

АВТОМАТИЗАЦИЯ СЕТИ ЦОД С ПОМОЩЬЮ CONTRAIL ENTERPRISE MULTICLOUD

Антон Антонов

Системный инженер

aantonov@juniper.net

JUNIPER | Summit
NETWORKS

CONFIDENTIALITY AND LEGAL NOTICE

This material contains information that is confidential and proprietary to Juniper Networks, Inc. Recipient may not distribute, copy, or repeat information in the document.

This statement of product direction sets forth Juniper Networks' current intention and is subject to change at any time without notice. No purchases are contingent upon Juniper Networks delivering any feature or functionality depicted in this presentation.

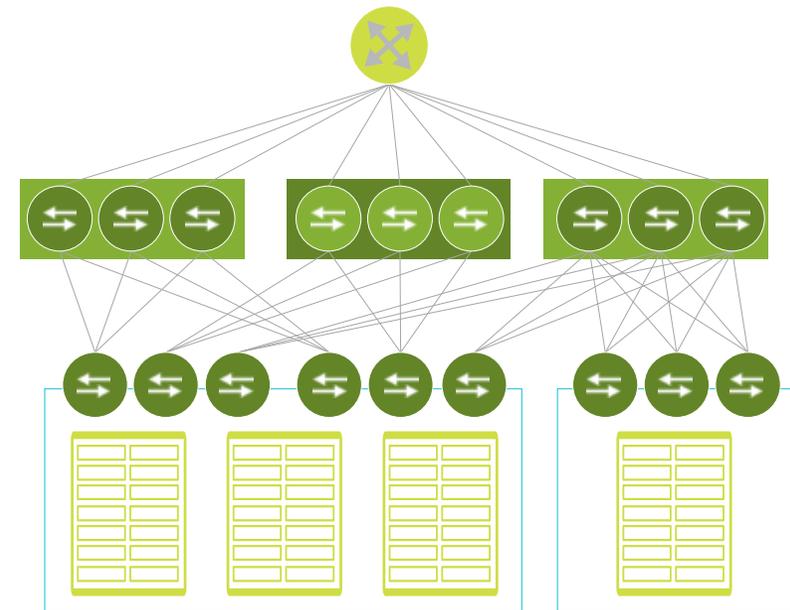
Conrail program participants are subject to a license agreement that describes program terms and conditions.

СЕТЬ ЦОД

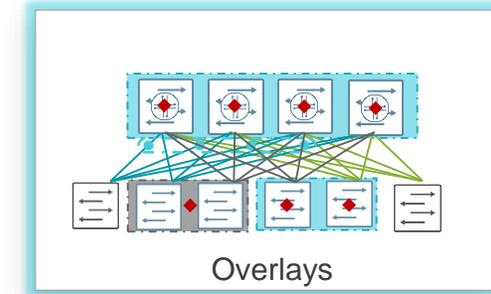
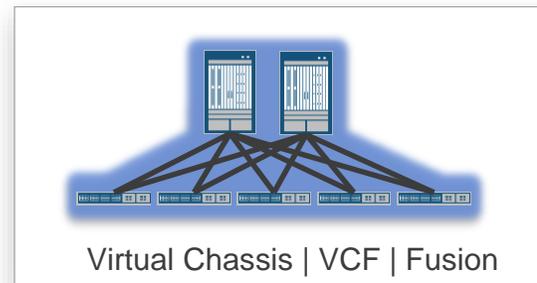
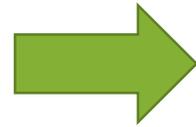
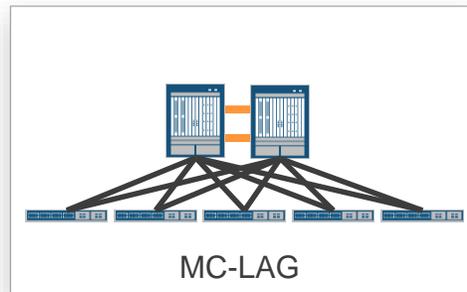
Сеть ЦОД (data center network) – это устройства и связи между ними, которые обеспечивают коммуникацию для всех ресурсов ЦОД (серверы, сетевые функции, маршрутизаторы и т.д.).

Требования к сети ЦОД:

- Отказоустойчивость
- Масштабируемость
- Простота управления
- Эффективное использование ресурсов



ЭВОЛЮЦИЯ СЕТИ ЦОД



Legacy Layer 2

- Ограниченная масштабируемость
- Сложное управление
- Проприетарное решение
- Ограниченная функциональность

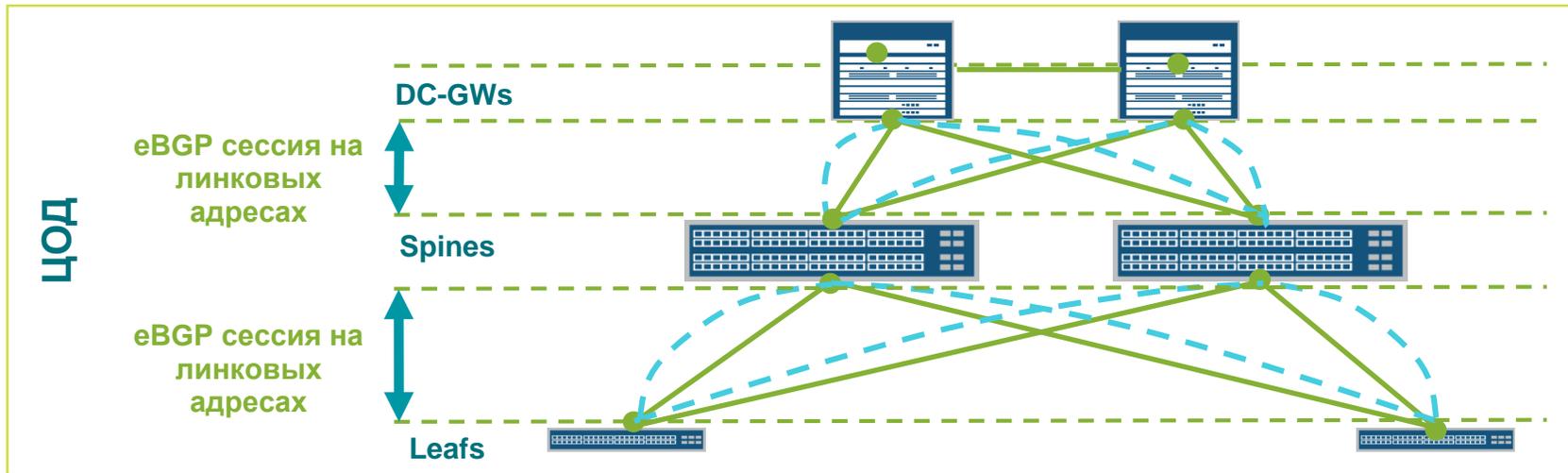
Ethernet Fabric

- Ограниченная масштабируемость
- Простое управление
- Проприетарное решение
- Ограниченная функциональность

IP Fabric

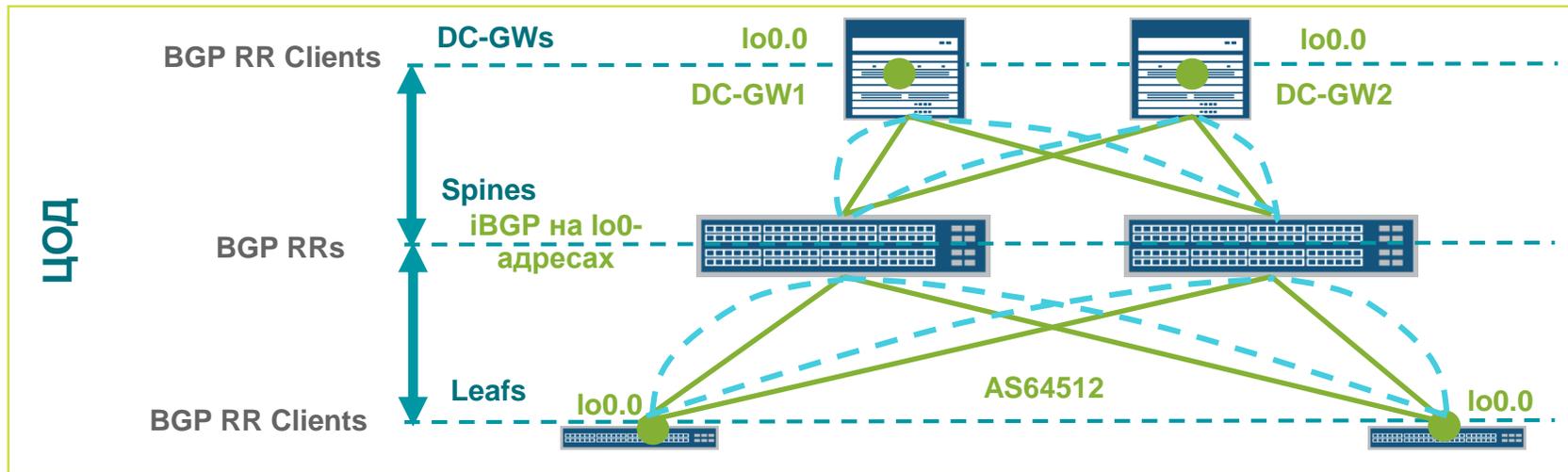
- Широкие возможности масштабирования
- Простое управление
- Решение построено на открытых стандартах
- Гибкая функциональность

МАРШРУТИЗАЦИЯ В UNDERLAY



- Протокол маршрутизации для underlay - **eBGP**
 - ✓ Встроенные механизмы предотвращения петель (AS_PATH). Каждый leaf/spine в отдельной AS
 - ✓ Встроенная поддержка большого числа маршрутов и пиров
 - ✓ Унифицированный протокол для DC и WAN
 - ✓ Гибкий механизм управления трафиком через манипуляцию атрибутами BGP (например, чтобы перенести трафик со spine на время плановых работ можно использовать AS-path prepend или communities)
- Другие варианты:
 - ✓ iBGP – можно использовать add-path и роут-рефлекторы, но вырастет сложность
 - ✓ IGP (OSPF/ISIS) - узкие места: размер LSDB и отсутствие гибких механизмов управления распространения маршрутов

МАРШРУТИЗАЦИЯ В OVERLAY



- Протокол BGP EVPN/VXLAN
 - ✓ Хорошо масштабируется (миллионы маршрутов)
 - ✓ Возможность гибкой настройки политик
- Изучение MAC-адресов в Control Plane
 - ✓ Снижается unknown unicast flooding
 - ✓ Снижается ARP Flooding
 - ✓ Быстрая сходимость
- Поддержка функциональности L3VPN
 - ✓ Используется VXLAN для транспорта вместо MPLS
- Передача трафика по всем активным путям
 - ✓ Использование нескольких путей при передаче трафика в IP-фабрике
 - ✓ Использование нескольких путей при передаче трафика к/от клиентскому хосту (active/active dual-homed device)
- Распределенный Layer 3 gateway

ПОЧЕМУ НЕОБХОДИМ CONTROLLER

- Настройка сетевых устройств с помощью проверенных темплейтов
 - ✓ Исключение риска случайной ошибки
 - ✓ Конфигурация всех устройств консистентна и не зависит от квалификации инженера
- Детали настройки конкретного устройства скрыты от верхнеуровневой системы
 - ✓ Возможность быстрой интеграции с различными оркестраторами
- Использование простых абстракций для управления сложным составным сервисом
 - ✓ Сокращается время создания/модификации/удаления сервиса
- Intend-based Networking
 - ✓ Администратор задает конечное состояние системы, а не последовательность операций
- Функции Element Management System:
 - ✓ Автоконфигурация
 - ✓ Обновление ПО
 - ✓ Мониторинг
 - ✓ Аналитика
 - ✓ Визуализация топологии и сервиса

CONTRAIL ENTERPRISE MULTICLOUD (CEM)



Contrail Enterprise Multicloud
(включает Contrail Networking,
Contrail Security & Appformix)

Contrail Security – Оркестрация политик безопасности в мультиоблаке

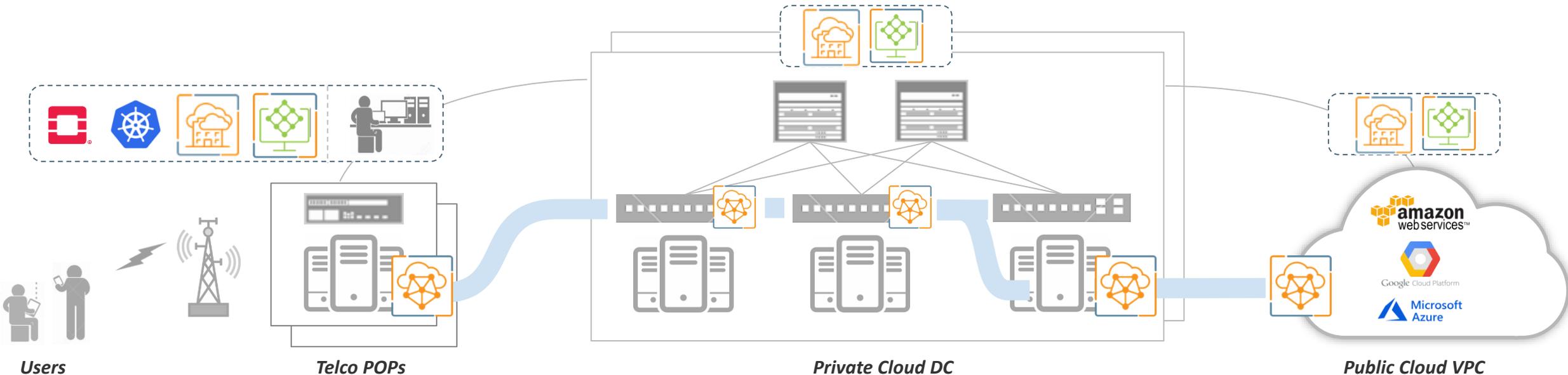
Appformix – Мониторинг и аналитика

Contrail Networking

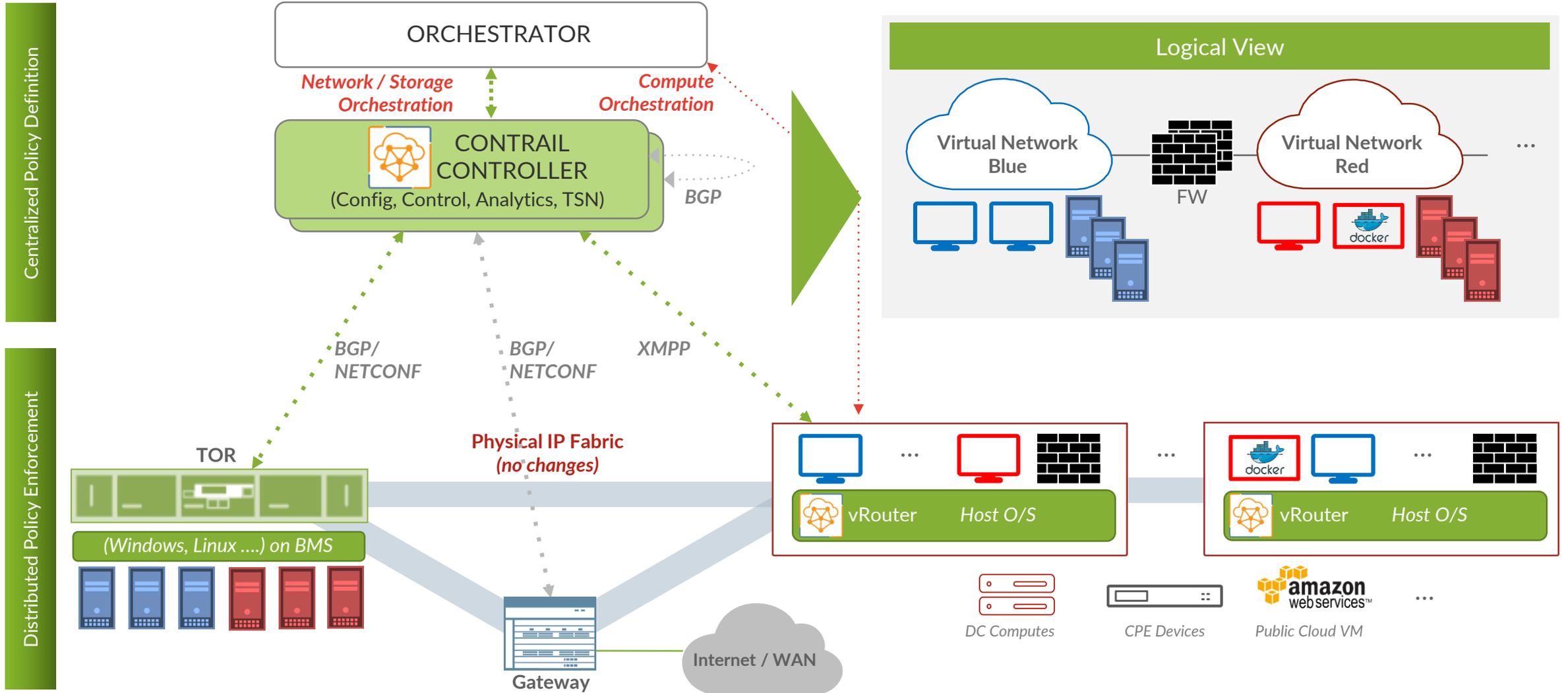
Virtual Networking: виртуальные overlay сети для сетевой связности между VM/Containers

Fabric Automation: управление сетевыми устройствами ЦОД и BMS (автоматизация в underlay and overlay), сетевая связность между VM/Containers и физическими BMS, PNF

Multicloud Automation: сетевая связность между виртуальными сетями частного ЦОД/облака и публичного облака



АРХИТЕКТУРА CONTRAIL ENTERPRISE MULTICLOUD



КЛЮЧЕВАЯ ФУНКЦИОНАЛЬНОСТЬ КОНТРОЛЛЕРА ФАБРИКИ В СОСТАВЕ CONTRAIL

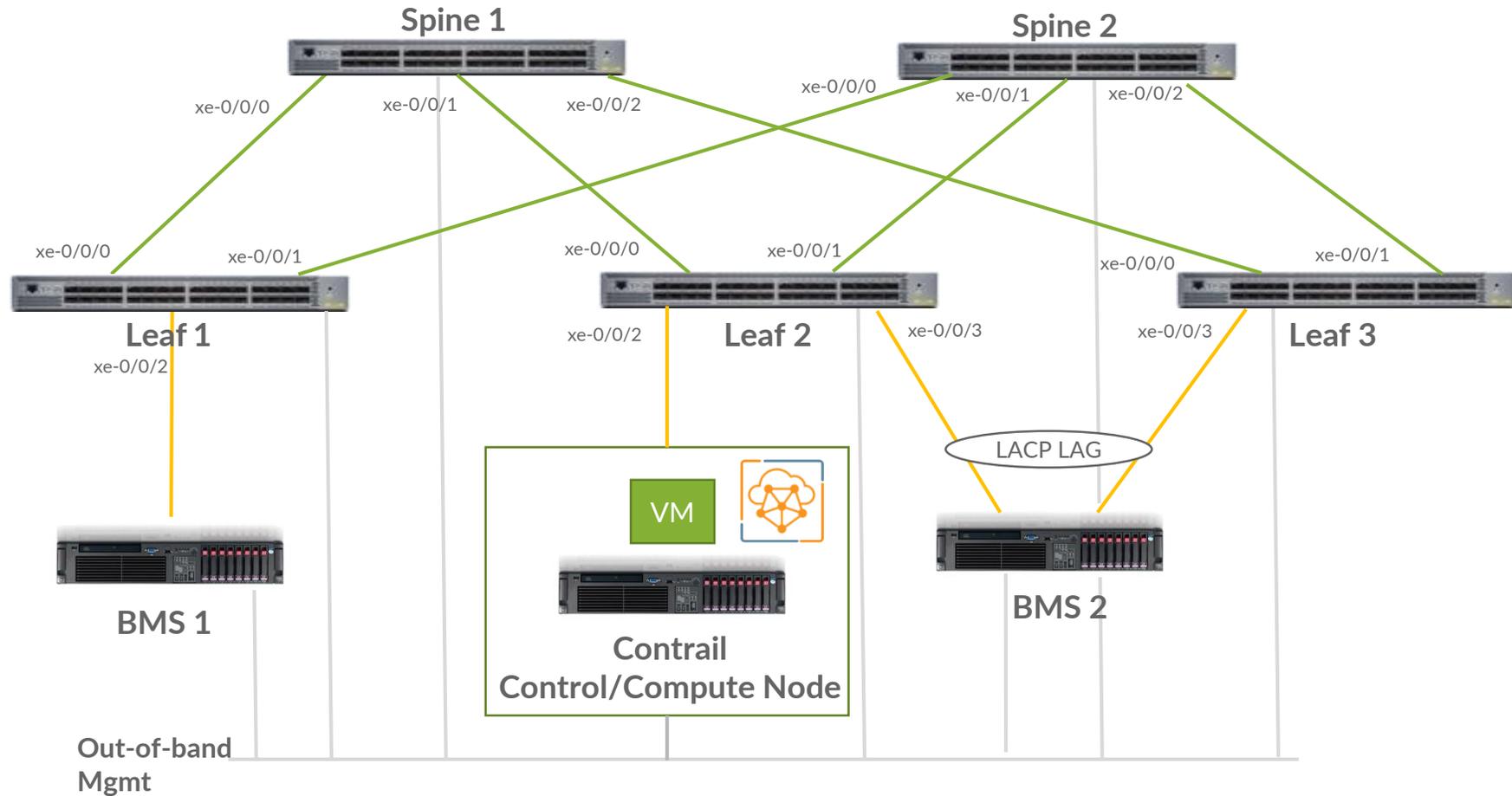
- Демо ➡ • Автообнаружение сетевых устройств IP-фабрики
- Демо ➡ • Автоконфигурация устройств на основе заданных ролей
 - Автоматическое обновление ПО
 - Активация maintenance-режима
 - Управление несколькими IP-фабриками
 - DC Interconnect
- Демо ➡ • Управление overlay-подсетями
- Демо ➡ • Управление профилями access-портов leaf-коммутаторов
 - Подключение BMS-серверов к фабрике
- Демо ➡ • Интерфейс управления виртуальными машинами
 - Role-based access
- Демо ➡ • Мониторинг и аналитика
- Демо ➡ • Визуализации топологии
- Демо ➡ • Интеграция с Openstack, Openshift, Kubernetes и другими оркестраторами
- Демо ➡ • Бесшовная маршрутизация между физическими и виртуальными компонентами фабрики
- Демо ➡ • BGP пиринг с устройствами ЦОД и внешними устройствами
 - и многое другое



Демонстрация управления IP-фабрикой с помощью Contrail Enterprise Multicloud

СХЕМА ЛАБОРАТОРИИ

- 2 x Spine
- 3 x Leaf
- 2 x BMS
- Contrail

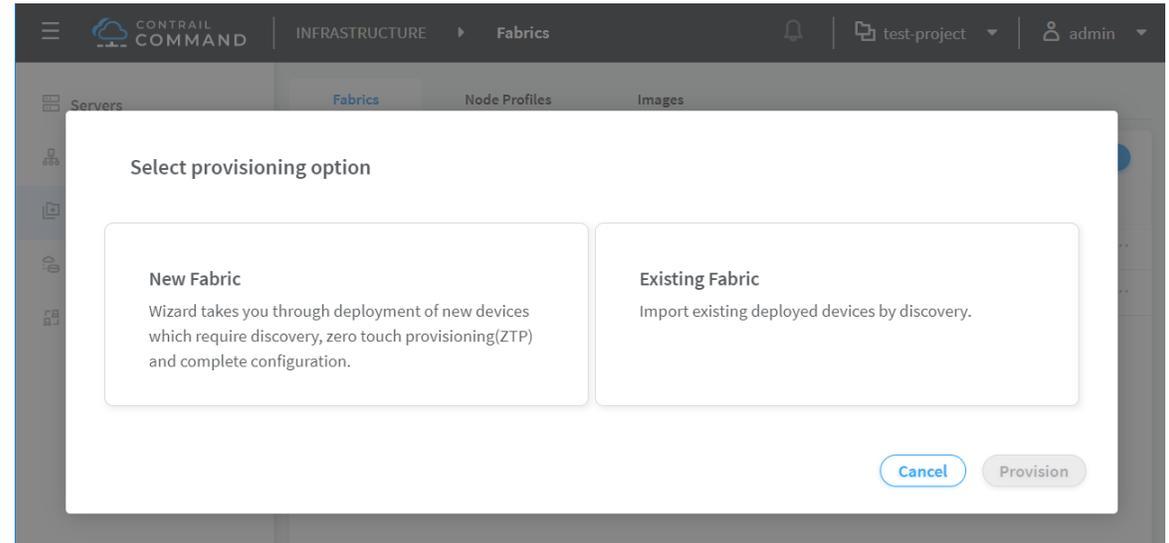


АВТОКОНФИГУРАЦИЯ IP-ФАБРИКИ (ZTP)

New Fabric (конфигурация на устройствах отсутствует)

Параметры:

- Имя фабрики
- Пароль для пользователя root
- Сеть управления
- Overlay ASN
- Диапазон underlay ASN
- Underlay-подсеть
- Подсеть для lo0-адресов
- Добавить серийные номера устройств в yml-файл



Existing Fabric (underlay преднастроен)

Параметры:

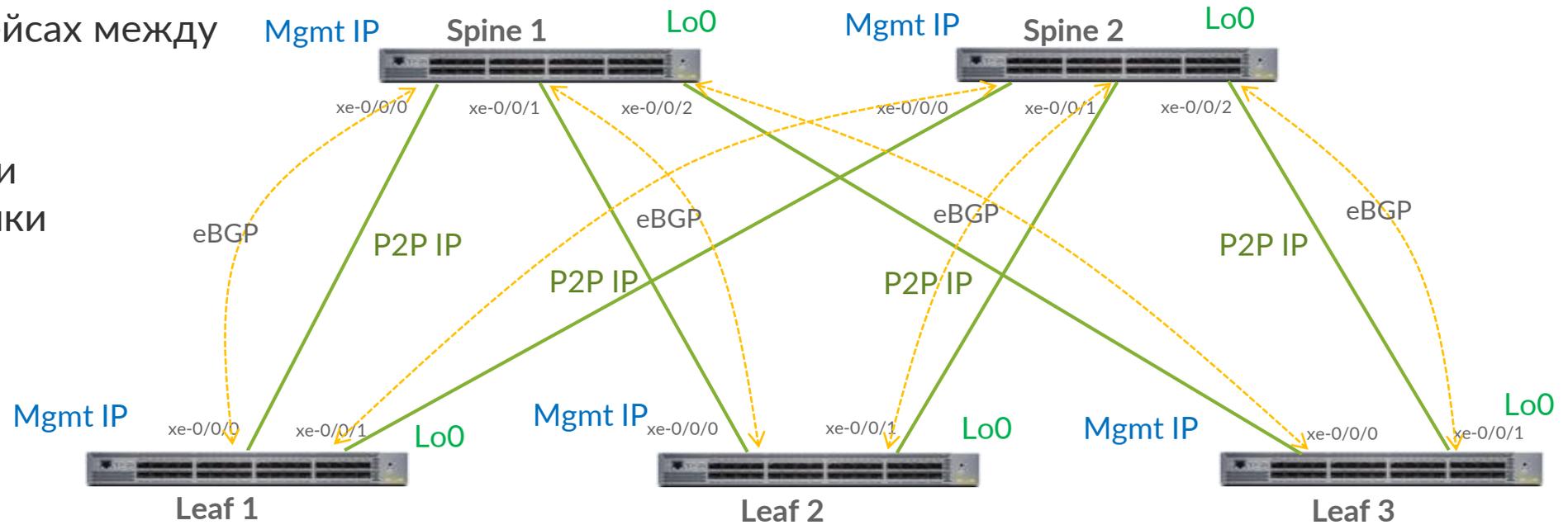
- Подсеть управления
- Пароль для пользователя root
- Overlay ASN
- Подсеть для lo0-адресов



```
supplemental_day_0_cfg:
  - name: "cfg"
  - cfg: |
      set system ntp server 10.0.0.32
      set interfaces em1 unit 0 family inet address 169.254.0.2/24
      set routing-options static route 0.0.0.0/0 next-hop 10.0.0.1
device_to_ztp:
  - serial_number: "85167200811"
    supplemental_day_0_cfg: "cfg"
    hostname: "spine1"
  - serial_number: "83431016507"
    supplemental_day_0_cfg: "cfg"
    hostname: "spine2"
```

АВТОКОНФИГУРАЦИЯ UNDERLAY

- IP адреса на интерфейсах управления
- IP адреса на интерфейсах между устройствами
- Loopback-адреса
- Underlay eBGP-сессии
- Import/export политики



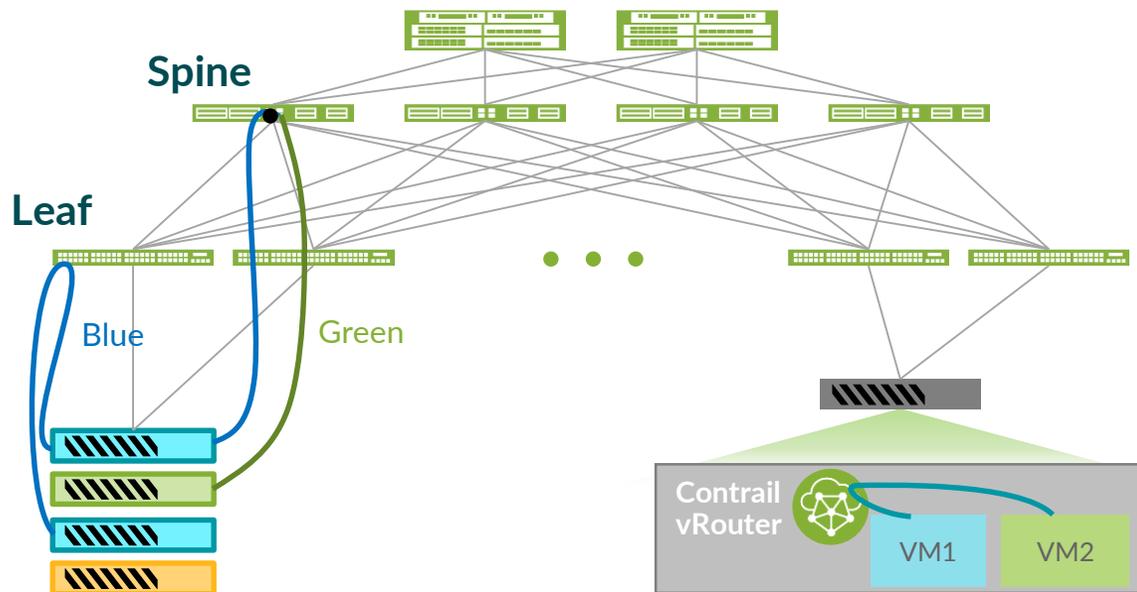
АВТОКОНФИГУРАЦИЯ UNDERLAY (VIDEO)

```
C:\Users\aaantonov\Documents\MyFabric\devices.yml - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
devices.yml
1 supplemental_day_0_cfg:
2   - name: "cfg"
3     cfg: |
4       set system ntp server 10.0.0.32
5       set interfaces em1 unit 0 family inet address 169.254.0.2/24
6       set routing-options static route 0.0.0.0/0 next-hop 10.0.0.1
7 device_to_ztp:
8   - serial_number: "87304045641"
9     supplemental_day_0_cfg: "cfg"
10    hostname: "spine1"
11   - serial_number: "40446081277"
12    supplemental_day_0_cfg: "cfg"
13    hostname: "spine2"
14   - serial_number: "37004265743"
15    supplemental_day_0_cfg: "cfg"
16    hostname: "leaf1"
17   - serial_number: "71724676010"
18    supplemental_day_0_cfg: "cfg"
19    hostname: "leaf2"
20   - serial_number: "71006004155"
21    supplemental_day_0_cfg: "cfg"
22    hostname: "leaf3"
YAML Ain't Markup Language length: 684 lines: 22 Ln: 1 Col: 7 Sel: 0 | 0 Unix (LF) UTF-8 INS
```

АРХИТЕКТУРЫ OVERLAY СЕТЕЙ В EVPN-VXLAN ФАБРИКЕ

CENTRALLY ROUTED BRIDGING (CRB)

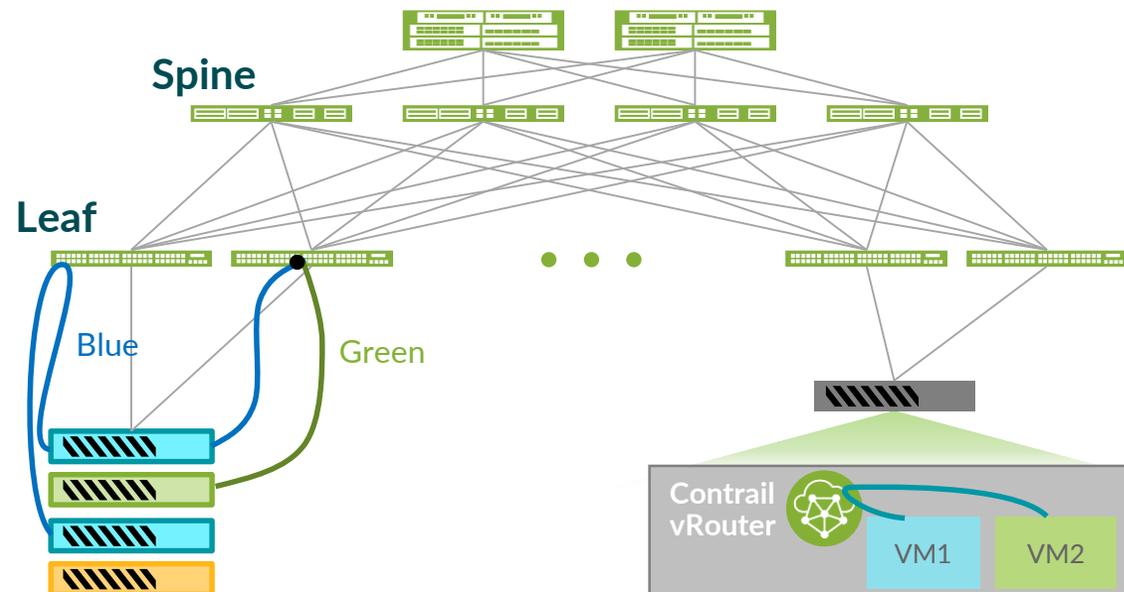
- Маршрутизация между overlay-сетями на уровне Spine
- L2-коммутация внутри overlay-сети на уровне Leaf



- ✓ Большая часть трафика в направлении north-south
- ✓ Низкая степень сегментации трафика
- ✓ Отсутствует автоматизация для управления IP-VRF
- ✓ Leaf-коммутаторы не поддерживают VXLAN Routing

EDGE ROUTED BRIDGING (ERB)

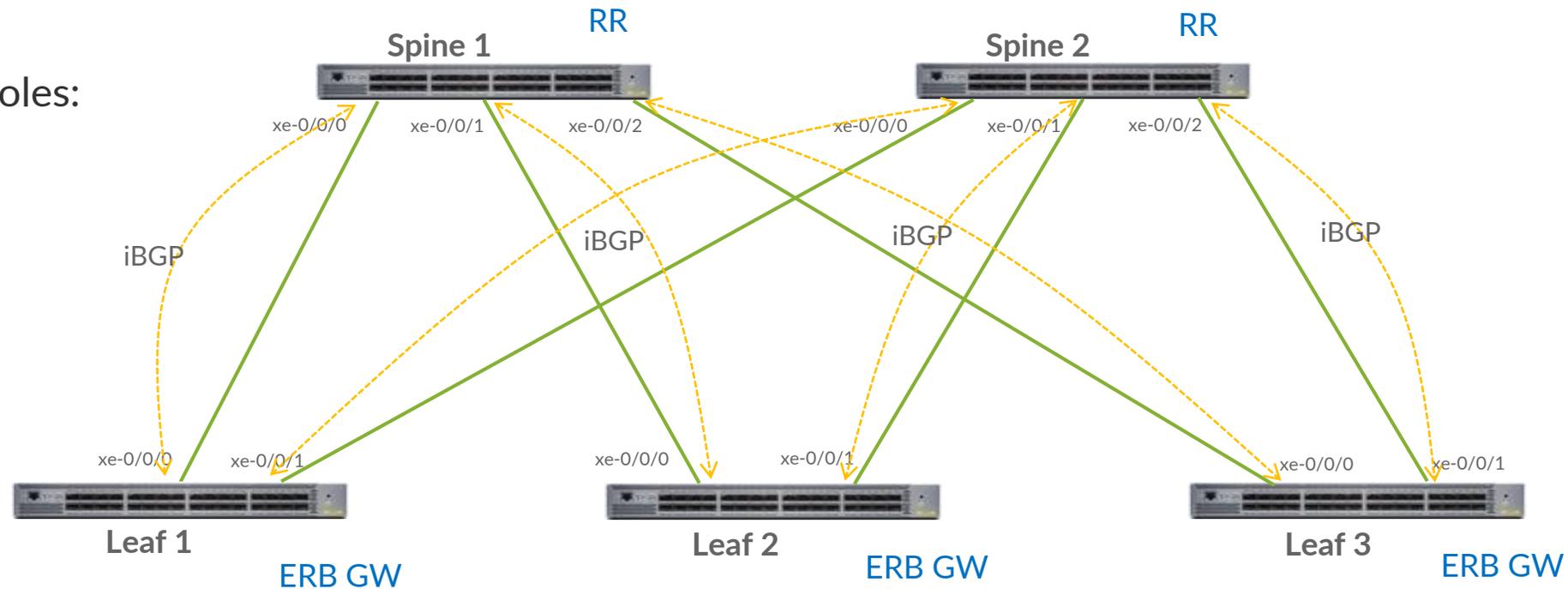
- Маршрутизация и коммутация для overlay-сетей выполняются на уровне Leaf



- ✓ Большая часть трафика в направлении east-west
- ✓ Высокая степень сегментации трафика
- ✓ Управление IP-VRF автоматизировано (Contrail)
- ✓ Leaf-коммутаторы поддерживают VXLAN Routing

АВТОКОНФИГУРАЦИЯ OVERLAY

- Назначение физических ролей:
 - ✓ Leaf
 - ✓ Spine
- Назначение логических ролей:
 - ✓ Route Reflector
 - ✓ ERB
 - ✓ CRB GW
 - ✓ CRB Access
 - ✓ PNF
 - ✓ DC-GW
 - ✓ DCI
 - ✓ и другие



АВТОКОНФИГУРАЦИЯ OVERLAY (VIDEO)

Contrail Command

172.30.129.39:9091/#/contrail_command/infrastructure/fabrics/instances/create/new

CONTRAIL COMMAND | INFRASTRUCTURE > Fabrics > Create Fabric

admin | admin

STEP 1 Create Fabric | **STEP 2 Device discovery** | STEP 3 Assign the roles | STEP 4 Autoconfigure

Discovered devices

<input type="checkbox"/>	NAME	MANAGEMENT IP	PRODUCT NAME	STATUS	INTERFACES	
<input type="checkbox"/>	leaf1	10.0.0.11	vqfx-10000	ONBOARDED	13	...
<input type="checkbox"/>	leaf2	10.0.0.7	vqfx-10000	ONBOARDED	13	...
<input type="checkbox"/>	leaf3	10.0.0.10	vqfx-10000	ONBOARDED	13	...
<input type="checkbox"/>	spine1	10.0.0.2	vqfx-10000	ONBOARDED	13	...
<input type="checkbox"/>	spine2	10.0.0.4	vqfx-10000	ONBOARDED	13	...

No items selected

Device discovery progress

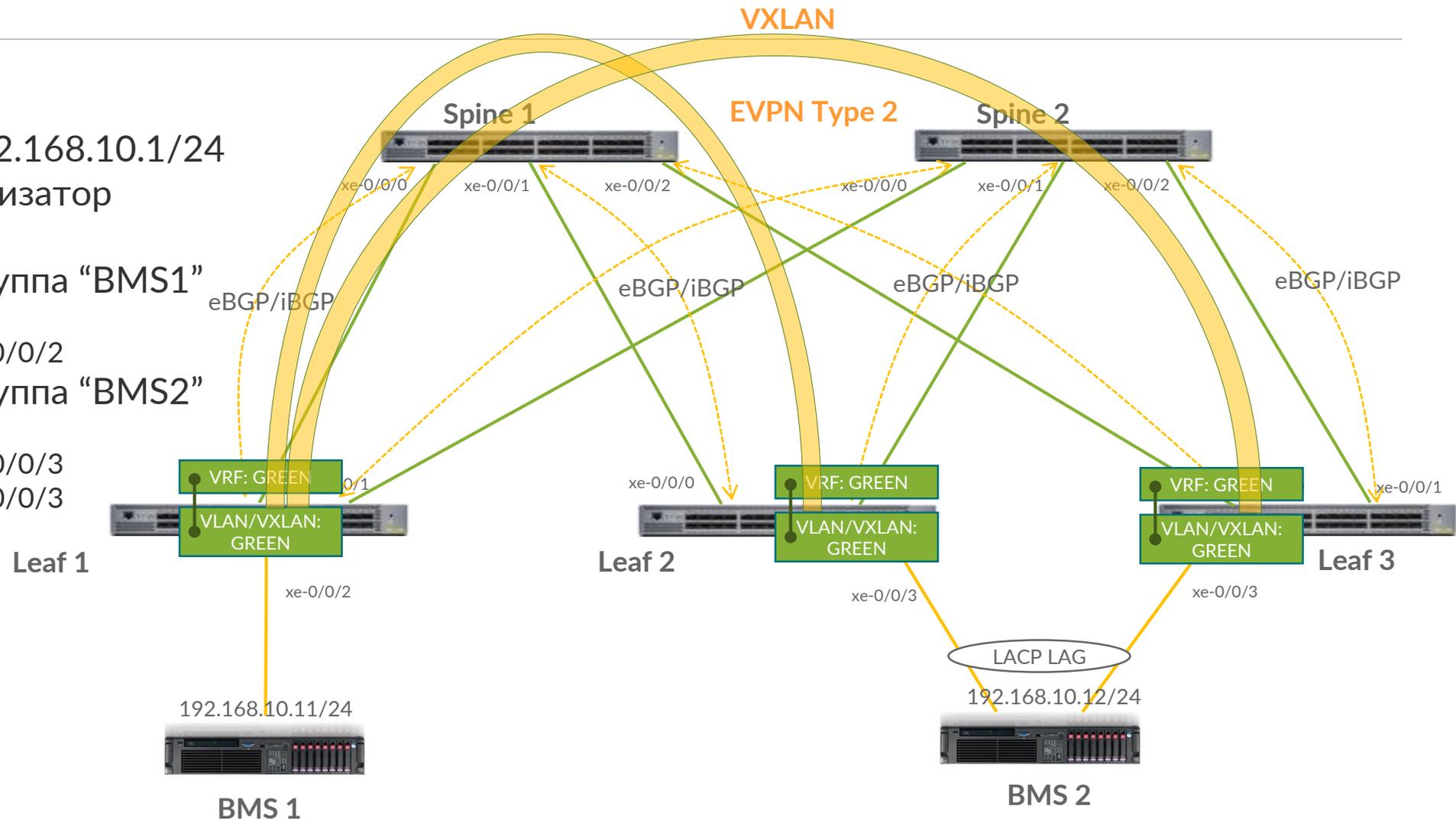
Fri Oct 04 2019 11:48:09 GMT+0300 (Moscow Standard Time)
Job summary: Job execution completed successfully. Detailed job results:
Successfully completed job for 5 devices.
Completed playbook execution for job template "fabric_onboard_template" with execution id "1570178506566_c6854c1f-12c4-4ea8-9cd9-d75f64f7376b"

Previous | **Next** | Cancel

OVERLAY СЕТЬ ДЛЯ BMS

L2-СВЯЗНОСТЬ

- Виртуальная сеть
“VN_Green”: 192.168.10.1/24
- Логический маршрутизатор
LR_Green
- Виртуальная порт-группа “BMS1”
 - VN_Green
 - Phys device: Leaf1:xe-0/0/2
- Виртуальная порт-группа “BMS2”
 - VN_Green
 - Phys device: Leaf2:xe-0/0/3
 - Phys device: Leaf3:xe-0/0/3



OVERLAY СЕТЬ ДЛЯ VMS (VIDEO)

L2-СВЯЗНОСТЬ

Contrail Command

AppFormix

Not secure | 172.30.129.39:9091/#/contrail_command/infrastructure/fabrics/instances/details/4c02f570-9bae-41a8-a2f9-a1355150829f/fabric-devices-graph

admin admin

Servers

Cluster

Fabrics

Multi Cloud

Networks

INFRASTRUCTURE

Monitoring

Dashboards

Contrail Cluster

Alarms

Infrastructure

Servers

Cluster

Fabrics

Multi Cloud

Networks

Overlay

Virtual Networks

Virtual Port Group

Network Policies

Multicast Policies

Logical Routers

Security Groups

Floating IPs

IPAM

Routing

Virtual Ports

DCI

Port Profiles

Workloads

Instances

Flavors

Images

SSH Keys

Debug

Introspect

Object Logs

IAM

Domains

Projects

Users

RBAC

Services

Catalog

Deployments

BGPaaS

Health Check

Appliances

Load Balancers

Security

Insights

Tags

Service Groups

Address Groups

Policies

Policy Sets

Security Logging Object

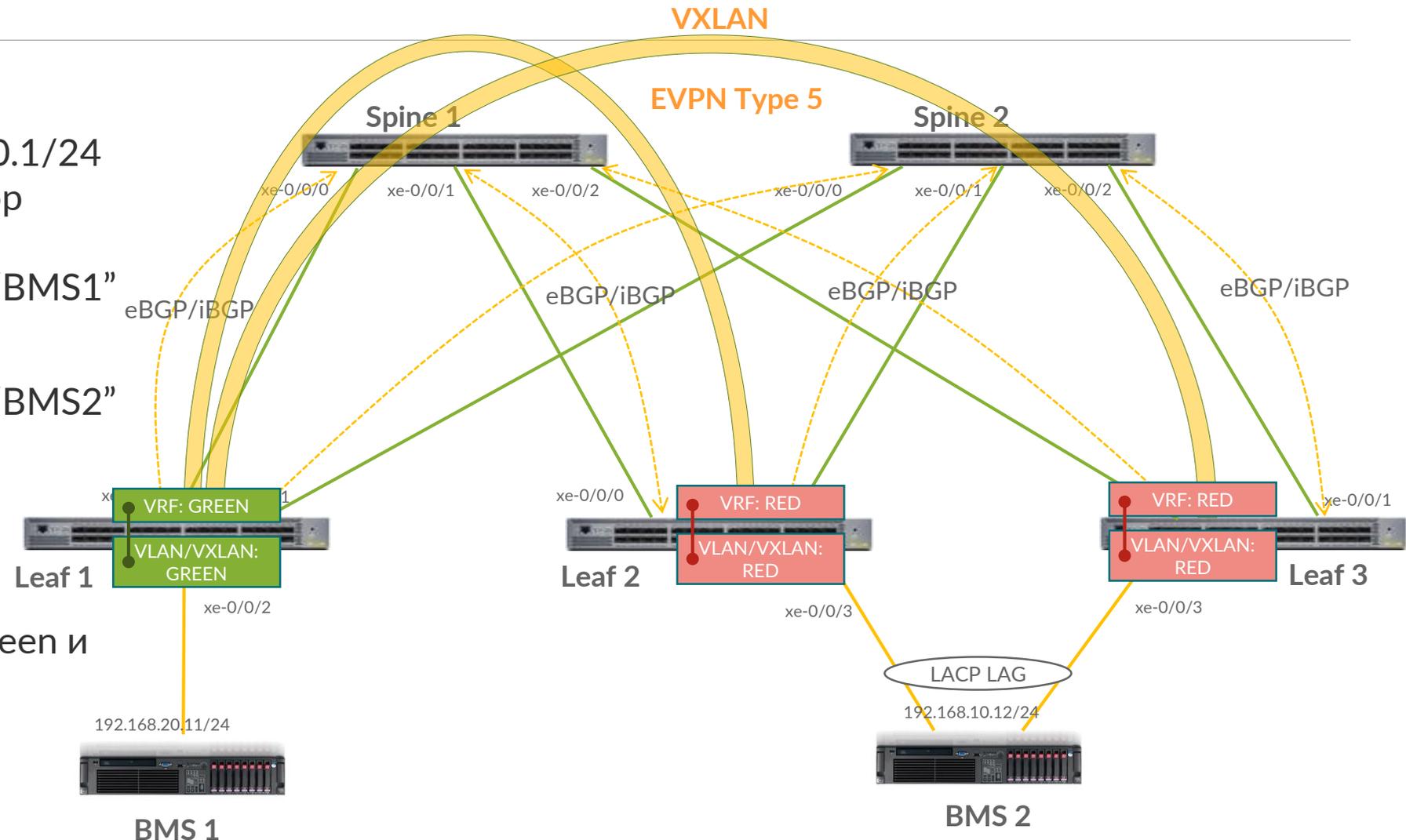
External Applications: APPFORMIX

10.0.0.41

OVERLAY СЕТЬ ДЛЯ BMS

L3-СВЯЗНОСТЬ

- Виртуальная сеть
“VN_Red”: 192.168.20.1/24
- Логический маршрутизатор
LR_Red
- Виртуальная порт-группа “BMS1”
 - VN_Green
 - Phys device: Leaf1:xe-0/0/2
- Виртуальная порт-группа “BMS2”
 - VN_Red
 - Phys device: Leaf2:xe-0/0/3
 - Phys device: Leaf3:xe-0/0/3
- Маршрутизация между Green и Red
 - LR_Green
 - LR_Red

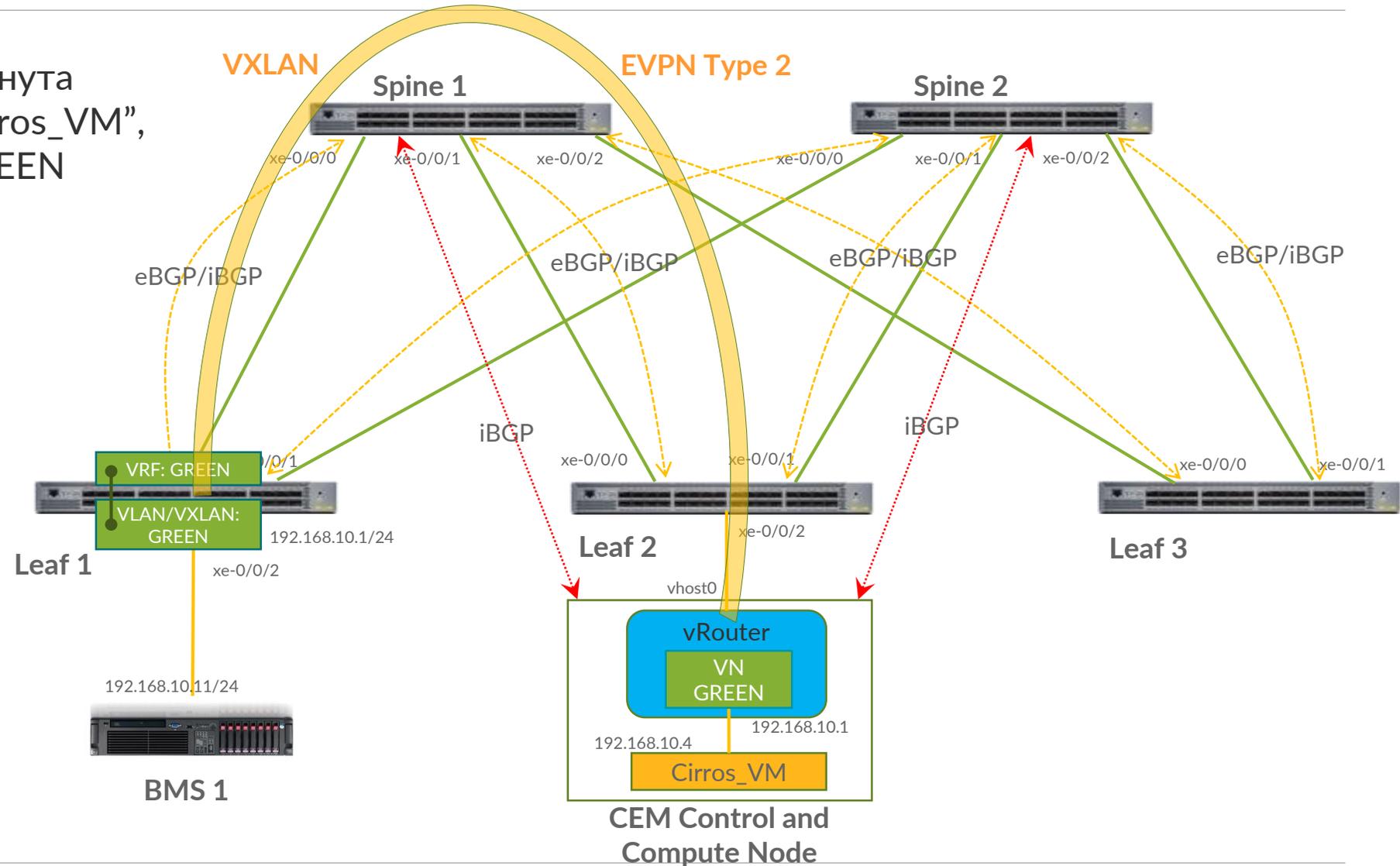


OVERLAY СЕТЬ ДЛЯ VMS (VIDEO) L3-СВЯЗНОСТЬ

The screenshot displays the Contrail Command web interface. The browser address bar shows the URL: `172.30.129.39:9091/#/contrail_command/overlay/virtual-port-groups`. The interface features a dark sidebar on the left with the 'CONTRAIL COMMAND' logo and a list of navigation items: Virtual Networks, Virtual Port Group (highlighted), Network Policies, Multicast Policies, Logical Routers, Security Groups, Floating IPs, IPAM, Routing, Virtual Ports, DCI, and Port Profiles. The main content area is titled 'OVERLAY' and contains a grid of menu items categorized into Monitoring, Infrastructure, Overlay, Workloads, IAM, Services, Security, Debug, and DNS. The 'Virtual Port Group' item under the 'Overlay' category is highlighted. At the bottom of the sidebar, there is a section for 'External Applications' with the 'APPFORMIX' logo. On the right side, a modal window is partially visible, showing a 'Create' button and a list of items including 'VIRTUAL NETWORK', 'N_Green', and 'N_Controller'.

СЕТЕВАЯ СВЯЗНОСТЬ МЕЖДУ BMS И VM

- На Compute Node развернута виртуальная машина "Cirros_VM", подключенная к сети GREEN



СЕТЕВАЯ СВЯЗНОСТЬ МЕЖДУ VMS И VM - VIDEO

The screenshot displays the Contrail Command web interface. The browser address bar shows the URL `172.30.129.39:9091/#/contrail_command/overlay/logical_routers`. The interface features a dark sidebar on the left with the 'CONTRAIL COMMAND' logo and a main content area with a grid of menu items. The 'Logical Routers' item in the sidebar is highlighted. The main content area shows a grid of categories including Monitoring, Infrastructure, Overlay, Workloads, IAM, Services, Security, Debug, and DNS. The 'Logical Routers' item under the 'Overlay' category is selected and highlighted. At the bottom of the main content area, there is a section for 'External Applications' with the 'APPFORMIX' logo.



Contrail Northbound API

NORTHBOUND API

← → ↻ 🔒 Not secure | 172.30.129.39:9091/doc#operation--contrail-webui-node--id--put

- GET /dashboard/{id}
- PUT /dashboard/{id}
- DELETE /dashboard/{id}
- GET /dashboards
- POST /dashboards
- GET /data-center-intercon...
- PUT /data-center-intercon...
- DELETE /data-center-inte...
- GET /data-center-intercon...
- POST /data-center-interco...
- GET /database-node/{id}
- PUT /database-node/{id}
- DELETE /database-node/...
- GET /database-nodes
- POST /database-nodes
- GET /device-image/{id}
- PUT /device-image/{id}
- DELETE /device-image/{id}
- GET /device-images
- POST /device-images
- GET /devicemgr-node/{id}
- PUT /devicemgr-node/{id}
- DELETE /devicemgr-node...
- GET /devicemgr-nodes
- POST /devicemgr-nodes
- GET /discovery-service-a...
- PUT /discovery-service-as...
- DELETE /discovery-servic...
- GET /discovery-service-a...
- POST /discovery-service-...
- GET /domain/{id}
- PUT /domain/{id}
- DELETE /domain/{id}

GET /data-center-interconnect/{id}

REQUEST PARAMETERS

id: string (no description)
required
in path

RESPONSES

200 OK	Show resource
DataCenterInterconnectAPISingleType	
401 Unauthorized	Unauthorized
404 Not Found	Resource not found
500 Internal Server Error	Server Side Error

Response Example (200 OK)

```
{
  "data-center-interconnect": {
    "annotations": {
      "key_value_pair": [
        {
          "key": "string",
          "value": "string"
        }
      ]
    },
    "configuration_version": "integer",
    "data_center_interconnect_bgp_address_families": {
      "family": [
        "string"
      ]
    },
    "data_center_interconnect_bgp_hold_time": "integer",
    "data_center_interconnect_configured_route_target_list": {
      "route_target": [
        "string"
      ]
    },
    "data_center_interconnect_mode": "string",
    "display_name": "string",
    "fq_name": [
      "string"
    ],
    "href": "string",
    "id_perms": {
      "created": "string",
      "creator": "string",
      "description": "string",
      "enable": "boolean",
      "last_modified": "string",
```

NORTHBOUND API: НАСТРОЙКА VIRTUAL PORT GROUP (VPG)

Создаем Virtual Port Group

```
# curl -s -X POST -H "X-Auth-Token: $TOKEN" -H "Content-Type: application/json" -d @vpg-create.json http://10.0.0.32:8082/virtual-port-groups
```

Название фабрики

Название VPG

```
# cat vpg-create.json
{"virtual-port-group": {"display_name": "VPG_REST_API_Test", "fq_name": ["default-global-system-config", "myfabric", "VPG_REST_API_Test"], "parent_type": "fabric"}}
```

Создаем Virtual Interface

```
# curl -s -X POST -H "X-Auth-Token: $TOKEN" -H "Content-Type: application/json" -d @vmi-create.json http://10.0.0.32:8082/virtual-machine-interfaces
```

Название VMI

```
# cat vmi-create.json
{"virtual-machine-interface": {"display_name": "VPG_REST_API_Test-100", "fq_name": ["default-domain", "admin", "VPG_REST_API_Test-100"], "name": "VPG_REST_API_Test-100", "parent_type": "project", "virtual_machine_interface_bindings": {"key_value_pairs": [{"key": "vnic_type", "value": "baremetal"}, {"key": "vrouter", "value": "vrouter"}, {"key": "profile", "value": {"local_link_information": [{"port_id": "xe-0/0/5", "switch_id": "leaf1", "switch_info": "leaf1", "fabric": "myfabric"}], "vpg": "vpg", "value": "VPG_REST_API_Test"}]}, "virtual_machine_interface_properties": {"sub_interface_vlan_tag": "100"}, "virtual_network_refs": [{"to": ["default-domain", "admin", "VN_Green"]}]}]}
```

Интерфейс

Коммутатор

VLAN ID

Overlay сеть

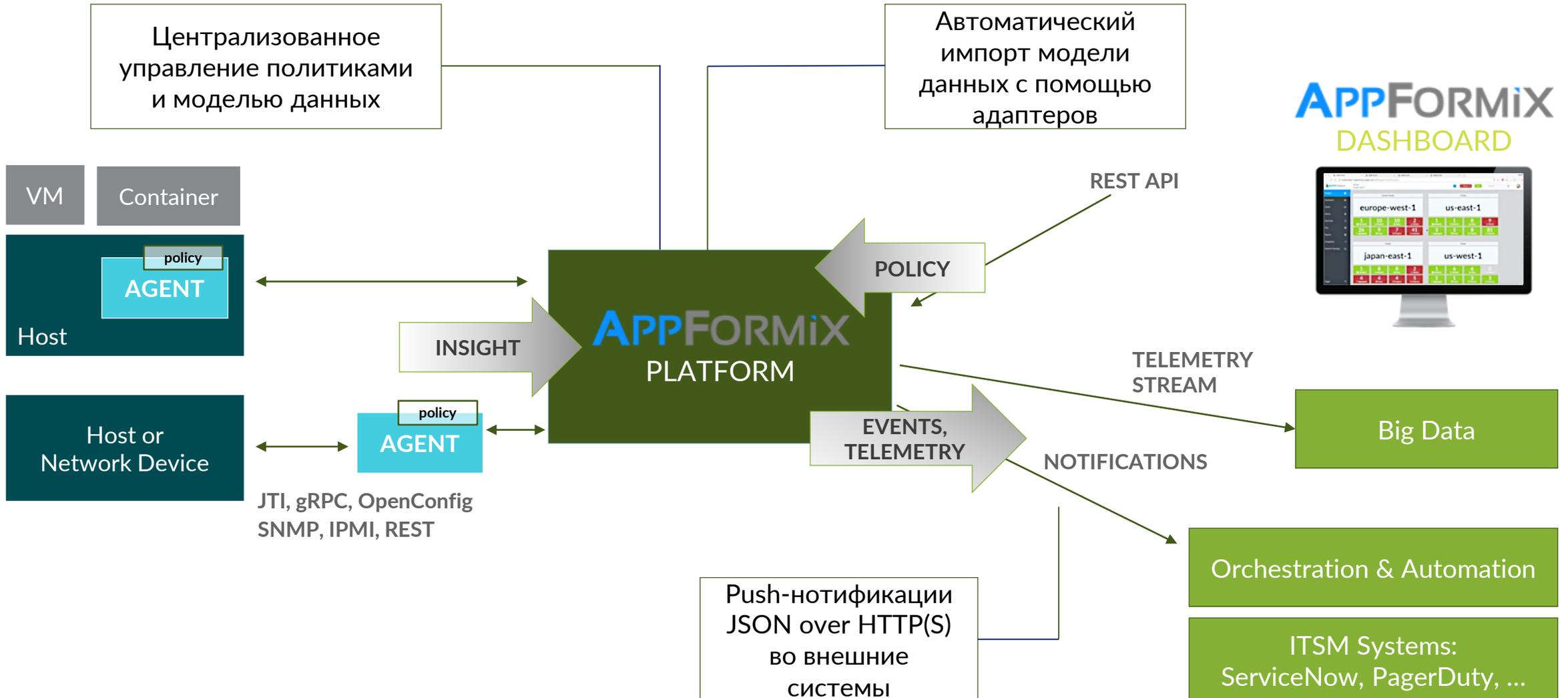
NORTHBOUND API: НАСТРОЙКА VPG - VIDEO

The screenshot displays the Contrail Command web interface. The browser address bar shows the URL: `172.30.129.39:9091/#/contrail_command/overlay/virtual_networks/vns_summary`. The interface features a dark sidebar on the left with a menu of options: Virtual Networks, Virtual Port Group, Network Policies, Multicast Policies, Logical Routers, Security Groups, Floating IPs, IPAM, Routing, Virtual Ports, DCI, and Port Profiles. The main content area is titled "OVERLAY" and contains a grid of navigation tiles for various categories: Monitoring (Dashboards, Contrail Cluster, Alarms), Infrastructure (Servers, Cluster, Fabrics, Multi Cloud, Networks), Overlay (Virtual Networks, Virtual Port Group, Network Policies, Multicast Policies, Logical Routers, Security Groups, Floating IPs, IPAM, Routing, Virtual Ports, DCI, Port Profiles), Workloads (Instances, Flavors, Images, SSH Keys), IAM (Domains, Projects, Users, RBAC), Services (Catalog, Deployments, BGPaaS, Health Check, Appliances, Load Balancers), Security (Insights, Tags, Service Groups, Address Groups, Policies, Policy Sets, Security Logging Object), Debug (Introspect, Object Logs), and DNS (Servers, Records). On the right side, a summary panel shows "Instances: 1" and "Network Policies: 0". The top right corner indicates the user is logged in as "admin".



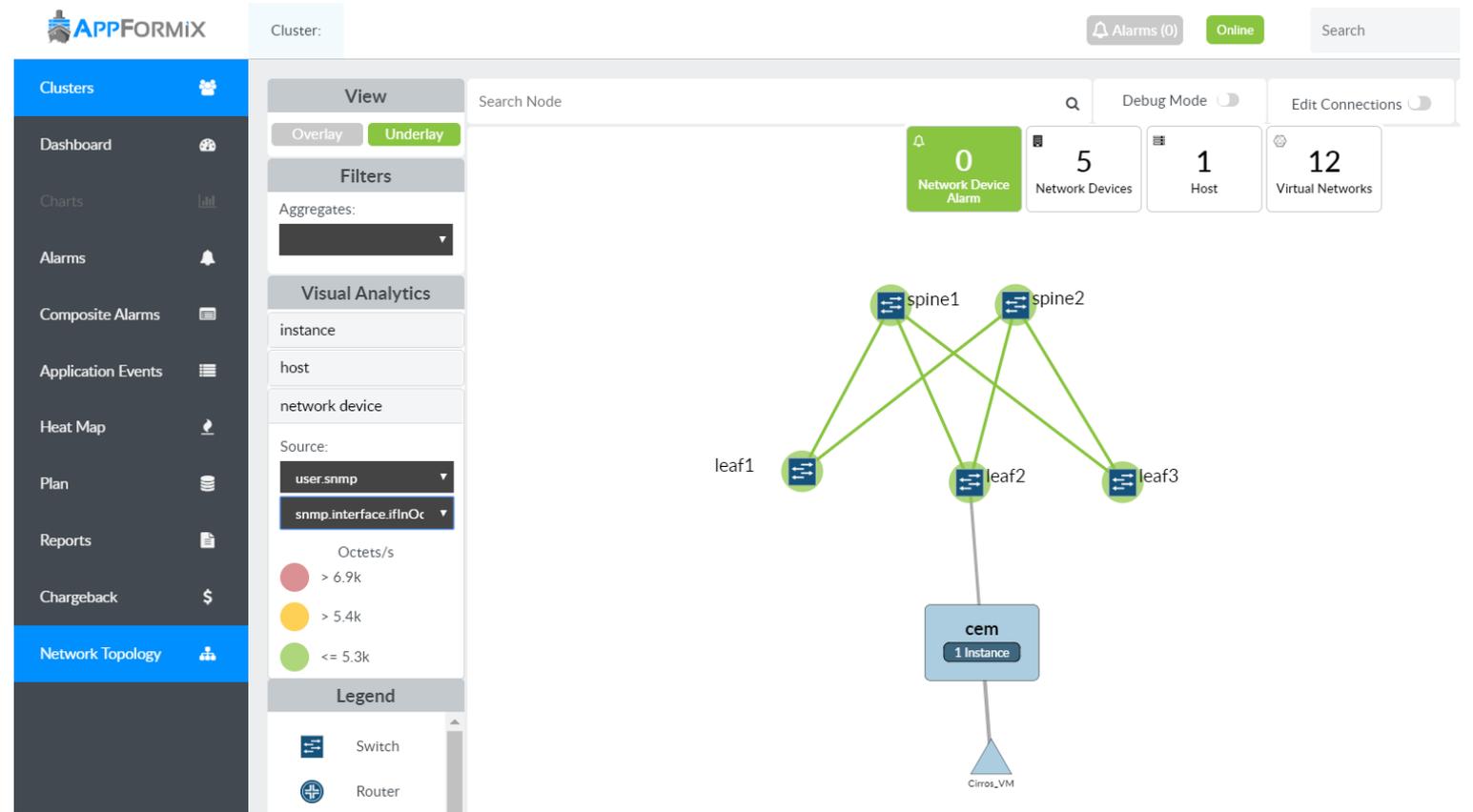
AppFormix: мониторинг и аналитика

АРХИТЕКТУРА APPFORMIX



МОНИТОРИНГ И АНАЛИТИКА

- Автоматическое обнаружение устройств и сетевой топологии
- Мониторинг сетевых устройств, серверов, виртуальных машин
- SNMP, gRPC, JT1
- Статические и динамические алармы
- Heat Map
- Визуализация аналитики
- Расширение с помощью плагинов



CONTRAIL ENTERPRISE MULTICLOUD

- Открытая платформа для автоматизации управления виртуальной и физической инфраструктурой ЦОД
- Автообнаружение и визуализация сетевой топологии overlay и underlay
- Мониторинг и аналитика по протоколам gRPC, JTI, SNMP и т.д.
- Northbound API для интеграции с оркестратором
- Гибкая масштабируемость и расширяемая функциональность



CONTRAIL
CONTROLLER



СПАСИБО!

JUNIPER
NETWORKS

Engineering
Simplicity