



Introduction to OpenNMS

v1.1



What is OpenNMS?

Vision: A world where monitoring just happens



Scalable

Monitors tens of thousands of devices while processing terabytes of data from a single instance.



Extensible

Extensible platform enabling adaptation and integration into core business processes.



Open Source

Published under the AGPLv3 license, OpenNMS is a fully open source solution.



Supported

Sustained by a large community of users and supported commercially by The OpenNMS Group

OpenNMS is a scalable and highly configurable open-source network management platform with comprehensive fault, performance, and traffic monitoring.

It easily integrates with your core business applications and workflows to monitor and visualize everything in your network.

OpenNMS Open Source Community

GitHub Stats

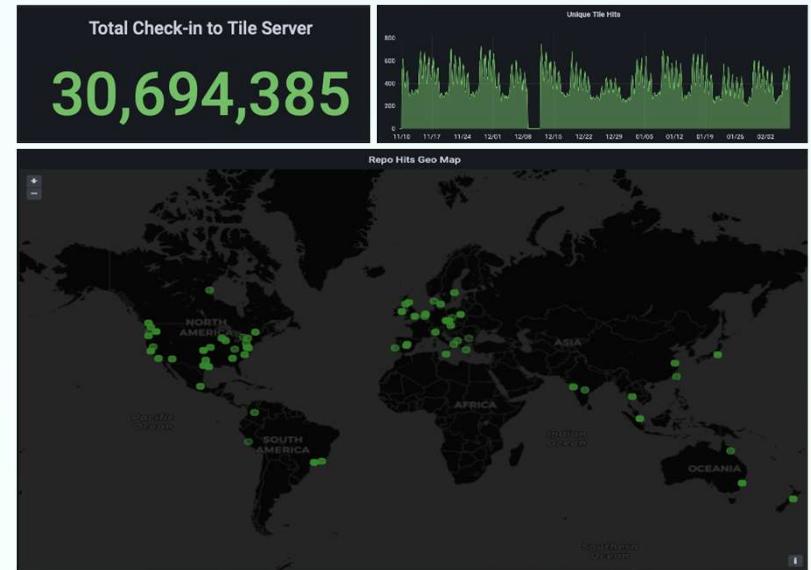


DockerHub Stats

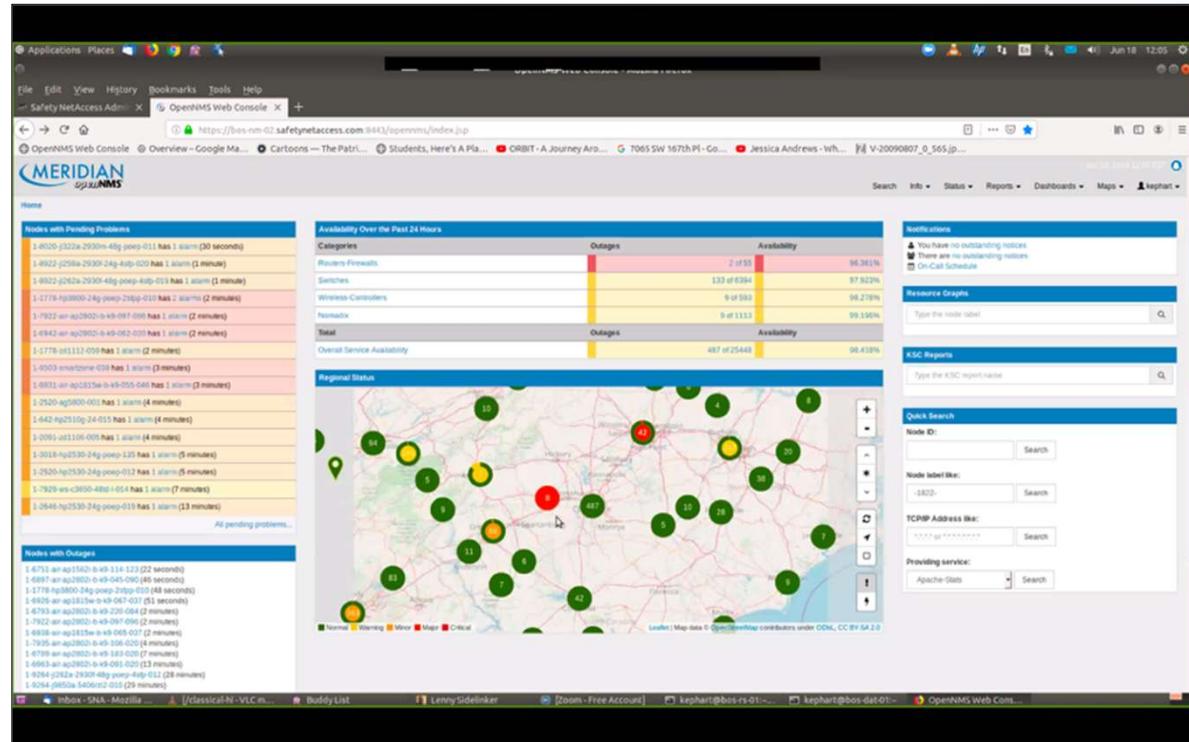
 opennms/minion ·  5M+ ·  5 By opennms · Updated 4 hours ago Image	 opennms/horizon ·  1M+ ·  12 By opennms · Updated 4 hours ago Image
---	---

9M Minion Container Downloads!

Web Stats (90 Days)

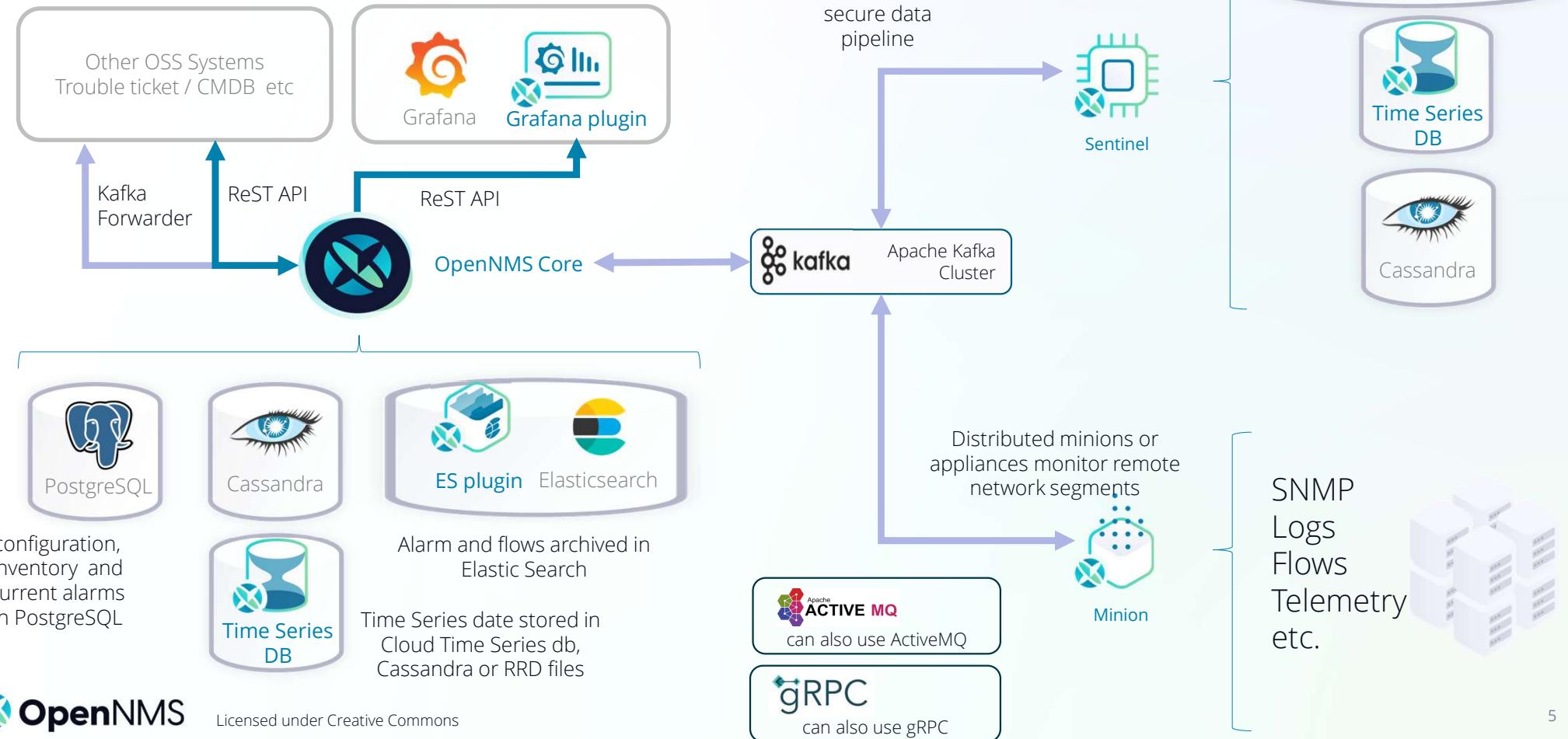


The OpenNMS Solution



- Event Management
- Fault / Alarm Management
- Performance Management
- Network Traffic Management
- Network Inventory Management
- AI Correlation

OpenNMS Architecture



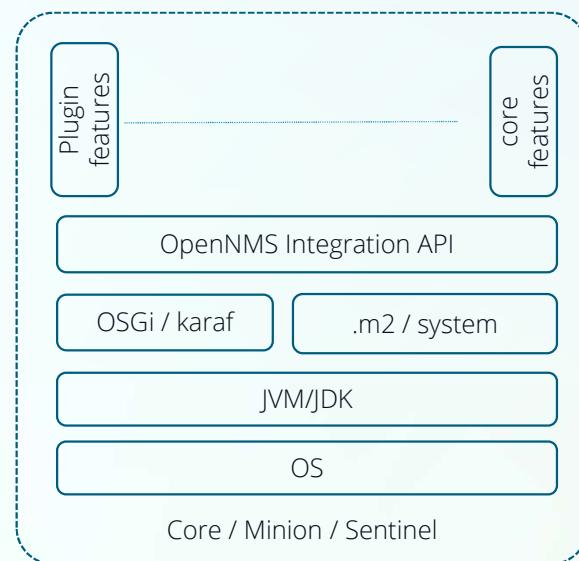
Plugin Architecture

- Key Features

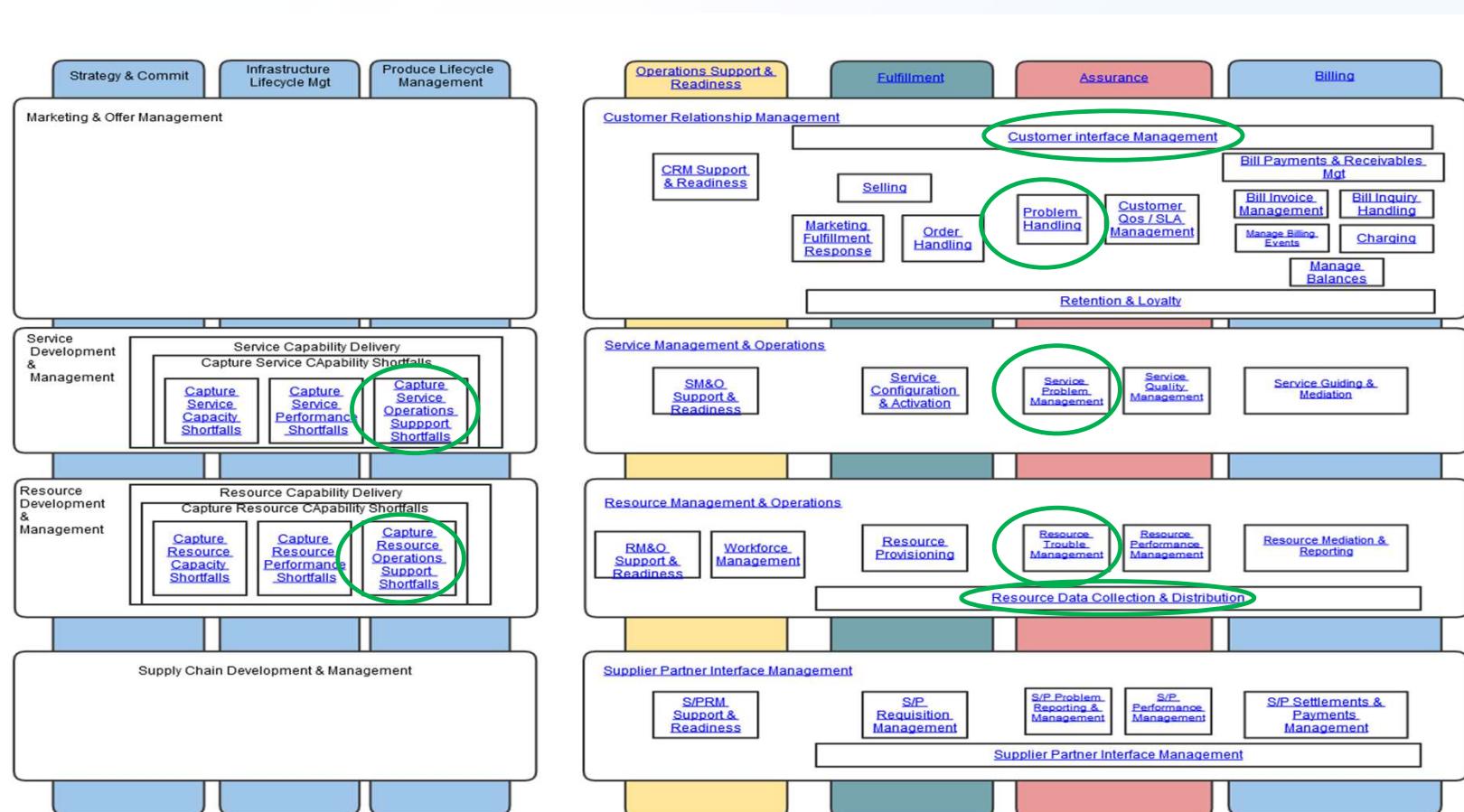
- OpenNMS Integration API
 - Lifecycle Independent of core OpenNMS
 - Based on OSGi (Apache Karaf)
 - Class path / feature / bundle isolation
 - Reuse of code 'bundles' across plugins
- Plugin Capabilities
 - UI components which automatically register and extend the core dashboard
 - Configuration Components which add definitions for events / alarms / data collection / Correlation Rules
 - Topology Provider components which show up as domain specific topologies and can be used by ALEC
 - Interface components which provide new external API's (Data collection Protocols and Integration Protocols)

- Benefits

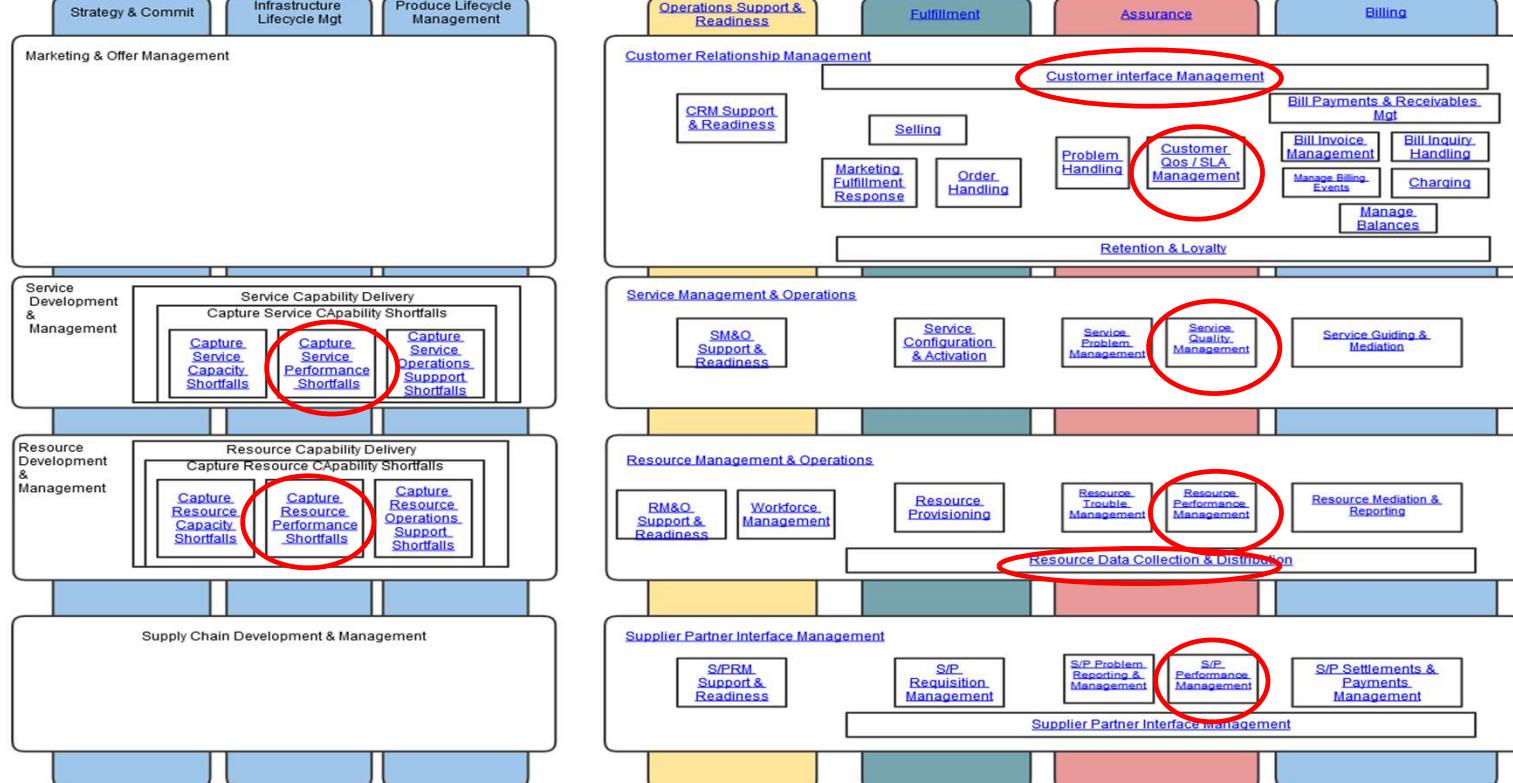
- Allows new and complex functionality to be incrementally developed, tested and safely deployed in a production system



Problem Handling Touch Points

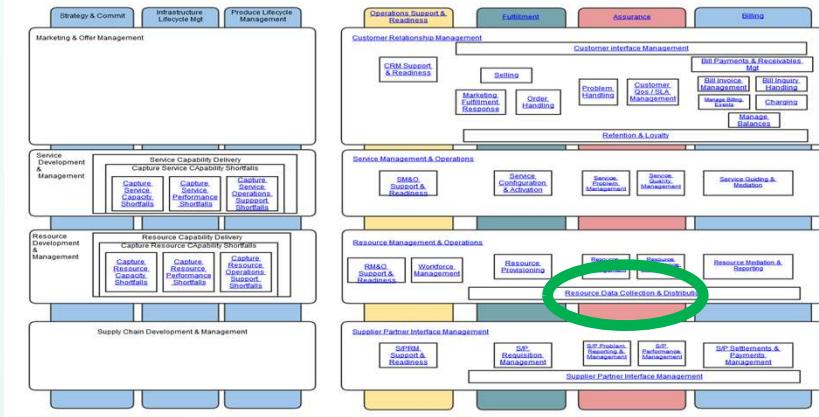


Performance Management Touch Points



TM Forum Business Process Framework (eTOM)

Resource Data Collection at All Layers

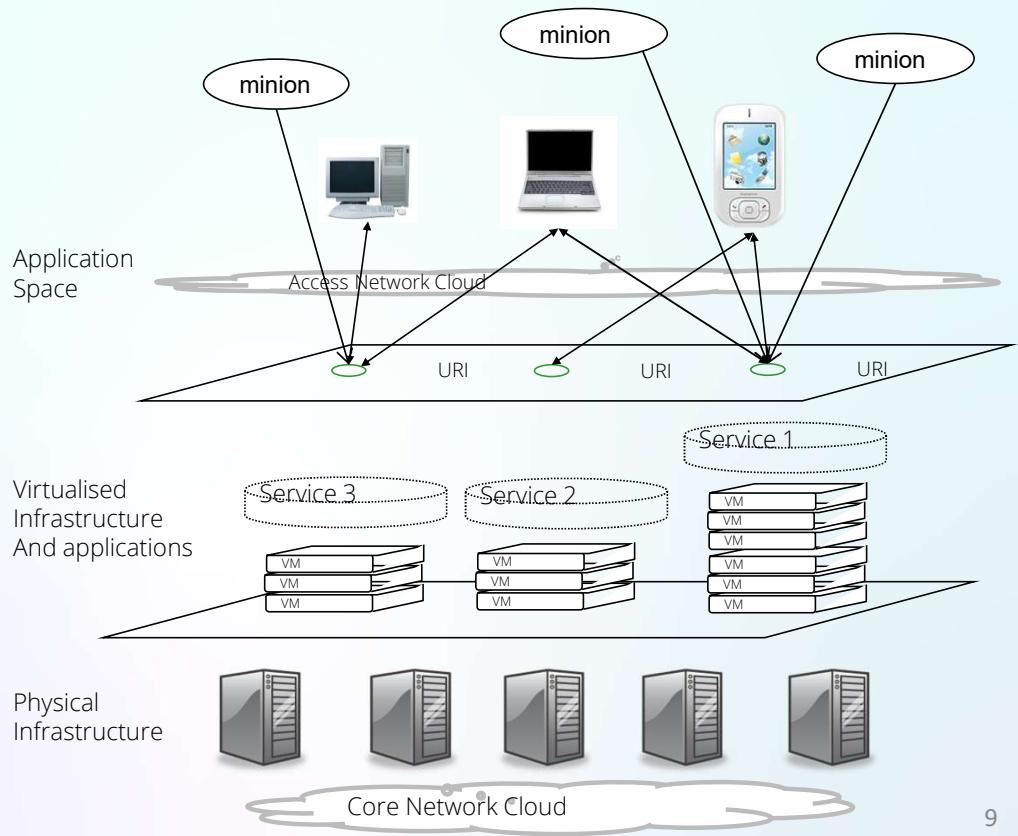


- **Synthetic Transactions / Data Collection**
 - ICMP / HTTP / HTTPS
 - ReST / WS / XML
 - DHCP / DNS / FTP / LDAP / Radius
 - IMAP / POP3 / SMTP / NTP
 - JDBC / JSR160 (JMX) / WMS / WBEM
 - NSClient (Nagios Agent) / NRPE (Nagios Remote Plugin Executor)
 - SMB / Citrix
 - SNMP / SSH / TCP
- **Virtualisation**
 - VMware integration
 - Open Stack (being developed)
- **Service & Network discovery**
 - VMware integration
 - Policy driven Layer 2 network discovery

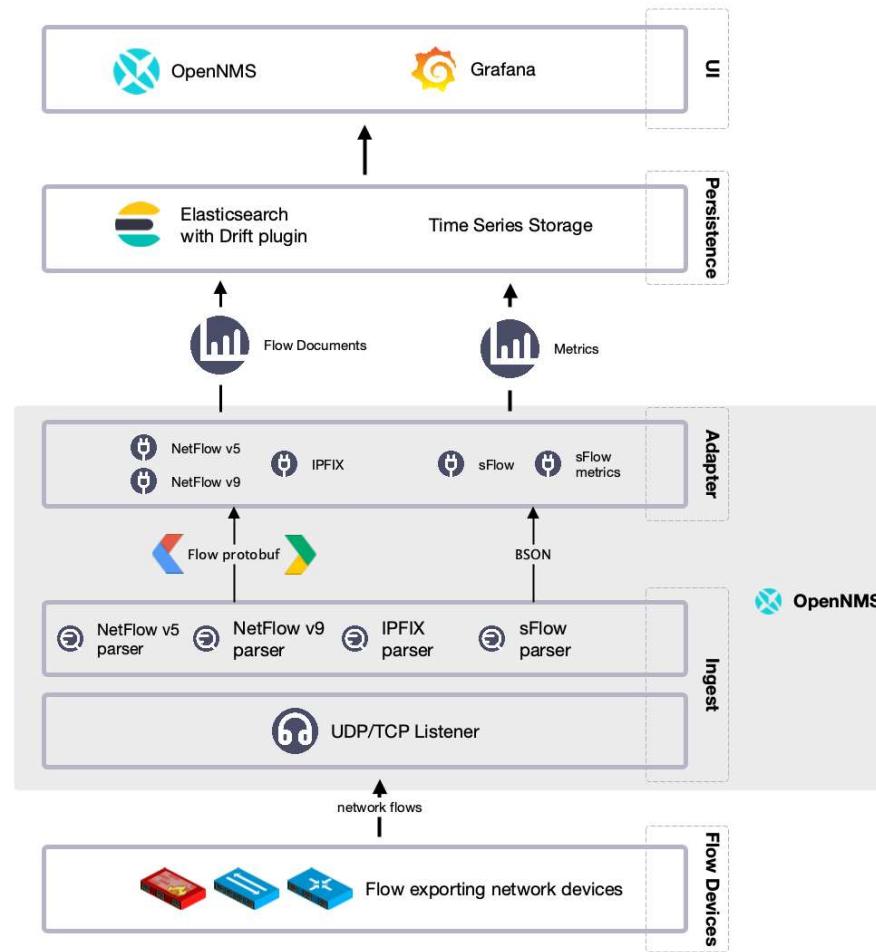
Licensed under Creative Commons

• Remote Minions

- Remotely monitor services from multiple locations



Flow Data Collection



Licensed under Creative Commons

Traffic Analysis (NetFlow)

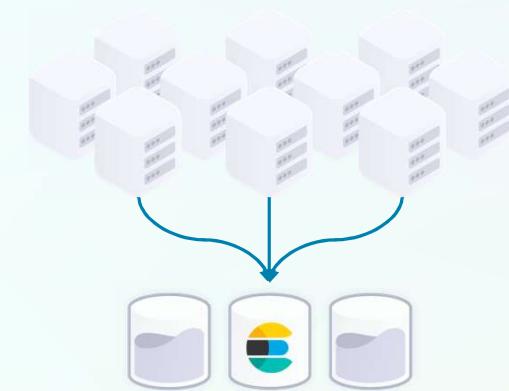
Who's using all the bandwidth?

Single source of truth



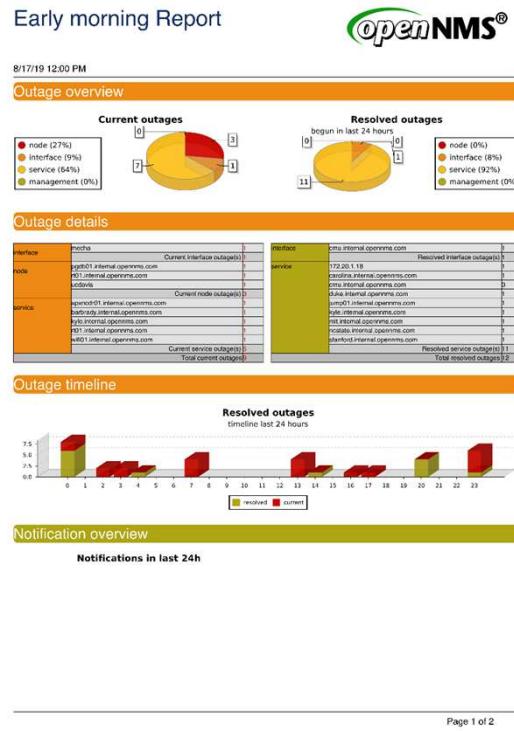
Who's talking to whom?
What are they talking about?

Be the hero when a security incident response team asks,
"Do you have flows?"

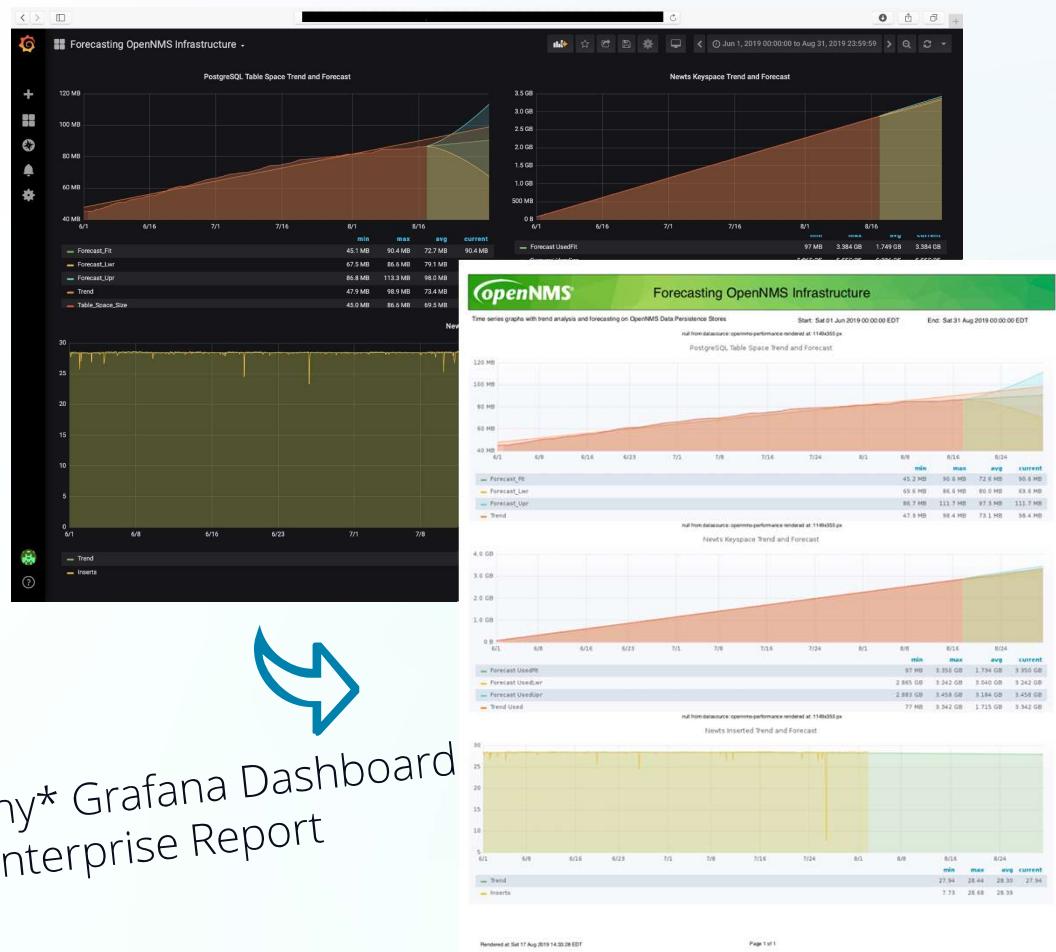


Enterprise Reporting

Early morning Report



Run *any* Grafana Dashboard
as an Enterprise Report



Network Topology

Focal Point Driven Context

Enhanced Linkd Discovery

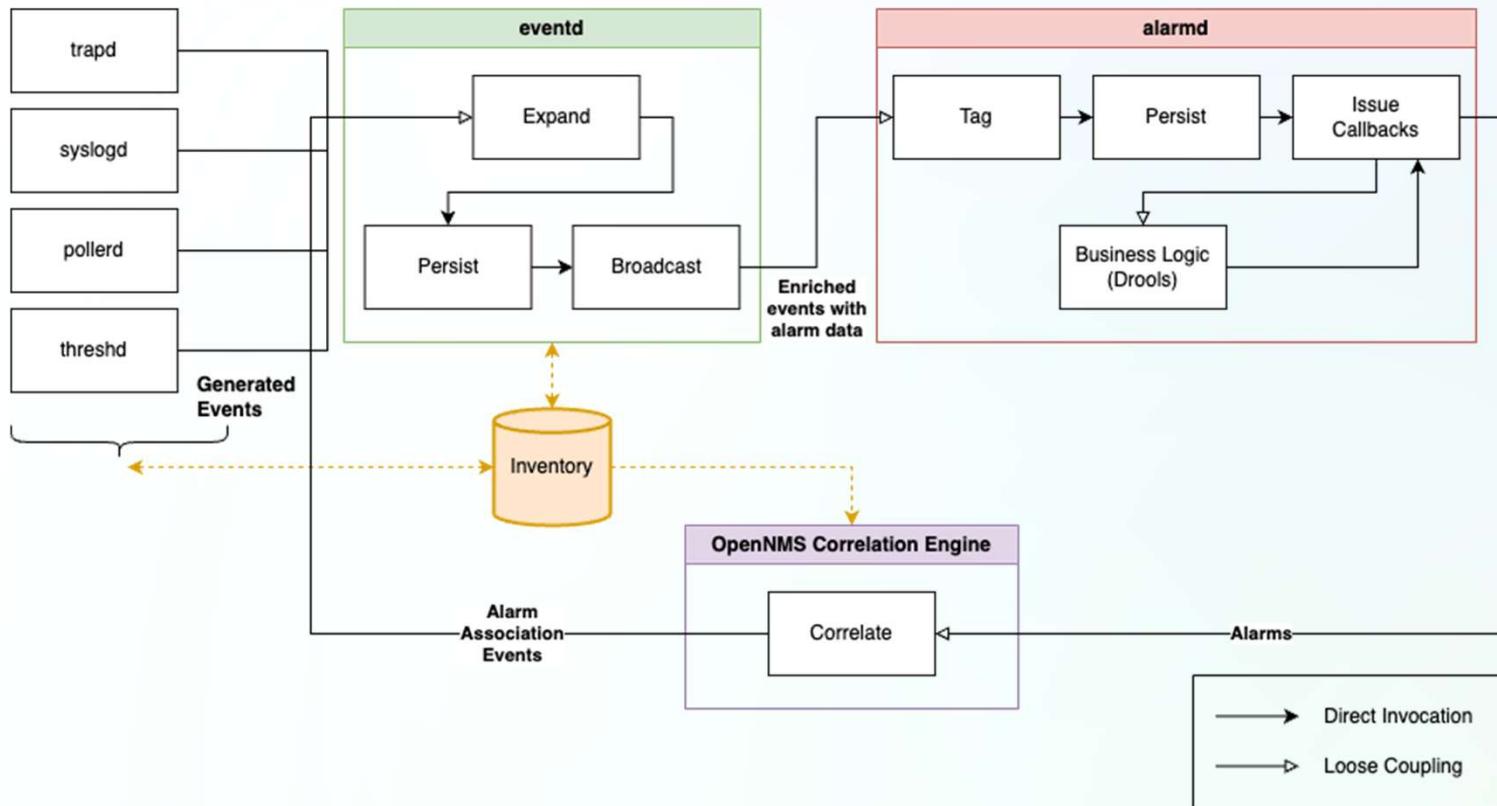
- ospf (layer 3)
- is-is
- cdp
- llldp
- bridge
- other (graph-ml)



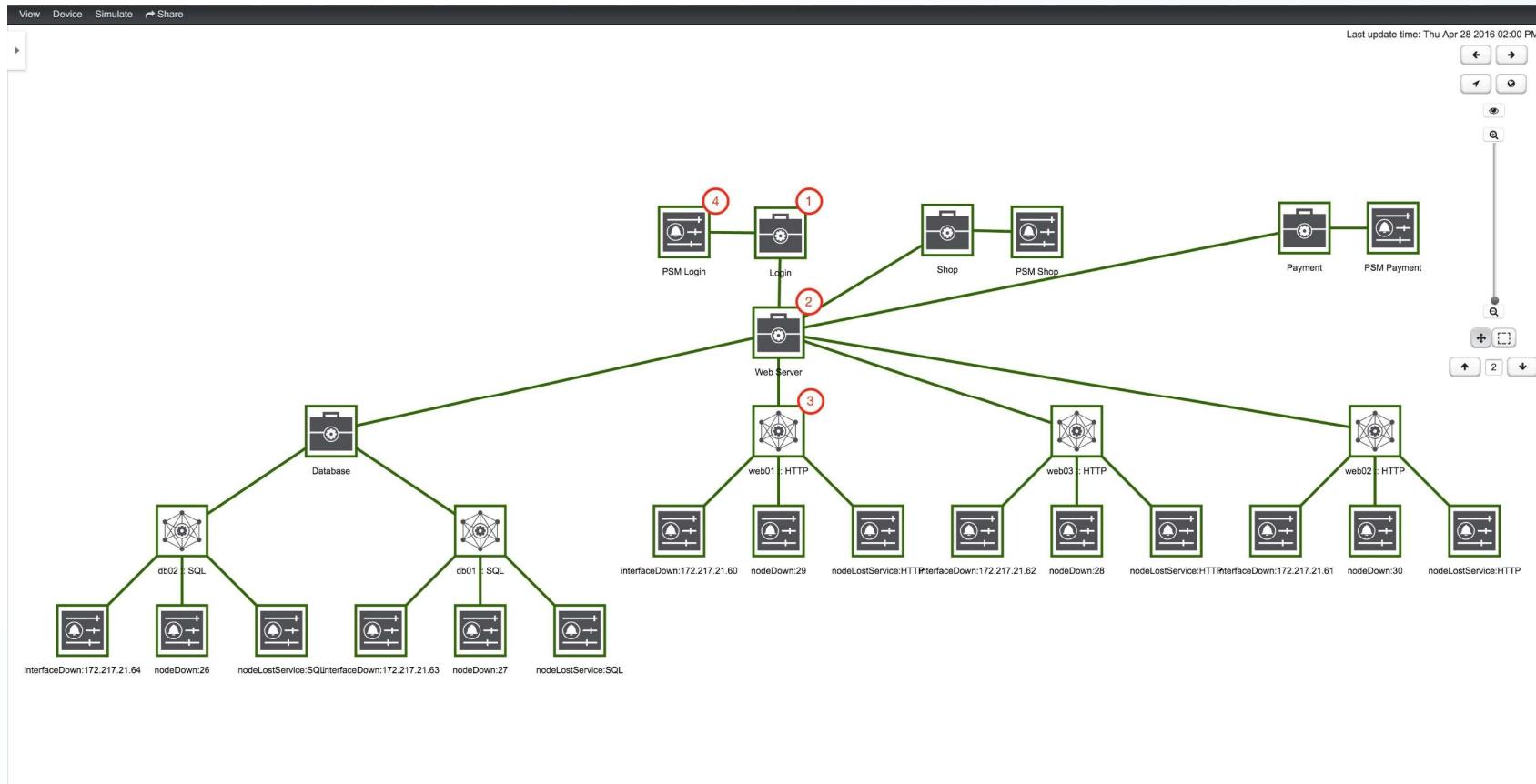
The screenshot shows the OpenNMS Topology Map interface. At the top, there's a search bar with the URL "salesdemo01.opennms.com/opennms/topology#(2),(-2875,-1431,2399,1041),(-1676.0,-911.0),(6A3078B0),(46E597...)" and a navigation bar with links like "Search", "Info", "Status", "Reports", "Dashboards", "Maps", "Help", and "admin". On the left, there's a sidebar with a "Horizon" section showing a timestamp "2021-05-12T13:37:12-04:00", a "Search" field with results for "Nodes: phx-2-25" and "Nodes: PHX-2990-CORE.five3genomics.com", a "Geolocation (32/71)" map, and a "Selection Context" table. The main area is a network topology graph with many nodes and green edges. At the bottom, there's a table titled "Alarms" with two rows:

ID	Severity	Node	UEI	Count	Last Event Time	Log Message
139239	Cleared	phx-2/2-tor2.vpnlocal.five3genomics.com	uei.opennms.org/threshold/highThresholdExceeded	1	2021-05-12T13:32:50-04:00	High threshold reached for service SNMP metric ifInDiscards + iOutDiscards on interface swp9/172.16.253.37
139154	Warning	phx-2/2-tor1.vpnlocal.five3genomics.com	uei.opennms.org/threshold/highThresholdExceeded	8	2021-05-12T13:32:31-04:00	High threshold exceeded for service SNMP metric ifInDiscards + iOutDiscards on interface swp3/172.16.253.36

Event and Alarm Corelation



Business Service Monitoring



Thank you!



OpenNMS