

NSX 日志记录和系统事件

Update 5

修改日期：2017 年 11 月 16 日

VMware NSX Data Center for vSphere 6.3



vmware®

您可以从 VMware 网站下载最新的技术文档：

<https://docs.vmware.com/cn/>。

VMware 网站还提供了最近的产品更新。

如果您对本文档有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

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

北京办公室
北京市
朝阳区新源南路 8 号
启皓北京东塔 8 层 801
www.vmware.com/cn

上海办公室
上海市
淮海中路 333 号
瑞安大厦 804-809 室
www.vmware.com/cn

广州办公室
广州市
天河路 385 号
太古汇一座 3502 室
www.vmware.com/cn

目录

NSX 日志记录和系统事件 4

1 系统事件、警报和日志 5

系统事件 5

警报 6

设置 NSX 组件的日志记录级别 8

审核日志 10

配置 syslog 服务器 11

收集技术支持日志 13

2 NSX 和主机日志 15

关于 NSX 日志 15

防火墙日志 16

与路由有关的 NSX 日志 20

Guest Introspection 日志 22

3 系统事件 30

安全系统事件 31

分布式防火墙系统事件 32

NSX Edge 系统事件 38

结构层系统事件 44

部署插件系统事件 50

消息传递系统事件 51

服务编排系统事件 52

GI SVM 系统事件 54

SVM 操作系统事件 55

复制 - 通用同步系统事件 57

NSX 管理系统事件 57

逻辑网络系统事件 57

身份防火墙系统事件 61

主机准备系统事件 61

NSX 日志记录和系统事件

《NSX 日志记录和系统事件》文档介绍了使用 NSX Manager 用户界面和 vSphere Web Client 查看 VMware NSX[®] for vSphere[®] 系统中的日志消息、事件和警报。

目标读者

本手册适用于要在 VMware vCenter 环境中使用 NSX 或解决任何 NSX 问题的用户。本手册的目标读者为熟悉虚拟机技术和虚拟数据中心操作且经验丰富的系统管理员。本手册假设您熟悉 VMware vSphere，包括 VMware ESXi、vCenter Server 和 vSphere Web Client。

VMware 技术出版物术语表

VMware 技术出版物提供了一个术语表，其中包含一些您可能不熟悉的术语。有关 VMware 技术文档中使用的术语的定义，请访问 <http://www.vmware.com/support/pubs>。

系统事件、警报和日志

您可以使用系统事件、警报和日志监控 NSX 环境的运行状况和安全以及解决问题。

本章讨论了以下主题：

- 系统事件
- 警报
- 设置 NSX 组件的日志记录级别
- 审核日志
- 配置 syslog 服务器
- 收集技术支持日志

系统事件

系统事件是系统操作的记录。每个事件具有一个严重性级别（如“信息”或“严重”）以指示事件的严重程度。还会将系统事件作为 SNMP 陷阱推送，以便任何 SNMP 管理软件可以监控 NSX 系统事件。

查看系统事件报告

从 vSphere Web Client 中，您可以查看由 NSX Manager 管理的所有组件的系统事件。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中单击 **NSX Manager**，然后单击**监控**选项卡。
- 4 单击**系统事件**选项卡。

您可以单击列标题中的箭头对事件进行排序，也可以使用**筛选器**文本框筛选事件。

系统事件格式

如果指定了 syslog 服务器，则 NSX Manager 将所有系统事件发送到 syslog 服务器。

这些消息具有与下面显示的消息类似的格式：

```
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'
```

系统事件包含以下信息。

```
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.
```

警报

警报是激活的通知以响应一个事件、一组状况或某个对象的状态。警报以及其他警示显示在 vSphere Web Client UI 的 NSX 仪表板和其他屏幕上。

您可以使用 `GET api/2.0/services/systemalarms` API 查看针对 NSX 对象的警报。

NSX 支持使用两种方法生成警报：

- 警报对应于一个系统事件，并具有关联的解决程序以尝试解决触发该警报的问题。这种方法适用于网络和安全结构层部署（例如，EAM、消息总线、部署插件），服务编排也支持这种方法。这些警报将事件代码作为警报代码。有关更多详细信息，请参阅《*NSX 日志记录和系统事件*》文档。
- **Edge** 通知警报采用触发和解决警报对形式。一些 **Edge** 功能支持这种方法，包括 IPsec VPN、负载均衡器、高可用性、运行状况检查、**Edge** 文件系统以及资源预留。这些警报使用与事件代码不同的唯一警报代码。有关更多详细信息，请参阅《*NSX 日志记录和系统事件*》文档。

通常，在纠正错误状况后，系统自动删除警报。在进行配置更新时，不会自动清除某些警报。在解决问题后，您必须手动清除警报。

下面是一个可用于清除警报的 API 示例。

您可以获取特定来源的警报，例如，群集、主机、资源池、安全组或 NSX Edge。按 `sourceId` 查看来源的警报：

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

按 *sourceId* 解决来源的所有警报：

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

您可以查看 NSX 警报，包括消息总线、部署插件、服务编排以及 Edge 警报：

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

您可以按 *alarmId* 查看特定的 NSX 警报：

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

您可以按 *alarmId* 解决特定的 NSX 警报：

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

有关 API 的详细信息，请参阅 NSX API 指南。

警报格式

您可以通过 API 查看警报格式。

警报格式包含以下信息。

```
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.
```

Guest Introspection 警报

警报用信号通知 vCenter Server 管理员存在需要特别注意的 Guest Introspection 事件。如果警报状态不再存在，这些警报便会自动取消。

vCenter Server 警报可在未安装自定义 vSphere 插件的情况下显示。请参见《vCenter Server 管理指南》了解有关事件和警报的信息。

注册为 vCenter Server 扩展组件后，NSX Manager 会定义规则，以便基于来自以下三个 Guest Introspection 组件的事件来创建和移除警报：SVM、Guest Introspection 模块和瘦代理。规则可进行自定义。有关如何为警报创建新的自定义规则的说明，请参见 vCenter Server 文档。在某些情况下，导致出现警报的可能原因有很多种。下文的表格列出了可能的原因以及修复问题所需采取的相应操作。

主机警报

主机警报由影响 Guest Introspection 模块的运行状态的事件生成。

表 1-1. 错误（标记为红色）

可能的原因	操作
Guest Introspection 模块已安装在主机上，但不再向 NSX Manager 报告状态。	<ol style="list-style-type: none"> 1 通过登录主机并键入命令 <code>/etc/init.d/vShield-Endpoint-Mux start</code> 确保 Guest Introspection 正在运行。 2 确保网络配置正确，以便 Guest Introspection 可以连接到 NSX Manager。 3 重新引导 NSX Manager。

SVM 警报

SVM 警报是由影响 SVM 运行状况的事件生成的。

表 1-2. 红色 SVM 警报

问题	操作
协议版本与 Guest Introspection 模块不匹配	确保 Guest Introspection 模块和 SVM 具有相互兼容的协议。
Guest Introspection 无法建立与 SVM 的连接	确保已打开 SVM 电源并正确配置了网络。
即使连接了客户机，SVM 也不会报告其状况。	内部错误。请联系您的 VMware 技术支持代表。

设置 NSX 组件的日志记录级别

您可以为每个 NSX 组件设置日志记录级别。

支持的级别因组件而异，如下所示。

```

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

```

为 IPsec VPN 启用日志记录

可以对所有 IPsec VPN 流量启用日志记录。

默认情况下，将启用日志记录并设置为警告级别。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击一个 NSX Edge。
- 4 单击**管理 (Manage)**选项卡，然后单击 **VPN** 选项卡。

- 5 单击 **IPSec VPN**。
- 6 单击**日志记录策略 (Logging Policy)**旁边的 ，然后单击**启用日志记录 (Enable logging)**以记录在本地子网和对等子网之间流动的流量，再选择日志记录级别。
- 7 选择日志级别，然后单击**发布更改 (Publish Changes)**。

SSL VPN-Plus 日志

SSL VPN-Plus 网关日志将发送到在 NSX Edge 设备上配置的 syslog 服务器。SSL VPN-Plus 客户端日志将存储在远程用户计算机的以下目录中：%PROGRAMFILES%/VMWARE/SSL VPN Client/。

更改 SSL VPN-Plus 客户端日志和日志级别

- 1 在 **SSL VPN-Plus** 选项卡中，从左侧面板单击**服务器设置 (Server Settings)**。
- 2 转到“日志记录策略”部分，并展开该部分以查看当前设置。
- 3 单击**更改 (Change)**。
- 4 选中**启用日志记录 (Enable logging)**复选框以启用日志记录。
或
取消选中**启用日志记录 (Enable logging)**复选框以禁用日志记录。
- 5 选择所需的日志级别。

注 默认情况下，将启用 SSL VPN-Plus 客户端日志，并且日志级别会被设置为“通知”。

- 6 单击**确定 (OK)**。

审核日志

审核日志记录登录到 NSX Manager 的用户的所有操作。

查看审核日志

审核日志提供的视图中列出所有 NSX Manager 用户执行操作。NSX Manager 最多保留 100,000 条审核日志。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击 **网络和安全**，然后单击 **网络和安全清单**下的 **NSX Manager**。
- 3 在**名称**列中，单击某个 NSX 服务器，然后单击**监控**选项卡。
- 4 单击**审核日志**选项卡。
- 5 如果该审核日志有详细信息，则可以单击**操作**列中该日志所对应的文本。要查看某一审核日志的详细信息，请单击**操作**列中的文本。
- 6 在**审核日志更改详细信息**中，选择**已更改的行**可以仅显示因该审核日志操作而值发生变化的属性。

配置 syslog 服务器

您可以配置一个 syslog 服务器，以作为 NSX 组件和主机的日志的存储库。

为 NSX Manager 配置 syslog 服务器

如果指定了 syslog 服务器，则 NSX Manager 将所有审核日志和系统事件发送到 syslog 服务器。

syslog 数据有助于进行故障排除以及查看安装和配置期间记录的数据。

NSX Edge 支持两个 syslog 服务器。NSX Manager 和 NSX Controller 支持一个 syslog 服务器。

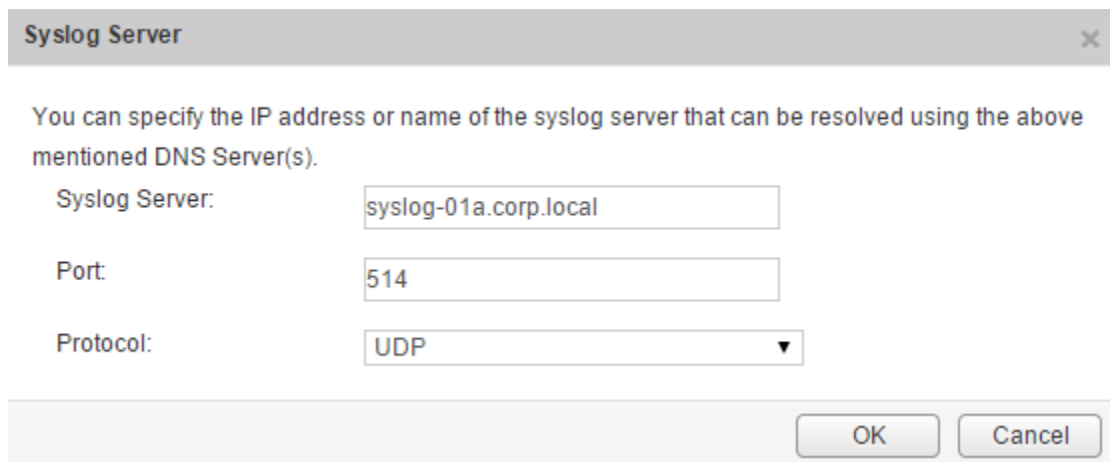
步骤

- 1 登录到 NSX Manager 虚拟设备。

在 Web 浏览器中，导航到 NSX Manager 设备 GUI（位于 <https://<nsx-manager-ip>> 或 <https://<nsx-manager-hostname>>），然后以管理员身份使用您在 NSX Manager 安装期间配置的密码登录。

- 2 从主页中，单击**管理设备设置 (Manage Appliance Settings) > 常规 (General)**。
- 3 单击 **Syslog 服务器 (Syslog Server)** 旁边的**编辑 (Edit)**。
- 4 键入 syslog 服务器的 IP 地址或主机名、端口和协议。

例如：



- 5 单击**确定 (OK)**。

将启用 NSX Manager 远程日志记录，并在单独的 syslog 服务器中存储日志。

为 NSX Edge 配置 Syslog 服务器

您可以配置一个或两个远程 syslog 服务器。与从 NSX Edge 设备流出的防火墙事件相关联的 NSX Edge 事件和日志发送到 syslog 服务器。

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 双击 NSX Edge。
- 4 单击**管理**选项卡，然后单击**设置**选项卡。
- 5 在**详细信息**面板中，单击 Syslog 服务器旁边的**更改**。
- 6 键入这两个远程 syslog 服务器的 IP 地址并选择协议。
- 7 单击**确定**保存配置。

为 NSX Controller 配置 Syslog 服务器

如果为 NSX Controller 配置了 syslog 服务器，则 NSX Manager 会将所有审核日志和系统事件发送至 syslog 服务器。syslog 数据有助于进行故障排除以及查看安装和配置期间记录的数据。唯一支持在 NSX Controller 上配置 syslog 服务器的方法是通过 NSX API。VMware 建议使用 UDP 作为 syslog 的协议。

步骤

- 1 要在 NSX Controller 上启用 syslog，请使用以下 NSX API。它会添加控制器 syslog 导出程序并在指定的控制器节点上配置一个 syslog 导出程序。

```
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 您可以使用以下 NSX API 查询控制器 syslog 导出程序并检索在指定的控制器节点上配置的 syslog 导出程序的详细信息。

```
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 如果不需要，您可以使用以下 **NSX API** 删除指定的控制器节点上的控制器 **syslog** 导出程序。

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

后续步骤

有关 API 的详细信息，请参阅 **NSX API 指南**。

收集技术支持日志

有时，您可能需要收集 **NSX** 组件和主机的技术支持日志以向 **VMware** 报告问题。

要收集主机技术支持日志，请运行 **export host-tech-support** 命令（请参阅《**NSX 故障排除指南**》中的“对分布式防火墙进行故障排除”）。

下载 NSX 的技术支持日志

可以将 **NSX Manager** 系统日志和 **Web Manager** 日志下载到桌面。

步骤

- 1 登录到 **NSX Manager** 虚拟设备。
- 2 在“设备管理”下方，单击**管理设备设置**。
- 3 单击 ，然后单击**下载技术支持日志**。
- 4 单击**下载**。
- 5 日志准备就绪后，单击**保存**将日志下载到桌面上。

该日志已压缩，其文件扩展名为 **.gz**。


后续步骤

您可以在保存文件的目录中浏览查找**所有文件**，然后使用解压缩实用程序打开该日志。

下载 NSX Edge 的技术支持日志

可以为每个 **NSX Edge** 实例下载技术支持日志。如果已为 **NSX Edge** 实例启用高可用性，则将从两个 **NSX Edge** 虚拟机下载技术支持日志。

步骤

- 1 登录到 **vSphere Web Client**。
- 2 单击**网络和安全 (Networking & Security)**，然后单击 **NSX Edge (NSX Edges)**。
- 3 选择一个 **NSX Edge** 实例。
- 4 单击**操作** ()，然后选择**下载技术支持日志**。
- 5 生成技术支持日志后，单击**下载**。

下载 NSX Controller 的技术支持日志

可以为每个 NSX Controller 实例下载技术支持日志。这些产品特定的日志中包含可用于进行分析的诊断信息。

要收集 NSX Controller 日志，请执行以下操作：

步骤

- 1 登录到 vSphere Web Client。
- 2 单击**网络和安全**，然后单击**安装**。
- 3 在**管理**下面，选择要从中下载日志的控制器。
- 4 单击**下载技术支持日志**。
- 5 单击**下载**。

NSX Manager 将开始下载 NSX Controller 日志并获取锁。

注 一次下载一个 NSX Controller 日志。第一个日志下载完成后，开始下载其他日志。如果同时从多个控制器下载日志，可能会出错。

- 6 日志准备就绪后，单击**保存**将日志下载到桌面上。

该日志已压缩，其文件扩展名为 **.gz**。

您现在可以分析所下载的日志。

后续步骤

如果您希望为 VMware 技术支持人员上载诊断信息，请参阅[知识库文章 2070100](#)。

NSX 和主机日志

您可以使用位于各种 NSX 组件和主机上的日志检测 and 解决问题。

本章讨论了以下主题：

- 关于 NSX 日志
- 防火墙日志
- 与路由有关的 NSX 日志
- Guest Introspection 日志

关于 NSX 日志

您可以配置 syslog 服务器并查看每个 NSX 组件的技术支持日志。可以通过 NSX Manager 获取管理层面日志，并通过 vCenter Server 获取数据层面日志。因此，建议您为 NSX 组件和 vCenter Server 指定同一 syslog 服务器，以便在查看 syslog 服务器上的日志时获得完整的信息。

有关为 vCenter Server 管理的主机配置 syslog 服务器的信息，请参见相应版本的 vSphere 文档，网址为 <https://docs.vmware.com>。

注 用于收集日志和访问 NSX 分布式逻辑路由器 (DLR) 控制虚拟机的 syslog 或跳转服务器不能位于直接连接到该 DLR 的逻辑接口的逻辑交换机上。

表 2-1. NSX 日志

组件	说明
ESXi 日志	这些日志是作为从 vCenter Server 中生成的虚拟机支持包的一部分收集的。 有关 ESXi 日志文件的详细信息，请参阅 vSphere 文档。
NSX Edge 日志	在 NSX Edge CLI 中使用 <code>show log [follow reverse]</code> 命令。 通过 NSX Edge UI 下载技术支持日志包。
NSX Manager 日志	在 NSX Manager CLI 中使用 <code>show log CLI</code> 命令。 通过 NSX Manager 虚拟设备 UI 下载技术支持日志包。
路由日志	请参见 NSX 日志记录和系统事件指南。
防火墙日志	请参见 防火墙日志 。
Guest Introspection 日志	请参见 Guest Introspection 日志 。

NSX Manager

要指定 syslog 服务器，请参见[为 NSX Manager 配置 syslog 服务器](#)。

要下载技术支持日志，请参见[下载 NSX 的技术支持日志](#)。

NSX Edge

要指定 syslog 服务器，请参见[为 NSX Edge 配置 Syslog 服务器](#)。

要下载技术支持日志，请参见[下载 NSX Edge 的技术支持日志](#)。

NSX Controller

要指定 syslog 服务器，请参见[为 NSX Controller 配置 Syslog 服务器](#)。

要下载技术支持日志，请参见[下载 NSX Controller 的技术支持日志](#)。

防火墙

有关更多详细信息，请参阅[防火墙日志](#)。

防火墙日志

防火墙将生成并存储日志文件，例如审核日志、规则消息日志和系统事件日志。您必须为每个启用了防火墙的群集配置一个 syslog 服务器。syslog 服务器在 `Syslog.global.logHost` 属性中指定。

防火墙生成下表中所述的日志。

表 2-2. 防火墙日志

日志类型	说明	位置
规则消息日志	包括所有访问决定，如每个规则的允许或拒绝流量（如果为该规则启用了日志记录）。包含启用了日志记录的规则的 DFW 数据包日志。	<code>/var/log/dfwpktlogs.log</code>
审核日志	包括管理日志和分布式防火墙配置更改。	<code>/home/secureall/secureall/logs/vsm.log</code>
系统事件日志	包括已应用分布式防火墙配置，已创建或删除筛选器或筛选器失败以及已将虚拟机添加到安全组，等等。	<code>/home/secureall/secureall/logs/vsm.log</code>
数据层面/VMKernel 日志	捕获与防火墙内核模块 (VSIP) 相关的活动。它包含系统生成的消息的日志条目。	<code>/var/log/vmkernel.log</code>
消息总线客户端/VSFWD 日志	捕获防火墙代理的活动。	<code>/var/log/vsfwd.log</code>

注 可以从 NSX Manager 命令行界面 (CLI) 中运行 `show log manager` 命令，然后为 `vsm.log` 关键字执行 `grep` 以访问 `vsm.log` 文件。仅具有 `root` 特权的用户或用户组可以访问该文件。

规则消息日志

规则消息日志包括所有访问决定，如每个规则的允许或拒绝流量（如果为该规则启用了日志记录）。这些日志存储在每个主机上的 `/var/log/dfwptlogs.log` 中。

以下是防火墙日志消息示例：

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

更多示例：

```
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
```

在以下示例中：

- 1002 是分布式防火墙规则 ID。
- domain-c7 是 vCenter Managed Object Browser (MOB) 中的群集 ID。
- 192.168.110.10/138 是源 IP 地址。
- 192.168.110.255/138 是目标 IP 地址。
- **RULE_TAG** 是在添加或编辑防火墙规则时在 **标记** 文本框中添加的文本示例。

以下示例显示了从 192.168.110.10 到 172.16.10.12 的 Ping 操作的结果。

```
# tail -f /var/log/dfwptlogs.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
```

下表介绍了防火墙日志消息中的文本框。

表 2-3. 日志文件条目的组成部分

组成部分	示例中的值
时间戳	2017-04-11T21:09:59
防火墙特定的部分	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. 日志文件条目的防火墙特定部分

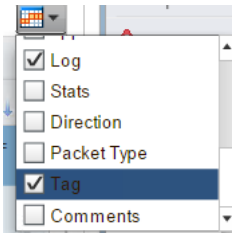
实体	可能值
筛选器哈希值	可用于获取筛选器名称和其他信息的数字。
AF 值	INET、INET6
原因	<ul style="list-style-type: none"> match: 数据包与规则匹配。 bad-offset: 在获取数据包时出现数据路径内部错误。 fragment: 组合到第一个分段的后续分段。 short: 数据包太短（例如，不太完整而不包括 IP 标头或 TCP/UDP 标头）。 normalize: 不包含正确标头或负载的不正确格式的数据包。 memory: 数据路径内存不足。 bad-timestamp: 不正确的 TCP 时间戳。 proto-cksum: 不正确的协议校验和。 state-mismatch: 未通过 TCP 状态机检查的 TCP 数据包。 state-insert: 发现重复的连接。 state-limit: 已达到数据路径可跟踪的最大状态数。 SpoofGuard: SpoofGuard 丢弃的数据包。 TERM: 已终止连接。
操作	<ul style="list-style-type: none"> PASS: 接受数据包。 DROP: 丢弃数据包。 NAT: SNAT 规则。 NONAT: 与 SNAT 规则匹配，但无法转换地址。 RDR: DNAT 规则。 NORDR: 与 DNAT 规则匹配，但无法转换地址。 PUNT: 将数据包发送到在当前虚拟机的相同管理程序上运行的服务虚拟机。 REDIRECT: 将数据包发送到从当前虚拟机的管理程序中运行的网络服务。 COPY: 接受数据包，并将其复制到当前虚拟机的相同管理程序上运行的服务虚拟机中。 REJECT: 拒绝数据包。
规则集和规则 ID	规则集/规则 ID
方向	入站、出站
数据包长度	长度
协议	<p>TCP、UDP、ICMP 或 PROTO（协议号）</p> <p>对于 TCP 连接，将在 TCP 关键字后面指示终止连接的实际原因。</p> <p>如果 TERM 是 TCP 会话的原因，则会在 PROTO 行中显示额外的说明。终止 TCP 连接的可能原因包括：RST（TCP RST 数据包）、FIN（TCP FIN 数据包）和 TIMEOUT（空闲时间太长）</p> <p>在上面的示例中，原因是 RST。因此，这意味着在必须重置的连接中具有 RST 数据包。</p> <p>对于非 TCP 连接（UDP、ICMP 或其他协议），终止连接的原因只能是 TIMEOUT。</p>

表 2-4. 日志文件条目的防火墙特定部分（续）

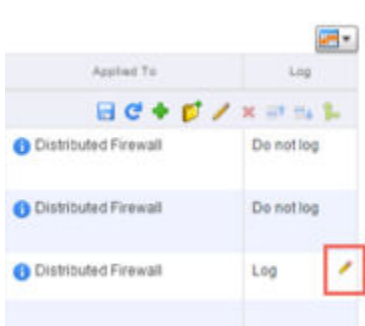
实体	可能值
源 IP 地址和端口	IP 地址/端口
目标 IP 地址和端口	IP 地址/端口
TCP 标记	S (SYN)、SA (SYN-ACK)、A (ACK)、P (PUSH)、U (URGENT)、F (FIN)、R (RESET)
数据包数	数据包的数量。 22/14 - 入站/出站数据包数
字节数	字节的数量。 7684/1070 - 入站/出站字节数

要启用规则消息，请登录到 vSphere Web Client：

- 1 在**网络和安全 > 防火墙**页面上启用日志列。



- 2 要为某个规则启用日志记录，请将光标悬停在日志表单元格上并单击铅笔图标。



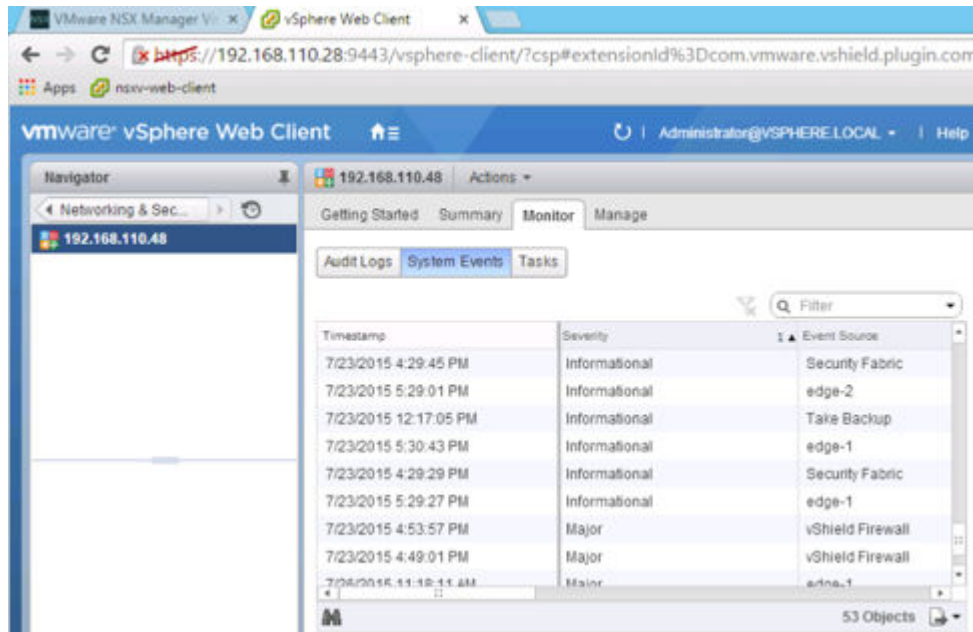
注 如果要在防火墙日志消息中显示自定义的文本，您可以启用**标记**列，然后单击铅笔图标以添加所需的文本。

审核日志和系统事件日志

审核日志包括管理日志和分布式防火墙配置更改。这些日志存储在 `/home/secureall/secureall/logs/vsm.log` 中。

系统事件日志包括已应用分布式防火墙配置，已创建或删除筛选器或筛选器失败以及已将虚拟机添加到安全组，等等。这些日志存储在 `/home/secureall/secureall/logs/vsm.log` 中。

要在 UI 中查看审核日志和系统事件日志，请导航到**网络和安全 > 安装 > 管理**，然后双击 **NSX Manager** 的 IP 地址。接下来，单击**监控**选项卡。



有关详细信息，请参见 NSX 日志记录和系统事件。

与路由有关的 NSX 日志

最佳做法是，配置 NSX 的所有组件以将其日志发送到集中式收集器，以便在一个地方检查这些日志。

如有必要，您可以更改 NSX 组件的日志级别。有关详细信息，请参见 NSX 日志记录和系统事件中的“设置 NSX 组件的日志记录级别”主题。

NSX Manager 日志

- NSX Manager CLI 中的 `show log`
- 通过 NSX Manager UI 收集的技术支持日志包

NSX Manager Virtual Appliance Management



NSX Manager 日志包含与管理层面有关的信息，其中包括创建、读取、更新和删除 (CRUD) 操作。

控制器日志

控制器包含多个模块，很多模块具有自己的日志文件。可以使用 `show log <log file> [filtered-by <string>]` 命令访问控制器日志。与路由有关的日志文件如下所示：

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: 该日志管理配置和内部 API 服务器。

- `cloudnet/cloudnet.nsx-controller.log`: 这是控制器主进程日志。
- `cloudnet/cloudnet_cpp.log.nsx-controller.log`: 该日志管理群集和引导。
- `cloudnet/cloudnet_cpp.log.ERROR`: 如果出现任何错误, 则包含该文件。

控制器日志非常详细, 在大多数情况下, 只有在请求 VMware 工程团队帮助解决更困难的问题时, 才需要使用这些日志。

除了 `show log CLI` 以外, 还可以使用 `watch log <logfile> [filtered-by <string>]` 命令在更新各个日志文件时实时观察这些文件。

这些日志包含在控制器支持包中, 可以在 NSX UI 中选择一个控制器节点并单击 **下载技术支持日志 (Download tech support logs)** 图标以生成并下载该支持包。

ESXi 主机日志

在 ESXi 主机上运行的 NSX 组件写入几个日志文件:

- VMkernel 日志: `/var/log/vmkernel.log`
- 控制层面代理日志: `/var/log/netcpa.log`
- 消息总线客户端日志: `/var/log/vsfwd.log`

也可以将这些日志作为从 vCenter Server 中生成的虚拟机支持包的一部分进行收集。仅具有 `root` 特权的用户或用户组可以访问这些文件。

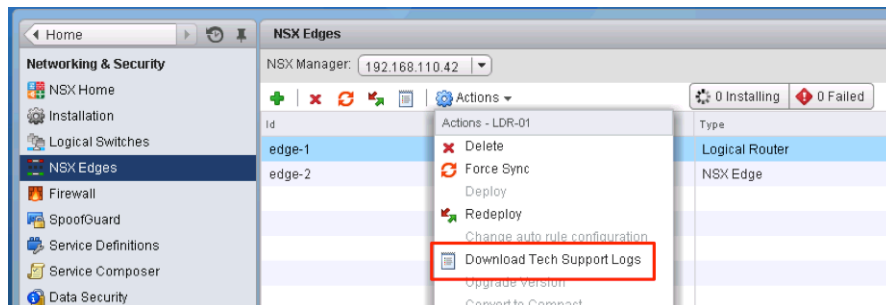
ESG/DLR 控制虚拟机日志

可以使用两种方法访问 ESG 和 DLR 控制虚拟机上的日志文件: 使用 CLI 显示这些文件, 或者使用 CLI 或 UI 下载技术支持包。

用于显示日志的 CLI 命令是 `show log [follow | reverse]`。

要下载技术支持包, 请执行以下操作:

- 从 CLI 中, 进入 `enable` 模式, 然后运行 `export tech-support <[scp | ftp]> <URI>` 命令。
- 从 vSphere Web Client 中, 在 **操作 (Actions)** 菜单中选择 **下载技术支持日志 (Download Tech Support Logs)** 选项。



其他有用的文件及其位置

虽然严格来说很多文件并不是日志，但它们可以帮助了解和解决 NSX 路由问题。

- 控制层面代理配置 `/etc/vmware/netcpa/config-by-vsm.xml` 包含有关以下组件的信息：
 - 控制器、IP 地址、TCP 端口、证书指纹、SSL 启用/禁用
 - 启用了 VXLAN 的 DVS 上的 dvUplink（绑定策略、名称、UUID）
 - 主机了解的 DLR 实例（DLR ID、名称）
- 控制层面代理配置 `/etc/vmware/netcpa/netcpa.xml` 包含各种 netcpa 配置选项，包括日志记录级别（默认为 **info**）。
- 控制层面证书文件：`/etc/vmware/ssl/rui-for-netcpa.*`
 - 两个文件：主机证书和主机私钥
 - 用于验证到控制器的主机连接

所有这些文件都是控制层面代理使用从 NSX Manager 收到的信息（通过 vsfwd 提供的消息总线连接）创建的。

Guest Introspection 日志

您可以捕获几种不同的日志以在排除 Guest Introspection 故障时使用。

ESX GI 模块 (MUX) 日志

如果 ESXi 主机上的虚拟机未使用 Guest Introspection，或者在主机上出现有关到 SVA 的通信的警报，则可能是 ESXi 主机上的 ESX GI 模块出现问题。

日志路径和示例消息

MUX 日志路径

`/var/log/syslog`

`var/run/syslog.log`

ESX GI 模块 (MUX) 消息采用以下格式：<timestamp>EPSecMUX<[ThreadID]>: <message>

例如：

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

在上面的示例中

- [ERROR] 是消息类型。其他类型可能是 [DEBUG]、[INFO]
- (EPSEC) 表示消息是端点安全特定的消息

启用和查看日志文件

要查看在主机上安装的 ESX GI 模块 VIB 版本，请运行 `#esxcli software vib list | grep epsec-mux` 命令。

要启用完整日志记录，请在 ESXi 主机命令 `shell` 上执行以下步骤：

- 1 运行 `ps -c | grep Mux` 命令以查找当前运行的 ESX GI 模块进程。

例如：

```
~ # 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 如果该服务未运行，您可以使用以下命令重新启动该服务：`/etc/init.d/vShield-Endpoint-Mux start` 或 `/etc//init.d/vShield-Endpoint-Mux restart`。
- 3 要停止运行的 ESX GI 模块进程（包括 `watchdog.sh` 进程），请运行 `~ # kill -9 192223 192233 192236` 命令。

请注意，生成了两个 ESX GI 模块进程。

- 4 使用新的 `-d` 选项启动 ESX GI 模块。请注意，对于 `epsec-mux` 内部版本 5.1.0-01255202 和 5.1.0-01814505，无法使用 `-d` 选项：`~ # /usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910`
- 5 查看 ESXi 主机上的 `/var/log/syslog.log` 文件中的 ESX GI 模块日志消息。请检查是否正确指定了与全局解决方案、解决方案 ID 和端口号对应的条目。

示例：示例 `muxconfig.xml` 文件

```
<?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>

```

GI 瘦代理日志

瘦代理安装在虚拟机客户机操作系统上，可以检测用户登录详细信息。

日志路径和示例消息

瘦代理由 GI 驱动程序组成 - vsepflt.sys、vnetflt.sys、vnetwfp.sys（Windows 10 和更高版本）。

瘦代理日志位于 ESXi 主机上，它是 vCenter 日志包的一部分。日志路径

是 /vmfs/volumes/<datastore>/<vmname>/vmware.log。例

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

瘦代理消息采用以下格式：<timestamp> <VM Name><Process Name><[PID]>: <message>。

在下面的日志示例中，Guest: vnet or Guest:vsep 指示与相应的 GI 驱动程序相关的日志消息，后跟调试消息。

例如：

```

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

```

示例：启用 vShield Guest Introspection 瘦代理驱动程序日志记录

由于调试设置可能会导致 `vmware.log` 文件填满而对其进行限制，因此，我们建议您在收集所需的所有信息后立即禁用调试模式。

该过程要求您修改 Windows 注册表。在修改注册表之前，请确保创建注册表的备份。有关备份和还原注册表的详细信息，请参见 Microsoft 知识库文章 [136393](#)。

要为瘦代理驱动程序启用调试日志记录，请执行以下操作：

- 1 单击**开始 > 运行 (Start > Run)**。输入 `regedit`，然后单击**确定 (OK)**。将打开“注册表编辑器”窗口。有关详细信息，请参见 Microsoft 知识库文章 [256986](#)。
- 2 使用注册表编辑器创建以下项：
`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\vsepflt\parameters`。
- 3 在新创建的参数项下面，创建以下 DWORD。在输入这些值时，请确保选择十六进制值：

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

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

`log_level` 参数项的其他值：

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

- 4 以管理员身份打开命令提示符。运行以下命令以卸载并重新加载 vShield Endpoint 文件系统小型驱动程序：

- `fltmc unload vsepflt`
- `fltmc load vsepflt`

您可以在位于虚拟机的 `vmware.log` 文件中找到这些日志条目。

启用 vShield GI 网络自检驱动程序日志记录

由于调试设置可能会导致 `vmware.log` 文件填满而对其进行限制，因此，我们建议您在收集所需的所有信息后立即禁用调试模式。

该过程要求您修改 Windows 注册表。在修改注册表之前，请确保创建注册表的备份。有关备份和还原注册表的详细信息，请参见 Microsoft 知识库文章 [136393](#)。

- 1 单击**开始 > 运行 (Start > Run)**。输入 `regedit`，然后单击**确定 (OK)**。将打开“注册表编辑器”窗口。有关详细信息，请参见 Microsoft 知识库文章 [256986](#)。

2 编辑注册表：

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

3 重新引导虚拟机。

vsepfilt.sys 和 vnetflt.sys 日志文件位置

在使用 `log_dest` 注册表设置 `DWORD:0x00000001` 时，Endpoint 瘦代理驱动程序将日志记录到调试程序中。运行调试程序（SysInternals 中的 DbgView 或 windbg）以捕获调试输出。

或者，您也可以将 `log_dest` 注册表设置设为 `DWORD:0x000000002`，在这种情况下，驱动程序日志将输出到 `vmware.log` 文件，该文件位于 ESXi 主机上的相应虚拟机文件夹中。

启用 UMC 日志记录

Guest Introspection 用户模式组件 (UMC) 在受保护的虚拟机上的 VMware Tools 服务中运行。

- 1 在 Windows XP 和 Windows Server 2003 上，创建一个 `tools.config` 文件（如果在以下路径中不存在）：`C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf`。
- 2 在 Windows Vista、Windows 7 和 Windows Server 2008 上，创建一个 `tools.config` 文件（如果在以下路径中不存在）：`C:\ProgramData\VMware\VMware Tools\tools.conf`。
- 3 在 `tools.conf` 文件中添加以下行以启用 UMC 组件日志记录。

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

在使用 `vsep.handler = vmx` 设置时，UMC 组件将日志记录到 `vmware.log` 文件中，该文件位于 ESXi 主机上的相应虚拟机文件夹中。

在使用以下设置时，将在指定的日志文件中输出 UMC 组件日志。

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

GI EPSecLib 和 SVM 日志

EPSecLib 从 ESXi 主机 ESX GI 模块 (MUX) 中接收事件。

日志路径和示例消息

EPSecLib 日志路径

/var/log/syslog

var/run/syslog

EPSecLib 消息采用以下格式: <timestamp> <VM Name><Process Name><[PID]>: <message>

在下面的示例中, [ERROR] 是消息类型, (EPSEC) 表示 Guest Introspection 特定的消息。

例如:

```
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.
```

收集日志

要为 EPSec 库 (GI SVM 中的组件) 启用调试日志记录, 请执行以下操作:

1 从 NSX Manager 中获取控制台密码以登录到 GI SVM。

2 创建 /etc/epseclib.conf 文件并添加:

```
ENABLE_DEBUG=TRUE
```

```
ENABLE_SUPPORT=TRUE
```

3 运行 `chmod 644 /etc/epseclib.conf` 命令以更改权限。

4 运行 `/usr/local/sbin/rcusvm restart` 命令以重新启动 GI-SVM 进程。

这会为 GI SVM 上的 EPSecLib 启用调试日志记录, 可以在 /var/log/messages 中找到适用于 NSX for vSphere 6.2.x 和 6.3.x 的调试日志。由于调试设置可能会导致 vmware.log 文件填满而对其进行限制, 因此, 我们建议您在收集所需的所有信息后立即禁用调试模式。

GI SVM 日志

在捕获日志之前, 请确定主机 ID 或主机 MOID:

- 在 NSX Manager 中运行 `show cluster all` 和 `show cluster <cluster ID>` 命令。

例如:

```
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 要确定当前日志记录状态，请运行以下命令：

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

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

- 2 要更改当前日志记录状态，请运行以下命令：

```
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 要生成日志，请运行以下命令：

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

选择 **Send** 和 **Download**。

请注意，该命令生成 **GI SVM** 日志，并将该文件另存为 **techsupportlogs.log.gz** 文件。由于调试设置可能会导致 **vmware.log** 文件填满而对其进行限制，因此，我们建议您在收集所需的所有信息后立即禁用调试模式。

系统事件

NSX 中的所有组件均报告系统事件。这些事件可以帮助监控环境的运行状况和安全以及解决问题。

每条事件消息包含以下信息：

- 唯一的事件代码
- 严重性级别
- 事件说明和建议的措施（如果适用）

收集技术支持日志并与 VMware 支持部门联系

对于某些事件，建议的措施包括收集技术支持日志并与 VMware 支持部门联系。

- 要收集 NSX Manager 技术支持日志，请参阅[下载 NSX 的技术支持日志](#)。
- 要收集 NSX Edge 技术支持日志，请参阅[下载 NSX Edge 的技术支持日志](#)。
- 要收集主机技术支持日志，请运行 `export host-tech-support` 命令（请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”）。
- 要与 VMware 支持部门联系，请参阅“如何在 My VMware 中提出支持请求”(<http://kb.vmware.com/kb/2006985>)。

在 NSX Edge 上执行强制同步

对于某些事件，建议的措施包括在 NSX Edge 上执行强制同步。有关详细信息，请参阅《NSX 管理指南》中的“使用 NSX Manager 对 NSX Edge 执行强制同步”。强制同步是一种破坏性操作并重新引导 NSX Edge 虚拟机。

系统事件严重性级别

每个事件具有以下严重性级别之一：

- 信息
- 低
- 中等
- 主要

- 严重
- 高

以下主题介绍了各种组件的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

本章讨论了以下主题：

- [安全系统事件](#)
- [分布式防火墙系统事件](#)
- [NSX Edge 系统事件](#)
- [结构层系统事件](#)
- [部署插件系统事件](#)
- [消息传递系统事件](#)
- [服务编排系统事件](#)
- [GI SVM 系统事件](#)
- [SVM 操作系统事件](#)
- [复制 - 通用同步系统事件](#)
- [NSX 管理系统事件](#)
- [逻辑网络系统事件](#)
- [身份防火墙系统事件](#)
- [主机准备系统事件](#)

安全系统事件

下表介绍了安全系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
11002	严重	否	无法连接到 vCenter Server。用户名/密码错误。(Unable to connect to vCenter Server Bad username/password.)	vCenter Server 配置失败。 措施：确认 vCenter Server 配置正确无误并提供了正确的凭据。请参阅《NSX 管理指南》中的“在 NSX Manager 中注册 vCenter Server”以及《NSX 故障排除指南》中的“将 NSX Manager 连接到 vCenter Server”。
11006	严重	否	丢失 vCenter Server 连接。(Lost vCenter Server connectivity.)	到 vCenter Server 的连接中断。 措施：调查 vCenter Server 的任何连接问题。请参阅 NSX 故障排除指南中的“将 NSX Manager 连接到 vCenter Server”和“解决 NSX Manager 问题”。

事件代码	事件严重性	触发的警报	事件消息	说明
230000	严重	否	NSX Manager 上的 SSO 配置任务失败。(SSO Configuration Task on NSX Manager failed.)	<p>单点登录 (SSO) 配置失败。原因包括凭据无效、配置无效或时间不同步。</p> <p>措施：查看错误消息并重新配置 SSO。请参阅 NSX 管理指南中的“配置单点登录”。另请参阅《NSX 故障排除指南》中的“配置 NSX SSO 查找服务失败”。</p>
230002	严重	否	SSO STS 客户端已断开连接。(SSO STS Client disconnected.)	<p>在 SSO 服务中注册 NSX Manager 失败，或者到 SSO 服务的连接中断。</p> <p>措施：检查配置问题（例如，凭据无效）、不同步问题以及网络连接问题。由于特定的 VMware 技术问题，也可能发生该事件。请参阅知识库文章“无法验证 STS 服务的 SSL 证书”(http://kb.vmware.com/kb/2121696)以及“在具有 Platform Service Controller (PSC) 的 Lookup Service 中注册 NSX Manager 失败并出现以下错误：未验证服务器证书链”(http://kb.vmware.com/kb/2132645)。</p>
240000	严重	否	已将条目 {0} 添加到身份验证黑名单。(Added an entry {0} to authentication black list.)	<p>具有特定 IP 地址的用户无法连续 10 次登录，并锁定 30 分钟。</p> <p>措施：调查潜在的安全问题。</p>

分布式防火墙系统事件

下表介绍了分布式防火墙的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
301001	严重	否	主机上的过滤器配置更新失败。(Filter config update failed on host.)	<p>主机无法接收/分析筛选器配置或打开设备 <code>/dev/dvfilterb1</code>。</p> <p>措施：查看键值对以了解上下文和失败原因，其中可能包括 NSX Manager 与准备主机之间的 VIB 版本不匹配问题以及意外的升级问题。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。</p>
301002	主要	否	过滤器配置未应用到 vnic。(Filter config not applied to vnic.)	<p>无法将筛选器配置应用于 vNIC。</p> <p>可能的原因：打开、分析或更新筛选器配置失败。不会在分布式防火墙中出现该错误，但可能在网络可扩展性 (NetX) 方案中出现该错误。</p> <p>措施：为 ESXi 和 NSX Manager 收集技术支持包，并与 VMware 技术支持部门联系。</p>

事件代码	事件严重性	触发的警报	事件消息	说明
301031	严重	否	主机上的防火墙配置更新失败。(Firewall config update failed on host.)	<p>无法接收/分析/更新防火墙配置。键值具有上下文信息，例如，生成编号以及其他调试信息。</p> <p>措施：验证是否执行了主机准备过程。登录到主机并收集 <code>/var/log/vsftd.log</code> 文件，然后使用 API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> 强制同步防火墙配置（请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”）。如果仍然无法在主机上更新分布式防火墙配置，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。</p>
301032	主要	否	无法将防火墙规则应用到 vnic。(Failed to apply firewall rule to vnic.)	<p>无法将防火墙规则应用于 vNIC。</p> <p>措施：验证 vsip 内核堆是否具有足够的可用内存（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。请确保主机日志（<code>vmkernel.log</code> 和 <code>vsftd.log</code>）包含将防火墙配置应用于 vNIC 的时间段。</p>
301041	严重	否	主机上的容器配置更新失败。(Container configuration update failed on host.)	<p>与网络和安全容器配置有关的操作失败。键值具有上下文信息，例如，容器名称和生成编号。</p> <p>措施：验证 vsip 内核堆是否具有足够的可用内存（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。请确保主机日志（<code>vmkernel.log</code> 和 <code>vsftd.log</code>）包含将容器配置应用于 vNIC 的时间段。</p>
301051	主要	否	主机上流量丢失。(Flow missed on host.)	<p>与保护的虚拟机之间的一个或多个会话的流量数据已丢弃、无法读取或无法发送到 NSX Manager。</p> <p>措施：验证 vsip 内核堆是否具有足够的可用内存以及 vsftd 内存消耗是否在资源限制内（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。</p>
301061	严重	否	主机上的 Spoofguard 配置更新失败。(Spoofguard config update failed on host.)	<p>与 SpoofGuard 有关的配置操作失败。</p> <p>措施：验证是否执行了主机准备过程。登录到主机并收集 <code>/var/log/vsftd.log</code> 文件，然后使用 API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> 强制同步防火墙配置（请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”）。如果 SpoofGuard 配置仍然失败，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。请确保日志包含主机收到 SpoofGuard 配置的时间段。</p>

事件代码	事件严重性	触发的警报	事件消息	说明
301062	主要	否	无法将 Spoofguard 应用到 vnic。(Failed to apply spoofguard to vnic.)	无法将 SpoofGuard 应用于 vNIC。 措施: 验证是否执行了主机准备过程。登录到主机并收集 /var/log/vsfwd.log 文件, 然后使用 API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> 强制同步防火墙配置 (请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”)。如果 SpoofGuard 配置仍然失败, 请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301064	主要	否	无法为 vnic 禁用 Spoofguard。(Failed to disable spoofguard for vnic.)	无法为 vNIC 禁用 SpoofGuard。 措施: 收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301072	严重	否	无法删除旧版应用程序服务虚拟机。(Failed to delete legacy App service vm.)	无法删除 vCloud Networking and Security 的 vShield App 服务虚拟机。 措施: 验证是否执行了《NSX 升级指南》中的“将 vShield App 升级到分布式防火墙”过程。
301080	严重	否	已超出防火墙 CPU 阈值。(Firewall CPU threshold crossed.)	已超出 vsfwd CPU 使用率阈值。 措施: 请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”部分。您可能需要降低主机资源利用率。如果问题仍然存在, 请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301081	严重	否	已超出防火墙内存阈值。(Firewall memory threshold crossed.)	已超出 vsfwd 内存阈值。 措施: 请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”部分。您可能需要降低主机资源利用率, 包括减少配置的防火墙规则或网络和安全容器数。要减少防火墙规则数, 请使用 <code>appliedTo</code> 功能。如果问题仍然存在, 请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301082	严重	否	已超出防火墙每秒连接数阈值。(Firewall ConnectionsPerSecond threshold crossed.)	已超出防火墙每秒连接数阈值。 措施: 请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”部分。您可能需要降低主机资源利用率, 包括减少与主机上的虚拟机之间的活动连接数。

事件代码	事件严重性	触发的警报	事件消息	说明
301501	严重	否	主机 {hostID} 上的防火墙配置更新版本 {version#} 超时。主机上的防火墙配置已同步到更高版本 {version#}。(Firewall configuration update version {version#} to host {hostID} timed out. Firewall configuration on host is synced upto version {version#}.)	主机需要超过 2 分钟的时间以处理防火墙配置更新，并且更新超时。 措施：验证 vsfwd 是否正常工作，以及是否正在将规则发布到主机。请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301502	严重	否	主机 {hostID} 上的 Spoofguard 配置更新版本 {hostID} 超时。主机上的 Spoofguard 配置已同步到更高版本 {version#}。(Spoofguard configuration update number {number#} to host {hostID} timed out. Spoofguard configuration on host is synced upto version {version#}.)	主机需要超过 2 分钟的时间以处理 SpoofGuard 配置更新，并且更新超时。 措施：验证 vsfwd 是否正常工作，以及是否正在将规则发布到主机。请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301503	严重	否	无法将防火墙配置版本 {version#} 发布到群集 {clusterID}。有关详细信息，请参见日志。(Failed to publish firewall configuration version {version#} to cluster {clusterID}. Refer logs for details.)	为群集或一个或多个主机发布防火墙规则失败。 措施：请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301504	严重	否	无法将容器更新发布到群集 {clusterID}。有关详细信息，请参见日志。(Failed to publish container updates to cluster {clusterID}. Refer logs for details.)	为群集或一个或多个主机发布网络和安全容器更新失败。 措施：请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301505	严重	否	无法将 Spoofguard 更新发布到群集 {clusterID}。有关详细信息，请参见日志。(Failed to publish spoofguard updates to cluster {clusterID}. Refer logs for details.)	为群集或一个或多个主机发布 SpoofGuard 更新失败。 措施：请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。

事件代码	事件严重性	触发的警报	事件消息	说明
301506	严重	否	无法将排除列表更新发布到群集 {clusterID}。有关详细信息，请参见日志。(Failed to publish exclude list updates to cluster {clusterID}. Refer logs for details.)	为群集或一个或多个主机发布排除列表更新失败。 措施：请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301508	严重	否	无法同步主机 {hostID}。有关详细信息，请参见日志。(Failed to sync host {hostID}. Refer logs for details.)	通过 API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> 进行的防火墙强制同步操作失败。 措施：请参阅《NSX 故障排除指南》中的“对分布式防火墙进行故障排除”。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301510	严重	否	群集的强制同步操作失败。(Force sync operation failed for the cluster.)	通过 API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> 进行的防火墙强制同步操作失败。 措施：收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301512	主要	否	主机 {hostID} [{hostID}] 上已安装防火墙。(Firewall is installed on host {hostID} [{hostID}].)	已成功在主机上安装分布式防火墙。 措施：在 vCenter Server 中，导航到 主页 > 网络和安全 > 安装 ，然后选择“主机准备”选项卡。验证“防火墙状态”是否显示为绿色。
301513	主要	否	主机 {hostID} [{hostID}] 上已卸载防火墙。(Firewall is uninstalled on host {hostID} [{hostID}].)	已从主机中卸载分布式防火墙。 如果无法卸载分布式防火墙组件，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301514	严重	否	群集 {clusterID} 上已启用防火墙。(Firewall is enabled on cluster {clusterID}.)	已成功在群集上安装分布式防火墙。 措施：在 vCenter Server 中，导航到 主页 > 网络和安全 > 安装 ，然后选择“主机准备”选项卡。验证“防火墙状态”是否显示为绿色。
301515	严重	否	群集 {clusterID} 上已卸载防火墙。(Firewall is uninstalled on cluster {clusterID}.)	已从群集中卸载分布式防火墙。 措施：如果无法卸载分布式防火墙组件，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301516	严重	否	群集 {clusterID} 上已禁用防火墙。(Firewall is disabled on cluster {clusterID}.)	已在群集中的所有主机上禁用分布式防火墙。 措施：不需要采取任何措施。
301034	主要	否	无法将防火墙规则应用到主机。(Failed to apply Firewall rules to host.)	无法应用分布式防火墙规则区域。 措施：验证 vsip 内核堆是否具有足够的可用内存（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。

事件代码	事件严重性	触发的警报	事件消息	说明
301043	严重	否	无法将容器配置应用到 vnic。(Failed to apply container configuration to vnic.)	无法应用网络或安全容器配置。 措施：验证 vsip 内核堆是否具有足够的可用内存（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301044	严重	否	无法将容器配置应用到主机。(Failed to apply container configuration to host.)	无法应用网络或安全容器配置。 措施：验证 vsip 内核堆是否具有足够的可用内存（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301066	主要	否	无法将 Spoofguard 配置应用到主机。(Failed to apply Spoofguard configuration to host.)	无法将所有 Spoofguard 应用于 vnic。 措施：验证 vsip 内核堆是否具有足够的可用内存（请参阅《NSX 管理指南》中的“查看防火墙 CPU 和内存阈值事件”）。如果问题仍然存在，请收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。
301100	严重	否	主机上的防火墙超时配置更新失败。(Firewall timeout configuration update failed on host.)	无法更新防火墙会话定时器超时配置。 措施：收集 NSX Manager 和主机的技术支持日志并与 VMware 支持部门联系。在收集日志后，使用 REST API <a href="https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>">https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> 强制同步防火墙配置，或者转到 安装 > 主机准备 ，然后在 操作 下面选择 强制同步服务 以进行强制同步。
301101	主要	否	无法将防火墙超时配置应用到 vnic。(Failed to apply firewall timeout configuration to vnic.)	无法更新防火墙会话定时器超时配置。 措施：收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。在收集日志后，使用 REST API <a href="https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>">https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> 强制同步防火墙配置，或者转到 安装 > 主机准备 ，然后在 操作 下面选择 强制同步服务 以进行强制同步。
301103	主要	否	无法将防火墙超时配置应用到主机。(Failed to apply firewall timeout configuration to host.)	无法更新防火墙会话定时器超时配置。 措施：收集 NSX Manager 和主机的技术支持日志并与 VMware 技术支持部门联系。在收集日志后，使用 REST API <a href="https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>">https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id> 强制同步防火墙配置，或者转到 安装 > 主机准备 ，然后在 操作 下面选择 强制同步服务 以进行强制同步。
301200	主要	否	应用程序规则管理器流量分析已启动。(Application Rule Manager flow analysis started.)	应用程序规则管理器流量分析已启动。 措施：不需要采取任何措施。

事件代码	事件严重性	触发的警报	事件消息	说明
301201	主要	否	应用程序规则管理器流量分析失败。(Application Rule Manager flow analysis failed.)	应用程序规则管理器流量分析失败。 措施：收集 NSX Manager 的技术支持日志并与 VMware 技术支持部门联系。为与失败会话相同的 vNIC 启动新的监控会话以重试该操作。
301202	主要	否	应用程序规则管理器流量分析已完成。(Application Rule Manager flow analysis completed.)	应用程序规则管理器的流量分析已完成。 措施：不需要采取任何措施。

NSX Edge 系统事件

下表介绍了 NSX Edge 的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。如果具有信息严重性的系统事件触发警报，则会列出这些事件。

事件代码	事件严重性	警报代码	事件消息	说明
30011	高	不适用	未发现任何 NSX Edge 虚拟机处于服务状态。网络可能中断。(None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.)	NSX Edge 虚拟机将自动从该状态中恢复。查找具有事件代码 30202 或 30203 的陷阱。 措施：请参阅《NSX 故障排除指南》中的“Edge 设备故障排除”。
30013	严重	130013	NSX Manager 发现 NSX Edge 虚拟机 (vmId 为 {#}) 处于错误状态。需要强制执行同步。(NSX Manager found NSX Edge VM (vmId : {#}) in bad state. Needs a force sync.)	NSX Edge 虚拟机报告错误状态，并且可能无法正常工作。 措施：在检测到有问题的状态时，将触发自动强制同步。如果自动强制同步失败，请尝试手动强制同步。
30014	主要	不适用	无法与 NSX Edge 虚拟机进行通信。(Failed to communicate with the NSX Edge VM.)	NSX Manager 与 NSX Edge 通过 VIX 或消息总线进行通信。NSX Manager 根据在 Edge 部署或重新部署时是否完成主机准备来选择通信通道。该事件指示 NSX Manager 与 NSX Edge 的通信中断。 措施：请参阅《NSX 故障排除指南》中的“Edge 设备故障排除”。
30027	信息	130027	NSX Edge 虚拟机 (vmId 为 {#}) 已关闭电源。(NSX Edge VM (vmId : {#}) is powered off.)	已关闭 NSX Edge 虚拟机电源。 措施：仅信息事件。
30032	高	130032	在 vCenter 清单中未找到 vmId 为 {0} 的 NSX Edge 设备。(NSX Edge appliance with vmId : {#} not found in the vCenter inventory.)	可能直接从 vCenter Server 中删除了 NSX Edge 虚拟机。这不是支持的操作，因为必须在用于 NSX 的 vSphere Web Client 界面中添加或删除 NSX 受管对象。 措施：重新部署 Edge 或部署新的 Edge。

事件代码	事件严重性	警报代码	事件消息	说明
30033	高	130033	在 vCenter 清单中未找到 NSX Edge 虚拟机 (vmId 为 {#})。 (NSX Edge VM (vmId : {#}) not found in the vCenter inventory.)	在 vCenter 清单中找不到 NSX Edge 虚拟机。 措施：检查是否意外删除该虚拟机。如果已确认，请重新部署 Edge。
30034	严重	130034	未发现任何 NSX Edge 虚拟机处于服务状态。网络可能中断。 (None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.)	Edge 虚拟机未响应 NSX Manager 发送的运行状况检查。 措施：确认已打开 Edge 虚拟机电源。然后，收集 Edge 日志并与 VMware 技术支持部门联系。
30037	严重	不适用	Edge 防火墙规则已修改为 {#}，不再适用于 {#}。 (Edge firewall rule modified as {#} is no longer available for {#}.)	在防火墙规则中具有无效的 GroupingObject (IPSet、securityGroup 等)。 措施：重新访问防火墙规则并进行所需的更新。
30038	严重	不适用	已打开电源的 NSX Edge 设备 (edgeId 为 {#}、vmName 为 {#}) 违反了虚拟机反关联性规则。 (Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule.)	NSX Edge 高可用性自动将反关联性规则应用于 vSphere 主机，以便在不同的主机上部署活动和备用 Edge 虚拟机。该事件指示已从群集中移除这些反关联性规则，并且两个 Edge 虚拟机在同一主机上运行。 措施：转到 vCenter Server 并验证反关联性规则。
30045	严重	不适用	NSX Edge 虚拟机运行状况检查因严重的 vix 错误而失败。已为虚拟机禁用其他运行状况检查。请重新部署或强制同步虚拟机以恢复运行状况检查。 (NSX Edge VM health check failing with critical vix errors. Further health check is disabled for vm. Please redeploy or forcesync vm to resume health check.)	网络环境可能导致 VIX 通道上的 Edge 虚拟机通信反复失败。 措施：如果 NSX Edge 响应，请收集 NSX Manager 和 NSX Edge 技术支持日志。然后，执行强制同步。如果问题仍然存在，请重新部署 NSX Edge（请参阅《NSX 管理指南》中的“重新部署 NSX Edge”）。 注 重新部署是一种破坏性操作。建议您先执行强制同步；如果未解决该问题，则重新进行部署。

事件代码	事件严重性	警报代码	事件消息	说明
30046	严重	不适用	Edge {EdgeID#} 虚拟机 {#} 上的预规则发布失败，生成编号为 {#}。请参阅日志以了解详细信息。这可能需要强制进行同步。(Pre rules publish failed on edge: {EdgeID#}, vm: {#} for generation number {#}. Refer logs for detail. It may need forcesync.)	NSX Edge 防火墙规则可能不同步。如果预规则（从 DFW UI/API 中配置）失败，则会生成该错误。 措施：如果内置恢复过程未自动解决该问题，请执行手动强制同步。
30100	严重	不适用	NSX Edge 已强制执行同步。(NSX Edge was force synced.)	已强制同步 NSX Edge 虚拟机。 措施：如果强制同步未解决该问题，请收集 NSX Manager 和 NSX Edge 的技术支持日志并与 VMware 技术支持部门联系。
30102	高	130102	NSX Edge (vmId 为 {IP Address}) 处于错误状态。需要强制执行同步。(NSX Edge (vmId : {IP Address}) is in Bad State. Needs a force sync.)	NSX Edge 虚拟机遇到内部错误。 措施：如果内置恢复过程未自动解决该问题，请尝试手动强制同步。
30148	严重	不适用	NSX Edge CPU 使用量已增加。前 {#} 个进程为：{#}。(NSX Edge CPU usage has increased. {#} Top processes are: {#}.)	在一段时间内，NSX Edge 虚拟机 CPU 占用率持续较高。 措施：请参阅《NSX 故障排除指南》中的“Edge 设备故障排除”。如果问题仍然存在，请收集 NSX Manager 和 NSX Edge 的技术支持日志并与 VMware 技术支持部门联系。
30153	主要	不适用	AESNI 加密引擎已启动。(AESNI crypto engine is up.)	AESNI 加密引擎已启动。 措施：不需要采取任何措施。
30154	主要	不适用	AESNI 加密引擎已关闭。(AESNI crypto engine is down.)	AESNI 加密引擎已关闭。 措施：不需要采取任何措施。这是预期的状态。
30155	高	130155	在部署 NSX Edge 时预留资源期间，主机或资源池上没有足够的可用 CPU 和/或内存资源。(Insufficient CPU and/or Memory Resources available on Host or Resource Pool, during resource reservation at the time of NSX Edge deployment.)	主机或资源池上的 CPU 和/或内存资源不足。 您可以导航到 主页 (Home) > 主机和群集 > [群集名称] (Hosts and Clusters > [Cluster-name]) > 监控 (Monitor) > 资源预留 (Resource Reservation) 页以查看可用的资源和预留的资源。 在检查可用的资源后，再次将这些资源指定为设备配置的一部分，以便资源预留限制成功。

事件代码	事件严重性	警报代码	事件消息	说明
30180	严重	不适用	NSX Edge 内存不足。Edge 将在 3 秒钟内重新引导。前 5 个进程为：{#}。 (NSX Edge is out of memory. The Edge is rebooting in 3 seconds. Top 5 processes are: {#}.)	NSX Edge 虚拟机内存不足。已启动重新引导以进行恢复。 措施：请参阅《NSX 故障排除指南》中的“Edge 设备故障排除”。如果问题仍然存在，请收集 NSX Manager 和 NSX Edge 的技术支持日志并与 VMware 技术支持部门联系。
30181	严重	130181	NSX Edge {EdgeID#} 虚拟机名称 {#} 文件系统为只读。(NSX Edge {EdgeID#} VM name {#} file system is read only.)	支持 NSX Edge 虚拟机的存储设备出现连接问题。 措施：检查并纠正支持数据存储的任何连接问题。在解决连接问题后，您可能需要执行手动强制同步。
30202	主要	不适用	NSX Edge {EdgeID#} 高可用性发生切换。虚拟机 {#} 名称 {#} 已切换到 ACTIVE 状态。(NSX Edge {EdgeID#} HighAvailability switch over happened. VM {#} name {#} has moved to ACTIVE state.)	发生了 HA 故障切换，辅助 NSX Edge 虚拟机从备用转变为活动状态。 措施：不需要采取任何措施。
30203	主要	不适用	NSX Edge {EdgeID} 高可用性发生切换。虚拟机 {#} 名称 {#} 已切换到 STANDBY 状态。(NSX Edge {EdgeID} HighAvailability switch over happened. VM {#} name {#} has moved to STANDBY state.)	发生了 HA 故障切换，主 NSX Edge 虚拟机从活动转变为备用状态。 措施：不需要采取任何措施。
30205	严重	130205	启用了高可用性的 NSX Edge {EdgeID} 中检测到脑裂。(Split Brain detected for NSX Edge {EdgeID} with HighAvailability.)	由于网络故障，为 HA 配置的 NSX Edge 虚拟机无法确定另一个虚拟机是否处于联机状态。在这种情况下，两个虚拟机将另一个虚拟机视为未处于联机状态，并都变为活动状态。这可能会导致网络中断。 措施：检查网络基础架构（虚拟和物理）以查找任何故障，尤其是为 HA 配置的接口和路径。

事件代码	事件严重性	警报代码	事件消息	说明
30302	严重	130302	LoadBalancer virtualServer/pool {virtualServerName}} (协议为 {#}, serverIp 为 {IP Address}) 的状态已更改为关闭。 (LoadBalancer virtualServer/pool : {virtualServerName}} Protocol : {#} serverIp : {IP Address} changed the state to down.)	NSX Edge 负载均衡器上的虚拟服务器或池已关闭。 措施: 请参阅《NSX 故障排除指南》中的“负载均衡”部分。
30303	主要	不适用	LoadBalancer virtualServer/pool {0} (协议为 {#}, serverIp 为 {IP Address}) 已更改为错误状态。 (LoadBalancer virtualServer/pool : {0} Protocol : {#} serverIp : {IP Address} changed to a wrong state.)	NSX Edge 负载均衡器上的虚拟服务器或池遇到内部错误。 措施: 请参阅《NSX 故障排除指南》中的“负载均衡”部分。
30304	主要	130304	LoadBalancer 池 {0} (协议为 {#}, serverIp 为 {IP address}) 已更改为警告状态。 (LoadBalancer pool : {0} Protocol : {#} serverIp : {IP address} changed to a warning state.)	NSX Edge 负载均衡器池已将其状态更改为 警告 (warning) 。 措施: 请参阅《NSX 故障排除指南》中的“负载均衡”部分。
30402	严重	130402	从 localIp {IP address} 到 peerIp {IP address} 的 IPsec 通道状态已更改为关闭。 (IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down.)	NSX Edge IPSec VPN 通道已关闭。 措施: 请参阅《NSX 故障排除指南》中的“虚拟专用网络 (VPN)”部分。

事件代码	事件严重性	警报代码	事件消息	说明
30404	严重	130404	Edge IPsec 隧道关闭: 从 localSubnet {subnet} 到 peerSubnet {subnet} 的 IPsec 隧道状态已更改为关闭。(EDGE IPSEC TUNNEL DOWN : IPsec Tunnel from localSubnet : {subnet} to peerSubnet : {subnet} changed the status to down.)	NSX Edge IPsec VPN 通道已关闭。 措施: 请参阅《NSX 故障排除指南》中的“虚拟专用网络 (VPN)”部分。
30405	主要	不适用	从 localIp {IP address} 到 peerIp {IP address} 的 IPsec 通道状态已更改为未知。(IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.)	无法确定 NSX Edge IPsec VPN 通道的状态。 措施: 请参阅《NSX 故障排除指南》中的“虚拟专用网络 (VPN)”部分。
30406	主要	不适用	从 localIp {IP address} 到 peerIp {IP address} 的 IPsec 通道状态已更改为未知。(IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.)	无法确定 NSX Edge IPsec VPN 通道的状态。 措施: 请参阅《NSX 故障排除指南》中的“虚拟专用网络 (VPN)”部分。
30701	严重	不适用	由于没有提供外部 DHCP 服务器, Edge {EdgeID} 上的 NSX Edge DHCP 中继服务已禁用。请检查服务器 IP 或引用的分组对象。(NSX Edge DHCP Relay service on edge {EdgeID} is disabled because there is no external DHCP server provided. Please check server IP or referenced grouping object.)	已禁用 NSX Edge Edge DHCP 中继服务。可能的原因: (1) DHCP 中继进程未运行。(2) 没有外部 DHCP 服务器。这可能是由删除中继引用的分组对象造成的。 措施: 请参阅《NSX 管理指南》中的“配置 DHCP 中继”。

事件代码	事件严重性	警报代码	事件消息	说明
30206	严重	不适用	已启用了高可用性的 NSX Edge {EdgeID} 解决脑裂。(Resolved Split Brain for NSX Edge {EdgeID} with HighAvailability.)	两个 NSX Edge HA 设备可以相互通信，并且已重新协商活动和备用状态。 措施：请参阅“解决 NSX Edge 高可用性 (HA) 问题”(http://kb.vmware.com/kb/2126560)。
30207	严重	不适用	已尝试 {value} 次为 NSX Edge {EdgeID} 解决脑裂。(Attempted Split Brain resolution for NSX Edge {EdgeID} with count {value}.)	两个 NSX Edge HA 设备正在尝试重新协商并从裂脑情况中恢复。 注 ：仅在 NSX Edge 6.2.3 之前的版本中提供该事件报告的恢复机制。 措施：请参阅“解决 NSX Edge 高可用性 (HA) 问题”(http://kb.vmware.com/kb/2126560)。

结构层系统事件

下表介绍了结构层系统事件的系统事件消息。

事件代码	事件严重性	触发的警报	事件消息	说明
250000	信息	否	部署单元的旧操作状态为 {#}，新操作状态为 {#}，旧进度状态为 {#}，新进度状态为 {#}。请检查警报字符串以了解根本原因。(Deployment unit old operational status was {#} , new operational status is {#} and old progress state was {#}, new progress state is {#}. Check alarm string for root cause.)	仅信息事件。
250001	信息	否	已创建部署单元。(A deployment unit has been created.)	仅信息事件。
250002	信息	否	已更新 NSX 中的部署单元。将在群集上更新结构层服务。(A deployment unit in NSX has been updated. Fabric services will be updated on the cluster.)	仅信息事件。
250003	信息	否	已从 NSX 中删除部署单元。(A deployment unit has been deleted from NSX.)	仅信息事件。
250004	高	是	无法在主机 {#} 上部署服务 {#}，因为数据存储 {#} 未连接到该主机。请确认已连接该数据存储，或者提供不同的数据存储。(Failed to deploy service {#} on host {#} since datastore (#) is not connected to the host. Please verify that it is connected, or provide a different datastore.)	无法配置存储主机安全虚拟机的数据存储。 措施：确认主机可以访问该数据存储。

事件代码	事件严重性	触发的警报	事件消息	说明
250005	高	是	部署单元安装失败。请确认可以访问 OVF/VIB URL，已配置 DNS，并且已打开所需的网络端口。(Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)	在主机上安装 NSX 服务期间，ESXi 主机无法从 NSX 中访问 VIB/OVF。在 vCenter 系统事件表中，将会看到：Event Message: 'Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module: 'Security Fabric'. 措施：请参阅 NSX 故障排除指南。
250006	信息	否	已在主机上成功安装用于网络结构层服务的结构层代理。(The fabric agent for network fabric services installed successfully on a host.)	仅信息事件。
250007	信息	否	已从主机中成功移除结构层代理。(The fabric agent was removed successfully from a host.)	仅信息事件。
250008	高	是	OVF/VIB 文件的位置已更改。必须重新部署服务。(Location of OVF / VIB files has changed. Service must be redeployed.)	获取 NSX VIB 和 OVF 时使用的 URL 因 NSX 版本而异。要找到正确的 VIB，您必须访问 <a href="https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties">https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties 。如果 NSX Manager IP 地址发生变化，则可能需要重新部署 NSX OVF 或 VIB。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
250009	高	是	部署单元升级失败。请确认可以访问 OVF/VIB URL、已配置 DNS，并且已打开所需的网络端口。(Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)	在主机升级期间，EAM 无法从 NSX 中访问 VIB/OVF。在 vCenter 系统事件表中，将会看到：Event Message: 'Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.', Module: 'Security Fabric'. 措施：请参阅 NSX 故障排除指南。
250012	高	是	要使服务 {#} 能够正常运行，需要成功安装以下服务：{#}。(Following service(s) need to be installed successfully for Service {#} to function: {#}.)	要安装的服务依赖于另一个尚未安装的服务。 措施：在群集上部署所需的服务。

事件代码	事件严重性	触发的警报	事件消息	说明
250014	高	是	在升级之前通知安全解决方案时出现错误。解决方案可能无法访问/无响应。请确保可以从 NSX 访问该解决方案的 URL。请使用解决方案 API 来解决此警报。将重新部署服务。(Error while notifying security solution before upgrade. The solution may not be reachable/responding. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be redeployed.)	在升级之前通知安全解决方案时出现错误。可能无法访问该解决方案，或者该解决方案没有响应。 措施：确保可以从 NSX 中访问该解决方案 URL。请使用 systemalarms API 中的 action=resolve 参数解决该警报。将重新部署服务。
250015	高	是	即使在超时后也未接收到安全解决方案针对升级通知的回叫。请确保可以从 NSX 访问该解决方案的 URL，也可以从该解决方案 API 访问 NSX。请使用解决方案 API 来解决此警报。将重新部署服务。(Did not receive callback from security solution for upgrade notification even after timeout. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be redeployed.)	即使在超时后也未接收到安全解决方案针对升级通知的回叫。 措施：确保可以从 NSX 中访问该解决方案 URL，并且可以从该解决方案中访问 NSX。请使用 systemalarms API 中的 action=resolve 参数解决该警报。
250016	高	否	卸载服务失败。请确保可以从 NSX 访问解决方案的 URL，也可以从该解决方案访问 NSX。请使用解决方案 API 来解决此警报。将移除服务。(Uninstallation of service failed. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.)	卸载服务失败。 措施：确保可以从 NSX 中访问该解决方案 URL，并且可以从该解决方案中访问 NSX。请使用 systemalarms API 中的 action=resolve 参数解决该警报。

事件代码	事件严重性	触发的警报	事件消息	说明
250017	高	是	在卸载之前通知安全解决方案时出现错误。解决警报以再次通知，或删除警报以在不通知的情况下卸载。请确保可以从 NSX 访问该解决方案的 URL，也可以从该解决方案访问 NSX。请使用解决方案 API 来解决此警报。将移除服务。(Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.)	在卸载之前通知安全解决方案时出现错误。请解决该警报以再次通知，或者删除该警报以在不通知的情况下卸载。 措施：确保可以从 NSX 中访问该解决方案 URL，并且可以从该解决方案中访问 NSX。请使用 systemalarms API 中的 action=resolve 参数解决该警报。
250018	高	是	在卸载之前通知安全解决方案时出现错误。解决警报以再次通知，或删除警报以在不通知的情况下卸载。请确保可以从 NSX 访问该解决方案的 URL，也可以从该解决方案访问 NSX。请使用解决方案 API 来解决此警报。将移除服务。(Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification. Ensure that solution urls are accessible from NSX, and NSX is reachable from the solution. Use resolve API to resolve the Alarm. Service will be removed.)	在卸载之前通知安全解决方案时出现错误。请解决该警报以再次通知，或者删除该警报以在不通知的情况下卸载。 措施：确保可以从 NSX 中访问该解决方案 URL，并且可以从该解决方案中访问 NSX。请使用 systemalarms API 中的 action=resolve 参数解决该警报。
250019	高	是	正在向安全解决方案通知卸载时服务器发生重新引导。请确保可以从 NSX 访问该解决方案的 URL。请使用解决方案 API 来解决此警报。将卸载服务。(Server rebooted while security solution notification for uninstall was going on. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be uninstalled.)	在向安全解决方案通知卸载时，重新引导了服务器。 措施：确保可以从 NSX 中访问该解决方案 URL。请使用 systemalarms API 中的 action=resolve 参数解决该警报。将卸载服务。

事件代码	事件严重性	触发的警报	事件消息	说明
250020	高	是	正在向安全解决方案通知升级时服务器发生重新引导。请确保可以从 NSX 访问该解决方案的 URL。请使用解决方案 API 来解决此警报。将重新部署服务。(Server rebooted while security solution notification for upgrade was going on. Ensure that solution urls are accessible from NSX. Use resolve API to resolve the Alarm. Service will be redeployed.)	在向安全解决方案通知升级时，重新引导了服务器。 措施：确保可以从 NSX 中访问该解决方案 URL。请使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。将重新部署服务。
250021	严重	否	NSX Manager 依赖于 vCenter 中的 EAM 服务来部署/监控 ESX 上的 NSX VIB。与此 EAM 服务的连接已断开。这可能是由于 EAM 服务或 vCenter 重新启动/停止或 EAM 服务中出现问题而导致。验证 vCenter 是否已启动，以及 vCenter 中的 EAM 服务是否正在运行。此外，我们可以通过查看 EAM mob 来验证 EAM 是否正常运行。(NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX vib on ESX. The connection to this EAM service has gone down. 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 依赖于 vCenter 中的 EAM 服务在 ESX 上部署/监控 NSX VIB。与该 EAM 服务的连接中断。这可能是由于 EAM 服务或 vCenter 已重新启动/停止，或者在 EAM 服务中出现问题。 措施：验证 vCenter 是否已启动以及 vCenter 中的 EAM 服务是否正在运行。验证是否可以访问 EAM MOB URL <code>http://{vCenter_IP}/eam/mob/</code> 以及 EAM 是否正常工作。有关详细信息，请参阅《NSX 故障排除指南》中的“基础架构准备”。

事件代码	事件严重性	触发的警报	事件消息	说明
250022	严重	否	NSX Manager 依赖于 VC 中的 EAM 服务来部署/监控 ESX 上的 NSX VIB。与此 EAM 服务的连接已断开。这可能是由于 EAM 服务或 VC 重新启动/停止或 EAM 服务中出现问题而导致。验证 VC 是否已启动，以及 VC 中的 EAM 服务是否正在运行。此外，我们可以通过查看 EAM mob 来验证 EAM 是否正常运行。(NSX Manager relies on the EAM service in VC for deploying/monitoring NSX vib on ESX. The connection to this EAM service has gone down. This could be due to EAM service or VC restart/stop or an issue in the EAM service. Verify that VC is up, and the EAM service in VC is running. Further, we can look at EAM mob to verify that EAM is functioning as expected.)	NSX Manager 依赖于 vCenter 中的 EAM 服务在 ESX 上部署/监控 NSX VIB。与该 EAM 服务的连接中断。这可能是由于 EAM 服务或 vCenter 已重新启动/停止，或者在 EAM 服务中出现问题。 措施：验证 vCenter 是否已启动以及 vCenter 中的 EAM 服务是否正在运行。验证是否可以访问 EAM MOB URL http://{vCenter_IP}/eam/mob/ 以及 EAM 是否正常工作。有关详细信息，请参阅《NSX 故障排除指南》中的“基础架构准备”。
250023	高	是	预卸载清除失败。请使用解决方案 API 来解决此警报。将移除服务。(Pre Uninstall cleanup failed. Use resolve API to resolve the Alarm. Service will be removed.)	在卸载之前执行的内部清理任务无法完成。 措施：使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。将移除服务。

事件代码	事件严重性	触发的警报	事件消息	说明
250024	高	是	找不到此部署单元的备份 EAM 代理。VC 服务可能仍在初始化。请尝试解决该警报以检查代理机构是否存在。如果您已手动删除了代理机构，请从 NSX 中删除部署单元条目。(The backing EAM agency for this deployment unit 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 unit entry from NSX.)	EAM 将 VIB 部署到 ESXi 主机上。将在每个 NSX 准备的群集上安装一个 EAM 代理。如果找不到该代理，则 vCenter Server 服务可能正在初始化，或者手动误删了该代理。
250025	高	是	尝试使用 EAM 升级或卸载无状态主机上的 NSX VIB 时会生成此事件。应使用自动部署功能准备所有无状态主机。请使用自动部署功能修复配置，并使用解决方案 API 来解决该警报。(This event is generated when an attempt is made to upgrade or uninstall NSX vib on stateless host using EAM. All stateless host should be prepared using the auto deploy feature. Fix configuration using auto deploy feature, and use the resolve API to resolve the alarm.)	在尝试使用 EAM 升级或卸载无状态主机上的 NSX VIB 时，将会生成该事件。应使用 Auto Deploy 功能准备所有无状态主机。措施：使用 Auto Deploy 功能修复配置，然后使用 systemalarms API 中的 action=resolve 参数解决该警报。

部署插件系统事件

下表介绍了部署插件的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
280000	高	是	部署插件 IP 池耗尽警报。(Deployment Plugin IP pool exhausted alarm.)	由于源 IP 池已耗尽，无法为 NSX 服务虚拟机分配 IP 地址。 措施：在该池中添加 IP 地址。
280001	高	是	部署插件一般警报。(Deployment Plugin generic alarm.)	每个服务（如 Guest Introspection）具有一组插件以在每个主机上配置该服务。插件代码中的任何问题将报告为一般警报。只有在服务的所有插件均成功后，该服务才会变为绿色。该事件捕获一部分可能的异常。 措施：使用 resolve API 解决该警报。将部署服务。

事件代码	事件严重性	触发的警报	事件消息	说明
280004	高	是	部署插件异常一般警报。(Deployment Plugin generic exception alarm.)	每个服务（如 Guest Introspection ）具有一组插件以在每个主机上配置该服务。插件代码中的任何问题将报告为一般异常警报。只有在服务的所有插件均成功后，该服务才会变为绿色。该事件捕获所有可能的异常。 措施：使用 resolve API 解决该警报。将部署服务。
280005	高	是	要使某些更改生效，需要重新引导虚拟机。(VM needs to be rebooted for some changes to be made/take effect.)	必须重新引导虚拟机以进行某些更改或使更改生效。 措施：使用 resolve API 解决该警报。这会重新引导虚拟机。

消息传递系统事件

下表介绍了与消息传递相关的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
39000 1	高	是	主机消息配置失败。(Host messaging configuration failed.)	在 ESX Agent Manager (EAM) 通知 NSX 已成功在 ESXi 主机上安装 NSX VIB 后，将在主机准备后设置 NSX 消息总线。该事件指示主机上的消息总线设置失败。从 NSX 6.2.3 开始，将在 安装 > 主机准备 选项卡上的受影响主机旁边显示一个红色错误图标。 措施：有关故障排除步骤，请参阅 NSX 故障排除指南 。
39000 2	高	是	主机消息连接重新配置失败。(Host messaging connection reconfiguration failed.)	在某些情况下， NSX 发现 RMQ 代理详细信息已更改，并尝试将最新的 RMQ 代理信息发送到主机。如果 NSX 无法发送该信息，则会发出该警报。 措施：有关故障排除步骤，请参阅 NSX 故障排除指南 。
39000 3	高	是	主机消息配置失败并跳过通知。(Host messaging configuration failed and notifications were skipped.)	在准备的主机连接回 vCenter Server 时， NSX 将再次尝试设置消息通道。该事件指示设置失败，并且未通知依赖于消息通道的其他 NSX 模块。 措施：有关故障排除步骤，请参阅 NSX 故障排除指南 。

事件代码	事件严重性	触发的警报	事件消息	说明
391002	严重	否	消息基础架构在主机上关闭。(Messaging infrastructure down on host.)	缺少 NSX Manager 和 NSX 主机之间的两个或更多检测信号消息。 措施：有关故障排除步骤，请参阅 NSX 故障排除指南。
321100	严重	否	禁用消息帐户 {account #}。密码已过期。(Disabling messaging account {account #}. Password has expired.)	在初始部署或主机准备后，用作消息总线客户端的 ESXi 主机、NSX Edge 虚拟机或 USVM 在预期时间（2 小时）内没有更改其 Rabbit MQ 密码。 措施：调查 NSX Manager 和消息总线客户端之间的通信问题。验证该客户端是否正在运行。在执行重新同步或重新部署之前，请收集相应的日志。有关故障排除步骤，请参阅 NSX 故障排除指南。

服务编排系统事件

下表介绍了服务编排的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
300000	严重	是	由于直接删除其从属 SecurityGroup，策略 {#} 也被删除。(Policy {#} is deleted as a result of explicit deletion of its dependent SecurityGroup.)	在删除从属安全组时，删除了一个服务策略。 措施：调查是否需要再次创建该安全策略。
300001	高	是	策略不同步。(Policy is out of sync.)	在尝试强制实施该服务策略上的规则时，服务编排遇到错误。 措施：查看错误消息以了解要在该策略中更改哪些规则的输入内容。 通过服务编排解决该警报，或者使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。
300002	高	是	此策略上的防火墙规则不同步。在解决该警报之前，将不会从此策略推送与防火墙相关的更改。(Firewall rules on this Policy are out of sync. No Firewall related changes from this policy will be pushed, until this alarm is resolved.)	该错误是由防火墙配置问题引起的。 措施：查看错误消息以了解导致该错误的策略和规则（如果可能）的详细信息。确保使用服务编排或 <code>resolve API</code> 解决该警报以同步该策略。另请参阅“在 NSX 6.x 中使用服务编排解决问题”(http://kb.vmware.com/kb/2132612)。

事件代码	事件严重性	触发的警报	事件消息	说明
300003	高	是	此策略上的网络自检规则不同步。在解决该警报之前，将不会从此策略推送与网络自检相关的更改。(Network Introspection rules on this Policy are out of sync. No Network Introspection related changes from this policy will be pushed, until this alarm is resolved.)	该错误是由网络自检配置问题引起的。 措施：查看错误消息以了解导致该错误的策略和规则（如果可能）的详细信息。确保使用服务编排或 <code>systemalarms API</code> 中的 <code>action=resolve</code> 参数解决该警报以同步该策略。另请参阅“在 NSX 6.x 中使用服务编排解决问题”(http://kb.vmware.com/kb/2132612)。 通过服务编排解决该警报，或者使用 <code>systemalarms API</code> 中的 <code>action=resolve</code> 参数解决该警报。
300004	高	是	此策略上的 Guest Introspection 规则不同步。在解决该警报之前，将不会从此策略推送与 Guest Introspection 相关的更改。(Guest Introspection rules on this Policy are out of sync. No Guest Introspection related changes from this policy will be pushed, until this alarm is resolved.)	该错误是由 Guest Introspection 配置问题引起的。 措施：查看错误消息以了解导致该错误的策略和规则（如果可能）的详细信息。确保使用服务编排或 <code>systemalarms API</code> 中的 <code>action=resolve</code> 参数解决该警报以同步该策略。另请参阅“在 NSX 6.x 中使用服务编排解决问题”(http://kb.vmware.com/kb/2132612)。
300005	高	是	服务编排不同步。将不会从服务编排向防火墙/网络自检推送任何更改。(Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection.)	在同步策略时，服务编排遇到错误。不会将任何更改发送到防火墙或网络自检服务。 措施：查看错误消息以确定要编辑的策略和/或防火墙区域。请通过服务编排或 <code>resolve API</code> 解决该警报。
300006	高	是	由于在执行重新引导操作时同步失败，服务编排不同步。(Service Composer is out of sync due to failure on sync on reboot operation.)	在重新引导时，服务编排在同步策略时遇到错误。不会将任何更改发送到防火墙或网络自检服务。 措施：查看错误消息以确定要编辑的策略和/或防火墙区域。通过服务编排解决该警报，或者使用 <code>systemalarms API</code> 中的 <code>action=resolve</code> 参数解决该警报。

事件代码	事件严重性	触发的警报	事件消息	说明
300007	高	是	由于回滚了防火墙中的草稿，服务编排不同步。将不会从服务编排向防火墙/网络自检推送任何更改。(Service Composer is out of sync due to rollback of drafts from Firewall. No changes from Service Composer will be pushed to Firewall/Network Introspection.)	在将防火墙规则集恢复为较早的草稿时，服务编排遇到同步错误。不会将任何更改发送到防火墙或网络自检服务。 措施：通过服务编排解决该警报，或者使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。
300008	高	是	在删除与策略对应的区域时失败。(Failure while deleting section corresponding to the Policy.)	在删除策略的防火墙规则区域时，服务编排遇到错误。在无法访问使用 NSX 服务插入的第三方服务的管理器时，将会出现该问题。 措施：调查到第三方服务管理器的连接问题。通过服务编排解决该警报，或者使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。
300009	高	是	在对区域重新排序以反映优先级变化时失败。(Failure while reordering section to reflect precedence change.)	在重新引导时，服务编排在同步策略时遇到错误。不会将任何更改发送到防火墙或网络自检服务。 措施：查看错误消息以确定要编辑的策略和/或防火墙区域。通过服务编排解决该警报，或者使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。
300010	高	是	在初始化自动保存草稿设置时失败。(Failure while initializing auto save drafts setting.)	在初始化自动保存的草稿设置时，服务编排遇到错误。 措施：查看错误消息以确定要编辑的策略和/或防火墙区域。通过服务编排解决该警报，或者使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。

GI SVM 系统事件

下表介绍了 Guest Introspection 通用服务虚拟机 (GI SVM) 操作的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
295002	主要			<p>NSX Manager 未从 Guest Introspection USVM 收到检测信号。</p> <p>措施：收集 NSX Manager 和 USVM 技术支持日志，并提交一个技术支持请求。</p>
295003	信息			<p>NSX Manager 从 USVM 收到检测信号。</p> <p>措施：在报告事件 295002 后恢复事件。</p>
295010	信息			<p>已建立 USVM 和 Guest Introspection 主机模块之间的连接。</p> <p>措施：仅信息事件。不需要采取任何措施。</p>

SVM 操作系统事件

下表介绍了服务虚拟机 (SVM) 操作的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
280002	高	是	NSX 丢失了此代理的某些事件。可能的原因是，重新引导或与 vCenter Server 的连接临时丢失。警告：解决此警报将删除虚拟机，并引发另一个警报，指示代理虚拟机丢失。如果按相同方式解决，则会重新部署虚拟机。(Some of the events for this agent were missed by NSX. Probably reason could be reboot or temporary connectivity loss with Vcenter Server.Warning: Resolving the alarm will delete the VM and raise another indicating agent VM is missing. Resolving same will redeploy the VM.)	部署的服务虚拟机遇到内部错误。 措施：解决该警报将删除虚拟机，并报告有关该删除的第二个警报。解决第二个警报将重新安装虚拟机。如果虚拟机重新部署失败，将再次报告原来的警报。如果再次出现该警报，请使用知识库文章 http://kb.vmware.com/kb/2144624 中的过程收集 SVM 日志并与 VMware 技术支持部门联系。
280003	高	是	NSX 丢失了此代理的某些事件。可能的原因是，重新引导或与 vCenter Server 的连接临时丢失。警告：解决此警报将重新启动虚拟机。(Some of the events for this agent were missed by NSX. Probably reason could be reboot or temporary connectivity loss with vCenter Server.Warning: Resolving the alarm will restart the VM.)	已重新启动部署的服务虚拟机。 措施：解决该警报将重新启动虚拟机。如果重新启动失败，则会再次出现该警报。请使用知识库文章 http://kb.vmware.com/kb/2144624 中的过程收集 SVM 日志并与 VMware 技术支持部门联系。
280006	高	是	无法将代理标记为可用。(Failed to mark agent as available.)	将 ESX 代理虚拟机标记为可用时出现内部错误。 措施：使用 <code>systemalarms</code> API 中的 <code>action=resolve</code> 参数解决该警报。如果无法解决该警报，请使用知识库文章 http://kb.vmware.com/kb/2144624 中的过程收集 SVM 日志并与 VMware 技术支持部门联系。

复制 - 通用同步系统事件

下表介绍了复制 - 通用同步的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
310001	严重	否	对象类型 {#} (位于 NSX Manager {#} 上) 的完全同步操作失败。(Full sync failed for object type {#} on NSX Manager {#}.)	在辅助 NSX Manager 上执行通用对象完全同步失败。 措施: 收集 NSX Manager 的技术支持日志并与 VMware 技术支持部门联系。
310003	严重	否	实体 {#} (位于 NSX Manager {#} 上) 的通用同步操作失败。(Universal sync operation failed for the entity {#} on NSX Manager {#}.)	在跨 vCenter 环境中将通用对象同步到辅助 NSX Manager 失败。 措施: 收集 NSX Manager 的技术支持日志并与 VMware 技术支持部门联系。

NSX 管理系统事件

下表介绍了 NSX 管理的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
320001	严重	否	NSX Manager IP 已分配给另一台具有 MAC 地址的计算机。(The NSX Manager IP has been assigned to another machine with the MAC Address.)	NSX Manager 管理 IP 地址已分配给同一网络上的某个虚拟机。在 6.2.3 之前，不会检测或禁止重复的 NSX Manager IP 地址。这可能会导致数据路径中断。在 6.2.3 和更高版本中，在检测到重复的地址时，将发出该事件。 措施: 解决重复的地址问题。

逻辑网络系统事件

下表介绍了与逻辑网络相关的系统事件消息。

事件代码	事件严重性	触发的警报	事件消息	说明
814	严重	否	逻辑交换机 {#} 的配置不再正确，因为某些后备分布式虚拟端口组已修改和/或移除。(Logical Switch {#} is no longer properly configured since some of the backing distributed virtual port groups were modified and/or removed.)	已修改或删除一个或多个支持 NSX 逻辑交换机的 DVS 端口组，或者更改逻辑交换机控制层面模式失败。 措施：如果该事件是删除或修改端口组触发的，则会在 vSphere Web Client 的“逻辑交换机”页面上显示一个错误。请单击该错误以创建缺少的 DVS 端口组。如果该事件是由于更改控制层面模式失败触发的，请再次执行更新。请参阅《NSX 升级指南》中的“更新传输区域和逻辑交换机”。
1900	严重	否	主机上的 VXLAN 初始化失败。(VXLAN initialization failed on the host.)	VXLAN 初始化失败，因为无法为所需数量的 VTEP 配置 VMkernel 网卡。NSX 准备用户为 VXLAN 选择的 DVS，并创建一个 DV 端口组以供 VTEP VMkernel 网卡使用。成组、负载平衡方法、MTU 和 VLAN ID 是在 VXLAN 配置期间选择的。成组和负载平衡方法必须与为 VXLAN 选择的 DVS 配置相匹配。 措施：查看 vmkernel.log。另请参阅《NSX 故障排除指南》中的“基础架构准备”部分。
1901	严重	否	主机上的 VXLAN 端口初始化失败。(VXLAN port initialization failed on the host.)	无法在关联的 DV 端口上配置 VXLAN，并且已断开连接该端口。NSX 准备用户为 VXLAN 选择的 DVS，并创建一个 DV 端口组以供每个配置的逻辑交换机使用。 措施：查看 vmkernel.log。另请参阅《NSX 故障排除指南》中的“基础架构准备”部分。
1902	严重	否	主机上不存在 VXLAN 实例。(VXLAN instance does not exist on the host.)	在尚未为 VXLAN 启用 ESXi 主机上的 DVS 时，DV 端口收到 VXLAN 配置。 措施：查看 vmkernel.log。另请参阅《NSX 故障排除指南》中的“基础架构准备”部分。
1903	严重	否	逻辑交换机 {#} 无法正常工作，因为后备 IP 接口无法加入特定多播组。(Logical Switch {#} can't work properly since the backing IP interface couldn't join specific multicast group.)	VTEP 接口无法加入指定的多播组。将影响到某些主机的流量，直到解决了该问题。NSX 使用定期重试机制（每 5 秒一次）以加入多播组。 措施：查看 vmkernel.log。另请参阅《NSX 故障排除指南》中的“基础架构准备”部分。
1905	严重	否	传输区域 {#} 可能无法使用，因为后备 IP 接口无法获取正确的 IP 地址。(Transport Zone may not be used since the backing IP interface can't acquire correct IP Address.)	没有为 VTEP VMkernel 网卡分配有效的 IP 地址。将丢弃通过 VMkernel 网卡的所有 VXLAN 流量。 措施：如果使用 DHCP 为 VMKNic 分配 IP，请确认在 VXLAN 传输 VLAN 上具有 DHCP。请参阅“NSX 主机准备失败并出现错误：IP 池中的 IP 地址不足”(http://kb.vmware.com/kb/2137025)。

事件代码	事件严重性	触发的警报	事件消息	说明
1906	严重	否	DVS 上缺少 VXLAN 覆盖类。(VXLAN overlay class is missing on DVS.)	在为 VXLAN 配置 DVS 时，未安装 NSX VIB。所有 VXLAN 接口无法连接到 DVS。 措施：请参阅“在 NSX/VCNS 环境中升级后出现网络连接问题”(http://kb.vmware.com/kb/2107951)。
1920	严重	否	由于无法建立连接，VXLAN 控制器 {#} 已移除。请检查控制器 IP 配置，然后重新部署。(VXLAN Controller {#} has been removed due to the connection can't be built, please check controller IP configuration and deploy again.)	控制器部署失败。 措施：检查是否可以访问分配的 IP 地址。另请参阅《NSX 故障排除指南》中的“NSX Controller”部分。
1930	严重	否	控制器 {#} 无法与节点 {#} 建立连接 (active={#})。当前连接状态 = {#}。(The controller {#} cannot establish the connection to the node {#}(active={#}). Current connection status = {#}.)	两个控制器节点已断开连接，这会影响控制器之间的通信。 措施：请参阅《NSX 故障排除指南》中的“NSX Controller”部分。
1935	严重	否	无法将主机 {#} 信息发送到控制器，因为所有控制器均处于非活动状态。当控制器变为活动状态后，可能需要进行控制器同步。(Host {#} information could not be sent to controllers as all controllers are inactive. Controller synchronization may be needed once controllers become active.)	无法将主机证书信息发送到 NSX Controller 群集。主机和控制器群集之间的通信通道可能会出现意外的行为。 措施：在准备 ESXi 主机之前，确认 NSX Controller 群集状态为正常。请使用 controller sync API 解决该问题。
1937	严重	否	主机 {#} 中的 VXLAN vmknics {#} [PortGroup = {#}] 缺失或已删除。(VXLAN vmknics {#} [PortGroup = {#}] is missing or deleted from host {#}.)	在主机中缺少 VXLAN VMkernel 网卡或已将其删除。将影响与主机之间的流量。 措施：要解决该问题，请单击 安装 > 逻辑网络准备 > VXLAN 传输 选项卡上的 解决 按钮。

事件代码	事件严重性	触发的警报	事件消息	说明
1939	严重	否	VXLAN vmknics {#} [PortGroup = {#}] 可能已从主机 {#} 上删除，或者主机与 vCenter 之间的连接可能出现了问题。(VXLAN vmknics {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues.)	NSX Manager 检测到在 Virtual Center 上缺少 VXLAN VMkernel 网卡。这可能是由 vCenter Server 到主机的通信问题引起的。此外，在重新引导 vCenter Server 或主机时，NSX Manager 在很短的时间内检测不到 VXLAN VMkernel 网卡并标记该事件。在 vCenter Server 和主机完成重新引导后，NSX Manager 将再次检查 VXLAN VMkernel 网卡，如果一切正常，则会清除该事件。 措施：如果这不是临时性问题，请单击 安装 > 逻辑网络准备 > VXLAN 传输 选项卡上的 解决 按钮以解决该问题。
1941	严重	否	主机连接状态已更改：事件代码：{#}，主机：{#}（ID：{#}），NSX Manager - 防火墙代理：{#}，NSX Manager - 控制层面代理：{#}，控制层面代理 - 控制器：{#}。（Host Connection Status Changed: Event Code: {#}, Host: {#} (ID: {#}), NSX Manager - Firewall Agent: {#}, NSX Manager - Control Plane Agent: {#}, Control Plane Agent - Controllers: {#}。）	NSX Manager 检测到以下连接之一处于关闭状态： NSX Manager 到主机防火墙代理、NSX Manager 到主机控制层面代理或主机控制层面代理到 NSX Controller。 措施：如果 NSX Manager 到主机防火墙代理的连接关闭，请检查 NSX Manager 和防火墙代理日志 (/var/log/vsfwd.log)，或发送 POST https://NSX-Manager-IP-Address/api/2.0/nwfabric/configure?action=synchronize REST API 调用以重新同步该连接。如果 NSX Manager 到控制层面代理的连接关闭，请检查 NSX Manager 和控制层面代理日志 (/var/log/netcpa.log)。如果控制层面代理到 NSX Controller 的连接关闭，请导航到 网络和安全 > 安装 并检查主机连接状态。
1942	严重	否	LogicalSwitch {#} 的后备端口组 [moid = {#}] 标记为缺失。(The backing portgroup [moid = {#}] of LogicalSwitch {#} is marked as missing.)	NSX Manager 检测到在 Virtual Center 中缺少 NSX 逻辑交换机的支持 DV 端口组。 措施：单击 安装 > 逻辑网络准备 > VXLAN 传输 选项卡上的 解决 按钮，或者使用 REST API (POST https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate) 重新创建该端口组。
1945	严重	否	控制器 {#} 上的设备 {#} 已打开磁盘延迟警报。(The device {#} on controller {#} has the disk latency alert on.)	NSX Manager 检测到 NSX Controller 具有较高的磁盘延迟。 措施：请参阅《NSX 故障排除指南》中的“NSX Controller”部分。
1946	信息	否	控制器 {0} 上的所有磁盘延迟警报均已关闭。(All disk latency alerts on controller {0} are off.)	NSX Manager 不再检测控制器上的高磁盘延迟。 措施：仅信息事件。不需要采取任何措施。

事件代码	事件严重性	触发的警报	事件消息	说明
1947	严重	否	vCenter 上的控制器虚拟机已关闭电源。(Controller Virtual Machine is powered off on vCenter.)	NSX Manager 检测到已从 Virtual Center 中关闭 NSX Controller 虚拟机电源。控制器群集状态可能变为已断开连接，这会影响需要使用正常工作的群集的任何操作。 措施：在 安装 > 管理 选项卡上单击控制器的 解决 按钮，或者调用 API POST https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate 以打开控制器虚拟机电源。
1948	严重	否	已从 vCenter 中删除控制器虚拟机。(Controller Virtual Machine is deleted from vCenter.)	NSX Manager 检测到已从 Virtual Center 中删除 NSX Controller 虚拟机。控制器群集状态可能变为已断开连接，这会影响需要使用正常工作的群集的任何操作。 措施：在 安装 > 管理 选项卡上单击控制器的 解决 按钮，或者调用 API POST https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate 以在 NSX Manager 数据库中移除控制器的状态。
1952	严重	否	VXLAN 端口组 [moid = dvportgroup-xx] 和相关的 DVS 具有不同的绑定策略。(The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies.)	NSX Manager 检测到 VXLAN 端口组的绑定策略与关联的 DVS 的绑定策略不同。这可能会导致无法预测的行为。 措施：重新配置 VXLAN 端口组或 DVS，以便它们具有相同的绑定策略。

身份防火墙系统事件

下表介绍了身份防火墙 (IDFW) 的系统事件消息，这些消息具有“主要”、“严重”或“高”严重性。

事件代码	事件严重性	触发的警报	事件消息	说明
395000	严重	否	域控制器事件日志服务器上的安全日志已满。(SecurityLog on Domain Controller Eventlog Server is Full.)	Active Directory 事件日志服务器中的安全日志已满。在配置为使用日志提取时，IDFW 将停止工作。 措施：与 Active Directory 服务器管理员联系并增加安全日志大小，清除安全日志或存档安全日志。

主机准备系统事件

下表介绍了与主机准备相关的所有系统事件消息。

注 多个 ESX Agent Manager 事件映射到 NSX 上的单个事件。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	信息	是	VIB 模块已上载到主机 {hostID}，但在将主机 {hostID} 置于维护模式之前不会完全安装该模块。ESX Agent Manager 将主机置于维护模式。(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 puts host in the maintenance mode.) 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	严重	是	需要在主机上部署代理虚拟机，但由于 vSphere ESX Agent Manager 无法访问代理的 OVF 软件包，无法部署代理虚拟机。发生这种情况通常是因为，提供 OVF 软件包的 Web 服务器已关闭。该 Web 服务器通常位于创建代理机构的解决方案内部。(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 重新部署代理。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	严重	是	需要在主机上部署代理 VIB 模块，但由于 vSphere ESX Agent Manager 无法访问代理的 VIB 软件包，无法部署 VIM 模块。发生这种情况通常是因为，提供 VIB 软件包的 Web 服务器已关闭。该 Web 服务器通常位于创建代理机构的解决方案内部。(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 重新安装 VIB 模块。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要在主机上部署代理虚拟机，但由于与主机 {hostID} 不兼容，无法部署代理。(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 重新部署代理。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。 不过，在升级主机或解决方案以使代理与主机兼容之前，该问题可能一直存在。
270000	高	是	需要打开代理虚拟机电源，但在代理的虚拟机 IP 地址池中没有可用的 IP 地址。(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.)	措施：要解决该问题，请释放一些 IP 地址或在 IP 池中再添加一些 IP 地址，然后使用 systemalarms API 中的 action=resolve 参数解决该警报。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	需要在主机上部署代理虚拟机，但由于主机 {hostID} 没有足够的可用 CPU 或内存资源，无法部署代理虚拟机。(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 重新部署代理虚拟机。 不过，在提供足够的 CPU 和内存资源之前，该问题可能一直存在。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要在主机上部署代理虚拟机，但由于主机的代理数据存储空间没有足够的可用空间，无法部署代理虚拟机。(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 重新部署代理虚拟机。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。 不过，在采取以下措施之前，该问题可能一直存在： 在主机的代理虚拟机数据存储上释放一些空间。 或 配置具有足够可用空间的新代理虚拟机数据存储。
270000	高	是	需要打开代理虚拟机电源，但由于在代理的虚拟机网络上没有定义任何 IP 地址，已关闭代理虚拟机电源。(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.)	措施：在代理的虚拟机网络上创建一个 IP 池，然后使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要在主机上部署代理虚拟机，但由于未在主机 {hostID} 上配置代理数据存储，无法部署代理。(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}.)	措施：您必须在主机上配置代理虚拟机数据存储。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	需要在主机上部署代理虚拟机，但由于未在主机上配置代理网络，无法部署代理。(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.)	措施：您必须在主机上配置代理虚拟机网络。
270000	高	是	需要在主机上部署代理虚拟机，但由于未在主机上配置代理网络，无法部署代理。需要将主机添加到 customAgentVmNetwork 中列出的网络之一。(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.)	措施：您必须将其中的一个 <i>customAgentVmNetwork</i> 网络添加到主机中。
270000	高	是	需要在主机上部署代理虚拟机，但由于未在主机上配置代理数据存储，无法部署代理。需要将主机添加到 customAgentVmDatastore 中列出的数据存储之一。(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 .)	措施：您必须将其中的一个名为 <i>customAgentVmDatastore</i> 的数据存储添加到主机中。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	在 vCenter Server 中不再注册创建代理机构的解决方案。(The solution that created the agency is no longer registered with the vCenter server.)	ESX Agent Manager 移除代理机构。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	在主机上存在 dvFilter 交换机，但主机上的代理均不依赖于 dvFilter。如果在更改代理机构配置时主机断开连接，通常会发生这种情况。(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 移除 dvFilterSwitch。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要在主机上置备代理虚拟机，但由于 OVF 软件包置备失败，无法执行该操作。在已升级或修补提供 OVF 软件包的解决方案以提供代理虚拟机的有效 OVF 软件包之前，置备不太可能会成功。(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 再次尝试进行 OVF 置备。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要打开代理虚拟机电源，但缺少 OVF 属性或具有无效的值。(An agent virtual machine needs to be powered on, but an OVF property is either missing or has an invalid value.)	措施：在用于置备代理虚拟机的代理配置中更新 OVF 环境。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	在 vCenter 清单中找到不属于该 vSphere ESX Agent Manager 服务器实例中的任何代理机构的代理虚拟机。(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 关闭代理虚拟机电源（如果已打开电源）并删除该虚拟机。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	VIB 模块要求主机处于维护模式，但 vSphere ESX Agent Manager 无法将主机置于维护模式。如果无法移动在主机上运行的虚拟机，则可能会发生这种情况，必须在主机进入维护模式之前将其停止。(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 尝试将主机置于维护模式。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。 不过，在关闭虚拟机电源或移动虚拟机以将主机置于维护模式之前，该问题可能一直存在。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	严重	是	需要在主机上安装 VIB 模块，但由于 VIB 软件包具有无效的格式，无法安装该模块。在已升级或修补提供该软件包的解决方案以提供有效的 VIB 软件包之前，安装不太可能会成功。(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 再次尝试进行 VIB 安装。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要在主机上安装 VIB 模块，但未安装该模块。通常，更具体的问题（该问题的子类）指示 VIB 模块安装失败的特定原因。(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 再次尝试进行 VIB 安装。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	信息	是	已将 VIB 模块上载到主机中，但在重新引导主机后才会激活该模块。(A VIB module has been uploaded to the host, but will not be activated until the host is rebooted.)	ESX Agent Manager 将主机置于维护模式并重新引导主机。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	无法安装 VIB 模块，原因是不允许 vSphere ESX Agent Manager 在主机上进行自动安装。(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.)	措施：转到 vSphere Update Manager 并在主机上安装所需的公告，或者将公告添加到主机的映像配置文件中。有关更多详细信息，请参阅 vSphere 文档。
270000	高	是	无法卸载 VIB 模块，原因是不允许 vSphere ESX Agent Manager 在主机上进行自动卸载。(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.)	措施：转到 vSphere Update Manager 并在主机上卸载所需的公告，或者从主机的映像配置文件中删除公告。有关更多详细信息，请参阅 vSphere 文档。
270000	高	是	代理虚拟机已损坏。(An agent virtual machine is corrupt.)	ESX Agent Manager 删除并重新置备代理虚拟机。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。 要手动解决这个问题，请解决与缺少的文件相关的问题，然后打开代理虚拟机电源。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	<p>需从主机中移除代理虚拟机，但并未移除代理虚拟机。通常，更具体的问题（该问题的子类）指示 vSphere ESX Agent Manager 无法移除代理虚拟机的特定原因，例如，主机处于维护模式，已关闭电源或处于待机模式。(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.)</p>	<p>ESX Agent Manager 重新部署代理。</p> <p>措施：单击主机准备 (Host Preparation)选项卡上的解决 (Resolve)选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。</p>
270000	高	是	<p>代理虚拟机是一个虚拟机模板。(An agent virtual machine is a virtual machine template.)</p>	<p>ESX Agent Manager 将代理虚拟机模板转换为虚拟机。</p> <p>措施：单击主机准备 (Host Preparation)选项卡上的解决 (Resolve)选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。</p>

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	需要在主机上部署代理虚拟机，但并未部署代理虚拟机。通常，更具体的问题（该问题的子类）指示 vSphere ESX Agent Manager 无法部署代理的特定原因，例如，无法访问代理的 OVF 软件包或缺少主机配置。如果从主机中明确删除代理虚拟机，则也会出现该问题。（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 重新部署代理虚拟机。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要打开代理虚拟机电源，但已关闭代理虚拟机电源。（An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off.）	ESX Agent Manager 打开代理虚拟机电源。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	需要关闭代理虚拟机电源，但已打开代理虚拟机电源。（An agent virtual machine is expected to be powered off, but the agent virtual machine is powered on.）	ESX Agent Manager 关闭代理虚拟机电源。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。

事件代码	事件严重性	触发的警报	事件消息	说明
270000	高	是	需要关闭代理虚拟机电源，但代理虚拟机已挂起。(An agent virtual machine is expected to be powered on, but the agent virtual machine is suspended.)	ESX Agent Manager 打开代理虚拟机电源。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	代理虚拟机需要位于指定的代理虚拟机文件夹中，但位于其他文件夹中。(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 将代理虚拟机移回到指定的代理文件夹中。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	代理虚拟机需要位于指定的代理虚拟机资源池中，但位于其他资源池中。(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 将代理虚拟机移回到指定的代理资源池中。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。
270000	高	是	收到 EAM 警报。(EAM alarm received.)	ESX Agent Manager 检测到 NSX VIB 或服务虚拟机出现 NSX 安装或升级问题。 措施：单击 主机准备 (Host Preparation) 选项卡上的 解决 (Resolve) 选项，或者使用 systemalarms API 中的 action=resolve 参数解决该警报。