Сеть ЦОД на основе VXLAN/EVPN за 5 дней

День 5: VXLAN/EVPN фабрика – эксплуатация и поддержка

Максим Хаванкин, Александр Скороходов, Илья Дрей

Обсуждение – в Telegram канале:

Программа спринта

День	Тема
5 апреля, понедельник	VXLAN/EVPN фабрика – основы
6 апреля, вторник	VXLAN/EVPN фабрика – клиенты и внешние сегменты, расширенные функции NX-OS
7 апреля, среда	VXLAN/EVPN фабрика – распределенные топологии
8 апреля, четверг	VXLAN/EVPN фабрика – интеграция L4-L7 сервисов
9 апреля, пятница	**VXLAN/EVPN фабрика – эксплуатация и поддержка**

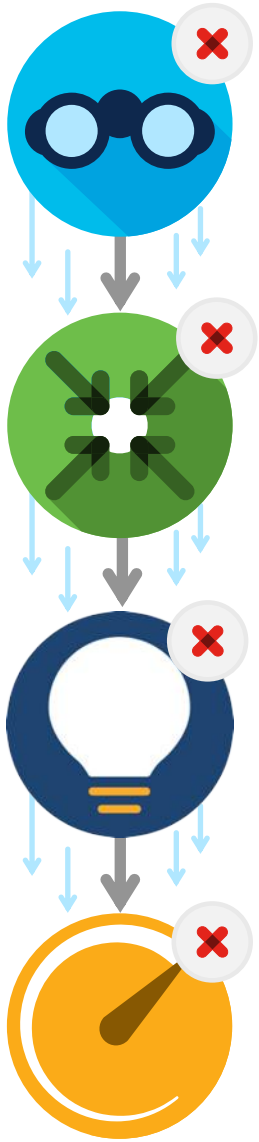
Содержание

- Основные проблемы эксплуатации сети
- VXLAN OAM
- Day2 Ops возможности, встроенные в DCNM
- Nexus Assurance Engine
- Nexus Dashboard
- Nexus Insights
- Практические аспекты разворачивания DCNM и MSO

Основные проблемы эксплуатации сети

Эксплуатация сети ЦОД – важнее и дороже построения и настройки

Основные проблемы эксплуатации сети



Нет сквозной видимости и понимания происходящего

Нет корреляции событий и проблем

Нет возможности предсказать последствия изменений

Проблемы производительности и надёжности

Cisco ACI и NX-OS

Intent

“Что вы хотите **получить**”

Cisco Network Insights

Analytics

“Что **происходит**”

Анализ телеметрии

Аномалии и рекомендации

Cisco Network Assurance

Assurance

“Что **случится** и что **должно случиться**”

Анализ конфигурации и состояния

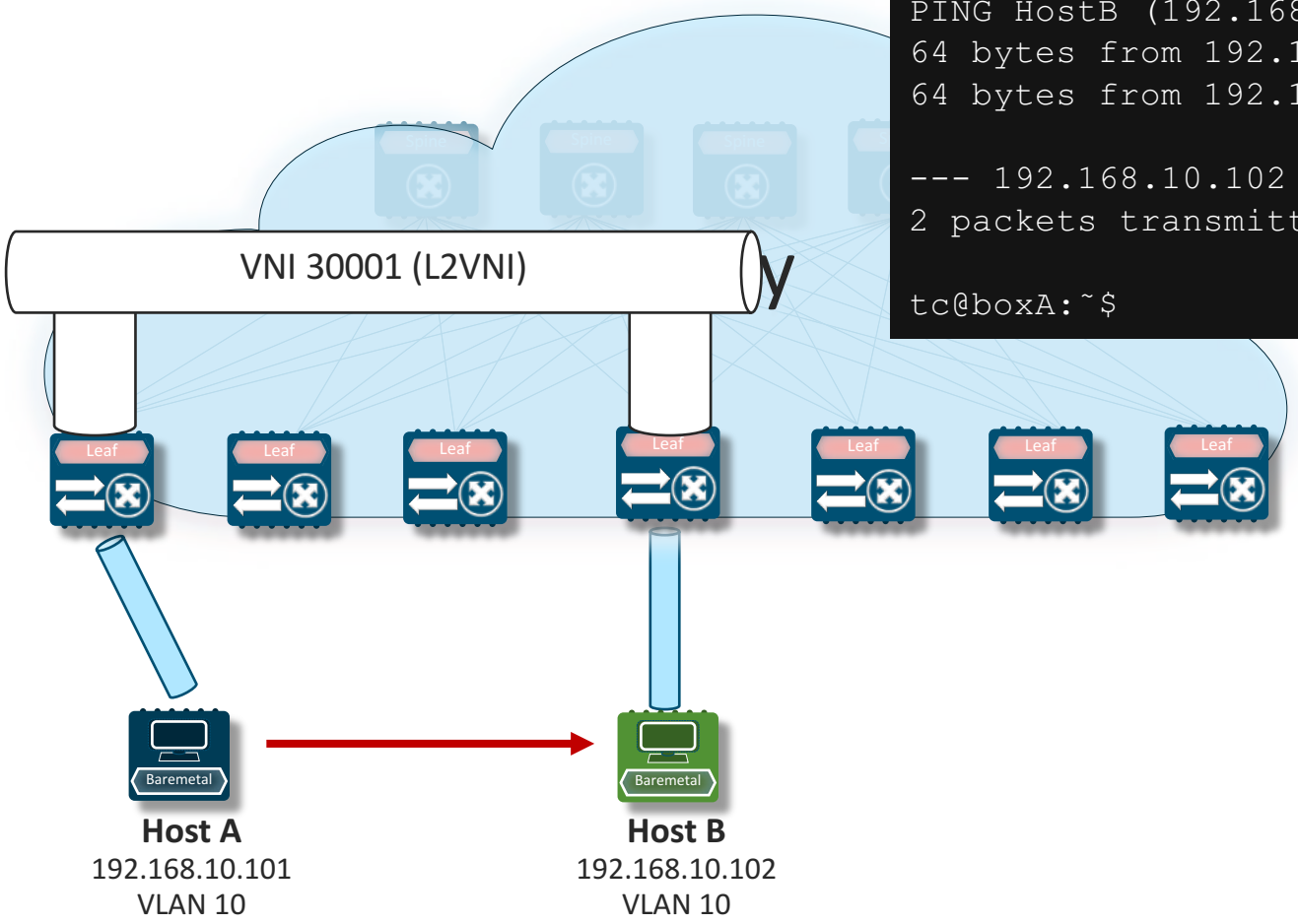
Где ошибки и как их исправить

Лицензия Essentials

VXLAN OAM

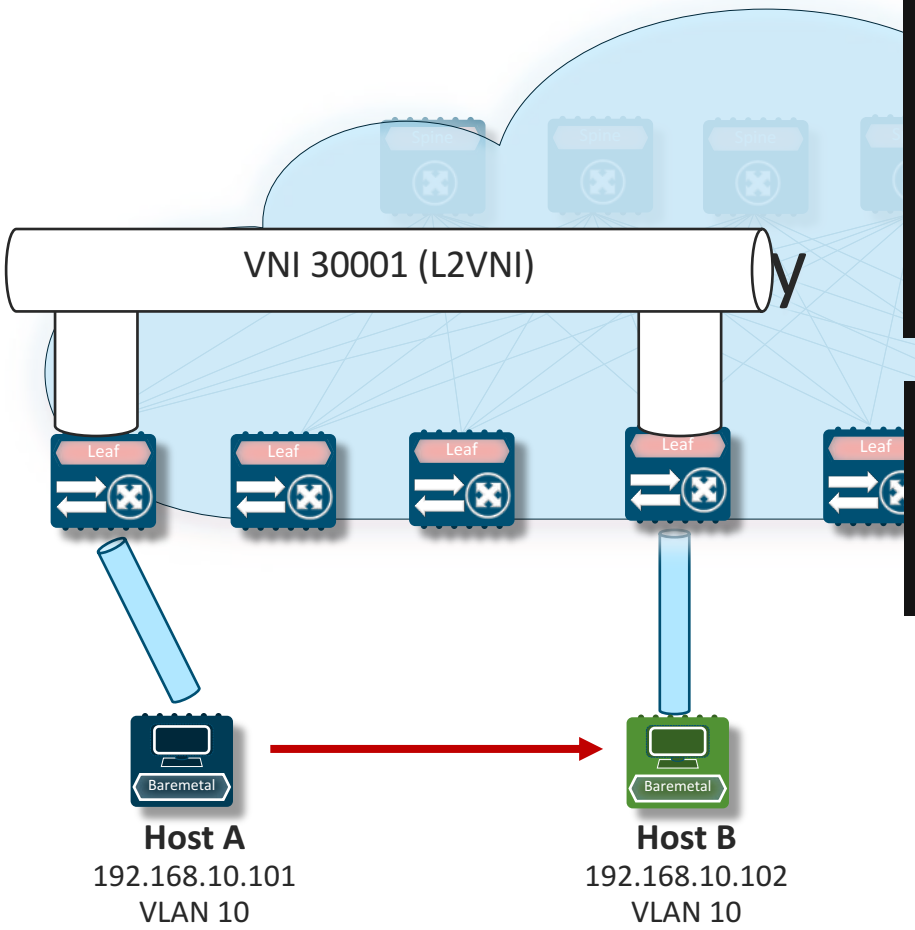
Предпосылки появления

Ping/Traceroute в оверлейных сетях – коммутация




```
tc@boxA:~$ ping HostB
PING HostB (192.168.10.102): 56 data bytes
64 bytes from 192.168.10.102 : icmp_seq=0 ttl=64 time=0.653 ms
64 bytes from 192.168.10.102 : icmp_seq=1 ttl=64 time=0.631 ms

--- 192.168.10.102 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss

tc@boxA:~$
```

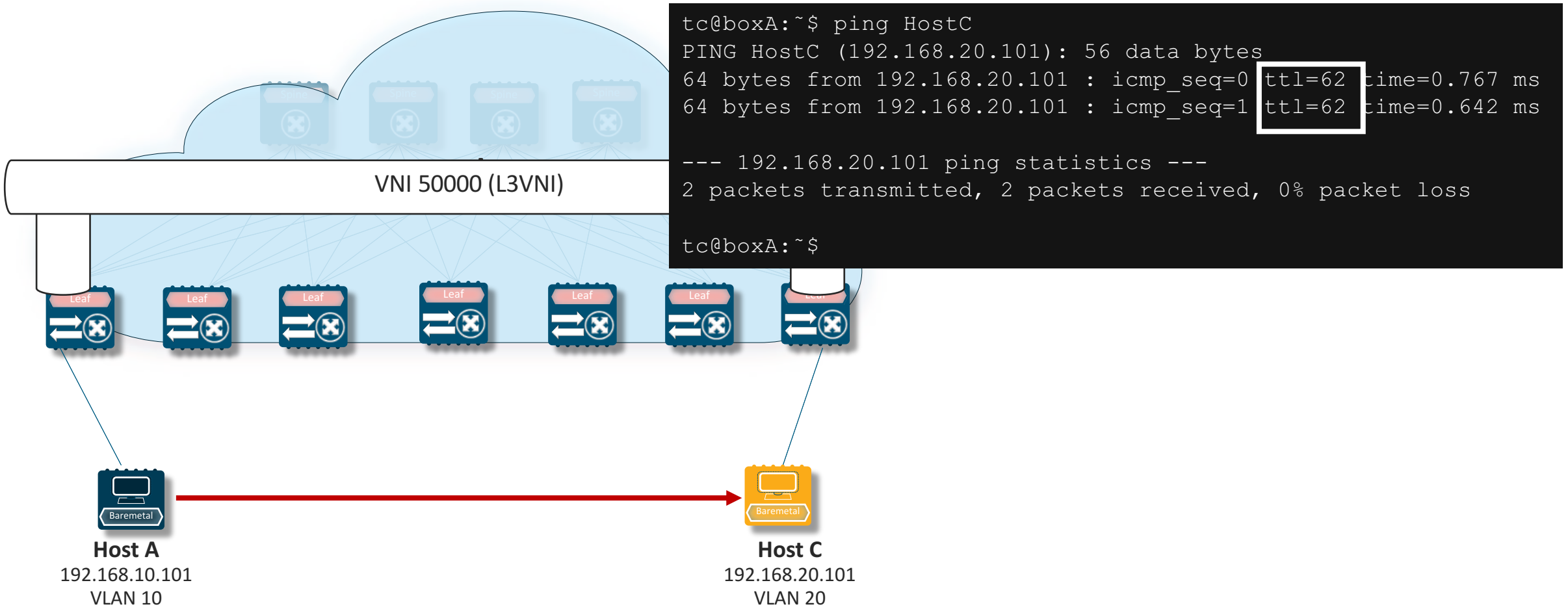
Ping/Traceroute в оверлейных сетях – коммутация




```
tc@boxA:~$ ping HostB
PING HostB (192.168.10.102): 56 data bytes
64 bytes from 192.168.10.102 : icmp_seq=0 ttl=64 time=0.653 ms
64 bytes from 192.168.10.102 : icmp_seq=1 ttl=64 time=0.631 ms

--- 192.168.10.102 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss

tc@boxA:~$
```

```
tc@boxA:~$ traceroute HostB
traceroute to HostB (192.168.10.102), 30 hops max, 38 byte packets
1 192.168.10.102 (192.168.10.102)  0.302 ms  0.251 ms  0.259 ms

tc@boxA:~$
```

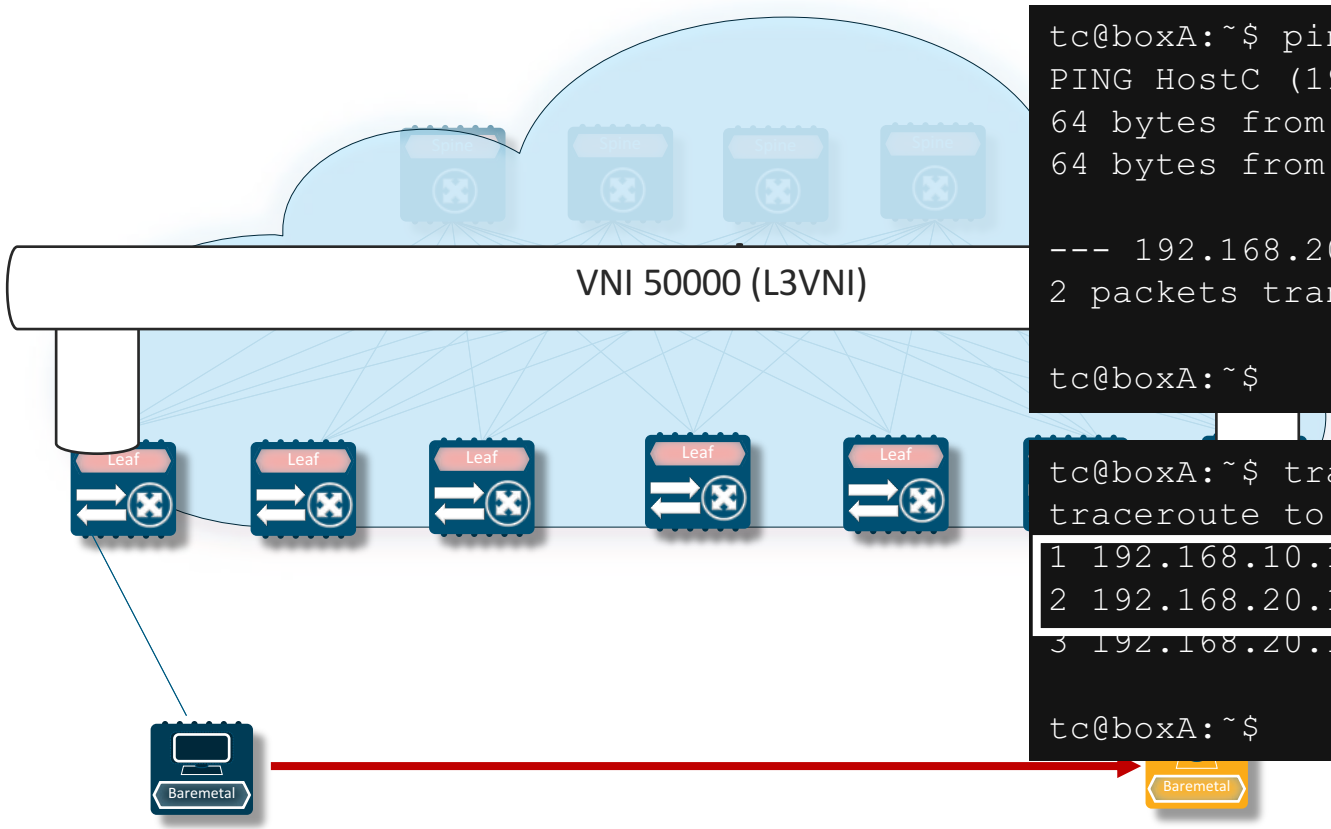
Ping/Traceroute в оверлейных сетях – маршрутизация




```
tc@boxA:~$ ping HostC
PING HostC (192.168.20.101): 56 data bytes
64 bytes from 192.168.20.101 : icmp_seq=0 ttl=62 time=0.767 ms
64 bytes from 192.168.20.101 : icmp_seq=1 ttl=62 time=0.642 ms

--- 192.168.20.101 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss

tc@boxA:~$
```

*L3VNI: VNI for all Routing operation (”VRF-VNI”)

Ping/Traceroute в оверлейных сетях – маршрутизация




```
tc@boxA:~$ ping HostC
PING HostC (192.168.20.101): 56 data bytes
64 bytes from 192.168.20.101 : icmp_seq=0 ttl=62 time=0.767 ms
64 bytes from 192.168.20.101 : icmp_seq=1 ttl=62 time=0.642 ms

--- 192.168.20.101 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss

tc@boxA:~$
```

```
tc@boxA:~$ traceroute HostC
traceroute to HostC (192.168.20.101), 30 hops max, 38 byte packets
1 192.168.10.1 (192.168.10.1)  0.593 ms  0.303 ms  0.312 ms
2 192.168.20.1 (192.168.20.1)  0.661 ms  0.400 ms  0.378 ms
3 192.168.20.101 (192.168.20.101)  0.509 ms  0.387 ms  0.217 ms

tc@boxA:~$
```

Host A
192.168.10.101
VLAN 10

Host C
192.168.20.101
VLAN 20

Как узнать что «под капотом» у VXLAN EVPN фабрики?

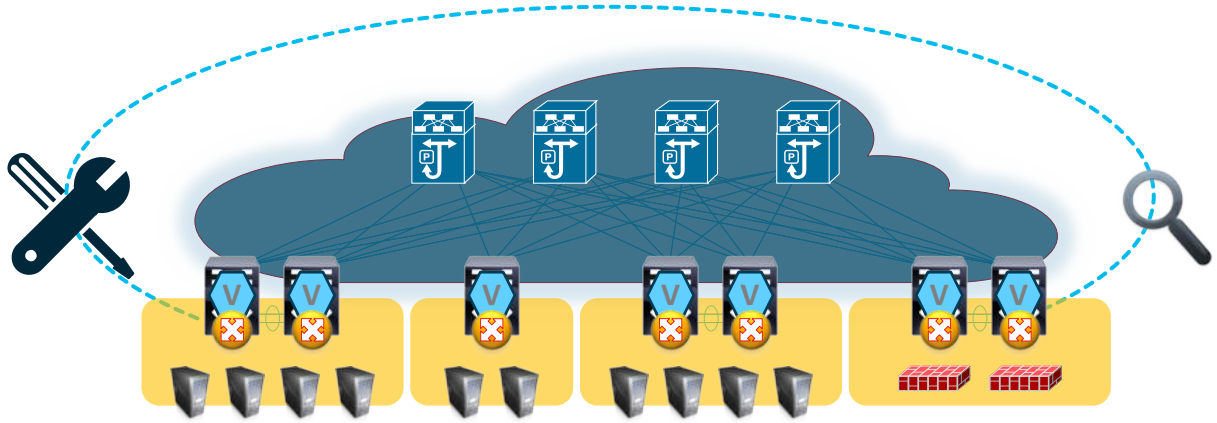
Возможности VXLAN OAM, использование в CLI

Operations, Administration and Management (OAM)

- OAM – процессы, активности, средства и стандарты
- Различные режимы работы
- Pro-Active
  - Контроль над ситуацией
- Re-Active
  - Реакция на события

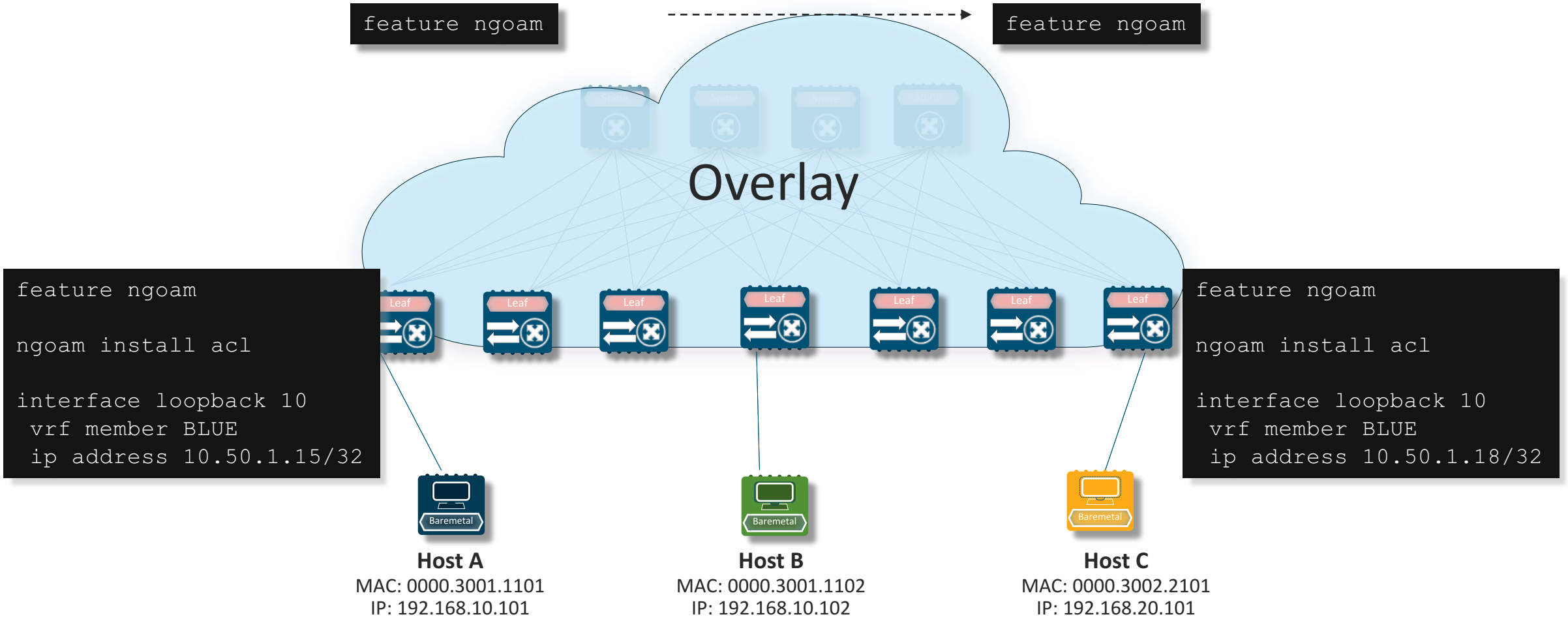
https://tools.ietf.org/html/draft-tissa-nvo3-oam-fm-04

Арсенал средств VXLAN OAM

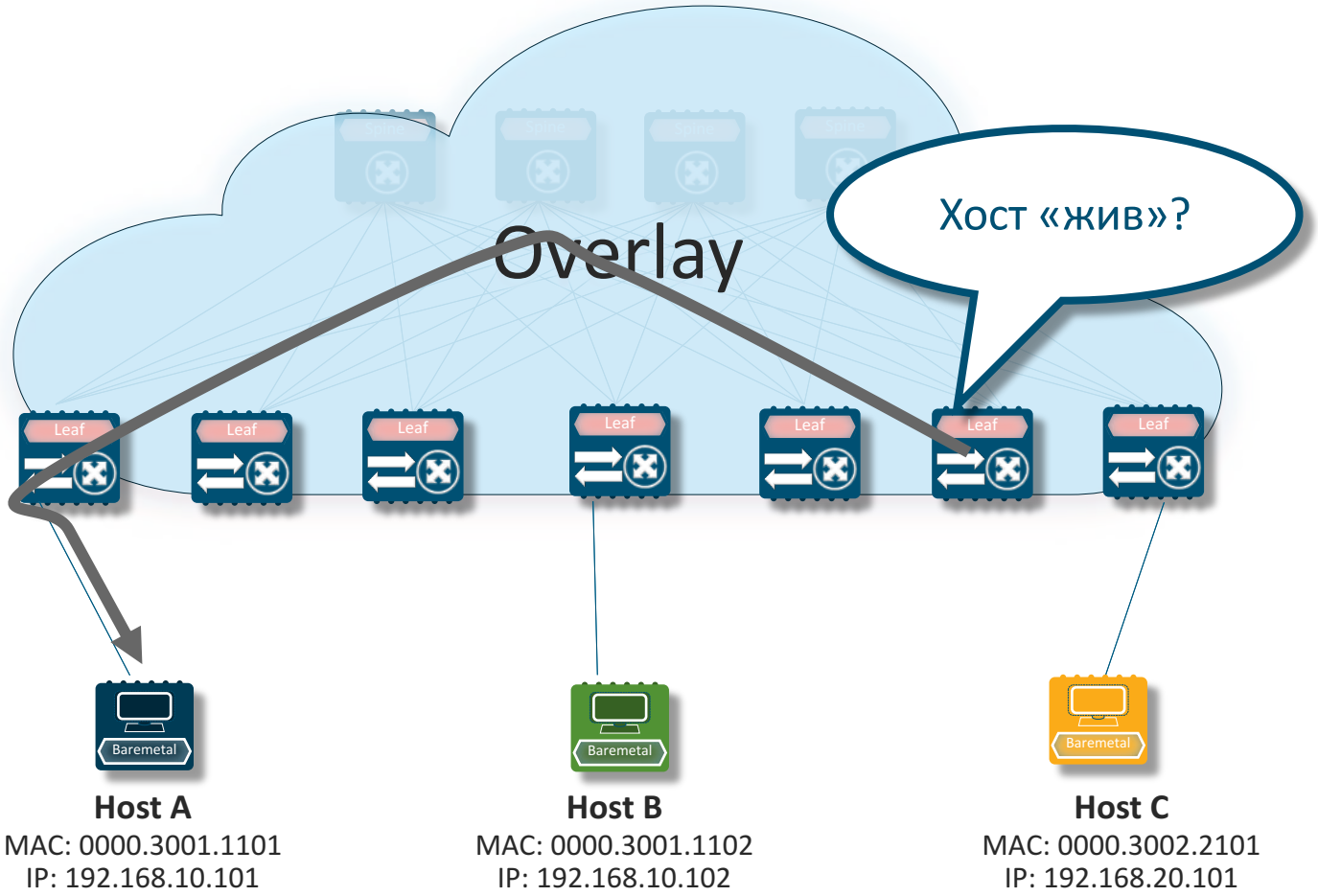


Ping / Path MTU	Pathtrace	Endpoint Locator	Pro-Active Monitoring
• Проверка доступности хоста • Возможно проверить доступность для пакета с определенной нагрузкой	• Поиск путей до хостов и VTEP • Идентификация устройств, интерфейсов, статистика по ошибкам на пути	• Обнаружение хостов • Отслеживание истории перемещений • Статистика и активности хостов	• Мониторинг и уведомления

VXLAN OAM – активация функции (Command Line)

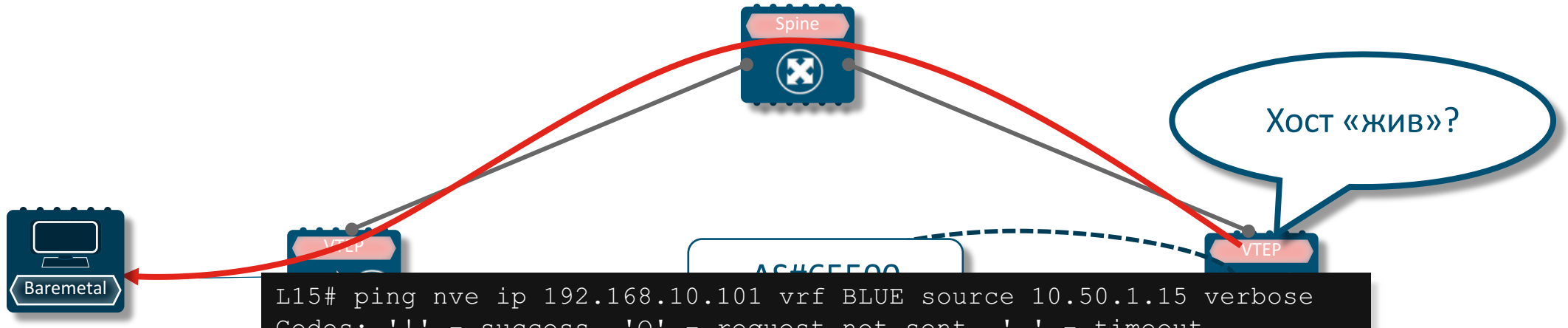


Проверка доступности хоста через оверлей



- Доступность хоста
  - Используется ICMP
  - Связь между VTEP и Endpoint
  - Связь между VTEP и VTEP
- Проверка ECMP путей
  - Single Random Path
  - Multiple, Random/Specified Path

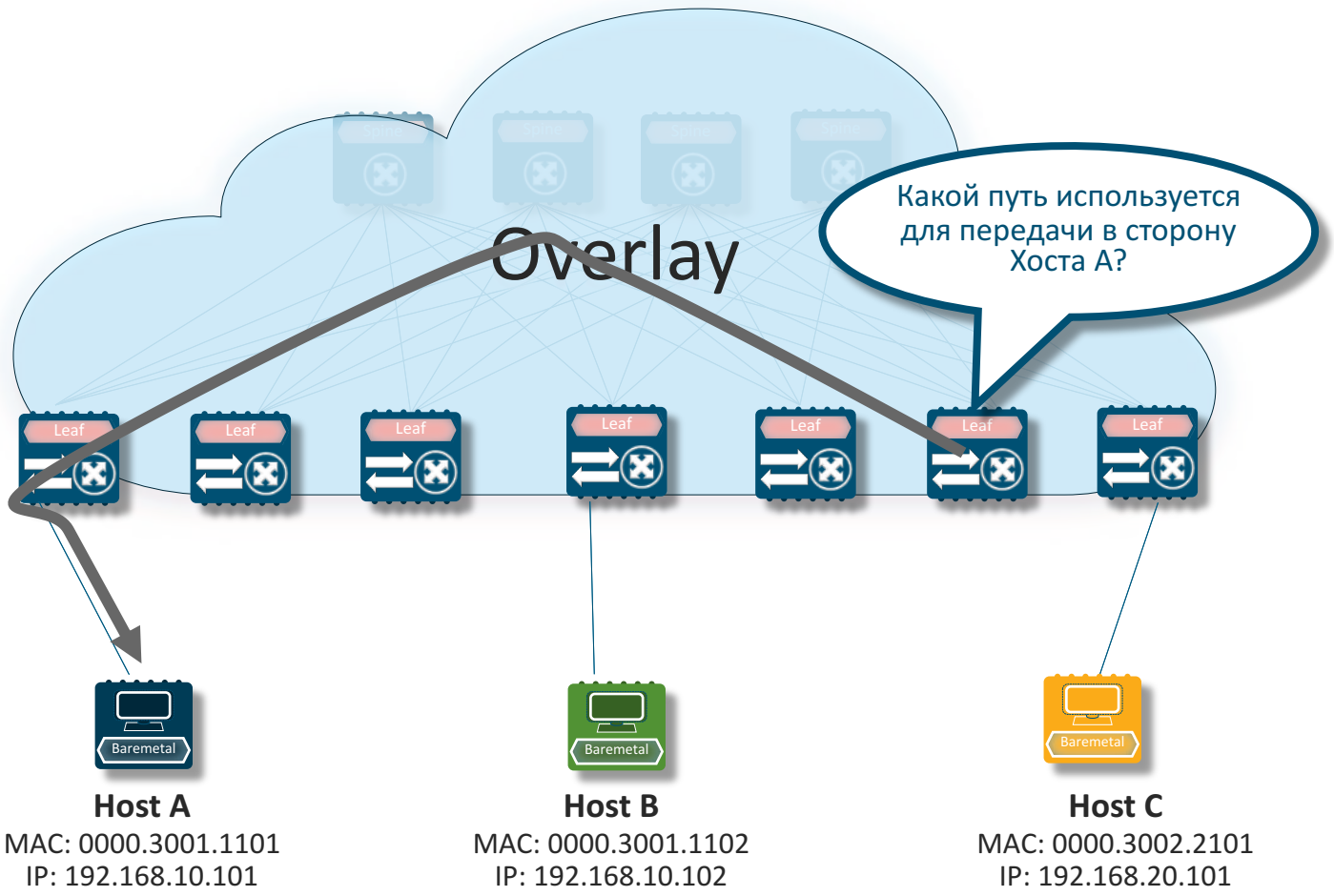
Проверка доступности хоста через оверлей
Пример



Host A
MAC: 0000.3001.1101
IP: 192.168.10.101

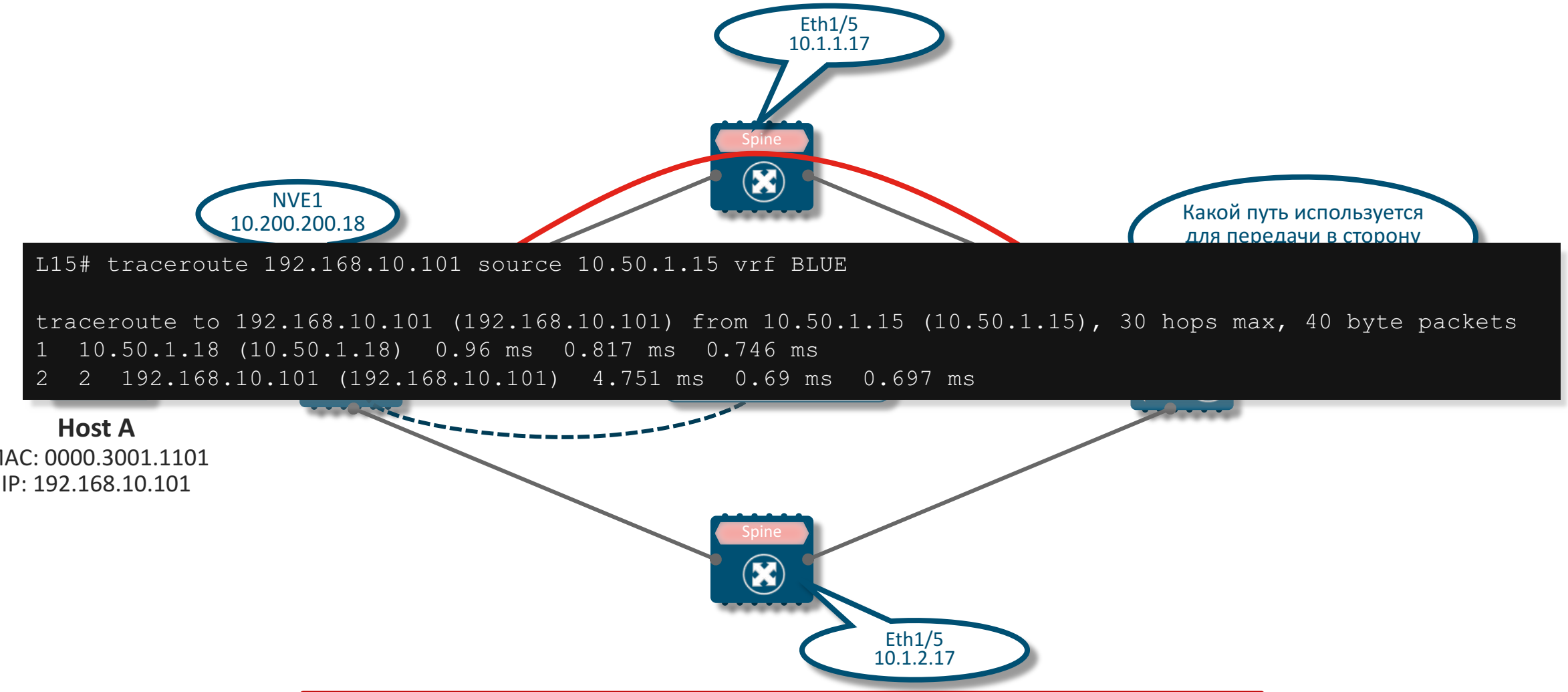
```
L15# ping nve ip 192.168.10.101 vrf BLUE source 10.50.1.15 verbose
Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'D' - Destination Unreachable, 'X' - unknown return code,
'm' - malformed request(parameter problem),
'c' - Corrupted Data/Test, '#' - Duplicate response

Sender handle: 32
! sport 35977 size 56,Reply from 192.168.10.101,time = 1 ms
! sport 35977 size 56,Reply from 192.168.10.101,time = 2 ms
! sport 35977 size 56,Reply from 192.168.10.101,time = 1 ms
! sport 35977 size 56,Reply from 192.168.10.101,time = 1 ms
! sport 35977 size 56,Reply from 192.168.10.101,time = 1 ms

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/2 ms
Total time elapsed 89 ms
```

Endpoint Traceroute – VXLAN OAM



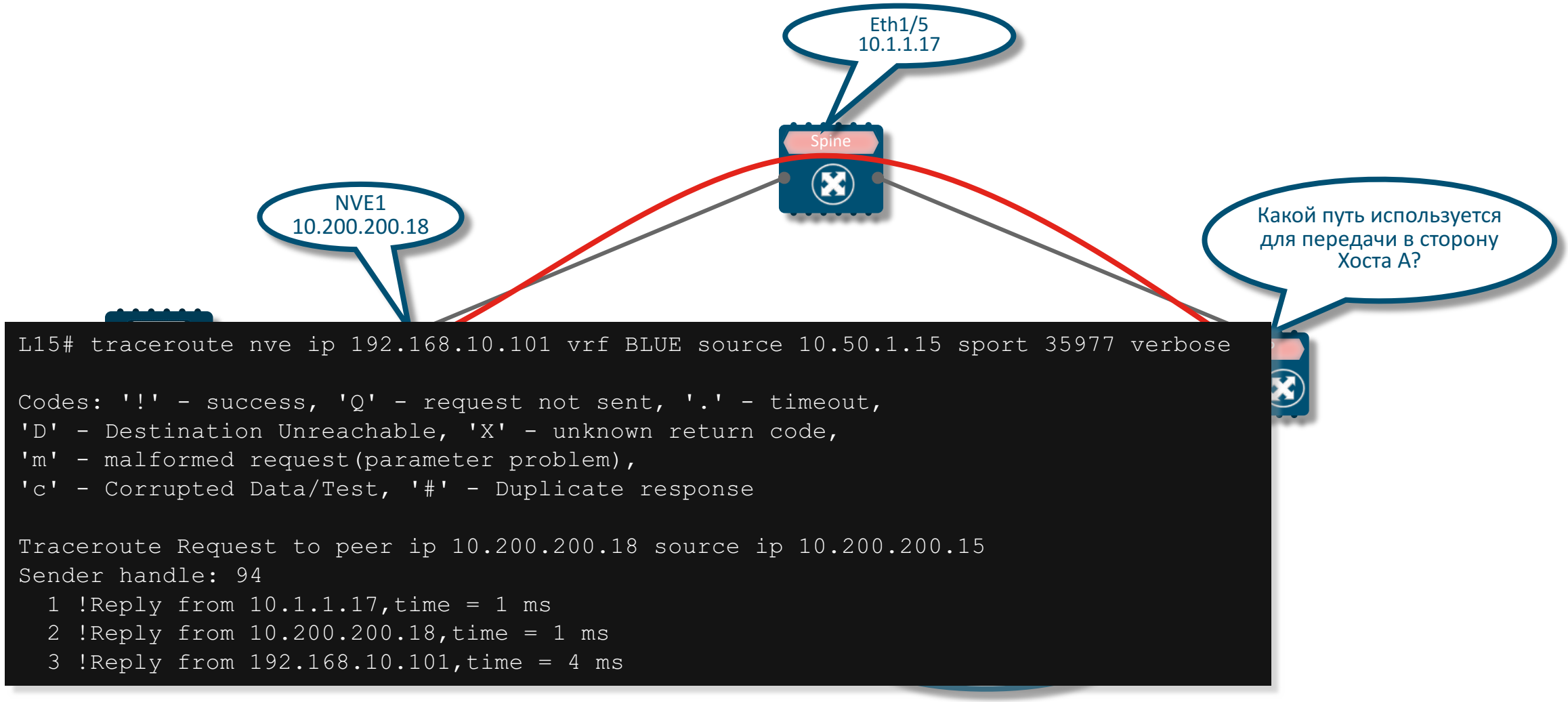
- Доступность хоста
  - Используется ICMP
  - Связь между VTEP и Endpoint
  - Связь между VTEP и VTEP
- Проверка путей
  - Single Specified Path
  - Multiple, Specified Path

Как выглядит обычный Traceroute?



По какому пути передаются пакеты?

Traceroute для VXLAN




```
L15# traceroute nve ip 192.168.10.101 vrf BLUE source 10.50.1.15 sport 35977 verbose

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'D' - Destination Unreachable, 'X' - unknown return code,
'm' - malformed request(parameter problem),
'c' - Corrupted Data/Test, '#' - Duplicate response

Traceroute Request to peer ip 10.200.200.18 source ip 10.200.200.15
Sender handle: 94
  1 !Reply from 10.1.1.17,time = 1 ms
  2 !Reply from 10.200.200.18,time = 1 ms
  3 !Reply from 192.168.10.101,time = 4 ms
```

Traceroute для VXLAN OAM

```
L15# traceroute nve ip 192.168.10.101 vrf BLUE source 10.50.1.15 sport 35977 verbose

Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
'D' - Destination Unreachable, 'X' - unknown return code,
'm' - malformed request(parameter problem),
'c' - Corrupted Data/Test, '#' - Duplicate response

Traceroute Request to peer ip 10.200.200.18 source ip 10.200.200.15
Sender handle: 94
  1 !Reply from 10.1.1.17,time = 1 ms
  2 !Reply from 10.200.200.18,time = 1 ms
  3 !Reply from 192.168.10.101,time = 4 ms
```

Spine Ingress Interface IP

Destination VTEP IP

Host A IP

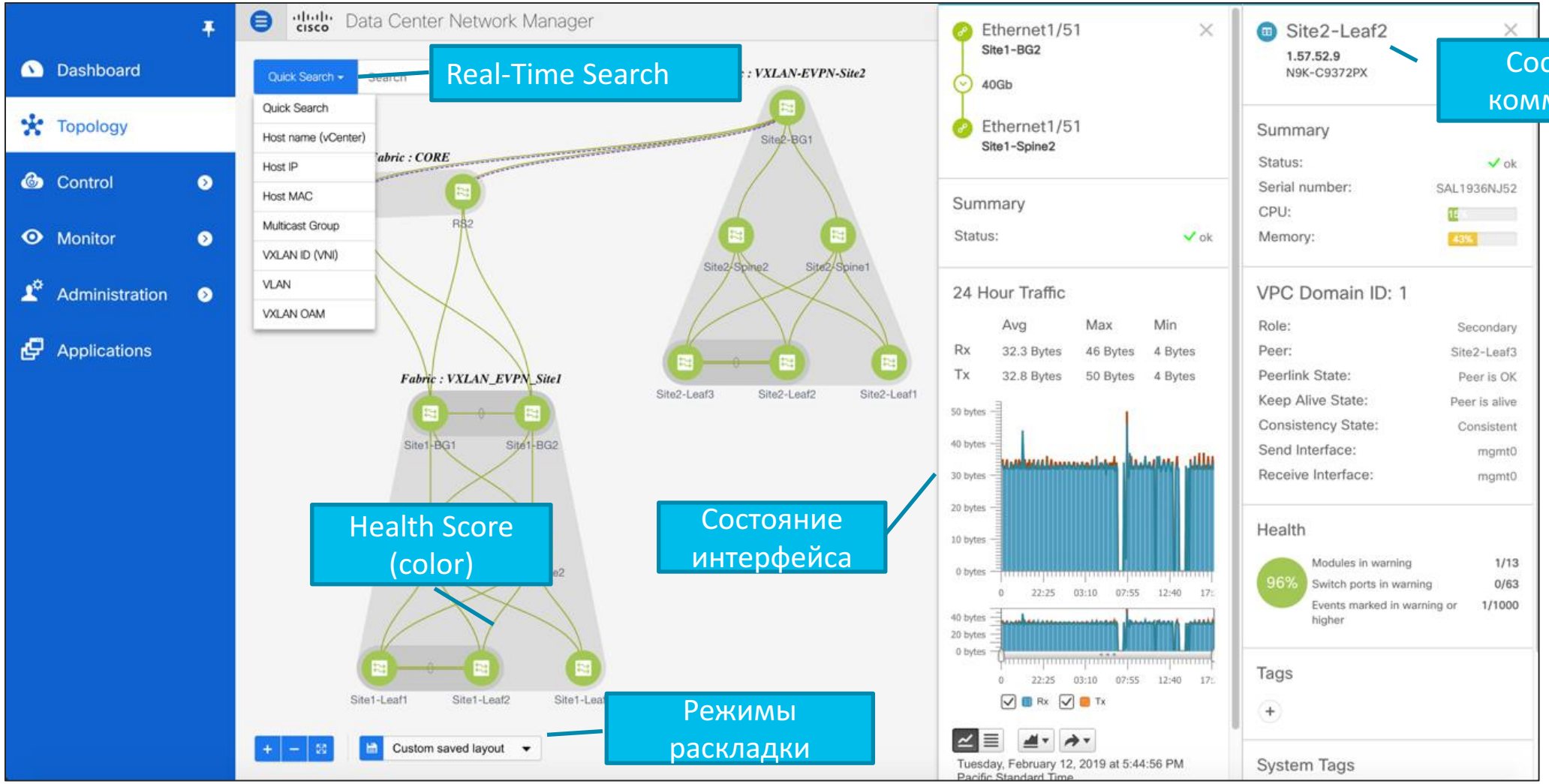
Дополнительно к обычной для команды Traceroute информации, доступны детали по передаче через spine и leaf

Лицензия Essentials

Day2 Ops возможности, встроенные в DCNM

Dashboard – общее состояние здоровья Real Time Network View

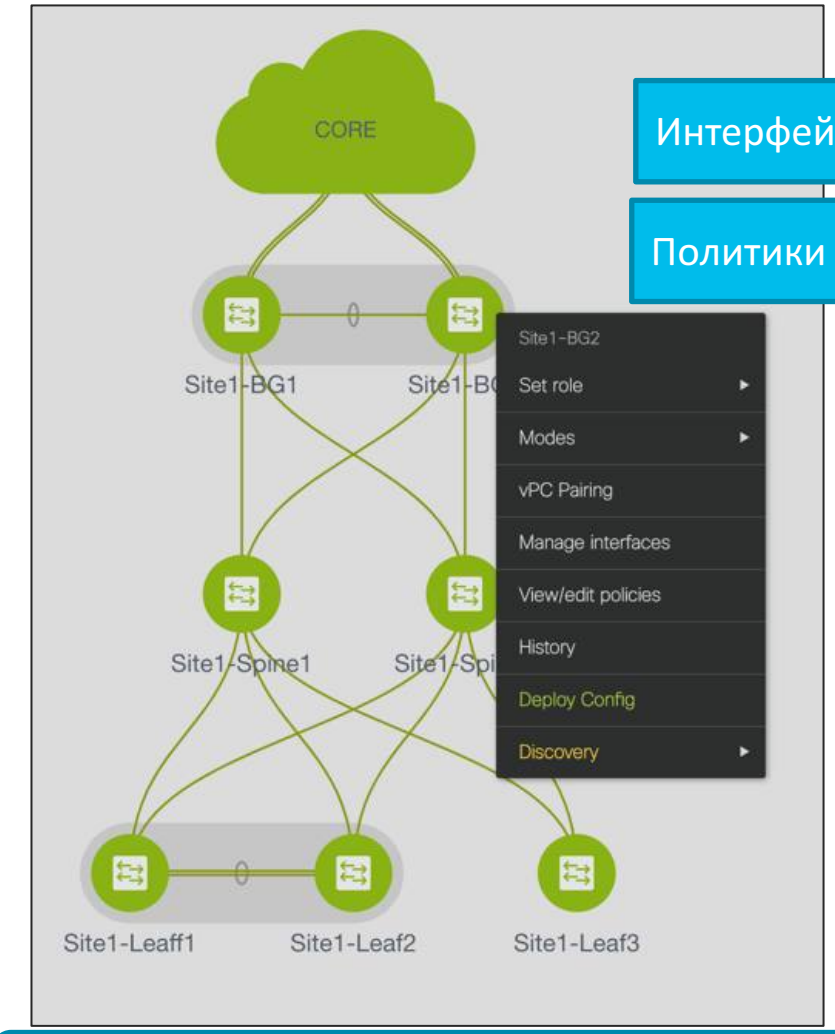
Day 2 Operations - мониторинг



Состояние топологии фабрики

Мониторинг и поддержка

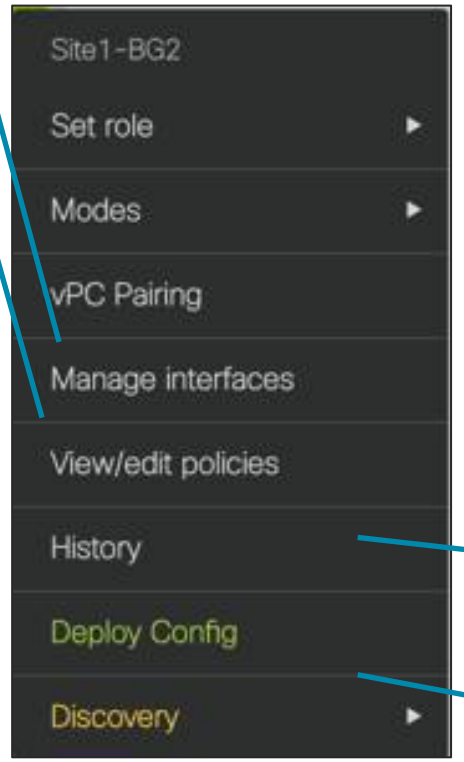
Day 2 Operations – Device Maintenance



Интерфейсы

Политики

Операции с устройством



Роли устройств

Режимы работы устройств

RMA

Configuration Status & History

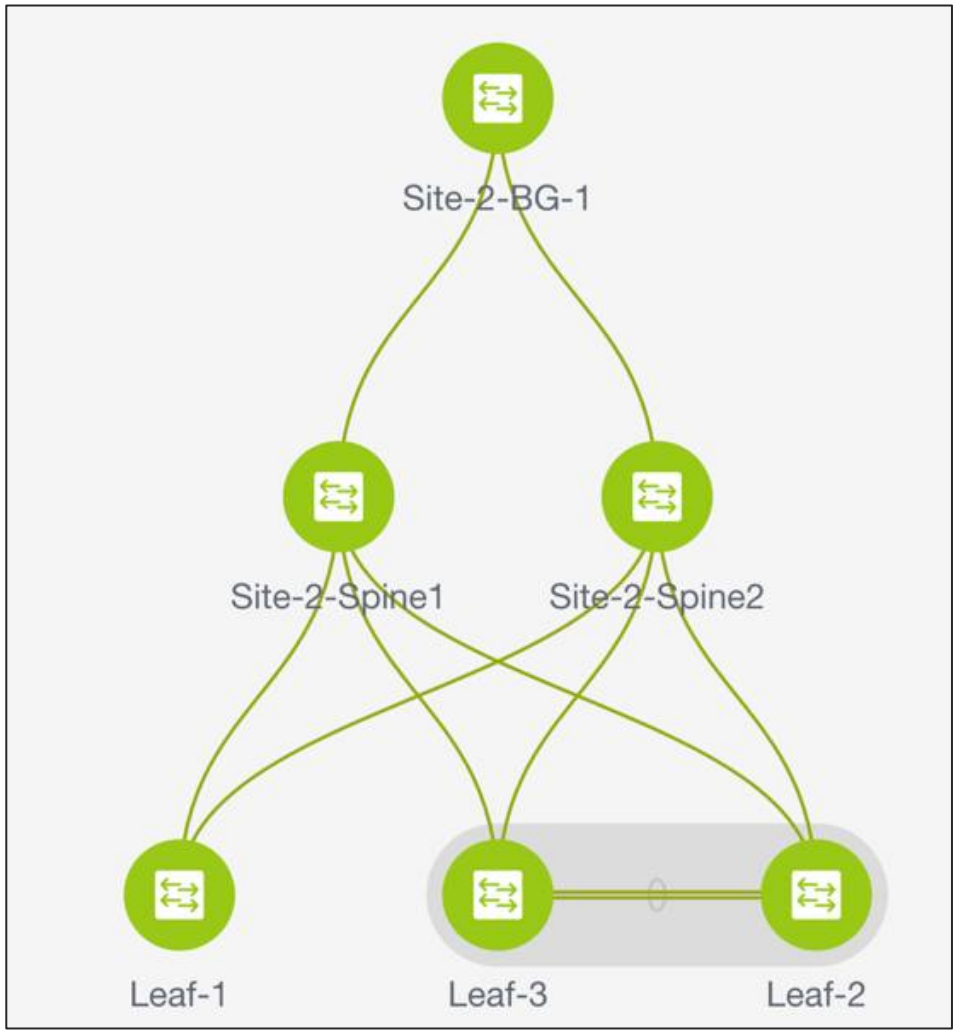
Применение конфигурации на утсройстве

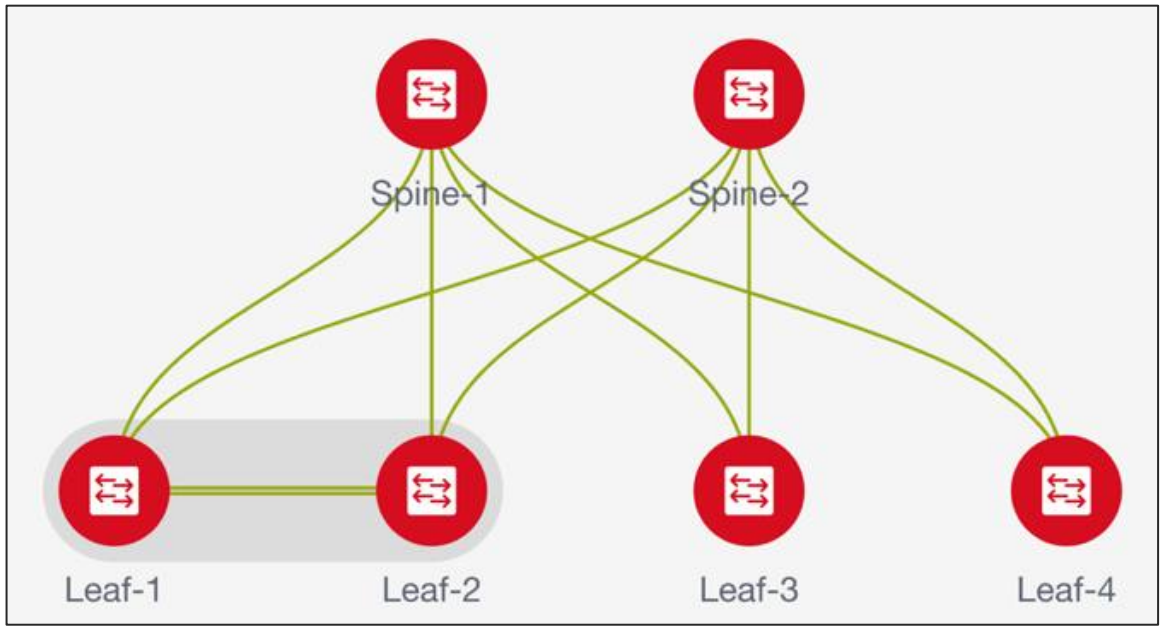
Discovery

Fabric Builder Day 2 Topology Views

Мониторинг и поддержка…

Day 2 Operations – состояние устройства



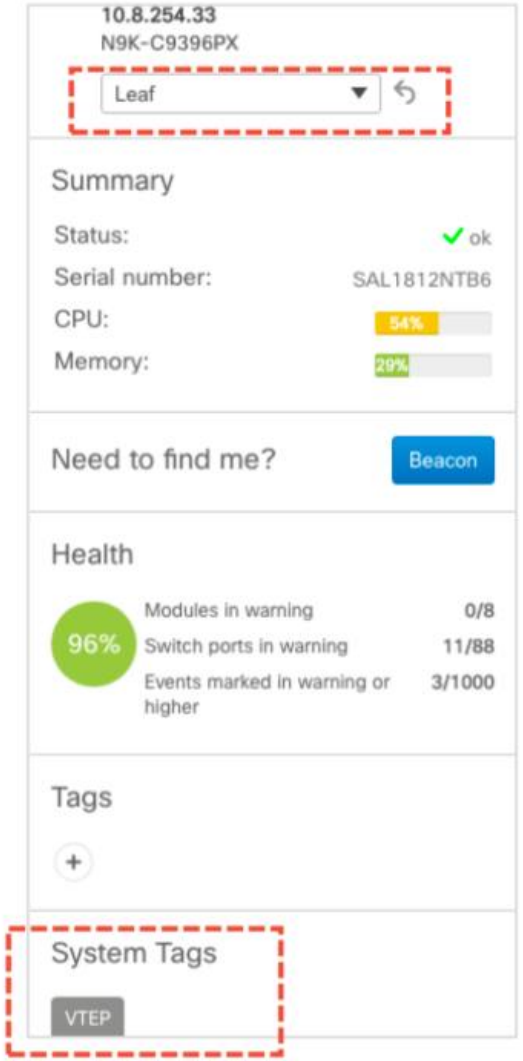


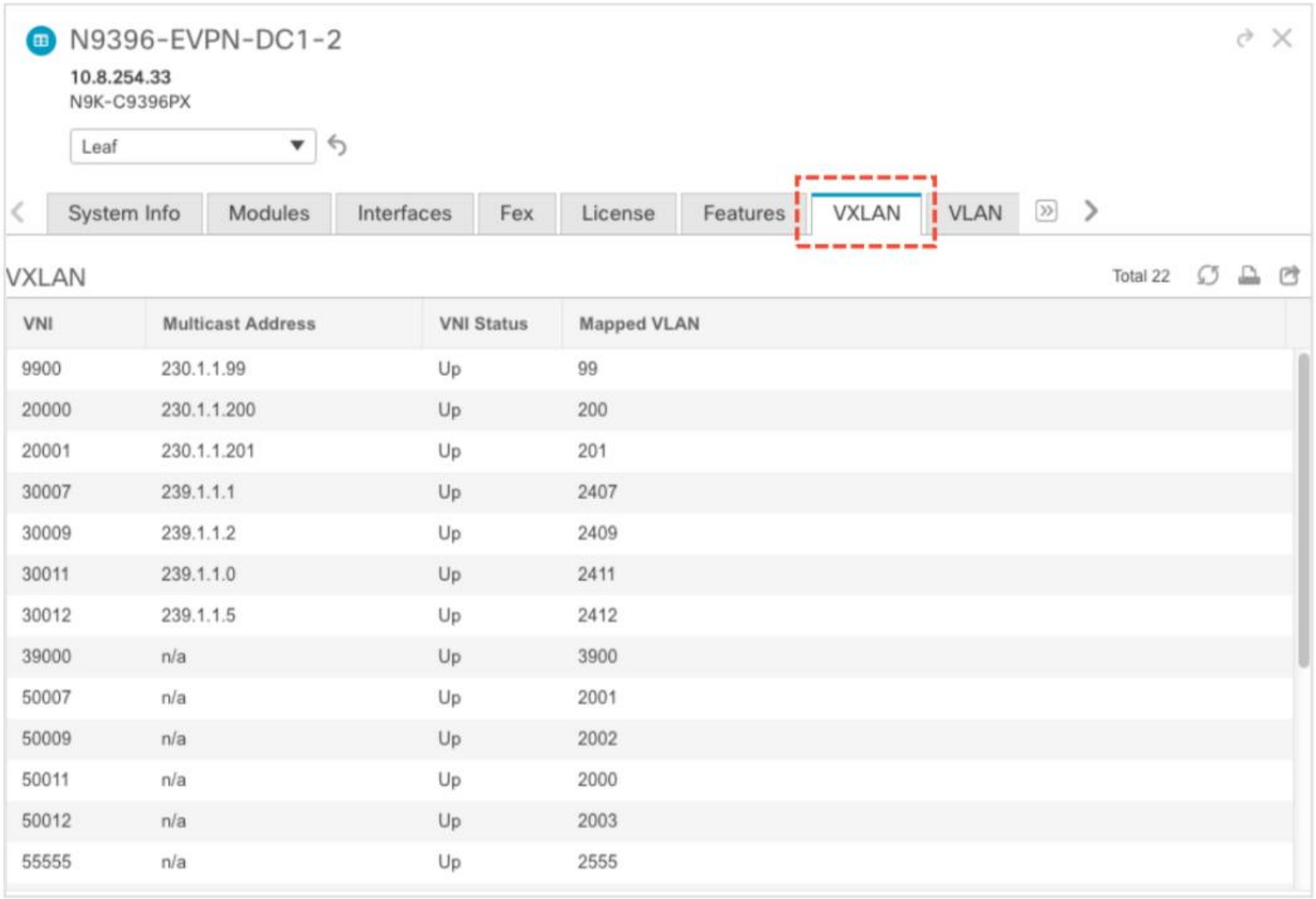
Ready to Deploy	Success/In Sync	Failed/Out of Sync	In Progress	Unknown State / NA
Leaf-1	Leaf-1	Leaf-1	Leaf-1	Leaf-1

Fabric Builder Real Time Status

Day 2 Operations - мониторинг

Детальная информация о коммутаторе

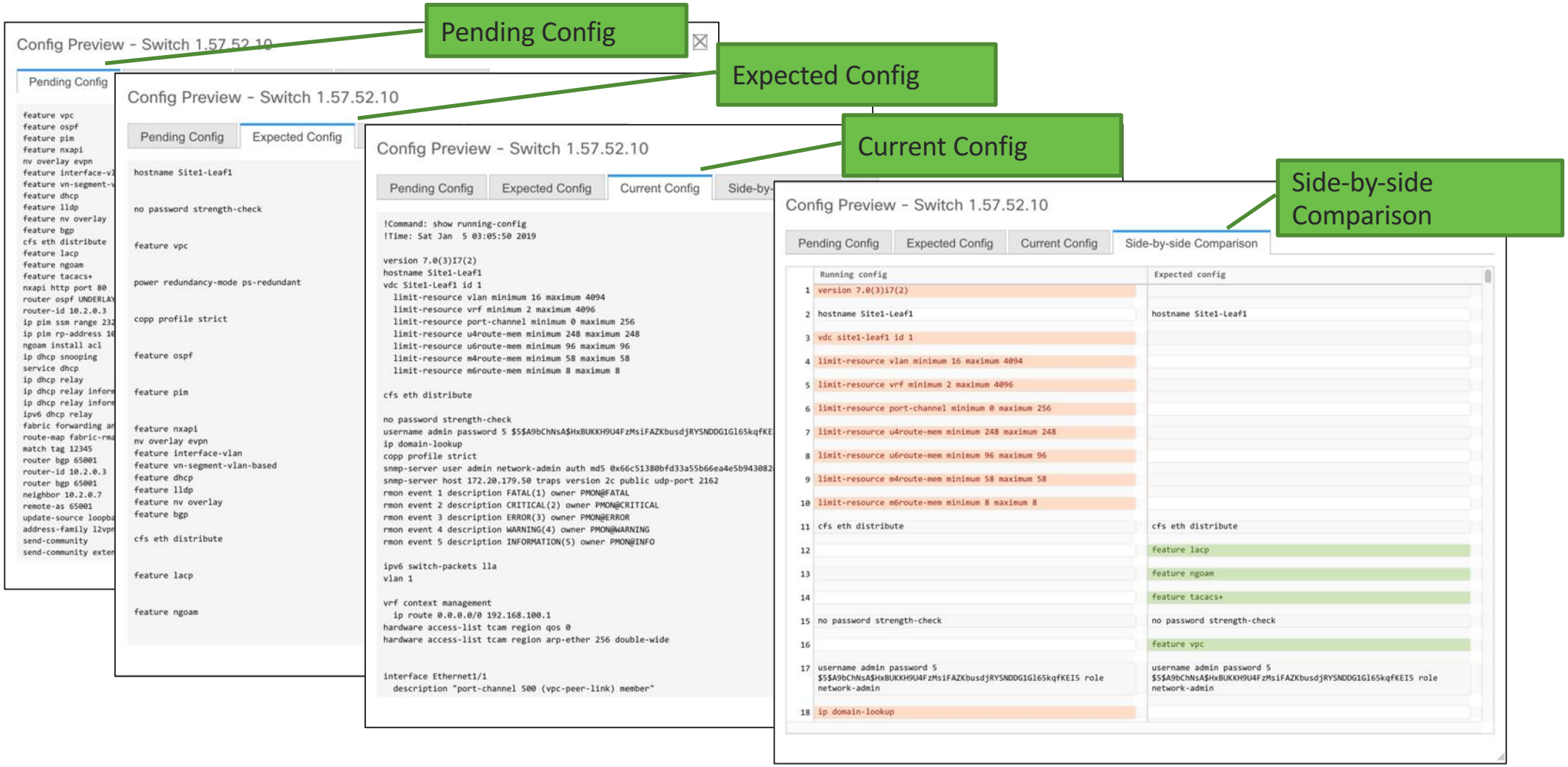




VNI	Multicast Address	VNI Status	Mapped VLAN
9900	230.1.1.99	Up	99
20000	230.1.1.200	Up	200
20001	230.1.1.201	Up	201
30007	239.1.1.1	Up	2407
30009	239.1.1.2	Up	2409
30011	239.1.1.0	Up	2411
30012	239.1.1.5	Up	2412
39000	n/a	Up	3900
50007	n/a	Up	2001
50009	n/a	Up	2002
50011	n/a	Up	2000
50012	n/a	Up	2003
55555	n/a	Up	2555

Мониторинг, поддержка, поиск неисправностей

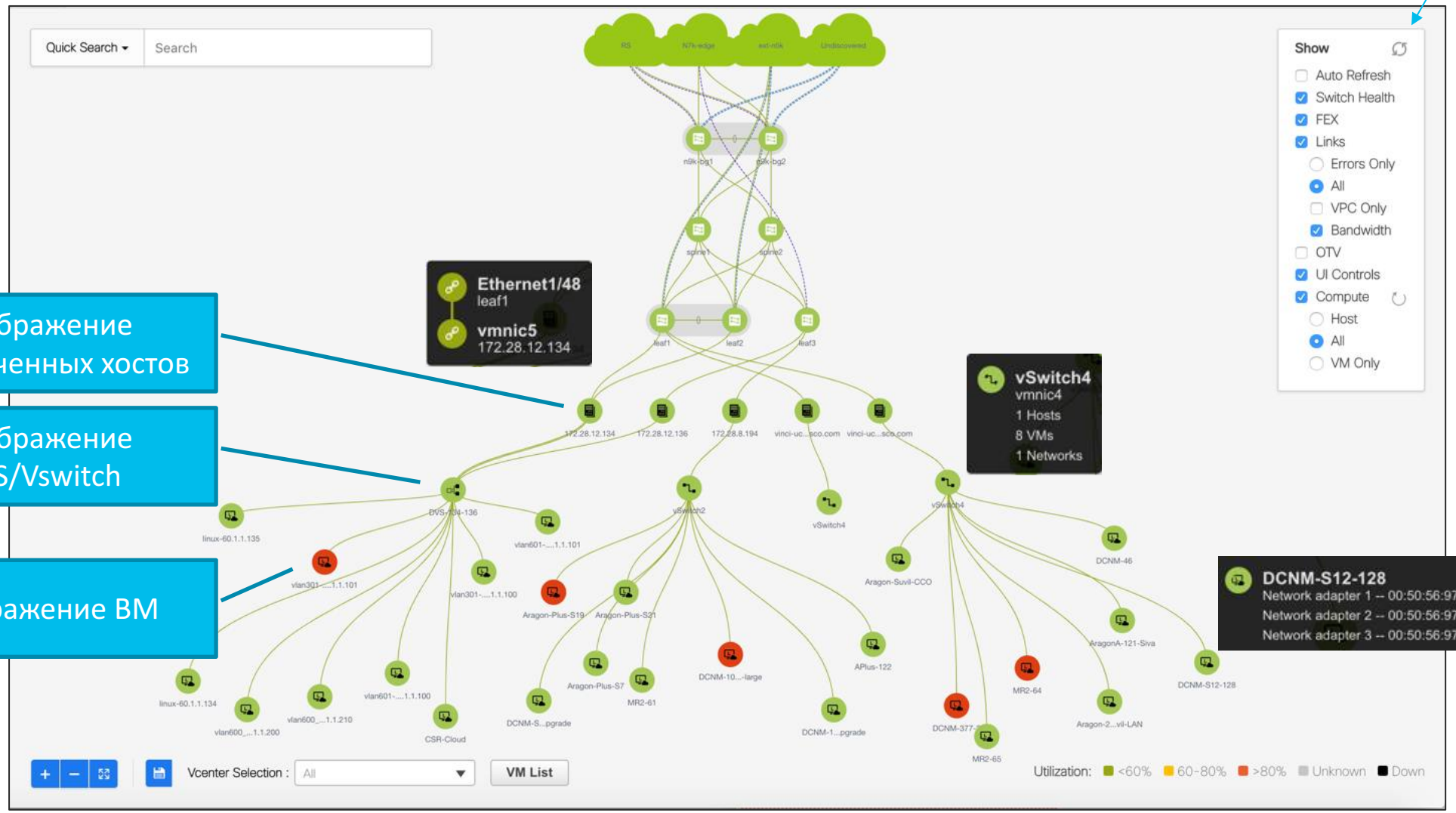
Day 2 Operations – Configuration Compliance Status & Visibility



Configuration Compliance (Expected или Current Configuration View)

Day 2 Operations - мониторинг

!= VMM интеграции в ACI



Отображение подключенных хостов

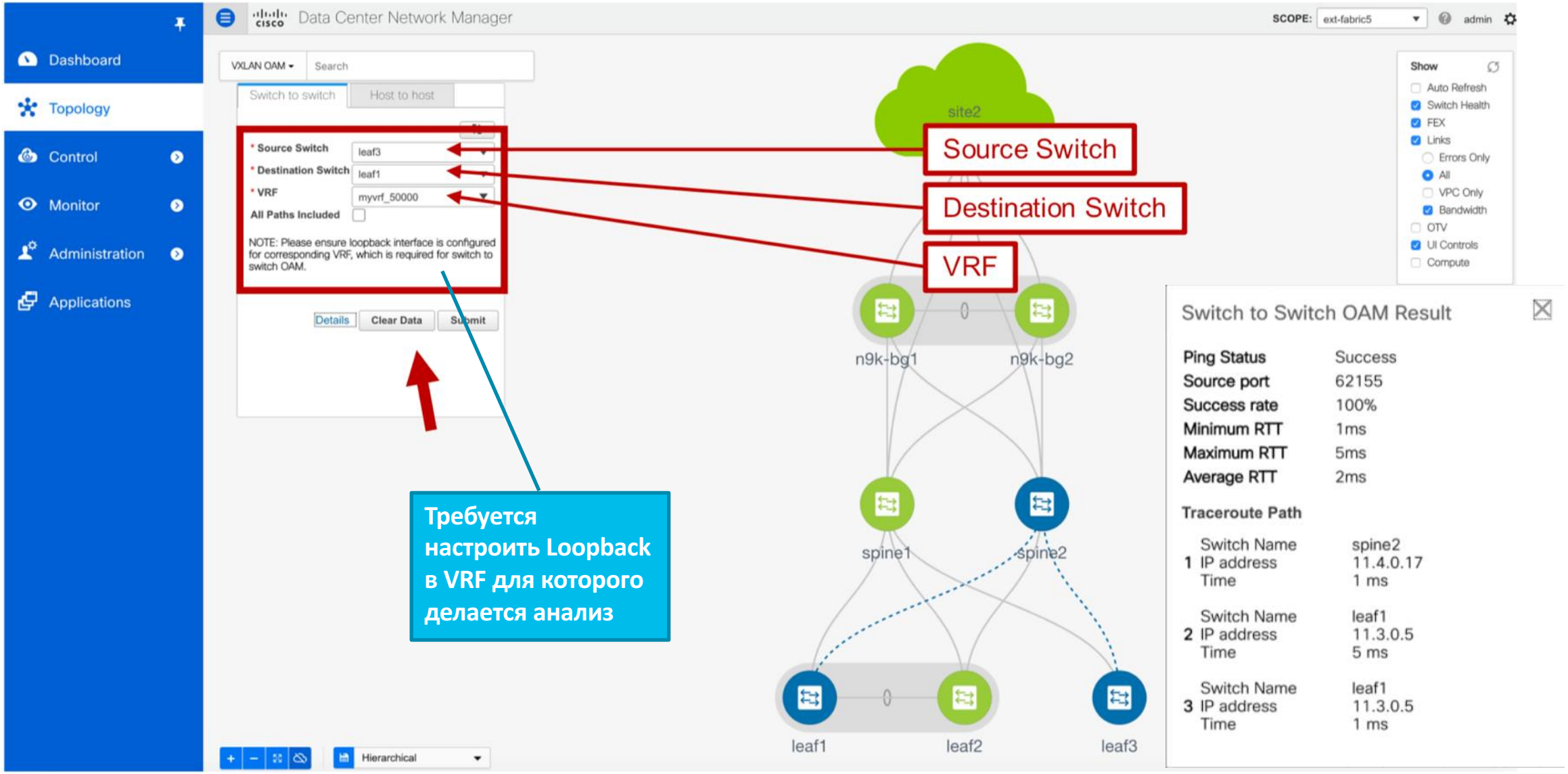
Отображение DVS/Vswitch

Отображение ВМ

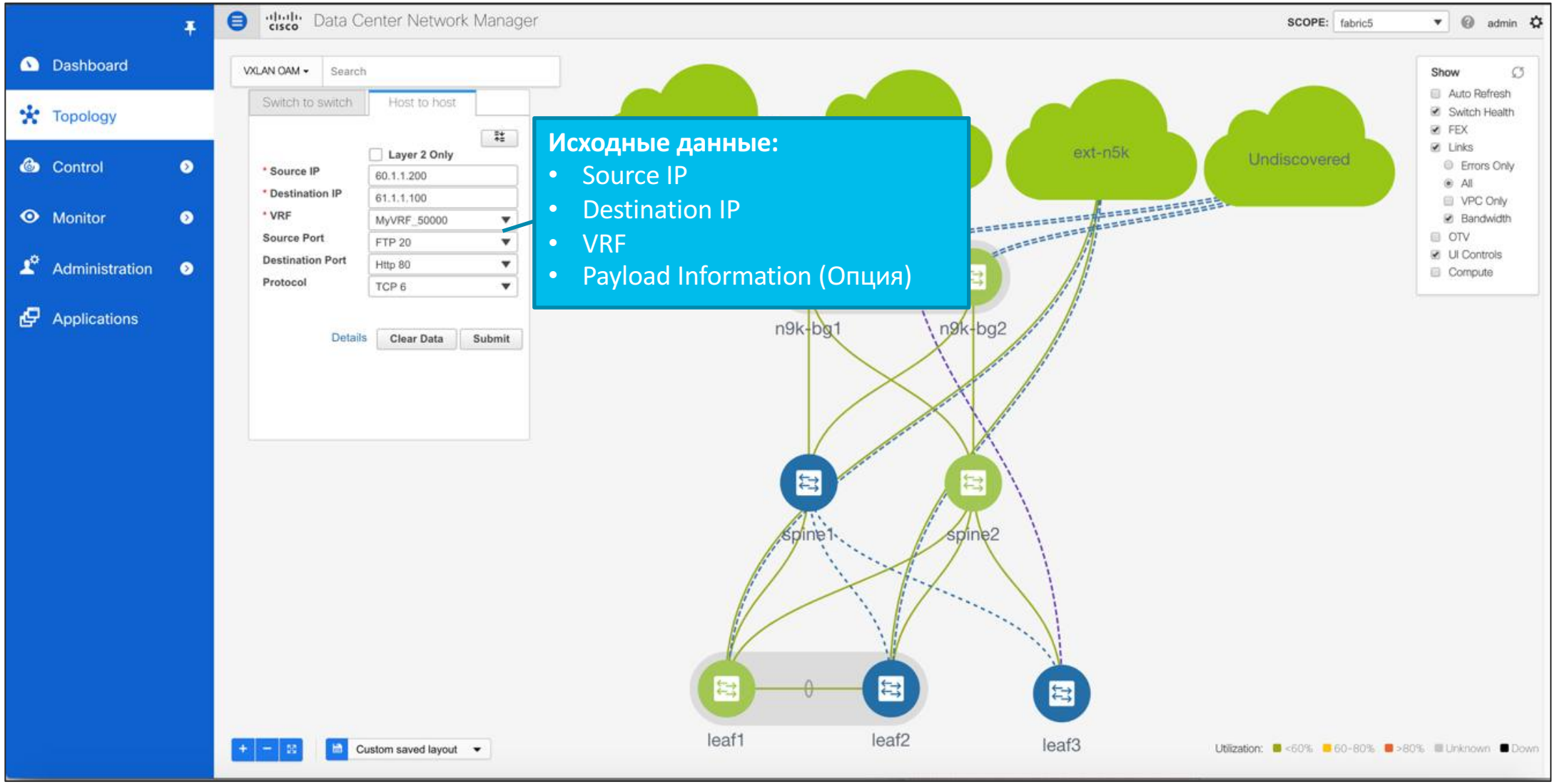
Virtual Machine Manager (VMM) – видимость происходящего на VMware vCenter

VXLAN OAM – возможности, встроенные в DCNM

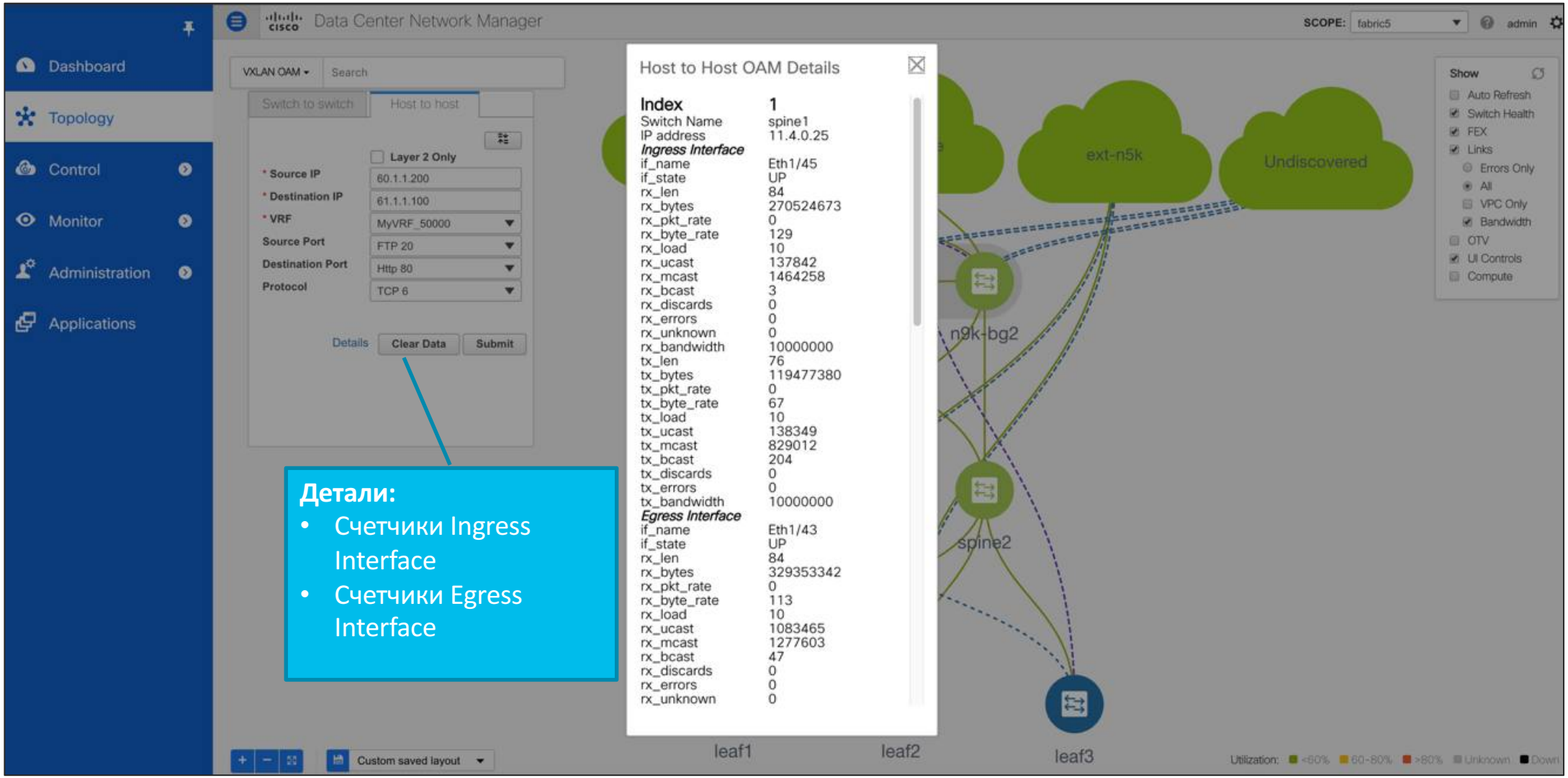
Day *2 Operations - мониторинг*
VXLAN OAM – Ping Trace Route



Day *2 Operations* - мониторинг
VXLAN OAM – Endpoint Path Trace



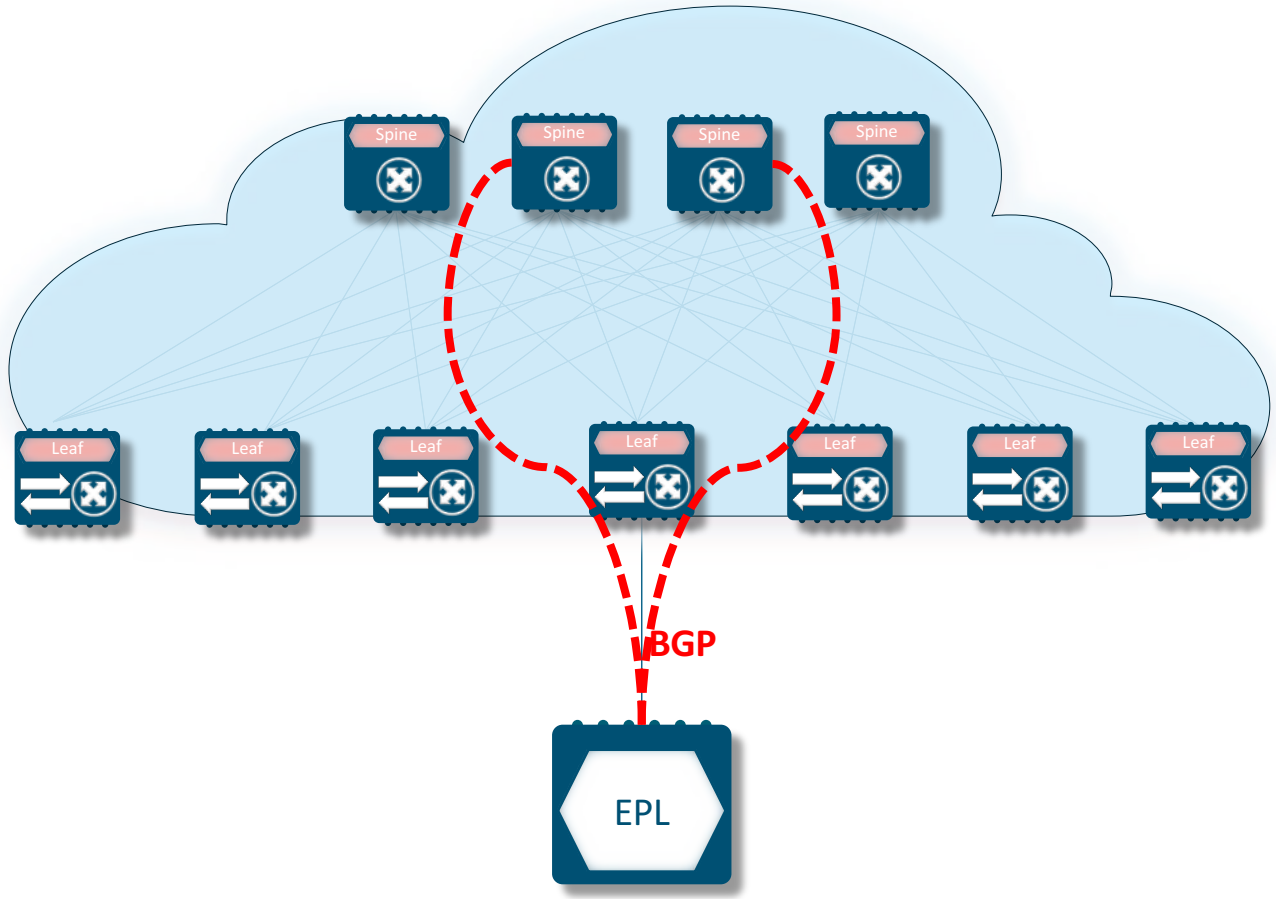
Day *2 Operations* - мониторинг
VXLAN OAM – Endpoint Path Trace



End Point Locator

Day *2 Operations* - мониторинг

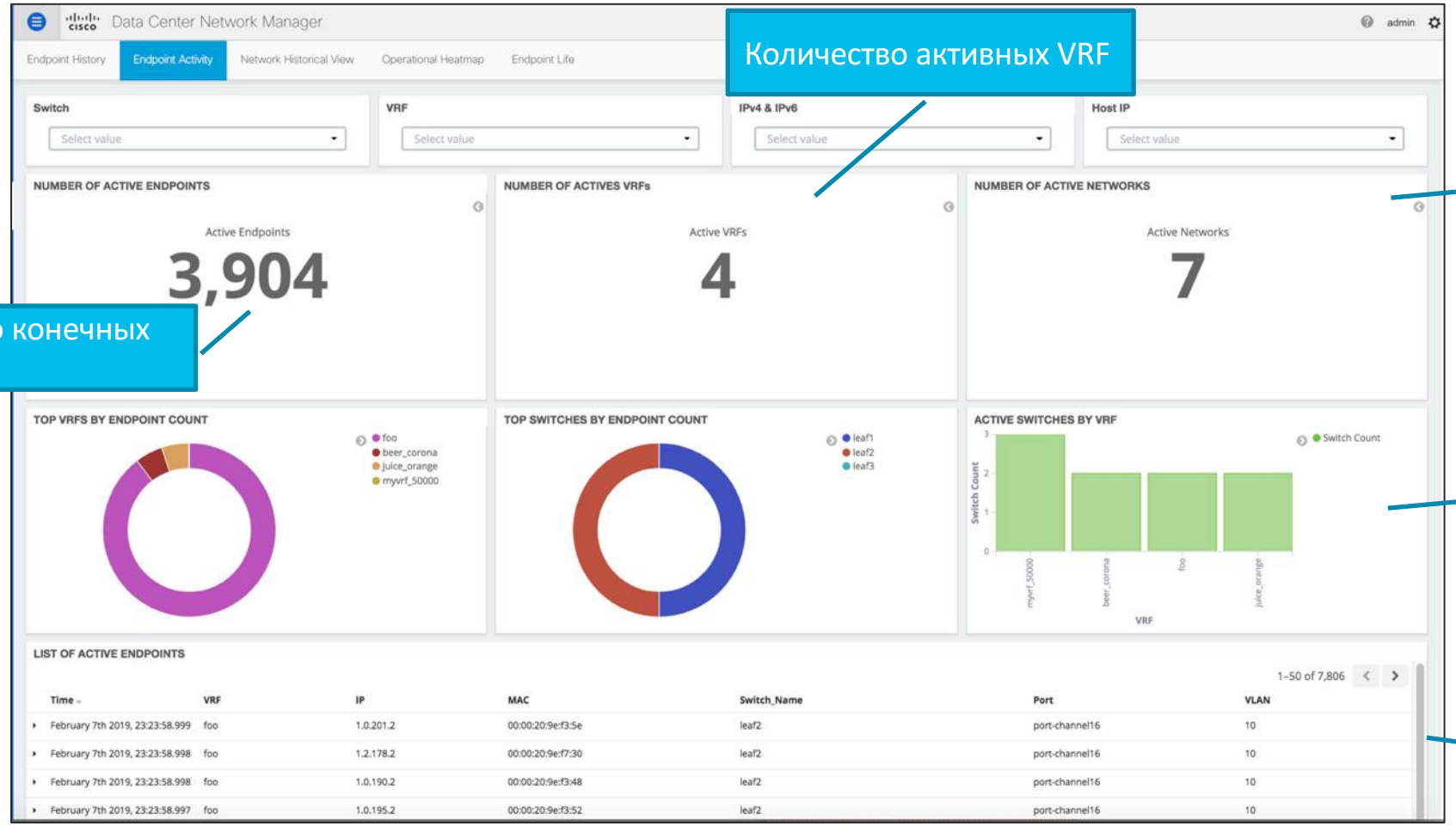
Мониторинг подключений



- Endpoint Locator (EPL)
  - Приложение внутри DCNM
  - Пиринг с Overlay Control-Plane (i.e. BGP EVPN)
  - BGP Receiver only (Passive)
- Создание БД поиск в которой можно производить в реальном масштабе времени
- Сохранение каждого события Endpoint Control-Plane
- Корреляция с инвентаризационными данными

Day *2 Operations* - мониторинг

Endpoint Monitoring Lifecycle



Количество активных VRF

Количество активных сетевых сегментов

Количество конечных хостов

Активных коммутаторов на VRF

Детали по конечным хостам

Endpoint Locator (EPL)

Лицензия Premier

Nexus Assurance Engine

Cisco Network Assurance Engine

Как валидировать сеть – сейчас и на будущее?

Предсказать* и показать результат изменений

Проверить состояние в масштабах сети

Гарантировать политику безопасности и ее соответствие*

Проверка изменений

Диагностика

Динамические проблемы

Оптимизация

Передача

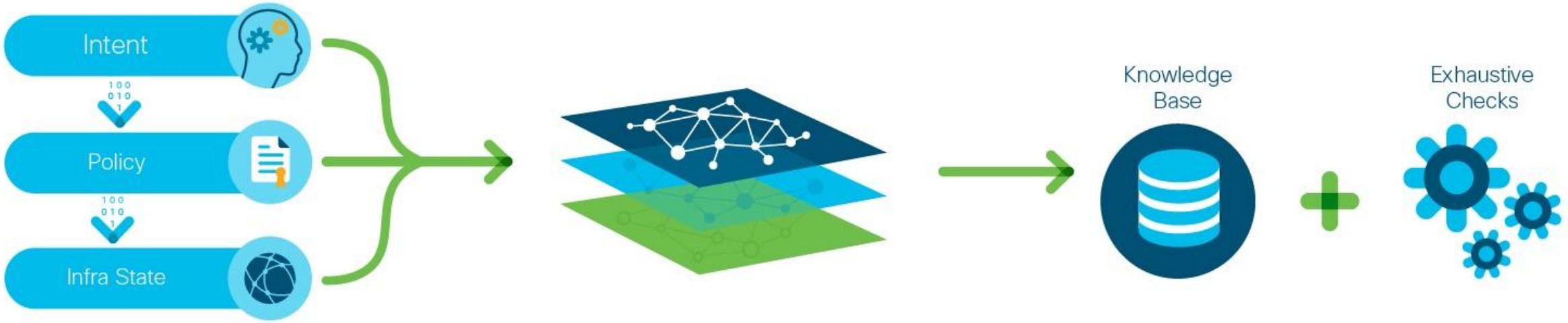
Соответствие

Подключения

Безопасность*

* Поддерживается только для ACI фабрики на момент релиза NAE 5.1(1a)

Как работает Cisco Network Assurance Engine



Сбор данных

Сбор всех данных о сети: намерения,политика, состояние

Формальное моделирование сети

Математически точное моделирование на основе 30+ лет опыта Cisco в сетях и смежных областях

Интеллектуальный анализ

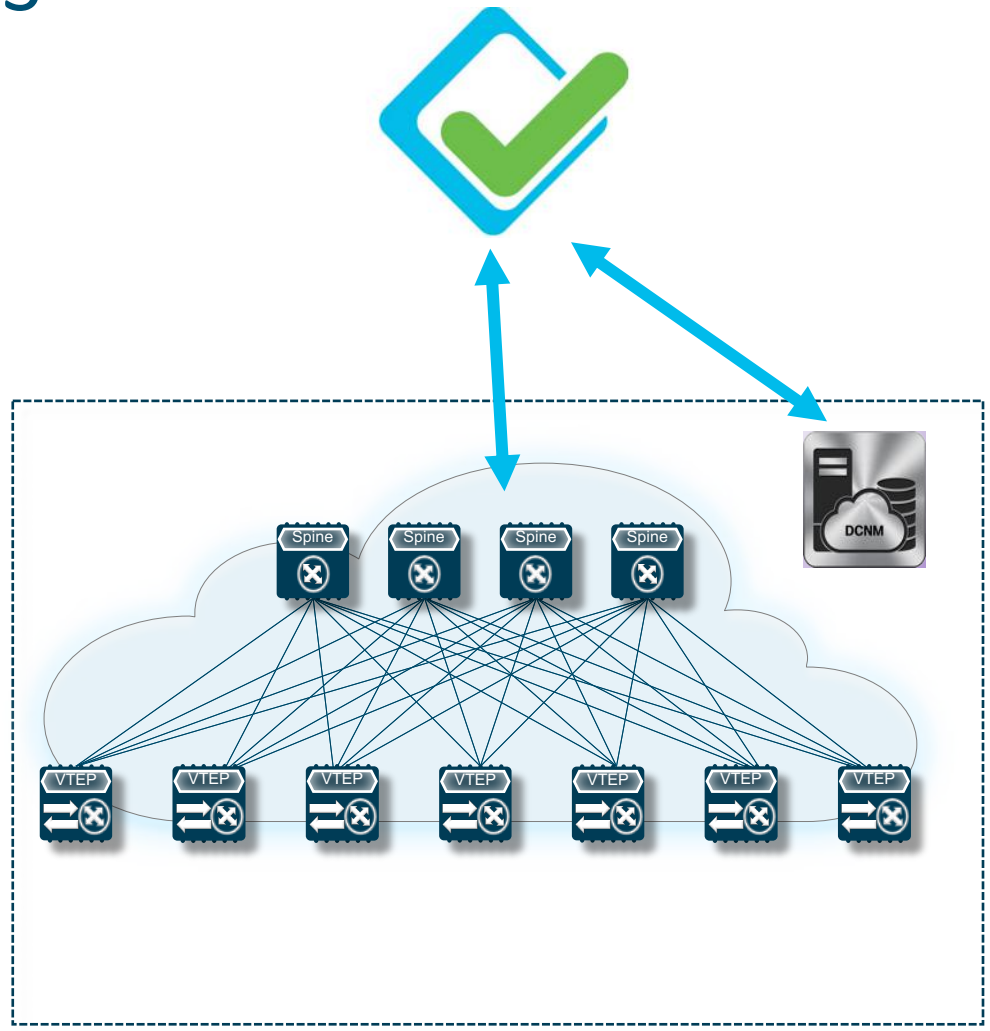
Контроль того, что сеть реализует намерения, и информация о том, что не так, где, почему, на что влияет и как устранить

5000+ сценариев проблем и ошибок

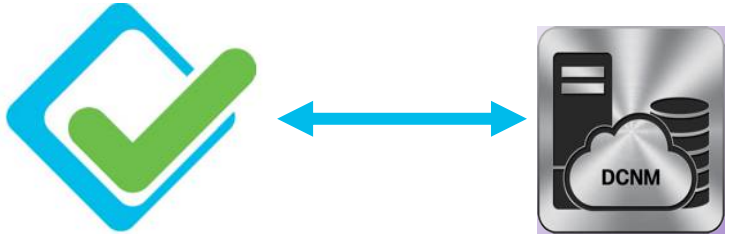
От устранения проблем к проактивной эксплуатации – непрерывно, в масштабах всей сети

NAE для фабрик ЦОД на основе NX-OS

- Контроль согласованности конфигураций и поведения в масштабах фабрики
- Обнаружение сетевой топологии с помощью DCNM
- Опрос конфигурации и состояния коммутаторов (с использованием NXAPI CLI и NXAPI REST) и построение сетевой модели для анализа
- Контроль многих фабрик на одном NAE с использованием assurance groups
  - Множество VXLAN фабрик/сайтов
  - Или смесь ACI и VXLAN фабрик

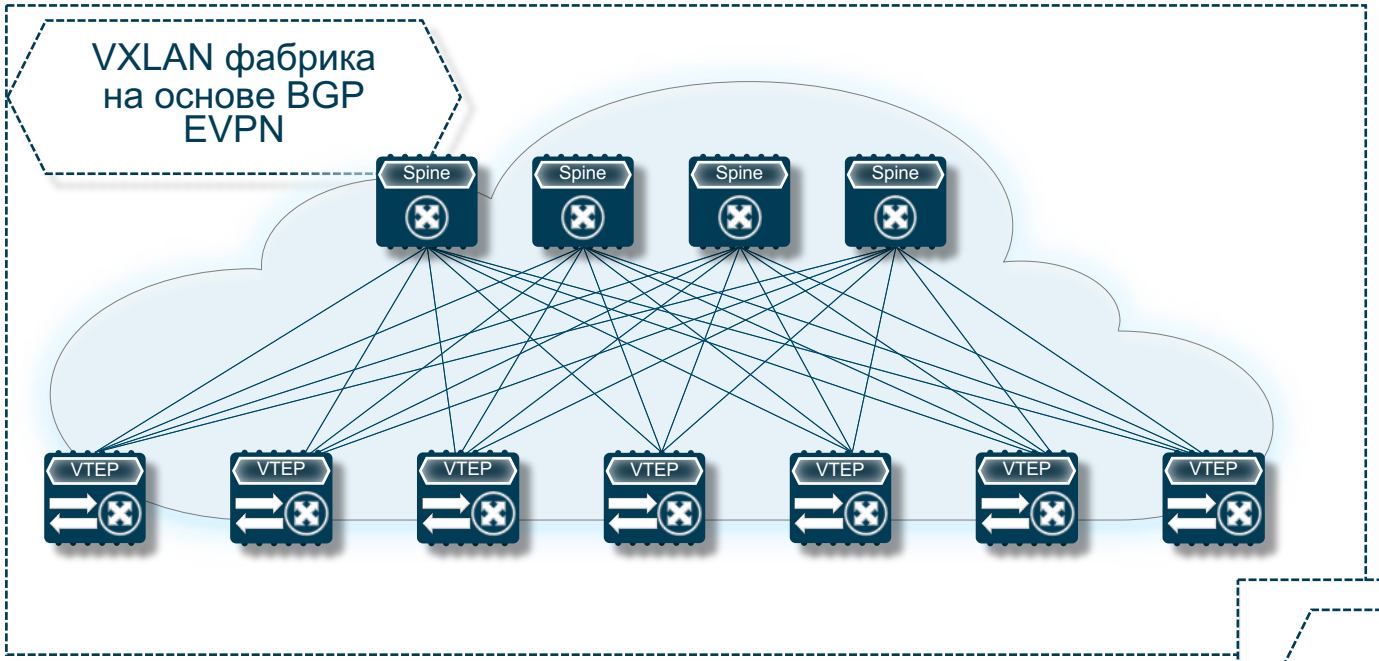


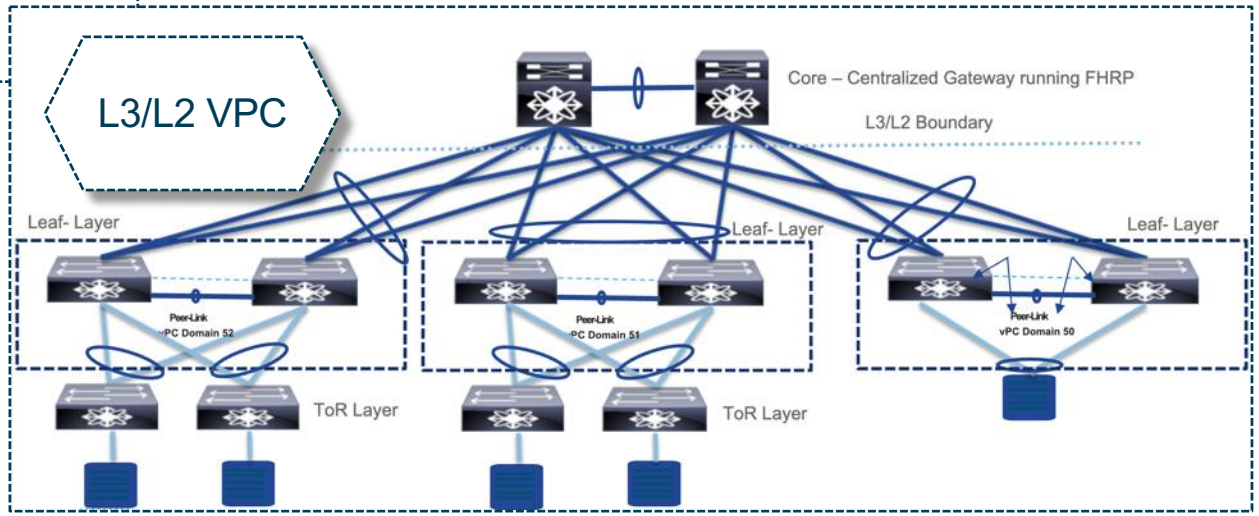
Замечание относительно DCNM



- Версия NAE 5.x требуется DCNM для получения информации о топологии
- Информация о желаемом состоянии оборудования, которая получается от DCNM ограничена
- Интеграция с DCNM поддерживается в 2-х режимах
  - Managed mode
  - Unmanaged mode
- Источниками событий о неконсистентном состоянии является анализ и сравнение конфигурации NX-OS устройства и его операционного состояния, с которыми NAE работает напрямую минуя DCNM

Поддерживаемые топологии в режиме NX-OS





NAE Smart Events

Smart Events
Какую информацию они дают

Что ?

⚠ MAJOR	CHANGE_ANALYSIS	VPC	VPC_DOMAIN_PEER_INCONSISTENT
⚠ MAJOR	FORWARDING	VPC	VPC_LACP_CONVERGENCE_ERROR

Кто и где?

Switch Name	vPC Domain Id	vPC-Id	Interface
DC1-BGW2	**4**	1	po1

Почему ?

Failing Condition
lacp vpc-convergence not configured on edge ports

Как устранить?

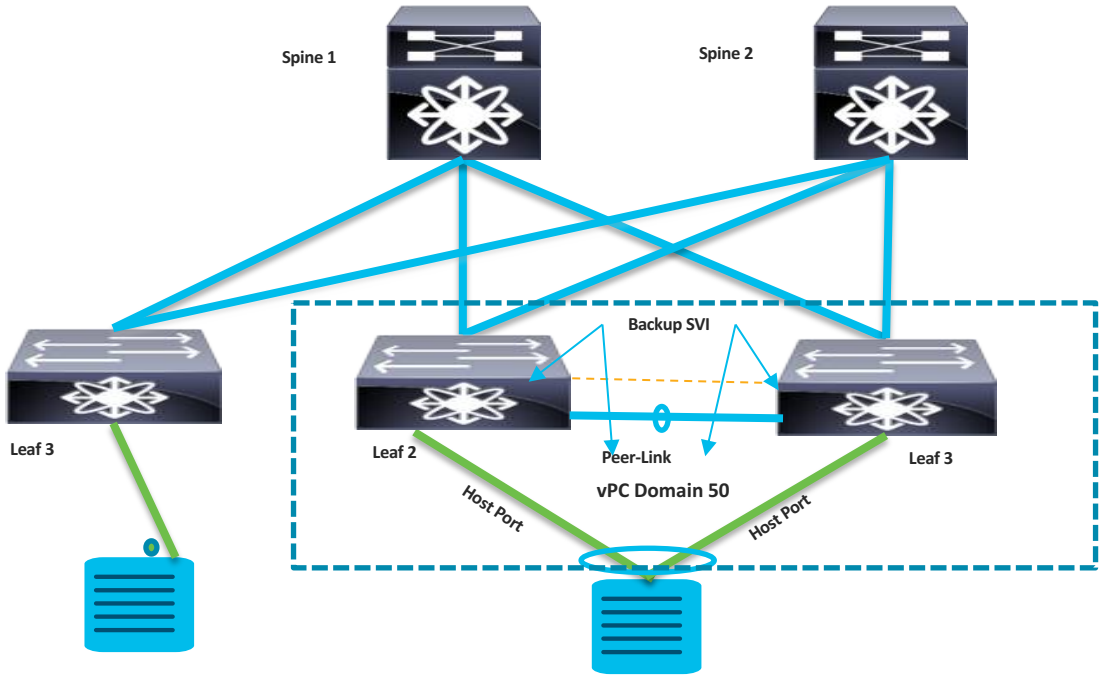
Suggested Next Steps
For best VPC convergence result make sure to configure lacp vpc-convergence under port-channel

Возможности по анализу NX-OS фабрик

Функция	VXLAN EVPN	L2/L3 vPC
VNI	Поддерживается	N/A
Underlay	Поддерживается (5.1)	Не поддерживается
BGP EVPN	Поддерживается (5.1)	N/A
vPC	Поддерживается	Поддерживается
L1	Поддерживается	Поддерживается
Endpoints	Поддерживается (5.1)	Не поддерживается

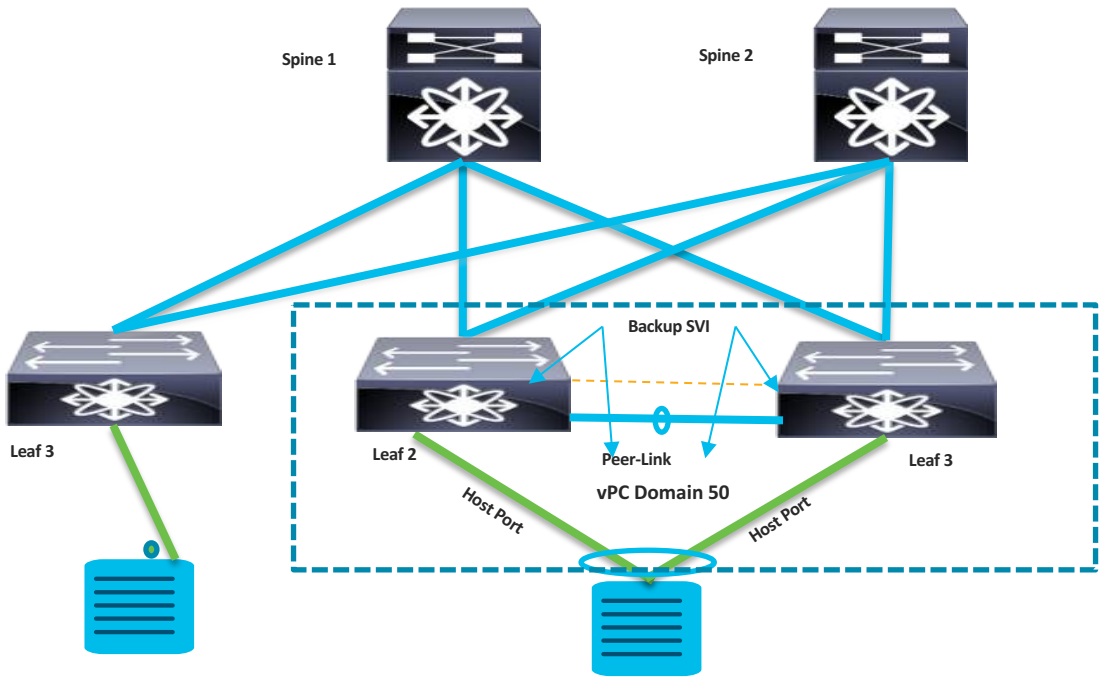
подробности по EVPN далее в этой презентации

VPC Assurance



- Проверка консистентности между участниками VPC пары
  - Type 1 и Type 2
- Ошибки peer-keepalive
- Backup SVI неконсистентность
- VPC host ports best practice
- VPC orphans best practice
- Консистентность настройки интерфейсов
- Проверка Peer link
- Проверка Feature vPC

vPC Smart Events



1	VPC_DOMAIN_OR_IP_MISCONFIGURED
2	VPC_DOMAIN_INCONSISTENT
3	VPC_PEER_KEEP_ALIVE_ERROR
4	VPC_PARAMETERS_INCONSISTENT
5	VPC_BACKUP_SVI_INCONSISTENT
6	VPC_BACKUP_VLAN_INCONSISTENT
7	VPC_BACKUP_SVI_ROUTING_ERROR
8	VPC_HOST_PORT_BEST_PRACTICE_CONFIG
9	VPC_ORPHAN_PORT_BEST_PRACTICE_CONFIG
10	VPC_LACP_CONVERGENCE_ERROR
11	VPC_PEER_LINK_ERROR

Пример из GUI

Description	The NVE infra VLAN or the vPC backup VLAN configuration error.
Impact	If a vPC switch has no uplinks, either due to misconfiguration or lack of an alternate path, traffic will be lost.

Affected Objects Details

Switch Name	vPC Domain Id	Nve Infra VLAN
N92160-L1b-S1	**1**	Vlan3900 Vlan3901

Checks

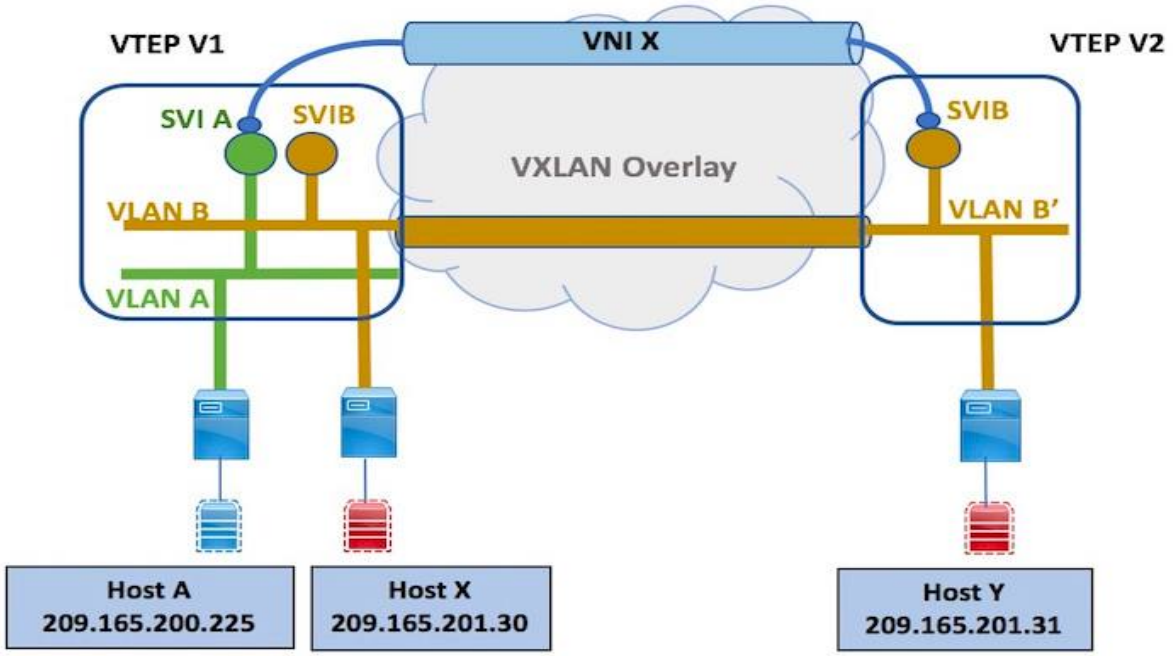
nve infra VLAN is configured but not allowed as part of the peer link

Check Code	Failing Condition	Suggested Next Steps

7015	The NVE infra VLAN is configured but is not allowed as part of the peer link.	Ensure that the NVE Infra VLAN is part of the allowed VLAN list on the vPC peer link.
		
		Example:
		`interface port-channel Y`
		`peer-switch`
		`switchport trunk allowed vlan add <X>`
		
		Helpful CLI:
		• `show vpc`
		• `show interface port-channel Y trunk`

Switch Name	Peer Link	Allowed VLANs	Nve Infra VLANs not on Peer Link
N92160-L1b-S1	po500	[1, 11-15, 21, 23-24, 33-34, 77, 88, 99, 2000-2001, 3600]	-

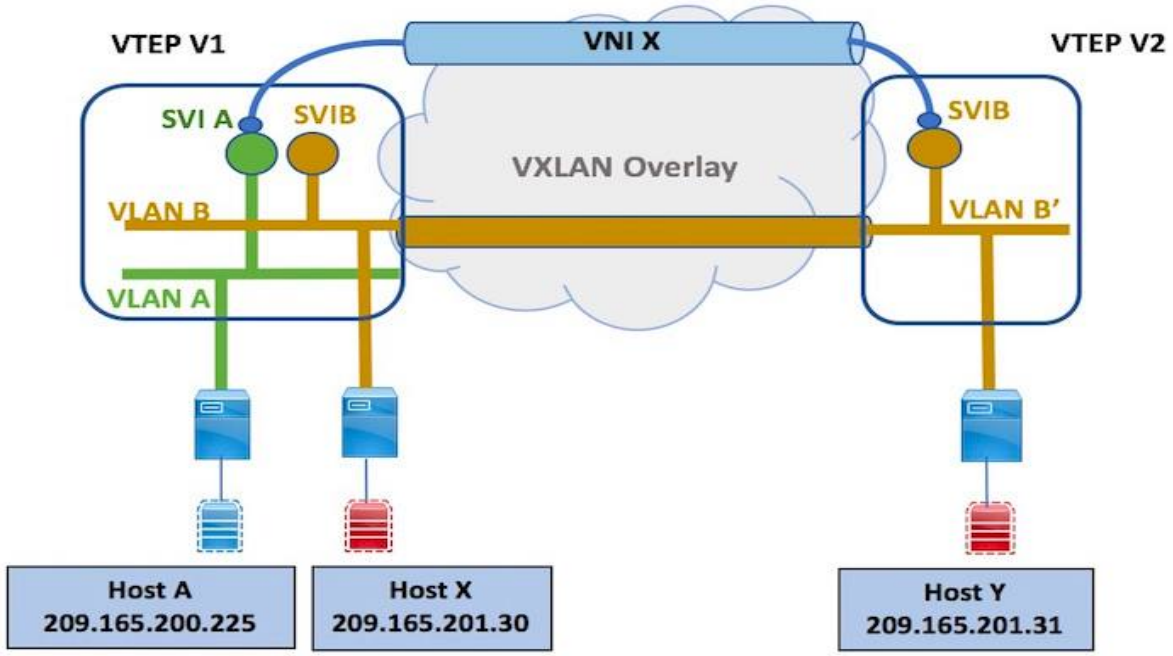
VNI Assurance



Настройка и изменения VNI

- Разные отображения VNI в VLAN на разных коммутаторах
- L2/L3 VNI configuration inconsistent
  - Например: replication mode, ingress replication, suppress arp, mcast group IP
- Консистентность L2/L3 VNI SVI
  - Например: VRF mapping, Anycast Gw enabled, MTU mismatch
- L2/L3 VNI SVI Operational Status
- L2/L3 VNI Operational Status

VNI Smart Events



	VNI Checks
1	L2_VNI_MISMATCH_VLAN
2	L3_VNI_MISMATCH_VLAN
3	L2_VNI_SVI_INCONSISTENT_CONFIG
4	L2_VNI_SVI_OPER_DOWN
5	L2_VNI_SVI_SECONDARY_IP_NOT_UNIQUE
6	L2_VNI_INCONSISTENT_CONFIG
7	L2_VNI_OPER_DOWN
8	L3_VNI_SVI_INCONSISTENT_CONFIG
9	L3_VNI_SVI_OPER_DOWN
10	L3_VNI_INCONSISTENT_CONFIG
11	L3_VNI_OPER_DOWN

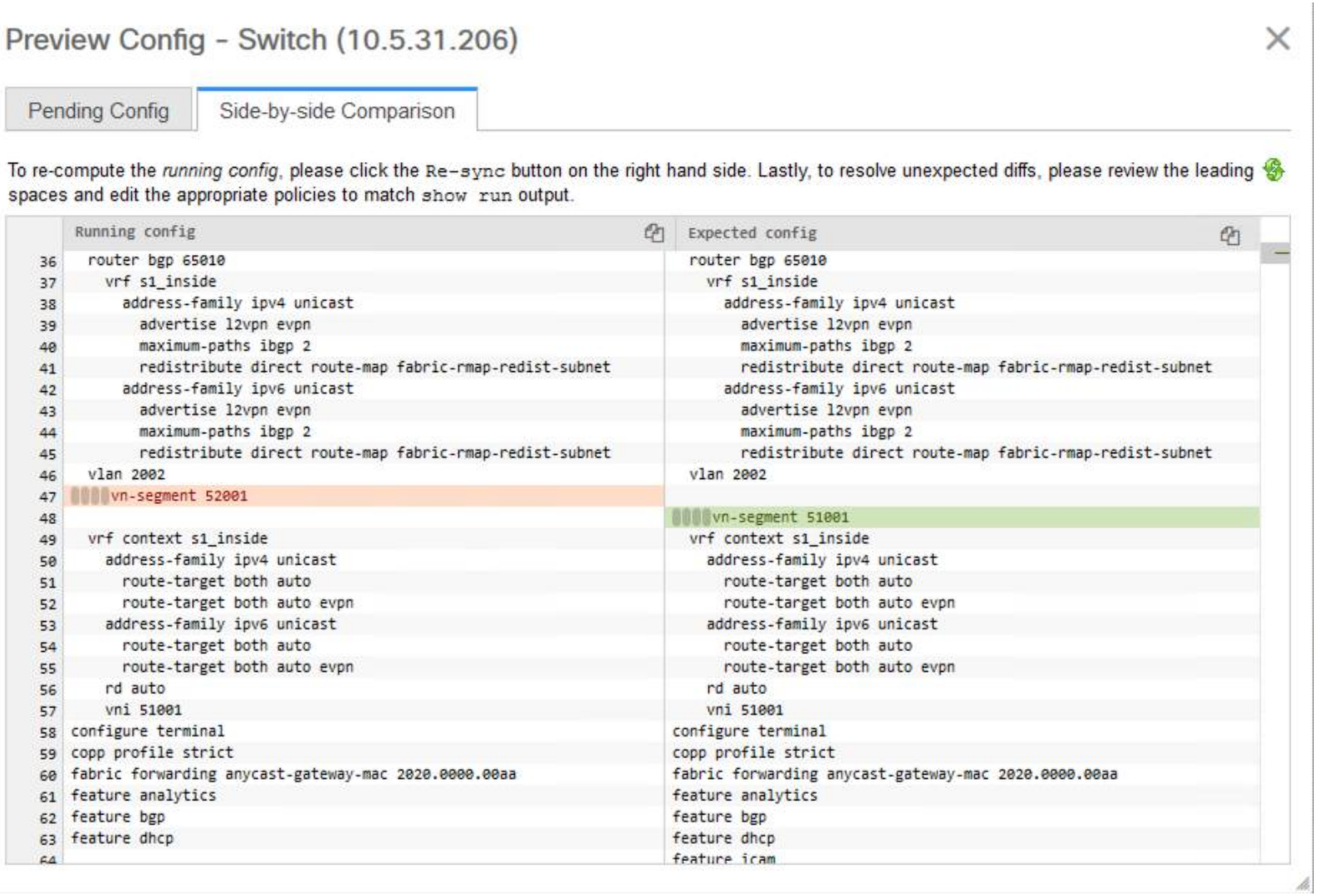
Пример из GUI

Description	A fabric-wide check has found inconsistent configuration on L2 VNI.
Impact	Traffic across VTEPs could be disrupted.
Affected Objects Details	L2 VNI **30014***
Checks	The L2 VNI is associated with an SVI on some VTEPs but not on others

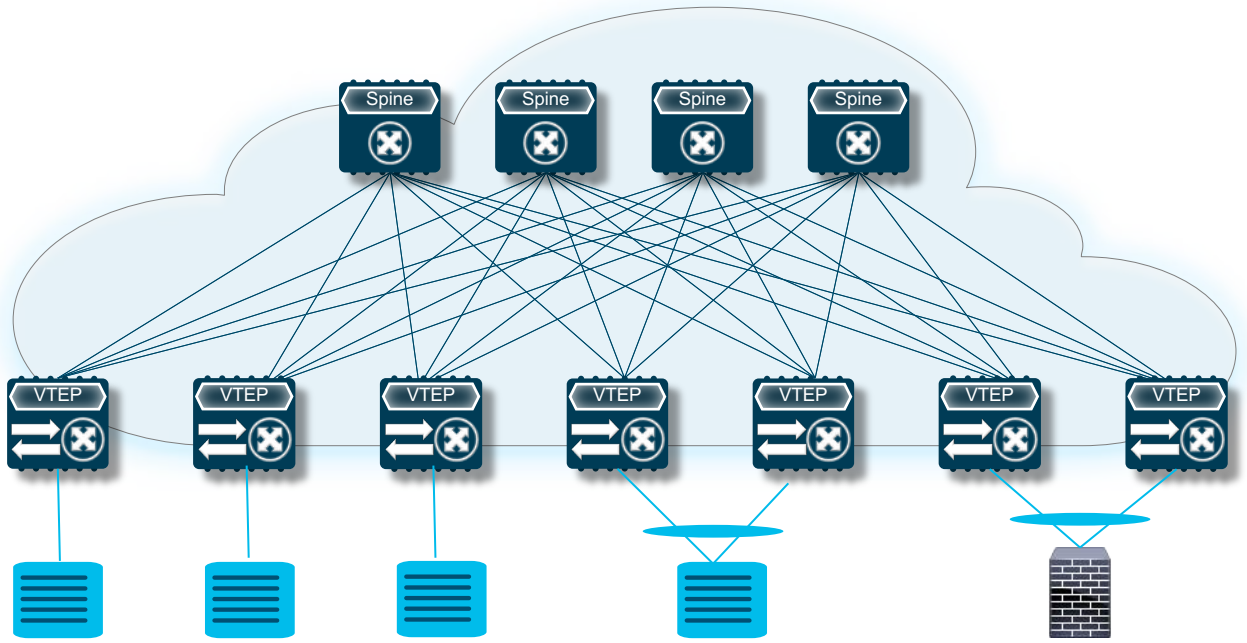
Check Code	Failing Condition	Suggested Next Steps
7115	The L2 VNI is associated with an SVI on some VTEPs but not on others.	Ensure that Anycast Gateway SVIs are defined on all VTEPs where L2VNI is present. Helpful CLI: • `show interface vlan X` • `show run interface vlan X`

SVI Associated?	Switch List
YES	Switch Name N92160-L1b-S1 N92160-L1a-S1
NO	Switch Name N93180EX-L3-S1

Устраняем неисправность

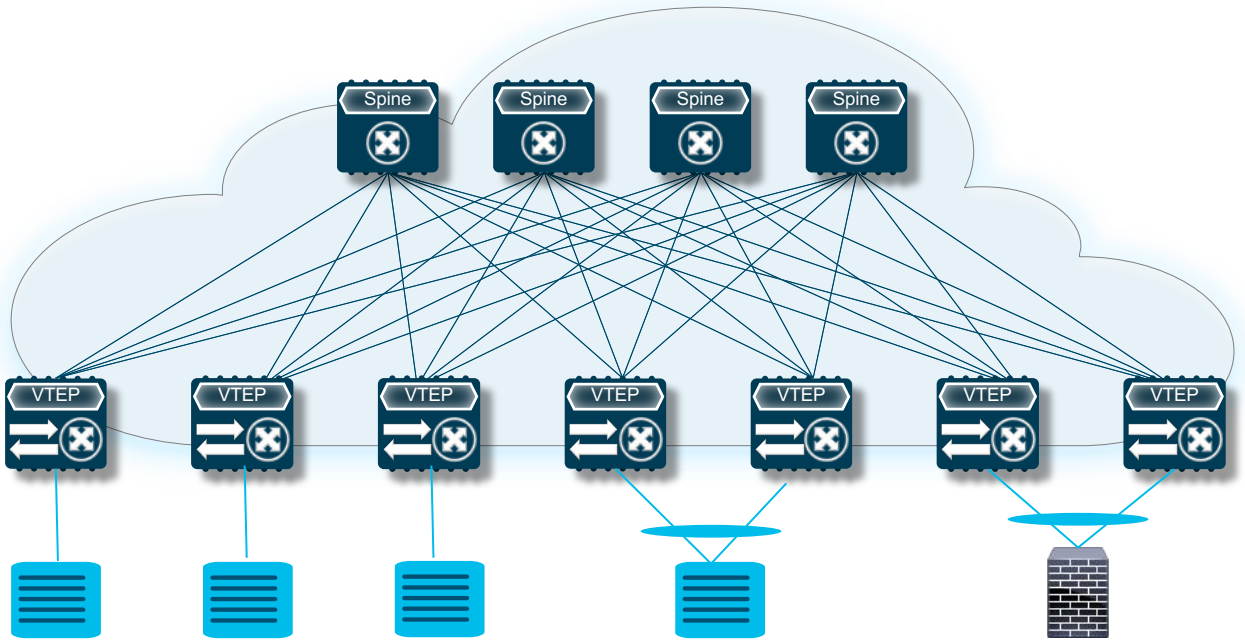


Layer 1 Assurance



- Проверка конфигурации и операционного состояния физических интерфейсов
- Обнаружение ситуации ”partial port-channel membership”

L1 Smart Events



	L1 Checks
1	PHYSICAL_INTERFACE_OPER_DOWN_ADMIN_DOWN
2	PC_INTERFACE_OPER_DOWN_ADMIN_DOWN
3	PHYSICAL_INTERFACE_OPER_DOWN_ADMIN_UP
4	PC_INTERFACE_OPER_DOWN_ADMIN_UP
5	PC_INTERFACE_OPER_UP_PARTIAL_MEMBER_OPER_UP
6	FABRIC_INTERFACE_OPER_DOWN_ADMIN_DOWN
7	FABRIC_INTERFACE_OPER_DOWN_ADMIN_UP

Dashboard

Smart Events by Severity

Critical	Major	Minor	Warning	Info	Total
0	228	0	0	10	238

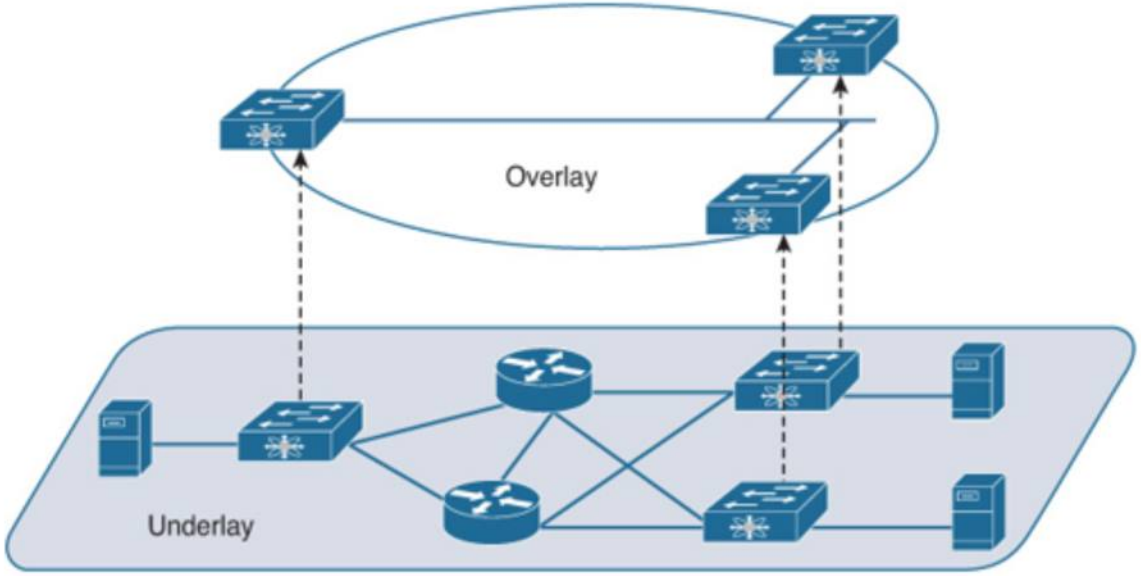
Category	Critical	Major	Minor	Warning	Info	Total
System	0	1	0	0	10	11
Change Analysis	0	6	0	0	0	6
Forwarding	0	221	0	0	0	221
Endpoint	0	0	0	0	0	0

Unhealthy Count by Resource

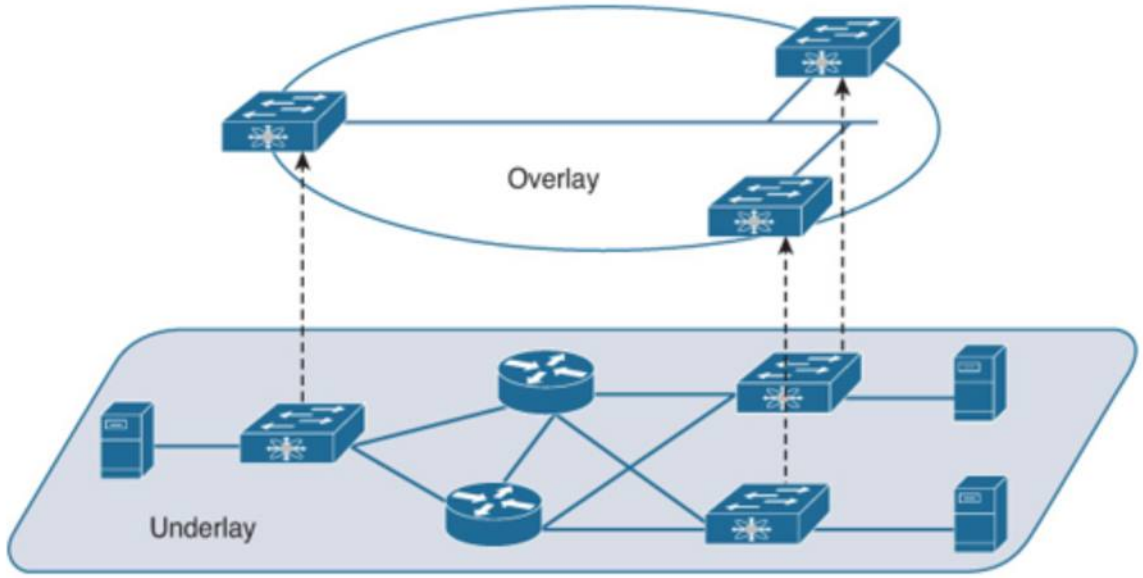
VRFs	VNIs	VLANs	VPCs	Interfaces	Leafs
0 / 3	0 / 10	0 / 7	2 / 2	270 / 367	0 / 4

EVPN Assurance

- Проверка консистентности RD и RT для каждого VRF
- Полнота конфигурации для BGP L2VPN EVPN



EVPN Smart Events



	EVPN Checks
1	EVPN_L2_VNI_INCONSISTENT_CONFIG
2	EVPN_VRF_IP4_INCONSISTENT_CONFIG
3	EVPN_VRF_IPV6_INCONSISTENT_CONFIG
4	EVPN_BGP_VRF_IPV4_INCONSISTENT_CONFIG
5	EVPN_BGP_VRF_IPV6_INCONSISTENT_CONFIG
6	EVPN_BGP_NEIGHBOUR_INCONSISTENT_CONFIG

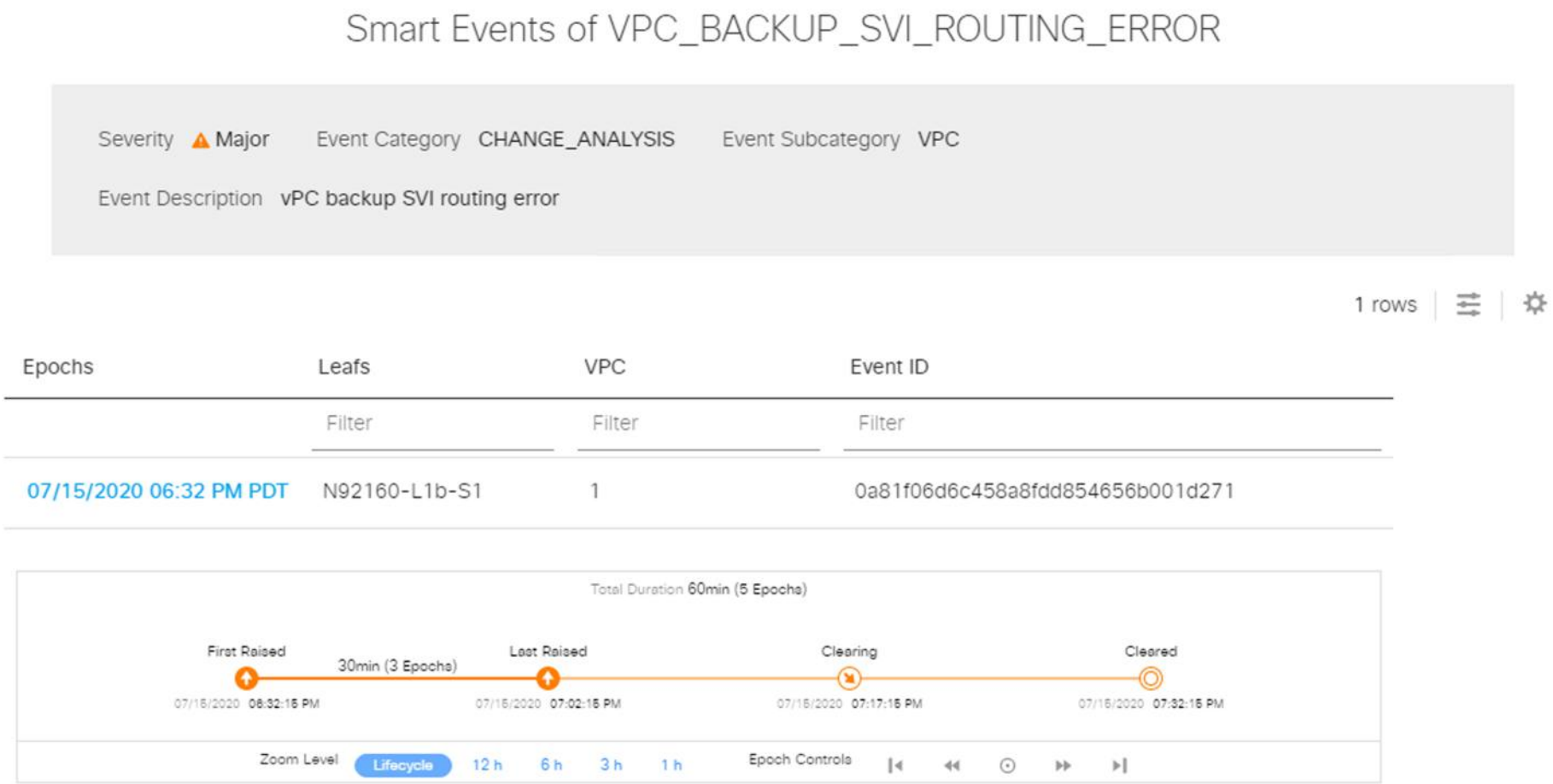
Пример из GUI

Description	The configuration of the VNI EVPN not consistent across fabric.
Impact	The traffic could be dropped or sub-optimal. Host mobility could fail. Switch operations may not be optimal.
Affected Objects Details	L2 VNI **30001***
Checks	Route Target Export value is not unique across all L2 VNIs in the fabric

Check Code	Failing Condition	Suggested Next Steps
7504	Route Target Export value is not unique across all L2 VNIs in the fabric	Ensure that 'route-target export X' parameter is unique across all L2 VNI in the switch. Each VNI must use a unique export value. Helpful CLI: • `show running bgp | section evpn` • `show system internal dme running-config all dn sys/evpn`

Switch Name	L2 VNI	Route Target Export Value
Rack2-Leaf2	20001	route-target:as2-nn2:20001:2
Rack2-Leaf2	30001	route-target:as2-nn2:20001:2

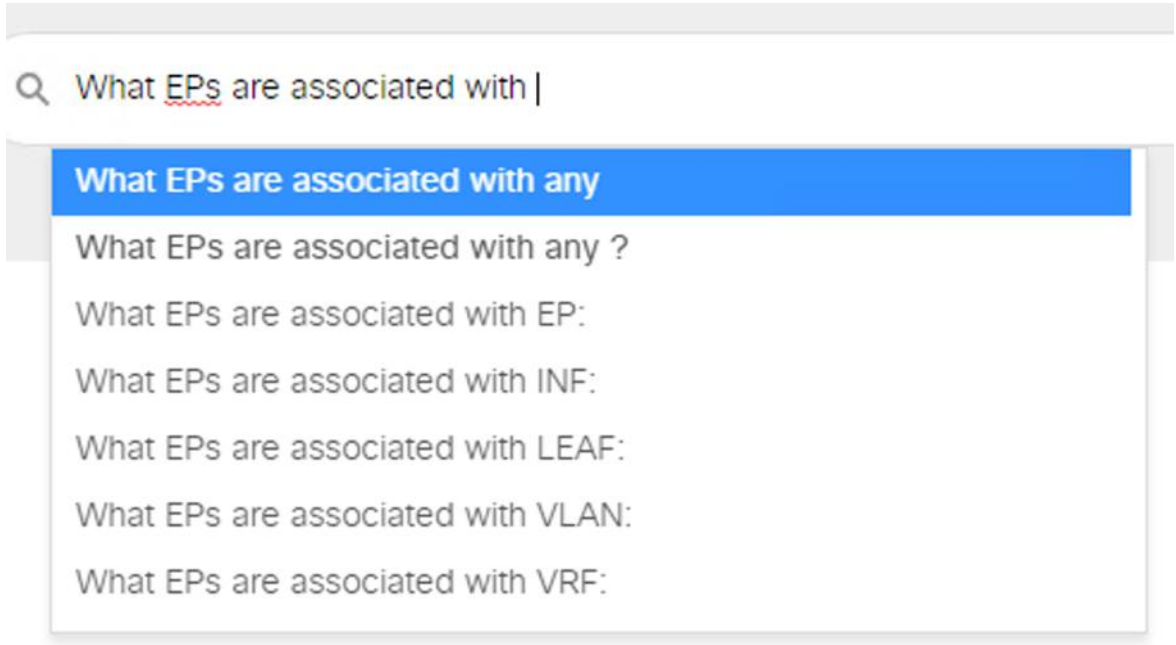
Жизненный цикл для Smart Event



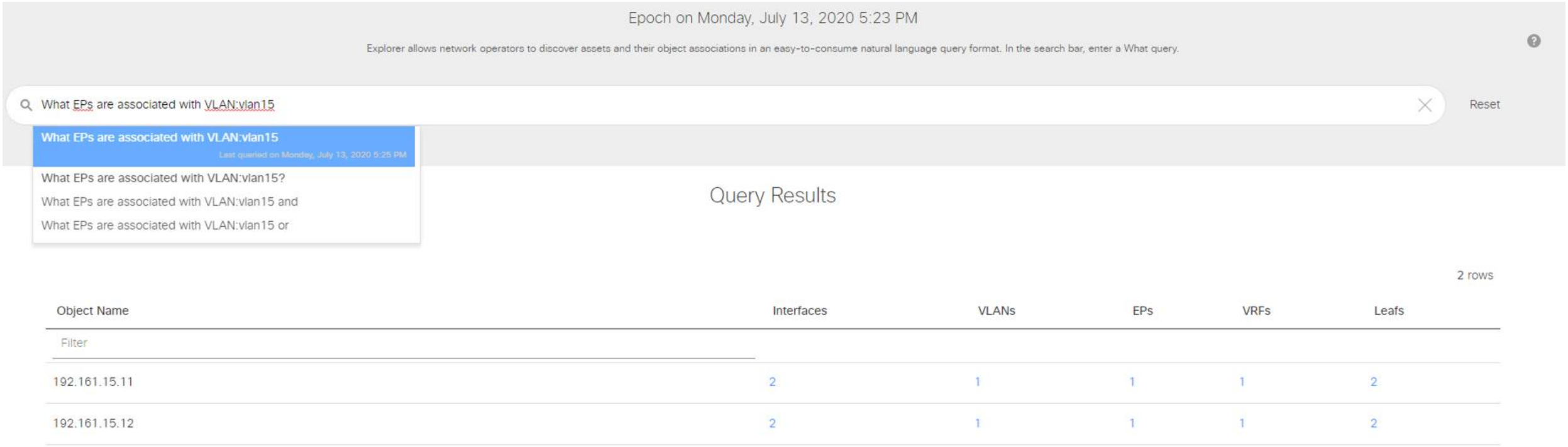
NAE Explorer

Endpoint Explorer

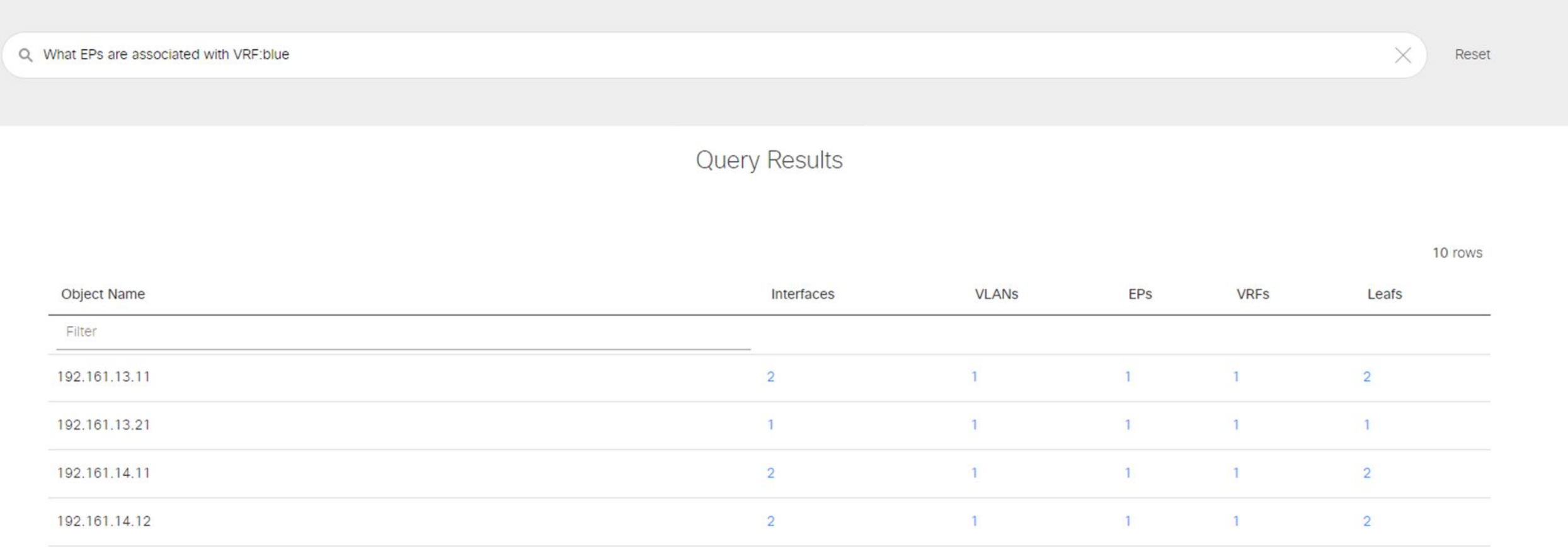
- Explorer дает делать разнообразные запросы о конечных хостах (endpoints), которые подключены к фабрике
- Например чтобы выяснить к какому коммутатору, VLAN, VRF они подключены в данный момент
- Пример запроса “What endpoints are associated with”
  - Any
  - INF (interface)
  - VLAN
  - LEAF
  - VRF



Пример запроса
Какие хосты внутри EVPN-фабрики подключены к VLAN?

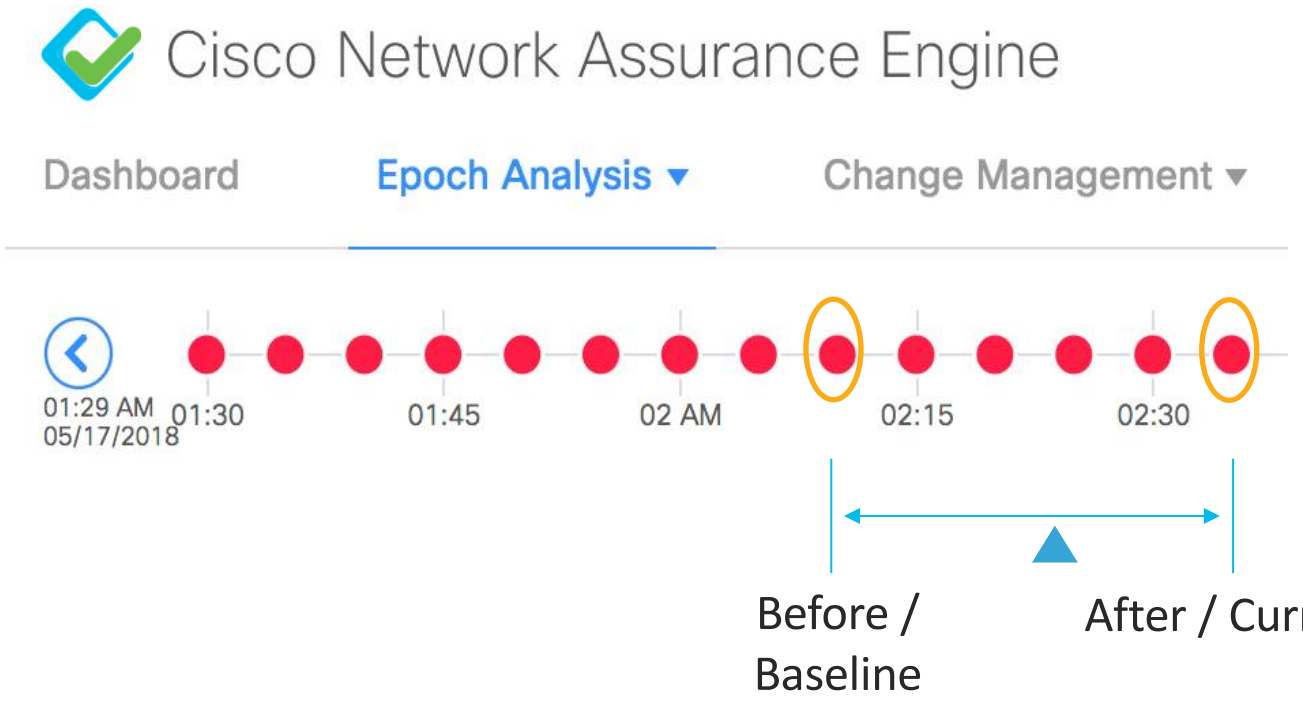


Пример запроса
Какие хосты внутри EVPN-фабрики подключены к VRF?



Анализ изменений

Анализ изменений между «эпохами»



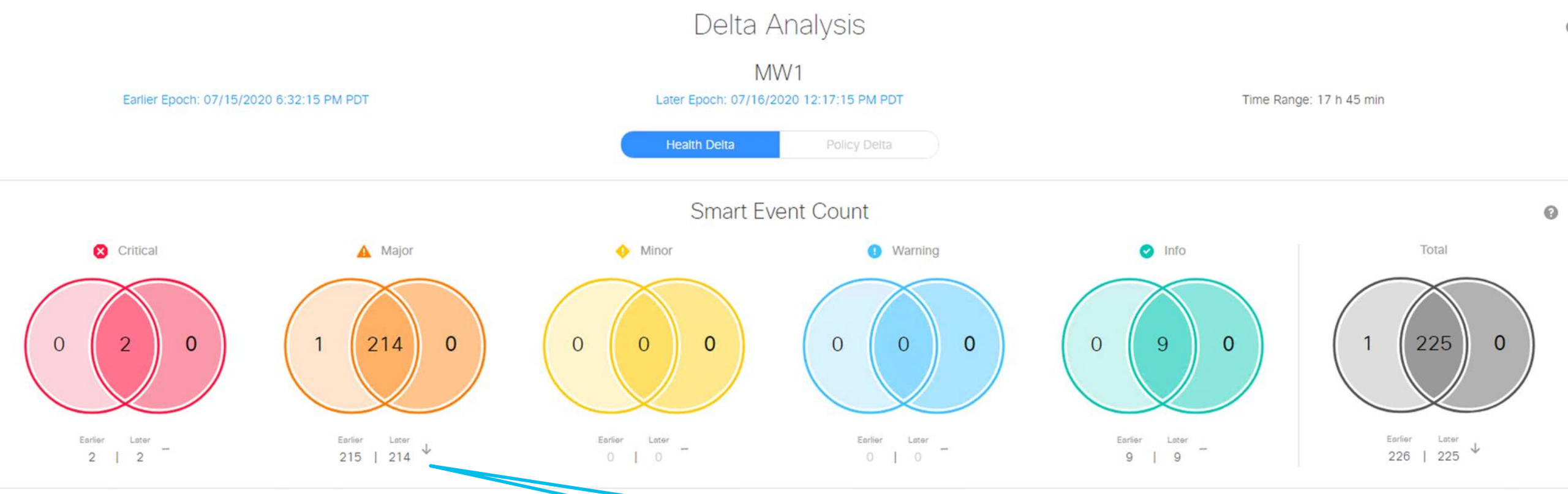
4 вопроса и ответы на них…

- Что изменилось?
- На что повлияло?
- Было ли связано с изменениями настройки?
- Что произошло в результате?

Сценарии

- Управление изменениями
- Поиск причин проблем
- Контроль апгрейдов

Общий анализ изменений между «эпохами»
Изменение «здоровья» фабрики



Количество событий между эпохами уменьшилось

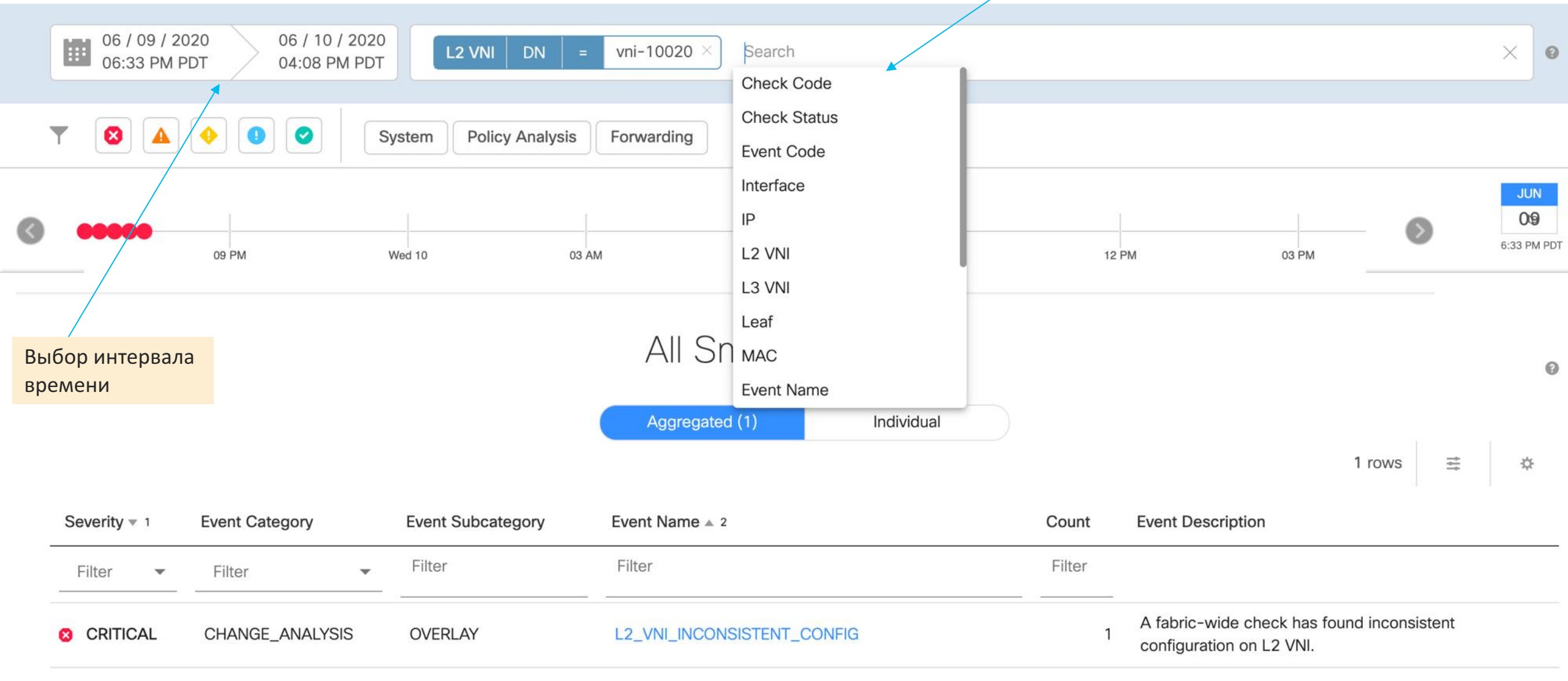
EPOC Delta Analysis

Health Delta by Resources

Resources	Total Earlier | Later		Unhealthy Earlier | Later		Total Unhealthy in Earlier Epoch Only	Total Unhealthy in Later Epoch Only	Total Unhealthy in Both Epochs	No Issues Earlier | Later	
VRFs	5 | 5	–	1 | 1	–	0	0	1	4 | 4	–
VNIs	21 | 21	–	8 | 8	–	0	0	8	13 | 13	–
VLANs	16 | 16	–	7 | 7	–	0	0	7	9 | 9	–
VPCs	1 | 1	–	1 | 1	–	0	0	1	0 | 0	–
Interfaces	278 | 277	↓	212 | 211	↓	1	0	211	66 | 66	–
Leafs	3 | 3	–	0 | 0	–	0	0	0	3 | 3	–

Глобальный поиск по всем изменениям

Поиск по объектам



Выбор интервала времени

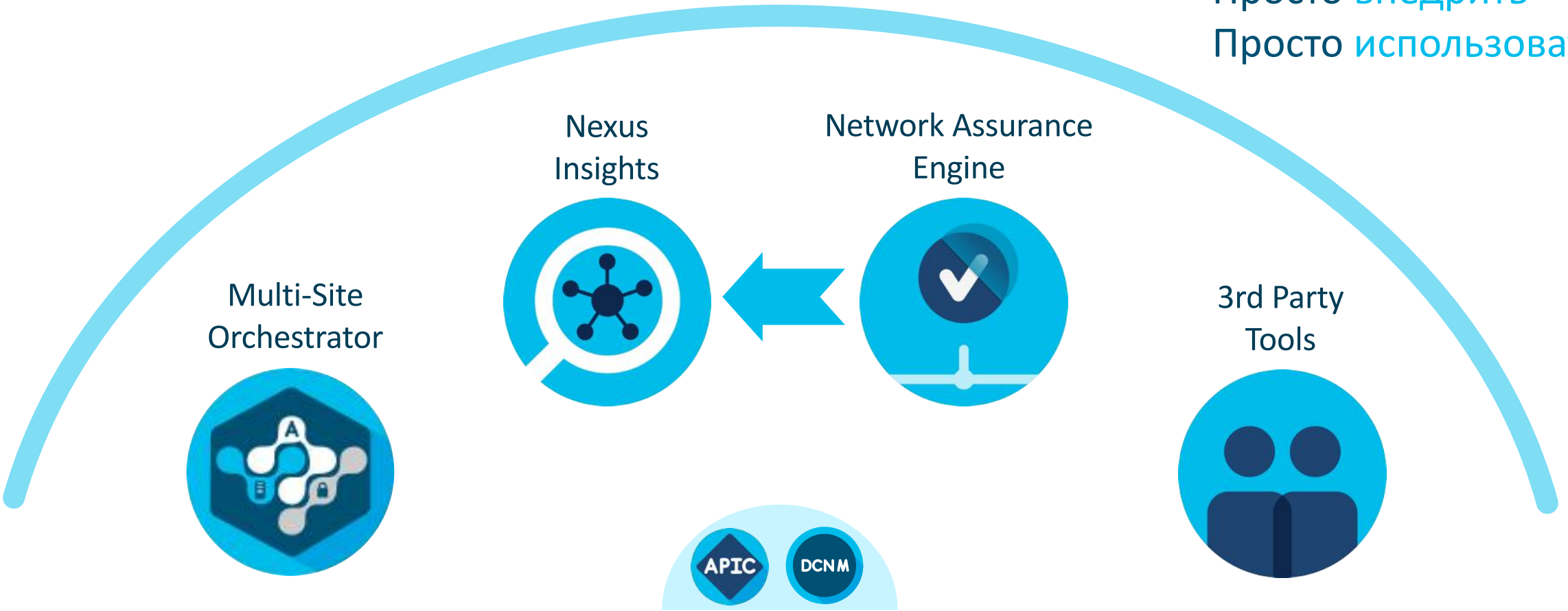
Nexus Dashboard

Nexus Dashboard

Трансформация подходов к эксплуатации сети ЦОД

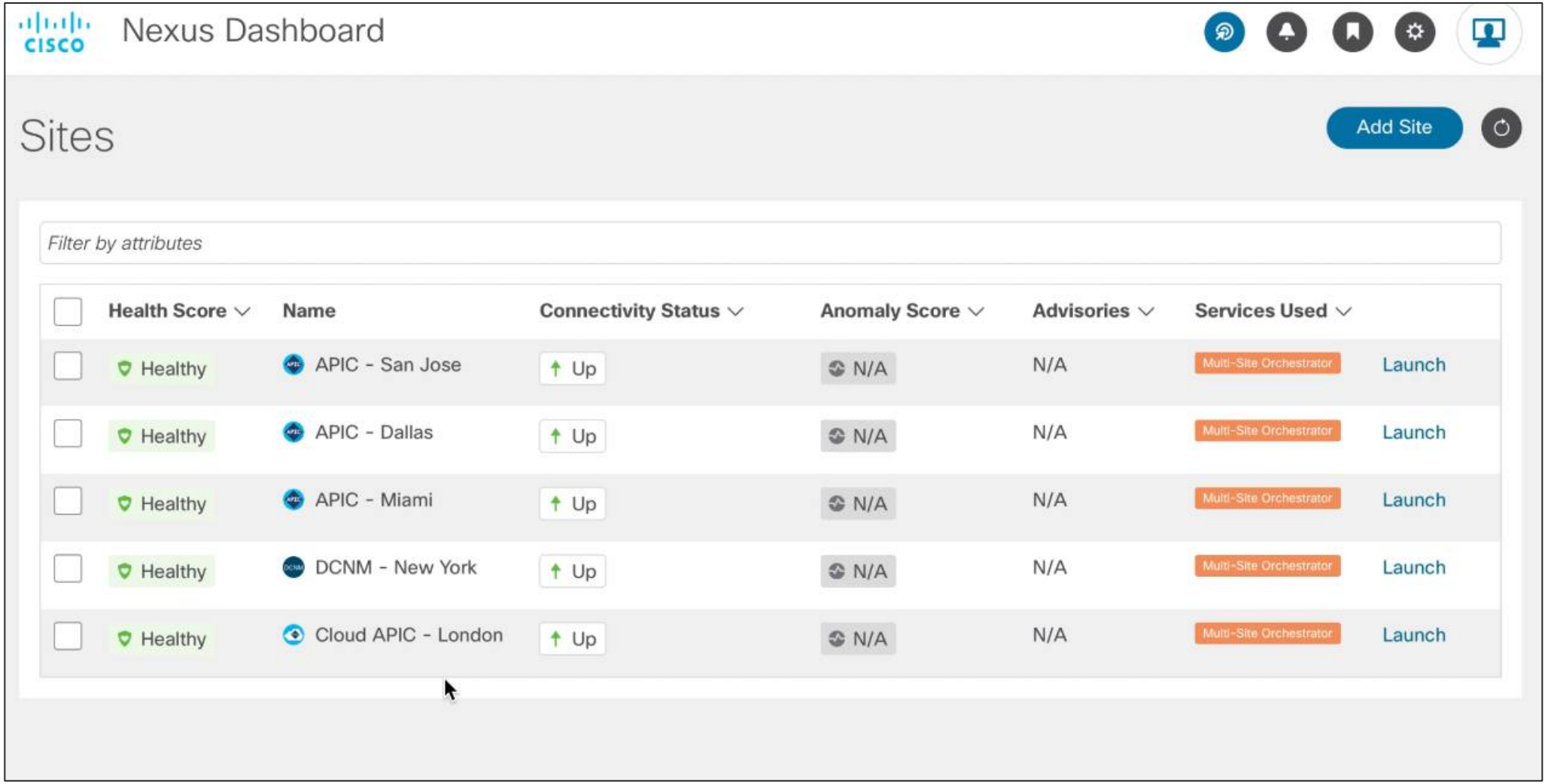
Просто внедрить

Просто использовать

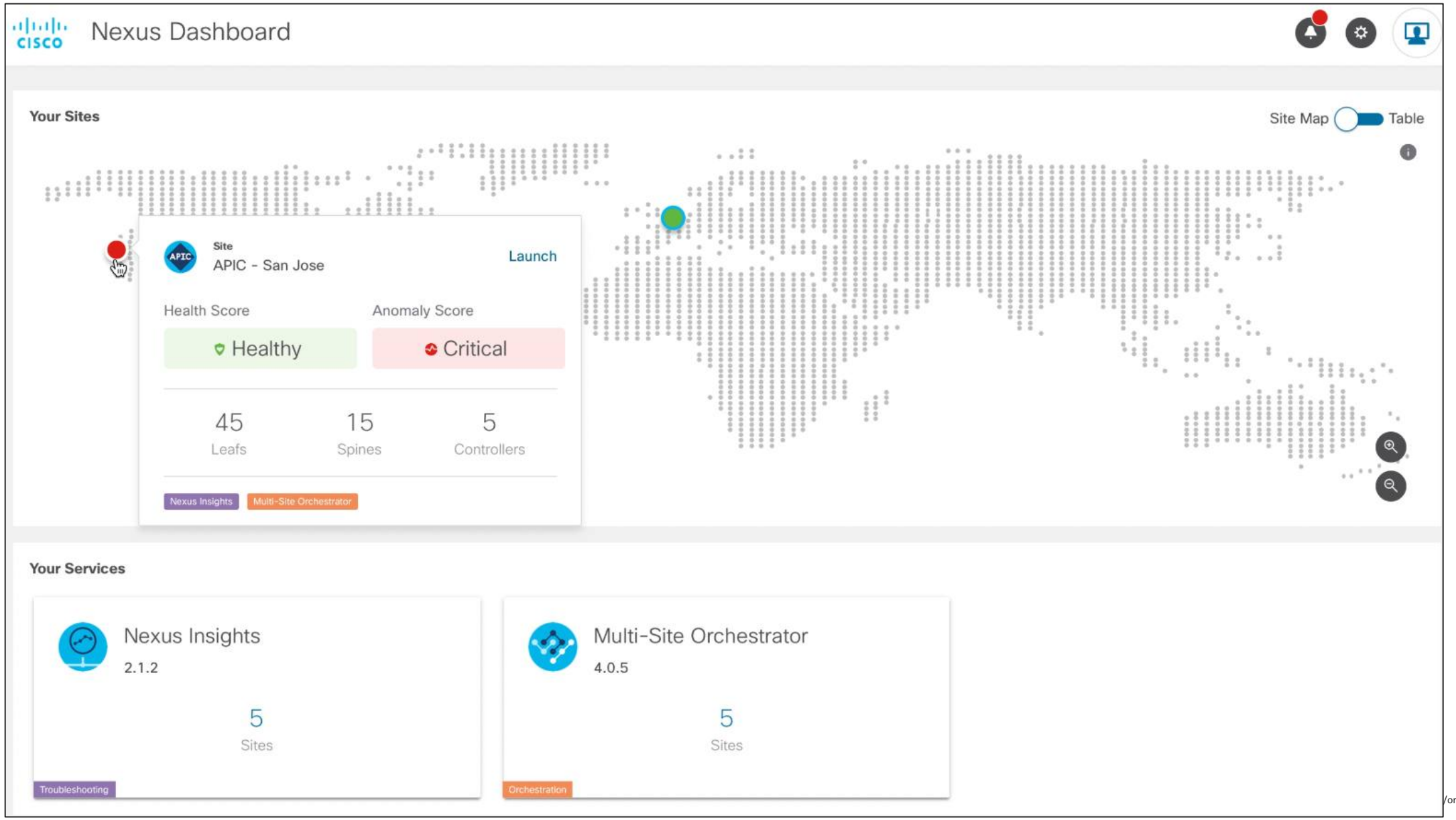


Nexus Dashboard: единое окно в эксплуатацию ACI и NX-OS фабрик

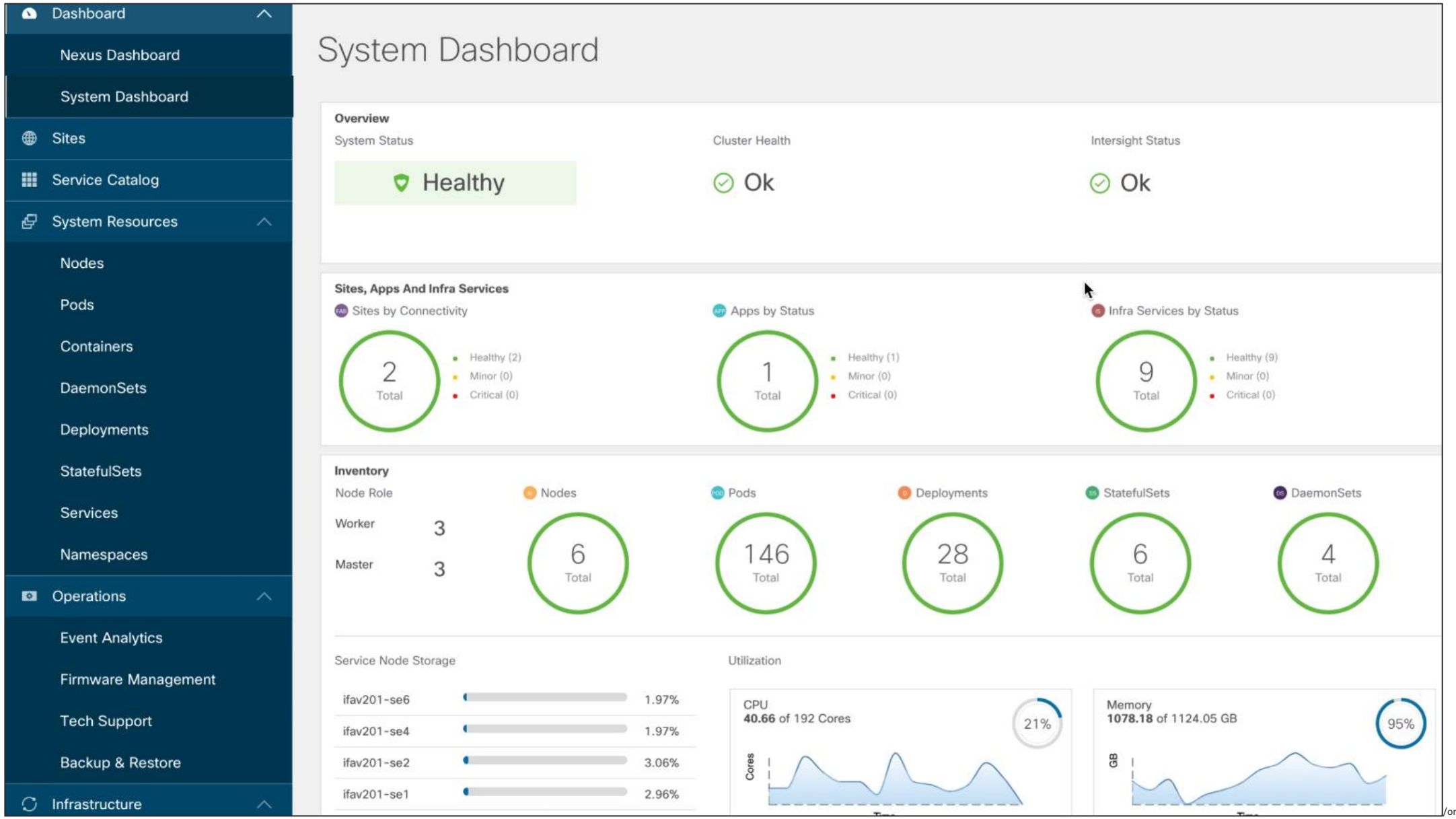
Nexus Dashboard
Эксплуатация многих сайтов



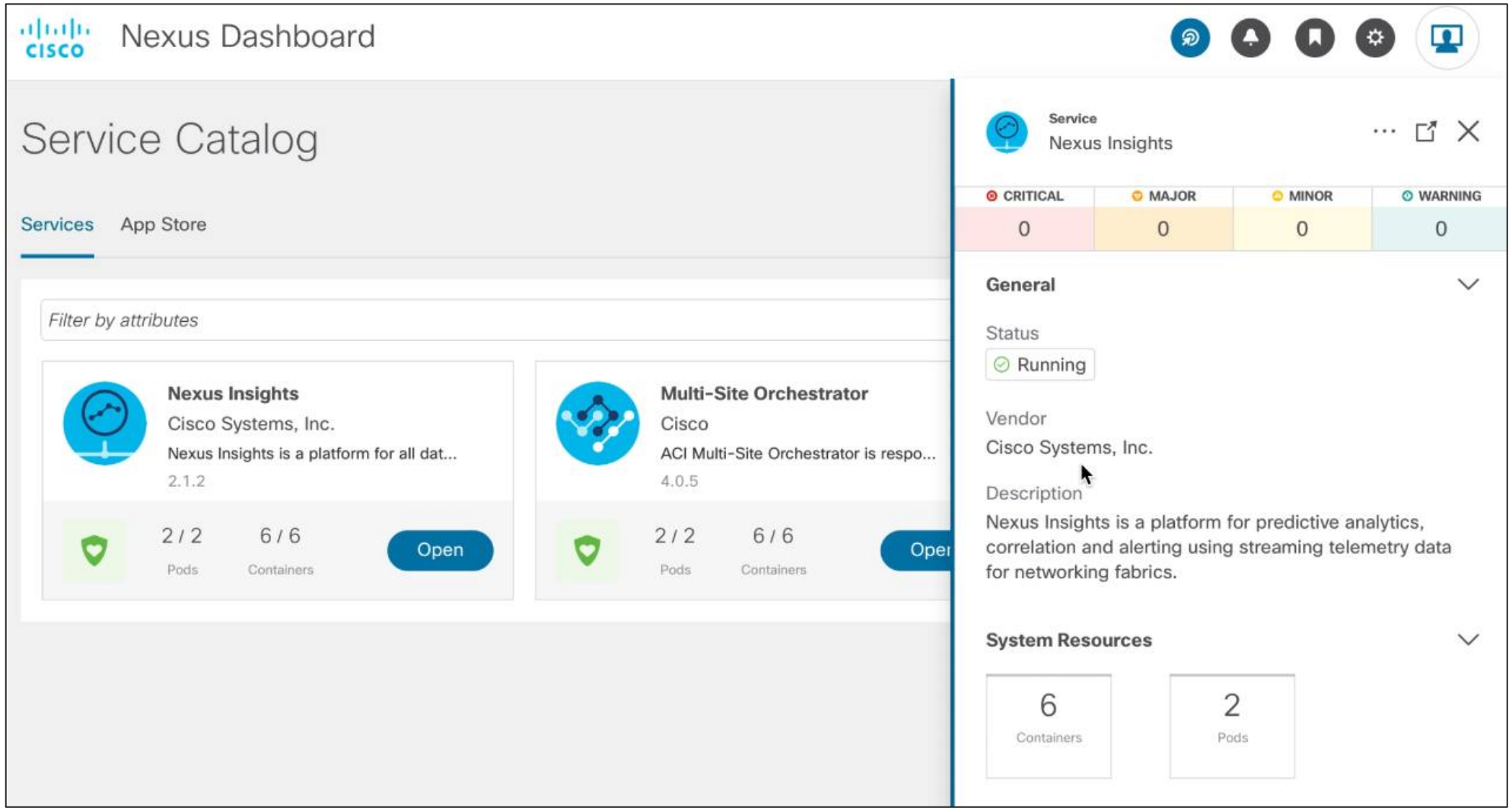
Nexus Dashboard
Эксплуатация многих сайтов



Nexus Dashboard
Администрирование платформы

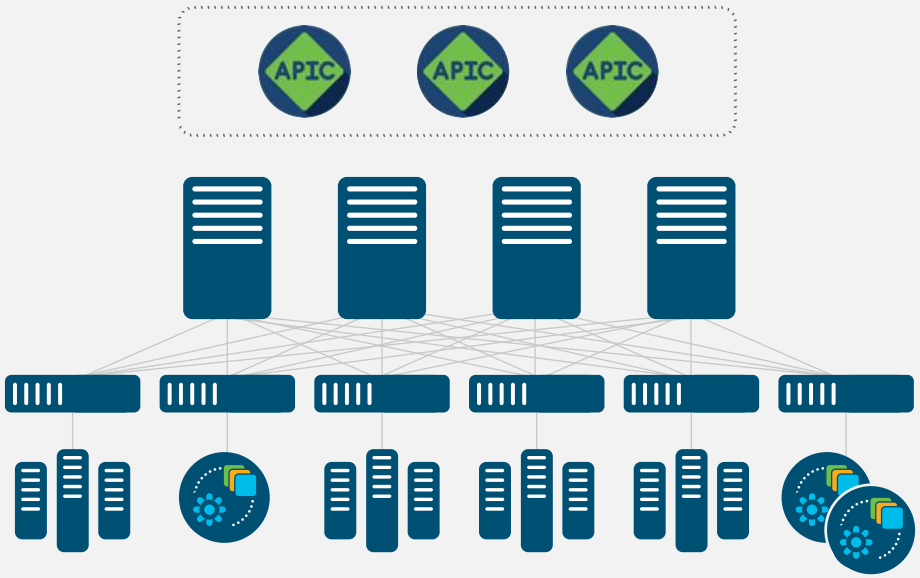


Nexus Dashboard
Размещение приложений



Платформа Cisco Nexus Dashboard Platform

Современный масштабируемый стек для размещения приложений для эксплуатации сети ЦОД



Nexus Insights

Network Assurance Engine

3rd Party apps

MSO

Multi-Site Orchestrator

2.2 GHz 10 core CPU x 2

256 GB memory

2.4 TB x 4 HDD

10G/25G/40G connect

Network automation

Scale-out cluster

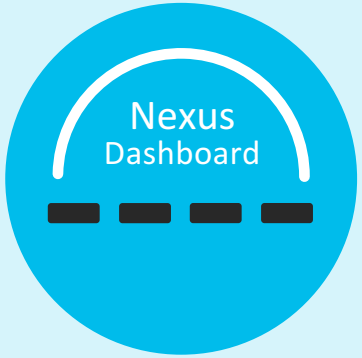
High Availability

Разверните Nexus Dashboard там, где вам удобно!

Appliance

Virtual Appliance*

Cloud Hosted*

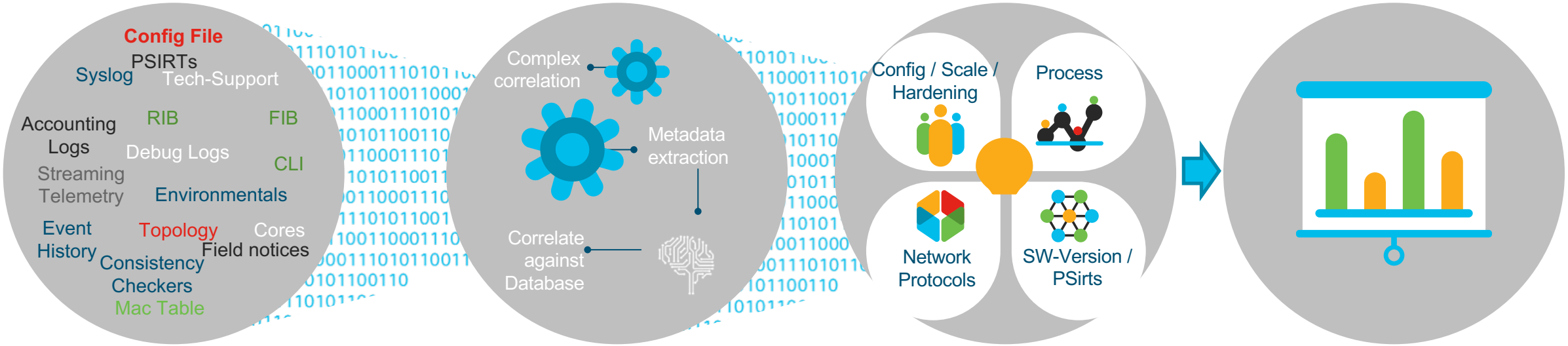


Лицензия Premier

Nexus Insights

Nexus Insights – проактивная эксплуатация на основе телеметрии

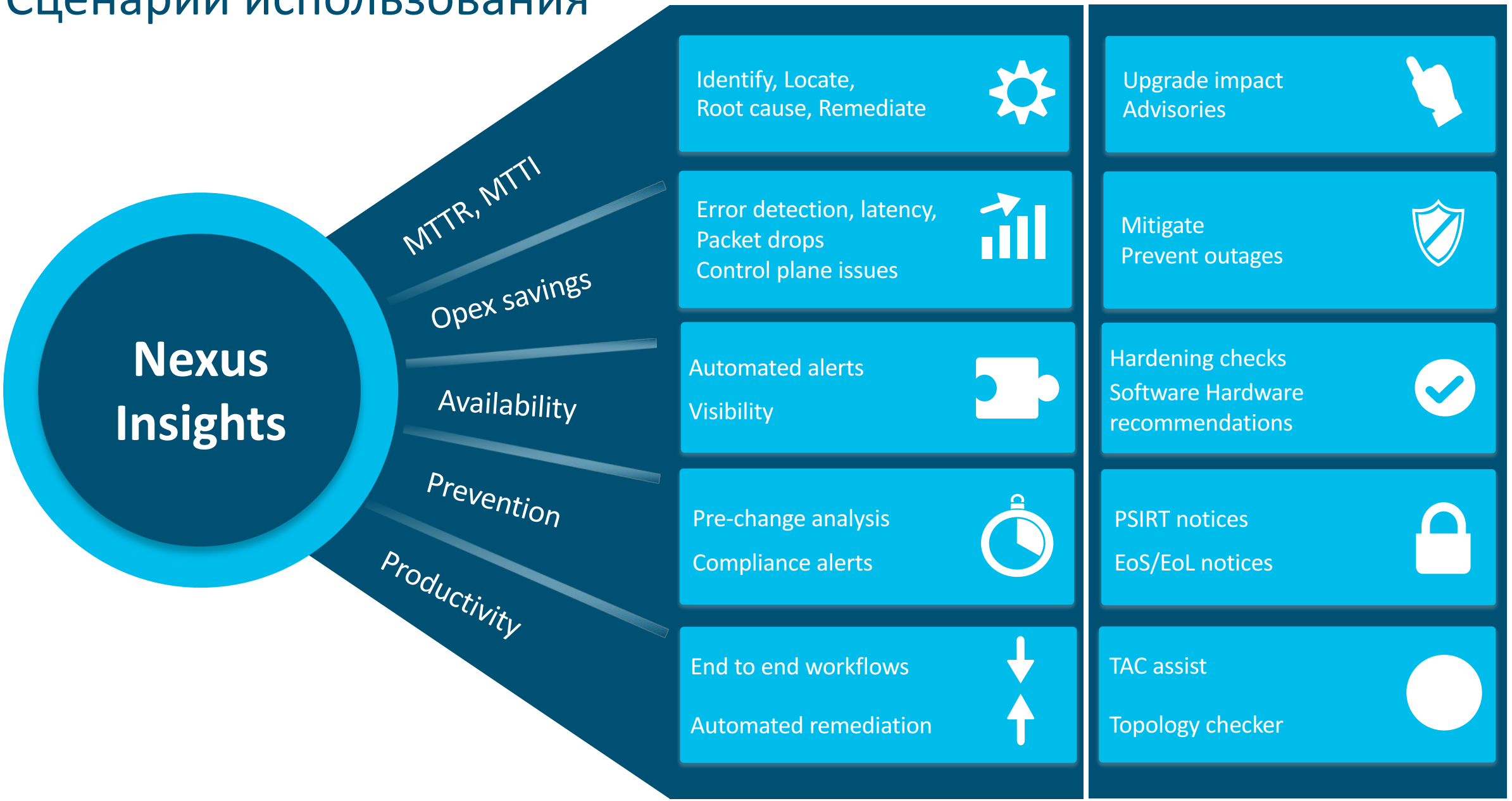
Источники телеметрии | Сбор и обработка | Сделать выводы | Рекомендованные действия



Повысить доступность и производительность

ACI | NX-OS

Nexus Insights
Сценарии использования



Какие данные получает Nexus Insights?

Программная телеметрия

Общая для Nexus

Даёт видимость в:

- Утилизацию ресурсов
- Параметры среды (темепература, питание и т.д.)
- Статистику интерфейсов
- Статистику и события протоколов уровня плоскости управления

Аппаратная телеметрия

Зависит от аппаратуры

Даёт видимость в :

- Информацию о потоках данных
- Путь потоков
- События потоков

Аппаратная телеметрия на семействе Cisco Cloud Scale

Flow Table (FT)

Собирает полную информацию о потоке данных через коммутатор + метаданные

Nexus 9300-EX и позднее

Flow Table Events (FTE)

Уведомления основанные на порогах или событиях в потоке данных

Nexus 9300-FX и позднее

Используются Nexus Insights сегодня (NI 5.0)

Streaming Statistics Export (SSX)

Потоковая передача статистики с чипа на основе заданных настроек

Data-Plane Flow Data

ASIC State

Развитие чипов Cisco Cloud Scale: функции, плотность, производительность

	CY16	CY17	CY18-CY19	CY20+
25.6Tbps				**LS25600 GX2** High Density 400G – 64x 400G 120MB Smart Buffer FT, FTE, SSX, INT-XD
12.8Tbps				**LS12800 GX2** High Density 400G – 32x 400G 120MB Smart Buffer FT, FTE, SSX, INT-XD
6.4Tbps		**S6400** **(Nexus 9332C/9364C)** **SSX**	**LS6400 GX** Smart Buffer FT, FTE, SSX, INT-XD 16x 400G, SRv6	
3.6Tbps	**S3600**	LS3600 FX2 Smart Buffer FT, FTE, SSX MACsec, CloudSec		
1.8Tbps	LS1800 EX Smart Buffer FT	LS1800 FX Smart Buffer FT, FTE MACsec	LS1800 FX3 Smart Buffer FT, FTE, SSX MACsec, CloudSec	

Legend

Features	**FT** – Flow Table
Density	**FTE** – Flow Table Event
Density + Features	**SSX** – Streaming Statistics Export
	INT – In-band Telemetry

Какая еще информация используется Nexus Insights кроме телеметрии?

On-prem

Pulled from the Cloud

Сеть

- Running config всех устройств
- “show tech” всех устройств

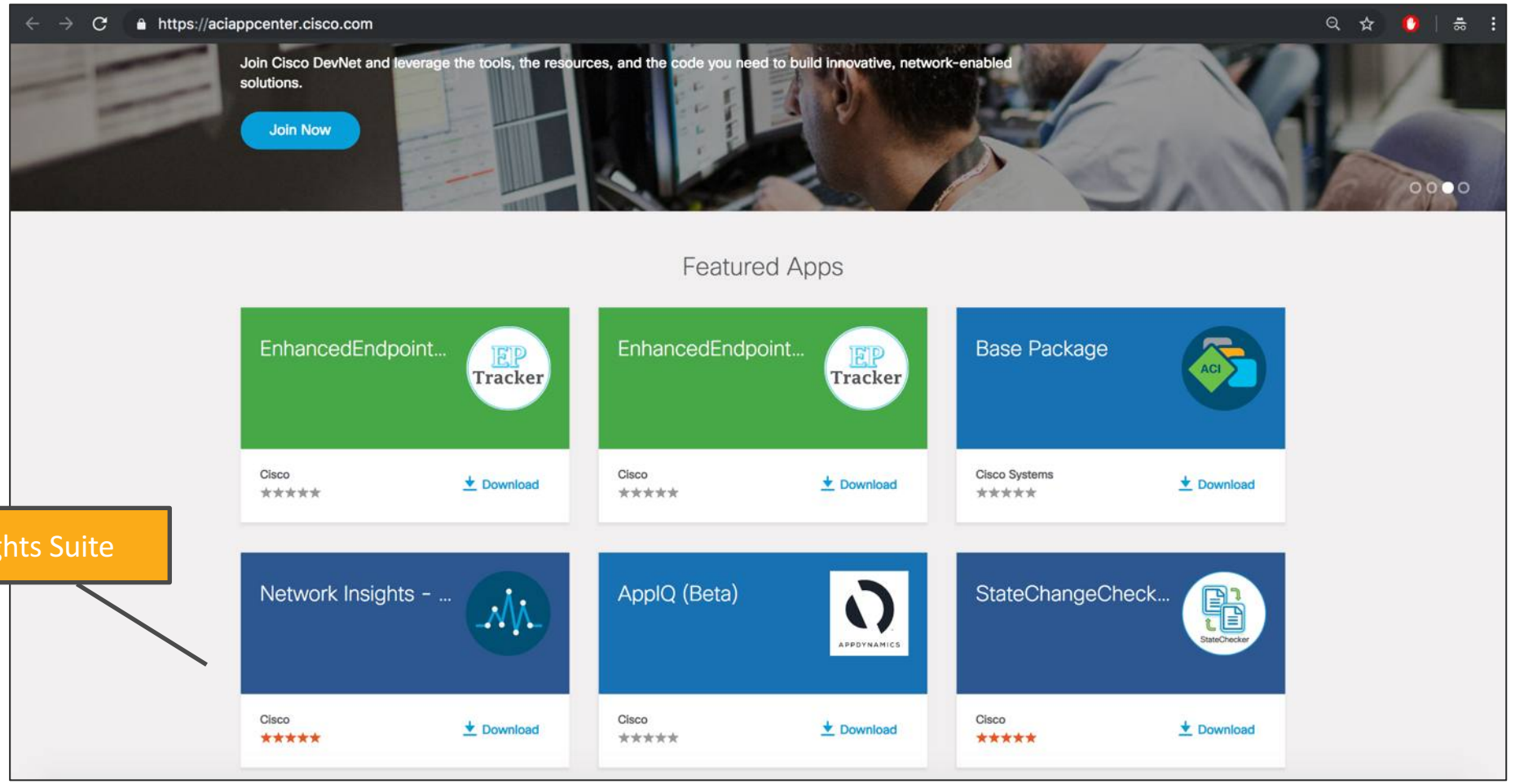
Cisco

- Наилучшие практики
- PSIRTs, FNs, EOS/EOL
- Software release notifications
- Цифровые сигнатуры известных дефектов

Nexus Insights: загрузка из Cisco App Store

Общий «магазин приложений» для ACI and NXOS - https://dcappcenter.cisco.com/

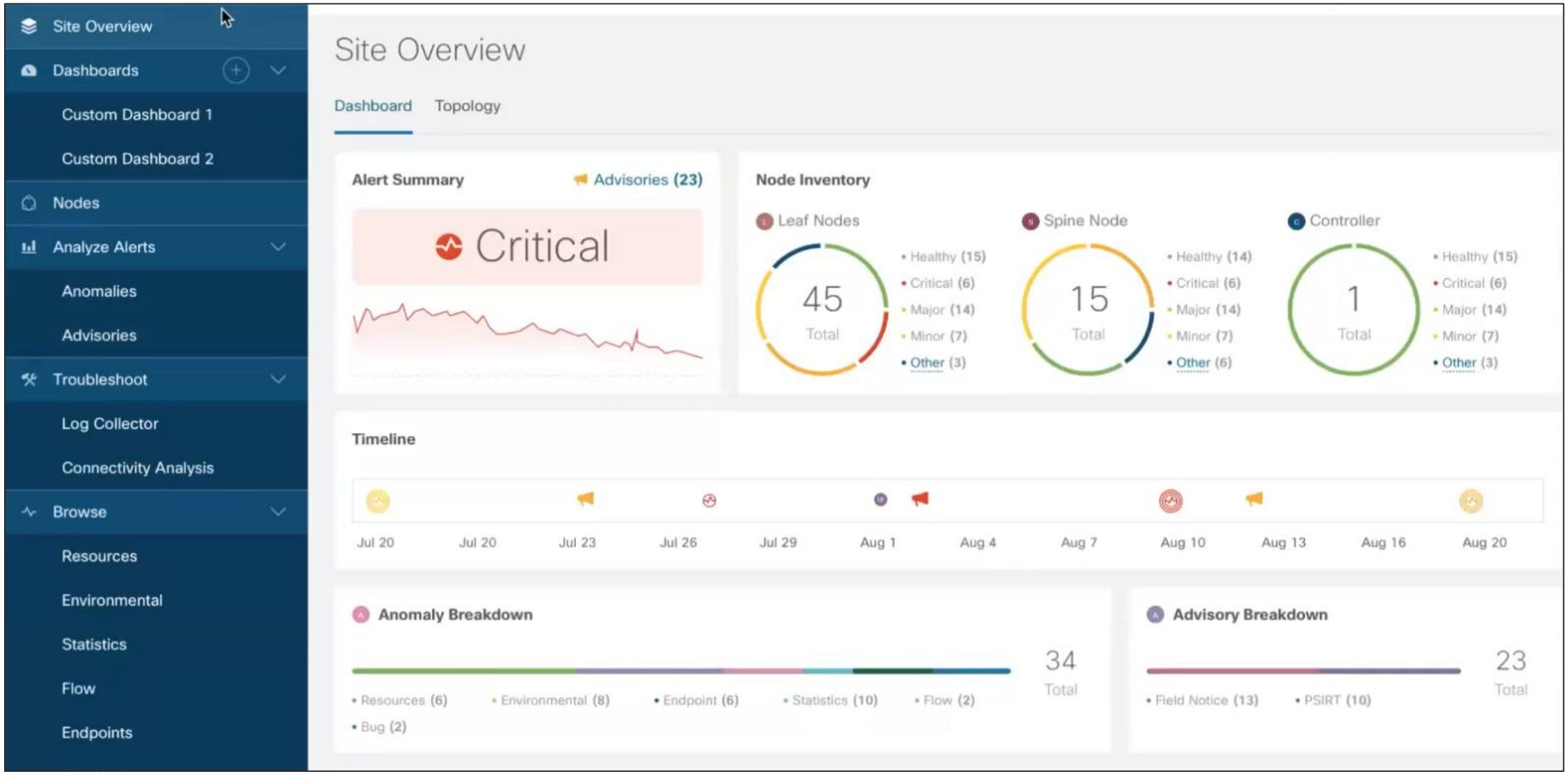
Непосредственно доступен на Nexus Dashboard -> Services -> App Store



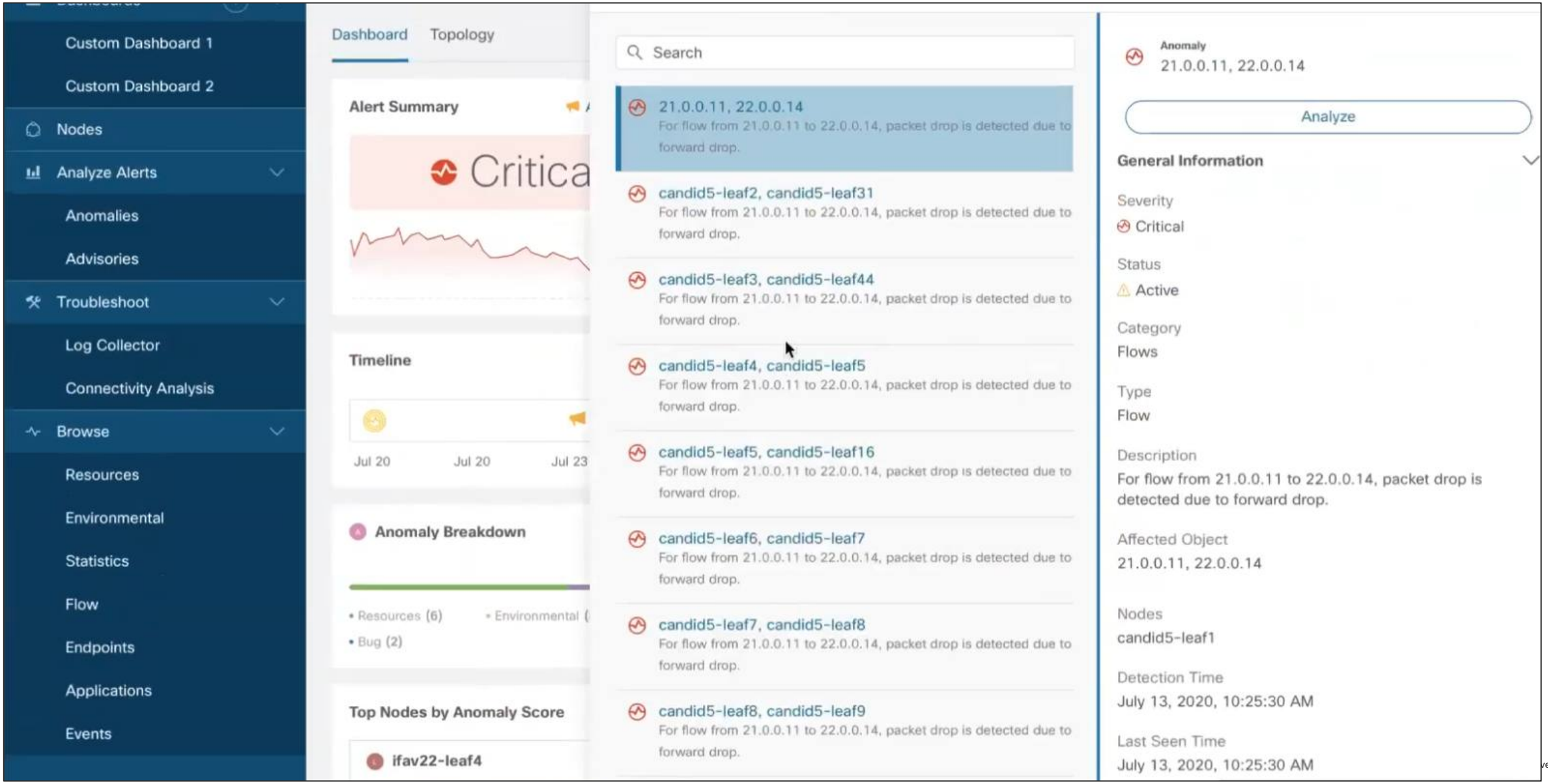
Nexus Insights Suite

© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

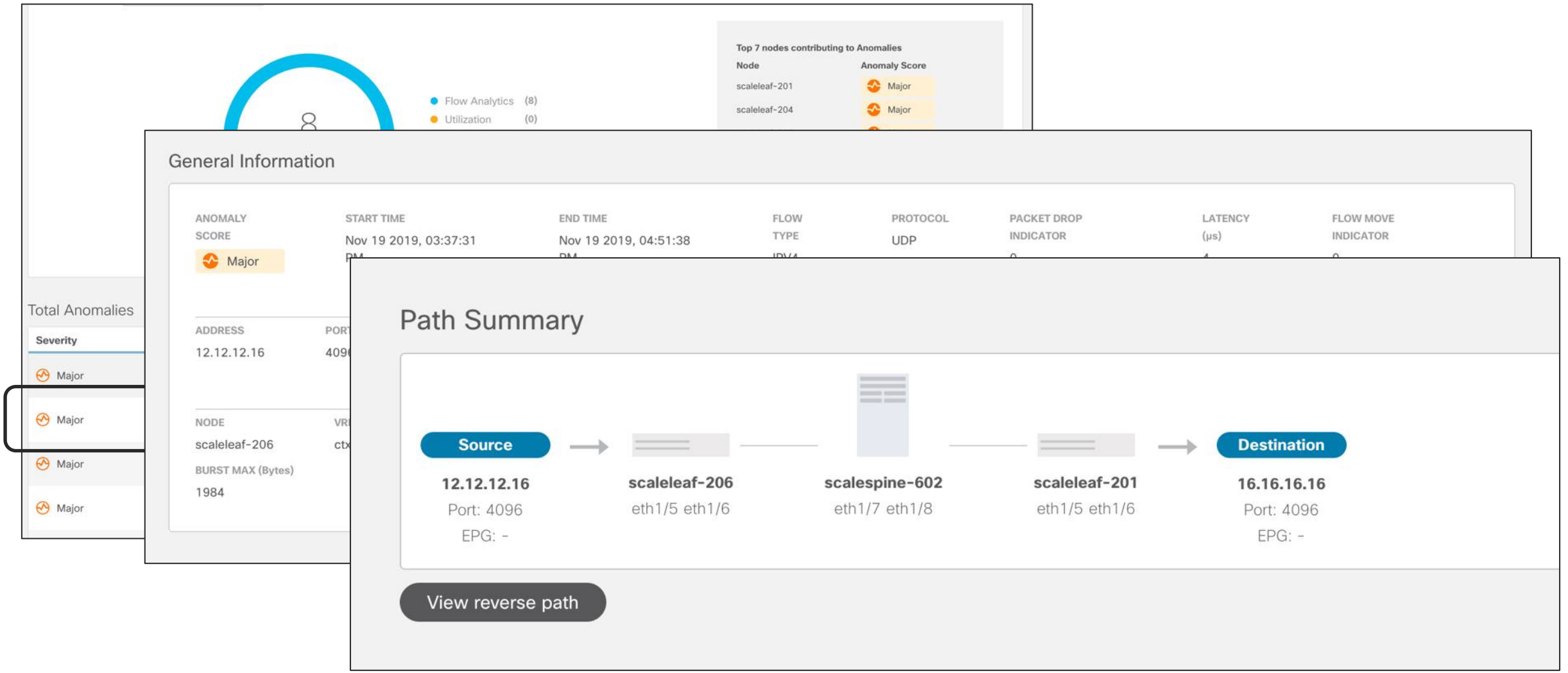
Nexus Insights
Обзор информации сайта



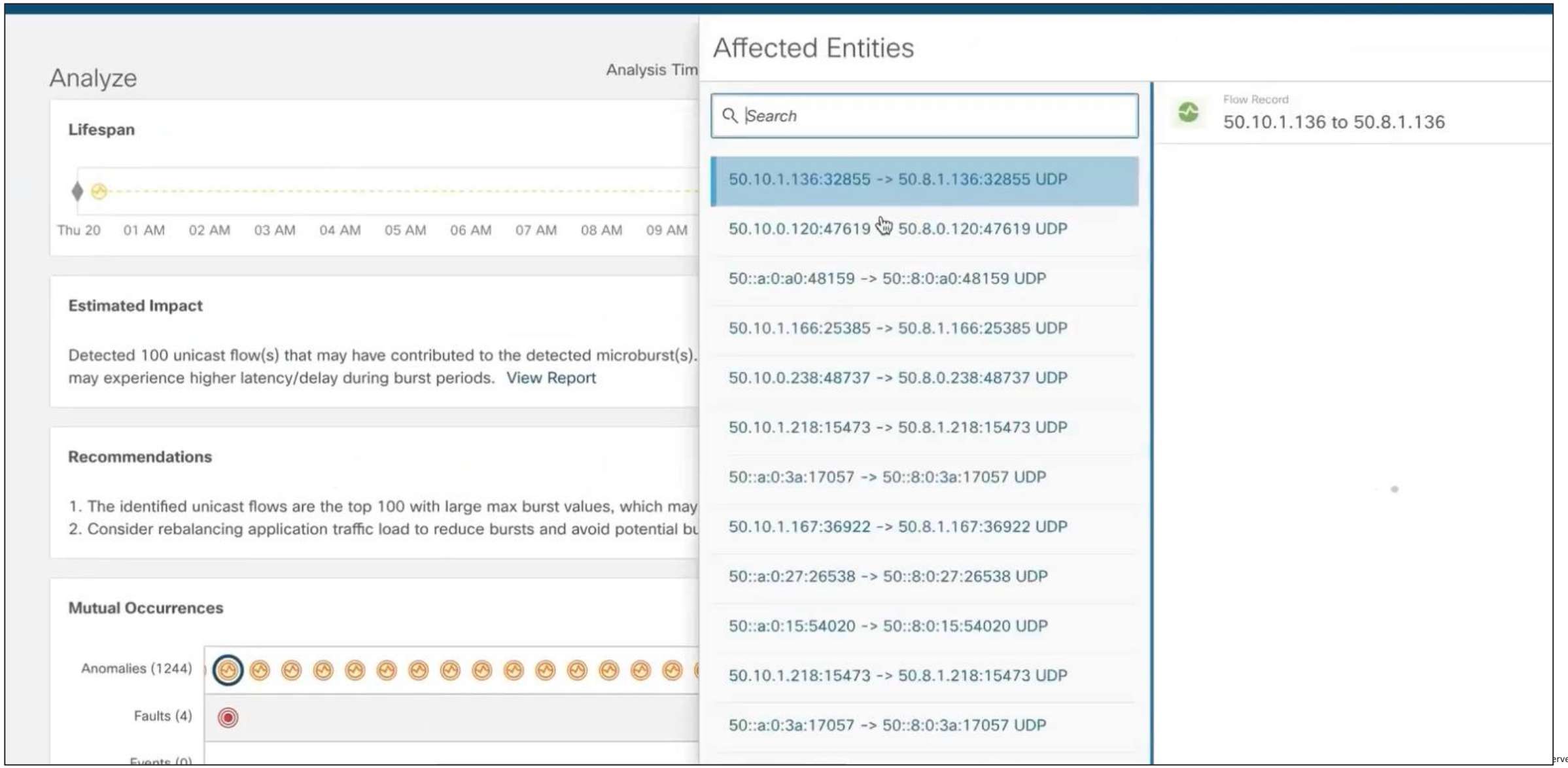
Nexus Insights
Список аномалий и их детали



Проблема производительности?

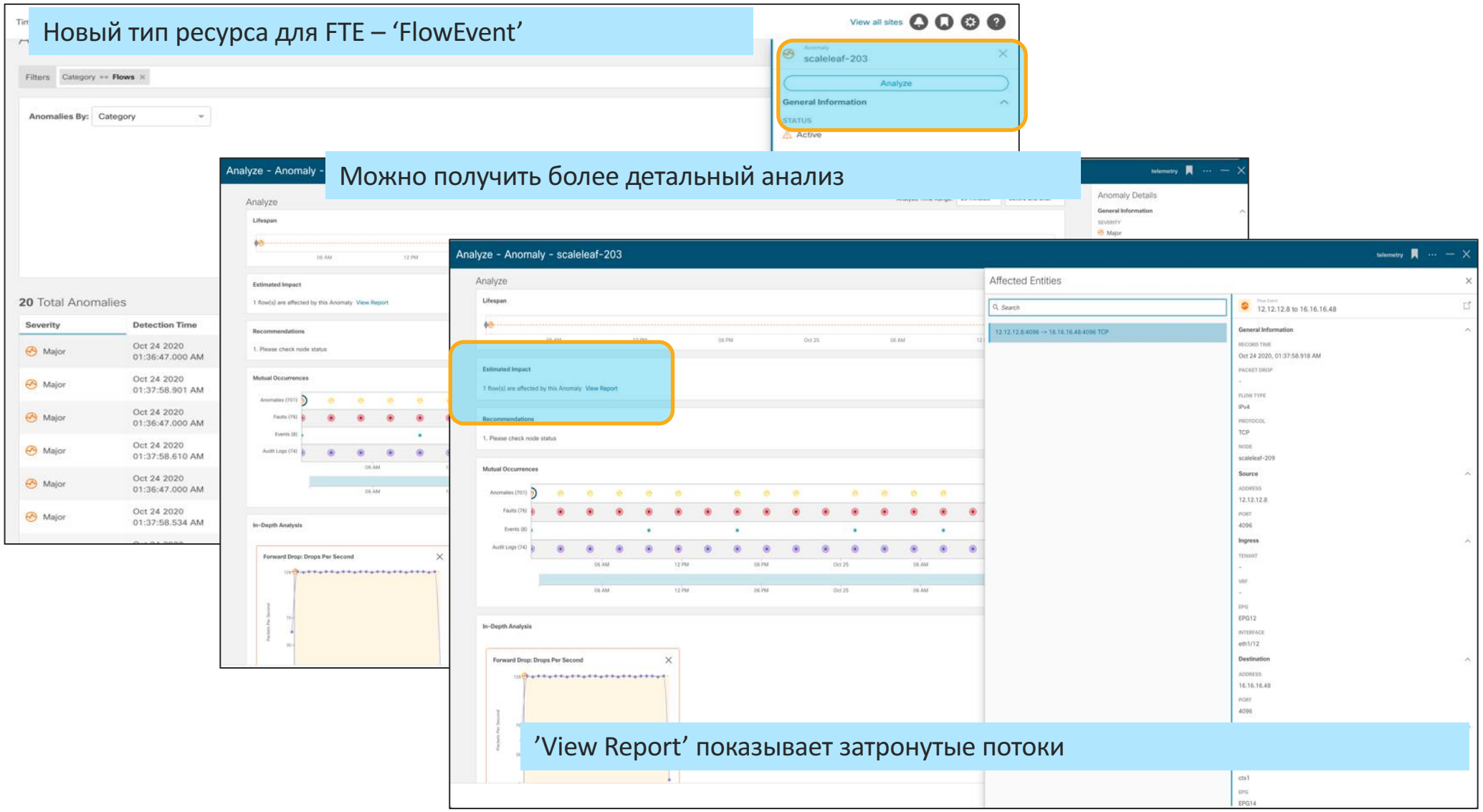


Nexus Insights
Анализ микровсплесков (microbursts)



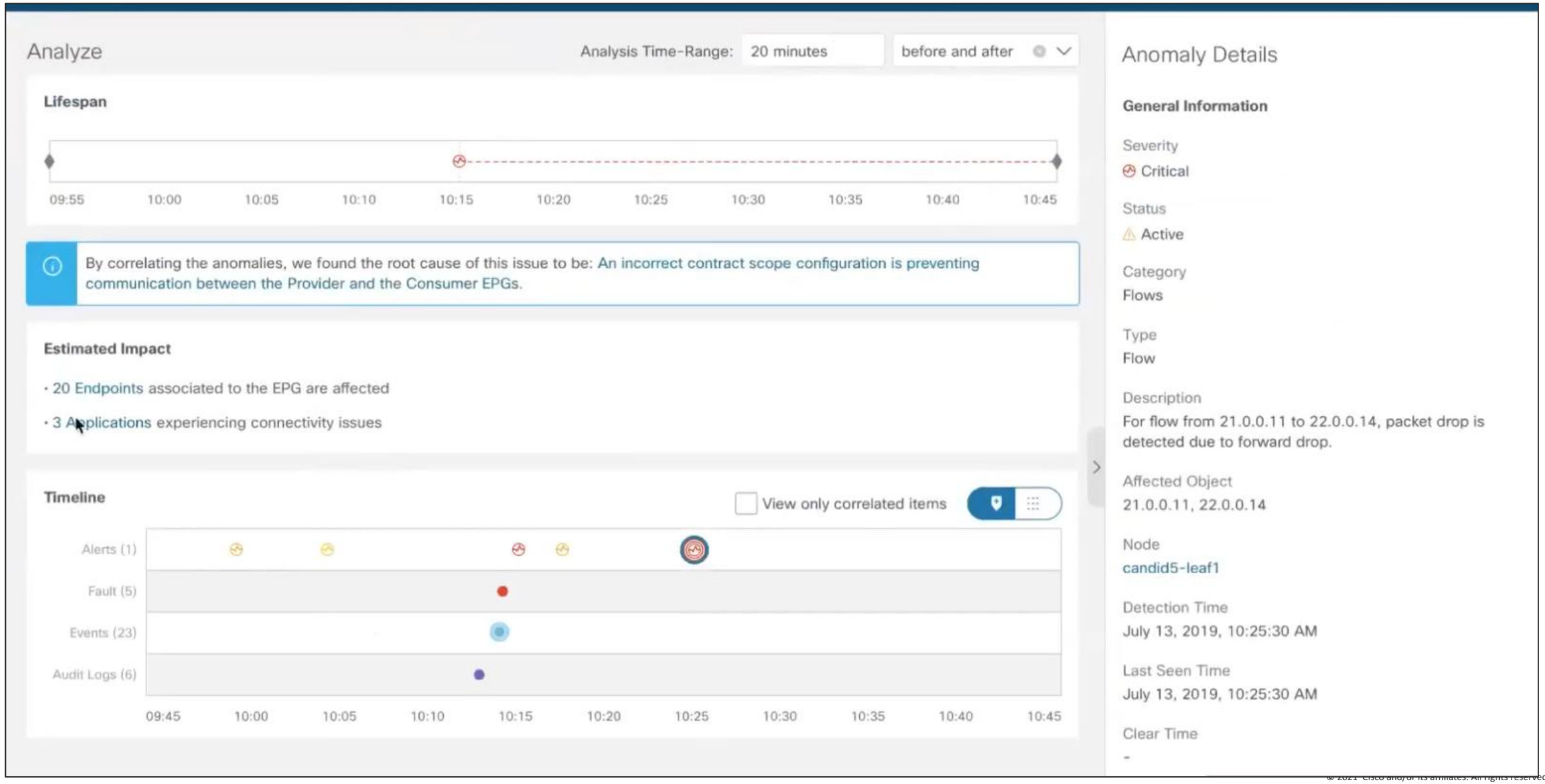
Поддержка FTE телеметрии в NI 5.0

Forward drop, Buffer drop, Policy drop, Policing drop, IDS drop

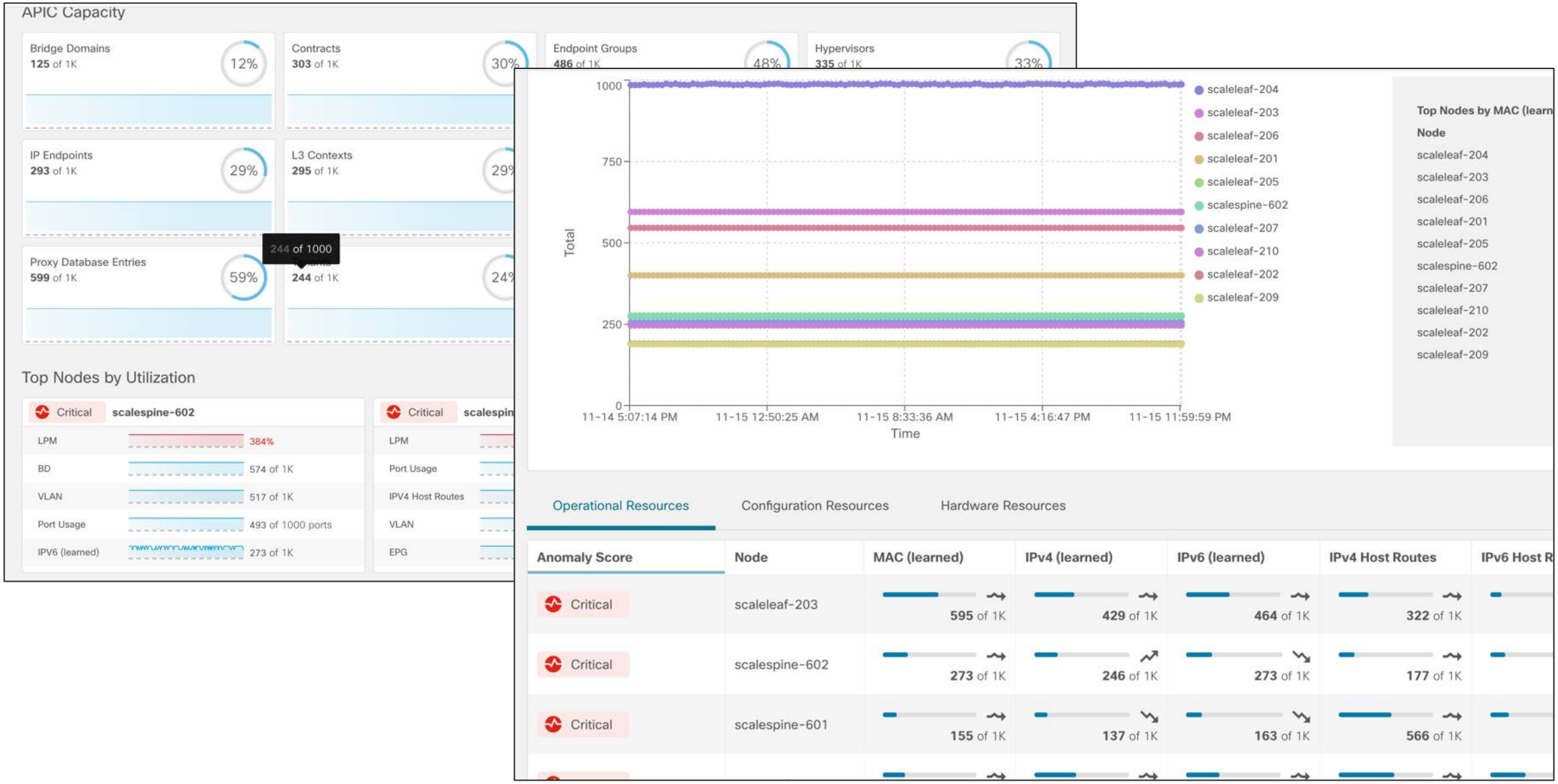


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

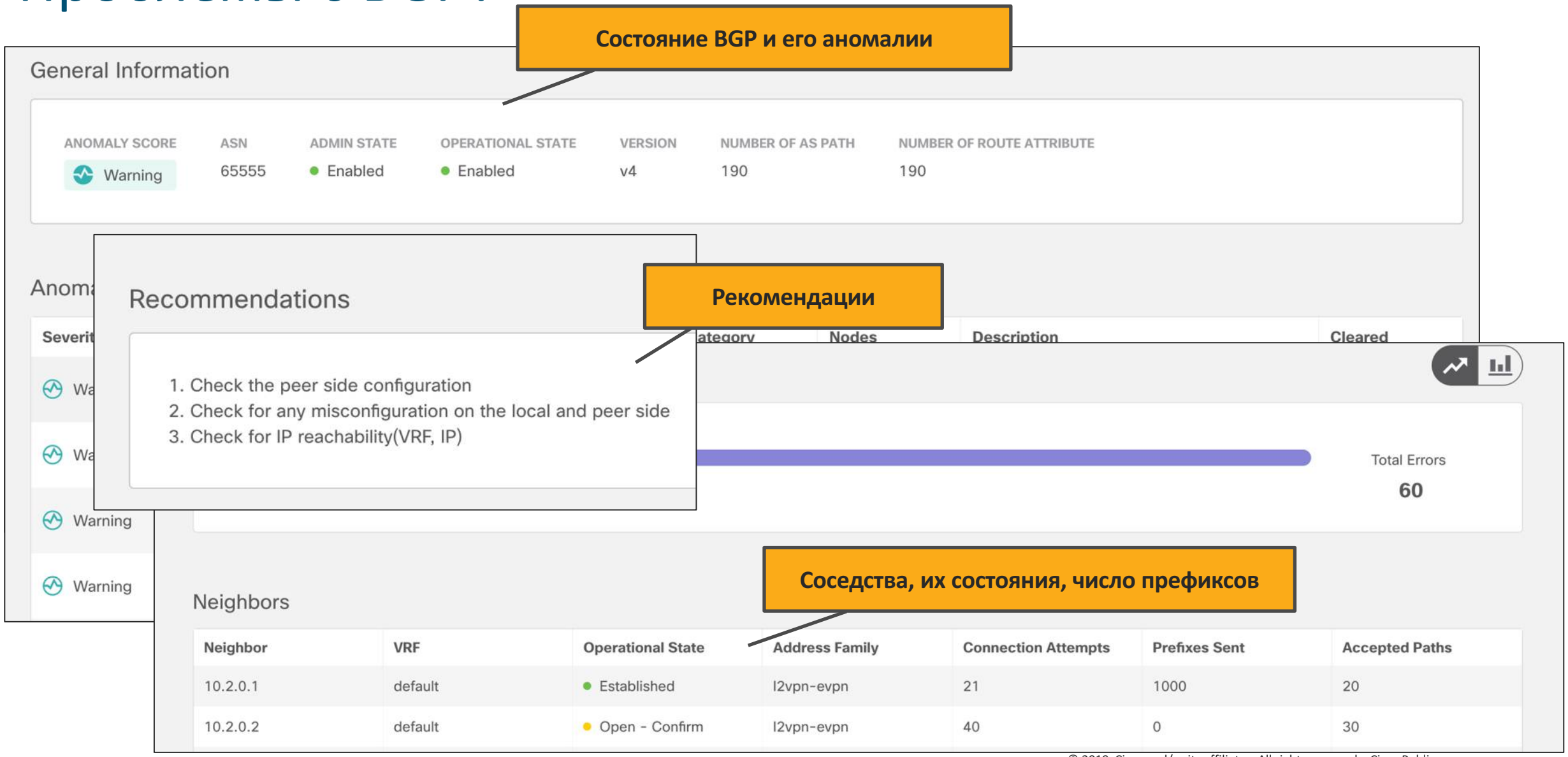
Nexus Insights
Анализ аномалии



Хватает ли ресурсов?

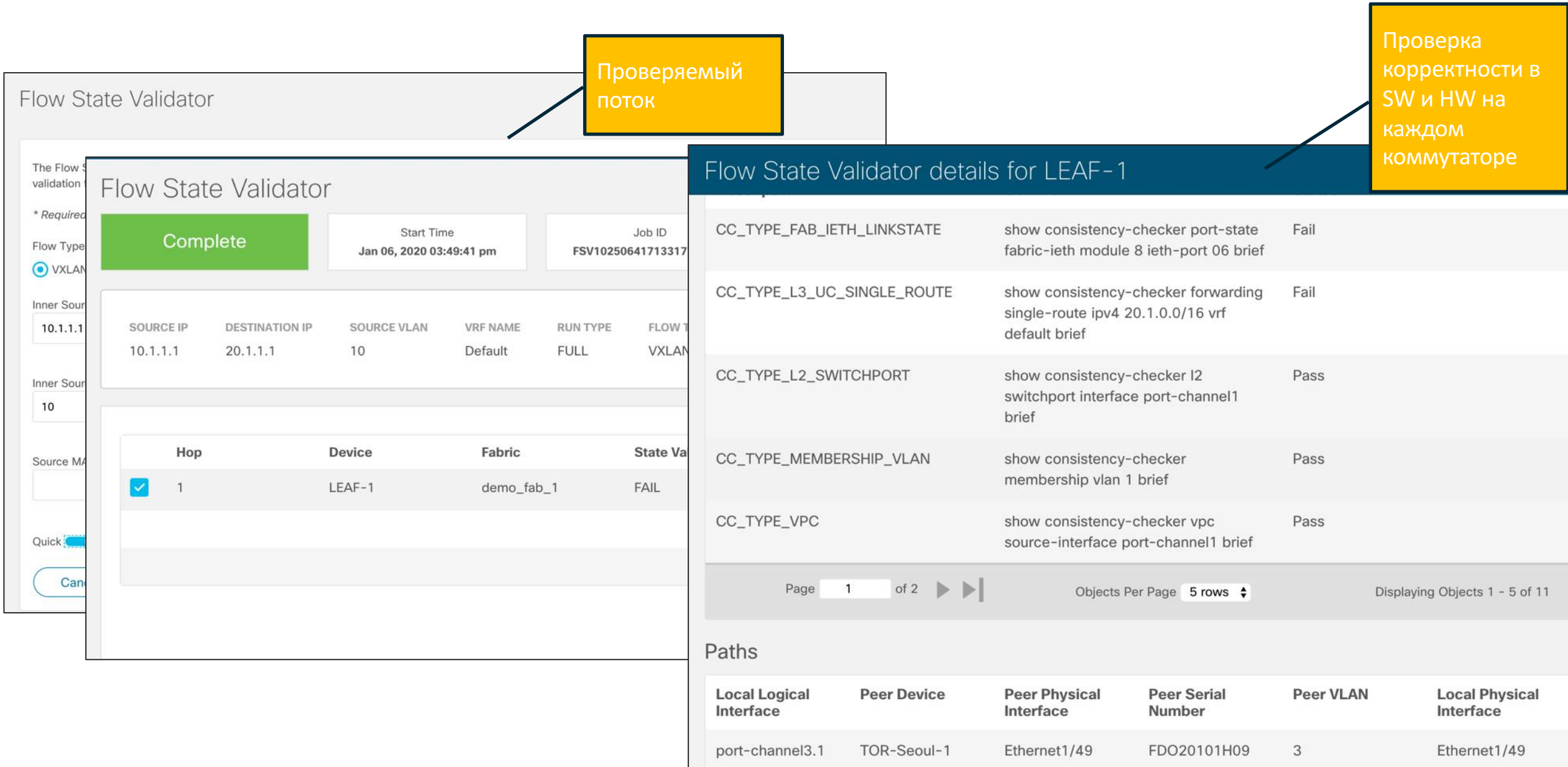


Проблемы с BGP?

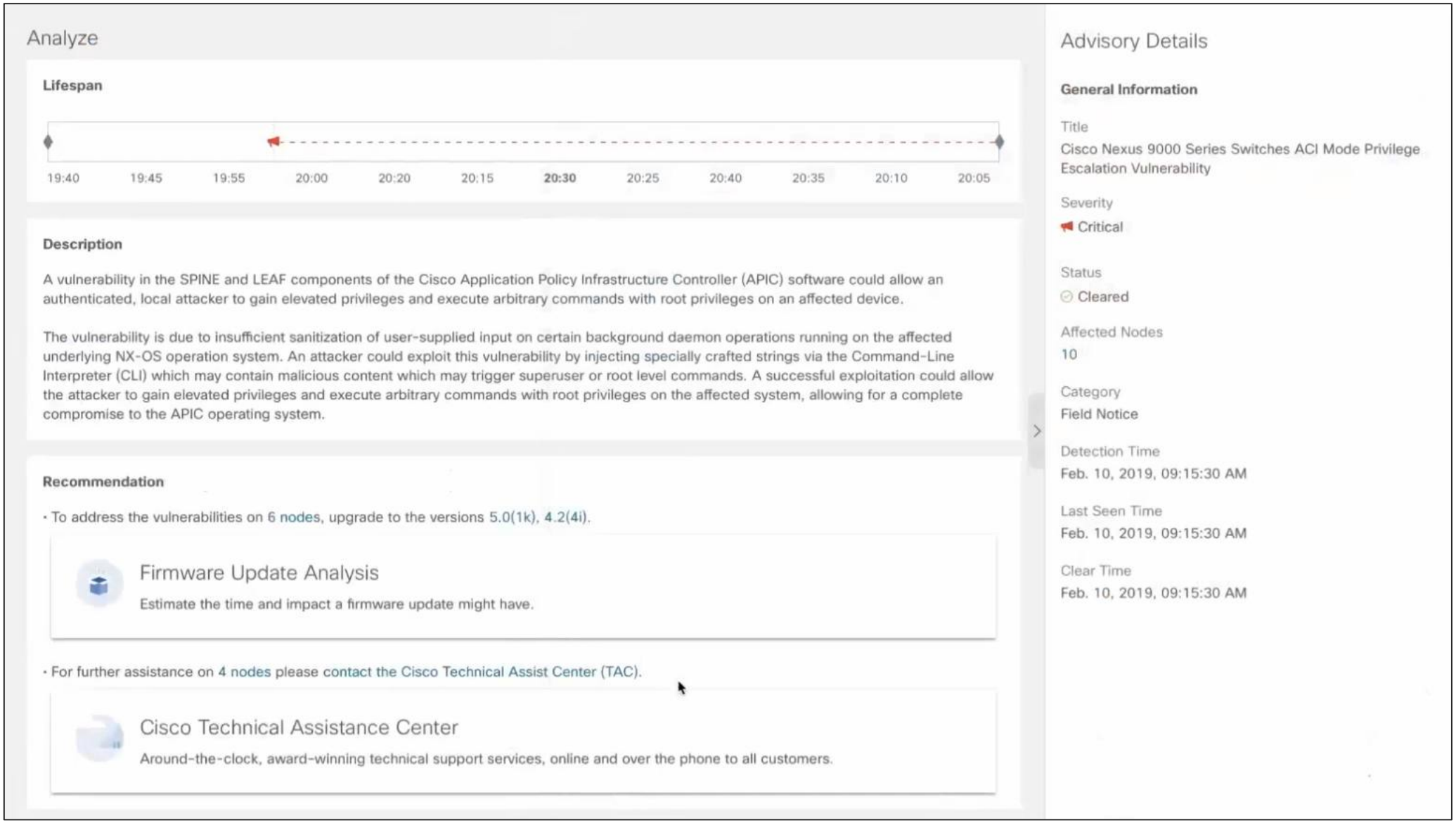


© 2021 Cisco and/or its affiliates. All rights reserved. Cisco Public

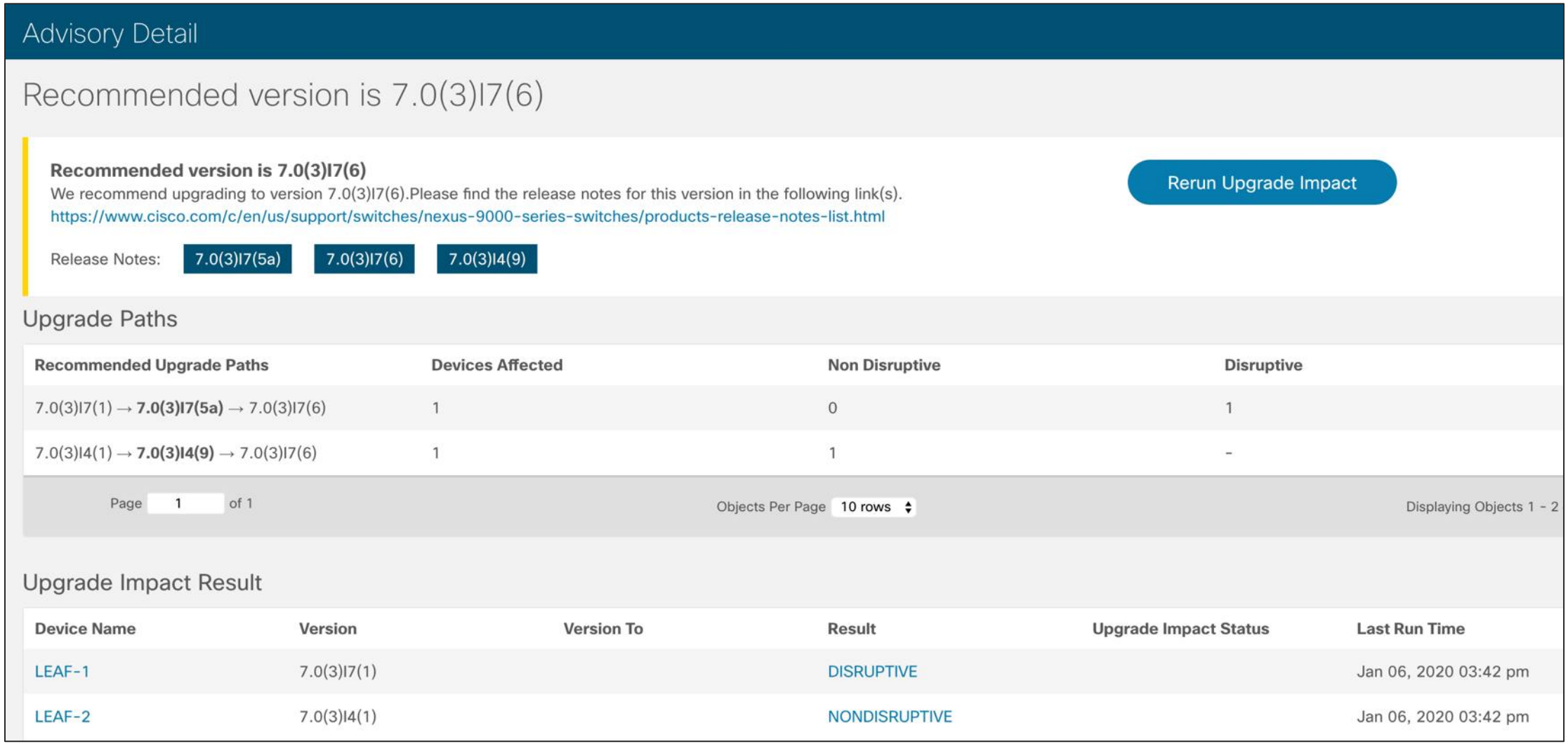
Flow State Validator –проверка корректного состояния в ПО и аппаратуре для потока



Предупреждения о PSIRT/Field Notice и т.д.

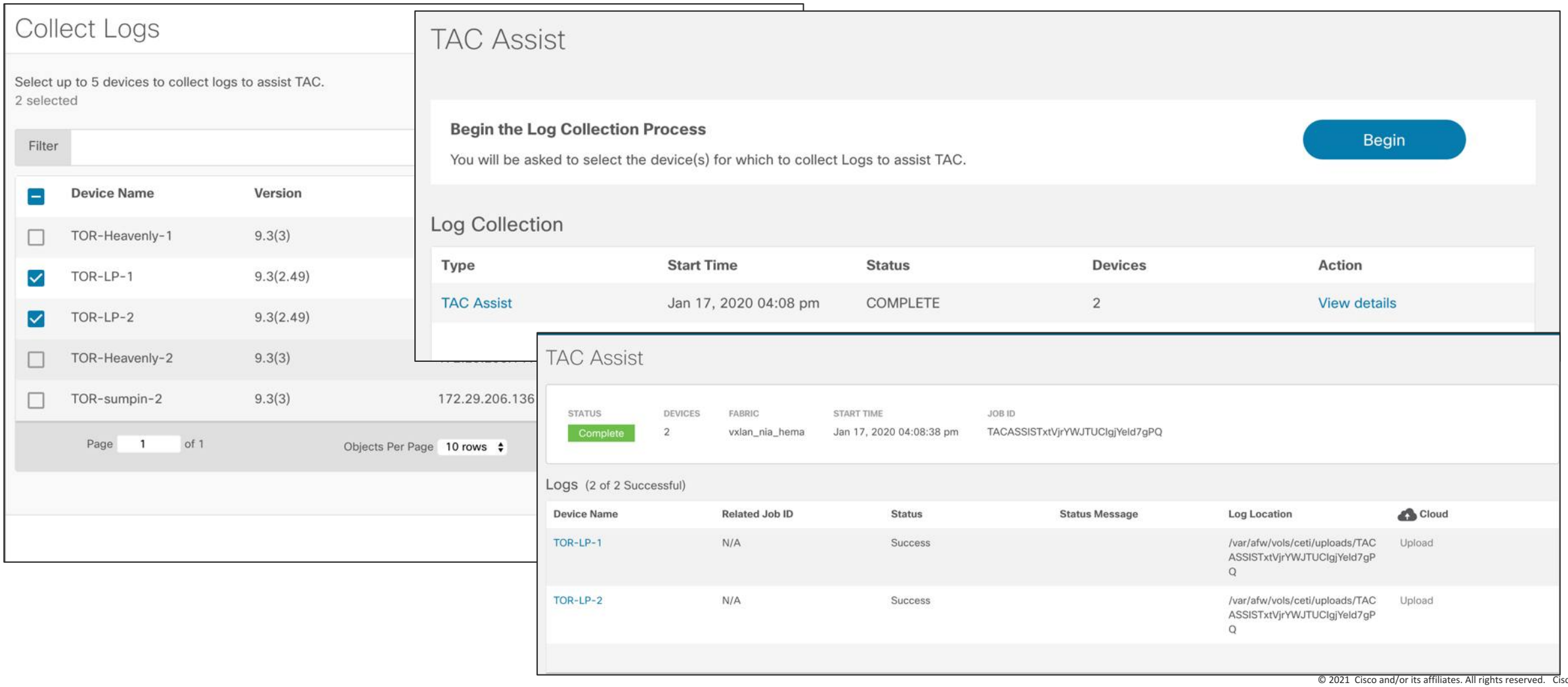


Рекомендации по обновлению и его влияние



TAC Assist

Помогает собрать логи для TAC SR непосредственно из приложения



Практические аспекты разворачивания DCNM и MSO

Экосистема Cisco DCNM

Сети хранения данных (SAN)

Управление & аналитика

Сетевые фабрики для медиавещания (IP Fabric for Media)

Управление и контроль

Платформа для хостинга приложений

(Day2 Operations и расширенные функций)

Network Insights Resources

Network Insights Advisor

Cisco DCNM – Лицензирование

SKU	Data Center Network Manager (DCNM)
DCNM-SVR-11-K9 DCNM-SVR-11-K9=	DCNM Server License per server instance
Switch Licenses	
DCNM LAN for Fixed Switch: e.g. DCNM-LAN-N93-K9= DCNM-LAN-N3K-K9=	Perpetual Fixed Chassis RTM Advanced feature license License for DCNM for one Switch
DCNM LAN for Modular Switch: e.g. DCNM-LAN-N95-K9=	Perpetual Modular Chassis RTM Advanced feature license License for DCNM for one Switch
	или

Лицензии NX-OS Essentials и Advantage включают Right-to-Manage лицензии на DCNM

Развертывание Cisco DCNM LAN Fabric

Cisco DCNM – Варианты развертывания

На данный момент доступно два варианта развертывания:

1. **Standalone** – одна виртуальная машина (OVA) или физический сервер (ISO)*
2. **Native HA** – две виртуальные машины (OVA) или два физических сервера (ISO)*

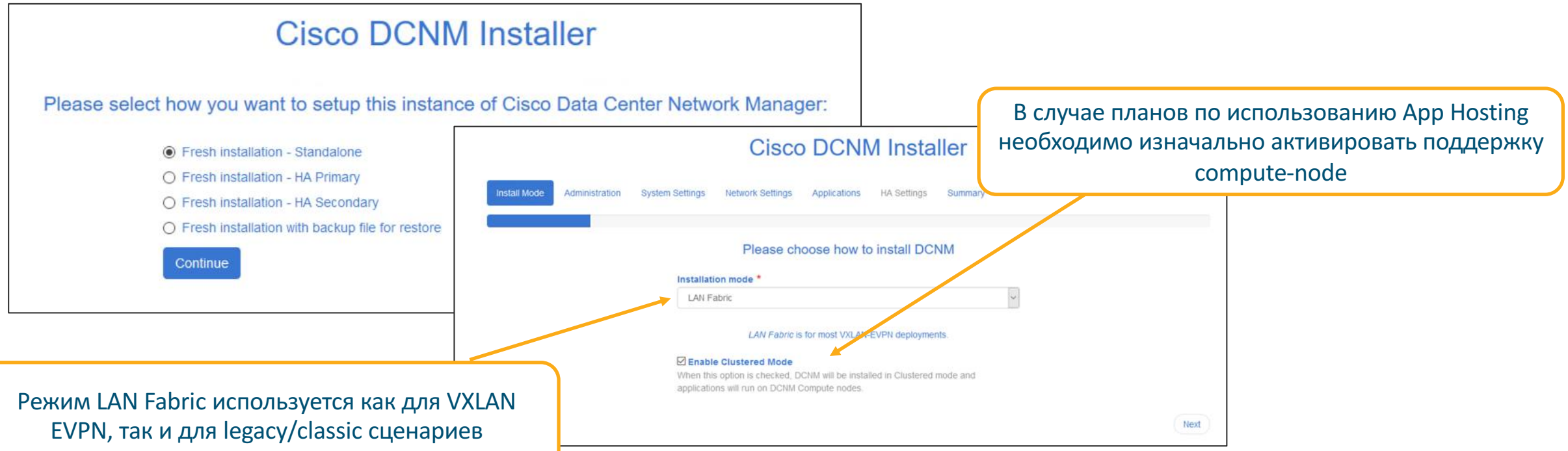
Каждый из вариантов может быть дополнен тремя вычислительными узлами, обеспечивающими запуск Day2 Operations продуктов и сторонних приложений.

Важно правильно выбрать целевую схему развертывания в самом начале, при первом старте VM/узла Cisco DCNM!

** Cisco Nexus Dashboard bare-metal*

Cisco DCNM – Мастер установки

После первого запуска виртуальной машины, либо ASE, запускается мастер установки.

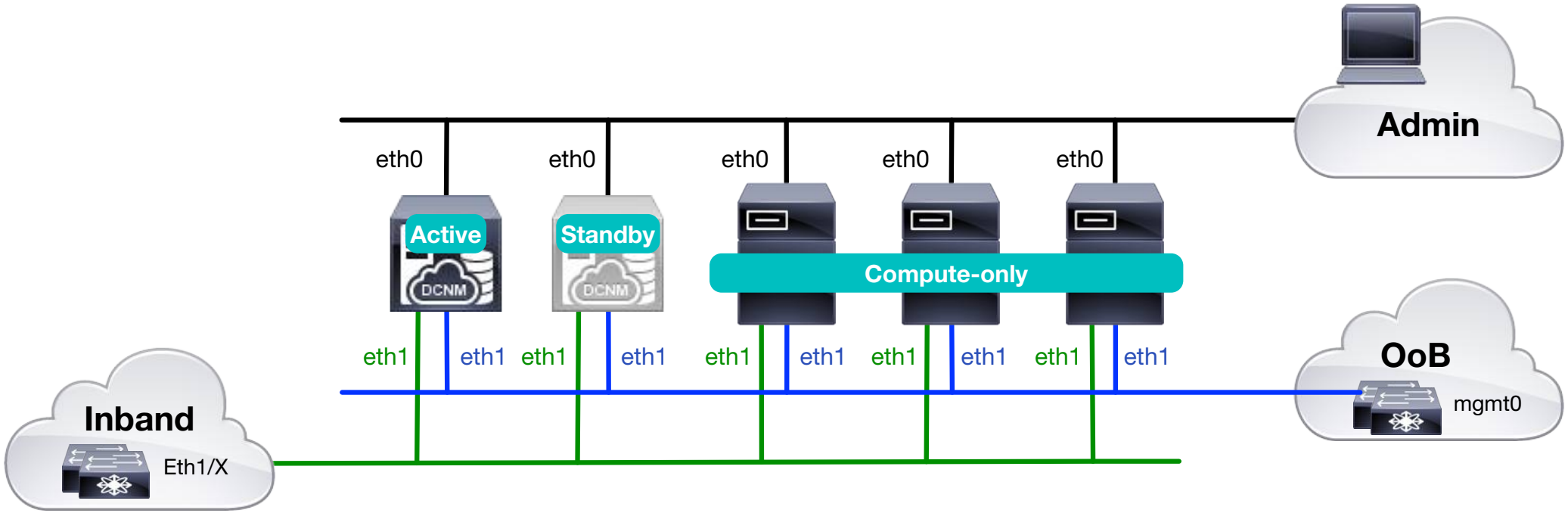


В случае планов по использованию App Hosting необходимо изначально активировать поддержку compute-node

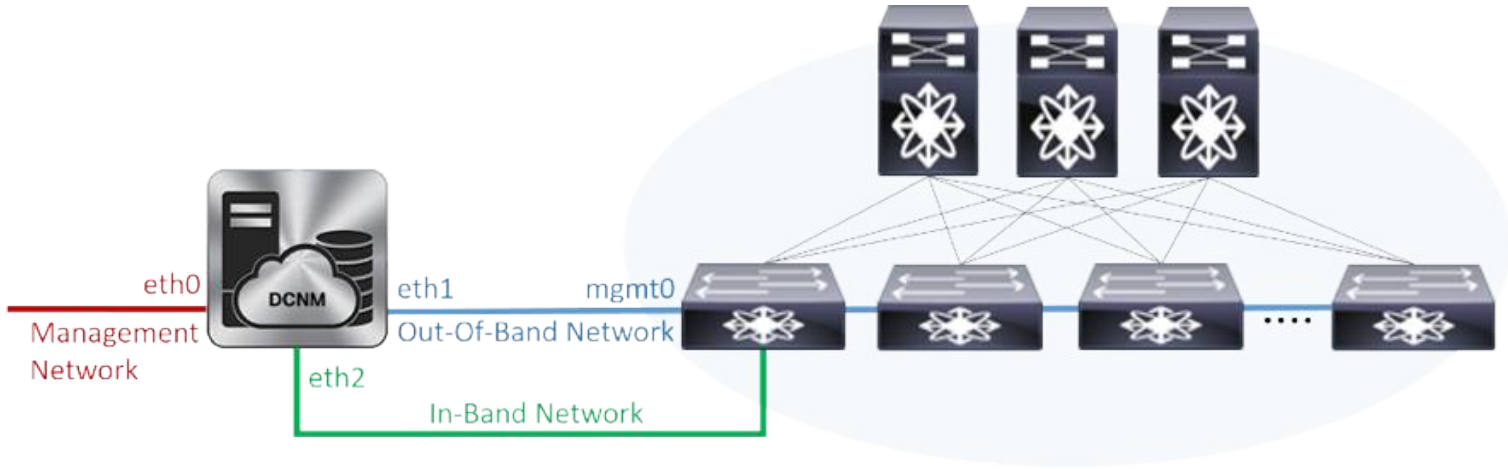
Режим LAN Fabric используется как для VXLAN EVPN, так и для legacy/classic сценариев

Cisco DCNM Native HA

Обеспечивает отказоустойчивую конфигурацию в рамках одной площадки. Требует наличие L2 связности между узлами.



Cisco DCNM LAN – Подключение к сети



Eth0 используется для доступа к DCNM GUI и DCNM REST API

Eth1 используется для работы с коммутаторами через внеполосную сеть управления

Eth2 используется для работы с коммутаторами через порты доступа (inband)

Cisco DCNM LAN – Назначение интерфейсов

Интерфейс	Функция Cisco DCNM
Eth0	Графический интерфейс, REST API
Eth1	Настройка коммутаторов, SNMP, Software Telemetry, DHCPv4, POAP, software upgrade
Eth2	**Endpoint Locator, Day2 Operations (NIR, NAE), MSO**

Рекомендуется изначально организовать подключение Cisco DCNM
тремя сетевыми интерфейсами!

Cisco DCNM – Системные требования

Small (Lab, Poc)	Large (Production)	Compute, 81-350 коммутаторов (Без Network Insights)	Compute, 80 коммутаторов (Network Insights)
CPU: 8 vCPUs RAM: 24 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 32 GB DISK: 500 GB	CPU: 16 vCPUs RAM: 64 GB DISK: 500 GB	CPU: 32 vCPUs RAM: 64 GB DISK: 500 GB

https://www.cisco.com/c/en/us/td/docs/dcn/dcnm/1151/verified-scalability/cisco-dcnm-verified-scalability-1151.pdf

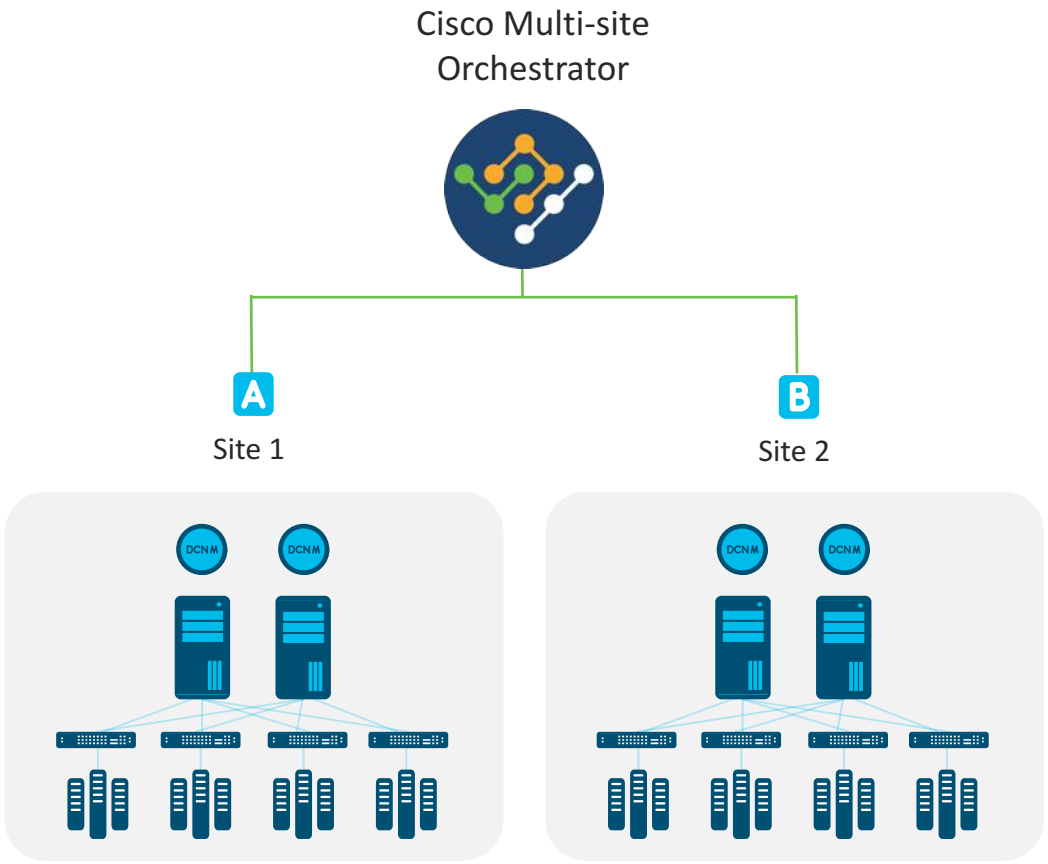
Cisco DCNM
Disaster Recovery

Какие сценарии Cisco DCNM DR поддерживаются?

1. Поддержка репликации виртуальной машины с Cisco DCNM 11.5(1) с помощью VMware SRM
2. Восстановление из резервной копии вручную
3. **Интеграция с Cisco MSO**

MSO 3.2

Cisco DCNM + MSO

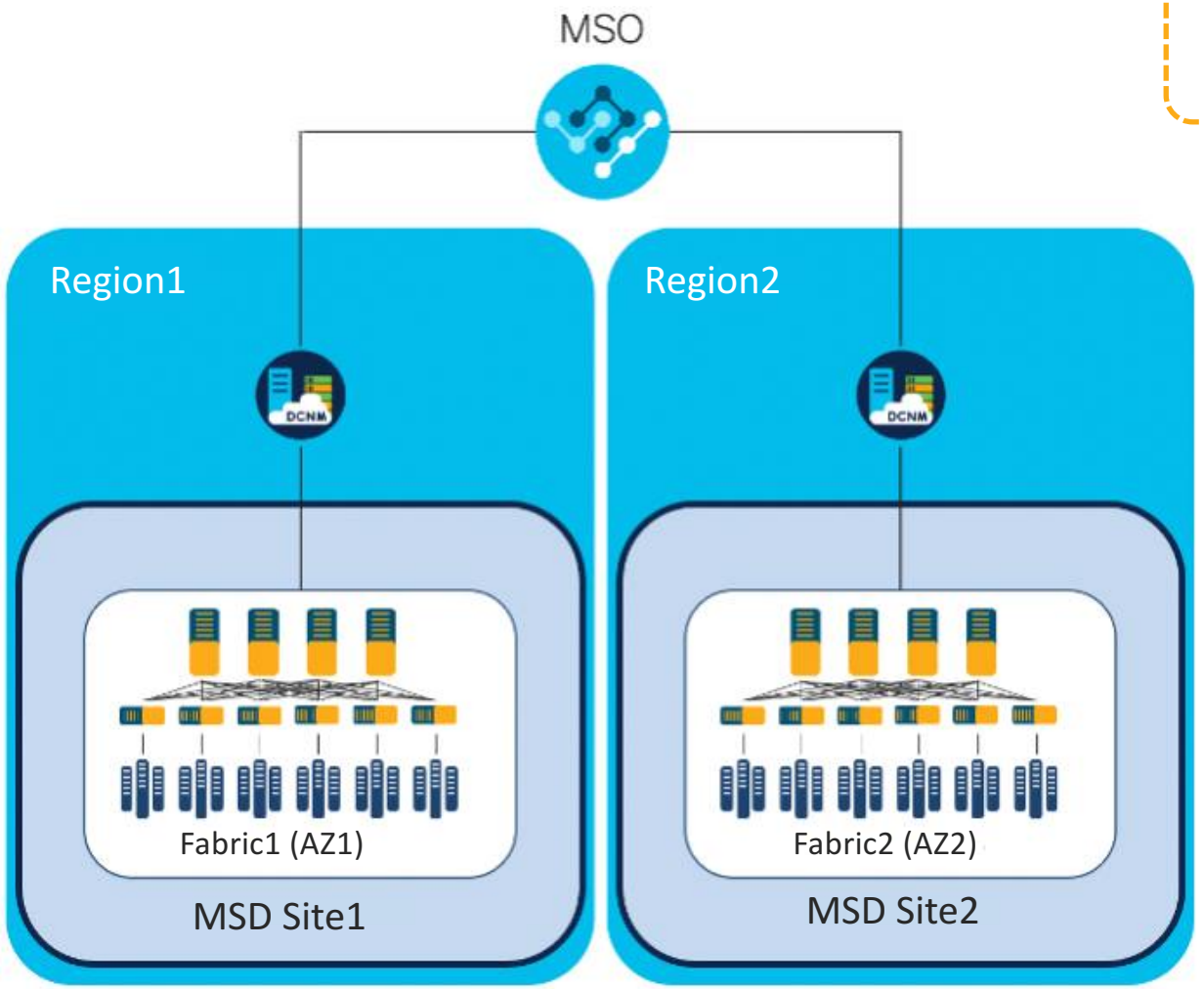


- Формирование Overlay между сайтами
- Горизонтальное масштабирование
  - 6 сайтов Cisco DCNM. До 900 коммутаторов
  - 500 VRFs & networks (L2 - 1500, L3 – 1000)
- Растягивание VRF
- Растягивание L2VNI
- Автоматизация конфигурации VXLAN EVPN Multi-Site BGW
- Поддержка различных топологий VXLAN EVPN Overlay (Full-mesh, Route-Server)
- Конфигурация underlay
- Отслеживание состояния туннелей

Централизованное управление | Disaster Recovery | Формирование зон доступности | Централизованный мониторинг

Интеграция Cisco DCNM и Cisco MSO
Минимальная конфигурация

Данная топология использовалась в рамках третьего дня спринта



Интеграция Cisco DCNM и Cisco MSO
Компоненты решения

Для настройки интеграции необходимо наличие трех компонент:

1. **Cisco Nexus Dashboard (ND)**

   Платформа для запуска Day2 Operations продуктов (Cisco Network Insights) и Cisco MSO.

1. **Cisco Multi-Site Orchestrator (MSO)**

   Единая консоль управления и мониторинга состояния нескольких сайтов. Cisco MSO обеспечивает централизованное управление политиками разных регионов, в каждом из которых присутствует свой экземпляр Cisco DCNM

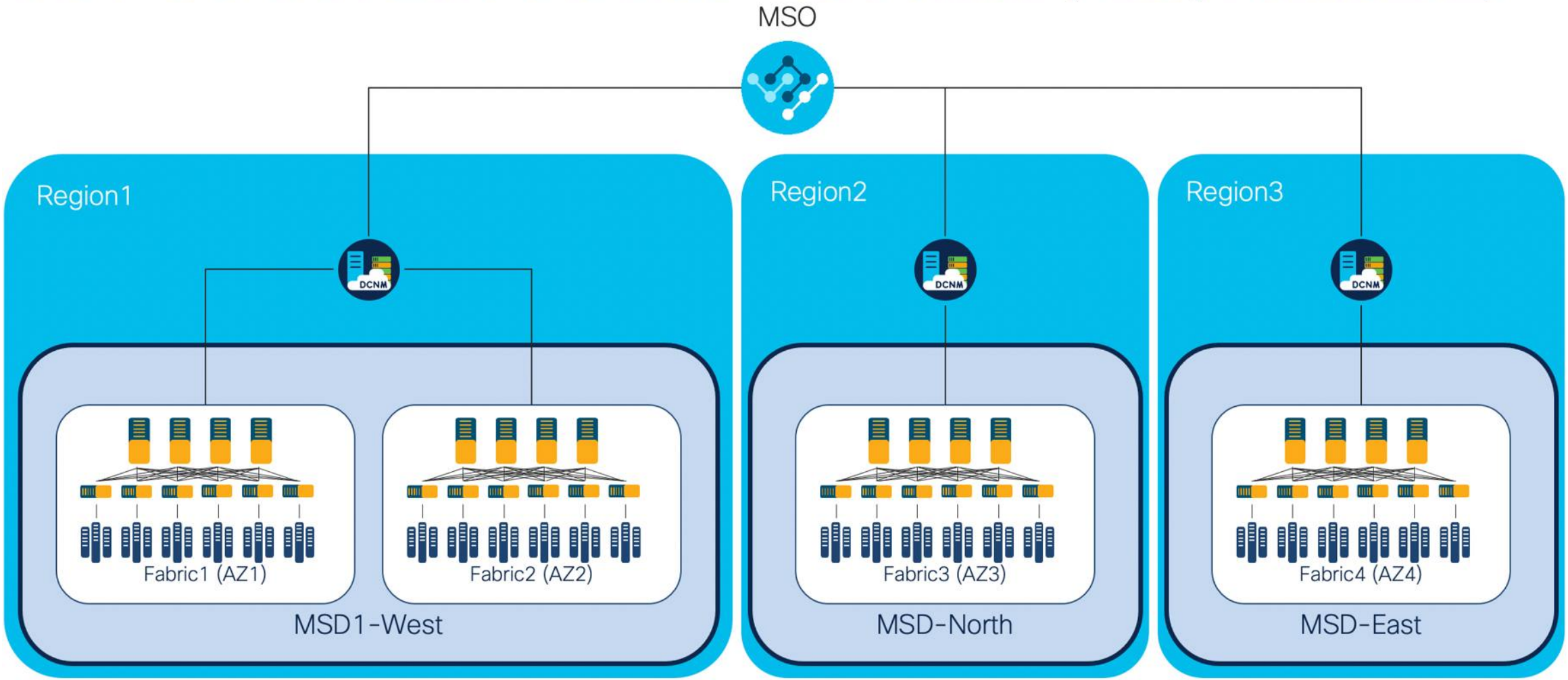
2. **Один или несколько доменов Cisco DCNM Multi-Site Domain (MSD)**

   Один экземпляр Cisco DCNM может управлять как одним, так и несколькими сайтами (MSD) в рамках Cisco VXLAN EVPN Multi-Site. Один или несколько MSD, находящихся под управлением одного экземпляра Cisco DCNM формируют один регион Cisco MSO.

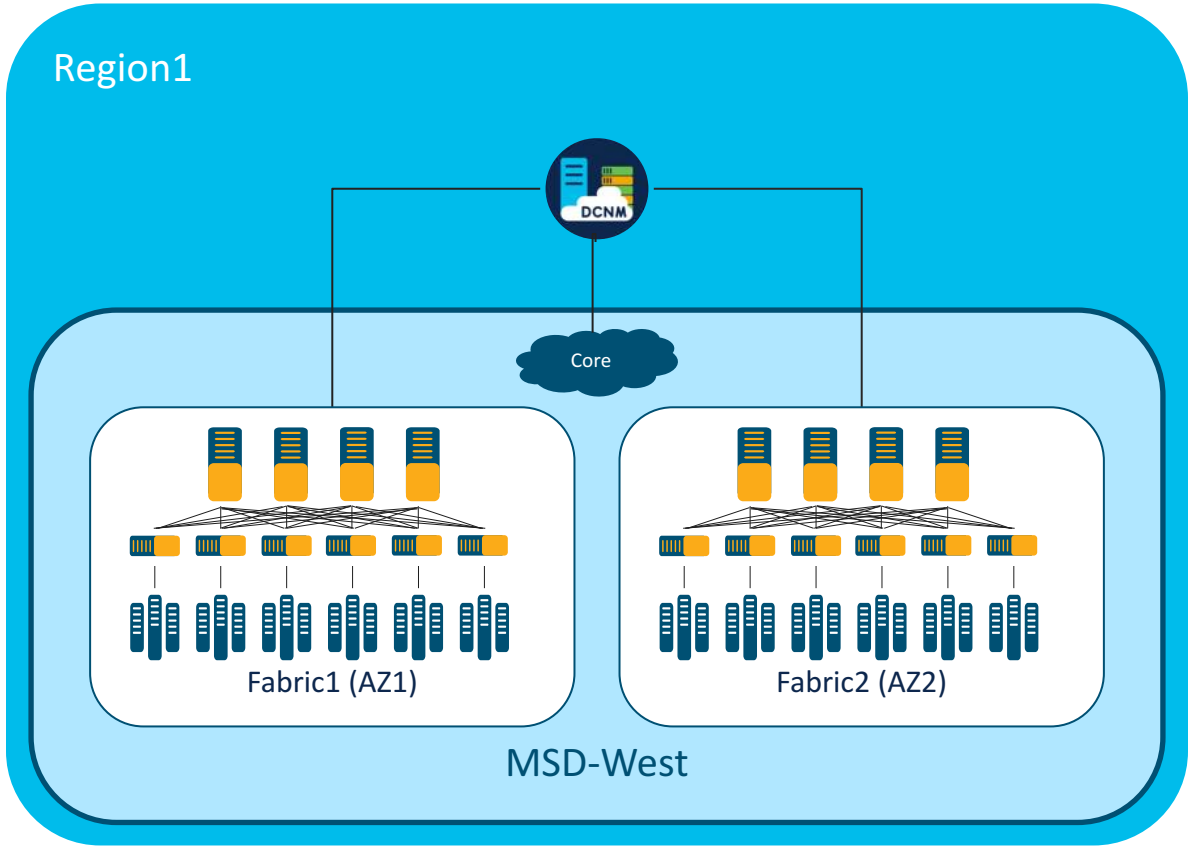
Для работы интеграции необходимо использовать Cisco DCNM 11.5(1), Cisco Nexus Dashboard 2.0.1, Cisco MSO 3.2

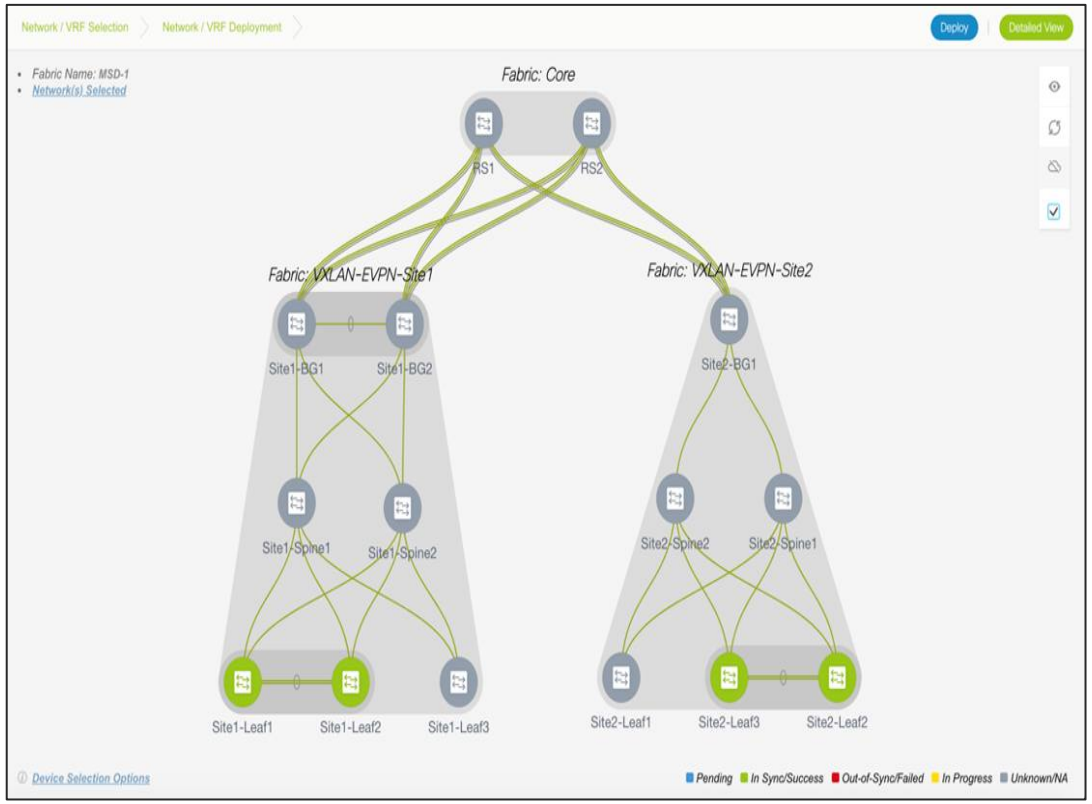
Интеграция Cisco DCNM и Cisco MSO

Несколько зон доступности в рамках одного из регионов



Интеграция Cisco DCNM и Cisco MSO
Формирование зон доступности





Интеграция Cisco DCNM и Cisco MSO
Cisco Nexus Dashboard

- Cisco Nexus Dashboard (ND) представляет собой аппаратный кластер* обеспечивающих хостинг приложений Day2 Operations и Cisco MSO. Члены кластера могут находиться в разных маршрутизируемых подсетях, на значительном расстоянии друг от друга, при условии обеспечения RTT не более чем в 150ms (приложения запускаемые на кластере могут иметь свои собственные требования к задержкам!).
- В текущей версии Cisco ND 2.0.1 не может являться платформой для запуска Cisco DCNM*, поэтому текущая реализация требует наличия отдельно развернутого Cisco DCNM (Standalone или Native HA) в каждом регионе. При необходимости запуска Day2 Ops приложений (Nexus Insights) необходимо использовать compute-only узлы Cisco DCNM.

**Поддержка виртуального Cisco Nexus Dashboard будет добавлена в ближайшем будущем*
***Cisco DCNM может быть установлен на сервер ND, как bare-metal*

Интеграция Cisco DCNM и Cisco MSO
Cisco MSO

Начиная с релиза Cisco MSO 3.2(1) данный компонент должен запускаться поверх Cisco Nexus Dashboard

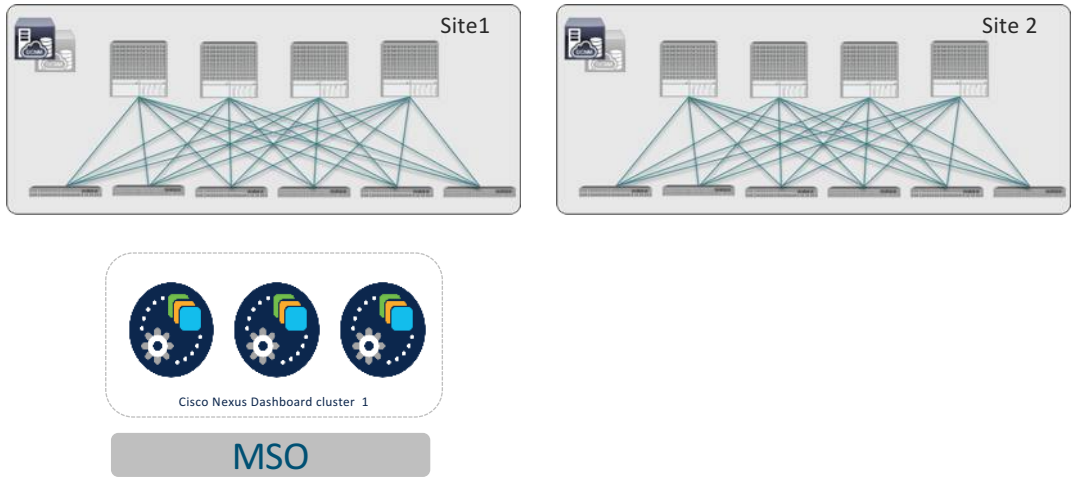
Cisco MSO отвечает за централизованную настройку, мониторинг состояния, и управление жизненным циклом политик сайтов находящихся под управлением разных экземпляров Cisco DCNM

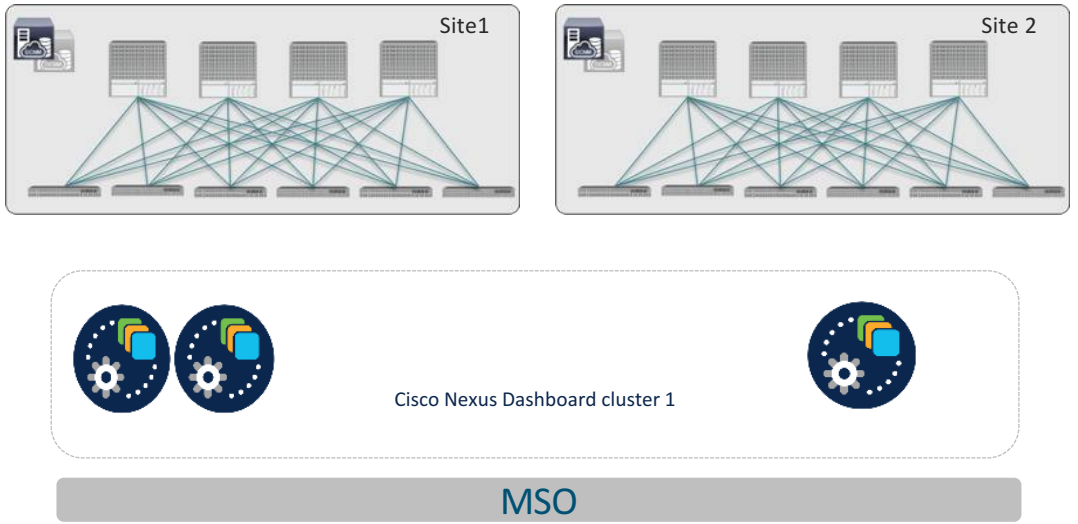
Кластер Cisco MSO состоит из трех нод, каждая из которых может находиться в разных маршрутизируемых подсетях на значительном расстоянии друг от друга (RTT до 150ms). RTT между MSO и DCNM до 500ms.

Размещение компонент по площадкам

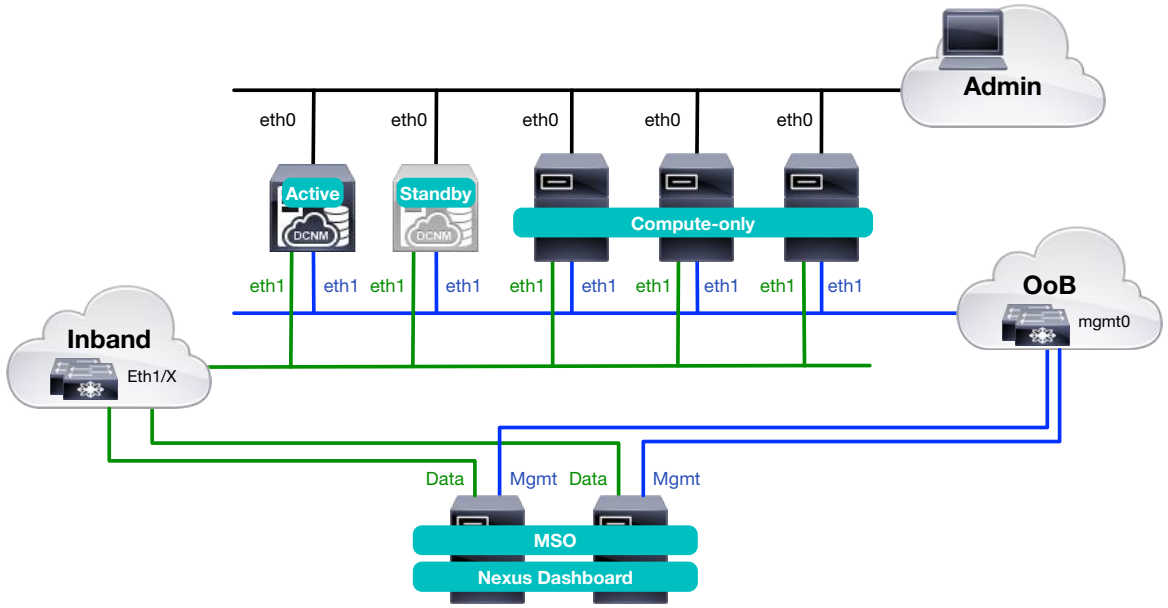
- Аппаратный кластер Cisco Nexus Dashboard состоящий из трех узлов

Не рекомендованный вариант, так как ноды MSO
не распределены по разным сайтам





Интеграция Cisco DCNM и Cisco MSO
Межсетевое взаимодействие в рамках сайта



- Каждый физический сервер Cisco Nexus Dashboard имеет два типа интерфейсов: data (inband) и mgmt. (OoB). Каждый из узлов может находиться в разных подсетях
- Между eth1 интерфейсами Cisco DCNM и Data интерфейсами Cisco Nexus Dashboard должна присутствовать IP связность


CISCO