

NSX 로깅 및 시스템 이벤트

업데이트 5

2017년 11월 16일에 수정됨

VMware NSX Data Center for vSphere 6.3



vmware®

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

VMware 웹 사이트에서는 최신 제품 업데이트도 제공합니다.

본 문서에 대한 의견이 있으시면 다음 주소로 피드백을 보내주십시오.

docfeedback@vmware.com

VMware, Inc.

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

VMware 코리아

서울시 강남구
영동대로 517
아셈타워 13층
(우) 06164
전화: +82 2 3016 6500
팩스: +82 2 3016 6501
www.vmware.com/kr

목차

NSX 로깅 및 시스템 이벤트 4

1 시스템 이벤트, 경고 및 로그 5

시스템 이벤트 5

경고 6

NSX 구성 요소의 로깅 수준 설정 8

감사 로그 10

Syslog 서버 구성 11

기술 지원 로그 수집 13

2 NSX 및 호스트 로그 16

NSX 로그 정보 16

Firewall 로그 17

라우팅 관련 NSX 로그 22

Guest Introspection 로그 24

3 시스템 이벤트 32

보안 시스템 이벤트 33

분산 방화벽 시스템 이벤트 34

NSX Edge 시스템 이벤트 41

패브릭 시스템 이벤트 48

배포 플러그인 시스템 이벤트 55

메시징 시스템 이벤트 56

Service Composer 시스템 이벤트 57

GI SVM 시스템 이벤트 60

SVM Operations 시스템 이벤트 61

복제 - 범용 동기화 시스템 이벤트 63

NSX 관리 시스템 이벤트 63

논리적 네트워크 시스템 이벤트 63

ID 방화벽 시스템 이벤트 68

호스트 준비 시스템 이벤트 68

NSX 로깅 및 시스템 이벤트

NSX 로깅 및 시스템 이벤트 문서에서는 NSX Manager 사용자 인터페이스 및 vSphere Web Client를 사용하여 VMware NSX[®] for vSphere[®] 시스템의 로그 메시지, 이벤트 및 경보에 대해 설명합니다.

대상 사용자

이 설명서는 VMware vCenter 환경에서 NSX를 사용하거나 문제를 해결하려는 모든 사용자를 대상으로 합니다. 이 설명서의 정보는 가상 시스템 기술 및 가상 데이터 센터 작업에 익숙한 숙련된 시스템 관리자를 대상으로 작성되었으며, 이 설명서에서는 VMware ESXi, vCenter Server 및 vSphere Web Client를 포함하는 VMware vSphere에 익숙하다고 가정합니다.

VMware 기술 자료 용어집

VMware 기술 자료 사이트에서는 새로운 용어를 정리한 용어집을 제공하고 있습니다. VMware 기술 설명서에 사용된 용어에 대한 정의를 보려면 <http://www.vmware.com/support/pubs>를 참조하십시오.

시스템 이벤트, 경보 및 로그

시스템 이벤트, 경보 및 로그를 사용하여 NSX 환경의 상태 및 보안을 모니터링하고 문제를 해결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- 시스템 이벤트
- 경보
- NSX 구성 요소의 로깅 수준 설정
- 감사 로그
- Syslog 서버 구성
- 기술 지원 로그 수집

시스템 이벤트

시스템 이벤트는 시스템 작업의 레코드입니다. 각 이벤트에는 정보 또는 위험과 같이 이벤트가 얼마나 심각한지를 나타내는 심각도 수준이 지정되어 있습니다. 시스템 이벤트는 SNMP 트랩으로도 표시되므로 SNMP 관리 소프트웨어에서 NSX 시스템 이벤트를 모니터링할 수 있습니다.

시스템 이벤트 보고서 보기

vSphere Web Client에서 NSX Manager를 통해 관리되는 모든 구성 요소에 대한 시스템 이벤트를 볼 수 있습니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열의 NSX Manager를 클릭한 후 **모니터** 탭을 클릭합니다.
- 4 **시스템 이벤트** 탭을 클릭합니다.

열 머리글의 화살표를 클릭하여 이벤트를 정렬하거나 **필터** 텍스트 상자를 사용하여 이벤트를 필터링할 수 있습니다.

시스템 이벤트 형식

Syslog 서버를 지정할 경우 NSX Manager에서는 모든 시스템 이벤트를 Syslog 서버로 보냅니다. 이러한 메시지는 아래 표시된 메시지와 비슷한 형식을 갖습니다.

```
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'
```

시스템 이벤트는 다음 정보를 포함합니다.

```
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.
```

경보

경보는 이벤트, 일련의 조건 또는 개체의 상태에 대한 응답으로 활성화되는 알림입니다. 다른 경고와 함께 경보가 NSX 대시보드 및 vSphere Web Client UI의 다른 화면에 표시됩니다.

GET api/2.0/services/systemalarms API를 사용하여 NSX 개체에 대한 경보를 볼 수 있습니다.

NSX는 경보에 대해 다음 2가지 방법을 지원합니다.

- 경보는 시스템 이벤트에 해당하며, 연결된 해결 기능이 경보를 트리거하는 문제를 해결하려고 합니다. 이 접근법은 네트워크 및 보안 패브릭 배포(예: EAM, 메시지 버스, 배포 플러그인)용으로 설계되었으며 Service Composer에서도 지원됩니다. 이러한 경보는 이벤트 코드를 경보 코드로 사용합니다. 자세한 내용은 NSX 로깅 및 시스템 이벤트 문서를 참조하십시오.
- Edge 알림 경보는 트리거 및 해결 정보 쌍으로 구성됩니다. 이 방법은 IPSec VPN, 로드 밸런서, 고가용성, 상태 점검, Edge 파일 시스템 및 리소스 예약을 비롯한 몇 가지 Edge 기능에서 지원됩니다. 이러한 경보는 이벤트 코드와는 다른 고유한 경보 코드를 사용합니다. 자세한 내용은 NSX 로깅 및 시스템 이벤트 문서를 참조하십시오.

일반적으로 경보는 오류 조건이 수정되면 시스템에서 자동으로 삭제됩니다. 일부 경보는 구성 업데이트 시 자동으로 지워지지 않습니다. 문제가 해결되면 경보를 수동으로 지워야 합니다.

다음은 경보를 지우기 위해 사용할 수 있는 API의 예입니다.

특정 소스(예: 클러스터, 호스트, 리소스 풀, 보안 그룹 또는 NSX Edge)에 대한 경보가 발생할 수 있습니다. sourceId별로 소스에 대한 경보를 봅니다.

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

sourceId별로 소스에 대한 모든 경보를 해결합니다.

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

메시지 버스, 배포 플러그인, Service Composer 및 Edge 경보를 비롯한 NSX 경보를 볼 수 있습니다.

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

alarmId별로 특정 NSX 경보를 볼 수 있습니다.

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

alarmId별로 특정 NSX 경보를 해결할 수 있습니다.

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

API에 대한 자세한 내용은 NSX API 가이드를 참조하십시오.

경보 형식

API를 통해 경보 형식을 볼 수 있습니다.

경보 형식에는 다음 정보가 포함됩니다.

```
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 경보

경보는 vCenter Server 관리자에게 주의가 필요한 Guest Introspection 이벤트에 대해 신호를 보냅니다. 경보 상태가 더 이상 존재하지 않을 경우 경보가 자동으로 취소됩니다.

사용자 지정 vSphere 플러그인 없이 vCenter Server 경보를 표시할 수 있습니다. 이벤트 및 경보에 대한 자세한 내용은 vCenter Server 관리 가이드를 참조하십시오.

vCenter Server 확장으로 등록된 NSX Manager는 SVM, Guest Introspection 모듈 및 Thin Agent의 세 개의 Guest Introspection 구성 요소로부터 수신되는 이벤트에 기반하여 경보를 생성하고 제거하는 규칙을 정의합니다. 규칙은 사용자 지정할 수 있습니다. 경보에 대한 새 사용자 지정 규칙을 생성하는 방법에 대한 지침은 vCenter Server 설명서를 참조하십시오. 경우에 따라 여러 가지 원인 때문에 경보가 발생할 수도 있습니다. 다음 표에는 가능한 원인과 이를 해결하기 위해 취할 수 있는 조치 작업이 나열되어 있습니다.

호스트 정보

호스트 정보는 Guest Introspection 모듈의 상태에 영향을 미치는 이벤트에 의해 생성됩니다.

표 1-1. 오류(빨간색 표시)

가능한 원인	작업
Guest Introspection 모듈이 호스트에 설치되었지만 더 이상 상태를 NSX Manager에 보고하지 않습니다.	<ol style="list-style-type: none"> 1 호스트에 로그인하고 <code>/etc/init.d/vShield-Endpoint-Mux start</code> 명령을 입력하여 Guest Introspection이 실행 중인지 확인합니다. 2 Guest Introspection이 NSX Manager에 연결할 수 있도록 네트워크가 적절히 구성되었는지 확인합니다. 3 NSX Manager를 재부팅합니다.

SVM 정보

SVM 정보는 SVM의 상태에 영향을 미치는 이벤트에 의해 생성됩니다.

표 1-2. 빨간색 SVM 정보

문제	작업
Guest Introspection 모듈과 프로토콜 버전이 일치하지 않습니다.	Guest Introspection 모듈 및 SVM의 프로토콜이 서로 호환되는지 확인하십시오.
Guest Introspection이 SVM에 연결할 수 없습니다.	SVM의 전원이 켜져 있고 네트워크가 올바르게 구성되었는지 확인하십시오.
게스트가 연결되었는데도 SVM이 상태를 보고하지 않습니다.	내부 오류입니다. VMware 지원 담당자에게 문의하십시오.

NSX 구성 요소의 로깅 수준 설정

각 NSX 구성 요소의 로깅 수준을 설정할 수 있습니다.

지원되는 수준은 여기에 표시된 것처럼 구성 요소마다 다릅니다.

```
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 VPN에 대한 로깅 사용

모든 IPSec VPN 트래픽 로깅을 사용하도록 설정할 수 있습니다.

기본적으로 로깅이 사용되도록 설정되고 주의 수준으로 설정됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리(Manage)** 탭을 클릭한 후 **VPN** 탭을 클릭합니다.
- 5 **IPSec VPN**을 클릭합니다.
- 6 **로깅 정책(Logging Policy)** 옆의 을 클릭하고 **로깅 사용(Enable logging)**을 클릭하여 로컬 서버넷과 피어 서버넷 간의 트래픽 흐름을 기록하도록 설정하고 로깅 수준을 선택합니다.
- 7 로그 수준을 선택하고 **변경 내용 게시(Publish Changes)**를 클릭합니다.

SSL VPN-Plus 로그

SSL VPN-Plus Gateway 로그는 NSX Edge Appliance에 구성된 Syslog 서버로 전송됩니다.

SSL VPN-Plus 클라이언트 로그는 원격 사용자 컴퓨터의 다음 디렉토리에 저장됩니다.

%PROGRAMFILES%/VMWARE/SSL VPN Client/.

SSL VPN-Plus Client 로그 및 로그 수준 변경

- 1 **SSL VPN-Plus** 탭에서 왼쪽 패널에 있는 **서버 설정(Server Settings)**을 클릭합니다.
- 2 [로깅 정책] 섹션으로 이동한 후 섹션을 확장하여 현재 설정을 봅니다.
- 3 **변경(Change)**을 클릭합니다.
- 4 **로깅 사용(Enable logging)** 확인란을 선택하여 로깅을 사용하도록 설정합니다.

또는

로깅 사용(Enable logging) 확인란을 선택 취소하여 로깅을 사용하지 않도록 설정합니다.

- 5 필요한 로그 수준을 선택합니다.

참고 SSL VPN-Plus 클라이언트 로그는 기본적으로 사용되지 않도록 설정되며 로그 수준은 [알림]으로 설정됩니다.

- 6 **확인(OK)**을 클릭합니다.

감사 로그

감사 로그는 NSX Manager에 로그인한 사용자가 수행하는 모든 작업을 기록합니다.

감사 로그 보기

감사 로그 탭에서는 모든 NSX Manager 사용자가 수행한 작업을 보여 줍니다. NSX Manager는 최대 10만 개의 감사 로그를 보관합니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **Networking & Security 인벤토리** 아래에서 **NSX Managers**를 클릭합니다.
- 3 이름 열에서 NSX 서버를 클릭한 후, **모니터** 탭을 클릭합니다.
- 4 **감사 로그** 탭을 클릭합니다.
- 5 감사 로그에 대한 세부 정보가 있을 경우 해당 로그의 **작업** 열에서 텍스트를 클릭할 수 있습니다. 감사 로그 세부 정보를 보려면 **작업** 열의 텍스트를 클릭합니다.
- 6 **감사 로그 변경 세부 정보**에서 **변경된 행**을 선택하면 이 감사 로그 작업에서 값이 변경된 속성만 표시됩니다.

Syslog 서버 구성

syslog 서버를 NSX 구성 요소 및 호스트의 로그 저장소로 구성할 수 있습니다.

NSX Manager 에 대한 Syslog 서버 구성

Syslog 서버를 지정할 경우 NSX Manager는 모든 감사 로그 및 시스템 이벤트를 Syslog 서버로 보냅니다.

Syslog 데이터는 설치와 구성 작업 중의 문제 해결과 기록된 데이터 검토에 유용합니다.

NSX Edge는 2개의 Syslog 서버를 지원합니다. NSX Manager 및 NSX Controller는 하나의 Syslog 서버를 지원합니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
웹 브라우저에서 `https://<nsx-manager-ip>` 또는 `https://<nsx-manager-hostname>`의 NSX Manager 장치 GUI로 이동하여 NSX Manager 설치 중에 설정한 암호를 사용하여 admin 권한으로 로그인합니다.
- 2 홈 페이지에서 **장치 설정 관리(Manage Appliance Settings) > 일반(General)**을 클릭합니다.
- 3 **Syslog 서버(Syslog Server)** 옆의 **편집(Edit)**을 클릭합니다.

- 4 syslog 서버의 IP 주소 또는 호스트 이름, 포트 및 프로토콜을 입력합니다.

예 :

- 5 확인(OK)을 클릭합니다.

NSX Manager 원격 로깅은 사용하도록 설정되어 있고, 로그는 독립형 syslog 서버에 저장되어 있습니다.

NSX Edge 에 대한 Syslog 서버 구성

하나 또는 두 개의 원격 Syslog 서버를 구성할 수 있습니다. NSX Edge 장치에서 생성되는 방화벽 이벤트 관련 NSX Edge 이벤트 및 로그는 Syslog 서버로 전송됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge를 두 번 클릭합니다.
- 4 **관리** 탭을 클릭한 후 **설정** 탭을 클릭합니다.
- 5 **세부 정보** 패널에서 Syslog 서버 옆의 **변경**을 클릭합니다.
- 6 두 원격 Syslog 서버의 IP 주소를 입력하고 프로토콜을 선택합니다.
- 7 **확인**을 클릭하여 구성을 저장합니다.

NSX Controller용 Syslog 서버 구성

NSX Controller용 Syslog 서버를 구성할 경우 NSX Manager는 모든 감사 로그 및 시스템 이벤트를 Syslog 서버로 보냅니다. Syslog 데이터는 설치와 구성 작업 중의 문제 해결과 기록된 데이터 검토에 유용합니다. NSX Controller에서 syslog 서버를 구성할 때는 NSX API를 사용하는 방법만 지원됩니다. VMware에서는 syslog의 프로토콜로 UDP를 사용하는 것을 권장합니다.

절차

- 1 NSX Controller에서 syslog를 사용하도록 설정하려면 다음 NSX API를 사용하십시오. 이 API는 컨트롤러 syslog 내보내기를 추가하고 지정된 컨트롤러 노드에서 syslog 내보내기를 구성합니다.

```
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 다음 NSX API를 사용하여 컨트롤러 syslog 내보내기를 쿼리하고 지정된 컨트롤러 노드의 구성된 syslog 내보내기에 대한 세부 정보를 검색할 수 있습니다.

```
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 필요하지 않은 경우 다음 NSX API를 사용하여 지정된 컨트롤러 노드에서 컨트롤러 syslog 내보내기를 삭제할 수 있습니다.

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

다음에 수행할 작업

API에 대한 자세한 내용은 NSX API 가이드를 참조하십시오.

기술 지원 로그 수집


경우에 따라 VMware에 문제를 보고하기 위해 NSX 구성 요소 및 호스트에서 기술 지원 로그를 수집해야 할 수 있습니다.

호스트 기술 지원 로그를 수집하려면 export host-tech-support 명령(NSX 문제 해결 가이드의 “분산 방화벽 문제 해결” 참조)을 실행하십시오.

NSX용 기술 지원 로그 다운로드

NSX Manager 시스템 로그 및 Web Manager 로그를 데스크톱에 다운로드할 수 있습니다.

절차

- 1 NSX Manager 가상 장치에 로그인합니다.
- 2 장치 관리에서 **장치 설정 관리**를 클릭합니다.
- 3 을 클릭하고 **기술 지원 로그 다운로드**를 클릭합니다.
- 4 **다운로드**를 클릭합니다.
- 5 로그를 다운로드할 준비가 되면 **저장**을 클릭하여 로그를 데스크톱에 다운로드합니다.
로그가 압축되고 파일 확장명 .gz가 붙습니다.


다음에 수행할 작업

파일을 저장한 디렉토리에서 **모든 파일**을 찾아보고 압축 해제 유틸리티를 사용해 로그를 열 수 있습니다.

NSX Edge 에 대한 기술 지원 로그 다운로드

각 NSX Edge 인스턴스에 대한 기술 지원 로그를 다운로드할 수 있습니다. NSX Edge 인스턴스에 대해 고가용성을 사용하도록 설정한 경우 두 NSX Edge 가상 시스템의 지원 로그가 모두 다운로드됩니다.

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.
- 3 NSX Edge 인스턴스를 선택합니다.
- 4 **작업**()을 클릭하고 **기술 지원 로그 다운로드**를 선택합니다.
- 5 기술 지원 로그가 생성되면 **다운로드**를 클릭합니다.

NSX Controller용 기술 지원 로그 다운로드

각 NSX Controller 인스턴스에 대한 기술 지원 로그를 다운로드할 수 있습니다. 이러한 제품별 로그에는 분석을 위한 진단 정보가 포함되어 있습니다.

NSX Controller 로그를 수집하려면:

절차

- 1 vSphere Web Client에 로그인합니다.
- 2 **Networking & Security**를 클릭한 다음 **설치**를 클릭합니다.
- 3 **관리**에서 로그를 다운로드하려는 컨트롤러를 선택합니다.
- 4 **기술 지원 로그 다운로드**를 클릭합니다.

5 다운로드를 클릭합니다.

NSX Manager는 NSX Controller 로그 다운로드를 시작하고 잠금을 획득합니다.

참고 한 번에 NSX Controller 로그를 하나씩 다운로드합니다. 첫 번째 로그 다운로드가 완료되면 다른 로그 다운로드를 시작합니다. 여러 컨트롤러에서 동시에 로그를 다운로드하면 오류가 발생할 수 있습니다.

6 로그를 다운로드할 준비가 되면 **저장**을 클릭하여 로그를 데스크톱에 다운로드합니다.

로그가 압축되고 .gz 파일 확장명이 붙습니다.

이제 다운로드한 로그를 분석할 수 있습니다.

다음에 수행할 작업

VMware 기술 지원에 대한 진단 정보를 업로드하려면 [기술 지원 문서 2070100](#)을 참조하십시오.

NSX 및 호스트 로그

다양한 NSX 구성 요소 및 호스트에 있는 로그를 사용하여 문제를 감지하고 해결할 수 있습니다.

본 장은 다음 항목을 포함합니다.

- NSX 로그 정보
- Firewall 로그
- 라우팅 관련 NSX 로그
- Guest Introspection 로그

NSX 로그 정보

syslog 서버를 구성하고 각 NSX 구성 요소에 대한 기술 지원 로그를 확인할 수 있습니다. 관리부 로그는 NSX Manager를 통해 제공되고 데이터부 로그는 vCenter Server를 통해 제공됩니다. 따라서 syslog 서버의 로그를 확인할 때 완전한 정보를 파악할 수 있도록 NSX 구성 요소 및 vCenter Server에 대해 동일한 syslog 서버를 지정하는 것이 좋습니다.

vCenter Server에서 관리되는 호스트에 대해 syslog 서버를 구성하는 방법에 대한 자세한 내용은 <https://docs.vmware.com>에서 적절한 vSphere 설명서 버전을 참조하십시오.

참고 로그를 수집하고 NSX DLR(논리적 분산 라우터) 제어 VM에 액세스하는 데 사용되는 Syslog 또는 점프 서버는 해당 DLR의 논리적 인터페이스에 직접 연결되는 논리적 스위치에 있을 수 없습니다.

표 2-1. NSX 로그

구성 요소	설명
ESXi 로그	이러한 로그는 vCenter Server에서 생성된 VM 지원 번들의 일부로 수집됩니다. ESXi 로그 파일에 대한 자세한 내용은 vSphere 설명서를 참조하십시오.
NSX Edge 로그	NSX Edge CLI에서 show log [follow reverse] 명령을 사용합니다. NSX Edge UI를 통해 기술 지원 로그 번들을 다운로드합니다.
NSX Manager 로그	NSX Manager CLI에서 show log CLI 명령을 사용합니다. NSX Manager 가상 장치 UI를 통해 기술 지원 로그 번들을 다운로드합니다.
라우팅 로그	NSX 로깅 및 시스템 이벤트 가이드를 참조하십시오.

표 2-1. NSX 로그 (계속)

구성 요소	설명
Firewall 로그	Firewall 로그 를 참조하십시오.
Guest Introspection 로그	Guest Introspection 로그 를 참조하십시오.

NSX Manager

syslog 서버를 지정하려면 [NSX Manager에 대한 Syslog 서버 구성](#) 항목을 참조하십시오.

기술 지원 로그를 다운로드하려면 [NSX용 기술 지원 로그 다운로드](#) 항목을 참조하십시오.

NSX Edge

syslog 서버를 지정하려면 [NSX Edge에 대한 Syslog 서버 구성](#) 항목을 참조하십시오.

기술 지원 로그를 다운로드하려면 [NSX Edge에 대한 기술 지원 로그 다운로드](#) 항목을 참조하십시오.

NSX Controller

syslog 서버를 지정하려면 [NSX Controller용 Syslog 서버 구성](#) 항목을 참조하십시오.

기술 지원 로그를 다운로드하려면 [NSX Controller용 기술 지원 로그 다운로드](#) 항목을 참조하십시오.

방화벽

자세한 내용은 [Firewall 로그](#)를 참조하십시오.

Firewall 로그

Firewall은 감사 로그, 규칙 메시지 로그 및 시스템 이벤트 로그와 같은 로그 파일을 생성하고 저장합니다. 방화벽을 사용하도록 설정된 각 클러스터에 대해 syslog 서버를 구성해야 합니다. syslog 서버는 Syslog.global.logHost 특성에 지정되어 있습니다.

방화벽은 다음 표에 설명된 대로 로그를 생성합니다.

표 2-2. Firewall 로그

로그 유형	설명	위치
규칙 메시지 로그	각 규칙에 대해 허용 또는 거부된 트래픽 같은 모든 액세스 결정 사항이 포함됩니다(해당 규칙에 대한 로깅이 사용하도록 설정된 경우). 로깅이 사용되도록 설정된 규칙에 대한 DFW 패킷 로그를 포함합니다.	/var/log/dfwpktlogs.log
감사 로그	관리 로그 및 분산 방화벽 구성 변경 사항이 포함됩니다.	/home/secureall/secureall/logs/vsm.log
시스템 이벤트 로그	적용된 분산 방화벽 구성, 생성 또는 삭제되거나 실패한 필터, 보안 그룹에 추가된 가상 시스템 등이 포함됩니다.	/home/secureall/secureall/logs/vsm.log

표 2-2. Firewall 로그 (계속)

로그 유형	설명	위치
데이터부/VMKernel 로그	방화벽 커널 모듈(VSIP)과 관련된 작업을 캡처합니다. 시스템에서 생성된 메시지에 대한 로그 항목이 포함됩니다.	/var/log/vmkernel.log
메시지 버스 클라이언트/VSFWD 로그	방화벽 에이전트의 활동을 캡처합니다.	/var/log/vsfwd.log

참고 vsm.log 파일은 NSX Manager CLI(명령줄 인터페이스)에서 show log manager 명령을 실행하고 키워드 vsm.log에 대해 grep를 수행하여 액세스할 수 있습니다. 이 파일은 루트 권한이 있는 사용자 또는 사용자 그룹에서만 액세스할 수 있습니다.

규칙 메시지 로그

규칙 메시지 로그에는 각 규칙에 대해 허용 또는 거부된 트래픽 같은 모든 액세스 결정 사항이 포함됩니다(해당 규칙에 대한 로깅이 사용하도록 설정된 경우). 이러한 로그는 각 호스트의 /var/log/dfwpktlogs.log에 저장됩니다.

방화벽 로그 메시지의 예는 다음과 같습니다.

```
# 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
```

자세한 예:

```
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
```

다음 예에서 각각의 의미는 다음과 같습니다.

- 1002는 분산 방화벽 규칙 ID입니다.
- domain-c7은 vCenter MOB(Managed Object Browser)에서의 클러스터 ID입니다.
- 192.168.110.10/138은 소스 IP 주소입니다.
- 192.168.110.255/138은 대상 IP 주소입니다.
- RULE_TAG는 방화벽 규칙을 추가 또는 편집하는 동안 **태그** 텍스트 상자에 추가하는 텍스트의 예입니다.

다음 예에서는 192.168.110.10에서 172.16.10.12로의 ping 결과를 보여 줍니다.

```
# 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
```

다음 표에서는 방화벽 로그 메시지의 텍스트 상자에 대해 설명합니다.

표 2-3. 로그 파일 항목의 구성 요소

구성 요소	예제 값
타임 스탬프	2017-04-11T21:09:59
방화벽 관련 부분	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

표 2-4. 로그 파일 항목의 방화벽 특정 부분

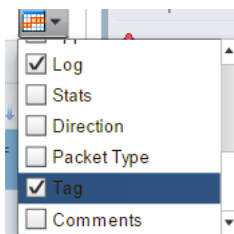
엔티티	가능한 값
필터 헤시	필터 이름 및 기타 정보를 가져오는 데 사용할 수 있는 숫자입니다.
AF 값	INET, INET6
이유	<ul style="list-style-type: none"> match: 패킷이 규칙과 일치하는지 확인합니다. bad-offset: 패킷을 가져오는 동안 데이터 경로 내부 오류가 발생했습니다. fragment: 첫 번째 조각으로 어셈블된 후 첫 번째가 아닌 조각입니다. short: 패킷이 너무 짧습니다(예를 들어 IP 헤더 또는 TCP/UDP 헤더를 포함하는 데 완전하지 않은 경우도 포함). normalize: 올바른 헤더 또는 페이로드가 없는 잘못된 형식의 패킷입니다. memory: 데이터 경로의 메모리가 부족합니다. bad-timestamp: 잘못된 TCP 타임 스탬프입니다. proto cksum: 잘못된 프로토콜 체크섬입니다. state-mismatch: TCP 상태 시스템을 확인을 통과하지 못한 TCP 패킷입니다. state-insert: 중복된 연결이 발견되었습니다. state-limit: 데이터 경로에서 추적할 수 있는 최대 상태 수에 도달했습니다. SpoofGuard: SpoofGuard에서 패킷을 삭제했습니다. TERM: 연결이 종료됩니다.
작업	<ul style="list-style-type: none"> PASS: 패킷을 수락합니다. DROP: 패킷을 삭제합니다. NAT: SNAT 규칙입니다. NONAT: SNAT 규칙과 일치하는 항목을 찾았으나 주소를 변환할 수 없습니다. RDR: DNAT 규칙입니다. NORDR: DNAT 규칙과 일치하는 항목을 찾았으나 주소를 변환할 수 없습니다. PUNT: 현재 VM의 동일한 하이퍼바이저에서 실행되는 서비스 VM으로 패킷을 보냅니다. REDIRECT: 현재 VM의 하이퍼바이저 외부에서 실행되는 네트워크 서비스에 패킷을 보냅니다. COPY: 패킷을 수락하고 현재 VM의 동일한 하이퍼바이저에서 실행되는 서비스 VM을 복사합니다. REJECT: 패킷을 거부합니다.

표 2-4. 로그 파일 항목의 방화벽 특정 부분 (계속)

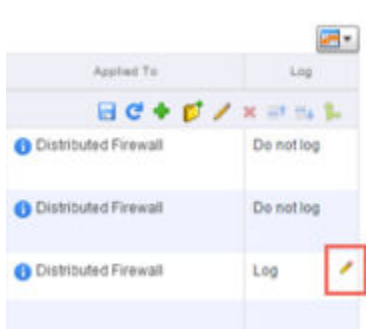
엔티티	가능한 값
규칙 집합 및 규칙 ID	규칙 집합/규칙 ID
방향	IN, OUT
패킷 길이	길이
프로토콜	TCP, UDP, ICMP 또는 PROTO(프로토콜 번호) TCP 연결의 경우 연결이 종료되는 실제 이유는 키워드 TCP 다음에 표시됩니다. TERM이 TCP 세션의 원인인 경우 PROTO 행에 추가 설명이 표시됩니다. TCP 연결 종료의 가능한 원인에는 RST(TCP RST 패킷), FIN(FIN TCP 패킷) 및 TIMEOUT(너무 오랫동안 유휴 상태임)이 포함됩니다. 위 예제에서는 RST입니다. 따라서 재설정해야 하는 연결에 RST 패킷이 있음을 의미합니다. TCP 이외의 연결(UDP, ICMP 또는 다른 프로토콜)에서는 연결 종료 이유가 TIMEOUT뿐입니다.
소스 IP 주소 및 포트	IP 주소/포트
대상 IP 주소 및 포트	IP 주소/포트
TCP 플래그	S (SYN), SA (SYN-ACK), A (ACK), P (PUSH), U (URGENT), F (FIN), R (RESET)
패킷 수	패킷의 수입입니다. 22/14 - 수신 패킷/송신 패킷
바이트 수	바이트의 수입입니다. 7684/1070 - 수신 바이트/송신 바이트

규칙 메시지를 사용하도록 설정하려면 vSphere Web Client에 로그인합니다.

1 Networking & Security > 방화벽 페이지에서 로그 열을 사용하도록 설정합니다.



- 2 [로그] 테이블 셀 위로 마우스를 이동하고 연필 아이콘을 클릭하여 로깅을 사용하도록 규칙을 설정합니다.



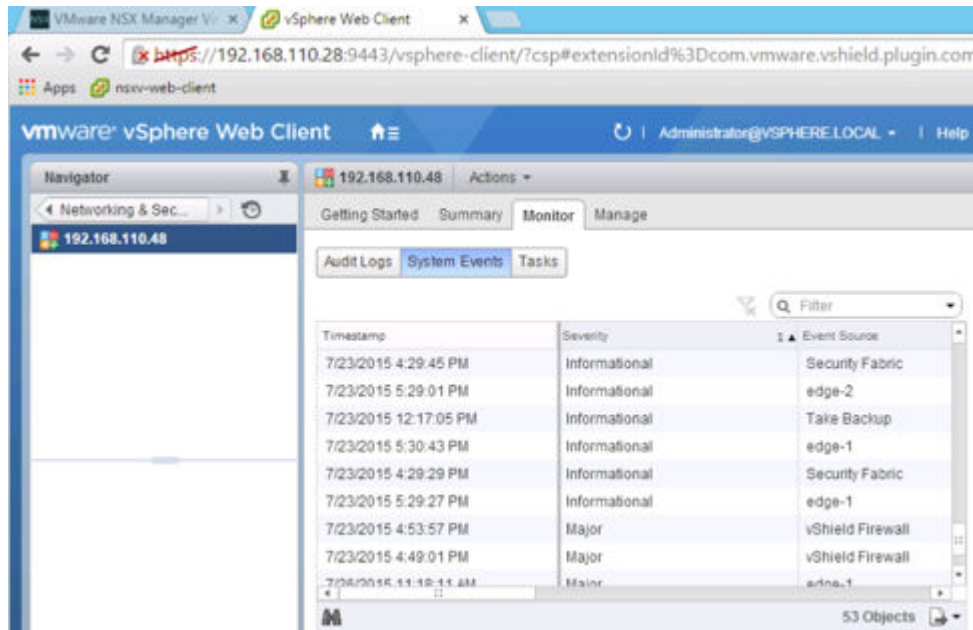
참고 사용자 지정된 텍스트를 방화벽 로그 메시지에 표시하려는 경우 **태그** 열을 사용하도록 설정하고 연필 아이콘을 클릭하여 필요한 텍스트를 추가할 수 있습니다.

감사 및 시스템 이벤트 로그

감사 로그에는 관리 로그 및 분산 방화벽 구성 변경 사항이 포함됩니다. 이 로그는 /home/secureall/secureall/logs/vsm.log에 저장됩니다.

시스템 이벤트 로그에는 적용된 분산 방화벽 구성, 생성 또는 삭제되거나 실패한 필터, 보안 그룹에 추가된 가상 시스템 등이 포함됩니다. 이러한 로그는 /home/secureall/secureall/logs/vsm.log에 저장됩니다.

UI에서 감사 및 시스템 이벤트 로그를 보려면 **Networking & Security > 설치 > 관리**로 이동한 다음 NSX Manager의 IP 주소를 두 번 클릭합니다. 그런 다음 **모니터** 탭을 클릭합니다.



자세한 내용은 NSX 로깅 및 시스템 이벤트를 참조하십시오.

라우팅 관련 NSX 로그

모범 사례는 로그를 중앙 수집기로 보내도록 NSX의 모든 구성 요소를 구성하는 것입니다. 그러면 중앙 수집기에서 이러한 구성 요소가 검사될 수 있습니다.

필요한 경우 NSX 구성 요소의 로그 수준을 변경할 수 있습니다. 자세한 내용은 NSX 로깅 및 시스템 이벤트에서 “NSX 구성 요소의 로깅 수준 설정” 항목을 참조하십시오.

NSX Manager 로그

- NSX Manager CLI에서 `show log`
- NSX Manager UI를 통해 수집된 기술 지원 로그 번들

NSX Manager Virtual Appliance Management



NSX Manager 로그에는 CRUD(생성, 읽기, 업데이트 및 삭제) 작업을 포함하는 관리부 관련 정보가 포함됩니다.

컨트롤러 로그

컨트롤러에는 여러 모듈이 포함되어 있으며 많은 경우에 자체 로그 파일이 있습니다. 컨트롤러 로그는 `show log <log file> [filtered-by <string>]` 명령을 사용하여 액세스할 수 있습니다. 라우팅과 관련된 로그 파일은 다음과 같습니다.

- `cloudnet/cloudnet_java-vnet-controller.<start-time-stamp>.log`: 이 로그는 구성 및 내부 API 서버를 관리합니다.
- `cloudnet/cloudnet.nsx-controller.log`: 컨트롤러 주 프로세스 로그입니다.
- `cloudnet/cloudnet_cpp.log.nsx-controller.log`: 이 로그는 클러스터링 및 부트스트랩을 관리합니다.
- `cloudnet/cloudnet_cpp.log.ERROR`: 이 파일은 오류가 발생하는 경우에 생깁니다.

컨트롤러 로그는 상세 로그로 대부분의 경우 까다로운 문제 상황에서 문제 해결을 지원하기 위해 VMware 엔지니어링 팀이 소집될 때만 필요합니다.

`show log` CLI 외에 `watch log <logfile> [filtered-by <string>]` 명령을 사용하여 개별 로그 파일이 업데이트될 때 실시간으로 로그 파일을 확인할 수 있습니다.

로그는 NSX UI에서 컨트롤러 노드를 선택하고 **기술 지원 로그 다운로드(Download tech support logs)** 아이콘을 클릭하여 생성 및 다운로드할 수 있는 컨트롤러 지원 번들에 포함되어 있습니다.

ESXi 호스트 로그

ESXi 호스트에서 실행되는 NSX 구성 요소는 다음과 같은 몇 가지 로그 파일을 작성합니다.

- VMkernel 로그: /var/log/vmkernel.log
- 제어부 에이전트 로그: /var/log/netcpa.log
- 메시지 버스 클라이언트 로그: /var/log/vsfwd.log

또한 vCenter Server에서 생성된 VM 지원 번들의 일부로 로그를 수집할 수도 있습니다. 로그 파일은 루트 권한이 있는 사용자 또는 사용자 그룹에서만 액세스할 수 있습니다.

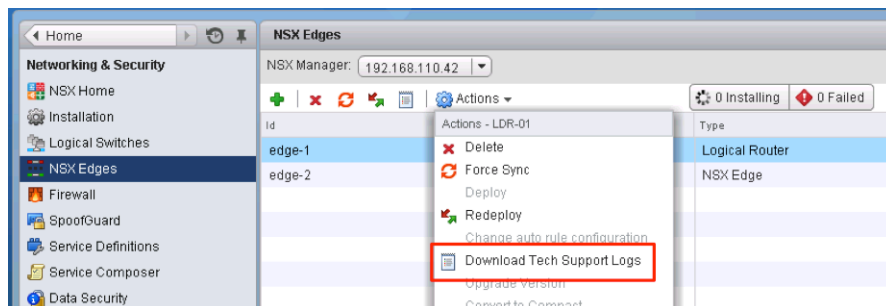
ESG/DLR 제어 VM 로그

ESG 및 DLR 제어 VM의 로그 파일에 액세스하는 방법에는 두 가지가 있습니다. 하나는 CLI를 사용하여 표시하는 것이고 다른 하나는 CLI 또는 UI를 사용하여 기술 지원 번들을 다운로드하는 것입니다.

로그를 표시하기 위한 CLI 명령은 `show log [follow | reverse]`입니다.

기술 지원 번들을 다운로드하려면:

- CLI에서 enable 모드를 입력하고 `export tech-support <[scp | ftp]> <URI>` 명령을 실행합니다.
- vSphere Web Client의 **작업(Actions)** 메뉴에서 **기술 지원 로그 다운로드(Download Tech Support Logs)** 옵션을 선택합니다.



기타 유용한 파일 및 해당 위치

엄격히 말해서 로그는 아니지만 NSX 라우팅을 이해하고 관련 문제를 해결하는 데 도움이 될 수 있는 많은 파일이 있습니다.

- 제어부 에이전트 구성(/etc/vmware/netcpa/config-by-vsm.xml)에는 다음 구성 요소에 대한 정보가 포함되어 있습니다.
 - 컨트롤러 IP 주소, TCP 포트, 인증서 지문, SSL 사용/사용 안 함
 - VXLAN을 사용하여 DVS가 사용되도록 설정된 dvUplink(팀 구성 정책, 이름, UUID)
 - 호스트가 알고 있는 DLR 인스턴스(DLR ID, 이름)
- 제어부 에이전트 구성(/etc/vmware/netcpa/netcpa.xml)에는 로깅 수준(기본적으로 **정보(info)**)을 비롯하여 netcpa에 대한 다양한 구성 옵션이 포함되어 있습니다.

- 제어부 인증서 파일: /etc/vmware/ssl/rui-for-netcpa.*
 - 2개의 파일: 호스트 인증서 및 호스트 개인 키
 - 컨트롤러에 대한 호스트 연결을 인증하는 데 사용

이러한 모든 파일은 vsfwd에서 제공하는 메시지 버스 연결을 통해 NSX Manager에서 수신된 정보를 사용하여 제어부 에이전트에서 만듭니다.

Guest Introspection 로그

Guest Introspection 문제를 해결하는 동안 사용할 수 있는 여러 가지 로그를 캡처할 수 있습니다.

ESX GI 모듈(MUX) 로그

ESXi 호스트의 가상 시스템에서 Guest Introspection이 작동하지 않거나 호스트에 SVA와의 통신과 관련된 경보가 발생하는 경우 ESXi 호스트의 ESX GI 모듈에 문제가 있는 것일 수 있습니다.

로그 경로 및 샘플 메시지

MUX 로그 경로

/var/log/syslog

var/run/syslog.log

ESX GI 모듈(MUX) 메시지는 <timestamp>EPSecMUX<[ThreadID]>: <message> 형식을 따릅니다.

예:

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

위 예에서 각각의 의미는 다음과 같습니다.

- [ERROR]는 메시지의 유형입니다. 다른 유형으로 [DEBUG], [INFO]가 있습니다.
- (EPSEC)는 메시지가 끝점 보안과 관련되어 있음을 나타냅니다.

로그 파일 사용 및 보기

호스트에 설치된 ESX GI 모듈 VIB의 버전을 확인하려면 #esxcli software vib list | grep epsec-mux 명령을 실행합니다.

전체 로깅을 설정하려면 ESXi 호스트 명령 셸에서 다음 단계를 수행합니다.

- 1 ps -c |grep Mux 명령을 실행하여 현재 실행 중인 ESX GI 모듈 프로세스를 찾습니다.

예:

```
~ # 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 서비스가 실행되지 않는 경우 `/etc/init.d/vShield-Endpoint-Mux start` 또는 `/etc/init.d/vShield-Endpoint-Mux restart` 명령을 사용하여 다시 시작할 수 있습니다.
- 3 `watchdog.sh` 프로세스를 포함하여 실행 중인 ESX GI 모듈 프로세스를 중지하려면 `~ # kill -9 192223 192233 192236` 명령을 실행합니다.
두 ESX GI 모듈 프로세스가 생성됩니다.
- 4 새 `-d` 옵션을 사용하여 ESX GI 모듈을 시작합니다. `epsec-mux` 빌드 5.1.0-01255202 및 5.1.0-01814505 ~ `# /usr/lib/vmware/vShield-Endpoint-Mux -d 900 -c 910`의 경우 옵션 `-d`가 없습니다.
- 5 ESXi 호스트에서 `/var/log/syslog.log` 파일의 ESX GI 모듈 로그 메시지를 확인합니다. 글로벌 솔루션, 솔루션 ID, 포트 번호에 해당하는 항목이 올바르게 지정되었는지 확인합니다.

예제: 샘플 muxconfig.xml 파일

```
<?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>
```

```

<listen0>ip</listen0>

<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>

<listen0>ip</listen0>

<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 Thin Agent 로그

Thin Agent는 VM 게스트 OS에 설치되고 사용자 로그인 세부 정보를 감지합니다.

로그 경로 및 샘플 메시지

Thin Agent는 GI 드라이버인 vsepflt.sys, vnetflt.sys, vnetwfp.sys(Windows 10 이상)로 구성되어 있습니다.

Thin Agent 로그는 VCenter 로그 번들의 일부로 ESXi 호스트에 있습니다. 로그 경로는 /vmfs/volumes/<datastore>/<vmname>/vmware.log입니다.

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

Thin Agent 메시지는 <timestamp> <VM Name><Process Name><[PID]>: <message> 형식을 따릅니다.

Guest: vnet or Guest:vsep 아래의 로그 예제에서는 해당 GI 드라이버와 관련된 로그 메시지와 디버그 메시지를 차례로 표시합니다.

예:

```

2017-10-17T14:25:19.877Z| vcpu-0| l125: Guest: vnet: AUDIT: DriverEntry :
vnetFilter build-4325502 loaded
2017-10-17T14:25:20.282Z| vcpu-0| l125: Guest: vsep:
AUDIT: VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T14:25:20.375Z| vcpu-0| l125:
Guest: vsep: AUDIT: DriverEntry : vfileFilter build-4286645 loaded

2017-10-17T18:22:35.924Z| vcpu-0| l125: Guest: vsep: AUDIT:
VFileSocketMgrConnectHelper : Mux is connected
2017-10-17T18:24:05.258Z| vcpu-0| l125: Guest: vsep: AUDIT:
VFileFltPostOpCreate : File (\\Windows\\System32\\Tasks\\Microsoft\\Windows\\
SoftwareProtectionPlatform\\SvcRestartTask) in a transaction, ignore

```

예제: vShield Guest Introspection Thin Agent 드라이버 로깅 사용

디버그 설정은 vmware.log 파일을 조절하는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

이 절차에서는 Windows 레지스트리를 수정해야 합니다. 레지스트리를 수정하기 전에 레지스트리 백업을 생성해야 합니다. 레지스트리 백업 및 복원에 대한 자세한 내용은 Microsoft 기술 자료 문서 [136393](#)을 참조하십시오.

Thin Agent 드라이버에 대한 디버그 로깅을 사용하도록 설정하려면:

- 1 **시작 > 실행(Start > Run)**을 클릭합니다. regedit를 입력하고 **확인(OK)**을 클릭합니다. 레지스트리 편집기 창이 열립니다. 자세한 내용은 Microsoft 기술 자료 문서 [256986](#)을 참조하십시오.
- 2 레지스트리 편집기를 사용하여 다음 키를 생성합니다.
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\fltmc\Parameters
- 3 새로 생성된 매개 변수 키 아래에 이러한 DWORD를 생성합니다. 이러한 값을 입력할 때는 16진수를 선택해야 합니다.

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

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

log_level 매개 변수 키의 다른 값:

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

- 4 관리자 권한으로 명령 프롬프트를 엽니다. 다음 명령을 실행하여 vShield Endpoint 파일 시스템 미니 드라이버를 언로드했다가 다시 로드합니다.

- fltmc unload vsepflt
- fltmc load vsepflt

가상 시스템에 있는 vmware.log 파일에서 로그 항목을 찾을 수 있습니다.

vShield GI 네트워크 검사 드라이버 로깅 사용

디버그 설정은 vmware.log 파일을 조절할 수 있는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

이 절차에서는 Windows 레지스트리를 수정해야 합니다. 레지스트리를 수정하기 전에 레지스트리 백업을 생성해야 합니다. 레지스트리 백업 및 복원에 대한 자세한 내용은 Microsoft 기술 자료 문서 [136393](#)을 참조하십시오.

- 1 **시작 > 실행(Start > Run)**을 클릭합니다. regedit를 입력하고 **확인(OK)**을 클릭합니다. 레지스트리 편집기 창이 열립니다. 자세한 내용은 Microsoft 기술 자료 문서 [256986](#)을 참조하십시오.

2 레지스트리를 편집합니다.

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

3 가상 시스템을 재부팅합니다.

vsepfilt.sys 및 vnetflt.sys 로그 파일 위치

log_dest 레지스트리 설정 DWORD: 0x00000001을 사용하여 Endpoint Thin Agent 드라이버가 디버거에 로깅합니다. 디버거(SysInternals 또는 windbg의 DbgView)를 실행하여 디버그 출력을 캡처합니다.

또는 log_dest 레지스트리 설정 DWORD:0x000000002를 설정할 수 있습니다. 이 경우 드라이버 로그는 ESXi 호스트의 해당 가상 시스템 폴더에 있는 vmware.log 파일에 인쇄됩니다.

UMC 로깅 사용

Guest Introspection UMC(사용자 모드 구성 요소)는 보호된 가상 시스템의 VMware Tools 서비스 내에서 실행됩니다.

- 1 Windows XP 및 Windows Server 2003에서는 경로 C:\Documents and Settings\All Users\Application Data\VMware\VMware Tools\tools.conf에 존재하지 않을 경우 tools config 파일을 생성합니다.
- 2 Windows Vista, Windows 7 및 Windows Server 2008에서는 경로 C:\ProgramData\VMware\VMware Tools\tools.conf에 존재하지 않을 경우 tools config 파일을 생성합니다.
- 3 tools.conf 파일에 다음 줄을 추가하여 UMC 구성 요소 로깅을 사용하도록 설정합니다.

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

vsep.handler = vmx 설정에서 UMC 구성 요소는 ESXi 호스트의 해당 가상 시스템 폴더에 있는 vmware.log 파일에 로그인합니다.

다음 설정 로그를 사용하면 UMC 구성 요소 로그가 지정한 로그 파일에 인쇄됩니다.

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

GI EPSecLib 및 SVM 로그

EPSecLib는 ESXi 호스트 ESX GI 모듈(MUX)에서 이벤트를 수신합니다.

로그 경로 및 샘플 메시지

EPSecLib 로그 경로

/var/log/syslog

var/run/syslog

EPSecLib 메시지는 <timestamp> <VM Name><Process Name><[PID]>: <message> 형식을 따릅니다.

[ERROR] 아래의 예제는 메시지의 유형이고 (EPSEC)는 Guest Introspection에만 관련되는 메시지를 나타냅니다.

예:

```
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.
```

로그 수집

GI SVM 내 구성 요소인 EPSec 라이브러리에 대한 디버그 로깅을 사용하도록 설정하려면:

- 1 NSX Manager에서 콘솔 암호를 가져와 GI SVM에 로그인합니다.
- 2 /etc/epseclib.conf 파일을 생성하고 다음을 추가합니다.


```
ENABLE_DEBUG=TRUE
ENABLE_SUPPORT=TRUE
```
- 3 chmod 644 /etc/epseclib.conf 명령을 실행하여 사용 권한을 변경합니다.
- 4 /usr/local/sbin/rcusvm restart 명령을 실행하여 GI-SVM 프로세스를 다시 시작합니다.

이렇게 하면 GI SVM에서 EPSecLib에 대해 디버그 로깅을 사용하도록 설정되고, NSX for vSphere 6.2.x 및 6.3.x에 적용할 수 있는 /var/log/messages에서 디버그 로그를 찾을 수 있습니다. 디버그 설정은 vmware.log 파일을 조절할 수 있는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

GI SVM 로그

로그를 캡처하기 전에 호스트 ID 또는 호스트 MOID를 확인합니다.

- NSX Manager에서 show cluster all 및 show cluster <cluster ID> 명령을 실행합니다.

예:

```
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 현재 로깅 상태를 확인하려면 다음 명령을 실행합니다.

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

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

- 2 현재 로깅 상태를 변경하려면 다음 명령을 실행합니다.

```
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 로그를 생성하려면 다음 명령을 실행합니다.

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

Send 및 Download를 선택합니다.

이 명령은 GI SVM 로그를 생성하고 파일을 techsupport logs.log.gz 파일로 저장합니다. 디버그 설정은 vmware.log 파일을 조절할 수 있는 지점까지 플러딩할 수 있으므로 필요한 모든 정보를 수집한 후에는 바로 디버그 모드를 사용하지 않도록 설정하는 것이 좋습니다.

시스템 이벤트

NSX의 모든 구성 요소는 시스템 이벤트를 보고합니다. 이러한 이벤트는 해당 환경의 상태 및 보안을 모니터링하고 문제를 해결하는 데 도움이 될 수 있습니다.

각 이벤트 메시지는 다음 정보를 포함합니다.

- 고유한 이벤트 코드
- 심각도 수준
- 이벤트에 대한 설명 및 권장 작업(해당되는 경우)

기술 지원 로그 수집 및 VMware 지원 서비스에 문의

일부 이벤트의 경우 권장되는 작업으로 기술 지원 로그 수집, VMware 지원 서비스에 문의가 있습니다.

- NSX Manager 기술 지원 로그를 수집하려면 [NSX용 기술 지원 로그 다운로드](#)를 참조하십시오.
- NSX Edge 기술 지원 로그를 수집하려면 [NSX Edge에 대한 기술 지원 로그 다운로드](#)를 참조하십시오.
- 호스트 기술 지원 로그를 수집하려면 export host-tech-support 명령(NSX 문제 해결 가이드의 “분산 방화벽 문제 해결” 참조)을 실행하십시오.
- VMware 지원 서비스에 문의하려면 “My VMware에 지원 요청을 파일하는 방법”(<http://kb.vmware.com/kb/2006985>)을 참조하십시오.

NSX Edge 에서 강제 동기화 수행

일부 이벤트의 경우 권장되는 작업으로 NSX Edge에 대한 강제 동기화 수행이 있습니다. 자세한 내용은 NSX 관리 가이드에서 “NSX Edge를 NSX Manager와 강제 동기화”를 참조하십시오. 강제 동기화는 지장을 주는 작업이며 NSX Edge VM을 재부팅합니다.

시스템 이벤트 심각도 수준

각 이벤트에는 다음 심각도 수준 중 하나가 지정됩니다.

- 정보
- 낮음

- 중간
- 심각
- 위험
- 높음

다음 항목에서는 다양한 구성 요소에서 발생하는 심각, 위험 또는 높음 심각도의 시스템 이벤트 메시지를 설명합니다.

본 장은 다음 항목을 포함합니다.

- 보안 시스템 이벤트
- 분산 방화벽 시스템 이벤트
- NSX Edge 시스템 이벤트
- 패브릭 시스템 이벤트
- 배포 플러그인 시스템 이벤트
- 메시징 시스템 이벤트
- Service Composer 시스템 이벤트
- GI SVM 시스템 이벤트
- SVM Operations 시스템 이벤트
- 복제 - 범용 동기화 시스템 이벤트
- NSX 관리 시스템 이벤트
- 논리적 네트워크 시스템 이벤트
- ID 방화벽 시스템 이벤트
- 호스트 준비 시스템 이벤트

보안 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 보안에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
11002	위험	아니요	vCenter Server에 연결할 수 없습니다. 사용자 이름 및 암호가 잘못되었습니다. (Unable to connect to vCenter Server Bad username/password.)	vCenter Server 구성에 실패했습니다. 작업: vCenter Server 구성이 올바른지와 올바른 자격 증명이 제공되었는지 확인합니다. NSX 관리 가이드에서 "NSX Manager에 vCenter Server 등록" 및 NSX 문제 해결 가이드에서 "vCenter Server에 NSX Manager 연결"을 참조하십시오.
11006	위험	아니요	vCenter Server 연결이 손실되었습니다.(Lost vCenter Server connectivity.)	vCenter Server에 대한 연결이 손실되었습니다. 작업: vCenter Server의 연결 문제가 있는지 조사합니다. NSX 문제 해결 가이드에서 "vCenter Server에 NSX Manager 연결" 및 "NSX Manager 문제 해결"을 참조하십시오.
230000	위험	아니요	NSX Manager에서 SSO 구성 작업 실패.(SSO Configuration Task on NSX Manager failed.)	SSO(Single Sign On) 구성에 실패했습니다. 이유로는 잘못된 자격 증명, 잘못된 구성 또는 시간 동기화 실패 등이 있습니다. 작업: 오류 메시지를 검토하고 SSO를 다시 구성합니다. NSX 관리 가이드에서 "Single Sign On 구성"을 참조하십시오. 또한 NSX 문제 해결 가이드에서 "NSX SSO 조회 서비스 구성 실패"를 참조하십시오.
230002	위험	아니요	SSO STS 클라이언트 연결이 끊겼습니다.(SSO STS Client disconnected.)	NSX Manager를 SSO 서비스에 등록하지 못했거나 SSO 서비스에 대한 연결이 끊어졌습니다. 작업: 잘못된 자격 증명, 동기화 실패 문제 및 네트워크 연결 문제와 같은 구성 문제가 있는지 확인합니다. 이 이벤트는 특정 VMware 기술 문제로 인해 발생할 수도 있습니다. KB 문서 "STS 서비스의 SSL 인증서를 확인할 수 없음" (http://kb.vmware.com/kb/2121696) 및 "오류로 인해 조회 서비스에 대한 NSX Manager를 외부 PSC(Platform Service Controller)에 등록하지 못함: 서버 인증서 체인이 확인되지 않음" (http://kb.vmware.com/kb/2132645)을 참조하십시오.
240000	위험	아니요	인증 차단 목록에 {0} 항목을 추가했습니다.(Added an entry {0} to authentication black list.)	특정 IP 주소를 갖는 사용자가 10회 연속해서 로그인에 실패했으며 30분 동안 잠겼습니다. 작업: 잠재적인 보안 문제를 조사합니다.

분산 방화벽 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 분산 방화벽에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
301001	위험	아니요	호스트에서 필터 구성 업데이트가 실패했습니다. (Filter config update failed on host.)	호스트가 필터 구성을 수신/구문 분석하지 못했거나 디바이스 /dev/dvfiltertbl 을 열지 못했습니다. 작업: 컨텍스트 및 실패 이유에 대해서는 키-값 쌍을 참조하십시오. 여기에는 NSX Manager 와 준비된 호스트 간의 VIB 버전 불일치와 예기치 않은 업그레이드 문제가 있을 수 있습니다. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301002	심각	아니요	필터 구성이 vNIC에 적용되지 않았습니다.(Filter config not applied to vnic.)	필터 구성을 vNIC에 적용하지 못했습니다. 가능한 원인: 필터 구성 열기, 구문 분석 또는 업데이트 실패. 이 오류는 분산 방화벽에서 발생하지 않고 네트워크 확장성(NetX) 시나리오에서 발생할 수 있습니다. 작업: ESXi 및 NSX Manager에 대한 기술 지원 번들을 수집하고 VMware 기술 지원에 문의하십시오.
301031	위험	아니요	호스트에서 방화벽 구성 업데이트가 실패했습니다. (Firewall config update failed on host.)	방화벽 구성을 수신/구문 분석/업데이트하지 못했습니다. 키 값은 생성 번호와 같은 컨텍스트 정보와 기타 디버그 정보를 포함합니다. 작업: 호스트 준비 절차를 따랐는지 확인합니다. 호스트에 로그인하고 /var/log/vsfwd.log 파일을 수집한 후 강제로 방화벽 구성을 API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> 와 동기화합니다(NSX 문제 해결 가이드의 "분산 방화벽 문제 해결" 참조). 호스트에서 여전히 분산 방화벽 구성을 업데이트할 수 없으면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집한 후 VMware 기술 지원에 문의하십시오.
301032	심각	아니요	방화벽 규칙을 vNIC에 적용하지 못했습니다.(Failed to apply firewall rule to vnic.)	방화벽 규칙을 vNIC에 적용하지 못했습니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오. 방화벽 구성을 vNIC에 적용하는 동안 호스트 로그 (vmkernel.log 및 vsfwd.log)에 기간이 포함되어 있는지 확인하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301041	위험	아니요	호스트에서 컨테이너 구성을 업데이트하지 못했습니다.(Container configuration update failed on host.)	네트워크 및 보안 컨테이너 구성 관련 작업에 실패했습니다. 키 값에는 컨테이너 이름 및 생성 번호와 같은 컨텍스트 정보가 포함됩니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오. 컨테이너 구성을 vNIC에 적용하는 동안 호스트 로그(vmkernel.log 및 vsfwd.log)에 기간이 포함되어 있는지 확인하십시오.
301051	심각	아니요	호스트에서 흐름이 누락되었습니다.(Flow missed on host.)	하나 이상의 세션과 보호된 가상 시스템 간의 흐름 데이터가 삭제되었으며 NSX Manager로 읽거나 전송하지 못했습니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지와 vsfwd 메모리 사용량이 리소스 제한을 벗어나지 않는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301061	위험	아니요	호스트에서 Spoofguard 구성 업데이트가 실패했습니다.(Spoofguard config update failed on host.)	SpoofGuard와 관련된 구성 작업에 실패했습니다. 작업: 호스트 준비 절차를 따랐는지 확인합니다. 호스트에 로그인하고 /var/log/vsfwd.log 파일을 수집한 후 강제로 방화벽 구성을 API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> 와 동기화합니다(NSX 문제 해결 가이드의 "분산 방화벽 문제 해결" 참조). SpoofGuard 구성에 여전히 실패하면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오. 로그에 호스트가 SpoofGuard 구성을 수신한 기간이 포함되어 있는지 확인하십시오.
301062	심각	아니요	vNIC에 Spoofguard를 적용하지 못했습니다.(Failed to apply spoofguard to vnic.)	SpoofGuard를 vNIC에 적용하지 못했습니다. 작업: 호스트 준비 절차를 따랐는지 확인합니다. 호스트에 로그인하고 /var/log/vsfwd.log 파일을 수집한 후 강제로 방화벽 구성을 API <code>https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id></code> 와 동기화합니다(NSX 문제 해결 가이드의 "분산 방화벽 문제 해결" 참조). SpoofGuard 구성에 여전히 실패하면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301064	심각	아니요	vNIC에 대해 Spoofguard를 사용하지 않도록 설정하지 못했습니다.(Failed to disable spoofguard for vnic.)	vNIC에 대해 SpoofGuard를 사용하지 않도록 설정하지 못했습니다. 작업: NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301072	위험	아니요	레거시 애플리케이션 서비스 VM을 삭제하지 못했습니다.(Failed to delete legacy App service vm.)	vCloud Networking and Security용 vShield App 서비스 VM을 삭제하지 못했습니다. 작업: NSX 업그레이드 가이드의 "vShield App을 분산 방화벽으로 업그레이드" 절차를 따랐는지 확인합니다.
301080	위험	아니요	방화벽 CPU 임계값에 도달했습니다.(Firewall CPU threshold crossed.)	vsfwd CPU 사용량 임계값에 도달했습니다. 작업: NSX 관리 가이드에서 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 섹션을 참조하십시오. 호스트 리소스 활용도를 줄여야 할 수 있습니다. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301081	위험	아니요	방화벽 메모리 임계값에 도달했습니다.(Firewall memory threshold crossed.)	vsfwd 메모리 임계값에 도달했습니다. 작업: NSX 관리 가이드에서 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 섹션을 참조하십시오. 구성된 방화벽 규칙이나 네트워크 및 보안 컨테이너의 수를 줄이는 것을 포함하여 호스트 리소스 활용도를 줄여야 할 수 있습니다. 방화벽 규칙 수를 줄이려면 appliedTo 용량을 사용하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301082	위험	아니요	방화벽 ConnectionsPerSecond 임계값에 도달했습니다.(Firewall ConnectionsPerSecond threshold crossed.)	초당 방화벽 연결 임계값에 도달했습니다. 작업: NSX 관리 가이드에서 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 섹션을 참조하십시오. 호스트의 VM과의 활성 연결 수를 줄이는 것을 포함하여 호스트 리소스 활용도를 줄여야 할 수 있습니다.
301501	위험	아니요	{hostID} 호스트에 대한 방화벽 구성 업데이트 버전 {version#}의 시간이 초과되었습니다. 호스트의 방화벽 구성은 {version#} 버전으로 동기화됩니다.(Firewall configuration update version {version#} to host {hostID} timed out. Firewall configuration on host is synced upto version {version#}.)	호스트가 방화벽 구성 업데이트를 처리하는 데 2분 넘게 소요되었으며 업데이트 시간이 초과되었습니다. 작업: vsfwd가 작동하는지와 규칙이 호스트로 게시되고 있는지 확인합니다. NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301502	위험	아니요	{hostID} 호스트에 대한 Spoofguard 구성 업데이트 번호 {number#}의 시간이 초과되었습니다. 호스트의 Spoofguard 구성은 {version#} 버전으로 동기화됩니다. (Spoofguard configuration update number {number#} to host {hostID} timed out. Spoofguard configuration on host is synced upto version {version#}.)	호스트가 Spoofguard 구성 업데이트를 처리하는 데 2분 넘게 소요되었으며 업데이트 시간이 초과되었습니다. 작업: vsfwd가 작동하는지와 규칙이 호스트로 게시되고 있는지 확인합니다. NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301503	위험	아니요	{clusterID} 클러스터에 대한 방화벽 구성 버전 {version#}을(를) 게시하지 못했습니다. 자세한 내용은 로그를 참조하십시오. (Failed to publish firewall configuration version {version#} to cluster {clusterID}. Refer logs for details.)	클러스터 또는 하나 이상의 호스트에 대해 방화벽 규칙을 게시하지 못했습니다. 작업: NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301504	위험	아니요	{clusterID} 클러스터에 대한 컨테이너 업데이트를 게시하지 못했습니다. 자세한 내용은 로그를 참조하십시오. (Failed to publish container updates to cluster {clusterID}. Refer logs for details.)	클러스터 또는 하나 이상의 호스트에 대해 네트워킹 및 보안 컨테이너 업데이트를 게시하지 못했습니다. 작업: NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301505	위험	아니요	{clusterID} 클러스터에 대한 spoofguard 업데이트를 게시하지 못했습니다. 자세한 내용은 로그를 참조하십시오. (Failed to publish spoofguard updates to cluster {clusterID}. Refer logs for details.)	클러스터 또는 하나 이상의 호스트에 대해 SpoofGuard 업데이트를 게시하지 못했습니다. 작업: NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301506	위험	아니요	{clusterID} 클러스터에 대한 제외 목록 업데이트를 게시하지 못했습니다. 자세한 내용은 로그를 참조하십시오. (Failed to publish exclude list updates to cluster {clusterID}. Refer logs for details.)	클러스터 또는 하나 이상의 호스트에 대해 제외 목록 업데이트를 게시하지 못했습니다. 작업: NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301508	위험	아니요	{hostID} 호스트를 동기화하지 못했습니다. 자세한 내용은 로그를 참조하십시오. (Failed to sync host {hostID}. Refer logs for details.)	API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>를 통한 방화벽 강제 동기화 작업이 실패했습니다. 작업: NSX 문제 해결 가이드에서 "분산 방화벽 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301510	위험	아니요	클러스터에 대한 강제 동기화 작업이 실패했습니다. (Force sync operation failed for the cluster.)	API https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>를 통한 방화벽 강제 동기화 작업이 실패했습니다. 작업: NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301512	심각	아니요	방화벽이 {hostID} [{hostID}] 호스트에 설치되었습니다. (Firewall is installed on host {hostID}[{hostID}].)	호스트에서 분산 방화벽이 성공적으로 설치되었습니다. 작업: vCenter Server에서 홈 > Networking & Security > 설치 로 이동하여 [호스트 준비] 탭을 선택합니다. 방화벽 상태가 녹색으로 표시되는지 확인합니다.
301513	심각	아니요	방화벽이 {hostID} [{hostID}] 호스트에서 제거되었습니다. (Firewall is uninstalled on host {hostID}[{hostID}].)	호스트에서 분산 방화벽이 제거되었습니다. 분산 방화벽 구성 요소 제거에 여전히 실패하면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301514	위험	아니요	클러스터 {clusterID}에 방화벽을 사용합니다. (Firewall is enabled on cluster {clusterID}).	클러스터에서 분산 방화벽이 성공적으로 설치되었습니다. 작업: vCenter Server에서 홈 > Networking & Security > 설치 로 이동하여 [호스트 준비] 탭을 선택합니다. 방화벽 상태가 녹색으로 표시되는지 확인합니다.
301515	위험	아니요	방화벽이 클러스터 {clusterID}에서 제거되었습니다. (Firewall is uninstalled on cluster {clusterID}).	클러스터에서 분산 방화벽이 제거되었습니다. 작업: 분산 방화벽 구성 요소 제거에 여전히 실패하면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301516	위험	아니요	클러스터 {clusterID}에 방화벽을 사용하지 않습니다. (Firewall is disabled on cluster {clusterID}).	클러스터의 모든 호스트에서 분산 방화벽이 사용되지 않도록 설정되었습니다. 작업: 필요한 작업이 없습니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301034	심각	아니요	방화벽 규칙을 호스트에 적용하지 못했습니다.(Failed to apply Firewall rules to host.)	분산 방화벽 규칙 섹션을 적용하지 못했습니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301043	위험	아니요	컨테이너 구성을 vNIC에 적용하지 못했습니다.(Failed to apply container configuration to vnic.)	네트워크 또는 보안 컨테이너 구성을 적용하지 못했습니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301044	위험	아니요	컨테이너 구성을 호스트에 적용하지 못했습니다. (Failed to apply container configuration to host.)	네트워크 또는 보안 컨테이너 구성을 적용하지 못했습니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301066	심각	아니요	Spoofguard 구성을 호스트에 적용하지 못했습니다. (Failed to apply Spoofguard configuration to host.)	vnic에 모든 SpoofGuard를 적용하지는 못했습니다. 작업: vsip 커널 힙에 충분한 여유 메모리가 있는지 확인하십시오(NSX 관리 가이드의 "방화벽 CPU 및 메모리 임계값 이벤트 보기" 참조). 문제가 지속되면 NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
301100	위험	아니요	호스트에서 방화벽 시간 초과 구성을 업데이트하지 못했습니다.(Firewall timeout configuration update failed on host.)	방화벽 세션 타이머 시간 초과 구성을 업데이트하지 못했습니다. 작업: NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 지원 서비스에 문의하십시오. 로그를 수집한 후에 REST API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> 를 사용하여 방화벽 구성을 강제로 동기화하거나 설치 > 호스트 준비 로 이동한 후 작업 에서 서비스 강제 동기화 를 선택합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301101	심각	아니요	방화벽 시간 초과 구성을 vNIC에 적용하지 못했습니다.(Failed to apply firewall timeout configuration to vnic.)	방화벽 세션 타이머 시간 초과 구성을 업데이트하지 못했습니다. 작업: NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오. 로그를 수집한 후에 REST API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> 를 사용하여 방화벽 구성을 강제로 동기화하거나 설치 > 호스트 준비 로 이동한 후 작업 에서 서비스 강제 동기화 를 선택합니다.
301103	심각	아니요	방화벽 시간 초과 구성을 호스트에 적용하지 못했습니다.(Failed to apply firewall timeout configuration to host.)	방화벽 세션 타이머 시간 초과 구성을 업데이트하지 못했습니다. 작업: NSX Manager 및 호스트에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오. 로그를 수집한 후에 REST API <code>https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id></code> 를 사용하여 방화벽 구성을 강제로 동기화하거나 설치 > 호스트 준비 로 이동한 후 작업 에서 서비스 강제 동기화 를 선택합니다.
301200	심각	아니요	애플리케이션 규칙 관리자 흐름 분석이 시작되었습니다.(Application Rule Manager flow analysis started.)	애플리케이션 규칙 관리자 흐름 분석이 시작되었습니다. 작업: 필요한 작업이 없습니다.
301201	심각	아니요	애플리케이션 규칙 관리자 흐름 분석이 실패했습니다.(Application Rule Manager flow analysis failed.)	애플리케이션 규칙 관리자 흐름 분석이 실패했습니다. 작업: NSX Manager에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오. 실패한 세션과 동일한 vNIC에 대해 새 모니터링 세션을 시작하여 작업을 다시 시도합니다.
301202	심각	아니요	애플리케이션 규칙 관리자에 대한 흐름 분석이 완료되었습니다.(Application Rule Manager flow analysis completed.)	애플리케이션 규칙 관리자에 대한 흐름 분석이 완료되었습니다. 작업: 필요한 작업이 없습니다.

NSX Edge 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 NSX Edge에 대한 시스템 이벤트 메시지를 설명합니다. 이러한 이벤트가 경보를 트리거하면 정보 심각도와 함께 시스템 이벤트가 나열됩니다.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30011	높음	해당 없음	작동 중인 상태의 NSX Edge VM을 찾을 수 없습니다. 네트워크가 중단되었을 수 있습니다.(None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.)	NSX Edge VM은 이 상태에서 자동으로 복구됩니다. 이벤트 코드 30202 또는 30203을 갖는 트랩을 확인하십시오. 작업: NSX 문제 해결 가이드에서 "Edge 장치 문제 해결"을 참조하십시오.
30013	위험	130013	NSX Manager가 잘못된 상태의 NSX Edge VM(vmlid : {#})을 찾았습니다. 강제 동기화가 필요합니다.(NSX Manager found NSX Edge VM (vmlid : {#}) in bad state. Needs a force sync.)	NSX Edge VM은 잘못된 상태를 보고하고 있으며 제대로 작동하지 않을 수 있습니다. 작업: 문제 상태가 감지되면 자동 강제 동기화가 트리거됩니다. 자동 강제 동기화가 실패하면 수동 강제 동기화를 시도하십시오.
30014	심각	해당 없음	NSX Edge VM과 통신하지 못했습니다.(Failed to communicate with the NSX Edge VM.)	NSX Manager는 VIX 또는 메시지 버스를 통해 NSX Edge와 통신합니다. 통신 채널은 Edge 배포 또는 다시 배포 시에 호스트 준비가 수행되었는지 여부에 따라 NSX Manager에서 선택합니다. 이 이벤트는 NSX Manager가 NSX Edge와의 통신이 끊어졌음을 나타냅니다. 작업: NSX 문제 해결 가이드에서 "Edge 장치 문제 해결"을 참조하십시오.
30027	정보	130027	NSX Edge VM(vmlid : {#})의 전원이 꺼짐.(NSX Edge VM (vmlid : {#}) is powered off.)	NSX Edge VM의 전원이 꺼졌습니다. 작업: 정보 전용 이벤트입니다.
30032	높음	130032	vCenter 인벤토리에서 NSX Edge Appliance(vmlid: {#})를 찾을 수 없습니다.(NSX Edge appliance with vmlid : {#} not found in the vCenter inventory.)	NSX Edge VM은 vCenter Server에서 직접 삭제된 것 같습니다. NSX 관리 개체는 NSX용 vSphere Web Client 인터페이스에서 추가 또는 삭제되어야 하므로 이것은 지원되지 않는 작업입니다. 작업: Edge를 다시 배포하거나 새 Edge를 배포하십시오.
30033	높음	130033	vCenter 인벤토리에서 NSX Edge VM(vmlid: {#})을 찾을 수 없습니다.(NSX Edge VM (vmlid : {#}) not found in the vCenter inventory.)	NSX Edge VM을 vCenter 인벤토리에서 찾을 수 없습니다. 작업: VM이 실수로 삭제되었는지 확인하십시오. 확인한 후에는 Edge를 다시 배포하십시오.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30034	위험	130034	작동 중인 상태의 NSX Edge VM을 찾을 수 없습니다. 네트워크가 중단되었을 수 있습니다.(None of the NSX Edge VMs found in serving state. There is a possibility of network disruption.)	Edge VM이 NSX Manager에서 보낸 상태 점검에 반응하지 않습니다. 작업: Edge VM 전원이 켜져 있는지 확인하십시오. 그런 다음 Edge 로그를 수집하고 VMware 기술 지원에 문의하십시오.
30037	위험	해당 없음	{#}(으)로 수정된 Edge Firewall 규칙은 더 이상 {#}에 사용할 수 없습니다.(Edge firewall rule modified as {#} is no longer available for {#}).	방화벽 규칙에 잘못된 GroupingObject(IPSet, securityGroup 등)가 있습니다. 작업: 방화벽 규칙을 다시 확인하고 필요한 업데이트를 수행합니다.
30038	위험	해당 없음	전원이 켜진 NSX Edge Appliance({EdgeId #}, {vmName #})가 가상 시스템 반선택도 규칙을 위반합니다.(Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule.)	NSX Edge 고가용성은 반선택도 규칙을 vSphere 호스트에 자동으로 적용하므로 활성 및 대기 Edge VM이 다른 호스트에 배포됩니다. 이 이벤트는 이러한 반선택도 규칙이 클러스터에서 제거되었으며 두 Edge VM이 모두 동일한 호스트에서 실행되고 있음을 나타냅니다. 작업: vCenter Server로 이동한 후 반선택도 규칙을 확인하십시오.
30045	위험	해당 없음	심각한 VIX 오류로 인해 NSX Edge VM 상태 점검을 하지 못했습니다. VM에 대한 추가 상태 점검을 사용하지 않도록 설정되었습니다. 상태 점검을 재개하려면 VM을 다시 배포하거나 강제 동기화하십시오.(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.)	네트워크 환경으로 인해 VIX 채널을 통한 Edge VM으로의 통신이 반복적으로 실패할 수 있습니다. 작업: NSX Edge가 응답하는 경우 NSX Manager 및 NSX Edge 기술 지원 로그를 수집하십시오. 그런 다음 강제 동기화를 수행합니다. 문제가 지속되면 NSX Edge를 다시 배포하십시오(NSX 관리 가이드의 "NSX Edge 다시 배포" 참조). 참고 다시 배포는 지장을 주는 작업입니다. 먼저 강제 동기화를 수행한 후 문제가 해결되지 않으면 다시 배포하십시오.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30046	위험	해당 없음	Edge {EdgeID#}, VM: {#}에서 생성 번호 {#}에 대한 사전 규칙을 게시하지 못했습니다. 자세한 내용은 로그를 참조하십시오. 강제 동기화가 필요할 수 있습니다. (Pre rules publish failed on edge: {EdgeID#}, vm: {#} for generation number {#}. Refer logs for detail. It may need forcesync.)	NSX Edge 방화벽 규칙이 동기화되지 않은 상태일 수 있습니다. 이 오류는 사전 규칙(DFW UI/API에서 구성)이 실패하는 경우에 발생합니다. 작업: 기본 제공 복구 프로세스를 통해 문제가 자동으로 해결되지 않으면 수동 강제 동기화를 수행합니다.
30100	위험	해당 없음	NSX Edge가 강제 동기화되었습니다.(NSX Edge was force synced.)	NSX Edge VM이 강제로 동기화되었습니다. 작업: 강제 동기화로 문제가 해결되지 않으면 NSX Manager 및 NSX Edge에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
30102	높음	130102	NSX Edge(vmlid : {IP Address})가 잘못된 상태입니다. 강제 동기화가 필요합니다. (NSX Edge (vmlid : {IP Address}) is in Bad State. Needs a force sync.)	NSX Edge VM에서 내부 오류가 발생하고 있습니다. 작업: 기본 제공 복구 프로세스를 통해 문제가 자동으로 해결되지 않으면 수동 강제 동기화를 수행합니다.
30148	위험	해당 없음	NSX Edge CPU 사용량이 증가했습니다.{#} 상위 프로세스는 {#}입니다. (NSX Edge CPU usage has increased. {#} Top processes are: {#}.)	NSX Edge VM CPU 활용률이 지속적으로 높게 유지됩니다. 작업: NSX 문제 해결 가이드에서 "Edge 장치 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 NSX Edge에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
30153	심각	해당 없음	AESNI crypto 엔진이 실행되었습니다.(AESNI crypto engine is up.)	AESNI crypto 엔진이 실행됩니다. 작업: 필요한 작업이 없습니다.
30154	심각	해당 없음	AESNI crypto 엔진이 다운되었습니다.(AESNI crypto engine is down.)	AESNI crypto 엔진이 다운되었습니다. 작업: 필요한 작업이 없습니다. 예상된 상태입니다.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30155	높음	130155	NSX Edge를 배포할 때 리소스 예약 중에 호스트 또는 리소스 풀의 CPU 및/또는 메모리 리소스가 부족합니다. (Insufficient CPU and/or Memory Resources available on Host or Resource Pool, during resource reservation at the time of NSX Edge deployment.)	호스트 또는 리소스 풀의 CPU 및/또는 메모리 리소스가 부족합니다. 홈(Home) > 호스트 및 클러스터 > [Cluster-name](Hosts and Clusters > [Cluster-name])> 모니터(Monitor) > 리소스 예약(Resource Reservation) 페이지로 이동하여 사용 가능한 리소스 및 예약된 리소스를 확인할 수 있습니다. 사용 가능한 리소스를 확인한 후에는 리소스 예약 제한이 성공적으로 수행되도록 리소스를 장치 구성의 일부로 다시 지정하십시오.
30180	위험	해당 없음	NSX Edge의 메모리가 부족합니다. 3초 후에 Edge가 재부팅됩니다. 상위 5개 프로세스는 다음과 같습니다. {#}(NSX Edge is out of memory. The Edge is rebooting in 3 seconds. Top 5 processes are: {#}.)	NSX Edge VM의 메모리가 부족합니다. 복구하기 위해 재부팅이 시작되었습니다. 작업: NSX 문제 해결 가이드에서 "Edge 장치 문제 해결"을 참조하십시오. 문제가 지속되면 NSX Manager 및 NSX Edge에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
30181	위험	130181	NSX Edge {EdgeID#} VM 이름 {#} 파일 시스템은 읽기 전용입니다.(NSX Edge {EdgeID#} VM name {#} file system is read only.)	NSX Edge VM을 지원하는 스토리지 디바이스의 연결 문제입니다. 작업: 지원 데이터스토어를 사용하여 연결 문제를 확인하고 해결합니다. 연결 문제가 해결된 후에는 수동 강제 동기화를 실행해야 할 수 있습니다.
30202	심각	해당 없음	NSX Edge {EdgeID#} HighAvailability가 전환되었습니다. VM {#} 이름 {#}이 ACTIVE 상태로 이동되었습니다. (NSX Edge {EdgeID#} HighAvailability switch over happened. VM {#} name {#} has moved to ACTIVE state.)	HA 페일오버가 발생했으며 보조 NSX Edge VM이 대기 상태에서 활성 상태로 전환되었습니다. 작업: 어떠한 작업도 필요하지 않습니다.
30203	심각	해당 없음	NSX Edge {EdgeID#} HighAvailability가 전환되었습니다. VM {#} 이름 {#}이 STANDBY 상태로 이동되었습니다. (NSX Edge {EdgeID#} HighAvailability switch over happened. VM {#} name {#} has moved to STANDBY state.)	HA 페일오버가 발생했으며 기본 NSX Edge VM이 활성 상태에서 대기 상태로 전환되었습니다. 작업: 어떠한 작업도 필요하지 않습니다.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30205	위험	130205	HighAvailability를 사용하는 NSX Edge {EdgeID}에 대해 분할 브레인이 감지되었습니다.(Split Brain detected for NSX Edge {EdgeID} with HighAvailability.)	네트워크 실패로 인해 HA용으로 구성된 NSX Edge VM에서 다른 VM이 온라인 상태인지를 확인할 수 없습니다. 이러한 시나리오에서 두 VM은 다른 VM이 온라인 상태가 아니라고 판단하고 ACTIVE 상태를 적용합니다. 이로 인해 네트워크가 중단될 수 있습니다. 작업: 네트워크 인프라(가상 및 물리적)를 확인하여 특히 HA용으로 구성된 인터페이스 및 경로에 오류가 있는지 확인하십시오.
30302	위험	130302	LoadBalancer virtualServer/pool: {virtualServerName} 프로토콜: {#} serverIp: {#}이(가) 다운 상태로 변경되었습니다.(LoadBalancer virtualServer/pool : {virtualServerName} Protocol : {#} serverIp : {IP Address} changed the state to down.)	NSX Edge 로드 밸런서의 가상 서버 또는 풀이 다운되었습니다. 작업: NSX 문제 해결 가이드에서 "로드 밸런싱" 섹션을 참조하십시오.
30303	심각	해당 없음	LoadBalancer virtualServer/pool: {0} 프로토콜: {#} serverIp: {IP Address}이(가) 잘못된 상태로 변경되었습니다.(LoadBalancer virtualServer/pool : {0} Protocol : {#} serverIp : {IP Address} changed to a wrong state.)	NSX Edge 로드 밸런서의 가상 서버 또는 풀에서 내부 오류가 발생합니다. 작업: NSX 문제 해결 가이드에서 "로드 밸런싱" 섹션을 참조하십시오.
30304	심각	130304	LoadBalancer 풀: {0} 프로토콜: {#} serverIp: {IP address}이(가) 주의 상태로 변경되었습니다.(LoadBalancer pool : {0} Protocol : {#} serverIp : {IP address} changed to a warning state.)	NSX Edge 로드 밸런서 풀의 상태가 주의(warning) 로 변경되었습니다. 작업: NSX 문제 해결 가이드에서 "로드 밸런싱" 섹션을 참조하십시오.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30402	위험	130402	localIp: {IP address}에서 peerIp: {IP address} (으)로 연결된 IPsec 채널이 다운 상태로 변경되었습니다.(IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to down.)	NSX Edge IPsec VPN 채널이 다운되었습니다. 작업: NSX 문제 해결 가이드에서 "VPN(Virtual Private Network)" 섹션을 참조하십시오.
30404	위험	130404	Edge Ipsec 터널 다운됨: localSubnet: {subnet}에서 peerSubnet: {subnet} (으)로 연결된 IPsec 터널이 다운 상태로 변경되었습니다.(EDGE IPSEC TUNNEL DOWN : IPsec Tunnel from localSubnet : {subnet} to peerSubnet : {subnet} changed the status to down.)	NSX Edge IPsec VPN 채널이 다운되었습니다. 작업: NSX 문제 해결 가이드에서 "VPN(Virtual Private Network)" 섹션을 참조하십시오.
30405	심각	해당 없음	localIp: {IP address}에서 peerIp: {IP address} (으)로 연결된 IPsec 채널이 알 수 없음 상태로 변경되었습니다.(IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.)	NSX Edge IPsec VPN 채널 상태를 확인할 수 없습니다. 작업: NSX 문제 해결 가이드에서 "VPN(Virtual Private Network)" 섹션을 참조하십시오.
30406	심각	해당 없음	localIp: {IP address}에서 peerIp: {IP address} (으)로 연결된 IPsec 채널이 알 수 없음 상태로 변경되었습니다.(IPsec Channel from localIp : {IP address} to peerIp : {IP address} changed the status to unknown.)	NSX Edge IPsec VPN 채널 상태를 확인할 수 없습니다. 작업: NSX 문제 해결 가이드에서 "VPN(Virtual Private Network)" 섹션을 참조하십시오.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30701	위험	해당 없음	외부 DHCP 서버가 제공되지 않았기 때문에 edge {EdgeID}의 NSX Edge DHCP 릴레이 서비스가 사용되지 않도록 설정되었습니다. 서버 IP 또는 참조된 그룹화 개체를 확인하십시오. (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.)	NSX Edge DHCP 릴레이 서비스가 사용되지 않도록 설정되었습니다. 가능한 이유: (1) DHCP 릴레이 프로세스가 실행되고 있지 않습니다. (2) 외부 DHCP 서버가 없습니다. 이 문제는 릴레이에 참조된 그룹화 개체가 삭제되었기 때문일 수 있습니다. 작업: NSX 관리 가이드에서 "DHCP 릴레이 구성"을 참조하십시오.
30206	위험	해당 없음	HighAvailability를 사용하는 NSX Edge {EdgeID}에 대한 분할 브레인을 확인했습니다.(Resolved Split Brain for NSX Edge {EdgeID} with HighAvailability.)	2개의 NSX Edge HA 장치가 서로 통신할 수 있으며 활성 및 대기 상태를 다시 협상했습니다. 작업: "NSX Edge HA(고가용성) 문제 해결 (http://kb.vmware.com/kb/2126560)을 참조하십시오.
30207	위험	해당 없음	NSX Edge {EdgeID}에 대한 분할 브레인 확인을 {value}번 시도했습니다. (Attempted Split Brain resolution for NSX Edge {EdgeID} with count {value}.)	2개의 NSX Edge HA 장치가 분할 브레인 조건을 다시 협상하고 복구하려고 합니다. 참고 이 이벤트에 의해 보고된 복구 메커니즘은 6.2.3 이전의 NSX Edge 릴리스에서만 발생합니다. 작업: "NSX Edge HA(고가용성) 문제 해결 (http://kb.vmware.com/kb/2126560)을 참조하십시오.

패브릭 시스템 이벤트

이 표에서는 패브릭 시스템 이벤트에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	정보가 트러거됨	이벤트 메시지	설명
250000	정보	아니요	배포 단위 이전 작동 상태는 {#}, 새 작동 상태는 {#}이고 이전 진행 상태는 {#}, 새 진행 상태는 {#}입니다. 경보 문자열에서 근본 원인을 확인하십시오. (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.)	정보 전용 이벤트입니다.
250001	정보	아니요	배포 단위가 생성되었습니다.(A deployment unit has been created.)	정보 전용 이벤트입니다.
250002	정보	아니요	NSX의 배포 단위가 업데이트되었습니다. 패브릭 서비스가 클러스터에서 업데이트됩니다.(A deployment unit in NSX has been updated. Fabric services will be updated on the cluster.)	정보 전용 이벤트입니다.
250003	정보	아니요	배포 단위가 NSX에서 삭제되었습니다.(A deployment unit has been deleted from NSX.)	정보 전용 이벤트입니다.
250004	높음	예	데이터스토어 {#}(이)가 호스트에 연결되어 있지 않으므로 {#} 호스트에서 {#} 서비스를 배포하지 못했습니다. 연결되어 있는지 확인하거나 다른 데이터스토어를 제공하십시오. (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.)	호스트에 대한 보안 가상 시스템을 저장할 데이터스토어를 구성할 수 없습니다. 작업: 호스트가 데이터스토어에 연결할 수 있는지 확인하십시오.
250005	높음	예	배포 단위 설치에 실패했습니다. OVF/VIB URL에 액세스할 수 있는지, DNS가 구성되어 있는지, 필요한 네트워크 포트가 열려 있는지 확인하십시오.(Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)	호스트에 NSX 서비스를 설치하는 동안 ESXi 호스트가 NSX에서 VIB/OVF에 액세스하지 못했습니다. vCenter 시스템 이벤트 테이블에 Event Message: '배포 단위 설치에 실패했습니다. OVF/VIB URL에 액세스할 수 있는지, DNS가 구성되어 있는지, 필요한 네트워크 포트가 열려 있는지 확인하십시오.(Installation of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)', Module: 'Security Fabric'이라고 표시됩니다. 작업: NSX 문제 해결 가이드를 참조하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250006	정보	아니요	네트워크 패브릭 서비스에 대한 패브릭 에이전트가 호스트에 설치되었습니다.(The fabric agent for network fabric services installed successfully on a host.)	정보 전용 이벤트입니다.
250007	정보	아니요	패브릭 에이전트가 호스트에서 제거되었습니다.(The fabric agent was removed successfully from a host.)	정보 전용 이벤트입니다.
250008	높음	예	OVF/VIB 파일의 위치가 변경되었습니다. 서비스를 다시 배포해야 합니다.(Location of OVF / VIB files has changed. Service must be redeployed.)	NSX VIB 및 OVF는 NSX 버전마다 다른 URL을 통해 사용할 수 있습니다. 올바른 VIB를 찾으려면 <a href="https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties">https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties 로 이동해야 합니다. NSX Manager IP 주소가 변경되면 NSX OVF 또는 VIB를 다시 배포해야 할 수 있습니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 확인하십시오.
250009	높음	예	배포 단위 업그레이드에 실패했습니다. OVF/VIB URL에 액세스할 수 있는지, DNS가 구성되어 있는지, 필요한 네트워크 포트가 열려 있는지 확인하십시오.(Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)	호스트 업그레이드 동안 EAM이 NSX에서 VIB/OVF에 액세스하지 못했습니다. vCenter 시스템 이벤트 테이블에 Event Message: '배포 단위 업그레이드에 실패했습니다. OVF/VIB URL에 액세스할 수 있는지, DNS가 구성되어 있는지, 필요한 네트워크 포트가 열려 있는지 확인하십시오. (Upgrade of deployment unit failed. Please confirm OVF/VIB URLs are accessible, DNS is configured, and required network ports are open.)', Module: 'Security Fabric' 이라고 표시됩니다. 작업: NSX 문제 해결 가이드를 참조하십시오.
250012	높음	예	{#} 서비스를 작동하려면 {#} 서비스가 설치되어 있어야 합니다.(Following service(s) need to be installed successfully for Service {#} to function: {#}.)	설치하려는 서비스가 아직 설치되지 않은 다른 서비스에 종속됩니다. 작업: 클러스터에 필요한 서비스를 배포하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250014	높음	예	업그레이드 전에 보안 솔루션에 알람을 보내는 동안 오류가 발생했습니다. 솔루션이 연결 가능 상태가 아니거나 응답하지 않는 경우일 수 있습니다. 솔루션 URL이 NSX에서 액세스 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 다시 배포됩니다.(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.)	업그레이드 전에 보안 솔루션에 알람을 보내는 동안 오류가 발생했습니다. 솔루션이 연결 가능/응답 상태가 아닐 수 있습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오. 서비스가 다시 배포됩니다.
250015	높음	예	시간이 초과된 후에도 업그레이드 알람에 대한 보안 솔루션의 콜백을 수신하지 못했습니다. 솔루션 URL이 NSX에서 액세스 가능한지, NSX가 솔루션에서 연결 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 다시 배포됩니다.(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.)	시간이 초과된 후에도 업그레이드 알람에 대한 보안 솔루션의 콜백을 수신하지 못했습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
250016	높음	아니요	서비스를 제거하지 못했습니다. 솔루션 URL이 NSX에서 액세스 가능한지, NSX가 솔루션에서 연결 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다.(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.)	서비스를 제거하지 못했습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250017	높음	예	제거 전에 보안 솔루션에 알람을 보내는 동안 오류가 발생했습니다. 다시 한 번 알리려면 확인하고 알람 없이 제거하려면 삭제하십시오. 솔루션 URL이 NSX에서 액세스 가능한지, NSX가 솔루션에서 연결 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다. (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.)	제거 전에 보안 솔루션에 알람을 보내는 동안 오류가 발생했습니다. 다시 한 번 알리려면 확인하고 알람 없이 제거하려면 삭제하십시오. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
250018	높음	예	제거 전에 보안 솔루션에 알람을 보내는 동안 오류가 발생했습니다. 다시 한 번 알리려면 확인하고 알람 없이 제거하려면 삭제하십시오. 솔루션 URL이 NSX에서 액세스 가능한지, NSX가 솔루션에서 연결 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다. (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.)	제거 전에 보안 솔루션에 알람을 보내는 동안 오류가 발생했습니다. 다시 한 번 알리려면 확인하고 알람 없이 제거하려면 삭제하십시오. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
250019	높음	예	보안 솔루션에 제거 알람을 보내는 동안 서버가 재부팅되었습니다. 솔루션 URL이 NSX에서 액세스 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다.(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.)	보안 솔루션에 제거 알람을 보내는 동안 서버가 재부팅되었습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오. 서비스가 제거됩니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250020	높음	예	보안 솔루션에 업그레이드 알림을 보내는 동안 서버가 재부팅되었습니다. 솔루션 URL이 NSX에서 액세스 가능한지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 다시 배포됩니다.(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.)	보안 솔루션에 업그레이드 알림을 보내는 동안 서버가 재부팅되었습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지 확인하십시오. systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오. 서비스가 다시 배포됩니다.
250021	위험	아니요	NSX Manager는 VC의 EAM 서비스를 통해 ESX의 NSX VIB를 배포/모니터링합니다. 이 EAM 서비스에 대한 연결이 중단되었습니다. EAM 서비스 또는 VC 다시 시작/중지 또는 EAM 서비스의 문제 때문일 수 있습니다. VC가 사용할 수 있는 상태인지, VC의 EAM 서비스가 실행 중인지 확인하십시오. 또한 EAM MOB를 보면 EAM이 예상대로 작동하는지 확인할 수도 있습니다. (NSX Manager relies on the EAM service in vCenter for deploying/monitoring NSX vibs 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 Manager가 ESX에 NSX VIB를 배포/모니터링하기 위해 vCenter의 EAM 서비스에 의존합니다. 이 EAM 서비스에 대한 연결이 다운되었습니다. 이 문제는 EAM 서비스 때문에 발생하거나 vCenter가 다시 시작/중지되었거나 EAM 서비스에 문제가 있기 때문에 발생할 수 있습니다. 작업: vCenter가 작동 중인지와 vCenter의 EAM 서비스가 실행되고 있는지 확인하십시오. EAM MOB URL http://{vCenter_IP}/eam/mob/ 에 액세스할 수 있는지와 EAM이 예상대로 작동하는지 확인하십시오. 자세한 내용은 NSX 문제 해결 가이드의 "인프라 준비"를 참조하십시오.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
250022	위험	아니요	NSX Manager는 VC의 EAM 서비스를 통해 ESX의 NSX VIB를 배포/모니터링합니다. 이 EAM 서비스에 대한 연결이 중단되었습니다. EAM 서비스 또는 VC 다시 시작/중지 또는 EAM 서비스의 문제 때문일 수 있습니다. VC가 사용할 수 있는 상태인지, VC의 EAM 서비스가 실행 중인지 확인하십시오. 또한 EAM MOB를 보면 EAM이 예상대로 작동하는지 확인할 수도 있습니다. (NSX Manager relies on the EAM service in VC for deploying/monitoring NSX vibs 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 Manager가 ESX에 NSX VIB를 배포/모니터링하기 위해 vCenter의 EAM 서비스에 의존합니다. 이 EAM 서비스에 대한 연결이 다문되었습니다. 이 문제는 EAM 서비스 때문에 발생하거나 vCenter가 다시 시작/중지되었거나 EAM 서비스에 문제가 있기 때문에 발생할 수 있습니다. 작업: vCenter가 작동 중인지와 vCenter의 EAM 서비스가 실행되고 있는지 확인하십시오. EAM MOB URL http://{vCenter_IP}/eam/mob/ 에 액세스할 수 있는지와 EAM이 예상대로 작동하는지 확인하십시오. 자세한 내용은 NSX 문제 해결 가이드의 “인프라 준비”를 참조하십시오.
250023	높음	예	제거 전 정리 작업에 실패했습니다. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다. (Pre Uninstall cleanup failed. Use resolve API to resolve the Alarm. Service will be removed.)	제거 전 내부 정리 작업이 완료되지 못했습니다. 작업: systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오. 서비스가 제거됩니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250024	높음	예	이 배포에 대해 지원되는 EAM 에이전시를 찾을 수 없습니다. VC 서비스가 아직 초기화 중일 수 있습니다. 경보를 해결하여 에이전시의 존재를 확인하십시오. 수동으로 에이전시를 삭제한 경우에는 NSX에서 배포 항목을 삭제하십시오. (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.)	EAM은 ESXi 호스트에 VIB를 배포합니다. 각 NSX 준비 클러스터에 EAM 에이전시가 설치됩니다. 이 에이전시를 찾을 수 없는 경우 vCenter Server 서비스가 초기화되고 있거나 에이전시가 오류를 나타내며 수동으로 삭제되었을 수 있습니다.
250025	높음	예	이 이벤트는 EAM을 사용하여 상태 비저장 호스트에서 NSX VIB를 업그레이드하거나 제거하려고 할 때 생성됩니다. 모든 상태 비저장 호스트는 자동 배포 기능을 사용하여 준비해야 합니다. 자동 배포 기능을 사용하여 구성을 수정하고 확인 API를 사용하여 경보를 확인하십시오.(This event is generated when an attempt is made to upgrade or uninstall NSX vibs 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.)	이 이벤트는 EAM을 사용하여 상태 비저장 호스트에서 NSX VIBS를 업그레이드하거나 제거하려고 할 때 생성됩니다. 모든 상태 비저장 호스트는 Auto Deploy 기능을 사용해서 준비해야 합니다. 작업: Auto Deploy 기능을 사용하여 구성을 수정하고 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결합니다.

배포 플러그인 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 배포 플러그인에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
280000	높음	예	모두 사용된 배포 플러그인 IP 풀 경보입니다.(Deployment Plugin IP pool exhausted alarm.)	소스 IP 풀이 고갈되었으므로 IP 주소를 NSX Service VM에 할당하지 못했습니다. 작업: 풀에 IP 주소를 추가하십시오.
280001	높음	예	배포 플러그인 일반 경보입니다.(Deployment Plugin generic alarm.)	Guest Introspection과 같은 각 서비스에는 각 호스트에 서비스를 구성하기 위한 플러그인 집합이 있습니다. 플러그인 코드의 문제는 일반 경보로 보고됩니다. 서비스는 서비스용 플러그인이 모두 성공한 후에만 녹색으로 바뀝니다. 이 이벤트는 가능한 예외 일부를 캡처합니다. 작업: resolve API를 사용하여 경보를 확인하십시오. 서비스가 배포됩니다.
280004	높음	예	배포 플러그인의 일반 예외 경보입니다.(Deployment Plugin generic exception alarm.)	Guest Introspection과 같은 각 서비스에는 각 호스트에 서비스를 구성하기 위한 플러그인 집합이 있습니다. 플러그인 코드의 문제는 일반 예외 경보로 보고됩니다. 서비스는 서비스용 플러그인이 모두 성공한 후에만 녹색으로 바뀝니다. 이 이벤트는 가능한 모든 예외를 캡처합니다. 작업: resolve API를 사용하여 경보를 확인하십시오. 서비스가 배포됩니다.
280005	높음	예	변경 내용을 적용하려면 VM을 재부팅해야 합니다.(VM needs to be rebooted for some changes to be made/take effect.)	변경 내용을 적용하려면 VM을 재부팅해야 합니다. 작업: resolve API를 사용하여 경보를 확인하십시오. 그러면 VM이 재부팅됩니다.

메시징 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 메시징에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
3900 01	높음	예	호스트 메시징을 구성하지 못했습니다.(Host messaging configuration failed.)	NSX 메시지 버스는 EAM(ESX Agent Manager)이 NSX VIB가 ESXi 호스트에 설치되었음을 NSX에 알리면 호스트 준비 후에 설정됩니다. 이 이벤트는 호스트에서 메시지 버스 설정이 실패했음을 나타냅니다. NSX 6.2.3부터 설치 > 호스트 준비 탭의 영향 받는 호스트 옆에 빨간색 오류 아이콘이 표시됩니다. 작업: 문제 해결 단계를 보려면 NSX 문제 해결 가이드를 참조하십시오.
3900 02	높음	예	호스트 메시징 연결을 재구성하지 못했습니다.(Host messaging connection reconfiguration failed.)	NSX는 RMQ 브로커 세부 정보가 변경되었음을 확인하면 호스트에 최신 RMQ 브로커 정보를 전송하려고 합니다. NSX가 이 정보를 전송하지 못하면 이 경보가 발생합니다. 작업: 문제 해결 단계를 보려면 NSX 문제 해결 가이드를 참조하십시오.
3900 03	높음	예	호스트 메시징을 구성하지 못했으며 알림을 건너뛰었습니다.(Host messaging configuration failed and notifications were skipped.)	NSX는 준비된 호스트가 vCenter Server에 다시 연결될 때 메시징 채널을 다시 설정하려고 합니다. 이 이벤트는 설치가 실패했으며 메시징 채널에 종속하는 다른 NSX 모듈로 알림이 전송되지 않았음을 나타냅니다. 작업: 문제 해결 단계를 보려면 NSX 문제 해결 가이드를 참조하십시오.
3910 02	위험	아니요	호스트에서 메시징 인프라가 중단되었습니다.(Messaging infrastructure down on host.)	NSX Manager와 NSX 호스트 간의 둘 이상의 하트비트 메시지가 누락되었습니다. 작업: 문제 해결 단계를 보려면 NSX 문제 해결 가이드를 참조하십시오.
3211 00	위험	아니요	메시징 계정 {account #}을(를) 사용하지 않도록 설정하는 중입니다. 암호가 만료되었습니다. (Disabling messaging account {account #}. Password has expired.)	메시지 버스 클라이언트로 작동하는 ESXi 호스트, NSX Edge VM 또는 USVM이 초기 배포 또는 호스트 준비 후 예상되는 2시간 이내에 해당 rabbit MQ 암호를 변경하지 않았습니다. 작업: NSX Manager와 메시지 버스 클라이언트 간의 통신 문제를 조사하십시오. 클라이언트가 실행되고 있는지 확인하십시오. 다시 동기화 또는 다시 배포를 수행하기 전에 해당 로그를 수집하십시오. 문제 해결 단계를 보려면 NSX 문제 해결 가이드를 참조하십시오.

Service Composer 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 Service Composer에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심 각도	경보가 트리 거됨	이벤트 메시지	설명
300000	위험	예	{#} 정책의 종속 보안 그룹을 명시적으로 삭제하여 해당 정책이 삭제되었습니다. (Policy {#} is deleted as a result of explicit deletion of its dependent SecurityGroup.)	종속 보안 그룹이 삭제될 때 서비스 정책이 삭제되었습니다. 작업: 보안 정책 생성을 다시 조사하십시오.
300001	높음	예	정책이 동기화되지 않습니다.(Policy is out of sync.)	Service Composer에서 이 서비스 정책의 규칙을 적용하는 동안 오류가 발생했습니다. 작업: 정책에서 변경할 규칙에 대한 입력을 오류 메시지에서 확인하십시오. Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 확인합니다.
300002	높음	예	이 정책에 대한 방화벽 규칙이 동기화되지 않았습니다. 이 경고가 해결될 때까지 이 정책의 방화벽과 관련된 변경 내용이 푸시되지 않습니다. (Firewall rules on this Policy are out of sync. No Firewall related changes from this policy will be pushed, until this alarm is resolved.)	이 오류는 방화벽 구성 문제로 인해 발생했습니다. 작업: 오류를 유발한 정책(규칙일 수 있음)에 대한 세부 정보를 오류 메시지에서 확인하십시오. Service Composer 또는 resolve API를 통해 경보를 확인하고 정책을 동기화해야 합니다. "NSX 6.x의 Service Composer 문제 해결"(http://kb.vmware.com/kb/2132612)도 참조하십시오.
300003	높음	예	이 정책에 대한 네트워크 검사 규칙이 동기화되지 않았습니다. 이 경고가 해결될 때까지 이 정책의 네트워크 검사와 관련된 변경 내용이 푸시되지 않습니다.(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.)	이 오류는 네트워크 검사 구성 문제로 인해 발생했습니다. 작업: 오류를 유발한 정책(규칙일 수 있음)에 대한 세부 정보를 오류 메시지에서 확인하십시오. Service Composer 또는 systemalarms API의 action=resolve 매개 변수를 통해 경보를 확인하고 정책을 동기화해야 합니다. "NSX 6.x의 Service Composer 문제 해결"(http://kb.vmware.com/kb/2132612)도 참조하십시오. Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 확인합니다.

이벤트 코드	이벤트 심 각도	경보가 트리 거됨	이벤트 메시지	설명
300004	높음	예	이 정책에 대한 Guest Introspection 규칙이 동기화되지 않았습니 다. 이 경고가 해결될 때까지 이 정책의 Guest Introspection 과 관련된 변경 내용 이 푸시되지 않습니 다.(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.)	이 오류는 Guest Introspection 구성 문제로 인해 발생했 습니다. 작업: 오류를 유발한 정책(규칙일 수 있음)에 대한 세부 정 보를 오류 메시지에서 확인하십시오. Service Composer 또는 systemalarms API의 action=resolve 매개 변수를 사용 하여 경보를 확인하고 정책을 동기화해야 합니다. "NSX 6.x의 Service Composer 문제 해결 "(http://kb.vmware.com/kb/2132612)도 참조하십시오.
300005	높음	예	Service Composer가 동기화되지 않았습니 다. Service Composer 의 변경 내용이 방화 벽/네트워크 검사로 푸시되지 않습니다. (Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection.)	Service Composer에서 정책을 동기화할 때 오류가 발생 했습니 다. 어떤 변경 내용도 방화벽 또는 네트워크 검사 서 비스로 전송되지 않습니다. 작업: 오류 메시지를 확인하여 편집할 정책 및/또는 방화벽 섹션을 결정하십시오. Service Composer 또는 resolve API를 통해 경보를 확인하십시오.
300006	높음	예	재부팅 시 동기화 작 업 실패로 인해 Service Composer가 동기화되지 않았습니 다.(Service Composer is out of sync due to failure on sync on reboot operation.)	재부팅 시 Service Composer에서 정책을 동기화할 때 오류가 발생했습니다. 어떤 변경 내용도 방화벽 또는 네트워 크 검사 서비스로 전송되지 않습니다. 작업: 오류 메시지를 확인하여 편집할 정책 및/또는 방화벽 섹션을 결정하십시오. Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수 를 사용하여 경보를 확인합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
300007	높음	예	이 방화벽에서의 초안 롤백으로 인해 Service Composer가 동기화되지 않았습니다. Service Composer의 변경 내용이 방화벽/네트워크 검사로 푸시되지 않습니다. (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.)	Service Composer에서 방화벽 규칙 집합을 이전 초안 상태로 되돌릴 때 동기화 오류가 발생했습니다. 어떤 변경 내용도 방화벽 또는 네트워크 검사 서비스로 전송되지 않습니다. 작업: Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 확인합니다.
300008	높음	예	정책에 해당하는 섹션을 삭제하는 동안 오류가 발생했습니다. (Failure while deleting section corresponding to the Policy.)	Service Composer에서 정책에 대한 방화벽 규칙 섹션을 삭제할 때 오류가 발생했습니다. 이 문제는 NSX 서비스 삽입이 있는 타사 서비스용 관리자에 연결할 수 없을 때 발생합니다. 작업: 타사 서비스 관리자에 대한 연결 문제를 조사하십시오. Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 확인합니다.
300009	높음	예	우선 순위 변경을 반영하도록 섹션 순서를 다시 지정하는 동안 오류가 발생했습니다. (Failure while reordering section to reflect precedence change.)	재부팅 시 Service Composer에서 정책을 동기화할 때 오류가 발생했습니다. 어떤 변경 내용도 방화벽 또는 네트워크 검사 서비스로 전송되지 않습니다. 작업: 오류 메시지를 확인하여 편집할 정책 및/또는 방화벽 섹션을 결정하십시오. Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 확인합니다.
300010	높음	예	초안 설정 자동 저장을 초기화하는 동안 오류가 발생했습니다. (Failure while initializing auto save drafts setting.)	자동 저장된 초안 설정을 초기화하는 동안 Service Composer에서 오류가 발생했습니다. 작업: 오류 메시지를 확인하여 편집할 정책 및/또는 방화벽 섹션을 결정하십시오. Service Composer를 통해 경보를 확인하거나 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 확인합니다.

GI SVM 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 Guest Introspection 범용 서비스 VM(GI SVM) 작업에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
295002	심각			NSX Manager는 Guest Introspection USVM에서 하트비트를 수신하지 않습니다. 작업: NSX Manager 및 USVM 기술 지원 로그를 수집하고 기술 지원 요청을 여십시오.
295003	정보			NSX Manager가 USVM에서 하트비트를 수신합니다. 작업: 이벤트 295002 이후의 복구 이벤트가 보고됩니다.
295010	정보			USVM 및 Guest Introspection 호스트 모듈 간에 연결이 설정됩니다. 작업: 정보 전용 이벤트입니다. 어떠한 작업도 필요하지 않습니다.

SVM Operations 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 SVM(서비스 VM) Operations에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
280002	높음	예	이 에이전트에 대한 일부 이벤트가 NSX에서 누락되었습니다. vCenter Server에서 재부팅했거나 임시 연결 손실이 발생했기 때문일 수 있습니다. 경고: 경보를 해결하면 VM이 삭제되고 에이전트 VM이 누락되었음을 나타내는 다른 경보가 나타납니다. 이 경보를 해결하면 VM이 다시 배포됩니다.(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.)	배포된 서비스 VM에서 내부 오류가 발생했습니다. 작업: 경보를 확인하면 VM이 삭제되고 삭제에 대한 두 번째 경보가 보고됩니다. 두 번째 경보를 확인하면 VM이 다시 설치됩니다. VM을 다시 배포하지 못하면 원래 경보가 다시 보고됩니다. 경보가 다시 나타나면 KB http://kb.vmware.com/kb/2144624 의 절차를 사용하여 SVM 로그를 수집하고 VMware 기술 지원에 문의하십시오.
280003	높음	예	이 에이전트에 대한 일부 이벤트가 NSX에서 누락되었습니다. vCenter Server에서 재부팅했거나 임시 연결 손실이 발생했기 때문일 수 있습니다. 경고: 이 경보를 해결하면 VM이 다시 시작됩니다.(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.)	배포된 서비스 VM이 다시 시작되었습니다. 작업: 경보를 확인하면 VM이 다시 시작됩니다. 다시 시작하지 못할 경우 경보가 다시 나타납니다. KB http://kb.vmware.com/kb/2144624 의 절차를 사용하여 SVM 로그를 수집하고 VMware 기술 지원에 문의하십시오.
280006	높음	예	사용 가능한 에이전트로 표시하지 못했습니다. (Failed to mark agent as available.)	ESX Agent VM을 사용 가능 상태로 표시하는 동안 내부 오류가 발생했습니다. 작업: systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 확인하십시오. 경보를 확인할 수 없으면 KB http://kb.vmware.com/kb/2144624 의 절차를 사용하여 SVM 로그를 수집하고 VMware

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
기술 지원에 문의하십시오.				

복제 - 범용 동기화 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 복제 - 범용 동기화에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
31000 1	위험	아니요	NSX Manager {#}에서 개체 유형 {#}에 대한 전체 동기화가 실패했습니다.(Full sync failed for object type {#} on NSX Manager {#}.)	보조 NSX Manager에서 범용 개체의 전체 동기화를 수행하지 못했습니다. 작업: NSX Manager에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.
31000 3	위험	아니요	NSX Manager {#}에서 엔티티 {#}에 대한 범용 동기화 작업이 실패했습니다.(Universal sync operation failed for the entity {#} on NSX Manager {#}.)	크로스 vCenter 환경에서 보조 NSX Manager와 범용 개체를 동기화하지 못했습니다. 작업: NSX Manager에 대한 기술 지원 로그를 수집하고 VMware 기술 지원에 문의하십시오.

NSX 관리 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 NSX 관리에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
32000 1	위험	아니요	NSX Manager IP가 MAC 주소인 다른 컴퓨터에 할당되었습니다.(The NSX Manager IP has been assigned to another machine with the MAC Address.)	NSX Manager 관리 IP 주소가 동일한 네트워크의 VM에 할당되었습니다. 6.2.3 이전에는 중복된 NSX Manager IP 주소가 감지 또는 방지되지 않았습니다. 이로 인해 데이터 경로 중단이 발생할 수 있습니다. 6.2.3 이상에서는 중복된 주소가 감지되면 이 이벤트가 발생합니다. 작업: 중복된 주소 문제를 해결하십시오.

논리적 네트워크 시스템 이벤트

이 표에서는 논리적 네트워킹과 관련된 시스템 이벤트 메시지에 대해 설명합니다.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
814	위험	아니요	지원되는 분산 가상 포트 그룹 중 일부가 수정 및/또는 제거되었기 때문에 논리적 스위치 {#}이(가) 더 이상 올바르게 구성되지 않습니다.(Logical Switch {#} is no longer properly configured since some of the backing distributed virtual port groups were modified and/or removed.)	NSX 논리적 스위치를 지원하는 하나 이상의 DVS 포트 그룹이 수정 또는 삭제되었거나 논리적 스위치 제어부 모드를 변경하지 못했습니다. 작업: 포트 그룹을 삭제 또는 수정하여 이 이벤트가 트리거된 경우 vSphere Web Client의 [논리적 스위치] 페이지에 오류가 표시됩니다. 오류를 클릭하여 누락된 DVS 포트 그룹을 생성하십시오. 제어부 모드 변경에 실패하여 이벤트가 트리거된 경우 업데이트를 다시 수행하십시오. NSX 업그레이드 가이드에서 "전송 영역 및 논리적 스위치 업데이트"를 참조하십시오.
1900	위험	아니요	호스트에서 VXLAN을 초기화하지 못했습니다.(VXLAN initialization failed on the host.)	필요한 수의 VTEP에 대해 VMkernel NIC를 구성하지 못했으므로 VXLAN 초기화에 실패했습니다. NSX는 VXLAN에 대해 사용자가 선택한 DVS를 준비하고 사용할 VTEP VMkernel NIC용 DV 포트 그룹을 생성합니다. VXLAN 구성 중에 팀 구성, 로드 밸런싱 메서드, MTU 및 VLAN ID가 선택됩니다. 팀 구성 및 로드 밸런싱 메서드는 VXLAN에 대해 선택된 DVS의 구성과 일치해야 합니다. 작업: vmkernel.log를 검토하십시오. NSX 문제 해결 가이드의 "인프라 준비" 섹션도 참조하십시오.
1901	위험	아니요	호스트에서 VXLAN 포트를 초기화하지 못했습니다.(VXLAN port initialization failed on the host.)	연결된 DV 포트에서 VXLAN을 구성하지 못했으며 포트 연결이 끊어졌습니다. NSX는 VXLAN에 대해 사용자가 선택한 DVS를 준비하고 사용할 각 구성된 논리적 스위치용 DV 포트 그룹을 생성합니다. 작업: vmkernel.log를 검토하십시오. NSX 문제 해결 가이드의 "인프라 준비" 섹션도 참조하십시오.
1902	위험	아니요	VXLAN 인스턴스가 호스트에 없습니다.(VXLAN instance does not exist on the host.)	ESXi 호스트의 DVS가 VXLAN에 대해 아직 사용되도록 설정되지 않았을 때 DV 포트에 대해 VXLAN 구성이 수신되었습니다. 작업: vmkernel.log를 검토하십시오. NSX 문제 해결 가이드의 "인프라 준비" 섹션도 참조하십시오.
1903	위험	아니요	지원되는 IP 인터페이스가 특정 멀티캐스트 그룹에 가입하지 못하기 때문에 논리적 스위치 {#}이(가) 올바르게 작동할 수 없습니다.(Logical Switch {#} can't work properly since the backing IP interface couldn't join specific multicast group.)	VTEP 인터페이스가 지정된 멀티캐스트 그룹에 연결하지 못했습니다. 특정 호스트에 대한 트래픽은 문제가 해결될 때까지 영향을 받습니다. NSX는 멀티캐스트 그룹에 연결하기 위해 주기적인 재시도 메커니즘(5초 간격)을 사용합니다. 작업: vmkernel.log를 검토하십시오. NSX 문제 해결 가이드의 "인프라 준비" 섹션도 참조하십시오.

이벤트 코드	이벤트 심각도	정보가 트리거됨	이벤트 메시지	설명
1905	위험	아니요	지원되는 IP 인터페이스에서 올바른 IP 주소를 얻을 수 없으므로 전송 영역을 사용하지 못할 수 있습니다.(Transport Zone may not be used since the backing IP interface can't acquire correct IP Address.)	VTEP VMkernel NIC에 올바른 IP 주소를 할당하지 못했습니다. VMkernel NIC를 통과하는 모든 VXLAN 트래픽이 삭제됩니다. 작업: VMKNics를 위한 IP 할당에 DHCP를 사용할 경우 VXLAN 전송 VLAN에서 DHCP를 사용할 수 있는지 확인하십시오. "IP 풀에 IP 주소 부족 오류: NSX 호스트 준비 실패"(http://kb.vmware.com/kb/2137025)를 참조하십시오.
1906	위험	아니요	VXLAN overlay class is missing on DVS.	VXLAN에 대해 DVS가 구성되었을 때 NSX VIB가 설치되지 않았습니다. 모든 VXLAN 인터페이스가 DVS에 연결되지 않습니다. 작업: "NSX/VCNS 환경에서 업그레이드 후에 네트워크 연결 문제 발생"(http://kb.vmware.com/kb/2107951)을 참조하십시오.
1920	위험	아니요	연결을 설정할 수 없어 VXLAN 컨트롤러 {#}이(가) 제거되었습니다. 컨트롤러 IP 구성을 확인하고 다시 배포하십시오.(VXLAN Controller {#} has been removed due to the connection can't be built, please check controller IP configuration and deploy again.)	컨트롤러 배포가 실패했습니다. 작업: 할당된 IP 주소에 연결할 수 있는지 확인하십시오. NSX 문제 해결 가이드의 "NSX Controller" 섹션도 참조하십시오.
1930	위험	아니요	컨트롤러 {#}에서 노드 {1}에 연결할 수 없습니다(활성={#}). 현재 연결 상태는 {#}입니다. (The controller {#} cannot establish the connection to the node {#} (active={#}). Current connection status = {#}.)	두 컨트롤러 노드의 연결이 끊어져서 컨트롤러 간 통신에 영향을 미칩니다. 작업: NSX 문제 해결 가이드에서 "NSX Controller" 섹션을 참조하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
1935	위험	아니요	모든 컨트롤러가 비활성 상태이므로 호스트 {#} 정보를 컨트롤러로 전송할 수 없습니다. 컨트롤러가 활성화되면 컨트롤러 동기화가 필요할 수 있습니다. (Host {#} information could not be sent to controllers as all controllers are inactive. Controller synchronization may be needed once controllers become active.)	호스트 인증서 정보를 NSX Controller 클러스터로 전송하지 못했습니다. 호스트와 컨트롤러 클러스터 간 통신 채널이 예상치 않게 동작할 수 있습니다. 작업: ESXi 호스트를 준비하기 전에 NSX Controller 클러스터 상태가 정상인지 확인하십시오. controller sync API를 사용하여 이 문제를 해결하십시오.
1937	위험	아니요	VXLAN vmknics {#} [PortGroup = {#}]이(가) 없거나 호스트 {#}에서 삭제되었습니다. (VXLAN vmknics {#} [PortGroup = {#}] is missing or deleted from host {#}.)	VXLAN VMkernel NIC가 호스트에서 누락되었거나 삭제되었습니다. 호스트를 들어오거나 나가는 트래픽이 영향을 받습니다. 작업: 이 문제를 해결하려면 설치 > 논리적 네트워크 준비 > VXLAN 전송 탭에서 해결 버튼을 클릭합니다.
1939	위험	아니요	VXLAN vmknics {#} [PortGroup = {#}]이(가) 호스트 {#}에서 삭제되었거나 호스트-vCenter 연결에 문제가 있을 수 있습니다. (VXLAN vmknics {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues.)	NSX Manager에서 VXLAN VMkernel NIC가 Virtual Center에 없음을 감지했습니다. 이 문제는 vCenter Server-호스트 통신 문제로 인해 발생할 수 있습니다. 또한 vCenter Server 또는 호스트가 재부팅되면 짧은 기간 동안 NSX Manager가 VXLAN VMkernel NIC를 감지할 수 없게 되어 이 이벤트에 플래그가 지정됩니다. vCenter Server 및 호스트가 재부팅을 끝내면 NSX Manager는 VXLAN VMkernel NIC를 다시 확인하고 모든 것이 정상 상태가 되면 이 이벤트를 지웁니다. 작업: 이 문제가 지속되는 경우 설치 > 논리적 네트워크 준비 > VXLAN 전송 탭에서 해결 버튼을 클릭하여 이 문제를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
1941	위험	아니요	호스트 연결 상태 변경됨: 이벤트 코드: {#}, 호스트: {#} (ID: {#}), NSX Manager - 방화벽 에이전트: {#}, NSX Manager - 제어부 에이전트: {#}, 제어부 에이전트 - 컨트롤러: {#}.(Host Connection Status Changed: Event Code: {#}, Host: {#} (ID: {#}), NSX Manager - Firewall Agent: {#}, NSX Manager - Control Plane Agent: {#}, Control Plane Agent - Controllers: {#}.)	NSX Manager가 NSX Manager-호스트 방화벽 에이전트 간 연결, NSX Manager-호스트 제어부 에이전트 간 연결 또는 호스트 제어부 에이전트-NSX Controller 간 연결 중 하나에 대해 다운 상태를 감지했습니다. 작업: NSX Manager-호스트 방화벽 에이전트 간 연결이 다운되면 NSX Manager 및 방화벽 에이전트 로그 (/var/log/vsfwd.log)를 확인하거나 POST https://NSX-Manager-IP-Address/api/2.0/nwfabric/configure?action=synchronize REST API 호출을 전송하여 연결을 다시 동기화하십시오. NSX Manager-제어부 에이전트 간 연결이 다운된 경우 NSX Manager 및 제어부 에이전트 로그 (/var/log/netcpa.log)를 확인하십시오. 제어부 에이전트-NSX Controller 간 연결이 다운된 경우 Networking & Security > 설치 로 이동한 후 호스트 연결 상태를 확인하십시오.
1942	위험	아니요	LogicalSwitch {#}의 지원되는 포트 그룹 [moid = {#}]이 누락으로 표시되었습니다.(The backing portgroup [moid = {#}] of LogicalSwitch {#} is marked as missing.)	NSX Manager는 NSX 논리적 스위치에 대한 지원 DV 포트 그룹이 Virtual Center에 없음을 감지했습니다. 작업: 설치 > 논리적 네트워크 준비 > VXLAN 전송 탭에서 해결 버튼을 클릭하거나 REST API(POST <a href="https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate">https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate)를 사용하여 포트 그룹을 다시 생성하십시오.
1945	위험	아니요	컨트롤러 {#}의 디바이스 {#}에 디스크 지연 경고가 설정되었습니다.(The device {#} on controller {#} has the disk latency alert on.)	NSX Manager에서 NSX Controller에 대해 높은 디스크 지연 시간을 감지했습니다. 작업: NSX 문제 해결 가이드에서 "NSX Controller" 섹션을 참조하십시오.
1946	정보	아니요	컨트롤러 {0}의 모든 디스크 지연 경고가 꺼졌습니다.(All disk latency alerts on controller {0} are off.)	NSX Manager에서 더 이상 컨트롤러에 대해 높은 디스크 지연 시간을 감지하지 못합니다. 작업: 정보 전용 이벤트입니다. 어떠한 작업도 필요하지 않습니다.
1947	위험	아니요	vCenter에서 컨트롤러 가상 시스템의 전원이 꺼졌습니다.(Controller Virtual Machine is powered off on vCenter.)	NSX Manager가 Virtual Center에서 NSX Controller VM 전원이 꺼져 있음을 감지했습니다. 컨트롤러 클러스터 상태가 연결 끊김이 될 수도 있습니다. 이 경우 작업 클러스터를 필요로 하는 작업을 줄 수 있습니다. 작업: 설치 > 관리 탭에서 컨트롤러에 대한 해결 버튼을 클릭하거나 API POST <a href="https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate">https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate 를 호출하여 컨트롤러 VM의 전원을 켜십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
1948	위험	아니요	vCenter에서 컨트롤러 가상 시스템이 삭제되었습니다. (Controller Virtual Machine is deleted from vCenter.)	NSX Manager가 Virtual Center에서 NSX Controller VM이 삭제되었음을 감지했습니다. 컨트롤러 클러스터 상태가 연결 끊김이 될 수도 있습니다. 이 경우 작업 클러스터를 필요로 하는 작업에 영향을 줄 수 있습니다. 작업: 설치 > 관리 탭에서 컨트롤러에 대한 해결 버튼을 클릭하거나 API POST <code>https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate</code> 를 호출하여 NSX Manager 데이터베이스에서 해당 컨트롤러의 상태를 제거하십시오.
1952	위험	아니요	VXLAN 포트 그룹 [moid = dvportgroup-xx] 및 관련 DVS에는 다른 팀 구성 정책이 있습니다. (The VXLAN portgroup [moid = dvportgroup-xx] and associated DVS have different teaming policies.)	NSX Manager가 VXLAN 포트 그룹의 팀 구성 정책이 관련된 DVS의 팀 구성 정책과 다르다는 것을 감지했습니다. 이로 인해 예측할 수 없는 동작이 발생할 수 있습니다. 작업: 같은 팀 구성 정책을 갖도록 VXLAN 포트 그룹 또는 DVS를 다시 구성하십시오.

ID 방화벽 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 IDFW(ID 방화벽)에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
395000	위험	아니요	도메인 컨트롤러 Eventlog 서버의 SecurityLog가 꽉 찼습니다. (SecurityLog on Domain Controller Eventlog Server is Full.)	Active Directory 이벤트 로그 서버의 보안 로그가 꽉 찼습니다. 로그 스크랩을 사용하도록 구성된 IDFW 작동이 중단됩니다. 작업: Active Directory 서버 관리자에게 문의하고 보안 로그 크기를 늘리거나 보안 로그를 지우거나 보안 로그를 아카이브하십시오.

호스트 준비 시스템 이벤트

이 표에서는 호스트 준비와 관련된 모든 시스템 이벤트 메시지에 대해 설명합니다.

참고 여러 ESX Agent Manager 이벤트가 NSX의 단일 이벤트에 매핑됩니다.

이벤트 코드	이벤트 심 각도	경보가 트리 거됨	이벤트 메시지	설명
270000	정보	예	VIB 모듈이 {hostID} 호스트로 업로드되었지만 {hostID} 호스트가 유지 보수 모드로 전환될 때까지 완전히 업로드되지 않습니다.(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 Manager는 호스트를 유지 보수 모드로 전환합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	위험	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 vSphere ESX Agent Manager가 해당 에이전트에 대한 OVF 패키지에 액세스할 수 없어 에이전트 가상 시스템을 배포할 수 없습니다. 일반적으로 이는 OVF 패키지를 제공하는 웹 서버가 다운되었을 때 발생합니다. 웹 서버는 에이전트를 생성한 솔루션에 대한 내부용으로 사용되는 경우가 많습니다.(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 Manager는 에이전트를 다시 배포합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	위험	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 vSphere ESX Agent Manager가 해당 에이전트에 대한 VIB 패키지에 액세스할 수 없어 VIB 모듈을 배포할 수 없습니다. 일반적으로 이는 VIB 패키지를 제공하는 웹 서버가 다운되었을 때 발생합니다. 웹 서버는 에이전트를 생성한 솔루션에 대한 내부용으로 사용되는 경우가 많습니다. (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 Manager는 VIB 모듈을 다시 설치합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트가 {hostID} 호스트와 호환되지 않았으므로 에이전트를 배포할 수 없습니다.(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 Manager는 에이전트를 다시 배포합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오. 그러나 이 문제는 에이전트가 호스트와 호환될 수 있도록 호스트 또는 솔루션을 업그레이드할 때까지 지속되기 쉽습니다.
270000	높음	예	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트 가상 시스템 IP 주소 풀에 사용 가능한 IP 주소가 없습니다.(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.)	작업: 이 문제를 해결하려면 일부 IP 주소를 사용 가능하게 해제하거나 IP 풀에 IP 주소를 추가한 다음 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 {hostID} 호스트에 사용 가능한 CPU 또는 메모리 리소스가 충분하지 않아 에이전트 가상 시스템을 배포할 수 없습니다.(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.)	<p>ESX Agent Manager는 에이전트 가상 시스템을 다시 배포합니다.</p> <p>그러나 이 문제는 충분한 CPU 및 메모리 리소스를 사용할 수 있게 될 때까지 지속되기 쉽습니다.</p> <p>작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.</p>
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 {hostID} 호스트에 사용 가능한 CPU 또는 메모리 리소스가 충분하지 않아 에이전트 가상 시스템을 배포할 수 없습니다.(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.)	<p>ESX Agent Manager는 에이전트 가상 시스템을 다시 배포합니다.</p> <p>작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.</p> <p>그러나 이 문제는 다음을 수행할 때까지 지속되기 쉽습니다.</p> <p>호스트 에이전트 가상 시스템 데이터스토어의 공간을 확보합니다.</p> <p>-또는-</p> <p>충분한 여유 공간이 있는 새 에이전트 가상 시스템 데이터스토어를 구성합니다.</p>
270000	높음	예	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트 가상 시스템 IP 주소 풀에 사용 가능한 IP 주소가 없어 에이전트 가상 시스템의 전원이 꺼져 있습니다.(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.)	<p>작업: 에이전트 가상 시스템 네트워크에 IP 풀을 생성하고 systemalarms API의 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.</p>

이벤트 코드	이벤트 심 각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 데이터스토어가 {hostID} 호스트에서 구성되어 있지 않아 에이전트를 배포할 수 없습니다.(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}.)	작업: 호스트에 에이전트 가상 시스템 데이터스토어를 구성해야 합니다.
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 네트워크가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다.(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.)	작업: 호스트에 에이전트 가상 시스템 네트워크를 구성해야 합니다.
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 네트워크가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다.호스트에 customAgentVmNetwork에 나열된 네트워크 중 하나가 추가되어야 합니다. (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.)	작업: 호스트에 customAgentVmNetwork 네트워크 중 하나를 추가해야 합니다.

이벤트 코드	이벤트 심 각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 데이터스토어가 호스트에 구성되어 있지 않아 에이전트를 배포할 수 없습니다. 호스트에 customAgentVmDatastore에 나열된 데이터스토어 중 하나가 추가되어야 합니다. (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.)	호스트에 customAgentVmDatastore 라는 데이터스토어 중 하나를 추가해야 합니다.
270000	높음	예	에이전시를 생성한 솔루션이 더 이상 vCenter 서버에 등록되어 있지 않습니다. (The solution that created the agency is no longer registered with the vCenter server.)	ESX Agent Manager는 에이전시를 제거합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	dvFilter 스위치가 호스트에 있지만 호스트에서 dvFilter에 종속된 에이전트가 없습니다. 일반적으로 에이전트 구성이 변경되었을 때 호스트의 연결이 끊기는 경우에 발생합니다. (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 Manager가 dvFilterSwitch를 제거합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템이 호스트에서 프로비저닝되어야 하지만 OVF 패키지가 프로비저닝되지 않아 가상 시스템이 프로비저닝되지 않았습니다. OVF 패키지를 제공하는 솔루션이 업그레이드되거나 패치되어 에이전트 가상 시스템에 대한 유효한 패키지를 제공할 때까지는 프로비저닝이 성공하지 않을 수 있습니다. (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 Manager는 OVF 프로비저닝을 다시 시도합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	에이전트 가상 시스템의 전원이 켜져야 하지만 OVF 속성이 누락되어 있거나 유효한 값이 아닙니다.(An agent virtual machine needs to be powered on, but an OVF property is either missing or has an invalid value.)	작업: 에이전트 가상 시스템을 프로비저닝하는 데 사용되는 에이전트 구성의 OVF 환경을 업데이트하십시오.
270000	높음	예	에이전트 가상 시스템이 이 vSphere ESX Agent Manager 서버 인스턴스의 에이전트에 속하지 않은 vCenter 인벤토리에서 발견되었습니다.(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 Manager의 전원이 꺼지고(전원이 켜져 있는 경우) 에이전트 가상 시스템이 삭제됩니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	VIB 모듈을 사용하려면 호스트가 유지 보수 모드여야 하지만 vSphere ESX Agent Manager를 유지 보수 모드로 전환할 수 없습니다. 이는 호스트가 유지 보수 모드로 전환하기 전에 이동하거나 중단하지 못하는 호스트에서 가상 시스템이 실행 중인 경우에 발생할 수 있습니다. (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 Manager는 호스트를 유지 보수 모드로 전환하려고 시도합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오. 그러나 이 문제는 가상 시스템 전원을 끄거나 가상 시스템을 이동하여 호스트를 유지 보수 모드로 전환할 때까지 지속되기 쉽습니다.
270000	위험	예	VIB 모듈이 호스트에서 설치되어야 하지만 VIB 패키지가 올바르지 않은 형식이기 때문에 설치하지 못했습니다. 번들을 제공하는 솔루션이 업그레이드되어가 패치되어 유효한 VIB 패키지를 제공할 때까지는 설치하지 못할 수 있습니다. (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 Manager는 VIB 설치를 다시 시도합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	VIB 모듈이 호스트에서 설치되어야 하지만 설치하지 못했습니다. 일반적으로 구체적인 문제(이 문제의 하위 클래스)가 VIB 모듈이 설치되지 않는 구체적인 이유를 나타냅니다. (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 Manager는 VIB 설치를 다시 시도합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	정보	예	VIB 모듈이 호스트로 업로드되었지만 호스트가 재부팅될 때까지는 활성화되지 않습니다.(A VIB module has been uploaded to the host, but will not be activated until the host is rebooted.)	ESX Agent Manager는 호스트를 유지 보수 모드로 전환하고 재부팅합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	VIB 모듈을 설치하지 못했으나 호스트에 있는 vSphere ESX Agent Manager에서 자동 설치를 허용하지 않았기 때문에 설치하지 못했습니다.(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.)	작업: vSphere Update Manager로 이동하고 호스트에 필수 공지를 설치하거나 호스트의 이미지 프로파일에 공지를 추가하십시오. 자세한 내용은 vSphere 설명서를 참조하십시오.
270000	높음	예	VIB 모듈의 설치를 제거하지 못했으나 호스트에 있는 vSphere ESX Agent Manager에서 자동 설치 제거를 허용하지 않았기 때문에 설치를 제거하지 못했습니다.(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.)	작업: vSphere Update Manager로 이동하고 호스트에서 필수 공지를 제거하거나 호스트의 이미지 프로파일에 공지를 추가하십시오. 자세한 내용은 vSphere 설명서를 참조하십시오.

이벤트 코드	이벤트 심 각도	경보가 트리 거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템이 손상되었습니다.(An agent virtual machine is corrupt.)	<p>ESX Agent Manager는 에이전트 가상 시스템을 삭제하고 다시 프로비저닝합니다.</p> <p>작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.</p> <p>이 문제를 수동으로 해결 하려면 누락된 파일과 관련된 문제를 해결하고 에이전트 가상 시스템의 전원을 켜십시오.</p>
270000	높음	예	에이전트 가상 시스템이 호스트에서 제거되어야 하지만 에이전트 가상 시스템이 제거되지 않았습니다. 일반적으로 구체적인 문제(이 문제의 하위 클래스)가 vSphere ESX Agent Manager가 에이전트 가상 시스템을 제거할 수 없는 구체적인 이유를 나타냅니다. 예를 들어 호스트가 유지 보수 모드이거나 전원이 꺼져 있거나 대기 모드일 때입니다. (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>ESX Agent Manager는 에이전트를 다시 배포합니다.</p> <p>작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.</p>
270000	높음	예	에이전트 가상 시스템이 가상 시스템 템플릿입니다. (An agent virtual machine is a virtual machine template.)	<p>ESX Agent Manager는 에이전트 가상 시스템 템플릿을 가상 시스템으로 변환합니다.</p> <p>작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.</p>

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템이 호스트에서 배포되어야 하지만 에이전트 가상 시스템이 배포되지 않았습니다. 일반적으로 구체적인 문제(이 문제의 하위 클래스)가 vSphere ESX Agent Manager에서 에이전트를 배포할 수 없는 구체적인 이유를 나타냅니다. 예를 들어 에이전트에 대한 OVF 패키지에 액세스할 수 없거나 호스트 구성이 누락되는 경우입니다. 또한 에이전트 가상 시스템이 명시적으로 호스트에서 제거된 경우에도 발생할 수 있습니다. (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 Manager는 에이전트 가상 시스템을 다시 배포합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트 가상 시스템의 전원이 켜지지 않습니다.(An agent virtual machine is expected to be powered on, but the agent virtual machine is powered off.)	ESX Agent Manager는 에이전트 가상 시스템의 전원을 켭니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.

이벤트 코드	이벤트 심 각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	에이전트 가상 시스템의 전원이 꺼져야 하지만 에이전트 가상 시스템의 전원이 꺼지지 않습니다.(An agent virtual machine is expected to be powered off, but the agent virtual machine is powered off.)	ESX Agent Manager는 에이전트 가상 시스템의 전원을 끕니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	에이전트 가상 시스템의 전원이 켜져야 하지만 에이전트 가상 시스템이 일시 중 단되었습니다.(An agent virtual machine is expected to be powered on, but the agent virtual machine is suspended.)	ESX Agent Manager는 에이전트 가상 시스템의 전원을 켭니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	에이전트 가상 시스템이 지정된 에이전트 가상 시스템 폴더에 있어야 하지만 다른 폴더에서 발견되었습니다.(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 Manager는 에이전트 가상 시스템을 지정된 에이전트 폴더로 다시 이동합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	에이전트 가상 시스템이 지정된 에이전트 가상 시스템 리소스 풀에 있어야 하지만 다른 리소스 풀에서 발견되었습니다.(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 Manager는 에이전트 가상 시스템을 지정된 에이전트 리소스 풀로 다시 이동합니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.
270000	높음	예	EAM 경보를 받았습니다.(EAM alarm received.)	ESX Agent Manager가 NSX VIB 또는 서비스 VM에서 NSX 설치 또는 업그레이드 문제를 감지했습니다. 작업: 호스트 준비(Host Preparation) 탭에서 해결(Resolve) 옵션을 클릭하거나 systemalarms API에서 action=resolve 매개 변수를 사용하여 경보를 해결하십시오.