

Сбор и анализ ЛОГОВ

Андрей Ветров

Senior Systems Engineer,
VMware



Cloud Thinking

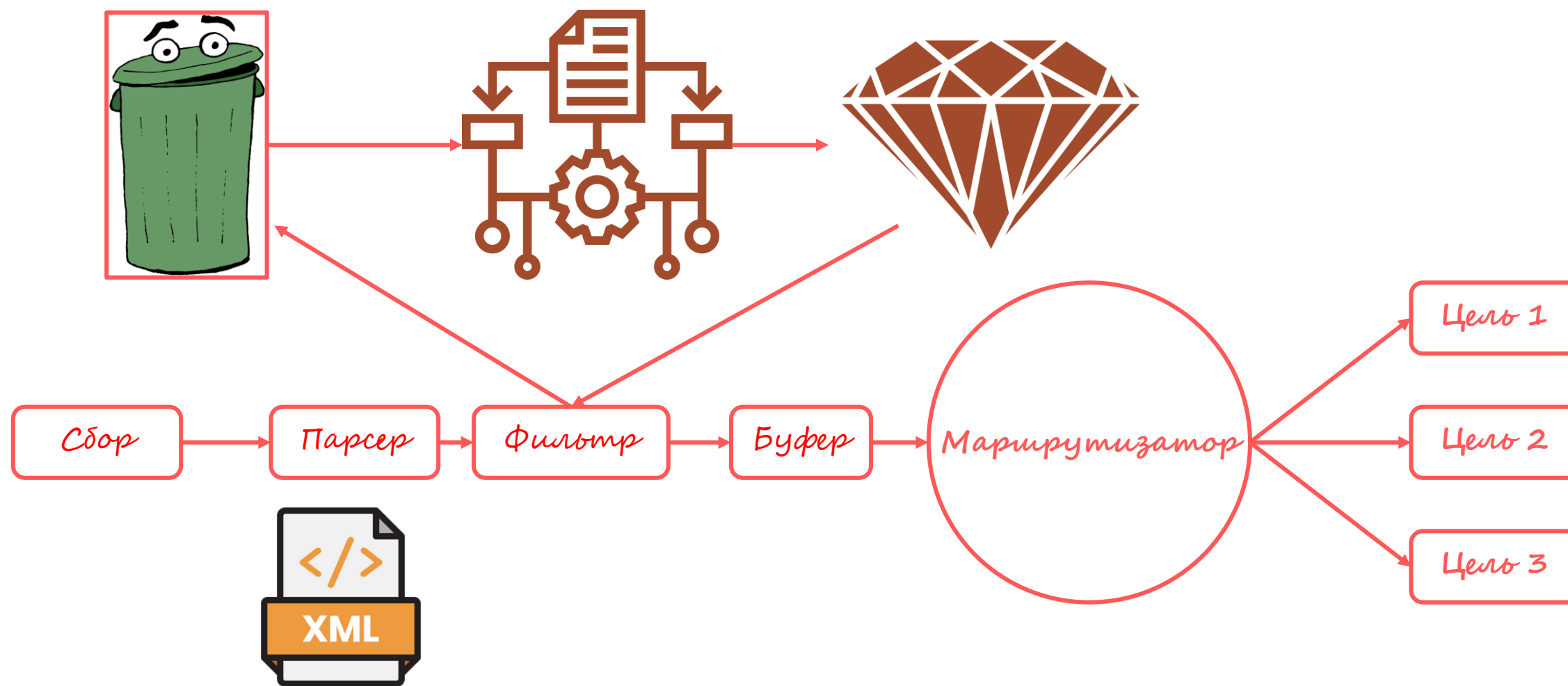


Что такое Fluent Bit?

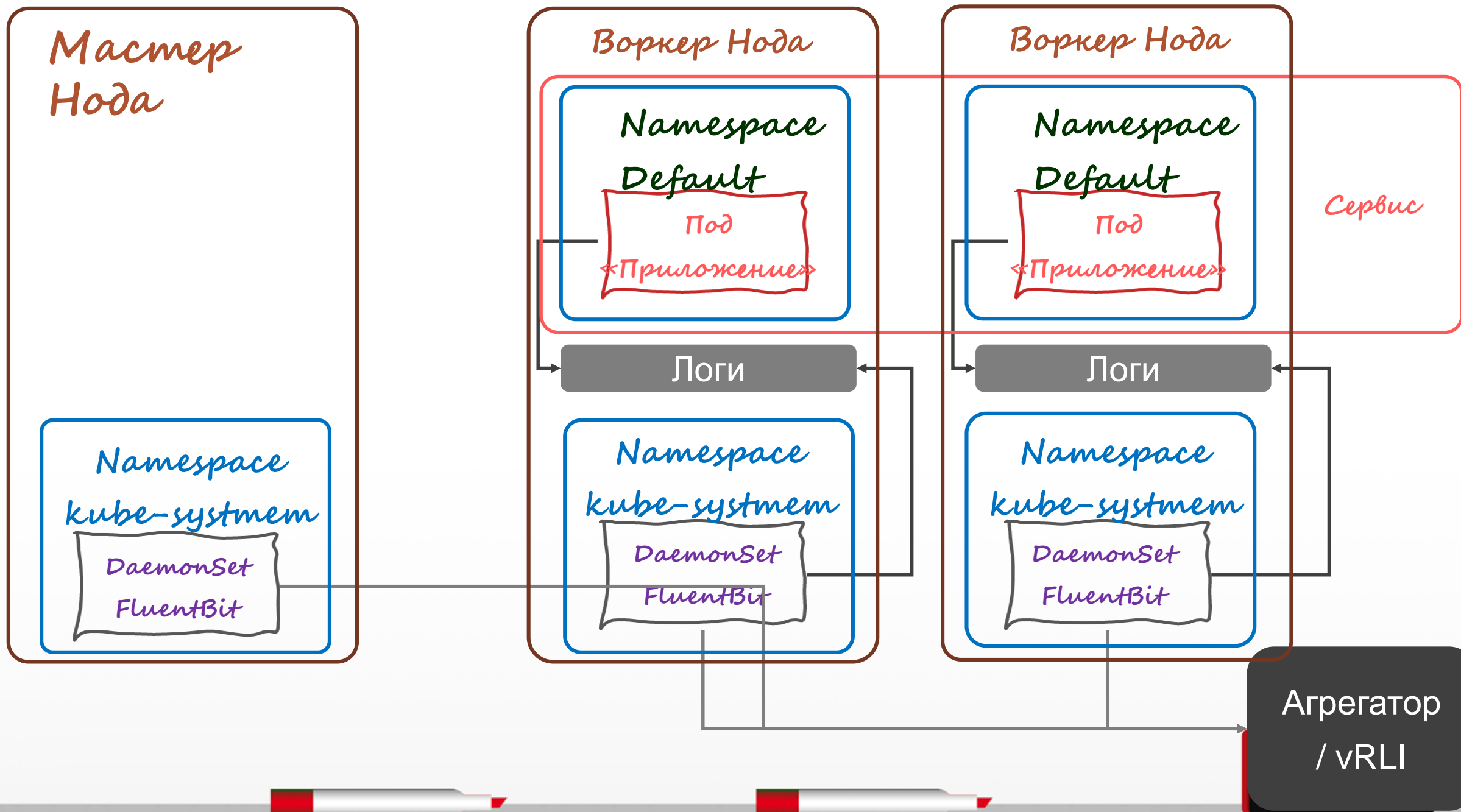


fluentbit

Поток данных

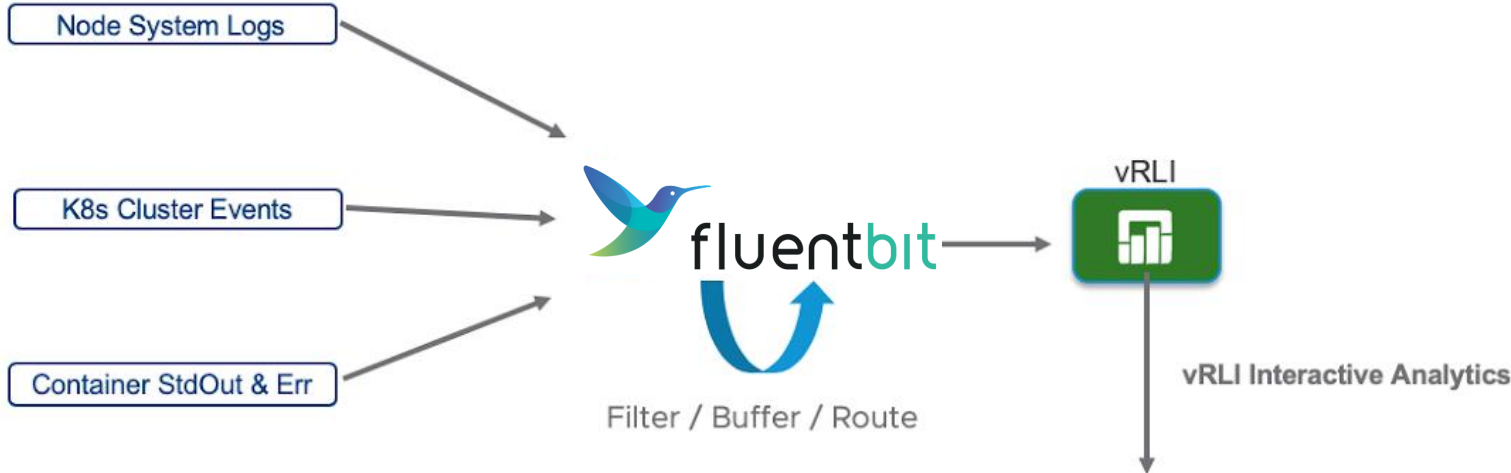


Логи



Сбор и анализ логов Kubernetes

vRealize Log Insight



Match all of the following filters:

- X kubernetes__container_... contains mysql vke-app
- X kubernetes__namespac... contains vke-app
- X kubernetes__pod_name contains vke-app-8769bf494-vcx2c
- X bosh_deployment contains service-instance_7a0436f5-1d6b-41f7-9254-d92005faae13
- X bosh_id contains 62aa48b6-bea2-46c1-9ecf-b29e4d80b1c1

+ A bosh

Event bosh_deployment

bosh_id

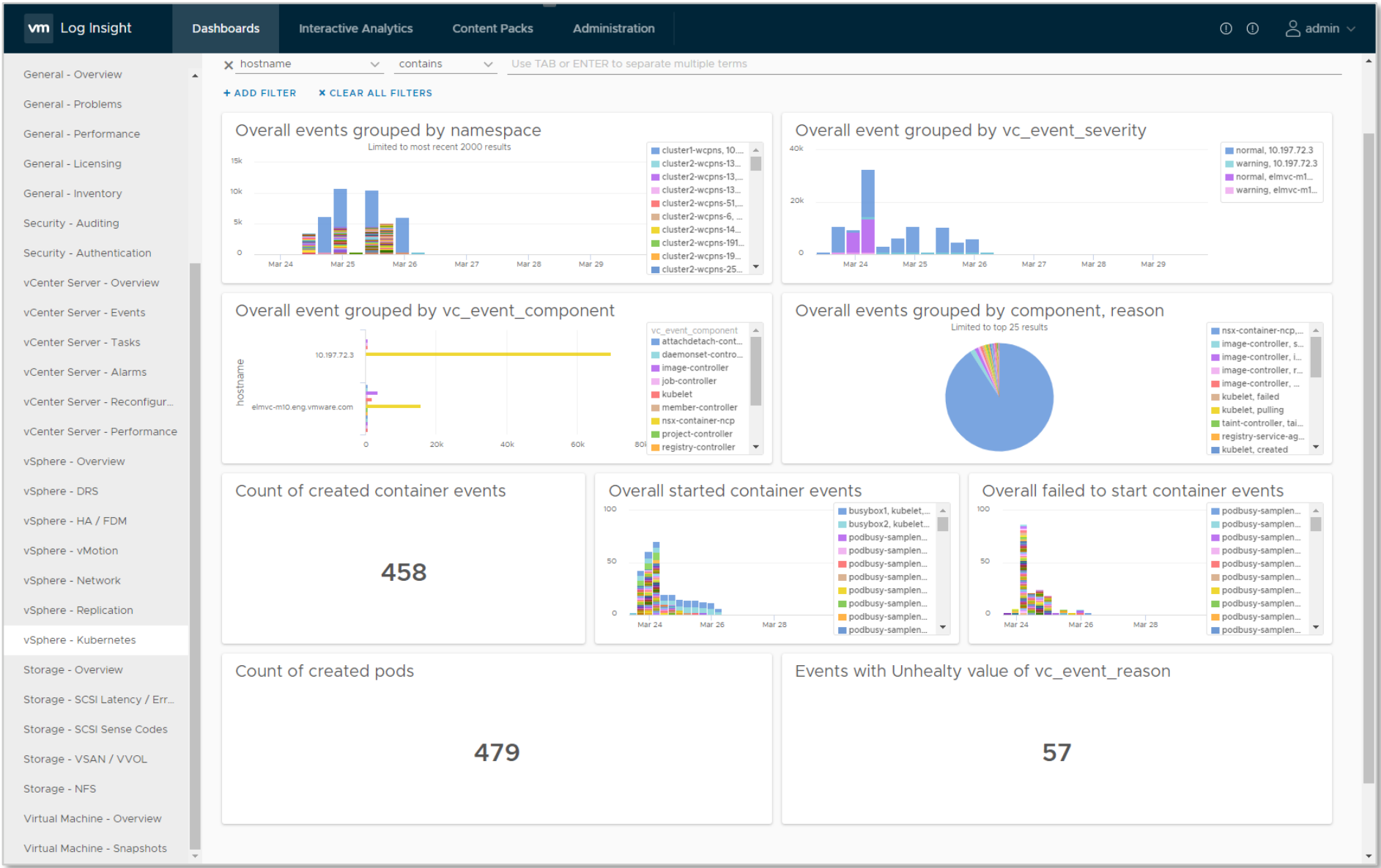
bosh_index

id event_type hostname Instance_type kubernetes__cont...

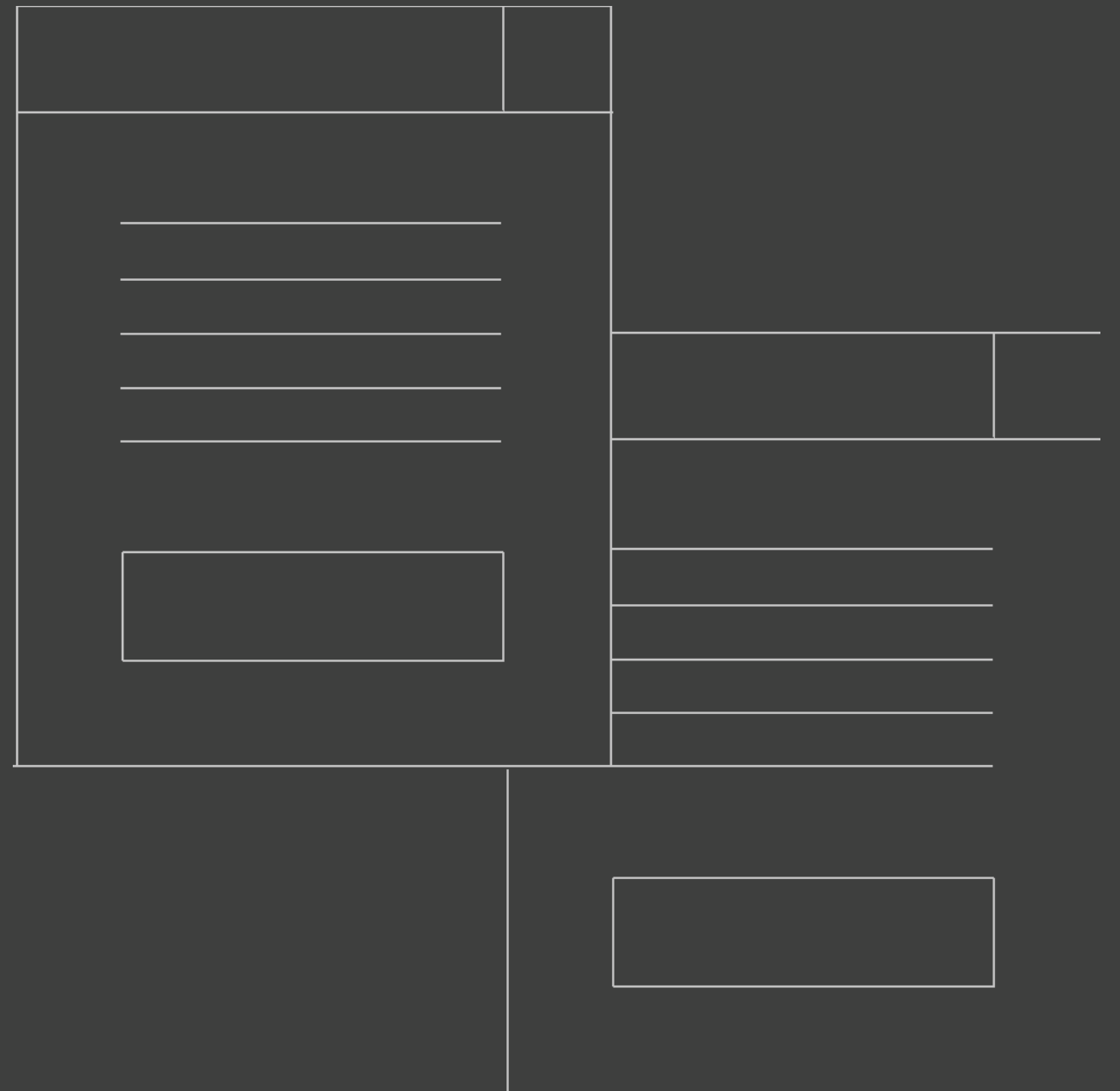
kubernetes__pod_name stream log

Сбор и анализ логов Kubernetes

vRealize Log Insight

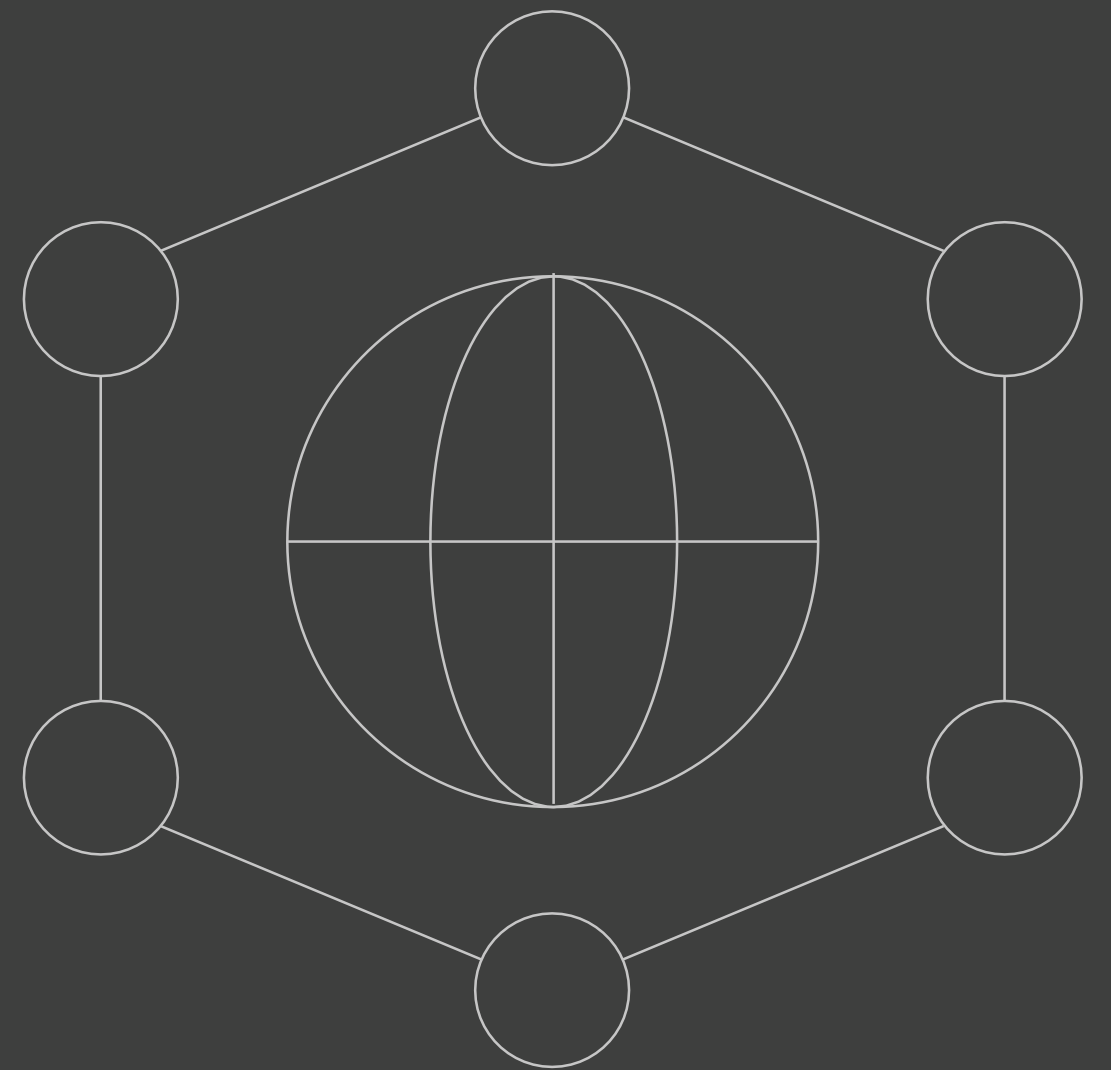


Демо

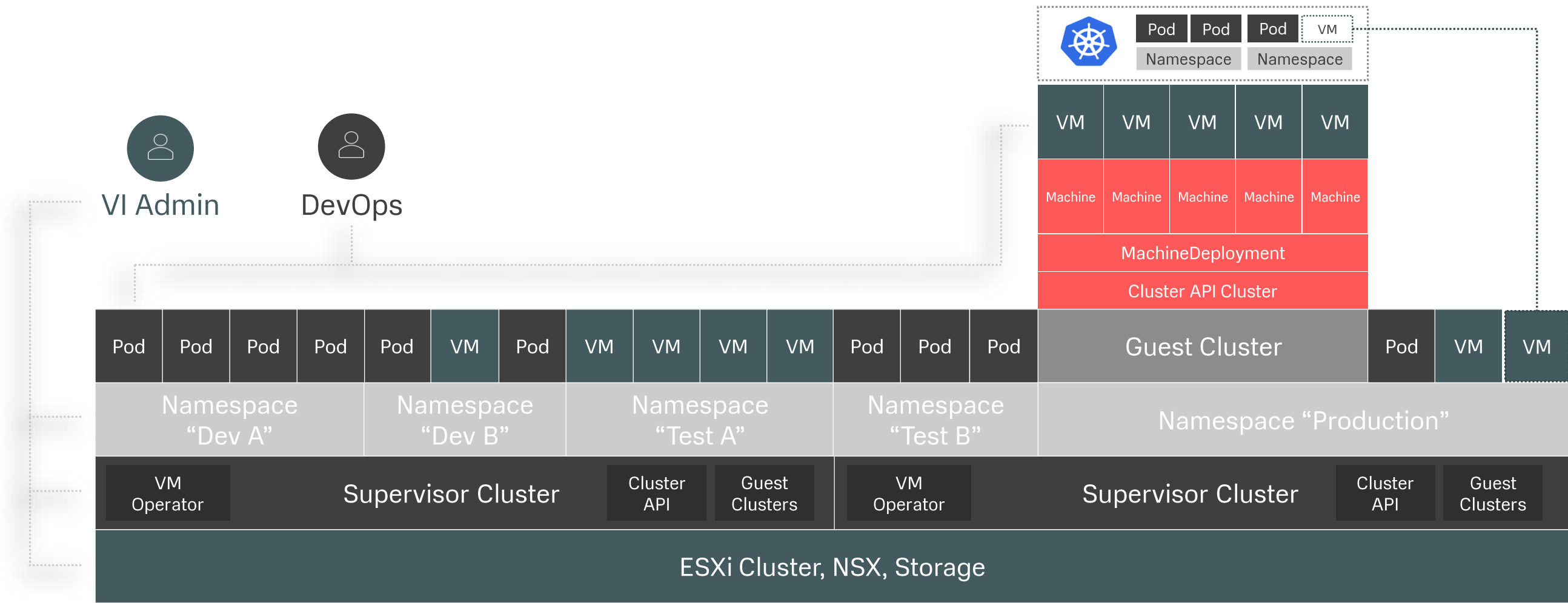


Мониторинг сети и визуализация

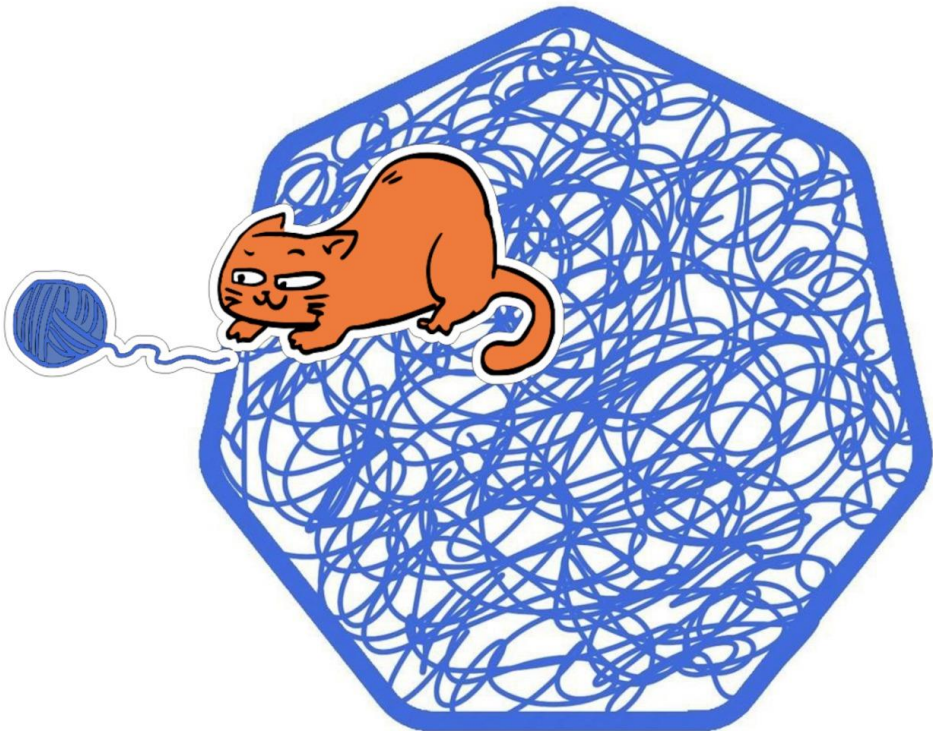
vRealize Network Insight



Что происходит на самом деле

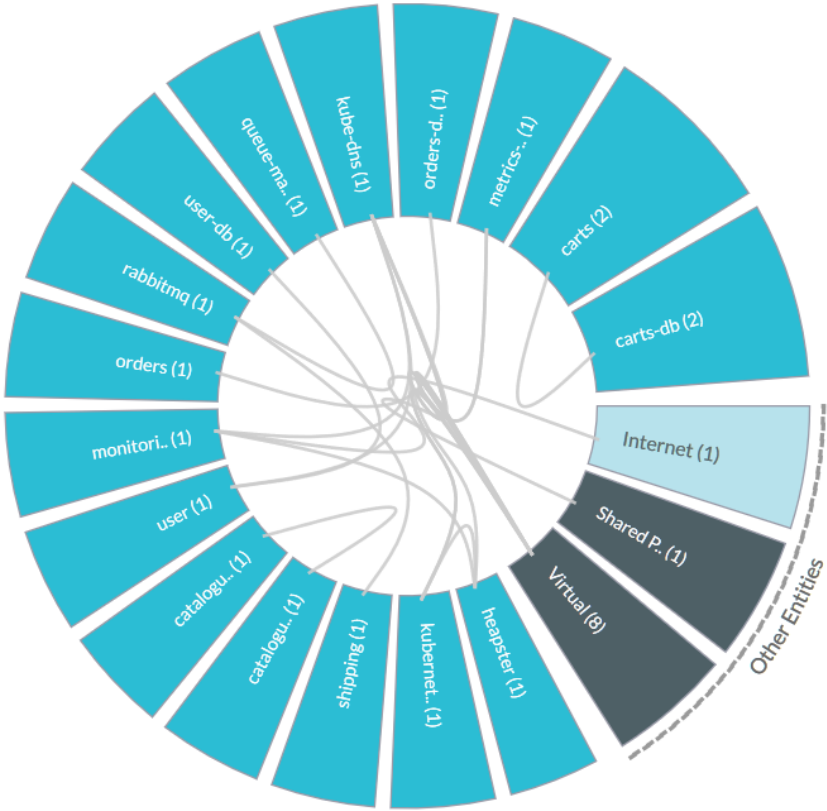


Что происходит на самом деле



Kubernetes Networking

Group By: Kubernetes Service
Flow Type: All Allowed Flows



High-Level Architecture

vmware®
vRealize® Network Insight™

From PKS / Kubernetes

From NSX-T

- Objects – Cluster, Namespace, Service, Pods, Nodes
- Watch
- Events / Metrics

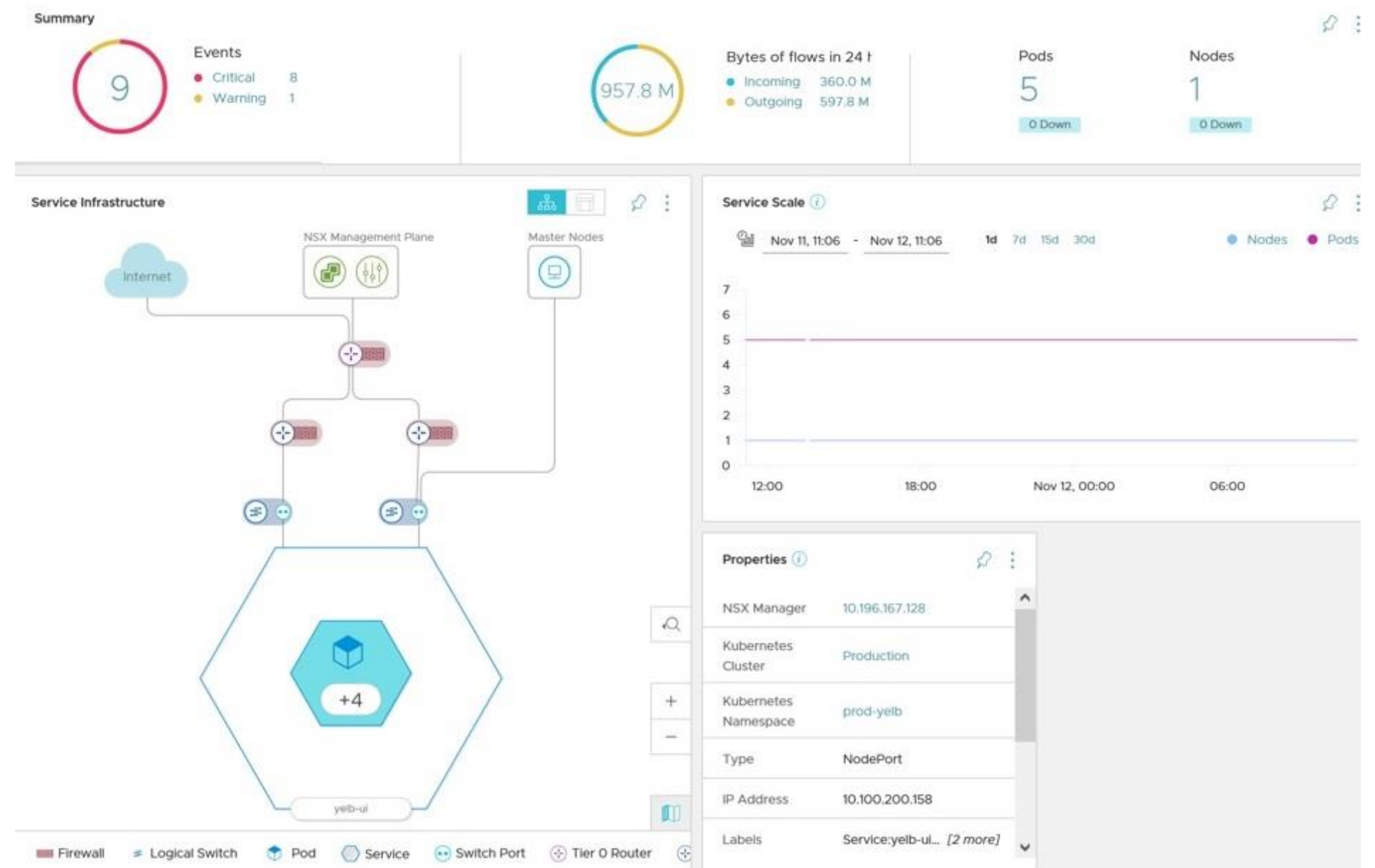
- Logical Switches and their detailed information
- Logical Routers (T0 and T1) and their detailed information
- Router and switch ports and their detailed information
- Associated IP Blocks
- NSX Groups and their members
- Associated DFW rules with NSX Groups
- Associated Load balancers
- TX/RX Counters
- IPFIX – traffic flow records

Детализация сетевой топологии сервиса

vRealize Network Insight

Ключевые возможности

- Отображение архитектуры решения
- Взаимосвязь ивентов NSX-T и Kubernetes
- Диаграммы и графики сетевых взаимодействий



Планирование безопасности

Экспорт YAML из коробки

- Сетевые политики
- Кластеры
- Сервисы
- Namespace

Plan Security

Scope Kubernetes Cluster prod-cluster

Duration Last 7 days

Analyze

Micro-Segments

Group By
Kubernetes Service

Flow Type
All Allowed Flows

Export Rules as XML

Export Rules as
YAML

Maximize

Детализация: рекомендации политик сетевой безопасности

Возможность применить на лету

- kubectl apply -f *.yaml

```
1  apiVersion: networking.k8s.io/v1
2  kind: NetworkPolicy
3  metadata: {name: network-policy-d, namespace: kube-system}
4  spec:
5    egress:
6      - ports:
7        - {port: 5000, protocol: TCP}
8        to:
9          - podSelector:
10             matchLabels: {Service: ca}
11             policyTypes: [Egress]
12
13
14
15
16
17
18
19
20
21  apiVersion: networking.k8s.io/v1
22  kind: NetworkPolicy
23  metadata: {name: network-policy-d, namespace: kube-system}
24  spec:
25    ingress:
26      - from:
27        - podSelector:
28            matchLabels: {Service: ca}
29        ports:
30          - {port: 20000, protocol: TCP}
31          - {port: 20001, protocol: TCP}
32          - {port: 20002, protocol: TCP}
33          - {port: 20003, protocol: TCP}
34          - {port: 20004, protocol: TCP}
35          - {port: 20005, protocol: TCP}
36          - {port: 20006, protocol: TCP}
37          - {port: 20007, protocol: TCP}
38          - {port: 20008, protocol: TCP}
39          - {port: 20009, protocol: TCP}
40          - {port: 20010, protocol: TCP}
41
42
43
44
45
46
47
48
49
50
51  apiVersion: networking.k8s.io/v1
52  kind: NetworkPolicy
53  metadata: {name: network-policy-src-metrics-server-kube-system-Others_Physical-tcp, namespace: kube-system}
54  spec:
55    egress:
56      - ports:
57        - {port: 443, protocol: TCP}
58        to:
59          - ipBlock: {cidr: 10.100.200.1/32}
60      - ports:
61        - {port: 443, protocol: TCP}
62        to:
63          - ipBlock: {cidr: 192.168.115.1/32}
64    podSelector:
65      matchLabels: {Service: metrics-server-Others_Physical}
66    policyTypes: [Egress]
```

Спасибо!

