kentik

TOP EAST-WEST DATA CENTER USE CASES

KENTIK DETECT FOR INFRASTRUCTURE

As application and service components become increasingly distributed, east-west traffic is less predictable and bottlenecks are more common. To assure optimal application and service performance, you need comprehensive network intelligence both within and between data centers. Legacy tools summarize data and discard the details, but Kentik Detect delivers deep, big data-powered visibility, offering multiple ways for infrastructure and network operations teams to gain valuable insight. Here's a high-level look at some top application and service use cases.

1 Find top contributors to congestion or capacity issues.

Speed resolution with ad-hoc traffic analyses that identify what's causing hot spots and bottlenecks:
- Drill down into traffic grouped by application-related dimensions such as port and subnet.
- Pivot among dimensions to find outliers that indicate likely root causes.
- See real-time details to inform decisions about suspending or rescheduling non-critical loads.

2 Alert on unusual dips in service traffic.

Set alarms on drop-outs or anomalous dips for critical server and service-port combinations:
- Profile server and service combinations by grouping destination IP and IP ports under 10000.
- Use baselining to determine 25th-percentile traffic volume of top 100 combinations.
- Set alerts to trigger alarms based on a specified magnitude of under-baseline deviation.

3 Alert on anomalous spikes in service traffic.

Receive instant notification of unexpected traffic peaks on critical server and port combinations:
- Profile your server and service combinations by grouping top destination IP and IP ports under 10000.
- Use baselining to determine 98th-percentile traffic volume of top 100 combinations.
- Set alerts to trigger alarms when traffic exceeds historical baselines by a specified magnitude.
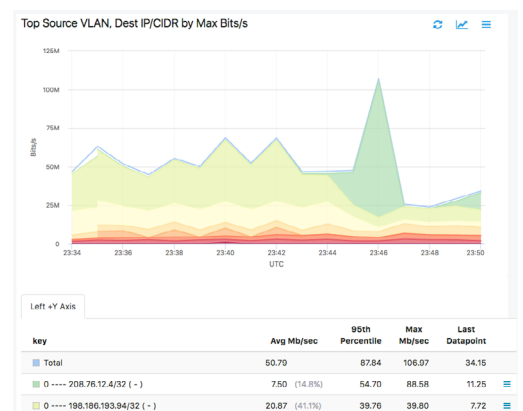
4 Alert on existence of unexpected flows.

Get notifications when unexpected and significant new flows enter your application and service top-N:
- Group source and destination IP pairs and filter for critical application destination ports or specific subnets.
- Baseline 50th-percentile for top N pairs.
- Set alerts to trigger alarms on new pairs in top-N.

5

Reveal the business context of VLAN + subnet flows.

Assess the direct and collateral impact of spikes or congestion on applications on a shared network:
- Define custom columns that map VLAN IDs to services, and subnets to data center names.
- Group by source and destination data center and service traffic.
- Create flow chart and matrix table visualizations that map traffic to infrastructure and key services.
- Set alerts that identify changes to top-N traffic flows between data center and service combinations.

6

Analyze BGP-enabled Clos datacenter traffic.

Assess the impact of spikes or congestion on leaf nodes, as well as the collateral damage in a shared network:
- Define custom columns that map ASNs to leaf-node switches, and subnets to data center names.
- Group by source and destination data center and leaf-switch traffic.
- Create flow chart and matrix table visualizations that map traffic to infrastructure and leaf-node switches.
- Set alerts that quickly identify changes to top-N flows between data center and leaf-switch combinations.
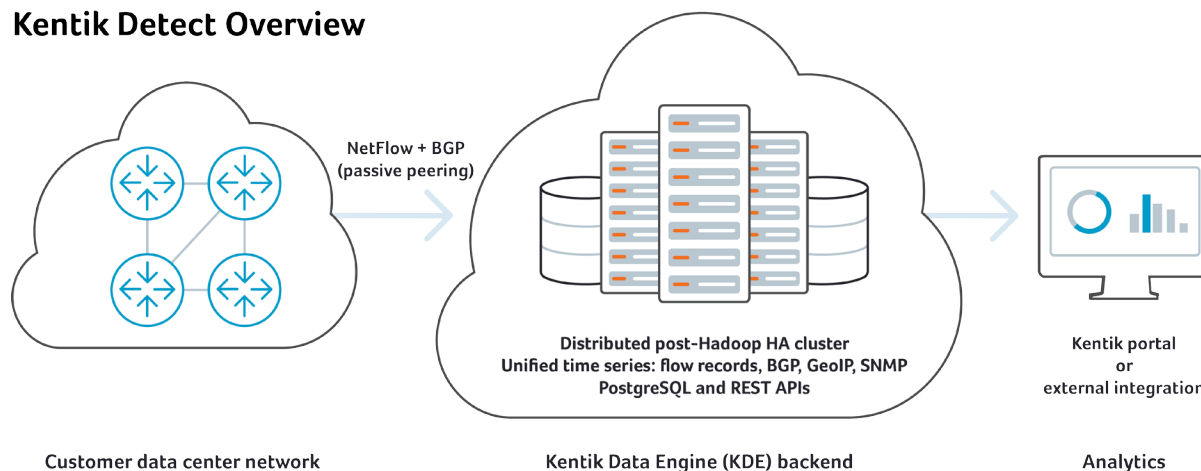
7

Gather key NPM metrics from Kentik's cloud-friendly host agent.

Collect host data for server-contextualized views of key network performance metrics:
- Instrument key servers and load balancers with nProbe agents that collect network performance metrics.
- Examine latency and the percentage of TCP retransmits (see our NPM how-to).
- Build SQL alerts when performance metrics fall outside of specified bounds.

Kentik Detect Overview

NetFlow + BGP
(passive peering)

Distributed post-Hadoop HA cluster
Unified time series: flow records, BGP, GeoIP, SNMP
PostgreSQL and REST APIs

Kentik portal
or
external integration

Customer data center network   Kentik Data Engine (KDE) backend   Analytics

IMMEDIATE VALUE, ZERO OVERHEAD

Kentik Detect is a SaaS. That means you can sign up and register devices in minutes, start seeing results immediately, and forget about extra costs for hardware, software, upgrades, maintenance, developers, and added IT personnel. And Kentik scales as needed, on demand, without limits. Ready to learn more? We'd love to show you our powerful, intuitive portal, hear about your network visibility needs, and discuss how Kentik Detect can help. Contact sales@kentik.com or sign up for a free trial.