

VMware NSX for vSphere 6.3.4 リリース ノート

VMware NSX for vSphere 6.3.4 | 2017 年 10 月 12 日リリース | ビルド 7087695

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。

- [NSX 6.3.4 の新機能](#)
- [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](#)
- [FIPS コンプライアンス](#)
- [改訂履歴](#)
- [解決した問題](#)
- [既知の問題](#)

NSX 6.3.4 の新機能

NSX 6.3.4 に関する重要な情報： VMware のナレッジベースの記事 [KB2151719](#) と [KB000051144](#) に記載されている問題を解決するため、NSX for vSphere 6.3.4 が再パッケージされました。最初にリリースされたビルド 6845891 はビルド 7087695 に変更されました。詳細については、ナレッジベースの記事を参照してください。アップグレードの情報については、[アップグレードに関する注意事項](#)を参照してください。

NSX for vSphere 6.3.4 では、ユーザーから報告された複数のバグが修正されています。詳細については、[解決した問題](#)を参照してください。

以前のバージョンのリリース ノート：

- [NSX 6.3.3](#)
- [NSX 6.3.2](#)
- [NSX 6.3.1](#)
- [NSX 6.3.0](#)

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ックス](#)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。
 - NSX 6.3.2 と NSX 6.3.3 では、NSX の相互運用性に必要な vSphere の最小バージョンが異なります。詳細については、[VMware 製品の相互運用性マトリックス](#)を参照してください。

製品またはコンポーネント

推奨されるバージョン

NSX for vSphere

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。

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。

ゲスト イントロスペクション (Windows)

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 イントロスペクション ベースの機能には、VMware Tools の最新バージョンが必要です。

- 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。
- Windows Server 2016 には VMware Tools 10.1.10 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 イントロスペ
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)

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 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 を削除：NSX 6.3.0 から、NSX Data Security 機能が削除されました。
- 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。
- 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。
- 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。
- vCNS Edge のサポートを終了：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 /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にのみ適用されます。

- 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

CLI の削除と動作の変更

NSX Controller ノードで、サポートされていないコマンドを使用しないでください。

NSX Controller ノードで NTP と DNS を設定する場合に、ドキュメントに記載されていないコマンドが使用できてしまう場合があります。ただし、これらのコマンドはサポートされていないため、NSX Controller ノードでは使用しないでください。『NSX CLI 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。

アップグレードに関する注意事項

- [アップグレードに関する全般的な注意事項](#)
- [NSX コンポーネントのアップグレードに関する注意事項](#)
- [FIPS のアップグレードに関する注意事項](#)

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。

アップグレードに関する注意事項

- NSX 6.3.4 ビルド 6845891 から NSX 6.3.4 ビルド 7087695 へのアップデート：NSX Manager と NSX Controller クラスタのみアップグレードが必要になります。ホスト、NSX Edge、ゲスト イントロスペクションをアップグレードする必要はありません。
- NSX の完全なアップグレード：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.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.x 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。
- 相互運用性：アップグレードを行う前に、関連する VMware 製品を[VMware 製品の相互運用性マトリックス](#)で確認してください。
 - vSphere 6.5a 以降へのアップグレード：vSphere 5.5 または 6.0 から vSphere 6.5a 以降にアップグレードする場合は、最初に NSX 6.3.x 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 との互換性はありません。
 - NSX 6.3.3 以降へのアップグレード：NSX 6.3.2 と NSX 6.3.3 では、NSX の相互運用性をサポートする vSphere の最小バージョンが異なります。詳細については、[VMware 製品の相互運用性マトリックス](#)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、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。
- Networking and Security プラグイン：NSX Manager をアップグレードした後は、vSphere Web Client からログアウトし、再度ログインする必要があります。NSX プラグインが正しく表示されない場合には、ブラウザのキャッシュと履歴を消去してください。Networking and Security プラグインが vSphere Web Client に表示されない場合には、[NSX アップグレードガイド](#)の説明に従って、vSphere Web Client サーバをリセットしてください。
- ステートレス環境：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。
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。
 1. 新しい VIB URL を `https://<NSXManager>/bin/vdn/nwfabric.properties` から見つけます。
 2. 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。
 3. 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 コンポーネントのアップグレードに関する注意事項

NSX Manager のアップグレード

- `hmac-sha1` はサポートされていないため、NSX バックアップに SFTP を使用する場合は、NSX 6.3.x へのアップグレード後に `hmac-sha2-256` に変更してください。NSX 6.3.x でサポートされるセキュリティ アルゴリズムについては、[VMware のナレッジベースの記事 KB2149282](#) を参照してください。
- NSX 6.3.3 から NSX 6.3.4 にアップグレードする場合は、[VMware のナレッジベースの記事 KB2151719](#) の回避策を行ってからアップグレードしてください。

コントローラのアップグレード

- NSX 6.3.3 では、NSX Controller アプライアンスのディスク サイズが 20 GB から 28 GB に変わりました。
- NSX 6.3.3 にアップグレードするには、NSX Controller クラスタに 3 台のコントローラ ノードが必要です。コントローラが 3 台未満の場合は、アップグレードを開始する前にコントローラを追加する必要があります。詳細については、[NSX Controller クラスタのデプロイ](#)を参照してください。
- NSX 6.3.3 では、NSX Controller の基盤となるオペレーティング システムが変わりました。NSX 6.3.2 以前から NSX 6.3.3 以降にアップグレードする場合、インプレース アップグレードは実行されません。既存のコントローラが 1 度に 1 つずつ削除され、同じ IP アドレスを使用して新しい Photon OS ベースのコントローラが展開されます。[NSX Controller クラスタのアップグレード](#)を参照してください。

ホスト クラスタのアップグレード

- NSX 6.3.3 で、NSX VIB 名が変更されました。NSX 6.3.3 をインストールすると、esx-vxlan と esx-vsip VIB が esx-nsxv に変更されます。
- アップグレードおよびアンインストールでホストの再起動が不要：vSphere 6.0 以降では、NSX 6.3.x へのアップデート後、NSX VIB を変更する際の再起動が不要になりました。代わりに、VIB を変更するには、ホストをメンテナンス モードにする必要があります。

次のタスクを実行する場合、ホストの再起動は必須ではありません。

- ESXi 6.0 以降での NSX 6.3.0 から NSX 6.3.x へのアップデート。
- ESXi を 6.0 から 6.5.0a 以降にアップデートした後に必要となる NSX 6.3.x VIB のインストール。
注：ESXi のアップグレード時には引き続きホストの再起動が必要になります。

- ESXi 6.0 以降での NSX 6.3.x VIB のアンインストール。

次のタスクを実行する場合、ホストの再起動は必須です。

- NSX 6.2.x 以前から NSX 6.3.x へのアップグレード（すべての ESXi バージョン）。
- ESXi 5.5 での NSX 6.3.0 から NSX 6.3.x へのアップデート。
- ESXi を 5.5 から 6.0 以降にアップグレードした後に必要となる NSX 6.3.x VIB のインストール。
- ESXi 5.5 での NSX 6.3.x VIB のアンインストール。
- 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。

NSX Edge のアップグレード

- 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 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る：NSX 6.3.0 以降では、NSX Manager と Edge 間で、VIX チャ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。

- 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。

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

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（デフォルト値は上の表を参照）。

- 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。

- 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"
}

```

FIPS のアップグレードに関する注意事項

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.x 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。

FIPS コンプライアンス

- **NSS と OpenSwan**：NSX Edge の IPsec VPN では、Mozilla NSS 暗号モジュールを使用しています。本バージョンの NSX では、重大なセキュリティ問題に対応するため、FIPS 140-2 認証を受けていない新しいバージョンの NSS を使用しています。VMware では、このモジュールが正常に動作することを確認していますが、これは公式な検証ではありません。
- **NSS とパスワードの入力**：NSX Edge のパスワード ハッシュで Mozilla NSS 暗号モジュールを使用しています。本バージョンの NSX では、重大なセキュリティ問題に対応するため、FIPS 140-2 認証を受けていない新しいバージョンの NSS を使用しています。VMware は、このモジュールが正常に動作することを確認していますが、これは公式な検証ではありません。
- **コントローラと VPN のクラスタリング**：NSX Controller は、IPsec VPN を使用してコントローラ クラスターに接続します。IPsec VPN では、VMware Linux カーネル暗号モジュール（Photon 1 環境）を使用していますが、このモジュールは現在 CMVP 認証を申請中です。

ドキュメントの改訂履歴

2017 年 10 月 12 日：初版。

2017 年 10 月 27 日：第 2 版。既知の問題 1965859 について記載しました。

2017 年 11 月 9 日：第 3 版。NSX 6.3.4 の新しいビルド情報を記載しました。解決した問題 1989763 について記載しました。既知の問題に追加した問題：1783528、1843197

2019 年 5 月 13 日：第 4 版。「ホスト クラスターのアップグレード」セクションを更新しました。

解決した問題

解決した問題には、次のトピックが含まれます。

- [NSX 6.3.4 で解決したネットワークと Edge サービスに関する問題](#)
- [NSX 6.3.4 で解決した NSX Controller に関する問題](#)

NSX 6.3.4 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 1970527**：分散論理ルーターの ARP テーブルが 5,000 の制限を超えると、ARP が仮想マシンの解決に失敗する
この問題は NSX 6.3.4 で修正されました。
- **解決した問題 1961105**：コントローラの再起動時にハードウェア VTEP との接続が切断する
特定のハードウェア VTEP 設定が NSX Manager から NSX Controller にプッシュされると、バッファ オーバーフロー例外が発生します。このオーバーフローが原因で、NSX Controller が完全なハードウェア ゲートウェイ設定を取得できなくなります。*この問題は NSX 6.3.4 で修正されました。*

NSX 6.3.4 で解決した NSX Controller に関する問題

- **解決した問題 1955855**：API サーバのリファレンス ファイルのクリーンアップにより、コントローラの API 経由でコントローラに接続できなくなる
必要なファイルがクリーンアップされると、トレースフローなどのワークフローやセントラル CLI が機能しなくなります。外部イベントによって NSX Manager とコントローラ間の TCP 接続が切断されると、NSX Manager は API 経由でコントローラに接続できなくなり、ユーザー インターフェイスにコントローラが切断状態と表示されます。これにより、データパスに影響が及ぶことはありません。*この問題は NSX 6.3.4 で修正されました。*
- **問題 1989763**：ユーザー アカウントのパスワードが期限切れで NSX Controller がデプロイされな

い

NSX Controller のユーザー アカウントの有効期間は 90 日間です。このため、ビルド作成日から 90 日が経過すると、NSX Controller のユーザー アカウントのパスワードが期限切れになります。データ パスへの影響はありません。

回避策： [VMware のナレッジベースの記事 KB000051144](#) を参照してください。

この問題は、NSX 6.3.3 bビルド 7087283 および NSX 6.3.4 ビルド 7087695 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 Controller 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](#)

一般的な既知の問題

- **問題 1874863**：ローカル認証サーバで SSL VPN サービスを無効にして有効にすると、変更後のパスワードで認証されない
ローカル認証を使用するときに、SSL VPN サービスを無効にして再度有効にすると、変更後のパスワードでログインできません。

詳細については、[VMware ナレッジベースの記事 KB2151236](#) を参照してください。

- **問題 1702339**：脆弱性スキャナが Quagga bgp_dump_routes の脆弱性 (CVE-2016-4049) をレポートすることがある
NSX for vSphere で、脆弱性スキャナが Quagga bgp_dump_routes の脆弱性 (CVE-2016-4049) をレポートすることがあります。NSX for vSphere は Quagga を使用しますが、この脆弱性の原因となる BGP 機能は使用していません。この脆弱性アラートは、無視しても問題ありません。

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 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 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。

- **問題 1932907** : ゲスト イントロスペクション サービス仮想マシン (GI SVM) のアップグレードに失敗する
ゲスト イントロスペクション サービス仮想マシン (GI SVM) をアップグレードすると、インストール ステータスが「失敗」になります。この問題は、クラスタ内の 1 台以上のホストの GI SVM で発生する場合があります。

回避策 :

- 1.vCenter Server から GI SVM を削除します。
- 2.GI SVM サービスのデプロイ ペインで[解決] をクリックします。GI SVM で再度デプロイが実行されず。

- **問題 1848058**: ESXi ホストの VIB を NSX 6.3.2 にアップグレードすると失敗する
ESXi ホストの VIB を NSX 6.3.2 にアップグレードするときに、古い VIB ディレクトリが NSX Manager から削除され、アップグレードに失敗する場合があります。[解決] ボタンをクリックしても、この問題は解決しません。

回避策 : この問題を解決するには、アップグレード API を使用します。

PUT <https://<nsx-mgr-ip>/api/2.0/nwfabric/configure>

```
<nwFabricFeatureConfig>
  <featureId>com.vmware.vshield.vsm.vxlan</featureId>
  <resourceConfig>
    <resourceId>domain-cXX</resourceId>
  </resourceConfig>
</nwFabricFeatureConfig>
```

<nsx-mgr-ip> は NSX Manager の IP アドレスで、domain-cXX はクラスタのドメイン ID です。

- **問題 1747217**: ESXi ホストの準備で **muxconfig.xml.bad** ファイルが生成されると、ゲスト イントロスペクションが正しく機能しない
muxconfig.xml 内で仮想マシンのいずれかに「vmx path」がない場合、MUX が構成ファイルを解析する際に、「xml path」プロパティが見つからないと、MUX は構成ファイルの名前を「muxconfig.xml.bad」に変更し、エラー「Error - MUX Parsing config」を USVM に送信して構成チャネルを閉じます。
回避策 : 実体のない仮想マシンを vCenter Server インベントリから削除します。

- **問題 1859572**: vCenter Server バージョン 6.0.0 で管理されている ESXi ホストから NSX バージョン 6.3.x の NSX VIB をアンインストールすると、ホストがメンテナンス モードのままになる
クラスタで NSX 6.3.x の NSX VIB をアンインストールする場合、vSphere ESX Agent Manager (EAM) サービスがホストをメンテナンス モードに切り替え、VIB をアンインストールし、ホストのメンテナンス モードを解除します。ただし、ホストを vCenter Server 6.0.0 で管理している場合、VIB のアンインストール後にホストがメンテナンス モードのままになります。VIB をアンインストールする EAM サービスは、ホス

トをメンテナンス モードに切り替えることはできますが、メンテナンス モードの解除に失敗します。

回避策：ホストのメンテナンス モードを手動で解除します。vCenter Server バージョン 6.5a 以降でホストを管理している場合、この問題は発生しません。

- **問題 1435504:** NSX 6.0.x または 6.1.x から 6.3.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 6.3.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 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。
- **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>
```

- **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。

- **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。

- **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 チャンネルが停止する
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>
```

- **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り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 のバックング 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 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 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 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せん。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 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 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-vdpi` 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 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：

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

- 問題 1892999：ユニバーサル セキュリティ タグに関連する仮想マシンがない場合でも、独自の選択基準を変更できない
ユニバーサル セキュリティ タグが設定されている仮想マシンを削除しても、仮想マシンを表す内部オブジェクトにはユニバーサル セキュリティ タグが残ります。このため、ユニバーサル選択基準の変更に失敗し、ユニバーサル セキュリティ エラーが仮想マシンに関連付けられていることを通知するエラーが返されます。

回避策：すべてのユニバーサル セキュリティ タグを削除して、ユニバーサル選択基準を変更します。

- 問題 1926309：NSX Manager プラグインが読み込みに失敗し、「認証例外」が表示される
NSX Manager プラグインがページの読み込みに失敗し、タイムアウト エラーが表示される場合があります。

回避策：NSX 管理サービスを再起動するか、NSX Manager アプライアンスを再起動してください。

- 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。

回避策：NSX 管理サービスを再起動するか、NSX Manager アプライアンスを再起動してください。

- 問題 1801325: NSX Manager で CPU またはディスクの使用率が高くなると、「重大」レベルのシステム イベントとログが生成される
NSX Manager で、ディスクの使用率が高い、ジョブ データのチャーン率が高い、またはジョブ キュー サイズが大きいと、次の問題が 1 つ以上発生することがあります。
 - vSphere Web Client で「重大」レベルのシステム イベントが発生する
 - /common パーティションで NSX Manager のディスク使用率が高くなる
 - CPU の使用率が長期間または定期的に高くなる
 - NSX Manager のパフォーマンスが低下する

回避策：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 KB2147907](#) を参照してください。

- 問題 1781080: 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
ドメイン検索のサフィックスを 2 個以上 NSX Manager に追加すると、完全修飾名を使用しないすべての DNS ルックアップに失敗します。これは、/etc/resolv.conf 内のフォーマットの問題です。

回避策：DNS の検索サフィックスは 1 つのみ使用してください。

- 問題 1806368: 障害が発生し、フェールオーバー後に再びプライマリに昇格した NSX Manager から

コントローラを再利用すると、分散論理ルーターの設定が一部のホストにプッシュされない
Cross-vCenter NSX 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 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 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 でユニバーサル同期サービス (レプリケーター) 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 でレプリケーター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。

- **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を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。

- **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。

- **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、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：

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。

- 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 1783528：毎週金曜日の夜と土曜日の朝に NSX Manager の CPU の使用率が急増する
NSX は、完全同期を行うために、毎週金曜日の夜に LDAP をポーリングします。NSX では、特定の Active Directory 組織単位またはコンテナを設定するオプションがないため、指定されたドメインに関連するすべてのオブジェクトを取得します。

回避策：NSX Manager の vCPU を 4 個から 6 個に増やします。

- 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せん。

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：

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 1477138: 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 1437664: 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 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：

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 1843197：** NSX Manager ネットワーク アダプタが「This type of network adapter is not supported by {0}Other Linux (64-bit)」という警告を表示する

NSX Manager を正常にインストールして構成した後、vCenter Server で、展開した NSX Manager の [設定の編集] 画面にアクセスします。[ネットワーク アダプタ] に、「This type of network adapter is not supported by {0}Other Linux (64-bit)」という警告が表示されます。

NSX Controller に関する既知の問題

- **問題 1856465：** NSX Cross-vCenter Server 環境のサイトの 1 つで ESXi ホストが停止すると、そのサイトで CDO モードが有効にならない

サイトで ESXi ホストが停止しているときに、CDO モードを有効または無効にしても、そのサイトでは変更されません。

セカンダリ サイトのホストが停止した場合、プライマリ サイトでは CDO モードの変更に成功します。ただし、セカンダリ サイトでは CDO モードの変更に失敗します。これにより、動作が不安定になる場合があります。

回避策： この問題は、NSX 6.3.0 以降に影響します。

- CDO 操作を実行する前に、すべての ESXi ホストが稼動していることを確認してください。
- 整合性のない状態からリカバリするには、vCenter Server のインベントリからホストを削除し、再度追加してください。

- **問題 1965859：ハードウェア VTEP 構成で NSX Controller の使用するメモリが増加すると、CPU の使用率が高くなる**

ハードウェア VTEP 構成で数日間経過後、NSX Controller のプロセス メモリが増加することがあります。このメモリが増加したことにより、NSX Controller がメモリをリカバリする間は、CPU 使用率が数分間上昇します。この間、データ パスは影響を受けます。

回避策： VMware サポートにお問い合わせください。

論理ネットワークと NSX Edge に関する既知の問題

- **問題 1904612：レイヤー 2 VPN トンネルで、クライアントがパワーオフの状態でも、L2VPN サーバが「up」と表示される**

2 つの NSX Edge 間で L2 VPN を作成する場合、クライアントの NSX Edge をパワーオフしますが、サーバ側の NSX Edge では、VPN トンネルが稼動中と表示されます。

回避策：なし。

- **問題 1242207：実行時にルーター ID を変更しても OSPF トポロジに反映されない**

OSPF を無効にせずにルーター ID を変更すると、新しい外部 LSA (Link-State Advertisements) が新しいルーター ID で再生成されないため、OSPF 外部ルートが消失します。

OSPF を無効にしてからルーター ID を変更し、OSPF を再度有効にしてください。

- **問題 1894277：ローカルまたはピア サブネットが変更されると、IPSec サイト設定の PSK が維持されない**

マスクされた PSK がデータベースに保存されるため、パスワードが一致せず、ピア間のトンネルが有効になりません。

回避策：有効なパスワードを使用して IPSec を再設定します。

- **問題 1492497：NSX Edge DHCP トラフィックをフィルタリングできない**

NSX Edge の DHCP サーバが TCP/IP スタックをバイパスする Raw ソケットを使用するため、NSX Edge で DHCP トラフィックにファイアウォール フィルタを適用できません。

回避策：なし。

- **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 を複数回受信すると、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。

- **問題 1786515：「Security Administrator」権限を持つユーザーが、vSphere Web Client ユーザー インターフェイスでロード バランサの設定を編集することができない**

特定の NSX Edge の「Security Administrator」権限を持つユーザーが、vSphere Web Client のユーザー イン

ターフェイスを使用して、この Edge のロード バランサのグローバル構成を編集することができません。次のようなエラー メッセージが表示されます。「ユーザーはオブジェクト Global および機能 si.service 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 スコープおよび機能の権限を確認してください。」

回避策：なし。

- **問題 1849042/1849043**：NSX Edge アプライアンスでパスワードの有効期限が設定されている場合、管理者アカウントがロックされる
NSX Edge アプライアンスで管理者ユーザーのパスワードに有効期間が設定されている場合、パスワードが期限切れになってから 7 日間は、ユーザーがアプライアンスにログインするときにパスワードの変更が要求されます。パスワードを変更しないと、アカウントがロックされます。また、CLI のプロンプトを使用してログイン時にパスワードを変更する場合、作成したパスワードの強度は、ユーザー インターフェイスや REST に適用されているパスワードの強度ポリシーを満たさない場合があります。

回避策：この問題を回避するには、パスワードが期限切れになる前に、ユーザー インターフェイスまたは REST API を使用して管理者パスワードを変更します。アカウントがロックされた場合は、ユーザー インターフェイスまたは REST API で新しいパスワードを設定してアカウントのロックを解除します。

- **問題 1711013**：スタンバイ仮想マシンの再起動後、アクティブ/スタンバイ NSX Edge 間の FIB の同期に約 15 分かかる
スタンバイ NSX Edge がパワーオフになっている場合、アクティブ モードとスタンバイ モード間の TCP セッションが閉じられません。アクティブ Edge は、キープアライブ (KA) 障害 (15 分) 後に、スタンバイ Edge がダウンしていると判断します。15 分後に、スタンバイ Edge との新しいソケット接続が確立されると、FIB がアクティブ/スタンバイ Edge の間で同期されます。

回避策：なし。

- **問題 1733282**：NSX Edge がデバイスのスタティック ルートをサポートしない
NSX Edge は、ネクスト ホップのアドレスが NULL に設定されたスタティック ルートをサポートしていません。

回避策：なし。

- **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 sysloger を設定すると問題が発生する
NSX Edge でリモートの sysloger 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。

- **問題 1850773**：ロード バランサの設定で複数のポートが使用されていると、NSX Edge の NAT の設定が無効であるとレポートされる
この問題は、ロード バランサ仮想サーバに 2 つ以上のポートを設定するたびに発生します。この設定を修正しない限り、影響を受ける NSX Edge では NAT を管理できなくなります。

回避策：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 KB2149942](#) を参照してください。

- **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。

- **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。

- **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せん。show network interface

回避策：VMware サポートにお問い合わせください。

- **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。

- **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。

- **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。

- **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。

- **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 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 : 次の API を使用して、NSX Edge の詳細なステータス情報を取得します。

GET <https://NSX-Manager-IP-Address/api/4.0/edges/edgeId/status?detailedStatus=true>

- **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 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 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 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</p  
roperty> </systemControl>
```

● **問題 1089238: 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 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. [DVSTManager] > [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 DVPD where trunk vnic got c
onected-->
</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

- 問題 1918023：ゲスト イントロスペクション ユニバーサル サービス仮想マシン (USVM) がメモリを 100% 使用する
ゲスト イントロスペクション USVM がメモリを 100% 使用します。このため、ゲスト仮想マシンとゲスト イントロスペクション USVM との接続が失われる可能性があります。

回避策：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 KB2151235](#) を参照してください。

- 問題 1897878：ESXi のタスクとイベントに「ESX モジュールとの通信が失われました」エラーが表示される
ESXi ホストのゲスト イントロスペクション モジュール (EPsec Mux) が ESX モジュールから切断されると、ESXi ホストに「ESX モジュールとの通信が失われました」というメッセージが表示されます。

回避策：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 KB2151235](#) を参照してください。

- 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。

回避策：

- 1.新しい仮想マシンをデプロイした、この問題の影響を受けるクラスターで、分散ファイアウォール ルールを強制的に同期します。「ファイアウォール ルールの強制同期」を参照してください。
- 2.仮想マシンの IP アドレスがないセキュリティ グループで [編集] をクリックし、変更を行わずに送信します。

- 問題 1854661：Cross-vCenter Server 環境で NSX Manager の切り替えを行うと、フィルタリングされたファイアウォール ルールにインデックス値が表示されない
ルールのフィルタ条件を NSX Manager に適用し、別の NSX Manager に切り替えると、フィルタリングされたルールのルール インデックスが「0」になり、ルールの実際の位置が表示されません。

回避策：フィルタをクリアして、ルールの位置を表示します。

- 問題 1846402：1 つの vNIC に複数の IP アドレスがあるとファイアウォールの発行操作に時間がかかる
この問題は、vNIC に複数の IP アドレスが設定され、ARP スヌーピングが有効である場合に発生します。vNIC から送信される各パケットは、新しく検出された IP アドレスを含む、ホストから NSX Manager への ARP メッセージになります。これは、ARP でスヌーピングされた IP アドレスの場合、ホストから NSX Manager に送信できるのは 1 つのみであるためです。vNIC の IP アドレスが切り替わると、ホストは IP アドレスを新しいものとして認識し、NSX Manager に ARP でスヌーピングされたメッセージを送信します。通常、NSX Manager でコンテナ メッセージが何度も処理されることになり、ホストでのファイアウォール構成の遅れにつながります。

回避策：vNIC に複数の IP アドレスが設定されている場合、ARP スヌーピングを無効にします。代わりに、DHCP スヌーピングまたは VMware Tools を使用してください。

- 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

- 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。

- 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 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 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 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、クラスター/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うまくいきません。

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。

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。