



# 4 BEST PRACTICES FOR MONITORING CLOUD INFRA- STRUCTURE YOU DON'T OWN.

Gone are the days of businesses owning their own software and hardware and keeping it all on premises in data centers.

And even though cloud computing is not a new way of doing business, technology leaders are finally embracing and harnessing its potential by beginning to move non-business critical applications to the cloud.

This trend has picked up significantly in the last five years, and now, more than ever, the cloud is gaining momentum. At tech conferences, in customer meetings and in boardroom discussions, cloud storage and compute is no longer a conversation for tomorrow. It's an imperative for today.

But this migration begs the question, "How do you monitor something you no longer own?" Moving resources to the cloud can create significant visibility gaps over your infrastructure performance.

In this whitepaper, we'll examine use cases for monitoring hybrid cloud infrastructures and best practices for ensuring delivery of applications and services in the cloud.



## RAPID PACE OF CLOUD ADOPTION.

451 Research recently reported that – out of 570 enterprise organizations interviewed – 35 percent said they increased their cloud budget from 2014 to 2015. In that same time frame, 50 percent said their budgets remained the same, and only 14 percent decreased their cloud budgets.

In Q1 of 2015, 451 Research polled 1,593 enterprise organizations, asking them to explain what they use cloud storage for. Sixty two percent said they use it to host Software as a Service (SaaS) applications.

Nearly half of all respondents use it for an on-premises private cloud; 34 percent use it to host a private cloud; 32 percent use it for Infrastructure as a Service (IaaS) and 25 percent use it for Platform as a Service (PaaS).

Your organization has likely transitioned or is in the process of transitioning some applications to the private, hybrid or public cloud for a myriad of reasons – broad network access, resource pooling, on-demand self-service, rapid elasticity or measured service, for instance.

With such a marked shift in where organizations run their applications, the time is now for leaders to evaluate how they can use infrastructure monitoring to ensure cloud-run applications are operating properly for customers.





## BEST PRACTICE 1

### Monitor Cloud and On-Premises Infrastructure from a Single Platform

Businesses have expectations for the performance of their on-premises infrastructure. But now they must utilize that existing infrastructure and the new cloud infrastructure as one. This often presents problems.

However, with a sophisticated monitoring platform, organizations can pull in third-party data – from Amazon Web Services (AWS), Microsoft Azure, IBM Bluemix and others – from the cloud. Just make sure you get a monitoring platform that can marry the metrics collected via the cloud platform's API with your existing infrastructure metrics collected via SNMP, IP SLA, or other standard protocols.

#### You'll want to monitor the following KPIs:

- Network KPIs will inform you about the bytes sent and received on the instance network interface.
- CPU KPIs will monitor estimated CPU utilization for the current billing period at the time of last collection.
- Billing KPIs will tell you the estimated credit balance, credit usages, and charges accrued for the current billing period at the time of last collection.
- System Integrity KPIs will let you know if the system instance, customer instance or system has failed.
- Storage KPIs will give you data on the length and number for Write Operations per collection cycle on an EBS Volume.

It's important to get a monitoring platform that can take this cloud data and "normalize" it alongside the traditional metric, flow, and log data the business is accustomed to working with. The right monitoring platform will treat cloud metrics the exact way it treats data from other sources. That means you can monitor, baseline, alert, and report on the data, regardless of the source. It also makes problem correlation much easier.

When your data is uniform across whatever objects and devices you're monitoring – whether they're in the datacenter or in the cloud – you have complete visibility into your network and applications.



## Use Case: Monitoring AWS


A leading mobile carrier company, until recently, was relying on AWS CloudWatch – a monitoring service for AWS cloud resources and applications that runs on AWS.

In September 2015, leaders made the decision to test the cloud by offloading some of their less-critical, internal IT applications to it. In the meantime, the company is maintaining an application in the data center. However, if the cloud proves beneficial, they will rely on the cloud alone for some of these applications.

The company decided to test the cloud for two reasons – cost and ease of implementation. Every time a version of an application changes, the IT department spends a lot of time and energy working on fixes and upgrades that are not core to the business.

Recently, however, the company's IT department said they have zero visibility into how the applications they are moving to the cloud are behaving. The CloudWatch API works somewhat well to provide insight into what's happening on the cloud, but the mobile carrier already monitors other devices and doesn't want to have to check two monitoring platforms to know the health of its applications.

By adding the monitoring platform's AWS adapter, the mobile carrier company can continue to receive routine monitoring data and metrics for datacenter-hosted applications, along with AWS metrics on the same dashboard.





## BEST PRACTICE 2

### Monitor, Trend and Alert on Cloud Resource Consumption

While leveraging the cloud provides unparalleled access to scalability and agility, it also results in IT losing direct control and visibility. Simply measuring cloud service availability isn't enough.

Organizations must measure consumption levels (especially KPIs used for billing), as well as the impact of cloud service access on the rest of the infrastructure. They also need to ensure their cloud-based resources are keeping up with what the business needs to evolve.

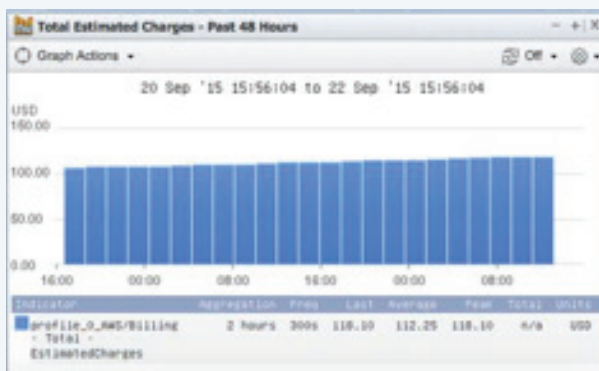
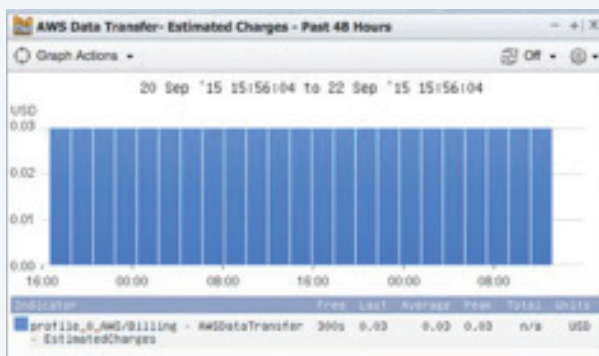
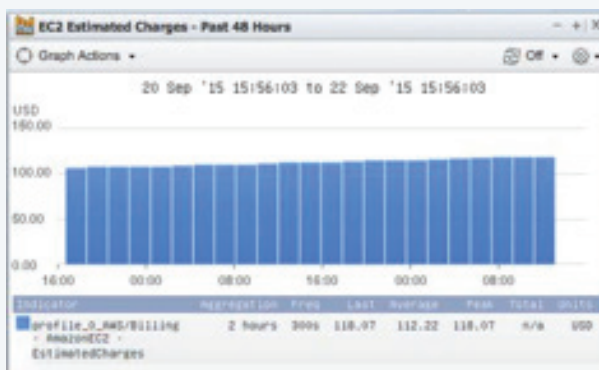
Billing charges are another unique metric that can be obtained by monitoring AWS. With the AWS adapter, businesses can keep track of the estimated EC2 charges, data transfers and total monthly charges they expect during any given month.

AWS adapter KPIs can inform users of the estimated credit balance for the current billing period at the time of last collection, estimated credit usage for the current billing period at the last time of collection, and estimated charges accrued for the current billing period at the last time of collection.

This can be critical if they require alerting on such metrics to keep costs under control. Also, when a business has planned capacity and has estimated their charges – if their estimates differ from reality – these metrics would provide an early warning.

And since all metric, flow and log data is treated the same in a sophisticated monitoring platform, businesses can baseline and set alerts to be prepared for any kind of spike or drop in services needed.

*In addition to monitoring AWS compute and storage, you should monitor, trend, and alert on your cloud resource consumption to ensure monthly usage remains in line with your budget.*







## BEST PRACTICE 3

### Monitor the End User Experience

Monitoring is most valuable when leaders know exactly what the end user is experiencing when he or she uses an application that is run in the cloud.

When your platform seamlessly syncs with an end user experience tool, the result is powerful. The end user experience tool will give sophisticated, detailed and specific response times for how and when users interact with an application on the cloud.

An adapter that has the ability to tap into end user experience testing shows how the network is being utilized. The adapter combines these advanced metrics with the other metric, flow and log data to provide the whole picture of digital infrastructure performance.

Organizations that use this adapter can customize alerts to meet their own needs and goals. For instance, they could get alerts when users from a particular region are experiencing slow response times for a critical business application – while analyzing infrastructure metric, flow and log data at the same time.

Again, the power is in the data. You'll want a sophisticated monitoring platform that can accept the response time data and feed it back through the system as familiar, recognizable data. With uniform metric, flow and log data, the IT department can set alerts and act quickly if an issue arises.

Some IT departments have engaged in IPSLA testing to measure the response times from a user to an application. With this information, IT can see how long it took the end user to load a page and other information about network performance in real time.

However, end user experience monitoring is more advanced and can deliver the same metrics with more confidence because the data can be delivered on the same dashboard and in the same way other tools and devices are monitored.



## End user experience monitoring use case

Back to our mobile carrier company – which will soon add the end user experience monitoring adapter for added visibility as it is now offloading some of its non-business critical applications to the cloud.

This carrier is accustomed to its applications behaving in a certain way. In the datacenter, the organization typically knew what to expect from applications and could easily predict response times.

But as the business makes the transition to the cloud, it must maintain that same level of monitoring precision, and it certainly needs to be able to compare how application A functioned in the datacenter versus how it's now behaving in the cloud.

The organization says it wants proactive, end-to-end visibility over the traffic between its datacenters, and also from the datacenter to the cloud. The carrier plans to use end user experience monitoring to synthetically replicate what the user is experiencing. If service is slow or degraded, the IT department can drill down into the performance monitoring data to find where the issue is and why it happened.

Whether applications are supported in data centers or in the cloud, there is a huge dollar impact on the company when they're not responding, not functioning, or not functioning well.

Again, a monitoring platform that also gathers end user experience monitoring data is ideal. While end user experience monitoring and an IPSLA test are similar, end user experience monitoring can show stats on a hop-by-hop basis.

With this data in hand – which is automatically translated into the same kind of metric, flow and log data the carrier already understands and utilizes from its monitoring dashboard – the organization can baseline data and proactively alert on it, providing a complete end-to-end view of its network both in the datacenter and the cloud.





## BEST PRACTICE

## 4

### Integrate Metrics, Flows and Logs for a Complete View

When your network lives in a multi-vendor environment, it's essential that your monitoring platform treat data from different vendors and places equally.

You're not just getting the cloud metrics, or just the end user experience flow data. You need all of this data to work together. The value of having a sophisticated monitoring platform is its ability to turn all of this different data into uniform metrics, which you can baseline, alert and trend on. These uniform metrics can provide a data point about an event, that you can compare with other data points.

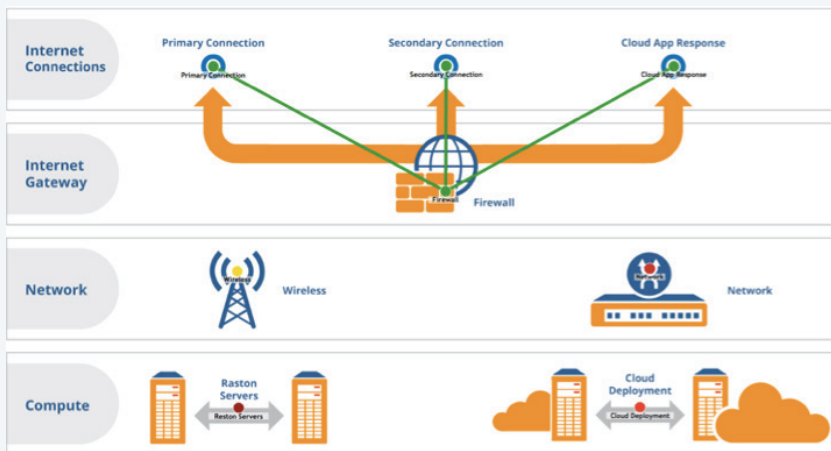
Metrics give us the what; flow data tells us who; and log data tells us why. During your organization's transition to the cloud, it's hard to imagine only having one of the pieces of the data puzzle to rely on.

Transitioning to the cloud is a big step, and your business needs to have the full data picture – integrated metrics, flows and logs – to tell the story of your journey from the datacenter to the cloud.

#### Get a Holistic View of Your Cloud Deployment

Consider this scenario: your organization hosts a document repository application and wants to deploy it to the hybrid cloud. Keeping in mind that an employee may access the application from office headquarters or from a remote location, what components should you monitor to ensure consistent application delivery?





**Application deployment:** You are hosting the application as an internal wiki solution, but also expose some portions to your customers. You host a local version at your Virginia datacenter, which is accessed by internal employees who work at the local offices.

**Datacenter deployment:** The Virginia location is your primary datacenter, but you have a full disaster recovery site located in San Francisco. This allows you to provide business continuity in the event of a disaster at the primary site. There is a constant replication of the application occurring from Virginia to San Francisco.

**Compute:** On the bottom left of our status map, you'll see the internal Virginia servers. On the bottom right – indicated with clouds – you'll see the AWS cloud-deployed servers. Status maps allow the user to upload custom images to logically or physically depict the environment to provide a holistic view.

**Network:** You'll see the infrastructure that provides users and applications accessibility to one another. Wireless utilizes laptops and other wireless-enabled devices; the physical network infrastructure provides wireless infrastructure connectivity for those using desktops and hardwired solutions.

**Internet / Gateway connections:** You'll see the gatekeeper or Internet firewall, and from here, you'll monitor additional nodes, which are tied to synthetic tests and the first hop of each provider. The links between the hops represent individual interfaces on the firewall that provide the physical connectivity. The last indicator provides data from synthetic tests to the border of the internal application server, as well as the external instances of the application. This allows for troubleshooting issues, and pinpointing where they may be occurring within the environment.

**Two alert summaries:** Alert summaries are broken up between on-premises equipment and cloud deployments. A sophisticated monitoring platform will aggregate on device instead of showing detail in order to force a user to utilize a monitoring report as part of a troubleshooting workflow. Your monitoring platform should not just be an alerting engine, but a powerful reporting platform.



## CONCLUSION.

When monitoring cloud deployments, you need to be able to depend on the data to ensure your business' application and service delivery. An advanced monitoring platform will treat data from both the datacenter and the cloud in a normalized fashion, supplying your IT department with a single integrated view.

When your monitoring platform can hook into cloud platform performance metrics and end user experience data, you have a complete, end-to-end view of your network. And that's what you need to successfully run your business as you transition from your on-premises datacenter to the hybrid cloud.



## About SevOne.

SevOne provides the only digital infrastructure performance monitoring solution engineered for Speed at Scale for the world's most demanding service-delivery environments. The patented SevOne Cluster™ architecture leverages distributed computing to monitor any device in the service-delivery path, integrating performance metrics, flows and logs at scale, and providing answers in seconds to prevent performance-impacting outages. SevOne's global customer base includes 5 of the 7 top global investment services companies, enterprises, CSPs, MSPs and MSOs. SevOne is backed by Bain Capital Ventures and was named a Visionary in Gartner's 2015 Magic Quadrant for Network Performance Monitoring and Diagnostics. More information can be found at [www.sevone.com](http://www.sevone.com) and SevOne's video channel and community, The Network Project. Follow SevOne on Twitter at @SevOneInc.