Cloud Computing

CHAPTER 6

WHAT ARE CLOUD BUSINESS CONCERNS?

Dr. JAMIL S. ALAGHA

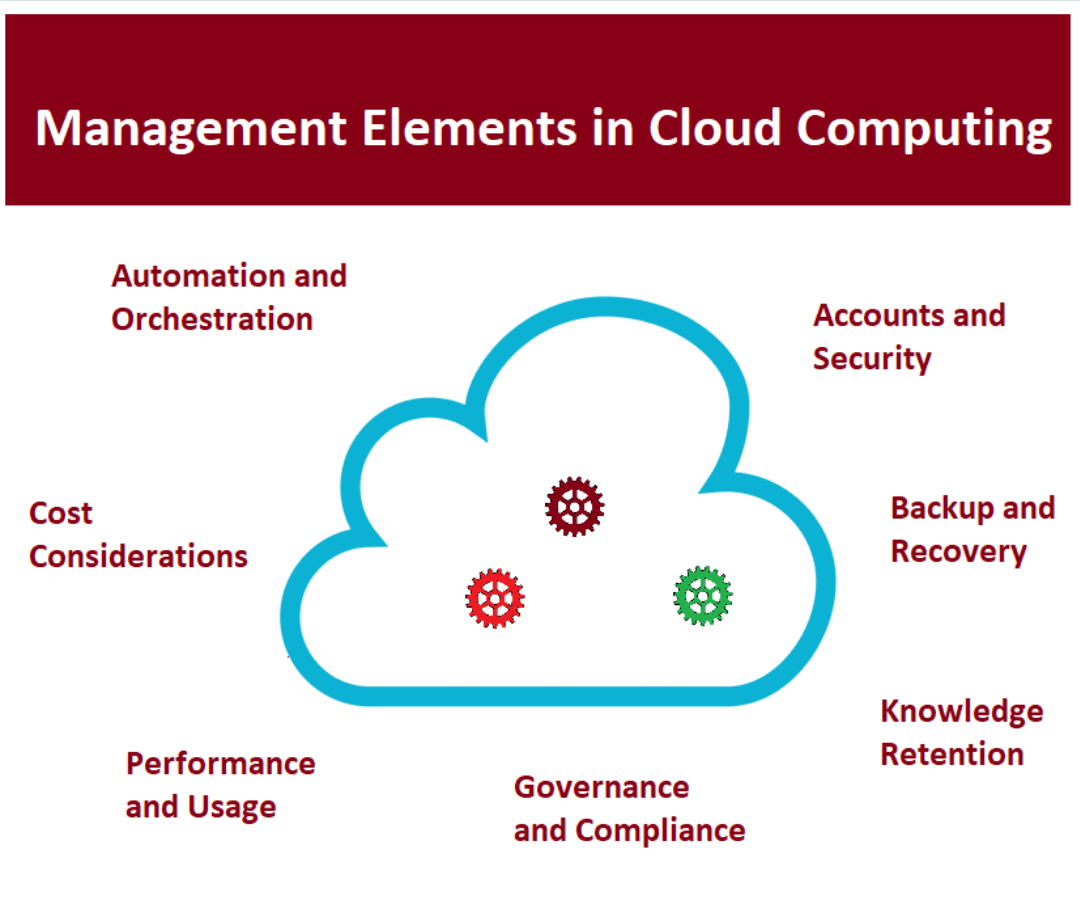
What are cloud business concerns?

Cloud computing has a complex business model that transforms how accountants and financial managers view IT costs

Movement away from upfront investment in capital equipment

Organization use pay-as-you-go model to directly tie use to expense

Management tools in areas such as monitoring and consoles, service level agreements (SLAs), and subscriptions/billing support business operations



MANAGEMENT ELEMENTS IN CLOUD COMPUTING

Monitoring and Console Tools

Usage tied directly to organizational entities

Knowing who uses what and to what extent enables understanding the costs of production, support, and organizational overhead

Helps avoid or at anticipate cost overruns

Ensure resources operate as desired.

Problems and issues with capacity can be watched directly or through automated management tools that send out alerts

Aids in security processes

Sources of Monitoring Tools

- *Cloud provider tools*: Default option because most cloud providers have these built into their platform. No installation is required, and administrators can use these immediately
- *Third party vendor tools*: Can be purchased, often on a subscription basis, to integrate monitoring operations and provide specialized reporting and oversight

Benefits of Cloud Monitoring

- Costs are contained and controlled
- Interruptions can be preempted and avoided
- Maintenance costs can be reduced
- Paying for more resources than required is avoided

Monitoring Tool Plan Considerations

- **Identification of key metrics** – Recognize important, key activities and monitor related resources
- **Integration of monitoring results** – Summarize key elements dashboard or other accessible medium
- **Cost considerations** – Linking costs to resource use should be integrated into reporting
- **Identify triggers for action** – Particular threshold levels should be identified, and automatic notifications sent to key personnel under appropriate conditions
- **User metrics** – Assess user experience, for instance, are response times acceptable, are there any bottlenecks in workflows or resource access?
- **Testing** – Monitoring events during failures and resource outages should be included in the plan. Does the system react as expected? What is user impact?

Example Native Cloud Monitoring Tools

- *Microsoft Azure Monitor*: Helps IT administrators gage performance of their cloud-based resources. Built into Azure cloud infrastructure. Some monitoring items free, and others use subscription model. The software permits highly granular review of resource performance and utilization. Features enable actions, based on alerts, to be automatically invoked. Provides drill down features.
- *Amazon CloudWatch*: Native suite of tools that oversees, monitors, and diagnoses issues on AWS Cloud. Available to all AWS Cloud users. Provides data describing resource performance, activity, and usage. Invokes actions automatically to correct ongoing issues or problems with overall dashboard describing system health. Collects operational data in logs, metrics, and events that can be ported into analytics tools.
- *Google Cloud Operations*: Google acquired Stackdriver which provides performance and diagnostics data derived from operations in Google Cloud. Offers monitoring, event logs, activity traces, error reporting, and alerts. Permits developers to engage with problems and track the source issues more easily with visual tools.

Software	Overview	Description of Third Party Cloud Monitoring Tools
AppNeta	SaaS app monitoring tool	Monitor networks. Looks at resource usage, user experience.
AppRiver	Monitors web apps, Office 365 and email services	Protect email systems, reduce spam and encrypt emails.
BMC TrueSight Pulse	Monitors web apps	Add-on to Amazon CloudWatch or Azure Monitoring and includes visualization features and advanced notifications.
Datadog	Infrastructure monitor	Provide additional monitoring features, dashboard capabilities, and visualizations.
Dynatrace	Monitors business analytics, containers, applications, and infrastructure	Mature package that is highly rated. It works with all major cloud platforms and offers a great deal to Google Cloud users.
LogicMonitor	Monitors overall stack of cloud operations	Comprehensive monitoring software that has received numerous accolades and awards.
Rackspace Monitoring	Used for enterprise-wide monitoring	Comprehensive package with excellent notification system for Openstack
Retrace by Stackify	Performance monitoring for .Net and Java development	Provides performance metrics, error monitoring, and logs.

Monitoring Challenges

Hybrid and multicloud systems present complexities with unique situations

Single monitoring solution may not be within the reach of all organizations (e.g. single pane of glass monitoring solution)

Development of monitoring as a service (MaaS)

Understanding end-user experience which may be deeply rooted in organizational culture and activities

Managing vast amount of data collected by monitoring, tracking, troubleshooting, and logging

Cost Monitoring

Several factors such as adding more VMs, storage, database instances, application licenses, and other more tangible items correlated to higher expense

Subtle issues like a surge in web app use might result in higher costs

Failing to manage deprecated VMs and other resources can result zombie instances

Monitoring tools can help locate and remove these cost incurring, non-productive items

Typical Cost Monitoring Tool Functions

Identification and removal of unused or unintentionally provisioned resources

If operational trends show an increase in cost without corresponding increases in demand, the tool can be used to identify why extra bandwidth or other consumption is taking place.

Regular costs are broken down into more detail both in reports and on a dashboard to help IT administrators track costs and assign these to organizational activities.

Insightful visualizations of costs over time can be produced.

Zombie Instances of Resources

Resources may be created and forgotten

Usually results from IT-related action that either fails, is interrupted, or is invoked incorrectly

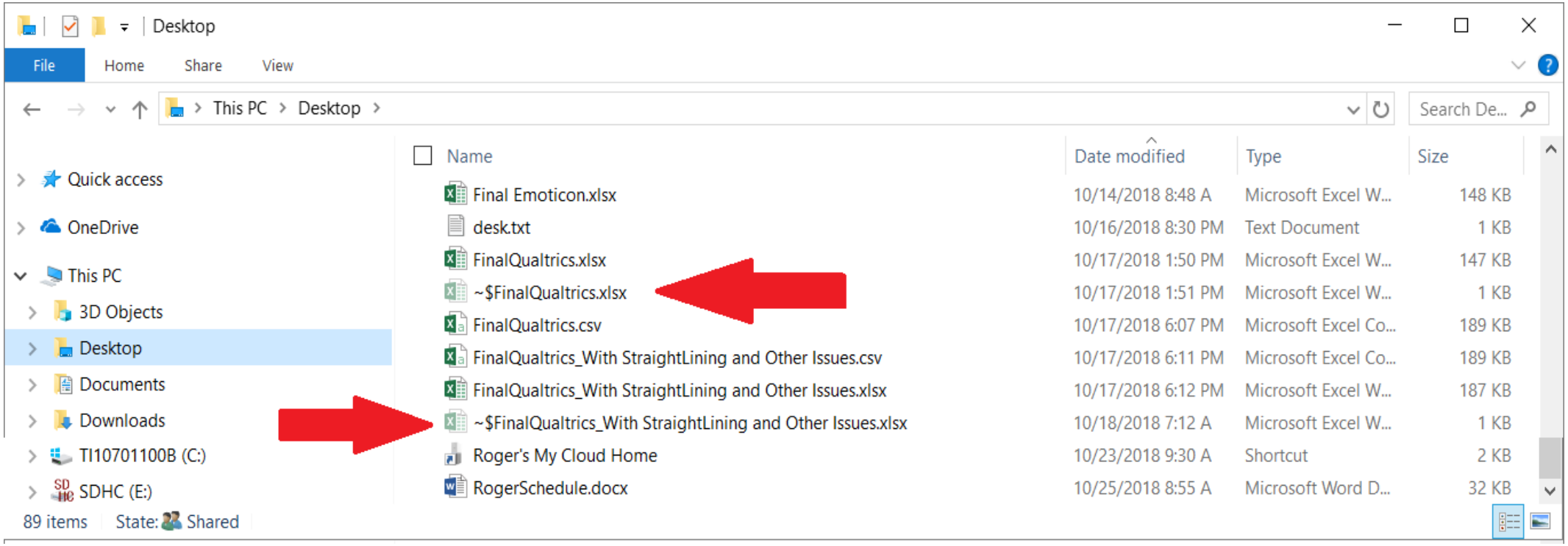
VM build failure can create a zombie VM

File may be opened and never closed by software

Obsolete datasets held in memory

Software makes updates or changes to files and temporary copy is not removed

Temporary files in Windows take up storage space



Gamification of Management Consoles

TotalCloud is a third-party cloud vendor that has created an immersive tool to control cloud resources. The idea is that gamification provides a natural way to interact with a system and this will motivate users to optimize resource usage. TotalCloud is inspired by Warcraft and provides a visual and aural environment to 'move' IT specialists into their cloud infrastructure. The goal becomes fixing security issues, optimizing resource usage, fixing problems, ensuring compliance, or finding unexpected cost savings. What a great idea! Fun at work for sure!

Service Level Agreement

Binding contact between a cloud vendor and their client

Describes conditions for use and minimum level of service and performance by cloud vendor

Service and performance levels include uptime, availability, reliability, and responsiveness

May contain information relating to actions if the system goes down or interruption occurs

SLA protects vendor and provides reasonable expectations for client

Many cloud vendors offer standard SLAs; others are negotiated

What should SLAs cover?

An excellent article by Thomas Trappler describes important aspects of SLAs and what they should cover at a minimum. He summarizes by suggesting a contract (Trappler, 2010):

- "Codifies the specific parameters and minimum levels required for each element of the service, as well as remedies for failure to meet those requirements.
- Affirms your institution's ownership of its data stored on the service provider's system and specifies your rights to get it back.
- Details the system infrastructure and security standards to be maintained by the service provider, along with your rights to audit their compliance.
- Specifies your rights and cost to continue and discontinue using the service."

General SLA Areas

Management features - Standards, measurement techniques, methods for collecting data, report types, and report frequencies to provide the information used to define service levels. Also include conflict resolution, SLA update processes, and finally an indemnification clause.

Service elements - Exact services provided, what is not specifically provided, conditions for service, time frames for service, responsibilities of each party related to service items, penalties for failures, metrics for service levels, and cost/service tradeoffs.

More on Indemnity

An indemnity clause is very important to the cloud service client and protects against lawsuits caused by cloud vendor actions. Most standard cloud provider SLAs do not include an indemnity clause but an organization about to enter a cloud service contract should demand that one be included. Many lawyers have experience with indemnity clause wording and can quickly put one together. The cloud vendor may seek to negotiate on this item, but it is very important and potentially very expensive considering the scope and number of recent data breaches.

SLA Metrics

Mean time between failures (MTBF)

Mean time to repair (MTTR)

Downtime per year or other time frame

SLA Metric Considerations

- SLA Metrics must not reward poor performance
- SLA Metric measurement source (vendor, client or third party?)
- Time frame for metric collection

Metric Types

Service availability metrics: Common metric used to assess vendor obligations. Basically, the vendor guarantees service uptime.

Service performance metrics: Service performance speed often considered in development of metrics.

Service quality metrics: Some cloud customers more worried about accuracy of storage, backups, web services, and other items.

Security metrics: For other organizations, privacy and security-related concerns are paramount.

Key business performance metrics: The best metric may be a key business performance related item to help cloud vendor and customer work together to achieve a desired outcome.

Example Service Uptime Metric Calculation

1 year of time = 24 hours X 60 minutes per hour X 60 Seconds per minute X 365 Days.

So, 1 year is about 31,536,000 seconds.

If we multiply that by the 99.5% uptime figure we get: 31,378,320 seconds.

If we subtract the uptime from the total time: 31,536,000 - 31,378,320 = 157,680 seconds

157,680 seconds / 60 seconds per minute / 60 minutes per hour = 43.8 hours of downtime

Is that too much downtime?

Other Metric Considers

Exclusions and exemptions

Crucial time frames or key uptime dates

Testing dates / frequency

Performance Failure Penalties

Service account credit

Direct compensation. Amounts could be tied to revenue loss during service outages

Outside oversight

Covering costs to switch to new vendor.

Earn-backs are the right to reduce service credits if actions accomplished by the cloud vendor---may not cover entire penalty amount but incentivizes cloud vendors to fix issues in a timely fashion

SLA Data Ownership Clause

Who owns the data?

Where is the data physically located?

What happens to the data upon contract termination?

What happens should a data breach occur?

How are government or other requests for data access managed?

Sample data ownership clause - SLA from Axiell ALM Cloud Service in the Netherlands

9 Ownership of data

At all times, the Client will remain the owner of the data that is stored and managed in the Adlib databases. The Client will have full custody over the content of their Adlib database and Client specific digital assets such as images and electronic documents.

Data Location

Legal issues have emerged due to data location. The laws of countries and jurisdictions vary, and legal problems concerning data migration, import, export, and storage can result if a data center or backup is physically located in a country other than your own.

Countries with Strong Data Privacy Laws

Organizations or individuals may wish to store data in locations where government access is limited. This could be for nefarious reasons (e.g. drug cartels or Mafia-based systems) or just because an organization feels threatened (e.g. political parties or religious groups). The following three countries offer good data protection and are good hosts for VPN services.

Switzerland: Of course, Switzerland has long been the paragon of neutrality. It maintains a longstanding policy of not being party to political agreements, extraditions, or other forms of international interaction. Switzerland also provides a good location for data storage and is a strong advocate for data privacy. It has a Federal Act on Data Protection law and generally refuses to allow access to its citizens' data. It is a pro-consumer country. It does, however, have an agreement with the US government that allows data access through a strict subpoena process related to banking fraud and terrorism.

Malaysia: This country has very strong data privacy laws which protect data owners. It also has a law called the Malaysian Personal Data Protection Act to keep its citizens' data private when possessed by others. It has heavy fines for violations. This is a good place for data storage if the data set does not contain the personal data of Malaysian citizens.

Iceland: This geographically isolated nation has no agreements for data sharing or access by the US or other countries. For US-based companies, this is a great data storage choice located between Europe and North America. Iceland has a long history of challenging foreign government data access requests and takes its custodial role very seriously.

Of course, no data is 100% guaranteed to never be accessed by government agencies, particularly when crime or terrorism is motivating the access.

Data Disposition

Deal with vendor actions after a contract is terminated

Organization does not want to be indefinitely tied to the same vendor---need for orderly way out

Must be economically feasible and realistic way to transfer to another vendor

Migration

- Issues relate to vendor performance or costs
- Need to migrate because of consolidation or purchased and systems will be integrated

What media migration will use, time delays involved, and who completes the migration

Data Breaches

Contracts may include indemnity clause that shifts the cost of a data breach to the cloud provider should it be their fault

Ensures any lawsuits are covered by the vendor rather than the cloud client

Important to consider actions needed should a worst-case scenario occur

Sample Data Breach Indemnity Wording

"[Vendor] shall defend and hold Institution harmless from all claims, liabilities, damages, or judgments involving a third party, including Institution's costs and attorney fees, which arise as a result of [Vendor]'s failure to meet any of its obligations under this contract."

And:

"[Vendor] shall indemnify, defend and hold Institution harmless from all lawsuits, claims, liabilities, damages, settlements, or judgments, including Institution's costs and attorney fees, which arise as a result of [Vendor]'s negligent acts or omissions or willful misconduct." [3]

Governmental Access Rights

Both client and vendor expect to follow all laws within the terms of service

May require vendor to turn over data for a criminal investigation of an individual whose credit card or other data resides on their system.

Could be circumstances where another client of the cloud provider is under investigation and as a result government agency has access to all portions of the provider's cloud

Cloud customer should ensure the provider is responsible for contacting them should this occur

Ideally, prior to releasing data but some court orders could prohibit that from occurring

Other SLA Considerations

SLA revision policies

SLA Transfers with ownership changes

SLA Advice

Read agreement carefully prior to subscribing. May impact choice of a cloud vendor.

Have an IT specialist from within the organization, or technical consultant from an uninvolved organization, review the SLA for any details that might not be clear.

Ensure the legal framework for the SLA is sound and fair. Get legal counsel to review the agreement and provide advice.

Ensure you have contingency plans in case the vendor goes out of business or has other difficulties. This may mean having an onsite backup periodically made or having another solution.

Billing

Side benefit of cloud computing is approach to billing.

Instead of paying large, up-front costs, most cloud users start the service and pay a periodic bill much as they would with any utility.

Many cloud systems have native billing systems

Third party billing tools are available

Chapter 6 Summary

Cloud computing has complex business model that matches well with a modern businesses' information requirements

Managers and accountants must be able to understand IT costs from a usage perspective and tie that into requirements for elasticity, resource demand changes, flexibility, agility, and smart planning

Cloud moves businesses from a capital investment model for computing infrastructure to one that more closely matches a utility company

Monitoring and console tools provide IT specialists and managers with ways to understand and predict usage

Issues with capacity and other important attributes can be 'watched' either directly or through automated management tools that send out alerts

Monitoring aids in the security process and ensures the correct resources are accessed only by authorized users

SLAs are binding contacts between cloud vendors and their clients that describe conditions for use and minimum level of service and performance the cloud vendor provides

Performance level requirements may be uptime, availability, reliability, and responsiveness

SLAs generally contain information describing actions should the system go down or an interruption occurs

SLA protects the vendor and provides reasonable expectations for the client

Cloud providers use the utility billing approach to charge for services