Observability Trends and Pragmatic Techniques to Optimize Multicloud Operations

David S. Linthicum

LINTHICUM
RESEARCH

Introduction 3

Cloud Complexity and Costs Are the Problem 3

Observability And AIOps To The Rescue? 3

Conclusions 4

Things Are Becoming More Complex. Now What? 5

Complexity Impacts the Business 6

Complexity Can Be a Death Spiral 7

Single Cloud Vs Multicloud 8

State Of Observability 10

Components of Observability 10

Finding The Right Insights For Operation 13

Finding Trust Transparency 14

How Would Your AI Stand Up In Court? 14

Case Study 15

Call To Action 17

About The Author 18

Introduction

Complexity is now an issue after the deployment of complex cloud architectures, including hybrid- and multicloud. Indeed, many enterprises are finding that they are hitting a "complexity wall," or where enterprises understand that adding additional technology only makes the problem worse. Thus, the push to leverage best-of-breed technology becomes a clear business value that has a huge downside. For a business to become or stay relevant, it needs to figure out how to deal with complexity with approaches and innovations that can operate current and future systems in scalable ways. Operations teams that embrace observability can break the complexity wall.

Cloud complexity and costs are the problem

Typical hybrid architectures combine existing system operations with multicloud deployments. As enterprises continue their march to hybrid architectures, an epidemic of operational complexity continues to arise in their wake. Most IT operations find themselves on the edge of a cliff, in terms of the costs to operate and deal with these complex deployments. To make IT's life even more painful, outages and security breach risks may go up 10-fold.

Yes, innovative development within a company has a net benefit to the business. However, complexity is a byproduct. Those who build solutions will provide the most productivity and innovation by using best-of-breed services, which means they will introduce much more heterogeneity and an increased number of deployed platforms. This naturally leads to more end points to operate and more complexity to manage. Thus, the likelihood of more outages and breaches increases unless you can mediate the complexity by using better operational approaches and tooling.

Although we get different messages from cloud computing providers, we now have data that suggests public cloud outages are getting worse. The Uptime Institute recently released its 2022 Outage Analysis report that included findings such as "high outage rates remain an issue." One in five organizations reported a "serious" or "severe" outage that resulted in significant financial losses, reputational damage, compliance breaches, or, in some severe cases, loss of life. The report concludes that there has been a slight upward trend in the prevalence of major outages in the past three years.

Increased outages and breaches can result from many root causes. However, increased complexity takes the blame for most breaches and outages. Although this increase could be offset by doubling or tripling operations budgets and increasing the number of on-staff skills required, most corporate leaders won't view that as a viable option.

Observability and AIOps to the rescue?

So, what can be done to deal with the explosion in complexity? How about some solutions that will be more cost-effective than just tossing money at the problem? The industry now puts forth concepts such as "observability" and "AIOps" as new buzzwords that will save us from rising complexity by providing better insights and automation into traditional IT systems and better application monitoring approaches. The general premise is to provide a new layer of technologies and approaches that will save us from ourselves.

The applied reality is much different from the premise. Operations teams that embrace tools that provide observability soon discover a huge divide between promotions for the shiny new tool and the operations team's ability to effectively use that tool.

The new push by the cloud operations industry is toward the more pragmatic use of emerging concepts such as observability (as it relates to operations). The push for "observability" includes normalizing the approaches and concepts to make them more relatable and usable to rank-and-file operations teams. This means finding more pragmatic uses for the observability concepts, including better ways to present and better trust of the insights provided by advanced tooling such as AIOps and other operations tools. This brings us to the focus of this paper.

Conclusions reached in this paper include:

- Complexity is a reality that can't be avoided.
- The primary weapons to deal with complexity are automation and abstraction tools that leverage the objectives of observability.
- Complexity is a result of leveraging best-of-breed technology that utilizes core cloud services that are optimized for a specific solution.
- Observability needs to be a pragmatic concept that creates objectives for IT operations, including cloud and legacy systems.
- Core to the success of these solutions is to possess the capability and creativity to find the right insights from the gigabytes of data that spin off traditional monitoring systems and emerging AIOps platforms that support observability concepts.
- The need to move from overly abstract insights to practical and immediately actionable insights.
- Transparency of trust is a core issue.
- The observability maturity models presented in this paper will help determine your organization's level of observability maturity, and what can be done to progress to higher maturity levels that provide more business value.
- Identification of the most likely changes required in operational processes and tooling. How to create a change plan to reach a fully optimized operation. Changes affect culture, processes, approaches, and leveraged technology.
- IT operations' ability to holistically return value back to the business for all investments in the technology will measure the success of observability and supporting technology for your cloud and IT operations.

Things are becoming more complex. Now what?

Many enterprises have or will hit what's called a "complexity wall." This is the tipping point every enterprise reaches after adding a certain number of cloud-based systems. Remember, traditional systems still need to be operated and maintained, usually by the staff that's also trying to manage the complexity of new cloud-based systems. Eventually the number of operational resources (including technology and human resources) can't scale to effectively operate the systems. We can see this tipping point in Figure 1 at about 50 precent into a multicloud deployment (cloud and traditional systems) and ongoing operations over a 10-year period. Also keep in mind that this tipping point will vary depending upon the business sector and how well IT planned the deployment.

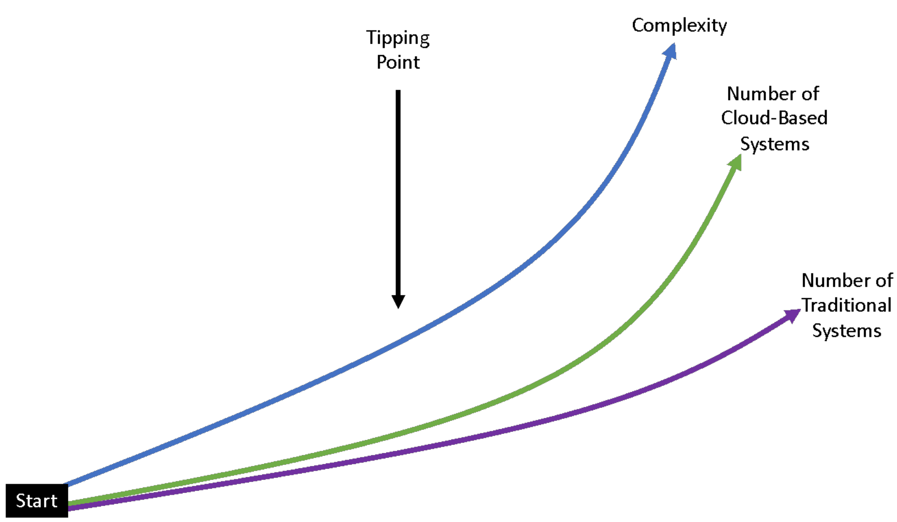

Figure 1: As we add more computer systems, cloud or not, the amount of complexity rises. This adds to the cost of operations, security, and governance. All deployments will reach a tipping point where adding more systems generates more complexity than can be cost justified.

So, what drives us to this complexity wall? First and foremost is the abundance of choice that we now have when it comes to services, which drives our ability to leverage best-of-breed technologies as force multipliers for business solutions. For instance, instead of having 10 different databases to leverage from a single cloud provider, a multicloud opens our cloud services catalogs to multiple cloud providers that offer access to as many as 100 different databases of all types and models. We can build a solution using the database that will bring the maximum amount of value back to the business, rather than having to settle for a database supported by a single specific cloud provider.

We can extend the best-of-breed benefits from cloud services to AI and machine learning systems, business analytics, security, and many other services that are instantly deployable from public cloud platforms. Another best-of-breed benefit is near zero latency between the selection of a service needed for a specific solution and getting that service deployed and operational.

Complexity is the drawback. Many multicloud deployments quickly surpass 5,000 services in use. There are many more moving parts to manage along with the increasing levels of complexity and heterogeneity that require skill sets you may not have on staff. Most IT managers struggle to keep the operational budget as level as possible. In some cases, managers reduced operations budgets based upon the premise made years ago that cloud computing would cost less.

Another report, Bridging the Cloud Transformation Gap, evaluates the findings of Aptum's annual Global Cloud Impact Study that's based upon the opinions of 400 senior IT decision makers. 62% of respondents cite complexity and abundance of choice as a hindrance when planning a cloud transformation. Clearly, complexity and abundance of choice problems are (or soon will be) on everyone's radar.

62% percent of respondents is a large number, even more than I thought would be aware of the problem. Of course, these are the IT leaders who understand that they have a problem. Based upon experience, the percentage of IT leaders/executives who actually have complexity problems is likely higher. One of the biggest sources of complexity that crops up in more advanced cloud projects involves mixing legacy systems with multicloud deployments.

Complexity impacts the business

Let's look at the business impact of rising complexity and heterogeneity. Many organizations have already hit that complexity wall and its tipping point, where the amount of complexity and heterogeneity extends beyond IT's ability to effectively manage the new levels of complexity. The resulting impact is that many of those enterprises will experience negative value. For each dollar they invest into new systems there is a loss of business value, such as adding services to multicloud or changing or adding traditional systems (see Figure 2).

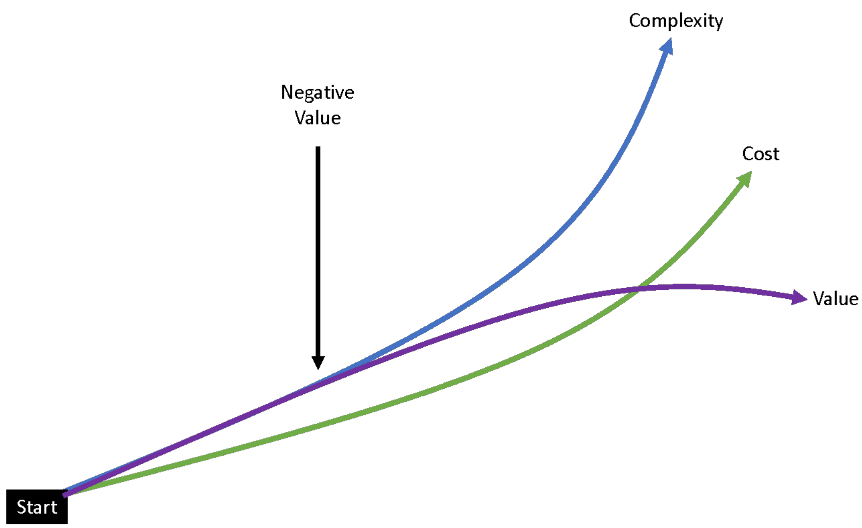

Figure 2: As we spend more money on computing, cloud and not, we increase complexity. At some point the additional investments generate negative value. From that point forward, what we spend on cloud and other systems (hard costs) returns a diminished or negative value to the business. Again, this must be offset by soft value business benefits such as agility, innovation, etc..

Figure 2 depicts a tipping point about halfway through a 10-year timeline. Again, each enterprise's tipping point depends upon how they leverage technology, cost optimization, and acceleration patterns of complexity and heterogeneity. Eventually they will add more applications, databases, and other services than they can effectively operate, given the available human and budgetary resources. Events that typically occur around the tipping point include outages that are caused by too many technology offerings managed by too few resources, rising security risks due to added complexity and heterogeneity with static security resources, and application performance and reliability issues that impact productivity and the ultimate customer experience. All these events will systemically damage the business.

Complexity can be a death spiral

While many of these risks can be managed if there are enough resources available to deal with them, the likelihood is that complexity becomes a death spiral as more best-of-breed choices are made to support the business. The more complexity, the greater the cost and impact of dealing with that complexity.

Many enterprises that see complexity becoming a challenge have decided to deal with it via policy. They limit the use of cloud services to a single public cloud provider that they consider the enterprise's 'primary cloud.' Thus, complexity is mediated by setting strict polices that forbid employees from using other public clouds, no matter how compelling the reasons. Most IT organizations carry out this policy by refusing to support other cloud providers, thus forbidding the use of best-of-breed technology. This approach will backfire as well, and perhaps produce an even more negative impact than complexity itself.

Single cloud vs multicloud

Figure 3 depicts two approaches to solve a problem where the "Need for Innovation" is the same for both scenarios. The first depicts a single cloud deployment with other cloud usage banned by policies. The second depicts a multicloud deployment that includes the choice of best-of-breed technology that typically provides more business value.

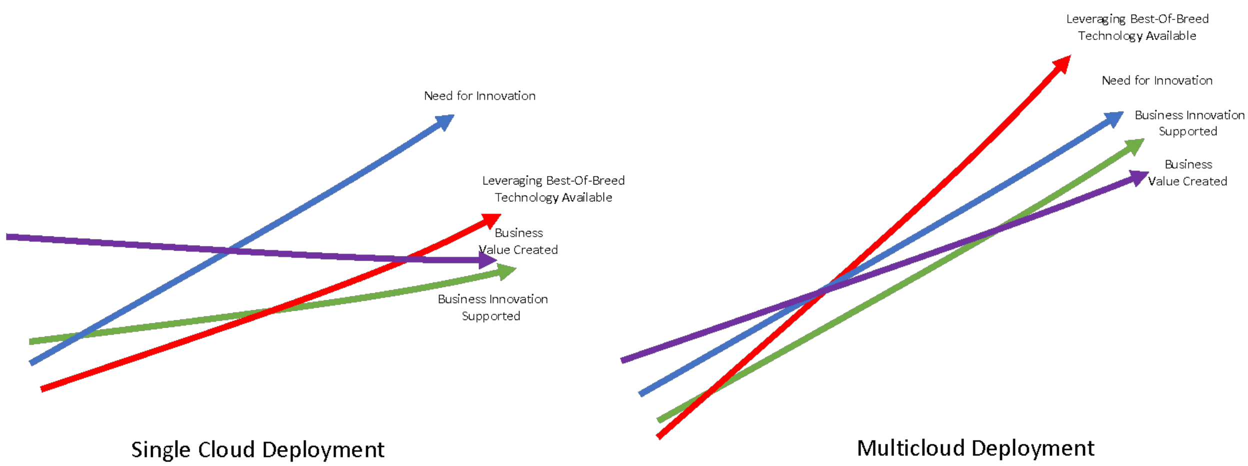

Figure 3: Leveraging a single public cloud provider limits the technology we can use. This leads to less optimized solutions than if we had access to more cloud services or best-of-breed technologies that could create more innovative solutions. When leveraging a multicloud, you have access to more cloud services and thus more cloud technology such as specialized analytics, AI and high-speed computing. You can use whatever services you need to optimize your business solutions which will support more innovation and thus grow business value. These are the primary reasons we leverage multicloud.

As you can see, the single cloud model can't respond to any increased need for innovation and access to best-of-breed technology is limited to the cloud services included with the enterprise's primary cloud. In turn, diminished use of best-of-breed technology also diminishes the level of "Business Innovation Supported" and "Business Value Created." The enterprise's primary cloud provider may offer some general best-of-breed services, but the overall percentage that applies to specific scenarios and deployments will be small.

The multicloud deployment model defines more complexity that also delivers more business value. There are no limitations on the use of best-of-breed technology for the multicloud deployment, or, in this case, public cloud services from any public cloud on the market. This allows developers to find optimal cloud services for the problems they want to solve vs. making do with services that happen to be available from a single IT-approved cloud provider. Thus, the ability to "Leverage Best-Of-Breed Technology Available" raises the levels of "Business Innovation Supported," and, more importantly, increases "Business Value Created." Therefore, limiting complexity by policy has a substantial negative impact on the business.

Figure 4 depicts a multicloud deployment where the number of services (including platforms, databases, etc.) can be expanded by adding more cloud providers, and thus more choice of the cloud services that solution developers can leverage to create solutions that drive more value to the business.

These days businesses are valued by their ability to innovate. Innovators can take existing businesses from the brink of irrelevance or bankruptcy back onto solid ground. Examples are magazines and newspapers that no longer print a single word on paper, delivery services with world-wide point-to-point tracking, or retailers that no longer own physical stores but thrive online. Innovators can also take advantage of new markets such as house rental services that own no real-estate or taxi services that own no taxis. Innovation and digital transformation will define next generation business value. For innovation and transformation to thrive, there can be no limitation on what tools innovators can leverage to optimize innovation and thus optimize business value.

For a business to become or stay relevant, it needs to figure out how to deal with complexity with approaches and innovations that can operate current and future systems in scalable ways. The remainder of this paper will address how to leverage modern technologies such as AIOps along with observability to deal with complexity on complexity's terms.

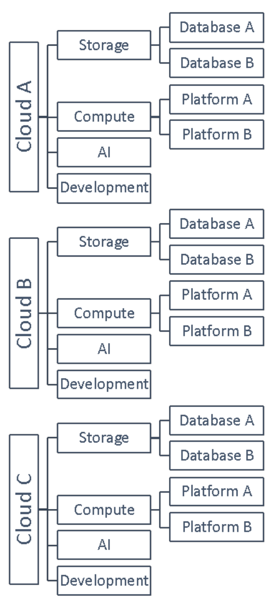

Figure 4: Choice relates to best-of-breed and its ability to enhance innovation. This is the single highest reason that enterprises move to multicloud. They have access to more services, including types of services, that are provided by different public cloud providers. However, you must figure out operations, security, and governance for each cloud. That additional complexity costs more time and money.

State of observability

Fact: Using best-of-breed technology creates complexity that can lead to a true business value, considering that it's able to provide better innovation to the business, but it's still a core challenge. So, how do we solve the complexity management problem? The key is to find tools, where observability is an outcome, to deal with the rising complexity. This is something that has been evolving over the years, with a few key approaches and technologies that promise to deal with the complexity challenge.

Observability itself, both the term and the concept, has evolved over years. At its core, observability provides the ability to monitor internal states of systems. Observability uses externally exhibited characteristics that can predict the future behavior of those monitored systems using data analysis and other technologies. Core to the observability concept is the ability to find insights that are unapparent by just looking at the monitored data.

Tools that provide observability as an outcome and automation, makes it possible to build hyper-automated, self-healing enterprises that fully understand what's happening within the systems under management. This is the definition of observability. It moves the enterprise to a state where core business systems in and out of the cloud are operated in a way that solves issues before they become issues. Proactive maintenance and operations lead to much higher uptime that approaches zero outages and lower operational costs. An inflection of complexity and heterogeneity no longer impacts the business. Thus, no complexity wall and no tipping point.

Enterprises can reactively fix issues as they occur by monitoring systems and fixing problems as they arise. Proactive observability helps predict issues before they become issues. A proactive enterprise can deploy very complex systems without impacting the return value of those systems. If used correctly, observability allows enterprises to leverage best-of-breed technology and its resulting complexity with little or no impact on the business.

Observability is strategic while monitoring is tactical. There are many places to learn about the differences between the two, so we won't dwell on these concepts here. Instead let's focus on the value of observability as a concept, and how to implement observability using technology that you can leverage today.

Components of observability

So, what's the value of observability as a concept? Let's break it down into components. Figure 5 represents the major components of observability as related to IT operations, cloud and non-cloud:

Trending: What patterns occur over time and what do they mean for future behavior? For example, if performance trends downward, that indicates likely I/O problems that arise from organic database growth. This is based upon historical and current data, and then using this as training data for an AI system such as AIOps.

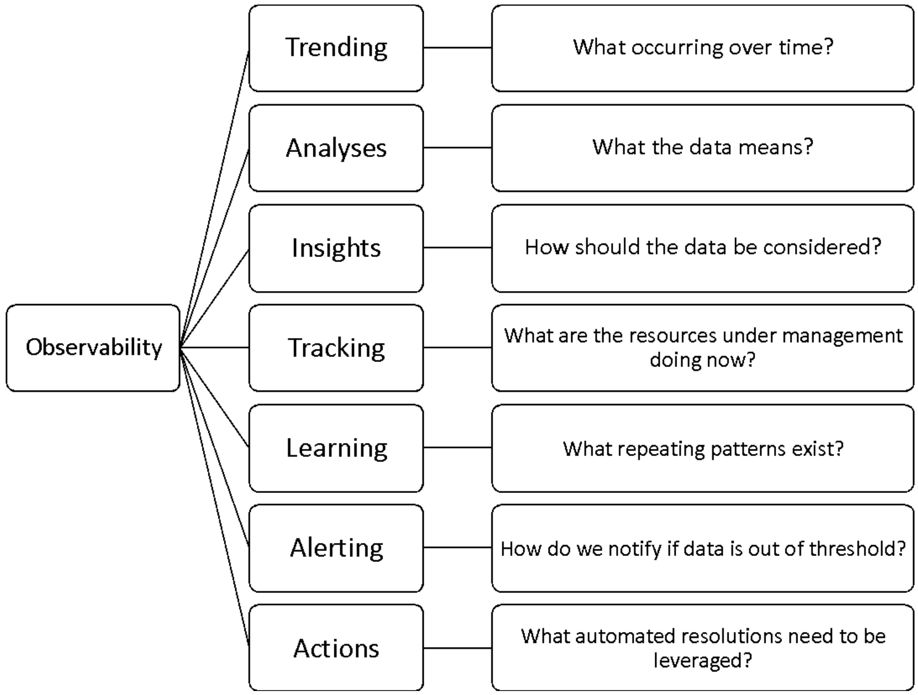

Figure 5: Observability provides thoughtful insights around considerable amounts of interrelated data by reviewing trends and patterns, continuously learning and alerting when actions need to be taken.

Analyses: What the data means and any insights we can draw from the data. Observability provides the ability to analyze what the data means. This is a core feature of observability that sets it apart from just monitoring the data. This analysis can be very deep and complex, such as determining training requirements based upon system outages analysis. Or it can be rudimentary, such as determining that a drop in network traffic means there is a 67% probability that an I/O error exists in a core storage system.

Insights: What we can understand from the data, or what we need to understand from the data. This involves finding meaning in the data that's not readily understood or apparent. For example, finding correlations between a rise in sales revenue and a drop in overall system performance. This doesn't make sense on the surface. A decrease in system performance usually has a negative impact on customer access and sales order entry. However, in this case, excessive users on the sales order system (including the ecommerce Web site) pushed down system performance. Thus, the operations team can take action to ensure that capacity will increase elastically to support more sales activities. Many won't suspect that these data points are connected, but observability allows you to get such insights into past, current, and even forecasted data,

Tracking: Monitoring systems activity data in real time or near real time, and leveraging this data to find, diagnose, and fix issues ongoing. Traditional tracking monitors the activity of multiple systems in the cloud and in the data center. Under the concept of observability, the system can find dynamic insights around real-time data and look at it in the context of related operations data. The system may determine and diagnose issues that can be self-healed through automation. For example, tracking CPU performance of a single virtual server that exists on a major IaaS provider. Tracking can provide real-time insights as to what this performance data means in relation to future performance, processor failure, memory failure, and other insights that may be derived from this relatively innocuous data that was once displayed on an operator's dashboard for a few seconds and then gone forever.

Learning: Learning systems look at massive amount of data to find trends and insights, and then leverage that data to learn about emerging patterns and what they mean. Any system that embraces the concept of observability leverages AI systems to train knowledge engines around patterns of data. This can be simple patterns such as an increase in the internal temperature of a server that will accurately indicate an impending failure, which is something that most humans experienced with IT operations already understand. Looking at the correlation of systems' data from hundreds of sources involves much more complex uses of learning to look at patterns over time and what they typically indicate. This can include performance data from specific applications, networks, database, I/O, and so forth.

The knowledge engine can identify and use these patterns to predict and avoid negative issues that impact operations. Complex patterns will emerge that may encompass detailed review of thousands of current and historical data sets to pinpoint most network, storage, and application failures before they happen. Humans can never physically replicate the same processes to achieve this level of understanding.

Alerting: What issues need to be dealt with in a timely manner? For example, a low-level priority alert for a network performance issue that will eventually lead to the replacement of a network hub. Or an immediate alert that requires immediate attention, such as capacity that needs to be automatically expanded because an application processing load is nearing the limits of a virtual server cluster in the cloud. Again, these can be simple alerts that just let a system or human know about some issue or warning while complex alerts could go out based upon different humans and/or systems that need to be involved.

This is a key component of observability that's often overlooked. Remember, the alerts themselves are a result of analytics, insights, trending, and learning, where the alerts and the actions (covered next) all become part of the data that encompasses observability.

Actions: What happens because of an alert? It could result in a manual action such as rebooting a cloud-based server, or some automated action such as kicking off very sophisticated processing to automatically recover from a ransomware attack before there is an impact on core business systems. Complex actions may involve dozens of actions taken by humans and thousands of automated actions to carry out immediate self-healing operations.

Observability provides the ability to manage and monitor modern systems that include applications built to run at faster velocities with more agile features. It will no longer work to deploy applications and then bolt on monitoring and management tools. The new tools must do so much more than simply monitor operations data. Refer to Figure 5 when it's time to build a machine that will define what your data means and how it must be acted upon.

Finding the right insights for operation

So, if observability requires a holistic understanding of the deeper meaning of operational data, how do we define the required insights? More importantly, how do we define the actions to take?

Figure 6 shows some types of useful insights that may come from observability. This includes questions that need to be asked. Based upon the data and other current insights, what will happen? If something happens, what happened and how does it affect other things? What's the current state of the data (what's going on now), and how does that corelate with historical and forecasted data? What specific insights are important and should alerts be generated? If so, to whom?

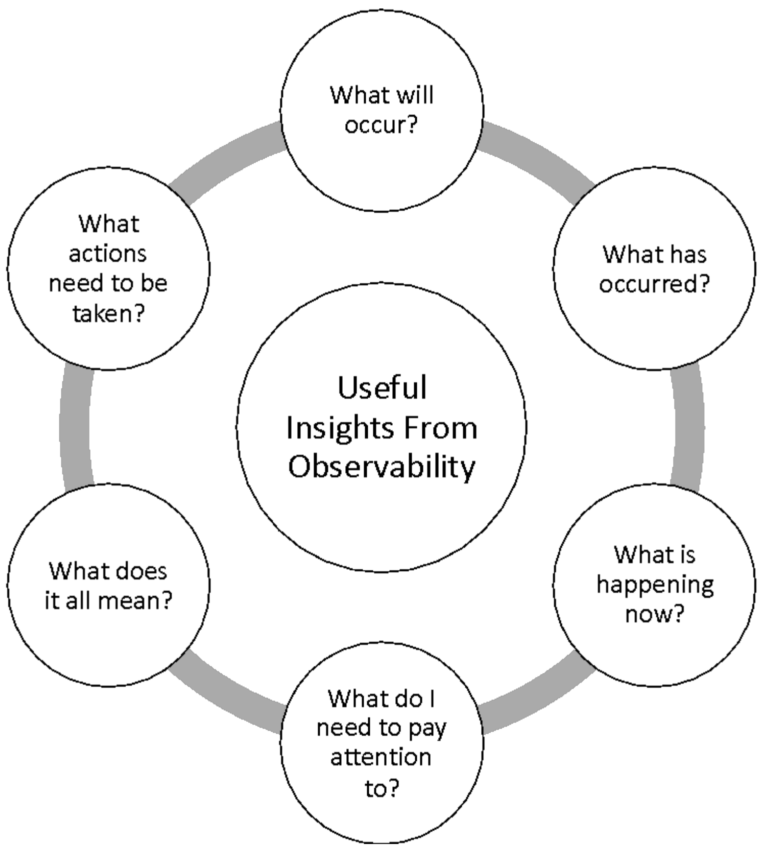

Figure 6: To find value from any observability approach and supporting technology, determine the state of data. For example, determine the state of data from systems under management in the past, current, and forecasted future. What things need to be considered and what actions need to take place? Assemble all of this under a learning framework that can turn massive amounts of interrelated data into repeatable understandings.

Also consider more holistic insights, such as a more comprehensive look at the meaning and patterns of the data. This is where learning functions come into play with their ability to decipher complex data and patterns of data to come up with insights that are based upon thousands of data points and millions of data records gathered over the course of years. Finally, determine what actions need to be taken. This includes the timing of the actions, involvement of humans and systems, and how to deal with complex actions such as self-healing processes that have dependencies. For instance, the sales order entry system should not be shut down until all users on the system have been alerted and they successfully log off.

Finding trust transparency

Trust needs to exist between systems and humans, and systems that are relied upon to make core decisions around important processes such as cloud operations and security operations. Trust transparency is the core means to explain data sources, data provenance, model algorithms, and model outcomes to mitigate any emerging concerns pertaining to fairness, equality, inclusivity, and privacy. It's about earning the trust of human users and validating their trust in the systems they use to react to data-oriented and cognitive decisions being made by automated mechanisms.

Trust in the fidelity of core business processes and supporting technology is built upon transparent and ethical AI. Focus the concepts of observability on cloud and IT operations in our care to build trust and faith that the data being generated and the decisions being made are free from erroneous data, innate biases, and outright errors. A lack of transparency is what makes the use of cognitive systems untrustworthy.

For example, approximately one-third of executives in a recent Deloitte survey named ethical risks as one of the top three concerns related to AI for any purpose. While this leads to issues with complex knowledge engines that deal with important tasks, such as approving loans, this is likely not to be an issue as related to operations, or AIOps. However, transparency is the key to eliminate growing unease about the uses of these emerging systems. As observability implementations within tools such as AIOps become the standard in cloud operations, transparency should be a highly valued characteristic.

How would your AI stand up in court?

That challenge with AI systems is not that they function, it's that they are trusted. This includes AI systems that are tightly coupled with data, such as training data. The system won't provide a core value if the data and decisions generated are called into question or, worst case, prove incorrect. Many who leverage AI systems still consider AI to be a "black box" project that is beyond scrutiny. Therefore, many of these AI systems do not provide the transparency that many need to trust AI and AI-generated data.

AI systems and coupled data need to have as much transparency as needed to gain trust. Even your own. Yes, you 'know' the AIOps-generated data is 'right.' How do you prove it's right? AIOps technology systems will make critical business decisions that could potentially create a catastrophic business failure, such as major system outages that are a result of faulty data or cognitive processing. It's one thousand times better to discover a significant oversight or transposition error before a business-critical system deploys than if it implodes one week, month, or a year later. If you build transparency into the system and thoroughly test it, you will be the one to discover any problems. Encourage users to help test transparency but incorporate their help before deployment.

The core lesson here is that you must leverage cognitive systems to drive IT operations and leverage the value of true observability. It's equally important to provide transparency so that those who need to trust these systems understand specifically what the systems are doing and how they operate. This is foundational to the use of the most cognitive-capable technology to bring the value of observability to enterprises. Success in this endeavor will move the enterprise toward a fully automated zero touch operations state and the highest operations maturity level.

Case study

To illustrate the value of observability it's helpful to walk through a simple case study. This case study demonstrates the steps to maturity that many organizations will progress through as they improve their ability to leverage observability to reach a state where operations are fully optimized using AIOps or other tools. This typically means zero touch, where most IT operations are fully automated, including core observability processing. Thus, complexity is fully mitigated and we reach a point where the number of humans needed to drive these processes is minimized as well. This comes with the added benefit of creating a foundational architecture where the tradeoff to creating more complexity is the high business value provided by best-of-breed services for solutions built by innovators who can take the business to the next level.

Figure 7 is an observability maturity model for IT operations, including cloud and legacy operations. It's a good guide for the progression of a company that wants to optimize observability for IT operations. Note that we define these degrees of maturity as CloudOps (cloud operations) 1.0, 2.0, 3.0, and 4.0. The lower number, 1.0, is the least amount of observability maturity, and the highest, 4.0, is the most amount of maturity. The higher numbers come with more advanced capabilities and technologies deployed and thus generate the most business value. Obviously, it's desirable to move from the lowest to the highest maturity levels.

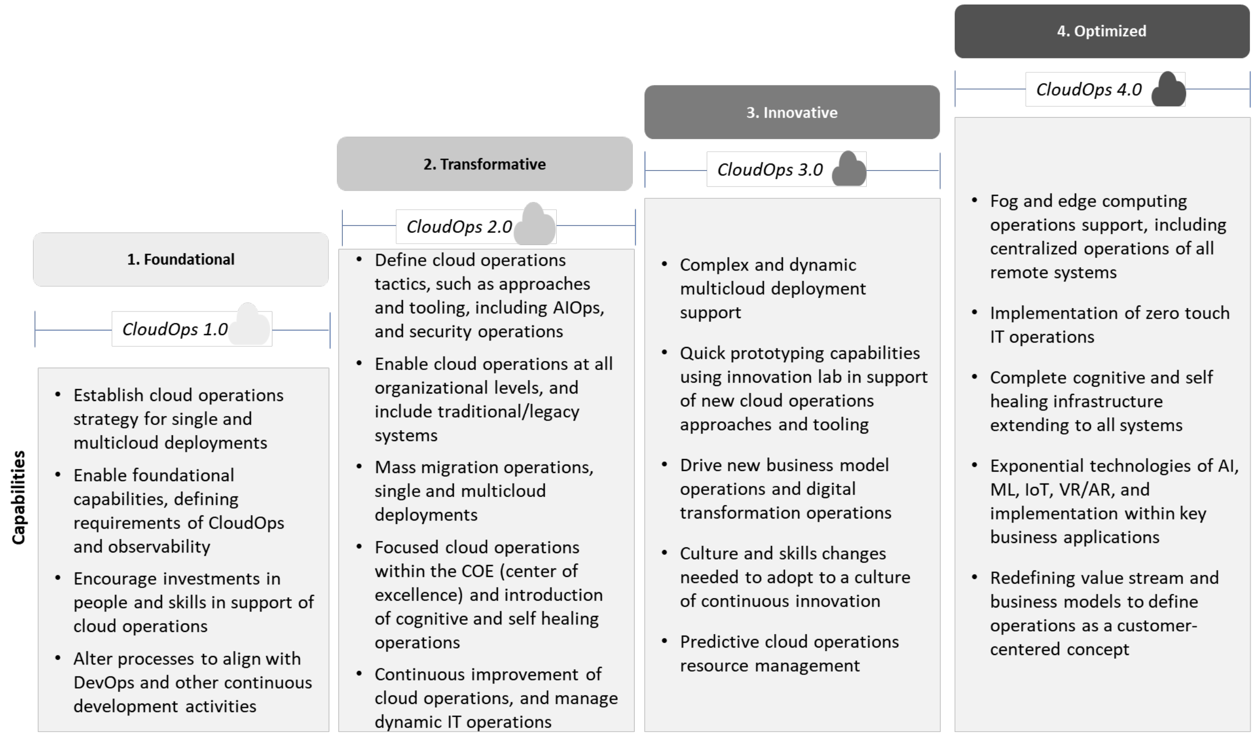

Figure 7: Using operations-oriented observability we can define several steps of maturity that enterprises will progress through to achieve "zero touch" IT operations that include all cloud and non-cloud resources.

To begin the journey, our company would first start with capabilities that are considered "Foundational," or CloudOps 1.0. They could even build upon existing operational approaches and tooling to find a starting point for next generation IT operations, including ongoing cloud operations. The most important capability here would be to establish a cloud operations strategy that would cover a single and multicloud deployment, as well as extend operations to legacy systems.

If our company progressed to CloudOps 2.0 "Transformative," the most important capability to add for that level of maturity would include defining the cloud operations tactics to support observability. This would include adding AIOps and other tooling, which is just an implementation of the cloud operations strategy that we created at the previous level of maturity.

At CloudOps 3.0 and 4.0, "Innovative" and "Optimized," respectively, many of these capabilities take our company to the next level to return value back to the business for the investment made in observability approaches and tooling. Some of the most important capabilities include the ability to support complex cloud deployments, such as complex and distributed multiclouds that would also include traditional systems (legacy) under the observability umbrella. Moving up, a fully optimized maturity state includes the ultimate destination of zero touch IT operations that include fully optimized and automated legacy and cloud operations. Humans have been removed from the operations processes, including fully automated self-healing systems that proactively correct operational issues using cognitive tools such as AIOps and other force multipliers to fully automate all IT operations.

Call to action

Businesses leave money on the table when it comes to the optimization of IT operations when they are using solutions that only provide tactical metrics that don't provide the insights required for today's businesses. The biggest opportunities to recoup that money require optimization of existing legacy systems and emerging multicloud deployments. Many organizations do not yet see this as a deficiency because most IT organizations do not yet track operations around its ability to return business value.

The focus is shifting to operational concepts such as observability and the ability to leverage emerging technologies (such as AIOps) as true force multipliers. These concepts will take operations to the highest maturity levels, and thus optimize operations' ability to return more value to the business. Businesses that ignore observability opportunities will find negative value of IT investments will be a fundamental reason why IT will fail to provide business value, and thus drive business failure.

The call to action is one of understanding. Complexity is a byproduct of multicloud and other complex distributed architecture deployments. These types of deployments can't be avoided given the innovative advantages that they offer a business. We need to understand the core tenets of observability and learn how to weaponize observability using AIOps and other tooling that optimizes the business for business agility and innovation. That's where you'll find the business value.

About the author

David Linthicum is on most top 10 lists of technology innovators and influencers, including cloud computing, edge computing, and security concepts. David is a best-selling author of over 15 books and over 7,000 published articles. He is also the originator of many business-related technology concepts, including Enterprise Application Integration (EAI). He's an innovator within Service-Oriented Architecture (SOA), and now cloud computing and the use of cloud computing for digital transformations.

David's 50+ courses on LinkedIn Learning consistently appear on the "Popular Courses" list and provide course content on cloud computing, cloud architecture, cloud security, cloud governance, cloud operations, DevOps, and many other concepts related to cloud computing and enterprise technology in general. He's also an adjunct professor for Louisiana State University (LSU), where he's created courses on DevOps, Cloud Computing, Cloud Architecture, and other courses that are in-demand by the LSU student body. David has done over 1,000 conference presentations in the U.S. and abroad, often as a keynote speaker at conferences related to enterprise technology. He has hosted over 2,000 Webinars on the correct use of enterprise technology, including cloud computing, edge computing, DevOps, and data science.

David's holistic view of the technology value model cuts through the hype cycles and other distractions to provide clear solutions. His goal is to provide opportunities for businesses to lead their markets by weaponizing technology to provide better products, services, and customer experiences. His mission is to use innovative technology approaches that provide the best outcomes for his clients.