NSX 로깅 및 시스템 이벤트

업데이트 4
2017년 8월 10일에 수정됨
VMware NSX for vSphere 6.3

vmware®

VMware 웹 사이트 (https://docs.vmware.com/kr/) 에서 최신 기술 문서를 확인할 수 있습니다.
또한 VMware 웹 사이트에서 최신 제품 업데이트를 제공합니다.
이 문서에 대한 의견이 있으면 docfeedback@vmware.com으로 사용자 의견을 보내주십시오.

Copyright © 2010 – 2017 VMware, Inc. 판권 소유. 저작권 및 상표 정보.

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

목차

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/pubs를 참조하십시오.

1 시스템 이벤트, 경보 및 로그

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

이 장에서는 다음 주제에 대해 설명합니다.

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 푸시되므로 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.

프로시저

1 vSphere Web Client에 로그인합니다.

2 **네트워킹 및 보안(Networking & Security)**을 클릭한 다음 **네트워킹 및 보안 인벤토리(Networking & Security Inventory)** 아래에서 **NSX Managers**를 클릭합니다.

3 **이름(Name)** 열의 NSX Manager를 클릭한 후 **모니터(Monitor)** 탭을 클릭합니다.

4 **시스템 이벤트(System Events)** 탭을 클릭합니다.

열 머리글의 화살표를 클릭하여 이벤트를 정렬하거나 **필터(Filter)** 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 경보 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 경보

호스트 경보는 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.	1 호스트에 로그인하고 /etc/init.d/vShield-Endpoint-Mux start 명령을 입력하여 Guest Introspection이 실행 중인지 확인합니다. 2 Guest Introspection이 NSX Manager에 연결할 수 있도록 네트워크가 적절히 구성되었는지 확인합니다. 3 NSX Manager를 재부팅합니다.

SVM 경보

SVM 경보는 SVM의 상태에 영향을 미치는 이벤트에 의해 생성됩니다.

표 1-2. 빨간색 SVM 경보

문제	조치
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 및 호스트 로그

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

NSX 및 호스트 로그 파일 목록에 대해서는 NSX 문제 해결 가이드의 "인프라 준비"를 참조하십시오.

감사 로그

감사 로그는 NSX Manager에 로그인한 사용자가 수행하는 모든 작업을 기록합니다.

감사 로그 보기

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

프로시저

1 vSphere Web Client에 로그인합니다.

2 **네트워킹 및 보안(Networking & Security)**을 클릭한 다음 **네트워킹 및 보안 인벤토리(Networking & Security Inventory)** 아래에서 **NSX Managers**를 클릭합니다.

3 **이름(Name)** 열에서 NSX 서버를 클릭한 후, **모니터(Monitor)** 탭을 클릭합니다.

4 **감사 로그(Audit Logs)** 탭을 클릭합니다.

5 감사 로그에 대한 세부 정보가 있을 경우 해당 로그의 **작업(Operation)** 열에서 텍스트를 클릭할 수 있습니다. 감사 로그 세부 정보를 보려면 **작업(Operation)** 열의 텍스트를 클릭합니다.

6 **감사 로그 변경 세부 정보(Audit Log Change Details)**에서 **변경된 행(Changed Rows)**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.

프로시저

1 NSX Manager 가상 장치에 로그인합니다.

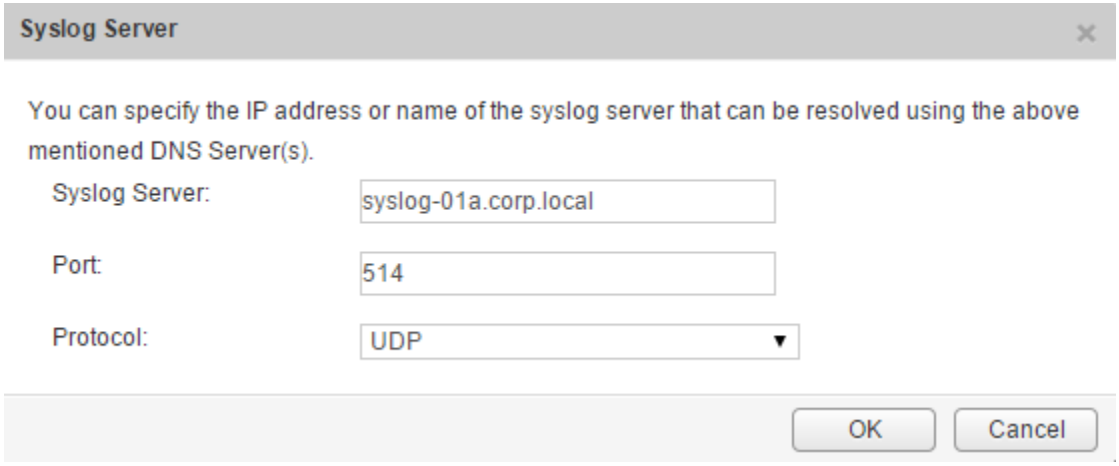
웹 브라우저에서 https://<nsx-manager-ip> 또는 https://<nsx-manager-hostname>의 NSX Manager 장치 GUI로 이동하여 NSX Manager 설치 중에 설정한 암호를 사용하여 admin 권한으로 로그인합니다.

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.

프로시저

1 vSphere Web Client에 로그인합니다.

2 **네트워킹 및 보안(Networking & Security)**을 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.

3 NSX Edge를 두 번 클릭합니다.

4 **관리(Manage)** 탭을 클릭한 후 **설정(Settings)** 탭을 클릭합니다.

5 **세부 정보(Details)** 패널에서 Syslog 서버 옆의 **변경(Change)**을 클릭합니다.

6 두 원격 Syslog 서버의 IP 주소를 입력하고 프로토콜을 선택합니다.

7 **확인(OK)**을 클릭하여 구성을 저장합니다.

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.

프로시저

1 NSX Manager 가상 장치에 로그인합니다.

2 장치 관리에서 **장치 설정 관리(Manage Appliance Settings)**를 클릭합니다.

3  을 클릭하고 **기술 지원 로그 다운로드(Download Tech Support Log)**를 클릭합니다.

4 **다운로드(Download)**를 클릭합니다.

5 로그를 다운로드할 준비가 되면 **저장(Save)**을 클릭하여 로그를 데스크톱에 다운로드합니다.

로그가 압축되고 파일 확장명 .gz가 붙습니다.

후속 작업

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

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:

프로시저

1 vSphere Web Client에 로그인합니다.

2 **Networking & Security**를 클릭한 다음 **설치(Installation)**를 클릭합니다.

3 **관리(Management)**에서 로그를 다운로드하려는 컨트롤러를 선택합니다.

4 **기술 지원 로그 다운로드(Download tech support logs)**를 클릭합니다.

5 **다운로드(Download)**를 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(Save)**을 클릭하여 로그를 데스크톱에 다운로드합니다.

로그가 압축되고 .gz 파일 확장명이 붙습니다.

이제 다운로드한 로그를 분석할 수 있습니다.

후속 작업

VMware 기술 지원에 대한 진단 정보를 업로드하려면 기술 지원 문서 2070100을 참조하십시오.

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.

프로시저

1 vSphere Web Client에 로그인합니다.

2 **네트워킹 및 보안(Networking & Security)**을 클릭한 다음 **NSX Edge(NSX Edges)**를 클릭합니다.

3 NSX Edge 인스턴스를 선택합니다.

4 **추가 작업(More Actions)**( ) 아이콘을 클릭하고 **기술 지원 로그 다운로드(Download Tech Support Logs)**를 선택합니다.

5 기술 지원 로그가 생성되면 **다운로드(Download)**를 클릭합니다.

6 다운로드 위치 선택 대화상자에서 로그 파일을 저장할 디렉토리를 찾아 선택합니다.

7 **저장(Save)**을 클릭합니다.

8 **닫기(Close)**를 클릭합니다.

2 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," (12 페이지)를 참조하십시오.
- NSX Edge 기술 지원 로그를 수집하려면 "NSX Edge에 대한 기술 지원 로그 다운로드," (13 페이지)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.

이 장에서는 다음 주제에 대해 설명합니다.

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	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 끊어졌습니다.	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	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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
230002	위험	아니요	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	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	경보가 트리거됨	이벤트 메시지	설명
301001	위험	아니요	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 Manager와 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	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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301031	위험	아니요	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 https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>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	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.
301041	위험	아니요	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	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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301061	위험	아니요	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 https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id> 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	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 https://<nsx-mgr>/api/4.0/firewall/forceSync/<host-id>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.
301064	심각	아니요	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	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	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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301081	위험	아니요	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	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	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.
301502	위험	아니요	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	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	Failed to publish container updates to cluster {clusterID}. Refer logs for details.	클러스터 또는 하나 이상의 호스트에 대해 네트워크 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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301505	위험	아니요	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	Failed to publish exclude list updates to cluster {clusterID}. Refer logs for details.	클러스터 또는 하나 이상의 호스트에 대해 예외 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.
301508	위험	아니요	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	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	Firewall is installed on host {hostID} [{hostID}].	호스트에서 분산 방화벽이 성공적으로 설치되었습니다. 작업: vCenter Server에서 **홈(Home) > Networking & Security > 설치(Installation)**로 이동하여 [호스트 준비] 탭을 선택합니다. 방화벽 상태가 녹색으로 표시되는지 확인합니다.
301513	심각	아니요	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	Firewall is enabled on cluster {clusterID}.	클러스터에서 분산 방화벽이 성공적으로 설치되었습니다. 작업: vCenter Server에서 **홈(Home) > Networking & Security > 설치(Installation)**로 이동하여 [호스트 준비] 탭을 선택합니다. 방화벽 상태가 녹색으로 표시되는지 확인합니다.
301515	위험	아니요	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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301516	위험	아니요	Firewall is disabled on cluster {clusterID}.	클러스터의 모든 호스트에서 분산 방화벽이 사용되지 않도록 설정되었습니다. 작업: 필요한 작업이 없습니다.
301034	심각	아니요	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	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	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	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	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 `https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>` 를 사용하여 방화벽 구성을 강제로 동기화하거나 **설치(Installation) > 호스트 준비(Host Preparation)**로 이동한 후 **작업(Actions)**에서 **서비스 강제 동기화(Force Sync Services)**를 선택합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
301101	심각	아니요	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 https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>를 사용하여 방화벽 구성을 강제로 동기화하거나 **설치(Installation) > 호스트 준비(Host Preparation)**로 이동한 후 **작업(Actions)**에서 **서비스 강제 동기화(Force Sync Services)**를 선택합니다.
301103	심각	아니요	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 https://<nsx-mgr-ip>/api/4.0/firewall/forceSync/<host-id>를 사용하여 방화벽 구성을 강제로 동기화하거나 **설치(Installation) > 호스트 준비(Host Preparation)**로 이동한 후 **작업(Actions)**에서 **서비스 강제 동기화(Force Sync Services)**를 선택합니다.
301200	심각	아니요	Application Rule Manager flow analysis started.	애플리케이션 규칙 관리자 흐름 분석이 시작되었습니다. 작업: 필요한 작업이 없습니다.
301201	심각	아니요	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	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	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 Manager found NSX Edge VM (vmId : {#}) 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.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30014	심각	해당 없음	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 (vmId : {#}) is powered off.	NSX Edge VM의 전원이 꺼졌습니다. 작업: 정보 전용 이벤트입니다.
30032	높음	130032	NSX Edge appliance with vmId : {#} 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	NSX Edge VM (vmId : {#}) not found in the vCenter inventory.	NSX Edge VM을 vCenter 인벤토리에서 찾을 수 없습니다. 작업: VM이 실수로 삭제되었는지 확인하십시오. 확인한 후에는 Edge를 다시 배포하십시오.
30034	위험	130034	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	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	Powered-on NSX Edge appliance : {EdgeId #}, {vmName #} violates the virtual machine anti-affinity rule.	NSX Edge 고가용성은 반선호도 규칙을 vSphere 호스트에 자동으로 적용하므로 활성 및 대기 Edge VM이 다른 호스트에 배포됩니다. 이 이벤트는 이러한 반선호도 규칙이 클러스터에서 제거되었으며 두 Edge VM이 모두 동일한 호스트에서 실행되고 있음을 나타냅니다. 작업: vCenter Server로 이동한 후 반선호도 규칙을 확인하십시오.
30045	위험	해당 없음	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	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 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 (vmId : {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 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 engine is up.	AESNI crypto 엔진이 실행됩니다. 작업: 필요한 작업이 없습니다.
30154	심각	해당 없음	AESNI crypto engine is down.	AESNI crypto 엔진이 다운되었습니다. 작업: 필요한 작업이 없습니다. 예상된 상태입니다.
30155	높음	130155	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 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 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.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30202	심각	해당 없음	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} 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.
30205	위험	130205	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]} 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} 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 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.
30402	위험	130402	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 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.

이벤트 코드	이벤트 심각도	경보 코드	이벤트 메시지	설명
30405	심각	해당 없음	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	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.
30701	위험	해당 없음	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	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	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 심각, 위험 또는 높음 심각도의 패브릭에 대한 시스템 이벤트 메시지를 설명합니다.

패브릭 시스템 이벤트와 관련된 몇 가지 용어가 아래에 설명되어 있습니다.

- 패브릭은 NSX Manager가 호스트에서 네트워크 및 보안 서비스를 설치하기 위해 EAM(ESX Agent Manager)과 상호 작용하는 소프트웨어 계층입니다. NSX가 EAM에서 NSX VIB가 호스트에 성공적으로 설치되었다는 확인을 수신하면 패브릭 계층이 메시지 버스 설정을 트리거합니다. NSX API를 사용하는 /api/2.0/nwfabric/ 패브릭 세부 정보를 볼 수 있습니다.
- EAM(ESX Agent Manager) 에이전시는 배포 단위의 NSX Manager 데이터베이스이며 EAM 에이전시의 vCenter EAM 데이터베이스는 동기화 상태를 유지해야 합니다. EAM 에이전시는 배포를 위해 EAM에 의존하는 NSX 서비스를 정의하기 위해 vCenter EAM 데이터베이스에서 생성되는 개체입니다. 드문 경우지만 두 데이터베이스가 동기화되지 않을 수 있으며 이 경우 NSX는 이벤트 및 경보를 통해 이러한 상황을 알립니다.

다음 표에서는 패브릭 시스템 이벤트에 대해 심각, 위험 또는 높음 심각도의 시스템 이벤트 메시지를 문서화합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250004	높음	예	Datastore {#} could not be configured on host, probably its not connected.	호스트에 대한 보안 가상 시스템을 저장할 데이터스토어를 구성할 수 없습니다. 작업: 호스트가 데이터스토어에 연결할 수 있는지 확인하십시오.
250005	높음	예	Installation of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.	호스트에 NSX 서비스를 설치하는 동안 ESXi 호스트가 NSX에서 VIB/OVF에 액세스하지 못했습니다. vCenter 시스템 이벤트 테이블에서 이벤트 메시지: '배포 단위를 설치하지 못했습니다. ovf/vib url에 액세스할 수 있는지, 형식이 올바른지 그리고 ovf 환경의 모든 속성이 서비스 특성에 구성되어 있는지 확인하십시오. 자세한 내용은 로그를 참조하십시오.', 모듈:'보안 패브릭'을 확인하십시오. 작업: "NSX로 vSphere EAM(ESX Agent Manager) 문제 해결"(http://kb.vmware.com/kb/2122392)을 참조하십시오.
250008	높음	예	Service will need to be redeployed as the location of the OVF / VIB bundles to be deployed has changed.	NSX VIB 및 OVF는 NSX 버전마다 다른 URL을 통해 사용할 수 있습니다. 올바른 VIB를 찾으려면 https://<NSX-Manager-IP>/bin/vdn/nwfabric.properties로 이동해야 합니다. NSX Manager IP 주소가 변경되면 NSX OVF 또는 VIB를 다시 배포해야 할 수 있습니다. 작업: 경보를 해결하려면 **설치(Installation) > 호스트 준비(Host Preparation)** 탭에서 **해결(Resolve)** 링크를 클릭하거나 resolve API를 사용하십시오.
250009	높음	예	Upgrade of deployment unit failed, please check if ovf/vib urls are accessible, in correct format and all the properties in ovf environment have been configured in service attributes. Please check logs for details.	호스트 업그레이드 동안 EAM이 NSX에서 VIB/OVF에 액세스하지 못했습니다. vCenter 시스템 이벤트 테이블에서 이벤트 메시지: 배포 단위를 설치하지 못했습니다. ovf/vib url에 액세스할 수 있는지, 형식이 올바른지 그리고 ovf 환경의 모든 속성이 서비스 특성에 구성되어 있는지 확인하십시오. 자세한 내용은 로그를 참조하십시오.', 모듈:'보안 패브릭'을 확인하십시오. 작업: "NSX로 vSphere EAM(ESX Agent Manager) 문제 해결"(http://kb.vmware.com/kb/2122392)을 참조하십시오.
250012	높음	예	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.
250014	높음	예	Error while notifying security solution before upgrade.	업그레이드 전에 보안 솔루션에 알림을 보내는 동안 오류가 발생했습니다. 솔루션이 연결 가능/응답 상태가 아닐 수 있습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지 확인하십시오. resolve API를 사용하여 경보를 확인하십시오. 서비스가 다시 배포됩니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250015	높음	예	Did not receive callback from security solution for upgrade notification even after timeout.	시간이 초과된 후에도 업그레이드 알림에 대한 보안 솔루션의 콜백을 수신하지 못했습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. resolve API를 사용하여 경보를 확인하십시오. 서비스가 다시 배포됩니다.
250016	높음	아니요	Did not receive callback from security solution for uninstall notification even after timeout.	서비스를 제거하지 못했습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. resolve API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다.
250017	높음	예	Uninstallation of service failed.	제거 전에 보안 솔루션에 알림을 보내는 동안 오류가 발생했습니다. 다시 한 번 알리려면 확인하고 알림 없이 제거하려면 삭제하십시오. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. resolve API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다.
250018	높음	예	Error while notifying security solution before uninstall. Resolve to notify once again, or delete to uninstall without notification.	제거 전에 보안 솔루션에 알림을 보내는 동안 오류가 발생했습니다. 다시 한 번 알리려면 확인하고 알림 없이 제거하려면 삭제하십시오. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지와 솔루션에서 NSX에 연결할 수 있는지 확인하십시오. resolve API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다.
250019	높음	예	Server rebooted while security solution notification for uninstall was going on.	보안 솔루션에 제거 알림을 보내는 동안 서버가 재부팅되었습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지 확인하십시오. resolve API를 사용하여 경보를 확인하십시오. 서비스가 제거됩니다.
250020	높음	예	Server rebooted while security solution notification for upgrade was going on.	보안 솔루션에 제거 알림을 보내는 동안 서버가 재부팅되었습니다. 작업: NSX에서 솔루션 URL에 액세스할 수 있는지 확인하십시오. 확인 API를 사용하여 경보를 확인하십시오. 서비스가 다시 배포됩니다.
250021	위험	아니요	Connection to EAM server failed.	NSX Manager와 vCenter EAM 서비스 간의 연결이 다운되었습니다. 작업: vCenter가 작동 중인지와 EAM 서비스가 실행되고 있는지 확인하십시오. URL **http://{VC_IP}/eam/mob/**에 액세스할 수 있는지 확인하십시오. 자세한 내용은 NSX 문제 해결 가이드의 "인프라 준비"를 참조하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
250023	높음	예	Pre Uninstall cleanup failed.	제거 전 내부 정리 작업이 완료되지 못했습니다. 작업: 요청 본문 SystemAlarmsDto에 POST https://<<NSX-IP>>/api/2.0/services/systemalarms/<alarmId>?action=resolve API를 사용하여 경보를 확인하고 서비스를 제거하십시오.
250024	높음	예	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.	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	VIB는 수동 설치해야 합니다.	이 이벤트는 EAM을 사용하여 상태 비저장 호스트에서 NSX BITS를 업그레이드하거나 제거하려고 할 때 생성됩니다. 모든 상태 비저장 호스트는 Auto Deploy 기능을 사용해서 준비해야 합니다. 작업: Auto Deploy 기능을 사용하여 구성을 수정하고 resolve API를 사용하여 경보를 해결합니다.

배포 플러그인 시스템 이벤트

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

배포 플러그인 시스템 이벤트와 관련된 몇 가지 용어가 아래에 설명되어 있습니다.

- 배포 플러그인은 배포 전 및 배포 후 작업을 수행하기 위해 NSX 패브릭에 추가되는 추가 코드입니다.
- 배포 단위는 모든 클러스터에 대해 NSX Manager 데이터베이스에서 생성되는 개체입니다. 배포 단위는 네트워킹 및 보안 서비스가 설치되기 전에 생성되어야 합니다.

다음 표에서는 배포 플러그인 시스템 이벤트에 대해 심각, 위험 또는 높음 심각도의 시스템 이벤트 메시지를 문서화합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
280000	높음	예	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	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	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	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
390001	높음	예	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 (Installation) > 호스트 준비(Host Preparation)** 탭의 영향 받는 호스트 옆에 빨간색 오류 아이콘이 표시됩니다. 작업: "VMware NSX for vSphere 6.x의 메시지 버스 이해 및 문제 해결 "(http://kb.vmware.com/kb/2133897)에서 문제 해결 단계를 참조하십시오.
390002	높음	예	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: "VMware NSX for vSphere 6.x의 메시지 버스 이해 및 문제 해결 "(http://kb.vmware.com/kb/2133897)에서 문제 해결 단계를 참조하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
390003	높음	예	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: "VMware NSX for vSphere 6.x의 메시지 버스 이해 및 문제 해결 "(http://kb.vmware.com/kb/2133897)에서 문제 해결 단계를 참조하십시오.
391002	위험	아니요	Messaging infrastructure down on host.	NSX Manager와 NSX 호스트 간의 둘 이상의 하트비트 메시지가 누락되었습니다. 작업: "VMware NSX for vSphere 6.x의 메시지 버스 이해 및 문제 해결 "(http://kb.vmware.com/kb/2133897)에서 문제 해결 단계를 참조하십시오.
321100	위험	아니요	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. "VMware NSX for vSphere 6.x의 메시지 버스 이해 및 문제 해결 "(http://kb.vmware.com/kb/2133897)에서 문제 해결 단계를 참조하십시오.

Service Composer 시스템 이벤트

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

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
300000	위험	예	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	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 Composer 또는 resolve API를 사용하여 이 경보를 확인하십시오.
300002	높음	예	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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
300003	높음	예	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 resolve API를 통해 경보를 확인하고 정책을 동기화해야 합니다. "NSX 6.x의 Service Composer 문제 해결 "(http://kb.vmware.com/kb/2132612)도 참조하십시오.
300004	높음	예	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 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.
300005	높음	예	Service Composer is out of sync. No changes from Service Composer will be pushed to Firewall/Network Introspection.	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 Composer 또는 resolve API를 통해 경보를 확인하십시오.
300006	높음	예	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 네트워크 검사 서비스로 전송되지 않습니다. 작업: 오류 메시지를 확인하여 편집할 정책 및/또는 방화벽 섹션을 결정하십시오. Service Composer 또는 resolve API를 통해 경보를 확인하십시오.
300007	높음	예	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 Composer 또는 resolve API를 통해 경보를 확인하십시오.
300008	높음	예	Failure while deleting section corresponding to the Policy.	Service Composer에서 정책에 대한 방화벽 규칙 섹션을 삭제할 때 오류가 발생했습니다. 이 문제는 NSX Service Insertion이 있는 타사 서비스용 관리자에 연결할 수 없을 때 발생합니다. 작업: 타사 서비스 관리자에 대한 연결 문제를 조사하십시오. Service Composer 또는 resolve API를 통해 경보를 확인하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
300009	높음	예	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 Composer 또는 resolve API를 통해 경보를 확인하십시오.
300010	높음	예	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 Composer 또는 resolve API를 통해 경보를 확인하십시오.

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	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/2144624의 절차를 사용하여 SVM 로그를 수집하고 VMware 기술 지원에 문의하십시오.
280003	높음	예	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/2144624의 절차를 사용하여 SVM 로그를 수집하고 VMware 기술 지원에 문의하십시오.
280006	높음	예	Failed to mark agent as available.	ESX Agent VM을 사용 가능 상태로 표시하는 동안 내부 오류가 발생했습니다. 작업: resolve API를 사용하여 경보를 확인하십시오. 경보를 확인할 수 없으면 KB http://kb.vmware.com/kb/2144624의 절차를 사용하여 SVM 로그를 수집하고 VMware 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	경보가 트리거됨	이벤트 메시지	설명
310001	위험	아니요	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.
310003	위험	아니요	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	경보가 트리거됨	이벤트 메시지	설명
320001	위험	아니요	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.

VXLAN 시스템 이벤트

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

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
814	위험	아니요	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	VXLAN initialization failed on the host.	필요한 수의 VTEP에 대해 vmknic를 구성하지 못했으므로 VXLAN 초기화에 실패했습니다. NSX는 VXLAN에 대해 사용자가 선택한 DVS를 준비하고 사용할 VTEP vmknic용 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	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 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	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.
1905	위험	아니요	Transport Zone may not be used since the backing IP interface can't acquire correct IP Address.	VTEP vmknic에 올바른 IP 주소를 할당하지 못했습니다. vmknic를 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.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
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	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	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.
1935	위험	아니요	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 vmknic {#} [PortGroup = {#}] is missing or deleted from host {#}.	VXLAN vmknic가 없거나 호스트에서 삭제되었습니다. 호스트를 들어오거나 나가는 트래픽이 영향을 받습니다. 작업: **설치(Installation) > 논리적 네트워크 준비(Logical Network Preparation) > VXLAN 전송(VXLAN Transport)** 탭에서 **해결(Resolve)** 링크를 클릭하여 이 문제를 해결하십시오.
1939	위험	아니요	VXLAN vmknic {#} [PortGroup = {#}] may have been deleted from the host {#} or the host-vCenter connection may have issues.	NSX Manager에서 VXLAN vmknic가 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 vmknic를 감지할 수 없게 되어 이 이벤트에 플래그가 지정됩니다. vCenter Server 및 호스트가 재부팅을 끝내면 NSX Manager는 VXLAN vmknic를 다시 확인하고 모든 것이 정상 상태가 되면 이 이벤트를 지웁니다. 작업: 이 문제가 지속되는 경우 **설치(Installation) > 논리적 네트워크 준비(Logical Network Preparation) > VXLAN 전송(VXLAN Transport)** 탭에서 **해결(Resolve)** 링크를 클릭하여 이 문제를 해결하십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
1941	위험	아니요	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(Installation)**로 이동한 후 호스트 연결 상태를 확인하십시오.
1942	위험	아니요	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(Installation) > 논리적 네트워크 준비(Logical Network Preparation) > VXLAN 전송(VXLAN Transport)** 탭에서 **해결(Resolve)** 링크를 클릭하거나 REST API(POST https://<vsm-ip>/api/2.0/vdn/virtualwires/<vw-id>/backing?action=remediate)를 사용하여 포트 그룹을 다시 생성하십시오.
1945	위험	아니요	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.
1947	위험	아니요	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 작업에 영향을 줄 수 있습니다. 작업: **설치(Installation) > 관리(Management)** 탭에서 컨트롤러에 대한 **해결(Resolve)** 버튼을 클릭하거나 API POST https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate를 호출하여 컨트롤러 VM의 전원을 켜십시오.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
1948	위험	아니요	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(Installation) > 관리(Management)** 탭에서 컨트롤러에 대한 **해결(Resolve)** 버튼을 클릭하거나 API POST https://<vsm-ip>/api/2.0/vdn/controller/{controllerId}?action=remediate를 호출하여 NSX Manager 데이터베이스에서 해당 컨트롤러의 상태를 제거하십시오.
1952	위험	아니요	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	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.

EAM 시스템 이벤트

이 표에서는 심각, 위험 또는 높음 심각도의 EAM(ESX Agent Manager)에 대한 시스템 이벤트 메시지를 설명합니다.

이벤트 코드	이벤트 심각도	경보가 트리거됨	이벤트 메시지	설명
270000	높음	예	EAM alarm received.	EAM(ESX Agent Manager)이 NSX VIB 또는 서비스 VM에서 NSX 설치 또는 업그레이드 문제를 감지했습니다. 작업: 경보를 해결하려면 **설치(Installation) > 호스트 준비(Host Preparation)** 탭에서 **해결(Resolve)** 링크를 클릭하거나 resolve API를 사용하십시오.

색인