

PGDAY'
RUSSIA 17

КОНФЕРЕНЦИЯ
ПО БАЗАМ ДАННЫХ

Гонимые
Станислав
Uniteller

Использован
ие OVS в KVM

Обо мне:

1

Системный администратор

2

Более 15 лет опыта

3

100+ нод виртуализации

4

Платёжные системы

5

Архитектура сетей

6

Веб и не веб приложения

7

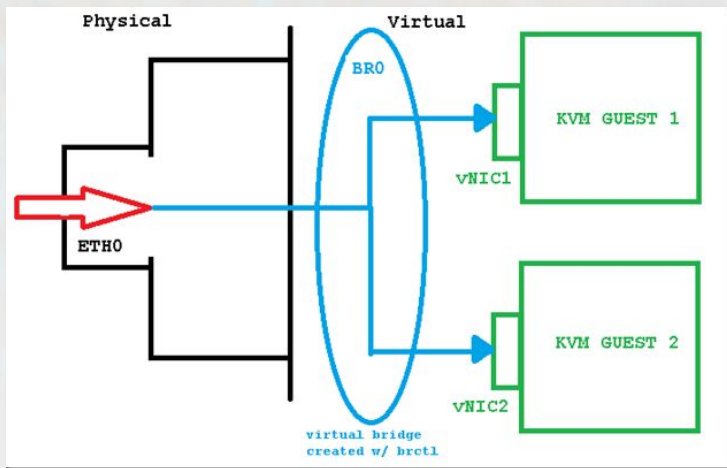
Весело вытащил пару сервисов в девятки

8

Не умею в презентации

OVS vs Linux bridge

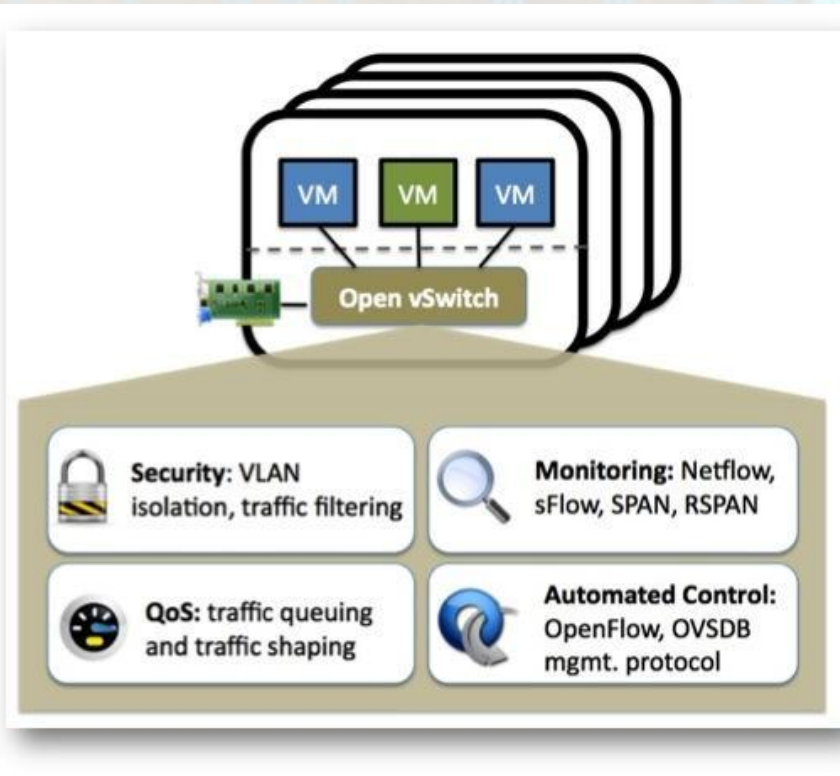
Linux bridge:



- Обычный виртуальный интерфейс основанный на агрегации, либо порте
- Управление через стандартные средства
- Представляет собой HUB
- Перемешивает трафик внутри себя
- Сложности с контролем трафика между VM
- Подключается в KVM как порт.

OVS vs Linux bridge

ovs:



- Представляет собой коммутатор.
- Позволяет изолировать трафик
- Умеет мониторить нагрузку портов из коробки
- Может осуществлять контроль пропускной способности.
- Позволяет сложную коммутацию трафика в рамках ноды.
- Управляется через CLI, OpenFlow, OvsDB
- Подключается в KVM как порт, или группа портов.

Подключение в KVM

Linux bridge:

Virtual Network Interface

Network source: **Мост br0: Устройство хоста em1**

Device model: Мост br1: Устройство хоста vnet1

MAC address: Виртуальная сеть 'default' : NAT

Устройство хоста em1: macvtap

Устройство хоста em2: macvtap

Устройство хоста em3: macvtap

Устройство хоста eth3: macvtap

Общее устройство

OVS:

Virtual Network Interface

Network source: Виртуальная сеть 'test-mgmt' : Сеть Bridge ▼

Portgroup:

Device model: virtio

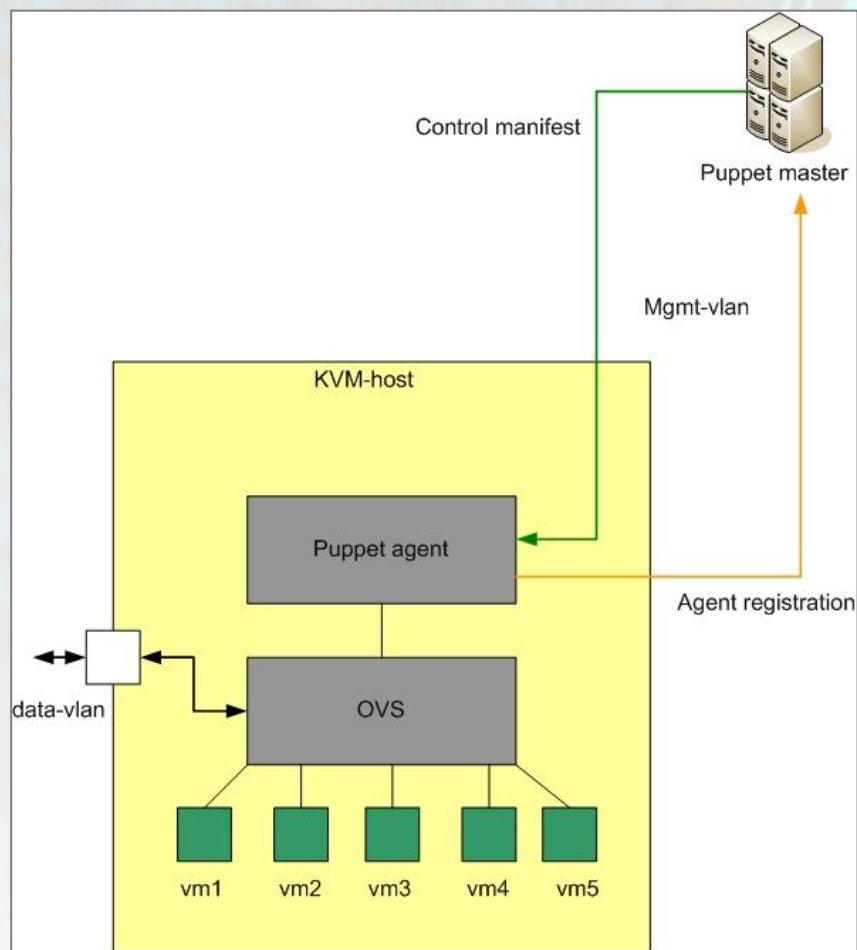
MAC address: 52:54:00:93

mgmt

vpn-mgmt

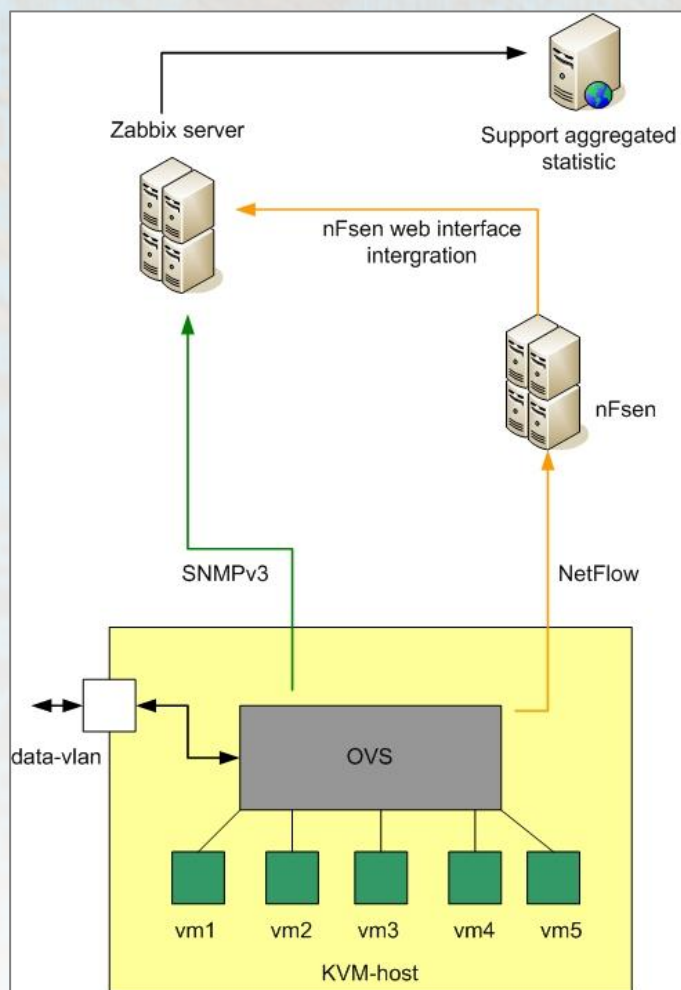
local-mgmp

- Нельзя на лету переключить VLAN интерфейса
- Требуется перезагрузка гостевой системы
- Можно изменить VLAN на лету
- Перезагрузка не требуется



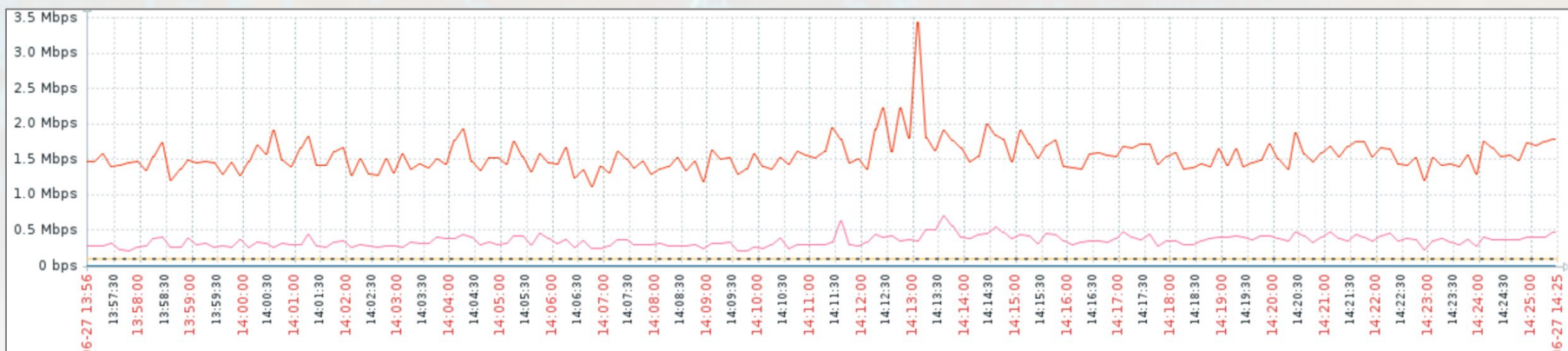
Puppet:

- При первичной регистрации в сети, происходит запрос управляющего манифеста для ноды, либо группы нод.
- Puppet следит за состоянием интерфейсов.
- Централизованное добавление интерфейсов.
- Проверка статуса всех необходимых демонов.
- Проверка статуса ВМ.

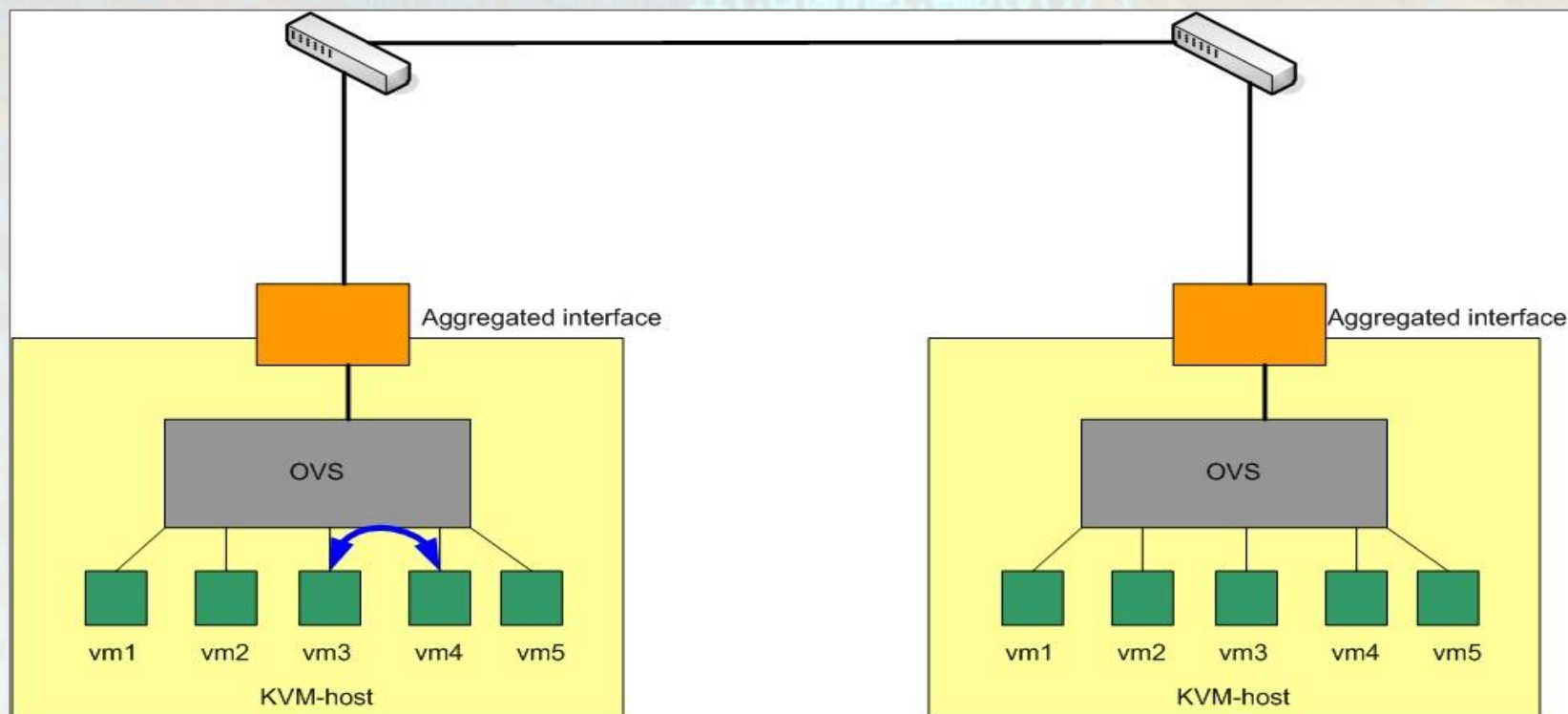


Используя стандартные механизмы мониторинга, мы можем контролировать как загрузку портов на виртуальном коммутаторе в реальном времени, так и делать выборки по типам трафика, или IP отправителя/получателя.

2017-06-27	14:13:00.880	313.932	any	185.38.205.1	1434(21.0)	2433(0.8)	240665(0.1)	7	6132	98
2017-06-27	14:13:13.916	311.364	any	10.11.4.4	700(10.3)	1271(0.4)	114685(0.0)	4	2946	90
2017-06-27	14:13:26.236	288.428	any	10.11.2.100	590(8.6)	757(0.2)	148286(0.1)	2	4112	195
2017-06-27	14:12:51.212	334.928	any	10.11.12.13	468(6.9)	5308(1.7)	1.8 M(0.8)	15	42299	333
2017-06-27	14:13:20.556	281.524	any	192.168.200.236	450(6.6)	827(0.3)	66961(0.0)	2	1902	80
2017-06-27	14:13:17.596	283.164	any	192.168.0.2	376(5.5)	655(0.2)	52192(0.0)	2	1474	79
2017-06-27	14:13:14.664	312.612	any	10.11.4.2	376(5.5)	471(0.2)	39319(0.0)	1	1006	83
2017-06-27	14:13:14.664	312.612	any	192.168.200.205	359(5.3)	359(0.1)	15788(0.0)	1	404	43
2017-06-27	14:12:54.912	332.572	any	185.38.205.2	330(4.8)	1071(0.3)	121303(0.1)	3	2917	113
2017-06-27	14:13:19.140	309.084	any	192.168.0.120	307(4.5)	2075(0.7)	562878(0.2)	6	14568	271

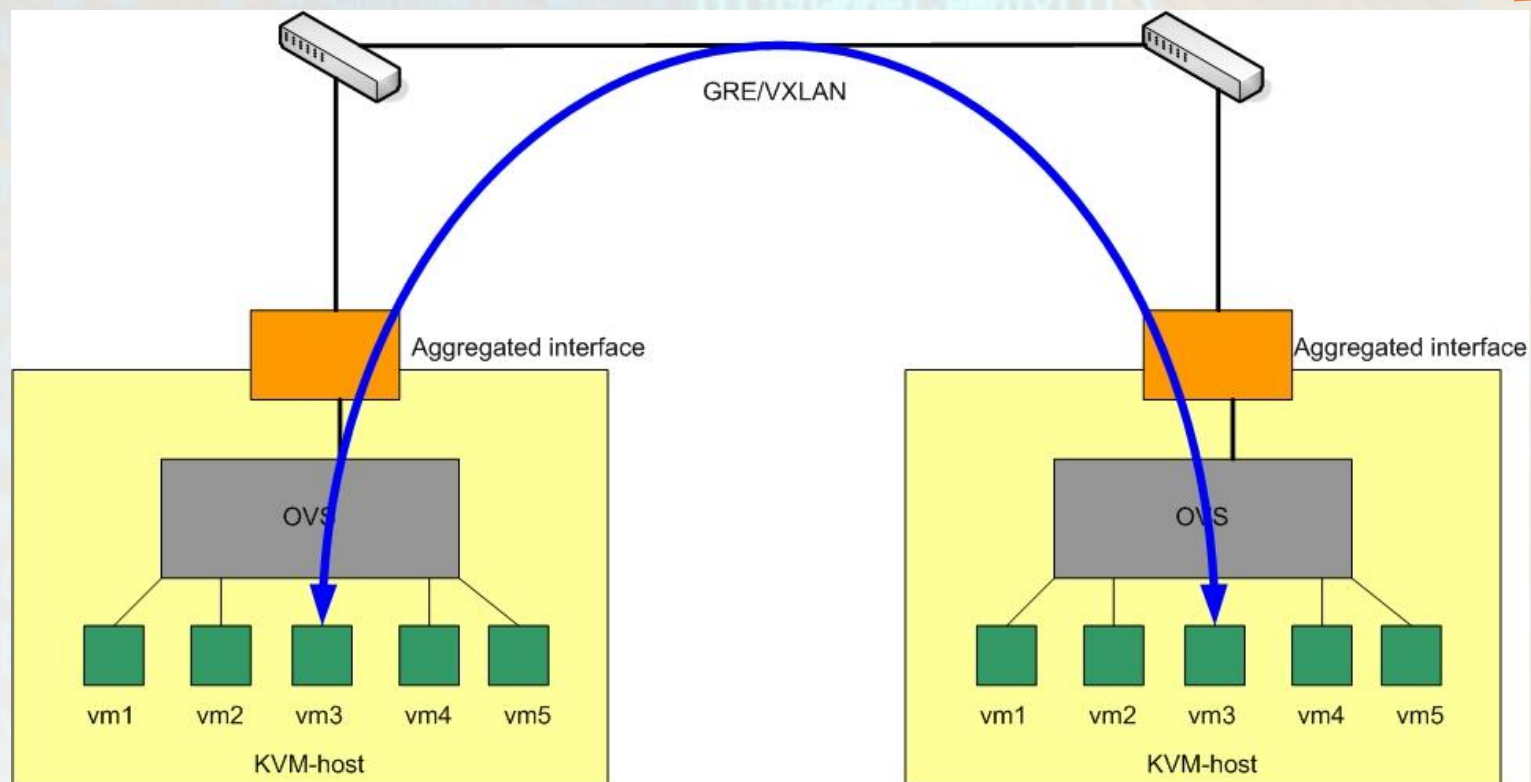


Изоляция и безопасность OVS



Внутренний трафик не достигает физического интерфейса и остальных мостов, если не выходит за пределы гипервизора.

Изоляция и безопасность OVS



Также есть возможность встроенными средствами OVS изолировать трафик, выходящий за пределы гипервизора.

Производительность

Есть множество разных тестов, от комьюнити, или от вендеров, от себя хочу заметить, что в нашей ситуации, OVS позволил добиться ~30% прироста пропускной способности и уменьшения на ~15% задержек на сети, а внутрихостовом соединении пропускная способность выросла на ~30%.

Производительность с VXLAN/IPSec/GRE требует отдельного обсуждения и зависит от инфраструктуры.

Вопросы?

