Progress® | ipswitch®

Cloud Monitoring and the 9 Best Practices You Need to Adopt

ABSTRACT

Nearly every organization is taking advantage of cloud resources, but that poses a challenge for the ongoing monitoring of the organization's overall network environment. As more and more functionality migrates to the cloud, the ability to see the entire networking environment in context becomes more and more difficult. As well, tools and techniques used by IT staff to monitor their networking environment may not always be applicable to the cloud, causing confusion, finger-pointing and delays in issue resolution.

The solution to these challenges is a monitoring solution that can monitor the entire network environment, including the cloud. However, just monitoring the entire networking environment is the bare minimum required and will usually not meet the needs of today's IT departments. Cloud monitoring is a different animal from traditional network monitoring and there are some key factors that IT staff need to take into consideration.

This document examines what is involved in cloud monitoring and why it's important to your organization in terms of security, workload, application workflow and API integration. It also details some of the key factors you need to consider when determining how to monitor your cloud environment and outlines nine best practices IT organizations need to adopt in order to be successful.

Introduction

If you're responsible for maintaining any sort of network, you're almost definitely using cloud resources in some manner. In fact, 93 percent of businesses say they use cloud services, and many anticipate investing in it more. According to research, enterprises expect to increase spending by nearly 26% on cloud services annually, which outpaces spending increases on overall IT. And it makes sense: the cloud provides unparalleled business advantages such as scalability and agility.

Today it's extremely rare for an organization to rely solely upon on-premises, physical equipment for all their networking environment needs. This even applies in situations where security is a key concern; the advantages of migrating to the cloud are just too great to be ignored. However, the opposite is true when it comes to cloud resources: almost no organization has a networking environment that resides entirely within the cloud. This means that nearly every single network administrator or IT manager needs to monitor a mix of cloud resources and physical networking equipment. But with increased cloud usage comes a greater need to monitor performance.

That's where cloud monitoring comes in. You can't afford to have delayed web application response times, under-resourced workloads, downtime, or data breaches. Cloud monitoring helps you observe response times, availability, resource consumption levels, performance, as well as predict potential issues.

With all of this in mind, what's the best way to monitor the cloud? What are some of the things that should be monitored? What kind of tools should be used? What are the best practices? We'll answer all of these questions and more in this Cloud Monitoring eBook.

What is Cloud Monitoring?

Essentially, cloud monitoring is the process of reviewing and managing the operational workflow and processes within a cloud infrastructure or asset. It's generally implemented through automated monitoring software that gives central access and control over the cloud infrastructure. IT staff can review the operational status and health of cloud devices and components.

Concerns arise based on the type of cloud structure you use. If you're using a public cloud service, you tend to have limited control and visibility for managing and monitoring the infrastructure. A private cloud, which most large organizations use, provides the internal IT department more control and flexibility, with added consumption benefits.

Regardless of the type of cloud structure your company uses, monitoring is critical to performance and security.

The cloud has many moving parts, and it's important to ensure everything works together seamlessly to optimize performance. Cloud monitoring primarily includes functions such as:

❯ **Website monitoring:** Tracking the processes, traffic, availability and resource utilization of cloud-hosted websites

❯ **Virtual machine monitoring:** Monitoring the virtualization infrastructure and individual virtual machines

❯ **Database monitoring:** Monitoring processes, queries, availability, and consumption of cloud database resources

❯ **Virtual network monitoring:** Monitoring virtual network resources, devices, connections, and performance

❯ **Cloud storage monitoring:** Monitoring storage resources and their processes provisioned to virtual machines, services, databases, and applications

Cloud monitoring makes it easier to identify patterns and discover potential security risks in the infrastructure. Some key capabilities of cloud monitoring include:

> Ability to monitor large volumes of data across many distributed locations

> Gain visibility into application, user, and file behavior to identify potential attacks or compromises

> Continuous monitoring to ensure new and modified files are scanned in real time

> Auditing and reporting capabilities to manage security compliance

> Integrating monitoring tools with a range of cloud service providers

Cloud monitoring is easier if you operate in a private cloud for reasons we mentioned earlier (control and visibility), as you have access to the systems and software stack. Though monitoring can be more difficult in public or hybrid clouds, application performance monitoring tools (APM) give you visibility into performance behaviors.

A hybrid cloud environment presents unique challenges because data resides in both the private and public cloud. Limitations due to security and compliance can create issues for users accessing data. Admins can solve performance issues by determining what data to store in which cloud as well as what data to asynchronously update. Database synchronization can be a challenge as well, but sharding—partitioning data into smaller, faster and more easily managed parts—helps reduce issues.

Though private cloud gives you more control, you still need to monitor workloads to ensure optimum performance. Without a clear picture of workload and network performance, you can't justify configuration or architectural changes or quantify the effectiveness of quality of service implementations or other technologies.

APM tools are helpful in private cloud environments as well, as they work hand-in-hand with existing data monitoring and management and can track performance, report results, and alert you to possible service disruptions.

Even though private cloud gives you more control you still need to monitor workloads.

Why Monitor The Cloud?

In larger networks, sysadmins will daisy-chain multiple switches otherwise known as "cascading". A failed switch at the head of a chain will generate hundreds of unnecessary alerts throughout the chain. We call this an alert storm.

Alert storms can overwhelm an IT team and waste several hours of valuable time. Some storms involve the generation of several thousand alerts within a single hour.

An IT monitoring tool should identify network dependencies to automatically suppress redundant alerts. In other words, it would know what devices are connected to the failed switch and only issue an alert for the failed switch, suppressing all others.

Security

Security is crucial in the cloud so gaining strict control over data at all endpoints helps mitigate risks. Solutions that scan, analyze, and take action on data before it leaves the network help protect against data loss. It's also important to scan, evaluate, and classify data before it's downloaded to the network to avoid malware and data breaches.

APIs

The cloud can have an array of performance issues from poorly designed APIs. You can avoid poor cloud API performance by using APIs that operate via objects instead of operations. This results in fewer individual API calls and less traffic. APIs with consistent designs and few data type restrictions result in better performance.

Application Workflow

An application's response time and supporting resources are vital to understanding what's hindering performance. Following an application's workflow helps you identify where and when delays occur.

Workload

Overprovisioning cloud services—also known as cloud sprawl—eats up resources, availability and can impede performance. APM tools can help you find the issues, then proper policies and procedures can help mitigate sprawl and pull back resource and network use when necessary.

Monitoring the cloud requires tools that track performance, consumption, and availability while ensuring the secure transfer of data. A proper solution and management enables companies to find a balance between mitigating risks while leveraging the benefits of the cloud.

Remember that once you've adopted a cloud resource it should be indistinguishable from the rest of your existing networking environment from a user perspective. Anything you'd want to monitor in your physical networking environment should also be monitored in the cloud.

The 9 Best Practices

9

Monitoring your cloud resources is the first step. The next step is to figure out what you can do with that information. Ideally you'll be wanting to run your cloud resources as efficiently as possible in order to keep costs under control while providing a seamless experience for your end-users. Your organization's needs will determine your priorities, but in general here are the nine best practices you should be adopting when it comes to cloud monitoring:

Identify and List Important Metrics and Events

What activity needs to be monitored? Not everything that can be measured needs to be reported. You're going to want to carefully determine the metrics that matter to your organization's goals as well as the bottom line. Take some time to review exactly what your monitoring solution can track and consider what's going to be useful to you.

See Everything in Context

Your cloud-based resources are part of your overall networking infrastructure. They should be managed that way. Your cloud monitoring solution should allow you to see everything (cloud and physical resources) in context so you can quickly drill-down to issues and isolate the cause of problems that span technology silos.

Use One Platform to Report All the Data

It's hard to overstate how critical this is. Organizations have their own physical networking infrastructures in addition to cloud services to monitor. They need solutions that can report data from different sources on a single platform, which allows for calculating uniform metrics and results in a comprehensive view of performance. Every cloud provider will include monitoring tools, but those tools may not integrate with your existing monitoring solution. Research proves that having too many management tools severely degrades IT response time to networking issues and destroys IT productivity. Having one tool that reports on the ENTIRE networking environment makes troubleshooting faster, easier and eliminates finger-pointing.

Monitor Cloud Service Usages and Costs

This is where most traditional IT teams can get caught flat-footed. The ability to scale is a key feature of cloud services, but increased use can trigger increased costs. Robust monitoring solutions should track how much of your organization's networking activity is on the cloud and how much it costs. Idle resources aren't a big deal when it comes to on premise networking equipment like servers and routers, but most cloud resources cost money if they're not being used – and MORE money if they are. A monitoring solution that alerts IT when cloud resources exceed budget or usage limits can save your organization a fortune.

Track Long-Term Trends

Most monitoring tools provided by cloud service providers only maintain data for a limited time (usually 30-60 days). That's not nearly adequate for long-term trend analysis. Your monitoring tool should support maintaining that data in order to show trends over several months at least. Network activity in January is likely to be very different from network activity in July, but that's impossible to analyze within a 30-60 day window. Understanding long-term network trends can make it easier to run your network more efficiently, saving both time and money.

Set Up Alerts and Proactive Automated Actions

Alerting IT staff is a good start, but IT teams need to be able to proactively handle issues in the cloud. If activity exceeds or falls below defined thresholds, the right solution should be able to automatically add or subtract servers to maintain efficiency and performance. The same thing goes for performance issues. Not only does this make IT teams much more productive, it makes them look good by resolving issues before they impact end-users.

Monitor the End-User Experience

Organizations need to know what users experience when using their cloud-based applications. Monitor metrics like response times and frequency of use to get a complete performance picture.

Set Up Instant Visibility for Everyone

Regardless of whether or not you have a NOC, network status and performance should be something that can be seen at a glance by anyone. Your monitoring solution should support customizable dashboards that provide instant visibility into what's up, what's down, what's seeing heavy usage, what's idle, etc. Not only does this make it easier to troubleshoot, it allows IT teams to see issues develop and resolve them proactively before they impact end-users.

Test for Failure

Test your tools to see what happens when there is an outage or data breach and evaluate the alerting and/or automated response systems when certain thresholds are met.

Conclusion

Extending your network environment to the cloud offers a huge number of advantages, but monitoring the results is crucial. We've outlined what you should be doing and why, but the final step is likely the most time-consuming: choosing a monitoring tool for your entire networking environment. Obviously we have our own opinion on the most effective tool out there, but it's important to review the options available. Use the above best practices as a checklist to determine if the solution you're considering is going to do what you need it to. However, bear in mind that the most important requirements are going to be how well it integrates information from the cloud provider, how well it puts that information in context with the rest of your networking environment and how well it lets you proactively resolve issues before they impact your end-users. Remember that you're losing money once an end-user is impacted by a network issue and a good network monitoring solution allows you to be proactive instead of just reactive!

Appendix - Cloud Glossary

Amazon Web Services (AWS) – The world most widely-used cloud service provider. Amazon Web Services (AWS) is Amazon Inc.'s bundle of more than 36 cloud computing services, including PaaS, SaaS, and IaaS offerings. AWS currently holds over 30% of global cloud computing market share.

Cloud Computing – In the simplest terms possible, cloud computing is the delivery of information technology services or resources via a network, rather than from on premise hardware and resources. As you've probably already surmised, 99% of the time, that delivery network is the internet.

According to the official definition from the NIST, there are five main components of cloud computing: on-demand self-service, broad network access, resource pooling, rapid expansion (typically referred to as elasticity), and measured service.

Essentially, a cloud provider works like a utility company (think electric or water)—they host the resources or services that you need, and deliver them on-demand, scaling up or down to suit your needs.

Cloud Management Platform (CMP) – A cloud management platform allows integrated management of private, hybrid, and public clouds.

Cloud Marketplace – Cloud marketplaces are online stores where customers can explore and subscribe to software applications and developer services that supplement, integrate into, or build on top of existing software. Amazon's AWS Marketplace is a good example.

Cloud Migration – The process of moving applications, services, and data from on premise to the cloud. This has become big business as many large enterprises struggle to migrate their data and deployments to cloud workloads.

Cloud Monitoring – The process of reviewing and managing the operational workflow and processes within a cloud infrastructure or asset. It's generally implemented through automated monitoring software that gives central access and control over the cloud infrastructure. Admins can review operational status and health of cloud devices and components. For more information, check out our post What is Cloud Monitoring?

Cloud Service Provider (CSP) – A cloud service provider is—you guessed it—any company that sells a cloud computing service, be it PaaS, IaaS, or SaaS.

Cloud Storage – A method of computer storage where data is stored in facilities managed by a cloud service provider and can be accessed remotely by the user through a network. Typically, data stored in the cloud is collocated, which means it is duplicated in multiple locations as a failover.

Container – A virtualization instance where the kernel of an operating system allows for multiple isolated user-space instances. While virtual machines (VMs) need to run a full operating system (OS) image for each instance, containers do not. Instead, they create an isolation boundary at the application level. The benefits of this are multi-fold. First, if a something goes awry in a single container, only that container is affected, rather than the entire VM. Second, the application-level isolation boundary prevents compatibility issues between applications running on the same operating system.

DevOps – An abbreviation of "development and operations," DevOps is the combination of tasks performed by applications development and systems operations teams. DevOps as a method of software development emphasizes communication, integration, and collaboration between developers and IT people to streamline the software development, delivery, and support processes and improve product quality.

Elasticity – The ability of a system to adapt to a shifting workload demand by provisioning and de-provisioning pooled resources to match current demand as much as possible.

Extensibility- The ability to add new functionality and framework support.

Google Cloud Platform (GCP) – Google's cloud services offering, Google Cloud Platform (GCP) has both infrastructure as a service (IaaS) and platform as a service (PaaS) products.

Host Machine – The physical hardware (i.e., Server) that stores virtual machines or containers.

Hybrid Cloud – A cloud computing environment made up of a combination of private and public clouds, as well as on-premises solutions. Private and public cloud infrastructures stay distinct from one another, but the hybrid cloud ensures data and services portability by binding them together without sacrificing their integrity.

Hypervisor – A hypervisor, which creates, runs, and manages virtual machines (VMs) is also called a virtual machine monitor (VMM). It is a piece of software that allows physical devices to share resources among virtual machines supported by physical hardware.

Infrastructure – IT infrastructure is the combined hardware and virtual resources that support an overall IT environment.

Infrastructure as a Service (IaaS) – A model of cloud computing where the vendor hosts and provides to its customers compute resources, as well as networking and storage capabilities.

Instance – An instance is a single virtual machine or server supporting a workload. Most cloud platforms allow users to choose from several instance types to determine the hardware that hosts the instance.

Load Balancing – The process of distributing computing workloads across multiple resources, including servers. A load balancer in cloud computing acts as a reverse proxy and distributes application traffic to several different servers to prevent any single application server from being overwhelmed and becoming a point of failure.

Microsoft Azure – Microsoft Azure, formerly known as Windows Azure, is Microsoft's cloud computing platform. Initially, Azure only offered a PaaS solution, but now it provides both PaaS and IaaS options.

Middleware – Software that connects different kinds of software components or enterprise applications.

Multi-Cloud – The concurrent use of separate cloud service providers for different infrastructure, platform, and software uses. A multi-cloud strategy can help prevent vendor lock-in, as well as increasing the ability of an enterprise to handle diverse workloads and partners. However, using a multi-cloud approach can complicate processes such as security and governance.

Multi-Tenancy – A mode of operation for software, wherein multiple instances of one or more applications run in a shared environment. In a cloud computing model, pooled virtual and physical resources are dynamically assigned and reassigned to tenants (groups of users) to keep up with consumer demand.

On-Demand Self Service – A service model that lets a customer provision and deploy additional cloud resources on-demand, usually through an online control panel, without involving the service provider.

Platform as a Service (PaaS) – A model of cloud computing where a vendor provides, as a service, the hardware and software tools to create, deploy and manage applications at scale to the user through the internet.

Private Cloud – A cloud infrastructure that is provisioned for use by a single organization. A private cloud cab can exist on or off premises and is managed and operated by either the organization, a third party, of some combination of both.

Public Cloud – A cloud infrastructure that is hosted by cloud services provider and made available to the public through the internet.

Scalability – The ability of a process, system, or framework to handle a growing workload. A scalable system is adaptable to increasing or changing demands.

Software as a Service (SaaS) – A model of cloud computing where applications and software are hosted by a vendor that provides them to the user as a service. SaaS applications are licensed on a subscription basis.

SaaS has become a popular model of delivery for business applications because they can be accessed in any location, at any time, and on any platform. Microsoft's Office 365, which houses web-based email and productivity software including MS Word and Excel as services, is an example of a popular SaaS application.

Virtual Machine (VM) – A software emulation of a computer system that provides all of the functionality of a physical computer. VMs are used to run multiple instances of the same operating system on a single server.

Workload – The amount of work running on an instance.

About Progress

Progress (NASDAQ: PRGS) offers the leading platform for developing and deploying strategic business applications. We enable customers and partners to deliver modern, high-impact digital experiences with a fraction of the effort, time and cost. Progress offers powerful tools for easily building adaptive user experiences across any type of device or touchpoint, award-winning machine learning that enables cognitive capabilities to be a part of any application, the flexibility of a serverless cloud to deploy modern apps, business rules, web content management, plus leading data connectivity technology. Over 1,700 independent software vendors, 100,000 enterprise customers, and 2 million developers rely on Progress to power their applications.

Learn about Progress at www.progress.com or +1-800-477-6473.

Progress
WhatsUp® Gold

Download your FREE TRIAL of WhatsUp Gold ❯