Nexus Data Broker Openflowモードとその制限事項

内容

概要

Cisco Nexus Data Broker(NDB)は、大容量のビジネスクリティカルなトラフィックを監視するための、シンプルでスケーラブルなコスト効率の高いソリューションを提供します。このトラフィックの可視性は、セキュリティの維持、トラブルシューティングのサポート、コンプライアンスの確保、リソース計画の実行に不可欠です。このソフトウェア定義のパケットブローカアプローチは、Cisco Nexus 3000および9000シリーズデータセンタースイッチで使用できます。

NDB機能

ネットワークトラフィックの監視

インフラストラクチャの運用において、セキュリティの維持、問題の解決、リソース計画の実行を行うには、アプリケーショントラフィックの可視性が重要です。

スケーラブルなTAPおよびSPANアグリゲーション

従来の専用マトリックススイッチを1つ以上のCisco Nexus 3000または9000シリーズスイッチに置き換えます。これらのスイッチを相互接続して、1、10、40、および100 Gbpsをサポートするスケーラブルなネットワークテストアクセスポート(TAP)およびCisco® Switched Port Analyzer(SPAN)アグリゲーションインフラストラクチャを構築できます。また、TAPとSPANおよび従来のイーサネット接続の両方に専用ポートを割り当てることもできます。

シスコアプリケーションセントリックインフラストラクチャの統合

Cisco Nexus Data Brokerは、Cisco ACIと統合してSPANセッションを設定したり、Cisco ACIファブリック内のトラフィックを監視するコピー機能を設定したりします。この統合により、APICでSPANセッションまたはコピー機能を個別に設定する必要がなくなります。

実稼働ネットワークでの自動SPAN設定

NDBは、Cisco Nexus Data Brokerに実稼働スイッチを追加し、SPANの宛先とセッションの設定を自動化できるようになりました。この機能により、管理者は単一のインターフェイスを使用して、モニタリング目的でトラフィックを取り込むことができます。

Cisco Nexus Data Brokerインラインオプションによるスケーラブルなトラフィックモニタリング

Cisco Nexus Data Brokerインラインオプションを使用すると、セキュリティツール（またはサービスノード）が接続されている実稼働インフラストラクチャに、1つ以上のCisco Nexus 3000シリーズまたは9300プラットフォームスイッチを挿入できます。Data Brokerソフトウェアを使用して、特定のトラフィックに一致するリダイレクトポリシーを設定し、トラフィックがデータセンターに出入りする前に複数のセキュリティツールを介してリダイレクトします。

次のモードで導入できます

- Linux VMにNDBがインストールされている中規模から大規模のタップ/SPANアグリゲーション用の集中型モード。
- Nexusスイッチ自体のLinuxコンテナにNDBがインストールされている小規模なタップ/SPANアグリゲーション用の組み込みシングルスイッチモード。

操作のモード

- OpenFlowモード
- NX-APIモード

OpenFlow

OpenFlowは、ソフトウェア定義型ネットワーク(SDN)コントローラでネットワークのフォワーディングプレーンを管理できる、オープンで標準化されたインターフェイスです。

Cisco OpenFlow Agentは、ネットワークをよりオープンでプログラム可能なアプリケーション認識型に制御し、Open Networking Foundation(ONF)標準化団体によって定義された次の仕様をサポートします。

- OpenFlow Switch Specification Version 1.0.1(Wire Protocol 0x01)（OpenFlow 1.0と呼ばれる）
- OpenFlow Switch Specification Version 1.3.0(Wire Protocol 0x04)（OpenFlow 1.3と呼ばれる）

これらの仕様は、イーサネットスイッチの概念に基づいており、内部フローテーブルと標準化されたインターフェイスを使用して、デバイス上のトラフィックフローを追加または削除できます。OpenFlow 1.3は、Cisco OpenFlow Agentとコントローラ間の通信チャネルを定義します。

コントローラは、Cisco Open SDN Controllerでも、OpenFlow 1.3に準拠した任意のコントローラでもかまいません。

OpenFlowネットワークでは、Cisco OpenFlow Agentはデバイス上に存在し、コントローラはデバイスの外部にあるサーバ上に存在します。フロー管理およびネットワーク管理は、コントローラの一部であるか、コントローラを介して実行されます。フロー管理には、フローの追加、変更、または削除、およびOpenFlowエラーメッセージの処理が含まれます。

Openflowコンポーネント

Cisco OpenFlow Agentは、Cisco OpenFlow Agent論理スイッチのコントローラへのOpenFlowベースのTCP/IP接続を作成します。Cisco OpenFlow Agentは、設定された論理スイッチ、OpenFlow対応インターフェイス、およびフローのデータベースを作成します。論理スイッチデータベースには、コントローラへの接続に必要なすべての情報が含まれています。インターフェイスデータベースには、論理スイッチに関連付けられたOpenFlow対応インターフェイスのリストが含まれ、フローデータベースには、論理スイッチおよび転送トラフィックにプログラムされているインターフェイス上のフローのリストが含まれます。

OpenFlowコントローラ（コントローラと呼ばれます）はスイッチを制御し、Cisco OpenFlow Agent論理スイッチを介して、OpenFlow 1.3および1.0の一致基準とアクション基準のサブセットを持つフローを挿入します。Cisco OpenFlow Agentは、他のアクションを持つすべてのOpenFlowメッセージを拒否します。

OpenflowでNDBを使用する場合の制限

特定のポートでOpenflowが有効になっている場合は、インターフェイスで「spanning-tree bpdufilter enable」が自動的に設定され、その結果ソフトウェアでSTP BPDUがドロップされます。

さらに、インターフェイスでも「no lldp transmit」が設定されています。したがって、これらのインターフェイスのLLDPネイバーシップはスイッチでは形成されません。ただし、LLDPパケットはACLエントリによってキャプチャされます。

現在、NDBは次のリンクレベルのコントロールプレーンプロトコルからのトラフィックをキャプチャしません。

-STP

-LACP

-CDP

既知の障害

CSCvr09006 3500を搭載したNDBはSTP/CDPパケットをキャプチャできない
CSCvr01876:OpenflowのLLDPポートに類似したSTPおよびCDPパケットをリダイレクトする

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。