

(<https://www.gartner.com/home>)

LICENSED FOR
DISTRIBUTION

Cloud Computing Deployments Should Begin With Service Definition

Published: 28 July 2016 **ID:** G00294396

Analyst(s): Dennis Smith

Summary

Infrastructure and operations leaders often struggle to understand the role of cloud computing and develop strategies that exploit its potential. I&O leaders should complete the prerequisites before making the technology decisions required for successful, service-centered cloud computing strategies.

Overview

Key Challenges

Many enterprises have failed to achieve success with cloud computing, because they failed to develop a cloud strategy rooted in the definition and delivery of IT services linked to business outcomes.

Many companies are unsure how to initiate their cloud projects, which could cause them to miss chances to capitalize on business opportunities.

Recommendations

Identify the cloud-computing-related IT services you will offer or procure.

Document the internal processes that will be affected by the identified cloud services.

Map applications and workloads to the associated cloud services.

Introduction

Infrastructure and operations (I&O) leaders should plan for cloud services that are made up of orchestrated technology and/or application elements, not just the individual technology components. These cloud services could be varied and be sourced from internal IT teams, third parties providing private cloud services or public cloud services. Although there is an increase in the adoption of public cloud services, the future for many organizations will involve hybrid cloud deployments that increase complexity and the need to strategically handle the delivery of a suite of cloud services — for example, infrastructure as a service (IaaS), platform as a service (PaaS) and SaaS from different providers.

I&O leaders need an approach for focusing on cloud computing services and not just the technology, because the latter approach will not increase the likelihood of the users achieving value. There are three steps in ensuring that the service aspect is adequately addressed and linked to the activities

needed in delivering the services:

Identify the cloud-computing-related IT services that you will offer or procure.

Document the internal processes that will be affected by selected cloud services.

Map the workloads to the associated cloud services.

These three steps should be systematically targeted at achieving business outcomes – for example, cost-efficiencies, operational efficiencies and agility. You will not have cloud computing success without the disciplined development of a systematic cloud strategy. This begins with a focus on services.

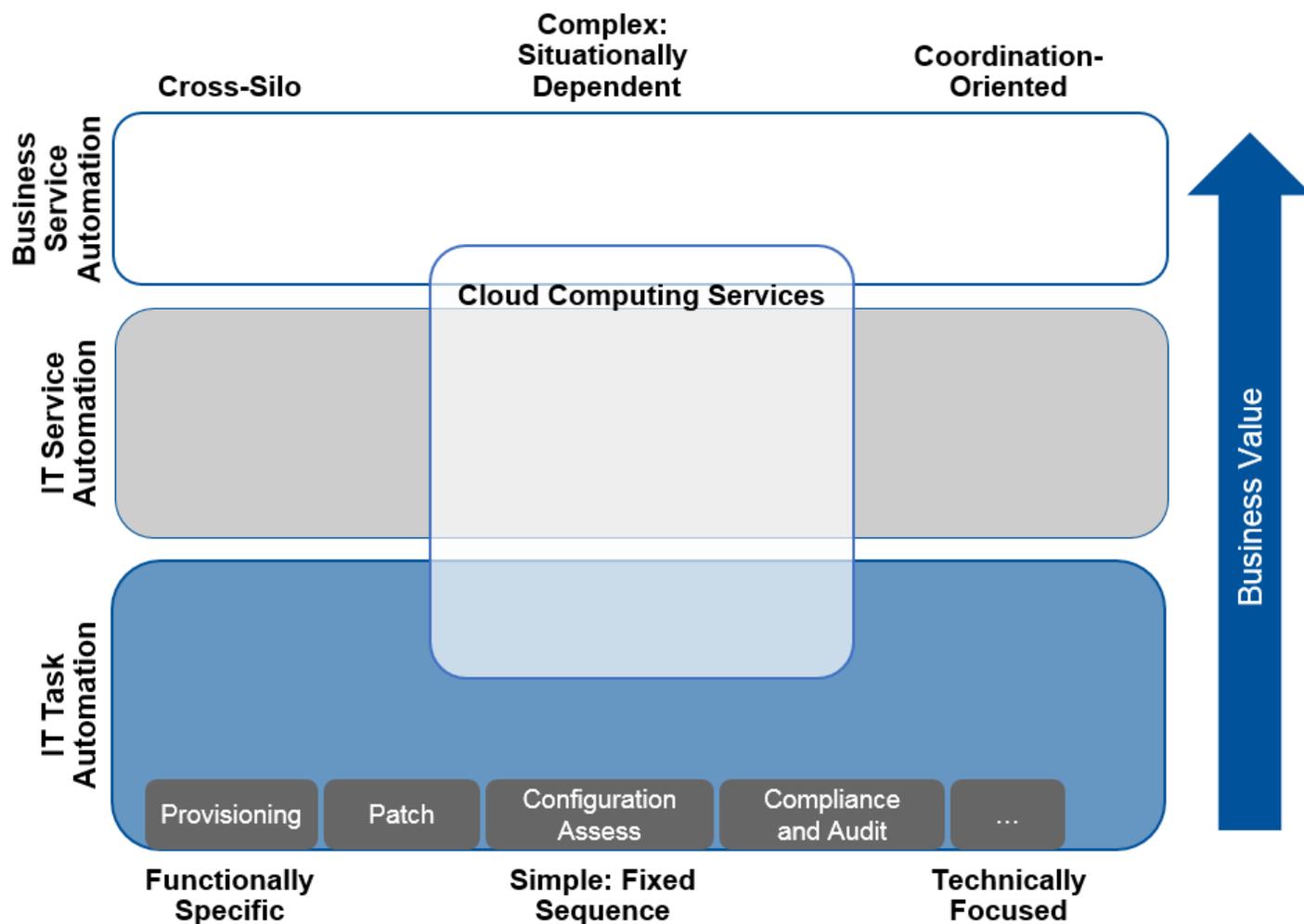
Analysis

Identify the Cloud Computing Services You Will Offer or Procure

Cloud computing differs from other historical IT models in that it focuses primarily on services, rather than technology. As a result, the delivery of cloud computing services is analogous to a traditional supply chain in which services are offered to users in terms that they understand, and the underlying technical details are abstracted away from them. Consumers of the service can place service requests via self-service and are billed for what they use.

Cloud computing services will be varied and must be defined from the perspective of the users of the service. These services can range from one-off automated IT tasks to services that are made up of application and infrastructure components and tethered to business processes. The most impactful deployments encompass IT task and service automation and also venture into business service automation (see Figure 1). Here, technology (e.g., storage, CPU cores and IP addresses) is not the service, but the building blocks for a service. This requires a focus on identifying the business processes and the services they need.

Figure 1. Cloud Computing Services



Source: Gartner (July 2016)

I&O leaders must first identify the services that will be offered after fully understanding the desired business outcomes – for example, cost savings, speed to market and increased service levels. The following questions can help in solidifying the services:

Which users will consume the cloud services?

What services do the users want and/or need; of these, which will you offer, procure and/or support?

How much of the service will the users generally consume?

When will users normally consume the service – for example, are there any peak periods?

What is a reasonable price for the service?

Document How the Cloud Services You Offer Will Affect Processes

Automation (that is, eliminating manual human effort performed for repetitive tasks) is key for any successful cloud deployment. Thus, it's important to study the internal IT processes involved with offering the services. These affected processes span beyond the I&O organization. During this

analysis, it is a good time to refine or eliminate inefficient processes and target manual repetitive processes to be automated. Process areas that should be targeted are described in the sections that follow.

Governance

What is the process for defining and providing governance for the infrastructure and application infrastructure technology components that make up the services? The goal is to limit the "ingredients" (compute and storage elements, OSs, network designs, etc.) used to deliver the services, because doing so will make the deployment and support of the service easier and more cost-effective.

Application Development Support

Because application developer agility is a main outcome for many cloud strategies, it is important to know how I&O can enable agility for your application development community. Here, understanding the application development pipeline (i.e., how developers conduct test, development and production activities) is important, because cloud computing can automate the movement among the environments (see "Set the Stage for Successful DevOps With Combined IaaS and PaaS for Continuous Delivery" and "Avoid Failure by Developing a Toolchain That Enables DevOps"). The I&O organization should have a basic understanding of the tools being used by application developers and, more importantly, an understanding of the handoffs between development and operations.

Automation

Where can synergies be built across the infrastructure silos that support a given service or application? This analysis might highlight a need to flatten, reconfigure or realign the infrastructure organization or to form virtual organizations or centers of excellence (or COEs) for areas such as automation, patching and provisioning. These areas are key deployment, particularly automation, where the goal should be automated should be automated (see "Six Key Steps to Move IT Process Automation From Basics to Best Practices" and "Choose the Right I&O Automation Tool Categories to Drive Efficiency, Improve Reliability and Reduce Costs").

Operations

Once it has been provisioned, how will you monitor and maintain the environment? Some of the legacy processes might not work in the new environment (see "Network Performance Monitoring Tools Leave Gaps in Cloud Monitoring"). An architecture and a set of processes need to be developed to address reactive, proactive and forensics operational support (see Note 1). A goal is to link instrumentation and monitoring with automation, so that actions are taken before humans engage.

Security

What security will I apply to my cloud deployment? This includes providing identity and access management (IAM) for the consumers and the providers of the system, which often means linkages into existing security process tooling. Key management for encryption might also be needed for data that is stored off-premises (see "Cloud Security and Emerging Technology Security Primer for 2016" and "How to Make Cloud IaaS Workloads More Secure Than Your Own Data Center").

Once the services and related processes have been defined, it's time to dig deeper into the technology and the tooling.

Map Workloads to the Associated Cloud Services

A detailed review at the workload level is required in which each workload is analyzed for its applicability to cloud computing and its location (private versus public cloud environment). The workloads that make up the applications that provide the services should be the focus. I&O leaders should ask the following questions:

What is the overall architecture of the workloads that make up the application – for example, what is at the user interface tier, the application tier and the data tier?

How do the tiers communicate – for example, what protocols are used, and are there any latency sensitivities?

Could the tiers be split – for example, one portion on-premises and another in a public cloud?

What is the security profile for each workload – for example, can it reside off-premises, and must it be encrypted?

After the workloads have been analyzed, the focus switches to where best to run them. For example, should the workload run in a public cloud or an on-premises private cloud. If it's on-premises, where, or should it be run on a combination of on-premises and public. I&O leaders must be objective and not force-fit an on-premises solution, because a hybrid cloud computing model is likely to be in their future (see Note 2 for the most common hybrid cloud architectures).

Gartner's pace layering (see "How to Develop a Pace-Layered Application Strategy") can be helpful here in advising what applications and workload should be tackled first. For example, systems of differentiation and innovation are often the first targeted for critical systems of record are candidates for SaaS services.

Finally (and only after going through the previous steps) can the tooling decisions be made. Hybrid cloud management will involve multiple tools (see "IaaS Cloud Management Tool Selection Methodology"), so the analysis should consider how a set of tools will interact. I&O leaders must also consider the organization's ability to perform this system integration effort. The analysis might show that a hosted private cloud or a public cloud service is the better option, versus having the I&O team build and manage a private cloud.

I&O leaders should systematically walk through the steps described above as they craft their cloud strategies. They will lessen the probability of achieving success from their cloud plans, if they do not go through the rigor defined in the above three steps – for example, jumping straight to the technology.

Evidence

This research is based on more than 100 interactions with enterprises and vendors during the past 12 months associated with cloud management strategies.

Note 1

Operational Monitoring Capabilities

Reactive: Alerting, after a consumer is affected.

Proactive: Alerting, before a consumer is affected. Often paired with automation, when corrective action is automatically taken.

Forensics: Analysis, post facto, of chronic abnormalities.

Note 2

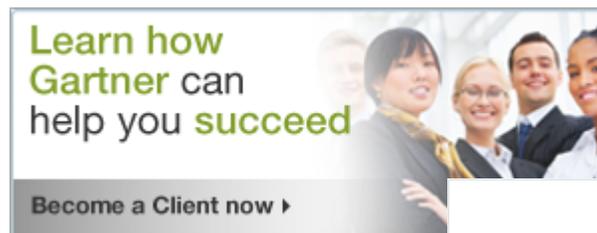
Common Hybrid Cloud Use Cases

Application/Data Integration: Application on public cloud, data on-premises or in a colocation facility.

Development/Test: Development and test are in the public cloud, but the production activity is in a private cloud.

Disaster Recovery or Data Synchronization/Backup/Archiving: Leveraging public IaaS facilities.

Cloudbursting: Typically active/active scale-out applications with autoscaling.



(https://www.gartner.com/technology/contact/become-a-client.jsp?cm_sp=bac_-_reprint_-_banner)

© 2016 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. or its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. If you are authorized to access this publication, your use of it is subject to the Usage Guidelines for Gartner Services (/technology/about/policies/usage_guidelines.jsp) posted on gartner.com. The information contained in this publication has been obtained from sources believed to be reliable. Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information and shall have no liability for errors, omissions or inadequacies in such information. This publication consists of the opinions of Gartner's research organization and should not be construed as statements of fact. The opinions expressed herein are subject to change without notice. Gartner provides information technology research and advisory services to a wide range of technology consumers, manufacturers and sellers, and may have client relationships with, and derive revenues from, companies discussed herein. Although Gartner research may include a discussion of related legal issues, Gartner does not provide legal advice or services and its research should not be construed or used as such. Gartner is a public company, and its shareholders may include firms and funds that have financial interests in entities covered in Gartner research. Gartner's Board of Directors may include senior managers of these firms or funds. Gartner research is produced independently by its research organization without input or influence from these firms, funds or their managers. For further information on the independence and integrity of Gartner research, see "Guiding Principles on Independence and Objectivity." (/technology/about/ombudsman/omb_guide2.jsp)"

About (<http://www.gartner.com/technology/about.jsp>)

Careers (<http://www.gartner.com/technology/careers/>)

Newsroom (<http://www.gartner.com/newsroom/>)

Policies (http://www.gartner.com/technology/about/policies/guidelines_ov.jsp)

Privacy (<https://www.gartner.com/privacy>)

Site Index (<http://www.gartner.com/technology/site-index.jsp>)

IT Glossary (<http://www.gartner.com/it-glossary/>)

Contact Gartner (http://www.gartner.com/technology/contact/contact_gartner.jsp)

