989：ホスト クラスタのアップグレード中に、データ プレーンでパケット ロスが発生する
場合がある

VIB アップグレード中に VIB で保持される VSFWD (vShield Firewall Daemon) のパスワード ファイルが削除されるため、VSFWD は古いパスワードを使用して NSX Manager に接続することができず、新しいパスワードが更新されるまで待機しなければなりません。ホストの再起動後、このプロセスが完了するにはしばらく時間がかかりますが、完全に自動化された DRS クラスタでは、準備済みのホストが起動すると仮想マシンの移行がすぐに始まります。しかし、この時点では VSFWD プロセスの準備はできていないため、データ プレーンで短時間のパケット ロスが発生する場合があります。

回避策：準備のできたホストにただちにフェイルバックせずに、新しく準備したホストへの仮想マシンのフェイルバックを遅らせます。

新規問題 1797929：ホスト クラスタのアップグレード後に、メッセージ バス チャネルが停止する
ホスト クラスタ アップグレードの後、vCenter Server 6.0（およびそれ以前）ではイベント「reconnect」が生成されず、その結果 NSX Manager はホスト上でメッセージング インフラストラクチャをセットアップしませんでした。vCenter Server 6.5 で、この問題は修正されました。

回避策：次のようにメッセージング インフラストラクチャを再同期します。

POST <https://<ip>/api/2.0/nwfabric/configure?action=synchronize>

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.messagingInfra</featureId>
  <resourceConfig>
    <resourceId>host-15</resourceId>
  </resourceConfig>
```


</nwFabricFeatureConfig>

新規問題 1802688：NSX 6.2.x から 6.3.0 へのアップグレードでは、分散ファイアウォールのステータスが有効になったことが反映されない

NSX 6.2.x から NSX 6.3.0 にアップグレードし、クラスタ VIB を NSX 6.3.0 にアップグレードした後、アップグレードしたクラスタに新しいホストを追加すると、新しい VIB が新しいホストにインストールされても、関連するホストおよびクラスタのファイアウォール ステータスはビジー状態のままになり、ステータスが更新されません。

回避策：次の手順を実行します。

1. API POST: `https://<NSX-IP>/api/2.0/nwfabric/configure?action=synchronize` を使用して、メッセージ バス同期 API 呼び出しを実行します。これで、ホストとクラスタのファイアウォール ステータスが「Disabled」になります。

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

2. ユーザー インターフェイスの [インストール] > [ホストの準備] ページで、クラスタのファイアウォールを有効にします。これによって、クラスタのすべてのホストの分散ファイアウォールが有効になります。

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、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、6.2.5 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 1600281：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) のインストール ステータスが [サービス デプロイ] タブで「失敗」と表示される

ゲスト イントロスペクション USVM のバックアップ データストアがオフラインになるか、アクセスできなくなると、USVM をリカバリするために再起動または再デプロイが必要になる場合があります。

回避策：USVM を再起動または再デプロイしてリカバリします。

問題 1660373：vCenter Server で期限切れの NSX ライセンスが適用される

vSphere 5.5 Update 3 または vSphere 6.0.x では、NSX ライセンスに vSphere Distributed Switch が含まれます。しかし、NSX ライセンスの有効期限が切れると、vCenter Server は vSphere Distributed Switch への ESX ホストの追加を許可しません。

回避策：vSphere Distributed Switch にホストを追加するには、有効な NSX ライセンスが必要です。

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 へアップグレードすると、[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 1636916：vCloud Air 環境で vCloud Networking and Security (vCNS) 5.5.x から NSX 6.x へ NSX Edge をアップグレードすると、Edge ファイアウォール ルールで送信元のプロトコルの種類が「any」から「tcp:any, udp:any」に変更される

このために ICMP トラフィックがブロックされ、パケット ドロップが発生することがあります。

回避策：NSX Edge のバージョンをアップグレードする前に、Edge ファイアウォール ルールをより具体的に作成し、必要に応じてプロトコルの種類を追加し、「any」を特定の送信元ポート値に置き換えます。

問題 1660355：NSX 6.1.5 から NSX 6.2.3 以降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、NSX 6.1.5 から NSX 6.2.3 以降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 NSX 6.2.3 以降の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 1474238：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 1332563：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 1473537：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 1215460：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。

問題 1413125：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。

問題 1266433：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 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 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 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 ログに出力される場合があります。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。

[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。

NSX Manager に関する既知の問題

新規問題 1800820：古いユニバーサル分散論理ルーター (UDLR) インターフェイスがシステムから削除されている場合、セカンダリ NSX Manager で UDLR インターフェイスの更新に失敗する
プライマリ NSX Manager でレプリケータが動作しなくなった場合、プライマリ NSX Manager でユニバーサル分散論理ルーター (UDLR) とユニバーサル論理スイッチ (ULS) のインターフェイスを削除して、新しいインターフェイスを作成した後、セカンダリ NSX Manager にレプリケートする必要があります。この場合、セカンダリ NSX Manager では UDLR インターフェイスが更新されません。これは、レプリケーション中にセカンダリ NSX Manager で新しい ULS が作成されますが、UDLR は新しい ULS と接続されないためです。

回避策：新しいバックアップとして、ULS が作成されたプライマリ NSX Manager でレプリケータが実行されていることを確認して、UDLR インターフェイス (LIF) を削除し、同じ ULS がバックアップする UDLR インターフェイス (LIF) を再作成します。

新規問題 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。

回避策：VMware サポートにお問い合わせください。

新規問題 1772911：NSX Manager の処理がディスク容量の消費とともに低速になり、タスクとジョブのテーブル サイズが増加して CPU の使用率がほぼ 100% になる
以下の状況が発生します。

- NSX Manager の CPU 使用率が 100% になる、または定期的に 100% に到達し、追加のリソースを NSX Manager アプライアンスにリソースに追加しても状況が変わらない。
- 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、最も高い CPU サイクルを消費している Java プロセスが表示される。
- NSX Manager CLI 上で `show filesystems` コマンドを実行すると、`/common` ディレクトリの CPU 使用率が「> 90%」のように非常に高い数値を示す。
- 一部の設定変更のタイムアウト（50 分以上かかる場合がある）が発生し変更が有効にならない。

詳細については、[VMware のナレッジベースの記事 KB2147907](#) を参照してください。

回避策： この問題の解決策については、VMware サポートにお問い合わせください。

新規問題 1785142：プライマリとセカンダリの NSX Manager 間で通信がブロックされると、プライマリ NSX Manager に「同期の問題」と表示されるまでに時間がかかる
プライマリおよびセカンダリ NSX Manager 間の通信がブロックされると、プライマリ NSX Manager に「同期の問題」と表示されるまで時間がかかります。

回避策：通信が再度接続されるまで約 20 分待機してください。

新規問題 1786066：NSX の Cross-vCenter インストールでは、セカンダリ NSX Manager を切断すると、その NSX Manager はセカンダリとして再接続できない可能性がある

NSX の Cross-vCenter インストールで、セカンダリ NSX Manager を切断すると、後でその NSX Manager をセカンダリ NSX Manager として再追加することができない場合があります。NSX Manager をセカンダリとして再接続しようとすると、NSX Manager は vSphere Web Client の [管理] タブに「Secondary」としてリストされますが、プライマリへの接続は確立されません。

回避策：次の手順を実行します。

1. プライマリ NSX Manager からセカンダリ NSX Manager を切断します。
2. プライマリ NSX Manager にセカンダリ NSX Manager を再度追加します。

新規問題 1713669：データベース テーブル `ai_useripmap` が大きくなりすぎるとディスクがいっぱいになるため、NSX Manager が機能しなくなる

この問題によって NSX Manager アプライアンス ディスクがいっぱいになり、NSX Manager が機能しなくなります。再起動しても postgres プロセスを開始できません。「/common」パーティションがいっぱいです。これは一般に、イベント ログ サーバ (ELS) に大きな負荷のかかるサイトおよび大量のゲスト イントロスペクション (GI) トラフィックが生じるサイトで発生します。Identity Firewall (IDFW) を使用するサイトでは、頻繁にこの問題が発生します。詳細については、[VMware のナレッジベースの記事 KB2148341](#) を参照してください。

回避策：この問題の解決方法については、VMware サポートにお問い合わせください。

問題 1787542：プライマリ NSX Manager でデータベースが復旧した後に、セカンダリ NSX Manager ログに例外が記録される

プライマリでデータベースをリストアした後、リカバリしたユニバーサル分散ファイアウォール セクションがセカンダリ NSX Manager に表示されません。

回避策：なし。セカンダリ NSX Manager を再起動してリカバリします。

新規問題 1715354：REST API の可用性の遅延

FIPS モードを切り替えると、NSX Manager が再起動した後に NSX Manager API が起動して実行状態になるまでしばらく時間がかかります。API がハングしているように見えることがありますが、これは、コントローラが NSX Manager との接続を再度確立するまでに時間がかかるためです。NSX API サーバが起動して実行状態になるまで待機し、すべてのコントローラが接続された状態になったことを確認してから操作を実行することを推奨します。

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 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 1534877：ホスト名が 64 文字を超える場合、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。

問題 1537258：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。

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 1492880：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 1468613：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。

論理ネットワークと NSX Edge に関する既知の問題

新規問題 1825416: NSX for vSphere 6.3.x にアップグレードすると、vCloud Director 8.20 で、フェンシングされた vApp との通信に失敗する

vCloud Director 8.20 で、NSX 6.3.x および NSX Edge Gateway 6.3.x にアップグレードすると、フェンシングされた vApp に問題が発生し、フェンシングされたネットワーク内の仮想マシンがゲートウェイと通信できなくなります。詳細については、[VMware のナレッジベースの記事 KB2150010](#) を参照してください。

回避策： VMware サポートにお問い合わせください。

新規問題 1781438：ESG または分散論理ルーターの NSX Edge アプライアンスで、BGP パス属性 MULTI_EXIT_DISC を複数回受信したときに、ルーティング サービスがエラー メッセージを送信しない BGP パス属性 MULTI_EXIT_DISC を複数回受信しても、Edge ルーターまたは分散論理ルーターがエラー メッセージを送信しません。RFC 4271 [Sec 5] により、特定の UPDATE メッセージのパス属性フィールドに同じ属性（同じタイプの属性）を複数回使用することはできません。

回避策：なし。

新規問題 1860583：DNS にアクセスできない場合、FQDN を使用してリモートの syslogger を設定すると問題が発生する

NSX Edge でリモートの syslogger が FQDN を使用して設定されていて、DNS にアクセスできない場合、ルーティング機能に影響する可能性があります。この問題は必ず発生するとは限りません。

回避策：FQDN ではなく IP アドレスを使用することをお勧めします。

新規問題 1791264：トランスポート ゾーンをダブルクリックすると、CDO モードの有効化/無効化に失敗する

vSphere Web Client でトランスポート ゾーンをダブルクリックし、[サマリ] ページから CDO モードを有効または無効にしても、実行されません。

回避策：次の手順を実行します。

1. トランスポート ゾーンの一覧ページに戻ります。[インストール] > [論理ネットワークの準備] > [トランスポート ゾーン] に移動して、目的のトランスポート ゾーンを選択します。
2. [アクション] ドロップダウン メニューから [CDO モードの有効化] / [CDO モードの無効化] を選択します。
3. これにより、選択したアクションが適用されます。

新規問題 1773500：無効なルート (0.0.0.0/32) により NSX がクラッシュする

NSX 分散論理ルーターでルート 0.0.0.0/32 をプッシュしても、このルートがサポートされていないため拒否されます。ただし、関連する LIF を削除し、同じサブネット上の IP アドレスを使用して再度追加すると、クラッシュ (PSOD) が発生します。

回避策：0.0.0.0/32 は有効なルートではありません。このルートを設定しないでください。または、このルートをブロックするため、ルートマップを使用してください。

新規問題 1769941：ARP リプライ重複発生時に、分散論理ルーターの PMAC によって、L2VPN のブリッジ テーブルがポイズニングされる

クライアント仮想マシンから ARP リプライを受信する場合、ホスト上の L2VPN サーバの VXLAN トランク ポートからは、宛先 MAC アドレスが pMAC に設定されている ARP リプライをドロップせず、ブリッジの MAC テーブルがポイズニングされ、結果としてトラフィックにドロップが発生します。

回避策：この問題を回避するには、宛先が pMAC に設定された ARP リプライをドロップできるように、VXLAN トランクの dvport 用にトラフィック フィルタを追加します。

トラフィック修飾子を追加する手順は次のとおりです。

1. NSX Edge が接続されている dvport に移動します。
2. [設定の編集] > [トラフィック フィルタリングおよびマーキング] の順に移動します。
3. 宛先が pMAC に設定された MAC 修飾子を追加します。

新規問題 1782321：高可用性のステータスが正しく表示される場合でも、一部の NSX Edge でスプリット ブレインが発生する場合がある

高可用性構成で競合状態が発生すると、NSX 6.2.5 以降にアップグレードした NSX Edge の一部で、高可用性のステータスが正しく表示されていてもスプリット ブレインが発生する可能性があります。これは、Edge の再デプロイ後にも発生します。

回避策：スタンバイ NSX Edge を再起動してください。

新規問題 1764258：サブインターフェイスが設定された NSX Edge で高可用性によるフェイルオーバーまたは強制同期が実行されると、トラフィックが最大 8 分間ブラックホール状態になる

サブインターフェイスを介して、高可用性によるフェイルオーバーをトリガするか、強制同期を開始した場合、最大 8 分間ブラックホール状態が発生し、トラフィックが失われます。

回避策：高可用性ではサブインターフェイスを使用しないでください。

新規問題 1771760：NAT が有効になっている場合、OID タイプ Counter64 を含む SNMP 応答パケットが NSX Edge によりドロップされる

NSX Edge の SNMP ALG は、Counter64 タイプを含む SNMP 応答パケットを処理できないため、パケットがドロップされます。したがって、要求に対する応答はクライアントに送信されません。

回避策：この問題が発生した場合は、VMware サポートまでご連絡ください。

新規問題 1767135：ロード バランサの証明書とアプリケーション プロファイルにアクセスしようとするとエラーが発生する

セキュリティ管理者の権限と Edge スコープが設定されているユーザーは、ロード バランサの証明書とアプリケーション プロファイルにアクセスできません。vSphere Web Client にエラー メッセージが表示されます。

回避策：なし。

新規問題 1792548：NSX Controller で次のメッセージが表示され、スタックする場合がある：Waiting to join cluster

NSX Controller で次のメッセージが表示され、スタックする場合がある：Waiting to join cluster (CLI コマンド：show control-cluster status)。この問題は、NSX Controller の起動中に NSX Controller の eth0 インターフェイスと breth0 インターフェイスに同じ IP アドレスが設定されることが原因で発生します。NSX Controller で次の CLI コマンドを使用すると、インターフェイスの IP アドレスを確認できます。show network interface

回避策：VMware サポートにお問い合わせください。

新規問題 1747978：NSX Edge 高可用性のフェイルオーバー後に、OSPF 隣接関係が MD5 認証で削除される

NSX for vSphere 6.2.4 環境で、NSX Edge が高可用性構成となっており、OSPF グレースフル リスタートが設定され、認証に MD5 が使用される場合、OSPF は正常に起動できません。隣接関係は、Dead タイマーが OSPF ネイバー ノード上で終了した後にのみ発生します。

回避策：なし。

新規問題 1803220：コントローラとホスト間の接続が停止すると、CDO が有効なホストへの VXLAN 接続が失われる

コントローラ クラスタ全体が停止している、またはアクセスできない場合でも、Controller Disconnected Operation (CDO) 機能は VXLAN 接続を維持します。ただし、コントローラ クラスタが起動していても、ホストとの接続が失われると、コントローラに接続された他のホストからそのホストへのデータ プレーン トラフィックは失われる場合があります。この条件が発生すると、ホストは VNI ごとの VTEP リストから削除されているため、リモート ホストが送信した ARP が失われます。コントローラとの接続を失ったホストからのトラフィックの場合は、CDO 機能により、正しい宛先に送信されます。

新規問題 1804116：分散論理ルーターが、NSX Manager との通信を失ったホスト上で不整合状態になる
分散分散論理ルーターがパワーオンの状態または NSX VIB のアップグレード/インストールの失敗またはホスト通信の問題が原因で、NSX Manager との通信を失ったホスト上に再デプロイされると、分散論理ルーターは不整合の状態になり、Force-Sync を使用した連続自動リカバリの操作に失敗します。

回避策：ホストと NSX Manager 間の通信の問題を解決した後、NSX Edge を手動で再起動して、すべてのインターフェイスが起動するまで待機します。force-sync を使用した自動リカバリ プロセスにより、NSX Edge が再起動されるため、この回避策は分散論理ルーターには必要ですが NSX Edge Services Gateway (ESG) には必要ありません。

新規問題 1783065：IPv4 および IPv6 アドレスが共存する場合、TCP と一緒に UDP ポートのロード バランサを設定することができない

UDP は ipv4-ipv4、ipv6-ipv6（フロントエンド - バックエンド）のみをサポートします。NSX Manager では、IPv6 のリンク ローカル アドレスさえも読み取られ、グループ オブジェクトの IP アドレスとしてプッシュされてしまい、ロード バランサ設定で使用する IP プロトコルを選択することができないというバグがあります。

次はこの問題が発生するロード バランサ設定の例です。

ロード バランサ設定で、「vCloud_Connector」プールはグループ オブジェクト (vm-2681) でプール メンバーとして設定されています。このオブジェクトには IPv4 と IPv6 のアドレスが両方とも含まれているため、これはロード バランサの L4 エンジンでサポートされません。

```
{
    "algorithm" : {
        ...
    },
    "members" : [
        {
            ... ,
            ...
        }
    ],
    "applicationRules" : [],
    "name" : "vCloud_Connector",
    "transparent" : {
        "enable" : false
    }
}

{
    "value" : [
        "fe80::250:56ff:feb0:d6c9",
        "10.204.252.220"
    ],
    "id" : "vm-2681"
}
```

回避策：

- オプション 1：プール メンバーのグループ オブジェクトの代わりに、プール メンバーの IP アドレスを入力します。
- オプション 2：仮想マシンで IPv6 を使用しないようにします。

新規問題 1773127：セットアップするホストおよび論理スイッチの数が非常に多い場合、特定の論理スイッチに関連するホストの表示画面が正常に読み込まれない

ホスト数の多いセットアップで [論理スイッチ] > [関連オブジェクト] > [ホスト] の順に選択すると、数分後に vSphere Web Client は読み込みに失敗し、以下のエラー メッセージが表示されます。**バックエンドのタスクに 120 秒以上かかったためにデータ サービスはタイムアウトしました。**これは、NSX Manager へのリモート API 呼び出しが結果を返すまでに長い時間がかかるために発生します。

回避策：この問題を回避する方法は 2 つあります。

- オプション 1：「[VMware ナレッジベースの記事 KB2040626](#)」に従って API タイムアウトの値を増やすことで、この問題を回避できます。このタイムアウト値を増やした後で、vSphere Web Client の再起動が必要になる場合があります。通常、タイムアウトの値を増やすとエラーはなくなりますが、ページが再度読み込まれるまでに約 2 ～ 4 分待機する必要があります。

- オプション 2：関連するホストを正確に表示することのみが目的であれば、[ホーム]>[ネットワーク]>[ポート グループ]>[関連オブジェクト]>[ホスト]の順に移動して、論理スイッチに関連付けられたホストのリストを表示することができます。

新規問題 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+XAUTH を使用して認証の要求を送信すると、Edge には次のエラー メッセージ「initial Main Mode message received on XXX.XXX.XX.XX:500 but no connection has been authorized with policy=PSK+XAUTH」が表示され、IPsec を確立することができません。

回避策：ANY の代わりに、IPsec VPN 設定で特定のピア 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) を使用します。

新規問題 1770114：ホストの準備に成功した後、クラスタ レベルのエラー メッセージが残ったままになる
IP アドレス プールの数が十分でないクラスタに IP アドレス プールを割り当て、ホストをそのクラスタに追加しようとする、と「Insufficient IP addresses」というエラーが表示されます。このプールを変更して IP アドレスを追加した場合、クラスタへのホストの追加は成功しますが、クラスタ レベルでエラー メッセージが残ります。

回避策：VMware サポートにお問い合わせください。

問題 1789088：NSX Edge が **grub** コマンドライン プロンプトでスタックする
NSX Edge が起動に失敗し、grub コマンドライン プロンプトでスタックする場合があります。

回避策：

- 最初に、次の項目を確認します。
 1. set コマンドで既存の環境を確認します。
 2. ls および cat コマンドを使用して /boot/grub/grub.cfg ファイルを見つけ、ダンプします。

```
grub> ls /boot
grub> ls /boot/grub
grub> cat /boot/grub/grub.cfg
```
 3. この時点でホスト ログをキャプチャします。（問題発生から時間が経っていない方が望ましい）。NFS ストレージの問題を示す NFS ログが見つかる場合があります。
- 次に、NSX Edge を手動で起動します。次の手順を順序通りに実行します（前の手順で Edge が正常に起動しなかった場合のみ次のオプションに進んでください）。
 1. vSphere Web Client のパワー リセット オプションを選択して Edge 仮想マシンを再起動します。
 2. または、grub 構成ファイルを再度指定して、メニューを読み込むと、Edge が迅速に起動します。grub プロンプトで次のコマンドを実行します。

```
grub> configfile /boot/grub/grub.cfg
```
 3. または、grub プロンプトで次のコマンドを実行します。

```
grub> insmod ext2
grub> set root=(hd0,1)
grub> linux /boot/vmlinuz loglevel=3 root=/dev/sda1
grub> boot
```


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 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 1753621：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 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トが維持される

「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 認証で使用され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 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 1556924： VXLAN の「Would block」エラーで、L3 接続が失われる

ホストで分散論理ルーター (DLR) の LIF が設定されている一方で、基盤となる VXLAN レイヤーがホストで完全に準備されていない場合、DLR LIF の一部に影響することがあります。このため、分散論理ルーターに属する仮想マシンの一部にアクセスできません。「*Failed to Create VXLAN trunk status: Would block*」というログが、`/var/log/vmkernel.log` ファイルに表示される場合があります。

回避策： LIF を削除して再度作成します。または、問題が発生している ESX ホストを再起動します。

問題 1647657： 分散論理ルーターを有効にしている ESXi ホストで `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ルートが 2,000 個までしか表示されない

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： なし。

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 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 1604514：管理対象外の分散論理ルーター (DLR) のデフォルト ゲートウェイを編集/設定し、[発行] をクリックすると失敗する

管理対象外の分散論理ルーターにデフォルト ゲートウェイを追加すると、発行に失敗し、「アドミニストレーティブ ディスタンスは、NSX Edge 仮想マシンがデプロイされている NSX Edge バージョン 6.2.0 以降でのみサポートされます」というエラーが表示されます。この問題は、デフォルトのアドミニストレーティブ ディスタンスを表す「1」がユーザー インターフェイス上に入力されてしまうために発生します。

回避策： デフォルトで表示され、アドミニストレーティブ ディスタンスを表す「1」を削除します。

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、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 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 1534603：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 では稼動中と表示されます。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 1534799：一番大きい数字の 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。

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 1089745：複数の分散論理ルーター Edge アップリンク上で OSPF を設定できない

現在、複数の分散論理ルーター Edge のアップリンク（合計 8 つ）に OSPF を設定することはできません。この制限は、分散論理ルーターの複数のインスタンスが 1 つの転送アドレスを共有するために発生します。

回避策： これは現在のシステムの制限であり、回避策はありません。

問題 1498965：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 1494025：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 1288487：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?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. [DVManager] > [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。

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。

セキュリティ サービスに関する既知の問題

新規問題 1847753: ALG が有効なプロトコルのフローを取得すると、ホストで障害が発生し、パープル スクリーンが表示される

NSX for vSphere 6.2.4 から 6.3.0 または 6.3.1 へのアップグレード後、環境でフロー モニタリングを有効にすると、ESXi ホストでパープル スクリーンが表示されます。回避策および詳細については、[VMware のナレッジベースの記事 KB2149908](#) を参照してください。

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。

回避策 : NetX の最小要件を満たす次の ESXi バージョンに ESXi ホストをアップグレードしてください。

- ESXi 5.5 パッチ 10
- ESXi 6.0U3
- ESXi 6.5

新規問題 1676043 : 同じ仮想マシンのエントリを 2 つ同時に追加すると除外リストからその仮想マシンが削除される

ユーザー インターフェイスを更新せずに、2 人のユーザーが同じ仮想マシンのエントリを除外リストに同時に追加すると、追加済みの仮想マシンが除外リストから削除されます。

回避策 : 仮想マシンを除外リストに追加する前に、vSphere Web Client ユーザー インターフェイスを更新します。

新規問題 1770259 : 分散ファイアウォール ルールの **appliedTo** フィールドを変更して、**appliedTo** オブジェクトを複数にすることはできない

分散ファイアウォール ルールを vNIC や仮想マシンのセット、クラスタ、データセンターに適用し、発行した後に、**appliedTo** フィールドを変更してオブジェクトを追加する場合、発行は正常に終了しますが、変更は有効になりません。

回避策 : なし。

新規問題 1798779 : NSX を 6.2.x から 6.3.0 にアップグレードした後、vSphere Web Client の GUI は、誤ってユニバーサル セキュリティ タグを追加可能にする

6.3.0 には、ユニバーサル セキュリティ タグが採用されています。NSX 6.3.0 へのアップグレードの前に 6.2.x で作成されたユニバーサル セキュリティ グループにユニバーサル セキュリティ タグを追加しようとすると、操作が失敗し「The requested member is not a valid member」というエラー メッセージが表示されます。NSX 6.2.x ユニバーサル セキュリティ グループにユニバーサル セキュリティ タグを追加することはできないため、エラー メッセージが表示されるのは、通常の動作です。エラー メッセージの内容に問題があります。

回避策 : アップグレードの後、NSX 6.3.0 ユニバーサル セキュリティ グループを作成し、そのグループにユニバーサル セキュリティ タグを追加します。

新規問題 1799543 : NSX 6.2.x から NSX 6.3.0 にアップグレードした後、最初のアクティブ/スタンバイユニバーサル セキュリティ グループを作成するときに、NSX 6.2.x ユニバーサル セキュリティ グループとアクティブ/スタンバイでないユニバーサル セキュリティ グループを選択できることが、vSphere Web Client によって誤って表示される

最初のアクティブ/スタンバイ ユニバーサル セキュリティ グループを作成するときに、vSphere Web Client ユーザー インターフェイスには、NSX 6.2.x で作成されたユニバーサル セキュリティ グループを追加できることが示されます。この操作は失敗し、「The requested member is not a valid member」というエラー メッセージが表示されます。

回避策：少なくとも 1 つのアクティブ/スタンバイ ユニバーサル セキュリティ グループを作成し、続いて、次のアクティブ/スタンバイ ユニバーサル セキュリティ グループを作成すれば、この問題は発生しません。

新規問題 1786780：Service Composer ユーザー インターフェイスのポリシーの順番を変更/移動すると、CPU の使用率が高くなり、処理に時間がかかる

Service Composer ユーザー インターフェイスからポリシーの順番の変更または移動を行うと、CPU の使用率が高くなり、処理に時間がかかります。

回避策：次の手順が役に立ちます。

- ポリシーの作成中に、ポリシーに正しい優先順位（重み）を指定します。それにより、最初の操作でポリシーは適切な場所に配置され、ポリシーの順序を変える必要がなくなります。
- ポリシーを別の場所に移動する必要がある場合は、移動するポリシーを編集して優先順位（重み）を適切な値に変更します。これによって、単一のポリシーが変更され、操作は迅速に完了します。

新規問題 1787680：NSX Manager が移行モードにある場合、ユニバーサル ファイアウォール セクションの削除に失敗する

移行モードで NSX Manager のユーザー インターフェイスからユニバーサル ファイアウォール セクションを削除し、発行しようとする、発行に失敗し、その結果 NSX Manager をスタンドアロン モードに設定できなくなります。

回避策：Single Delete Section REST API を使用してユニバーサル ファイアウォール セクションを削除してください。

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の vNIC-IP アドレス マッピングを変更しようとしています。

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 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すると、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 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、重複と判断できません。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-lfd96022-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-lfd96022-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-lfd96022-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-lfd96022-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と、ルールの発行に失敗します。

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とすると失敗します。

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 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。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。

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。

ソリューションの相互運用性に関する既知の問題

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、再デプロイを含む NSX Edge のアクションを vCloud Director から実行すると失敗します。

回避策: vCenter Server の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。

NSX Controller に関する既知の問題

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 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。

解決した問題

新規 NSX 6.3.0 で解決した問題

NSX 6.3.0 で解決した問題には次のトピックが含まれます。

- [NSX 6.3.0 で解決した一般的な問題](#)
- [NSX 6.3.0 で解決したインストールとアップグレードに関する問題](#)
- [NSX 6.3.0 で解決した NSX Manager に関する問題](#)
- [NSX 6.3.0 で解決したネットワークと Edge サービスに関する問題](#)
- [NSX 6.3.0 で解決したセキュリティ サービスに関連する問題](#)
- [NSX 6.3.0 で解決したソリューションの相互運用性に関連する問題](#)

NSX 6.3.0 で解決した一般的な問題

解決した問題 1497389 : NSX 管理者権限を持つユーザーが自身の権限を変更して、より強い権限を持つユーザー ロールであるエンタープライズ管理者になることができる NSX 6.3.0 以降では NSX 管理者権限を持つユーザーがユーザー管理を行えないように仕様が変更され、エンタープライズ管理者権限を持つユーザーのみがユーザー管理を行うことができます。6.3.0 で、この問題は修正されました。

解決した問題 1575342/1719402：NSX for vSphere 6.x 環境で、サービス仮想マシン (SVM) の移行時 (vMotion/SvMotion) に、サービスが中断されるか、ESXi ホストがクラッシュすることがある

6.3.0 以降、vMotion/SvMotion を使用してサービス仮想マシン (SVM) を移行することはできませんでした。サービス仮想マシンが正常に動作するには、デプロイされたホストに配置しておく必要があります。

別のホストへの移行は可能でしたが、サポート対象ではなく、サービス中断やホストの問題の原因になっていました。

詳細については、[VMware のナレッジベースの記事 KB2141410](#) を参照してください。6.3.0 で、この問題は修正されました。

解決した問題 1708769：NSX でスナップショットを作成した後にサービス仮想マシン (SVM) の遅延が大きくなる

この問題は、サービス仮想マシン (SVM) のスナップショット作成によってネットワークに遅延が加わるために発生することがあります。また、環境内で実行しているバックアップ アプリケーションが、スナップショットを作成している場合があります。6.3.0 で、この問題は修正されました。

解決した問題 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 6.2.4/6.2.5 環境の NSX Controller は、ストレージの障害が発生すると読み取り専用モードになる場合があります。また、その状態を解除するためにコントローラを削除して再デプロイすると、一部の仮想マシンが通信できなくなる可能性があります。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。6.3.0 で、この問題は修正されました。

解決した問題 1662842：ゲスト イントロスペクション：解決できない Windows セキュリティ ID (SID) を解決しようとする Mux とユニバーサル サービス仮想マシン (USVM) の接続が失われる

ゲスト イントロスペクション サービスが「警告」状態になり、個々のゲスト イントロスペクションが「警告」状態になったり、安定した状態に戻ったりします。ゲスト イントロスペクション仮想マシンが再接続するまで、ネットワーク イベントは NSX Manager に配信されません。これは、ゲスト イントロスペクション パスでログイン イベントが検出された場合に、アクティビティ モニタリングと、ID ベースのファイアウォールの両方に影響します。6.3.0 で、この問題は修正されました。

解決した問題 1752051：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。6.3.0 で、この問題は修正されました。

解決した問題 1716328：メンテナンス モードのホストを削除すると、後でクラスタの準備に失敗する

管理者が、NSX を使用する ESXi ホストをメンテナンス モードにして、NSX 準備済みクラスタからそのホストを削除すると、NSX は削除されたホストの ID 番号の記録の削除に失敗します。このような環境では、同じ ID を持つホストが別のクラスタにあるか、削除したホストを別のクラスタに追加した場合、それらのクラスタの準備プロセスに失敗します。6.3.0 で、この問題は修正されました。

解決した問題 1710624：REST API 要求の本文で serverType を指定しない場合、"TYPE" が "WIN2K3" の Windows 2008 イベント ログ サーバが追加される

イベント ログ サーバの API 要求を作成すると、サーバが追加されて "TYPE" が "WIN2K3" になります。イベント ログ サーバを Identity Firewall (IDFW) 用にのみ使用する場合、IDFW が正しく動作しない可能性があります。6.3.0 で、この問題は修正されました。

NSX 6.3.0 で解決したインストールとアップグレードに関する問題

解決した問題 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）置かれることがある

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、「ユニバーサル セクションは、セカンダリ NSX Manager の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。

6.3.0 で、この問題は修正されました。

解決した問題 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。

6.3.0 で、この問題は修正されました。

解決した問題 1495307：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に変更を発行した後、ユーザー インターフェイスと API の両方でステータスが「InProgress」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。6.3.0 で、この問題は修正されました。

解決した問題 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。この問題は NSX 6.3.0 で修正されました。

NSX 6.3.0 で解決した NSX Manager に関する問題

解決した問題 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。6.3.0 で、この問題は修正されました。

NSX 6.3.0 で解決したネットワークと Edge サービスに関する問題

解決した問題 1740231：高可用性インターフェイスで IP アドレスを追加できない

6.3.0 以降では、分散論理ルーター高可用性インターフェイスで IP アドレスを追加できます。この機能は一部の旧バージョンの NSX には搭載されていませんでした。今回、分散論理ルーター高可用性管理インターフェイスの API 動作と一致するようになりました。6.3.0 で、この問題は修正されました。

解決した問題 1716333：Edge HA を有効または無効にしている間に Edge 仮想マシンのサイズまたは配置パラメータを変更すると、余分な Edge 仮想マシンが作成される場合がある

Edge 仮想マシンのサイズまたは配置パラメータ（データストアまたはリソース プールなど）の変更と、Edge HA を有効または無効にする操作を同時に実行すると、NSX 管理対象オブジェクト データベースが破損して、使用できない Edge 仮想マシンが後に残る場合があります。さらに、Cross-vCenter 環境では、後に残った Edge 仮想マシンがセカンダリ サイトにレプリケートされます。6.3.0 で、この問題は修正されました。

解決した問題 1717369：高可用性モードを構成すると、アクティブとスタンバイの両方の Edge 仮想マシンが同じホストに展開される場合がある

この問題は、非アフィニティ ルールが作成されておらず、再展開およびアップグレード時に、非アフィニティ ルールが自動的に vSphere ホストに適用されないことが原因で発生します。既存の Edge で高可用性が有効になっている場合は、この問題は発生しません。

6.3.0 で、この問題は修正されました。以下は正常な動作です。

- vSphere HA を有効にすると、再展開とアップグレード時に、高可用性構成の Edge 仮想マシン用の非アフィニティ ルールが作成されます。
- vSphere HA を無効にすると、高可用性構成の Edge 仮想マシン用の非アフィニティ ルールは作成されません。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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

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します。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。

6.3.0 で、この問題は修正されました。

解決した問題 1704540：NSX L2 ブリッジおよび LACP によって MAC ラーニング テーブルが大量に更新されると、メモリ不足の状態になる

NSX L2 ブリッジは、別のアップリンクの MAC アドレスを認識すると、netcpa プロセスを介して、MAC ラーニング テーブルの変更をコントローラにレポートします。LACP を使用するネットワーク環境は、複数のインターフェイス上の同一の MAC アドレスを学習します。その結果、大量のテーブル更新が発生して、netcpa プロセスのレポートに使用するメモリが不足する可能性があります。[VMware ナレッジベースの記事 KB2147181](#) を参照してください。6.3.0 で、この問題は修正されました。

解決した問題 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。

解決した問題 1772004：高可用性構成の Edge がノード 0 からノード 1 にフェイルオーバーする際に予想よりも時間がかかる

Edge が高可用性構成になっている環境では、ノード 1 からノード 0 へのトラフィックのフェイルオーバーは正常である一方で、ノード 0 からノード 1 へのフェイルオーバーに予想よりも時間がかかります。6.3.0 で、この問題は修正されました。

解決した問題 1726379：IP マルチキャストアドレスの範囲での上限に関して、最後の 3 つのオクテットに 99 を超える値である場合、VXLAN トランク ポートグループ設定が失敗する

セグメント ID の設定時、最後の 3 つのオクテットが 99 を超える (1.100.100.100 など) マルチキャスト IP アドレス範囲の上限値を作成し、それと同じ範囲でマルチキャストまたはハイブリッド論理スイッチを作成すると、VXLAN トランク ポートグループ設定が失敗します。6.3.0 で、この問題は修正されました。

NSX 6.3.0 で解決したセキュリティ サービスに関連する問題

解決した問題 1767402：[適用先] が [セキュリティ グループ] に設定された分散ファイアウォール ルールがホストに発行されない

[適用先] フィールドが [セキュリティ グループ] に設定された分散ファイアウォール ルールが、新しいクラスター内の ESXi ホストにプッシュされません。6.3.0 で、この問題は修正されました。

解決した問題 1743366：潜在的なクラッシュを回避するため NSX しきい値監視がデフォルトで無効になっている

ファイアウォール モジュールの実行中に、NSX はメモリのしきい値の監視を無効にして、潜在的な衝突を回避します。ホストが ESX 6.5P01 または ESX 6.0U3 以降を実行している場合、メモリのしきい値の監視は自動的に有効になります。6.3.0 で、この問題は修正されました。

解決した問題 1491046：IPv4 の IP アドレスが自動承認されない

VMware NSX for vSphere 6.2.x で SpoofGuard ポリシーが「最初の使用を信頼する (TOFU)」に設定されていると、IPv4 IP アドレスが自動承認されません。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。
`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`
6.3.0 で、この問題は修正されました。

解決した問題 1707931：Service Composer に定義されたサービス ポリシーがあり、[ファイアウォール] ユーザー インターフェイスで適用されたフィルタを使用して、ファイアウォール ルールが修正または発行される場合、分散ファイアウォール ルールの順序が変更される

[Networking and Security] > [ファイアウォール] ユーザー インターフェイスで 1 回以上の発行操作を行った後、Service Composer で作成されたサービス ポリシー順序の変更、追加、または削除を実行すると、ファイアウォール ルールの順序が変更され、予期しない問題が発生することがあります。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

解決した問題 1445897：VMware NSX for vSphere 6.1.x および 6.2.x でリファレンス オブジェクトを削除した後、分散ファイアウォール (DFW) ルールの発行に失敗する。6.2.3 で、この問題は修正されました。

解決した問題 1704661/1739613：仮想マシンがネットワーク接続を失い、次のようなエラーが表示される：「PF 状態から復旧できませんでした。制限を超えました」

仮想マシンがネットワーク接続を失い、次のようなエラーが表示される：「PF 状態から復旧できませんでした。制限を超えました」 6.3.0 で、この問題は修正されました。

NSX 6.3.0 で解決したソリューションの相互運用性に関連する問題

解決した問題 1527402 : NSX ネットワーク イントロスペクション ドライバを持つ Windows 仮想マシンで TCP 接続が失われる

VMware NSX for vSphere 6.x 環境では、USVM (ゲスト イントロスペクション SVM) に接続された NSX ネットワーク イントロスペクション ドライバ (vnetflt.sys) を備えた Windows 仮想マシンで、一時的な TCP ネットワーク接続が失われる。6.3.0 で、この問題は修正されました。

解決した問題 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。6.3.0 で、この問題は修正されました。

ドキュメントの改訂履歴

2017 年 2 月 2 日 : NSX 6.3.0 用初版。

2017 年 2 月 3 日 : NSX 6.3.0 用第 2 版。既知の問題 1799543 について記載しました。

2017 年 2 月 22 日 : NSX 6.3.0 用第 3 版。CDO の情報を更新しました。

2017 年 2 月 27 日 : NSX 6.3.0 用第 4 版。既知の問題 1808478 と 1818257 について記載しました。

2017 年 3 月 30 日 : NSX 6.3.0 用第 5 版。既知の問題 1474650 と 1782321 について記載しました。

2017 年 4 月 10 日 : NSX 6.3.0 用第 6 版。アップグレードの注意事項セクションに情報を追加しました。

2017 年 5 月 3 日 : NSX 6.3.0 用第 7 版。vCNS Edge と VIX の廃止に関する情報を追加しました。

2017 年 6 月 2 日 : NSX 6.3.0 用第 8 版。既知の問題 1860583、1781438、および 1825416 を追加しました。

2017 年 6 月 22 日 : NSX 6.3.0 用第 9 版。既知の問題 1847753 について記載しました。

2017 年 8 月 21 日 : NSX 6.3.0 用第 10 版。解決した問題 1463767 について記載しました。また、以前発生していた問題をいくつか削除しました。

2017 年 10 月 2 日 : NSX 6.3.0 用第 11 版。推奨される最小バージョンを更新しました。