

ДОСЛІДЖЕННЯ ВИКОРИСТАННЯ OPEN VIRTUAL SWITCH В МЕРЕЖАХ SDN

Лящук А.А.

*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна
E-mail: aliashchuk@outlook.com*

Researches of using Open vSwitch in SDN networks

The article describes the most important characteristics and design considerations preferences Open Virtual Switch (OVS).

Open vSwitch являє собою програмний комутатор, що працює як з фізичними інтерфейсами, так і з віртуальними інтерфейсами віртуальних машин. Це багаторівневий віртуальний комутатор з відкритим вихідним кодом, який поширюється під ліцензією Apache. Open vSwitch підтримує найбільш популярні Open-source гіпервізори, такі як VirtualBox, Xen, KVM і XenServer. Також Open vSwitch може використовуватися в якості заміни мостового модулю (bridge module), що використовується в Linux.

Гіпервізори потребують можливості переміщувати трафік між віртуальними машинами та зовнішнім світом. Для гіпервізорів на базі Linux, це зазвичай означає використання вбудованого комутатора L2 (the Linux bridge), що є швидким і надійним. Отже, виникає питання, для чого використовувати Open vSwitch?

Відповідь полягає в тому, що Open vSwitch призначений для розгортання багатосерверної віртуалізації. Ці середовища часто характеризуються високо динамічними кінцевими точками, підтримкою логічних абстракцій та (іноді) інтеграцією або розвантаженням на спеціальне комутуюче обладнання [1].

Наступні характеристики допомагають Open vSwitch впоратися з вищенаведеними вимогами.

Мобільність стану. Весь стан мережі, пов'язаний з мережевим об'єктом, повинен легко ідентифікуватися та мігрувати між різними хостами. Це може включати традиційний "м'який стан" (наприклад, запис у таблицю вивчення L2), стан переадресації L3, політику маршрутизації, список контролю доступу (ACL), політику QoS, конфігурацію моніторингу (наприклад, NetFlow, IPFIX, sFlow) тощо.

Open vSwitch підтримує конфігурування та міграцію як повільного так і швидкого стану мережі між екземплярами. Наприклад, якщо віртуальна машина мігрує між кінцевими хостами, можна не тільки перемістити пов'язану конфігурацію (правила SPAN, ACL, QoS), а й будь-який стан мережі (включаючи, наприклад, існуючий стан, який може бути складним для

реконструкції). Крім того, стан Open vSwitch набирається та підтримується реальною моделлю даних, що дозволяє розробляти структуровані системи автоматизації.

Реагування на динаміку мережі. Віртуальне середовище характеризується високими темпами змін(додавання та видалення віртуальних машин, їх переміщення та зміна в середовищі мережі).

Open vSwitch підтримує ряд функцій, які дозволяють мережевій системі реагувати та адаптуватися при будь-яких змінах середовища. Це включає в себе просту підтримку обліку та видимості(NetFlow, IPFIX та sFlow). Але більш корисним є те, що Open vSwitch підтримує базу даних про стан мережі (OVSDDB), яка підтримує віддалені тригери. Тому, частина програмного забезпечення для оркестровки може "спостерігати" різні аспекти мережі та відповідати, коли вони змінюються. Сьогодні це використовується, наприклад, для реагування та відстеження міграцій віртуальних машин.

Open vSwitch також підтримує OpenFlow як метод експортування віддаленого доступу для керування трафіком. Для цього існує безліч застосувань, включаючи глобальне виявлення мережі через перевірку трафіку, відкриття або зв'язку (наприклад, LLDP, CDP, OSPF тощо).

Технічне обслуговування логічних тегів. Розподілені віртуальні комутатори (такі як VMware vDS та Cisco Nexus 1000V) часто підтримують логічний контекст у мережі за рахунок додавання або маніпулювання тегамі в мережеских пакетах. Це може бути використано для унікальної ідентифікації віртуальної машини (у спосіб, стійкий до апаратних спотворень), або для зберігання іншого контексту, який є відповідним лише в логічному домені. Значна частина проблеми з побудовою розподіленого віртуального комутатора полягає в тому, щоб ефективно і правильно керувати цими тегамі.

Open vSwitch включає в себе кілька методів для визначення та підтримки правил позначення, всі з яких доступні для віддаленого процесу для оркестровки. Крім того, у багатьох випадках ці правила додавання тегів зберігаються в оптимізованій формі, тому їх не потрібно поєднувати з важкими мережевими пристроями. Це дозволяє, наприклад, налаштовувати, змінювати та переносити тисячі правил для повторного розміщення тегів або адрес.

Аналогічно, Open vSwitch підтримує реалізацію GRE, яка може обробляти тисячі одночасних тунелів GRE і підтримує віддалену конфігурацію для створення, налаштування та розриву тунелів. Це, наприклад, може бути використане для підключення приватних віртуальних мереж до різних центрів обробки даних.

Апаратна інтеграція. Шлях пересилання в Open vSwitch (вбудований канал передачі даних в ядрі) призначений для «розвантаження» пакетної обробки на апаратні чіпсети, не зважаючи на те, чи розміщено це в класичному корпусі комутуючого обладнання або в мережевому адаптері кінцевого вузла. Це

дозволяє шляху управління (control path) Open vSwitch мати можливість контролювати як чисту реалізацію програмного забезпечення, так і апаратний комутатор.

Перевага апаратної інтеграції - це не тільки продуктивність в віртуалізованих середовищах. Якщо фізичні перемикачі також відображають абстракції управління Open vSwitch, тоді можна управляти як середовищем, так і віртуалізувати хостинг, використовуючи той же механізм автоматичного управління мережею.

Безпека. Open vSwitch надає найвищий рівень безпеки дозволяючи встановлювати політики для віртуальних інтерфейсів VM [2].

LACP і обізнаність про VLAN. Open vSwitch повністю підтримує агрегацію зв'язків LACP і позначку VLAN. Наявна можливість налаштувати один окремий Open vSwitch з безліччю тегів VLAN, тим самим зменшуючи накладні витрати управління безліччю віртуальних мостів для тегів VLAN.

Quality of Service. Повна підтримка QoS або рівнів сервісів.

Моніторинг мережевої середовища. Присутня можливість отримати найвищий рівень управління проходженням пакетів через Open vSwitch шляхом реалізації потужного моніторингу з застосуванням Netflow і sFlow.

IPv6. Open vSwitch повністю підтримує IPv6.

Протокол тунелювання. Open vSwitch має повну підтримку безлічі протоколів тунелювання, наприклад, GRE, VXLAN, STT, IPsec і тому подібних.

Підтримка Proxmox. Open vSwitch повністю інтегрований і підтримується Proxmox, роблячи його життєздатним вибором для настройки віртуальної мережі.

Підсумовуючи вищенаведене бачимо, що багато в чому, Open vSwitch націлюється на іншу точку дизайнерського простору, ніж попередні версії гіпервізорів, зосереджуючи увагу на необхідності автоматичного та динамічного управління мережею у великих середовищах віртуалізації на базі Linux.

Отже метою Open vSwitch є забезпечення мінімального обсягу вбудованого коду (так як це необхідно для продуктивності) та повторне використання існуючих підсистем. Open vSwitch включено як частину ядра і є доступним в більшості популярних дистрибутивів.

Література

1. Open vSwitch Documentation. – 361 с. – (Release 2.9.90).
2. Wasim Ahmed. Mastering Proxmox / Wasim Ahmed. – Birmingham B3 2PB, UK: Packt Publishing Ltd.