

Conversational Cloud Monitoring



A
Conversational**Geek**
Book

Sponsored by **ca**
technologies



Learn about:

- The complexities of modern cloud environments that complicate effective monitoring
- Critical aspects of performance management that can make or break your cloud
- Best practices for monitoring to drive efficiency and support SLAs

By **Brien M. Posey** (Cloud Expert)

Sponsored by CA Technologies

CA Unified Infrastructure Management (CA UIM) is an award winning, analytics driven solution for proactively and efficiently managing cloud and hybrid IT infrastructures. It's the only solution that provides intelligent analytics, comprehensive coverage and an open, extensible architecture. By leveraging the solution, your organization can speed mean time to repair by up to 40%, reduce monitoring efforts by up to 60%, and boost end-user experience. The solution also provides unified, automated monitoring configuration and deployment, making it optimally suited to today's DevOps and high-scale environments.

For more information, visit: ca.com/uim



Conversational Cloud Monitoring

By Brien M. Posey

Copyright© 2017



Conversational**Geek**[®]

Conversational Cloud Monitoring

Published by Conversational Geek Inc.

www.conversationalgeek.com

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Trademarks

Conversational Geek, the Conversational Geek logo and J. the Geek are trademarks of Conversational Geek. All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. We cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or programs accompanying it.

Additional Information

For general information on our other products and services, or how to create a custom Conversational Geek book for your business or organization, please visit our website at ConversationalGeek.com

Publisher Acknowledgments

All of the folks responsible for the creation of this guide:

Author:	Brien M. Posey
Project Editor:	Steven Zimmerman
Copy Editor:	Steven Zimmerman
Content Reviewer(s):	Jaclyn McGovern

Note from the Author

Hi, I'm Brien. I've been writing for Conversational Geek for a long time, and have covered a wide variety of topics. When I say "wide variety" I really mean it. I have written Conversational Geek books on everything from Amazon Web Services to rocket science!

With so many titles under my belt, you might be wondering why I chose to write about cloud monitoring for my latest Conversational Geek book. No, it's not because rocket science isn't difficult enough, and I needed a real challenge. The main reason why I wanted to write about cloud monitoring is because the cloud is a game changer. Monitoring tools have been around for decades, and yet existing tools tend to be inadequate for monitoring backend infrastructure in cloud environments. These tools can also be fairly difficult to use in hybrid environments. And since businesses are already heading the hybrid route, I wanted to take the opportunity to write about what is really needed for effective cloud monitoring.

Oh, and one more thing... Although this book will eventually have a sponsor (we can't print these books for free), it is not intended to be a vendor product pitch. My goal here is to take a vendor neutral approach, and talk about strategies for effective cloud monitoring.

Enjoy!



Brien

The “Conversational” Method

We have two objectives when we create a “Conversational” book: First, to make sure it’s written in a conversational tone so that it’s fun and easy to read. Second, to make sure you, the reader, can immediately take what you read and include it into your own conversations (personal or business-focused) with confidence.

These books are meant to increase your understanding of the subject. Terminology, conceptual ideas, trends in the market, and even fringe subject matter are brought together to ensure you can engage your customer, team, co-worker, friend and even the know-it-all Best Buy geek on a level playing field.

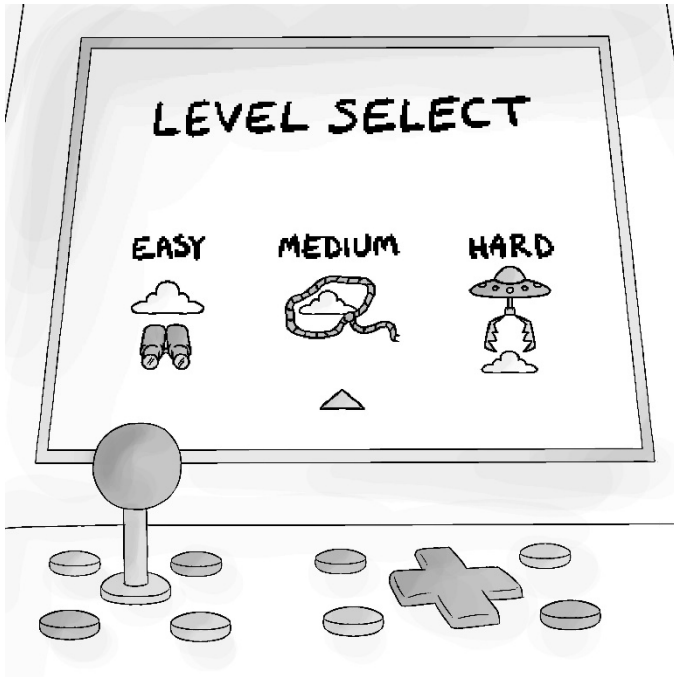
“Geek in the Mirror” Boxes

We infuse humor into our books through both cartoons and light banter from the author. When you see one of these boxes it’s the author stepping outside the dialog to speak directly to you. It might be an anecdote, it might be a personal experience or gut reaction and analysis, it might just be a sarcastic quip, but these “geek in the mirror” boxes are not to be skipped.



Within these boxes I can share just about anything on the subject at hand. Read 'em!

Cloud Monitoring: Making a Game Plan



Whenever someone mentions infrastructure monitoring, I am guessing that most IT pros probably find their eyes glazing over and their mind wandering. After all, monitoring tools have been around for decades, and even though technology changes, the basic concepts of monitoring remain largely the same. So discussions of cloud monitoring are largely a case of “been there, done that, end of story,” right? Not quite.

Even though public clouds such as Amazon Web Services (AWS) and Microsoft Azure expose many of the same resources that we all use in our own datacenters, at an anatomical level the cloud is quite different from anything that we might have used in the past. These differences mean that, in many cases, tried and true monitoring techniques break down when they are applied to public, hybrid, or even to private clouds.

Of course, I couldn't write a book like this one without taking at least a moment to talk about cloud monitoring from a philosophical standpoint. Compared to legacy IT, the cloud represents a new way of doing things. Whether it's right or wrong, there is a perception that the cloud enables agile IT, and that tasks that would have been monstrously difficult in on-premises environments, can be completed with ease in the cloud. The point is that people adopt the cloud because they want a better, and more agile experience. As such, monitoring tools should be able to keep pace with whatever an organization is doing in the cloud, without getting in the way, or becoming a barrier to agility.

In some cases, difficulties monitoring cloud resources stem from the inability of a monitoring tool to scale to meet the scope of the hybrid or multi-cloud environment. More often, however, tools that are not specifically designed for these environments, and may provide incomplete, or even inaccurate, information.

History Repeats Itself

The challenge of monitoring cloud resources is not entirely unprecedented. It pros went through a somewhat similar situation about a decade ago, when server virtualization first became a mainstream technology.

Prior to the introduction of server virtualization, server monitoring tools were designed to monitor physical servers. When people started to use virtual servers, there was initially a tendency to try to use legacy monitoring tools and techniques in a virtual server environment.

In some cases, these legacy tools simply did not work. An out of band monitoring tool, for example, generally won't be able to connect to a virtual server because virtual machines lack the dedicated, hardware-level management channel.

In other cases, IT pros found that legacy monitoring tools did work in a virtualized environment, but the tools yielded completely unexpected results. Consider the Windows Performance Monitor for example... If you run the Performance Monitor on a physical server and look at the %Processor Time counter, you will see the percentage of time that the server's CPU is in use. If you look at the same counter inside of a virtual machine however, the number that is displayed does not truly reflect CPU use. Instead, it shows what percentage of the CPU resources that have been allocated to the virtual machine is in use at that moment. In other words, the counter shows you a percentage of a percentage, rather than showing you actual CPU usage.

Today, I think that most IT pros probably understand the implications of performance monitoring inside of a virtual machine, but in 2006 those implications caught a lot of IT pros off guard. The takeaway from all of this is that the same basic lessons that were learned by IT pros so long ago have once again become relevant due to the need for cloud monitoring, and the fact that so many monitoring tools are not specifically designed for use with the cloud.



The longer I work in IT, the more I begin to realize that concepts and lessons from the distant past often remain relevant in spite of changing technology.

The Key to Effective Cloud Monitoring

Monitoring cloud resources in any kind of meaningful way can be a complex undertaking. Over the years, I have found that the key to successfully completing any complex project is to

start out by asking a single, simple question. That question is “what is it that I am hoping to achieve?”

The quick answer to this question is obviously “I want to monitor the cloud,” but that answer isn’t very helpful because it lacks any specific goals. Sure, you want to monitor your cloud resources, but what specifically is it that you want to monitor? Do you want to know if you are meeting your SLAs? Do you want to know how many virtual machines or containers are in use? Do you want to know at what point your use of the cloud will break the Internet?

OK, maybe that last question is a little bit over the top, but the overall point remains the same. Effective cloud monitoring means different things to different people. Therefore, the first step is to figure out what it is that you want to accomplish.



In addition to my work in IT, I have spent the last few years training to go to space on a commercial science mission. During my training, the instructors often talk about defining the criteria for success. Although space flight training and Information Technology are far removed from one another, I have found that the concept of defining the criteria for success works well for IT, and is especially applicable to cloud monitoring.

The Elephant in the Room

Before I begin to look at the best practices for cloud monitoring in the next chapter, I want to take a moment and address one of the big questions that I am sure is on many of your minds. Public cloud providers such as Amazon and Microsoft offer native monitoring tools, so why not just use those tools?

I'm not going to sit here behind my keyboard and tell you not to use your cloud provider's native tools. Amazon, Microsoft, and the other major providers give you tools for a reason. If the native tools meet your needs then that's great, use them!

Having said that, there are two things that you should consider before you make a decision to base all of your cloud monitoring efforts solely on the native tools.

First, the native tools are most effective for organizations that operate solely within a single public cloud. Think about it for a minute... Cloud service providers bill their subscribers based on the resources that they consume. As such, cloud providers want their subscribers to do everything within their own cloud.

Of course, the public cloud providers realize that, with the exception of some startups, most organizations continue to host some resources on-premises. Likewise, larger organizations will inevitably leverage services across multiple public cloud providers (a practice called multi-cloud).

As such, the cloud providers reluctantly allow their subscribers to have hybrid clouds and / or multi-clouds, and to interoperate with resources that the provider does not own. From a business perspective, the cloud providers would definitely prefer that their subscribers operate solely in the public cloud.

So, think about this idea from a monitoring standpoint. There is little incentive for a public cloud provider to create native tools that provide consistent and comprehensive management and monitoring capabilities across hybrid cloud (or multi-cloud) environments. The native tools are likely to be adequate for single public cloud use, but severely lacking when it comes to monitoring hybrid or multi-clouds.

Of course, each provider makes a suite of monitoring tools available to subscribers, but I think that it's safe to say that most IT pros have to use too many different tools as it is. It is

far better to use a single third-party monitoring tool (so long as it does a good job, and meets all of the organization's needs) than to keep adding single purpose tools to the organization's administrative toolbox.

A second reason why it is worth considering whether the native tools are good enough, has to do with the amount of effort that the cloud provider puts into creating good monitoring tools.

Remember earlier when I said that historical concepts from IT's distant past often remain relevant, even today? Well, here is another example. If you are a Windows admin, then you are no doubt familiar with the management and monitoring tools that are baked into the Windows operating system. Even though these tools will work in a pinch, there are countless companies whose entire business model is based on selling tools that are vastly superior to the ones that are included with Windows.

This same basic principle also applies to the public cloud. Public cloud providers (and not just Microsoft) put most of their effort into creating a stable and reliable cloud platform, and seem to readily accept the idea that third-party vendors will create better management and monitoring tools than the ones that the provider creates itself.

What Should You Be Monitoring?

As noted in the previous chapter, the key to truly effective cloud monitoring is to begin by setting some goals for what you hope to accomplish. Once you have defined some objectives, then you can begin to work toward coming up with a plan for meeting those objectives.



In the world of IT, there are about a zillion different types of monitoring. For the purposes of this book, I am focusing on infrastructure monitoring, with an emphasis on the cloud. That means that I am going to be talking about monitoring as it related to things like compute, storage, and databases.

This of course raises the question of what you should be monitoring. As is the case for so many different things in the world of IT, the answer to this question varies widely from one organization to the next. The answer is based on the organization's own unique needs, and also on the type of cloud environment that the organization is using. An organization that is operating solely within the public cloud, for example, will have different monitoring needs from an organization that has a multi-cloud deployment, or that has built a hybrid cloud.



Monitoring requirements can vary based on cloud types. In public cloud environments, admins tend to focus on monitoring metrics related to performance and availability.

Performance and availability are, of course, also important in a private cloud, but monitoring in a private cloud also tends to focus on the elimination of hardware

bottlenecks. Private cloud monitoring might also focus on things like usage patterns or license tracking.

Hybrid and multi-cloud monitoring tends to be even more complex, as it adds the requirement to monitor performance across cloud environments.

So back to the question at hand... What should you be monitoring? As I said earlier, everybody's needs are unique, so I can't tell you exactly what you should be monitoring. What I will do, however, is to give you my thoughts on a number of different things that you could potentially monitor. That way, you can use that information to come up with a cloud monitoring plan that is right for you.

End-to-End Visibility

When it comes to establishing goals and objectives for cloud monitoring, one of the first things to come to mind is often end-to-end visibility. In other words, you need to be able to see the full stack of IT services, without any of the services becoming a black box that cannot be monitored.

Having end-to-end visibility isn't really an issue if you are operating solely within the confines of a single public cloud. However, end-to-end visibility becomes critically important when you start dealing with hybrid clouds and multi-cloud environments; even on-premises IT can have its visibility issues. After all, hybrid clouds and multi-clouds involve linking together dissimilar systems, and an administrator needs to be able to see what is going on across all of those systems infrastructure elements – not just systems, but databases application servers, storage, VMs, containers; the list goes on.

As important as end-to-end visibility is, however, it is not the be-all and end-all. Don't get me wrong, having end-to-end

visibility should be one of the first things on your cloud monitoring wish list. Even so, it is important not to stop there. The next step is to determine the types of things that you need visibility into.

Full Stack Monitoring

Throughout this book, I have expressed a variety of ideas as to what a good cloud monitoring solution should be able to do. If I had to choose one single capability that is more important than everything else however, I would have to pick full stack monitoring. Full stack monitoring is based on the idea that any public cloud is made up of numerous individual services and resources, and the software must be able to monitor all of those resources in order to prevent monitoring gaps.

Compute

A good cloud monitoring solution should also be able to monitor your compute resource usage. Compute resource allocation in a cloud environment can be a tricky thing. Public cloud providers such as Amazon and Microsoft require subscribers to specify an instance size when deploying new virtual machines. Higher-end virtual machine instances are more capable, but at a greater cost. As such, administrators are forced to strike a balance between performance and cost. If a virtual machine instance is oversized, then some of the virtual machine's compute capacity is wasted. Conversely, a virtual machine that is undersized will likely suffer from performance problems.

A cloud monitoring tool should be able to monitor compute resource usage in a way that helps the administrative staff to determine whether virtual machines have been sized appropriately. By taking a critical look at virtual machine instance sizing, it becomes possible to optimize the performance of cloud virtual machines, while also minimizing instance-related costs.

Storage

Just as it is important to monitor compute resource usage, it is equally important to monitor storage consumption. As previously noted, cloud providers bill their customers based on resource consumption. When it comes to storage, billing is usually a monthly charge that is based on the total number of gigabytes of storage in use that month. There may also be transfer charges related to reading or writing to cloud storage.



The crazy thing about cloud storage, is that you never actually own it. Instead, you are leasing virtual real estate occupied by your data.

In addition, public cloud providers usually offer several different types of storage. Amazon, for instance, offers S3 and Glacier, just to name a couple. These storage types are billed at different rates based on their capabilities.

A cloud monitoring solution should help you to monitor the way in which cloud storage is being used, while also helping you to optimize cost and performance by using the appropriate storage tier.

Network

Often, when people think of monitoring, their thoughts instantly turn to network monitoring. I have to confess, I thought about not even talking about network monitoring in this book, because it is such an obvious thing. While I don't want to waste a lot of time writing about network monitoring, I ultimately decided that it should at least be mentioned. After all, you can't connect to the cloud without a reliable network.

The one thing that I will say about network monitoring is that if you are looking for a network monitoring solution for the cloud, then it is important to use a tool that supports Software Defined Networking.

Database

Database performance monitoring is one of those things that I hardly ever hear anyone talk about with regard to the cloud. Part of the reason for that is probably that database monitoring has been around in one form or another for what seems like forever. Even so, operating in the cloud sometimes changes things. Let me give you an example.

Suppose for a moment that you have an on-premises SQL Server running on a virtualized Windows Server 2016 instance. Let's also suppose that you use all the normal SQL Server and Windows Server monitoring techniques in an effort to keep SQL Server healthy. Now imagine that you perform a cloud migration and move that virtual machine instance to Microsoft Azure. From a SQL Server standpoint, nothing has really changed. SQL Server is still running inside of a VM, on top of a Windows Server 2016 operating system. All the same monitoring best practices still apply.

The reason why the cloud sometimes changes things is because cloud providers such as Microsoft and Amazon have begun pushing customers toward serverless databases. Microsoft for example offers something called Azure SQL, which is essentially a SQL Server that runs at the cloud level, without the need for a virtual machine instance. Because Azure SQL does not run inside of a virtual machine, the usual monitoring techniques cannot be used. As such, it becomes necessary to adopt a completely new set of techniques and best practices for keeping tabs on the SQL databases. Keep in mind that this trend is not unique to Microsoft. Amazon also offers a variety of cloud databases including Amazon RDS, Aurora, and Redshift.

Docker Containers

I don't want to spend a lot of time on this one, because it falls a little bit outside the scope of the rest of the book. Even so, I wanted to take a moment to talk about containers. Over the last couple of years, numerous workloads have been shifted from VMs to containers. Now that containers are supported by all of the major cloud providers, and are natively baked into Windows Server and Linux, the trend' momentum is sure to continue. As such, it's a good idea to make sure that any cloud monitoring solution that you might be considering includes support for container monitoring.

Availability

When it comes to cloud monitoring, the solution that you use should also be able to track cloud resource availability. Doing so helps to ensure compliance with service level agreements (SLAs).

If you are operating in a public cloud, then SLA tracking is of minimal importance. I'm sure that there are those who would disagree with me on that statement, but hear me out. Public cloud providers such as Amazon and Microsoft do a really good job of SLA tracking for their customers. As such, you don't really have to worry about tracking cloud availability, because the provider does that for you.

The exception to this is that SLA tracking can be useful if you are trying to ensure the availability of a specific resource within the public cloud, such as a workload that is running on a virtual machine instance.

SLA tracking is also of the utmost importance in private cloud or hybrid cloud environments because, in those cases, the IT department is responsible for ensuring that cloud resources remain available at a level that adheres to established SLA's.

Capacity

Another thing to think about regarding cloud monitoring is how the monitoring process might help with capacity planning. This is especially true for private clouds or for hybrid clouds, because both of these cloud types depend on hardware resources that reside on-premises.

The tricky thing about capacity planning in private or hybrid cloud environments is that users can claim resources (up to the limits that you have set) without warning. This means that capacity planning is a critically important task, because accurate forecasting of your capacity needs in constant cloud monitoring are the only things that will keep your cloud environment from running out of resources unexpectedly.

Contextual Log Analysis

Log file analytics are kind of a funny thing in the realm of IT. Back in the 1980s when I was first starting out in IT, log files were often the only source of reliable diagnostic information. Eventually though, it kind of seemed as though log files fell out of fashion for whatever reason. Maybe that's an inaccurate perception on my part, but at the time it seemed like almost overnight everybody stopped using log files.

Today of course, log files are ever-present and widely used across nearly every area of IT. When it comes to monitoring, or even diagnostics and remediation, log files very often contain the most comprehensive and reliable information available.

The bottom line is that log files provide a wealth of information about what is going on with the various systems that make up your cloud infrastructure. While it is technically possible to perform cloud monitoring without ever touching a log file, correlating log files with performance data often allows for root cause analysis.

Cost

Ideally, your chosen monitoring solution should provide you with some insight into the overall operational costs. One of the big differentiators between public cloud environments and legacy, on-premises client/server environments is that public cloud providers bill their subscribers based on the resources that they use. Although the public cloud is often marketed as being the inexpensive alternative to on-premises operations, the costs associated with operating in the public cloud can add up surprisingly quickly.

A good monitoring solution for cloud environments should provide insight into cloud resource usage, thereby also providing insight into operational costs. Even if such a tool does not directly address cloud billing, it should help the administrative staff to determine which resources are being used most heavily, as well as areas in which it may be possible to bring down costs by eliminating waste or by doing things in a more efficient manner.

What's Missing?

Hopefully, the information in this chapter has helped you to come up with a list of the things that you want to monitor, so that you can begin developing a cloud monitoring strategy. Before you finalize your key success criteria though, there are a couple of things that are often overlooked.

Alerting

The fact that I have not talked about alerting until now is not an accident; it is kind of a basic thing that any monitoring solution should have built-in. Even so, there is one aspect to the alerting engine that warrants attention.

Regardless of whether you are working in a hybrid, public, or even multi-cloud environment, one of the primary benefits offered by the cloud is scalability. Clouds can scale to a

ridiculous level. However, this scalability can sometimes wreak havoc when it comes to alerting.

I think it's safe to say that most IT pros have probably seen monitoring systems that generated way too many alerts. When this happens, it is only a matter of time before alert fatigue begins to set in. Administrators grow so weary of meaningless noise alerts, that they begin to ignore the alerts altogether.

With that in mind, imagine what would happen if you were to use that noisy monitoring solution with a much larger-scale environment. If the environment were a thousand times larger, you would presumably get a thousand times more alerts.

Because clouds can scale to such a huge level, it becomes extremely important for a monitoring solution to use very intelligent alerting. A good monitoring solution should only alert you when there is a condition that legitimately needs the attention of the IT staff. Noise alerts are simply unacceptable at cloud scale, because they have the potential to be a major disruption, and to choke out meaningful alerts.

Consistency

Probably the number one thing that is overlooked about cloud monitoring is the consistency of the metrics that are used. Without consistency, it becomes impossible to correlate data across environments.

Suppose, for the sake of example, that you've got a hybrid cloud environment and that you have implemented a monitoring solution that provides end-to-end visibility across both your on-premises and public cloud environments. Having end-to-end visibility is obviously a big accomplishment, but is of limited benefit if you don't have a way to correlate data in a consistent manner across the two environments.

In other words, you should be using a single set of metrics to monitor both your public cloud resources and your on-

premises resources. If, for example, you had a hybrid application with the front-end server in the public cloud and the database was on-premises, and you were not collecting a singular metric set, then the resulting data would provide an inaccurate picture of what's really going on across the two environments, because two dissimilar sets of metrics are being used. In such a situation, you would be presented with accurate monitoring data for one environment, while the performance data for the other environment would be shown to be either better or worse than it really is. Only by using a common set of metrics that spans all cloud environments does it become possible to make an accurate assessment of what is really going on.

The key to achieving optimal cloud monitoring capabilities is not only to use a consistent set of metrics (which is of critical importance), but also to blend data from all available sources in order to achieve a comprehensive picture of what is going on. For today, this usually means examining performance data and log data. In the future however, vendors are almost certain to also leverage machine learning capabilities. One way in which you can get ahead of the curve is to check with prospective vendors to see if their product roadmap includes any sort of AI or machine learning initiatives.

The Big Takeaway

The big take away is that even though monitoring has been used in IT in one form or another for decades, cloud changes all the rules. While it is tempting to think of a cloud monitoring tool as being something that provides end-to-end visibility across hybrid cloud or multi-cloud environments, end-to-end visibility by itself is not enough. A good monitoring tool needs to provide meaningful insight into the way that cloud resources are being used in order to ensure SLA compliance, good performance, and control over cost.

Vendor-Sponsor Chapter: CA Technologies

Comprehensive Monitoring for Cloud and Hybrid IT Environments



Although the media often portrays cloud services as a new, up and coming technology, the truth is that organizations of all sizes have been utilizing the public cloud in at least some capacity for many years. Most IT departments have moved well beyond basic cloud adoption, and on to more advanced configurations such as hybrid cloud, multi-cloud, or even some combination of the two.

Of course, the transition to using more sophisticated cloud models has not been without its challenges. IT pros have often learned the hard way that these new types of cloud infrastructures cannot be monitored in the same way as legacy IT resources. Furthermore, current generation tools commonly

lack visibility into significant portions of an organization's hybrid IT infrastructure.

CA Unified Infrastructure Management seeks to address these challenges by providing visibility and consistent monitoring capabilities across all tiers of an organization's IT infrastructure.

A comprehensive cloud monitoring platform such as the one provided by CA Technologies should be considered essential for any organization that uses a mixture of public cloud and on-premises resources, or whose infrastructure spans multiple clouds. The reason for this is simple. Extending an IT infrastructure so that it spans multiple clouds, or includes a mixture of cloud and on-premises resources, will by definition result in the infrastructure becoming more complex. The more complex the infrastructure becomes, the more difficult it will be for the IT department to troubleshoot problems or to track resource utilization.

CA Unified Infrastructure Management is specifically designed to address the cloud monitoring pain points that IT pros find most frustrating. These challenges range from determining the cause of a poor user experience to optimizing the cloud infrastructure in a way that improves performance while also potentially reducing operating costs.

Decrease Mean Time-to-Resolution

One of the administrative challenges that CA Unified Infrastructure Management is designed to help with is that when problems occur within a complex environment, there is often a high mean time to resolution.

Naturally, the more complicated the infrastructure, the longer it will take to diagnose problems within that infrastructure, but there is more to it than that. Hybrid cloud and multi-cloud environments are not based on products or services from a single vendor. The infrastructure may span multiple public

cloud providers, and use numerous hardware and software solutions on-premises.

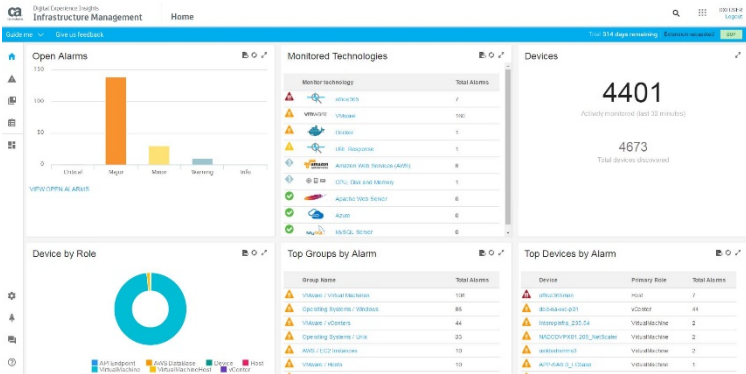
The problem with this is of course, the potential for internal groups or vendor finger pointing. All too often, an issue results in long triage calls involving multiple departments or vendors. Everyone using their own tool/view to look at the problem.

CA Unified Infrastructure Management helps to eliminate this finger pointing by providing IT with a single pane of glass view of all their infrastructure elements or services spread across on-premises or cloud(s) resources

Track Experience Degradation Across Multi or Hybrid Clouds

Throughout the entire history of Information Technology, one of the most common problems has always been that of a poor user experience. One of the reasons why user experience issues have so often plagued IT pros in hybrid or multi-cloud environments is that the interconnected nature of these systems can make it tough to locate the source of a problem.

To further illustrate this idea, imagine that a user is experiencing problems with application responsiveness. Now imagine that this Web based application depends on a customer database located in the organization's own datacenter, a parts database that is hosted on the AWS cloud, and an inventory database that is running on Microsoft Azure SQL. So why is the application not being more responsive? Is Microsoft having a problem with Azure? Is the storage array in the organization's datacenter performing poorly because of a recent disk replacement?



In the past, diagnosing this type of problem would have been both tedious and time consuming. However, CA Unified Infrastructure Management provides end-to-end visibility into such environments and integrates with CA Application Performance Management, providing detailed status and diagnostic information for every part of your IT infrastructure.

Optimize Cloud & IT Resources

Another problem that is often experienced in cloud environments is that of improperly sized IT resources. On the surface, resource sizing might not seem to be as important as some of the other administrative pain points that are being discussed, because resources could conceivably be completely functional, even if they are sized incorrectly. Even so, there are consequences to improper resource sizing.

Virtual machines running within on-premises hypervisors tend to be highly customizable. Administrators can specify exactly the amount of memory and the number of CPU cores that they wish to allocate to a VM.

Cloud based virtual machine instances however, are a completely different story. Public cloud service providers require subscribers to create virtual machines based on several

pre-configured sizing templates. These templates determine the hardware allocation for the resulting virtual machine instance.

If a VM is undersized, then it means that its hardware configuration is inadequate, and that the virtual machine is not performing as well as it would if it were allocated additional resources. Conversely, an oversized virtual machine is a VM instance that has been allocated more hardware than is needed by the VM workload, resulting in unnecessary costs.

In addition to optimizing sizing, simply keeping track of provisioned VMs – particularly in the cloud – limits the expense of running unused VMs.

CA Unified Infrastructure Management can administrators to properly size IT resources. The software provides detailed utilization reports that admins can use to make sizing decisions.

App to Infrastructure Correlation for App-Centric Triage.

It's about all applications in today's software powered businesses. CA Unified Infrastructure Management (CA UIM) in conjunction with CA Application Performance Management provides end to end visibility from cloud native applications all the way to the underlying infrastructure across cloud and traditional IT resources. Users are able to triage easily and intuitively to find root cause of issues regardless of them being an app or infrastructure issue.

Contextual Operational Intelligence for Smarter Operations

Alerting without context just creates chaos and repetitive issues keep popping up. Today's cloud based environments are highly dynamic and complex in nature, they require a much

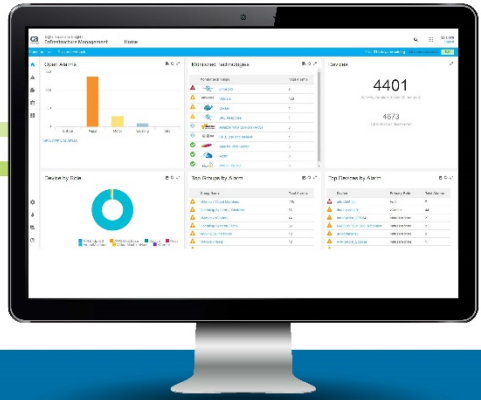
more intelligent approach. CA UIM in conjunction with CA Digital Operational Intelligence provides contextual insights leveraging log, capacity and service analytics to help you proactively resolve issues and identifying underlying root cause of issues faster. CA Digital Operational Intelligence also polls data from CA's network monitoring portfolio to provide you the ability to triage and correlate data from modern networks include SDN/NFV with infrastructure data from CA UIM.

The Big Takeaways

IT monitoring has always been complicated, but the complexity is taken to a whole other level when clouds are joined together. CA Unified Infrastructure Management makes monitoring such complex environments far easier by providing intuitive, end-to-end monitoring information for the entire IT infrastructure.

NOTES

NOTES



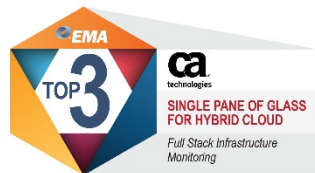
CA Unified Infrastructure Management



Analytics-driven monitoring for today's cloud and hybrid IT infrastructures

- + Optimize hybrid infrastructure experience. Use a single, analytics-driven solution to speed mean time to repair and enhance the user experience.
- + Reduce complexity and boost productivity. Eliminate the effort associated with using and managing multiple monitoring tools.
- + Improve resource utilization. Gain intelligent and holistic insights to optimize utilization across cloud and hybrid IT infrastructures.
- + Future proof your business. Leverage comprehensive coverage and an open, scalable architecture that can address your needs of today and adapt to emerging requirements.

For more details and a free trial please visit ca.com/uim



The cloud has fundamentally changed the technology operations landscape, and managing resource consumption has become more complicated as a result. With a diverse set of cloud deployment models available, it's more important than ever to establish deep insight into performance. Traditional monitoring tools are inadequate for modern infrastructures, and native monitoring tools lack the sophistication for hybrid and multi-cloud environments. In this book, you'll learn the best practices for monitoring complex clouds to deliver on SLAs, improve performance, and keep costs in-check.



About Brien M. Posey

Brien Posey is a 14-time Microsoft MVP and an internationally published author and conference speaker with over two decades of IT experience. In addition to his technology work, Posey is also a Commercial Scientist Astronaut Candidate.

(<http://www.brienposey.com/space>).

Follow him on Twitter @BrienPosey



ConversationalGeek®

Visit conversationalgeek.com for more books on topics geeks love.