



VMware NSX for vSphere 6.3.7 リリース ノート

VMware NSX for vSphere 6.3.7 | 2018 年 11 月 15 日リリース | ビルド 10667122

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 6.3.7 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 6.3.7 の新機能

NSX for vSphere 6.3.7 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 6.3.6](#)
- [NSX 6.3.5](#)
- [NSX 6.3.4](#)
- [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

新たに導入する場合には、最新の NSX 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。

ゲスト イントロスペクション (Linux)

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。

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

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 for vSphere 6.2.x のジェネラル サポートの終了日 (EOGS) は 2018 年 8 月 20 日です。
- 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。

全般的な動作変更

vSphere Distributed Switch が複数ある環境で、その 1 つに VXLAN が設定されている場合、vSphere Distributed Switch のポート グループにすべての分散論理ルーター インターフェイスを接続する必要があります。NSX 6.3.6 以降、ユーザー インターフェイスと API でこの構成が強制されます。以前のリリースでは、正しくない設定が可能となっていました。

API の削除と動作の変更

API エラー処理の変更

NSX 6.3.5 では、エラー処理が次のように変更されています。

- API 要求により NSX Manager でデータベース例外が発生した場合、「500 Internal server error」が返されます。以前のリリースでは、NSX Manager で要求の処理に失敗しても「200 OK」と返していました。
- 要求の本文が空の API 要求を送信すると、「400 Bad request」が返されます。以前のリリースでは、NSX Manager が「500 Internal server error」と返していました。
- API の GET /api/2.0/services/policy/securitygroup/{ID}/securitypolicies で間違ったセキュリティ グループを指定すると、「404 Not found」が返されます。以前のリリースでは、NSX Manager が「200 OK」と返していました。

バックアップとリストアの API のデフォルトの変更

NSX 6.3.3 以降では、ユーザー インターフェイスのデフォルトと一致するように、バックアップとリストアの 2 つのパラメータのデフォルトが変更されました。以前は、`passiveMode` と `useEPSV` のデフォルトは `false` でしたが、現在は `true` になっています。この変更は次の API に影響します。

- PUT /api/1.0/appliance-management/backuprestore/backupsettings
- PUT /api/1.0/appliance-management/backuprestore/backupsettings/ftpsettings

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

- NSX 6.3.0 以降では、デフォルト セクションが指定されていると、次のリクエストは拒否されます。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}

defaultOriginate パラメータ：

NSX 6.3.0 以降では、分散論理ルーター NSX Edge アプライアンスの場合のみ、次のメソッドから defaultOriginate パラメータが削除されました。

- 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 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 との互換性がありません。
 - 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 で利用できません。正しい VIB を見つけるには、以下の手順を実行する必要があります。

 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

- **重要**：NSX 6.2.0、6.2.1 または 6.2.2 から NSX 6.3.5 以降にアップデートする場合は、アップデートを開始する前に、既知の問題への回避策を実行しておく必要があります。詳細については、[VMware のナレッジベースの記事 KB000051624](#) を参照してください。
- 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 へのアップデート後に 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 以降にアップデートする場合は、[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デートしてください。
- NSX Manager を NSX 6.3.6 以降にアップグレードすると、アップグレード中にバックアップが自動的に作成され、ローカルに保存されます。詳細については、[NSX Manager のアップグレード](#)を参照してください。

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 以降にアップデートする場合、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。

コントローラを削除すると、関連する DRS の非アフィニティ ルールも削除されます。vCenter Server で新しい非アフィニティ ルールを作成して、新しいコントローラ仮想マシンが同じホストに配置されないようにする必要があります。

コントローラのアップグレードの詳細については、[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。
- **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"  
}
```

ゲスト イントロスペクションのアップグレード

- ゲスト イントロスペクション仮想マシンで、マシンの XML ファイルに追加ホストの識別情報が含まれるようになりました。ゲスト イントロスペクション仮想マシンにログインするときに、`/opt/vmware/etc/vami/ovfEnv.xml` ファイルにホスト識別情報が含まれている必要があります。

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

2018 年 11 月 15 日：初版。

2019 年 3 月 3 日：第 2 版。解決した問題 2249307 について記載しました。

2019 年 5 月 13 日。第 3 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。

- [論理ネットワークと NSX Edge に関する解決した問題](#)
- [解決した一般的な問題](#)
- [NSX Controller に関する解決した問題](#)
- [NSX Manager に関する解決した問題](#)
- [インストールとアップグレードに関する解決した問題](#)
- [セキュリティ サービスに関する解決した問題](#)

論理ネットワークと NSX Edge に関する解決した問題

- **解決した問題 2207483：East-West と North-South の両方のルーティング トラフィックのネットワーク遅延が大きい**
ルーティング トラフィックを生成する仮想マシンの TxWorld の CPU 使用率が 100% になり、ネットワーク遅延が大きくなります。
- **解決した問題 2188666：SSL VPN Linux クライアント CLI を使用して、5 桁のポート番号のゲートウェイに接続できない**
SSL VPN Linux CLI は 4 桁までのポート番号にしか対応していないため、5 桁のポート番号のゲートウェイに接続するには、Linux で SSL VPN クライアント GUI を使用する必要があります。
- **解決した問題 2185457：ブリッジされたワークロードでネットワーク遅延が大きくなる**
ブリッジされたネットワークのワークロードでトラフィック (pps) が増加すると、VLAN と VXLAN 間で遅延が発生することがあります。
- **解決した問題 2182874：サイト間で分散論理ルーター ID が重複していると、分散論理ルーター ID が機能しない**
サイトをマルチ vCenter Server に切り換えるときに、複数のサイトでセグメント範囲が重複していると、サイトのセグメント範囲の変更が必要になります。
- **解決した問題 2181650：ARP 要求を送信して ARP エントリを更新するときに、GARP を有効な応答として受け入れない**
一部の古いデバイスは、ARP 要求の応答として GARP を送信します。
- **解決した問題 2181435：ESX 5.5 で、統計情報のポーリング中に hostd がクラッシュする**
ESX 5.5 で、統計情報のポーリング中に hostd がクラッシュします。hostd の再起動が必要です。
- **解決した問題 2179054：NSX のインストールまたはアップグレードで IXGBE ドライバの再起動を回避する必要がある**
ホストのサービスで 5 ～ 10 秒のネットワーク障害が発生します。
- **解決した問題 2178950：高可用性 (HA) を有効にすると、トラフィックが中断するか、同じ Edge の vCenter Server に 3 台以上の仮想マシンが表示される**
高可用性 (HA) を有効にすると、トラフィックが中断するか、同じ Edge の vCenter Server に 3 台以上の仮想マシンが表示されます。アプライアンスの編集またはアプライアンス配置変更でリストアを行うと、仮想マシンが正常に動作しないことが原因でネットワークが中断します。
- **解決した問題 2177514：DaD ping が戻され、DaD プロセスが重複する IP アドレスを検出することがある**
システム イベントで、IP アドレスの重複が誤ってレポートされます。
- **解決した問題 2176316：ファイアウォール ルールの Edge 名が更新されない**
Edge UI (ユーザー インターフェイス) で Edge 名を変更すると、ファイアウォールの UI に古い Edge 名が表示されます。
- **解決した問題 2172005："show ip bgp" CLI コマンドを実行すると、BGP ネイバーがフラップする**

BGP が 126 文字より長い AS_PATH でルートを学習しているときに "show ip bgp" コマンドを実行すると、ルーティング スタックが再起動します。BGP が再収束するまで、ルーティングで遅延が発生し、トラフィック障害が発生する可能性があります。

- **解決した問題 2171616** : ESG ホスト名が解決できないと、SSL VPN Windows クライアント プロセスがクラッシュする
HTTP プロキシが設定されているときに、ESG ホスト名が解決できないと、クライアント プロセスがクラッシュします。
- **解決した問題 2167176** : 分散論理ルーターの Edge で高可用性 (HA) を有効にすると、tmpfs パーティションがいっぱいになる
高可用性 (HA) を有効にすると、/var/run ディレクトリ (tmpfs) がいっぱいになります。いっぱいになると、構成が機能しなくなります。
- **解決した問題 2164068** : 高可用性 (HA) を有効にしてしばらくすると、Edge tmpfs パーティションがいっぱいになる
高可用性 (HA) ペアの Edge 仮想マシン間のファイルの同期に rsync が使用されます。rsync のコンパイル方法が原因で、rsync が定期的に呼び出され、そのたびにエラー ログ メッセージが生成されます。このメッセージが tmpfs パーティションのログ ファイルに保存されます。しばらくするとパーティションがいっぱいになり、Edge の通常動作に重大な影響を及ぼす可能性があります。
- **解決した問題 2156094** : SSL VPN Linux クライアント CLI を使用して、5 桁のポート番号のゲートウェイに接続できない
SSL VPN Linux CLI は 4 桁までのポート番号にしか対応していないため、5 桁のポート番号のゲートウェイに接続するには、Linux で SSL VPN クライアント GUI を使用する必要があります。
- **解決した問題 2152060** : Edge の monitor サービス エンジン (Nagios) でメモリ リークが発生する
ロード バランサの構成で使用されている monitor サービスのメモリが不足すると、ロード バランサが正常に動作しなくなります。
- **解決した問題 2140512** : NSX 6.3.x 以降にアップグレードした後で、MP データベースに TransportZone (vdscope) のエントリがなくなり、VXLAN と論理ネットワークでエラーが発生する
NSX 用に準備されたクラスタの VXLAN と論理ネットワークでエラーが発生します。
- **解決した問題 2134760** : SSL VPN Mac クライアントのインストールに成功しても、アプリケーションを実行できない
インストールに成功してもクライアントが開きません。
- **解決した問題 2100704** : NSX Edge で NSX Manager との VMCI 接続が失われることがある
Edge が管理不能になり、Edge に構成情報をプッシュできなくなります。
- **解決した問題 2092516** : 複数のモニター ワーカーがプール メンバーのステータスを同時に更新する
ロード バランシングが正常に機能しません。不良なサーバへのトラフィックの送信が遅くなったり、良好なサーバにトラフィックが送信されなくなります。
- **解決した問題 2078866** : ホストの再起動で nsxv-vib が refreshHostdNetstackCache() で失敗する
VXLAN Rx スループットのパフォーマンスが低下する可能性があります。
- **解決した問題 2028337** : Edge の CPU 使用率が 90% を超えても、CPU 使用率の高い上位 5 つのプロセスが表示されない
Edge の CPU 使用率が 90% を超えると、Manager に通知が送信され、Edge を開始して以降の CPU 使用率が高い上位 5 つのプロセスが表示されます。このリストに CPU 使用率の高い上位 5 つのプロセスがすぐに表示されないことが多く、CPU 使用率の問題を簡単に診断できない場合があります。
- **解決した問題 1983497** : ブリッジ フェイルオーバーとブリッジの設定変更が同時に発生すると、パープル スクリーンが表示される

ブリッジ フェイルオーバーとブリッジの設定変更が同時に実行されると、デッドロックが発生し、パープル スクリーンが表示される場合があります。デッドロックは頻繁に発生するわけではありません。

- 解決した問題 2181633：ゲスト仮想マシンで、サブ インターフェイスの IP アドレスの ARP 抑制に失敗する
ゲスト仮想マシンで、サブ インターフェイスの ARP 抑制を初めて行う場合、通常（1 秒）よりも若干時間がかかります。
- 解決した問題 2170329：SSL VPN Windows クライアント インターフェイスに DNS 構成を適用できない
DNS クエリに失敗するため、アクセスに問題が発生する場合があります。

解決した一般的な問題

- 解決した問題 2183198：ポートのない ToR（トップ オブ ラック）スイッチからポートを取得すると、ユーザー インターフェイス (UI) にエラーが表示される
ハードウェア ゲートウェイの物理スイッチにポートを設定していない場合、スイッチのポートを取得しようとする、NSX UI がエラーを返します。ポート情報を取得しようとする、「インベントリ情報を取得できません」というエラーが UI に表示されます。
- 解決した問題 2176000：管理プレーンが送信したメッセージのエンコーディングが、ホストが予期したものが異なると、分散仮想スイッチのアップリンク ポート名が無効になり、MAC アドレスの解決に失敗する
分散論理ルーターが、異なる ESXi ホストに存在する仮想マシンの MAC アドレスを解決できません。
- 解決した問題 2170413：API /api/3.0/ai/directorygroup が機能しない
バックエンドで NullPointerException が発生し、API がエラーを返します。ワークフローを自動化できません。
- 解決した問題 2170395: domain_object が ai_group テーブルと同期しない
Service Composer のページが読み込まれるときに、SQL にグループ ID が空白のリストが含まれていると、SQLGrammarException が返されます。
- 解決した問題 2131680：マルチキャスト パケットが拒否ファイアウォール ルールに一致すると、VMkernel ログに過剰なログが記録される
VMkernel ログに過剰なログが記録され、ホストのログ記録が停止します。
- 解決した問題 2129177：アップグレードまたは後方互換性モードで、ゲスト イントロスペクション サービス仮想マシンを削除すると、ゲスト イントロスペクション クラスタがアップグレードされるまで、ゲスト イントロスペクションを使用した Identity Firewall が機能しない
Identity Firewall が機能せず、Identity Firewall に関連するログが表示されません。クラスタがアップグレードされない限り、Identity Firewall による保護が中断したままになります。
- 解決した問題 2105632：USVM が Google（外部）NTP サーバと時間の同期を試みる
timesync サービスが変更され、この動作は実行されません。
- 解決した問題 2003396：大量のルートが設定されていると、再起動後または新しいホストの参加後に分散論理ルーターの論理インターフェイス/ルートが表示されなくなる
ルートが設定どおり表示されません。
- 問題 1960383: 短時間に大量のインベントリ オブジェクトが削除されると、タイムアウトが発生し、ネットワークの作成に失敗する
NSX で分散仮想ポート グループの作成が遅延することで、ネットワーク作成タイムアウトが発生します。
- 解決した問題 2058770：vCenter Server でログイン イベントが過剰に発生し、vCenter Single Sign-On サーバの負荷が高くなる

vCenter Single Sign-On ユーザーが短期間で大量の NSX API 要求を送信すると、vCenter Single Sign-On サーバでログイン イベントが過剰に発生し、負荷が高くなります。これにより、動作が遅くなる可能性があります。

- **解決した問題 2046427**：vmknic または LS dvs ポートグループのチーミング ポリシーを変更すると、データ パスが停止することがある
ホストの準備 (VXLAN) で、vmknic チーミング ポリシーを設定すると、これに従って分散仮想スイッチのアップリンク チーミング ポリシーが設定されます。新しい論理スイッチで作成される分散仮想スイッチのポート グループもこのチーミング ポリシーを取得します。
- **解決した問題 2178339**：systemd サービス ファイルの ExecReload 行から rsyslog 8.15.0-7.ph1 が削除され、/var/log/syslog と /var/log/messages でログが正しくローテーションされない
この問題により、/var/log パーティションのディスク容量がすべて使用され、新しいログの書き込みができなくなります。
- **解決した問題 2146879**：スタンドアローン設定で、強制同期で ToR （トップ オブ ラック） の割り当てが同期されない
スタンドアローン設定で、ハードウェアの割り当てまたはハードウェアのトランスポート ノードの設定が管理プレーンとコントローラ間で同期されていないと、強制同期で設定が同期されません。ToR の割り当てが同期されていない場合、ToR の設定がコントローラと同期されません。
- **解決した問題 2146749**：再起動後に ESXi ホストからロケール ID の設定が削除される
ホストが間違ったロケール ID を受信し、対応するルートが消去されます。
- **解決した問題 2200396**：フェイルオーバー後にセカンダリ サイトの ESXi ホストで分散論理ルーター インスタンスが再作成される
フェイルオーバー後、約 40 秒間トラフィックが中断し、ネットワーク障害が発生します。
- **解決した問題 2100296**：vCenter Server/PSC で SSL/TLS1.0 を無効にすると、NSX 6.3.5 Web Client プラグインに NSX Manager が表示されない
vCenter Server で SSL/TLS1.0 を無効にすると、NSX は vCenter Server、NSX、または ESX との通信を中断します。vCenter Server のアプリケーションは NSX Manager と通信しません。
- **解決した問題 2077492**：NSX Manager が、既存の IPsec サイトに ipsecsite ID を自動的に作成する
 - NSX Manager が、既存の IPsec サイトに ipsecsite ID を自動的に作成します。
 - NSX for vSphere を 6.2.x から 6.3.5 または 6.4.0a にアップグレードすると、IPsec サイトのサイト ID が重複する場合があります。
 - サイト ID が重複すると、次の IPsec の設定に失敗します。
 - 次のようなエラーが表示されます。[13646] [IPsec] IPsec サイト ID ipsecsite-id が重複しています。
- **解決した問題 2177097**：API 呼び出し /api/2.0/vdn/config/segments を使用して、セグメント ID が 1 のプールを作成すると、エラーが発生し、「セグメント ID が範囲外になっています。有効な範囲は 5000-16777215 です」とメッセージが返されます。
API /api/2.0/vdn/config/segments を使用して単一値のセグメントを作成するときに、開始値と終了値に同じ値を指定すると、エラーが発生します。
- **解決した問題 2172267**：ホストが応答していないときに NSX Edge を削除すると、vCenter Server に実体のないオブジェクトが生成される
NSX Manager の Edge インスタンスが削除されても、NSX Manager がこの Edge を実態なしとマークし、クリーンアップ プロセスで Edge を削除するまで、Edge アプライアンスが vCenter Server に残り、データパスを提供します。NSX Manager から Edge アプライアンスを削除する方法はありません。
- **解決した問題 2097255**：NSX Manager アプライアンスで FIPS が有効になっていると、SNMP トラップが送信されない
SNMP トラップが受信されません。

NSX Controller に関する解決した問題

- 解決した問題 2181306：コントローラのメモリが不足し、通常のサービスを提供できない
コントローラでは、SSH インターフェイスを使用してクラスタ メンバーシップとステータスを問い合わせることができます。クライアントがインターフェイスにアクセスし、セッションを閉じないと、コントローラはセッションを無期限に維持します。多くのセッションが開いた状態になっていると、コントローラのメモリが不足します。

NSX Manager に関する解決した問題

- 解決した問題 2171653：NSX Manager のセキュリティ スキャンで「HTTP Security Header Not Detected」が報告される
セキュリティ スキャンでこの問題が報告されます。クリックジャック攻撃が発生している可能性があります。
- 解決した問題 2161066：使用量メーターと NSX Manager の接続に失敗するか、API 応答の処理で無効な XML 文字エラーが発生する
使用量メーターと NSX Manager の接続でエラーが発生します。
- 解決した問題 2145195：すべてのユニバーサル サービス仮想マシン (USVM) でハートビートアラートが発生し、NSX Manager の CPU 使用率が高くなる
NSX Manager によって、すべての USVM がハートビートに回答していないことを通知します。postgres セッションが原因で CPU 使用率が高くなります。
- 解決した問題 2144825：nsx-tcserver-wrapper.log ファイルが多すぎるため、NSX Manager のルートパーティションがいっぱいになる
容量不足のため、NSX UI にアクセスできず、ほとんどのサービスも機能しません。
- 解決した問題 2141490：NSX Manager とコントローラにバインドされたトップ オブ ラック (ToR) が同期されない
論理スイッチにバインドされたハードウェアを変更したり、設定を削除できません。ユーザー インターフェイスに次のエラーが表示されます。「Failed to do operation on the Controller.{0}」
- 解決した問題 2066631：セキュリティ管理者のユーザー ロールでログインして仮想マシンを選択すると、ポップアップでエラー メッセージが表示される
「There is no authority to access object global and function library.tagging.Confirm the authority of the function and object access scope」というエラー メッセージがポップアップで表示されます。
- 解決した問題 2189810：サードパーティのサービス挿入ソリューションで NSX Manager に API 呼び出しを行い、サービス挿入で設定されたすべてのセキュリティ グループ/IP セットを取得すると、PAN で保護されたゲスト仮想マシンがトラフィックをドロップする
NSX Manager が、IP セットまたは IP セットを含むセキュリティ グループの空の設定を返します。結果として、IP セットまたは IP セットを含むセキュリティ グループが空白としてサードパーティの Manager に報告されます。一致するルールがなく、デフォルトの拒否ルールが適用されるため、PAN または他のサードパーティ ファイアウォール デバイスで保護されたゲスト仮想マシンがトラフィックをドロップします。API 呼び出し https://NSXMGR_IP/api/2.0/si/serviceprofile/serviceprofile-10/containerset を実行しても、IP セットの IP アドレスまたは IP セットを含むセキュリティ グループは返されません。

一致するルールがなく、デフォルトの拒否ルールが適用されるため、PAN または他のサードパーティ ファイアウォール デバイスで保護されたすべてのゲスト仮想マシンがトラフィックをドロップします。

- 解決した問題 2178700：分散論理ルーターの論理インターフェイスの 1 つが削除された virtualwire を使用していると、NSX Manager が分散論理ルーターの論理インターフェイス情報とコントローラの同期に失敗する
分散論理ルーターの論理インターフェイスの処理に失敗し、ユーザーは論理インターフェイスの設定を変更できなくなります。

- 解決した問題 2249307 : ESXi ホストが NSX Manager に再接続したときに、ESXi ホストのロケール ID がデフォルトにリセットされる
分散論理ルーターのルートがありません。分散論理ルーターがトラフィックをルーティングできなくなります。ホストは誤ったロケール ID を受信し、目的の分散論理ルーターのルートが維持されません。

インストールとアップグレードに関する解決した問題

- 解決した問題 2133143 : NSX データベース内に古いクラスタ エントリがある
NSX 6.2.2 から 6.2.9 にアップデート後、NSX データベースに古いクラスタ エントリが残ります。
- 解決した問題 2112773 : コントローラのアップグレードに失敗する
コントローラを 6.2.4 から 6.3.6 にアップグレードできません。

セキュリティ サービスに関する解決した問題

- 解決した問題 2098645 : セキュリティ グループが削除された Active Directory グループを参照していると、null ポインタ例外が発生する
Active Directory グループ (ai_group) が削除され、そのグループをセキュリティ グループが参照している場合、セキュリティ グループから仮想マシンへの解釈によって null ポインタ例外が発生します。Service Composer ページが正しく読み込まれません。
- 解決された問題 2032988、2032990、2032991 : CVE-2017-5753、CVE-2017-5715 (Specter)、CVE-2017-5754 (Meltdown) の脆弱性が存在する
CVE-2017-5753、CVE-2017-5715 (Specter)、CVE-2017-5754 (Meltdown) の脆弱性が存在するため、セキュリティの問題が発生する可能性があります。

既知の問題

既知の問題には次の項目が含まれます。

- [インストールとアップグレードに関する既知の問題](#)
- [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

- 問題 2001988 : NSX ホスト クラスタのアップグレードで各クラスタをアップグレードしているときに、[ホストの準備] タブでクラスタ全体のインストール状況を確認すると、「準備ができていません」と「インストール中」が交互に表示される
NSX のアップグレードで、NSX が準備したクラスタの「アップグレードを利用可能」をクリックすると、ホストのアップグレードを開始します。DRS FULL AUTOMATIC が設定されたクラスタの場合、ホストのアップグレードがバックグラウンドで問題なく実行されているにも関わらず、インストール状況として「インストール中」と「準備ができていません」が交互に表示されます。

回避策：これはユーザー インターフェイスの問題で、無視しても問題ありません。ホスト クラスタのアップグレードが完了するまでお待ちください。

一般的な既知の問題

- 問題 2158182 : DHCP サービスとリンクローカル IP アドレスの高可用性 (HA) が同じ vNIC を共有するため、DHCP 更新パケットがドロップされる
高可用性 (HA) アドレスがリンクローカル アドレス (169.x.x.x) の場合、DR がこのリンクローカル アドレスに対する DHCP 更新ユニキャスト パケットをドロップし、DHCP クライアントの更新に失敗する場合があります。

回避策：高可用性 (HA) インターフェイスとして DHCP サービスを使用しない vNIC を選択するか、高可用性 (HA) インターフェイスの IP アドレスとしてルーティング可能な IP アドレス（例:192.168.x.x）を使用します。

- **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. [アプライアンス管理] で、[アプライアンス設定の管理] をクリックします。
3. [設定] パネルで、[ネットワーク] をクリックします。
4. DNS サーバ の横にある [編集] 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 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 2204383：SSL VPN Linux クライアントが、sql cert9.db を使用する Linux バージョンのサーバ証明書を検証できない**

内部エラーが発生し、サーバの検証に失敗します。

回避策：なし。