riverbed

Solution Brief

Network Visibility for AWS and AWS GovCloud

Enterprise digital transformation is the leading factor driving greater public cloud engagement today.[1] In fact, more than half of global enterprises rely on "at least one public cloud platform to drive digital transformation and delight customers."[2]

As a result, cloud has grown in usage and is now a central, integral component of the enterprise network and application strategy. An almost ubiquitous 96% of enterprises are using cloud today, and 81% have a multi-cloud strategy.[3] In fact, enterprises can trace 45% of all network traffic to external, public cloud applications.[4]

The Visibility Challenges

The distributed, ephemeral nature of cloud applications makes the challenge of managing performance extremely difficult. Migrating legacy systems and applications to the cloud, all while customers are demanding fast, flawless performance can be a daunting task.

The transition to cloud must be managed carefully to ensure service continuity. Public cloud infrastructure as a service (IaaS) has obvious benefits – scalability, availability and agility to name a few. However, when it comes to monitoring in the cloud, it is often unclear who is responsible.

As applications migrate to the cloud, communication between the end user and server no longer flows within your organization's boundary, but leaves the perimeter and heads off to the cloud service provider's infrastructure. Anything outside your network perimeter can be a huge visibility blind spot.

In a highly demanding digital world, where slow is the new off, IT organizations are expected to deliver consistently high levels of performance and end-user satisfaction for cloud apps. It may be difficult to identify and troubleshoot performance problems due to visibility gaps between the network, applications and end-user.

Service provider SLAs end at the edge of the cloud. Yet IT organizations are still responsible for the overall performance of the network and applications. You need the ability to set, manage, and deliver on network and application performance SLAs that extend through the cloud to your end users.

Hybrid Visibility

Enterprises have come to depend on network performance monitoring (NPM) solutions to identify blind spots across their traditional enterprise networks, in virtual environments, and now in the cloud.

[1] LogicMonitor's Cloud Vision 2020: The Future of The Cloud Study

[2] Forrester's Predictions 2018: Cloud Computing Accelerates Enterprise Transformation Everywhere

[3] Rightscale 2018 State of the Cloud Report

[4] EMA, Network Management Megatrends 2018, April 2018

In fact, network visibility is more important in cloud environments than ever before. At the same time, it's a challenge to implement in the cloud because you don't have access to the physical network infrastructure. Riverbed provides two ways to understand what's happen in the cloud from a network perspective: high-level end-to-end visibility with flow and deep-dive performance troubleshooting with packets.

Let's dig into detail on both to determine what you can see and how you achieve visibility with each option:

Packet-based Cloud Visibility

Packet visibility is essential for identifying and remediating performance problems in the cloud. It enables real-time and historical monitoring and troubleshooting of both network and application performance.

Riverbed AppResponse Cloud provides rich network and application visibility into AWS and AWS GovCloud West. It enables you to:

- Quickly pinpoint the cause of performance degradations and high latency in your cloud network through analysis of throughput, errors, retransmissions, connections, resets, etc.
- Quickly determine if an issue is caused by network or server delay using detailed response time analysis
- Automatically identify 2000+ applications. Identify worst performing apps, busiest apps by: highest server turns, round trip time, resets, bandwidth usage, etc.
- Collect and store all packets and view each transaction using patented TruePlot™ technology to quickly identify trends and patterns in behavior
- Aggregate traffic by applications, users, servers, clients, conversations, and host groups for faster, easier analysis
- Packets are stored directly on the AppResponse Cloud to enable fast triage and diagnosis of intermittent and hard-to-solve performance issues. You can also export packet-based flow metrics to SteelCentral NetProfiler for consolidated analysis of your hybrid environment.

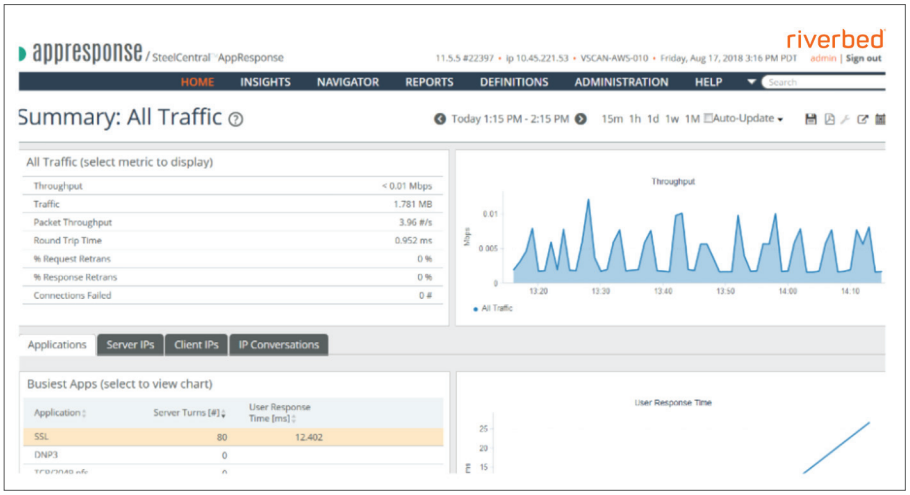

Figure 1
SteelCentral AppResponse Cloud looks and acts just like the on-prem version of AppResponse.

SteelCentral AppResponse Cloud can be deployed in combination with physical and virtual SteelCentral AppResponse appliances to provide seamless, end-to-end network and application analysis across your on-premises, virtual, and cloud environments.

Packet Telemetry for AppResponse Cloud

SteelCentral AppResponse Cloud can obtain packets in the cloud in a variety of ways, including:

- **SteelCentral Agent**, installed on a virtual server in an Amazon EC2 instance, it captures raw packets in the cloud and mirrors them to SteelCentral AppResponse Cloud for analysis. SteelCentral Agent can also convert packets into SteelFlow, a Riverbed extension of NetFlow, and send the flow data to SteelCentral NetProfiler for enterprise-wide network analysis.
- **AWS VPC traffic mirroring** lets you natively copy network traffic at any Elastic Network Interface (ENI) in your Virtual Private Cloud (VPC), and send it to SteelCentral AppResponse Cloud for analysis.
- **Cisco CSR 1000v** is an example of a cloud router that uses **ERSPAN** to mirror the traffic on one or more source ports then encapsulate and route it across a switched network using GRE encapsulation to an instance of AppResponse Cloud running in your AWS VPC.
- **Packet aggregator agents or sensors** use Layer 2 GRE tunneling or encrypted P2P to mirror traffic to a virtual Network Packet Broker which can aggregate, filter, optimize, and distribute the traffic to AppResponse Cloud.

AppResponse Cloud Telemetry		
	AWS	AWS GovCloud
SteelCentral Agent	Yes	
AWS Traffic Mirroring	Yes	Yes
Gigamon GigaSECURE Cloud	Yes	Yes
IXIA CloudLens	Yes	
Cisco CSR ER-SPAN	Yes	Yes
Big Switch Big Cloud Fabric	Yes	

AppResponse Cloud can get packet telemetry from the above solutions, as well as support AWS (see AWS brief).

Flow-based Cloud Monitoring

Riverbed flow monitoring provides a hybrid view of your network performance. It enables you to see your cloud and on-premises resources in the same views so you get a truly end-to-end perspective on network and application performance.

Riverbed NetProfiler analyzes flow traffic from the core, to the branch, to the cloud for an enterprise-wide view of performance. It discovers all assets, map dependencies and monitors network and application services, regardless of where they sit.

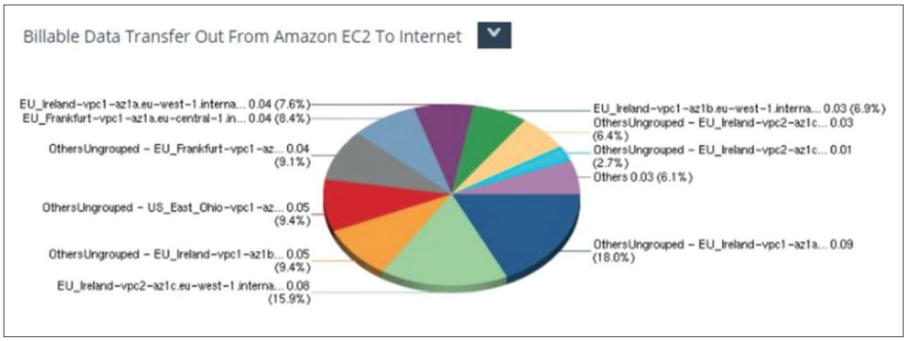

Figure 2
SteelCentral NetProfiler reports on "Billable data transfers from Amazon EC2 to Internet" to help you understand where you are incurring costs.

NetProfiler can be deployed in AWS and AWS Government (West). It can also be deployed in Azure and in Azure Government and in virtual and physical appliance form factors for easy multi-cloud and hybrid cloud monitoring.

NetProfiler cloud-specific workflows include:

- What apps are running in the cloud?
- How's the cloud network performing?
- Who's talking to whom
- Traffic diagrams that show how traffic flows through the network
- Understand where you are incurring costs

Whether you're selecting which applications to migrate, planning the move, or monitoring network and application performance, NetProfiler offers rich visibility to make your cloud transformation a success.

SteelCentral NetProfiler can receive flow from a number of flow cloud solutions:

- **AWS VPC flow logs** provide information about IP traffic going to and from network interfaces in your VPC. It logs traffic on 10 to 15-minute intervals
- **SteelCentral Agent** also converts raw packets into SteelFlow data, Riverbed's enhanced version of NetFlow, and sends it to your SteelCentral NetProfiler for analysis. SteelFlow enriches NetFlow v9 with application names, latency, and retransmissions information.
- As noted, **SteelCentral AppResponse Cloud** also sends SteelFlow to NetProfiler.

NetProfiler Cloud Telemetry		
	AWS	AWS GovCloud
SteelCentral Agent	Yes	
AppResponse Cloud	Yes	Yes
AWS VPC Flow Logs	Yes	Yes

NetProfiler runs in AWS and AWS GovCloud West, as well as Azure (see Azure brief).

NetProfiler is available as a physical, virtual, or cloud appliance.

Benefits of Riverbed NPM in Hybrid Environments

Having one seamless visibility solution across your data center, the Internet, and cloud providers, helps you understand the impact performance issues have on your business. With Riverbed, you gain:

Ubiquitous cloud visibility. Deploy in Azure and AWS multi-cloud or hybrid environments.

Deploy in the cloud with confidence. Get the same proven performance monitoring in the cloud and on-premises.

Decreases downtime. Reduce diagnosis time by using the same rich analytics and proven workflows across hybrid and multi-cloud environments to locate trouble spots quickly.