EXTENDING IT GOVERNANCE FROM PRIVATE TO HYBRID CLOUDS THROUGH CONSISTENCY AND PORTABILITY

GORDON HAFF

EXECUTIVE SUMMARY

Public cloud resources can augment in-house IT in many useful ways. In fact, they can be so useful and easy to consume that we see public clouds widely used in organizations without going through the usual IT processes and procedures—indeed, that's often sort of the point. Ad hoc cloud adoption can make sense. However, when production applications or critical data is involved, it's important to extend on-premise governance to these public or hybrid resources.

IT shouldn't try to stop public clouds—not that they likely could even if they wanted to. But by working with their users, IT can make an organization's use of public and hybrid clouds a useful complement to in-house IT rather than a renegade operation that increases an organization's risks and costs.

- Governance means designing, building, testing, and implementing policies for services—and monitoring their use.
- What are frequently termed security risks in cloud computing often really concern a broader group of IT governance issues.
- Governance relates to all aspects of IT, whether on-premise or otherwise—but public clouds raise some unique risks and exacerbate others.
- Governance areas relevant to cloud computing include: Data leakage/breaches/loss, legal and regulatory, service delivery or failure, transparency and visibility, and the ability to move applications and data in-house or to a different external provider.
- Governance often leads to a requirement that workloads be capable of moving between public clouds and private clouds or from one public cloud provider to another. This requires consistency and portability.
- Consistency refers to having a consistent runtime environment (such as an operating system or middleware) in different clouds, public and private.
- Consistency between on-premise and public clouds for production applications requires a consistent runtime environment that is certified from both technical and business relationship perspectives.
- Portability has multiple aspects including computing/APIs, application environments, cloud services, and programming models.
- Red Hat addresses issues of governance, consistency, and portability with a wide range of technologies, approaches, and business relationships including: Red Hat Enterprise Linux, JBoss Enterprise Middleware, Red Hat Cloud Foundations, Red Hat Network Satellite, the Red Hat Certified Cloud Provider Program, and Red Hat Cloud Access.
- Best practices are needed when selecting public cloud providers, determining which applications are appropriate for those providers, and accessing how applications and data can be moved between clouds as needed.

BEYOND INFORMATION SECURITY

When discussions with IT people turn to cloud computing as they are wont to do these days, the word "security" is likely to pop up sooner rather than later.

Dig a little deeper, though, and you soon discover that what concerns people mostly isn't security risks per se. Indeed, when the European Network and Information Security Agency (ENISA) put out a broad analysis of the "benefits, risks, and recommendations for information security" associated with cloud computing, they led off with a discussion of the security benefits of cloud computing. For example, they note that all kinds of security measures are cheaper when implemented at a large scale. Therefore, given that cloud computing suggests a greater centralization of computing infrastructure (whether internally or externally hosted), security processes can well be more effective than when implemented at smaller scale by less-expert administrators.

This isn't to suggest that an organization implementing a savvy cloud strategy doesn't need to consider potential risks and mitigate them. But this isn't anything fundamentally different from a savvy IT strategy today—although it does need to take into account factors that often don't exist in traditional IT. What we're talking about is governance and, as industry expert and author David Linthicum puts it: "Cloud computing needs governance in order to be successful…We need an approach, processes, procedures, and technology—we need governance."

Linthicum goes on to say that "In the world of enterprise architecture, governance means control, or the ability to mandate the use of standards and approaches, almost a management concept…simply put, governance means designing, building, testing, and implementing policies for services, and monitoring their use." So governance is a much bigger concept than some relatively low-level security concepts like encryption or patching—though policies around those are certainly part of governance as well.

As we discuss risk throughout this paper, it's important to remember that no IT activity can be made entirely without risk whether cloud computing is part of the picture or not. Furthermore, as ENISA notes: "Risk should always be understood in relation to overall business opportunity and appetite for risk—sometimes risk can be mitigated by opportunity." Governance means assessing risk and making the appropriate decisions in the context of business impact, cost, legal, and regulatory requirements, and opportunities to mitigate the risk.

In this whitepaper, we examine:

- Some of the key governance issues affecting both private and public clouds
- Frequently cited risks and ways to mitigate them
- Approaches that Red Hat is taking to help customers implement effective cloud governance
- Best practices that are part of a savvy cloud strategy

FROM PRIVATE TO PUBLIC AND BACK AGAIN

Governance considerations aren't limited to public clouds. And many of the risks that have to be mitigated in a public cloud environment apply to various degrees and in various ways to outsourced services in general, and even to on-premise infrastructures. After all, in many ways, no IT infrastructure is an island totally divorced from dependencies on external providers of various types.

That said, third-party services introduce their own unique governance issues and amplify others. Legal and regulatory procedures, transparency, service levels, indemnification, notification, and portability are all among the considerations when selecting a public cloud provider. This is an involved topic that deserves a deeper dive than we can provide here. However, suffice it to say that governance often leads to a requirement that workloads and data be capable of moving between public clouds and private ones or from one public cloud provider to another. One of the biggest concerns is the ability to move data back on-premise once it is in the cloud or to back up data that is stored in the cloud.

The need for interoperability and portability have often been discussed in the context of operations such as "cloudbursting"--the use of public clouds to temporarily expand computing capacity in the event of a demand spike. Running workloads dynamically across multiple public cloud providers could potentially even allow for spot markets to develop in cloud computing pricing—thereby allowing consumers to dynamically consume capacity where it is cheapest. Advanced usages like these are certainly something to keep aware of as cloud computing develops—and something to consider as you make architectural decisions. But consistency and portability between different cloud environments are also important considerations in the here and now.

CONSISTENCY ACROSS PRIVATE AND PUBLIC CLOUDS

Consistency and portability are closely related, although they're not the same thing.

Consistency refers to having a consistent runtime environment (such as an operating system or middleware) in different clouds, private and public. The same application should be able to run in both places. For starters, this means that you can take a given Linux, Java, PHP, or whatever application and the target environment(s) will have the supporting software and hardware infrastructure that allows that application to run in the same way in all these places. The bottom line is that the user of that application should not be able to tell where it is running.

One of the ways that consistency breaks down is that public clouds encourage ad hoc development that doesn't necessarily comply with an organization's standards for applications run on-premise. This may be fine for prototyping or other work that is throwaway by design. However, it's far too easy for prototypes to evolve into something more—as often happened in the case of early visual programming languages—and the result is applications that either have to be rewritten or that may have support, reliability, or scalability issues down the road.

Just because developers find that a given public cloud environment offers the cheapest and easiest path to write and test an application doesn't mean total application lifecycle costs will be lower. Public cloud-based development will happen though, so the best strategy is to recognize this inevitability and channel it in a way that fits within organizational standards.

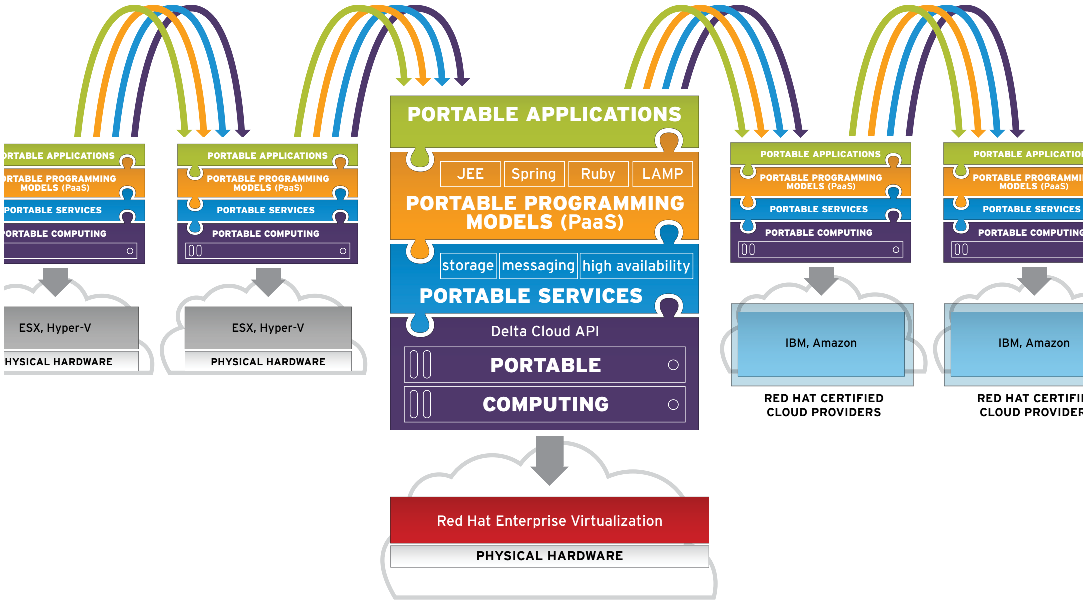
Consistency goes beyond just technical factors, though. Consistency between on-premise and public cloud environments also requires that the full runtime—including the applications running on it—be supported and certified by the same ISVs and others when running in the cloud , a commitment that is as much about business relationships as technical ones.

MULTIDIMENSIONAL PORTABILITY

True portability takes multiple forms and must include four primary areas: computing, applications, services, and programming models.

Portable computing creates scalable private clouds that can be federated to a public cloud provider under a unified management framework. Portable applications mean that developers can write once and deploy anywhere, thereby preserving their strategic flexibility and keeping their options open, while lowering maintenance and support costs. Portable services simplify development and operations by eliminating the need to re-implement frequently needed functions in private clouds and enable the movement of data and application features across clouds. Portable programming models let existing applications be brought over to cloud environments or evolved incrementally.

PORTABLE APPLICATIONS



And, as with consistency, there are aspects of portability that aren't primarily technical—such as whether software subscriptions and licenses can be transferred from one location to another. Consistent support and maintenance environments are also important elements.

The key point here is that, while individual dimensions of portability are certainly useful and desirable, individually they only do so much to ensure that applications and skills can be moved across different IT environments from physical servers to virtualized platforms from private clouds to a choice of public clouds. Portability isn't just about having a standardized API or cloud services. It's about having all the dimensions of portability.

SOME BEST PRACTICES

There is no single right way to build a cloud on-premise or to procure cloud services from an external cloud provider. Something that's appropriate to build lightweight applications used only by developers may not be appropriate for an application that interacts with live customer credit card data. However, based on our experiences with helping customers to build and otherwise consume clouds, the following are some of our recommendations to craft a savvy cloud strategy based on solid governance principles.

- Software-as-a-Service (SaaS) applications, public cloud resources, and mobile devices of many types are going to be used by people within an organization whether officially sanctioned or otherwise. Therefore, it makes sense for IT to recognize this reality and establish appropriate policies that leverage the flexibility and acquisition ease of cloud resources without compromising the security of data or other aspects of IT governance. For example, IT might, after doing due diligence, create a list of approved public cloud providers in the same manner as many organizations have a list of other approved vendors.
- Recognize that selecting a public cloud provider or hosted application requires the same sort of due diligence that should accompany any outsourcing project to ensure that the selected provider is a trusted destination for your applications and data.
- Even if you have decided to use infrastructure or applications in the cloud, it is critical that you always have a path to exporting and/or maintaining a regular backup of your data in a usable form. The organization's informational governance policies have to apply to all corporate data, wherever it resides. While these concerns are typically greatest with SaaS, understanding where data resides and how it is protected is important in any situation where you lack direct visibility and control.
- Wherever possible, favor cloud providers that use or can interface to common sets of APIs. However, recognize that cloud computing is a rapidly developing area that doesn't have, nor is likely to develop in the near future, a single set of standards. Investigate APIs, such as the Apache Software Foundation's Deltacloud, that enable interoperability among different clouds.
- Develop a strategy that allows applications and data, to the degree possible, to be moved with minimum effort between public cloud providers, from private clouds to public clouds, and from public clouds to private clouds. While transparent movement of resources is not always possible, especially in the case of proprietary applications and platforms hosted by a single provider, the goal should be to maximize mobility and to only give it up when the benefits outweigh the risks.
- When initially hosting applications on a public cloud, develop and deploy them with an eye to maintaining a consistent, certified environment across multiple private clouds and public clouds.
- While recognizing that individual applications have their own unique circumstances, establish overall policies that define acceptable cloud usage within the organization. These policies should, among other factors, take into account organizational audit requirements and any relevant regulations or industry best practices. These policies should be flexible enough not to prohibit reasonable uses that will happen whether sanctioned or under the radar. Having consistent environments across on-premise and public environments can eliminate much of the uncertainty associated with using a unique, publicly hosted service.

- Different cloud platforms will be more suitable for some uses than others. It also makes sense to have some diversity of suppliers as a risk mitigation technique. Nonetheless, you should make an effort to control unwarranted proliferation of platforms, especially to the degree that they are not fully interoperable, if only because of the effort required to monitor all suppliers for continued adherence to your established policies.
- Investigate SaaS solutions primarily for those functions that are relatively standardized, needed by a wide range of organizations, and that are not core to your business (even if they're important). Customer Relationship Management and email are common examples.
- Many of the new governance concerns related to cloud computing primarily relate to public clouds and how they interface with private clouds. However, be aware that the pervasive virtualization and automation that help to define private clouds also introduce new wrinkles for audit and other aspects of governance relative to an environment in which applications run on a known physical server.
- Enable developers to utilize public cloud resources as appropriate, but with an eye to having consistent development tools and platform environment on-premise and in the cloud. Cloud-based application development and test strategies should take into account the complete application lifecycle, including production deployment.

RED HAT'S CLOUD ADVANTAGES

Red Hat addresses issues of governance, consistency, and portability with a wide range of technologies, approaches, and business relationships, just some of which we discuss in this section.

Fundamentally, it's the operating system's layer of abstraction that determines whether a given application can run on one type of hardware or many. In the case of Linux, these APIs are open source and they're based on open standards. They also run across a broad swath of computer architectures. This brings in a large community of developers and users and eliminates the possibility of being locked into any single vendor's API as was the historical norm.

Red Hat Enterprise Linux is the enterprise Linux platform for any application across the IT infrastructure. Our latest release, Red Hat Enterprise Linux 6, sets new standards for flexibility, efficiency, and control. It works across a broad range of hardware architectures, hypervisors, and clouds. Corporations and agencies that standardize on Red Hat Enterprise Linux are free to focus on building their businesses, knowing they have a platform that delivers more of what they need.

But it's not just about Linux. Red Hat delivers a consistent development and deployment platform across on-premise and cloud environments. Red Hat's approach to cloud computing is to support the broadest choice of operating and development environments. Red Hat Enterprise Linux and JBoss Enterprise Middleware make the cloud usable for new and existing enterprise-class applications, while lightweight frameworks like Struts and Spring enable fast and easy application development. There's no need to rewrite applications to take advantage of a cloud computing infrastructure.

Red Hat Cloud Foundations provides everything needed to help you plan, build, and manage a private cloud today. Red Hat delivers the most complete and comprehensive cloud solutions in the market, with the flexibility that comes only from the open source leader. Red Hat Cloud Foundations includes products, references, training, and reference architectures.

Red Hat Network Satellite's ability to divide and organize large groups of systems, both physical and virtual, is a key element of managing IT infrastructures as they evolve to private, public, and hybrid clouds. Templates allow groups of systems to remain compliant, consistent, and secure throughout their lifecycle with automated processes that take businesses beyond basic virtualization and into a flexible, dynamic cloud infrastructure. Furthermore, Red Hat Network Satellite provides reports to track inventory and content compliance as required in any well-governed cloud.

Through the Red Hat Certified Cloud Provider Program, Red Hat has established the industry's first cloud certification program to certify that vendors have tested the cloud and have support processes in place to quickly resolve problems should they occur. Certified providers have passed business, operational, and technical requirements to be able to offer Red Hat solutions under cloud appropriate business models and are backed by Red Hat support relationships.

Red Hat Cloud Access lets qualified enterprise customers migrate their current subscriptions for use at select Red Hat Premier Certified Clouds. This gives customers the ability to make use of Red Hat support, relationships, and technology on certified clouds, while maintaining a consistent level of service and support across all certified deployment infrastructures with consistent and predictable pricing.

CONCLUSION

Cloud computing, in some form, will play a role throughout all organizations whether it's in the formal evaluation and adoption of a new CRM platform through a formal IT process, the ad hoc use of public cloud infrastructure by developers, or the "bursting" of an on-premise cloud to a public cloud to gain temporary capacity. Especially given the importance of properly securing data and minimizing lock-in to specific third-party provider, it's critical to bring cloud computing activity that involves corporate data or production applications under a common governance umbrella.

Cloud computing isn't "risky" any more than IT more broadly is risky. Rather, like all IT activities, cloud computing projects should be undertaken in a way that both mitigates risk and that considers those projects in the context of IT as a whole.

FURTHER READING

Red Hat Cloud Foundations: Cloud 101 (Red Hat)
http://www.redhat.com/f/pdf/cloud/101_whitepaper.pdf

Cloud Computing Risk Assessment (ENISA)
http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment

Cloud Computing and SOA Convergence in Your Enterprise by David S. Linthicum

RED HAT SALES AND INQUIRIES

NORTH AMERICA
1-888-REDHAT1
www.redhat.com
sales@redhat.com

EUROPE, MIDDLE EAST AND AFRICA
00800 7334 2835
www.europe.redhat.com
europe@redhat.com

ASIA PACIFIC
+65 6490 4200
www.apac.redhat.com
apac@redhat.com

LATIN AMERICA
+54 11 4329 7300
www.latam.redhat.com
info-latam@redhat.com