

# vRealize Network Insight FAQ

VMware vRealize Network Insight 5.2

다음 VMware 웹 사이트에서 최신 기술 문서를 확인할 수 있습니다.

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

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://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](http://www.vmware.com/kr)

Copyright © 2020 VMware, Inc. All rights reserved. [저작권 및 상표 정보](#)

# 목차

<b>1</b>	<b>vRealize Network Insight FAQ 가이드 정보</b>	<b>4</b>
<b>2</b>	<b>일반</b>	<b>5</b>
<b>3</b>	<b>설치 및 구성</b>	<b>8</b>
<b>4</b>	<b>vRealize Network Insight에서 데이터 소스 추가 또는 구성</b>	<b>14</b>
<b>5</b>	<b>미세 세분화 및 흐름</b>	<b>17</b>
<b>6</b>	<b>클러스터링</b>	<b>19</b>
	클러스터링 - 일반	19
	클러스터링 - 설치 및 구성	21
	클러스터링 - 확장	22
	클러스터링 - 배포	23
<b>7</b>	<b>데이터 관리 및 처리</b>	<b>26</b>
<b>8</b>	<b>IPFIX</b>	<b>28</b>

# vRealize Network Insight FAQ 가이드 정보

# 1

vRealize Network Insight FAQ 가이드는 vRealize Network Insight에 관련한 질문과 대답을 사용자에게 제공합니다.

## 대상 사용자

이 정보는 vRealize Network Insight를 사용하는 사용자를 대상으로 합니다.

## 지원 번들을 생성하려면 어떻게 합니까?

"vRealize Network Insight 명령줄 참조 가이드" 에서 지원 번들 섹션을 참조하십시오.

## XML API 액세스를 위해 Palo Alto Networks Panorama에서 읽기 전용 관리자 역할을 생성하는 방법은 무엇입니까?

XML API 액세스를 위해 **관리자** 역할을 추가하려면 다음과 같이 하십시오.

- 1 **Panorama** → **관리자 역할**을 선택합니다.
- 2 **추가**를 클릭하여 새 관리자 역할을 추가하고 [관리자 역할 프로파일] 대화 상자를 엽니다.
- 3 [관리자 역할 프로파일] 대화 상자에서,
  - a 역할에 이름을 지정합니다(예: api-only-admin).
  - b 역할을 **Panorama**로 선택합니다.
  - c [웹 UI] 탭에 있는 모든 항목을 사용하지 않도록 설정합니다.
  - d [XML API] 탭에서 **커밋**을 제외한 모든 항목을 사용하도록 설정합니다.
  - e **확인**을 클릭하여 대화 상자를 닫으면 **관리자 역할**이 해당 이름과 함께 목록에 나타납니다.
  - f **커밋**을 클릭하여 변경 내용을 Panorama에 커밋합니다.
- 4 이 **관리자** 역할을 관리 계정에 할당합니다.

## 서비스는 언제 공유된 것으로 간주됩니까?

다음 포트는 공유로 구성되었습니다.

프로토콜	포트
DNS	53
Bootpc	68
Kerberos	110

프로토콜	포트
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269

## 데이터 소스에서 "인증서 또는 키 같은 데이터 소스 ID 정보가 변경되었습니다."라는 이벤트/오류가 수신되었습니다. 이것은 어떤 의미입니까?

vRealize Network Insight가 데이터 소스로부터 제품에 저장된 것과 동일하지 않은 새 인증서를 받았습니 다. vRealize Network Insight는 데이터 소스가 제공한 인증서를 자동으로 수락합니다. 이 과정 중에 이전 인증서 및 새 인증서를 다운로드할 수 있는 데이터 소스에서 이벤트가 수신됩니다.

## vRealize Network Insight에서 DNS 레코드 가져오기 제한은 어떻게 됩니까?

DNS 레코드 가져오기 제한은 다음과 같습니다.

- Infobox DNS 데이터 소스: 단일 데이터 소스에서 90만 개의 레코드를 가져올 수 있습니다.

- 수동 DNS 레코드 가져오기: zip 파일로 패키징된 여러 개의 .csv 또는 Bind 파일을 사용하여 DNS 레코드를 가져올 수 있습니다. 가져올 수 있는 레코드의 수에는 제한이 없지만 다음과 같은 업로드 제한이 있습니다.
  - 단일 zip 파일에 포함된 파일 수 - 25
  - 단일 zip 파일의 최대 크기 - 10MB.

## vRealize Network Insight의 리소스 요구 사항은 무엇입니까?

리소스 요구 사항은 vRealize Network Insight 설치 가이드를 참조하십시오.

## vRealize Network Insight 프록시 OVA 배포 중 잘못된 키를 입력하면 어떻게 됩니까?

비밀 키는 vRealize Network Insight 프록시 OVA 배포 중 검증되지 않습니다. 잘못된 비밀 키를 사용하는 경우에도 배포는 완료됩니다. 그러나 쌍 구성이 실패하고 vRealize Network Insight 프록시가 vRealize Network Insight UI에서 감지된 것으로 표시되지 않습니다.

공유 암호를 수정하려면 vRealize Network Insight 프록시 CLI에 로그인하고 `set-proxy-shared-secret` 명령을 실행하여 올바른 비밀 키를 설정합니다. 이 명령은 이전 키를 새 키로 대체하므로 vRealize Network Insight 플랫폼에서 vRealize Network Insight 프록시를 감지하고 쌍을 구성할 수 있습니다.

## vRealize Network Insight 프록시 OVA를 배포한 후 DNS를 구성하려면 어떻게 합니까?

vRealize Network Insight 프록시 CLI에 로그인하고 `change-network-settings` 명령을 실행합니다. 이 대화형 명령은 사용자가 DNS를 추가 또는 수정한 후 새 DNS로 vRealize Network Insight 프록시를 재구성할 수 있는 옵션을 제공합니다.

특정 네트워크 매개 변수가 올바르게 구성되지 않은 경우 `change-network-settings` 명령을 사용하여 네트워크 구성 매개 변수를 수정합니다.

## UI에서 vRealize Network Insight 프록시 VM IP를 찾으려면 어떻게 합니까?

[설정] 페이지로 이동하여 vRealize Network Insight 인프라 메뉴 옵션을 선택합니다. vRealize Network Insight 플랫폼과 vRealize Network Insight 프록시 VM 모두의 IP 주소가 표시됩니다.



## vRealize Network Insight 프록시 OVA를 배포하고 5분이 지났는데도 vRealize Network Insight 프록시가 감지되지 않으면 어떻게 해야 할까요?

consoleuser(vRealize Network Insight 명령줄 인터페이스 가이드 참조)를 사용하여 vRealize Network Insight 프록시에 로그인하고 다음을 확인합니다.

- CLI `show-connectivity-status`를 사용하여 vRealize Network Insight 프록시와 vRealize Network Insight 플랫폼의 쌍 구성 상태를 확인합니다.
- 쌍 구성 상태가 `Passed`로 표시되면 새 웹 브라우저 창에서 플랫폼 UI를 열고 로그인하여 상태를 확인합니다.
- 쌍 구성 상태가 `Failed`로 표시된다면 vRealize Network Insight 프록시 OVA 배포 중에 지정한 공유 비밀 키가 잘못되었을 수 있습니다. 이 문제를 해결하려면 `set-proxy-shared-secret` 명령을 사용하여 올바른 비밀 키를 설정합니다. 이 명령은 이전 키를 새 키로 대체하므로 vRealize Network Insight 플랫폼에서 vRealize Network Insight 프록시를 감지할 수 있습니다.
- `show-connectivity-status`에서 vRealize Network Insight 플랫폼에 대한 네트워크 연결이 **실패함**으로 표시되면 ping 명령을 사용하여 vRealize Network Insight 프록시 VM에서 vRealize Network Insight 플랫폼에 연결할 수 있는지 확인합니다.
- 연결할 수 없다면 `show-config` 명령을 사용하여 NTP, DNS, 게이트웨이 및 기타 네트워크 매개 변수가 올바르게 구성되었는지 확인합니다.
- 특정 네트워크 매개 변수가 올바르게 구성되지 않은 경우 `setup` 명령을 사용하여 네트워크 구성 매개 변수를 수정할 수 있습니다.

## 내 로그인 자격 증명이 기억나지 않으면 어떻게 해야 할까요?

UI 로컬 사용자인 경우: vRealize Network Insight UI 관리자에게 연락하여 자격 증명 재설정을 요청합니다.

관리자인 경우: vRealize Network Insight 3.4부터는 CLI `modify-password`를 사용하여 UI 자격 증명을 변경할 수 있습니다. 자세한 내용은 CLI 가이드를 참조하십시오. 버전 3.4 이전의 vRealize Network Insight를 사용 중이라면 지원 부서에 문의하십시오.

## 로그인 암호를 변경하려면 어떻게 할까요?

로그인 암호를 변경하려면 다음과 같이 하십시오.

- 1 **관리자 > 설정**으로 이동한 다음 왼쪽 창에서 **내 프로필**을 클릭합니다.
- 2 **암호 변경** 페이지에서 필요한 정보를 입력하고 **저장**을 클릭합니다.

## vRealize Network Insight 프록시 VM이 감지되기 전에 로그인 화면이 표시되면 어떻게 해야 하나요?

- 프록시가 감지되기 전에 브라우저를 새로 고치거나 새 창에 URL이 열리는 경우 이러한 동작이 예상됩니다.
- admin@local 사용자 이름에 대한 라이선스 활성화 중에 설정한 자격 증명을 사용하여 로그인합니다.

## vRealize Network Insight에서 여러 vCenter Server/NSX Manager를 지원하나요?

예, vRealize Network Insight는 여러 vCenter Server 및 NSX Manager를 지원합니다.

## vRealize Network Insight 서비스 중 인터넷 액세스가 필요한 서비스는 어떤 것이고 그 이유는 무엇입니까?

vRealize Network Insight는 인터넷 액세스가 필요한 원격 홈 호출 기능을 지원합니다. vRealize Network Insight 팀은 이 기능 또는 서비스를 통해 고객 환경을 더 잘 이해하고 문제점을 사전 예방적으로 해결하거나 교정할 수 있습니다. 다음 서비스에는 인터넷 액세스가 필요합니다.

- 자동 업데이트 서비스(svc.ni.vmware.com:443): 새로 릴리스된 비트 패키지를 사용할 수 있게 되면 vRealize Network Insight는 이 서비스를 사용하여 원격 업그레이드 호스트에 연결하여 가져옵니다. 업데이트를 사용할 수 있게 되면 사용자에게 UI 알림이 표시됩니다. 이 서비스는 기본적으로 사용되도록 설정되지만 UI를 통해 또는 CLI에서 online-upgrade 명령을 사용하여 이 서비스를 사용하지 않도록 설정할 수 있습니다.
- 성능 원격 분석 서비스(svc.ni.vmware.com:443): vRealize Network Insight의 주요 서비스 및 성능과 관련된 특정 메트릭이 주기적으로 수집되어 vRealize Network Insight에 업로드됩니다. 지원 팀은 이러한 메트릭을 모니터링하고 환경의 이상 징후를 식별하여 중요한 서비스에 영향을 주기 전에 조치를 취할 수 있습니다. 이 서비스는 기본적으로 사용되지 않도록 설정되지만 CLI에서 telemetry 명령을 사용하여 이 서비스를 사용하거나 사용하지 않도록 설정할 수 있습니다. 자세한 정보는 <https://kb.vmware.com/s/article/59242>에서 확인할 수 있습니다.
- 지원 서비스(support2.ni.vmware.com:443): 이 서비스는 vRealize Network Insight 지원 호스트에 대한 원격 보안 터널을 설정하여 권한 있는 직원이 원격으로 배포에 액세스하고 작업할 수 있도록 합니다. 이 서비스는 기본적으로 사용하지 않도록 설정되어 있으며, UI 및 "support-tunnel" CLI를 통해 사용 또는 사용하지 않도록 설정할 수 있습니다.

- 등록 서비스(reg.ni.vmware.com:443): 모든 외부 서비스에 장치를 등록하기 위한 서비스입니다. 이 서비스는 위에 언급된 서비스 간에 신뢰할 수 있는 통신을 설정합니다. 설치 프로그램이 인터넷에 액세스하면 자동으로 등록이 이루어집니다. 분리된 환경에서는 "offline-registration" CLI(자세한 내용은 CLI 가이드 참조)를 사용하여 작업을 수행할 수 있습니다. 이것은 지원 터널을 사용하도록 설정하는 데 필요합니다.

**참고** vRealize Network Insight 플랫폼이 인터넷 프록시 뒤에 있는 경우에는 다음 도메인 이름 및 포트를 화이트리스트에 추가하십시오.

표 3-1.

서비스	URL	포트
업그레이드 서비스/메트릭 서비스	svc.ni.vmware.com	443
지원 터널 서비스	support2.ni.vmware.com	443
등록 서비스	reg.ni.vmware.com	443

## 장치에서 인터넷 액세스를 사용하지 않도록 설정하는 방법

다음 서비스는 보안 원격/인터넷 서비스를 사용합니다.

- 자동 업데이트 서비스
- 성능 원격 분석 서비스
- 지원 서비스
- 등록 서비스

이러한 서비스를 사용하거나 사용하지 않도록 설정하는 방법에 대한 자세한 내용은 [vRealize Network Insight 서비스 중 인터넷 액세스가 필요한 서비스는 어떤 것이고 그 이유는 무엇입니까? FAQ](#)를 참조하십시오. 이러한 서비스 중 하나를 사용하도록 설정한 경우 vRealize Network Insight에 인터넷 액세스가 필요합니다.

## 포트 집계란 무엇이고 이를 수행하기 위한 메커니즘은 어떻게 됩니까?

포트 집계는 동적 FTP, Oracle, MS-RPC 등과 같은 사용 후 삭제 포트 흐름을 집계하기 위해 내장되어 있습니다. 이는 시스템의 흐름 수를 줄이는 데 도움이 되며, 동일한 서비스를 위해 필수적인 다수의 흐름에 대한 집계된 보기를 제공합니다.

이를 수행하기 위한 메커니즘은 다음과 같습니다.

- destination\_ip를 관찰하는 첫 3일 동안 해당 특정 IP의 대상 포트를 10K 버킷에 집계하고 이 IP에 대한 포트-프로파일 구축을 시작합니다(대상 IP당 하나의 포트-프로파일 구축).

- 3일이 지나 프로파일을 구축한 후에는 포트 밀도가 높은(사용 후 삭제 포트 열기 패턴을 반영하는) 포트 범위 집계를 시작합니다. 범위 자체의 크기는 동적이며(예: 100, 1000, 10000), 얼마나 많은 포트가 열려 있고 지정된 집계 범위에서 얼마나 광범위한지를 기준으로 생성됩니다.

---

**참고** 이러한 결정은 각 서버 IP 주소에 독립적으로 이루어집니다.

---

- 이를 통해 대량 포트 열기 활동이 없는 곳에서 집계 없이 높은 포트 흐름을 보고할 수 있고 그러한 활동이 발생하는 곳에서 동적 집계를 적용할 수 있습니다.
- 프로파일은 시간 경과에 따라 소멸하는 방식으로 지속적으로 업데이트되어 새로운 포트가 열리고 이전 포트는 더 이상 사용되지 않음을 설명합니다.

## vRealize Network Insight OVA를 배포한 후 IP 주소, 게이트웨이 또는 넷마스크를 변경하려면 어떻게 합니까?

vRealize Network Insight 플랫폼/프록시 네트워크 설정을 변경하려면 CLI에 로그인하고 `change-network-settings` 명령을 실행합니다. 이 대화형 명령은 사용자가 IP 주소, 게이트웨이, 넷마스크 등을 수정한 후 새로운 세부 정보를 사용하여 vRealize Network Insight 장치를 재구성할 수 있는 옵션을 제공합니다.

---

### 참고

- 장치는 결국 재부팅되므로 이 작업은 VM 콘솔 세션을 사용하여 수행해야 합니다.
- vRNI 플랫폼 IP가 수정되고 프록시와 쌍으로 구성된 경우에는 각 프록시 VM에서 다음 CLI 명령을 실행합니다.

```
vrni-proxy set-platform --ip-or-fqdn <New_Platform_IP>
```

---

## 평가판 라이선스에서 영구 라이선스로 변경하려면 어떻게 합니까?

vRealize Network Insight 사용자 가이드에서 "라이선스 추가 및 변경" 섹션을 참조하십시오.

## vRealize Network Insight에서 라이선스의 특징은 어떻게 됩니까?

표 3-2.

라이선스 이름	라이선스 유형	기능
엔터프라이즈	전체/운영: 영구적이거나 시간 제한적일 수 있습니다.	다음과 같은 기능이 설정되어 있습니다. <ul style="list-style-type: none"> <li>■ 데이터 제공자로서의 AWS</li> <li>■ 조정 가능한 데이터 보존 정책</li> <li>■ Infoblox DNS 데이터 소스</li> <li>■ 물리적 IP 및 DNS 매핑</li> <li>■ 분석</li> </ul>
고급	전체/운영: 영구적이거나 시간 제한적일 수 있습니다.	해당 없음

**참고** 모든 라이선스는 CPU 소켓 및 CCU(동시 사용자) 기준으로 용량이 부여됩니다. 평가판 라이선스는 업데이트된 키를 사용하여(UI -> 설정 -> 정보) 갱신하거나 운영으로 변환할 수 있습니다. 자세한 내용은 사용자 가이드를 참조하십시오.

## vRealize Network Insight에서 VM을 백업하려면 어떻게 합니까?

VMware VADP/VDP API와 같은 VM의 백업을 수행하려면 "VMware 모범 사례"를 참조하십시오. 클러스터를 생성 또는 확장하기 전에 백업을 수행하는 것이 좋습니다.

# vRealize Network Insight에서 데이터 소스 추가 또는 구성

## 4

### IP 주소를 사용하여 vCenter Server를 추가하는 동안 "요청 시간 초과" 메시지가 표시되면 어떻게 합니까?

- vRealize Network Insight 프록시 VM에서 vCenter Server IP 주소에 연결할 수 있는지 확인합니다.
- vRealize Network Insight 프록시 CLI에 로그인한 후 ping을 사용하여 IP에 연결할 수 있고 Telnet을 사용하여 포트 443에서 vCenter Server에 연결할 수 있는지 확인합니다.
- vCenter Server에 연결할 수 있는 경우 추가를 다시 시도합니다.
- IP 주소에 연결할 수 없는 경우에는 show-config 명령을 사용하여 vRealize Network Insight 프록시 VM에서 게이트웨이가 올바르게 구성되어 있는지 확인합니다.
- 게이트웨이가 잘못되었다면 setup 명령을 사용하여 게이트웨이를 수정합니다.

### vCenter Server를 추가하는 동안 "IP/FQDN이 잘못됨" 메시지가 표시되면 어떻게 합니까?

- vCenter Server에 대해 제공된 IP/FQDN이 올바른지 확인합니다.
- ping 명령을 사용하여 vRealize Network Insight 프록시 VM에서 FQDN에 연결할 수 있는지 확인합니다.
- 연결할 수 없다면 nslookup FQDN 및 show-config 명령을 사용하여 vRealize Network Insight 프록시 VM에서 DNS가 올바르게 구성되어 있는지 확인합니다.
- DNS가 잘못되었다면 setup 명령을 사용하여 DNS를 수정합니다.

### vRealize Network Insight 보안 및 작업 플랫폼에 필요한 권한은 무엇입니까?

vRealize Network Insight에는 다음 권한을 가진 VMware vCenter Server 자격 증명이 필요합니다.

- Distributed Switch: 수정
- dvPort 그룹: 수정

## vCenter Server 데이터 소스 페이지에서 IPFIX를 사용하도록 설정하는 동안 "사용자에게 필요한 권한이 없습니다." 메시지가 표시되면 어떻게 합니까?

IPFIX를 사용하도록 설정 하려면 vRealize Network Insight에 다음 권한을 가진 VMware vCenter Server 자격 증명이 필요합니다.

- Distributed Switch: 수정
- dvPort 그룹: 수정

제공된 VMware vCenter Server 사용자에게 vCenter Server의 루트 폴더 및 그 하위 엔티티(예: 모든 폴더 및 모든 데이터 센터)에 대한 권한이 있는지 확인합니다.

## 환경에서 데이터를 가져오는 빈도는 어떻게 됩니까?

vRealize Network Insight 프록시는 10분 간격으로 환경에서 데이터를 가져옵니다.

## vCenter Server를 추가한 후 데이터 분석은 언제 시작됩니까?

데이터 분석은 vCenter Server를 추가한 직후 시작됩니다. 제품 UI는 몇 분 내에 데이터의 일부 그림을 표시하며 완료하는 데 2시간이 걸릴 수 있습니다.

---

**참고** 흐름 트래픽 데이터는 지속적으로 변경되며 그 분석에는 최소 24시간의 데이터가 포함됩니다.

---

## vRealize Network Insight OVA를 삭제한 경우 vCenter Server에서 IPFIX 설정을 정리하려면 어떻게 합니까?

- VMware vSphere Web Client 사용: **홈 > 네트워킹 > VDS(이름) > NetFlow 설정**으로 이동합니다. [수집기 설정]에서 vRealize Network Insight 프록시 IP를 제거합니다.
- VMware vSphere Windows Client 사용: **홈 > 인벤토리 > 네트워킹 > VDS(이름) > 설정 편집**으로 이동합니다. [NetFlow] 탭의 [수집기 설정]에서 vRealize Network Insight 프록시 IP를 제거합니다. 이 단계는 IPFIX가 사용되도록 설정된 각 VDS에 대해 수행해야 합니다.

## vRealize Network Insight에서 IPFIX 구성을 정리하려면 어떻게 합니까?

vRealize Network Insight UI에서 **설정 > 데이터 소스**로 이동하고 vCenter Server를 삭제합니다. 이렇게 하면 vRealize Network Insight에서 수행한 IPFIX 구성이 제거됩니다.

## **vRealize Network Insight에서 VMware NSX Manager를 추가한 후 VM-VM 경로에서 올바른 방화벽 규칙을 표시하는 데 걸리는 시간은 얼마나 됩니까?**

vRealize Network Insight에서 VMware NSX Manager를 추가한 후 방화벽 규칙 관계에 대해 VM을 계산하는 데 최대 24시간이 걸릴 수 있습니다.

## **vRealize Network Insight에서 VMware vCenter를 추가한 후에 VM-VM 경로에서 PNIC를 볼 수 없는 이유는 무엇입니까?**

일반적으로, vRealize Network Insight에서 데이터 소스로 VMware vCenter를 추가한 후 vRealize Network Insight가 VM-VM 경로를 계산하는 데에는 약 2시간이 걸립니다. 드문 경우이긴 하지만 vRealize Network Insight에서 VMware vCenter를 추가한 후 VM-VM 경로에서 PNIC를 올바르게 표시하는 데 약 8-10시간이 걸릴 수도 있습니다.



## 트래픽 배포 핀의 숫자는 무엇을 나타냅니까?

백분율은 흐름 분석에 기반한 트래픽 배포의 개요를 제공합니다.

표 5-1.

트래픽	설명
EW(East-West)	그룹 전체 트래픽의 백분율로 표시된 East-West 트래픽
전환됨(EW 비율)	East-West 트래픽의 백분율로 표시된 전환된 트래픽
라우팅됨(EW 비율)	East-West 트래픽의 백분율(%)로 표시된 라우팅된 트래픽
호스트 내부(VM-VM의 비율)	가상 시스템 간 트래픽의 백분율로 표시된 동일한 호스트에 소스 및 대상이 있는 트래픽
VM - VM(EW 비율)	East-West 트래픽의 백분율로 표시된 가상 시스템 간 트래픽
인터넷	그룹 전체 트래픽의 백분율로 표시된 인터넷 트래픽

## 포트는 흐름에서 어떻게 집계됩니다?

포트 집계는 동적 FTP, Oracle, MS-RPC 등과 같은 사용 후 삭제 포트 흐름을 집계하기 위해 내장되어 있습니다. 이는 시스템의 흐름 수를 줄이는 데 도움이 되며, 동일한 서비스를 위해 필수적인 다수의 흐름에 대한 집계된 보기를 제공합니다. 이를 수행하기 위한 메커니즘은 다음과 같습니다.

- destination\_ip를 관찰하는 첫 3일 동안 해당 IP의 대상 포트를 10K 버킷에 집계하고 이 IP에 대한 포트-프로파일 구축을 시작합니다.
- 3일이 지나 신뢰할 수 있는 프로파일을 구축한 후에는 포트 밀도가 높은(다른 말로, 사용 후 삭제 포트 열기 패턴을 반영하는) 포트 범위 집계를 시작합니다. 범위 자체는 100, 1000, 10000 크기로 동적이며, 얼마나 많은 포트가 열려 있고 지정된 집계 범위에서 얼마나 광범위한지를 기준으로 생성됩니다.
- 이를 통해 대량 포트 열기 활동이 없는 곳에서 집계 없이 높은 포트 흐름을 보고할 수 있고 그러한 활동이 발생하는 곳에서 동적 집계를 적용할 수 있습니다.
- 프로파일은 시간 경과에 따라 소멸하는 방식으로 지속적으로 업데이트되어 새로운 포트가 열리고 이전 포트는 더 이상 사용되지 않음을 설명합니다.

## vRealize Network Insight에서 240.240.240.240 IP 주소는 무엇을 나타냅니까?

240.240.240.240은 vRealize Network Insight에서 자리 표시자 IP 주소입니다. 이 IP 주소는 특정 IP를 히팅하는 다수의 IP 주소(> 5000)가 있는 경우에 사용됩니다. 이 자리 표시자 IP 240.240.240.240을 포함하는, 추가로 수신되는 모든 인터넷 IP(5001번째부터)는 해당 서비스 끝점에 대해 대체가 가능합니다.

이것은 각 인터넷 클라이언트를 개별적으로 기록하는 공개 노출 서비스가 매우 많은 수의 흐름을 발생시켜 시스템 로드가 증가할 수 있으므로 시스템에서 흐름 수를 제한하기 위한 것입니다.

이 자리 표시자 IP로 대체된 모든 흐름의 경우, 모든 메트릭이 이 IP 주소를 포함하는 해당 흐름에서 집계되므로 집계 수준에서 통계가 손실되지 않습니다.

240.240.240.240에서 시작된 것으로 표시되어 흐름 보기에 보고된 흐름에 대한 모든 대상 IP는 실제로 다수의 인터넷 IP(>5000)에서 히팅한 것입니다.

# 클러스터링

# 6

본 장은 다음 항목을 포함합니다.

- 클러스터링 - 일반
- 클러스터링 - 설치 및 구성
- 클러스터링 - 확장
- 클러스터링 - 배포

## 클러스터링 - 일반

### 프록시 또는 수집기 VM을 클러스터링할 수 있습니까?

아니요. 수집기/프록시 VM에 대한 클러스터링은 지원되지 않습니다.

### vRealize Network Insight에 vRealize Log Insight와 같은 로드 밸런서가 필요합니까?

vRealize Network Insight 클러스터링은 HA 솔루션이 아닌 확장 솔루션입니다. 기본 플랫폼 VM/마스터 노드에서 장애가 발생하면 전체 서비스를 사용할 수 없게 됩니다.

### 원격 프록시와 플랫폼 간 연결이 다운되면 어떻게 됩니까?

플랫폼과 프록시 VM 간 연결이 다운되면 프록시 VM이 데이터를 로컬로 저장하고(디스크 공간에 따라 다름) 다시 연결되면 해당 데이터를 전송합니다.

### vRealize Log Insight가 vRealize Network Insight와 통합되었습니까?

예, vRealize Log Insight는 vRealize Network Insight 3.4와 통합되었습니다. 경고는 vRealize Log Insight일 수 있는 Syslog로 전송됩니다.

### 노드가 재부팅되면 어떻게 됩니까?

노드가 재부팅되면 자동으로 클러스터에 가입하고 계속 작동합니다. 이 노드가 기본 노드인 경우 서비스는 다운된 시간 동안 완전하게 손실됩니다.

## 클러스터에서 플랫폼 노드 또는 수집기의 IP는 어떻게 변경합니까?

클러스터에서 CLI 명령을 사용하여 원하는 수집기 또는 플랫폼 노드의 IP를 변경할 수 있습니다.

### 참고

- 이 작업을 수행하기 전에 VMware 지원에 문의하십시오.
  - 프로세스가 완료되면 장치가 재부팅됩니다. 따라서 VM 콘솔에서 다음 단계를 수행해야 합니다.
- 
- 수집기 IP를 변경하려면 `change-network-settings` 명령을 실행합니다.
  - 플랫폼 IP를 변경하려면 다음을 수행합니다.
    - a `change-network-settings` 명령을 실행합니다.
    - b 다른 모든 플랫폼에서 `update-IP-change` 명령을 실행하여 새 IP를 반영합니다.
    - c 수집기에서 `show-connectivity-status` 명령을 실행하고 **Platform VM IP/URL**을 검색하여 이 플랫폼과 연결되어 있는지 확인합니다.
    - d `vrni-proxy`를 실행하여 새 플랫폼 IP를 연결된 수집기에 반영합니다.

사용 사례 1: 3노드 클러스터에서 플랫폼2 IP만 변경되었습니다. 이 플랫폼에 연결된 수집기가 없습니다.

- 1 플랫폼2에서 `change-network-settings`를 실행합니다.
- 2 플랫폼1과 플랫폼3에서 `update-IP-change`를 실행하여 플랫폼2의 새 IP를 반영합니다.

사용 사례 2: 3노드 클러스터에서 플랫폼1 및 플랫폼2 IP가 변경되었습니다. 수집기A는 플랫폼2에 연결되어 있고 나머지는 플랫폼3에 연결되어 있습니다.

- 1 플랫폼1에서 `change-network-settings`를 실행합니다.
- 2 플랫폼2에서 `change-network-settings`를 실행합니다.
- 3 플랫폼2 및 플랫폼3에서 `update-IP-change platform1-oldIP platform1-newIP`를 실행합니다.
- 4 플랫폼1 및 플랫폼3에서 `update-IP-change platform2-oldIP platform2-newIP`를 실행합니다.
- 5 수집기A에서 `vrni-proxy set-platform --ip-or-fqdn platform2-newIP`를 실행합니다.

## 플랫폼1에 얼마나 많은 디스크 공간이 필요합니까?

플랫폼1에만 저장되는 일부 구성 데이터가 있기 때문에 플랫폼1은 클러스터의 다른 노드에 비해 더 많은 디스크 공간이 필요합니다.

## 특정 노드에 디스크 공간 부족이 발생하면 어떻게 됩니까?

특정 플랫폼 노드의 디스크 공간이 정해진 임계값에 도달하면 UI에서 오류 메시지를 표시하기 시작합니다. vCenter에 로그인하여 플랫폼 노드에 디스크 공간을 추가해야 합니다.

## 데이터는 클러스터에서 몇 번 복제됩니까?

데이터 복제 메커니즘은 플랫폼 노드에 있는 구성 요소에 따라 다릅니다.

## 클러스터링 - 설치 및 구성

### 모든 플랫폼 VM이 동일한 L2/L3 세그먼트에 있어야 합니까?

아니요. 하지만 모든 플랫폼 노드를 노드 간 지연 시간이 짧은 공통 네트워크에 유지하는 것이 좋습니다. 이것은 많은 분산된 구성 요소가 노드 간에 데이터를 복제하고 지연 시간이 길면 시스템 성능 및 안정성 문제가 발생할 수 있기 때문입니다.

### 제품 내 업그레이드 기능을 사용하여 클러스터를 업그레이드할 수 있습니까?

릴리스 3.7까지는 클러스터에 대한 온라인 업그레이드가 지원되지 않습니다. 릴리스 3.8부터는 온라인 업그레이드를 통해 클러스터를 업그레이드할 수 있습니다.

### 클러스터 생성 프로세스 중 장애가 발생하면 어떻게 합니까?

클러스터 생성 프로세스를 시작하기 전에 기본 플랫폼 및 프록시의 스냅샷을 생성하는 것이 좋습니다. 장애가 발생하면 보조 플랫폼 노드를 삭제하고 스냅샷에서 기본 플랫폼 및 프록시 VM을 복구합니다.

### 단일 노드 배포를 클러스터로 확장할 때 기존 데이터 및 구성은 어떻게 됩니까?

모든 데이터 및 구성은 변경 없이 유지됩니다. 데이터는 클러스터 생성 후 액세스할 수 있습니다.

### 플랫폼 VM이 서로 다른 영역에 있어도 됩니까?

아니요. 플랫폼 노드는 동일한 사이트에 배치해야 합니다. 프록시 서버는 지리적으로 분산이 가능합니다.

### 플랫폼을 vSAN 확장 클러스터(2개의 데이터 센터)에서 호스팅할 수 있습니까?

예, 동일한 데이터 센터 내 또는 데이터 센터 간의 vSAN 클러스터는 여전히 로컬 스토리지와 같은 특정 IO 성능을 보장합니다.

### 서로 다른 vSAN 클러스터에서 클러스터 노드를 호스팅할 수 있습니까?

예, 상이한 기본 데이터스토어에서 서로 다른 플랫폼 클러스터 노드를 호스팅할 수 있습니다.

### 백업 플랫폼 노드가 필요합니까?

예, 백업은 VMware 권장 스냅샷/백업 기술을 사용하여 생성해야 합니다.

### 특정 영역의 클러스터 프록시 VM 및 다른 영역의 플랫폼 VM 클러스터 간의 대역폭을 추정하는 방법은 무엇입니까?

일부 대규모 배포에서 이러한 대역폭의 범위는 1mbps에서 20mbps 사이입니다. 데이터가 플랫폼 VM으로 전송되기 전 프록시 VM에서 많은 중복 제거와 압축이 발생합니다.

## 클러스터 노드 간 네트워크 트래픽은 얼마나 됩니까?

트래픽은 보통 클러스터의 크기 및 데이터 센터 환경 유형에 따라 다릅니다.

3-5만 개의 VM이 있는 설치의 경우:

- 클러스터 간: 약 50-400Mbps
- 프록시 및 플랫폼 간: 약 100Kbps-15Mbps

## 클러스터의 노드 간에 허용되는 최대 지연 시간은 얼마나 됩니까?

플랫폼 노드는 동일한 사이트에 배치해야 합니다. 그러한 경우 지연 시간은 최소화됩니다. 플랫폼 노드가 vSAN 확장 클러스터(2개의 데이터 센터)에서 호스팅되는 경우 클러스터 내 또는 클러스터 간의 vSAN 클러스터는 로컬 스토리지와 같은 특정 IO 성능을 보장합니다. 데이터 센터에서 실행되는 vRealize Network Insight와 같은 애플리케이션은 정상적으로 작동합니다. 상이한 기본 데이터스토어에서 서로 다른 플랫폼 클러스터 노드를 호스팅할 수 있습니다. 하지만 클러스터의 모든 플랫폼 VM이 동일한 사이트에 배치되어 있는지 확인해야 합니다.

## 특정 영역의 프록시 VM 및 다른 영역의 플랫폼 VM 클러스터 간에 허용되는 최대 지연 시간은 얼마나 됩니까?

사용자 설정에 지리적으로 분산된 프록시를 둘 수 있습니다. 프록시 VM에서 플랫폼 VM으로의 HTTPS 연결이 있으므로 필요에 따라 몇 초 동안 긴 지연 시간이 허용됩니다. vRealize Network Insight는 클러스터 하나에서 최대 10개의 노드를 지원합니다(흐름이 있는 3만 개의 VM 또는 흐름이 없는 5만 개의 VM).

## 프록시/플랫폼 VM의 크기는 어떻게 됩니까?

대형 브릭 구성 사용: 설치 가이드를 참조하십시오.

## 클러스터링 - 확장

### 이미 생성된 클러스터를 확장할 수 있습니까?

예, 클러스터 확장은 10개 노드까지 지원됩니다.

### 기본이 아닌 플랫폼 VM을 사용할 수 없게 되면 어떻게 됩니까?

내부 서비스는 기본이 아닌 노드 장애에 대해서는 복원력이 제한적입니다. 일반적으로 노드 장애가 발생하면 NI의 계산 성능이 손실됩니다.

### 어떤 종류의 로드 밸런싱이 지원됩니까?

프록시와 플랫폼의 매핑이 수정되었습니다. 프록시 VM의 데이터가 플랫폼 VM에 도달하면 그 처리가 모든 플랫폼 VM 간에 내부적으로 로드 밸런싱됩니다.

## 플랫폼 클러스터를 생성하면 대역폭 사용량이 증가합니까?

프록시 또는 수집기 VM은 계속 기본 또는 플랫폼 VM과만 통신합니다. 플랫폼 VM 클러스터링 통신을 위한 대역폭 요구 사항은 최소 수준입니다. 따라서 대역폭 사용량은 크게 증가하지 않습니다.

## 프록시 VM과 플랫폼 VM 간 데이터 전송 빈도는 어떻게 됩니까?

프록시 VM은 중복 제거된 데이터 또는 압축된 데이터를 지속적으로 플랫폼 VM에 전송합니다.

## 프록시 VM에서 데이터 최적화가 이루어집니까?

프록시 VM에서는 다양한 형식의 중복 제거, 압축, 감소 또는 일괄 처리 단계가 수행됩니다. 플랫폼 VM과 프록시 VM 간 연결이 다운되면 프록시 VM이 데이터를 로컬로 저장하고(디스크 공간에 따라 다름) 연결이 복원되면 해당 데이터를 전송합니다.

## 네트워크 대역폭에 대한 최적화가 이루어집니까?

예, 프록시 VM에서는 다양한 형식의 중복 제거/압축/감소/일괄 처리 단계가 수행됩니다.

## 프록시 서버에서 클러스터링이 가능합니까?

아니요, 프록시 서버에서 클러스터링은 가능하지 않습니다.

## vCenter는 프록시 서버에 어떤 방식으로 트래픽을 전송합니까?

vCenter는 프록시 서버에 트래픽을 전송하지 않습니다. 실제로 프록시 서버는 지정된 해당 vCenter에 연결하여 정보를 가져옵니다.

## 클러스터를 배포할 때 vCenter는 다양한 프록시 서버에 어떤 방식으로 트래픽을 전송합니까?

실제로 프록시는 vCenter에 연결하여 정보를 가져옵니다. 개별 프록시가 지정된 vCenter에 연결하여 정보를 가져옵니다. 프록시에서는 클러스터링을 사용할 수 없습니다.

## 클러스터링 - 배포

### 클러스터 확장 후 UI에 액세스하려면 어떻게 합니까?

UI 액세스는 플랫폼1에서의 액세스로만 제한됩니다.

### 플랫폼1은 무엇이고 이 노드를 기억해야 하는 이유는 무엇입니까?

클러스터 생성 프로세스가 시작되는 플랫폼 노드가 플랫폼1로 간주됩니다. UI는 클러스터에 있는 n개 노드 중 이 노드에서만 액세스해야 합니다.

## UI 액세스가 플랫폼1로 제한된다면 다른 노드에서는 데이터를 어떻게 검색합니까?

데이터 센터의 데이터는 클러스터의 모든 노드에 분산됩니다. UI 레이어가 플랫폼1에서 데이터를 요청할 때 플랫폼1 노드는 모든 노드에 저장된 데이터를 가져온 후 UI에 응답을 보냅니다.

## 클러스터 생성을 위해 다른 데이터 센터에 배포된 플랫폼 노드를 사용할 수 있습니까?

클러스터의 모든 노드는 서로 간에 데이터를 교환합니다. 따라서 지연 시간 관련 문제를 피하려면 동일한 데이터 센터에 배포된 플랫폼 노드를 사용하여 클러스터를 생성하는 것이 좋습니다.

## 플랫폼 노드를 확장하는 경우 기존 플랫폼의 데이터는 어떻게 됩니까?

기존 플랫폼 노드의 데이터는 보존되고 클러스터의 모든 노드에 분산됩니다.

## 필요한 플랫폼 브릭의 수를 결정하는 데 프록시 VM의 수가 문제가 됩니까?

아니요. 모든 vCenter의 총 VM 수와 흐름의 상태(사용 또는 사용 안 함)만 필요한 브릭의 수에 영향을 줍니다. "vRealize Network Insight 설치 가이드"에서 브릭 모델 테이블을 참조하십시오.

## vCenter의 수, 물리적 디바이스(예: 라우터)의 수 또는 기타 유형의 데이터 소스가 필요한 플랫폼 브릭의 수에 영향을 줍니까?

아니요. 모든 vCenter의 총 VM 수와 흐름의 상태(사용 또는 사용 안 함)만 필요한 브릭의 수에 영향을 줍니다. "vRealize Network Insight 설치 가이드"에서 브릭 모델 테이블을 참조하십시오.

## vRNI는 HA를 이유로 데이터 센터 2개에 분산된 플랫폼 클러스터를 지원하지합니까?

아니요. 플랫폼 클러스터는 데이터 센터의 분할을 지원하지 않습니다. 모든 플랫폼 클러스터 VM은 동일한 사이트에 있어야 합니다. 플랫폼 클러스터는 현재 HA를 지원하지 않습니다. 현재 로드맵 구상 중에 있습니다. 고객은 2개 사이트의 DR에 대해 HA용 SRM을 사용할 수 있습니다.

## vRNI는 포함된 VM의 수가 6000개가 넘고 흐름을 사용하는 단일 vCenter를 지원하지합니까?

릴리스 3.5까지, vRNI는 6000개가 넘는 VM이 있고 흐름을 사용하는 하나의 대형 vCenter로부터의 데이터 수집을 지원하지 않습니다. 현재 로드맵 구상 중에 있습니다.

## 플랫폼1에 얼마나 많은 디스크 공간이 필요합니까?

플랫폼1에만 저장되는 일부 구성 데이터가 있기 때문에 플랫폼1은 클러스터의 다른 노드에 비해 더 많은 디스크 공간이 필요합니다.



## 특정 노드에 디스크 공간 부족이 발생하면 어떻게 됩니까?

특정 플랫폼 노드의 디스크 공간이 정해진 임계값에 도달하면 UI에서 오류 메시지를 표시하기 시작합니다. vCenter에 로그인하여 플랫폼 노드에 디스크 공간을 추가해야 합니다.

## 데이터는 클러스터에서 몇 번 복제됩니까?

데이터 복제 메커니즘은 플랫폼 노드에 있는 구성 요소에 따라 다릅니다.

## 클러스터는 어떤 방식으로 작동합니까?

- 배포의 모든 프록시는 하나의 플랫폼(플랫폼1)에 연결됩니다. 플랫폼과 프록시 간 연결은 포트 443의 https를 통해 이루어집니다. 따라서 플랫폼1의 프록시에는 포트 443만 표시됩니다.
- 플랫폼1 노드는 프록시에서 요청을 받는 즉시 라운드 로빈 방식으로 클러스터의 다른 플랫폼 노드에 요청을 로드 밸런싱합니다.
- 플랫폼 노드는 데이터를 표준화하고 계산 엔진에서 처리할 수 있도록 메시징 대기열에 넣습니다.
- 계산 엔진은 데이터 복제 메커니즘을 사용하여 데이터를 클러스터의 모든 노드에 분산합니다. 이렇게 하면 클러스터에서 특정 노드(플랫폼1 제외)의 작동이 중지되더라도 데이터 손실이 발생하지 않습니다.
- 일부 구성 데이터는 복제되지 않은 플랫폼1 노드에 명시적으로 저장됩니다. 이것이 바로고가용성 솔루션이 지원되지 않는 이유입니다.

# 데이터 관리 및 처리

## 7

### 데이터 처리 파이프라인은 플랫폼-프록시 서버 통신이 중단되는 경우와 같은 경계 조건에서 어떻게 동작합니까?

- 기본 보존 기간은 어떻게 됩니까?

30일입니다. 엔터프라이즈 라이선스를 사용하여 UI에서 기간을 늘릴 수 있습니다. 참고: 기간을 늘릴 때 디스크 지침을 준수해야 합니다.

- 데이터는 프록시에서 어떻게 처리됩니까?

프록시의 모든 데이터는 흐름 데이터를 포함하여 플랫폼으로 보내지기 전에 SDM(Self Describing Message)으로 변환됩니다. 여기에는 모든 데이터 소스의 전체 구성, 인벤토리 및 메트릭 데이터가 포함됩니다. 플랫폼에 연결할 수 없거나 Kafka 대기열로의 SDM 업로드가 실패하면 프록시 VM의 디스크에 기록됩니다(/var/BLOB\_STORE 아래).

- 프록시에서 데이터 제거는 언제 시작됩니까?

흐름 데이터가 아닌 경우: SDM을 저장하도록 디스크에 10GB 공간이 할당되어 있습니다 (BLOB\_STORE). 이 저장소가 가득 차면 수집기가 이전 SDM을 삭제하기 시작하고 새 SDM을 디스크에 추가합니다. 이 제한이 얼마나 빨리 위반될지는 모든 데이터 소스에서 수집되는 데이터의 크기에 달려 있습니다.

흐름 데이터의 경우: 원시 흐름을 저장하도록 15GB 공간이 할당되어 있습니다(/var/flows/vds/nfcpd 아래). 이 공간이 다 사용되면 흐름 프로세서가 이전 흐름 파일을 삭제하기 시작합니다. 2M/분 이하의 원시 수신 흐름 속도에서 순환 발생 시작까지는 최대 10시간이 걸립니다.

- 제거 논리는 어떻게 됩니까?

가장 오래된 SDM이 가장 먼저 삭제됩니다.

- 프록시에서 새 데이터 처리는 언제 중단됩니까?

서비스가 정상적으로 실행된다면 중단되지 않습니다.

- 플랫폼과 프록시 간 연결이 끊겼고 제거 조건이 충족되지 않는다고 가정할 때 다시 연결되면 플랫폼에서 모든 데이터가 조정됩니까?

디스크에 저장된 모든 데이터는 플랫폼으로 전송됩니다. 데이터는 플랫폼에 데이터 손실 조건이 있는 경우를 제외하고 완전하게 조정됩니다(아래에서 자세한 내용 참조).

■ 플랫폼에서 데이터 손실이 발생할 수 있는 조건이란 무엇입니까?

플랫폼은 **Kafka** 대기열에 추가된 지 **6시간**이 넘은 **SDM**을 삭제하기 시작합니다(**3-노드 클러스터**의 경우 **18시간**). 다른 가능성은 대기열이 포화 상태가 되는 경우입니다. 시스템에 지연이 있고 수신 데이터 속도가 높은 경우에 이러한 문제가 발생할 수 있습니다.

■ 먼저 게시되는 **SDM**은 최신의 **SDM**입니까 아니면 가장 오래된 **SDM**입니까?

가장 오래된 **SDM**이 먼저 전송됩니다. 버전 **3.9**까지는 일부 데이터가 손실되는 알려진 문제가 있습니다. 자세한 내용은 **GSS**에 문의하십시오.

■ 통신 문제가 없는 경우 데이터가 프록시의 디스크에 저장된 다음 플랫폼으로 푸시됩니까?

통신 문제가 없다면 **SDM**은 디스크에 저장되지 않습니다. 메모리 자체에서 플랫폼으로 전송됩니다. 프록시가 **SDM** 전송에 문제가 있음을 수신한 경우에만 **SDM**이 디스크에 저장됩니다.

■ 문제가 발생했을 때 프록시는 어떤 것이 마지막으로 처리된 흐름 파일인지 어떻게 알 수 있습니까?

흐름 프로세서는 어떤 것이 마지막으로 처리된 **nfcapd** 파일인지에 대한 체크포인트를 **DB**에 유지합니다.

■ 문제 없이 처리할 수 있는 **SDM**의 최대 크기는 얼마나 됩니까? 사용자는 이 위반에 대해 어떻게 알 수 있습니까?

**SDM** 크기 제한은 **15MB**입니다. 버전 **3.9**부터는 플랫폼에서 대용량의 **SDM**을 삭제할 때마다 이벤트가 발생합니다.

## IPFIX란 무엇입니까?

IPFIX는 흐름 정보 내보내기에 대한 IETF 프로토콜입니다. 흐름은 특정 시간 슬롯 내에 전송되며 5-튜플 값(소스 IP 주소, 소스 포트, 대상 IP 주소, 대상 포트 및 프로토콜)을 공유하는 패킷 집합으로 정의됩니다. 흐름 정보에는 타임 스탬프, 패킷/바이트 수, 입/출력 인터페이스, TCP 플래그, VXLAN ID, 캡슐화된 흐름 정보 등과 같은 속성이 포함될 수 있습니다. 이것을 종종 NetFlow라고 합니다. 하지만 IPFIX가 표준 IETF 프로토콜입니다.

## VDS는 어떤 흐름 정보를 내보냅니까?

vSphere 환경의 VDS는 IPFIX를 사용하여 흐름 정보를 내보내도록 구성할 수 있습니다. VDS에 연결된 모든 포트 그룹에서 흐름 모니터링을 사용하도록 설정합니다. 패킷이 VDS의 포트 X에 도착하고 포트 Y에서 나가는 경우 포트 Y에서 흐름 모니터링을 사용하도록 설정하면 해당하는 흐름 레코드가 발생합니다. 모든 흐름 레코드의 방향은 "송신"으로 설정되어 있습니다.

## vRealize Network Insight는 IPFIX를 어떻게 사용합니까?

vRealize Network Insight는 VMware VDS IPFIX를 사용하여 네트워크 트래픽 데이터를 수집합니다. 모든 세션에는 두 개의 경로가 있습니다. 예를 들어 세션 A↔C에는 A→C 패킷과 C→A 패킷이 있습니다. 세션의 전체 정보를 분석하기 위해서는 양방향의 패킷에 대한 IPFIX 데이터가 필요합니다. VM-A가 DVPG-A에 연결되어 있고 VM-C와 통신하는 다음 다이어그램을 참조하십시오. 여기에서 DVPG-A는 C→A 패킷에 대한 데이터만 제공하고 DVPG-업링크는 A→C 패킷에 대한 데이터를 제공합니다. A 트래픽에 대한 전체 정보를 가져오려면 DVPG-A와 DVPG-업링크에서 IPFIX를 사용하도록 설정해야 합니다.

## vRealize Network Insight 흐름 수집 문제는 어떻게 해결합니까?

- 1 특정 VDS와 해당 DVPG 및 업링크 속성에 Netflow 모니터링이 **사용**으로 설정되어 있고 수집기 IP 주소가 vRealize Network Insight 수집기의 주소인지 확인하십시오.
- 2 IPFIX Netflow 패킷이 방화벽(NSX, 가상 또는 물리적)에 의해 삭제됩니다. vRealize Network Insight 수집기 IP의 UDP 포트 2055로 향하는 Netflow 패킷이 ESXi 호스트와 vRealize Network Insight 수집기 사이의 경로에 있을 수 있는 방화벽에 의해 허용되는지 확인하십시오.

- 3 ESXi 호스트가 IPFIX Netflow 패킷 전송을 중단했습니다. ESXi 호스트는 UDP 포트 2055에 연결할 수 없는 경우 잠시 후 Netflow 패킷 전송을 중단합니다. 이 문제는 방화벽의 패킷 삭제로 인해 발생할 수 있습니다.
- 4 네트워크 라우팅 문제로 인해 ESXi 호스트에서 vRealize Network Insight 수집기에 연결할 수 없습니다. ESXi 호스트와 vRealize Network Insight 수집기 사이에 적합한 경로가 있는지 확인하십시오.

## IPFIX와 관련하여 알아야 하는 VMware KB 문서는 무엇입니까?

VMware ESXi 6.0 업데이트 1: [2135956](#) .

## 서비스는 언제 공유된 것으로 간주됩니까?

프로토콜	포트
DNS	53
Bootpc	68
Kerberos	88
Pop3	110
sunrpc	111
NTP	123
map	143
Imap3	220
SMTP	25
LDAP	389
IGMPv3Lite	465
syslog	514
Submission	587
syslog-conn	601
LDAPS	636
IMAPS	993
POP3S	995
NFS	2049
MSFT-GC	3268
MSFT-GC-SSL	3269