Hybrid Cloud and the Network Observability Gap

KENTIK WHITEPAPER

kentik®

kentik

Executive Summary

The widespread use of hybrid cloud infrastructures creates significant challenges for network and infrastructure teams. They're finding it increasingly difficult to fully understand and control what's happening in complex networks that span data centers and public/private clouds. This lack of visibility leads to a network intelligence gap, which threatens network reliability and quality, service-level agreements (SLAs), application performance, and the quality of end-user experiences. Bridging this intelligence gap not only enhances the performance and stability of these networks but helps the organizations that rely on them to achieve their digital transformation goals.

Business Drivers for Hybrid Clouds

Organizations of all types and sizes have put a high priority on continuously improving the digital experience for their end-users. Whether it's a physician accessing a radiology image, a consumer placing an online order, a manufacturer streamlining its supply chain, or a university conducting classes remotely, organizations are racing (and occasionally stumbling) to implement digital strategies.

With senior management of many organizations pushing for digital transformation, IT departments are evolving from a cost center to a source of revenue and competitive advantage. At the same time, they are under stringent mandates to deliver services with greater efficiency and productivity.

To fully capitalize on the promises of digital transformation, IT leaders recognize that a hybrid mix of cloud and data center infrastructure can provide several business advantages, including increased agility, greater cost efficiencies, and better customer experiences.

BY 2024,

50%

of network operations teams will be required to re-architect their network monitoring stack, due to the impact of hybrid networking, which will be a significant increase from 20% IN 2019

Hybrid Cloud is the Reality for Network and Infrastructure Teams

As network and infrastructure teams take on more strategic responsibilities to meet the demands of digital transformation, they are pulled into managing complex hybrid cloud architectures. Managers of traditional data centers are building their own private clouds even as they actively cede a portion of their operations to public clouds, driven by software, platform and infrastructure services.

Gartner, which estimates worldwide revenues for public cloud services at $266 billion in 2020[1], bluntly says "cloud computing is firmly established as the new normal for enterprise IT."[2]

But despite growing adoption, both public and private clouds have their drawbacks. According to research by International Data Corporation (IDC),[3] a global provider of market intelligence, they found the top three challenges of public cloud services were security, application performance and costs/

billing. That's why 86% of enterprises reported they were considering bringing back one or more applications from the public cloud to on-prem deployments.

Private clouds, IDC added, also have their challenges: high operating costs, limited availability of higher-level services, and inability to scale quickly. So, while the industry buzz may be about "cloud-first" strategies, the vast majority of organizations deploy some kind of "hybrid cloud" strategy that mixes traditional data center operations with private cloud infrastructures and public cloud services. Organizations are by no means abandoning their on-prem operations. Rather, hybrid cloud infrastructures are being implemented to meet the evolving digital transformation mandates for IT.

Using traditional network management tools, network professionals charged with tracking down bandwidth, performance, and availability problems struggle to piece the network together in time to fix critical issues. It's difficult to discover which devices and interfaces make up a data path. Correlating the traffic, health, and performance of these elements consumes valuable time that could instead be spent understanding and fixing problems.

IDC[4] concludes that "a mix of public and private clouds (can) create a best-of-breed IT environment." And according to the 2020 Flexera State of the Cloud Report,[5] 86% of respondents to its survey "...said they're incorporating multiple public clouds while 60% reported using more than one private cloud. The most common combination is a mix of various public and private clouds, with 53% taking this approach" (Figure 1). A mere 1% reported using only a single private cloud (Figure 2).

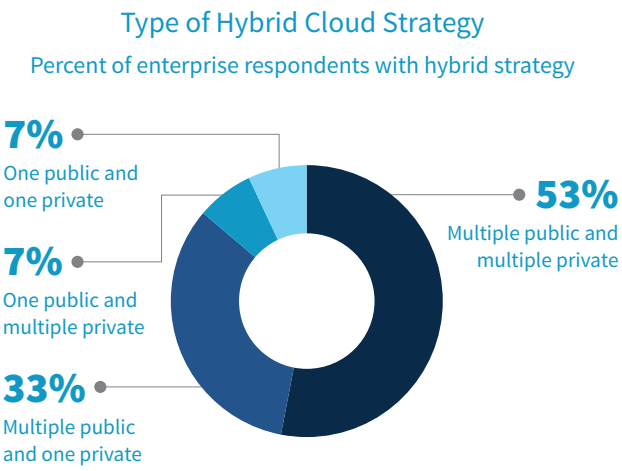

Figure 1

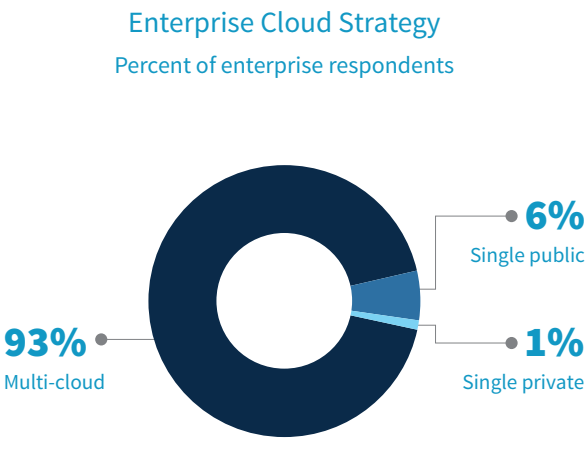

Figure 2

Source: Flexera 2020 State of the Cloud Report

Hybrid Clouds and Networking

The ongoing reinvention of IT impacts all infrastructure layers, from bare metal to end-user applications, data center devices to IoT sensors. But of all the infrastructure changes under way, arguably the most profound are taking place in networking.

This is because networks are changing in the volume of traffic they carry, the variety of applications they support, and their strategic value to the business. For decades, data networks were perceived as behind-the-scenes "plumbing" that drew the attention of a handful of specialists. Today, a network (more often a network of networks) is now fully embraced as a strategic foundation that drives entire lines of business and sources of revenue.

59%

of respondents who answered a question about COVID-19 expect cloud use to exceed plans due to the pandemic, according to the 2020 Flexera State of the Cloud Report.

On top of this, the COVID-19 pandemic has brought home the importance of voice, data, video and streaming services around the globe. Imagine an even greater impact the pandemic would have had on society and commerce if there hadn't been ways to order goods online, work or study from home, and stay in touch with friends and relatives.

A highly functional, reliable, secure network has never been a higher global priority. For organizations of all types and sizes, networks are no longer viewed as just a line item on a departmental budget.

Modern digital enterprises understand that their long-term competitiveness depends on leveraging their IT assets to create exceptional user experiences. In response, business managers and infrastructure leaders are expanding their definition of "network performance" from reactive monitoring of flat networks to a global awareness of the entire infrastructure, software and platform ecosystems of the cloud.

But if they are to deliver on expanded expectations of network performance, network and infrastructure engineering teams need greater visibility into these complex hybrid cloud infrastructures. Gartner[6] observes that "new dynamic network architectures are affecting the efficacy of traditional network monitoring stacks," and predicts that "by 2024, 50% of network operations teams will be required to re-architect their network monitoring stack, due to the impact of hybrid networking … a significant increase from 20% in 2019."

Network and infrastructure engineering teams are caught in a vice: They are expected to deliver networks with ever-higher levels of functionality, reliability, performance, and security while having to cope with the complexity and uncertainty caused by the division of resources between private and public clouds and legacy data center facilities.

Five Issues Network and Infrastructure Teams Need to Address in the Era of Hybrid Clouds

For network and infrastructure teams to address and thrive in the era of hybrid clouds, they need to adapt to these five things:

1. Clouds and data centers can have very different architectures

As more and more applications are moved to the public or private cloud or are natively built in the cloud, the increased use of containers and microservices is fundamentally changing the visibility and flow of network traffic. Accenture notes, "As a result of digital decoupling and the adoption of microservices, applications are evolving to more complex patterns and topologies, increasingly requiring more dynamic underlying compute, storage and networking infrastructure. Cloud-native patterns and technologies are typically more ephemeral than traditional environments."[7]

As such, monitoring tools are forced to engage alternative telemetry methods to gain visibility into container-to-container traffic by leveraging APIs from orchestration tools and mesh services. In addition, they need to ingest new types of data (such as VPC flow logs and NSG VNet flow) to monitor flows between services in different virtual cloud subnets.

Distributed architectures to accommodate microservices are also changing the intra-data center traffic topology, creating a highly dynamic network between services and tiers. According to Cisco's Global Cloud Index[8], east-west traffic will represent 85% of total data center traffic by 2021, and north-south traffic will account for the remaining 15% of traffic associated with data centers.

Cisco Annual Internet Report (2018–2023) White Paper reported that Global Cloud Index projects cloud traffic to represent 95% of total data center traffic.[9] BY 2021

In view of this, it's important to recognize that data center architectures are highly dynamic. Network architecture upgrades, device upgrades, acquisitions, and changing business priorities mean that all data centers are unique. As a result, each needs to be accurately described by network performance tools so network and infrastructure teams can have a fighting chance to do their job effectively and support the organization's mission.

And not only are public cloud architectures different from private clouds and data centers, there are differences between public clouds. Dealing with more than one cloud provider is not at all unusual. A Gartner survey of public cloud users found that 81% of respondents said they were working with two or more providers.[10] And the Flexera State of the Cloud Report found that enterprises employed an average of 2.2 public and 2.2 private clouds.

This change in the IT landscape — where applications, data and users fluidly interact — means network and infrastructure teams cannot use siloed legacy monitoring tools. Why not?

Data center architectures are radically changing to accommodate new paradigms like containerized microservices while still supporting legacy apps, incorporating mergers and acquisitions, and keeping pace with advancing technology. This requires an investment in new tooling to bridge visibility

gaps. For instance, when microservices are deployed in the cloud, network and infrastructure teams cannot simply assume that the cloud infrastructure runs perfectly all the time and does not require monitoring. Quite the opposite is true. When hybrid environments are involved, network and infrastructure teams are responsible for the entirety of the application delivery and user experience across all infrastructures and networks. That's why fragmented tooling is inadequate. This is yet another example of how strategic IT decisions (like moving to the cloud and adopting containerization) sometimes are made without fully considering and understanding the impact on network requirements and monitoring capabilities.

2. Highly diverse toolsets and increased vendor complexity

While monitoring connectivity within and between on-prem, internet and WAN infrastructures is a traditional capability of network performance monitoring and diagnostic (NPMD) solutions, the addition of cloud-specific network management solutions from public cloud providers creates an unmanageable number of tools and vendor complexity.

According to a survey of IT professionals reported in "The State of Cloud Monitoring,"[11] 35% of respondents use up to five monitoring tools to keep tabs on hybrid cloud and multi-cloud environments. Each tool has a specific purpose — device health, synthetic performance monitoring, traffic flow metrics, packet data capture, etc. — and thus tells only an isolated portion of the story.

The same research found that nearly 70% felt "public cloud monitoring is more difficult than monitoring data centers and private clouds," and a stunning 95% said they had experienced one or more performance issues caused by a lack of visibility into the public cloud. Only 19% said they had all the data they needed to monitor a hybrid network (compared to 82% who had enough information to monitor their on-prem network).

3. Network and infrastructure teams have no single view of network activity across a hybrid infrastructure

There are backbone network maps, capacity maps between sites and devices, cloud visualization maps for a specific cloud, and edge maps for WAN/SD-WAN edge networks. But there is not a consolidated, fully integrated map focused on the performance, health and traffic analytics needed to operate a hybrid cloud network.

With applications and data shifting between on-prem and cloud environments — and the absence of a single point of observability — there are gaps in visibility, leading to gaps in network intelligence.

With applications and data shifting between on-prem and cloud environments — and the absence of a single point of observability — there are gaps in visibility, leading to gaps in network intelligence.

The bottom line is that hybrid clouds are complex and difficult to work with, and here's why: Using traditional network management tools, network and infrastructure professionals charged with tracking down bandwidth, performance and availability problems struggle to piece the network together

in time to fix critical issues. It's difficult to discover which devices and interfaces make up a data path. Correlating the traffic, health, and performance of these elements consumes valuable time that could instead be spent understanding and fixing problems.

Automation, orchestration, and software-defined networking further complicate matters by constantly shifting where applications are located and redefining how they connect to one another. Without tooling built to comprehend this new reality, the network — and those who run it — are at a disadvantage.

4. Limited visibility leads to decreased agility

Visibility and intelligence gaps created by separate network monitoring and diagnostic tools slow down troubleshooting, increase infrastructure engineering burn-out, and prevent proactive operations by keeping the team consumed with reactive tasks.

Fragmented apps lead to increased risk of outages, reachability issues, errant traffic flows, increased cyber threats, impact from unknown dependencies, and other threats to network stability. Network and infrastructure teams can't troubleshoot as fast as necessary when apps and data have moved to the cloud.

Even as networks are ever-more critical to business success, network operations are becoming increasingly complex, with disruptions intrinsically harder to foresee and to recover from.

These visibility gaps create an agility gap that:

- Undermines mean time to resolution (MTTR) with disparate and uncorrelated data
- Diminishes analytics intelligence that could be used for automation and prevention
- Increases the chances of operator error from always working in reactive mode

Even as networks are ever-more critical to business success, network operations are becoming increasingly complex, with disruptions intrinsically harder to foresee and to recover from.

5. Network and infrastructure teams are in danger of falling behind in meeting their organizations' increased expectations

Network and infrastructure managers are largely left out of decisions about the balance between on-prem and cloud deployments. Decisions about moving to the cloud are usually made for reasons of cost containment, flexibility, business agility, and efficiency. They are seldom, if ever, made with consideration of the impact on network and infrastructure teams as regards to network performance monitoring.

As a result, network managers are presented with a *fait accompli*: manage a new — and more complex — environment that few, if any, IT staff have experience with.

Given these realities, it's easy to see why network engineers and operators face a daunting challenge. New engineers come into an environment without context and the maps available to them don't provide any. Yet, speed to insight for a new data center network engineer is critical. Incumbent engineers, meanwhile, can't keep up with all the changes, and the tools they have don't reflect or accommodate the new and constantly evolving environment.

Compounding the challenge are business pressures to optimize operations across multiple infrastructures, especially when the business is migrating from data centers to clouds, acquiring additional infrastructures through mergers and acquisitions, and/or integrating with legacy systems.

Looking Ahead

If infrastructure engineering teams are to meet the increasingly high expectation being placed on them, they need to adopt a proactive approach to meeting the challenges posed by hybrid cloud environments.

And, they need the right kind of tools. Most helpful would be a comprehensive, integrated platform that provides visibility across public/private clouds, on-prem networks, SaaS apps, and other critical workloads as a means of delivering compelling, actionable intelligence. It would be a single place to go for network maps that help operators visualize — in real-time — every aspect of their network and keep track of changes to their infrastructure.

Hybrid cloud networking is just one of the areas where Kentik's Hybrid Map helps NetOps professionals increase their network intelligence and visibility to deliver value in support of their organizations' goals. Visit www.kentik.com for more information or contact a sales representative at sales@kentik.com.

Endnotes

1 https://www.gartner.com/en/newsroom/press-releases/2019-11-13-gartner-forecasts-worldwide-public-cloud-revenue-to-grow-17-percent-in-2020#

2 https://www.gartner.com/smarterwithgartner/4-trends-impacting-cloud-adoption-in-2020/

3 "The Power of the Hybrid Cloud Strategy," Chris Kanthan and Deepak Mohan, May 2019

4 *Op. cit.*

5 https://info.flexera.com/SLO-CM-REPORT-State-of-the-Cloud-2020

6 "Market Guide for Network Performance Monitoring and Diagnostics," March 2020

7 *Op. cit.*

8 https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

9 https://www.cisco.com/c/en/us/solutions/executive-perspectives/annual-internet-report/index.html

10 https://www.gartner.com/smarterwithgartner/why-organizations-choose-a-multicloud-strategy/

11 https://about.keysight.com/en/newsroom/pr/2019/25mar-nr19044-ixia-c-r-state-cloud-monitoring.pdf

ABOUT KENTIK

Kentik® is the network intelligence platform for the connected world, trusted by leading digital enterprises and service providers. With Kentik, businesses eliminate the visibility and intelligence gaps associated with running dynamic and complex networks, and achieve greater network performance, reliability and security. The Kentik Network Intelligence Platform ingests diverse data streams from the internet, edge, cloud, data center and hybrid infrastructures and provides real-time visualizations and AIOps-powered insights and automation. Learn more at kentik.com.

Products from Kentik have patents pending in the US and elsewhere.

kentik®

Revised 20201119