



WHITE PAPER

How to Securely Migrate to the Cloud



sumo logic

Cloud Migration Challenge

Over the past several years, enterprises and government entities of all sizes have been enthusiastically supplanting their on-premise servers with information processing resources provided by major cloud computing vendors. There are numerous justifications for these wholesale migrations, ranging from diminished capital outlays to the heightened scalability and agility that are the hallmarks of on-demand computing.

To their dismay, however, many organizations discover that their cloud computing initiatives don't deliver the anticipated results; in some cases, the entire undertaking stalls. There's rarely a single culprit for such undesirable outcomes. Instead, these failures usually stem from a combination of factors such

as unaddressed security exposures, performance shortfalls, neglected regulatory compliance, or user resistance. Even successful cloud computing projects are routinely plagued by the challenges of untangling complex, intertwined applications and an overall lack of visibility into their original computing environment.

To gain visibility throughout your environment, there are helpful strategies and tools at your disposal to analyze the mass amounts of data being generated. This is particularly true for those enterprises with the foresight to establish a baseline prior to the initiative and then compare it with the same metrics captured after the transition: essentially, these efforts act as an "insurance policy" to help mitigate risk.

Instead, these failures usually stem from a combination of factors such as unaddressed security exposures, performance shortfalls, neglected regulatory compliance, or user resistance.

What You'll Learn

In this paper, we depict five specific scenarios where using a machine data aggregation and analytics platform such as Sumo Logic can be an invaluable aid as you prepare to carry out a shift from on-premise to cloud computing:

- 01** Planning for the Migration
- 02** Monitoring Application Performance
- 03** Validating Security
- 04** Assuring Compliance
- 05** Establishing Crucial Key Performance Indicators (KPI)

This paper is intended for anyone dedicated to ensuring that his or her organization's passage from on-premise to cloud computing proceeds as smoothly as possible. This community ranges from IT leaders such as DevOps and security executives to individual contributors responsible for architecture, software delivery, and safeguarding the new environment.

Sumo Logic Overview

Sumo Logic is a comprehensive, born-in-the-cloud machine data analytics solution with over 2,000 paying customers. Each day, these clients employ Sumo Logic’s extensive analytics features to derive insight from more than 100 petabytes of raw log data aggregated in the platform. Greater than 75% of Sumo Logic’s clientele themselves rely on cloud computing technologies to perform key information processing responsibilities; a significant portion of these enterprises also utilize hybrid and multi-cloud vendor frameworks.

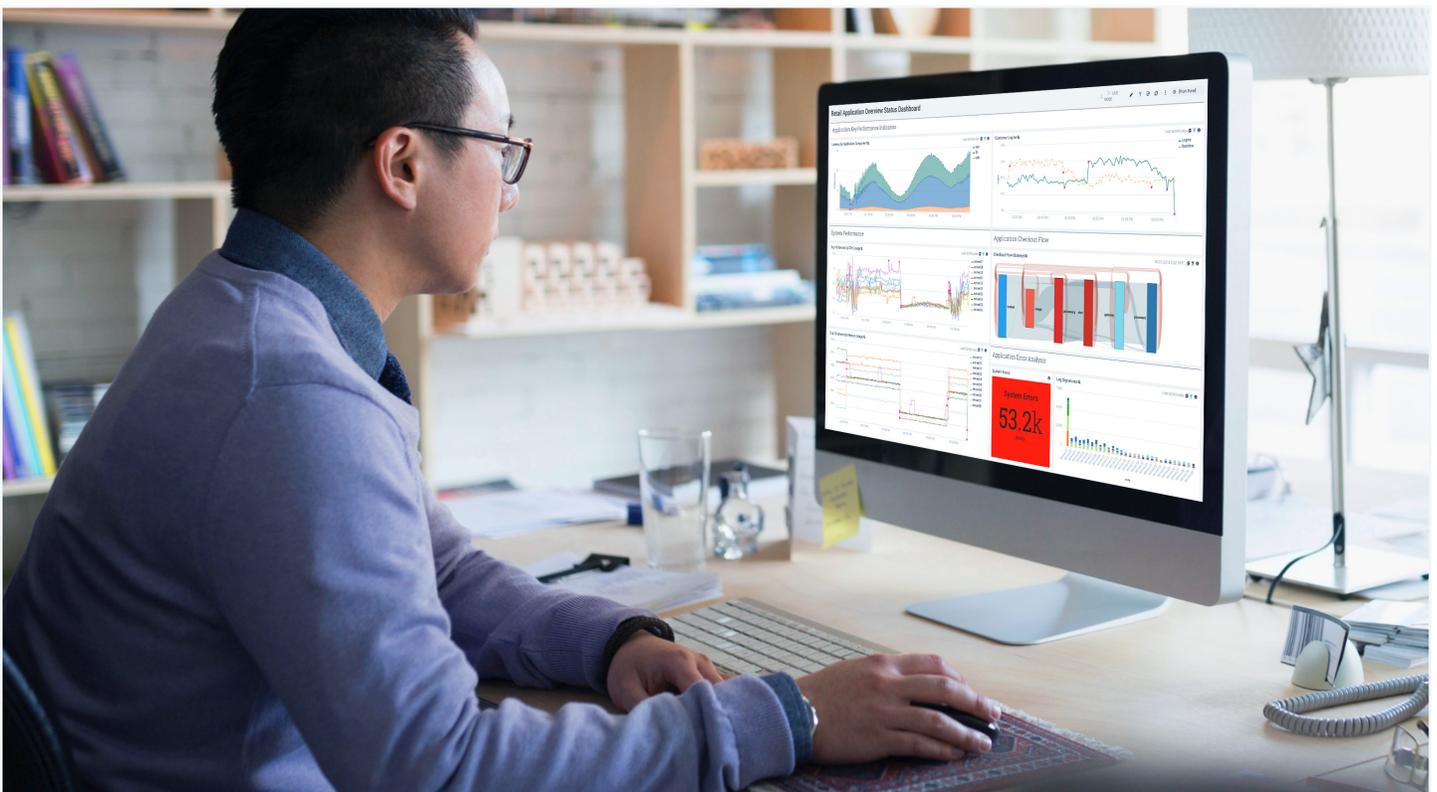
Regardless of their exact computing topography, all of Sumo Logic’s customers profit from how it extracts meaning from their machine data. These observations furnish greater visibility into the entire computing landscape, aid in IT management, and monitor the state of the organization’s performance, security, and regulatory compliance.

Using Sumo Logic in concert with the machine data that it gathers, organizes, and analyzes is especially applicable if you’re contemplating a transition towards cloud computing. Whether your organization will be following a either “lift-and-shift” or re-architecture strategy, properly

understanding machine data can help steer the transformation and confirm that the resulting environment is living up to expectations.

Getting started is easy - as a Software as a Service (SaaS) solution, Sumo Logic lets you take advantage of its cloud economics. This means that you can launch the initial deployment for minimal cost - ideally before the computing relocation project gets started - and can scale to whatever degree is necessary to support the venture. This is in stark contrast to legacy on-premise log management applications (both open source and proprietary) that compel you to make major investments in hardware, staffing, and other resources from the very beginning.

Beyond their hefty expenditures, existing on-premise log management tools just don’t translate well to modern cloud computing environments. They have difficulty coping with its scale and scope, vastly different resource composition, enormous data volumes, altered processes, more stringent regulations, and novel security threats. In comparison, Sumo Logic is a cloud-native offering that was designed – from the beginning – as an affordable, secure, and highly scalable solution meant for the unique realities that are encountered in cloud computing.



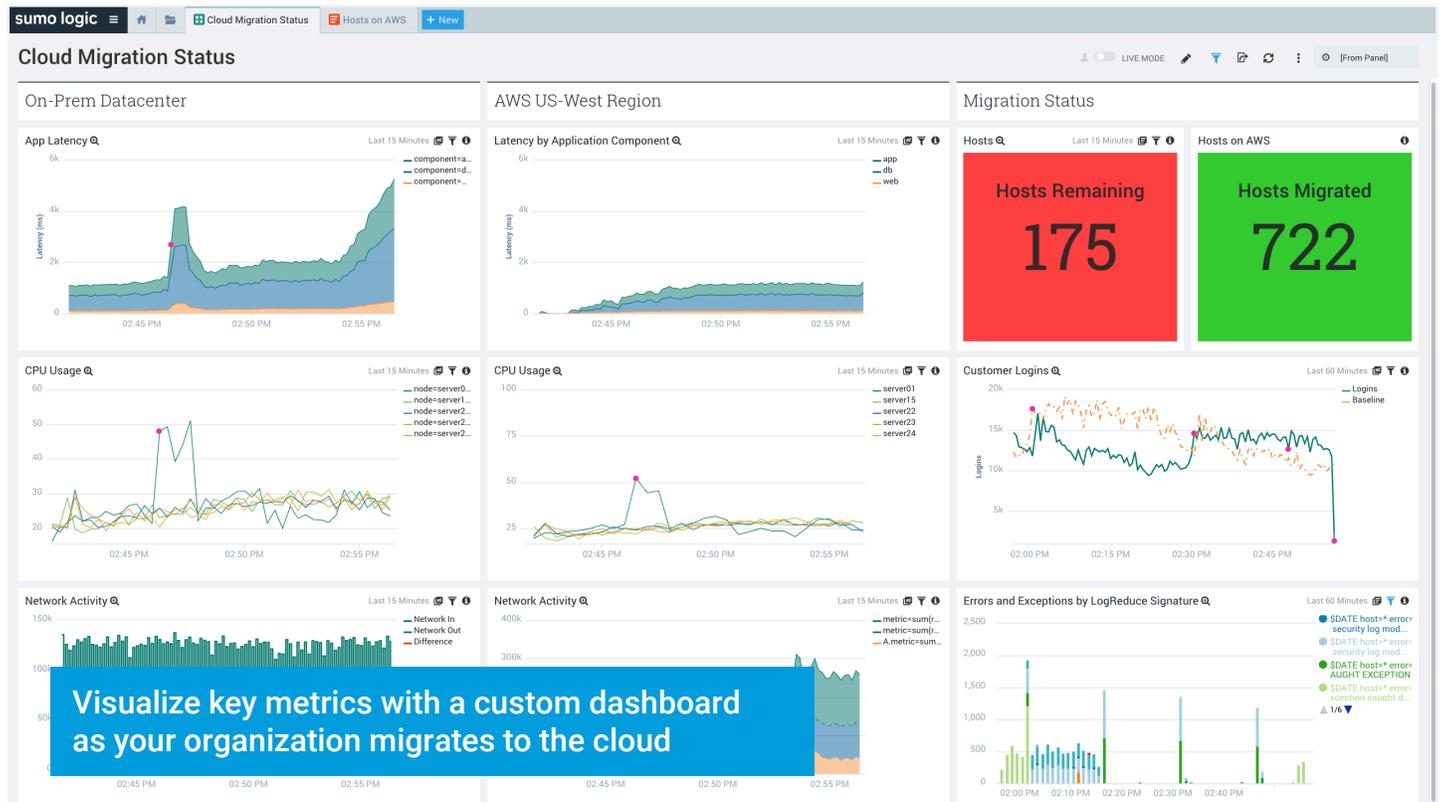
In the next sections, we discuss five distinct scenarios where machine data and Sumo Logic can help you chart a course from on-premise information processing to cloud computing.

01 Planning for the Migration

A major percentage of enterprises preparing to relocate some or all of their computing resources to the cloud conduct a thorough assessment – either internally or with assistance from a third party consultancy – that catalogues their current technology assets, business processes, application code, and so on. Other organizations follow a different approach and bypass these studies to simply concentrate on preparing the destination to receive the transfer. Unfortunately, in both cases it’s far too easy to omit important details and then be forced to correct these issues after the conversion.

Even the most prepared enterprise commonly doesn’t ordinarily pay much attention to the often-gargantuan amounts of machine data that are being generated each day as byproducts of routine operations. This is unfortunate, because the information concealed in these raw log files can offer precious clues that will help yield:

- A comprehensive inventory of servers, applications, and supporting technologies
- The connections among applications





- Accurate data transfer volumes
- Cross-application dependencies
- Performance challenges and hidden latencies

Machine data can also aid in arriving at meaningful metrics and thresholds that you can then evaluate once the relocation is complete. This will help you confirm that the initiative is meeting its objectives, and that nothing has been forgotten. These benefits are available regardless the approach you're taking: for "lift-and-shift" migrations, machine data can help visualize how all of the applications interact. For re-architecture projects, machine data can aid in determining how microservices and containers should interact.

When it comes to working with machine data, it's much more effective to automate the job of gathering and analyzing this information: if you attempt to manually review logs, you'll find that it's a tedious, time-consuming, and error-prone chore. This is another strong argument in favor of deploying a solution such as Sumo Logic prior to the changeover. Getting started is simple: enabling Sumo Logic's machine data collectors is easy, and will begin adding value on the first day.

02 Monitoring Application Performance

You already have plenty of tools for monitoring the low-level resources (e.g. CPU, disk, network, and storage) that power your applications, whether they're hosted on-premise or in the cloud. Although this information is a useful indicator of base system health, it sheds minimal light on the state of the applications, their responsiveness, and if they're encountering errors.

On the other hand, machine data can fill in the missing details to provide an all-encompassing picture of everything in your data center, including inspecting information flow through your servers as well as carrying out load monitoring and testing.

You can attain even deeper awareness if you first gather and review this information in the current on-premise configuration and then later once the transfer to the cloud has taken place. By combining system-level resource observations with application monitoring, you can uncover over or under-provisioning in the new environment.

Sumo Logic works equally well examining applications whether they're on-premise or in the cloud. This means that it's easy to 'flip the switch' and continue to monitor them once they've made the move. This results in a seamless experience that preserves the same operational procedures while fine-tuning the journey to the cloud. It offers out of the box monitoring for these major cloud computing platforms:

- Amazon Web Services (AWS)
- Microsoft Azure
- Salesforce.com
- Google Application Engine (GAE)
- Pivotal

Sumo Logic also offers built-in features that can identify differences before and after the transition. It's able to compare machine data across domains by acquiring log status in the initial environment and then comparing it with the destination. The results can be delivered programmatically as well as visually via dashboards. This information is useful not only for catching and correcting errors, but for performance monitoring and security too.



03 Validating Security

Keeping applications and their data safe is a vital responsibility at all times. Of all the things that can go wrong - or simply be neglected - when migrating to the cloud, security is at the top of the list. There are many reasons for this potentially dangerous situation. First, transitioning to the cloud means that it's no longer sufficient to only secure the on-premise environment: it's now necessary to consider internal vulnerabilities as well as those introduced by the cloud vendor. These types of inquiries go far beyond merely auditing applications and their servers and include determining:

- Who has access to the cloud platform?
- What are their permissions?
- How long will these privileges be in effect?
- What activities are being carried out?
- Who is performing these activities?
- What are the organization's policies?
- Are they being enforced?

Assuming that the vendor will handle all security and compliance tasks is one of the most common mistakes made by customers progressing to cloud platforms. This is not the case, however. The reality is that cloud platform providers deliver security and compliance using a 'shared responsibility' model. This means that they're charged with operating, managing, and securing numerous assets such as the physical locations where the servers reside, the host operating systems, and the virtualization layer. As the customer, it's your job to look after the operating system, application software, firewalls, and other security-oriented technologies.

Machine data has a major role to play in securing your information-processing environment before, during, and after the move to the cloud. Specifically, its analytics and machine learning capabilities can speedily digest huge volumes of raw log data to pinpoint potential vulnerabilities.

Deploying a machine data solution before the change is especially wise. First, this immediately helps establish good policies and procedures for safeguarding your current environment. It will then uncover any new exposures introduced while the conversion is underway: for example, numerous enterprises permit relatively open network access to aid in the changeover, and then forget to close these gateways and ports. After the switch, you'll be well positioned to continuing securing your new cloud assets, including removing the new risk vectors embodied in the cloud platform itself.

Of all the things that can go wrong - or simply be neglected - when migrating to the cloud, security is at the top of the list. There are many reasons for this potentially dangerous situation.

Setting up a **machine data-driven compliance** baseline before the shift takes place is a superb technique to protect your enterprise. First, it will immediately **uncover existing conformance violations and gaps**, which you can then resolve in your current on-premise environment and carry forward into your cloud computing destination. This strategy demonstrates **'continuous compliance'**, which will be very helpful during the inevitable regulatory audits to come.



04 Assuring Compliance

No matter what industry your organization serves, there’s an excellent chance that it’s subject to an imposing number of regulations. A small selection of the most noteworthy decrees includes:

- Payment Card Industry (PCI)
- Health Insurance Portability and Accountability Act (HIPAA)
- Sarbanes-Oxley (SOX)
- General Data Protection Regulation (GDPR)

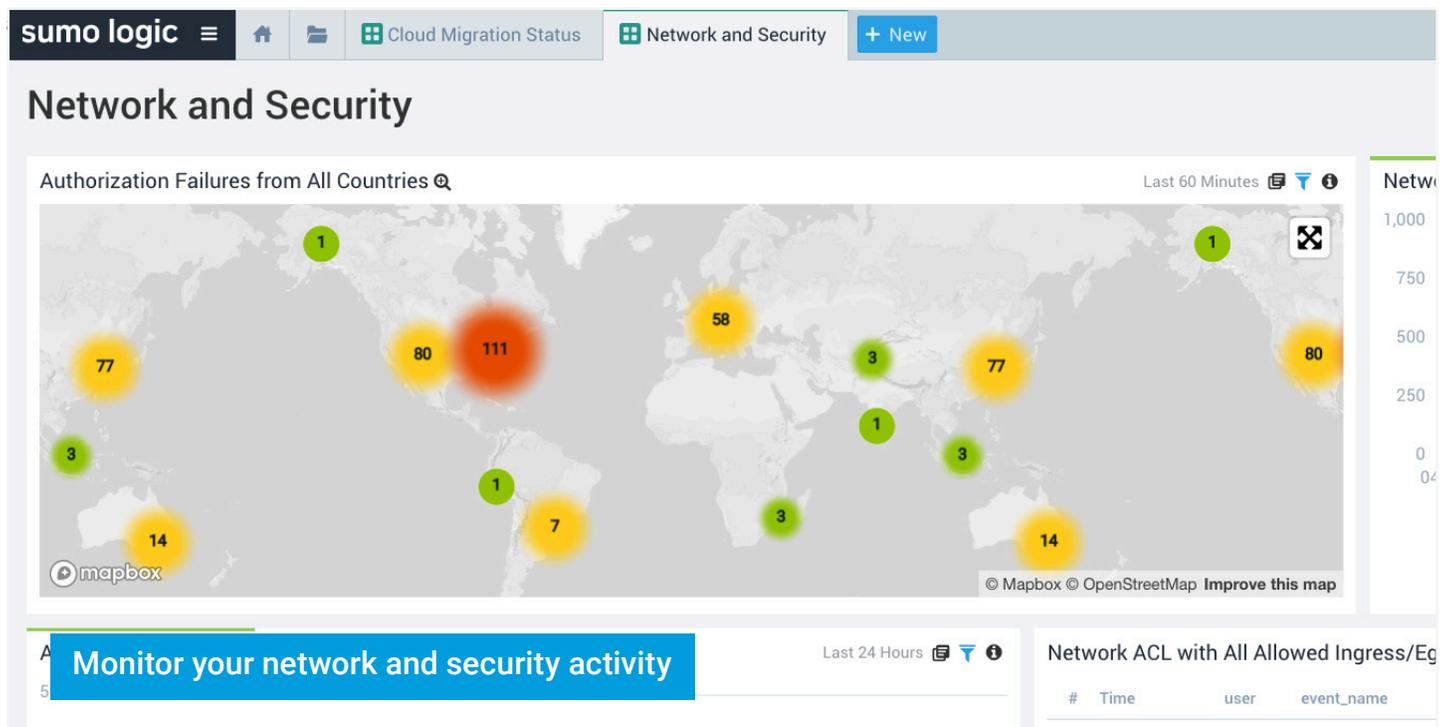
This is just a tiny sample of a much larger collection. Additionally, existing rules are constantly updated; new statutes are frequently created too. Failing to keep up with these requirements has serious implications, including potential civil and even criminal penalties.

It’s tempting to imagine that migrating from on-premise to cloud computing eases these regulatory burdens, but in many instances distributing your technology assets across remote locations actually increases your commitments. Along with potential new regulations, the post-transition environment ushers in a fresh set of possible

these new realities introduce new ways to inadvertently violate your compliance obligations.

For example, a major characteristic of many of these rules entails determining - and restricting - which people have access to resources, information, and so on. This can be a major headache to police when your assets reside on-premise. Things get much more difficult once you’ve changed over to the new cloud platform, where a rogue operator can silently carry out nefarious activities ranging from unauthorized data access to redirecting your traffic with a flip of a switch.

Setting up a machine data-driven compliance baseline before the shift takes place is a superb technique to protect your enterprise. First, it will immediately uncover existing conformance violations and gaps, which you can then resolve in your current on-premise environment and carry forward into your cloud computing destination. This strategy demonstrates ‘continuous compliance’, which will be very helpful during the inevitable regulatory audits to come.



05 Establishing Crucial Key Performance Indicators (KPI)

As we pointed out earlier, there are plenty of incentives for enterprises to make the journey from on-premise to cloud computing. Some are enticed by the prospect of slashing capital expenditures and replacing them with smaller, more predictable operational outlays. Others are drawn to the streamlined administrative responsibilities that cloud computing promises. Profiting from the limitless elasticity and scalability inherent in cloud computing is a key motivator for organizations subject to more variable information processing needs.

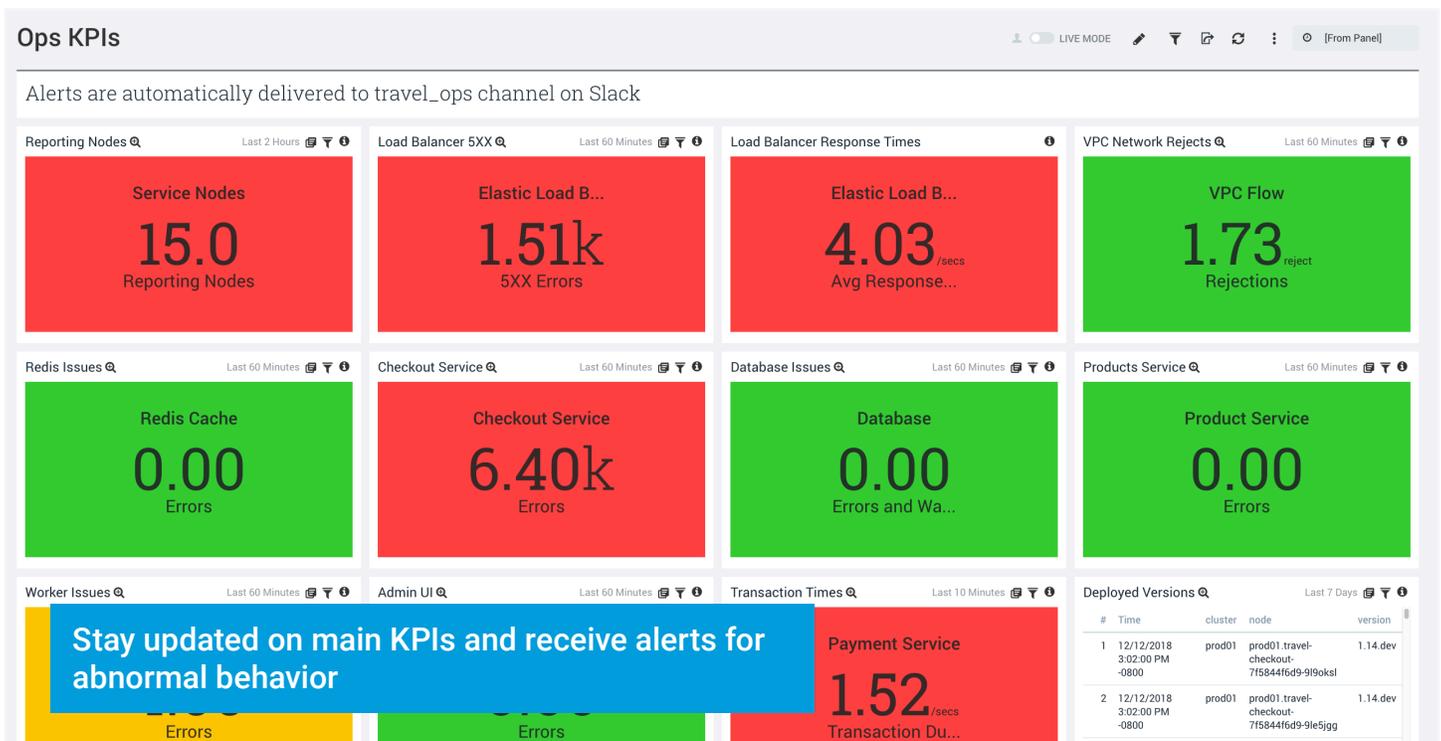
Whatever the rationale(s) may be for your enterprise's venture, the only way to know if it's truly living up to its advertised potential is to set up and then regularly evaluate key performance indicators (KPI). Examples of these metrics can include technical and business-oriented indicators such as:

- Transaction volume
- Throughput limits
- Number of active users

- Orders/revenue processed
- Errors
- Response time

Ideally, these KPIs should be in place prior to the initiative. Otherwise, it's impossible to know if the transformation has made things better or even degraded the overall experience. KPIs can also provide guidance about the cost-effectiveness of the cloud computing initiative, perhaps helping to justify expanded investment in it.

When correctly ingested and analyzed by technology such as Sumo Logic, your machine data is a fundamental ingredient in deriving these KPIs. It not only supplies pervasive visibility into the ongoing business and technical aspects of your organization, but it can also shed light on your software development and delivery processes through integration with tools such as Jenkins and Github. This makes it much easier to identify flaws with these procedures and thus deliver higher quality applications more quickly.



Next Steps

Getting started on using machine data to help your cloud migration consists of gathering important information as well as consulting external resources for additional guidance.

Additional Resources

To learn more about how to use Sumo Logic and machine data to bolster your move from on-premise to cloud computing, visit our Cloud Migration Webpage at: sumologic.com/cloud-migration/

Ready to start your cloud journey? Set up your own free Sumo Logic trial at: sumologic.com/freetrial

Checklist

Completing each of these steps can go a long way towards ensuring a successful migration. Several can be carried out prior to deploying Sumo Logic, while others can be only be accurately realized with Sumo Logic in place.

- Assemble a cross-functional migration team
Collect a comprehensive list of your hardware and software assets
- Identify as many dependencies among these assets as possible
- Determine which metrics – both low level and application details – are of special interest
- Select the technical staff that will be involved in the migration
- Specify the permissions that they'll have during the initiative
- Decide on how long they'll have these permissions
- Create list of regulations that the organization must comply with
- Measure compliance with these regulations prior to the migration
- Ascertain what impact - if any - migrating to the cloud will have on how you meet these requirements
- Create an inventory of KPIs that you'll want to track - even before the migration
- Try to link these KPIs with ROI justification for the initial and potential subsequent migration