



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

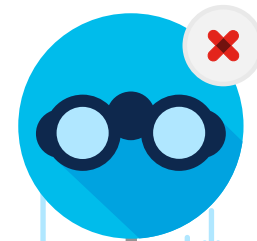
- Основные проблемы эксплуатации сети
- VXLAN OAM
- Day2 Ops возможности, встроенные в DCNM
- Nexus Assurance Engine
- Nexus Dashboard
- Nexus Insights
- Практические аспекты разворачивания DCNM и MSO

Основные проблемы эксплуатации сети

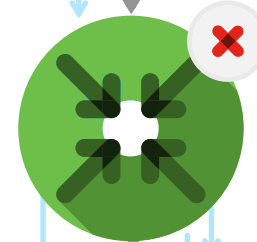
Эксплуатация сети ЦОД – важнее и дороже построения и настройки



Основные проблемы эксплуатации сети



Нет сквозной видимости и понимания происходящего



Нет корреляции событий и проблем



Нет возможности предсказать последствия изменений



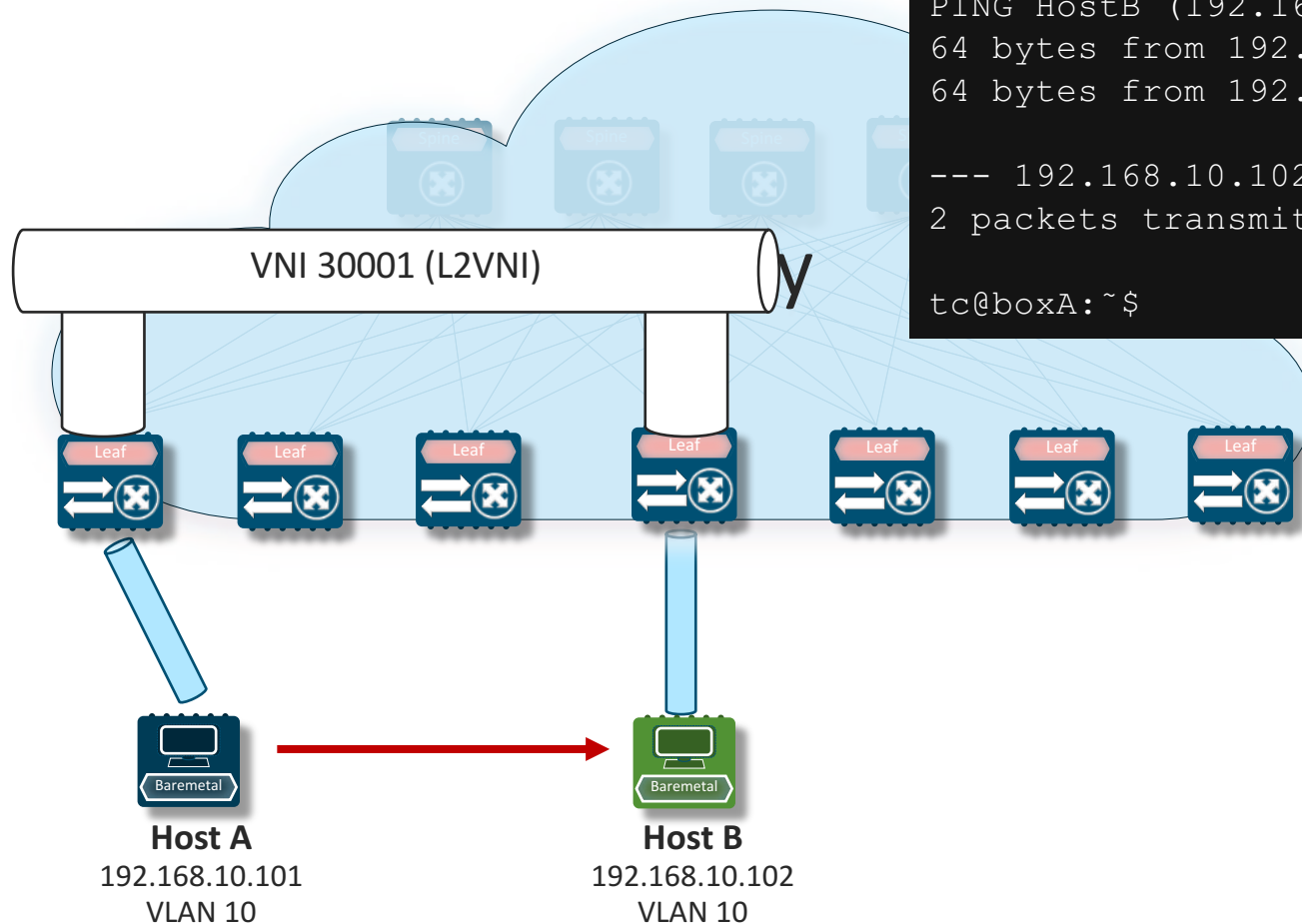
Проблемы производительности и надёжности



VXLAN OAM

Предпосылки появления

Ping/Traceroute в оверлейных сетях – коммутация

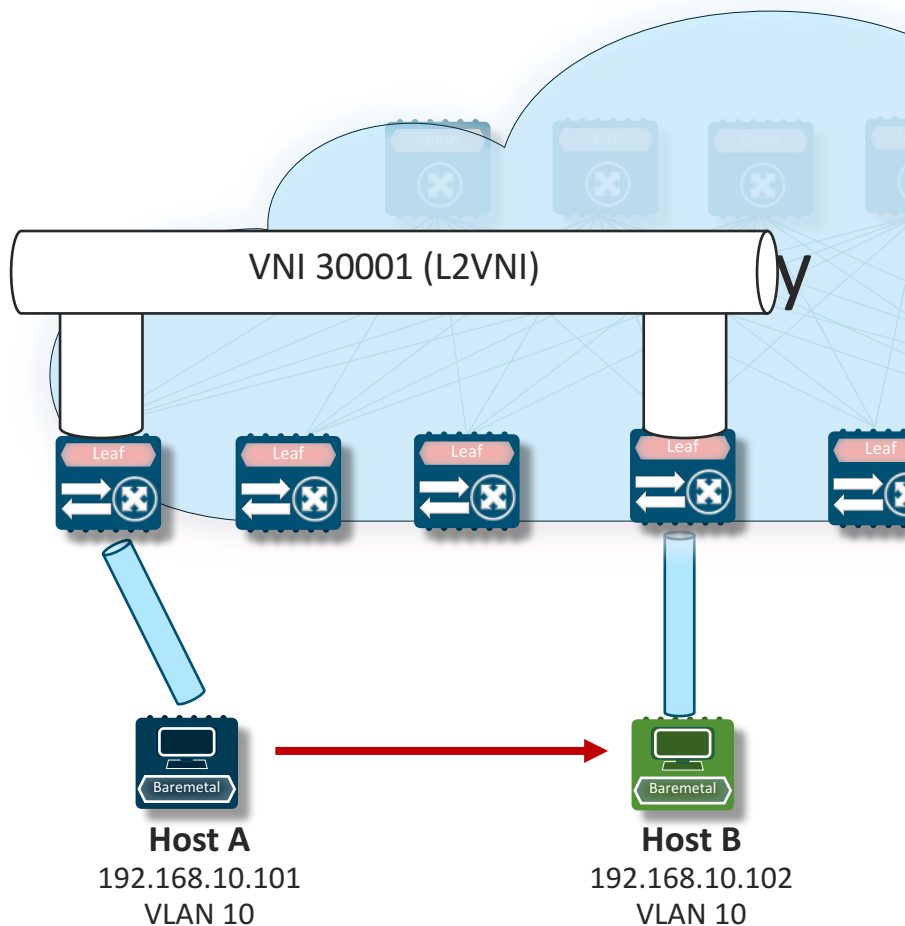


```
tc@boxA:~$ ping HostB
PING HostB (192.168.10.102): 56 data bytes
64 bytes from 192.168.10.102 : icmp_seq=0 ttl=64 time=0.653 ms
64 bytes from 192.168.10.102 : icmp_seq=1 ttl=64 time=0.631 ms

--- 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

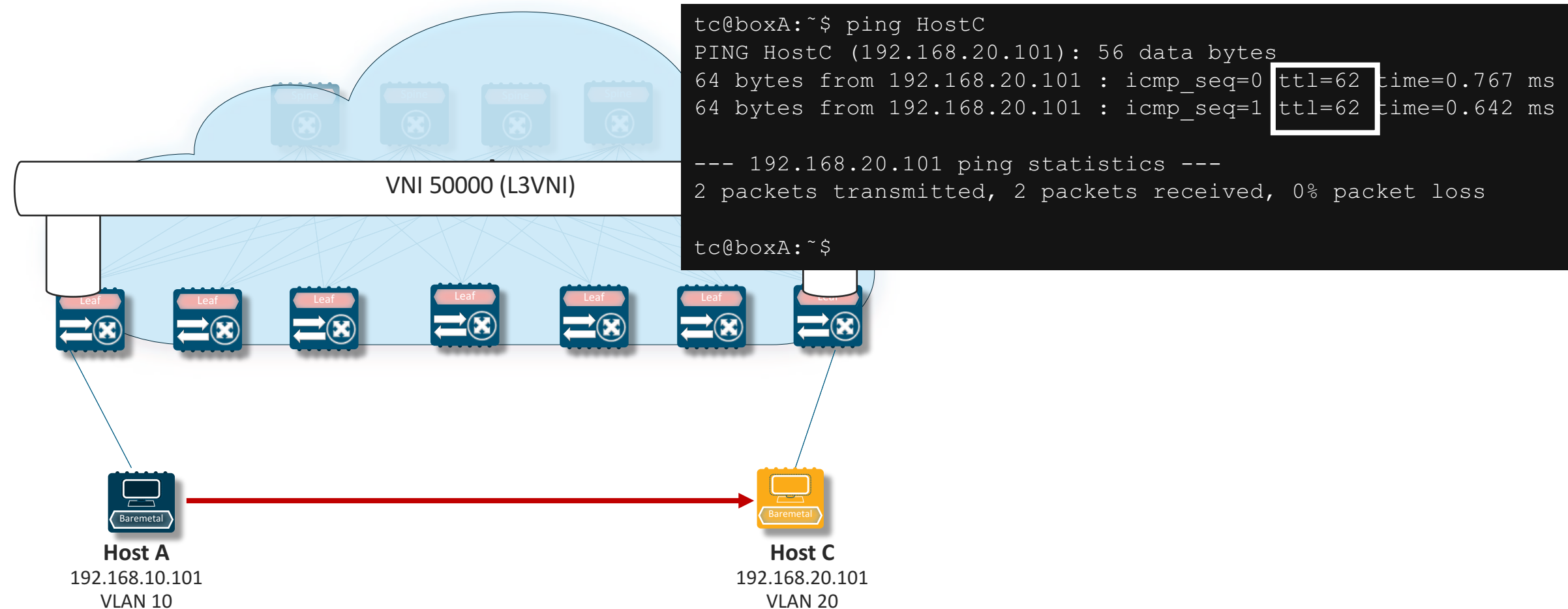
--- 192.168.10.102 ping statistics ---
2 packets transmitted, 2 packets received, 0% packet loss

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

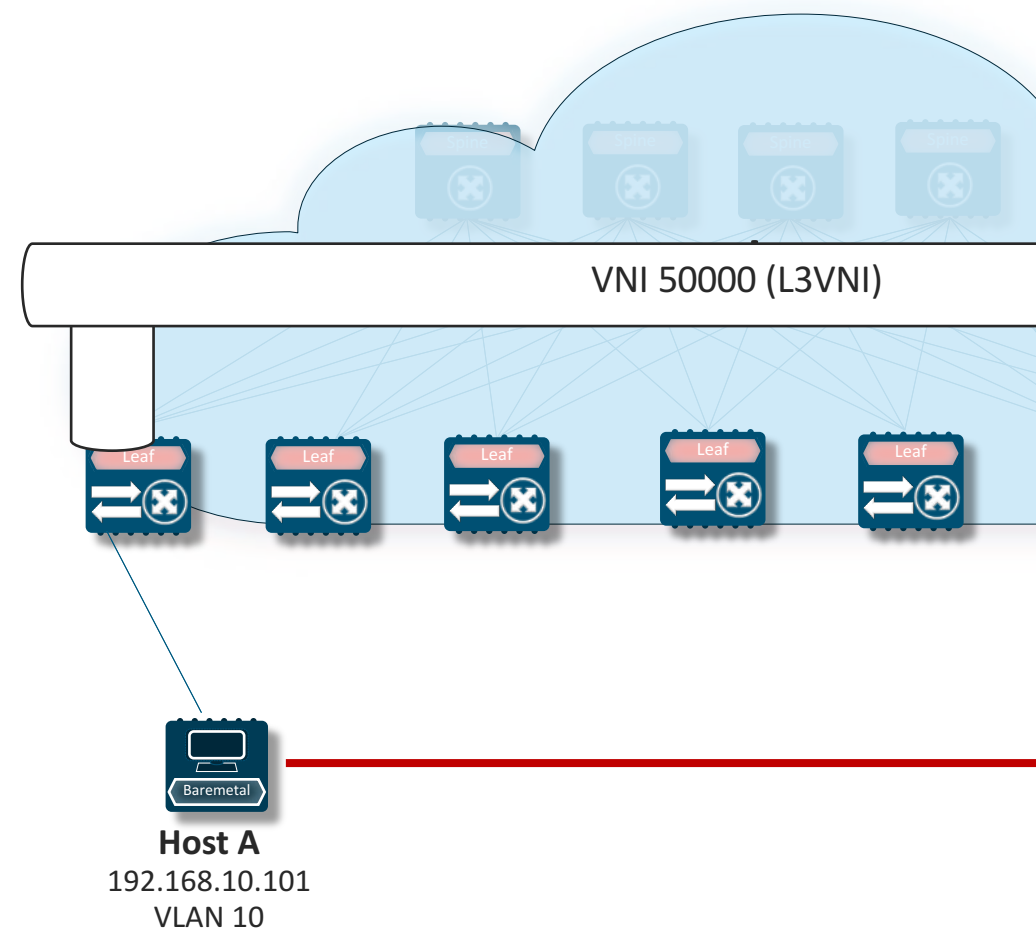
tc@boxA:~$
```

Ping/Traceroute в оверлейных сетях – маршрутизация



*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:~$
```

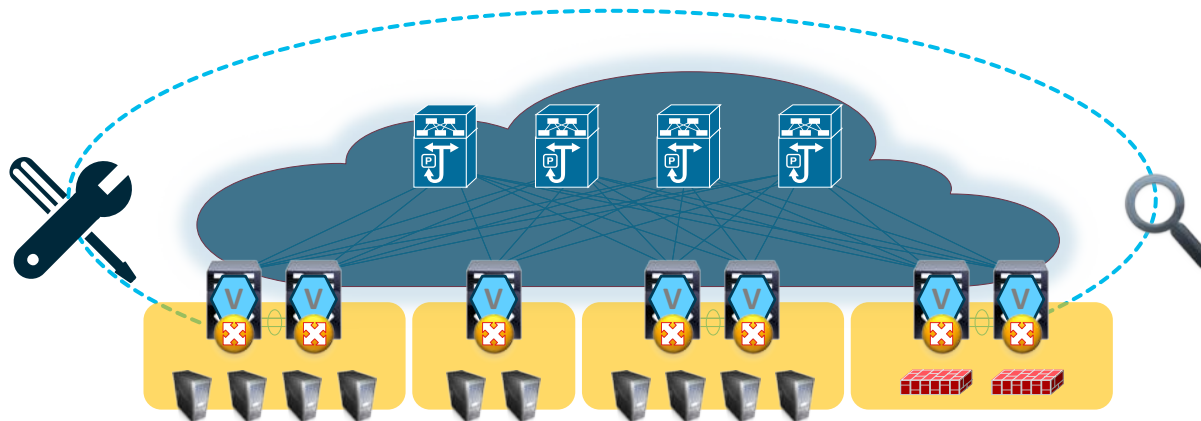
*Как узнать что «под капотом» у
VXLAN EVPN фабрики?*

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

Арсенал средств VXLAN OAM



Ping / Path MTU

- Проверка доступности хоста
- Возможно проверить доступность для пакета с определенной нагрузкой

Pathtrace

- Поиск путей до хостов и VTEP
- Идентификация устройств, интерфейсов, статистика по ошибкам на пути

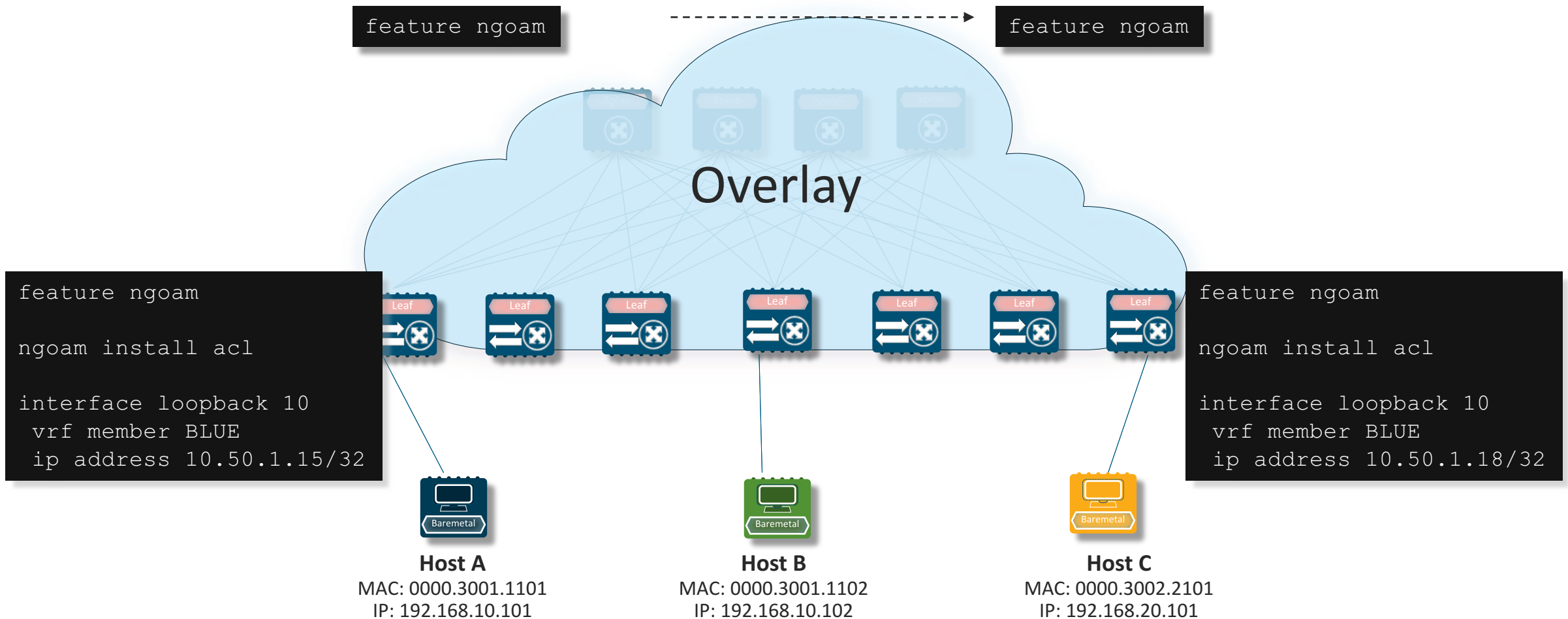
Endpoint Locator

- Обнаружение хостов
- Отслеживание истории перемещений
- Статистика и активности хостов

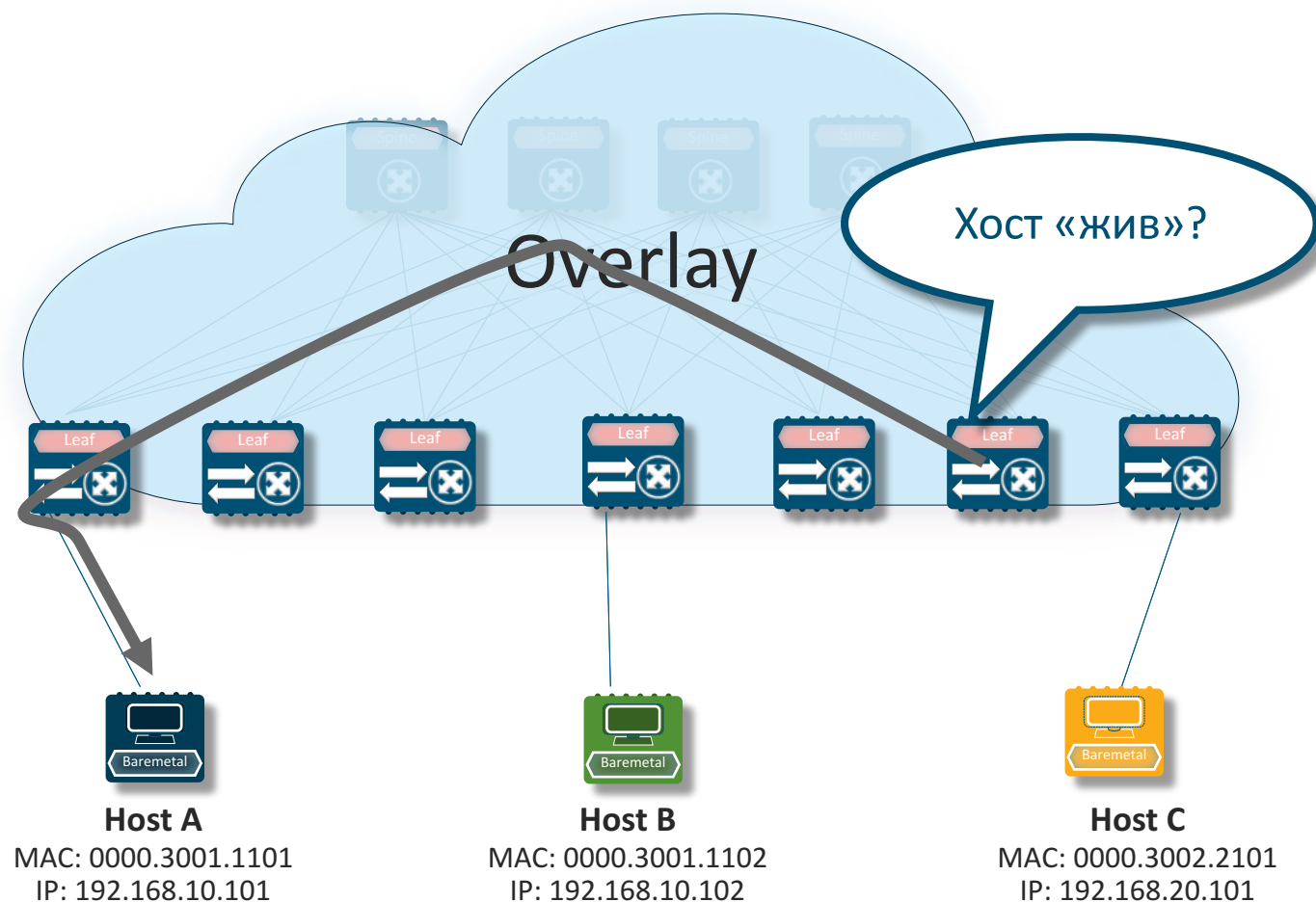
Pro-Active Monitoring

- Мониторинг и уведомления

VXLAN OAM – активация функции (Command Line)



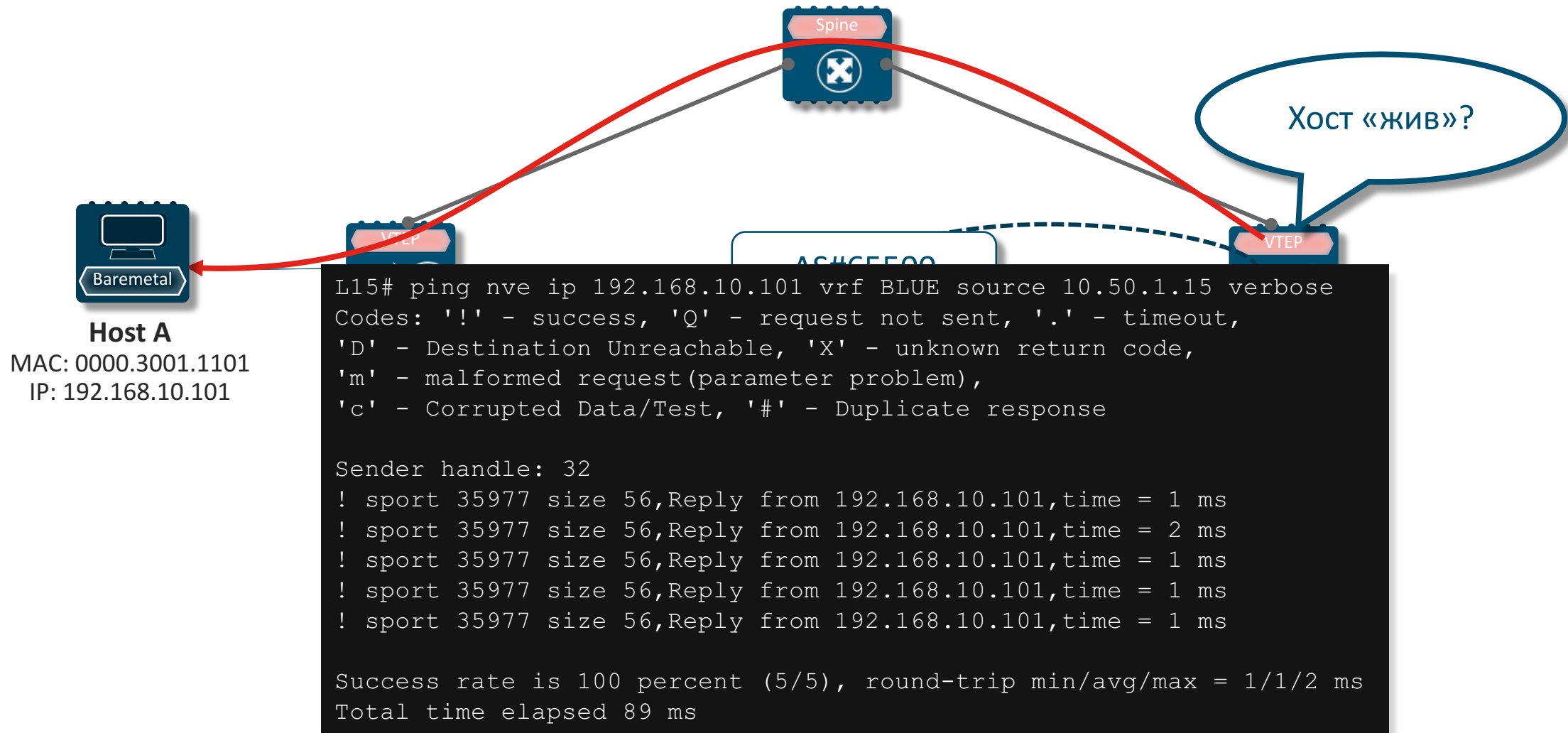
Проверка доступности хоста через оверлей



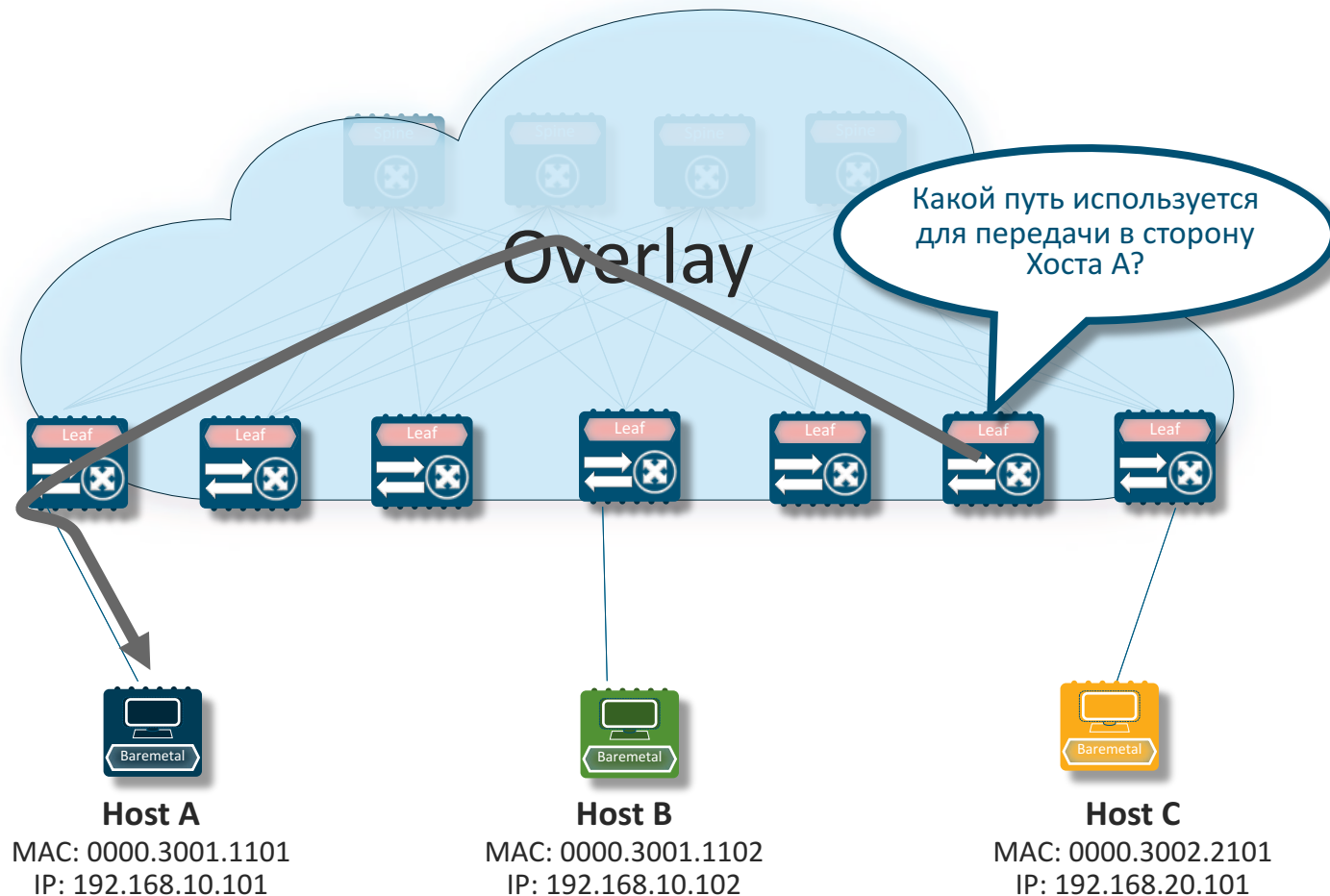
- Доступность хоста
 - Используется ICMP
 - Связь между VTEP и Endpoint
 - Связь между VTEP и VTEP
- Проверка ECMP путей
 - Single Random Path
 - Multiple, Random/Specified Path

Проверка доступности хоста через оверлей

Пример

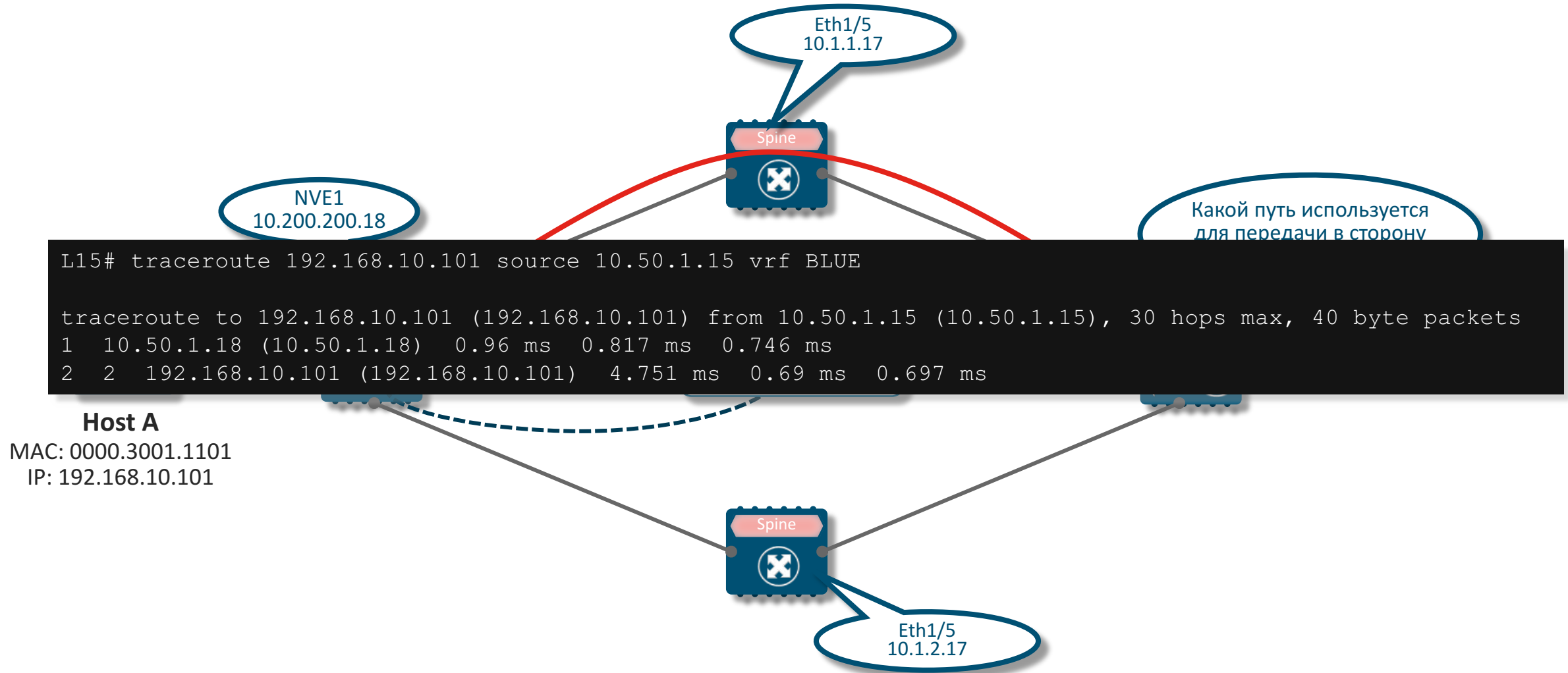


Endpoint Traceroute – VXLAN OAM



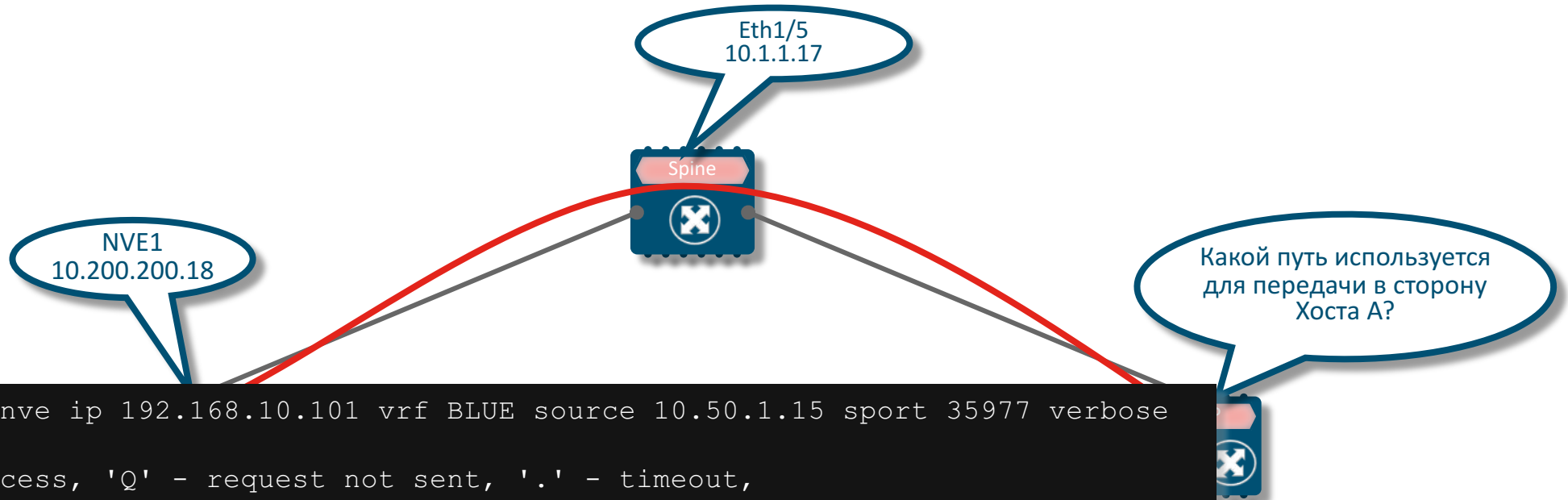
- Доступность хоста
 - Используется ICMP
 - Связь между VTEP и Endpoint
 - Связь между VTEP и VTEP
- Проверка путей
 - Single Specified Path
 - Multiple, Specified Path

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

Day2 Ops возможности, встроенные в DCNM

Dashboard – общее состояние здоровья
Real Time Network View

Day 2 Operations - мониторинг

The screenshot displays the Cisco Data Center Network Manager interface. On the left is a blue sidebar with navigation options: Dashboard, Topology, Control, Monitor, Administration, and Applications. The main area shows a network topology with two fabric regions: 'Fabric : CORE' and 'Fabric : VXLAN_EVPN_Site1'. A 'Quick Search' dropdown menu is open, listing search criteria like Host name, IP, MAC, etc. A 'Real-Time Search' label points to the search bar. A 'Health Score (color)' label points to a green node in the topology. A 'Состояние интерфейса' (Interface Status) label points to a detailed view of 'Ethernet1/51' on 'Site1-BG2', which includes a summary, 24-hour traffic graphs, and a health status of 96%. A 'Состояние коммутатора' (Switch Status) label points to the details of 'Site2-Leaf2', showing its status as 'ok', serial number, CPU usage, and memory usage. A 'Режимы раскладки' (Layout Modes) label points to the bottom of the topology view. A large blue bar at the bottom indicates the overall 'Состояние топологии фабрики' (Fabric topology status).

Dashboard

Topology

Control

Monitor

Administration

Applications

Quick Search

Quick Search

Host name (vCenter)

Host IP

Host MAC

Multicast Group

VXLAN ID (VNI)

VLAN

VXLAN OAM

Real-Time Search

Health Score (color)

Состояние интерфейса

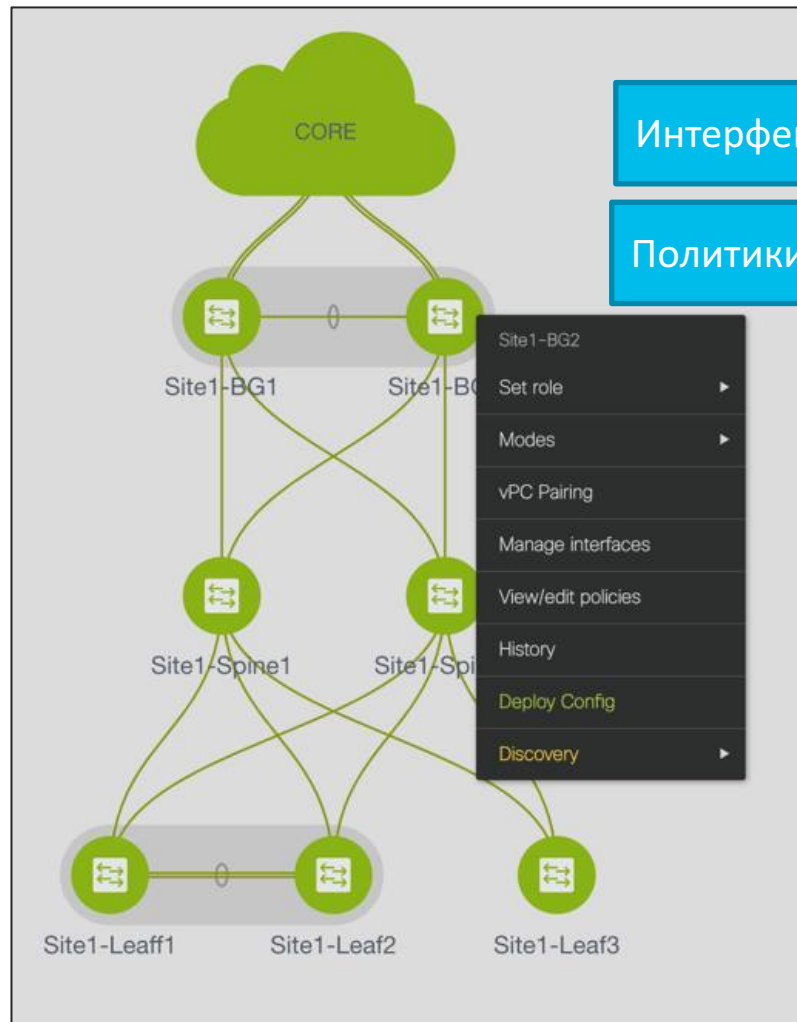
Режимы раскладки

Состояние коммутатора

Состояние топологии фабрики

Мониторинг и поддержка

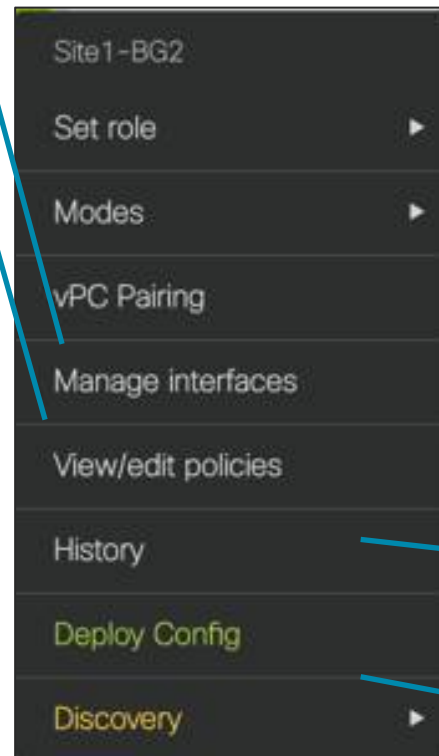
Day 2 Operations – Device Maintenance



Интерфейсы

Политики

Операции с устройством



Роли устройств



Configuration Status & History

Применение конфигурации на устройстве

Режимы работы устройств

Maintenance Mode
Active/Operational Mode

RMA

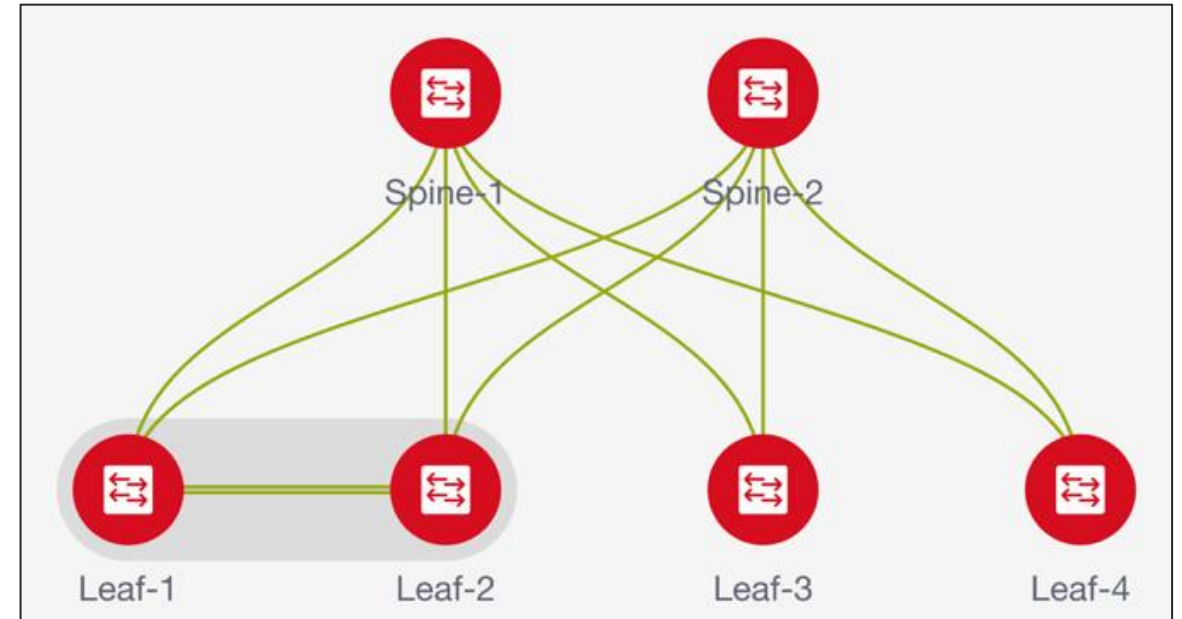
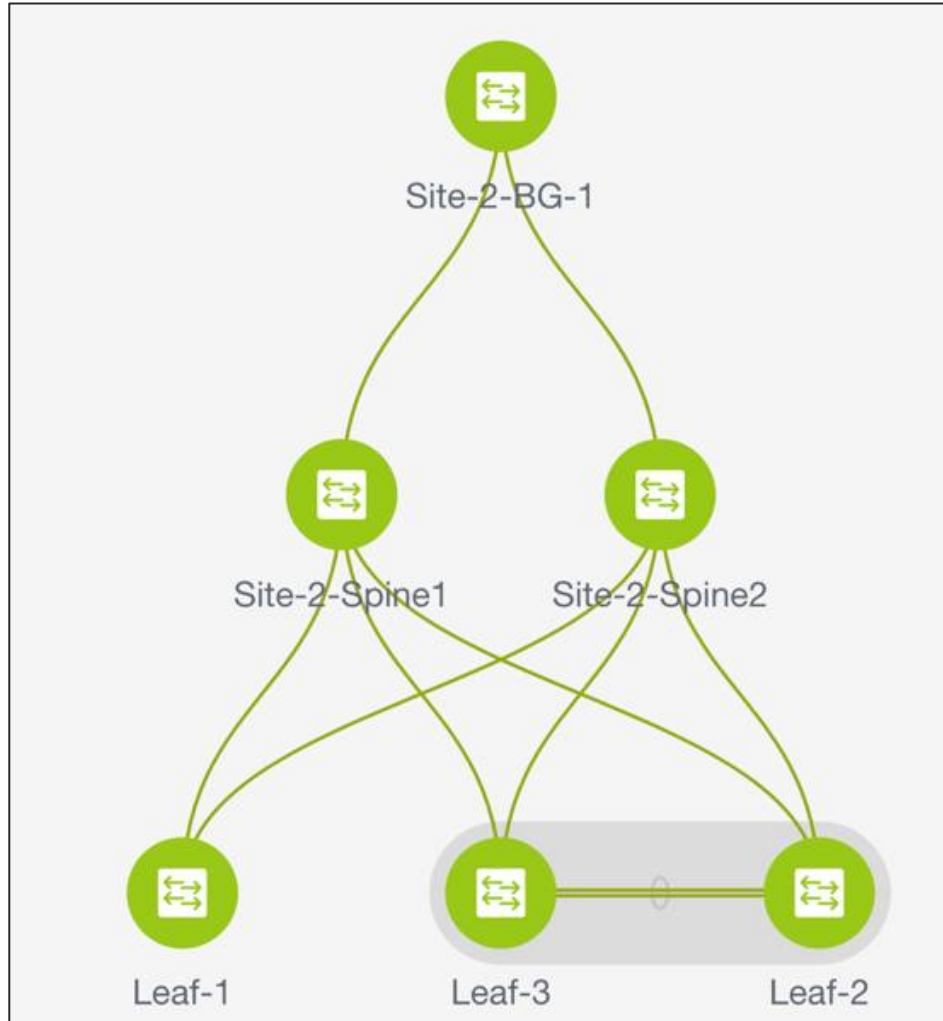
Discovery

Update device credentials
Reload
Rediscover
Remove from fabric

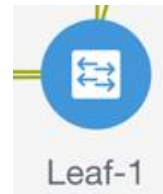
Fabric Builder Day 2 Topology Views

Мониторинг и поддержка...

Day 2 Operations – состояние устройства



Ready to
Deploy



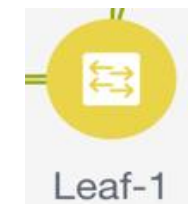
Success/In
Sync



Failed/Out of
Sync



In Progress



Unknown
State / NA



Fabric Builder Real Time Status

Day 2 Operations - мониторинг

Детальная информация о коммутаторе

10.8.254.33
N9K-C9396PX

Leaf

Summary

Status: ok

Serial number: SAL1812NTB6

CPU: 54%

Memory: 29%

Need to find me?

Beacon

Health

96%

Modules in warning 0/8

Switch ports in warning 11/88

Events marked in warning or higher 3/1000

Tags

+

System Tags

VTEP

N9396-EVPN-DC1-2

10.8.254.33
N9K-C9396PX

Leaf

System Info

Modules

Interfaces

Fex

License

Features

VXLAN

VLAN

VXLAN

Total 22

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

The screenshot displays the Configuration Compliance interface for Switch 1.57.52.10. It features four main panels: Pending Config, Expected Config, Current Config, and Side-by-side Comparison. The Pending Config panel lists various features like vpc, ospf, pim, nxapi, and nv overlay. The Expected Config panel shows the configuration as it should be, including hostname, password strength check, and various resource limits. The Current Config panel shows the actual running configuration, including version, hostname, vdc, resource limits, cfs eth distribute, no password strength-check, username admin password, ip domain-lookup, snmp-server, rmon event, and interface Ethernet1/1. The Side-by-side Comparison panel compares the running configuration with the expected configuration, highlighting differences in color (orange for running, green for expected).

Pending Config

Config Preview - Switch 1.57.52.10

Pending Config

- feature vpc
- feature ospf
- feature pim
- feature nxapi
- nv overlay evpn
- feature interface-vl
- feature vn-segment-v
- feature dhcp
- feature lldp
- feature nv overlay
- feature bgp
- cfs eth distribute
- feature lacp
- feature ngom
- feature tacacs+
- nxapi http port 80
- router ospf UNDERLAY
- router-id 10.2.0.3
- ip pim ssm range 232
- ip pim rp-address 10
- ngom install acl
- ip dhcp snooping
- service dhcp
- ip dhcp relay
- ip dhcp relay inform
- ip dhcp relay inform
- ip6 dhcp relay
- fabric forwarding an
- route-map fabric-rma
- match tag 12345
- router bgp 65001
- router-id 10.2.0.3
- router bgp 65001
- neighbor 10.2.0.7
- feature nv overlay
- remote-as 65001
- update-source loopba
- address-family 12vpr
- send-community
- send-community exte

Expected Config

Config Preview - Switch 1.57.52.10

Expected Config

- hostname Site1-Leaf1
- no password strength-check
- feature vpc
- power redundancy-mode ps-redundant
- copp profile strict
- feature ospf
- feature pim
- feature nxapi
- nv overlay evpn
- feature interface-vlan
- feature vn-segment-vlan-based
- feature dhcp
- feature lldp
- feature nv overlay
- feature bgp
- cfs eth distribute
- feature lacp
- feature ngom

Current Config

Config Preview - Switch 1.57.52.10

Current Config

```
!Command: show running-config
!Time: Sat Jan 5 03:05:50 2019

version 7.0(3)I7(2)
hostname Site1-Leaf1
vdc Site1-Leaf1 id 1
  limit-resource vlan minimum 16 maximum 4094
  limit-resource vrf minimum 2 maximum 4096
  limit-resource port-channel minimum 0 maximum 256
  limit-resource u4route-mem minimum 248 maximum 248
  limit-resource u6route-mem minimum 96 maximum 96
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

cfs eth distribute

no password strength-check
username admin password 5 $$$A9bChNsA$HxBUKKh9U4fzMs1FAZKbusdJRYSDDG1G16skqfKE
ip domain-lookup
copp profile strict
snmp-server user admin network-admin auth md5 0x66c51380bfd33a55b66ea4e5b943082
snmp-server host 172.20.179.50 traps version 2c public udp-port 2162
rmon event 1 description FATAL(1) owner PMON@FATAL
rmon event 2 description CRITICAL(2) owner PMON@CRITICAL
rmon event 3 description ERROR(3) owner PMON@ERROR
rmon event 4 description WARNING(4) owner PMON@WARNING
rmon event 5 description INFORMATION(5) owner PMON@INFO

ip6 switch-packets lla
vlan 1

vrf context management
  ip route 0.0.0.0/0 192.168.100.1
hardware access-list tcam region qos 0
hardware access-list tcam region arp-ether 256 double-wide

interface Ethernet1/1
  description "port-channel 500 (vpc-peer-link) member"
```

Side-by-side Comparison

Config Preview - Switch 1.57.52.10

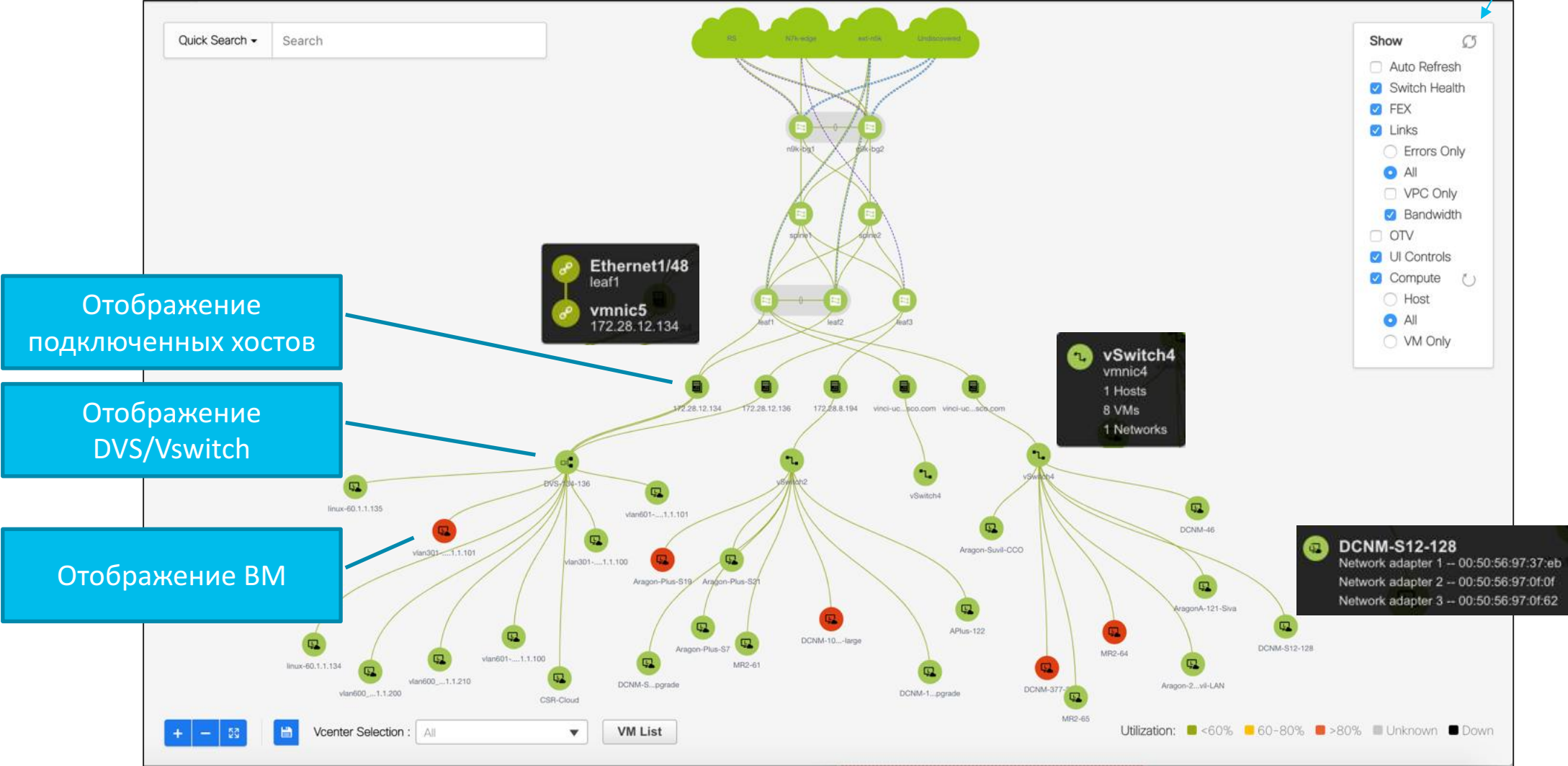
Side-by-side Comparison

Running config	Expected config
1 version 7.0(3)I7(2)	
2 hostname Site1-Leaf1	hostname Site1-Leaf1
3 vdc site1-leaf1 id 1	
4 limit-resource vlan minimum 16 maximum 4094	
5 limit-resource vrf minimum 2 maximum 4096	
6 limit-resource port-channel minimum 0 maximum 256	
7 limit-resource u4route-mem minimum 248 maximum 248	
8 limit-resource u6route-mem minimum 96 maximum 96	
9 limit-resource m4route-mem minimum 58 maximum 58	
10 limit-resource m6route-mem minimum 8 maximum 8	
11 cfs eth distribute	cfs eth distribute
12	feature lacp
13	feature ngom
14	feature tacacs+
15 no password strength-check	no password strength-check
16	feature vpc
17 username admin password 5 \$\$\$A9bChNsA\$HxBUKKh9U4fzMs1FAZKbusdJRYSDDG1G16skqfKEIS role network-admin	username admin password 5 \$\$\$A9bChNsA\$HxBUKKh9U4fzMs1FAZKbusdJRYSDDG1G16skqfKEIS role network-admin
18 ip domain-lookup	

Configuration Compliance (Expected или Current Configuration View)

Day 2 Operations - мониторинг

!= VMM интеграции в ACI



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

VXLAN OAM – возможности,
встроенные в DCNM

Day 2 Operations - мониторинг

VXLAN OAM – Ping Trace Route

The screenshot displays the Cisco Data Center Network Manager interface. On the left is a navigation sidebar with options: Dashboard, Topology, Control, Monitor, Administration, and Applications. The main panel is titled 'VXLAN OAM' and contains a configuration form. The form has two tabs: 'Switch to switch' (selected) and 'Host to host'. Under the 'Switch to switch' tab, there are three dropdown menus: 'Source Switch' (set to leaf3), 'Destination Switch' (set to leaf1), and 'VRF' (set to myvrf_50000). Below these is a checkbox for 'All Paths Included' which is unchecked. A note states: 'NOTE: Please ensure loopback interface is configured for corresponding VRF, which is required for switch to switch OAM.' At the bottom of the form are buttons for 'Details', 'Clear Data', and 'Submit'. A red box highlights the configuration fields, with red arrows pointing to them from external labels: 'Source Switch' pointing to leaf3, 'Destination Switch' pointing to leaf1, and 'VRF' pointing to myvrf_50000. A blue box with Russian text points to the 'VRF' dropdown. The network topology on the right shows a cloud labeled 'site2' connected to a VRF. Below it are two spine switches (spine1, spine2) and three leaf switches (leaf1, leaf2, leaf3). The 'Switch to Switch OAM Result' panel on the right shows the following data:

Switch to Switch OAM Result	
Ping Status	Success
Source port	62155
Success rate	100%
Minimum RTT	1ms
Maximum RTT	5ms
Average RTT	2ms
Traceroute Path	
Switch Name	spine2
1 IP address	11.4.0.17
Time	1 ms
Switch Name	leaf1
2 IP address	11.3.0.5
Time	5 ms
Switch Name	leaf1
3 IP address	11.3.0.5
Time	1 ms

Требуется
настроить Loopback
в VRF для которого
делается анализ

Day 2 Operations - мониторинг VXLAN OAM – Endpoint Path Trace

The screenshot displays the Cisco Data Center Network Manager interface. On the left is a blue sidebar with navigation links: Dashboard, Topology, Control, Monitor, Administration, and Applications. The main panel is titled 'VXLAN OAM' and includes a search bar and a 'Switch to switch' dropdown set to 'Host to host'. Below this, there are input fields for Source IP (60.1.1.200), Destination IP (61.1.1.100), VRF (MyVRF_50000), Source Port (FTP 20), Destination Port (Http 80), and Protocol (TCP 6). A 'Layer 2 Only' checkbox is also present. A blue callout box with the text 'Исходные данные:' (Initial data:) points to the VRF field and lists: Source IP, Destination IP, VRF, and Payload Information (Option). The network topology diagram shows three leaf switches (leaf1, leaf2, leaf3) connected to two spine switches (spine1, spine2). Leaf1 and leaf2 are connected to spine1, while leaf2 and leaf3 are connected to spine2. Above the spines are two boundary gateways (n9k-bg1, n9k-bg2) and two external networks (ext-n5k, Undiscovered). A legend at the bottom right indicates utilization levels: <60% (green), 60-80% (yellow), >80% (red), Unknown (grey), and Down (black).

Исходные данные:

- Source IP
- Destination IP
- VRF
- Payload Information (Опция)

Day 2 Operations - мониторинг

VXLAN OAM – Endpoint Path Trace

The screenshot displays the Cisco Data Center Network Manager interface. On the left is a navigation sidebar with links to Dashboard, Topology, Control, Monitor, Administration, and Applications. The main panel is titled 'VXLAN OAM' and includes a search bar and tabs for 'Switch to switch' and 'Host to host'. The 'Host to host' tab is active, showing configuration fields for Source IP (60.1.1.200), Destination IP (61.1.1.100), VRF (MyVRF_50000), Source Port (FTP 20), Destination Port (Http 80), and Protocol (TCP 6). Below these fields are 'Details', 'Clear Data', and 'Submit' buttons. A blue arrow points from the 'Details' button to a blue callout box. The callout box, titled 'Детали:', contains a bulleted list: 'Счетчики Ingress Interface' and 'Счетчики Egress Interface'. A white modal window titled 'Host to Host OAM Details' is open, displaying a table of statistics for Index 1. The table lists metrics for both Ingress and Egress interfaces, including switch name, IP address, interface name, state, and various counters like rx_len, rx_bytes, rx_pkt_rate, rx_byte_rate, rx_load, rx_ucast, rx_mcast, rx_bcast, rx_discards, rx_errors, rx_unknown, tx_len, tx_bytes, tx_pkt_rate, tx_byte_rate, tx_load, tx_ucast, tx_mcast, tx_bcast, tx_discards, tx_errors, and tx_unknown. The background shows a network topology with nodes labeled leaf1, leaf2, leaf3, spine1, spine2, n9k-bg2, ext-n5k, and Undiscovered. A legend at the bottom right indicates utilization levels: <60% (green), 60-80% (yellow), >80% (red), Unknown (grey), and Down (black).

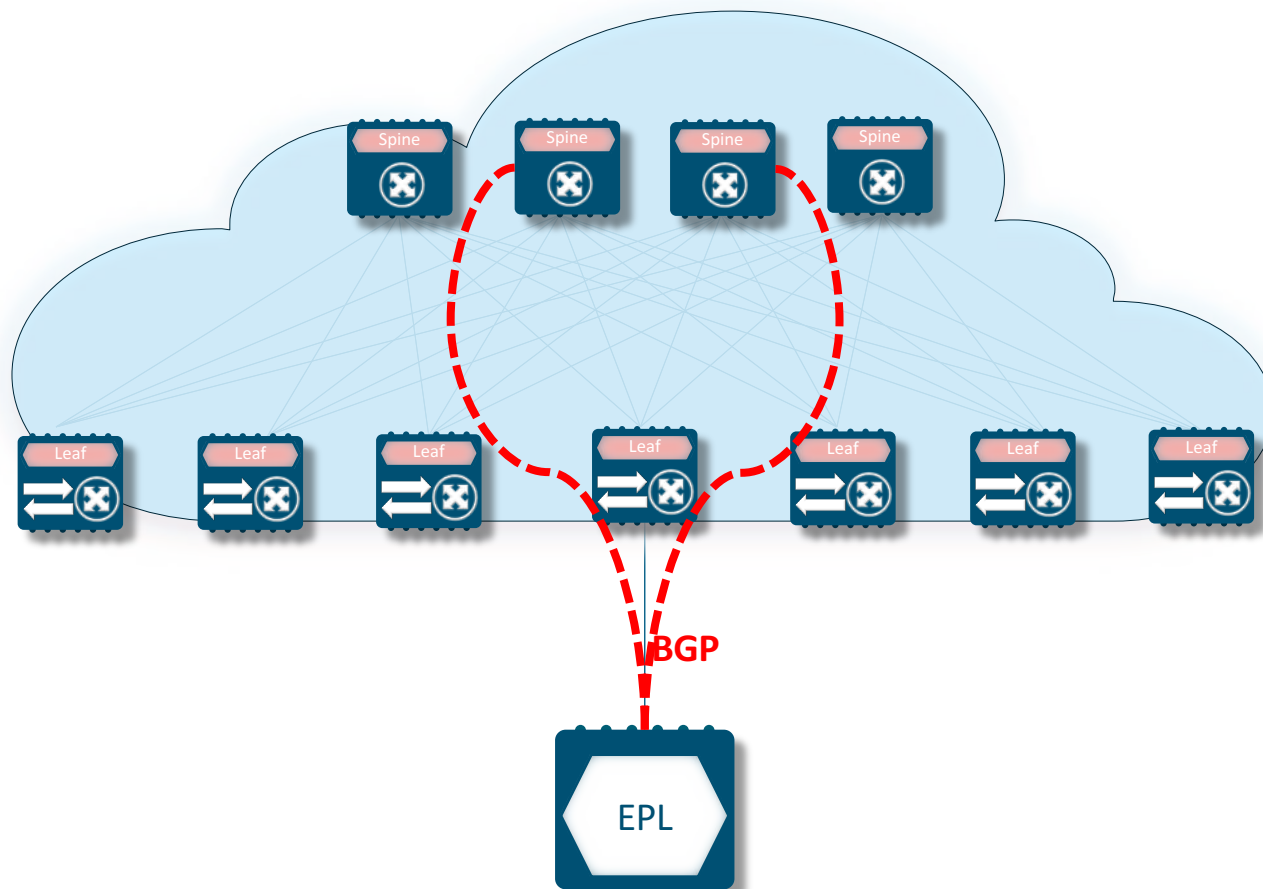
Host to Host OAM Details

Index	1
Switch Name	spine1
IP address	11.4.0.25
Ingress Interface	
if_name	Eth1/45
if_state	UP
rx_len	84
rx_bytes	270524673
rx_pkt_rate	0
rx_byte_rate	129
rx_load	10
rx_ucast	137842
rx_mcast	1464258
rx_bcast	3
rx_discards	0
rx_errors	0
rx_unknown	0
rx_bandwidth	10000000
tx_len	76
tx_bytes	119477380
tx_pkt_rate	0
tx_byte_rate	67
tx_load	10
tx_ucast	138349
tx_mcast	829012
tx_bcast	204
tx_discards	0
tx_errors	0
tx_bandwidth	10000000
Egress Interface	
if_name	Eth1/43
if_state	UP
rx_len	84
rx_bytes	329353342
rx_pkt_rate	0
rx_byte_rate	113
rx_load	10
rx_ucast	1083465
rx_mcast	1277603
rx_bcast	47
rx_discards	0
rx_errors	0
rx_unknown	0

End Point Locator

Day 2 Operations - мониторинг

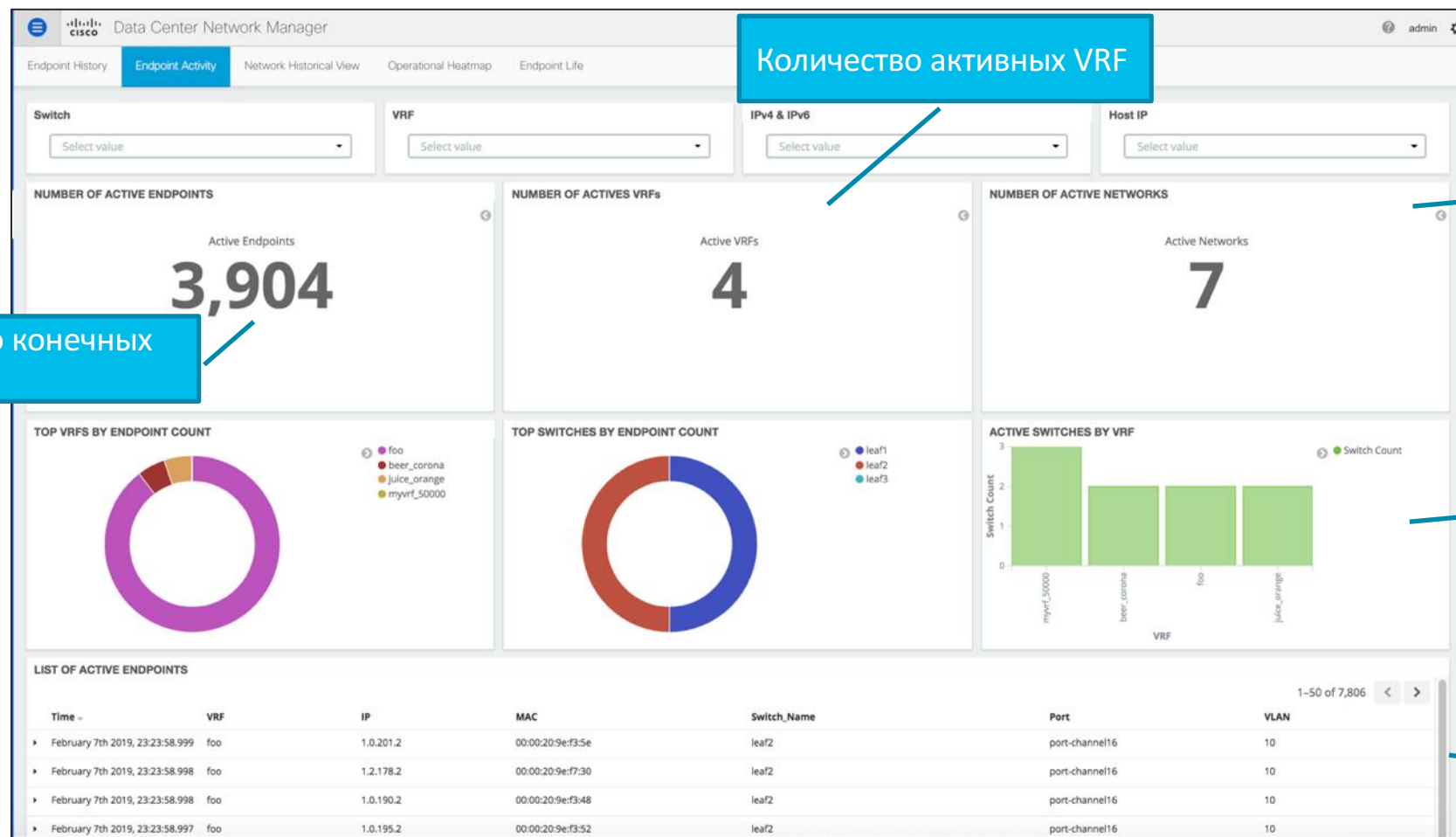
Мониторинг подключений



- 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



Endpoint Locator (EPL)

Nexus Assurance Engine

Cisco Network Assurance Engine

Как валидировать сеть – сейчас и на будущее?



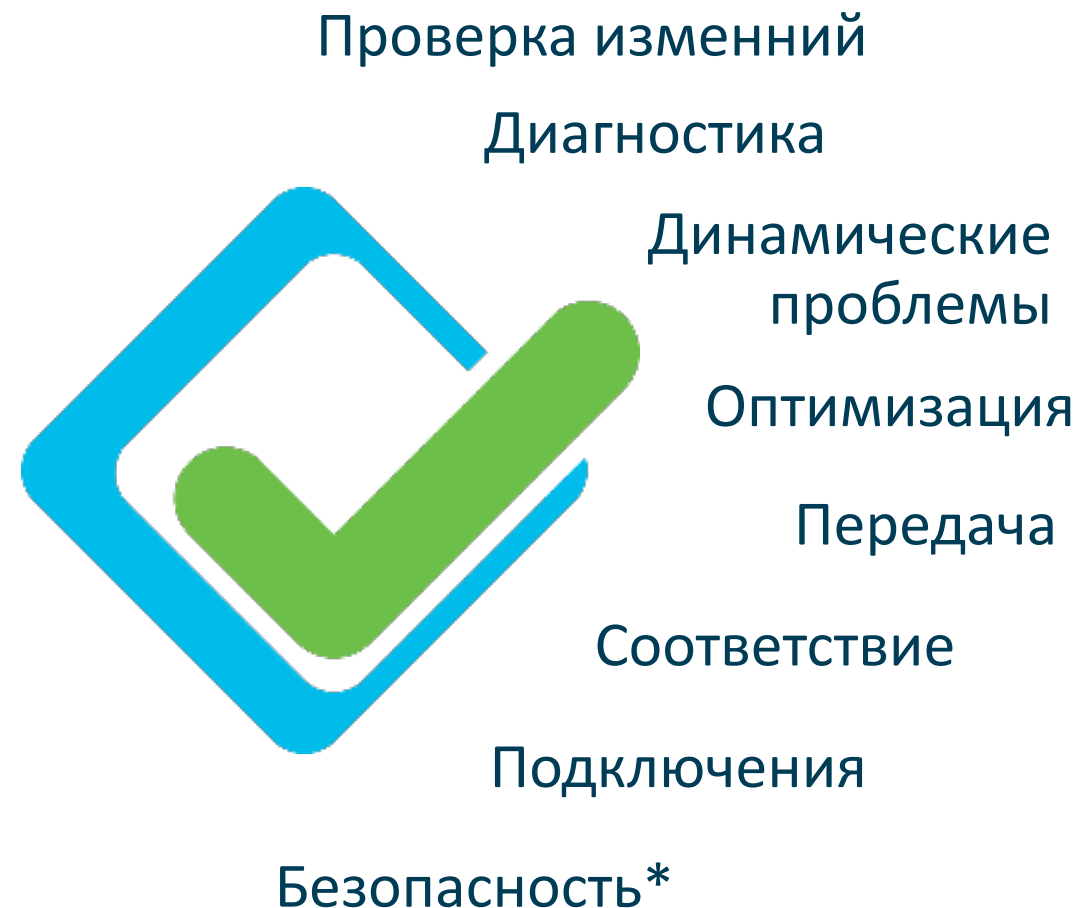
Предсказать* и показать
результат изменений



Проверить состояние в
масштабах сети

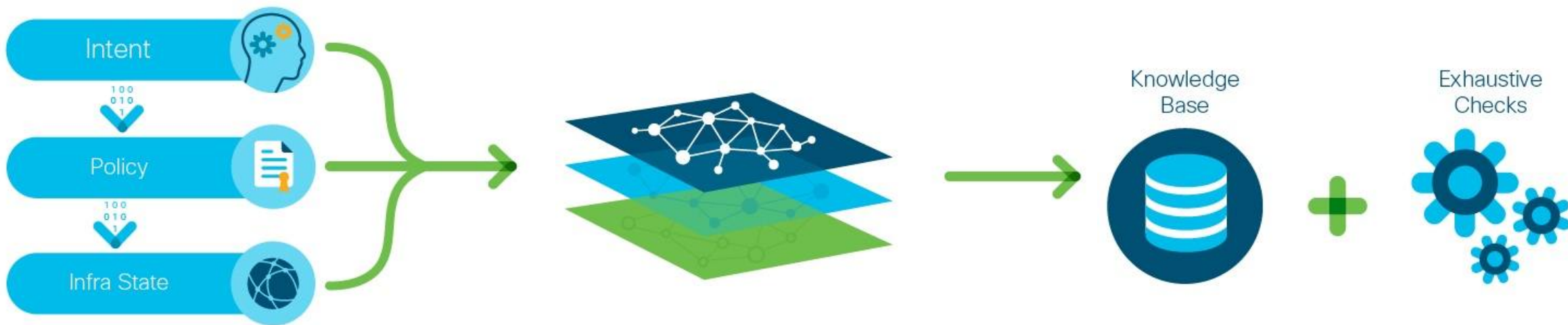


Гарантировать политику
безопасности и ее
соответствие*



* 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

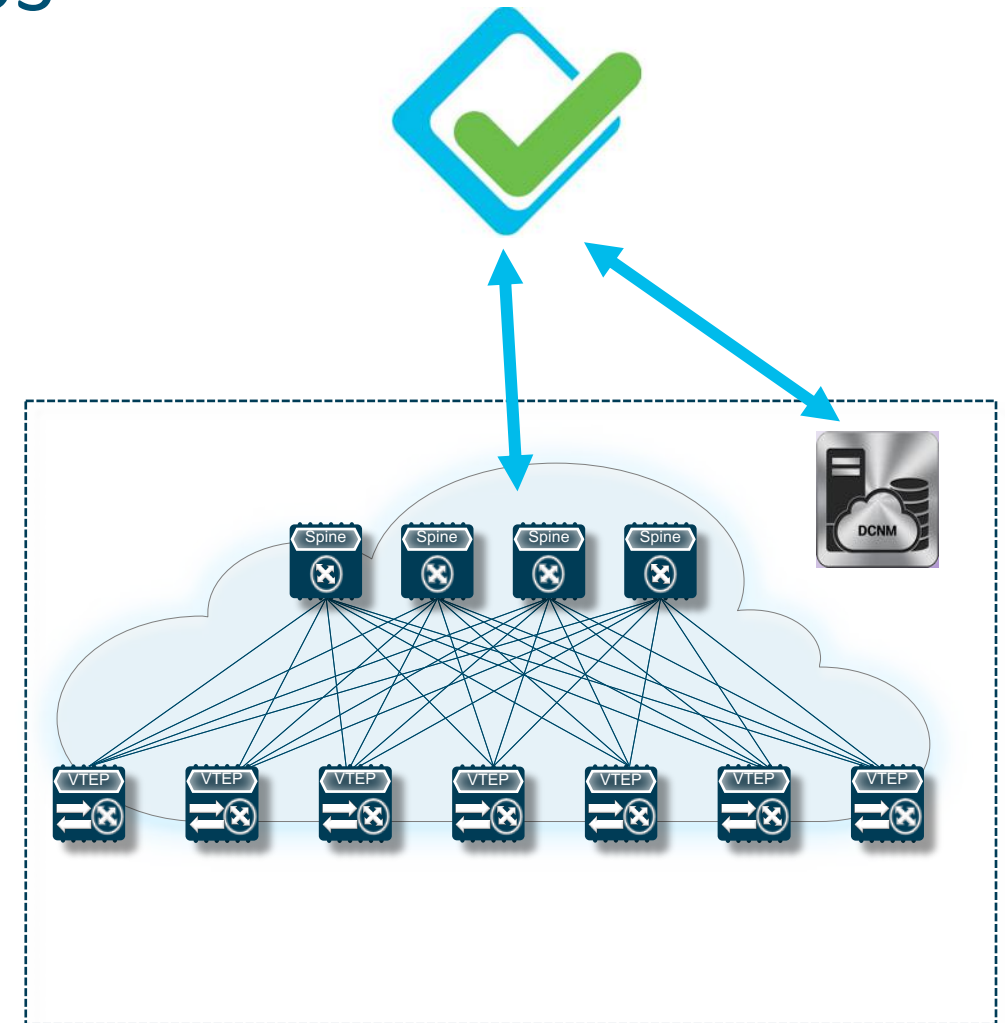
Контроль того, что сеть реализует намерения, и
информация о том, что не так, где, почему, на что
влияет и как устранить

5000+ сценариев проблем и ошибок

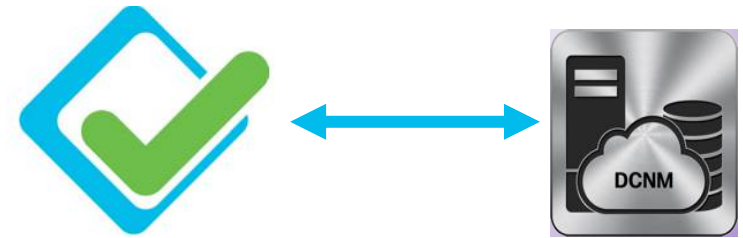
От устранения проблем к проактивной эксплуатации – непрерывно, в масштабах всей сети

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



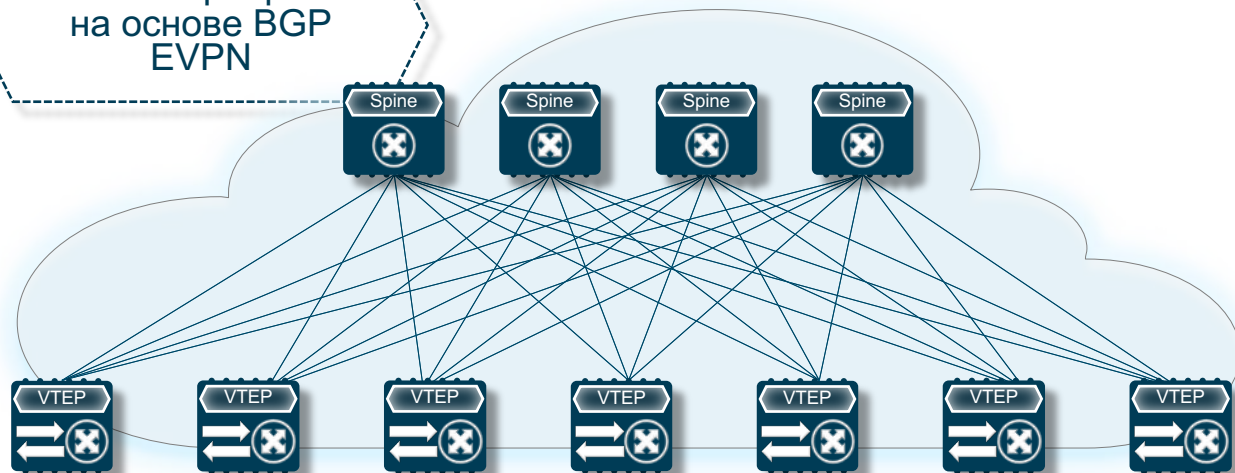
Замечание относительно DCNM



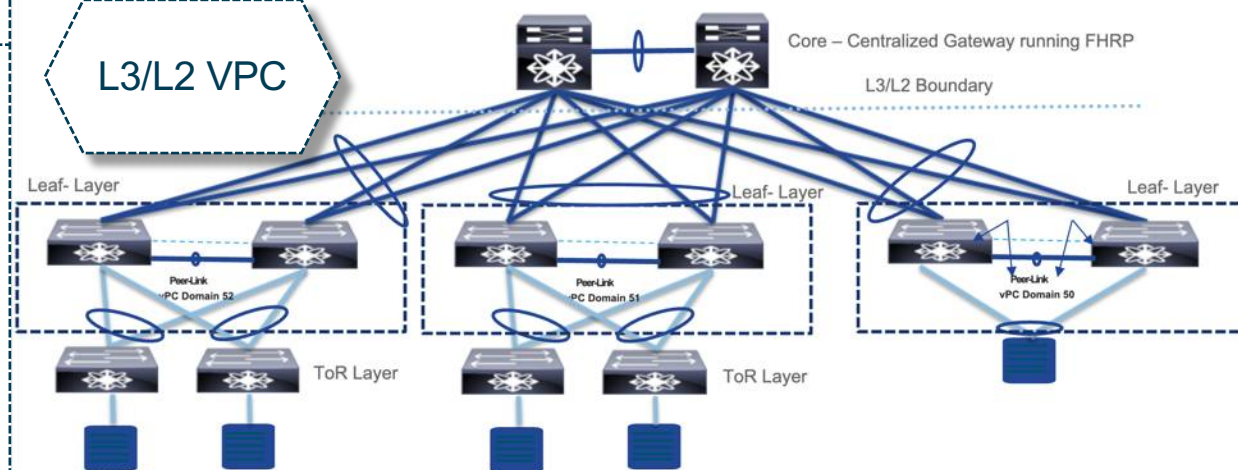
- Версия NAE 5.x требуется DCNM для получения информации о топологии
- Информация о желаемом состоянии оборудования, которая получается от DCNM ограничена
- Интеграция с DCNM поддерживается в 2-х режимах
 - Managed mode
 - Unmanaged mode
- Источниками событий о неконсистентном состоянии является анализ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

Поддерживаемые топологии в режиме NX-OS

VXLAN фабрика
на основе BGP
EVPN



L3/L2 VPC



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

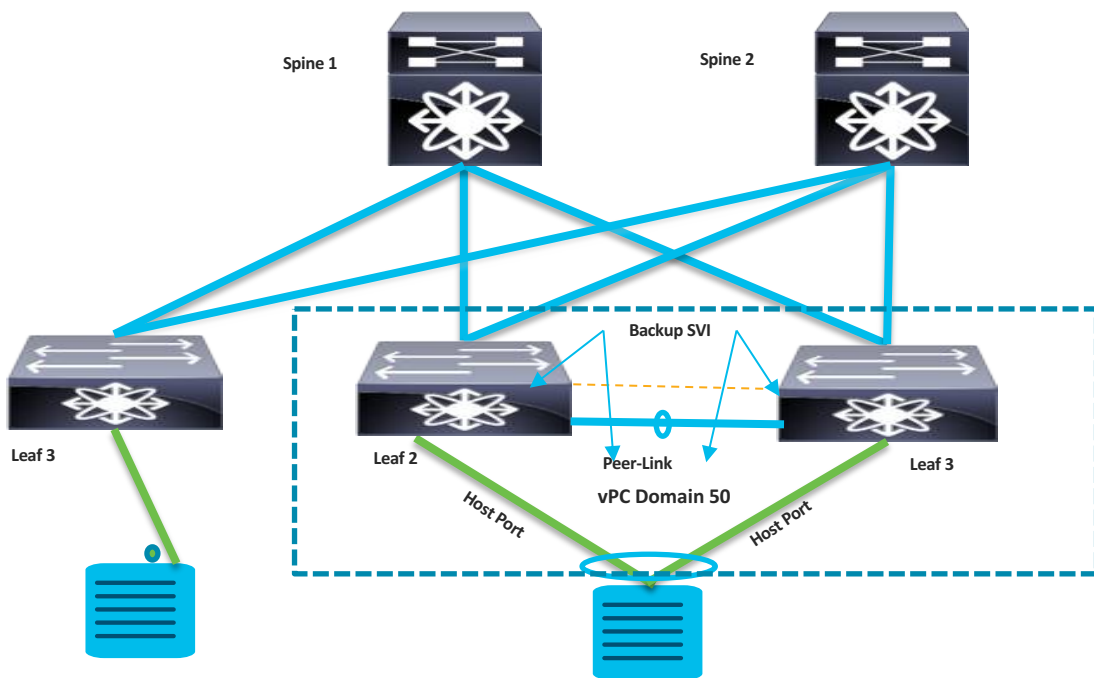
For best VPC convergence result make sure to configure lacp vpc-convergence under port-channel

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

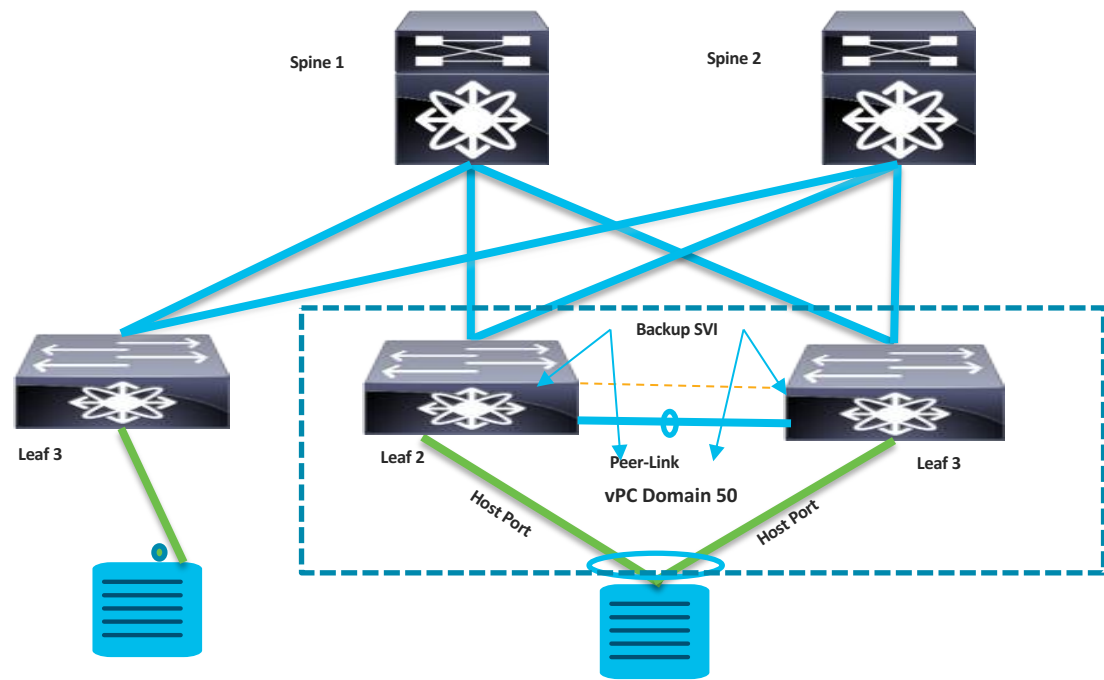
подробности по EVPN далее в этой презентации

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

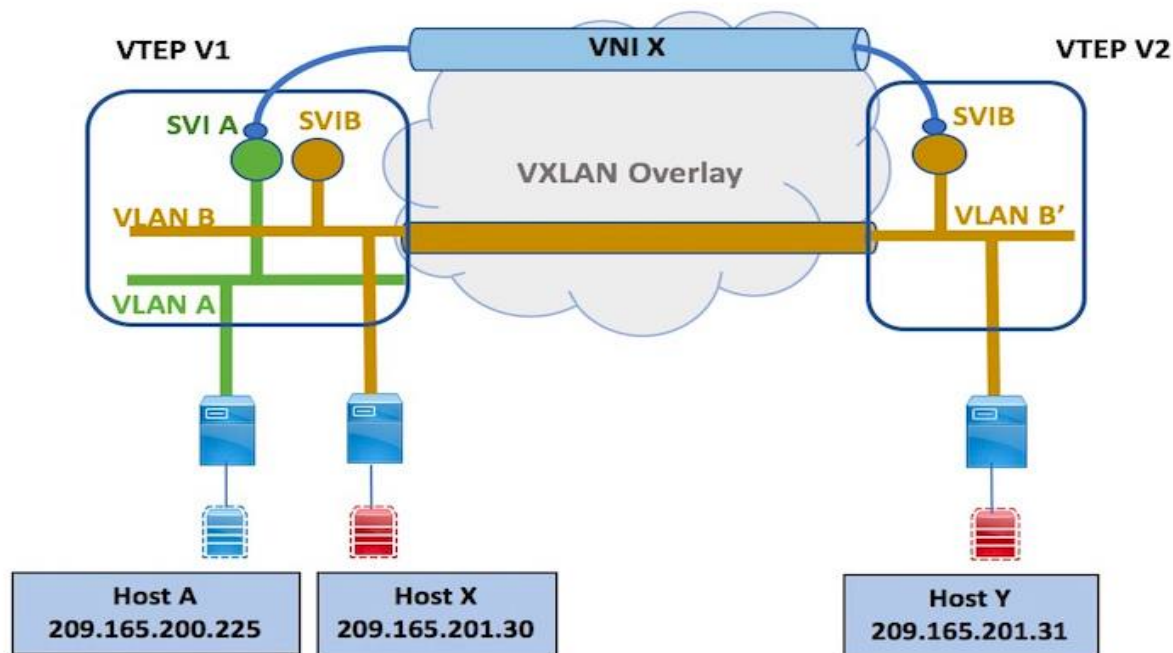


1	VPC_DOMAIN_OR_IP_MISCONFIGURED
2	VPC_DOMAIN_INCONSISTENT
3	VPC_PEER_KEEP_ALIVE_ERROR
4	VPC_PARAMETERS_INCONSISTENT
5	VPC_BACKUP_SVI_INCONSISTENT
6	VPC_BACKUP_VLAN_INCONSISTENT
7	VPC_BACKUP_SVI_ROUTING_ERROR
8	VPC_HOST_PORT_BEST_PRACTICE_CONFIG
9	VPC_ORPHAN_PORT_BEST_PRACTICE_CONFIG
10	VPC_LACP_CONVERGENCE_ERROR
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 <table><tr><th>Check Code</th><th>Failing Condition</th><th colspan="2">Suggested Next Steps</th></tr><tr><td>7015</td><td>The NVE infra VLAN is configured but is not allowed as part of the peer link.</td><td colspan="2"> Ensure that the NVE Infra VLAN is part of the allowed VLAN list on the vPC peer link. Example: <pre>interface port-channel Y peer-switch switchport trunk allowed vlan add <X></pre> Helpful CLI: • show vpc • show interface port-channel Y trunk </td></tr></table> <table><tr><th>Switch Name</th><th>Peer Link</th><th>Allowed VLANs</th><th>Nve Infra VLANs not on Peer Link</th></tr><tr><td>N92160-L1b-S1</td><td>po500</td><td>[1, 11-15, 21, 23-24, 33-34, 77, 88, 99, 2000-2001, 3600]</td><td>-</td></tr></table>			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: <pre>interface port-channel Y peer-switch switchport trunk allowed vlan add <X></pre> 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]	-
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: <pre>interface port-channel Y peer-switch switchport trunk allowed vlan add <X></pre> 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]	-																

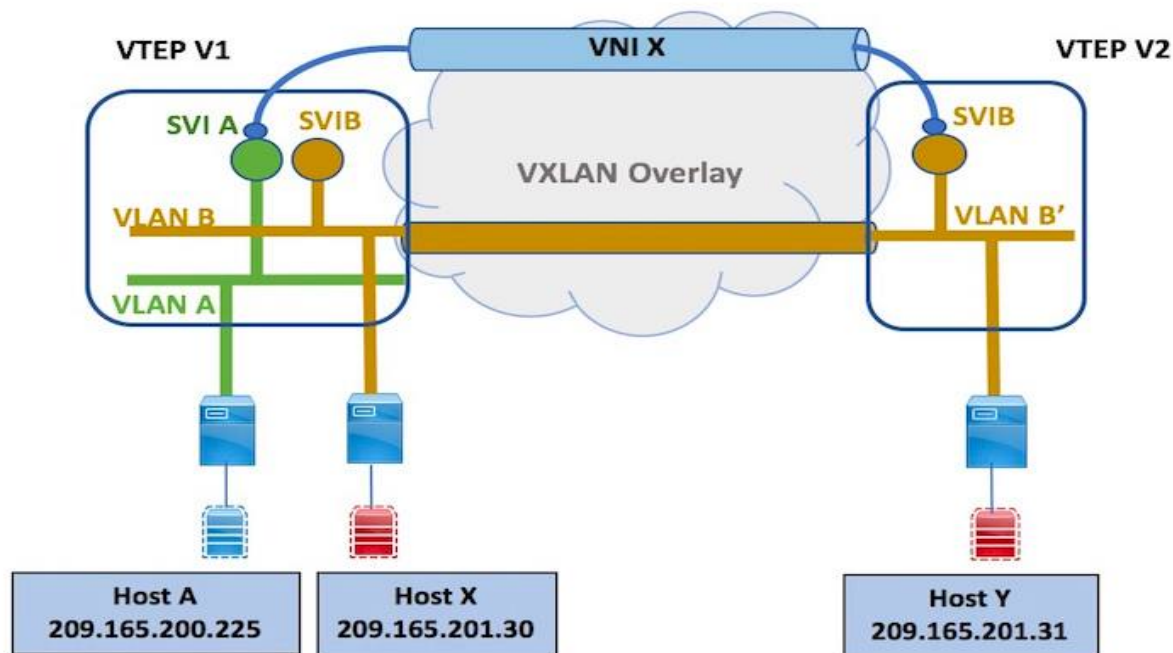
VNI Assurance



Настройка и изменения VNI

- Разные отображения VNI в VLAN на разных коммутаторах
 - Например: replication mode, ingress replication, suppress arp, mcast group IP
- 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 <table><tr><th>Check Code</th><th>Failing Condition</th><th>Suggested Next Steps</th></tr><tr><td>7115</td><td>The L2 VNI is associated with an SVI on some VTEPs but not on others.</td><td>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 </td></tr></table> <table><tr><th>SVI Associated?</th><th>Switch List</th></tr><tr><td>YES</td><td> Switch Name N92160-L1b-S1 N92160-L1a-S1 </td></tr><tr><td>NO</td><td> Switch Name N93180EX-L3-S1 </td></tr></table>			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
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

Preview Config - Switch (10.5.31.206)



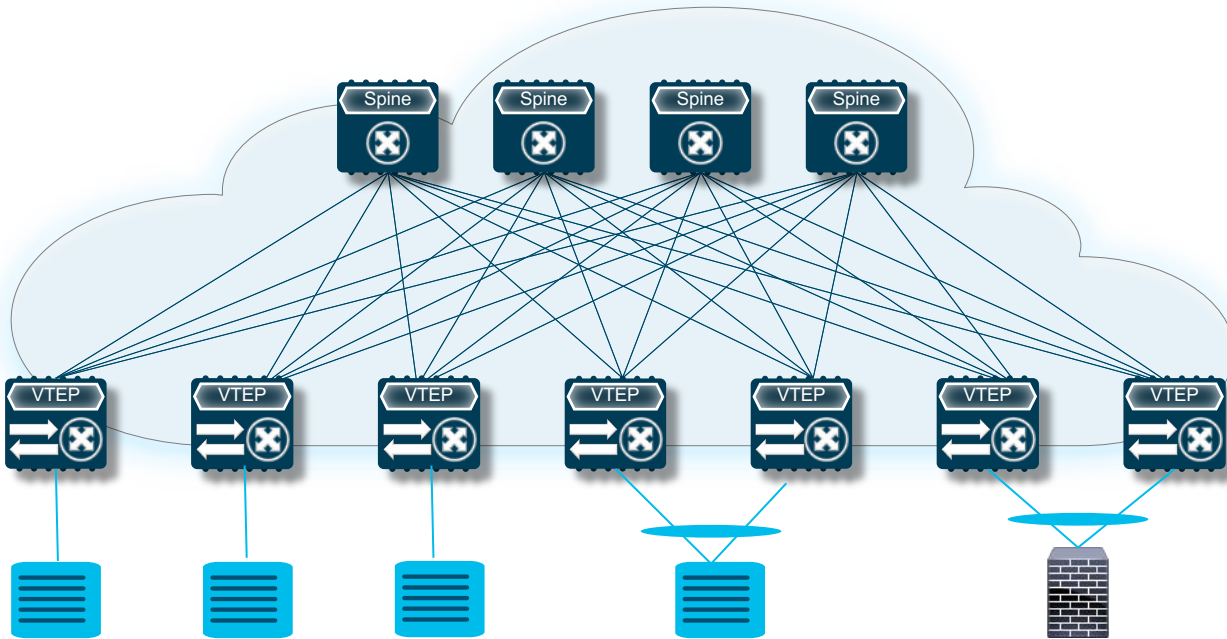
Pending Config

Side-by-side Comparison

To re-compute the *running config*, please click the Re-sync button on the right hand side. Lastly, to resolve unexpected diffs, please review the leading  spaces and edit the appropriate policies to match `show run` output.

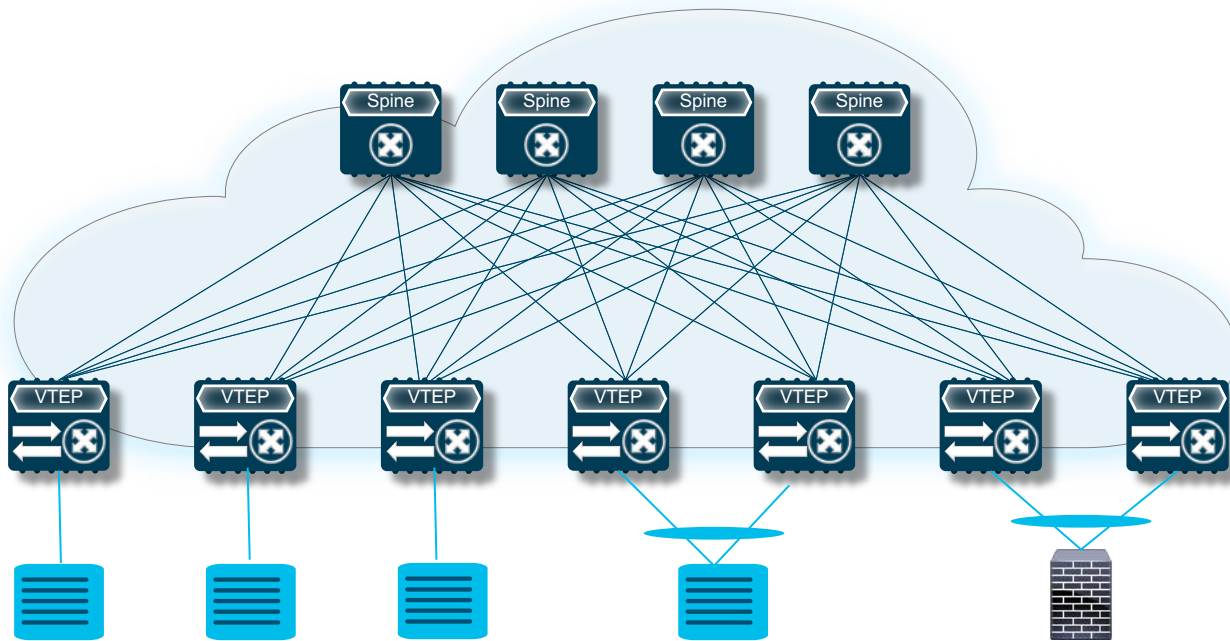
	Running config	Expected config
36	router bgp 65010	router bgp 65010
37	vrf s1_inside	vrf s1_inside
38	address-family ipv4 unicast	address-family ipv4 unicast
39	advertise l2vpn evpn	advertise l2vpn evpn
40	maximum-paths ibgp 2	maximum-paths ibgp 2
41	redistribute direct route-map fabric-rmap-redist-subnet	redistribute direct route-map fabric-rmap-redist-subnet
42	address-family ipv6 unicast	address-family ipv6 unicast
43	advertise l2vpn evpn	advertise l2vpn evpn
44	maximum-paths ibgp 2	maximum-paths ibgp 2
45	redistribute direct route-map fabric-rmap-redist-subnet	redistribute direct route-map fabric-rmap-redist-subnet
46	vlan 2002	vlan 2002
47	vn-segment 52001	vn-segment 51001
48		
49	vrf context s1_inside	vrf context s1_inside
50	address-family ipv4 unicast	address-family ipv4 unicast
51	route-target both auto	route-target both auto
52	route-target both auto evpn	route-target both auto evpn
53	address-family ipv6 unicast	address-family ipv6 unicast
54	route-target both auto	route-target both auto
55	route-target both auto evpn	route-target both auto evpn
56	rd auto	rd auto
57	vni 51001	vni 51001
58	configure terminal	configure terminal
59	copp profile strict	copp profile strict
60	fabric forwarding anycast-gateway-mac 2020.0000.00aa	fabric forwarding anycast-gateway-mac 2020.0000.00aa
61	feature analytics	feature analytics
62	feature bgp	feature bgp
63	feature dhcp	feature dhcp
64		feature icam

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



?

228



10

238

Category						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

?

0 / 3

0 / 10

0 1 7

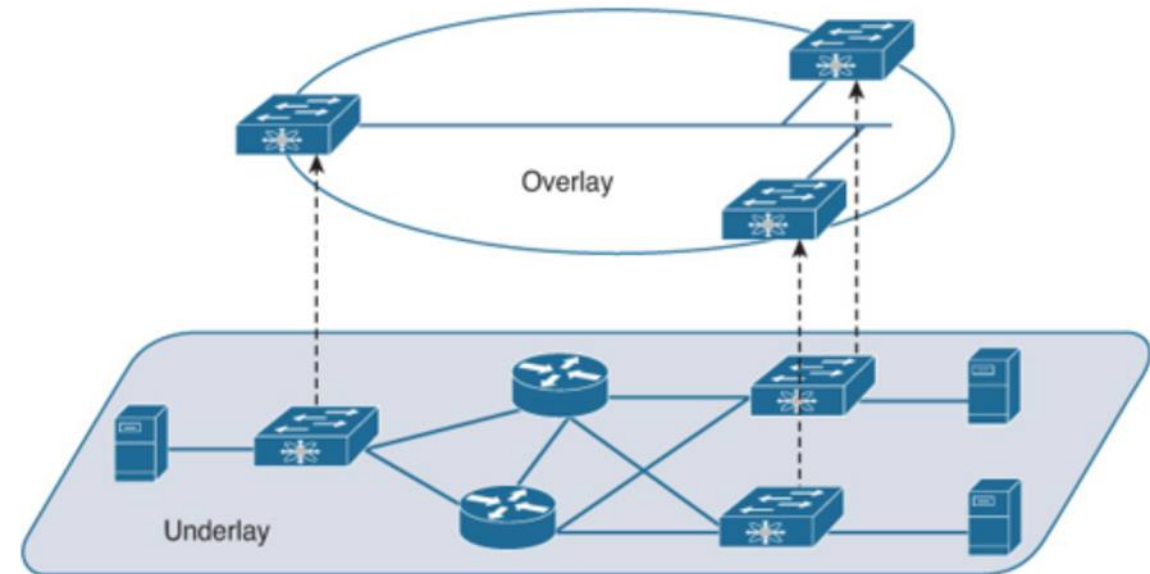
2 / 2

270 / 367

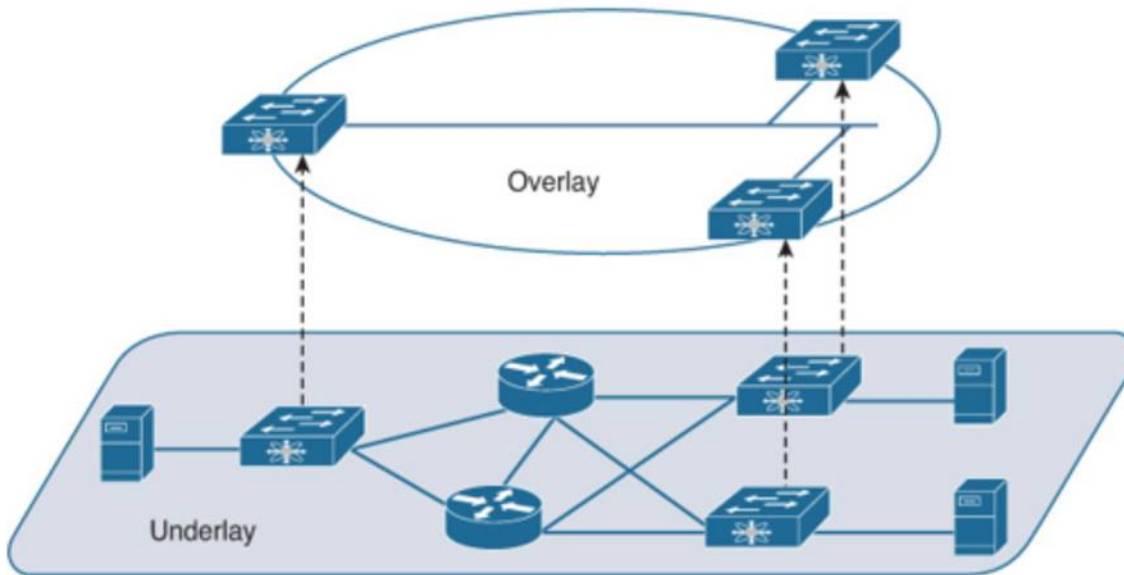
0 / 4

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: • <code>show running bgp section evpn</code> • <code>show system internal dme running-config all dn sys/evpn</code>
	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

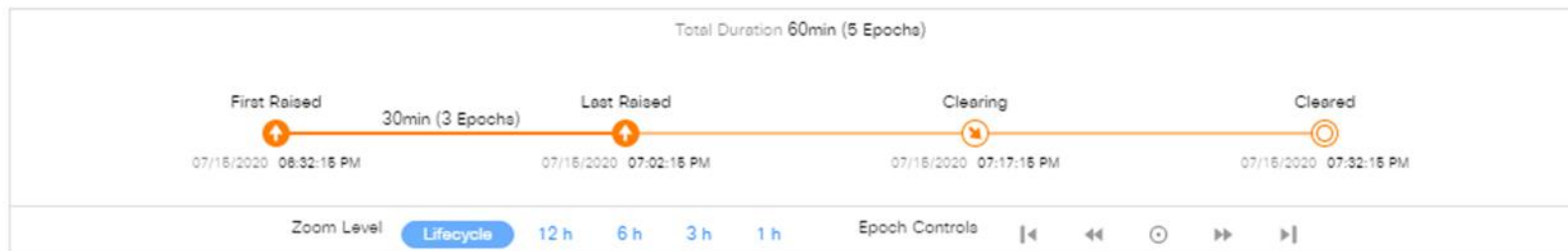
Жизненный цикл для Smart Event

Smart Events of VPC_BACKUP_SVI_ROUTING_ERROR

Severity ▲ Major Event Category CHANGE_ANALYSIS Event Subcategory VPC
Event Description vPC backup SVI routing error

1 rows |  | 

Epochs	Leafs	VPC	Event ID
	Filter	Filter	Filter
07/15/2020 06:32 PM PDT	N92160-L1b-S1	1	0a81f06d6c458a8fdd854656b001d271



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

Q What EPs are associated with |

What EPs are associated with any

What EPs are associated with any ?

What EPs are associated with EP:

What EPs are associated with INF:

What EPs are associated with LEAF:

What EPs are associated with VLAN:

What EPs are associated with VRF:

Пример запроса

Какие хосты внутри EVPN-фабрики подключены к VLAN?

Epoch on Monday, July 13, 2020 5:23 PM

Explorer allows network operators to discover assets and their object associations in an easy-to-consume natural language query format. In the search bar, enter a What query.

Q What EPs are associated with VLAN:vlan15

What EPs are associated with VLAN:vlan15
Last queried on Monday, July 13, 2020 5:25 PM

What EPs are associated with VLAN:vlan15?

What EPs are associated with VLAN:vlan15 and

What EPs are associated with VLAN:vlan15 or

Reset

Query Results

2 rows

Object Name	Interfaces	VLANs	EPs	VRFs	Leafs
Filter					
192.161.15.11	2	1	1	1	2
192.161.15.12	2	1	1	1	2

Пример запроса

Какие хосты внутри EVPN-фабрики подключены к VRF?

Q What EPs are associated with VRF:blue

✕

Reset

Query Results

10 rows

Object Name	Interfaces	VLANs	EPs	VRFs	Leafs
Filter					
192.161.13.11	2	1	1	1	2
192.161.13.21	1	1	1	1	1
192.161.14.11	2	1	1	1	2
192.161.14.12	2	1	1	1	2

Анализ изменений

Анализ изменений между «эпохами»



Cisco Network Assurance Engine

Dashboard

Epoch Analysis ▼

Change Management ▼



01:29 AM
05/17/2018



Before /
Baseline

After / Current

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

Delta Analysis

MW1

Earlier Epoch: 07/15/2020 6:32:15 PM PDT

Later Epoch: 07/16/2020 12:17:15 PM PDT

Time Range: 17 h 45 min

Health Delta

Policy Delta

Smart Event Count



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

06 / 09 / 2020 06:33 PM PDT

06 / 10 / 2020 04:08 PM PDT

L2 VNI DN = vni-10020

Search

- Check Code
- Check Status
- Event Code
- Interface
- IP
- L2 VNI
- L3 VNI
- Leaf
- MAC
- Event Name

System Policy Analysis Forwarding

09 PM Wed 10 03 AM 12 PM 03 PM JUN 09 6:33 PM PDT

All Sn

Aggregated (1) Individual

1 rows

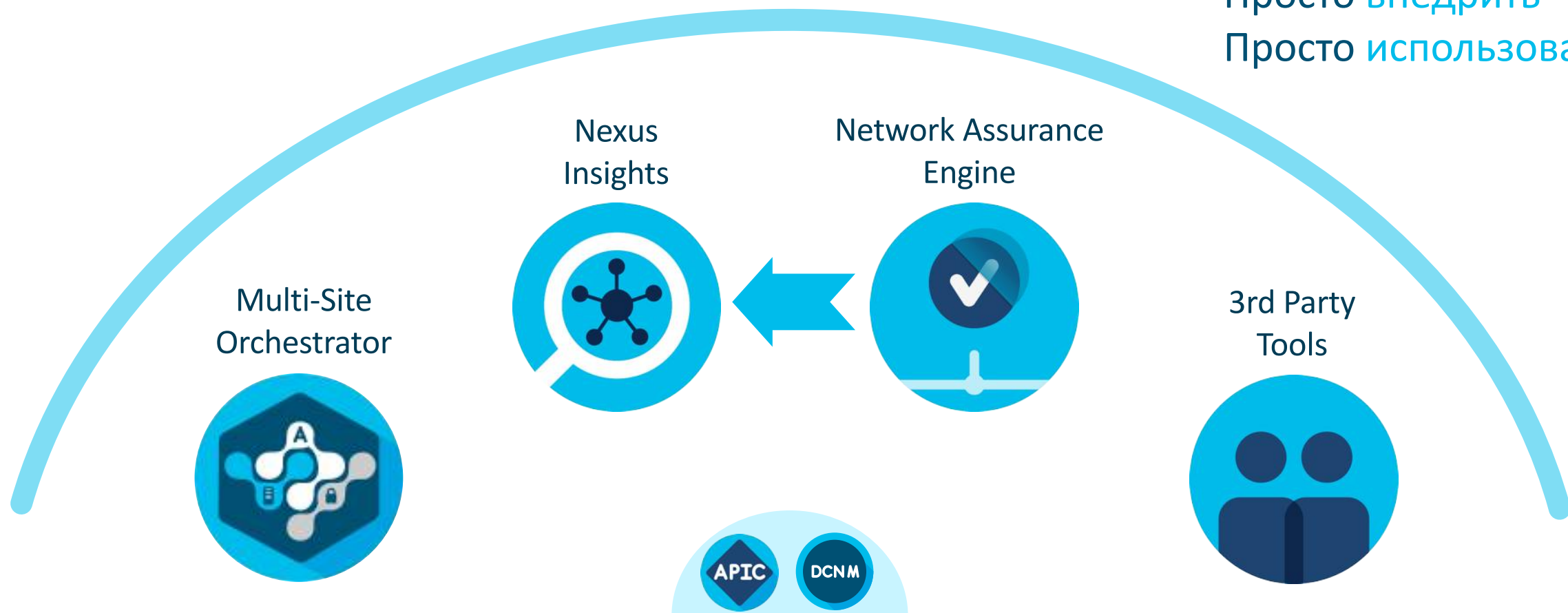
Severity ▼ 1	Event Category	Event Subcategory	Event Name ▲ 2	Count	Event Description
Filter ▼	Filter ▼	Filter	Filter	Filter	
CRITICAL	CHANGE_ANALYSIS	OVERLAY	L2_VNI_INCONSISTENT_CONFIG	1	A fabric-wide check has found inconsistent configuration on L2 VNI.

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



Sites

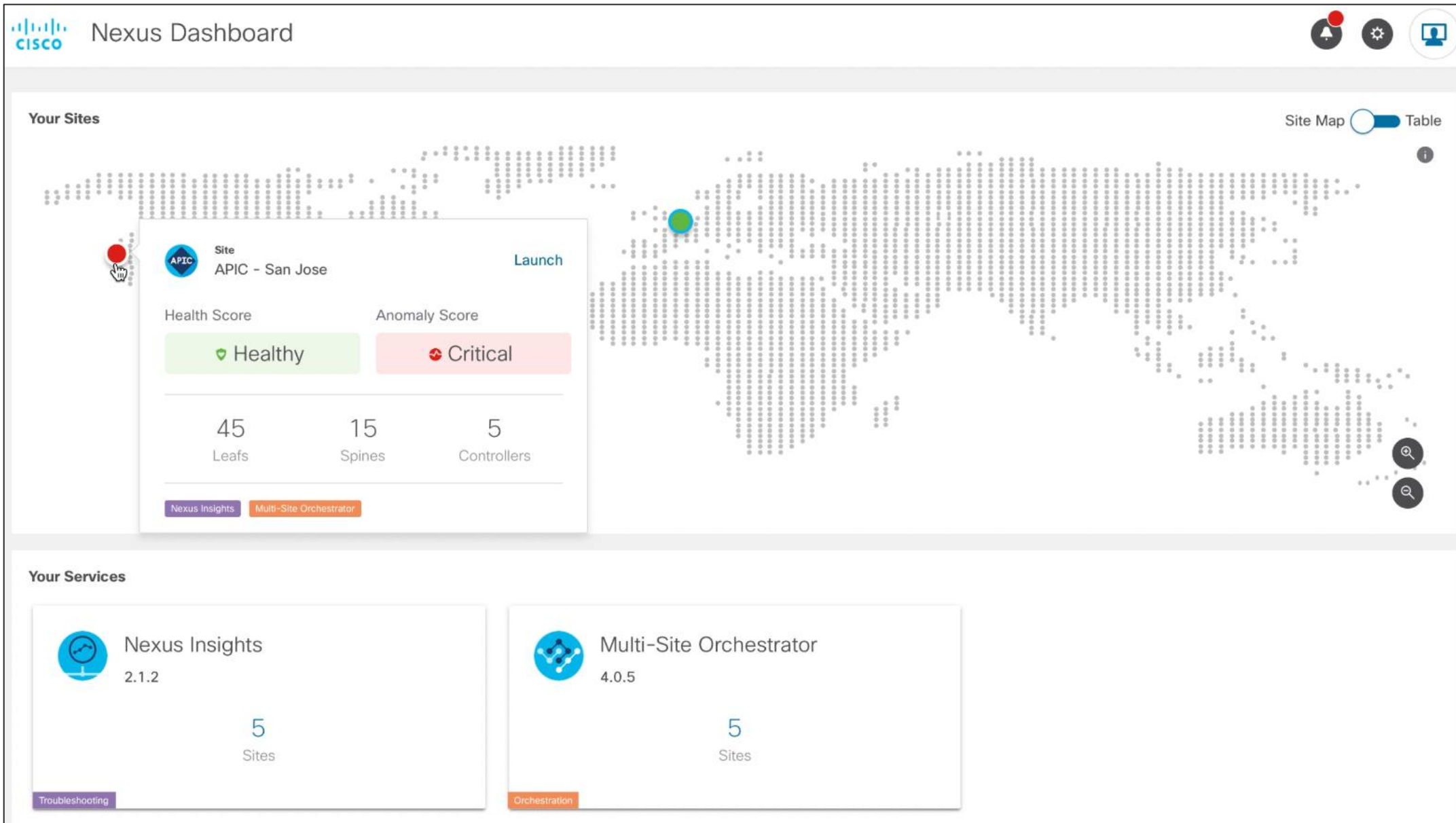
Add Site

Filter by attributes

☐	Health Score ▾	Name	Connectivity Status ▾	Anomaly Score ▾	Advisories ▾	Services Used ▾	
☐	Healthy	 APIC - San Jose	 Up	 N/A	N/A	Multi-Site Orchestrator	Launch
☐	Healthy	 APIC - Dallas	 Up	 N/A	N/A	Multi-Site Orchestrator	Launch
☐	Healthy	 APIC - Miami	 Up	 N/A	N/A	Multi-Site Orchestrator	Launch
☐	Healthy	 DCNM - New York	 Up	 N/A	N/A	Multi-Site Orchestrator	Launch
☐	Healthy	 Cloud APIC - London	 Up	 N/A	N/A	Multi-Site Orchestrator	Launch

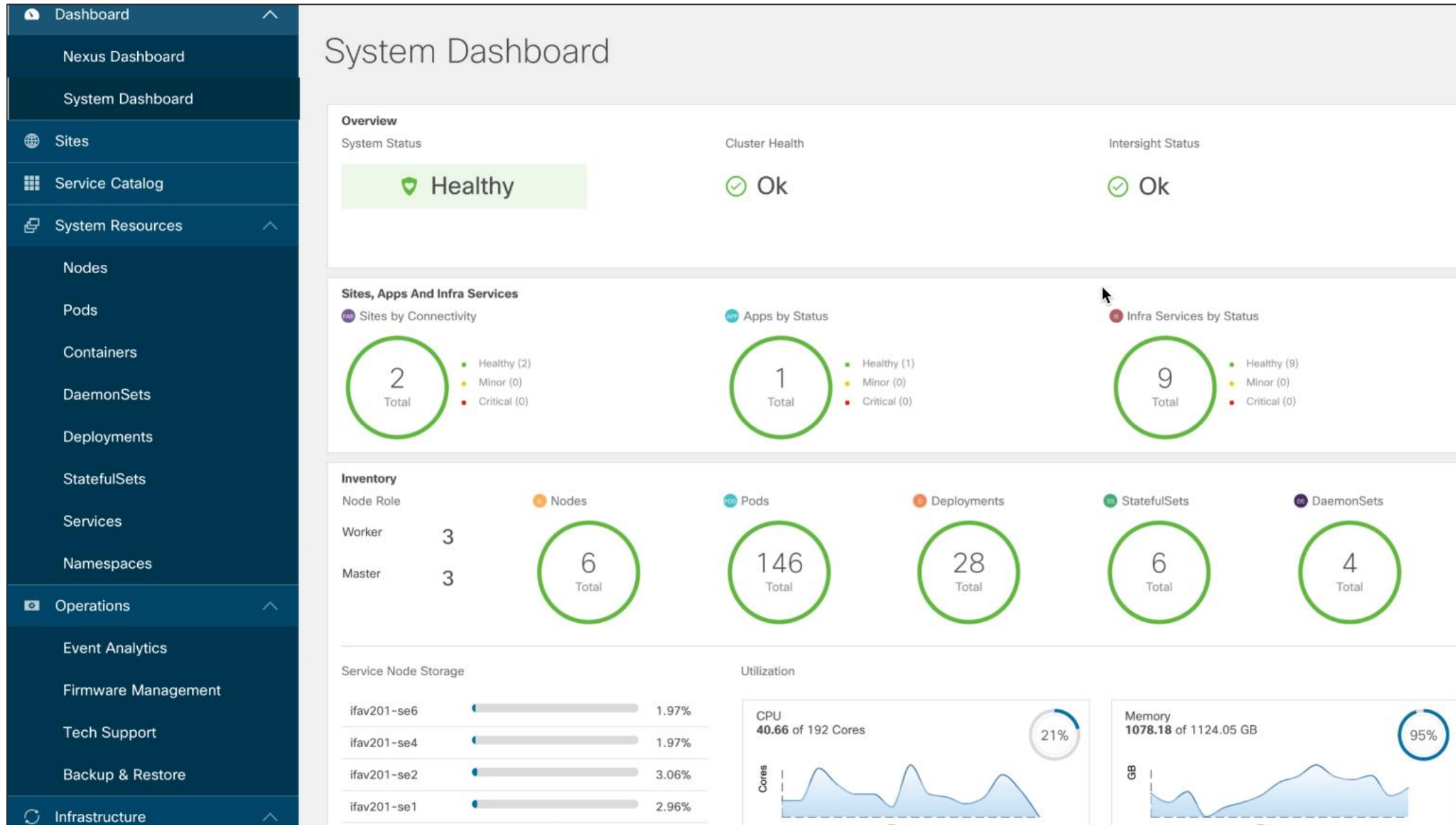
Nexus Dashboard

Эксплуатация многих сайтов



Nexus Dashboard

Администрирование платформы



Nexus Dashboard

Размещение приложений

 Nexus Dashboard

Service Catalog

Services App Store

Filter by attributes



Nexus Insights

Cisco Systems, Inc.

Nexus Insights is a platform for all dat...

2.1.2

2 / 2

6 / 6

Pods

Containers

Open



Multi-Site Orchestrator

Cisco

ACI Multi-Site Orchestrator is respo...

4.0.5

2 / 2

6 / 6

Pods

Containers

Open

Service

Nexus Insights

...

CRITICAL

MAJOR

MINOR

WARNING

0

0

0

0

General

Status

Running

Vendor

Cisco Systems, Inc.

Description

Nexus Insights is a platform for predictive analytics, correlation and alerting using streaming telemetry data for networking fabrics.

System Resources

6

Containers

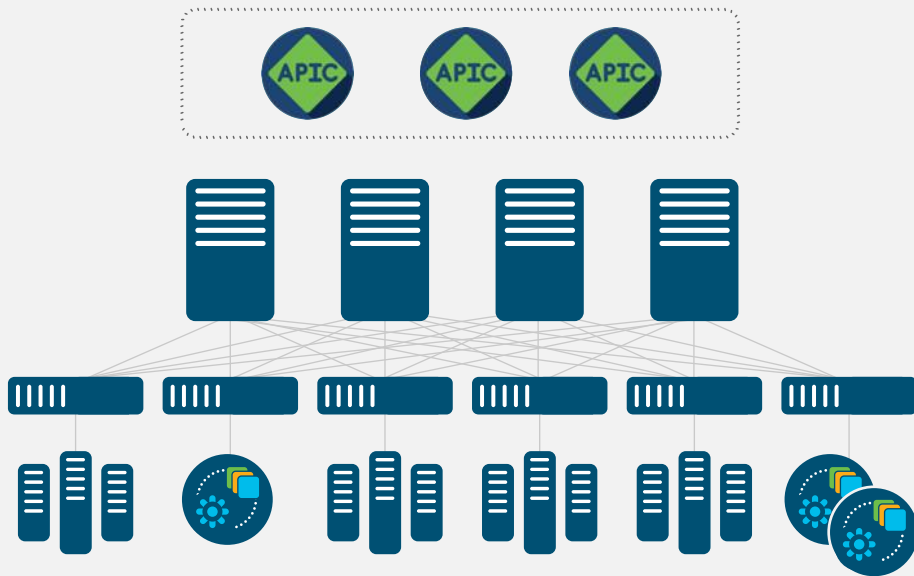
2

Pods

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

Платформа Cisco Nexus Dashboard Platform

Современный масштабируемый стек для размещения приложений для эксплуатации сети ЦОД



Nexus
Insights



Network
Assurance
Engine



3rd Party
apps



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

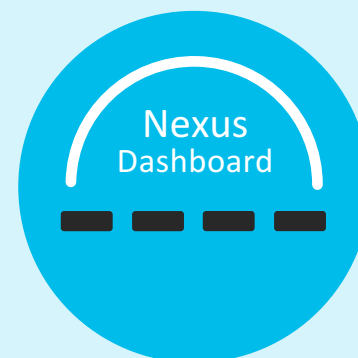
High Availability

Разверните Nexus Dashboard там, где вам удобно!

Appliance

Virtual Appliance*

Cloud Hosted*



Nexus Insights

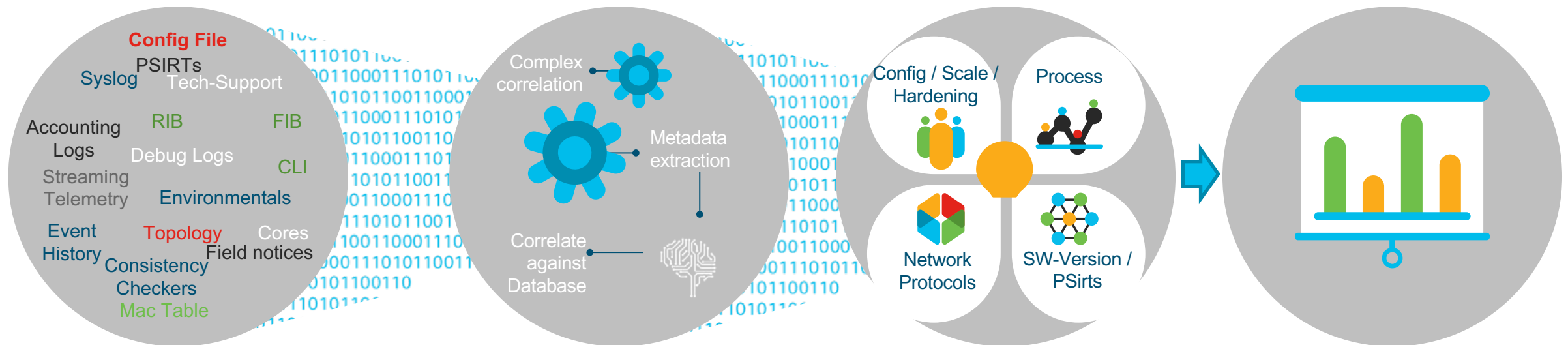
Nexus Insights – проактивная эксплуатация на основе телеметрии

Источники
телеметрии

Сбор и обработка

Сделать выводы

Рекомендованные
действия

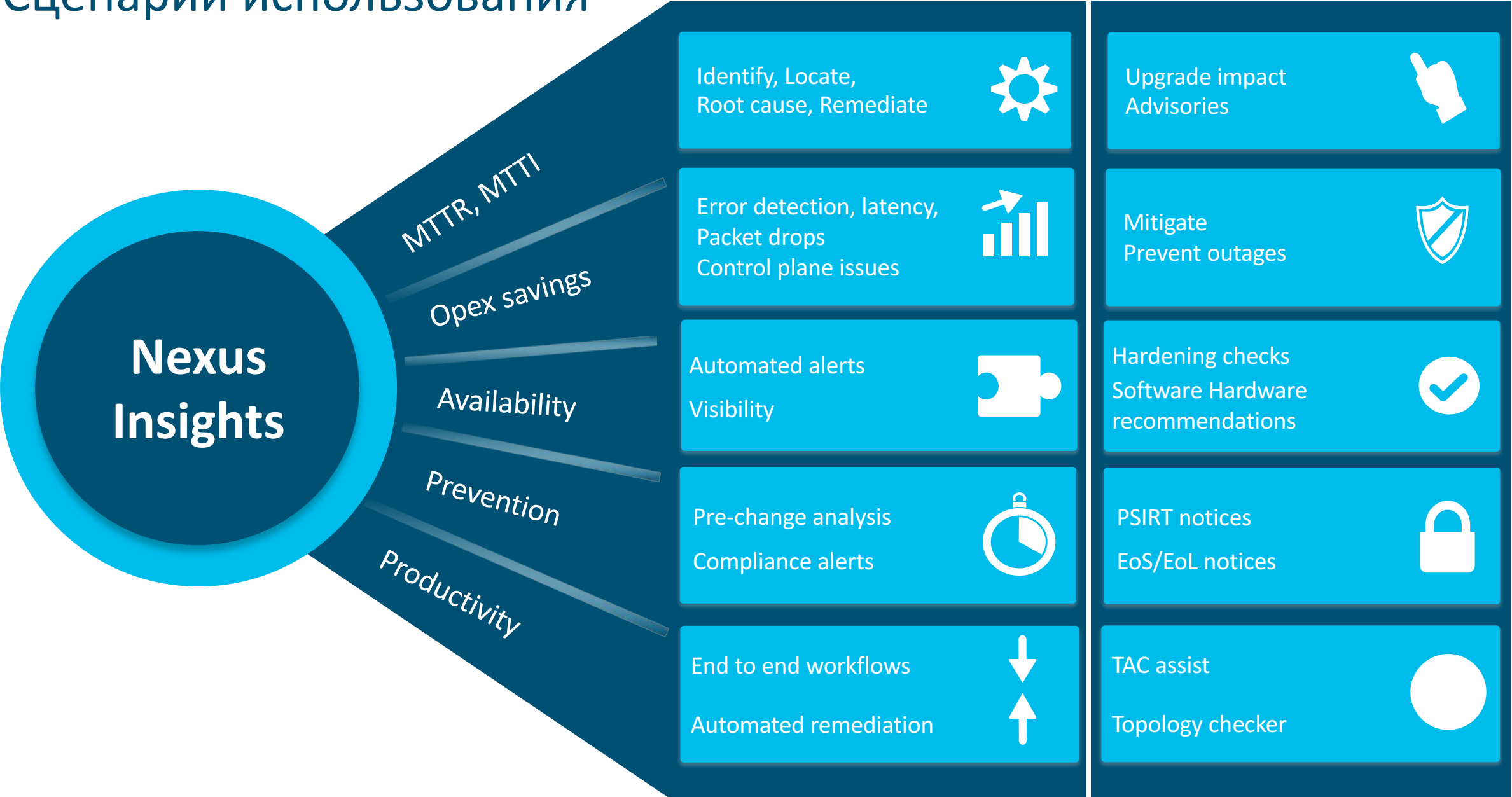


Повысить доступность и производительность

ACI | NX-OS

Nexus Insights

Сценарии использования



Какие данные получает Nexus Insights?

Программная телеметрия

Даёт видимость в:

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

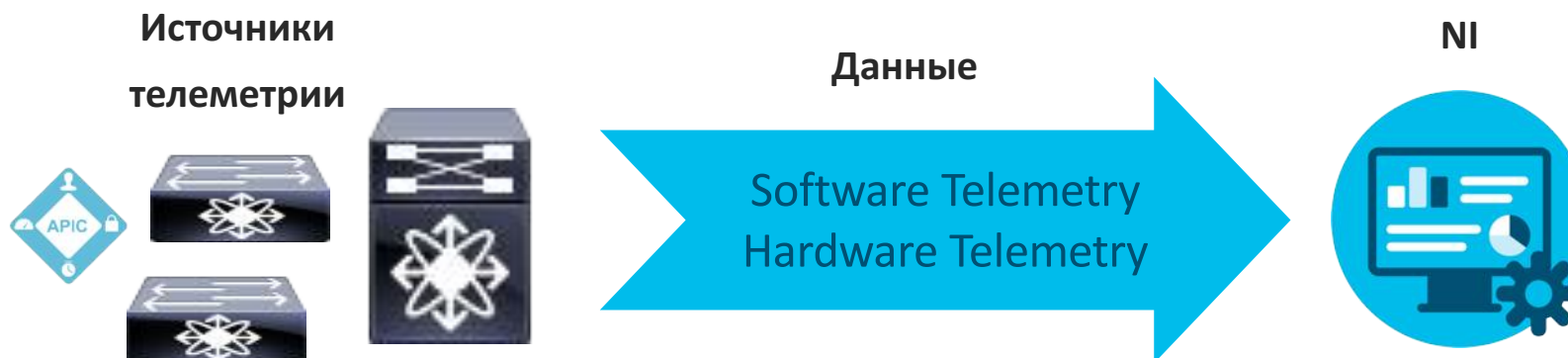
Общая для
Nexus

Аппаратная телеметрия

Даёт видимость в :

- Информацию о потоках данных
- Путь потоков
- События потоков

Зависит от
аппаратуры



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)

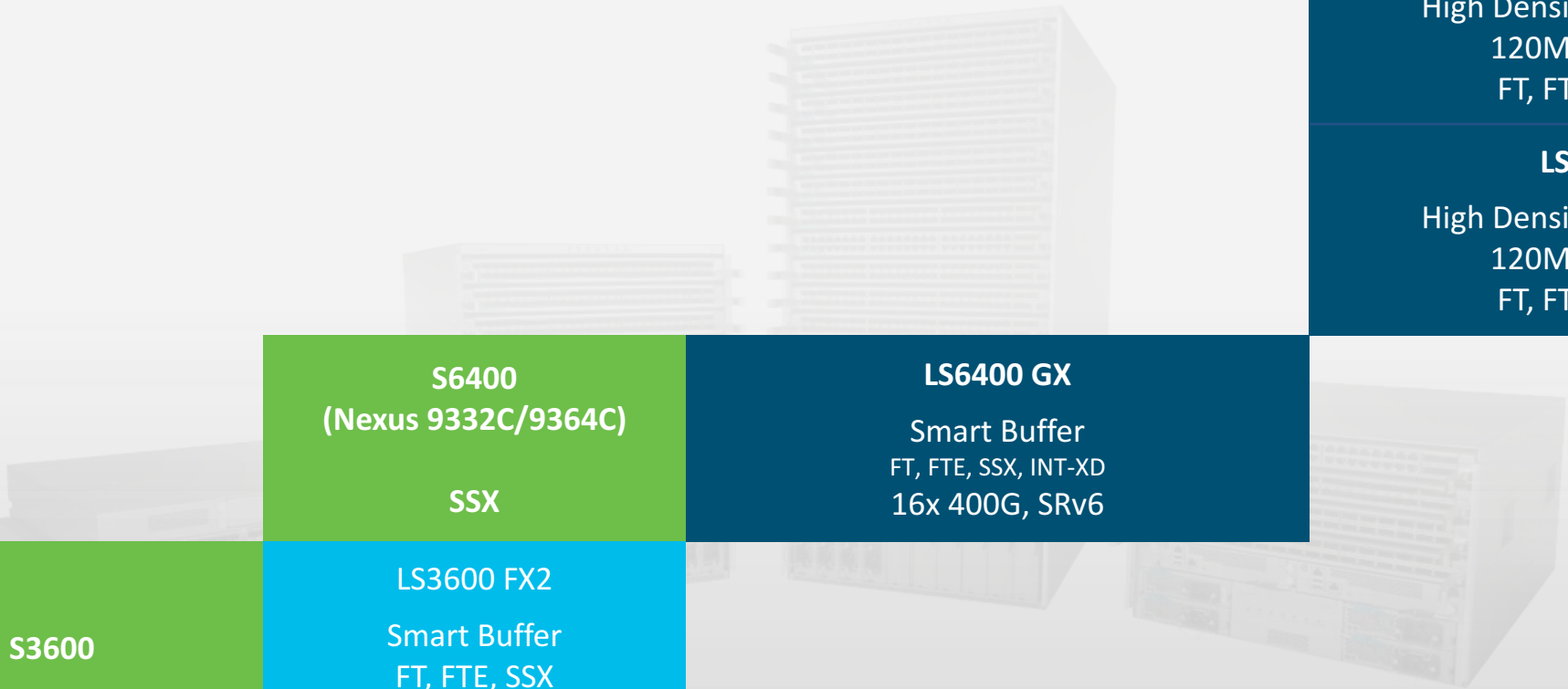
Data-Plane Flow Data

Streaming Statistics Export (SSX)

Потоковая передача статистики с чипа на основе заданных настроек

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

Какая еще информация используется Nexus Insights кроме телеметрии?

Сеть

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

On-prem

Cisco

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

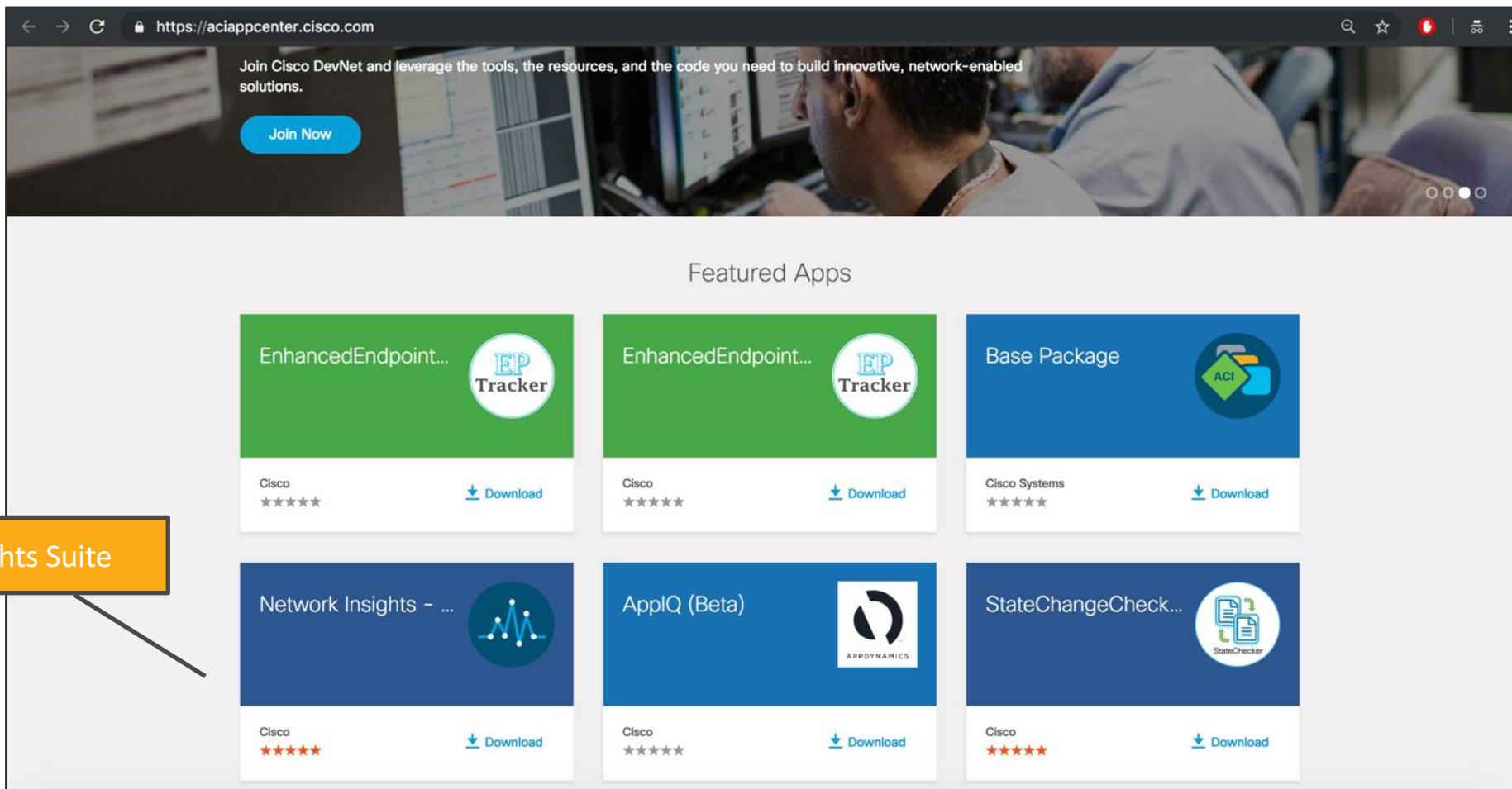
Pulled from the Cloud



Nexus Insights: загрузка из Cisco App Store

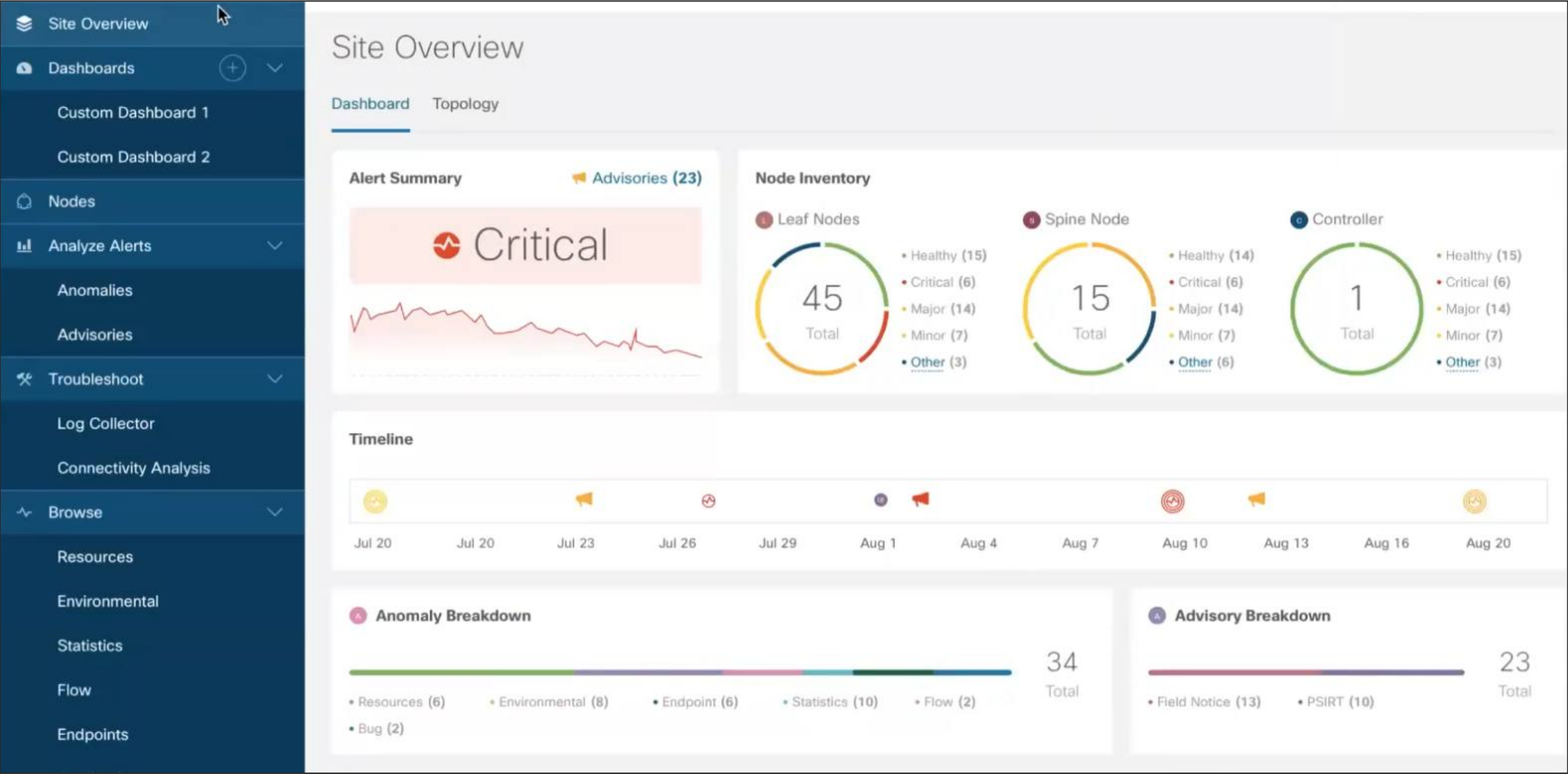
Общий «магазин приложений» для ACI and NXOS - <https://dcappcenter.cisco.com/>

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



Nexus Insights

Обзор информации сайта



Nexus Insights

Список аномалий и их детали

Custom Dashboard 1

Custom Dashboard 2

Nodes

Analyze Alerts

Anomalies

Advisories

Troubleshoot

Log Collector

Connectivity Analysis

Browse

Resources

Environmental

Statistics

Flow

Endpoints

Applications

Events

Dashboard

Topology

Alert Summary

Critical

Timeline

Anomaly Breakdown

Resources (6)

Environmental (0)

Bug (2)

Top Nodes by Anomaly Score

ifav22-leaf4

Search

21.0.0.11, 22.0.0.14

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf2, candid5-leaf31

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf3, candid5-leaf44

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf4, candid5-leaf5

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf5, candid5-leaf16

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf6, candid5-leaf7

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf7, candid5-leaf8

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

candid5-leaf8, candid5-leaf9

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

Anomaly

21.0.0.11, 22.0.0.14

Analyze

General Information

Severity

Critical

Status

Active

Category

Flows

Type

Flow

Description

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

Affected Object

21.0.0.11, 22.0.0.14

Nodes

candid5-leaf1

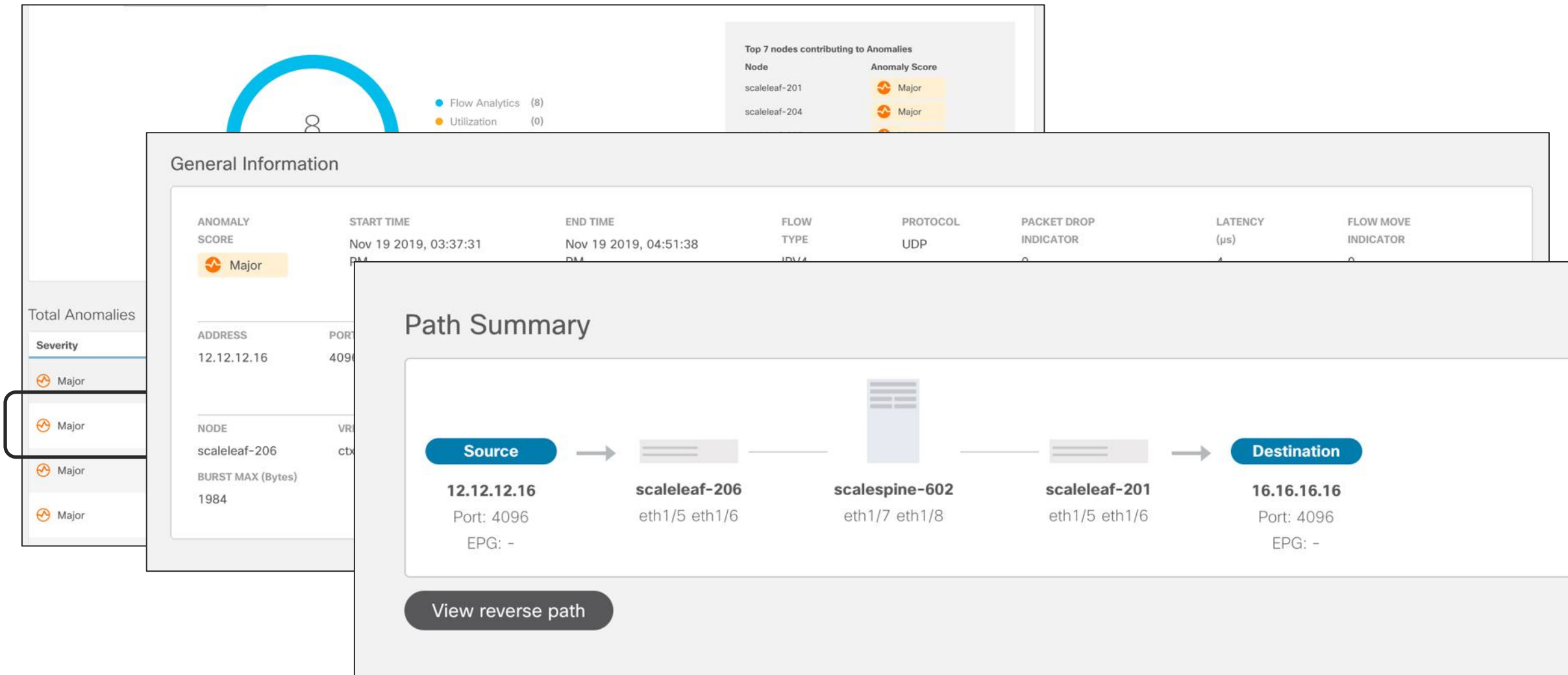
Detection Time

July 13, 2020, 10:25:30 AM

Last Seen Time

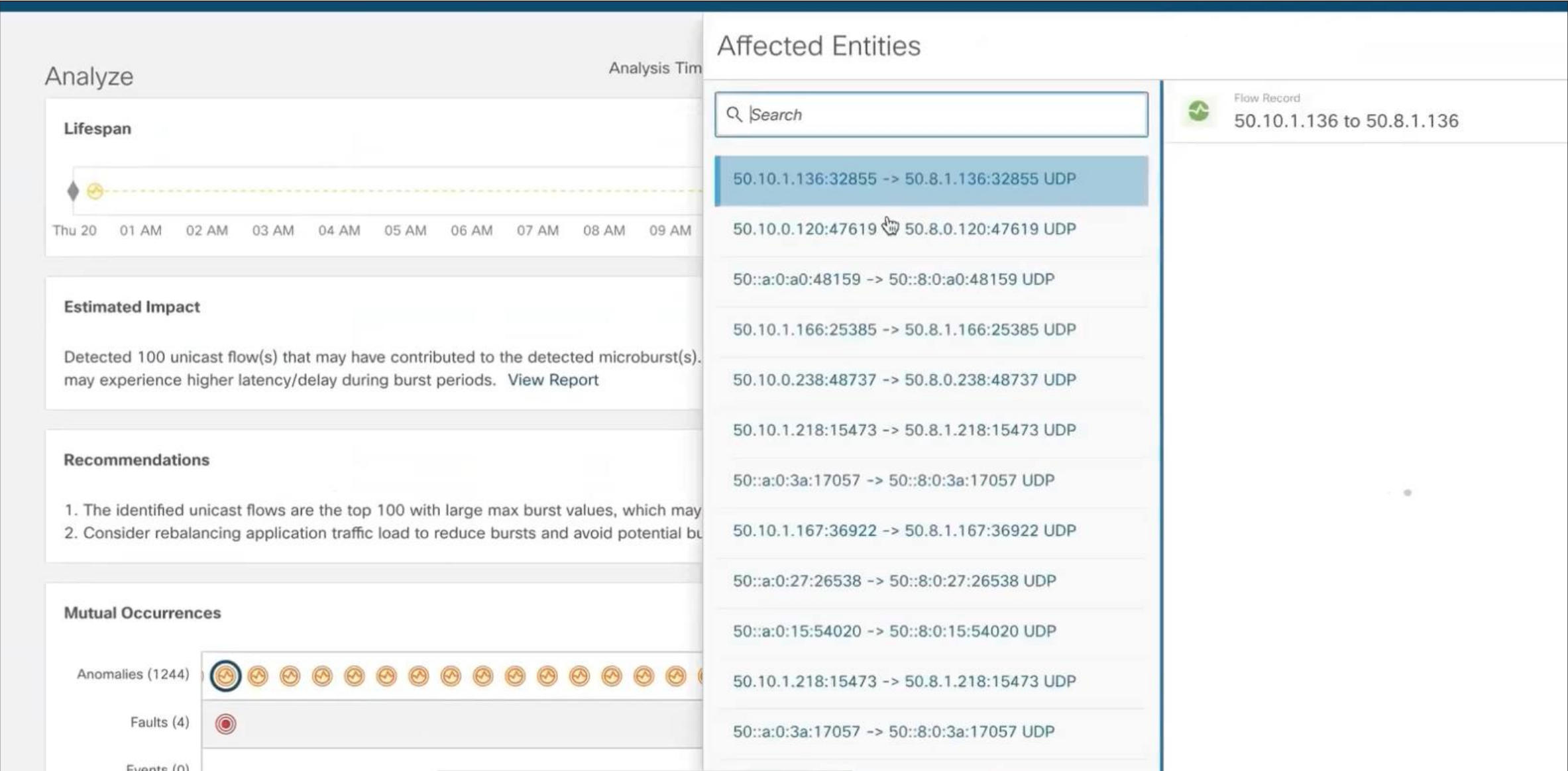
July 13, 2020, 10:25:30 AM

Проблема производительности?



Nexus Insights

Анализ микровсплесков (microbursts)



Microburst

50.10.1.136 to 50.8.1.136

Поддержка FTE телеметрии в NI 5.0

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

Новый тип ресурса для FTE – 'FlowEvent'

Можно получить более детальный анализ

'View Report' показывает затронутые потоки

The screenshot displays the Cisco NIS interface for FTE analysis. On the left, a list of 20 total anomalies is shown, all categorized as 'Major' and detected on Oct 24, 2020. The main panel shows a detailed view of an anomaly named 'scaleleaf-203'. This view includes a timeline, a 'View Report' button, and a section titled 'Affected Entities' which lists the specific flows impacted by the anomaly. The 'Affected Entities' section shows a search bar and a list of flows, including one from 12.12.12.8 to 16.16.16.48 on TCP port 4096.

Severity	Detection Time
Major	Oct 24 2020 01:36:47.000 AM
Major	Oct 24 2020 01:37:58.901 AM
Major	Oct 24 2020 01:36:47.000 AM
Major	Oct 24 2020 01:37:58.610 AM
Major	Oct 24 2020 01:36:47.000 AM
Major	Oct 24 2020 01:37:58.534 AM

20 Total Anomalies

Anomaly Details

General Information

SEVERITY

Major

Affected Entities

Search

12.12.12.8 to 16.16.16.48

General Information

RECORD TIME

Oct 24 2020, 01:37:58.918 AM

PACKET DROP

FLOW TYPE

IPv4

PROTOCOL

TCP

NODE

scaleleaf-209

Source

ADDRESS

12.12.12.8

PORT

4096

Ingress

TENANT

SRF

EPG

EPG12

INTERFACE

eth1/12

Destination

ADDRESS

16.16.16.48

PORT

4096

ctx1

EPG

EPG14

Nexus Insights

Анализ аномалии

Analyze

Analysis Time-Range: 20 minutes

before and after

Lifespan



By correlating the anomalies, we found the root cause of this issue to be: An incorrect contract scope configuration is preventing communication between the Provider and the Consumer EPGs.

Estimated Impact

- 20 Endpoints associated to the EPG are affected
- 3 Applications experiencing connectivity issues

Timeline

☐ View only correlated items



Anomaly Details

General Information

Severity

Critical

Status

Active

Category

Flows

Type

Flow

Description

For flow from 21.0.0.11 to 22.0.0.14, packet drop is detected due to forward drop.

Affected Object

21.0.0.11, 22.0.0.14

Node

candid5-leaf1

Detection Time

July 13, 2019, 10:25:30 AM

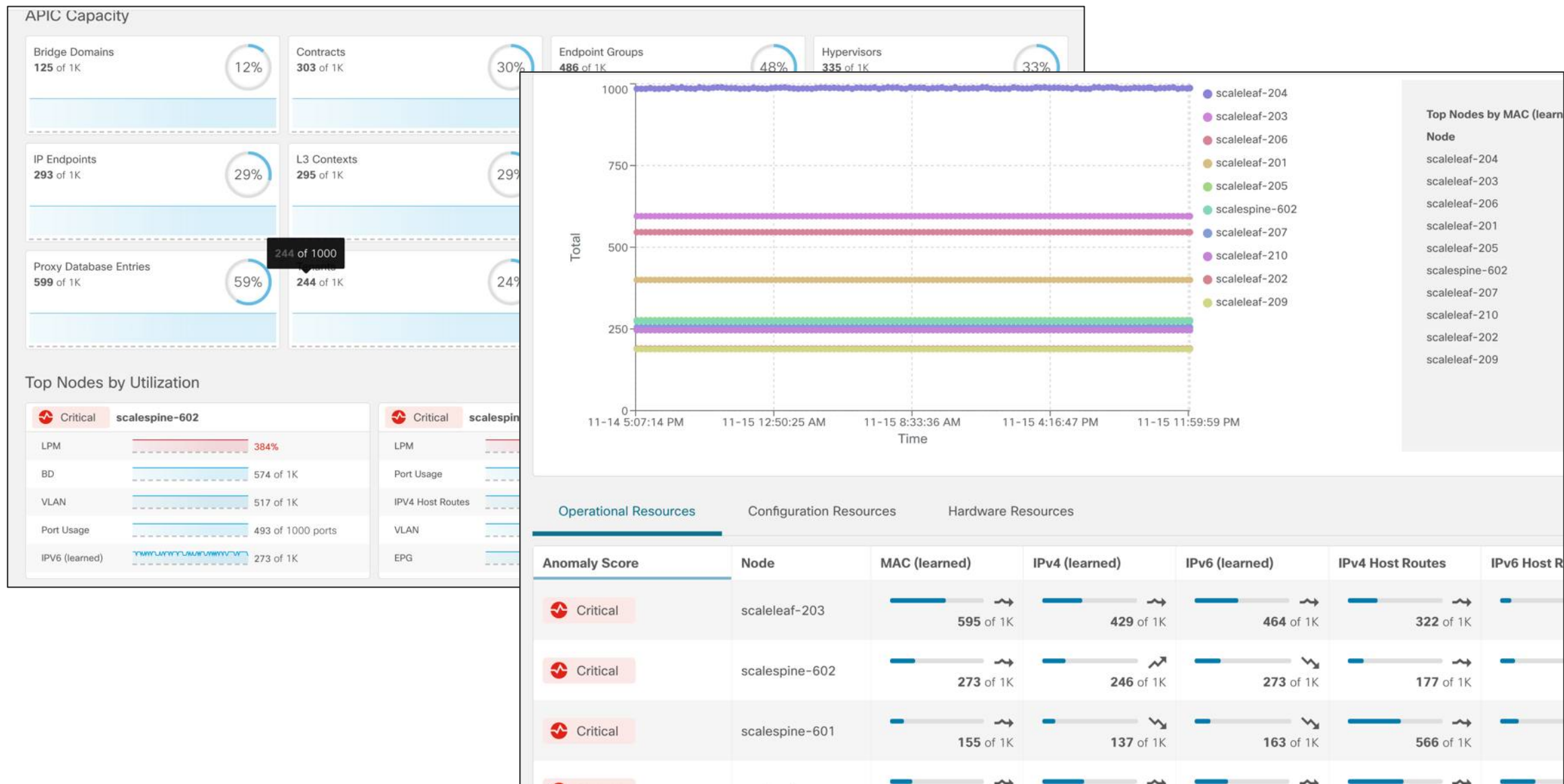
Last Seen Time

July 13, 2019, 10:25:30 AM

Clear Time

-

Хватает ли ресурсов?



Проблемы с BGP?

Состояние BGP и его аномалии

General Information

ANOMALY SCORE	ASN	ADMIN STATE	OPERATIONAL STATE	VERSION	NUMBER OF AS PATH	NUMBER OF ROUTE ATTRIBUTE
 Warning	65555	 Enabled	 Enabled	v4	190	190

Recommendations

1. Check the peer side configuration
2. Check for any misconfiguration on the local and peer side
3. Check for IP reachability(VRF, IP)

Рекомендации

Category	Nodes	Description	Cleared
----------	-------	-------------	---------

Total Errors
60

Neighbors

Neighbor	VRF	Operational State	Address Family	Connection Attempts	Prefixed Sent	Accepted Paths
10.2.0.1	default	 Established	I2vpn-evpn	21	1000	20
10.2.0.2	default	 Open - Confirm	I2vpn-evpn	40	0	30

Соседства, их состояния, число префиксов

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

Flow State Validator

The Flow S validation

* Required

Flow Type

☒ VXLAN

Inner Sour

10.1.1.1

Inner Sour

10

Source MA

Quick

Can

Flow State Validator

Complete

Start Time

Jan 06, 2020 03:49:41 pm

Job ID

FSV10250641713317

SOURCE IP	DESTINATION IP	SOURCE VLAN	VRF NAME	RUN TYPE	FLOW T
10.1.1.1	20.1.1.1	10	Default	FULL	VXLAN

Hop	Device	Fabric	State Va	
☒	1	LEAF-1	demo_fab_1	FAIL

Flow State Validator details for LEAF-1

CC_TYPE_FAB_IETH_LINKSTATE	show consistency-checker port-state fabric-ieth module 8 ieth-port 06 brief	Fail
CC_TYPE_L3_UC_SINGLE_ROUTE	show consistency-checker forwarding single-route ipv4 20.1.0.0/16 vrf default brief	Fail
CC_TYPE_L2_SWITCHPORT	show consistency-checker l2 switchport interface port-channel1 brief	Pass
CC_TYPE_MEMBERSHIP_VLAN	show consistency-checker membership vlan 1 brief	Pass
CC_TYPE_VPC	show consistency-checker vpc source-interface port-channel1 brief	Pass

Page 1 of 2

Objects Per Page 5 rows

Displaying Objects 1 - 5 of 11

Paths

Local Logical Interface	Peer Device	Peer Physical Interface	Peer Serial Number	Peer VLAN	Local Physical Interface
port-channel3.1	TOR-Seoul-1	Ethernet1/49	FDO20101H09	3	Ethernet1/49

Проверяемый поток

Проверка корректности в SW и HW на каждом коммутаторе

Предупреждения о PSIRT/Field Notice и т.д.

Analyze

Lifespan



19:40 19:45 19:55 20:00 20:20 20:15 20:30 20:25 20:40 20:35 20:10 20:05

Description

A vulnerability in the SPINE and LEAF components of the Cisco Application Policy Infrastructure Controller (APIC) software could allow an authenticated, local attacker to gain elevated privileges and execute arbitrary commands with root privileges on an affected device.

The vulnerability is due to insufficient sanitization of user-supplied input on certain background daemon operations running on the affected underlying NX-OS operation system. An attacker could exploit this vulnerability by injecting specially crafted strings via the Command-Line Interpreter (CLI) which may contain malicious content which may trigger superuser or root level commands. A successful exploitation could allow the attacker to gain elevated privileges and execute arbitrary commands with root privileges on the affected system, allowing for a complete compromise to the APIC operating system.

Recommendation

- To address the vulnerabilities on 6 nodes, upgrade to the versions 5.0(1k), 4.2(4i).



Firmware Update Analysis

Estimate the time and impact a firmware update might have.

- For further assistance on 4 nodes please contact the Cisco Technical Assist Center (TAC).



Cisco Technical Assistance Center

Around-the-clock, award-winning technical support services, online and over the phone to all customers.

Advisory Details

General Information

Title

Cisco Nexus 9000 Series Switches ACI Mode Privilege Escalation Vulnerability

Severity

 Critical

Status

 Cleared

Affected Nodes

10

Category

Field Notice

Detection Time

Feb. 10, 2019, 09:15:30 AM

Last Seen Time

Feb. 10, 2019, 09:15:30 AM

Clear Time

Feb. 10, 2019, 09:15:30 AM

Рекомендации по обновлению и его влияние

Advisory Detail

Recommended version is 7.0(3)I7(6)

Recommended version is 7.0(3)I7(6)

We recommend upgrading to version 7.0(3)I7(6).Please find the release notes for this version in the following link(s).
<https://www.cisco.com/c/en/us/support/switches/nexus-9000-series-switches/products-release-notes-list.html>

Rerun Upgrade Impact

Release Notes:

7.0(3)I7(5a)

7.0(3)I7(6)

7.0(3)I4(9)

Upgrade Paths

Recommended Upgrade Paths	Devices Affected	Non Disruptive	Disruptive
7.0(3)I7(1) → 7.0(3)I7(5a) → 7.0(3)I7(6)	1	0	1
7.0(3)I4(1) → 7.0(3)I4(9) → 7.0(3)I7(6)	1	1	-

Page 1 of 1

Objects Per Page 10 rows

Displaying Objects 1 - 2

Upgrade Impact Result

Device Name	Version	Version To	Result	Upgrade Impact Status	Last Run Time
LEAF-1	7.0(3)I7(1)		DISRUPTIVE		Jan 06, 2020 03:42 pm
LEAF-2	7.0(3)I4(1)		NONDISRUPTIVE		Jan 06, 2020 03:42 pm

TAC Assist

Помогает собрать логи для TAC SR непосредственно из приложения

Collect Logs

Select up to 5 devices to collect logs to assist TAC.
2 selected

Filter

	Device Name	Version
☐	TOR-Heavenly-1	9.3(3)
☒	TOR-LP-1	9.3(2.49)
☒	TOR-LP-2	9.3(2.49)
☐	TOR-Heavenly-2	9.3(3)
☐	TOR-sumpin-2	9.3(3)

Page 1 of 1

Objects Per Page 10 rows

TAC Assist

Begin the Log Collection Process

You will be asked to select the device(s) for which to collect Logs to assist TAC.

Begin

Log Collection

Type	Start Time	Status	Devices	Action
TAC Assist	Jan 17, 2020 04:08 pm	COMPLETE	2	View details

TAC Assist

STATUS	DEVICES	FABRIC	START TIME	JOB ID
Complete	2	vxlan_nia_hema	Jan 17, 2020 04:08:38 pm	TACASSISTxtVjrYWJTUCIgjYeld7gPQ

Logs (2 of 2 Successful)

Device Name	Related Job ID	Status	Status Message	Log Location	Cloud
TOR-LP-1	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTxtVjrYWJTUCIgjYeld7gPQ	Upload
TOR-LP-2	N/A	Success		/var/afw/vols/ceti/uploads/TACASSISTxtVjrYWJTUCIgjYeld7gPQ	Upload

Практические аспекты разворачивания DCNM и MSO

Экосистема Cisco DCNM



Платформа для хостинга приложений
(Day2 Operations и расширенные функции)



**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.

The image displays two screenshots of the Cisco DCNM Installer. The left screenshot shows the initial selection screen with four radio button options: 'Fresh installation - Standalone' (selected), 'Fresh installation - HA Primary', 'Fresh installation - HA Secondary', and 'Fresh installation with backup file for restore'. A 'Continue' button is at the bottom. The right screenshot shows a more detailed configuration screen with a progress bar and tabs: 'Install Mode', 'Administration', 'System Settings', 'Network Settings', 'Applications', 'HA Settings', and 'Summary'. The 'Install Mode' tab is active. It prompts the user to 'Please choose how to install DCNM' with a dropdown menu set to 'LAN Fabric'. Below this, it states 'LAN Fabric is for most VXLAN-EVPN deployments.' and has a checked checkbox for 'Enable Clustered Mode' with a note: 'When this option is checked, DCNM will be installed in Clustered mode and applications will run on DCNM Compute nodes.' A 'Next' button is at the bottom right. Two orange callout boxes provide additional context: one points to the 'LAN Fabric' dropdown and explains its use for both VXLAN EVPN and legacy/classic scenarios; the other points to the 'Enable Clustered Mode' checkbox and states that for App Hosting plans, this support must be activated initially.

Cisco DCNM Installer

Please select how you want to setup this instance of Cisco Data Center Network Manager:

- ☒ Fresh installation - Standalone
- ☐ Fresh installation - HA Primary
- ☐ Fresh installation - HA Secondary
- ☐ Fresh installation with backup file for restore

Continue

Cisco DCNM Installer

Install Mode Administration System Settings Network Settings Applications HA Settings Summary

Please choose how to install DCNM

Installation mode *

LAN Fabric

LAN Fabric is for most VXLAN-EVPN deployments.

☒ Enable Clustered Mode

When this option is checked, DCNM will be installed in Clustered mode and applications will run on DCNM Compute nodes.

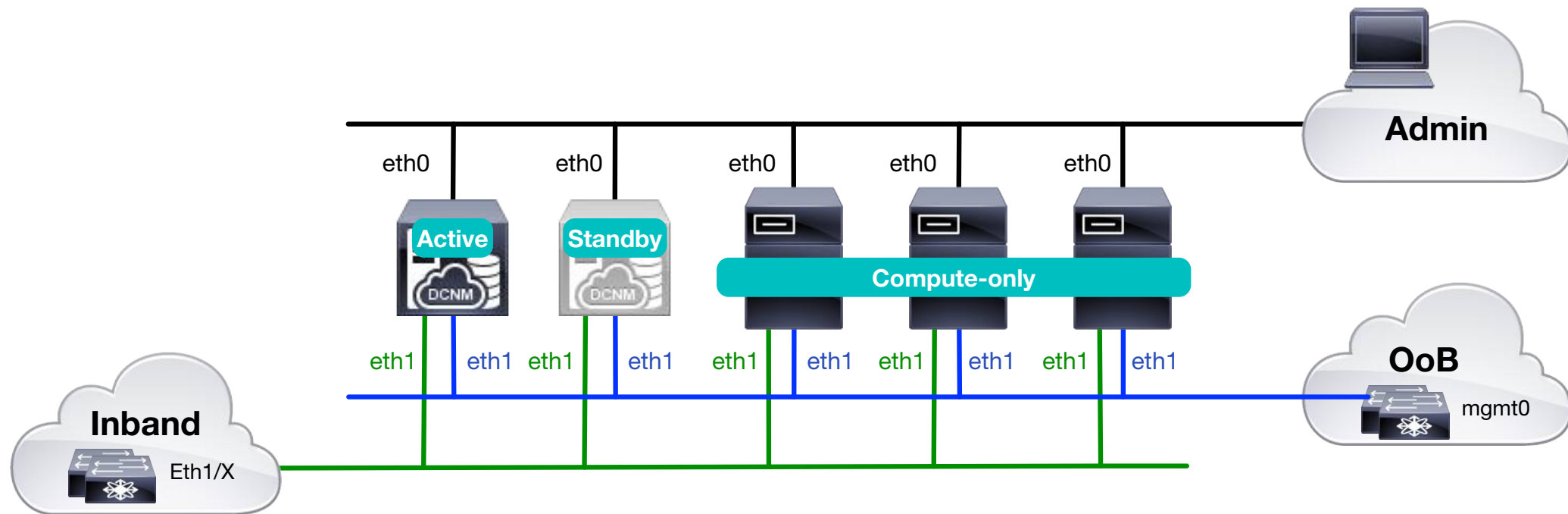
Next

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

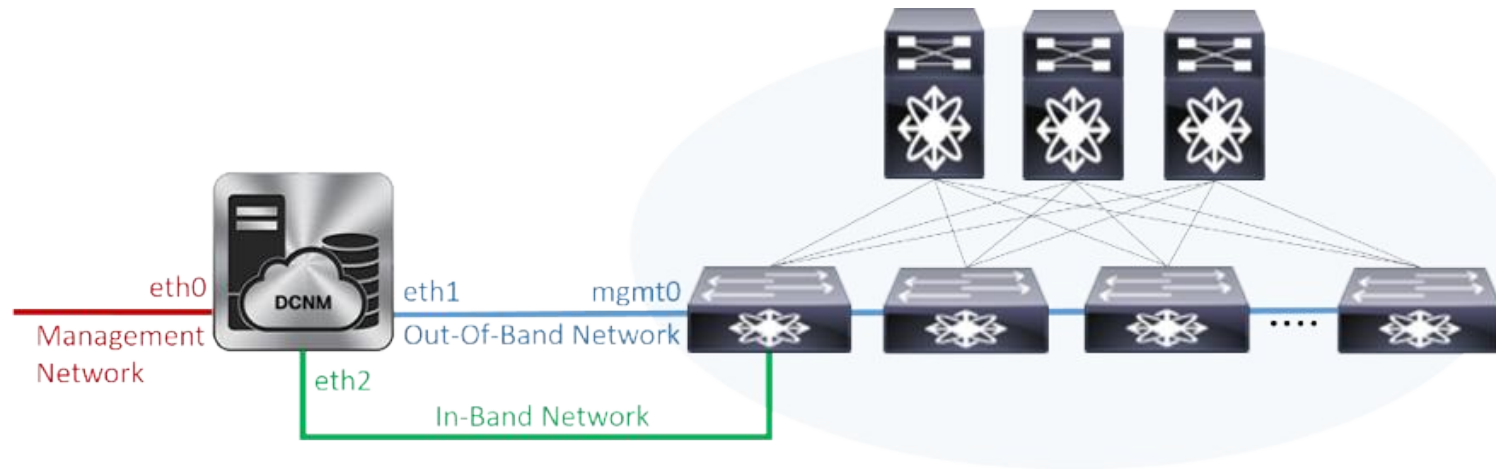
Режим LAN Fabric используется как для VXLAN EVPN, так и для legacy/classic сценариев

Cisco DCNM Native HA

Обеспечивает отказоустойчивую конфигурацию в рамках одной площадки. Требуется 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>

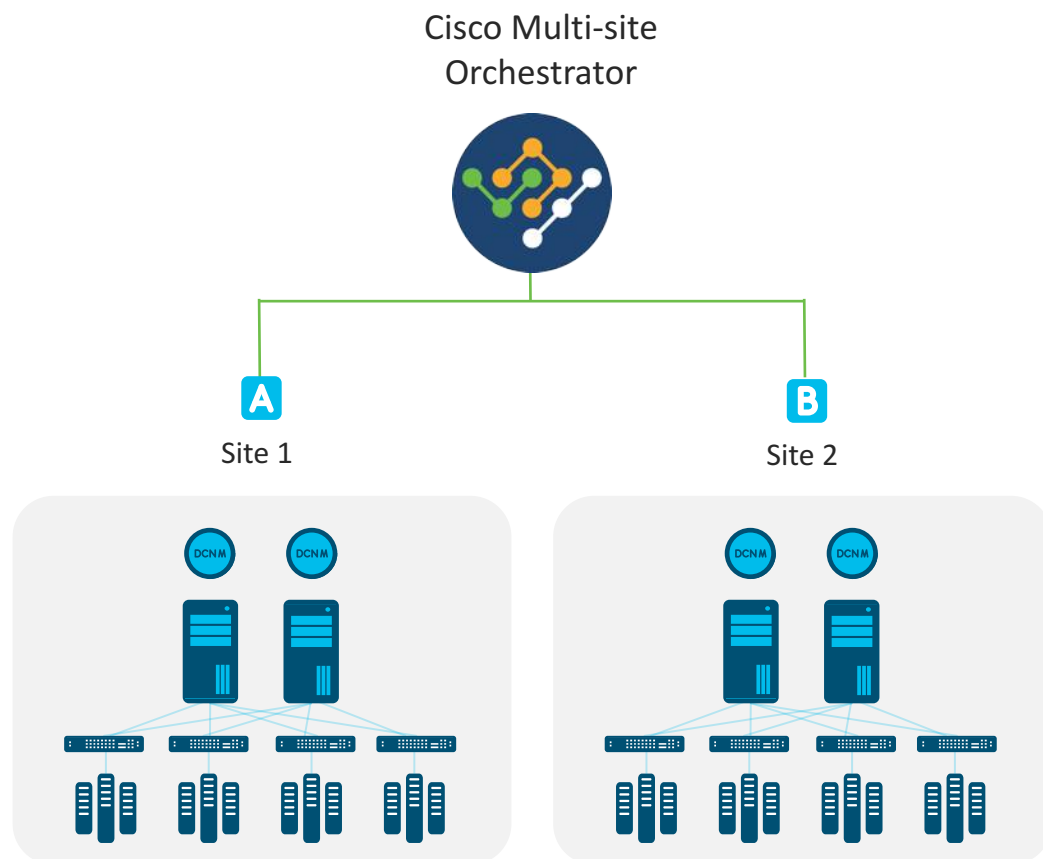
Cisco DCNM

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**

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

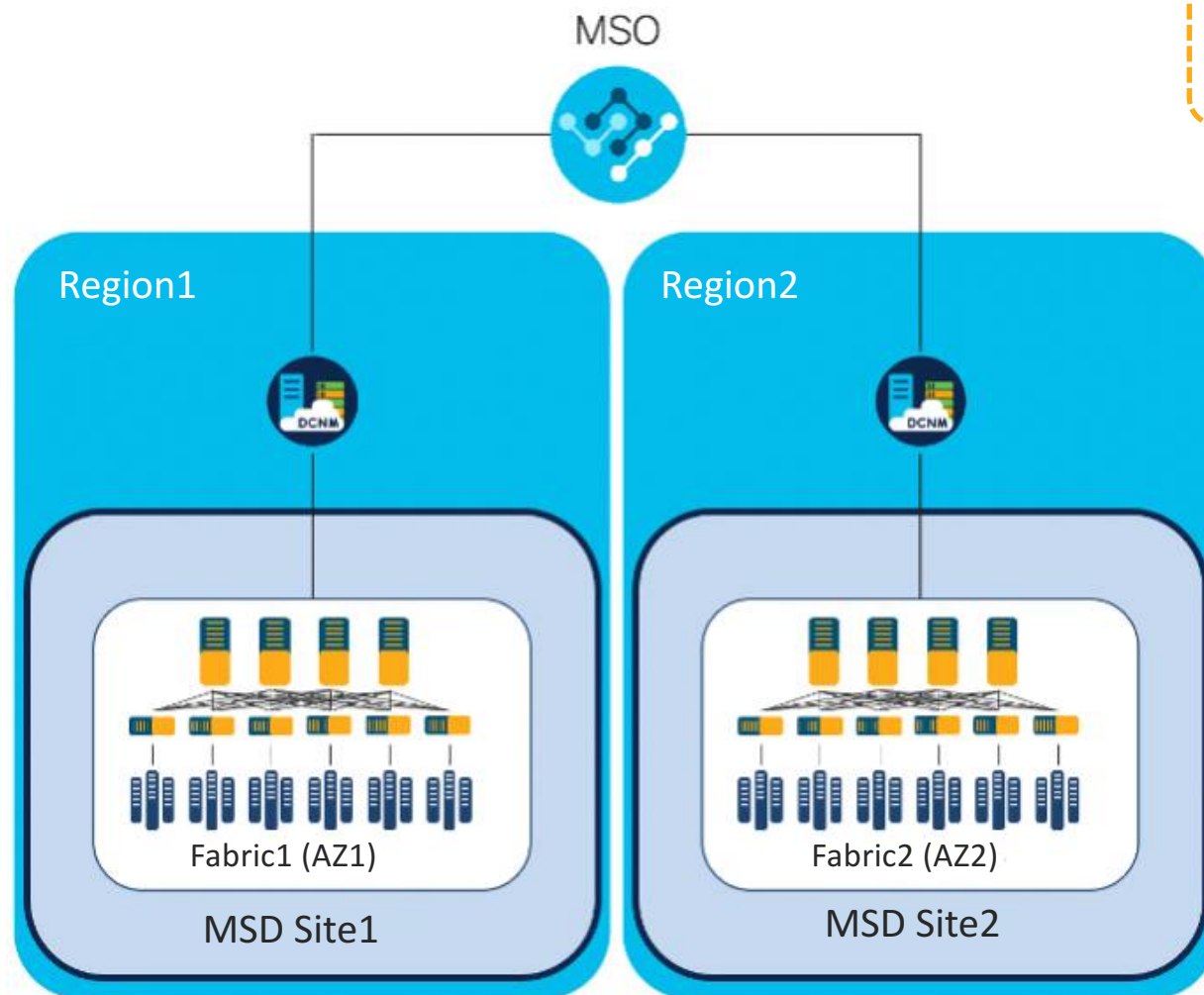
Disaster Recovery

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

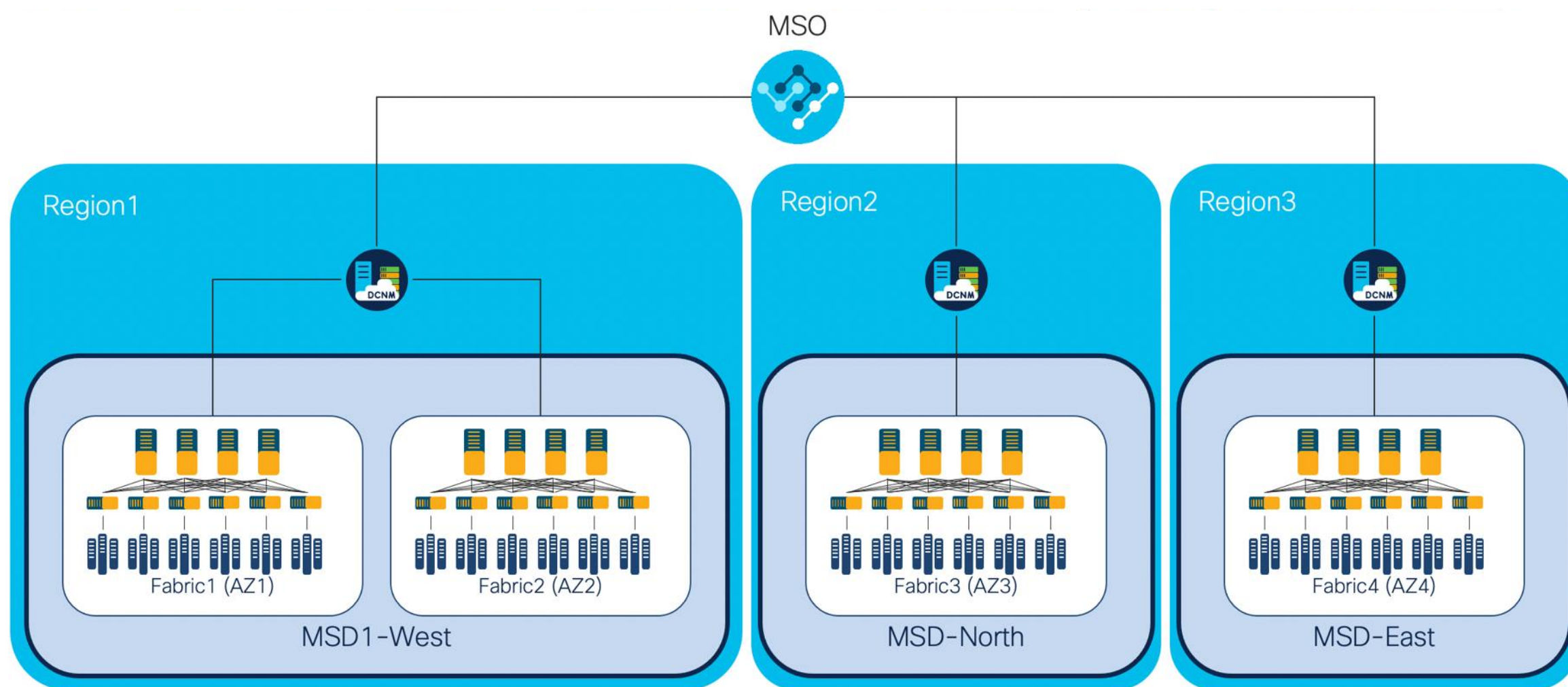
2. **Один или несколько доменов Cisco DCNM Multi-Site Domain (MSD)**

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

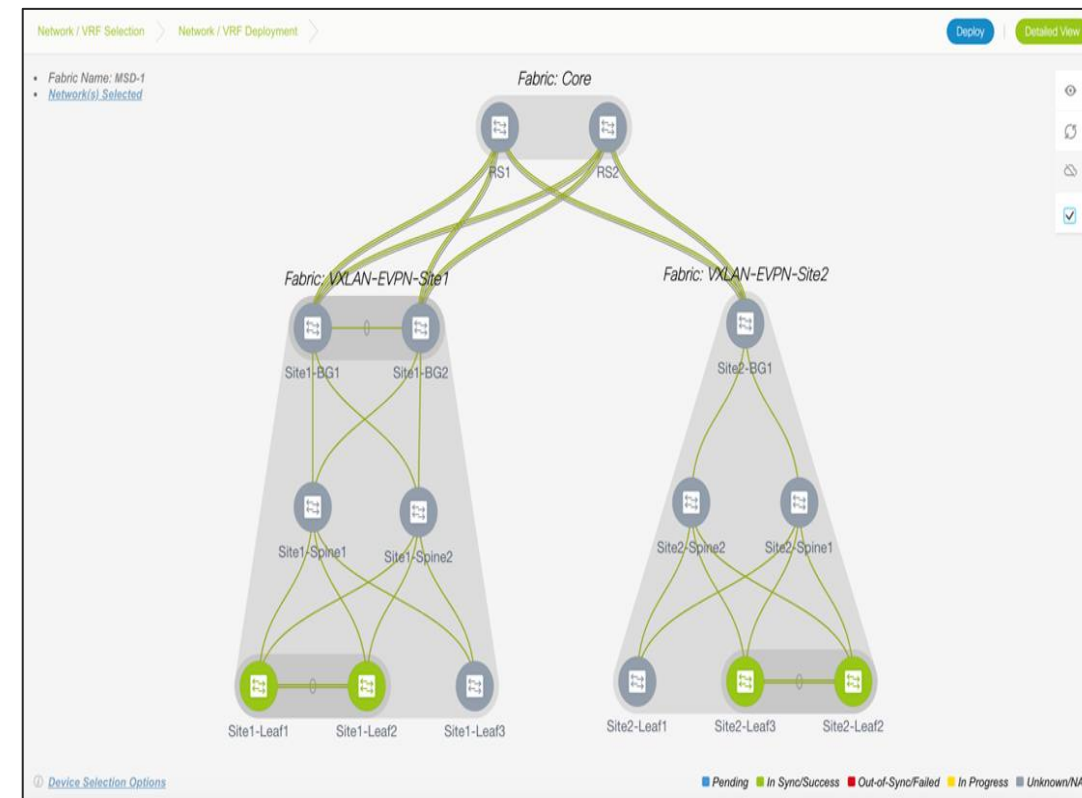
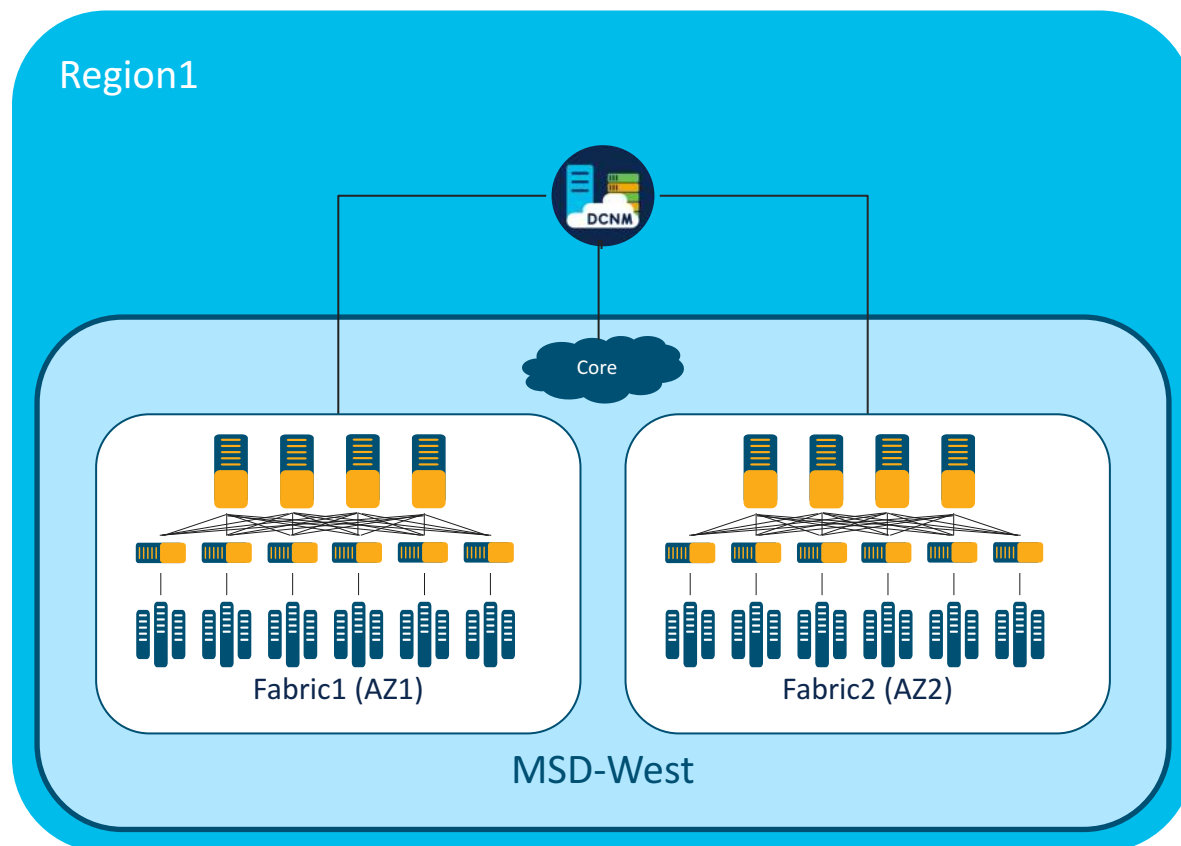
Интеграция Cisco DCNM и Cisco MSO

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

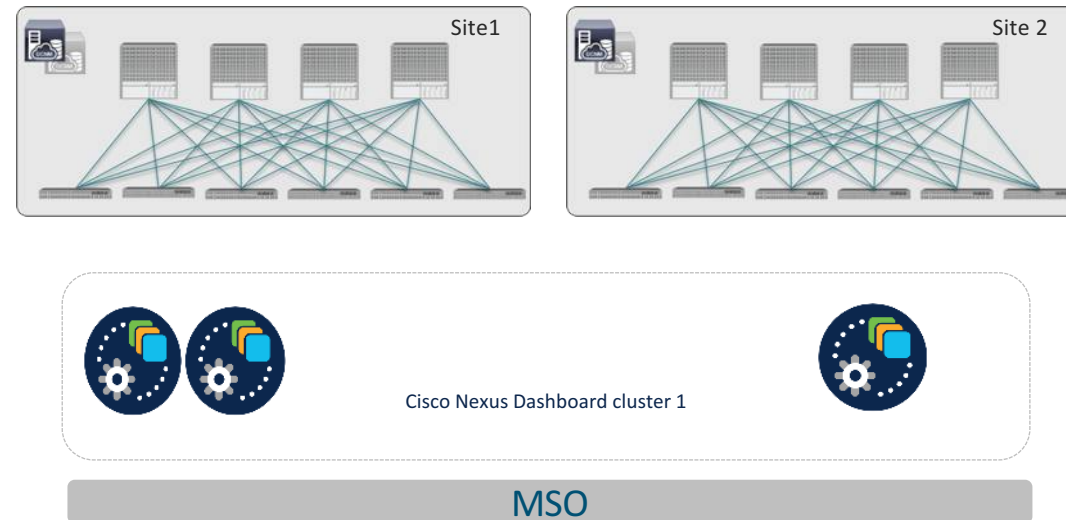
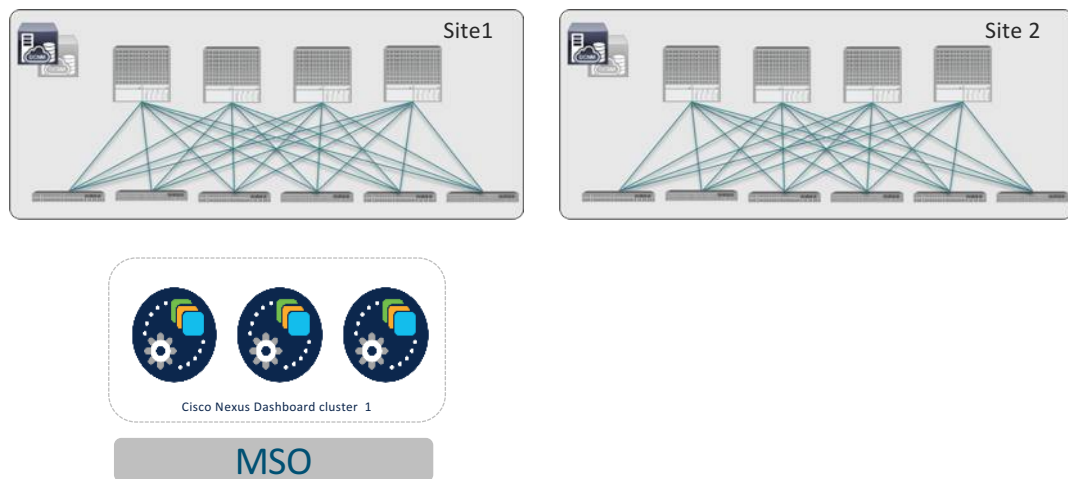
Cisco MSO отвечает за централизованную настройку, мониторинг состояния, и управление жизненным циклом политик сайтов находящихся под управлением разных экземпляров Cisco DCNM

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

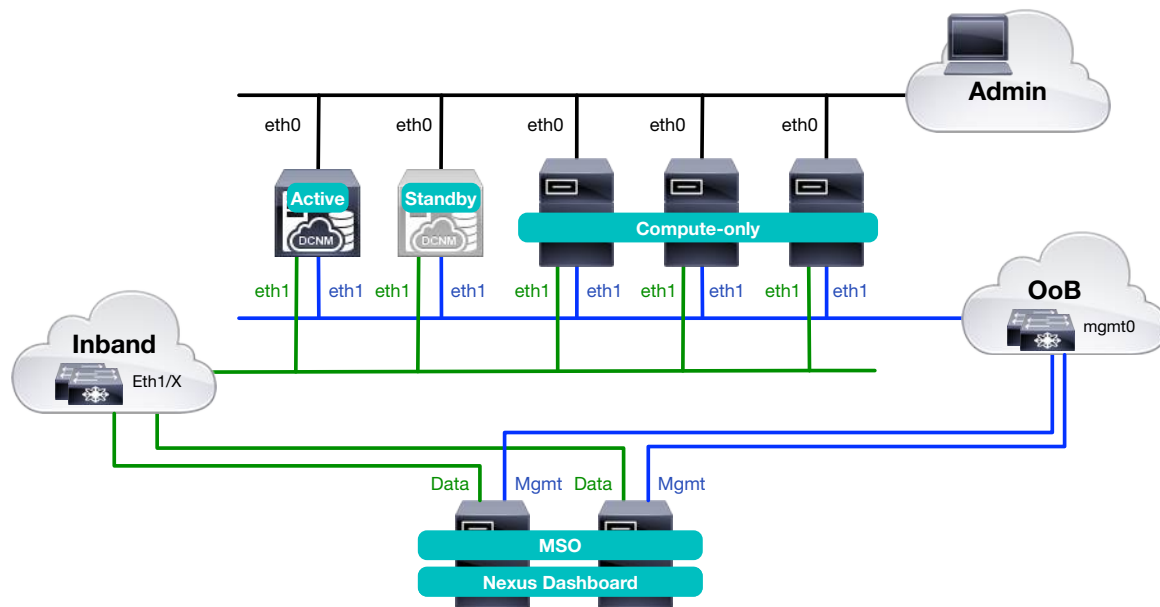
- Аппаратный кластер Cisco Nexus Dashboard состоящий из трех узлов

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

