WHITEPAPER

DEPLOYING IN A PUBLIC CLOUD ENVIRONMENT

Run your workloads efficiently, securely, and under control

"While the IT department may not necessarily be able to reassert its control over all IT decisions, IT leaders should establish a businesswide cloud IaaS strategy, if for no other reason than to reduce risk. This strategy should include educating the business on the value of cloud IaaS, and establishing and disseminating clear guidelines for using such technology."

"THREE STEPS TO ESTABLISHING AN ENTERPRISEWIDE, CLOUD IAAS STRATEGY,"
GARTNER, INC., APRIL 2015

EXECUTIVE SUMMARY

Public cloud environments are here to stay. They promise nearly unlimited capacity, potentially attractive costs stemming from large-scale infrastructures and associated operational best practices, and a pay-as-you-go pricing model that can make up-front server purchases a thing of the past. But, especially for enterprises, effectively and safely using public cloud environments involves more than whipping out a credit card and clicking some buttons on a website.

Running a small, simple application on one public cloud environment may be a prudent first step. But the end goal should be to reliably run large, scalable applications made up of many loosely coupled components across a mixture of on-premise, dedicated external, or multi-tenant cloud resources of various types. And to do so efficiently and compliantly in service of the business' objectives.

Many different considerations go into developing a cloud strategy that meets these objectives—and then implementing, operating, and developing the associated applications. However, based on a wide range of conversations with customers, partners, analysts, and others, the following are some of the most important steps to take in order to make the best use of public cloud environments as part of a broader hybrid IT strategy:

- Take a business-based approach to risk
- Understand legal and regulatory compliance
- Consider portability
- Establish a trusted software supply chain
- Enable hybrid cloud policy and management
- Adopt consistent operational approaches
- Maintain control over services and workloads
- Develop an appropriate application architecture

INTRODUCTION

The decision to run a particular workload in a public cloud environment depends on a wide range of factors—from control to cost to compliance to available capital. Regulatory requirements and other legal or risk management considerations can constrain where particular workloads run. So

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com

can the technical architecture of the workloads themselves. Running workloads across a hybrid environment, or even keeping options open for where they might run in the future, introduces additional considerations.

For the purposes of this whitepaper, we have distilled a short list of public cloud adoption considerations that come up repeatedly in our conversations with customers, partners, and providers. We selected considerations that are particularly relevant to choosing a public cloud environment for Infrastructure-as-a-Service (IaaS). However, many of these considerations also apply in various degrees to other types of services, as well as to hybrid IT infrastructures. You should also consider your own IT governance plans and best practices—as well as the external risk assessment and security controls documents of your choice. But we think this list is a good place to begin.

"I&O pros must set expectations with their CIOs and CISOs that you cannot secure cloud workloads by retrofitting your on-premises approach and security products and solutions. Security is important as you transition to the cloud. Take the time to address user access, workload set-up, and configuration scenarios for on-premises and cloud-based workloads."

ROBERT STROUD,
"IS SECURITY FUD DELAYING YOUR PUBLIC CLOUD ADOPTION?"
FORRESTER BLOG,
JANUARY 2016[1]

KEY CONSIDERATIONS

TAKE A BUSINESS-BASED APPROACH TO RISK

There are a variety of available frameworks to help IT executives and architects evaluate and mitigate risks associated with using public cloud providers. A good example is the Cloud Controls Matrix (CCM) from the Cloud Security Alliance (CSA).

The CSA CCM provides a controls framework across 16 domains, including business continuity management and operational resilience, encryption and key management, identity and access management, mobile security, and threat and vulnerability management. CCM v3.0.1 defines 133 controls and maps the relationship between these and industry-accepted security standards, regulations, and controls frameworks—including ISO 27001/27002, ISACA COBIT, PCI, the National Institute of Standards and Technology (NIST), and the North American Reliability Corporation Critical Infrastructure Protection (NERC CIP).

However, more broadly, security needs to be approached in the context of overall business needs—not simply addressed as a technology problem. Perhaps using a given third-party service does introduce a new level or type of risk. But if the business benefits of getting access to, for example, better customer analytics is significant, perhaps the (appropriately evaluated) incremental risk is worthwhile. Or not. In any case, the risk has to be viewed in a broader context.

UNDERSTAND LEGAL AND REGULATORY COMPLIANCE

The CSA CCM is also a useful source for learning about the types of controls relevant to a cloud provider and its customers, as well as their relationship to specific standards and regulations. A variety of cloud-specific standards and certifications aim to clarify best practices and requirements for particular uses. For example, FEDRamp provides standardized security assessment, authorization, and continuous monitoring for cloud services and products across the entire U.S. federal government.

Learn more about the Cloud Security Alliance's 133 control areas at https://cloudsecurityalliance.org/group/cloud-controls-matrix/

1 *http://blogs.forrester.com/robert_stroud/16-01-07-is_security_fud_delaying_your_public_cloud_adoption*

LEGAL AND REGULATORY QUESTIONS MIGHT INCLUDE:

- Does the provider comply with PCI, DSS, or HIPAA standards?
- What notification processes does the provider have in the event of a data breach or a subpoena of data?
- Are there laws restricting certain types of data to a particular country or other locality?
- What types of audit information does the provider make available to customers?

It's particularly important to understand the nature of data to be stored in an IaaS platform. The usual rules concerning financial and personal information apply as they would on-premise. However, in public cloud environments, local data sovereignty laws may restrict the use of providers depending upon where they have datacenters and the degree to which they allow control over data placement.

CONSIDER PORTABILITY

One of the most important aspects of workload portability is having the ability to deploy certified operating systems and middleware across a variety of internal and external providers. These common runtimes act as a container for applications running in different environments and help insulate the applications from having to deal with platform specifics—historically one of the most important operating system functions.

Of course, ensuring portability of applications running in a public cloud environment is not solely a technology issue. Maintaining portability also requires that applications be written in a way that does not lock them into a single platform. While it sometimes will make sense to take advantage of technology unique to a single public cloud provider, do so with a full understanding of the tradeoffs involved.

Portability also extends to business relationships. For example, Red Hat® Cloud Access is a feature of some Red Hat subscriptions, and permits customers to use Red Hat support and products on certified clouds, while maintaining a consistent level of service, pricing, and support across all certified deployment infrastructures.

ESTABLISH A TRUSTED SOFTWARE SUPPLY CHAIN

82% [of the enterprise early adopters surveyed] say Open Source is a critical or significant enabler of their DevOps strategy.

IDC DEVOPS THOUGHT LEADERSHIP SURVEY, IDC, MAY 2015[2]

It's also important to understand that many practices do not—or should not—change in a public cloud environment. Obtain software from known, trusted sources and ensure that mechanisms are in place to provide and install updates in a timely way.

For example, Red Hat helps to secure the supply chain by digitally signing all released packages and distributing them through secure channels. Red Hat also provides vulnerability and errata information in machine-readable form, so it can be used at scale—such as through the use of a Security Content Automation Protocol (SCAP) scanner. A reproducible build system that logs all actions also lets Red Hat know where, when, why, and how a given build happened so that it can be recreated at a future date—even years later—if required.

ADOPT CONSISTENT OPERATIONAL MODELS

In addition to using certified software images, it is equally important to maintain those images throughout their life cycle. One effective way to do this is to use public cloud providers with back-end services that can provide timely updates to software patches and install them as necessary. For example, Red Hat certified cloud and service providers deploy a Red Hat Update Appliance (RHUA) infrastructure to deploy patches at scale within the service provider's infrastructure.[3]

However, consistency goes beyond technology, encompassing business and support relationships. If there's a problem, should you expect finger-pointing or a well-established joint escalation process between your certified software vendor and the service provider? Can you move software across providers? These are the sort of questions to ask when running workloads across public cloud environments and on-premise.

2 http://blogs.gartner.com/thomas_bittman/2015/03/05/some-perspective-on-the-explosion-of-vms-in-the-cloud/

3 Customers using Cloud Access can also use Red Hat Satellite to deploy patches. This maintains operational consistency with on-premise processes.

ENABLE HYBRID CLOUD POLICY AND MANAGEMENT

Tools such as a cloud management platform (CMP) can provide consistent processes and governance across different infrastructures and public cloud providers. A CMP can enforce resource quotas, allocate usage-based costs to align internal financial incentives, and improve compliance using automated policy enforcement and remediation.

Red Hat CloudForms is a CMP that supports web-based access to your service catalogs with role-delegated automated provisioning, quota enforcement, and chargeback across a hybrid cloud environment. With CloudForms, resources are automatically and optimally used via policy-based workload and resource orchestration, guaranteeing service availability and performance. You can simulate resource allocation and continuous insights into granular workload and consumption levels to allow chargeback, showback, proactive planning, and policy creation. CloudForms allows you to consolidate management and provisioning of on-premise and cloud-based virtual machines (VMs) through self-service portals and service catalogs.

This consistency can be extended to automation, which provides configurations in a format readable by both people and machines. Automation eliminates the labor associated with repetitive tasks, documents them, and ensures they are performed correctly, securely, and repeatedly across different infrastructure types and at different scale points.

MAINTAIN CONTROL OVER SERVICES AND WORKLOADS

In March 2015, Gartner's Tom Bittman wrote "Life-cycle management and governance for VMs in the public cloud are not nearly as rigorous as management and governance in on-premises private clouds. Perhaps 30-50 percent of the VMs in the public cloud are zombies (private clouds have zombies and life-cycle management challenges, too – just not as bad)."[4] This highlights how public cloud environments essentially take advantage of utility pricing by halting unused compute instances and deleting unneeded data. Furthermore, especially as cloud provider services and pricing options proliferate, matching resources with the workloads is increasingly important. The cost differences between poorly planned and optimized resource use can be an order of magnitude or more.

It's also important to maintain control over the running environment. Real-time monitoring and policy enforcement can address early performance and reliability issues, as well as detect and mitigate potential compliance issues. Operational monitoring and remediation should continue throughout the system life cycle.

DEVELOP AN APPROPRIATE APPLICATION ARCHITECTURE

Learn more about the Red Hat Certified Cloud and Service Provider Program at https://access.redhat.com/ecosystem

Cloud architectures serve more modular applications that containerize their components and communicate through well-documented application programming interfaces (APIs). In practice, there is a great deal of variation in how applications are componentized and the details of a service-oriented approach. However, microservices is often used as a shorthand term for the general trend even when it doesn't strictly apply.

Microservices are often described as being autonomous (with changes happening independently) and small (typically equated with a single, well-defined function). Microservices can make it easier for teams to choose the right tool for the job and the release cycle most appropriate for the component.

4 http://blogs.gartner.com/thomas_bittman/2015/03/05/some-perspective-on-the-explosion-of-vms-in-the-cloud/

Small units of functionality also encourage experimentation—which can lead to innovation as well as make it easier to push rapid updates. In addition, the ability to quickly change small units of code can reduce the time needed to patch security holes or other code flaws.

ABOUT THE RED HAT CERTIFIED CLOUD AND SERVICE PROVIDER PROGRAM

Launched in 2009, the Red Hat Certified Cloud and Service Provider Program (CCSP) assembles the solutions cloud providers need to plan, build, manage, and offer hosted cloud solutions and Red Hat technologies to customers. A Red Hat Certified Cloud Provider offers a trusted destination for Red Hat customers, independent software vendors (ISVs), and partners to access Red Hat offerings in public cloud environments delivered by the cloud providers.

Each Red Hat Certified Cloud Provider meets testing and certification requirements demonstrating that they can deliver a safe, scalable, supported, and consistent environment for enterprise cloud deployments. The program provides customers, ISVs, and partners with the confidence that their implementations have a solid foundation. And the CCSP insists that providers offer certified images for Red Hat products, back-end infrastructure to keep those images updated, and joint support agreements.

CONCLUSION

Like any other IT asset or service, public cloud environments should be evaluated, adopted, and operated in accordance with the same sort of due diligence and attention to benefits and costs—including legal or regulatory exposure—that should apply when sourcing any type of service.

Choosing a public cloud provider is no longer an isolated tactical decision that can be readily undertaken without consideration of the bigger picture. Public cloud environments should be viewed in context with the portfolio of services that IT brings together and manages, in order to meet business needs while managing risk.

ABOUT RED HAT

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to reliable and high-performing cloud, Linux, middleware, storage, and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

NORTH AMERICA
1 888 REDHAT1

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

ASIA PACIFIC
+65 6490 4200
apac@redhat.com

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

facebook.com/redhatinc
@redhatnews
linkedin.com/company/red-hat

redhat.com
inc0383774-0416