OpenFlow-Modus für Nexus Data Broker und dessen Einschränkungen

Inhalt

Einleitung

Cisco Nexus Data Broker (NDB) ist eine einfache, skalierbare und kosteneffiziente Lösung zur Überwachung von umfangreichem und geschäftskritischem Datenverkehr. Die Transparenz dieses Datenverkehrs ist für die Aufrechterhaltung der Sicherheit, die Unterstützung der Fehlerbehebung, die Gewährleistung der Compliance und die Ressourcenplanung von entscheidender Bedeutung. Dieser softwaredefinierte Packet-Broker-Ansatz ist für Rechenzentrums-Switches der Serien Cisco Nexus 3000 und 9000 verfügbar.

NDB-Funktionen

Netzwerkverkehr überwachen

Die Transparenz des Anwendungsdatenverkehrs ist für den Infrastrukturbetrieb wichtig, um die Sicherheit aufrechtzuerhalten, Probleme zu lösen und die Ressourcenplanung durchzuführen.

Skalierbare TAP- und SPAN-Aggregation

Sie ersetzt herkömmliche Matrix-Switches durch einen oder mehrere Cisco Nexus Switches der Serien 3000 oder 9000, die zur Erstellung eines skalierbaren Netzwerktest-Access-Ports (TAP) und einer Cisco® Switched Port Analyzer (SPAN)-Aggregationsinfrastruktur, die 1, 10, 40 und 100 Gbit/s unterstützt, miteinander verbunden werden können. Außerdem können Ports sowohl für TAP und SPAN als auch für herkömmliche Ethernet-Verbindungen reserviert werden.

Cisco Application Centric Infrastructure-Integration

Cisco Nexus Data Broker kann mit der Cisco ACI integriert werden, um SPAN-Sitzungen und/oder Kopierfunktionen zur Überwachung des Datenverkehrs in der Cisco ACI-Fabric zu konfigurieren. Dank dieser Integration müssen keine SPAN-Sitzungen oder die Kopierfunktion im APIC separat konfiguriert werden.

Automatisierte SPAN-Konfiguration im Produktionsnetzwerk

NDB kann jetzt Produktions-Switches in Cisco Nexus Data Broker hinzufügen und die SPAN-Ziel- und Sitzungskonfiguration automatisieren. Dank dieser Funktion können Administratoren Datenverkehr zu Überwachungszwecken über eine einzige Schnittstelle einspeisen.

Skalierbare Datenverkehrsüberwachung mit Cisco Nexus Data Broker Inline-Option

Mit der Cisco Nexus Data Broker Inline-Option können Sie einen oder mehrere Cisco Nexus Switches der Serie 3000 oder 9300 in Ihre Produktionsinfrastruktur einfügen, mit denen die Sicherheitstools (oder Serviceknoten) verbunden sind. Konfigurieren Sie mithilfe der Datenbroker-Software Umleitungsrichtlinien, die auf bestimmten Datenverkehr abgestimmt sein können, und leiten Sie diesen über mehrere Sicherheitstools um, bevor der Datenverkehr in das Rechenzentrum eintritt oder es verlässt.

Sie kann in folgenden Modi bereitgestellt werden:

- **Zentralisierter** Modus für mittelgroße bis große Tap-/SPAN-Aggregation, bei dem NDB auf dem Linux VM installiert ist.
- **Eingebetteter** Einzel-Switch-Modus für kleine Tap-/SPAN-Aggregation, bei dem NDB im Linux-Container des Nexus-Switches selbst installiert ist.

Betriebsmodi

- **OpenFlow-Modus**
- **NX-API-Modus**

OpenFlow

OpenFlow ist eine offene, standardisierte Schnittstelle, die es einem SDN-Controller (Software-defined Networking) ermöglicht, die Weiterleitungsebene eines Netzwerks zu verwalten.

Cisco OpenFlow Agent bietet eine bessere Kontrolle über Netzwerke, wodurch diese offener, programmierbarer und anwendungsorientierter werden, und unterstützt die folgenden, von der Organisation der Open Networking Foundation (ONF) definierten Spezifikationen:

- OpenFlow Switch Specification Version 1.0.1 (Wire Protocol 0x01) (bezeichnet als OpenFlow 1.0)
- OpenFlow Switch Specification Version 1.3.0 (Wire Protocol 0x04) (bezeichnet als OpenFlow 1.3)

Diese Spezifikationen basieren auf dem Konzept eines Ethernet-Switches mit einer internen Flow-Tabelle und einer standardisierten Schnittstelle, über die Datenverkehrsflüsse auf einem Gerät hinzugefügt oder entfernt werden können. OpenFlow 1.3 definiert den Kommunikationskanal zwischen dem Cisco OpenFlow Agent und den Controllern.

Ein Controller kann ein Cisco Open SDN Controller oder ein beliebiger Controller sein, der mit OpenFlow 1.3 kompatibel ist.

In einem OpenFlow-Netzwerk ist Cisco OpenFlow Agent auf dem Gerät vorhanden, und die Controller befinden sich auf einem Server, der sich außerhalb des Geräts befindet. Flow-Management und Netzwerkmanagement sind entweder Teil eines Controllers oder werden über einen Controller durchgeführt. Das Flow-Management umfasst das Hinzufügen, Ändern oder Entfernen von Flows und die Behandlung von OpenFlow-Fehlermeldungen.

OpenFlow-Komponenten

Cisco OpenFlow Agent erstellt OpenFlow-basierte TCP/IP-Verbindungen zu Controllern für einen logischen Switch des Cisco OpenFlow Agent. Cisco OpenFlow Agent erstellt Datenbanken für

einen konfigurierten logischen Switch, OpenFlow-fähige Schnittstellen und Flows. Die Datenbank des logischen Switches enthält alle Informationen, die für die Verbindung mit einem Controller erforderlich sind. Die Schnittstellendatenbank enthält die Liste der OpenFlow-fähigen Schnittstellen, die einem logischen Switch zugeordnet sind, und die Flussdatenbank enthält die Liste der Flows auf einem logischen Switch sowie für Schnittstellen, die in weitergeleiteten Datenverkehr programmiert sind.

Der OpenFlow-Controller (auch als Controller bezeichnet) steuert den Switch und fügt Flows mit einer Teilmenge der Übereinstimmung und Aktionskriterien von OpenFlow 1.3 und 1.0 über den logischen Switch von Cisco OpenFlow Agent ein. Cisco OpenFlow-Agent lehnt alle OpenFlow-Nachrichten mit einer anderen Aktion ab.

Einschränkung bei Verwendung von NDB mit OpenFlow

Wenn OpenFlow auf einem bestimmten Port aktiviert ist, wird "spanning-tree bpdufilter enable" automatisch auf der Schnittstelle konfiguriert, sodass STP BPDU in der Software verloren geht.

Darüber hinaus ist auf der Schnittstelle auch "no lldp transmission" konfiguriert. Daher bildet sich auf dem Switch keine LLDP-Nachbarschaft für diese Schnittstellen. LLDP-Pakete werden jedoch über einen ACL-Eintrag erfasst.

Derzeit erfasst NDB keinen Datenverkehr von den Protokollen der Steuerungsebene auf Verbindungsebene:

- STP
- LACP
- CDP

Bekannte Fehler

CSCvr09006 NDB mit 3500 kann STP-/CDP-Pakete nicht erfassen
CSCvr01876 STP umleiten, CDP-Pakete ähnlich wie LLDP-Port für OpenFlow

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.