

Modo Openflow do Nexus Data Broker e suas limitações

Contents

[Introduction](#)

[Recursos NDB](#)

[Modos de funcionamento](#)

[Fluxo De Abertura](#)

[Componentes Openflow](#)

[Limitação ao usar NDB com Openflow](#)

[Defeitos conhecidos](#)

Introduction

O Cisco Nexus Data Broker (NDB) oferece uma solução simples, escalável e econômica para monitorar o tráfego de alto volume e crítico para os negócios. A visibilidade desse tráfego é essencial para manter a segurança, oferecer suporte à solução de problemas, ajudar a garantir a conformidade e executar o planejamento de recursos. Essa abordagem de agente de pacotes definida por software está disponível para os switches de data center Cisco Nexus 3000 e 9000 Series.

Recursos NDB

Monitorar o tráfego de rede

A visibilidade do tráfego de aplicativos é importante para que as operações de infraestrutura mantenham a segurança, resolvam problemas e executem o planejamento de recursos.

Agregação escalável de TAP e SPAN

Ele substitui os switches de matriz de uso específico tradicionais por um ou mais switches Cisco Nexus 3000 ou 9000 Series que podem ser interconectados para criar uma infraestrutura de agregação de porta de acesso de teste de rede (TAP) escalável e Cisco[®] Switched Port Analyzer (SPAN) que comporta 1, 10, 40 e 100 Gbps. Também pode dedicar portas para TAP e SPAN e para conectividade Ethernet tradicional.

Integração da Cisco Application Centric Infrastructure

O Cisco Nexus Data Broker se integra à Cisco ACI para configurar sessões de SPAN e/ou função de cópia para monitorar o tráfego na estrutura da Cisco ACI. Essa integração elimina a necessidade de o usuário configurar separadamente as sessões de SPAN ou a função Copiar no APIC.

Configuração de SPAN automatizada na rede de produção

O NDB agora pode adicionar switches de produção no Cisco Nexus Data Broker e automatizar a configuração de sessão e de destino de SPAN. Esse recurso permite que os administradores usem uma única interface para trazer o tráfego para fins de monitoramento.

Monitoramento de tráfego escalável com a opção em linha Cisco Nexus Data Broker

A opção Cisco Nexus Data Broker Inline permite inserir um ou mais switches de plataforma Cisco Nexus 3000 Series ou 9300 na infraestrutura de produção à qual as ferramentas de segurança (ou nós de serviço) estão conectadas. Usando o software de agente de dados, configure políticas de redirecionamento que possam corresponder ao tráfego específico e redirecioná-lo através de várias ferramentas de segurança antes que o tráfego entre ou saia do data center.

Ele pode ser implantado nos seguintes modos

- Modo **centralizado** para agregação de toque/SPAN de média a grande escala em que o NDB é instalado na VM Linux.
- **Modo de switch único incorporado** para agregação de toque/SPAN de pequena escala, onde o NDB é instalado no contêiner Linux do próprio switch Nexus.

Modos de funcionamento

- modo OpenFlow
- modo NX-API

Fluxo De Abertura

O OpenFlow é uma interface padronizada aberta que permite que um controlador de rede definida por software (SDN) gerencie o plano de encaminhamento de uma rede.

O Cisco OpenFlow Agent oferece melhor controle sobre as redes, tornando-as mais abertas, programáveis e sensíveis a aplicativos, e suporta as seguintes especificações definidas pela organização de padrões Open Networking Foundation (ONF):

- OpenFlow Switch Specification Versão 1.0.1 (Wire Protocol 0x01) (conhecido como OpenFlow 1.0)
- OpenFlow Switch Specification Versão 1.3.0 (Wire Protocol 0x04) (conhecido como OpenFlow 1.3)

Essas especificações são baseadas no conceito de um switch Ethernet, com uma tabela de fluxo interno e uma interface padronizada para permitir que os fluxos de tráfego em um dispositivo sejam adicionados ou removidos. O OpenFlow 1.3 define o canal de comunicação entre o Cisco OpenFlow Agent e os controladores.

Um controlador pode ser o Cisco Open SDN Controller ou qualquer controlador compatível com o OpenFlow 1.3.

Em uma rede OpenFlow, o Cisco OpenFlow Agent existe no dispositivo e os controladores existem em um servidor externo ao dispositivo. O gerenciamento de fluxo e qualquer gerenciamento de rede são parte de um controlador ou realizados por meio de um controlador. O gerenciamento de fluxo inclui a adição, modificação ou remoção de fluxos e o tratamento de mensagens de erro do OpenFlow.

Componentes Openflow

O Cisco OpenFlow Agent cria conexões TCP/IP com base em OpenFlow para controladores para um switch lógico do Cisco OpenFlow Agent. O Cisco OpenFlow Agent cria bancos de dados para

um switch lógico configurado, interfaces ativadas para OpenFlow e fluxos. O banco de dados do comutador lógico contém todas as informações necessárias para se conectar a um controlador. O banco de dados de interface contém a lista de interfaces ativadas para OpenFlow associadas a um comutador lógico e o banco de dados de fluxo contém a lista de fluxos em um comutador lógico, bem como para a interface que é programada no tráfego encaminhado.

O controlador OpenFlow (chamado de controlador) controla o switch e insere fluxos com um subconjunto de correspondência do OpenFlow 1.3 e 1.0 e critérios de ação por meio do switch lógico do Cisco OpenFlow Agent. O Cisco OpenFlow Agent rejeita todas as mensagens OpenFlow com qualquer outra ação.

Limitação ao usar NDB com Openflow

Quando o Openflow é habilitado em uma porta específica, 'spanning-tree bpdudfilter enable' é configurado automaticamente na interface, resultando em queda de STP BPDU no software.

Além disso, 'no lldp transmit' também é configurado na interface. Assim, a vizinhança LLDP para essas interfaces não é formada no switch. No entanto, os pacotes LLDP são capturados através da entrada da ACL.

Atualmente, o NDB não captura o tráfego dos protocolos de plano de controle abaixo do nível do link:

- STP
- LACP
- CDP

Defeitos conhecidos

[CSCvr09006](#) NDB com 3500 não pode capturar pacotes STP/CDP

[CSCvr01876](#) Redirecione pacotes STP, CDP semelhantes à porta LLDP para Openflow

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.