CLOUDTRUTH

Configuration Management for Today's Cloud

The rise of containers and serverless means infrastructure and application configuration is becoming distributed & decentralized and "pushed to the edge." Organizations need visibility and control to ensure security & reliability goals are met.

CloudTruth, Inc. | Spring 2020 Position Paper

Table of Contents

Executive Summary

- Cloud configuration is moving into the application layer for speed and innovation.
- The unfortunate downside is increased configuration complexity, pressures on customization and organizational and process misalignment.
- Three approaches to ameliorate this complexity lie in review of existing configuration integration, cross team training and awareness, and new solutions to improve visibility across the newly distributed and decentralized world of cloud configuration.

What We'll Cover in This White Paper

Containers, serverless and infrastructure as code (IaC) techniques are changing the way modern cloud systems are configured. Applications and components are becoming self-contained, with substantial infrastructure configuration embedded inside their source repositories. Along with this, system configuration is becoming decentralized and distributed, which substantially increases the difficulty of managing the cross-cutting concerns of security, compliance and reliability. And when these self-contained components are also inconsistent across time - from development to testing to staging to production - the complexity increases.

Methodology

CloudTuth interviewed over one hundred IT professionals across roles ranging from CTO, CIO, VP Eng, DevOps, CISO and SecOps to research their perspectives on the current state of cloud configuration management, the challenges they were experiencing across their teams, and the tools they were using or missing to address change management.

1. Cloud Configuration Challenges

1.1 Keeping Up with Innovation

As millions of people adjust to working virtually during the Covid-19 pandemic, software as a service (SaaS) applications, and the public cloud infrastructure they rely on, have expanded overnight to keep up with increased online activity. And when we are on the other side of this health crisis, it is likely that our work habits will be permanently modified to accommodate more online work. As a result, application developers are under even more pressure to bring new multi-cloud applications and advanced versions of existing ones to market quickly.

However, application development tools are also advancing quickly. Applications and components are becoming self-contained, with substantial infrastructure configuration embedded inside their source repositories. As a result, there is a more distributed and decentralized definition of the system configuration which substantially increases the difficulty of managing the cross-cutting concerns of the organization like security, compliance and reliability. When these self-contained components are also inconsistent across time - from development to testing to staging to production - the challenge increases.

The resulting complexity has been an underlying cause of unexpected downtime and security breaches. These days, any organization with a SaaS offering that engages customers via the cloud can recall an incident or close call where the security of their software was made vulnerable or the application experienced unexpected downtime.

This comes at great cost to business. A 2020 Divvy Cloud study of publicly-reported breaches estimated that 21.2 billion records were exposed in 2019 at the cost of $3.18 trillion. As for downtime, we learned last summer that one to five minutes cost Google upwards of $500,000 (never mind the cost to those who depend on Google) and an hour of downtime cost Amazon nearly $5 million.

69% of enterprises are moving towards hybrid adoption

84% of enterprises are adopting multicloud strategy

75% of network outages and performance issues result from misconfiguration

https://www.channelpartnersonline.com/2019/02/27/multicloud-hybrid-cloud-adoption-growing
https://blog.ipswitch.com/best-practices-in-network-configuration-and-change-management

How, in a world of increasingly sophisticated rapid development tools and environments, can this be happening? Let's look more closely at what's causing the accelerating complexity.

1.2 Advances in Cloud Tech – Greater Speed but Added Complexity

In short, today's application developers benefit from an expanding tools ecosystem allowing faster time to market for new features, but these new conveniences increase the complexity of managing configurations in development, test, staging and production environments. The impact of this can be seen in three major areas:

Operating in a Fog of Accumulating, Interconnected Cloud Systems

The cloud world includes micro services, 3rd party systems, serverless computing, and a service mesh to connect it all together. The surface area is huge, and the amount of configuration and security information required to stitch it all together creates an unsustainable cognitive load for your team. Worse, each of these new wonderful services often comes with it's own bespoke configuration approach, and it's own management tooling.

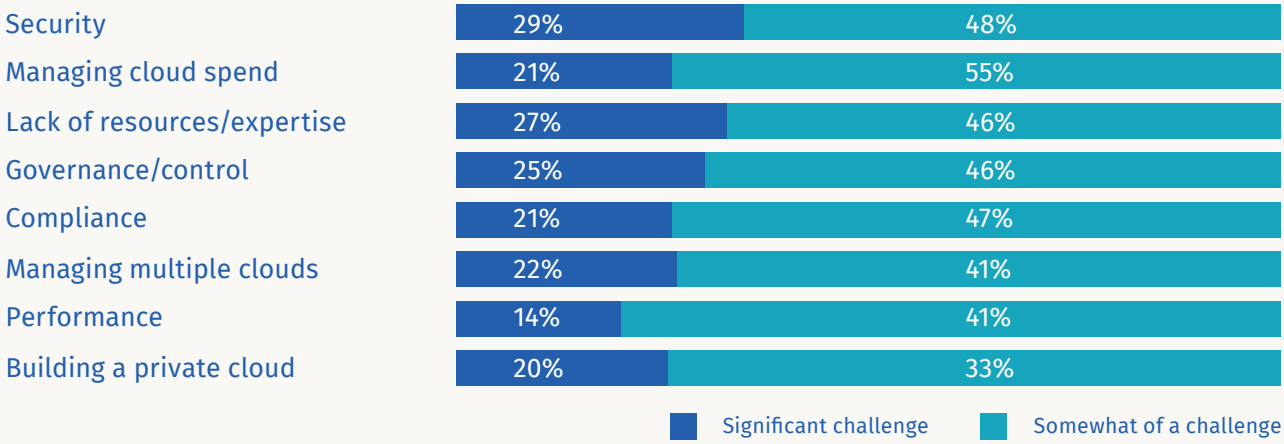
We don't live exclusively in the "data center model" anymore, where system admins and in-house developers built everything themselves and had visibility into all the entire stack. Today's complexity has changed that.

Unchecked, this can slow you down when you think it will speed you up, and really hurt your repair efforts when something goes wrong.

Take, for example, Auth0, a SaaS tool that helps companies manage user identity and access controls without needing to build that capability internally. Services like this speed up development time for companies where authenticating users is necessary but not core enough to the business to justify building equivalent functionality in-house. But here's the catch: services like Auth0 offer a whole host of different configuration settings and customization options in order to address needs across a wide range of different customer applications, and to make the most effective use of these tools, those settings need to be managed appropriately. Compared to an in-house solution that is designed and managed for a single specific use case, this adds more complexity.

The average cloud technology stack subscribes to at least six third-party services such as Auth0. Multiply that times an increasing number of similar tools in the company's tech stack, and not only does each of those systems require its own configuration, but the configuration of each system impacts the configurations of other systems, creating a network effect of exponential complexity. The danger? Any "shared team awareness" across these varied and interdependent configurations either dissolves as the development team grows and specializes, or worse, disappears entirely with team change and turnover.

Cloud Challenges



Source: RightScale 2018 State of the Cloud Report

Choosing between Customization and Reliability/Security

As cloud systems grow more complex, configuration setting oversight lags, and that impacts the security and reliability of the entire product in unpredictable ways. Because of inter-dependent functionalities, troubleshooting problems to determine the root cause takes longer and often requires the expertise of senior developers. As a result, a small product reliability bug or security flaw can snowball into a larger issue and larger productivity hit.

Even Google engineers have experienced this. During their outage last summer, according to Benjamin Treynor Sloss, Google's VP of engineering, “Engineering teams detected the issue within seconds, but diagnosis and correction took far longer than our target of a few minutes. Once alerted, engineering teams quickly identified the cause of the network congestion, but the same network congestion which was creating service degradation also slowed the engineering teams’ ability to restore the correct configurations, prolonging the outage.”

Cloud customers must move beyond the defaults, or risk becoming obsolete.

One fallback is to stick with the default configuration settings for each tool in the stack, but as soon as a project needs to scale, moving beyond default settings is required to improve performance. Skipping the tuning phase will diminish the value of the tool, which may have been the reason for choosing it in the first place.

Adapting to Cloud Evolution - Organizational and Process Impact

One logical reaction of fast-moving organizations is to attempt to define and build their own tool in-house to manage these systems, but this takes time and resources away from critical product development work. Since developing these tools is only tangentially related to the core business, there is rarely an adequate budget for both initial development and on-going improvements. Bespoke DIY tools often become a spare-time activity, and become a maintenance headache over time.

Traditional organizational charts simply don't account for the additional resources necessary to manage these new, complex systems.

In the past, companies hired individual personnel to manage specific systems (example: A DBA for all the databases, a network engineer for VPN, WAN, etc.), and it would be relatively straightforward to determine the necessary skill set for the job. Today, individual systems are no longer isolated, and so developers with experience in single systems will struggle to effectively manage the matrix of tools that comprise the modern tech stack. As such, companies are searching for people with experience in managing complex, multi-layered cloud systems. These cloud operations experts are hard to find, both because the necessary experience is less common, and also because it can be difficult to develop quantitative hiring practices and clear job descriptions for the right fit.

Finally, the interconnectedness of the various tools that support different parts of the organization can make traditional development team structures less effective. If multiple teams are working in parallel on separate components of an integrated system, it can be challenging to ensure coordination between those teams. This can result in duplicated effort, conflicting efforts, and other personnel issues that interfere with productivity. Many people start with "out of the box" defaults to reduce complexity, but in the long run that will only work in the most basic of cases, and will negate all the increased efficiency and performance improvement made possible by new, integrated tools.

What, then, can organizations do to remove the fog, empower customization without increased risk, and support a more productive team environment?

1.3 Steps to Build Team Visibility + Coordination Around a Single Record of Truth

Consider these three steps to manage these highly customizable cloud ecosystems:

Evaluation and decoupling of unnecessary integrations

Hiring, training and awareness to support cross-team collaboration

Sharing a single consolidated view of configurations across the ecosystem

Or course, wherever possible, cloud customers should decouple systems which have become unnecessarily entangled over time. If component tools can work in isolation, there is less risk of a domino effect of taking down the entire system when a single piece has an issue. A cost benefit analysis of integration for improved efficiency versus system isolation for minimized failure impact needs to be conducted holistically across the cloud ecosystem.

In addition, integrated systems require integrated teams, which is why cloud customers are hiring for diverse skill sets, as well as restructuring teams to encourage cross-functional collaboration and communication. As organizations adapt to new tools and technologies, it is vital to ensure that employees at every level and function -- from junior developers to middle management to senior leadership -- are communicating openly and effectively.

But most importantly, a consolidated view of configurations across all cloud systems – a single record of truth – becomes the glue for teams that now work independently but need to benefit from the learnings of other teams. For simple systems, in-house management tools may be sufficient, but for most scaled-up, tech-savvy companies, a third-party configuration management solution is the missing piece to ensuring that critical systems are always updated and configured properly.

As a result of this research, CloudTruth has focused on delivering a single record of truth across the cloud via a SaaS configuration orchestration platform with a central configuration data hub that combines all the cloud ecosystem configuration settings and files in a way that:

- makes configuration settings understandable to all parts of the organization responsible for application security and support,
- speeds up access control,
- builds confidence in the correct provisioning of new releases,
- makes troubleshooting a matter of minutes rather than hours, and
- facilitates audit and compliance.

Over time, analytics and machine learning layered on top of the central configuration database will reveal system tuning best practices (not just individual system settings), automate the prevention of configuration errors and orchestrate global configuration change implementations.

2. Conclusion

Today's development teams should not feel like they must sacrifice innovation and speed for reliability and security. But efficient guardrails are needed to make this happen.

While building visibility and coordination across a myriad of cloud tools is a big undertaking, CloudTruth is dedicated to this goal, making it possible for development teams to choose and customize best of breed tools while maintaining coordination, operations and infrastructure leaders to focus on performance evolution rather than fire drills, and security professionals to look ahead to future risk prevention rather than catching existing threats in the making.

Contacts

cloudtruth.com

hello@cloudtruth.com

(617) 297-8890

Boston & Chicago

3. References

[1] https://www.channelpartnersonline.com/2019/02/27/multicloud-hybrid-cloud-adoption-growing/

[2] https://blog.ipswitch.com/best-practices-in-network-configuration-and-change-management

[3] https://itrevolution.com/team-cognitive-load-team-topologies

[4] https://securityboulevard.com/2020/01/api-security-a-top-concern-for-cybersecurity-in-2020/

[5] https://www.oreilly.com/library/view/infrastructure-as-code/9781491924334/ch01.html

[6] https://www.infoworld.com/article/3250255/standard-or-custom-cloud-instances-how-to-decide.html

[7] https://www.forbes.com/sites/emilsayegh/2020/03/05/3-steps-to-address-the-cloud-talent-drought/

[8] https://www.infoworld.com/article/3250255/standard-or-custom-cloud-instances-how-to-decide.html

[9] https://teamtopologies.com/videos-and-slides/2019/08/28/beyond-the-spotify-model-using-team-topologies-for-fast-flow-and-organisation-evolution