Nexus Data Broker OpenFlow Mode en zijn beperkingen

Inhoud

Inleiding

Cisco Nexus Data Broker (NDB) biedt een eenvoudige, schaalbare, rendabele oplossing voor de bewaking van grote hoeveelheden en bedrijfskritiek verkeer. Zichtbaarheid in dit verkeer is essentieel voor het behoud van de beveiliging, het ondersteunen van probleemoplossing, het garanderen van naleving en het uitvoeren van resourceplanning. Deze softwaregedefinieerde pakketbrokerbenadering is beschikbaar voor Cisco Nexus 3000 en 9000 Series datacenterswitches.

NDB-functies

Netwerkverkeer controleren

Zichtbaarheid in toepassingsverkeer is belangrijk voor infrastructurele activiteiten om de beveiliging te behouden, problemen op te lossen en resourceplanning uit te voeren.

Schaalbare TAP- en SPAN-aggregatie

switch Het vervangt traditionele speciaal gebouwde matrixinfrastructuren met een of meer Cisco Nexus 3000 of 9000 Series Switches die u kunt verbinden om een schaalbare Network Test Access Port (TAP) en Cisco® Switched Port Analyzer (SPAN) aggregatie-infrastructuur te bouwen die 1, 10, 40 en 100 Gbps ondersteunt. Het kan ook poorten toewijzen voor zowel TAP en SPAN als voor traditionele Ethernet-connectiviteit.

Cisco-infrastructuur voor toepassingscentra - integratie

Cisco Nexus Data Broker integreert met Cisco ACI om SPAN-sessies te configureren en/of de functie Kopiëren om verkeer binnen de Cisco ACI-fabric te controleren. Door deze integratie hoeft de gebruiker geen SPAN-sessies of kopieerfunctie in de APIC afzonderlijk te configureren.

Geautomatiseerde SPAN-configuratie in productienetwerk

NDB kan nu productie-switches toevoegen in Cisco Nexus Data Broker en SPAN-bestemming en sessieconfiguratie automatiseren. Met deze mogelijkheid kunnen beheerders één interface gebruiken om verkeer in te voeren voor controledoeleinden.

Schaalbare verkeersbewaking met Cisco Nexus Data Broker Inline optie

Met de inline optie van Cisco Nexus Data Broker kunnen een of meer Cisco Nexus 3000 Series- of 9300-switches in uw productieinfrastructuur worden geplaatst waarmee de beveiligingstools (of serviceknooppunten) zijn verbonden. Met behulp van de data broker software, configureer omleidingsbeleid dat kan overeenkomen met specifiek verkeer en omleiden door meerdere security tools voordat het verkeer binnengaat of het datacenter verlaat.

Het kan in de volgende modi worden uitgevoerd

- **Gecentraliseerde** modus voor tap/SPAN-aggregatie op middellange tot grote schaal waar NDB is geïnstalleerd op Linux-VM.
- **Ingesloten** single switch mode voor kleinschalige tap/SPAN aggregatie waar NDB is geïnstalleerd op de Linux Container van de Nexus Switch zelf.

Bedieningswijzen

- **OpenFlow-modus**
- **NX-API-modus**

OpenFlow

OpenFlow is een open gestandaardiseerde interface die een software-defined networking (SDN) controller in staat stelt om het doorstuurvlak van een netwerk te beheren.

Cisco OpenFlow Agent biedt betere controle over netwerken, waardoor ze opener, programmeerbaar en toepassingsbewust worden, en ondersteunt de volgende specificaties die worden gedefinieerd door de Open Networking Foundation (ONF)-standaardisatieorganisatie:

- OpenFlow Switch Specificatie versie 1.0.1 (Wire Protocol 0x01) (bekend als OpenFlow 1.0)
- OpenFlow Switch Specificatie versie 1.3.0 (Wire Protocol 0x04) (bekend als OpenFlow 1.3)

Deze specificaties zijn gebaseerd op het concept van een Ethernet-switch, met een interne-stroomtabel en een gestandaardiseerde interface om verkeersstromen op een toestel toe te voegen of te verwijderen. OpenFlow 1.3 definieert het communicatiekanaal tussen de Cisco OpenFlow Agent en controllers.

Een controller kan Cisco Open SDN-controller zijn, of elke controller die compatibel is met OpenFlow 1.3.

In een OpenFlow-netwerk is Cisco OpenFlow Agent aanwezig op het apparaat en controllers bestaan op een server die extern is aan het apparaat. Stroombeheer en elk netwerkbeheer zijn ofwel onderdeel van een controller, ofwel gerealiseerd via een controller. Flow management omvat de toevoeging, wijziging of verwijdering van stromen en de verwerking van OpenFlow foutmeldingen.

OpenFlow-componenten

Cisco OpenFlow Agent maakt op OpenFlow gebaseerde TCP/IP-verbindingen met controllers voor een logische switch met Cisco OpenFlow Agent. Cisco OpenFlow Agent maakt databases voor een geconfigureerde logische switch, interfaces en stromen met OpenFlow. De logical switch database bevat alle informatie die nodig is om verbinding te maken met een controller. De interfacedatabase bevat de lijst van OpenFlow-enabled interfaces gekoppeld aan een logische

switch, en de stroomdatabase bevat de lijst van stromen op een logische switch evenals voor de interface die geprogrammeerd is in doorgestuurd verkeer.

OpenFlow-controller (ook wel controller genoemd) controleert de switch en voegt stromen in met een subset van OpenFlow 1.3 en 1.0 matching- en actiecriteria via Cisco OpenFlow Agent logical switch. Cisco OpenFlow Agent wijst alle OpenFlow-berichten met een andere actie af.

Beperking bij gebruik van NDB met OpenFlow

Wanneer OpenFlow op een bepaalde poort is ingeschakeld, wordt 'Spanning-Tree Bpdufilter Enable' automatisch op de interface geconfigureerd, wat resulteert in een STP BPDU-drop-in-software.

Daarnaast is 'no lldp zend' ook geconfigureerd op de interface. LLDP-buurten voor deze interfaces worden dus niet gevormd op de switch. LLDP-pakketten worden echter via ACL-vermeldingen opgenomen.

Momenteel neemt NDB geen verkeer op van onder de protocollen van het link-level controlevliegtuig:

- STP

- LACP

- CDP

Bekende gebreken

CSCv09006 NDB met 3500 kan STP/CDP-pakketten niet opnemen
CSCvr01876 Re-direct STP, CDP-pakketten vergelijkbaar met LLDP-poort voor OpenFlow

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.