

Cloud Computing

The Value of Application Service Governance for Cloud Computing



Layer 7 Technologies

White Paper



Contents

- Introduction 3
 - Why do Governance? 3
- Application Service Governance Technology 5
 - The Value of Application Service Governance for Cloud Computing 5
- Conclusions 8
 - About the Authors 9
- About Layer 7 Technologies 10
- Contact Layer 7 Technologies 10
- Legal Information 10

Introduction

Governance as related to service, or application service governance, is most applicable to the use of cloud computing since companies basically define their Service-Oriented Architecture (SOA) as a set of services that are relocate-able between on-premise and cloud computing-based systems, whether that be in a publicly hosted or private cloud environment. SOA is the approach here, and thus SOA or application service governance is the approach and the technology that will be leveraged to manage the services within the enterprise and cloud.

The way in which you implement application service governance and security is just as important to the concept. We implement application service governance and security technology systems to avoid risk when implementing a system in a piecemeal and ad-hoc way. However, if application governance and security is layered into the organization as an ongoing project, this will quickly diminish the value of leveraging cloud computing.

In this paper we'll look at the value of application service governance and security in the context of cloud computing. These are the issues you need to consider as you move your governance and security strategy forward in the shift toward cloud computing, specifically understanding the value and the tradeoffs.

Why do Governance?

We do governance for the simple reason that, once we get to a certain number of services, we won't be able to keep track of them all and provide the control they will require. Those who build SOA call this the "tipping point," or the point where the number of services under management becomes so high that it's impossible to manage them properly without a governance model, approach, and service governance technology.

Governance places a layer of processes and technology around the services so that anything occurring...will be quickly known.

The number of services, as well as the complexities around using those services within the context of cloud computing, makes application service governance even more compelling, including:

- Location of the services
- Service dependencies
- Service monitoring
- Service security

Many of the services are not hosted and owned by the business; they are cloud-based, and thus controls need to be placed around them to mediate the risks. What is important when leveraging on-premise SOAs is even more important in the world of cloud computing. In essence, it's using the model of "trust, but verify," placing a layer of processes and technology around the services so that anything occurring, such as a change to services or services not operating properly, will be quickly known, allowing you to take corrective action, or perhaps allowing the technology itself to self-correct (see Figure 1).

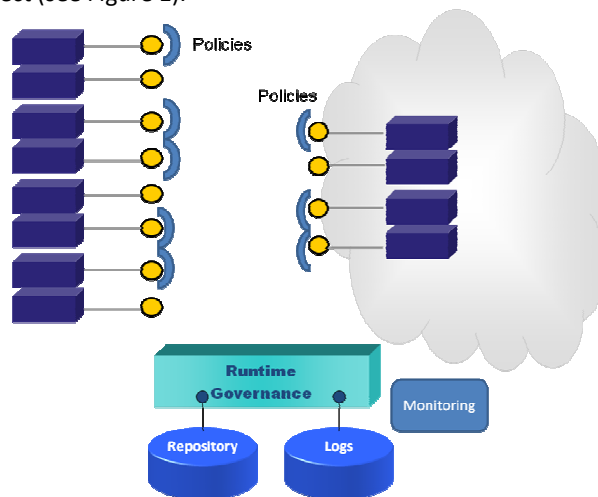


Figure 1: Application service governance encompasses policy-based access control, service tracking via repositories, as well as service logging & monitoring

When considering the end-state architecture we're talking about as a combination of SOA using cloud computing, we're looking to build a series of services that are formed and reformed to build business solutions. The services may exist on-premise or are cloud-delivered, but the use of those services by applications and processes should be completely transparent to the service consumer, including the fact that some exist on-premise, while some are cloud delivered.

Thus, we create something that has a tremendous amount of value when it comes to agility and the ability to operate enterprise IT at greatly reduced costs. However, the architecture is very complex and thus needs a specialized service governance mechanism to manage this complexity.

Services are interdependent... a single service that is altered without the knowledge and understanding of the impact that change may have, could bring down many core enterprise systems.

Dependencies, as reflected in the example given at the beginning of this paper, mean that many of these services are interdependent, meaning services calling services, or composite services. Moreover, many applications are dependent upon these services (see Figure 2).

Thus, services that fail or, more likely, services that change without authorization, will have a domino effect on other services and applications that leverage them. Indeed, a single service that is altered without the knowledge and understanding of the impact that change may have, could bring down many core enterprise systems, perhaps costing thousands of dollars an hour in lost revenue, which quickly diminishes the value of cloud computing. The use of service governance approaches and technology mitigates the risks.

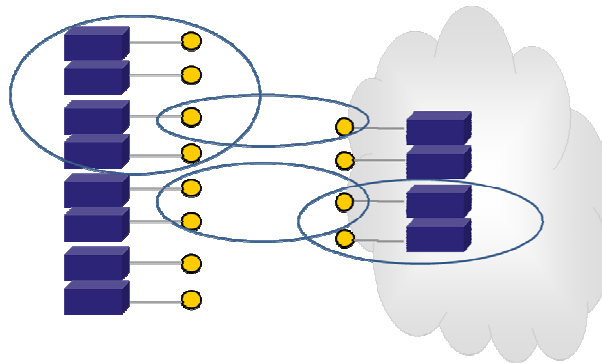


Figure 2: Interdependencies between services can cause disruptions when any one service fails or changes

Operational monitoring means that we place controls around the services through the use of policies, and we can monitor the services during runtime, on-premise or cloud-delivered. What's core here is that you understand what needs to be monitored, and at what granularity.

Since there is a performance impact of service monitoring, it's important that companies monitor only those services that are critical to the operations of the business. You must make sure they are up-and-running and providing the performance servicing to the other services and applications that leverage them.

Granularity means that we look at the services to be monitored, and how deeply we can go, or should go, in that monitoring. While some services just need a "live/dead" status, others may need to have their performance closely monitored, including database and CPU utilization, and perhaps other attributes of the service.

Application Service Governance Technology

Application service governance includes:

- **Service discovery**
- **Service delivery**
- **Security**
- **Setting & maintaining service levels**
- **Managing errors & exceptions**
- **Service validation**
- **Auditing & logging**

Service discovery refers to the process of finding, analyzing, and detailing an existing service and the use of a policy to govern that service. The great thing about this feature is that you simply enter in the location of the service, and the runtime service governance technology does the rest, including entering aspects of the service into the repository (discussed below).

Service delivery is the process of moving services from development to execution or production. Moreover, it means moving services from a staging to execution environment, such as on-premise to cloud-computing platforms.

Security encompasses the functions around protection of the services that are managed, and enforcement of the policies.

Setting and maintaining appropriate service levels refers to making sure that all of the services execute per the service agreements and preset levels. This is especially important in an architecture that leverages cloud computing since they may come with SLAs, or service level agreements, that must also be managed.

Managing errors and exceptions is a feature where any errors and exceptions that occur are captured, analyzed, and perhaps recovered from automatically. Typically this means that those who implement the policies must define how errors and exceptions should be managed for a specific service, or group of services. The objective is to recover from most errors and exceptions without human intervention, if possible.

Service validation, as the name implies, is the feature of the governance technology that validates that the services are well formed, and prepared to go into production. This assures that any changes made to the service do not risk that the services will not execute if they are indeed invalid.

Auditing and logging means that the governance technology will track the execution of the services and the policies, including what they do, when they do it, and who they do it with. This allows those who manage the holistic architecture to analyze auditing and logging information to determine why problems occurred, or better yet, prevent them. Auditing is required by many legal compliance standards, such as those imposed on public companies or those in regulated vertical markets, such as health care.

The Value of Application Service Governance for Cloud Computing

Now that we understand what application service governance brings to the table, it's helpful to drill down a bit to the core value of leveraging this technology within the context of cloud computing. It is our contention that the cost of risk associated with not implementing an application service governance system outweighs the benefits of converting capital expenditures to operational expenditures (see Figure 3).

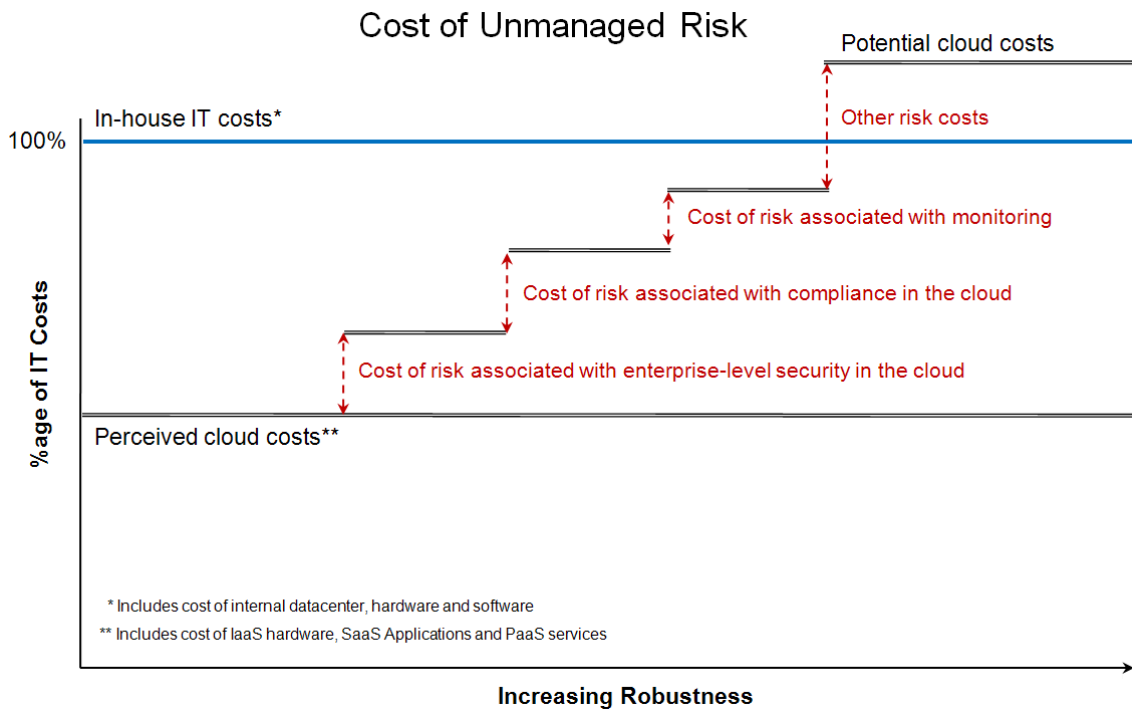


Figure 3: CapEx to OpEx cost savings versus Cost of Risk for cloud computing

As you may recall from the beginning of this paper, many organizations are weighing cloud computing cost savings against the business risks associated with:

- Security in the cloud
- Compliance in the cloud
- Monitoring services in the cloud
- Operational inefficiencies

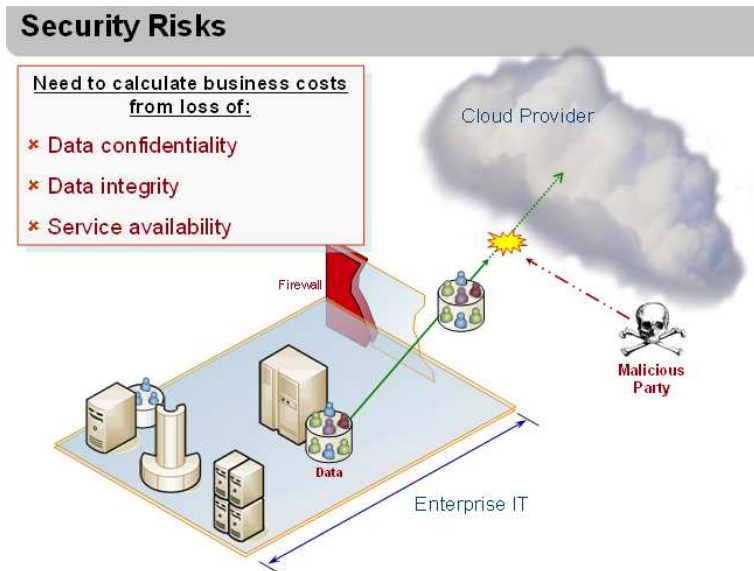


Figure 4: Cost factors associated with lack of security in the cloud

Security pertains to issues associated with trust. How is data integrity and confidentiality maintained on data in flight or residing on a cloud provider? How is authentication and authorization enforced on services and data? How are keys and identities administered? How are audits managed? Whose laws apply in clouds that may be in other jurisdictions? Who's liable for breaches? Can cloud providers access your data after you have terminated relationships with them (for example, on backups or by inspecting disk images)?

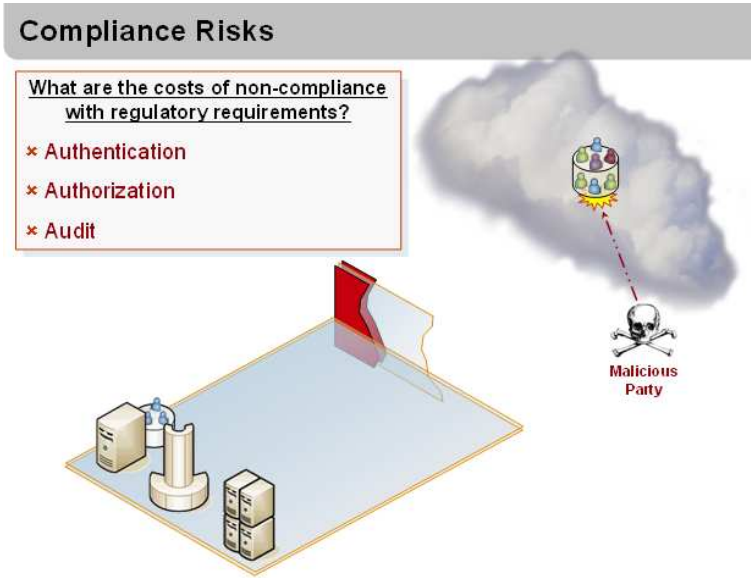


Figure 5: Cost factors associated with lack of compliance in the cloud

Compliance pertains to tracking and enforcing regulatory requirements when transactions take place in the cloud. Because compliance is generally associated with identity, it is particularly concerned with traditional IT AAA: Authentication, Authorization and Audit. Compliance also covers the regulatory and intellectual property risks around data loss.

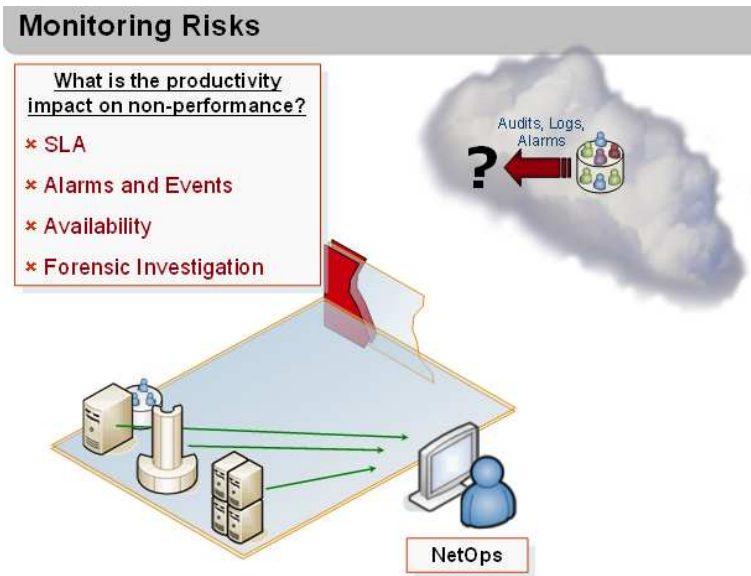


Figure 6: Cost factors associated with lack of monitoring in the cloud

Monitoring covers how to measure and track service and network performance. Who’s accountable when shared systems, networks, and services fail? Are these meeting the SLAs in place between the provider and the customer? Are logs and audits available for forensic investigation after transactions take place?

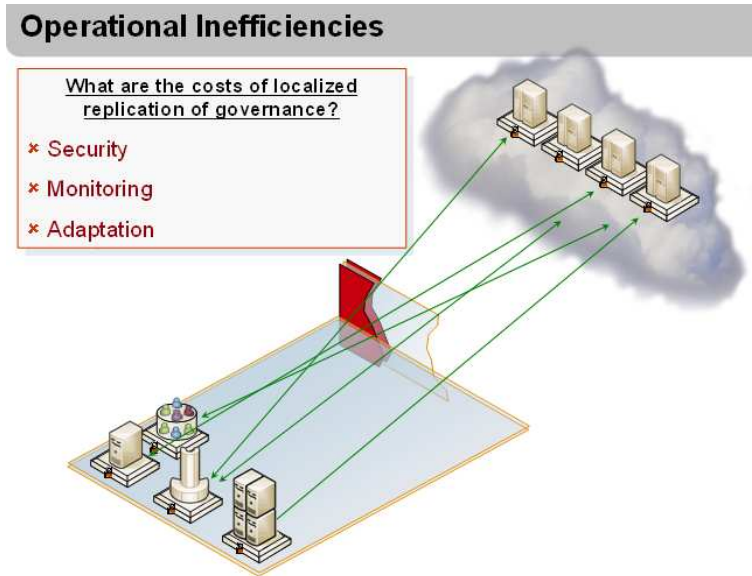


Figure 7: Cost factors associated with implementing governance for each cloud-based service separately

Operational Inefficiencies occur when security, monitoring, and compliance requirements are met on an individualized basis with every service. Because of the diverse platforms hosting most services (even in the cloud), there are few options for reuse or consistent management here. As the number of services grows, it becomes intractable to maintain this approach. A much more effective solution is to decouple these functions from applications, and apply these consistently, independent of the applications themselves.

Conclusions

To maximize the value of cloud computing enterprise should “trust, but verify” by leveraging proven, COTS application service governance technology.

While small and medium businesses may be content with accepting whatever security, compliance, and monitoring capabilities cloud vendors have to offer, most enterprises have the resources – and the need – to manage the risk associated with their cloud-based implementations.

Application service governance gives enterprises the ability to define, control, monitor, and adapt runtime service execution on any number of platforms, both on-premise and in the cloud. The value of application service governance is clear when you consider the amount of risk governance removes, since those who manage the systems can be more proactive, and get well ahead of issues that will bring down services which, in turn, will bring down the systems. They will also have the control to monitor and manage application services themselves, without needing to trust cloud vendors who are

incented to provide customers with positive security and performance statistics.

Considering all of the information presented in this paper, it’s easy to conclude that cloud computing is a high value approach to computing that allows you to convert capital expenditures to operational expenditures. However, approaching application service governance in an ad-hoc way – or not implementing governance at all – quickly diminishes the value of cloud computing. In order to maximizing the value of cloud computing, enterprises should follow the basic rule of “trust, but verify” by leveraging proven, COTS application service governance technology.

About the Authors

David Linthicum (Dave) is an internationally known Enterprise Application Integration (EAI), Service Oriented Architecture (SOA), and cloud computing expert. In his career, Dave has formed or enhanced many of the ideas behind modern distributed computing including EAI, B2B Application Integration, and SOA, approaches and technologies in wide use today.

Dave is the founder of David S. Linthicum, LLC, a consulting organization dedicated to excellence in SOA product development, SOA implementation, corporate SOA strategy, and leveraging cloud computing. Dave is the former CEO of BRIDGEWERX, former CTO of Mercator Software, and has held key technology management roles with a number of organizations including CTO of SAGA Software, Mobil Oil, EDS, AT&T, and Ernst and Young.

In addition, Dave was an associate professor of computer science for eight years, and continues to lecture at major technical colleges and universities including the University of Virginia, Arizona State University, and the University of Wisconsin. Dave keynotes at many leading technology conferences on application integration, SOA, Web 2.0, cloud computing, and enterprise architecture, and has appeared on a number of TV and radio shows as a computing expert.

David S. Linthicum, LLC
www.davidlinthicum.com
11654 Plaza America Drive, #103
Reston, VA 20190
david@davidlinthicum.com

K. Scott Morrison is the Chief Architect at Layer 7 Technologies, where he works to govern and secure Web applications. He has extensive IT and scientific experience in a number of industries, was previously Director of Technology at Infowave Software, and has also held senior architect positions at IBM.

Scott is a dynamic and highly sought-after speaker with extensive speaking experience at over 70 shows around the world, including the InfoWorld SOA Forum, JavaOne, ZapThink podcasts, OMG SOA Consortium, IDC IT Forum, Web Services on Wall Street, as well as several Gartner events and Networld+Interop.

Scott has published over 40 book chapters, magazine articles, and papers in medical, physics, and engineering journals, including ComputerWorld, ZDNet, Web Services Unleashed, Professional JMS, Ajax World Magazine, SOA World Magazine, Communications News, DM Review, and Business Integration Journal.

Layer 7 Technologies
Suite 405-1100 Melville Street
Vancouver, BC
V6E 4A6 Canada
www.layer7tech.com
smorrison@layer7tech.com

About Layer 7 Technologies

With offices in San Mateo, California; New York, New York; and Vancouver, British Columbia, Canada; Layer 7 Technologies helps enterprises accomplish secure and cost-effective business integration using XML and Web services. Layer 7 Technologies' SecureSpan™ Solution is the first technology that addresses security and governance across a Web services integration without expensive and inflexible programming. With the SecureSpan™ Solution, customers realize lowered integration costs, increased security reliability, and the ability to future-proof their Web services investments. Contact Layer 7 Technologies or visit www.layer7tech.com for more information.

Contact Layer 7 Technologies

Layer 7 Technologies welcomes your questions, comments, and general feedback.

Email:

info@layer7tech.com

Web Site:

www.layer7tech.com

Phone:

(+1) 604-681-9377

1-800-681-9377 (toll free within North America)

Fax:

604-681-9387

Address:

Layer 7 Technologies
Suite 405-1100 Melville Street
Vancouver, BC
V6E 4A6 Canada

Legal Information

Copyright © 2009 by Layer 7 Technologies, Inc. (www.layer7tech.com). Contents confidential. All rights reserved. SecureSpan™ is a registered trademark of Layer 7 Technologies, Inc. All other mentioned trade names and/or trademarks are the property of their respective owners.