

Nexus Data Broker Openflow 모드 및 제한 사항

목차

[소개](#)

[NDB 기능](#)

[작동 모드](#)

[Openflow](#)

[Openflow 구성 요소](#)

[Openflow와 함께 NDB 사용 시 제한](#)

[알려진 결함](#)

소개

Cisco Nexus NDB(Data Broker)는 대량의 비즈니스 크리티컬 트래픽을 모니터링할 수 있는 간단하고 확장 가능하며 비용 효율적인 솔루션을 제공합니다. 이 트래픽에 대한 가시성은 보안 유지, 문제 해결 지원, 규정 준수 보장 및 리소스 계획 수행에 매우 중요합니다. 이 소프트웨어 정의 패킷 브로커 방식은 Cisco Nexus 3000 및 9000 Series 데이터 센터 스위치에 사용할 수 있습니다.

NDB 기능

네트워크 트래픽 모니터링

애플리케이션 트래픽에 대한 가시성은 보안 유지, 문제 해결 및 리소스 계획 수행을 위한 인프라 운영에 중요합니다.

확장 가능한 TAP 및 SPAN 어그리게이션

이 제품은 기존의 특수 목적 매트릭스 스위치를 상호 연결할 수 있는 하나 이상의 Cisco Nexus 3000 또는 9000 Series 스위치로 대체하며, 이를 통해 1, 10, 40 및 100Gbps를 지원하는 Cisco® SPAN(Switched Port Analyzer) 어그리게이션 인프라를 구축할 수 있습니다. 또한 TAP 및 SPAN 전용 포트와 기존 이더넷 연결을 모두 지정할 수 있습니다.

Cisco Application Centric Infrastructure 통합

Cisco Nexus Data Broker는 Cisco ACI와 통합되어 Cisco ACI 패브릭 내에서 트래픽을 모니터링하기 위한 SPAN 세션 및/또는 복사 기능을 구성합니다. 이러한 통합으로 인해 사용자가 APIC에서 SPAN 세션이나 Copy 기능을 별도로 구성할 필요가 없습니다.

프로덕션 네트워크의 자동화된 SPAN 구성

이제 NDB는 Cisco Nexus Data Broker에서 프로덕션 스위치를 추가하고 SPAN 대상 및 세션 컨피그레이션을 자동화할 수 있습니다. 이 기능을 통해 관리자는 단일 인터페이스를 사용하여 모니터링을 위해 트래픽을 가져올 수 있습니다.

Cisco Nexus Data Broker Inline 옵션을 통한 확장 가능한 트래픽 모니터링

Cisco Nexus Data Broker Inline 옵션을 사용하면 보안 툴(또는 서비스 노드)이 연결된 운영 인프라에 하나 이상의 Cisco Nexus 3000 Series 또는 9300 플랫폼 스위치를 삽입할 수 있습니다. 데이터 브로커 소프트웨어를 사용하여 특정 트래픽과 일치시킬 수 있는 리디렉션 정책을 구성하고, 트

래픽이 데이터 센터에 들어오거나 나가기 전에 여러 보안 톨을 통해 리디렉션합니다.

다음과 같은 모드로 구축할 수 있습니다

- NDB가 Linux VM에 설치된 종대형 탭/SPAN 어그리게이션을 위한 중앙 집중식 모드.
- Nexus 스위치 자체의 Linux 컨테이너에 NDB가 설치된 소규모 탭/SPAN 어그리게이션을 위한 임베디드 단일 스위치 모드.

작동 모드

- OpenFlow 모드
- NX-API 모드

Openflow

OpenFlow는 SDN(Software-Defined Networking) 컨트롤러가 네트워크의 포워딩 플레인을 관리할 수 있도록 하는 개방형 표준화 인터페이스입니다.

Cisco OpenFlow Agent는 네트워크를 보다 효율적으로 제어하여 보다 개방적이고 프로그래밍 가능하며 애플리케이션을 인식할 수 있도록 하며 ONF(Open Networking Foundation) 표준 조직에서 정의한 다음 사양을 지원합니다.

- OpenFlow 스위치 사양 버전 1.0.1(유선 프로토콜 0x01)(OpenFlow 1.0이라고 함)
- OpenFlow 스위치 사양 버전 1.3.0(유선 프로토콜 0x04)(OpenFlow 1.3이라고 함)

이러한 사양은 디바이스의 트래픽 흐름을 추가하거나 제거할 수 있도록 내부 플로우 테이블 및 표준화된 인터페이스가 포함된 이더넷 스위치의 개념을 기반으로 합니다. OpenFlow 1.3은 Cisco OpenFlow Agent와 컨트롤러 간의 통신 채널을 정의합니다.

컨트롤러는 Cisco Open SDN Controller 또는 OpenFlow 1.3을 준수하는 모든 컨트롤러일 수 있습니다.

OpenFlow 네트워크에서는 Cisco OpenFlow Agent가 디바이스에 있고 컨트롤러는 디바이스 외부의 서버에 있습니다. 플로우 관리 및 네트워크 관리는 컨트롤러의 일부이거나 컨트롤러를 통해 수행됩니다. 플로우 관리에는 플로우의 추가, 수정 또는 제거 및 OpenFlow 오류 메시지 처리가 포함됩니다.

Openflow 구성 요소

Cisco OpenFlow Agent는 Cisco OpenFlow Agent 논리 스위치의 컨트롤러에 대한 OpenFlow 기반 TCP/IP 연결을 생성합니다. Cisco OpenFlow Agent는 구성된 논리 스위치, OpenFlow 지원 인터페이스 및 흐름에 대한 데이터베이스를 생성합니다. 논리 스위치 데이터베이스에는 컨트롤러에 연결하는 데 필요한 모든 정보가 들어 있습니다. 인터페이스 데이터베이스에는 논리 스위치와 연결된 OpenFlow 지원 인터페이스 목록이 포함되어 있으며, 흐름 데이터베이스에는 논리 스위치의 흐름 목록과 전달된 트래픽으로 프로그래밍된 인터페이스의 목록이 포함되어 있습니다.

OpenFlow 컨트롤러(컨트롤러라고도 함)는 스위치를 제어하고 Cisco OpenFlow Agent 논리 스위치를 통해 OpenFlow 1.3 및 1.0 일치 및 작업 기준의 하위 집합을 가진 흐름을 삽입합니다. Cisco OpenFlow Agent는 다른 작업으로 모든 OpenFlow 메시지를 거부합니다.

Openflow와 함께 NDB 사용 시 제한

Openflow가 특정 포트에서 활성화되면 인터페이스에서 'spanning-tree bpdufilter enable'이 자동으로

로 구성되어 소프트웨어에서 STP BPDU가 삭제됩니다.

또한 인터페이스에 'lldp 전송 없음'이 구성됩니다. 따라서 이러한 인터페이스에 대한 LLDP 인접 관계가 스위치에 형성되지 않습니다. 그러나 LLDP 패킷은 ACL 엔트리를 통해 캡처됩니다.

현재 NDB는 아래의 링크 레벨 컨트롤 플레인 프로토콜에서 트래픽을 캡처하지 않습니다.

- STP
- LACP
- CDP

알려진 결함

[CSCvr09006](#) NDB with 3500은 STP/CDP 패킷을 캡처할 수 없습니다

[CSCvr01876](#) Re-direct STP, Openflow용 LLDP 포트와 유사한 CDP 패킷

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.