

NSX のログとシステム イベント

Update 5

変更日：2017 年 11 月 16 日

VMware NSX Data Center for vSphere 6.3



vmware®

VMware Web サイトで最新の技術ドキュメントをご確認いただけます。

<https://docs.vmware.com/jp/>

VMware の Web サイトでは、最新の製品アップデートを提供しています。

本書に関するご意見、ご要望をお寄せください。フィードバック送信先：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

Copyright © 2010 – 2018 VMware, Inc. All rights reserved. [著作権および商標](#).

内容

NSX のログとシステム イベント 4

1 システム イベント、アラームおよびログ 5

システム イベント 5

アラーム 6

NSX コンポーネントのログ レベルの設定 8

監査ログ 11

Syslog サーバの設定 11

テクニカル サポート ログの収集 13

2 NSX およびホスト ログ 16

NSX のログについて 16

ファイアウォールのログ 17

ルーティングに関連する NSX ログ 22

ゲストイントロスペクションのログ 24

3 システム イベント 33

セキュリティ システム イベント 34

分散ファイアウォール システム イベント 35

NSX Edge システム イベント 43

ファブリック システム イベント 47

デプロイ プラグインのシステム イベント 52

メッセージング システム イベント 53

Service Composer システム イベント 54

ゲストイントロスペクション サービス仮想マシンのシステム イベント 56

サービス仮想マシン (SVM) 運用システム イベント 57

レプリケーション - ユニバーサル同期システム イベント 57

NSX 管理システム イベント 58

論理ネットワークのシステム イベント 58

Identity Firewall システム イベント 62

ホストの準備のシステム イベント 62

NSX のログとシステム イベント

『のログとシステム イベント』では、NSX Manager ユーザー インターフェイスと vSphere Web Client を使用して、VMware NSX[®] for vSphere[®] システムのログ メッセージ、イベント、アラームについて説明します。

対象読者

本書は、VMware vCenter Server 環境で NSX のトラブルシューティングを行うユーザーを対象としています。本書に記載されている情報は、システム管理者としての経験があり、仮想マシン テクノロジーおよび仮想データセンターの操作に詳しい方を対象としています。本書は、VMware ESXi、vCenter Server、vSphere Web Client を含む VMware vSphere についての知識があることを前提としています。

VMware の技術ドキュメントの用語集

VMware は、新しい用語を集めた用語集を提供しています。当社の技術ドキュメントで使用されている用語の定義については、<http://www.vmware.com/support/pubs> をご覧ください。

システム イベント、アラームおよびログ

1

システム イベント、アラーム、およびログを使用して、NSX 環境の健全性およびセキュリティを監視し、問題のトラブルシューティングを行うことができます。

この章には、次のトピックが含まれています。

- システム イベント
- アラーム
- NSX コンポーネントのログ レベルの設定
- 監査ログ
- Syslog サーバの設定
- テクニカル サポート ログの収集

システム イベント

システム イベントはシステムのアクションを記録したものです。各イベントには、「情報」や「重大」など、イベントがどれだけ重要かを示す重要度レベルが指定されています。システム イベントを SNMP トラップとしてプッシュすると、SNMP 管理ソフトウェアが NSX システム イベントを監視できるようになります。

システム イベントのレポートの表示

vSphere Web Client では、NSX Manager が管理しているすべてのコンポーネントのシステム イベントを確認できます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で NSX Manager をクリックし、[監視] タブをクリックします。
- 4 [システム イベント] タブをクリックします。

列ヘッダーの矢印をクリックすると、イベントを並べ替えることができます。また、[フィルタ] テキスト ボックスを使用すると、イベントをフィルタリングできます。

システム イベントの形式

Syslog サーバを指定すると、NSX Manager は、その Syslog サーバにすべてのシステム イベントを送信します。

これらのメッセージは、以下に示すメッセージと類似した形式になっています。

```
Jan 8 04:35:00 NSXMGR 2017-01-08 04:35:00.422 GMT+00:00
INFO TaskFrameworkExecutor-18 SystemEventDaoImpl:133 -
[SystemEvent] Time:'Tue Nov 08 04:35:00.410 GMT+00:00 2016',
Severity:'High', Event Source:'Security Fabric', Code:'250024',
Event Message:'The backing EAM agency for this deployment could not be found.
It is possible that the VC services may still be initializing.
Please try to resolve the alarm to check existence of the agency.
In case you have deleted the agency manually, please delete the deployment
entry from NSX.', Module:'Security Fabric', Universal Object:'false'
```

システム イベントには、次の情報が含まれています。

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Event Message: Text containing detailed information about the event.
Module: Event component. May be the same as event source.
Universal Object: Value displayed is True or False.
```

アラーム

アラームは、イベント、条件のセット、またはオブジェクトの状態に応じて起動される通知です。NSX ダッシュボードや vSphere Web Client ユーザー インターフェイスの他の画面で、別のアラートと一緒にアラームが表示されます。

GET `api/2.0/services/systemalarms` API を使用すると、NSX オブジェクトでアラームを表示できます。

NSX では、アラームに次の 2 つの方法がサポートされています。

- アラームは、システム イベントに対応し、アラームの発生原因となった問題を解決するリゾルバが関連付けられています。このアプローチは、ネットワークやセキュリティ ファブリック環境（EAM、メッセージバス、プラグインのデプロイなど）向けに設計され、Service Composer にもサポートされています。これらのアラームは、イベントコードをアラームコードとして使用します。詳細については、『<NSX のログとシステム イベント>』のドキュメントを参照してください。
- Edge の通知アラームは、アラーム ペアをトリガし、解決できるように設定されています。この方法は、IPSec VPN、ロード バランサ、高可用性、健全性チェック、Edge ファイル システム、リソースの予約など、いくつかの Edge の機能で利用できます。アラームは、イベントコードとは別のアラームコードを使用します。詳細については、『<NSX のログとシステム イベント>』のドキュメントを参照してください。

通常、エラー状態が修復されると、アラームは自動的に削除されます。一部のアラームは、設定を更新する際に自動的にクリアされません。問題が解決したら、アラームを手動でクリアする必要があります。

次に、アラームのクリアに使用する API について説明します。

クラスタ、ホスト、リソース プール、セキュリティ グループ、NSX Edge のアラームなど、特定の送信元にアラームを個別に設定できます。送信元のアラームを表示するには、<sourceId> を使用します。

```
GET https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}
```

送信元のアラームをすべて解決するには、<sourceId> を使用します。

```
POST https://<<NSX-IP>>/api/2.0/services/alarms/{sourceId}?action=resolve
```

メッセージ バス、プラグインのデプロイ、Service Composer、Edge アラームなどの NSX アラームを確認できます。

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms
```

特定の NSX アラームを表示するには、<alarmId> を使用します。

```
GET https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>
```

特定の NSX アラームを解決するには、<alarmId> を使用します。

```
POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve
```

API の詳細については、『NSX API ガイド』を参照してください。

アラームの形式

API を使用してアラームの形式を表示できます。

アラームの形式には、次の情報が含まれています。

```
Event ID and Time
Severity: Possible values include informational, low, medium, major, critical, high.
Event Source: Source where you should look to resolve the reported event.
Event Code: Unique identifier for the event.
Message: Text containing detailed information about the event.
Alarm ID: ID of an alarm.
Alarm Code: Event code which uniquely identifies the system alarm.
Alarm Source: Source where you should look to resolve the reported event.
```

ゲスト イントロスペクションのアラーム

注意が必要なゲスト イントロスペクション イベントは、vCenter Server 管理者にアラームで通知されます。アラームはその状態が解除されると自動的にキャンセルされます。

vCenter Server アラームはカスタム vSphere プラグインなしでも表示できます。イベントとアラームについては『vCenter Server 管理ガイド』を参照してください。

NSX Manager が vCenter Server の拡張として登録されると、NSX Manager は、SVM、ゲスト イントロスペクション モジュール、シン エージェントという 3 つの ゲスト イントロスペクション コンポーネントからのイベントを基にしてアラームを作成および削除するルールを定義します。ルールはカスタマイズできます。アラームの新しいカスタム ルールを作成する方法については、vCenter Server のドキュメントを参照してください。いくつかのケースでは、アラームの発生には複数の原因があることがあります。下記の表では、可能性のある原因とそれに対応した改善のためのアクションがリストされています。

ホスト アラーム

ホスト アラームは ゲスト イントロスペクション モジュールの健全性ステータスに影響を及ぼすイベントにより生成されます。

表 1-1. エラー（赤で表示）

可能性のある原因	アクション
ゲスト イントロスペクション モジュールはホストにインストールされていますが、ステータスを NSX Manager に報告しなくなりました。	<ol style="list-style-type: none"> 1 ホストにログインし、<code>/etc/init.d/vShield-Endpoint-Mux start</code> コマンドを入力して、ゲスト イントロスペクション が動作していることを確認します。 2 ネットワークが適切に設定され、ゲスト イントロスペクション が NSX Manager に接続可能であることを確認します。 3 NSX Manager を再起動します。

SVM アラーム

SVM アラームは SVM の健全性ステータスに影響を及ぼすイベントによって生成されます。

表 1-2. SVM 赤アラーム

問題	アクション
ゲスト イントロスペクション モジュールと一致しないプロトコル バージョンがある。	ゲスト イントロスペクション モジュールと SVM に、互いに互換性のあるプロトコルが設定されていることを確認します。
ゲスト イントロスペクション が SVM への接続を確立できない。	SVM がパワーオン状態で、ネットワークが適切に設定されていることを確認します。
ゲストが接続されていても SVM がステータスを報告しない。 内部エラー。VMware のサポート担当者に問い合わせてください。	

NSX コンポーネントのログ レベルの設定

各 NSX コンポーネントについてログ レベルを設定できます。

次に示すように、サポートされるレベルはコンポーネントによって異なります。

```
nsxmgr> set
  hardware-gateway  Show Logical Switch Commands
  PACKAGE-NAME      Set log level
  controller         Show Logical Switch Commands
  host              Show Logical Switch Commands

nsxmgr> set hardware-gateway agent 10.1.1.1 logging-level
ERROR
```


WARN
INFO
DEBUG
TRACE

```
nsxmgr-01a> set <package-name> logging-level
```

OFF
FATAL
ERROR
WARN
INFO
DEBUG
TRACE

```
nsxmgr> set controller 192.168.110.31
```

java-domain Set controller node log level
native-domain Set controller node log level

```
nsxmgr> set controller 192.168.110.31 java-domain logging-level
```

OFF
FATAL
ERROR
WARN
INFO
DEBUG
TRACE

```
nsxmgr> set controller 192.168.110.31 native-domain logging-level
```

ERROR
WARN
INFO
DEBUG
TRACE

```
nsxmgr> set host host-28
```

netcpa Set host node log level by module
vdl2 Set host node log level by module
vdr Set host node log level by module

```
nsxmgr> set host host-28 netcpa logging-level
```

FATAL
ERROR
WARN
INFO
DEBUG

```
nsxmgr> set host host-28 vdl2 logging-level
```

ERROR
INFO
DEBUG
TRACE


```
nsxmgr> set host host-28 vdr logging-level
OFF
ERROR
INFO
```

IPSec VPN のログの有効化

すべての IPSec VPN トラフィックのログを有効にできます。

デフォルトでは、ログが有効になり、「警告」レベルに設定されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理 (Manage)] タブをクリックして、[VPN] タブをクリックします。
- 5 [IPsec VPN] をクリックします。
- 6 ローカル サブネットとピア サブネット間のトラフィック フローをログに記録してログ レベルを選択するには、[ログ ポリシー (Logging Policy)] の横の  を選択して、[ログの有効化 (Enable logging)] をクリックします。
- 7 ログ レベルを選択して、[変更の発行 (Publish Changes)] をクリックします。

SSL VPN-Plus のログ

SSL VPN-Plus ゲートウェイのログが、NSX Edge アプライアンスで設定された Syslog サーバに送信されます。SSL VPN-Plus Client のログは、リモートユーザーのコンピュータの次のディレクトリに格納されます。**%PROGRAMFILES %/VMWARE/SSL VPN Client/**。

SSL VPN-Plus Client ログとログ レベルの変更

- 1 [SSL VPN-Plus] タブで、左側のパネルから [サーバ設定 (Server Settings)] をクリックします。
- 2 [ログ ポリシー] セクションに移動し、セクションを展開して現在の設定を表示します。
- 3 [変更 (Change)] をクリックします。
- 4 ログを有効にするには、[ログの有効化 (Enable logging)] チェック ボックスをオンにします。

また

ログを無効にするには、[ログの有効化 (Enable logging)] チェック ボックスをオフにします。

- 5 必要なログ レベルを選択します。

注: デフォルトで、SSL VPN-Plus クライアントのログが有効になり、ログ レベルが通知に設定されます。

- 6 [OK] をクリックします。

監査ログ

監査ログは、NSX Manager にログインするユーザーのすべてのアクションを記録します。

監査ログの表示

[監査ログ] タブには、すべての NSX Manager ユーザーが実行したアクションが表示されます。NSX Manager では、最大 10 万件の監査ログが保持されます。 .

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、次に [ネットワークとセキュリティのインベントリ] から [NSX Manager] をクリックします。
- 3 [名前] 列で、NSX サーバをクリックし、[監視] タブをクリックします。
- 4 [監査ログ] タブをクリックします。
- 5 監査ログに関する詳細情報がある場合は、そのログの [操作] 列のテキストがクリック可能になります。監査ログの詳細を表示するには、[操作] 列のテキストをクリックします。
- 6 [監査ログ変更の詳細] で、[変更された行] を選択すると、この監査ログ操作で値が変更されたプロパティのみが表示されます。

Syslog サーバの設定

NSX コンポーネントおよびホストのログのリポジトリとして、Syslog サーバを設定できます。

NSX Manager の Syslog サーバの設定

Syslog サーバを指定すると、NSX Manager は、その Syslog サーバにすべての監査ログとシステム イベントを送信します。

Syslog データは、トラブルシューティングや、インストールおよび構成中、ログに記録されたデータを確認する際に役立ちます。

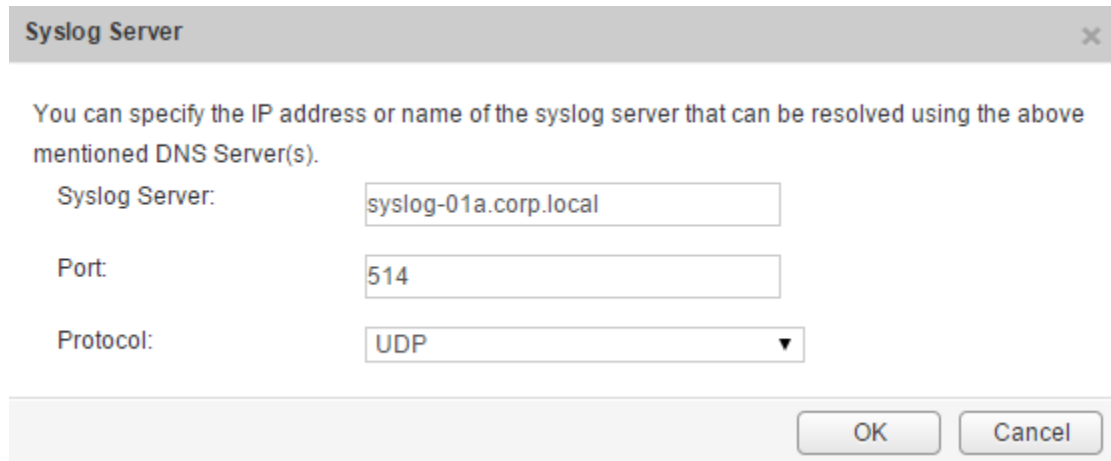
NSX Edge は 2 台の Syslog サーバをサポートします。NSX Manager と NSX Controller は 1 台の Syslog サーバをサポートします。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
Web ブラウザで、NSX Manager アプライアンスの GUI (<https://<nsx-manager-ip>> または <https://<nsx-manager-hostname>>) に移動し、NSX Manager のインストール時に設定したパスワードを使用して admin としてログインします。
- 2 ホーム ページで [アプライアンス設定の管理 (Manage Appliance Settings)] - [全般 (General)] の順にクリックします。

- 3 [Syslog サーバ (Edit)] の横にある [編集 (Syslog Server)] をクリックします。
- 4 Syslog サーバの IP アドレス/ホスト名、ポート、およびプロトコルを入力します。

次はその例です。



Syslog Server [X]

You can specify the IP address or name of the syslog server that can be resolved using the above mentioned DNS Server(s).

Syslog Server:

Port:

Protocol:

OK Cancel

- 5 [OK] をクリックします。

NSX Manager のリモート ログが有効になり、スタンドアロンの Syslog サーバにログが保存されます。

NSX Edge の Syslog サーバの設定

1 台または 2 台のリモート Syslog サーバを設定できます。NSX Edge アプライアンスから流れるファイアウォール イベントに関連した NSX Edge のイベントとログは、Syslog サーバに送信されます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge をダブルクリックします。
- 4 [管理] > [設定] タブの順にクリックします。
- 5 [詳細] パネルで、Syslog サーバの横の [変更] をクリックします。
- 6 両方のリモート Syslog サーバの IP アドレスを入力し、プロトコルを選択します。
- 7 [OK] をクリックして設定を保存します。

NSX Controller 用 Syslog サーバの設定

NSX Controller 用に Syslog サーバを設定すると、NSX Manager は、その Syslog サーバにすべての監査ログとシステム イベントを送信します。Syslog データは、トラブルシューティングや、インストールおよび構成中、ログに記録されたデータを確認する際に役立ちます。NSX Controller 上で Syslog サーバを設定する場合、NSX API を使用する方法のみがサポートされます。VMware は、Syslog のプロトコルとして UDP を使用することを推奨しています。

手順

- 1 NSX Controller 上で Syslog を有効にするには、次の NSX API を使用します。これにより、コントローラ Syslog エクスポートが追加され、指定したコントローラ ノード上に Syslog エクスポートが設定されます。

```
Request
POST https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Request Body:
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

- 2 次の NSX API を使用すると、コントローラ Syslog エクスポートに対するクエリを実行し、指定したコントローラ ノード上で設定済みの Syslog エクスポートに関する詳細を取得できます。

```
Request
GET https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
Response Body:
<?xml version="1.0" encoding="UTF-8"?>
<controllerSyslogServer>
<syslogServer>10.135.14.236</syslogServer>
<port>514</port>
<protocol>UDP</protocol>
<level>INFO</level>
</controllerSyslogServer>
```

- 3 指定したコントローラ ノード上のコントローラ Syslog エクスポートが不要な場合は、次の NSX API を使用して削除できます。

```
Request
DELETE https://<nsxmgr-ip>/api/2.0/vdn/controller/{controller-id}/syslog
```

次のステップ

API の詳細については、『NSX API ガイド』を参照してください。

テクニカル サポート ログの収集


NSX コンポーネントおよびホストからテクニカル サポート ログを収集して、VMware に問題をレポートする場合があります。

ホストのテクニカル サポート ログを収集するには、コマンド **export host-tech-support** を実行します。『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。

NSX のテクニカル サポート ログのダウンロード

自分のデスクトップに NSX Manager のシステム ログと Web Manager のログをダウンロードできます。

手順

- 1 NSX Manager 仮想アプライアンスにログインします。
- 2 [アプライアンス管理] で、[アプライアンス設定の管理] をクリックします。
- 3  をクリックし、[テクニカル サポート ログのダウンロード] をクリックします。
- 4 [ダウンロード] をクリックします。
- 5 ログの準備ができたなら、[保存] をクリックして、デスクトップにログをダウンロードします。
ログは圧縮され、ファイル拡張子 **.gz** が付加されます。


次のステップ

解凍ユーティリティを使用して、ファイルを保存したディレクトリの [すべてのファイル] を参照してログを開くことができます。

NSX Edge のテクニカル サポート ログのダウンロード

テクニカル サポート ログは、NSX Edge インスタンスごとにダウンロードできます。NSX Edge インスタンスで高可用性が有効になっている場合は、両方の NSX Edge 仮想マシンからサポート ログがダウンロードされます。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security (Networking & Security)] をクリックし、[NSX Edge (NSX Edges)] をクリックします。
- 3 NSX Edge インスタンスを選択します。
- 4 [アクション] () をクリックして、[テクニカル サポート ログのダウンロード] を選択します。
- 5 テクニカル サポート ログが生成されたら、[ダウンロード] をクリックします。

NSX Controller のテクニカル サポート ログのダウンロード

テクニカル サポート ログは、NSX Controller インスタンスごとにダウンロードできます。製品固有のこれらのログには、分析に使用する診断情報が含まれています。

NSX Controller のログを収集するには、次の手順を実行します。

手順

- 1 vSphere Web Client にログインします。
- 2 [Networking and Security] をクリックし、[インストール手順] をクリックします。
- 3 [管理] で、ログをダウンロードするコントローラを選択します。
- 4 [テクニカル サポート ログのダウンロード] をクリックします。

5 [ダウンロード] をクリックします。

NSX Manager が、NSX Controller ログのダウンロードを開始し、ロックを取得します。

注: 一度に 1 つの NSX Controller ログをダウンロードします。最初のダウンロードが完了してから、別のダウンロードを開始してください。複数のコントローラから同時にログをダウンロードすると、エラーが発生する可能性があります。

6 ログの準備ができたなら、[保存] をクリックして、デスクトップにログをダウンロードします。

ログは圧縮され、ファイル拡張子 **.gz** が付加されます。

これで、ダウンロードしたログを分析できます。

次のステップ

診断情報を VMware のテクニカル サポートにアップロードする場合は、[ナレッジベースの記事 KB2070100](#) を参照してください。

NSX およびホスト ログ

さまざまな NSX コンポーネントおよびホストのログを使用して問題の検出およびトラブルシューティングを行うことができます。

この章には、次のトピックが含まれています。

- [NSX のログについて](#)
- [ファイアウォールのログ](#)
- [ルーティングに関連する NSX ログ](#)
- [ゲスト イントロスペクションのログ](#)

NSX のログについて

Syslog サーバを設定し、各 NSX コンポーネントのテクニカル サポート ログを表示できます。管理プレーンのログは NSX Manager から、データ プレーンのログは vCenter Server を通じて提供されます。そのため、Syslog サーバで環境全体のログが記録できるように、NSX コンポーネントと vCenter Server で同じ Syslog サーバを指定することが推奨されます。

vCenter Server が管理するホストの Syslog サーバの設定については、<https://docs.vmware.com> にある、該当するバージョンの vSphere ドキュメントを参照してください。

注: ログの収集や NSX 分散論理ルーター (DLR) 制御仮想マシンへのアクセスに使用する Syslog サーバまたはジャンプサーバは、分散論理ルーターの論理インターフェイスに直接接続された論理スイッチ上に配置することはできません。

表 2-1. NSX のログ

コンポーネント	説明
ESXi のログ	これらのログは、vCenter Server から生成される仮想マシン サポート バンドルの一部として収集されます。 ESXi ログ ファイルの詳細については、vSphere のドキュメントを参照してください。
NSX Edge のログ	NSX Edge CLI で show log [follow reverse] コマンドを使用します。 NSX Edge ユーザー インターフェイスでテクニカル サポート ログ バンドルをダウンロードします。
NSX Manager のログ	NSX Manager CLI で show log CLI コマンドを使用します。 NSX Manager 仮想アプライアンス ユーザー インターフェイスでテクニカル サポート ログ バンドルをダウンロードします。

表 2-1. NSX のログ (続き)

コンポーネント	説明
ルーティングのログ	『NSX のログ作成とシステム イベント』ガイドを参照してください。
ファイアウォール ログ	『ファイアウォールのログ』を参照してください。
ゲスト イントロスペクションのログ	『ゲスト イントロスペクションのログ』を参照してください。

NSX Manager

Syslog サーバを指定するには、[『NSX Manager の Syslog サーバの設定』](#)を参照してください。

テクニカル サポート ログをダウンロードするには、[『NSX のテクニカル サポート ログのダウンロード』](#)を参照してください。

NSX Edge

Syslog サーバを指定するには、[『NSX Edge の Syslog サーバの設定』](#)を参照してください。

テクニカル サポート ログをダウンロードするには、[『NSX Edge のテクニカル サポート ログのダウンロード』](#)を参照してください。

NSX Controller

Syslog サーバを指定するには、[『NSX Controller 用 Syslog サーバの設定』](#)を参照してください。

テクニカル サポート ログをダウンロードするには、[『NSX Controller のテクニカル サポート ログのダウンロード』](#)を参照してください。

ファイアウォール

詳細については、[『ファイアウォールのログ』](#)を参照してください。

ファイアウォールのログ

ファイアウォールは、監査ログ、ルール メッセージ ログ、システム イベント ログなどのログ ファイルを生成して保存します。ファイアウォールが有効になっている各クラスタに対して、Syslog サーバを設定する必要があります。Syslog サーバは `Syslog.global.logHost` 属性で指定します。

ファイアウォールは、次の表にあるログを生成します。

表 2-2. ファイアウォール ログ

ログ タイプ	説明	場所
ルール メッセージ ログ	ルールでログ作成が有効な場合、各ルールで許可されるトラフィックや拒否されるトラフィックなどの、すべてのアクセスに関する決定事項が含まれます。ログ作成が有効なルールの分散ファイアウォール パケットのログが含まれます。	/var/log/dfwptlogs.log
監査ログ	管理ログと分散ファイアウォールの設定の変更が含まれます。	/home/secureall/secureall/logs/vsm.log

表 2-2. ファイアウォール ログ (続き)

ログ タイプ	説明	場所
システム イベント ログ	適用された分散ファイアウォールの設定のほか、作成、削除、または失敗したフィルタ、セキュリティ グループに追加された仮想マシンなどの情報が含まれます。	/home/secureall/secureall/logs/vsm.log
データ プレーン/VMkernel のログ	ファイアウォール カーネル モジュール (VSIP) に関連するアクティビティをキャプチャします。システムによって生成されるメッセージのログ エントリが含まれます。	/var/log/vmkernel.log
メッセージ バス クライアント/VSFWD のログ	ファイアウォール エージェントのアクティビティをキャプチャします。	/var/log/vsfwd.log

注: <vsm.log> ファイルにアクセスするには、NSX Manager コマンドライン インターフェイス (CLI) から **show log manager** コマンドを実行し、<vsm.log> をキーワードに指定して <grep> を実行します。このファイルにアクセスできるのは、<root> 権限を持つユーザーまたはユーザー グループだけです。

ルール メッセージ ログ

ルールでログ作成が有効な場合、各ルールで許可されるトラフィックや拒否されるトラフィックなどの、すべてのアクセスに関する決定事項が含まれます。これらのログは、各ホストの **/var/log/dfwpktlogs.log** に保存されます。

ファイアウォールのログ メッセージの例：

```
# more /var/log/dfwpktlogs.log
2015-03-10T03:22:22.671Z INET match DROP domain-c7/1002 IN 242 UDP 192.168.110.10/138->192.168.110.255/138

# more /var/log/dfwpktlogs.log
2017-04-11T21:09:59.877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST 10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070
```

その他の例：

```
2017-10-19T22:38:05.586Z 58734 INET match PASS domain-c8/1006 OUT 84 ICMP 172.18.8.121->172.18.8.119 RULE_TAG
2017-10-19T22:38:08.723Z 58734 INET match PASS domain-c8/1006 OUT 60 TCP 172.18.8.121/36485->172.18.8.119/22 S RULE_TAG
2017-10-19T22:38:18.785Z 58734 INET TERM domain-c8/1006 OUT ICMP 8 0 172.18.8.121->172.18.8.119 2/2 168/168 RULE_TAG
2017-10-19T22:38:20.789Z 58734 INET TERM domain-c8/1006 OUT TCP FIN 172.18.8.121/36484->172.18.8.119/22 44/33 4965/5009 RULE_TAG
```

次の例では、

- 1002 は分散ファイアウォールのルール ID です。
- domain-c7 は vCenter 管理対象オブジェクト ブラウザ (MOB) のクラスタ ID です。

- 192.168.110.10/138 はソース IP アドレスです。
- 192.168.110.255/138 はターゲット IP アドレスです。
- <RULE_TAG> は、ファイアウォール ルールの追加または編集で [タグ] テキスト ボックスに追加するテキストの例です。

次の例は、192.168.110.10 を 172.16.10.12 に ping した結果を示しています。

```
# tail -f /var/log/dfwpktlogs.log | grep 192.168.110.10

2015-03-10T03:20:31.274Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
2015-03-10T03:20:35.794Z INET match DROP domain-c27/1002 IN 60 PROTO 1 192.168.110.10->172.16.10.12
```

次の表で、ファイアウォール ログ メッセージのテキスト ボックスについて説明します。

表 2-3. ログ ファイル エントリのコンポーネント

コンポーネント	サンプル内の値
タイムスタンプ	2017-04-11T21:09:59
ファイアウォールに関する記述	877Z ESXi_FQDN dfwpktlogs: 50047 INET TERM domain-c1/1001 IN TCP RST 10.1.2.3/33491->10.4.5.6/10001 22/14 7684/1070

表 2-4. ログ ファイル エントリのファイアウォールに関する記述

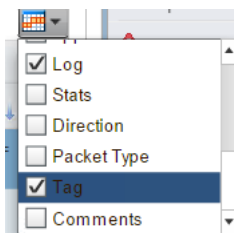
エンティティ	利用可能な値
フィルタ ハッシュ	フィルタ名およびその他の情報の取得に使用できる数値。
AF 値	INET、INET6
原因	<ul style="list-style-type: none"> ■ match: パケットがルールと一致します。 ■ bad-offset: パケットの取得中にデータベースで内部エラーが発生しました。 ■ fragment: 先頭のフラグメントにリアセンブルした後の先頭以外のフラグメントです。 ■ short: パケットが短すぎます。たとえば、IP ヘッダーまたは TCP/UDP ヘッダーが含まれていません。 ■ normalize: 正しいヘッダーまたはペイロードがない不正なパケットです。 ■ memory: データベースでメモリが不足しています。 ■ bad-timestamp: 不正な TCP タイムスタンプです。 ■ proto-cksum: 不正なプロトコル チェックサムです。 ■ state-mismatch: TCP 状態マシン チェックを通過していない TCP パケットです。 ■ state-insert: 重複する接続が見つかりました。 ■ state-limit: 状態の数が、データベースで追跡可能な最大数に達しました。 ■ SpoofGuard: SpoofGuard がドロップしたパケットです。 ■ TERM: 接続が切断されました。

表 2-4. ログ ファイル エントリのファイアウォールに関する記述 (続き)

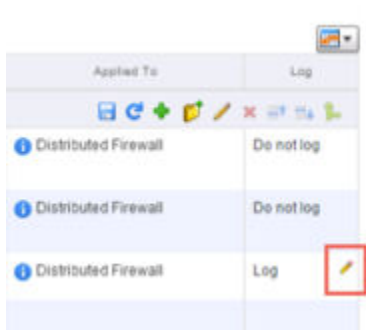
エンティティ	利用可能な値
アクション	<ul style="list-style-type: none"> ■ PASS: パケットを受け入れます。 ■ DROP: パケットをドロップします。 ■ NAT: SNAT ルールです。 ■ NONAT: SNAT ルールに一致しましたが、アドレス変換はできません。 ■ RDR: DNAT ルールです。 ■ NORDR: DNAT ルールに一致しましたが、アドレス変換はできません。 ■ PUNT: 現在の仮想マシンと同じハイパーバイザーで実行しているサービス仮想マシンにパケットを送信します。 ■ REDIRECT: 現在の仮想マシンのハイパーバイザー以外で実行しているネットワーク サービスにパケットを送信します。 ■ COPY: パケットを受け入れ、現在の仮想マシンと同じハイパーバイザーで実行されているサービス仮想マシンにコピーします。 ■ REJECT: パケットを拒否します。
ルール セットとルール ID	<rule set>/<rule ID>
方向	IN、OUT
パケットの長さ	<length>
プロトコル	<p>TCP、UDP、ICMP または PROTO (プロトコル番号)</p> <p>TCP 接続の場合、接続が終了する実際の原因が TCP キーワードの後に示されます。</p> <p>TCP セッションの原因が TERM の場合、追加の説明が PROTO 行に表示されます。TCP 接続の終了で考えられる原因は、RST (TCP RST パケット)、FIN (TCP FIN パケット)、TIMEOUT (長時間のアイドル状態) です。</p> <p>上の例では、<RST> になっています。これは、接続のリセットを要求する <RST> パケットがあることを意味します。</p> <p>TCP 以外の接続 (UDP、ICMP または他のプロトコル) の場合、接続の終了原因は TIMEOUT だけです。</p>
送信元の IP アドレスおよびポート	<IP address>/<port>
宛先の IP アドレスおよびポート	<IP address>/<port>
TCP フラグ	S (SYN)、SA (SYN-ACK)、A (ACK)、P (PUSH)、U (URGENT)、F (FIN)、R (RESET)
パケット数	<p>パケット数。</p> <p>22/14: 受信パケット数/送信パケット数</p>
バイト数	<p>バイト数。</p> <p>7684/1070: 受信バイト数/送信バイト数</p>

ルール メッセージを有効にするには、vSphere Web Client にログインします。

- 1 [Networking and Security] > [ファイアウォール] ページで [ログ] 列を有効にします。



- 2 [ログ] テーブル セルにマウスを合わせて鉛筆アイコンをクリックし、ルールへのロギングを有効にします。



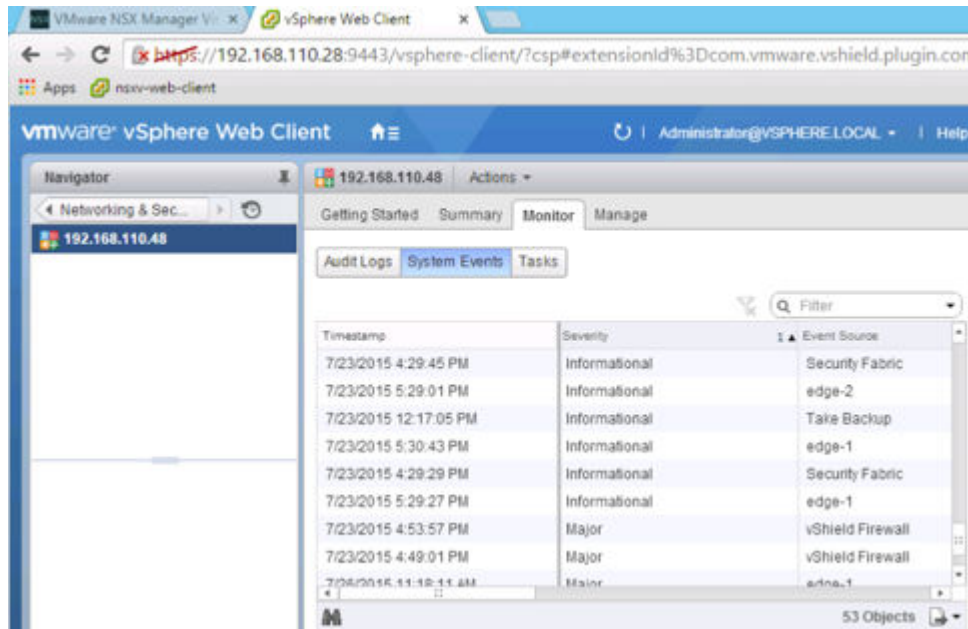
注: ファイアウォールのログ メッセージに表示されるテキストをカスタマイズするには、[タグ] 列を有効にし、鉛筆アイコンをクリックして必要なテキストを追加します。

監査ログとシステム イベント ログ

監査ログには、管理ログと分散ファイアウォールの設定の変更が含まれています。これらのログは、`/home/secureall/secureall/logs/vsm.log` に保存されます。

システム イベント ログには、適用された分散ファイアウォールの設定のほか、作成、削除、または失敗したフィルタ、セキュリティ グループに追加された仮想マシンなどの情報が含まれます。これらのログは、`/home/secureall/secureall/logs/vsm.log` に保存されます。

ユーザー インターフェイスで監査およびシステム イベント ログを表示するには、[Networking and Security] > [インストール手順] > [管理] の順に移動して NSX Manager の IP アドレスをダブルクリックします。[監視] タブをクリックします。



詳細については、『NSX のログ作成とシステム イベント』を参照してください。

ルーティングに関連する NSX ログ

ベスト プラクティスとして、ログを中央のコレクタに送信するように NSX のすべてのコンポーネントを設定することをお勧めします。

必要に応じて、NSX コンポーネントのログ レベルを変更できます。詳細については、『NSX のログ作成とシステム イベント』で「NSX コンポーネントのログ レベルの設定」を参照してください。

NSX Manager のログ

- NSX Manager CLI の **show log** コマンド
- テクニカル サポート ログ バンドル (NSX Manager ユーザー インターフェイスで収集されます)

NSX Manager Virtual Appliance Management



NSX Manager のログには、管理プレーンに関連する情報が含まれます。この情報の対象範囲は、CRUD（作成、読み取り、更新、削除）の操作です。

コントローラのログ

コントローラには複数のモジュールが含まれ、その多くでは独自のログ ファイルが使用されます。コントローラのログには、**show log <log file> [filtered-by <string>]** コマンドを使用してアクセスできます。ルーティングに関連するログ ファイルは、次のとおりです。

- **cloudnet/cloudnet_java-vnet-controller.<開始時のタイムスタンプ>.log**：このログは、設定と内部の API サーバを管理します。
- **cloudnet/cloudnet.nsx-controller.log**：コントローラのメイン プロセスのログです。
- **cloudnet/cloudnet_cpp.log.nsx-controller.log**：このログは、クラスタリングとブートストラップを管理します。
- **cloudnet/cloudnet_cpp.log.ERROR**：このファイルは、エラーが発生した場合に作成されます。

コントローラのログには詳細情報が含まれます。ほとんどの場合、VMware のエンジニアリング チームが困難な問題を解決するために必要となります。

CLI の **show log** コマンドに加えて、**watch log <logfile> [filtered-by <string>]** コマンドを使用することで個々のログ ファイルの更新状況をリアルタイムで確認できます。

ログは、コントローラ サポート バンドルに含まれます。このサポート バンドルを生成してダウンロードするには、NSX ユーザー インターフェイスでコントローラ ノードを選択して、[テクニカル サポート ログのダウンロード (Download tech support logs)] アイコンをクリックします。

ESXi ホストのログ

ESXi ホストで実行される NSX コンポーネントによって、いくつかの種類のログ ファイルが作成されます。

- VMkernel のログ: `/var/log/vmkernel.log`
- 制御プレーン エージェントのログ: `/var/log/netcpa.log`
- メッセージ バス クライアントのログ: `/var/log/vsfwd.log`

vCenter Server から生成される仮想マシン サポート バンドルの一部として、ログを収集することも可能です。ログ ファイルにアクセスできるのは、<root> 権限を持つユーザーまたはユーザー グループだけです。

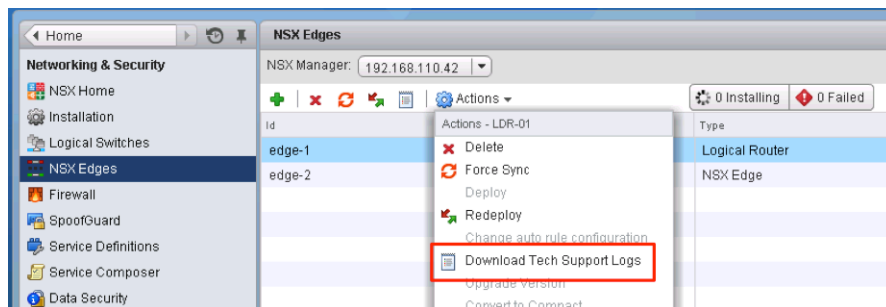
ESG/分散論理ルーター制御仮想マシンのログ

ESG および分散論理ルーター制御仮想マシンのログ ファイルにアクセスする方法は 2 種類あります。CLI を使用して表示する方法と、CLI またはユーザー インターフェイスを使用してテクニカル サポート バンドルをダウンロードする方法です。

ログを表示するための CLI コマンドは、`show log [follow | reverse]` です。

テクニカル サポート バンドルをダウンロードするには、次の手順を実行します。

- CLI から、**enable** モードを使用して `export tech-support <[scp | ftp]> <URI>` コマンドを実行します。
- vSphere Web Client から、[アクション (Actions)] メニューの [テクニカル サポート ログのダウンロード (Download Tech Support Logs)] オプションを選択します。



その他の役立つファイル、およびファイルの場所

正確にはログではありませんが、NSX のルーティングの理解とトラブルシューティングに役立つファイルが多数あります。

- 制御プレーン エージェント設定の `/etc/vmware/netcpa/config-by-vsm.xml` には、次のコンポーネントに関する情報が含まれます。
 - コントローラ、IP アドレス、TCP ポート、証明書のサムプリント、SSL の有効/無効
 - VXLAN を使用して有効にされた分散仮想スイッチの dvUplink (チーミング ポリシー、名前、UUID)
 - ホストが把握する分散論理ルーター インスタンス (DLR ID、名前)

- 制御プレーン エージェント設定の `/etc/vmware/netcpa/netcpa.xml` には、ログ レベル（デフォルトは [info]）など、netcpa の多様な設定オプションが含まれます。
- 制御プレーンの証明書ファイル：`/etc/vmware/ssl/rui-for-netcpa.*`
 - 2つのファイル：ホスト証明書、ホストのプライベート キー
 - コントローラでホストの接続を認証するために使用

これらのファイルはすべて、vsfwd によるメッセージ バス接続を介して NSX Manager から受信する情報を使用して、制御プレーン エージェントによって作成されます。

ゲスト イントロスペクションのログ

ゲスト イントロスペクションのトラブルシューティングで、複数のログをキャプチャして使用できます。

ESX ゲスト イントロスペクション モジュール (MUX) のログ

ESXi ホスト上の仮想マシンでゲスト イントロスペクションを使用していない場合、またはホストでサービス仮想アプライアンスとの通信に関するアラームが発生している場合は、ESXi ホスト上の ESX ゲスト イントロスペクション モジュールに問題がある可能性があります。

ログのパスとサンプル メッセージ

MUX ログのパス
/var/log/syslog
var/run/syslog.log

ESX ゲスト イントロスペクション モジュール (MUX) のメッセージは、<timestamp>EPsecMUX<[ThreadId]>:<message> の形式で記録されます。

次はその例です。

```
2017-07-16T05:44:49Z EPsecMux[38340669]: [ERROR] (EPSEC) [38340669]
Attempted to recv 4 bytes from sd 49, errno = 104 (Connection reset by peer)
```

上記の例で

- [ERROR] はメッセージのタイプです。他のタイプとしては、[DEBUG]、[INFO] があります。
- (EPSEC) は、エンドポイント セキュリティに関連するメッセージであることを意味します。

ログ作成の有効化とログの表示

ホストにインストールされている ESX ゲスト イントロスペクション モジュール VIB のバージョンを表示するには、`#esxcli software vib list | grep epsec-mux` コマンドを実行します。

完全なログ作成を有効にするには、ESXi ホストのコマンド シェルで次の手順を実行します。

- 1 `ps -c | grep Mux` コマンドを実行して、現在実行中の ESX ゲスト イントロスペクション モジュールを検索します。

次はその例です。

```
~ # ps -c | grep Mux
192223 192223 sh /bin/sh /sbin/watchdog.sh -s vShield-Endpoint-Mux -q 100 -t
1000000 /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192233 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
192236 192233 vShield-Endpoint-Mux /usr/lib/vmware/vShield-Endpoint-Mux 900 -c 910
```

- 2 サービスが実行されていない場合、`/etc/init.d/vShield-Endpoint-Mux start` または `/etc//init.d/vShield-Endpoint-Mux restart` コマンドを実行すると、サービスを再起動できます。
- 3 watchdog.sh プロセスなど、実行中の ESX ゲスト イントロスペクション モジュールのプロセスを停止するには、`~ # kill -9 192223 192233 192236` コマンドを実行します。
ESX ゲスト イントロスペクション モジュールの 2 つのプロセスが生成されています。
- 4 新しい `-d` オプションを使用して ESX ゲスト イントロスペクション モジュールを開始します。epsec-mux ビルド 5.1.0-01255202 と 5.1.0-01814505 の `~ # /usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910` には `-d` オプションがありません。
- 5 ESXi ホストの `/var/log/syslog.log` ファイルで、ESX ゲスト イントロスペクション モジュールのログメッセージを確認します。グローバル ソリューション、ソリューション ID、ポート番号に対応するエントリが正しく指定されていることを確認します。

例 : muxconfig.xml ファイルのサンプル

```
<?xml version="1.0" encoding="UTF-8"?>
<EndpointConfig>
  <InstalledSolutions>
    <Solution>
      <id>100</id>
      <ipAddress>xxx.xxx.xxx.xxx</ipAddress>
      <listenOn>ip</listenOn>
      <port>48655</port>
      <uuid>42383371-3630-47b0-8796-f1d9c52ab1d0</uuid>
      <vmxPath>/vmfs/volumes/7adf9e00-609186d9/EndpointService (216)/EndpointService
(216).vmx</vmxPath>
    </Solution>
    <Solution>
```

```

<id>102</id>

<ipAddress>xxx.xxx.xxx.xxx</ipAddress>

<listenOn>ip</listenOn>

<port>48651</port>

<uuid>423839c4-c7d6-e92e-b552-79870da05291</uuid>

<vmxPath>/vmfs/volumes/7adf9e00-609186d9/apoon/EndpointSVM-alpha-01/EndpointSVM-
alpha-01.vmx</vmxPath>

</Solution>

<Solution>

  <id>6341068275337723904</id>

  <ipAddress>xxx.xxx.xxx.xxx</ipAddress>

  <listenOn>ip</listenOn>

  <port>48655</port>

  <uuid>42388025-314f-829f-2770-a143b9cbd1ee</uuid>

  <vmxPath>/vmfs/volumes/7adf9e00-609186d9/DlpService (1)/DlpService (1).vmx</vmxPath>

</Solution>

</InstalledSolutions>

<DefaultSolutions/>

<GlobalSolutions>

  <solution>

    <id>100</id>

    <tag></tag>

    <order>0</order>

  </solution>

  <solution>

    <id>102</id>

    <tag></tag>

    <order>10000</order>

```

```

</solution>

<solution>

  <id>6341068275337723904</id>

  <tag></tag>

  <order>10001</order>

</solution>

</GlobalSolutions>

</EndpointConfig>

```

ゲスト イントロスペクション シン エージェントのログ

シン エージェントは、仮想マシンのゲスト OS にインストールされ、ユーザー ログインの詳細を検出します。

ログのパスとサンプル メッセージ

シン エージェントは、ゲスト イントロスペクション ドライバの vsepflt.sys、vnetflt.sys、vnetwfp.sys (Windows 10 以降) で構成されます。

シン エージェントのログは、vCenter Server のログ バンドルの一部として、ESXi ホストに保存されます。ログのパスは、/vmfs/volumes/<datastore>/<vmname>/vmware.log です。

例： /vmfs/volumes/5978d759-56c31014-53b6-1866abaace386/Windows10-(64-bit)/vmware.log

シン エージェントのメッセージは、<timestamp> <VM Name><Process Name><[PID]>: <message> の形式で記録されます。

以下の **Guest: vnet** or **Guest:vsep** のログの例では、ゲスト イントロスペクション ドライバ関連のログメッセージの後にデバッグ メッセージが続きます。

次はその例です。

```

2017-10-17T14:25:19.877Z| vcpu-0| I125: Guest: vnet: AUDIT: DriverEntry :
  vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| I125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| I125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| I125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\Windows\System32\Tasks\Microsoft\Windows\
SoftwareProtectionPlatform\SvcRestartTask) in a transaction, ignore

```

例：vShield ゲスト イントロスペクション シン エージェント ドライバのログ作成を有効にする

デバッグを設定すると、vmware.log ファイルがいっぱいになり、調整（スロットル）が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

この手順では、Windows レジストリを変更する必要があります。レジストリを変更する前に、レジストリのバックアップを行ってください。レジストリのバックアップとリストアの詳細については、Microsoft 社のナレッジベースの記事 [136393](#) を参照してください。

シン エージェント ドライバのデバッグ ログの作成を有効にするには：

- 1 [スタート(Start)] > [ファイル名を指定して実行(Run)] の順にクリックします。regedit と入力して、[OK] をクリックします。レジストリ エディターのウィンドウが開きます。詳細については、Microsoft 社のナレッジベースの記事 [256986](#) を参照してください。
- 2 レジストリ エディターで
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt\parameters
キーを作成します。
- 3 新しく作成したパラメータ キーの下に、次の DWORD を作成します。これらの値を入力するときに、16 進数が選択されていることを確認します。

```
Name: log_dest
Type: DWORD
Value: 0x2
```

```
Name: log_level
Type: DWORD
Value: 0x10
```

log_level パラメータ キーの他の値：

```
Audit 0x1
Error 0x2
Warn 0x4
Info 0x8
Debug 0x10
```

- 4 管理者としてコマンド プロンプトを開きます。次のコマンドを実行して、vShield Endpoint ファイル システム ミニドライバをアンロードし、再ロードします。

- fltmc unload vsepflt
- fltmc load vsepflt

仮想マシンにある vmware.log ファイルでログ エントリを確認できます。

vShield ゲスト イントロスペクション ネットワーク イントロスペクション ドライバのログインを有効にする

デバッグを設定すると、vmware.log ファイルがいっぱいになり、調整が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

この手順では、Windows レジストリを変更する必要があります。レジストリを変更する前に、レジストリのバックアップを行ってください。レジストリのバックアップとリストアの詳細については、Microsoft 社のナレッジベースの記事 [136393](#) を参照してください。

- 1 [スタート(Start)] > [ファイル名を指定して実行(Run)] の順にクリックします。regedit と入力して、[OK] をクリックします。レジストリ エディターのウィンドウが開きます。詳細については、Microsoft 社のナレッジベースの記事 [256986](#) を参照してください。
- 2 レジストリを編集します。

```
Windows Registry Editor Version 5.0
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\vnetflt\Parameters]
"log_level" = DWORD: 0x0000001F
"log_dest" = DWORD: 0x00000001
```

- 3 仮想マシンを再起動します。

vsepfilt.sys と vnetflt.sys のログ ファイルの場所

レジストリで log_dest が DWORD: 0x00000001 に設定されているため、エンドポイント シン エージェント ドライバのログがデバッグに出力されます。デバッグ (SysInternals の DbgView または windbg) を実行します。

あるいは、レジストリで log_dest を DWORD:0x00000002 に設定することもできます。この場合、ドライバ ログは vmware.log に出力されます。このファイルは、ESXi ホストの該当する仮想マシンのフォルダに保存されます。

UMC のログ作成を有効にする

ゲスト イントロスペクション ユーザー モード コンポーネント (UMC) は、保護対象の仮想マシンの VMware Tools サービス内で実行されます。

- 1 Windows XP または Windows Server 2003 で、**C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf** に **tools config** ファイルが見つからない場合、このファイルを作成します。
- 2 Windows Vista、Windows 7 または Windows Server 2008 で、**C:\ProgramData\VMware\VMware Tools\tools.conf** に **tools config** がみつからない場合、このファイルを作成します。
- 3 次の行を **tools.conf** ファイルに追加して、ユーザー モード コンポーネントのロギングを有効にします。

```
[logging]
log = true
vsep.level = debug
vsep.handler = vmx
```

`vsep.handler = vmx` が設定されているため、ユーザー モード コンポーネントのログは `vmware.log` に出力されます。このファイルは、ESXi ホストで該当する仮想マシンのフォルダにあります。

次の設定を行うと、指定したログ ファイルにユーザー モード コンポーネントのログが出力されます。

```
vsep.handler = file
vsep.data = c:/path/to/vsep.log
```

ゲスト イントロスペクション EPSecLib とサービス仮想マシンのログ

EPSecLib は、ESXi ホストの ESX ゲスト イントロスペクション モジュール (MUX) からイベントを受信します。

ログのパスとサンプル メッセージ

EPSecLib のログのパス

`/var/log/syslog`

`var/run/syslog`

EPSecLib メッセージは、`<timestamp> <VM Name><Process Name><[PID]>: <message>` の形式で記録されます。

この例の `[ERROR]` はメッセージのタイプを表し、`(EPSEC)` は、ゲスト イントロスペクション関連のメッセージであることを表しています。

次はその例です。

```
Oct 17 14:26:00 endpoint-virtual-machine EPSecTester[7203]: [NOTICE] (EPSEC)
[7203] Initializing EPSec library build: build-00000

Oct 17 14:37:41 endpoint-virtual-machine EPSecSample: [ERROR] (EPSEC) [7533] Event
terminated reading file. Ex: VFileGuestEventTerminated@tid=7533: Event id: 3554.
```

ログの収集

ゲスト イントロスペクション サービス仮想マシン内にあるコンポーネントの EPSec ライブラリでデバッグ ログを有効にするには：

- 1 NSX Manager からのコンソールのパスワードを取得して、ゲスト イントロスペクション サービス仮想マシンにログインします。
- 2 `/etc/epseclib.conf` ファイルを作成して、次の項目を追加します。

`ENABLE_DEBUG=TRUE`

`ENABLE_SUPPORT=TRUE`
- 3 `chmod 644 /etc/epseclib.conf` コマンドを実行して権限を変更します。

- 4 `/usr/local/sbin/rcusvm restart` コマンドを実行して、ゲスト イントロスペクション サービス仮想マシンを再起動します。

これにより、ゲスト イントロスペクション サービス仮想マシンで EPSecLib のデバッグ ログが有効になります。NSX for vSphere 6.2.x と 6.3.x の場合、デバッグ ログは `/var/log/messages` に保存されます。デバッグを設定すると、`vmware.log` ファイルがいっぱいになり、調整が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグ モードを無効にすることをお勧めします。

ゲスト イントロスペクション サービス仮想マシンのログ

ログをキャプチャする前に、ホスト ID またはホストの MOID を確認します。

- NSX Manager で `show cluster all` コマンドと `show cluster <cluster ID>` コマンドを実行します。

次はその例です。

```
nsxmgr-01a> show cluster all
```

No.	Cluster Name	Cluster Id	Datacenter Name	Firewall Status
1	RegionA01-COMP01	domain-c26	RegionA01	Enabled
2	RegionA01-MGMT01	domain-c71	RegionA01	Enabled

```
nsxmgr-01a> show cluster domain-c26
```

Datacenter: RegionA01
Cluster: RegionA01-COMP01

No.	Host Name	Host Id	Installation Status
1	esx-01a.corp.local	host-29	Ready
2	esx-02a.corp.local	host-31	Ready

- 1 現在のログの状態を確認するには、次のコマンドを実行します。

```
GET https://nsxmanager/api/1.0/usvmlogging/host-  
##/com.vmware.vshield.usvm
```

```
GET https://nsxmanager/api/1.0/usvmlogging/host-##/root
```

- 2 現在のログの状態を変更するには、次のコマンドを実行します。

```
POST https://nsxmanager/api/1.0/usvmlogging/host-##/changelevel
```

```
## Example to change root logger ##

<?xml version="1.0" encoding="UTF-8" ?>
<logginglevel>
<loggerName>root</loggerName>
<level>DEBUG</level>
</logginglevel>

## Example to change com.vmware.vshield.usvm ##

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

```
<logginglevel>  
<loggerName>com.vmware.vshield.usvm</loggerName>  
<level>DEBUG</level>  
</logginglevel>
```

- 3 ログを生成するには、次のコマンドを実行します。

GET https://NSXMGR_IP/api/1.0/hosts/host.###/techsupportlogs

Send と **Download** を選択します。

このコマンドを実行すると、ゲスト イントロスペクション サービス仮想マシンのログが生成され、**techsupportlogs.log.gz** という名前で保存されます。デバッグを設定すると、vmware.log ファイルがいっぱいになり、調整が行われる可能性があります。このため、必要な情報をすべて収集したらすぐにデバッグモードを無効にすることをお勧めします。

システム イベント

NSX のすべてのコンポーネントは、システム イベントをレポートします。これらのイベントは、環境の健全性および安全性の監視や、問題のトラブルシューティングに役立ちます。

各イベント メッセージには次の情報が含まれます。

- 一意のイベント コード
- 重要度
- イベントの説明と、必要な場合は推奨アクション

テクニカル サポート ログの収集および VMware サポートへの問い合わせ

一部のイベントでは、テクニカル サポート ログの収集と、VMware サポートへの問い合わせが推奨される場合があります。

- NSX Manager のテクニカル サポート ログを収集するには、[「NSX のテクニカル サポート ログのダウンロード」](#)を参照してください。
- NSX Edge のテクニカル サポート ログを収集するには、[「NSX Edge のテクニカル サポート ログのダウンロード」](#)を参照してください。
- ホストのテクニカル サポート ログを収集するには、コマンド **export host-tech-support** を実行します。『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。
- VMware サポートにお問い合わせいただくには、「How to file a Support Request in My VMware」(<http://kb.vmware.com/kb/2006985>) を参照してください。

NSX Edge での強制同期の実行

一部のイベントでは、NSX Edge への強制同期が推奨されることがあります。詳細については、『NSX 管理ガイド』の「NSX Edge と NSX Manager の強制同期」を参照してください。強制同期では、NSX Edge 仮想マシンの停止と再起動を行います。

システム イベントの重要度レベル

各イベントには次のいずれかの重要度レベルがあります。

- 情報
- 低
- 中
- メジャー
- 重大
- 高

次のトピックでは、さまざまなコンポーネントで発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

この章には、次のトピックが含まれています。

- [セキュリティ システム イベント](#)
- [分散ファイアウォール システム イベント](#)
- [NSX Edge システム イベント](#)
- [ファブリック システム イベント](#)
- [デプロイ プラグインのシステム イベント](#)
- [メッセージング システム イベント](#)
- [Service Composer システム イベント](#)
- [ゲスト イン트로スペクション サービス仮想マシンのシステム イベント](#)
- [サービス仮想マシン \(SVM\) 運用システム イベント](#)
- [レプリケーション - ユニバーサル同期システム イベント](#)
- [NSX 管理システム イベント](#)
- [論理ネットワークのシステム イベント](#)
- [Identity Firewall システム イベント](#)
- [ホストの準備のシステム イベント](#)

セキュリティ システム イベント

ここでは、セキュリティで発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの重要度	アラームのト リガ	イベント メッセージ	説明
11002	重大	いいえ	vCenter Server に接続できません。名前またはパスワードが不正です。	vCenter Server の設定に失敗しました。 アクション：vCenter Server の設定が正しく、正しい認証情報を使用していることを確認してください。『NSX 管理ガイド』の「NSX Manager への vCenter Server の登録」と『NSX トラブルシューティング ガイド』の「NSX Manager と vCenter Server の接続」を参照してください。
11006	重大	いいえ	vCenter Server 接続を失いました。	vCenter Server への接続が切れました。 アクション：vCenter Server との接続の問題があるかどうかを確認してください。『NSX トラブルシューティング ガイド』の「NSX Manager と vCenter Server の接続」および「NSX Manager の問題のトラブルシューティング」を参照してください。
230000	重大	いいえ	NSX Manager 上の SSO 設定タスクが失敗しました。	Single Sign On (SSO) の設定に失敗しました。認証情報が無効、設定が無効、時刻が同期されていない、などの原因が考えられます。 アクション：エラー メッセージを確認して、SSO を設定してください。『NSX 管理ガイド』の「シングルサインオン」を参照してください。また、『NSX トラブルシューティング ガイド』の「NSX SSO Lookup Service の設定の失敗」も参照してください。
230002	重大	いいえ	SSO STS クライアントが切断されました。	SSO サービスへの NSX Manager の登録に失敗したか、SSO サービスとの接続が切断されています。 アクション：認証情報が無効、同期していない、ネットワーク接続に問題があるなど、設定に問題がないかどうかを確認してください。また、製品の技術的な問題が原因でこの問題が発生することがあります。ナレッジベースの記事「SSL certificate of the STS service cannot be verified」(http://kb.vmware.com/kb/2121696) と「Registering NSX Manager to Lookup Service with External Platform Service Controller (PSC) fails with the error: server certificate chain not verified」(http://kb.vmware.com/kb/2132645) を参照してください。
240000	重大	いいえ	認証ブラック リストにエントリ {0} が追加されました。	特定の IP アドレスのユーザーが 10 回連続してログインに失敗しました。このユーザーは 30 分間ロックアウトされます。 アクション：潜在的なセキュリティ問題を調査してください。

分散ファイアウォール システム イベント

ここでは、分散ファイアウォールで発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301001	重大	いいえ	ホストでフィルタ設定の更新に失敗しました。	<p>ホストでフィルタ設定を受信または解析できなかったか、端末の <code></dev/dvfiltertbl></code> を開くことができませんでした。</p> <p>アクション：コンテキストのキー バリユー ペアと、エラーの原因を確認してください。NSX Manager と準備済みのホストとの間で VIB のバージョンが異なっているために、予期しないアップグレードの問題が発生している可能性があります。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。</p>
301002	メジャー	いいえ	フィルタ設定が vNIC に適用されませんでした。	<p>フィルタ設定を vNIC に適用できませんでした。</p> <p>可能性のある原因：フィルタ設定の開放、解析、更新処理に失敗しました。このエラーは、分散ファイアウォールでは発生しませんが、Network Extensibility (NetX) で発生する可能性があります。</p> <p>アクション：ESXi および NSX Manager のテクニカル サポート バンドルを収集して、VMware テクニカル サポートにお問い合わせください。</p>
301031	重大	いいえ	ホスト上でファイアウォール設定の更新に失敗しました。	<p>ファイアウォール設定の受信、解析、更新処理に失敗しました。キー バリユーには、生成番号などのコンテキスト情報や、その他のデバッグ情報が含まれます。</p> <p>アクション：手順に沿ってホストを準備していたかどうか確認してください。ホストにログインし、<code>/var/log/vsfwd.log</code> ファイルを収集してから、API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> を使用してファイアウォールの設定を強制的に同期します。『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。強制的に同期しても、ホスト上の分散ファイアウォール設定を更新できない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。</p>
301032	メジャー	いいえ	ファイアウォール ルールを vNIC に適用できませんでした。	<p>ファイアウォール ルールを vNIC に適用できませんでした。</p> <p>アクション：vsip カーネル ヒープに十分な空きメモリ容量があることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリ しきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。ファイアウォールの設定が vNIC に適用されたことをホストのログ (<code><vmkernel.log></code> および <code><vsfwd.log></code>) で確認してください。</p>

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301041	重大	いいえ	ホストでコンテナ設定の更新に失敗しました。	<p>ネットワークとセキュリティ コンテナの設定に関する処理に失敗しました。キー バリューには、コンテナ名や生成番号などのコンテキスト情報が含まれます。</p> <p>アクション：vsip カーネル ヒープに十分な空きメモリ容量があることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリしきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。コンテナの設定が vNIC に適用されたことをホストのログ (<vmkernel.log> および <vsfwd.log>) で確認してください。</p>
301051	メジャー	いいえ	ホストでフローが失われました。	<p>保護対象の仮想マシンとの間で、1 つまたは複数のセッションのフロー データがドロップされたため、読み取りまたは NSX Manager への送信に失敗しました。</p> <p>アクション：vsip カーネル ヒープに十分な空きメモリ容量があり、vsfwd メモリ使用量がリソースの制限内であることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリしきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。</p>
301061	重大	いいえ	ホストで Spoofguard 設定更新に失敗しました。	<p>SpoofGuard に関連する設定に失敗しました。</p> <p>アクション：手順に沿ってホストを準備していたかどうか確認してください。ホストにログインし、<var/log/vsfwd.log> ファイルを収集してから、API <https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>> を使用してファイアウォールの設定を強制的に同期します。『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。SpoofGuard の設定が引き続き失敗する場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。ホストが SpoofGuard の設定を受信したことをログで確認してください。</p>

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301062	メジャー	いいえ	Spoofguard を vNIC に適用できませんでした。	SpoofGuard を vNIC に適用できませんでした。 アクション：手順に沿ってホストを準備していたかどうか確認してください。ホストにログインし、 <code>/var/log/vsfd.log</code> ファイルを収集してから、API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> を使用してファイアウォールの設定を強制的に同期します。『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。SpoofGuard の設定が引き続き失敗する場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301064	メジャー	いいえ	vNIC の Spoofguard を無効にできませんでした。	vNIC で SpoofGuard を無効にできませんでした。 アクション：NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301072	重大	いいえ	レガシーの App サービス仮想マシンの削除に失敗しました。	vCloud Networking and Security 用の vShield App サービス仮想マシンを削除できませんでした。 アクション：『NSX アップグレード ガイド』の「vShield App から分散ファイアウォールへのアップグレード」に記載されている手順をご確認ください。
301080	重大	いいえ	ファイアウォールの CPU しきい値が超過しました。	vsfd の CPU 使用率がしきい値を超えました。 アクション：『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリしきい値イベントの表示」を参照してください。場合によっては、ホストのリソース使用率を低くする必要があります。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301081	重大	いいえ	ファイアウォールのメモリしきい値が超過しました。	vsfd のメモリ使用率がしきい値を超えました。 アクション：『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリしきい値イベントの表示」を参照してください。場合によっては、ホストのリソース使用率を低くする必要があります。また、設定されているファイアウォール ルールの数や、ネットワークとセキュリティ コンテナの数を削減します。ファイアウォール ルールの数を削減するには、 appliedTo 機能を使用します。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301082	重大	いいえ	ファイアウォールの 1 秒あたりの 接続数がしきい値を超過しまし た。	1 秒あたりのファイアウォール接続のしきい値を超えま した。 アクション：『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリしきい値イベントの表示」 を参照してください。場合によっては、ホストのリソー ス使用率を低くする必要があります。ホスト上の仮想マ シンとの間のアクティブな接続数を削減します。
301501	重大	いいえ	ホスト {hostID} へのファイ アウォール設定の更新バージョン {version#} がタイムアウトし ました。ホストでのファイアウォ ール設定は、バージョン {version#} まで同期されま す。	ホストでのファイアウォール設定の更新に 2 分以上か かったので、更新がタイムアウトになりました。 アクション：vsfwd が機能していて、ホストにルール が発行されていることを確認してください。『NSX トラ ブルシューティング ガイド』の「分散ファイアウォ ールのトラブルシューティング」を参照してください。問 題が解決しない場合は、NSX Manager とホストのテク ニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301502	重大	いいえ	ホスト {hostID} への Spoofguard 設定更新番号 {number#} がタイムアウトしま した。ホストでの Spoofguard 設定は、バージョン {version#} まで同期されま す。	ホストでの SpoofGuard 設定の更新に 2 分以上かかっ たので、更新がタイムアウトになりました。 アクション：vsfwd が機能していて、ホストにルール が発行されていることを確認してください。『NSX トラ ブルシューティング ガイド』の「分散ファイアウォ ールのトラブルシューティング」を参照してください。問 題が解決しない場合は、NSX Manager とホストのテク ニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301503	重大	いいえ	ファイアウォール設定バージョン {version#} をクラスタ {clusterID} に発行できま せんでした。詳細については、ログ を参照してください。	1 つのクラスタまたは 1 台以上のホストで、ファイ アウォール ルールの発行に失敗しました。 アクション：『NSX トラブルシューティング ガイド』 の「分散ファイアウォールのトラブルシューティング」 を参照してください。問題が解決しない場合は、 NSX Manager とホストのテクニカル サポート ログを 収集して、VMware テクニカル サポートにお問い合わせ ください。
301504	重大	いいえ	コンテナ更新をクラスタ {clusterID} に発行できま せんでした。詳細については、ロ グを参照してください。	1 つのクラスタまたは 1 台以上のホストで、ネットワ ークとセキュリティ コンテナの更新の発行に失敗しました。 アクション：『NSX トラブルシューティング ガイド』 の「分散ファイアウォールのトラブルシューティング」 を参照してください。問題が解決しない場合は、 NSX Manager とホストのテクニカル サポート ログを 収集して、VMware テクニカル サポートにお問い合わせ ください。

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301505	重大	いいえ	Spoofguard 更新をクラスター {clusterID} に発行できませんでした。詳細については、ログを参照してください。	1 つのクラスターまたは 1 台以上のホストで、SpoofGuard の更新の発行に失敗しました。 アクション：『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301506	重大	いいえ	除外リスト更新をクラスター {clusterID} に発行できませんでした。詳細については、ログを参照してください。	1 つのクラスターまたは 1 台以上のホストで、除外リストの更新の発行に失敗しました。 アクション：『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301508	重大	いいえ	ホスト {hostID} を同期できませんでした。詳細については、ログを参照してください。	API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> によるファイアウォールの強制同期に失敗しました。 アクション：『NSX トラブルシューティング ガイド』の「分散ファイアウォールのトラブルシューティング」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301510	重大	いいえ	クラスターで強制同期が失敗しました。	API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> によるファイアウォールの強制同期に失敗しました。 アクション：NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301512	メジャー	いいえ	ファイアウォールがホスト {hostID} [{hostID}] にインストールされました。	分散ファイアウォールがホストに正常にインストールされました。 アクション：vCenter Server で [ホーム] - [Networking and Security] - [インストール] の順に移動し、[ホストの準備] タブを選択してください。[ファイアウォール ステータス] が緑色で表示されることを確認します。
301513	メジャー	いいえ	ファイアウォールがホスト {hostID} [{hostID}] にアンインストールされました。	分散ファイアウォールがホストからアンインストールされました。 分散ファイアウォール コンポーネントのアンインストールに失敗する場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301514	重大	いいえ	クラスタ {clusterID} のファイアウォールは有効です。	分散ファイアウォールがクラスタに正常にインストールされました。 アクション：vCenter Server で [ホーム] - [Networking and Security] - [インストール] の順に移動し、[ホストの準備] タブを選択してください。[ファイアウォール ステータス] が緑色で表示されることを確認します。
301515	重大	いいえ	ファイアウォールがクラスタ {clusterID} でアンインストールされました。	分散ファイアウォールがクラスタからアンインストールされました。 アクション：分散ファイアウォール コンポーネントのアンインストールに失敗する場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301516	重大	いいえ	クラスタ {clusterID} のファイアウォールは無効です。	分散ファイアウォールがクラスタ内のすべてのホストで無効になりました。 アクション：必要ありません。
301034	メジャー	いいえ	ファイアウォール ルールをホストに適用できませんでした。	分散ファイアウォール ルール セクションの適用に失敗しました。 アクション：vsip カーネル ヒープに十分な空きメモリ容量があることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリ しきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301043	重大	いいえ	コンテナ設定を vNIC に適用できませんでした。	ネットワークとセキュリティ コンテナの設定を適用できませんでした。 アクション：vsip カーネル ヒープに十分な空きメモリ容量があることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリ しきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301044	重大	いいえ	コンテナ設定をホストに適用できませんでした。	ネットワークとセキュリティ コンテナの設定を適用できませんでした。 アクション：vsip カーネル ヒープに十分な空きメモリ容量があることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリ しきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301066	メジャー	いいえ	SpoofGuard 設定をホストに適用できませんでした。	Spoofguard を vNIC に適用できませんでした。 アクション：vsip カーネル ヒープに十分な空きメモリ容量があることを確認してください。『NSX 管理ガイド』の「ファイアウォール CPU イベントおよびメモリしきい値イベントの表示」を参照してください。問題が解決しない場合は、NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
301100	重大	いいえ	ホストでファイアウォール タイムアウト設定の更新に失敗しました。	ファイアウォール セッション タイマーのタイムアウト設定を更新できませんでした。 アクション：NSX Manager とホストのテクニカル サポート ログを収集して、VMware サポートにお問い合わせください。ログを収集したら、ファイアウォール設定を強制同期します。それには、REST API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> を使用するか、[インストール手順] - [ホストの準備] の順に移動し、[アクション] で [サービスの強制同期] を選択します。
301101	メジャー	いいえ	ファイアウォール タイムアウト設定を vNIC に適用できませんでした。	ファイアウォール セッション タイマーのタイムアウト設定を更新できませんでした。 アクション：NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。ログを収集したら、ファイアウォール設定を強制同期します。それには、REST API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> を使用するか、[インストール手順] - [ホストの準備] の順に移動し、[アクション] で [サービスの強制同期] を選択します。
301103	メジャー	いいえ	ファイアウォール タイムアウト設定をホストに適用できませんでした。	ファイアウォール セッション タイマーのタイムアウト設定を更新できませんでした。 アクション：NSX Manager とホストのテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。ログを収集したら、ファイアウォール設定を強制同期します。それには、REST API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> を使用するか、[インストール手順] - [ホストの準備] の順に移動し、[アクション] で [サービスの強制同期] を選択します。
301200	メジャー	いいえ	アプリケーション ルール マネージャのフロー分析が開始されました。	アプリケーション ルール マネージャのフロー分析が開始されました。 アクション：必要ありません。

イベント コード	イベントの重 要度	アラームをト リガ	イベント メッセージ	説明
301201	メジャー	いいえ	アプリケーション ルール マネージャ のフロー分析が失敗しました。	アプリケーション ルール マネージャのフロー分析に失敗しました。 アクション：NSX Manager のテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。失敗したセッションと同じ vNIC で新しい監視セッションを開始し、再度操作を試みます。
301202	メジャー	いいえ	アプリケーション ルール マネージャ のフロー分析が完了しました。	アプリケーション ルール マネージャのフロー分析が完了しました。 アクション：必要ありません。

NSX Edge システム イベント

ここでは、NSX Edge で発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。このようなイベントでアラームが発生すると、システム イベントの重要度が表示されます。

イベント コード	イベントの重 要度	アラーム コード	イベント メッセージ	説明
30011	高	該当なし	稼働中の Edge が見つかり ません。ネットワークが中断して いる可能性があります。	NSX Edge 仮想マシンは、この状態から自動的にリカバリします。イベントコード 30202 または 30203 のトラップを確認してください。 アクション：『NSX トラブルシューティングガイド』の「Edge アプライアンスのトラブルシューティング」を参照してください。
30013	重大	130013	NSX Manager が NSX Edge (vmId : {#}) の 状態の不整合を検出しました。 強制同期する必要があります。	NSX Edge 仮想マシンの状態に問題があることがレポートされており、適切に機能していない可能性があります。 アクション：問題のある状態が検出されると、自動的に強制同期が始まります。自動での強制同期に失敗した場合は、手動で強制同期を適用してください。
30014	メジャー	該当なし	NSX Edge と通信できません でした。	NSX Manager は、VIX またはメッセージ バスを介して NSX Edge と通信します。NSX Manager によってこの通信チャンネルが選択されます。これは、Edge のデプロイまたは再デプロイ時に、ホストの準備が完了しているかどうかに基づいて決定されます。このイベントは、NSX Manager と NSX Edge の通信が切断されていることを示しています。 アクション：『NSX トラブルシューティングガイド』の「Edge アプライアンスのトラブルシューティング」を参照してください。
30027	情報	130027	NSX Edge (vmId : {#}) がパワーオフされました。	NSX Edge 仮想マシンがパワーオフされました。 アクション：情報通知のイベントです。
30032	高	130032	仮想マシン ID が {#} の NSX Edge アプライアンスが vCenter Server インベ ントリ内に見つかりません。	NSX Edge 仮想マシンが、vCenter Server から直接削除された可能性があります。この操作はサポートされていません。NSX の管理対象オブジェクトは、vSphere Web Client の NSX 用インターフェイスを使用して追加または削除する必要があるためです。 アクション：Edge を再デプロイするか、新しい Edge をデプロイしてください。

イベント コード	イベントの重 要度	アラーム コード	イベント メッセージ	説明
30033	高	130033	vCenter Server インベ ントリに仮想マシン ID (vmId : {#}) が見つかり ません。	NSX Edge 仮想マシンが vCenter Server のインベントリにあ りません。 アクション：仮想マシンが誤って削除されていないか確認して ください。確認するには、Edge を再デプロイします。
30034	重大	130034	稼働中の Edge が見つかり ません。ネットワークが中断して いる可能性があります。	Edge 仮想マシンが、NSX Manager によって送信された健全 性チェックに応答していません。 アクション：Edge 仮想マシンが起動していることを確認して ください。Edge ログを収集して、VMware テクニカル サポート にお問い合わせください。
30037	重大	該当なし	{#} に変更された Edge ファイアウォール ルールは、{#} に使用できなくなりました。	ファイアウォール ルールに無効な GroupingObject (IPSet、 securityGroup など) が含まれています。 アクション：ファイアウォール ルールを再確認して、必要に応 じて更新を行ってください。
30038	重大	該当なし	NSX Edge アプライアンスが 起動しました。{EdgeId #}、{vmName #} は、仮想 マシンの非アフィニティ ルールに 違反しています。	NSX Edge 高可用性では、アクティブ Edge 仮想マシンとスタ ンバイ Edge 仮想マシンが別々のホストに展開されるため、 vSphere ホストに対して自動的に非アフィニティ ルールを適 用します。このイベントは、これらの非アフィニティ ルールが クラスタから削除され、両方の Edge 仮想マシンが同じホスト 上で稼働していることを示しています。 アクション：vCenter Server で非アフィニティ ルールを確認 してください。
30045	重大	該当なし	NSX Edge 仮想マシンの健 全性チェックが重大な VIX エ ラーで失敗しました。健全性 チェックを再開するには、仮想マ シンを再デプロイするか強制的 に同期してください。	ネットワーク環境が原因となり、VIX チャネル経由での通信障 害が Edge 仮想マシンで繰り返し発生している可能性があります。 アクション：NSX Edge からの応答がある場合は、 NSX Manager と NSX Edge のテクニカル サポート ログを収 集してから、強制的に同期してください。この問題が解決しな い場合は、NSX Edge を再デプロイしてください。『NSX 管理 ガイド』の「NSX Edge の再デプロイ」を参照してください。 注： 再デプロイを行う場合は、サービスを停止する必要があります。まず強制的に同期し、問題が解決しない場合に再デプロ イを行うことをお勧めします。
30046	重大	該当なし	事前ルールの発行が {EdgeID#}、仮想マシン： {#}、世代番号 {#} で失 敗しました。詳細はログを参照 してください。詳細はログを参照 してください。強制同期が必要 な場合があります。	NSX Edge のファイアウォール ルールが同期されていない可能 性があります。このエラーは事前ルール（分散ファイアウォ ールのユーザー インターフェイスまたは API で設定）でエラーが 発生した場合に生成されます。 アクション：組み込みのリカバリ プロセスで自動的に問題が解 決しない場合は、手動で強制的に同期してください。
30100	重大	該当なし	NSX Edge は強制的に同期 されました	NSX Edge 仮想マシンが強制的に同期されました。 アクション：強制同期を行っても問題が解決しない場合は、 NSX Manager と NSX Edge のテクニカル サポート ログを収 集して、VMware テクニカル サポートにお問い合わせください。

イベント コード	イベントの重 要度	アラーム コード	イベント メッセージ	説明
30102	高	130102	NSX Edge (vmId : {IP Address}) の状態の不整合を検出しました。強制同期する必要があります。	NSX Edge 仮想マシンで内部エラーが発生しています。 アクション：組み込みのリカバリ プロセスで自動的に問題が解決されない場合は、手動で強制的に同期してください。
30148	重大	該当なし	NSX Edge CPU 使用量が増加しました。{#} 上位のプロセス: {#}。	NSX Edge 仮想マシンの CPU 使用率が高い状態が一定期間続いています。 アクション：『NSX トラブルシューティングガイド』の「Edge アプライアンスのトラブルシューティング」を参照してください。問題が解決しない場合は、NSX Manager と NSX Edge のテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
30153	メジャー	該当なし	AESNI 暗号化エンジンが稼動しています。	AESNI 暗号化エンジンが稼動しています。 アクション：必要ありません。
30154	メジャー	該当なし	AESNI 暗号化エンジンが停止しています。	AESNI 暗号化エンジンが停止しています。 アクション：必要ありません。これは想定される動作です。
30155	高	130155	Insufficient CPU and/or Memory Resources available on Host or Resource Pool, during resource reservation at the time of NSX Edge deployment.	ホストまたはリソース プールの CPU またはメモリ リソースが不足しています。 使用可能なリソースと予約済みのリソースを確認するには、[ホーム(Home)]-[ホストおよびクラスタ(Hosts and Clusters)]>[クラスタ名(Cluster-name)]の順に移動し、[モニター(Monitor)]-[リソースの予約(Resource Reservation)]ページの順に移動します。 使用可能なリソースを確認したら、アプライアンスの設定でリソースを再度指定します。この設定は、リソースの予約制限で継承されます。
30180	重大	該当なし	NSX Edge のメモリがなくなりました。この Edge を 3 秒後に再起動します。上位 5 つのプロセス: {#}。	NSX Edge 仮想マシンのメモリが不足しています。リカバリを行うため、再起動が開始されました。 アクション：『NSX トラブルシューティングガイド』の「Edge アプライアンスのトラブルシューティング」を参照してください。問題が解決しない場合は、NSX Manager と NSX Edge のテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
30181	重大	130181	NSX Edge「{EdgeID#}」仮想マシン名「{#}」のファイルシステムは読み取り専用です。	NSX Edge 仮想マシンのバックアップ ストレージ デバイスで接続の問題があります。 アクション：バックアップ データストアで接続の問題があるかどうかを確認し、修正してください。接続の問題が解決した後、場合によっては手動で強制的に同期する必要があります。
30202	メジャー	該当なし	NSX Edge {EdgeID#} HighAvailability の切り替えが発生しました。{#} という名前の仮想マシン {#} は ACTIVE 状態に移行しました。	高可用性フェイルオーバーが発生し、NSX Edge セカンダリ仮想マシンの状態がスタンバイからアクティブに切り替わりました。 アクション：操作は必要ありません。

イベント コード	イベントの重 要度	アラーム コード	イベント メッセージ	説明
30203	メジャー	該当なし	NSX Edge {EdgeID} HighAvailability の切り替えが発生しました。{#} という名前の仮想マシン {#} は STANDBY 状態に移行しました。	高可用性フェイルオーバーが発生し、NSX Edge プライマリ仮想マシンの状態がアクティブからスタンバイに切り替わりました。 アクション：操作は必要ありません。
30205	重大	130205	高可用性が設定された NSX Edge {EdgeID} でスプリット ブレインが検出されました。	ネットワーク障害のため、高可用性設定の NSX Edge 仮想マシンが他の仮想マシンの状態を確認できません。この場合、いずれの仮想マシンも他のマシンがオフラインであると判断し、アクティブ状態に切り替わろうとします。このため、ネットワークに障害が発生する可能性があります。 アクション：ネットワーク インフラストラクチャ（仮想および物理）で障害が発生していないかどうか確認してください。特に、インターフェイスと 高可用性設定のパスを確認してください。
30302	重大	130302	ロード バランサ仮想サーバ/プール {virtualServerName}、プロトコル {#}、サーバ IP アドレス {IP Address} の状態が停止に変わりました。	NSX Edge ロード バランサ上の仮想サーバまたはプールが停止しています。 アクション：『NSX トラブルシューティング ガイド』の「ロード バランシング」セクションを参照してください。
30303	メジャー	該当なし	ロード バランサ仮想サーバ/プール {0}、プロトコル {#}、サーバ IP アドレス {IP Address} の状態が停止に変わりました。	NSX Edge ロード バランサ上の仮想サーバまたはプールで内部エラーが発生しています。 アクション：『NSX トラブルシューティング ガイド』の「ロード バランシング」セクションを参照してください。
30304	メジャー	130304	ロード バランサ プール {0}、プロトコル {#}、サーバ IP アドレス {IP address} が警告状態に変わりました。	NSX Edge ロード バランサのプールの状態が [警告 (warning)] に変わりました。 アクション：『NSX トラブルシューティング ガイド』の「ロード バランシング」セクションを参照してください。
30402	重大	130402	ローカル IP アドレス {IP address} からピア IP アドレス {IP address} への IPsec チャンネルの状態が停止に変わりました。	NSX Edge の IPSec VPN チャンネルが停止しています。 アクション：『NSX トラブルシューティング ガイド』の「Virtual Private Network (VPN)」セクションを参照してください。
30404	重大	130404	EDGE IPSEC TUNNEL DOWN : ローカル サブネット {subnet} からピア サブネット {subnet} への IPsec トンネルの状態が停止に変わりました。	NSX Edge の IPSec VPN チャンネルが停止しています。 アクション：『NSX トラブルシューティング ガイド』の「Virtual Private Network (VPN)」セクションを参照してください。

イベント コード	イベントの重 要度	アラーム コード	イベント メッセージ	説明
30405	メジャー	該当なし	ローカル IP アドレス {IP address} からピア IP アドレス {IP address} への IPsec チャンネルの状態が不明に変わりました。	NSX Edge の IPsec VPN チャンネルの状態を特定できません。 アクション：『NSX トラブルシューティングガイド』の「Virtual Private Network (VPN)」セクションを参照してください。
30406	メジャー	該当なし	ローカル IP アドレス {IP address} からピア IP アドレス {IP address} への IPsec チャンネルの状態が不明に変わりました。	NSX Edge の IPsec VPN チャンネルの状態を特定できません。 アクション：『NSX トラブルシューティングガイド』の「Virtual Private Network (VPN)」セクションを参照してください。
30701	重大	該当なし	外部 DHCP サーバが提供されていないため、エッジ {EdgeID} の NSX Edge DHCP リレー サービスは無効になっています。サーバ IP アドレスまたは参照先のグループオブジェクトを確認してください。	NSX Edge の DHCP リレー サービスが無効です。考えられる理由：(1) DHCP リレー プロセスが稼働していない。(2) 外部の DHCP サーバがない。リレーが参照していたグループオブジェクトの削除が原因になっている可能性があります。 アクション：『NSX 管理ガイド』の「DHCP リレーの設定」を参照してください。
30206	重大	該当なし	高可用性が設定された NSX Edge {EdgeID} でスプリット ブレインが解消されました。	2 台の NSX Edge 高可用性アプライアンスが相互に通信できる状態にあり、アクティブとスタンバイの状態を再ネゴシエートしました。 アクション：「Troubleshooting NSX Edge High Availability (HA) issues」(http://kb.vmware.com/kb/2126560) を参照してください。
30207	重大	該当なし	NSX Edge「{EdgeID}」でスプリット ブレインの解消が {value} 回試行されました。	2 台の NSX Edge 高可用性アプライアンスが再ネゴシエートを試み、スプリット ブレイン状態からリカバリしようとしています。 <u>注：</u> このイベントでレポートされたリカバリ メカニズムは、NSX Edge 6.2.3 より前のバージョンでのみ発生します。 アクション：「Troubleshooting NSX Edge High Availability (HA) issues」(http://kb.vmware.com/kb/2126560) を参照してください。

ファブリック システム イベント

ここでは、ファブリック システム イベントのシステム イベント メッセージについて説明します。

イベント コード	イベントの重 要度	アラームの トリガ	イベント メッセージ	説明
250000	情報	いいえ	デプロイ ユニットの処理状態は {#} ですが、{#} になりました。また、進捗状況は {#} から {#} に変わりました。アラームの内容から根本原因を確認してください。	情報通知のイベントです。
250001	情報	いいえ	A deployment unit has been created.	情報通知のイベントです。
250002	情報	いいえ	NSX のデプロイ ユニットが更新されました。クラスターでファブリック サービスが更新されます。	情報通知のイベントです。
250003	情報	いいえ	NSX からデプロイ ユニットが削除されました。	情報通知のイベントです。
250004	高	はい	展開できませんでした service {#} host {#} でデータストア (#) がホストに接続されていないためです。接続を認するか、別のデータストアを使用してください。	ホストのセキュリティ仮想マシンを格納するデータストアを設定できませんでした。 アクション：ホストがデータストアにアクセスできることを確認してください。
250005	高	はい	デプロイ ユニットのインストールに失敗しました。OVF/VIB URL にアクセス可能で、DNS が設定され、必要なネットワーク ポートが開いていることを確認してください。	ホストへの NSX サービスのインストール中に、ESXi ホストは NSX の VIB/OVF にアクセスできませんでした。vCenter Server システム イベント テーブルに、次のイベント メッセージが表示されます。 Event Message: 'デプロイ ユニットのインストールに失敗しました。Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module:'Security Fabric'. アクション：NSX トラブルシューティング ガイドを参照してください。
250006	情報	いいえ	ネットワーク ファブリック サービスのファブリック エージェントがホストに正常にインストールされました。	情報通知のイベントです。
250007	情報	いいえ	ファブリック エージェントがホストから正常に削除されました。	情報通知のイベントです。
250008	高	はい	OVF / VIB ファイルの場所が変更されました。サービスの再デプロイが必要です。	NSX VIB および OVF は、URL を介して利用できますが、URL は、NSX のバージョンが変わると変更されます。正しい VIB を見つけるには、次の URL に移動します。<https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties>NSX Manager の IP アドレスが変更されると、NSX OVF または VIB の再デプロイが必要になる場合があります。 アクション：[ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決してください。

イベント コード	イベントの重 要度	アラームの トリガ	イベント メッセージ	説明
250009	高	はい	デプロイ ユニットのアップグレードに失敗しました。OVF/VIB URL にアクセス可能で、DNS が設定され、必要なネットワーク ポートが開いていることを確認してください。	ホストのアップグレード中に、ESX Agent Manager (EAM) は NSX からの VIB/OVF にアクセスできませんでした。vCenter Server システム イベント テーブルに、次のイベント メッセージが表示されます。 Event Message: 'デプロイ ユニットのアップグレードに失敗しました。Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module:'Security Fabric'. アクション: NSX トラブルシューティング ガイド を参照してください。
250012	高	はい	サービス「{#}」が機能するためには、以下のサービスが正しくインストールされている必要があります: {#}	インストールするサービスは、まだインストールされていない別のサービスに依存します。 アクション: 必要なサービスをクラスタにデプロイしてください。
250014	高	はい	アップグレード前のセキュリティ ソリューションの通知中にエラーが発生しました。ソリューションにアクセスできない、またはソリューションが応答していない可能性があります。NSX からソリューションの URL にアクセスできることを確認してください。解決用の API を使用してアラームを解決してください。サービスは再度展開されます。	アップグレード前のセキュリティ ソリューションの通知中にエラーが発生しました。ソリューションにアクセスできない、またはソリューションが応答していない可能性があります。 アクション: NSX からソリューションの URL にアクセスできることを確認してください。 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。サービスが再デプロイされます。
250015	高	はい	タイムアウト後もアップグレード通知に関するセキュリティ ソリューションのコールバックを受信しませんでした。NSX からソリューションの URL にアクセスできること、およびソリューションから NSX にアクセスできることを確認してください。解決用の API を使用してアラームを解決してください。サービスは再度展開されます。	Did not receive callback from security solution for upgrade notification even after timeout. アクション: NSX からソリューションの URL にアクセスできること、およびソリューションから NSX にアクセスできることを確認してください。 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
250016	高	いいえ	サービスのアンインストールに失敗しました。NSX からソリューションの URL にアクセスできること、およびソリューションから NSX にアクセスできることを確認してください。解決用の API を使用してアラームを解決してください。サービスは削除されます。	Uninstallation of service failed. アクション: NSX からソリューションの URL にアクセスできること、およびソリューションから NSX にアクセスできることを確認してください。 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。

イベント コード	イベントの重 要度	アラームの トリガ	イベント メッセージ	説明
250017	高	はい	アンインストール前のセキュリティ ソリューション への通知中にエラーが発生しました。問題を 解決して再度通知を行うか、通知を行わずに サービスを削除してアンインストールを行って ください。NSX からソリューションの URL にア クセスできること、およびソリューションから NSX にアクセスできることを確認してください。解決 用の API を使用してアラームを解決して ください。サービスは削除されます。	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. アクション：NSX からソリューションの URL にアクセスできること、およびソリューション から NSX にアクセスできることを確認してくだ さい。 systemalarms API の action=resolve パラメータを使用して、 アラームを解決します。
250018	高	はい	アンインストール前のセキュリティ ソリューション への通知中にエラーが発生しました。問題を 解決して再通知するか、通知せずにサービス を削除してアンインストールしてください。NSX からソリューションの URL にアクセスできるこ と、およびソリューションから NSX にアクセス できることを確認してください。解決用の API を使用してアラームを解決してください。サービ スは削除されます。	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. アクション：NSX からソリューションの URL にアクセスできること、およびソリューション から NSX にアクセスできることを確認してくだ さい。 systemalarms API の action=resolve パラメータを使用して、 アラームを解決します。
250019	高	はい	セキュリティ ソリューションへのアンインストール の通知中にサーバが再起動しました。NSX からソリューションの URL にアクセスできるこ とを確認してください。解決用の API を使 用してアラームを解決してください。サービスは アンインストールされます。	セキュリティソリューションへのアンインストー ルの通知中に、サーバが再起動しました。 アクション：NSX からソリューションの URL にアクセスできることを確認してください。 systemalarms API の action=resolve パラメータを使用して、 アラームを解決します。サービスはアンインス トールされます。
250020	高	はい	セキュリティ ソリューションへのアンインストール の通知中にサーバが再起動しました。NSX からソリューションの URL にアクセスできるこ とを確認してください。解決用の API を使 用してアラームを解決してください。サービスは 再度展開されます。	セキュリティソリューションへのアップグレー ドの通知中に、サーバが再起動しました。 アクション：NSX からソリューションの URL にアクセスできることを確認してください。 systemalarms API の action=resolve パラメータを使用して、 アラームを解決します。サービスが再デプロイ されます。

イベント コード	イベントの重 要度	アラームの トリガ	イベント メッセージ	説明
250021	重大	いいえ	NSX Manager は、vCenter Server の EAM サービスを使用して、ESX 上の NSX VIB を展開/監視します。この EAM サービスへの接続が切断されています。This could be due to EAM service or vCenter restart/stop or an issue in the EAM service. Verify that vCenter is up, and the EAM service in vCenter is running. Further, we can look at EAM mob to verify that EAM is functioning as expected.	NSX Manager は、ESX での NSX VIB のデプロイ/モニタリングに vCenter Server の EAM サービスを使用します。この EAM サービスとの接続が切れています。EAM サービスまたは vCenter Server が再起動または停止したか、EAM サービスに問題がある可能性があります。 アクション：vCenter Server が稼動中で、vCenter Server で EAM サービスが実行されていることを確認します。EAM MOB URL http://{vCenter_IP}/eam/mob/ にアクセス可能で、EAM が想定どおりに機能していることを確認します。詳細については、『NSX トラブルシューティングガイド』の「インフラストラクチャの準備」を参照してください。
250022	重大	いいえ	NSX Manager は、vCenter Server で EAM サービスを使用し、ESX で NSX VIB を展開/監視します。この EAM サービスへの接続が切断されています。これは、EAM サービスや vCenter Server が再起動または停止していることが原因である場合があります。また、EAM サービスに問題がある場合もあります。vCenter Server が起動していること、および vCenter Server で EAM サービスが実行されていることを確認します。さらに、EAM の MOB を確認して、EAM が適切に機能していることを確認することもできます。	NSX Manager は、ESX での NSX VIB のデプロイ/モニタリングに vCenter Server の EAM サービスを使用します。この EAM サービスとの接続が切れています。EAM サービスまたは vCenter Server が再起動または停止したか、EAM サービスに問題がある可能性があります。 アクション：vCenter Server が稼動中で、vCenter Server で EAM サービスが実行されていることを確認します。EAM MOB URL http://{vCenter_IP}/eam/mob/ にアクセス可能で、EAM が想定どおりに機能していることを確認します。詳細については、『NSX トラブルシューティングガイド』の「インフラストラクチャの準備」を参照してください。
250023	高	はい	アンインストール前のクリーンアップに失敗しました。解決用の API を使用してアラームを解決してください。サービスは削除されます。	アンインストール前の内部クリーンアップ タスクを完了できませんでした。 アクション：systemalarms API の action=resolve パラメータを使用して、アラームを解決します。サービスは削除されません。

イベント コード	イベントの重 要度	アラームの トリガ	イベント メッセージ	説明
250024	高	はい	このデプロイ ユニットのバックアップ EAM エージェントが見つかりませんでした。vCenter Server が初期化を実行している可能性があります。アラームを解決してエージェントが配置されているか確認してください。In case you have deleted the agency manually, please delete the deployment unit entry from NSX.	EAM は、ESXi ホストに VIB を展開します。NSX 準備済みの各クラスタに、EAM エージェントがインストールされています。このエージェントが見つからない場合は、vCenter Server サービスが初期化されたか、エージェントが手動で削除されてエラーになった可能性があります。
250025	高	はい	ステートレス ホストで EAM を使用して NSX VIB のアップグレードまたはアンインストールを行うと、このイベントが生成されます。ステートレス ホストは自動デプロイ機能を使用して準備する必要があります。自動デプロイ機能を使用して構成を修正し、解決用の API を使用してアラームを解決してください。	ステートレス ホストで EAM を使用して NSX VIBS のアップグレードまたはアンインストールを行うと、このイベントが生成されます。すべてのステートレス ホストを Auto Deploy 機能で準備する必要があります。 アクション：Auto Deploy 機能を使用して設定を修正し、 systemalarms API の action=resolve パラメータを使用して、アラームを解決してください。

デプロイ プラグインのシステム イベント

ここでは、デプロイ プラグインで発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コー ド	イベントの重要度	アラームのト リガ	イベント メッセージ	説明
280000	高	はい	デプロイ プラグインの IP アドレス プール不足アラーム。	送信元の IP アドレス プールが不足しているため、IP アドレスを NSX サービス仮想マシンに割り当てることができませんでした。 アクション：プールに IP アドレスを追加してください。
280001	高	はい	デプロイ プラグインの汎用アラーム。	ゲスト イン트로スペクションなどのサービスには、それぞれホスト上でサービスを設定するプラグインのセットがあります。プラグイン コードの問題は汎用アラームとしてレポートされます。サービスのプラグインがすべて成功した後に、サービスは緑色になります。このイベントは可能性のある例外のサブセットをキャプチャします。 アクション： resolve API を使用してアラームを解決してください。サービスがデプロイされます。

イベント コード	イベントの重要度	アラームのトリガ	イベント メッセージ	説明
280004	高	はい	デプロイ プラグインの汎用例外アラーム。	<p>ゲスト イントロスペクションなどのサービスには、それぞれホスト上でサービスを設定するプラグインのセットがあります。プラグイン コードの問題は汎用例外アラームとしてレポートされます。サービスのプラグインがすべて成功した後に、サービスは緑色になります。このイベントはすべての可能性のある例外をキャプチャします。</p> <p>アクション: resolve API を使用してアラームを解決してください。サービスがデプロイされます。</p>
280005	高	はい	変更を有効にするには、仮想マシンを再起動する必要があります。	<p>変更を有効にするには、仮想マシンを再起動する必要があります。</p> <p>アクション: resolve API を使用してアラームを解決してください。これで仮想マシンが再起動されます。</p>

メッセージング システム イベント

ここでは、メッセージングに関連する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの重要度	アラームのトリガ	イベント メッセージ	説明
390001	高	はい	ホストのメッセージング設定に失敗しました。	<p>NSX VIB が ESXi ホストに正常にインストールされたことを ESX Agent Manager (EAM) が NSX に通知すると、ホストの準備の後で NSX メッセージパスがセットアップされます。このイベントは、ホストでのメッセージパスのセットアップに失敗したことを示しています。NSX 6.2.3 以降では、[インストール手順] - [ホストの準備] タブの順に選択すると、影響を受けたホストの横に赤色のエラー アイコンが表示されます。</p> <p>アクション: トラブルシューティングの手順については、NSX トラブルシューティング ガイドを参照してください。</p>
390002	高	はい	ホストのメッセージング接続の再設定に失敗しました。	<p>RMQ ブローカの詳細が変更されたことを NSX が検出すると、ホストに最新の RMQ ブローカ情報を送信しようと試みます。NSX が情報の送信に失敗すると、このアラームが発生します。</p> <p>アクション: トラブルシューティングの手順については、NSX トラブルシューティング ガイドを参照してください。</p>
390003	高	はい	ホストのメッセージング設定に失敗し、通知がスキップされました。	<p>準備が完了したホストが vCenter Server に接続し直したときに、NSX はメッセージング チャネルを再度セットアップしようと試みます。このイベントは、セットアップが失敗し、メッセージング チャネルに依存する他の NSX モジュールに通知されなかったことを示すものです。</p> <p>アクション: トラブルシューティングの手順については、NSX トラブルシューティング ガイドを参照してください。</p>

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
39100 2	重大	いいえ	メッセージング インフラストラクチャがホストで起動していません。	NSX Manager と NSX ホスト間で 2 つ以上のハートビート メッセージが失われました。 アクション：トラブルシューティングの手順については、NSX トラブルシューティング ガイドを参照してください。
32110 0	重大	いいえ	メッセージング アカウント {account #} を無効にしています。パスワードの有効期限が切れました。	メッセージ バス クライアントとして動作する ESXi ホスト、NSX Edge 仮想マシン、またはユニバーサル サービス仮想マシン (USVM) は、最初のデプロイまたはホストの準備後、2 時間以内に Rabbit MQ パスワードを変更しませんでした。 アクション：NSX Manager とメッセージ バス クライアント間の通信の問題を調査してください。クライアントを実行していることを確認してください。再同期または再デプロイを実行する前に、適切なログを収集してください。トラブルシューティングの手順については、NSX トラブルシューティング ガイドを参照してください。

Service Composer システム イベント

ここでは、Service Composer で発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
300000	重大	はい	ポリシー {#} は、依存している SecurityGroup の明示的な削除の結果、削除されました。	依存するセキュリティ グループが削除されたときに、サービス ポリシーが削除されました。 アクション：セキュリティ ポリシーが作成されているか再度確認してください。
300001	高	はい	ポリシーが同期されていません。	このサービス ポリシーにルールを適用したときに、Service Composer でエラーが発生しました。 アクション：エラー メッセージを参照して、ポリシーで変更が必要なルールを確認してください。 Service Composer 経由でアラームを解決するか、 systemalarms API の action=resolve パラメータを使用してアラームを解決してください。
300002	高	はい	このポリシーのファイアウォール ルールが同期されていません。このアラームが解決されるまでは、このポリシーのファイアウォールに関連する変更はブッシュされません。	このエラーはファイアウォールの設定の問題が原因で発生します。 アクション：エラーの原因となったポリシーまたはルールの詳細については、エラー メッセージを参照してください。Service Composer または resolve API を使用してアラームを解決し、ポリシーを同期してください。[Troubleshooting issues with Service Composer in NSX 6.X] (http://kb.vmware.com/kb/2132612) も参照してください。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
300003	高	はい	このポリシーのネットワーク イントロスペクション ルール が同期されていません。この アラームが解決されるまで は、このポリシーのネットワ ーク イントロスペクションに関 連する変更はプッシュされま せん。	このエラーは、ネットワーク イントロスペクションの設定の問題が原因で発生しています。 アクション：エラーの原因となったポリシーまたはルールの詳細については、エラー メッセージを参照してください。Service Composer または systemalarms API の action=resolve パラメータを使用してアラームを解決し、ポリシーを同期してください。 [Troubleshooting issues with Service Composer in NSX 6.x] (http://kb.vmware.com/kb/2132612) も参照してください。 Service Composer 経由でアラームを解決するか、 systemalarms API の action=resolve パラメータを使用してアラームを解決してください。
300004	高	はい	このポリシーのゲスト イント ロスペクション ルールが同 期されていません。このア ラームが解決されるまでは、 このポリシーのゲスト イント ロスペクションに関連する変 更はプッシュされません。	このエラーは、ゲスト イントロスペクションの設定の問題が原因で発生しています。 アクション：エラーの原因となったポリシーまたはルールの詳細については、エラー メッセージを参照してください。Service Composer または systemalarms API の action=resolve パラメータを使用してアラームを解決し、ポリシーを同期してください。 [Troubleshooting issues with Service Composer in NSX 6.x] (http://kb.vmware.com/kb/2132612) も参照してください。
300005	高	はい	Service Composer は同期されていません。 Service Composer の変更は、ファイアウォ ール/ネットワーク イントロ スペクションにプッシュされま せん。	ポリシーの同期中、Service Composer にエラーが発生しました。変更はファイアウォールまたはネットワーク イントロスペクション サービスに送信されません。 エラー メッセージを参照し、アクション：ポリシーやファイアウォールで編集が必要なセクションを確認してください。Service Composer または resolve API を使用してアラームを解決してください。
300006	高	はい	再起動時の同期に失敗し ました。Service Composer は同期され ていません。	再起動時に行うポリシーの同期中、Service Composer にエラーが発生しました。変更はファイアウォールまたはネットワーク イントロスペクション サービスに送信されません。 エラー メッセージを参照し、アクション：ポリシーやファイアウォールで編集が必要なセクションを確認してください。Service Composer 経由でアラームを解決するか、 systemalarms API の action=resolve パラメータを使用してアラームを解決してください。
300007	高	はい	ファイアウォールからドラフト をロールバックしたため、 Service Composer が同期されていません。 Service Composer の変更は、ファイアウォ ール/ネットワーク イントロ スペクションにプッシュされま せん。	ファイアウォール ルール セットを以前のドラフトに戻すときに、Service Composer に同期エラーが発生しました。変更はファイアウォールまたはネットワーク イントロスペクション サービスに送信されません。 アクション：Service Composer 経由でアラームを解決するか、 systemalarms API の action=resolve パラメータを使用してアラームを解決してください。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
300008	高	はい	ポリシーに対応するセクションの削除中にエラーが発生しました。	<p>ポリシーのファイアウォール ルール セクションの削除中に、Service Composer にエラーが発生しました。この問題は、NSX のサービス挿入機能を使用するサードパーティのサービス マネージャにアクセスできない場合に発生します。</p> <p>アクション：サードパーティのサービス マネージャへの接続の問題を調査してください。Service Composer 経由でアラームを解決するか、systemalarms API の action=resolve パラメータを使用してアラームを解決してください。</p>
300009	高	はい	優先順位の変更を反映するため、セクションの順序を入れ替え中にエラーが発生しました。	<p>再起動時に行うポリシーの同期中、Service Composer にエラーが発生しました。変更はファイアウォールまたはネットワーク イントロスペクション サービスに送信されません。</p> <p>エラー メッセージを参照し、アクション：ポリシーやファイアウォールで編集が必要なセクションを確認してください。Service Composer 経由でアラームを解決するか、systemalarms API の action=resolve パラメータを使用してアラームを解決してください。</p>
300010	高	はい	自動保存ドラフトの設定を初期化中にエラーが発生しました。	<p>自動保存されたドラフト設定を初期化するときに Service Composer でエラーが発生しました。</p> <p>エラー メッセージを参照し、アクション：ポリシーやファイアウォールで編集が必要なセクションを確認してください。Service Composer 経由でアラームを解決するか、systemalarms API の action=resolve パラメータを使用してアラームを解決してください。</p>

ゲスト イントロスペクション サービス仮想マシンのシステム イベント

ここでは、ゲスト イントロスペクション ユニバーサル サービス仮想マシンで発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
295002	メジャー			<p>NSX Manager が、ゲスト イントロスペクション ユニバーサル サービス仮想マシンからハートビートを受信していません。</p> <p>アクション：NSX Manager とユニバーサル サービス仮想マシンのテクニカル サポート ログを収集して、テクニカル サポート リクエストを発行してください。</p>
295003	情報			<p>NSX Manager が、ゲスト イントロスペクション ユニバーサル サービス仮想マシンからハートビートを受信しています。</p> <p>アクション：イベント 295002 がレポートされた後、イベントをリカバリします。</p>
295010	情報			<p>ユニバーサル サービス仮想マシンとゲスト イントロスペクション ホスト モジュール間で接続が確立しました。</p> <p>アクション：情報通知のイベントです。操作は必要ありません。</p>

サービス仮想マシン (SVM) 運用システム イベント

ここでは、サービス仮想マシン (SVM) で発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの 重要度	アラームのトリガ	イベント メッセージ	説明
280002	高	はい	このエージェントのイベントの一部が NSX によって失われました。再起動、または vCenter Server との接続が一時的に失われたことが原因の可能性があります。 警告： アラームを解決すると仮想マシンが削除され、仮想マシンが失われたことを示す別のアラームが表示されます。同様に解決した場合、仮想マシンが再デプロイされます。	デプロイされたサービス仮想マシンで内部エラーが発生しました。 アクション： アラームを解決すると仮想マシンが削除され、仮想マシンの削除についての 2 番目のアラームがレポートされます。2 番目のアラームを解決すると、仮想マシンの再インストールが実行されます。仮想マシンの再デプロイに失敗すると、最初のアラームが再度レポートされます。アラームが再表示される場合は、KB http://kb.vmware.com/kb/2144624 の手順を使用してサービス仮想マシンのログを収集し、VMware テクニカル サポートにお問い合わせください。
280003	高	はい	このエージェントのイベントの一部が NSX によって失われました。再起動、または vCenter Server との接続が一時的に失われたことが原因の可能性があります。 警告： アラームを解決すると仮想マシンが再起動します。	デプロイされたサービス仮想マシンが再起動しました。 アクション： アラームを解決すると、仮想マシンが再起動します。再起動が失敗すると、アラームが再表示されます。KB http://kb.vmware.com/kb/2144624 の手順を使用してサービス仮想マシンのログを収集し、VMware テクニカル サポートにお問い合わせください。
280006	高	はい	エージェントに使用可能なマークを付けるのに失敗しました。	ESX エージェント仮想マシンが利用可能であるとマークするときに、内部エラーが発生しました。 アクション： <code>systemalarms</code> API の <code>action=resolve</code> パラメータを使用してアラームを解決してください。アラームを解決できない場合は、KB http://kb.vmware.com/kb/2144624 の手順を使用してサービス仮想マシンのログを収集し、VMware テクニカル サポートにお問い合わせください。

レプリケーション - ユニバーサル同期システム イベント

ここでは、レプリケーション - ユニバーサル同期で発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
310001	重大	いいえ	NSX Manager {#} のオブジェクト タイプ {#} の完全同期に失敗しました。	セカンダリ NSX Manager 上でのユニバーサル オブジェクトの完全同期に失敗しました。 アクション：NSX Manager のテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。
310003	重大	いいえ	NSX Manager {#} のエンティティ {#} に対するユニバーサル同期に失敗しました。	Cross-vCenter 環境のセカンダリ NSX Manager へのユニバーサル オブジェクトの同期に失敗しました。 アクション：NSX Manager のテクニカル サポート ログを収集して、VMware テクニカル サポートにお問い合わせください。

NSX 管理システム イベント

ここでは、NSX 管理で発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベント の重要度	アラームのト リガ	イベント メッセージ	説明
320001	重大	いいえ	The NSX Manager IP has been assigned to another machine with the MAC Address.	NSX Manager 管理が IP アドレスが、同じネットワーク上の仮想マシンに割り当てられました。NSX 6.2.3 以前では、重複する NSX Manager IP アドレスを検出または回避する機能はありません。このため、データパスの障害が発生する可能性があります。NSX 6.2.3以降では、重複するアドレスが検知されるとこのイベントが発生します。 アクション：重複するアドレスの問題を解決してください。

論理ネットワークのシステム イベント

ここでは、論理ネットワークに関連するシステム イベント メッセージについて説明します。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
814	重大	いいえ	いくつかのバックアップ分散仮想ポートグループが変更または削除されたため、論理スイッチ {#} は正しく構成されなくなりました。	<p>NSX 論理スイッチをバックアップする 1 つまたは複数の分散仮想スイッチポートグループが変更または削除されたか、論理スイッチの制御プレーンモードの変更に失敗しました。</p> <p>アクション：イベントがポートグループの削除または変更によってトリガされた場合、エラーは vSphere Web Client の【論理スイッチ】ページに表示されます。エラーをクリックして、不足している分散仮想スイッチポートグループを作成してください。制御プレーンモードの変更に失敗したためにイベントがトリガされた場合は、更新を再度実行してください。『NSX アップグレードガイド』の「トランスポートゾーンと論理スイッチの更新」を参照してください。</p>
1900	重大	いいえ	ホストで VXLAN の初期化に失敗しました。	<p>必要な数の VTEP に VMkernel NIC を設定できなかったため、VXLAN の初期化に失敗しました。NSX は、ユーザーが選択した分散仮想スイッチを VXLAN 用に準備し、VTEP VMkernel NIC が使用する分散仮想ポートグループを作成します。VXLAN を設定するときに、チーミング、ロードバランシングの方法、MTU、および VLAN ID が選択されます。チーミングとロードバランシングの方法は、VXLAN に選択された分散仮想スイッチの設定と一致する必要があります。</p> <p>アクション：vmkernel.logを確認してください。『NSX トラブルシューティングガイド』の「インフラストラクチャの準備」セクションも参照してください。</p>
1901	重大	いいえ	ホストで VXLAN ポートの初期化に失敗しました。	<p>VXLAN を関連付けられた分散仮想ポート上で設定できず、ポートが切断されました。NSX は、ユーザーによって選択された分散仮想スイッチを VXLAN 用に準備し、設定された各論理スイッチが使用する分散仮想ポートグループを作成します。</p> <p>アクション：vmkernel.logを確認してください。『NSX トラブルシューティングガイド』の「インフラストラクチャの準備」セクションも参照してください。</p>
1902	重大	いいえ	VXLAN インスタンスがホストに存在しません。	<p>ESXi ホストの分散仮想スイッチがまだ VXLAN に対して有効でないときに分散仮想ポートの VXLAN 設定を受け取りました。</p> <p>アクション：vmkernel.logを確認してください。『NSX トラブルシューティングガイド』の「インフラストラクチャの準備」セクションも参照してください。</p>
1903	重大	いいえ	論理スイッチ {#} が適切に動作できません。これは、バックアップする IP インターフェイスが特定のマルチキャストグループに参加できなかったためです。	<p>VTEP インターフェイスは指定されたマルチキャストグループへの参加に失敗しました。問題が解決されるまで、特定のホストへのトラフィックが影響を受けます。NSX は定期的な再試行メカニズム (5 秒ごと) を使用して、マルチキャストグループへ参加します。</p> <p>アクション：vmkernel.logを確認してください。『NSX トラブルシューティングガイド』の「インフラストラクチャの準備」セクションも参照してください。</p>

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
1905	重大	いいえ	トランスポート ソーンを使用できない可能性があります。これは、バックアップする IP インターフェイスが正しい IP アドレスを取得できないためです。	VTEP VMkernel NIC に有効な IP アドレスを割り当てることができませんでした。VMkernel NIC を経由するすべての VXLAN トラフィックがドロップされます。 アクション：VMKNic への IP アドレス割り当てで DHCP を使用する場合は、VXLAN 転送 VLAN で DHCP を使用できることを確認してください。「NSX host preparation fails with error: Insufficient IP addresses in IP pool」(http://kb.vmware.com/kb/2137025) を参照してください。
1906	重大	いいえ	分散仮想スイッチに VXLAN オーバーレイ クラスがありません。	分散仮想スイッチが VXLAN に設定されたときに NSX VIB がインストールされませんでした。すべての VXLAN インターフェイスが分散仮想スイッチへの接続に失敗します。 アクション：「Network connectivity issues after upgrade in NSX/VCNS environment」(http://kb.vmware.com/kb/2107951) を参照してください。
1920	重大	いいえ	接続できないため VXLAN コントローラ {#} が削除されました。コントローラの IP アドレス設定を確認して、再デプロイしてください。	コントローラのデプロイに失敗しました。 アクション：割り当てられた IP アドレスにアクセスできることを確認してください。『NSX トラブルシューティングガイド』の「NSX Controller」セクションも参照してください。
1930	重大	いいえ	コントローラ {#} がノード {#} (アクティブ = {#}) への接続を確立できません。現在の接続ステータス = {#}。	2 台のコントローラ ノードが切断され、コントローラ間の通信が影響を受けます。 アクション：『NSX トラブルシューティングガイド』の「NSX Controller」セクションを参照してください。
1935	重大	いいえ	すべてのコントローラが無効なため、ホスト {#} の情報をコントローラに送信できませんでした。コントローラが有効になったら、コントローラの同期が必要になることがあります。	ホストの証明書情報を NSX Controller クラスタに送信できませんでした。ホストとコントローラ クラスタ間の通信チャンネルに予想外の動作が発生する場合があります。 アクション：ESXi ホストを準備する前に NSX Controller クラスタのステータスが正常であることを確認してください。 controller sync API を使用してこの問題を解決してください。
1937	重大	いいえ	VXLAN vmknics {#} [PortGroup = {#}] が見つからないか、ホスト {#} から削除されました。	VXLAN VMkernel NIC が見つからないか、ホストから削除されました。ホストの送受信トラフィックが影響を受けます。 アクション：問題を解決するには、[インストール手順] - [論理ネットワークの準備] - [VXLAN 転送] タブの順に選択し、[解決] ボタンをクリックします。
1939	重大	いいえ	VXLAN vmknics {#} [PortGroup = {#}] がホスト {2} から削除されているか、ホストと vCenter Server 間の接続に問題が発生している可能性があります。	NSX Manager は、VXLAN VMkernel NIC が vCenter Server に見つからないことを検出しました。これは、vCenter Server とホストの通信の問題が原因で発生する場合があります。また、vCenter Server またはホストを再起動するときに、NSX Manager が VXLAN VMkernel NIC を短時間検出できない場合、このイベントが発生します。vCenter Server とホストが再起動を完了した後、NSX Manager は VXLAN VMkernel NIC を再度チェックし、何も問題がなければイベントをクリアします。 アクション：これが一時的な問題でない場合は、[インストール手順] - [論理ネットワークの準備] - [VXLAN 転送] タブの順に選択し、[解決] ボタンをクリックして解決してください。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
1941	重大	いいえ	Host Connection Status Changed: イベント コード: {#}, ホスト: {#} (ID: {#}), NSX Manager - ファイアウォール エージェント: {#}, NSX Manager - 制御 プレーン エージェント: {#}, 制 御プレーン エージェント - コント ローラ: {#}。	NSX Manager が、NSX Manager からホストのファイアウォール エージェント、NSX Manager からホストの制御プレーン エー ジェント、ホストの制御プレーン エージェントから NSX Controller の いずれかの接続で切断状態を検出しました。 アクション: NSX Manager からホストのファイアウォール エー ジェントへの接続が切断している場合は、NSX Manager および ファイアウォール エージェント ログ (</var/log/vsfwd.log>) を 確認するか、POST https://NSX-Manager-IP- Address/api/2.0/nwfabric/configure? action=synchronize REST API 呼び出しを送信して接続を 再同期してください。NSX Manager から制御プレーン エー ジェントへの接続が切断されている場合は、NSX Manager および制御 プレーン エージェント ログ (</var/log/netcpa.log>) を確認して ください。制御プレーン エージェントから NSX Controller への接 続が切断されている場合は、[Networking and Security] - [イン ストール] の順に移動して、ホストの接続ステータスを確認してく ださい。
1942	重大	いいえ	論理スイッチ {#} のバックング ポート グループ [moid = {0}] が見つからないとマークされ ています。	NSX Manager は、vCenter Server 内で、NSX 論理スイッチの バックング分散仮想ポートグループを検出できませんでした。 アクション: [インストール手順] - [論理ネットワークの準備] - [VXLAN 転送] タブの順に移動して [解決] ボタンをクリックする か、REST API (POST https://vsm- ip/api/2.0/vdn/virtualwires/<vw- id/backing?action=remediate) を使用してポート グ ループを再作成してください。
1945	重大	いいえ	コントローラ {#} のデバイス {#} で、ディスク遅延のアラート がオンになっています。	NSX Manager が NSX Controller で高いディスク遅延を検出しま した。 アクション: [NSX トラブルシューティング ガイド] の「NSX Controller」セクションを参照してください。
1946	情報	いいえ	コントローラ {0} のすべてのディ スク遅延のアラートがオフになっ ています。	NSX Manager がコントローラで高いディスク遅延を検出しなくな りました。 アクション: 情報通知のイベントです。操作は必要ありません。
1947	重大	いいえ	コントローラ仮想マシンは、 vCenter Server でパワーオ フになっています。	vCenter Server で NSX Controller 仮想マシンがパワーオフされ ていることが NSX Manager によって検出されました。コントロー ラ クラスタのステータスが「切断」となり、クラスタの稼働が必要 な操作に影響が及ぶ可能性があります。 アクション: [インストール手順] - [管理] タブの順に移動してコン トローラの [解決] ボタンをクリックするか、API POST https://vsm- ip/api/2.0/vdn/controller/{controllerId} ?action=remediate を呼び出してコントローラ仮想マシンを パワーオンしてください。

イベント コード	イベントの 重要度	アラームのト リガ	イベント メッセージ	説明
1948	重大	いいえ	コントローラ仮想マシンが vCenter Server から削除 されました。	vCenter Server から NSX Controller 仮想マシンが削除されていることが NSX Manager によって検出されました。コントローラ クラスタのステータスが「切断」となり、クラスタの稼働が必要な 操作に影響が及ぶ可能性があります。 アクション：[インストール手順] - [管理] タブの順に移動してコン トローラの [解決] ボタンをクリックするか、API POST <code>https://<vsm- ip>/api/2.0/vdn/controller/{controllerId} ?action=remediate</code> を呼び出して NSX Manager データベ ースからコントローラの状態を削除してください。
1952	重大	いいえ	VXLAN ポートグループ [moid = dvportgroup-xx] と関 連する分散仮想スイッチでは、チー ミング ポリシーが異なります。	VXLAN ポート グループのチーミング ポリシーが、関連する分散仮 想スイッチのチーミング ポリシーと異なることが、NSX Manager によって検出されました。これにより、予期しない動作が発生する 場合があります。 アクション：同じチーミング ポリシーを使用するように、VXLAN ポート グループまたは分散仮想スイッチを再設定してください。

Identity Firewall システム イベント

ここでは、Identity Firewall (IDFW) で発生する、重要度が「メジャー」、「重大」、「高」のシステム イベント メッセージについて説明します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
395000	重大	いいえ	ドメイン コントローラ イベントログ サーバ上 のセキュリティ ログが いっぱいです。	Active Directory イベント ログ サーバのセキュリティ ログがいっぱい になりました。IDFW は、ログのスクレイピングが設定されている場合、動作 を停止します。 アクション：Active Directory サーバ管理者に問い合わせ、セキュリティ ログのサイズを増やすか、セキュリティ ログをクリアするか、セキュリティ ログをアーカイブしてください。

ホストの準備のシステム イベント

ここでは、ホストの準備に関連するシステム イベント メッセージについて説明します。

注： NSX では、複数の ESX Agent Manager イベントが 1 つのイベントにマッピングされます。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	情報	はい	A VIB module has been uploaded to the host {hostID}, but will not be fully installed until the host {hostID} has been put in maintenance mode.	ESX Agent Manager がホストをメンテナンス モードに移行します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	重大	はい	An agent virtual machine is expected to be deployed on a host, but the agent virtual machine cannot be deployed because the vSphere ESX Agent Manager is unable to access the OVF package for the agent. This typically happens because the Web server providing the OVF package is down. The Web server is often internal to the solution that created the Agency.	ESX Agent Manager がエージェントを再デプロイします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	重大	はい	An agent VIB module is expected to be deployed on a host, but the VIM module cannot be deployed because the vSphere ESX Agent Manager is unable to access the VIB package for the agent. This typically happens because the Web server providing the VIB package is down. The Web server is often internal to the solution that created the Agency.	ESX Agent Manager は、VIB モジュールを再インストールします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent could not be deployed because it was incompatible with the host {hostID}.	vSphere ESX Agent Manager がエージェントを再デプロイします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。 ただし、ホストまたはソリューションをアップグレードし、エージェントとホストの互換性が確保されるまで、問題が解決しない場合があります。
270000	高	はい	An agent virtual machine is expected to be powered on, but there are no free IP addresses in the agent's pool of virtual machine IP addresses.	アクション： 問題を解決するには、IP アドレスの一部を解放するか、IP アドレス プールに IP アドレスを追加してから、 systemalarms API の action=resolve パラメータを使用してアラームを解決します。
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent virtual machine could not be deployed because the host {hostID} does not have enough free CPU or memory resources.	ESX Agent Manager がエージェント仮想マシンを再デプロイします。 十分な CPU とメモリ リソースが使用可能になるまで、問題が解決しない場合があります。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent virtual machine could not be deployed because the host's agent datastore did not have enough free space.	ESX Agent Manager がエージェント仮想マシンを再デプロイします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。 ただし、次のいずれかを行うまで、問題が解決しない場合があります。 ホストのエージェント仮想マシンのデータストアの空き容量を増やす。 または エージェント仮想マシンに十分な空き容量のある新しいデータストアを設定する。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off because there are no IP addresses defined on the agent's virtual machine network.	アクション： エージェント仮想マシンのネットワークに IP アドレス プールを作成してから、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host {hostID}.	アクション： ホストにエージェント仮想マシンのデータストアを設定する必要があります。
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent network has not been configured on the host.	アクション： ホストにエージェント仮想マシン ネットワークを設定する必要があります。
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent network has not been configured on the host. The host needs to be added to one of the networks listed in customAgentVmNetwork .	アクション： <customAgentVmNetwork> ネットワークの 1 つをホストに追加する必要があります。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent cannot be deployed because the agent datastore has not been configured on the host. The host needs to be added to one of the datastores listed in customAgentVmDatastore.	データストアの 1 つを <customAgentVmDatastore> という名前のホストに追加する必要があります。
270000	高	はい	The solution that created the agency is no longer registered with the vCenter server.	ESX Agent Manager がエージェンシーを削除します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	A dvFilter switch exists on a host but no agents on the host depend on dvFilter. This typically happens if a host is disconnected when an agency configuration changed.	ESX Agent Manager が <dvFilterSwitch> を削除します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An Agent virtual machine is expected to be provisioned on a host, but it failed to do so because the provisioning of the OVF package failed. The provisioning is unlikely to succeed until the solution that provides the OVF package has been upgraded or patched to provide a valid OVF package for the agent virtual machine.	ESX Agent Manager が OVF のプロビジョニングを再度試みます。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine needs to be powered on, but an OVF property is either missing or has an invalid value.	アクション： エージェント仮想マシンのプロビジョニングに使用するエージェントの設定で OVF 環境を更新します。
270000	高	はい	An agent virtual machine has been found in the vCenter inventory that does not belong to any agency in this vSphere ESX Agent Manager server instance.	ESX Agent Manager をパワーオフし（パワーオンの場合）、エージェント仮想マシンを削除します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	A VIB module requires the host to be in maintenance mode, but the vSphere ESX Agent Manager is unable to put the host in maintenance mode. This can happen if there are virtual machines running on the host that cannot be moved and must be stopped before the host can enter maintenance mode.	ESX Agent Manager が、ホストのメンテナンス モードへの移行を試みます。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。 ただし、仮想マシンをパワーオフするか、移動して、ホストをメンテナンス モードに移行するまで、問題が解決しない場合があります。
270000	重大	はい	A VIB module is expected to be installed on a host, but it failed to install since the VIB package is in an invalid format. The installation is unlikely to succeed until the solution providing the bundle has been upgraded or patched to provide a valid VIB package.	ESX Agent Manager が VIB のインストールを再試行します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	A VIB module is expected to be installed on a host, but it has not been installed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why the VIB module installation failed.	ESX Agent Manager が VIB のインストールを再試行します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	情報	はい	A VIB module has been uploaded to the host, but will not be activated until the host is rebooted.	ESX Agent Manager がホストをメンテナンス モードに移行し、再起動します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	A VIB module failed to install, but failed to do so because automatic installation by vSphere ESX Agent Manager is not allowed on the host.	アクション： vSphere Update Manager に移動し、必要なパッチをホストにインストールするか、ホストのイメージ プロファイルにパッチを追加します。詳細については、vSphere のドキュメントを参照してください。
270000	高	はい	A VIB module failed to uninstall, but failed to do so because automatic uninstallation by vSphere ESX Agent Manager is not allowed on the host.	アクション： vSphere Update Manager に移動し、必要なパッチをホストからアンインストールするか、ホストのイメージ プロファイルにパッチを追加します。詳細については、vSphere のドキュメントを参照してください。
270000	高	はい	An agent virtual machine is corrupt.	ESX Agent Manager がエージェント仮想マシンを削除し、再プロビジョニングします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。 この問題を手動で解決するには、不足しているファイルに関する問題を解決してから、エージェント仮想マシンをパワーオンします。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine is expected to be removed from a host, but the agent virtual machine has not been removed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why vSphere ESX Agent Manager was unable to remove the agent virtual machine, such as the host is in maintenance mode, powered off or in standby mode.	ESX Agent Manager がエージェントを再デプロイします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is a virtual machine template.	ESX Agent Manager がエージェント仮想マシンのテンプレートを仮想マシンに変換します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine is expected to be deployed on a host, but the agent virtual machine has not been deployed. Typically, a more specific issue (a subclass of this issue) indicates the particular reason why vSphere ESX Agent Manager was unable to deploy the agent, such as being unable to access the OVF package for the agent or a missing host configuration. This issue can also happen if the agent virtual machine is explicitly deleted from the host.	ESX Agent Manager がエージェント仮想マシンを再デプロイします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off.	ESX Agent Manager がエージェント仮想マシンをパワーオンします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is expected to be powered off, but the agent virtual machine is powered off.	ESX Agent Manager がエージェント仮想マシンをパワーオフします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is expected to be powered on, but the agent virtual machine is suspended.	ESX Agent Manager がエージェント仮想マシンをパワーオンします。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。

イベント コード	イベントの重 要度	アラームのト リガ	イベント メッセージ	説明
270000	高	はい	An agent virtual machine is expected to be located in a designated agent virtual machine folder, but is found in a different folder.	ESX Agent Manager が、指定されたエーエージェント フォルダにエーエージェント仮想マシンを戻します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	An agent virtual machine is expected to be located in a designated agent virtual machine resource pool, but is found in a different resource pool.	ESX Agent Manager が、指定されたエーエージェント リソース プールにエーエージェント仮想マシンを戻します。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。
270000	高	はい	EAM アラームを受信しました。	NSX VIB またはサービス仮想マシンのいずれかに、NSX インストールまたはアップグレードの問題があることを ESX Agent Manager が検出しました。 アクション： [ホストの準備 (Host Preparation)] タブで [解決 (Resolve)] オプションをクリックするか、 systemalarms API の action=resolve パラメータを使用して、アラームを解決します。