

VMware NSX for vSphere 6.2.4 リリース ノート

ドキュメントの更新日：2016 年 11 月 28 日

VMware NSX for vSphere 6.2.4 | 2016 年 8 月 25 日リリース | ビルド 4292526

リリース ノートの概要

本リリース ノートには、次のトピックが含まれています。

- [新機能](#)
- [推奨されるバージョン、システム要件、およびインストール](#)
- [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 6.2.4、6.2.3、6.2.2、6.2.1 および 6.2.0 の新機能と変更点は次のとおりです。

[NSX 6.2.3 に関する重要な情報](#)をご確認ください。

6.2.4 の新機能

6.2.4 リリースには次の新機能が含まれています。また、このリリースでは多くのバグが解決され、「[解決した問題](#)」セクションに記載されています。「[NSX for vSphere 6.2.3 に関する重要な情報](#)」セクションに記載された問題も解決しています。

NSX for vSphere 6.2.4 の変更点は次のとおりです。

- ファイアウォール ステータス API (**GET /api/4.0/firewall/globalroot-0/status**) の変更
 - ファイアウォール ルールで使用するオブジェクトの更新状態を表示するように、ファイアウォール ステータス API を拡張：ファイアウォール ステータス API では、各ルールセットの生成番号 (generationNumber) が表示されます。この番号により、ルールセットの変更がホストに適用されているかを確認できます。NSX 6.2.4 では、オブジェクトの生成番号 (generationNumberObjects) がステータス API に追加されました。これにより、ファイアウォール ルールで使用するオブジェクトの変更が、ホストに適用されているか確認できるようになりました。オブジェクト生成番号は、頻繁に変更される場合があり、常にルールセットの生成番号以上の数字になることに注意してください。
 - ホストとクラスタにファイアウォールが設定されていない場合、ステータス表示に含まれなくなる：クラスタ レベルで分散ファイアウォールが無効になっているか、クラスタの準備が整っていない (NSX VIB がインストールされていない) 場合、それらのクラスタおよびクラスタ内のホストは、ステータス表示セクションに出力されなくなります。以前のバージョンの NSX では表示されていましたが、クラスタやホストにファイアウォールが設定されていないため、ファイアウォール ルールが発行されると、ステータスが *inprogress* となっていました。

NSX for vSphere 6.2.3 に関する重要な情報

VMware は、ダウンロードによる VMware NSX for vSphere 6.2.4 の提供を開始しました。VMware NSX 6.2.4 には、NSX 6.2.3 で発見された重大なバグに対する修正と、NSX SSL-VPN を使用するサイトでの入力内容検証の深刻な脆弱性 CVE-2016-2079 に対応するセキュリティ パッチが含まれます。

SSL VPN を使用するお客様には、CVE-2016-2079 をご確認のうえ、NSX 6.2.4 にアップグレードすることをお勧めします。

NSX 6.2.3 または 6.2.3a をインストールしたお客様は、重要なバグ修正に対応している NSX 6.2.4 をアップグレードしていただきますよう、お願いいたします。

6.2.3 の新機能

6.2.3 リリースでは、CVE-2016-2079 に対応するセキュリティ パッチを提供しています。CVE-2016-2079 は、NSX SSL-VPN を使用するサイトに影響する入力内容検証の深刻な脆弱性です。また、このリリースでは、「[解決した問題](#)」セクションに記載されている複数のバグ修正を提供します。

NSX for vSphere 6.2.3 の変更点は次のとおりです。

• 論理スイッチとルーティング

- NSX ハードウェア レイヤー 2 ゲートウェイの統合：サードパーティのハードウェア ゲートウェイ スイッチを NSX 論理ネットワークに統合することで、物理接続オプションを拡張します。
- NSX 6.2.3 以降で、新たに VXLAN ポート 4789 を導入：6.2.3 より前のバージョンでは、デフォルトの VXLAN UDP ポート番号は 8472 でした。詳細については、『NSX アップグレード ガイド』を参照してください。

• ネットワークと Edge サービス

- Edge の新しい DHCP オプション：DHCP オプション 121 は、DHCP サーバから DHCP クライアントへのスタティック ルートの発行に使用される、スタティック ルート オプションをサポートします。DHCP オプション 66、67、150 は、PXE ブートの DHCP オプションをサポートします。DHCP オプション 26 は、DHCP サーバによる DHCP クライアント ネットワーク インターフェイス MTU の設定をサポートします。
- DHCP プール、静的バインドの上限の引き上げ：各アプライアンスの新しい上限は次のとおりです。Compact：2048、Large：4096、Quad Large：4096、X-Large：8192。
- Edge ファイアウォールによる SYN flood 攻撃からの保護：SYN flood 攻撃からトランジットトラフィックを保護することで、サービス中断を回避できるようになりました。この機能はデフォルトでは無効になっています。有効にするには、NSX REST API を使用します。
- NSX Edge — オンデマンド フェイルオーバー：ユーザーは必要に応じてオンデマンド フェイルオーバーを開始できます。
- NSX Edge - Quad Large の NSX Edge のデフォルト メモリ：1 GB から 2 GB に増加されました。
- NSX Edge — リソースの予約：NSX Edge の作成中に CPU/メモリを予約します。予約される CPU/メモリは Edge アプライアンスのフォームファクタに応じて変わります。次の API を使用して、CPU およびメモリのリソース予約のデフォルト値 (%) を変更できます。CPU とメモリの割合をそれぞれ 0% に設定すると、リソースの予約を無効にすることができます。

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

```
<tuningConfiguration>
  <lockUpdatesOnEdge>false</lockUpdatesOnEdge>
  <aggregatePublishing>true</aggregatePublishing>
```

```

        <edgeVMHealthCheckIntervalInMin>0</edgeVMHealthCheckInterval
InMin>

        <healthCheckCommandTimeoutInMs>120000</healthCheckCommandTim
eoutInMs>

        <maxParallelVixCallsForHealthCheck>25</maxParallelVixCallsFo
rHealthCheck>

        <publishingTimeoutInMs>1200000</publishingTimeoutInMs>

        <edgeVCpuReservationPercentage>0</edgeVCpuReservationPercent
age>

        <edgeMemoryReservationPercentage>0</edgeMemoryReservationPer
centage>

        <megaHertzPerVCpu>1000</megaHertzPerVCpu>
</tuningConfiguration>

```

- **NSX Edge のアップグレード動作の変更**：置き換え用の NSX Edge 仮想マシンは、アップグレードまたは再デプロイの前にデプロイされます。高可用性構成の 2 台の Edge 仮想マシンをアップグレードまたは再デプロイする際は、4 台の NSX Edge 仮想マシンに十分なリソースがホストに必要です。TCP 接続のタイムアウトのデフォルト値は、以前の 3,600 秒から 21,600 秒に変更されました。
- **Cross-vCenter NSX — ユニバーサル分散論理ルーター (DLR) のアップグレード**：プライマリ NSX Manager でユニバーサル分散論理ルーターをアップグレードすると、セカンダリ NSX Manager でも自動的にアップグレードされます。
- **柔軟な SNAT/DNAT ルールの作成**：*vnictId* が入力パラメータとして不要になり、DNAT アドレスを NSX Edge vNIC のアドレスにするという要件が排除されました。
- **NSX Edge 仮想マシン (NSX Edge Services Gateway (ESG) と分散論理ルーター (DLR)) が、実際の配置場所と推奨される配置場所の両方を示します**。NSX Manager および GET `api/4.0/edges/appliances` を含む NSX API が、現在の位置に加えて `configuredResourcePool` と `configuredDataStore` を返すようになりました。
- **Edge ファイアウォールによる SYN flood 攻撃からの保護** SYN flood 攻撃からトランジットトラフィックを保護することで、サービス中断を回避できるようになりました。この機能はデフォルトでは無効になっています。有効にするには、NSX REST API を使用します。
- **NSX Manager による ESXi ホスト名の表示**：サードパーティの VM-Series ファイアウォールのサービス仮想マシンが実行されている ESXi ホスト名を公開することで、大規模環境運用の管理性を向上させます。
- **NAT ルールを IP アドレスだけでなく vNIC インターフェイスにも適用できるようになりました**。
- **ロード バランサのセッション エイジング タイマーを設定する新しいオプションの追加**：このリリースでは、サーバとクライアントの両方でセッションのタイムアウト値を設定するための、新しいアプリケーション ルール コマンドを追加しました。複数の仮想サーバがプールを共有している場合、プールに最大値が設定されます。
- **「Accept」ヘッダーが指定されていない場合、NSX API はデフォルトで XML 出力を返す**：NSX 6.2.3 以降、REST API 呼び出しで「Accept:」ヘッダーが指定されていない場合、NSX API の戻り値のデフォルト形式は XML になります。これより前の NSX API は、デフォルトで JSON 形式の出力を返していました。JSON 形式で出力するには、API ユーザーが関数を呼び出す際に、「Accept:」ヘッダーに「application/json」を明示的に設定する必要があります。
- **NSX 分散ファイアウォールの自動ドラフト設定を変更するための新しい NSX API の追加**：NSX 6.2.3 以降では、次の PUT API を使用して、NSX 分散ファイアウォールの自動ドラフト設定を変更できます。

- 既存のグローバル構成の取得

GET https://NSX-Manager-IP-

Address/api/4.0/firewall/config/globalconfiguration

注：GET メソッドでは、autoDraftDisabled フィールドは表示されません。

- autoDraftDisabled 構成プロパティをグローバル構成に追加して、次の PUT API を呼び出します。

PUT https://<NSX-Manager-IP-

Address>/api/4.0/firewall/config/globalconfiguration

要求本文：

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

- セキュリティ サービス

- 分散ファイアウォール — TFTP ALG：仮想マシンのネットワーク ブートなどが使用できるようになります。
- ファイアウォール：ルールの詳細なフィルタリング：ユーザー インターフェイスでルールを詳細にフィルタできるようにして、トラブルシューティングを簡素化します。送信元、宛先、アクション、有効/無効、ログ作成、名前、コメント、ルール ID、タグ、サービス、プロトコルに基づいてフィルタリングできます。
- ゲスト イントロスペクション — Windows 10 のサポート
- SSL VPN Client — Mac OS El Capitan のサポート
- Service Composer — パフォーマンスの向上：セキュリティ ポリシーとファイアウォール サービス間の同期を最適化し、ファイアウォール ドラフトの自動保存をデフォルトで無効にすることで、NSX Manager の起動/再起動が高速になります。
- Service Composer — ステータス アラーム：セキュリティ ポリシーが同期できていない場合、システム アラームを通知して、アラームのコードに基づいて特定のアクションを実行し、問題を解決します。
- ファイアウォールのヒープ メモリの使用量の削減：ファイアウォールによる IP アドレス セットの使用が最適化され、ヒープ メモリの使用量が削減されました。

- 操作とトラブルシューティング

- NSX ダッシュボード：NSX コンポーネント全体の健全性を単一の画面にまとめて表示できるため、トラブルシューティングが簡素化されます。
- トレースフローの機能強化 — ネットワーク イントロスペクション サービス：ソースからターゲットへのパケットをトレースする機能が強化され、パケットの転送先がサードパーティのネットワーク イントロスペクション サービスであるか、そしてサードパーティ サービス仮想マシンからパケットが戻されるかどうかを特定できるようになりました。
- SNMP のサポート：NSX Manager、NSX Controller、および Edge のイベント用に SNMP トラップを設定できます。

- SSL VPN および L2 VPN のログ作成がデフォルトで有効になります。ログ レベルはデフォルトで「注意」に設定されます。
- IPsec VPN のログ作成がデフォルトで有効になります。ログ レベルはデフォルトで「警告」に設定されます。ログの収集を無効にしたり、ログ レベルを変更したりする場合は、『NSX 管理ガイド』の「IPsec VPN のログの有効化」セクションを参照してください。
- ファイアウォール ルールのユーザー インターフェイスに、サービスに関連付けられている設定済み IP プロトコルと TCP/UDP ポート番号が表示されます。
- NSX Edge のテクニカル サポート ログの機能拡張により、各プロセスのメモリ使用量がレポートされるようになりました。
- 通信チャネルの健全性ステータス監視の機能強化：サーバまたはクラスタの通信チャネルの健全性ステータスが変化すると、新しいイベント ログ メッセージがレポートされます。
- セントラル CLI の機能強化
 - セントラル CLI でホストの健全性を表示：ホストの健全性ステータスを表示し、ネットワーク構成、VXLAN 設定、リソース使用率など、1 つのコマンドで 30 以上のステータスを確認できます。
 - セントラル CLI でパケットをキャプチャ：ホストでパケットをキャプチャし、キャプチャ ファイルをユーザーのリモート サーバに転送する機能を提供します。これにより、論理ネットワークの問題を解決する際、ネットワーク管理者にハイパーバイザーのアクセス権限を付与する必要がなくなります。
- ホスト単位のテクニカル サポート バンドル：各ホストのログを収集し、バンドルを作成して保存できます。これは、サポートを依頼する際に、VMware テクニカル サポートに送信することができます。

• ライセンスの機能強化

- デフォルトのライセンス キーおよび評価ライセンス キーの変更：インストール時のデフォルトのライセンスは「NSX for vShield Endpoint」です。このライセンスでは、アンチウイルスの負荷を軽減する目的にのみ、NSX を利用して vShield Endpoint をデプロイおよび管理できます。評価ライセンス キーをご希望の場合は、VMware のセールス担当者にご連絡ください。
- ライセンス使用状況のレポート機能：NSX ライセンスの使用状況は、NSX Manager ユーザー インターフェイスの [サマリ] に表示されます。また、API を使用して取得することもできます。今後 NSX ライセンスの使用状況は、vCenter Server のライセンス サービス経由ではレポートされません。

• ロード バランサの機能拡張

- 仮想 IP アドレス (VIP) のセッション タイムアウトをアクセラレーションなしで設定可能：ロード バランシング L7 エンジン（アクセラレーションなし）において、アプリケーション ルール「timeout client 3600s」を使用した仮想 IP アドレスのタイムアウトを 5 分以上に設定できます。
- CLI の統計情報の機能拡張：CLI でグローバル統計情報を取得できるようになりました特定の仮想 IP アドレスやプールの統計情報も取得できます。
- ロードバランシングのアクセラレーションの機能強化：ロード バランシング L4 エンジン（アクセラレーションあり）は、UDP と TCP の送信元 IP ハッシュの健全性チェックを常に考慮し、パシステンス エントリーを無効にします。
- ログ機能の向上：ロード バランサのログ機能が向上しています。

- 設定可能な SSL 認証：仮想 IP アドレスに End-to-End の SSL が設定されている場合、SSL サーバ認証を設定できます。
- 送信元 IP アドレスのパーシステンス テーブルの機能強化：設定を変更したあとも、送信元 IP アドレスのセッション維持テーブルを引き続き利用できます。
- NSX Manager のホワイトリストへの NSX Edge ロード バランサ システム コントロール (sysctl) sysctl.net.ipv4.vs.expire_nodest_conn パラメータの追加：
sysctl.net.ipv4.vs.expire_nodest_conn は、パーシステンス接続ステータスを変更します。

• ソリューションの相互運用性

- カスタマ エクスペリエンス改善プログラム：NSX は、システムの統計情報の収集する VMware カスタマ エクスペリエンス改善プログラム (CEIP) をサポートしています。プログラムへの参加は任意であり、vSphere Web Client で設定できます。
- VMware vRealize Log Insight 3.3.2 for NSX は、監視およびトラブルシューティング機能や、ネットワーク仮想化、フロー分析、アラート用のカスタマイズ可能なダッシュボードを備えており、NSX 向けのインテリジェントなログ分析を提供します。VMware vRealize Log Insight 3.3.2 for NSX は、NSX 6.2.2 以降のバージョンの NSX Standard/Advanced/Enterprise Edition のライセンス キーに対応しています。
- vShield Endpoint の管理のサポート：NSX は、vShield Endpoint のアンチウイルス オフロード機能の管理をサポートします。vSphere と vShield Endpoint (Essentials Plus および上位のエディション) をご購入いただいたお客様は、vSphere のダウンロード サイトから NSX をダウンロードできます。詳細については、[VMware ナレッジベースの記事 KB2110078](#) および [VMware ナレッジベースの記事 KB2105558](#) を参照してください。

6.2.2 の新機能

NSX 6.2.2 リリースでは、glibc の脆弱性に対応するセキュリティ パッチと、数多くのバグ修正を提供します。これらのバグは「[解決した問題](#)」セクションに記載されています。本リリースには、6.1.4 および 6.1.5 で提供されたパッチと同じ重要な修正がすべて含まれます。NSX 6.1.x を使用している場合は、NSX 6.1.6 リリースのパッチで同じ修正が提供されます。

本リリースの主な修正点は以下のとおりです。

- CVE-2015-7547 (glibc) のセキュリティ パッチ：このパッチは、glibc の脆弱性である [CVE-2015-7547](#) に対応します。
- 問題 1600484：DHCP ドメイン名設定の制約を削除：NSX 6.2.2 では、「.local」ドメインを使用する DHCP プールのサポートが再度可能になります。[VMware ナレッジベースの記事 KB2144097](#) を参照してください。
- 問題 1586149：ユーザーの操作性向上のための分散ファイアウォール ユーザー インターフェイスの機能拡張以前の実装では、ユーザーがテーブルに変更を加えると、グリッドがスクロールして、最初の項目に戻っていました。この問題が修正され、ルールが追加されると、グリッドは新しく追加されたルールにスクロールしたままになります。変更内容の発行または変更内容を元に戻した後など、何らかの理由でグリッドのデータを更新するとき、グリッドの縦のスクロール位置が保持されるようになりました。
- 問題 1592562：新しい Edge サービスを設定すると動作が変化するバージョン 6.2.2 より前のバージョンでは、新しい Edge サービスを設定すると、デフォルトで有効になりました。バージョン 6.2.2 では、この動作が変更されました。ご利用のライセンスが Edge サービスをサポートしている場合、機能はデフォルトで有効になりますが、そうでない場合は無効になります。

6.2.1 の新機能

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

- **6.1.5 の修正**：このリリースには、NSX for vSphere 6.1.5 と同じ重要な修正が含まれます。
- **新しい show control-cluster network ipsec status コマンド**により、IPsec (Internet Protocol Security) の状態を確認できる
- **接続ステータス**：NSX Manager ユーザー インターフェイスで NSX Controller クラスタの接続ステータスを表示可能
- **vRealize Orchestrator Plug-in for NSX 1.0.3 のサポート**：NSX 6.2.1 リリースでは、vRealize Automation 7.0.0 用に vRealize Orchestrator Plugin for NSX 1.0.3 が追加されます。このプラグインには、vRealize Automation 7.0 がネットワークとセキュリティのエンドポイントとして NSX for vSphere 6.2.1 を使用する際に、パフォーマンスが向上する修正が含まれます。
- **6.2.1 より、NSX Manager はクラスタ内の各コントローラ ノードでクエリを実行して、当該コントローラとクラスタ内の他のコントローラ間の接続情報を入手する**
これは、NSX REST API (「GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller」コマンド) の出力として提供され、コントローラ ノード間のピア接続ステータスを表示します。NSX Manager が、任意の 2 台のコントローラ ノード間の接続が切断されていることを認識すると、システム イベントが生成され、ユーザーに警告します。
- **Service Composer が公開する API により、ユーザーは Service Composer ワークフローのファイアウォール ドラフトの自動生成を設定できる**
REST API を用いて、この設定を有効/無効に切り替えることができ、再起動後もその変更が維持されます。無効にすると、ポリシー ワークフロー用のドラフトは分散ファイアウォール内に生成されません。これにより、システム内で自動生成されるドラフトの数が抑えられ、パフォーマンスが向上します。

6.2.0 の新機能

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

- **Cross-vCenter Networking and Security**
 - **NSX 6.2 と vSphere 6.0 の併用による、Cross-vCenter NSX のサポート**：これにより、論理スイッチ (LS)、分散論理ルーター (DLR)、分散ファイアウォール (DFW) を複数の vCenter Server にわたってデプロイできるようになるため、複数の vCenter Server や複数の物理的な場所にワークロード (仮想マシン) が分散しているアプリケーションに対し、論理ネットワークとセキュリティを提供できます。
 - **複数の vCenter Server 間で一貫したファイアウォール ポリシー**：NSX のファイアウォール ルールセクションを「ユニバーサル」としてマークし、このセクションで定義したルールが複数の NSX Manager に複製されるようになりました。これにより、複数の NSX 環境に一貫したファイアウォール ポリシーを定義するワークフローが簡素化されます。
 - **Cross-vCenter vMotion と分散ファイアウォール**：「ユニバーサル」セクションでポリシーが定義されている仮想マシンは、異なる vCenter Server に属するホスト間を移動しても、一貫したセキュリティ ポリシーが適用されます。
 - **ユニバーサル Security Group**：IP アドレス、IP セット、MAC アドレス、および MAC セットに基づく NSX 6.2 の Security Group をユニバーサル ルール内で使用して、グループとグループ メンバシップを複数の NSX Manager 間で同期できるようになりました。また、複数の NSX Manager にまたがるオブジェクト グループ定義の一貫性が向上し、ポリシーを一貫して適用できます。

- ユニバーサル論理スイッチ (ULS) : Cross-vCenter NSX の一部として NSX 6.2 で追加された新機能です。複数の vCenter Server にまたがる論理スイッチの作成が可能になるため、ネットワーク管理者はアプリケーションまたはテナント用に連続する L2 ドメインを作成できます。
- ユニバーサル分散論理ルーター (UDLR) : Cross-vCenter NSX の一部として NSX 6.2 で追加された新機能で、複数の vCenter Server にまたがる分散論理ルーターが作成できるようになります。ユニバーサル分散論理ルーターを使用すると、前述のユニバーサル論理スイッチ間のルーティングが可能になります。さらに、NSX UDLR ではワークロードの物理的な場所に基づいて垂直方向のルーティングを最適化することができます。

• 操作とトラブルシューティングの機能強化

- 新しいトレースフロー トラブルシューティング ツール : トレースフローは、問題が仮想ネットワークまたは物理ネットワークのどちらで発生しているかを特定するのに役立つトラブルシューティング ツールです。ソースからターゲットまでパケットをトレースして、そのパケットが仮想ネットワーク内のさまざまなネットワーク機能をどのように通過するかを確認できます。
- フロー モニタリングと IPFIX の分離 : NSX 6.1.x でも IPFIX レポートがサポートされていましたが、IPFIX レポートを有効にできるのは、NSX Manager への フロー モニタリング機能も有効にしている場合に限られていました。NSX 6.2.0 から、これらの機能が分離されます。NSX 6.2.0 以降では、NSX Manager での フロー モニタリング設定に関係なく IPFIX を有効にできます。
- 6.2 における監視およびトラブルシューティングの新しい CLI コマンド : 詳細については、[ナレッジベースの記事 KB2129062](#) を参照してください。
- セントラル CLI : セントラル CLI は、分散ネットワーク機能のトラブルシューティング時間を縮小します。NSX Manager のコマンド ラインからコマンドを実行し、コントローラ、ホスト、および NSX Manager から情報を取得します。これによって、複数のソースにすばやくアクセスし、情報を比較することができます。セントラル CLI は、論理スイッチ、分散論理ルーター、分散ファイアウォール、および Edge に関する情報を提供します。
- ping CLI コマンドに設定可能なパケット サイズと do-not-fragment フラグを追加 : NSX 6.2.0 から、NSX の「ping」CLI コマンドに、データ パケット サイズ (ICMP ヘッダを含まない) と do-not-fragment フラグを設定できるオプションが提供されます。詳細については、[NSX CLI リファレンス](#)を参照してください。
- 通信チャネルの健全性の表示 : NSX 6.2.0 では、通信チャネルの健全性を監視する機能が追加されました。NSX Manager とファイアウォール エージェント間、NSX Manager と制御プレーン エージェント間、ホストと NSX Controller 間のチャネルの健全性ステータスを NSX Manager のユーザー インターフェイスで確認できます。さらに、ホスト コマンド チャネルが、より優れたフォルト トレランスを提供します。
- スタンドアロン Edge L2 VPN クライアント CLI : NSX 6.2 以前は、スタンドアロン NSX Edge L2 VPN クライアントを構成するには、vCenter Server に提供されている OVF 設定をデプロイするしか方法はありませんでした。このたび、スタンドアロン NSX Edge 専用のコマンドが追加され、コマンド ライン インターフェイスで設定することが可能になりました。

• 論理ネットワークとルーティング

- L2 ブリッジと分散論理ルーターの相互運用性 : VMware NSX for vSphere 6.2 では、L2 ブリッジが分散論理ルーティングに参加できるようになりました。ブリッジ インスタンスに接続された VXLAN ネットワークが、ルーティング インスタンスとブリッジ インスタンスを接続するために使用されます。
- Edge Services Gateway (ESG) および分散論理ルーター インターフェイスでの RFC 3021 準拠の /31 プリフィックスのサポート

- ESG DHCP サーバ上でリレーされた DHCP 要求のサポートの強化
- NSX 仮想ネットワーク内で VLAN ID/ヘッダーを維持する機能
- 再分配フィルタにおける完全一致：再分配フィルタの一致アルゴリズムは ACL と同じです。したがって、デフォルトでは完全プリフィックス一致が実行されます（ただし、le または ge オプションが使用された場合を除く）。
- スタティック ルートのアドミニストレーティブ ディスタンスのサポート
- Edge のインターフェイスごとに uRPF チェックを有効、緩和、または無効にする機能
- CLI コマンド **show ip bgp** での AS パスの表示
- 分散論理ルーター制御仮想マシンでのルーティング プロトコルへの再分配から 高可用性インターフェイスを除外
- 分散論理ルーターの強制同期：分散論理ルーター間の East - West のルーティング トラフィックのデータ損失を回避します。North - South のルーティングとブリッジングでは引き続き中断が発生する場合があります。
- 高可用性構成の Edge アプライアンスが、アクティブかバックアップかを確認：NSX 6.2 Web クライアントでは、高可用性構成の 2 台の NSX Edge アプライアンスが、アクティブまたはバックアップのどちらであるかを確認できます。
- REST API が Edge でのリバース パス フィルタ (rp_filter) をサポート：システム制御 REST API を使用すると、ユーザー インターフェイスを使用して rp_filter sysctl を設定できます。また、これは vNIC インターフェイスおよびサブ インターフェイスの REST API にも発行されます。詳細については、[NSX API のドキュメント](#)を参照してください。
- IP プリフィックス **GE** および IP プリフィックス **LE** の BGP ルート フィルタの動作：NSX 6.2 では、BGP ルート フィルタが次のように機能強化されています。
 - LE/GE キーワードを使用できない：null ルート ネットワーク アドレス（ANY として定義または CIDR 形式 0.0.0.0/0 で定義）に対し、「以下 (LE)」と「以上 (GE)」のキーワードは使用できなくなりました。以前のリリースでは、これらのキーワードの使用は許可されていました。
 - LE と GE の値が 0 ～ 7 の場合、有効な値として処理されます。以前のリリースでは、この範囲は無効でした。
 - 所定のルート プリフィックスに対して、指定した LE 値よりも大きい GE 値を指定できなくなりました。

• ネットワークと Edge サービス

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

- 仮想 IP アドレスの最大数の増加：使用可能な仮想 IP アドレス数が増加し、最大 1024 までサポートされます。

- セキュリティ サービスの機能強化

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

- ソリューションの相互運用性

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

推奨されるバージョン、システム要件、およびインストール

推奨されるバージョンおよびシステム要件

次の表は、推奨される VMware ソフトウェアのバージョンおよび必要なバージョンを示したものです。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。最新の推奨事項については、[VMware ナレッジベースの記事 KB2144295](#) を参照してください。

| 製品またはコンポーネント | 推奨される最小バージョン |
|-----------------|---|
| NSX for vSphere | 6.2.2 注：SSL VPN に既知の問題があります。詳細については、CVE-2016-2079 を参照してください。バージョン 6.2.2 以前を利用しているお客様は、VMware にサポートを依頼してください。 VMware のサポートにお問い合わせいただくには、 My VMware でサポート リクエストを提出する方法 または サポート リクエストの送信方法 を参照してください。 |
| vSphere | 5.5U3、または 6.0U2 注：vSphere 6.0 と NSX オブジェクトに既知の問題があります。詳細については、 VMware ナレッジベースの記事 KB2144605 、「Duplicate VTEPs in ESXi hosts after rebooting vCenter Server」を参照してください。 |

ゲスト イントロスペクション

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

- VMware Tools 10.0.8 以降では、NSX または vCloud Networking and Security の VMware Tools をアップグレードしたあとに仮想マシンの動作が遅くなる問題が修正されています (VMware ナレッジベースの記事 [KB2144236](#)を参照)。
- VMware Tools 10.0.9 以降。このバージョンは Windows 10 をサポートします

vRealize Orchestrator

vRealize Orchestrator Plugin for NSX 1.0.3 以降

インストール

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。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。

廃止および提供を中止する機能

販売およびサポートの終了に関するご注意

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

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

サポートされていないコントローラ コマンドが表示されない

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

NSX 6.2.3 で TLS 1.0 のサポートが廃止に

NSX 6.2.3 では、NSX VPN および IPsec 暗号化スイートの中で TLS 1.0 のサポートが廃止になっています。以前のリリースに比べ、6.2.3 では暗号化のサポートにいくつかの変更が加えられています。これらの変更については、次の表をご覧ください。

SSL VPN 暗号化スイートのサポート：NSX 6.2.3 での変更

| 6.2.2 | 6.2.3 |
|-------------------------------|---------------------------------------|
| TLS_RSA_WITH_AES_128_CBC_SHA | TLS_RSA_WITH_AES_128_CBC_SHA |
| TLS_RSA_WITH_AES_256_CBC_SHA | TLS_RSA_WITH_AES_256_CBC_SHA |
| TLS_RSA_WITH_3DES_EDE_CBC_SHA | TLS_RSA_WITH_AES_128_GCM_SHA256 |
| | TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 |
| | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 |

L2 VPN 暗号化スイートのサポート：NSX 6.2.3 での変更

| 6.2.2 | 6.2.3 |
|-------------------|-----------------------------|
| AES128-SHA | AES128-GCM-SHA256 |
| AES256-SHA | ECDHE-RSA-AES128-GCM-SHA256 |
| AES128-GCM-SHA256 | ECDHE-RSA-AES256-GCM-SHA384 |
| DES-CBC3-SHA | NULL-SHA256 |
| NULL-MD5 | NULL-MD5 |

IP-Sec 暗号化スイート：NSX 6.2.3 での変更

| 6.2.2 | 6.2.3 |
|-------------------------|-------------------------|
| AES_128-HMAC_SHA1 | AES_128-HMAC_SHA1 |
| AES(12)_256-SHA1(2)_000 | AES(12)_256-SHA1(2)_000 |
| 3DES(3)_000-SHA1(2)_000 | 3DES(3)_000-SHA1(2)_000 |
| AES_GCM_C_160-NONE | AES_GCM_C_160-NONE |

アップグレードに関する注意事項

- ダウングレードはサポートされない:
 - アップグレードの前に、必ず NSX Manager をバックアップしてください。
 - NSX を正常にアップグレードしたあとは、ダウングレードすることはできません。

- NSX 6.2.4 にアップグレードするには、ホスト クラスタのアップグレード（ホストの VIB を 6.2.4 にアップグレード）を含む、完全な NSX アップグレードを実行する必要があります。手順については、『[NSX アップグレード ガイド](#)』の「[NSX 6.2 へのホスト クラスタのアップグレード](#)」のセクションを参照してください。
- コントローラ ディスクのレイアウト：NSX 6.2.3 以降の新規インストールでデプロイされる NSX Controller アプライアンスでは、ディスク パーティションを更新することにより、クラスタの回復性がさらに強化されます。以前のリリースでは、コントローラ ディスクでのログのオーバーフローがコントローラの安定性に影響する場合があります。NSX Controller アプライアンスは、オーバーフローを防止するためのログ管理機能の強化に加え、データとログに個別のディスク パーティションを使用することで、このような問題の発生を防ぎます。NSX 6.2.3 以降にアップグレードする場合、NSX Controller アプライアンスは元のディスク レイアウトを保持します。
- アップグレード パス：
 - NSX 6.x からのアップデート：VMware NSX のアップグレードの詳細については、[VMware 製品の相互運用性マトリクス](#)を参照してください。Cross-vCenter NSX のアップグレードについては、『[NSX アップグレード ガイド](#)』を参照してください。
 - VMware vCloud Network and Security (vCNS) 5.5.x からのアップグレード：2016 年 6 月 9 日以降に公開される NSX アップグレード バンドルでは、VMware vCloud Networking and Security (vCNS) 5.5.x から NSX 6.2.4 へ直接アップグレードできます。手順については、『[NSX アップグレード ガイド](#)』の「[vCloud Networking and Security から NSX へのアップグレード](#)」を参照してください。このセクションでは、vCloud Director 環境における vCNS 5.5.x から NSX へのアップグレードの手順についても説明しています。また、『[NSX for vShield Endpoint アップグレード ガイド](#)』では、vShield Endpoint をアンチウイルス保護にのみ使用する場合の vCNS 5.5.x から NSX 6.2.4 へのアップグレードの手順を説明しています。
 - NSX 6.1.6 から NSX 6.2.0、6.2.1、または 6.2.2 へのアップデートはサポートされません。
 - NSX 6.1.5 から NSX 6.2.0 へのアップデートはサポートされません。NSX 6.1.5 から NSX 6.2.4 以降へアップグレードすることで、最新のセキュリティ アップデートを取得できます。
- NSX 6.2.x へのアップデートが成功したことを確認するには、[ナレッジベースの記事 KB2134525](#) を参照してください。
- 他の VMware 製品との同時アップグレード：vCenter Server や ESXi などの他の VMware 製品とともに NSX をアップグレードする場合は、サポートされるアップグレード手順を実行する必要があります。アップグレード手順については、[ナレッジベースの記事 KB2109760](#) を参照してください。
- パートナー サービスとの互換性：ゲスト イントロスペクションまたはネットワーク イントロスペクション用に VMware のパートナー サービスをサイトで使用している場合、アップグレード前に [VMware 互換性ガイド](#)を参照して、このリリースの NSX とベンダーのサービスに互換性があることを確認してください。
- アップグレードに影響する既知の問題：アップグレードに関連する既知の問題については、このドキュメントの後半の「[インストールとアップグレードに関する既知の問題](#)」を参照してください。
- 新しいシステム要件：NSX Manager のインストールとアップグレードに必要なメモリと CPU の要件については、NSX 6.2 ドキュメントの「[NSX のシステム要件](#)」セクションを参照してください。
- NAT ルールの最大数：NSX Edge 6.2 より前のバージョンでは、ユーザーは SNAT ルールと DNAT ルールをそれぞれ 2048 ずつ設定できたため、ルールの最大数は 4096 でした。NSX Edge 6.2 以降は、NSX Edge アプライアンスのサイズに基づいて、NAT ルールの最大数が制限されます。

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

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

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

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

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

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

- ドラフトの自動保存と Service Composer：NSX 6.2.3 以降では、ドラフトの自動保存はデフォルトでオフに設定されます。ここで、NSX の分散ファイアウォールのファイアウォール ルールを自動的に保存するかどうかを設定します。アップグレードした場合、手動で行った設定は引き継がれます。パフォーマンスの問題を回避するため、ドラフトの自動保存機能は無効にすることをお勧めします。次の API 呼び出しを使用して、NSX 分散ファイアウォールの自動ドラフト設定を変更できます。

1. ファイアウォールの既存のグローバル構成 (GlobalConfiguration) の取得
GET `https://NSX-Manager-IP-`


```
Address/api/4.0/firewall/config/globalconfiguration
```

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

```
PUT https://NSX-Manager-IP-Address/api/4.0/firewall/config/globalconfiguration
```

要求の本文に次が含まれる：

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

GET メソッドでは、autoDraftDisabled フィールドは表示されません。

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

回避策： vSphere Web Client を使用して vCenter Server にログインします。スタックしている EAM タスクを右クリックして、キャンセルします。vSphere Web Client から、クラスタ上で [解決] を発行します。スタックしたホストの表示が処理中になります。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完了します。

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

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を作成する際に、ネットワーク遅延が増加することが原因で発生します。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。

回避策： 詳細は、[VMware ナレッジベースの記事 KB2146769](#) を参照してください。

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 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。

問題 1685375： VXLAN ゲートウェイにリモート MAC が見つからない

スイッチ（ハードウェア VTEP ゲートウェイ）を再ロードした後、リモート MAC アドレスが送信されません。まれに、ハードウェア VTEP ゲートウェイが再起動するときに、NSX Controller によって ovssdb MAC アドレス テーブルに情報がポピュレートされない場合があります。

回避策： 次の回避策のいずれかを実行して、ハードウェア VTEP の ovssdb リモート MAC アドレス テーブルに、コントローラが情報をポピュレートできるようにします。

1. VXLAN に接続された仮想マシンで次のコマンドを実行して、適切なネットワーク インターフェイスを設定します。
 - `ifconfig eth1 down`
 - `ifconfig eth1 up`
2. NSX Manager のユーザー インターフェイスで、ハードウェア VXLAN ゲートウェイ ポートを接続解除し、再度接続します。

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。

回避策： `serverType` を REST API 要求の本文に追加します。次はその例です。

```
<EventlogServer>
  <domainId>1</domainId>
  <hostName>AD_server_IP</hostName>
  <enabled>true</enabled>
  <serverType>WIN2k8</serverType>
</EventlogServer>
```

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。

回避策： NSX Manager を再起動するか、または次の API を実行して、余分なエントリを削除します。API の PUT メソッドを実行します。

`https://nsx-manager-address/api/internal/firewall/updatestatus`

問題 1659043： NSX Manager からユニバーサル サービス仮想マシン (USVM) への通信がタイムアウトすると、ゲスト イントロスペクションのサービス ステータスに「Not Ready」と表示される

内部のメッセージ バス (rabbit MQ) 上で NSX Manager によるパスワードの変更プロセスが正常に完了しなかった場合、ゲスト イントロスペクション USVM に対して、「PLAIN login refused: user 'usvm-admin-host-14' - invalid credentials」のようなエラー メッセージが表示される場合があります。

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

問題 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と 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。

回避策： ゲスト イントロスペクションを安定した状態に戻すには、既知の SID のルックアップを無視するように仮想マシンを設定する必要があります。そのためには、各ゲスト イントロスペクション仮想マシンの構成ファイルを更新して、サービスを再起動する必要があります。また、回避策として、Active Directory のログをスクレイピングして、ID ベースのファイアウォールに対するログイン イベントを検出することもできます。

解決できない SID へのルックアップを無視するには、次の手順を実行します。

1. ゲスト イントロスペクション仮想マシンにログインします。
2. ファイル /usr/local/usvmmgmt/config/ignore-sids.lst を編集します。
3. 次の 2 行を追加します。
S-1-18-1
S-1-18-2
4. ファイルを保存して閉じます。
5. 次のコマンドを実行して、ゲスト イントロスペクション サービスを再起動します。
rcusvm restart

問題 1558285：ゲスト イントロスペクションを利用しているクラスタを vCenter Server で削除すると、Null ポインタ例外が発生する

vCenter Server からクラスタを削除する前に、ゲスト イントロスペクションなどのサービスを削除する必要があります。

回避策： クラスタに関連付けられていないサービスの EAM エージェントを削除します。

問題 1629030：パケット キャプチャのセントラル CLI (パケット キャプチャのデバッグと表示用コマンド) は vSphere 5.5U3 以降でサポートされる

これらのコマンドは、vSphere 5.5 より前のバージョンではサポートされません。

回避策： NSX をご利用になる場合は、vSphere 5.5U3 以降を導入することをお勧めします。

問題 1568180：vCenter Server Appliance (vCSA) 5.5 を使用する場合、NSX の機能リストが正しく表示されない

vSphere Web Client のライセンスの機能を表示するには、ライセンスを選択して [操作] > [機能の表示] の順にクリックします。NSX 6.2.3 にアップグレードする場合、Enterprise ライセンスにアップグレードされ、すべての機能が有効になります。しかし、NSX Manager が vCenter Server Appliance (vCSA) 5.5 に登録されている場合、[機能の表示] を選択すると、新しい Enterprise ライセンスではなく、アップグレード前に使用されていたライセンスの機能が一覧表示されます。

回避策： vSphere Web Client に正しく表示されない場合でも、すべての Enterprise ライセンスでは同じ機能を利用できます。詳細については、[NSX ライセンス ページ](#)を参照してください。

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

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

回避策： なし。

問題 1491275：NSX API が特定の状況で XML ではなく JSON を返す
API 要求に対して、XML ではなく JSON がユーザーに返されることがあります。

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

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 1730017：NSX 6.2.3 から 6.2.4 にアップグレードすると、ゲスト イントロスペクションのバージョンが変更されたことが表示されない

NSX 6.2.3 には、最新バージョンのゲスト イントロスペクション モジュールが使用されており、6.2.4 へのアップグレードしてもバージョンは変更されません。NSX 6.2.3 より前の NSX リリースからのアップグレードでは、NSX 6.2.4 へのバージョン変更が示される場合があります。

回避策： これは機能には影響しません。

問題 1685894：NSX 6.2.3 VIB がインストールされたホストから古いバージョンの NSX VIB を持つホストに、DRS で仮想マシンを移行すると、ネットワーク接続が失われる
NSX ホスト（NSX VIB のエクスポート バージョンが新しい）から、古いバージョンの NSX VIB を持つ NSX ホストへの仮想マシンの vMotion はサポートされません。

回避策： これは NSX for vSphere 6.2.4 リリースに影響する既知の問題です。最新情報については、[VMware ナレッジベースの記事 KB2146171](#) を参照してください。

問題 1683879：メモリが 8 GB 未満のホストで、NSX 6.2.3 へのアップグレードに失敗する

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

回避策： なし。

問題 1673626：データベース サーバ エイリアス名を使用して DSN を作成すると、vCenter Server のインストールに失敗することがある

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

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

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

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

回避策： NSX Manager を再起動します。

問題 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：ユニバーサル サービス仮想マシン (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 へアップデートすると、[ライセンス キーの割り当て] ウィンドウの [製品] フィールドに、「NSX for vSphere - Enterprise」などの具体的な NSX ライセンス名ではなく、総称の「NSX for vSphere」と表示される

回避策：なし。

問題 1465249：ホストがオフラインであるにもかかわらず、ゲスト イントロスペクション のインストール ステータスが「成功しました」と表示される

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

回避策：なし。

問題 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 6.2.3 に移行した仮想マシンで TFTP ALG がサポートされない

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

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

問題 1394287：仮想ワイヤーから仮想マシンを追加または削除しても、vShield App ルールに設定された IP アドレスが更新されない

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

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

回避策：ルールをもう一度発行すると、新しいアドレスが設定されます。

問題 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 1088913：vSphere Distributed Switch MTU が更新されない

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

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

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 1288506：vCloud Networking and Security 5.5.3 を NSX for vSphere 6.0.5 以降にアップグレードした後、DSA-1024 のキーサイズを持つ SSL 証明書を使用すると、NSX Manager が開始されない
DSA-1024 のキーサイズを持つ SSL 証明書は、NSX for vSphere 6.0.5 以降ではサポートされないため、アップグレードは失敗します。

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

問題 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 1402307：NSX for vSphere のアップグレード プロセスで vCenter Server を再起動すると、クラスタのステータスが誤って表示される

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

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

問題 1487752：アップデート中にサードパーティ製アンチウイルスによる保護が一時的に失われる

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

回避策： なし。

問題 1498376：分散ファイアウォールの設定時にホストのエラーメッセージが表示される

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

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

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

<nwFabricFeatureConfig>

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

問題 1491820 : NSX 6.2 へのアップデート後、NSX Manager ログに「**WARN messagingTaskExecutor-7**」というメッセージが記録される

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

回避策： なし。

問題 1284735 : VMware vCloud Network and Security (vCNS) からのアップグレード後、アップグレードされたグループ オブジェクトに、新しいグループ オブジェクトを追加できない

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

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

問題 1495969 : vCloud Networking and Security 5.5.4 から NSX 6.2.x へとアップグレードした後、[ホストの準備] タブでファイアウォールが無効のままになる

vCloud Networking and Security 5.5.x から NSX 6.2.x へアップグレードし、すべてのクラスタをアップグレードした後、[ホストの準備] タブでファイアウォールが無効のままになります。また、ファイアウォールをアップグレードするオプションがユーザー インターフェイスに表示されません。この問題は、NSX が展開された準備されたクラスタの一部に含まれないホストがデータセンターに存在するときのみ発生します。これはクラスタ外の、ホストには VIB がインストールされないためです。

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

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

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

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 1479314 : NSX 6.0.7 SSL VPN クライアントが NSX 6.2 SSL VPN ゲートウェイに接続できない

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

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

問題 1434909：新規またはアップグレードした分散論理ルーター用にセグメント ID プールを作成する必要がある

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

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

問題 1459032：VXLAN ゲートウェイの構成エラー

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

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

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

回避策： エラーを修正するには、次のいずれかの方法を使用します。

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

問題 1463767：Cross-vCenter Server 環境で、ユニバーサル ファイアウォール構成セクションがローカル構成セクションの下位に（従属的に）置かれる場合がある

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

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

問題 1289348：アップデートの後、ファイアウォール ルールとネットワーク イントロスペクション サービスが NSX Manager と同期しなくなることがある

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

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

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-vsisp 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-vsisp および esx-vxlan の NSX VIB とともに、3 つめの VIB として esx-vgpi 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 1479314：NSX 6.2 では SSLv2 と SSLv3 が廃止される

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

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

問題 1411275： NSX for vSphere 6.2 でのバックアップとリストア後、vSphere Web Client で [Networking and Security] タブが表示されない

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

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

問題 1493777： NSX 6.2 へのアップグレード後、NSX Manager に割り当てられた物理メモリが 100% を超える

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

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

問題 1393889： IP アドレスの接続が確立されていない場合でも Data Security サービスのステータスが稼動中として表示される

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

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

[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。

NSX Manager に関する既知の問題

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

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

回避策： なし。

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

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

回避策： 次の手順で ESXTOP プラグインを削除します。

1. vCenter Server 仮想マシンのスナップショット（休止なし）の最新のバックアップがあることを確認します。
2. 次のように指定して、`/usr/lib/vmware-vmware-nsx-plugin/packages/esxtop-plugin` を削除します。
`rm -R /usr/lib/vmware-vmware-nsx-plugin/packages/esxtop-plugin`
3. 次のように指定して、`/usr/lib/vmware-vmware-nsx-plugin/server/work` を削除します。

```
rm -R /usr/lib/vmware-vmware-nsx-manager/server/work
```

4. Web Client を再起動します。

```
service vmware-nsx-manager restart
```

5. (オプション) `tail -f /var/log/vmware/vsphere-client/logs/eventlog.log | grep esx` コマンドからの出力がないことを確認します。

6. ロールバック オプションとして vCenter Server スナップショットの統合を選択する場合は、これを実行します。

問題 1466790 : NSX Manager はスペース区切りのある DNS 検索文字列を受け付けない

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

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

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 1446649/1445281 : セカンダリ NSX Manager の IP アドレス/サムプリントを変更すると、Cross-vCenter Server のセットアップでユニバーサル オブジェクトのレプリケーション エラーが発生する

セカンダリ NSX Manager の IP アドレス/サムプリントを変更すると、プライマリ NSX Manager がセカンダリ NSX Manager の最新の IP アドレス/サムプリントを認識しないため、Cross-vCenter Server のセットアップでユニバーサル オブジェクトのレプリケーション エラーが発生します。

回避策：ユニバーサル オブジェクトのユニバーサル同期ステータスをクリックすると、「ピアが認証されていません; ネストされている例外は `javax.net.ssl.SSLPeerUnverifiedException` です」のような例外が表示され、IP アドレス/サムプリントが変更されたことが分かります。

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が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 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 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 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作成するには、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、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 1534622：NSX Controller が切断されていると表示される

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

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

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 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 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 1415480 : NSX Manager のバックアップをリストアした後、REST 呼び出しでファブリック機能 **com.vmware.vshield.nsxmgr.messagingInfra** のステータスが赤で表示される

NSX Manager のバックアップをリストアし、REST API 呼び出しを使用してファブリック機能 com.vmware.vshield.nsxmgr.messagingInfra のステータスをチェックすると、ステータスは緑ではなく赤として表示されます。

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

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

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

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 : 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 1406471：バックアップ元の NSX Manager のホスト名が、リストア先 NSX Manager の Syslog に表示される

2 番目の NSX Manager をインストールするときに最初の NSX Manager と同じ IP アドレスと一意のホスト名を使用した場合、設定をリストアすると、リストア後に最初の NSX Manager のホスト名が表示され、再起動後に 2 番目の NSX Manager のホスト名が表示されます。

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

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 1467866：スタンドアロンの NSX Manager で、ユニバーサル ファイアウォール構成のインポートが誤って許可される

スタンドアロン モードで実行している NSX Manager では、適用されない場合でも、ユニバーサル ファイアウォール ルールがインポートされることがあります。一度インポートされると、これらのルールは API や Web Client を介して削除できず、ローカル セクションとして保持され、処理されます。

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

次の手順を実行してください。

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

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

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

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

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

問題 1733146：特定の状況で、制御仮想マシンが配置されていない場合に、ユニバーサル分散論理ルーター用に論理インターフェイスを作成または変更すると失敗する

この問題は以下の状況で発生しています。

- ECMP にデフォルトのスタティック ルートが 2 つある
- スタティック ルートに Local Egress (ローカル出力方向) フラグがある

この問題は、差分の更新ではなく完全な同期が要求される場合に発生し、その結果、重複したエンティティが拒否されて操作に失敗します。次のようなメッセージが表示されます：

`2016-09-22 20:18:58.080 GMT ERROR TaskFrameworkExecutor-24 NvpRestClientManagerImpl:774 - NVP API returns error: [409] Route with the same prefix and priority already exist on router dc5e541a-d7a6-4cb9-8d8a-9334a9c51127`

回避策：

1. ユニバーサル分散論理ルーターを削除します。
2. 新しいユニバーサル分散論理ルーターを展開します。Local Egress（ローカル出力方向）を有効にし、[Edge アプライアンスのデプロイ] を選択解除します。2 つのアップリンク インターフェイスを設定します。そのうち最初のアップリンクを経由するデフォルト ゲートウェイとして、プライマリ分散論理ルーターのロケール ID（たとえば 1111xxxx）を設定します。
3. セカンダリ サイトで使用されるロケール ID（たとえば 2222xxxx）には 0.0.0.0/0 のスタティック ルートを追加しないでください。
4. セカンダリ サイトの予期されるネクスト ホップ IP アドレスおよびロケール ID（たとえば 222xxxx）に次の 2 つのスタティック ルートを追加します。
ルート #1: 0.0.0.0/1
ルート #2: 128.0.0.0/1

問題 1716545： Edge のアプライアンス サイズを変更しても、スタンバイ Edge の CPU とメモリの予約が変更されない

予約設定は、高可用性構成の 2 台の Edge 仮想マシンのうち、最初に作成された仮想マシンにのみ割り当てられます。

両方の Edge 仮想マシンに同じ CPU/メモリ予約（以下、予約）を構成するには、次のいずれかの手順を実行します。

- PUT API <https://api/4.0/edgePublish/tuningConfiguration> を使用して、両方の Edge 仮想マシンに値を明示的に設定します。
または
- Edge の高可用性を一度無効にして再び有効にします。これで、2 番目の Edge 仮想マシンが削除され、デフォルトの予約が設定された新しい Edge 仮想マシンが展開されます。

回避策： なし。

問題 1717369： 高可用性モードで構成すると、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。この問題が修正された NSX リリースでは、次が期待される動作になります。

- 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。

回避策： なし。

問題 1510724： 新しいユニバーサル分散論理ルーター (UDLR) を作成した後にデフォルトのルートがホストにポピュレートされない

NSX for vSphere 6.2.x で、Cross-vCenter を構成するために NSX Manager をスタンドアロンからプライマリ モードに変更した後、次の問題が発生することがあります。

- 新しい UDLR を作成するときに、ホスト インスタンスにデフォルトのルートがポピュレートされない。
- ルートがホスト インスタンスではなくユニバーサル分散論理ルーター制御仮想マシンにポピュレートされる。
- `show logical-router host host-ID dlr Edge-ID route` コマンドを実行すると、デフォルトのルートが追加されない。

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

問題 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。

回避策： LACP を使用するときには、物理スイッチ上でフローベースのハッシング アルゴリズムを設定しないようにします。代わりに、MAC アドレスを同じアップリンクに固定するか、ポリシーをソース MAC に変更します。

問題 1703247：NSX で分散論理ルーターに高可用性を構成すると、仮想マシンのネットワーク接続が失われる

動的ルーティングを使用していて、分散論理ルーター制御仮想マシンに高可用性機能を構成している NSX 6.2.3 環境では、分散論理ルーター制御仮想マシンがスプリット ブレイン状態から復旧する際に、仮想マシンのネットワーク接続が失われます。

回避策： このネットワークの問題を解決するには、[VMware ナレッジベースの記事 KB2146413](#) を参照してください。

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

一番大きい数字の IP アドレスを持っていない Not-So-Stubby Area (NSSA) ABR をシャットダウンまたは再起動した場合、トラフィックは別のパスにただちに収束されます。一番大きい数字の IP アドレスを持つ NSSA ABR をシャットダウンまたは再起動すると、再コンバージェンスに時間がかかる場合があります。OSPF プロセスを手動でクリアして、コンバージェンスの時間を短縮できます。

回避策：[VMware ナレッジベースの記事 KB2127369](#) を参照してください。

問題 1542416：サブ インターフェイスを使用して Edge の再デプロイや高可用性フェイルオーバーを行った後、データ パスが 5 分間動作しない

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

回避策：回避策はありません。

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

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

回避策：高可用性インターフェイスへの接続ルートを失っている分散論理ルーター アプライアンスの vNIC への接続を解除してから再接続するか、または分散論理ルーター アプライアンスを再起動します。

問題 1461421：NSX Edge の「show ip bgp neighbor」コマンドの出力で、以前接続を確立したカウントが維持される

「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 認証で使用するパスワードを変更すると、ピア接続が破棄されて再作成されるため、カウンタがクリアされます。この問題は、Edge 分散論理ルーター (DLR) では発生しません。

回避策： カウンタをクリアするには、「clear ip bgp neighbor」コマンドを実行します。

問題 1676085：リソースの予約に失敗すると、Edge の高可用性機能の有効化に失敗する

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

回避策：これは、機能変更で想定される正常な動作です。

問題 1656713：HA フェイルオーバー後 NSX Edge に IPsec セキュリティ ポリシー (SP) が存在せず、トラフィックがトンネルを通過できない

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

回避策：NSX Edge の切り替え後、IPsec を一度無効にしてから有効にします。

問題 1588450：vSphere HA のイベント中は NSX Edge 仮想マシンがフェイルオーバーしない

この問題は、vSphere HA を構成したあとに NSX Edge 仮想マシンを設定すると発生します。NSX Edge 仮想マシンを設定すると、ESXi の自動シャットダウンと自動起動構成に追加されます。その後、ESXi ホストからのパワーオフ イベントを受信した際に、NSX Edge 仮想マシンが vSphere HA の保護リストから削除されます。

回避策：詳細は、[VMware ナレッジベースの記事 KB2143998](#) を参照してください。

問題 1624663：[詳細デバッグの設定] をクリックすると、vCenter Server ユーザー インターフェイスが更新され、変更が維持されない

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

回避策：Edge のリスト メニューに直接移動して Edge をハイライト表示し、[アクション] > [詳細デバッグの設定] の順にクリックして、変更を行います。

問題 1354824：Edge 仮想マシンが破損したり、電源障害などの理由によりアクセスできなくなると、NSX Manager からの健全性チェックが失敗した場合にシステム イベントが表示される

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

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

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

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

回避策：回避策はありません。

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

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

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

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

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

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

問題 1463856：NSX Edge ファイアウォールが有効になっていると、既存の TCP 接続がブロックされる Edge のステートフル ファイアウォールで、最初の 3 ウェイ ハンドシェイクが認識されないために、TCP 接続がブロックされます。

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

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

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

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

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

回避策： esxcli の代わりに localcli を使用します。

問題 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 1606785：NSX Edge ロード バランサの nagios.log ファイルのメッセージによって /var/log/partition が肥大する場合がある

毎日適切なタイミングでログをリセットするようにログのローテーション レートを設定していない場合、/var/log/partition フォルダにある NSX Edge ロード バランサの *nagios.log* ファイルが肥大することがあります。

回避策： *Nagios.log* メッセージを Syslog に書き込むようにします。

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

ターゲット 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 1562767：NSX ロード バランサへの接続が遅くなると、複数の仮想 IP アドレスがある場合、一貫した接続方法を提供できない

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

問題 1553600：IP アドレスをインターフェイスに割り当てると、RIB や FIB への接続が遅くなる

IP アドレスをインターフェイスに割り当てようとすると、通常、そのインターフェイスの情報が即座にアップデートされます。しかし、ポーリング イベントを待機しているとき、割り当てられた IP アドレスの表示が遅れることがあります。NSX 分散論理ルーターは、インターフェイスの変更を取得するために、定期的にポーリングを実行します。

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 1534602：ユーザー インターフェイスに Edge 管理プレーン モード (VIX/MSGBUS) が表示されず、VIX から MSGBUS に変更するオプションが提供されない

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

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

問題 1498243：BGP ネイバー フィルタを「拒否、任意、送信」に設定している場合、分散論理ルーターがデフォルト ルートの誤ったネクスト ホップを通知する

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

- 操作：拒否
- ネットワーク：任意
- 方向：送信

回避策： なし。

問題 1471561：直接接続されているルーターでは、BGP/OSPF の隣接関係が確立されない

ECMP ルートが直接接続されたネットワークに存在する場合、直接接続されたルーターでは動的ルーティングが期待したとおりに動作しません。

回避策： Edge を再起動します。または、関連付けられている vNIC インターフェイスを削除してから再作成します。

問題 1089745：分散論理ルーター OSPF が無効になっている場合でも、分散論理ルーター LIF のルートがアップストリーム Edge Services Gateway によってアドバタイズされる

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

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

問題 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、不透明チャンネル上の dvPort に設定されている VXLAN トランクがリセットされません。これは、トランクの設定が NSX Manager で管理されているためです。

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

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

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

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

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

6. [opaqueDataSpec] に次の XML を追加します。

```
<opaqueDataSpec>
  <operation>remove</operation>
</opaqueData>
```

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

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

セキュリティ サービスに関する既知の問題

問題 1704661：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：Failed to restore PF state : Limit exceeded

NSX for vSphere 6.1.x から 6.2.4 にアップグレードした後、次の問題が発生することがあります。

- 一部の仮想マシンが vMotion 後にネットワーク接続を失う。
- 仮想マシンの移行先である ESXi ホストの `/var/log/vmkernel.log` ファイルに次のようなエントリが表示される：
 - 2016-07-28T09:07:00.764Z cpu21:33397)<6>host7: libfc: Link up on port (0)
 - 2016-07-28T09:07:00.766Z cpu11:1294844)Vmxnet3: 15253: Using default queue delivery for vmxnet3 for port 0x2000065
 - 2016-07-28T09:07:00.767Z cpu11:1294844)PFImportState: unsupported version: 0
 - 2016-07-28T09:07:00.767Z cpu11:1294844)vsip VSIPDVFRestoreState:2059: Failed to restore PF state : Limit exceeded
 - 2016-07-28T09:07:00.767Z cpu11:1294844)WARNING: NetPort: 1579: failed to enable port 0x2000065: Failure
 - 2016-07-28T09:07:00.767Z cpu11:1294844)Vmxnet3: 16236: Port_Enable failed for port 0x2000065
- これは、NSX for vSphere 6.1.x に展開された仮想マシンの vMotion がサポートされないという VSIP モジュールの既知の問題により発生します。

回避策：これは NSX for vSphere 6.2.4 リリースに影響する既知の問題です。最新情報については、[VMware ナレッジベースの記事 KB2146171](#) を参照してください。

問題 1732337/1724222：NSX Manager が、ESXi 6.0 P03 ホストにファイアウォール ルールをプッシュできない

NSX Manager が、ESXi 6.0 P03 ホストにファイアウォール ルールをプッシュできず、vsfwd 接続が閉じているため、NSX Edge の健全性チェックに失敗します。これは ESXi 6.0 P03 を備えた VMware NSX for vSphere 6.2.x (ビルド 4192238) に影響する既知の問題です。この問題は、パスワード生成時の NSX の動作に影響する `/dev/random` 呼び出しがブロックされている場合に発生します。

回避策：VMware テクニカル サポートにお問い合わせください。最新情報については、[VMware のナレッジベースの記事 KB2146873](#) を参照してください。

問題 1620460: NSX は、Service Composer のルール セクションにユーザーがルールを作成することを許可してしまう

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

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

問題 1682552：分散ファイアウォール (DFW) の CPU、メモリ、1 秒あたりの接続数 (CPS) のしきい値イベントがレポートされない

分散ファイアウォールの CPU、メモリ、および CPS のしきい値イベントをレポートするように設定してあっても、しきい値を超えた際にレポートされません。

回避策：

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

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

問題 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] 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、予期しない結果がもたらされることがあります。

回避策： 次の回避策を実行できます。

- [セキュリティ ポリシー] タブの [アクション] メニューから [ファイアウォール ルールの同期] を選択して、Service Composer のルールと ファイアウォールのルールを同期します。
- フィルタはルール セットの表示にのみ使用し、ルール セットの更新には使用しません。
- フィルタを使用する前に、REST API `/api/4.0/firewall/globalroot-0/config PUT` または ユーザー インターフェイスを介して完全な発行を実行します。これにより、1 つのセクションだけでなく複数のセクションが更新されるため、ファイアウォールのグローバル構成を確実に行うことができます。

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

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

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

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

```
<error>
```

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

```
<errorCode>258
```

```
</errorCode>
```

```
</error>
```

回避策： ファイアウォール構成を同時に変更しないようにします。

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

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

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

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

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

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

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

問題 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ため、タグを割り当てる仮想マシンは、一度の呼び出しで最大 500 台にしてください。

問題 1662020：分散ファイアウォールのユーザー インターフェイスの [全般] および [パートナー セキュリティ サービス] セクションに、「前回の発行操作はホスト <ホストの番号> で失敗しました」という内容のエラー メッセージが表示され、発行操作に失敗する場合がある

任意のファイアウォール ルールを変更した後、ユーザー インターフェイスに「前回の発行操作はホスト <ホストの番号> で失敗しました」というエラー メッセージが表示されます。ユーザー インターフェイスに表示されるホストは、正しいバージョンのファイアウォール ルールを使用していない可能性があり、そのためにセキュリティ上の不備や、ネットワークの中断が発生します。

この問題は、通常次の状況で発生します。

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

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

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

回避策： なし。

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

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

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

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

回避策： なし。これは、設計上想定される正常な動作です。

問題 1662020：Cross-vCenter 環境のセットアップで、分散ファイアウォール (DFW) 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] タブに、「前回ホスト 10.156.221.88 上で発行に失敗しました」というエラー メッセージが表示される

このエラー メッセージは、ルールに関連付けられている NIC が存在しない場合に表示されます。

回避策： なし。

問題 1637939：ハードウェア ゲートウェイのデプロイ中に MD5 証明書がサポートされない

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

回避策： なし。

問題 1637943：ハードウェア ゲートウェイ バインドを含む VNI で、ハイブリッドまたはマルチキャスト レプリケーション モードがサポートされない

L2 VXLAN から VLAN へのブリッジ用 VTEP として使用されるハードウェア ゲートウェイ スイッチは、ユニキャスト レプリケーション モードのみをサポートします。

回避策： ユニキャスト レプリケーション モードのみを使用します。

問題 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-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="143" name="AutoSaved_Wednesday, August 5, 2015 11:08:40 PM GMT"
timestamp="1438816120713">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="128" name="AutoSaved_Wednesday, August 5, 2015 9:08:02 PM GMT"
timestamp="1438808882608">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
  <firewallDraft id="127" name="AutoSaved_Wednesday, August 5, 2015 9:08:01 PM GMT"
timestamp="1438808881750">
    <description>Auto saved configuration</description>
    <preserve>false</preserve>
    <user>replicator-1fd96022-db14-434d-811d-31912b1cb907</user>
    <mode>autosaved</mode>
  </firewallDraft>
</firewallDrafts>
```

問題 1449611 : Security Group の削除により Service Composer のファイアウォール ポリシーが同期なくなると、ユーザー インターフェイスでファイアウォール ルールを修正できない

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

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 1505316：選択したサービスがサービス グループである場合に、NSX NetX ルールがホストに発行されない

分散ファイアウォールの[パートナー サービス] タブで L3 リダイレクト ルールを作成する場合、サービス グループを選択してもルールは正しく作成されません。

回避策： ルールを作成する際は、サービス グループを使用せずに、個々のサービスを使用してください。

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 1493611：L2 VPN で VLAN ID 0 に接続できない

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

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

問題 1534574：SSLVPN-Plus で Cipher 3C (SHA-256) 暗号化アルゴリズムがサポートされない

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 1534585：VMware NSX for vSphere 6.1.x および 6.2.x でリファレンス オブジェクトの削除後、分散ファイアウォール (DFW) ルールの発行に失敗する

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

問題 1494718：新しいユニバーサル ルールを作成できず、既存のユニバーサル ルールを フロー モニタリングのユーザー インターフェイスで編集できない

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

問題 1442379：Service Composer のファイアウォール構成が同期していない

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

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

問題 1301627：229 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 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 1438859：アップグレードされた NSX 環境でファイアウォール ルールを発行すると、Web Client で Null ポインタ例外になることがある

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

監視サービスに関する既知の問題

問題 1655593：監査ロールまたはセキュリティ管理者ロールでログインしているときに、NSX ダッシュボードにステータスが表示されない

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

回避策： なし。

ソリューションの相互運用性に関する問題

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、デプロイに失敗する

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

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

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

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

回避策： なし。

NSX Controller に関する既知の問題

問題 1516207：NSX Controller クラスタで IPsec 通信が再び有効にされた後に、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

[NSX 6.2.4 で解決した問題](#)、または [NSX 6.2.3 以前で解決した問題](#)を参照してください。

NSX 6.2.4 で解決した問題

NSX 6.2.4 で解決した問題には次のトピックが含まれます。

- [NSX 6.2.4 で解決した一般的な問題](#)
- [NSX 6.2.4 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 6.2.4 で解決した NSX Manager に関する問題](#)
- [NSX 6.2.4 で解決した論理ネットワークに関する問題](#)
- [NSX 6.2.4 で解決したネットワークと Edge サービスに関する問題](#)
- [NSX 6.2.4 で解決したセキュリティ サービスに関連する問題](#)
- [NSX 6.2.4 で解決した監視サービスに関連する問題](#)
- [NSX 6.2.4 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 6.2.4 で解決した一般的な問題

- 解決した問題 1696192：NSX Manager の NTP 同期の問題
NSX 6.2.3 では新しいバージョンの fcron が追加されました。fcrontab には環境変数が定義されていないため、fcron 実行ジョブの環境が初期化されません。\$PATH が空であるため、スクリプトは ntpdate コマンドを見つけることができません。この問題は NSX 6.2.4 で修正されました。

NSX 6.2.4 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 1710454：新しく展開した分散論理ルーター (DLR) とアップグレードした DLR 間で高可用性のデッドタイムが一致しない
この問題は、分散論理ルーターを新しくアップグレードすると、アップグレード中に高可用性のデッドタイムが 15 秒から 6 秒に明示的に変更されることが原因で発生します。
回避策： 詳細は、[VMware ナレッジベースの記事 KB2146714](#) を参照してください。この問題は NSX 6.2.4 で修正されました。

NSX 6.2.4 で解決した NSX Manager に関する問題

- 解決した問題 1668519：NSX Manager の CPU 使用率が高い
NSX Manager の CPU 使用率が高い状態が続くことがあります。特に、再起動のあとは、タスクをパージするプロセスが NSX Manager データベースの大量のジョブ エントリを処理またはクリーンアップする必要があるため、CPU 使用率が高くなります。
回避策： VMware テクニカル サポートにお問い合わせください。[VMware ナレッジベースの記事 KB2145934](#) を参照してください。この問題は NSX 6.2.4 で修正されました。
- 解決した問題 1603954：NSX Manager のメモリ使用率が、常にほぼ 100% の状態で表示される
NSX Manager を再起動するとメモリ使用率は 100% から大きく低下しますが、時間とともに 100% に戻り、そのままの状態になります。この問題は NSX 6.2.4 で修正されました。

NSX 6.2.4 で解決した論理ネットワークに関する問題

- 解決した問題 1696887：仮想マシンが、論理分散ルーターの外部へのネットワーク接続を失う
仮想マシンが分散論理ルーターの pMAC を、汎用分散論理ルーターの MAC アドレスではなくデフォルトゲートウェイの MAC アドレスとして認識する場合、分散論理ルーターの外部接続を失います。
回避策：[VMware ナレッジベースの記事 KB2146293](#) を参照してください。この問題は NSX 6.2.4 で修正されました。

NSX 6.2.4 で解決した NSX Edge サービスに関連する問題

- 解決した問題 1703913：NSX で分散論理ルーター (DLR) に高可用性を構成したノードがスプリット ブレイン状態のままになる
動的ルーティングを使用していて、分散論理ルーター制御仮想マシンに高可用性機能を設定している NSX 6.2.3 環境では、分散論理ルーター (DLR) に高可用性を設定したプライマリ ノードとセカンダリ ノードの両方が同時にアクティブ状態になり、その状態が維持されることがあります。
回避策：詳細は、[VMware ナレッジベースの記事 KB2146506](#) を参照してください。この問題は NSX 6.2.4 で修正されました。
- 解決した問題 1674721：NSX 6.2.3 へのアップグレード後、NSX Edge を管理できなくなる
この問題は、以前のバージョンで、ロード バランサで serverSsl または clientSsl が設定され、暗号化の値が NULL に設定されていた場合に発生します。
回避策：詳細は、[VMware ナレッジベースの記事 KB2145887](#) を参照してください。この問題は NSX 6.2.4 で修正されました。
- 解決した問題 1698389：vSphere Web Client で特定のルーティング構成を変更すると、ルーティング構成が不正になる
編集する前に並べ替えを行うと、BGP ネイバー、OSPF エリアとインターフェイスのマッピング、ルート再配分 (IP アドレスのプリフィックス) または BGP フィルタを編集したときに設定が不正になります。大量の BGP ネイバーを設定すると、リストをスクロールしてから編集を行ったときに設定が不正になることがあります。
回避策：詳細は、[VMware ナレッジベースの記事 KB2146363](#) を参照してください。この問題は NSX 6.2.4 で修正されました。

NSX 6.2.4 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 1694483：NSX for vSphere 6.2.3 をインストールするか、これにアップグレードして、分散ファイアウォール (DFW) と Security Group (SG) を設定すると、コンピュート仮想マシンで vMotion が行われる際にトラフィックが中断する場合がある
[VMware ナレッジベースの記事 KB2146227](#) を参照してください。この問題は NSX 6.2.4 で修正されました。
- 解決した問題 1689356：検索した Security Group を編集すると、すべてのオブジェクトが Security Group から削除される
Security Group に静的に含まれているメンバー (仮想マシンなど) を検索してから編集した場合、検索したメンバーを削除すると、静的に含まれているすべてのメンバーが Security Group から削除されます。この問題は NSX 6.2.4 で修正されました。
- 解決した問題 1675694：接続が中断した後で同じ IP アドレスとポートを再度使用すると、分散ファイアウォールがパケットをドロップする
特定の IP アドレスとポートへの接続が途中まで閉じた状態で切断されていない場合、新たに同一の IP アドレス/ポートへの接続を試みると失敗します。この問題は NSX 6.2.4 で修正されました。
- 解決した問題 1698863：分散ファイアウォールが有効な状態で、確立された TFTP セッション上で最初の TFTP パケットを再転送すると、パープル スクリーンが表示される
この問題は NSX 6.2.4 で修正されました。

- 解決した問題 1701195：分散ファイアウォールのヒープが枯渇する
統合率（ホスト 1 台あたりのプロビジョニングされた仮想マシン数）の高い大規模な導入環境では、分散ファイアウォールで利用可能な VMkernel が、大容量メモリのホストで最大 1.5GB に制限されているため、分散ファイアウォールのヒープが枯渇します。この問題は NSX 6.2.4 で修正されました。メモリが 96GB 以上の ESXi 6.0 ホストの最大ヒープサイズが 3GB に増え、高い統合率が可能になりました。
- 解決した問題 1712698：セキュリティ ポリシー ファイアウォール ルールを変更しようとした後で、Service Composer のセキュリティ ポリシー ルールが削除される
この問題は NSX 6.2.4 で修正されました。

NSX 6.2.4 で解決した監視サービスに関連する問題

- 解決した問題 1697118：IPFIX フローはすべて、更新フローではなく新規フローとしてタグ付けされるため、IPFIX コレクタへの更新が頻繁に発生する
また、アクティブ フローを送信する頻度は、アクティブ フローのタイムアウトで設定された値を考慮しません。この問題は NSX 6.2.4 で修正されました。

次の問題が 6.2.3、6.2.2、6.2.1 および 6.2.0 リリースで解決されました。

6.2.3、6.2.2、6.2.1 および 6.2.0 で解決した問題には、次のトピックが含まれます。

- [NSX 6.2.3 以前で解決した一般的な問題](#)
- [NSX 6.2.3 以前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 6.2.3 以前で解決した NSX Manager に関する問題](#)
- [NSX 6.2.3 以前で解決した論理ネットワークと NSX Edge ルーティングに関する問題](#)
- [NSX 6.2.3 以前で解決した Edge サービスに関連する問題](#)
- [NSX 6.2.3 以前で解決したセキュリティ サービスに関連する問題](#)
- [NSX 6.2.3 以前で解決した監視サービスに関連する問題](#)
- [NSX 6.2.3 以前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 6.2.3 以前で解決した一般的な問題

- 解決した問題 1644529：セキュリティの脆弱性 (CVE-2016-2079) に対応するセキュリティ パッチ
6.2.3 リリースでは、[CVE-2016-2079](#) に対応するセキュリティ パッチを提供しています。
- 解決した問題 1571156：vCenter Server 6.0 を再開/再起動すると、VXLAN を使用する ESX ホストで VTEP が重複することがある
[VMware ナレッジベースの記事 KB2144605](#) を参照してください。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1529665：DaaS サービスが、完全に同一の設定であるが、一方は HTTP 用、他方は PCoIP 用の 2 つの仮想 IP アドレスを使用するサービスとして動作しない
NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1631261：Identity Firewall (IDFW) でログ スクレーパが機能するように設定され、ゲスト イントロスペクション (GI) もインストールされているとき、GI をアンインストールすると IDFW の動作が停止する
NSX 6.2.2 で、この問題は修正されました。
- 解決した問題 1551773：VMware NSX for vSphere 6.2.0 で、Edge Services Gateway (ESG) HA vNIC のドロップダウンの選択肢が常に空になる
NSX 6.2.2 で、この問題は修正されました。[VMware ナレッジベースの記事 KB2138158](#) を参照してください。
- 解決した問題 1608608：glibc の脆弱性 (CVE-2015-7547) に対応するセキュリティ パッチ
6.2.2 リリースでは、[CVE-2015-7547](#) に対応するセキュリティ パッチを提供しています。

- **解決した問題 1480581**：netcpa ソケットが閉じられていて、仮想マシンが VNI と サブネットを介した通信に失敗する

この問題は、スレッド アンセーフな vmacore での boost::asio のスレッド アンセーフな利用を修正することで解決されました。NSX 6.2.2 で、この問題は修正されました。 [VMware ナレッジベースの記事 KB2137011](#) を参照してください。
- **解決した問題 1583566**：ルールがホストにプッシュされない

NSX Manager のタスク フレームワーク リソースの制約により、分散ファイアウォール ルール/IP アドレス リストの更新がスケジュールされずに失敗する。エラー メッセージには、変更通知スレッドのタスクをキューに登録できなかったことが示されます。NSX 6.2.2 で、この問題は修正されました。
- **解決した問題 1573818**：Edge Security Gateway (ESG) で、HA フェイルオーバーの後にトラフィックが 50 秒間中断される

この問題は、NSX が HA NSX Edge ノード間でスタティック ルートの同期に失敗した場合に発生します。NSX 6.2.2 で、この問題は修正されました。
- **解決した問題 1570808**：NSX ロード バランサの IP_HASH 健全性チェックの問題

IP v では、送信元 IP アドレスのハッシュ アルゴリズムを使用する際に、選択されたバックエンド サーバの weight が 0 の場合は、健全なバックエンド サーバが存在していても、サービスを利用できないことを示すメッセージが返されます。NSX 6.2.2 で、この問題は修正されました。
- **解決した問題 1564005**：NSX NetX で、トラフィックをパートナー デバイスにリダイレクトするルールを追加できない

トラフィック リダイレクト ルールを NetX ルール セットに追加できないため、トラフィックをパートナー デバイスにリダイレクトすることができません。この問題は、IP アドレス セットを使用するルールに影響します。この問題の原因は、NetX ルールで IP アドレス範囲が適切に処理されないことにあります。NSX 6.2.2 で、この問題は修正されました。
- **解決した問題 1587660**：DVFilterProcessSlowPathPackets の NSX NetX エラー

分散ファイアウォール (DFW) を使わずに NSX NetX を使用すると、DVFilter でエラーが発生します。完全なエラー メッセージでは、DVFilterProcessSlowPathPackets、VSIPDVFilterProcessSlowPathPackets、PFFilterPacket の NetX エラー PF (err=11,cr2=0x10) が示されます。NSX 6.2.2 で、この問題は修正されました。 [VMware ナレッジベースの記事 KB2144018](#) を参照してください。
- **解決した問題 1591673**：ライセンス エラーにより、vSphere Distributed Switch に ESXi ホストを追加できない

NSX 6.2.1 において、vSphere Distributed Switch に ESXi ホストを追加しようとする時、「ホスト IP アドレスは、vSphere Distributed Switch 機能のライセンスが適用されていません。このホストは dvSwitch に追加できません」というライセンス エラーが発生し、追加できません。詳細については、 [VMware ナレッジベースの記事 KB2143397](#) を参照してください。NSX 6.2.2 で、この問題は修正されました。
- **解決した問題 1590563**：アップグレード後の Enterprise ライセンス エラー

NSX 6.2.1 のアップグレードでは、Enterprise ライセンスを所有していなくても 6.2.1 にアップグレードできますが、アップグレード後、NSX を使用するには Enterprise ライセンスが必要です。NSX 6.2.2 で、この問題は修正されました。 [VMware ナレッジベースの記事 KB2135310](#) を参照してください。
- **解決した問題 1589046**：DHCP リレーが有効でない LIF（論理インターフェイス）に送信されたパケットによって PSOD（パープル スクリーン）が発生する

DHCP ユニキャスト パケットの送信先に、DHCP リレーが有効な LIF の IP アドレスが指定されているが、実際の LIF で DHCP リレーが有効でない場合、ESXi ホストで PSOD（パープル スクリーン）が発生します。NSX 6.2.2 で、この問題は修正されました。 [VMware ナレッジベースの記事 KB2144314](#) を参照してください。

- 解決した問題 1593436：VXLAN のハイブリッド モードでコントローラが切断されたときに、マルチキャスト モードへのフォールバックが誤って開始される
 NSX 6.2.2 で、この問題は修正されました。 [VMware ナレッジベースの記事 KB2144457](#) を参照してください。
- 解決した問題 1574995：分散ファイアウォール (DFW) の発行エラー
 フィルタ処理されたモードで分散ファイアウォール ルールを変更して保存すると、ルールが保存および発行されないことがあります。NSX 6.2.2 で、この問題は修正されました。 [VMware ナレッジベースの記事 KB2141155](#) を参照してください。
- 解決した問題 1422110：NSX Controller のいずれかが、シャットダウン時に他のコントローラにマスター ロールを渡さない
 NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1483728：NSX Controller の制御プレーン接続が失敗する
 コントローラの制御プレーン接続が失敗し、txInProgress に関する netcpa にエラーが表示されます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1487910：Edge Services Gateway のアップグレードに失敗し、「Edge 仮想マシンの待機中にタイムアウトが発生しました」という内容のメッセージが表示される
 NSX 管理インターフェイスに IPv6 アドレスを適用すると、NSX Manager はホスト名を使用ようになります。しかし、Edge 仮想マシンを NSX Manager に接続する vsfwd プロキシは FQDN を適切に処理できないため、「ERROR TaskFrameworkExecutor-6 AbstractEdgeApplianceManager:185 - Edge 仮想マシン {} の待機中にタイムアウトが発生しました。仮想マシンはブートおよび応答できませんでした。com.vmware.vshield.edge.exception.VshieldEdgeException」という内容のエラーが返されます。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1571548：NSX for vSphere リリース 6.2.0 以降で、ホストまたは vCenter Server で VTEP の IP アドレスが直接変更された場合、VTEP の以前の IP アドレスが自動的に解放される
 NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1551164：NSX ユーザー インターフェイス (UI) が数秒間グレイアウトされ、NSX for vSphere 6.2.0 のパフォーマンスが低下していることが示される
[VMware ナレッジベースの記事 KB2141919](#) を参照してください。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1545840：VMware NSX for vSphere 6.x のホストで NSX 分散ファイアウォール (DFW) を無効にできない
[VMware ナレッジベースの記事 KB2141915](#) を参照してください。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1528680：VMware NSX for vSphere 6.2.0 で IP アドレス検出を使用すると、VMware ESXi 5.x および 6.x でパープル スクリーンが表示される (KB 2134329)
 VMware NSX for vSphere 6.2.0 の論理スイッチで IP アドレス検出を使用すると、ESXi 5.x および 6.x ホストで障害が発生し、パープル スクリーンが表示されます ([ナレッジベースの記事 KB2134329](#) で解説)。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1545885：セキュリティ タグ ポートレットの [管理] オプションがデフォルトでグレイアウトされ、選択できない
 仮想マシンのサマリ ページにあるセキュリティ タグ ポートレットの [管理] ハイパーリンクは、ユーザーが新しいセキュリティ タグを作成するまでグレイアウトされ、選択できません。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1476087：一部のコントローラ ログが、Syslog エクスポートに含まれない
 Zookeeper クラスタリング ログを含むコントローラ ログは、Syslog のエクスポートに含まれません。NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1545830：利用可能な MTU のサイズよりも大きなデータ サイズで ping すると、ESXi 6.0 の vdl2 で PSOD（パープル スクリーン）が発生する
NSX ホスト スイッチが接続された vmknics から ping を開始すると、データ サイズが MTU よりも大きい場合に、ホストで PSOD（パープル スクリーン）が表示されます。NSX 6.2.1 では、この問題は解決されています。
- 解決した問題 1545873：ユーザーは、TCP と UDP 双方のプロトコルに同じ IP アドレスとポート番号を設定する必要がある
このリリースでは、次の問題も解決されています。
 - プールが設定されていない UDP 仮想サーバの設定に失敗する
 - UDP 仮想サーバにプールが関連付けられていない場合、統計に誤ったデータが表示される

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

NSX 6.2.3 以前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 1578509：ESX Agent Manager (EAM) の再起動後、ゲスト イントロスペクション (GI) のサービス ステータスが「警告」状態になる
この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1539203：NSX のアップグレード後、Cross-vCenter 環境のアップグレード中に NSX プラグインがプライマリ vCenter Server から切断される
この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1558017：NSX Edge を 6.1.x から 6.2.x にアップデートすると、NSX Manager の vsm.log に「INVALID DHCP CONFIG」と表示される
インターフェイスに IPv6 サブネットを設定している場合、DHCP は空の共有サブネットを生成し、これを無効な操作として処理します。
- 解決した問題 1490496：NSX のアップデート後、ゲスト イントロスペクション が NSX Manager と通信できなくなる
NSX 6.0.x から NSX 6.1.x、または NSX 6.0.x から NSX 6.2 へのアップデートを行った後、ゲスト イントロスペクション サービスをアップデートするまで、NSX Manager は、ゲスト イントロスペクション のユニバーサル サービス仮想マシン (USVM) との通信ができなくなります。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1536179：Mac OS X Yosemite 以降に SSL VPN-Plus Client をインストールできない
Mac OS X は、Yosemite より前のバージョンのみがサポートされます。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1393503：NSX for vSphere を 6.0.7 から 6.1.3 にアップデートした後、vSphere Web Client がログイン画面でクラッシュする
NSX Manager を 6.0.7 から 6.1.3 にアップデートした後に、vSphere Web Client ユーザー インターフェイスのログイン画面に例外が表示されます。ユーザーは、vCenter Server または NSX Manager でログインと操作ができなくなります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1088497：ゲスト イントロスペクションのインストールがエラーで失敗する
クラスターでゲスト イントロスペクションをインストールする場合、インストールが次のエラーで失敗します。
VIB モジュールの無効なフォーマット NSX 6.2.0 で、この問題は修正されました。

- 解決した問題 1328589：ホストの準備の問題により、DVPort に「Would block」というエラーメッセージが出力され、有効化に失敗する
 NSX が有効な ESXi ホストで、ホストの準備の問題により「Would block」というエラーメッセージが出力され、DVPort の有効化に失敗します。この問題が発生した際に、最初に通知されるエラーメッセージはさまざまです。たとえば、VC/hostd.log では VTEP 作成失敗、vmkernel.log では DVPort 接続失敗、ゲストでは「SIOCSIFFLAGS」エラーと見なされる場合があります。この問題は、vSphere Distributed Switch (vDS) のプロパティが vCenter Server によってプッシュされた後に VIB がロードされると発生します。これはアップグレード中に発生する場合があります。[ナレッジベースの記事 KB2107951](#) を参照してください。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1446544：NSX 6.1.4 にアップデートされた環境で、既存の NSX Edge Gateway の削除に失敗する
 NSX インストール環境を 6.1.3 から 6.1.4 にアップデートすると、6.1.4 へのアップデート後に既存の NSX Edge Gateway を削除することができません。この問題は、アップデート後に作成された新しい Edge Gateway には影響しません。6.1.2 以前から直接アップデートされたインストール環境では、この問題の影響はありません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1418836：サードパーティのセキュアな FTP バックアップを使用して NSX バックアップを実行すると、AES 暗号化が使用できない NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1410153：ホストの再起動中、NSX Manager のユーザー インターフェイスでユーザーが理解できるエラーメッセージが表示されない
 この 6.2 のリリースでは、NSX Manager のユーザー インターフェイスは詳細なエラーメッセージを表示するよう更新されました。メッセージは、ホストの再起動中に発生する可能性のある問題を説明し、可能なソリューションを提供します。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1412133：NSX VIB をインストールすることができない
 サードパーティのモジュールから ixgbe ドライバのロードに失敗した場合、NSX VIB のインストールが予期したとおりに完了しないことがあります。これは、ドライバがロックされ、インストールに使用されないためです。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1467438：vCloud Networking and Security (vCNS) 5.5.3 からアップグレードすると、NSX Manager サービスを開始することができない
 vCloud Networking and Security (vCNS) 5.5.3 から NSX 6.1.3 にアップグレードすると、NSX Manager サービスがハングし、開始に失敗します。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1440867：NSX Edge の再起動後、メッセージ バスが開始されないことがある
 Edge 仮想マシンの再起動後、パワーオンしてもメッセージ バスが開始されない場合があります、追加で再起動が必要になります。NSX 6.2.0 で、この問題は修正されました。

NSX 6.2.3 以前で解決した NSX Manager に関する問題

- 解決した問題 1540187：ユーザー/グループに権限がないというエラーによって、ユーザーが vSphere Web Client にログインして NSX プラグインを使用できない
 この問題は、SAML トークンの生成中に発生したタイムアウトによるものです。SSO サービスと通信するときに、リクエスト処理が完了しないと、NSX はソリューション登録プロバイダを内部で更新できません。一度この状態になると、ほかのすべてのリクエストで Null ポインタ例外が発生します。
 この問題は NSX 6.2.3 で解決されました。Null ポインタ例外が発生しなくなり、必要に応じて SSO サービスに再接続できるようになりました。
- 解決した問題 1640388：仮想マシンを含まないクラスタからゲスト イントロスペクションをアンインストールするとき、「アンインストール前のクリーンアップに失敗しました」というエラーメッセージが表示され、ステータスが未解決として表示される
 これはゲスト イントロスペクションのアンインストール ロジックの既知の問題です。
 この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1534588：NSX Manager のユーザー インターフェイスで以前のバックアップが表示されない

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

この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1593910：NSX Manager の IP アドレスの重複が検出または回避されない

ネットワーク上の別のデバイスに NSX Manager の IP アドレスが割り当てられていても、明示的なエラーまたはイベント ログが生成されません。このため、NSX Controller およびホストが誤った MAC アドレスを使用して NSX Manager に応答する場合があります、これが原因でデータ パスに障害が発生します。回避策：重複した IP アドレスを持つネットワーク デバイスを特定して削除するか、そのデバイスに別の IP アドレスを割り当てます。ネットワーク上で NSX Manager の IP アドレスが重複している場合、ホストとコントローラは誤った MAC アドレスを使用して NSX Manager/仮想マシンに応答します。これは、NSX Manager と ESX 間、および NSX Manager と NSX Controller 間の通信に影響します。これが原因で、データパス障害が発生する可能性があります。この場合、重複する IP アドレスがネットワークから削除され、通信チャネルが復旧するまで、アプリケーションに影響を及ぼします。

この問題は NSX 6.2.3 で解決されました。IP アドレスの重複を検出すると、システム イベントが追加されます。
- 解決した問題 1489648：休止スナップショットを使用して NSX Manager のバックアップを作成した後、vSphere Web Client プラグインから NSX を使用できない

[VMware ナレッジベースの記事 KB2142263](#) を参照してください。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1440451：NSX Manager の証明書を置き換えた場合、NSX Manager の再起動が必要であり、場合によっては vSphere Web Client の再起動も必要になる

NSX Manager アプライアンスの証明書を置き換えた後は、常に NSX Manager アプライアンスを再起動する必要があります。状況によっては、証明書を置き換えた後、vSphere Web Client に [Networking and Security] タブが表示されないことがあります。
- 解決した問題 1568861：Firefox ブラウザの GUI 言語が日本語の場合、セカンダリ NSX Manager を追加できない

日本語、ドイツ語、韓国語、フランス語の Firefox ブラウザでセカンダリ NSX Manager を追加すると、サムプリントのダイアログが表示されず、設定がブロックされます。
- 解決した問題 1482989/1522092：NSX の [Networking and Security] タブですべてのホストのステータスが緑（正常）で表示されているにもかかわらず、クラスタのステータスが誤って赤（エラー）で表示される

NSX 6.1.4 以前では、NSX の [Networking and Security] タブですべてのホストのステータスが緑（正常）で表示されているにもかかわらず、クラスタのステータスが、エラーが発生していることを示す赤で誤って表示されることがありました。この問題は、NSX 6.1.5 で解決されました。
- 解決した問題 1515656：Active Directory ドメインに追加した後、NSX Manager の CPU 使用率が高くなる

Active Directory ドメインに追加した後、NSX Manager の CPU 使用率が高くなります。NSX Manager のシステム ログでは、複数の Postgres スレッドが実行中として表示されます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1484939：vCenter Server で NSX Manager 6.1.4 を登録できず、「NSX 管理サービスの操作に失敗した」というエラーが表示される

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

- 解決した問題 1521710 : NSX Manager の Web Client で、エラー「コード 301002」が表示される
説明 : [NSX Manager] > [監視] > [システム イベント] の順に選択すると、次のエラーが表示されま
す。Filter config not applied to vnic.コード 301002。NSX 6.1.5 および NSX 6.2.1 で、この問
題は修正されました。
- 解決した問題 1479665 : 6.2.1 より、NSX Manager はクラスタ内の各コントローラ ノードでクエリ
を実行して、当該コントローラとクラスタ内の他のコントローラ間の接続情報を入手する
これは、NSX REST API (「GET https://[NSX-MANAGER-IP-ADDRESS]/api/2.0/vdn/controller」 コマンド) の出力
として提供され、コントローラ ノード間のピア接続ステータスを表示します。NSX Manager が、任意の 2
台のコントローラ ノード間の接続が切断されていることを認識すると、システム イベントが生成され、
ユーザーに警告します。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1525516 : NSX Manager のバックアップ-リストアが別のアプライアンスで実施され
た場合、コントローラの強制同期が停止する
NSX Manager がバックアップからリストアされるか、バックアップからクローン作成された場合、NSX
Controller クラスタへの強制同期が失敗します。この問題は、新規にデプロイされた NSX Manager では発生
しません。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1509454 : NSX 環境に含まれないホストに対する、NSX のハートビートのログ作成
が失敗する
NSX 準備済みホストを、NSX で準備解除せずに直接 vCenter Server のインベントリから削除すると、NSX
は予期しない「ホスト接続」DCN を受け取り、ホストからメッセージング インフラストラクチャ コン
ポーネントが部分的に削除されます。結果として、削除されるはずの NSX/ホスト間のメッセージング リ
ンクがアクティブのままになり、NSX はホストに関して誤った「アラート」システム イベントを通知する
可能性があります。NSX 6.2.1 で、この問題は修正されました。NSX 6.2.1 で、この問題は修正されまし
た。
- 解決した問題 1418655 : NSX Manager が、**write erase** コマンドの実行後、機能しなくなる
write erase コマンドの実行後に NSX Manager を再起動すると、Linux シェルにアクセスするためのパス
ワードがリセットされる、セットアップ コマンドがないなど、NSX Manager が正しく動作しないことがあ
ります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1366669 : [ドメインの追加] で、LDAP オプションに **[ドメイン認証情報を使用]** エラー
が表示される
NSX 6.1.x では、LDAP ドメインにユーザーを追加する場合、ユーザー名がユーザー インターフェイスに提
供されていても、Web Client が「ユーザー名が指定されていませんでした」というエラーを表示しました。NSX
6.2.0 で、この問題は修正されました。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1352169 : CA 署名付き証明書のインポート後、NSX Manager を再起動しないと証明
書が有効にならない
CA によって署名された NSX Manager 証明書をインポートするとき、NSX Manager を再起動するまで新たに
インポートされた証明書が有効になりません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1497113 : NSX Manager を LDAPS ドメインにインポートできない
NSX Manager を LDAPS ドメインにインポートしようとする、次のエラー メッセージが表示されます。
ホスト <サーバ FQDN> に接続できません
エラー メッセージ: シンプル バインドに失敗しました:<サーバ FQDN:番号> NSX 6.2.0 で、この問題は修正されまし
た。

NSX 6.2.3 以前で解決した論理ネットワークと NSX Edge ルーティングに関する問題

- 解決した問題 : NSX Controller が切断された場合の VNI のデータ パスの問題
この問題は、IPSec の別の既知の問題を回避するために、NSX-V 6.1.5、6.1.6、6.2、6.2.1 および 6.2.2 リ
リースで IPSec のキーの再設定を無効にしている場合に発生します。

VMware ナレッジベースの記事 [KB2146973](#) を参照してください。この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1591582：一部の限られた状況において、分散論理ルーター インスタンスによって送信される ARP 要求がドロップされることがある
他のホスト上のリモート仮想マシンの VDR ARP 要求が、VDR アップリンク出力処理でドロップされ、接続の確立に時間がかかることがあります。
- 解決した問題 1501900：OSPF インターフェイスの IP アドレスを変更すると、Edge OSPF ルーターが ExchangeStart の状態のまま変わらなくなる
競合状態のため OSPF インターフェイスで IP アドレスを変更すると、OSPF ネイバーの状態が両側とも ExchangeStart のままになります。通常、OSPF インターフェイスの IP アドレスの変更はサポートされる操作です。
この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1498251：IS-IS ルーティング プロトコルは、Edge Services Gateway ルーターでサポートされない

NSX 6.2.3 では、ユーザー インターフェイスと API から IS-IS ルーティング プロトコルに関する記述が削除されました。
- 解決した問題 1492738：分散論理ルーター (DLR) の展開で、vSphere Web Client を使用して 8 個を超えるアップリンク インターフェイスを追加できない
この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1552038：NSX Edge から分散論理ルーター (DLR) のアップリンク インターフェイスへの接続が断続的に切断される
この問題は、NSX Edge が ARP テーブルに記録しているのが分散論理ルーターのローカル インスタンスの MAC アドレスではなく 分散論理ルーター制御仮想マシンの MAC アドレスである場合に発生します。このリリースでは、分散論理ルーターの IP アドレスに関する ARP リクエストを 分散論理ルーター制御仮想マシンが生成することを防ぐ、ARP の送信フィルタが追加されました。
- 解決した問題 1454161：/31 の IP アドレスをネクスト ホップとするスタティック ルートを設定できない
この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1528443：フェイルオーバー中に Edge 仮想マシンが GARP を送信すると、ホストの VXLAN ARP キャッシュが更新されない
仮想マシンと Edge が同一の VXLAN セグメント上に存在する環境では、Edge のフェイルオーバー後にホストの VXLAN ARP キャッシュが更新されない場合があります。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1600874：新しい Edge 仮想マシンがデプロイされると、標準的な仮想マシンが削除されない
Edge をアップグレードする際、発行とロール バックの両方の操作が失敗すると、元の Edge 仮想マシンは NSX Manager データベースに残りますが、vCenter Server は新しい Edge 仮想マシンの ID 番号を保持します。この不一致によって、Edge 仮想マシンの再デプロイが失敗します。強制同期も「仮想マシンが見つかりません」というエラーと共に失敗します。
- 解決した問題 1467774：show ip bgp neighbor コマンドのアドミニストレーティブ ディスタンスのフィールドに誤った値が表示される
EBGP ピアから学習し、同じ AS の IBGP ピアにアドバタイズされたルートが、以前のアドミニストレーティブ ディスタンスを誤って保持します。NSX 6.2.3 で、この問題は修正されました。

- 解決した問題 1613383 : L4 モードで実行される NSX Edge ロード バランサの現在の接続数に、合計接続数が誤って使用される

このリリースでは問題が修正され、アクティブな接続数の合計を使用して、現在の接続数を計算するように修正されました。NSX 6.2.3 で、この問題は修正されました。
- 解決した問題 1584664 : 最初に NSX で設定を解除せずに、vCenter Server インベントリからロード バランサ プールの仮想マシン メンバーを手動で削除した場合、NSX Manager データベースに実態のないエントリが残される。 NSX Manager ログに ObjectNotFoundException がレポートされる

NSX 6.2.3 で、この問題は修正されました。
- 解決した問題 1446809 : Edge の再起動後に健全性チェックのリカバリー イベントが送信されない場合、vCloud Director が NSX Edge を管理できなくなる

NSX Manager では、Edge の接続ステータスがメモリに保存されます。Edge 仮想マシンが健全性チェックへの応答に失敗すると、「ミス イベント」が発生し、リカバリが行われると「リカバリー イベント」が発生します。NSX Manager の再起動後に、健全性チェックに応答しない仮想マシンがなければ、「リカバリー イベント」が送信されないことがあります。vCloud Director はこれらのイベントに依存するため、リカバリー イベントが送信されない場合は、vCloud Director から Edge 仮想マシンを管理できなくなることがあります。
- 解決した問題 1441319 : 動的ルーティング環境で論理インターフェイス (LIF) を削除した後、接続が失われる

この問題は、NSX 分散論理ルーター (Edge および 分散論理ルーター) で発生していました。動的ルーティング (OSPF および BGP) を使用すると、LIF を削除した後にネットワーク接続が失われます。この問題は、NSX バージョン 6.0.x から 6.1.4 で発生します。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1445291 : NSX Edge で RADIUS 認証サーバの設定に失敗する

NSX 6.1.5 以前は、RADIUS サーバの秘密鍵には 32 文字の制限があり、文字列がこの上限を超えると、RADIUS サーバは NSX Edge との接続に失敗していました。現在は最大 64 文字です。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1534811 : VIO Heat スタックのデプロイが、次のようなエラーによって VMware NSX for vSphere 6.x Edge で断続的に失敗する : 「メモリを割り当てることができません」

健全性監視のメモリ使用量は時間とともに増加し、最終的には Edge で障害が発生します。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1500624 : BGP フィルタの適用が有効になるまでおよそ 40 秒かかる。

この間、すべての再分配ポリシーはフィルタなしで適用されます。この遅延は、送信方向の NSX 分散論理ルーター (DLR) にのみ発生します。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1484758 : NSX Edge のサブインターフェイスで [ICMP リダイレクトの送信] オプションを無効にしても、ICMP リダイレクトが送信される

NSX Edge のサブインターフェイスでは、デフォルトで [ICMP リダイレクトの送信] が無効になっています。このオプションが無効になっていても、Edge のサブインターフェイスで ICMP リダイレクトが送信されます。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1265605 : 分散論理ルーターのブリッジまたはテナント名に非 ASCII 文字を追加できない

NSX Controller API は非 ASCII 文字に対応していません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1341784 : BGP ネイバー フィルタ ルールが変更されると、既存のフィルタが最大 40 秒間適用されない可能性がある

BGP フィルタが IBGP を実行している NSX Edge に適用されると、IBGP セッションでフィルタが適用されるまで最大 40 秒かかる可能性があります。この時間に、NSX Edge が IBGP ピアの BGP フィルタで拒否されているルートを通知することがあります。NSX 6.2.0 で、この問題は修正されました。

- 解決した問題 1422110：NSX Controller のいずれかが、シャットダウン時に他のコントローラにマスター ロールを渡さない
 通常は、マスター ロールを操作するコントローラがシャットダウンの準備をするときに、他のコントローラにマスター ロールを自動的に渡します。この場合、コントローラがロールを他のコントローラに渡すことに失敗し、ステータスは中断になり、切断モードに移行します。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1440790：ホスト間の VXLAN トラフィックをユニキャストまたはマルチキャストで渡すことができない
 複数の仮想マシンが同じホスト上にある場合、ユニキャストやマルチキャストで VXLAN から通信することができます。しかし、仮想マシンが違うホスト上にある場合は、通信できません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1432420：NSX Edge や分散論理ルーター (DLR) で同時に複数の BGP ルールを削除すると Web Client のクラッシュが起こる NSX 6.2.0 で、この問題は修正されました。一度に複数の BGP ルールを削除することが可能になりました。
- 解決した問題 1431716：Border Gateway Protocol (BGP) 拒否ルールの追加後、プロトコル アドレスが一時的に表示される
 NSX Edge Services Gateway に Border Gateway Protocol (BGP) 拒否ルールを追加した後、プロトコル アドレスが一時的に表示されることがあります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1441773：vMotion の間、仮想マシンの接続が切断される
 vMotion の実行中に仮想マシンの接続が切断されたり、NIC が切断された仮想マシンに関するアラートを受け取ったりすることがあります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1463579：コントローラのスナップショットをダウンロードできない
 コントローラのスナップショットをダウンロードする場合、最後のコントローラのスナップショットをダウンロードできないことがあります。たとえば、コントローラが 3 つあった場合、最初の 2 つのコントローラに関してはスナップショットのダウンロードに成功しますが、3 つ目のコントローラのスナップショットがダウンロードできないことがあります。NSX 6.2.0 で、この問題は修正されました。

NSX 6.2.3 以前で解決した Edge サービスに関連する問題

- 解決した問題 1633694：ストレージの障害によって、NSX Manager データベースの VXLAN 設定が失われることがある
 ストレージで障害が発生すると、分散仮想スイッチ (DVS) が削除されたと vCenter Server がレポートし、NSX Manager がその DVS に関連付けられた VXLAN 設定を削除する場合があります。この状態になると、`[INFO DCNPool-9 VcDriver:1077 - Deleting vmknics info from host tables [host-21843 : 319]]` のようなメッセージが NSX Manager のログに出力されます。
 この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1456172：NSX Edge ファイアウォールが無効の場合、NAT が IP アドレスを変換しない
 Edge デバイスが 6.0 の X-Large サイズまたは 6.1 および 6.2 の場合、NSX Edge ファイアウォールが無効になっていると、すべてのステートフル サービスも無効になります。NSX 6.2.3 では、ほかのステートフル サービスも無効になっていることを示す警告がユーザー インターフェイスに追加されました。
- 解決した問題 1499601：スタティック ルートのみを使用する場合、Edge Services Gateway (ESG) または分散論理ルーター (DLR) の Edge 仮想マシンの高可用性フェイルオーバー時間が長くなる
 この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1618289：VMware NSX for vSphere 6.2.x で、Edge 高可用性 (HA) フェイルオーバー中の TCP セッションで予期しない TCP の中断が発生する
 この問題は、VMware NSX for vSphere 6.2.x で使用される古い内部ライブラリが原因で発生していました。この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1653484 : NSX Edge のコア ダンプが関数名を表示しない
NSX 6.2.3 ではコア ファイルにメモリのアドレス情報が表示されることで、デバッグ機能を強化しています。ただし、コア ダンプは、VMware のテクニカル サポートから要求されたときにのみ有効にする必要があります。

この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1604506 : スタティック ルーティングでデフォルト ゲートウェイを使用する場合、Edge 仮想マシンを含まない 分散論理ルーター (DLR) をデプロイできない

設定時に [デフォルト ゲートウェイの設定] オプションを選択して、Web Client から新しい分散論理ルーター (DLR) をデプロイすると、DLR の作成に失敗し、ポップアップ ウィンドウに次のエラーが表示されます。[Routing] 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ています。

詳細については、[VMware ナレッジベースの記事 KB2144551](#) を参照してください。この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1445057 : NSX Edge Services Gateway (ESG) に設定した OSPF ルートが分散論理ルーター (DLR) で受け入れられず、影響するパケットがドロップされる

この問題は、OSPF で IP_HDRINCL オプションを使用している場合に発生します。特定の Linux カーネルでは、このオプションが存在する場合、IP スタックでのパケットのフラグメント化が防止されます。このため、インターフェイスの MTU を上回るパケットはドロップされます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

解決した問題 1406471 : バックアップ元の NSX Manager のホスト名が、リストア先 NSX Manager の Syslog に表示される

1 番目の NSX Manager のホスト名が A で、この NSX Manager のバックアップを作成したとします。2 番目の NSX Manager は、バックアップおよびリストアのドキュメントに従って、1 番目の NSX Manager と同じ IP アドレスを使用してインストールおよび設定されていますが、ホスト名は B となっています。リストアされた NSX Manager では、リストア直後はホスト名が A と表示され、再起動後に正しいホスト名 B と表示されます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1444581 : ESXi ホストのネットワーク接続が失われることがある

ESXi ホストのネットワーク接続が失われ、安定性に問題が生じることがあり、次のような複数のエラーメッセージがログに記録されます。

WARNING: Heartbeat: 785: PCPU 63 didn't have a heartbeat for 7 seconds; *may* be locked up. NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1444784 : vMotion の間、仮想マシンの接続が切断される

6.0.8 では vMotion の間、仮想マシンの接続が切断され、「VISP ヒープが枯渇しました」というメッセージが表示されます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1462506 : CA 署名済み証明書を設定した L2 VPN サービスを利用する場合、NSX Edge を再デプロイできない

CA 署名済み証明書または自己署名済み証明書を設定した L2 VPN サービスでは、NSX Edge の再デプロイやサイズ変更を行うことができません。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1440867 : NSX Edge の再起動後、メッセージ バスが開始されないことがある
Edge 仮想マシンの再起動後、パワーオンしてもメッセージ バスが開始されない場合があり、追加で再起動が必要になります。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1548939：仮想サーバの設定時に、以前に選択した IP アドレスが適用される
 新しい仮想サーバを作成する際に、以前に選択した IP アドレス プールのリストから自動的に IP アドレスが適用される場合があります。これは、以前に IP アドレス プールを選択して仮想サーバの IP アドレスを獲得した場合に発生します。仮想サーバの IP アドレス プール情報を編集しようとする、ユーザー インターフェイスからバックエンドに情報が自動送信されず、IP アドレスプールから獲得した以前の IP アドレスが自動的に適用されます。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1599706：2 つの VNI 間の分散論理ルーターによる通信で SYN/ACK パケットが失われる
 NSX 6.2.2 で、この問題は修正されました。
- 解決した問題 1082549：Edge Services Gateway で HA が有効となっており、OSPF hello/dead 間隔がそれぞれ 30 秒または 120 秒以外の値に設定されていると、フェイルオーバー中にトラフィックが失われる場合がある
 OSPF を実行し、HA が有効な状態でプライマリ NSX Edge に障害が発生すると、引き継ぎ待機に必要な時間がグレースフル リスタートのタイムアウトを超過し、OSPF ネイバーで転送情報ベース (FIB) テーブルから学習済みのルートが削除されます。その結果、OSPF が再収束するまで、データプレーンは停止したままになります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1403594：仮想マシンが Edge DHCP サーバから ping を受信することができない
 仮想マシンが Edge Gateway に ping を送信することはできますが、オーバーレイ ネットワークで Edge Gateway トランクの DHCP の ping を受信できません。Edge DHCP サーバは、トランク ポートとしてセットアップされ、すべてのトラフィックの送受信に失敗します。ただし、Edge Gateway および DHCP Edge が同じホストにある場合、お互いに ping の送受信が可能です。DHCP Edge を別のホストに移動すると、DHCP Edge は Edge Gateway から ping の受信ができなくなります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1477176：Edge ロード バランサの統計情報が vSphere Web Client に正しく表示されない
 Edge ロード バランサで、vSphere Web Client ユーザー インターフェイスのチャートに同時接続統計の値が表示されません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1399863：o IPsec VPN チャンネルのローカルおよびリモート サブネットにある直接集約ネットワークを削除すると、ピア Edge の間接的なサブネットへの集約ルートが表示されない
 Edge にデフォルトのゲートウェイがなく、IPsec を設定しているときに、ローカルサブネットおよびリモート サブネットの一部にあるすべての直接接続のサブネットを削除すると、残ったピアのサブネットに IPsec VPN でアクセスできなくなります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1484743：NSX 6.1.2 以降にアップグレードした後、ロード バランサにトラフィックを渡すことができない
 NSX Edge ロード バランサで [X-Forwarded-For の挿入] オプションを使用すると、トラフィックがロード バランサを通過しない場合があります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1449461：clear ip ospf neighbor command コマンドを実行すると、セグメント障害エラーを返す
 NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1418264：Kerberos の要求を処理することができない
 特定の Kerberos の要求が、NSX Edge での分散処理中に失敗します。NSX 6.2.0 で、この問題は修正されました。

NSX 6.2.3 以前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 1620109：サードパーティ サービス仮想マシンのデプロイが、正常に完了せず、インストールの状態が「失敗」とレポートされることがある
たとえば、サービス仮想マシンが IP アドレスを受信しないことがあります。NSX Manager のログには、「パラメータ property.info.key に与えられた値が正しくありませんでした」というエラー メッセージが表示されます。

[VMware ナレッジベースの記事 KB2145376](#) を参照してください。この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1619570：膨大な数のルールおよび Service Composer を使用する大規模な分散ファイアウォール設定では、再起動後ルール発行までに数秒かかることがあるが、その間は新しいルールを発行できない
NSX 6.2.3 では、再起動のために最新版が適用されていないファイアウォール ポリシーのみを再同期することによって、再起動時にファイアウォール ルールの同期にかかる時間が短縮されました。
- 解決した問題 1526781：NSX 6.2.x で、getFirewallConfigLayer3SectionByName API のクエリが responseHeaders フィールドを返さない
この問題は 6.2.3 で修正され、API 出力に ETag ヘッダー情報が含まれるようになりました。
- 解決した問題 1599576：ユニバーサル セクションのファイアウォール ルールを編集して発行しようとする、グローバル セクションの ID フィールドの値が null に設定されているため、失敗する場合がある。
エラー メッセージは表示されません。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1558501：ユニバーサル サービス仮想マシン (USVM) から NSX Manager への接続が失敗すると、ゲスト イントロスペクションのインストールが失敗することがある
NSX Manager に FQDN のみが設定されている場合、NSX Manager とゲスト イントロスペクション サービス仮想マシン間のメッセージング チャネルで障害が発生することがあります。この問題が発生すると、ゲスト イントロスペクション サービスのステータスが「警告」のままになります。ユニバーサル サービス仮想マシン (USVM) の eventmanager.log ファイルには、「UnknownHostException」メッセージが表示されません。NSX 6.2.3 では自動 DNS サポートが追加され、この問題は修正されました。
- 解決した問題 1673068：Service Composer ポリシー セクション内でファイアウォール ルールを編集すると、設定が同期されなくなる
ファイアウォール構成画面の Service Composer ポリシー セクションで、ファイアウォール ルールが追加または編集されると、Service Composer が同期されなくなります。NSX 6.2.3 では、Service Composer のファイアウォール構成セクションが読み取り専用に変更され、この問題は修正されました。Service Composer で作成されたルールは、Service Composer で管理する必要があります。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1639612：NSX for vSphere 6.2.x では、Windows 2008 以降を使用すると MSRPC 接続の問題が発生する
64 ビットのアドレスをサポートする新しい Windows では、DCE/EPM プロトコルが転送エンコーディング形式として NDR64 のネゴシエーションを行います。このため、ファイアウォールが EPM 応答パケットを解析せず、動的ポートが開いていることを検知できません。[VMware ナレッジベースの記事 KB2145135](#) を参照してください。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1567693：NetX ルールで送信元/宛先として IPset を使用すると、[無効なコンテナタイプ：IPSet] というエラーが表示される
この問題は NSX 6.2.3 で修正されました。

- 解決した問題 1407920：REST API 呼び出しを使用してファイアウォール構成を削除する場合、保存した設定をロードして発行することができない

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

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

この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1498504：重複する 2 つのサービス グループの 1 つから仮想マシンを削除すると、その仮想マシンのファイアウォール保護が失われる

Service Composer のワークフローにより作成された別のサービスが同じ仮想マシンに適用されると、ファイアウォール ワークフローによって作成された NetX フィルタがホストから削除されます。この問題は、たとえば、重複する 2 つのサービス グループに 1 つのサービス プロファイルが適用されたときに発生します。この場合、両方のサービス グループに存在している仮想マシンが片方のサービス グループから削除されると、その仮想マシンの保護が失われます。この問題は NSX 6.2.3 で解決されました。サービス プロファイルに「優先順位」のフィールドが追加されます。ホストで vNIC のサービス グループが重複している場合、優先順位が最も高いサービス プロファイルが適用されます。
- 解決した問題 1550370：アップストリーム データパスで 15 分以上の停止が発生すると、NFSv3 マウントを行っている Linux 仮想マシンでオペレーティング システムがハングする

[VMware ナレッジベースの記事 KB2133815](#) を参照してください。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1494366：送信元/宛先の無効化オプションが有効になっているファイアウォール ルールをコピー アンド ペーストすると、コピーしたルールでは無効オプションが無効になる

送信元/宛先の否定オプションを有効にしてファイアウォール ルールをコピーすると、このオプションが無効な状態で新しいファイアウォールが作成されます。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1473767：フロー モニタリングでは、5 分間で 200 万フローの制限を超えるとフローがドロップされる

NSX フロー モニタリングは最大 200 万件のフロー レコードを保持します。ホストが 5 分間に 200 万件を超えるレコードを生成すると、新しいフローはドロップされます。この問題は NSX 6.2.3 で修正されました。

[VMware ナレッジベースの記事 KB2091376](#) を参照してください。
- 解決した問題 1611238：6.2.x Edge ファイアウォールでは、Edge スコープで作成された Security Group（Edge スコープの Security Group は REST からのみ作成可能）のみが表示される

6.2.3 では、グローバル スコープで作成された Security Group（ユーザー インターフェイスで作成可能）、および対応する Edge用に Edge スコープで作成された Security Group（REST のみで作成可能）は、「送信元/宛先」カラムの下に Security Group リストの「Edge ファイアウォール」に表示されます。

この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1516460：ファイアウォール ルールで、「論理スイッチに適用」が削除された後も、引き続きこのルールが有効とマークされる

この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1542157：セキュリティ保護された仮想マシンを vMotion で移行先のホストに移行すると、分散ファイアウォール機能が失われる

NSX が有効なホストを vCenter Server インベントリから削除すると、内部ファイアウォール テーブルからホストのエントリが削除されます。その後にホストを vCenter Server インベントリに戻しても、ファイアウォール テーブルのエントリは再作成されません。この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1592439：Service Composer が、仮想マシンの Security Group への変換に失敗する

この問題は、ユニバーサル サービス仮想マシン (USVM) での EpSecLib のデッドロックが原因で発生します。この問題は NSX 6.2.3 で解決されました。

- 解決した問題 1534597：NSX for vSphere 6.x Controller が断続的に切断される
 6.1.4 以前のリリースで出荷されていた StrongSWAN パッケージ内の IPSEC バグにより、IPSEC の再キー化後に、コントローラ間のトンネルが確立されませんでした。このためコントローラ間で部分的な接続障害が発生し、さまざまな問題が生じていました。詳細については、[ナレッジベースの記事 KB2127655](#) を参照してください。NSX 6.1.5 および 6.2.1 で、この問題は修正されました。
- 解決した問題 1491042：Security Group のオブジェクト選択画面で、LDAP ドメイン オブジェクトの応答に時間がかかるか、応答がないNSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1468169：ファイアウォール ルールの表示中にマウスの動きが遅れる
 vSphere Web Client の [Networking and Security] セクションで、ファイアウォール ルールの行の上でマウスを動かすと、マウスの表示が 3 秒遅れます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1476642：NSX-v における一部の IP SpoofGuard ルールが正しく適用されません。
 NSX-v における一部の IP SpoofGuard ルールが正しく適用されません。NSX-v の Security Group にはインスタンスが存在せず、Security Group に手動で追加する必要があります。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1510350：Service Composer のユーザー インターフェイスで一括削除を行うと、「0 ~ 0」というメッセージが表示される
 NSX Service Composer のユーザー インターフェイスでポリシーの一括削除（100 件以下）を行うと、「0 から 0 である必要があります」というメッセージが表示されます。このメッセージは無視しても問題ありません。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1515656：ポリシー削除のバックグラウンド処理に時間がかかり、CPU 使用率が高くなる場合がある
 ポリシーを削除すると、それ以外のすべてのポリシーがバックグラウンドで再評価されます。ポリシー、Security Group、ポリシーごとのルールが多数あると、セットアップに 1 時間以上かかる場合があります。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1515630：デフォルトのタイムアウトの 20 分が経過すると、キューに登録された発行可能なすべてのタスクに失敗のマークが付く
 キューは NSX Edge ごとに保持され、異なる Edge に対して同時に発行できます。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1545879：既存のファイアウォール ドラフトの名前を変更すると、ユーザー インターフェイスに「内部サーバ エラー」が表示されて操作が失敗する
 NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1545893：分散ファイアウォールのセントラル CLI で「ERROR output 100」が表示される場合がある
 特定の状況下で、vNIC (Virtual Network Adapter) が切断されると、NSX Manager とホスト間で vNIC の状態の情報が一致なくなり、セントラル CLI で「ERROR output 100」が出力される場合があります。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1545853：アプリケーション プロファイルのリストがソートされない
 サービス挿入が有効になっている場合、NSX Edge 内のアプリケーション プロファイル名のリストが不規則な順番で表示されます。6.2.1 リリースでは、アプリケーション プロファイルのリストをソートして表示できるよう修正されました。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1545895：特定の ESXi ホストに対して実行されるセントラル CLI コマンドが、一部のセットアップでタイムアウトする
 NSX 6.2.1 で、この問題は修正されました。

- 解決した問題 1491365：大量のコンテナ更新で vsfwd.log がすぐに上書きされる
SpoofGuard ポリシーが変更されると、NSX Manager は変更を速やかにホストに送りますが、ホストでの変更処理と仮想マシンの SpoofGuard 状態の更新に時間がかかります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1113755：グローバル スコープで定義された Security Group または他のグループ オブジェクトを使用して、NSX ファイアウォールを設定することができない
NSX Edge スコープで定義された管理者ユーザーは、グローバル スコープで定義されたオブジェクトにアクセスすることはできません。たとえば、ユーザー *abc* が Edge スコープで定義され、Security Group *sg-1* がグローバル スコープで定義された場合、*abc* は NSX Edge のファイアウォール構成で *sg-1* を使用することはできません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1425691：ファイアウォール ルールの表示中にマウスの動きが遅れる
vSphere Web Client の [Networking and Security] セクションで、ファイアウォール ルールの行の上にマウスを合わせると、表示が 3 秒遅れます。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1352926：発行が成功しているのに、ユーザー インターフェイスでエラー「**ファイアウォールを発行できませんでした**」が表示される
分散ファイアウォールが、環境内のクラスタのサブセットで有効になっていて、1 つ以上のアクティブなファイアウォール ルールで使用されているアプリケーション グループを更新すると、ユーザー インターフェイス上のすべての発行アクションにおいて、NSX ファイアウォールが有効でないクラスタに属しているホストの ID を含んだエラー メッセージが表示されます。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1295384：REST を使用したセキュリティ ルールの削除でエラーが表示される
Service Composer によって作成されたセキュリティ ルールを削除するために REST API 呼び出しが使用されると、対応するルール セットは実際にはサービス プロファイル キャッシュで削除されず、結果として `ObjectNotFoundException` エラーが発生します。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1412713：新たに追加された仮想マシンにファイアウォール ルールが反映されない
新たに仮想マシンが論理スイッチに追加されると、ファイアウォール ルールが正しく更新されず、新規の仮想マシンが追加されません。ファイアウォールに変更を加えて変更を発行すると、新しいオブジェクトがポリシーに追加されます。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1448022：Security Group の設定で Active Directory オブジェクトが選択できない
NSX 6.1.x では、Security Group オブジェクト選択画面で Active Directory ドメイン オブジェクトまたは LDAP ドメイン オブジェクトの応答に長い時間がかかります。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1473585：IP アドレスが複数のコンマで区切られているため、ファイアウォールをソースやターゲットに追加することができない
NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1460351：NSX 分散ファイアウォール (DFW) セクションをリストの最上位に移動できない
Service Composer で Security Group ポリシーを作成する場合、分散ファイアウォール テーブルで作成されたセクションをリストの最上位に追加することができません。分散ファイアウォール セクションは、上にも下にも動かすことができません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1501451：ポート範囲を使用して設定されたセキュリティ ポリシーにより、ファイアウォールが同期しない状態になる
ポート範囲（「5900-5964」など）としてセキュリティ ポリシーを設定すると `NumberFormatException` エラーが発生してファイアウォールが同期しなくなります。NSX 6.2.0 で、この問題は修正されました。

NSX 6.2.3 以前で解決した監視サービスに関連する問題

- 解決した問題 1617561 : *vmkernel* ログ ファイルに次のエントリが大量に記録される : *ALERT: vdrb: VdrArpInput:1015: CP:Malformed pkt*
 この問題は、サーバなどのネットワーク デバイスが ARP 要求を IEEE 802 Networks ARP 形式で送信するときには発生します。この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1525620 : 分散ファイアウォール ルールの icmpCode の値がホストに送信されず、protocolName および subProtocolName の値は正常に動作する
 この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1563830 : DLR アプライアンスにファイアウォール ルールを適用するときに、ソースまたはターゲットに「mgmtInterface」を指定すると、ルールの適用に失敗する
 NSX Manager ログでは、「vShield Edge:10014:NSX Edge 仮想マシンの構成に失敗しました」のようなメッセージがレポートされます。この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1474498 : REST API 要求により既存のファイアウォール構成が削除された後、ドラフト ファイアウォール ルールのインポートに失敗する
 VMware NSX for vSphere 6.1.x および 6.2.x でセクション ID = Null を含むドラフトが作成されたときに、この問題が発生します。この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1545888 : フロー統計のレポート作成時に、インデックス 0 (着信バイト) とインデックス 1 (発信バイト) のカウントが逆転している場合がある
 インデックス 0 は、元の方のトラフィック カウントを示し、インデックス 1 は反対方向のトラフィック カウントを示します。NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1460085 : **#show interface** コマンドで vNIC_0 インターフェイスのバンド幅や速度が表示されない
 #show interface コマンドを実行すると、「全二重、速度 0M/秒」と表示されますが、正しい NSX Edge vNIC_0 インターフェイスのバンド幅や速度が表示されません。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1288395 : 分散ファイアウォールで IPFIX 構成を有効にすると、vSphere Distributed Switch の NetFlow または SNMP の ESXi 管理インターフェイスでファイアウォール ポートが削除されることがある
 IPFIX 用にコレクタ IP アドレスおよびポートが定義されている場合、指定された UDP コレクタ ポートの送信方向に ESXi 管理インターフェイスのファイアウォールが開かれています。この操作により、事前に ESXi ホスト上で設定されていた場合、次のサービスの ESXi 管理インターフェイス ファイアウォール上の動的ルールセット設定が削除される可能性があります。
 - vSphere Distributed Switch 上の NetFlow コレクタ ポートの設定
 - SNMP ターゲット ポートの設定
 NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1354728 : IPFIX プロトコルで拒否/ブロック イベントが処理できない
 通常 vsfwd ユーザー プロセスはドロップや拒否などのフローを収集し、IPFIX 用に処理します。この問題は、IPFIX コレクタが拒否/ブロック イベントの認識に失敗すると発生します。これは、vSIP ドロップ パケット キューが狭すぎるか、非アクティブ フロー イベントによってラップ アラウンドされるためです。このリリースでは、拒否/ブロック イベントを IPFIX プロトコルで送信する機能が実装されました。NSX 6.2.0 で、この問題は修正されました。

NSX 6.2.3 以前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 1571170：一部の Log Insight レポートが、NSX 6.2 の vRealize コンテンツ パックのいくつかのバージョンでサポートされていない
この問題は、Log Insight のコンテンツ パックの最新バージョンで修正されました。 [VMware Solution Exchange](#) からコンテンツ パックをダウンロードし、インストールします。この問題は NSX 6.2.3 で修正されました。
- 解決した問題 1484506：ESXi のアップグレード中にパープル スクリーンが表示される
NSX を使用する vSphere 5.5U2 ホストを vSphere 6.0 にアップグレードする際、一部の ESXi ホストでパープル スクリーンが表示され、アップグレードが停止する場合があります。 [VMware ナレッジベースの記事 KB2137826](#) を参照してください。この問題は NSX 6.2.3 で解決されました。
- 解決した問題 1453802：NSX ロード バランサを通過するルートでは、vCloud Connector 経由の仮想マシンのコピーが失敗する NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1462006：VMware Integrated OpenStack (VIO) のデプロイにおいて、新たに展開された仮想マシンで、有効なポートと IP アドレスが割り当てられているように表示されても、ネットワークにアクセスできない場合がある NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1482665：Active Directory ベースの SSO で、vSphere Web Client の [NSX] タブにアクセスすると、ログインに時間がかかる
Active Directory 認証に SSO を使用する NSX for vSphere 環境では、ユーザーが初めて vSphere Web Client の [Networking and Security] セクションにログインする際に時間がかかります。NSX 6.1.5 および NSX 6.2.1 で、この問題は修正されました。
- 解決した問題 1326669：組織ネットワークをセットアップできない
組織規模のネットワークをセットアップしようとする、vCloud Director が失敗し、エラー メッセージが表示されます。NSX 6.2.0 で、この問題は修正されました。
- 解決した問題 1497044：VMware Integrated OpenStack (VIO) セットアップで複数の仮想マシンを起動できない
VMware Integrated OpenStack を使用している場合、短時間に大量の仮想マシンを起動したり、大量のファイアウォール ルールを発行することができませんでした。これによって、ログに「Error publishing ip for vnic」というメッセージが記録されます。NSX 6.2.0 で、この問題は修正されました。

ドキュメントの改訂履歴

2015 年 8 月 20 日 NSX 6.2.0 用初版。
2015 年 12 月 17 日 NSX 6.2.1 用初版。
2016 年 3 月 4 日 NSX 6.2.2 用初版。glibc の脆弱性に対応するセキュリティ パッチについて記載。
2016 年 6 月 9 日：NSX 6.2.3 用初版。
2016 年 8 月 25 日 NSX 6.2.4 用初版。
2016 年 9 月 2 日 NSX 6.2.4 用第 2 版。既知の問題について記載しました。
2016 年 9 月 9 日 NSX 6.2.4 用第 3 版。既知の問題について記載しました。
2016 年 9 月 23 日 NSX 6.2.4 用第 4 版。既知の問題の 2 つを「解決した問題」に移動しました。
2016 年 10 月 6 日：NSX 6.2.4 用第 5 版。既知の問題について記載しました。
2016 年 11 月 16 日：NSX 6.2.4 用第 6 版。ナレッジベースの記事について記載しました。
2016 年 11 月 28 日：NSX 6.2.4 用第 6 版。問題 1685894 に関する記述を変更しました。