Cloud Security, CLS

June 8, 2013

Mayur Pant

25 pages

Contents

Abstract

We are presented with a case study of an established consumer obligated business in the financial sector. In our hierarchy of business criticality, our example case is at the top; we expect 24/7 availability with high resilience to millions of simultaneous customers, with high security against intruders.

In answering this I found the flow of the questions naturally covered the material presented during our education, and as such we focus questions on particular topics from the reference material. Our reference material here is: Clouds Management & Security (CMS) [1], the slides [2] and exercise model answers [3] (the latter two derive from CMS).

In taking this approach, I found the following isolations for each question:

a: deployment type
b: service type
c: trust and assurance
d: self management and provenance

Research evidence has been provided extensively from the written material and realworld examples, with particular emphasis on tailoring the research to a derived conclusion that the answer requires. The Appendices contain additional applicable materials from the realworld.

a

a.1 Initial thoughts

My initial thoughts from a first reading of this question directly following a week of tuition are that:

FI has a well established private Cloud infrastructure; we have been taught that public Clouds are a far less secure deployment type than private, especially for industries of finance or medicine where numerous security obligations must be met.

Consequently, we hope that FI will maintain its private Cloud for most applications, yet outsource to BI's updated Risk Management Application as Software as a Service.

We are applying particular significance on mitigating the threat of insiders, and upgrading to BI's Risk Management application - as these are the two stated reasons for FI's losses.

Our answer is laid out as follows. First we will analyze each of the models using the literature and slides available from our education. This compromises of a matrix of quotations relevant to our argument, followed by commentary (I chose this approach because this is a relatively new field - evaluating written evidence is crucial for proving our decision). The matrix is followed by a discussion and conclusion to supplement our initial thoughts following our research.

For the matrices of a) and b) I have adopted a colour scheme the denotes whether the statement is positive or negative (pro or con). Comments (non-quoted material) are in italics.

	private	public	point
Security	*The most **secure** deployment type - although in the case of FI, still vulnerable to insiders*	Considered less **secure** than private Cloud. [S 32]	1
		risks involved when outsourcing their data and services to public Clouds [EX 1]	2
			3
		Public Cloud deployment type is associated with enormous **vulnerabilities** in comparison with other Cloud deployment types. For example, public Cloud is a **shared** infrastructure that could be used by anyone including competing organisations, public Cloud insiders have higher motivations to **attack** customers' applications (on shared, multi-tenant architectures), customers have no way to get the assurance of where their data is processed and stored. [EX 1]	
Mitigation	Is used by one **specific** enterprise [S 32] Most often banks & telecomms [CMS 1.5]	public Cloud should only host services which could be fully managed automatically with minimal human interventions [EX 1]	4
			5
		Fully automated management services are not yet available [EX 1] cases which currently require excessive human intervention: Automated and effective elasticity property ; Self-detection of failure and automated recovery; the lack of automated data management mechanisms has direct effects on the QoS [CMS 1.6 : Challenges of Cloud : Operational Management & Data Management]	
	Management could be **outsourced** to a third party [S 32]		
	The enterprise could either directly manage the private Cloud infrastructure or it could **outsource** its management to a third party [EX 1]	Such lack of automated management services forces public Cloud providers to mainly support only basic services which can be automated. These basic services currently cover the needs of **casual** users, **small** businesses, and **uncritical** applications. [EX 1]	6
	Perhaps FI could outsource its private infrastructure to be managed by BI	*Our experience tells us that private Clouds are more secure than the public Cloud (and more appropriate for financial institutions). The previous definitions contradict FI's business type.*	7
		It is likely to be cheaper than a private deployment	8
Issues	Community and private Cloud deployment types establish **strong relations** with their customers [EX 1]	It could be that BI is offering the public Cloud model for its own financial gain - it offers a fine application, and opted to provide a mass public Cloud so it could sell the product as a long term subscription cost rather than a one off payment (an	9
	customers typically have a relationship of mutual benefit or shared goals with the Cloud provider; customers may also be **contractually bound** to good behaviour [EX 1]	increasingly popular sales model (adopted by Adobe Creative Cloud, Google Docs, Microsoft Office 365). The whole "per usage" payment seems like a potential trap - assuming that FI has many (tens of thousands plus) customers, it may prefer to keep its own infrastructure, rather than giving a "variable annual share" of its success to BI. So FI offers the mass public Cloud 'per usage' model to reduce its costs and gain the most customers, but not necessarily for the optimum benefit of FI. Approach with caution (and future growth forecasts - a pay-per application usage billing scheme with SaaS should be less cryptic and more predictable than an IaaS billing scheme that depends on resource usage derived from logging and provenance).	10
	The above 2 statements seem appropriate to customers of a financial institution		
	By contrast, users of public Clouds are much more **reliant** upon infrastructure properties in order to establish **trust**. [EX 1]		11
	For *such an institution trust needs to be paramount (especially where insiders have already caused so much loss, even at a private deployment type)*	*FI may not be a small business, and its risk management application is critical. While we would like to reduce the **Operational Management** cost with a public Cloud, a primary concern must remain **security** and **Insider Management**.*	
	Far more costly to maintain independently (although may be a required overhead expense for a financial institution)	*If outsourced to BI's public Cloud, it must be aware of **legislation** in the country (or countries) the public Cloud is hosted in, to protect its financial law obligations. These are **Data Management** concerns.*	12
			13
	*That insiders have caused so much loss in a private model suggests that FI is not fit to manage its own private Cloud - yet we still wish to avoid going to public since it is more insecure. This suggests to us that FI should seek third party management of its existing private Cloud, thus: preventing losses from abandoning its existing investment; avoiding the insecurities of a public Cloud; excluding the insiders that have already threatened its private Cloud (and their annual staffing overhead). This is known as **Insider Management**.*	*Similarly, if the public Cloud is scaling up and down, FI must have assurance that the resource is scaling within a country of legislation, and data repositories used in the scaling process are secured (i.e. that BI's **chains of trust** are guaranteed [CMS 9.3]). So the public Cloud offers greater **Operational Management** concerns than private (if FI do not know the complete details of the public resources).*	
			14
		"Ask providers if they will commit to storing and processing data in specific jurisdictions, and whether they will make a contractual commitment to obey local privacy requirements on behalf of their customers, Gartner advises." Gartner: Seven Cloud computing security risks [http://www.idi.ntnu.no/emner/tdt60/papers/Cloud_Computing_Security_Risk.pdf]	
			15
		Data segregation. "Data in the Cloud is typically in a shared environment alongside data from other customers. Encryption is effective but isn't a cure all (encryption accidents can make data totally unusable, and even normal encryption can complicate availability). Find out what is done to segregate data at rest," Gartner advises.	
			16
		There is legislation that attempt to discourage breaches (e.g. Cloud Computing Act of 2012", Sept. 2012 http://www.govtrack.us/congress/bills/112/s3569, *which attempts to fine access each of unauthorized account) but at present they are in total infancy* [http://www.forbes.com/sites/ericgoldman/2012/10/02/the-proposed-cloud-computing-act-of-2012-and-how-internet-regulation-can-go-awry/]	

Key

positive
negative

[S ..] slide number (Bibliography: [2])
[EX ..] exercise number (Bibliography: [3])
[CMS ..] book chapter number (Bibliography: [1])

	community	hybrid	point
Security	More **secure** than public, but **less** than private (audio, own notes)	***Security*** *depends upon the use of the* ***weakest element*** *(the public Cloud)*	1
			2
	Security depends on a **security standard baseline** of all participants - **standards** that public Clouds do not have (audio, own notes) *Examples: OpenGrid for Universities* *Aerospace Industries Association (AIA) community Cloud for aerospace and defense industry [Cloud Computing Report on Cloud Computing used in the Aerospace and Defense Industry, http://www.aia-aerospace.org/assets/EEIC_2012-005-004-00_Cloud_computing.pdf]* *SWIFT provides community Cloud services for banks ("The not-for-profit cooperative began in 1973, with 239 banks on board from the start. It provides a network that sends an average of 17 million financial transaction messages every day across 209 countries. About 8,000 financial services businesses use it. During 2010, it processed more than four billion financial transactions.") [http://www.computerweekly.com/news/2240104825/Bank-app-store-part-of-community-cloud-developments]*		3
			4
Mitigation	Utilizes **shared expertise** from the financial sector to help **secure** and **set standards** for the community Cloud.	Reduces costs by establishing a private Cloud only where necessary (e.g. for its most important applications), and cheaper public or community solutions for applications that have different security or volume requirements	
			5
	On the flipside, competitors may act as an **insiders** - sharing platforms to launch security **exploits** and view competitor data	*E.g. Private / CPU intensive Cloud resources (e.g. high CPU rated machines) are used for current data. Archived financial records (or data records that for example, may become public domain, or require less access after a set number of years) could be moved to a cheaper public Cloud (with resources more suited to lowspeed data access and long term storage)*	
Issues	Organizations from the same business domain could collaborate and establish their own community Cloud infrastructure. [S 34] *We know that BI is used by many financial institutions. However, these financial institutions, if they are using BI, are presumably running independently on BI's public Cloud.* *FI might choose to collaborate with existing financial institutions to form a community Cloud (upon its existing private Cloud resources, or provide hosted PaaS - similar to how EngineYard Hosting builds on Amazon EC2 infrastructure to resell a PaaS to its own clients [15]); but due to lack of evidence in our text, and the established private infrastructure that it has already invested in (surely after consideration of a community Cloud option), we are drawn towards staying private. Of course, if it chooses to establish a community Cloud based on its infrastructure it may reduce its expenditure by leasing out, and increase security by coalition expertise. It may however, open itself to insiders from competing institutions running on the community Cloud (presumably Financial institutions prefer to compete rather than cooperate, unless they can pool their investments for a larger return, or make significant savings like the clients of SWIFT).*	Mixed deployment e.g. private Cloud when outsourcing its backup data to public Cloud [S 35] *An OK idea if the goal is to save costs.* *However, our case study gives no discussion of backups to a public Cloud (which may be a cheaper, more archive-centric Cloud than FI's private compute-centric Cloud). Secondly, the idea of a private financial firm creating backups to a* ***more vulnerable*** *public Cloud is worrying - better they lease some private encrypted backup services (with an assured,* ***secure distribution channel*** *) if we are to enter that discussion.*	6 7

a.3 Conclusion

Looking at our analysis matrix, we see that for FI it appears **we have more encouragement to stay with the private Cloud**. **However**, it is clear from the description that because FI's private Cloud is afflicted with insiders, a change must be made.

The second most attractive option seems to be the community Cloud.
Especially for financial institutions, it is conceivable that a community could exist that shares wealth of knowledge regarding security standards in Cloud infrastructure, and common Cloud resources.

However, we cannot make assumptions on this, as our text gives us no precedence for FI's desire to collaborate with other, potentially competing financial institutions (point: community, 7).

One could argue that BI, as an organization that works with other financial institutions, acts as a single interface for the collaborative knowledge of the community; it has dealt with this problem before, and therefore it is wise for FI to collude with them as a provider. This strengthens FI's reason to choose them. But what BI are stated as providing is a public Cloud, not a community Cloud. What BI are really offering is not the benefits of community - but instead the acquired expertise from working in the community, which essentially provides FI with a similar benefit but with an the desired requirement of confidentiality. We have taken the liberty of introducing an idea - that FI might open their existing private infrastructure to form a community Cloud (and hence, potentially gain security knowledge in operational management standards by learning from other providers) in (point: community, 4). We have also shown how the community Cloud exists with SWIFT (point: community, 3) in the financial industry.

Public is the least secure option for FI; but it seems more probable if we have hybrid.

We appreciate that public Clouds will have more customers; and so will be unable to build a stronger relationship with their clients (CMS p.21) (from experience with such providers - they have an exceptional level of support during the early stages when they try to win your contract, but after that a laborious and lengthy ticketing system to get subsequent timely support!). It is much better to have a dedicated, fully managed support team. A public provider CAN provide good support and scalability (as we have found with Amazon [Appendix A]), but at a premium. However - since it is still public, it does not provide the best security. And also, there is the risk of data leakage and account compromise on multitenant architectures (a vigorous assurance of role based security would be needed [Appendix A] - which may still succumb to future, inevitable security exploits). The book states that fully automated services are not yet available (point: public, 5), particularly for auto-scaling and auto-healing, and those that exist are unsuitable for critical applications. This opinion is supported by the EU study of Cloud computing [4].

We also touched (point: public, 13) on the legislation problems that might arise from leasing a Cloud that is not theirs (do the data protections laws of the remote data centre comply with the country of the parent company?), which will require assurances, and guarantees for provenance. It would be foolish for FI to outsource their most critical applications without having checked that BI can provide a high level of assurance (which FI must seek to obtain in question c). Security and legal obligation is more critical than cost (point: public, 9).

Hybrid would only be feasible if (as described in c) - we outsource non-critical functions securely, or we outsource isolated applications with different security requirements.

This doesn't actually seem like such a bad idea.

It brings us the benefits of private Cloud (which has still continued to be problematic for FI), with the added benefits of BI's security knowledge from working with the community, and the potential savings, and escape from insiders (provided that moving to BI doesn't introduce new insiders or shared platform attackers).
Essentially, BI are a specialist provider - one that offers SaaS (with their improved Risk Management Application). This is similar to the way Microsoft offer their services. Despite providing what is essentially a public Cloud (used by many customers), their solution of Office 365 incorporates the software service in quite an assured, trustworthy manner for business[1]. So while my inclination (and literature) points to staying

[1] "We help secure data from the time it is stored at rest within data centers to the time it reaches user devices...Logical

private, a well chosen *hybrid* solution will reap the best benefits of BI's community expertise with the cost savings of public infrastructure, while the more critical applications will remain on FI's private Cloud. In answer c) we go on to explain what assurances FI must seek if it invests in public infrastructure (in the case above for example, it would be perfectly adequate to use a cheap scalable public Cloud alongside a private Cloud for backups, provided the backups and transmission are entirely secured with strong encryption). If a federated, cloud-to-cloud solution is chosen, FI need to consider secure transmission policies - and the challenge of utilizing two different, non-standardized Cloud providers (which may be simplified if individual non-communicating applications are hosted as independent entities on different providers).

b

b.1 Initial thoughts

Now we come to choice of service. Again, my initial thoughts are that IaaS can be dismissed; FI have illustrated a difficulty in self-management security (so if they can outsource to a fully-managed application support team, why not go for it?).

Firstly, despite its private infrastructure, its system is riddled with insiders - in answer a) we suggested leasing the management of its Cloud to BI, who will be more practiced at this task from their work with other industries.
Secondly, it could help them reduce the cost of their current self-managed option — rather than continue to pay existing sysadmins, BI have analysed their expenditure and offered them a potentially cheaper rate to win their contract.

So we are left with the choice of PaaS or SaaS. PaaS suggests to us that BI provide the O/S & userland platform for FI to run or develop their application (e.g. Microsoft Azure[2]); but since the second factor of FI's loss comes from its old Risk Management Application, and its reason for approaching BI was for an upgrade, it makes sense that FI simply subscribe to their SaaS solution for a quick, seamless integration of BI's new program. It should be the quickest option to get running, and most secure since BI will be smoother at providing the solution than FI trying to set up on its PaaS.

Were the option available, we would suggest that BI are contracted to provide their SaaS on FI's private infrastructure, and takeover its management (while FI cleared out its insiders). With BI's SaaS on FI's private Cloud it will have optimium security due to guaranteed isolation from competitors. FI could have the security of a private Cloud with a mitigated threat from insiders - however, this is not assumed in the question.

I have approached this answer in a similar way to question a). My desire is to illustrate my research, outlining the pros and cons of each Cloud type.

1. I have coloured the statements to illustrate whether they are a pro or con of that particular type.
2. Since there are 3 contenders, I have deduced the best option from 2 rounds; (IaaS vs SaaS) and then (PaaS vs SaaS).

I then form a conclusion based on literary evidence. From an original matrix it has been tabulated for better printed readability.

isolation of data between tenants...controlled by a role-based access control process...Segregation of the internal datacenter network...security and privacy are incorporated by design...SSL/TLS encryption of data in transit", Relentless on security - Microsoft Office Cloud services [5]

[2]"Windows Azure Virtual Machines provides IaaS...The third compute option, Cloud Services, provides Platform as a Service (PaaS). This technology is designed to support applications that are scalable, reliable, and cheap to operate. It's also meant to free developers from worrying about managing the platform they're using, letting them focus entirely on their applications." Microsoft, http://www.windowsazure.com/en-us/develop/net/fundamentals/compute/#CloudServices

Round 1: IaaS versus SaaS

IaaS

Security

Control

IaaS Cloud service provides virtual compute and storage resources as services to customers. Cloud providers in IaaS manage the physical resources and their hypervisors. Cloud customers run their software stack and manage the content of their allocated virtual resources. Customers in this type should, in principle, have the overall control over their data. [EX 1]

Verdict con *FI are already struggling with the problem of insiders on their self-managed service. A step away from this towards BI's third party expertise (they specialize in management for many financial institutions) would probably provide a step up in security. Although it is usually considered a positive, overall in-house control has proved to be a negative issue for FI. Control is a good thing for most organizations; but in FI's case, outsourcing management with BI's fully managed software hosted solution will relieve its insider problem.*

Mitigation

Additional effort

If FI are on their own with IaaS, then it may require their system administrators to understand IaaS configurations (e.g. RBAC on shared hosts - additional training). It may be difficult for them to trace whether a software fault is due to their software or the infrastructure technology. At least choosing the SaaS option will allow BI's staff (and perhaps, automated tools) to deduce sources of fault (from having seen them before), and reduce the MTT-I/D/R.

Verdict con *Experience tells us that migrating to a new hosting platform is never easy – particularly if porting an existing app to a new provider (with a different API or new resource management control panel / environment). There may be a training cost. Why not reduce the time and expenses and get rid of existing insiders with outsourcing?*

SaaS

Security

Control

IaaS provides customers with the greatest control over their resources, while SaaS provides the most restrictive access to resources' control. [EX 1]

Verdict pro *In FI's circumstance where it only requires access as granted by certain employee roles, this will probably tighten security, and mitigate against insiders who are currently viewing data against authorization (by locking them out of the approved permissions list). By performing a process for insider analysis (S 124) they can set fine-tuned role based permissions (seeking assurances of optimum security via RBAC configuration & data isolation with key encryption – see answer c).*

Challenges

Transitive management liability

We first identify all actors within such a system, and we need to understand the relationships amongst the actors (*perhaps with a **UML usecase** diagram*) as well as their level of access to resources and assets that are part of the Cloud (S 115). E.g. FI's administrators (insiders) that could connect to hypervisors and leak sensitive data (S 168).

Verdict pro *If BI's administrators were found guilty of leaking customer data, they would not just be fired - BI would be taken to court for settlement and BI's reputation would be at jeopardy. It is hopefully less likely to occur with an accredited management provider. Amazon EC2 requires staff background checks (Appendix A).*

The change also introduces the opportunity for BI to evaluate FI's current role based set up in light of their community / industry expertise. If only IaaS is chosen, FI should not expect this level of assistance.

Mitigation

Performance management

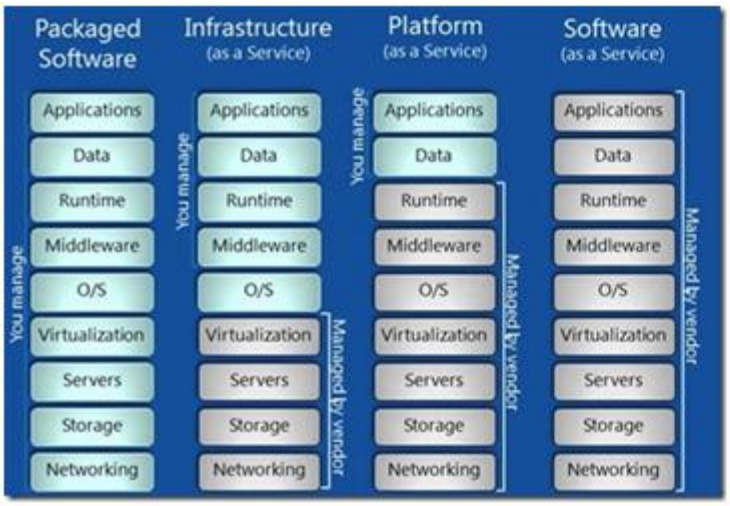
Choosing BI's integrated solution (their software running on their hardware), we expect that they will have optimized their configurations such that scaling and resource usage is optimum (from more expertise in the domain).

Verdict pro *We illustrate realworld feedback and compare the setup processes of SaaS over IaaS in Appendix B.*

Round 1 conclusion: SaaS Wins

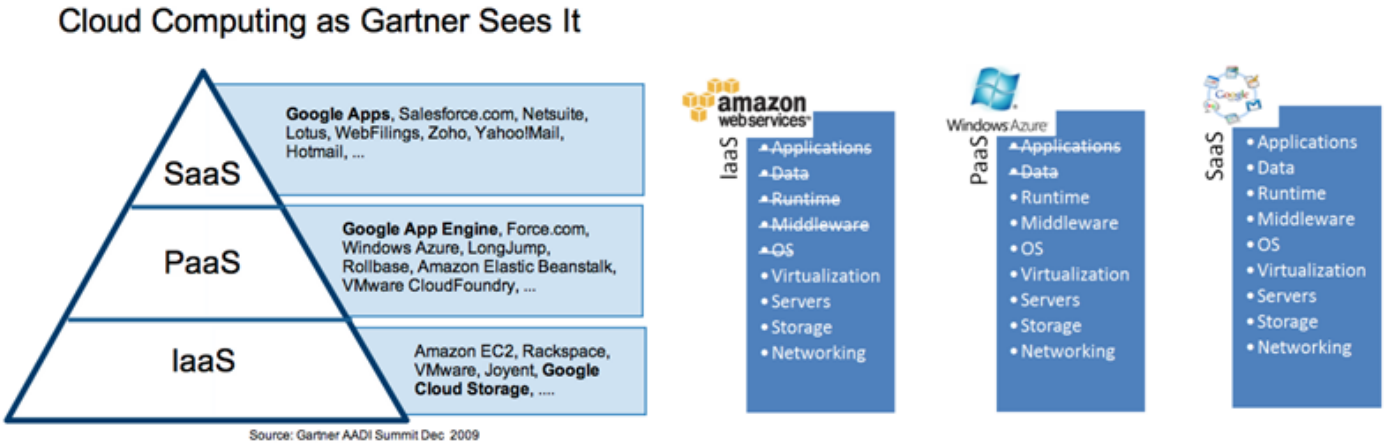
Types	Qualities					
	Control	Performance	Effort	Managed security	Cost	Responsibility (transitive management liability)
SaaS	pro	pro	pro	pro	con	pro
IaaS	con	con	con	con	pro	con

Comparing service types visually (external illustrations)



Is Office365 a PaaS or a SaaS?
http://blog.itayasaservice.com/2012/12/12/is-office365-a-paas-or-a-saas/, Slides by Microsoft

"Amazon EC2 is clearly IaaS, Azure is clearly PaaS, Gmail is clearly SaaS"



Comprehending real world examples
http://cs.uwec.edu/~buipj/teaching/cs.491.s13/lecture_13_google_app_engine_windows_azure.html
http://parasdoshi.com/2012/02/13/cloud-models-iaas-paas-saas-explained-with-examples/

PaaS

Mitigation

A New application
PaaS Cloud service provides the environment and software platforms upon which Cloud customers can develop and host their own software applications. Unlike IaaS customers, PaaS customers do not manage the Cloud's provided environment but only manage their own software stack. Cloud providers of PaaS expose their own APIs which are directly used by customer applications. [EX 1]

Verdict con *This sounds like a great option for any business - and a common issue. All systems administrators are faced with the question of whether to host their own hardware, or to outsource to a third party. FI initially chose to create its own private Cloud, but now sees management and security sense in outsourcing to BI.*

However, in the case of FI, we know that the second cause of losses after insiders was an outdated risk management application - they are ***not*** *looking to just re-host their existing application on more a secure platform.*

Challenges

Migration issues
Cloud providers of PaaS expose their own APIs which are directly used by customer applications. The exposed APIs, at the time of this writing, do not follow any standard. As a result, Cloud customers of PaaS cannot transparently move their applications across competing Cloud providers. (CMS 1.4)

The likelihood of FI being able to port their existing Risk Management Application easily to BI's platform is unlikely.

Multiple vendors
Log records are not properly managed and are dispersed amongst Clouds complex and distributed infrastructure...Log records do not adhere to any standard format...Log records do not explain the meaning of the items of log records [S 200]

Verdict con *Logging and provenance is again a trust challenge due to the lack of standardization. They should opt for SaaS (a complete solution), so they will not be trying to link their existing application logging system with BI's.*

Provenance in (un-controlled public) Clouds with the above problems, is not always practical considering complex infrastructure and dynamic nature [S 200]

Verdict con *As mentioned previously, FI may prefer a simpler single software application ' cost per usage' billing scheme with SaaS [suggested in our case study], than a more cryptic resource usage billing scheme with IaaS or PaaS. SaaS can offer simpler practical billing metrics (e.g. 'active user' licences rather than data usage).*

We will distinguish between the challenges of trust assurance (chains of trust) and provenance with logging for all service types in answers c) and d).

SaaS (in addition to the pros from our previous table)

Mitigation

All-in-one
SaaS provides ready to use software applications which address the needs of specific business functions and processes. Cloud providers manage the software applications and their hosting environment at their resources (CMS 1.4)

Verdict pro *Ideal for FI, who seek to* ***upgrade their application*** *while reducing operational management costs. They can fully outsource to BI.*

Security

Additional effort and knowledge level
The virtual layer should be transparent to Cloud customers using SaaS service, and possibly PaaS service (CMS 2.3.2)

Verdict pro *As mentioned with IaaS, the degree of training and debugging staff is reduced (BI's staff may have more expertise at patching and managing secure environments on having witnessed a larger variety of exploits), so*

an all-in-one managed solution allows FI's staff to focus on newer matters. Furthermore, it is not only time that is saved in setup – we assume that outsourcing to systems administrators with more security experience (for many customers in this domain) will be able to secure and identify breaches more adeptly. This answer's supplement includes excerpts of real world customer feedback that backs up this assumption in Appendix C.

Challenges

Transparency vs. trust evaluation

(IaaS, PaaS and SaaS) serve as forms of abstraction...Such abstraction requires users at a given level (i.e. IaaS, PaaS, or SaaS) to not have to deal with internal details of the operation, management or state of the underlying infrastructure [S 163 / CMS 7.3]

Verdict *affects both. This leads us back to the topic of trust. By outsourcing, surely we are opening FI to risk from insiders at BI? We will speak about how they can assure trust in answer c), and tracebacks of breaches with logging/provenance in answer d) - for now, we consider our trust challenges as the assurance of an ongoing* ***transparency strategy*** *from BI, stating the way they manage FI's customer data.*

If a verifier is a SaaS user then the verifier would need to be provided with the mechanisms to assure him about the trustworthiness of the Cloud to manage the software applications. This would cover the hosting environment (physical and virtual), as agreed in the SLA. If the verifier is a PaaS then he would need the same assurances as IaaS and, in addition, an assurance that the Cloud would manage the additional software components of the development environment provided by the Cloud which are required by the verifier when developing his applications at the Cloud. [CMS 9.4]

Verdict pro *This last conclusion illustrates the point about 'transitive management liability', and the benefits of SaaS over other service types. It is saying that with SaaS a simple definition in the SLA will cover responsibility for breaches of trust in the application. From experience, an SaaS (or 'fully managed environment', which always comes at a premium) is invaluable when a fault occurs – not least because BI's experts may recognise the fault quicker (reducing MTTR), but more importantly that they will not* ***deny responsibility*** *for fixing it (i.e. pointing the finger at the error of FI's programmers, or in the case of IaaS, sysadmins, thus delaying its resolution).This is a security premium worth paying for in business environments.*
Should IaaS or PaaS be chosen instead, FI's programmers will either be bound to strict coding compliance, and even then, a probable 'finger-pointing' delay scenario between BI's sysadmins and FI's programmers when a fault occurs.

This leads us nicely on to question c) where we discuss how assurances will be defined.

<u>Round 2 conclusion: SaaS Wins</u>

Quality / Types	Application upgrade	Control	Performance (scaling config.)	Migration effort	Compatibility (for provenence)	Training	Responsibility	Trusted implementation
SaaS	pro	con	pro	pro	pro	pro	pro	pro
IaaS	con	pro	con	con	con	con	con	con

b.3 Conclusion

"*you cannot decide on IaaS or PaaS without performing risk analysis*" [Ex 4]

While we have not gone so far as to create a Probability vs. Impact matrix, we have filtered the best choice in a suitable binary Cloud Type vs. Quality matrix.

We took into account the statement regarding FI's desire to upgrade to a new application; and the knowledge that BI already offer a newer application.

We considered it would take a greater time and cost to implement their existing solution on IaaS or PaaS, and not necessarily clear out insiders.

We considered the importance of an infrastructure provider offering an all-in-one, well configured and performance optimized product when it came to troubleshooting. Not only are they able to make guarantees of the hosting platform, but also of the Software itself. These guarantees, as we will establish in c), will include MTTR and security accreditations.

For FI, a trial of BI's new SaaS solution is instantly provisionable (with a beta testing timeframe of 3-6 months), at a lower cost than porting its existing application to IaaS or PaaS while not necessarily ridding the existing problem of insiders or an old Risk Management Application.

Following the ideas in B.1 Initial Thoughts, we have assessed various Qualities in a clinical and fair way.

The main points are that:
while SaaS offers a lack of control over IaaS or PaaS, it offers a seamless and quicker upgrade to BI's improved Risk Management Application. Choosing BI SaaS will mean a better maintained, likely optimized solution, which can be trialled within hours (as opposed to the lengthy process of FI porting their application to BI's PaaS infrastructure). We find that SaaS offers the most support from BI's management team. As a mature and tested existing solution, it probably offers better performance and standardization for provenance and billing too. It is worth FI testing BI's proposed application (at a low intial cost) before investing into a redevelopment strategy.

Now for additional discussion, please turn to Appendix B.

c Introduction

What are my requirements on the outsourced application (referred to as User Properties)?

- *Cloud service*
- *Cloud deployment type*
- *Cloud trust properties*
- *Legal related issues: location, collaboration with others, etc.*

[slide 166]

We now decide upon the trust properties of our pre-outsourcing steps.

The word trust has a relationship with the word assurance.
OED defines assurance as:

"a positive declaration intended to give confidence; a promise"

and as such trust in that promise is critical.

When FI asks for assurance, it entrusts that their management specification to BI is met (that is, BI adhere to their declaration). So in this section, we speak about both trust and assurance.

So we will first speak about trust in operational management, which is a well covered in our slides (breakdown in Appendix F). We then speak directly about the term "assurance", that leads us nicely into the final slides/CMS chapters 9 & 10 about provenance and logging which are the topic of question d).

c.1 The value of a Service Level Agreement

When switching host, it is standard practice to gather the terms and conditions in the form of a Service Level Agreement (SLA). In hosting support, it is most important to define uptime - and, in the case of a fault, the maximum number of hours between resolution (e.g. a guaranteed 1 hour MTTR, like Rackspace Cloud - excerpt in Appendix C. In the case of hosting, a Cloud SLA may guarantee auto-scaling to prevent downtime during peak times). Some companies guarantee their SLA, offering cash compensation when the terms are broken. This reassures FI that BI have an incentive to fix their problems, and that fault reports are unlikely to 'drag on' unresolved indefinitely.

c.2 Properties the SLA should define

Section 3.4 of our book tells us that the SLA allows FI to establish quality control, and state its legal and operational requirements with some form of guarantee. With the help of chapter 4 and our work in Exercise 3, we can list the properties that FI will want to specify[3] in the Service Level Agreement. Defining the properties helps us establish Operational Trust (CMS 4.1, slide 146) between two parties, and utilize metrics (MTTI/D/R) which help trust measurement (CMS 4.2, slide 63).

Adaptability The adaptability property reflects a Cloud provider's ability to provide timely and efficient reaction to infrastructure and application changes and events.

FI can considers the following factors in BI's SLA:

MTTD mean time to discover a problem

MTTI mean time to invoke an a remedial action

MTTR mean time to recover from the incident

[3] "Such properties are important for Cloud users when comparing different Cloud providers.", CMS p.57. This is our current status in the pre-outsourcing steps (slide 166)

These abbreviations are particularly important. In standard hosting environments, it is often the customer (or worse, their client) that discovers the problem - although hopefully this will be reduced as automatic fault detection and healing services improve in Clouds (providing adaptability as an automated service, CMS 4.1) - so FI should ask for an assurance and MMTR guarantee in hours. Assuming that BI can offer an automated adaptability service, the mean times of all these factors will reduce, as well as human intervention costs. FI should take these factors as assurance.

N.B. While it is not my desire to re-state the book in my own words needlessly, I do feel that the following properties must be understood, so the reader can watch for them when constructing an SLA. For full details, refer to CMS chapter 4.

Resilience the ability of a system to maintain its features (e.g. serviceability and security) despite a number of sub-system and component failures.

We refer back to our 4 factors to assess resilience. Why is this resilience important? Because FI must accept that hosting failures are inevitable. BI can prove their resilience by transparently publishing their architecture; if they can state there is no single point of failure, and especially high redundancy (at their cost), FI have the facts to believe that it is improbable for multiple backup nodes to fail simultaneously.

Secondly, FI can read through the formalized disaster recover processes (Incident Management history) and assess any compliance accreditations (see Appendix C for examples). An accurate way to gauge this for a new hosting provider is to look through the existing tickets of current customers. The most professional providers will always provide feedback of the steps they are following. Process execution should be visible from reviewing past incidents, to gauge if BI are trustworthy and perform the steps they say in practice[4].

Thirdly - we consider their resilience to attack. This is particularly important in gauging our trust property. Consider that a company states a guarantee for 99.9% uptime (e.g. http://support.hostgator.com/articles/pre-sales-questions/uptime-guarantee). It is important for customers to be pro-active in monitoring their websites independently of the hosting company (using third party monitoring services, such as http://pingdom.com), because from experience there is no guarantee that the provider will notify the customer when they are under attack. FI should check to see if BI's Incident Management strategy is transparent, and whether they publish their breaches transparently (e.g. http://forums.hostgator.com/forget-99-9-uptime-guarantee-resolved-t25642.html, Forget about 99.9% uptime guarantee!, 2008: a customer found his guarantee did not cover Apache webserver faults). A trust metric (from a trust assessment [6]) helps to gauge different vendors, and those with higher ratings will be suitable for finance (CMS 7.1).

Scalability is about enabling the virtual infrastructure to scale resources up and down based on demand and, simultaneously, to preserve security and privacy requirements.

To take an earlier example, FI will require BI's assurance that Clouds running PaaS will scale up (horizontally or vertically - CMS 4.2) during peak hours to prevent downtime (and even during exceptional circumstances - such as public holidays), and scale down automatically in order to protect FI's usage costs (something that only Cloud services can offer). This introduces new metrics for FI to consider: the Mean Time to Scale Up, and the Mean Time to Scale Down (CMS 4.4). As well as these Scalability statistics, Failure statistics (when scaling fails) give a genuine representation. The existence of all these metrics show that BI have considered these worst-case scenarios, and do not provide any misguiding information about realworld Cloud performance (thus providing assurance to the customer).

Availability the relative time a service provides its intended functions. High levels of availability are a result of excellent architecture, which considers well crafted procedures, redundant services, and high service reliability: that is, resilient design.

The availability incorporates the resilience property, and also considers the distribution of services and load via a scheduling algorithm. The quality of this algorithm is particularly valuable in reassuring BI. The algorithm should consider load balancing (hence performance), and also reaction to a resource being down (hence MTTD/I/R). Additional metrics of Mean Time to Failure (MTTF) and Mean Time Between Failure

[4] ISO 9001 Quality management Systems & ISO/IEC 27001 Information Security Management accreditation from the BSI is a popular way to gauge this, and is common for hosting and backup providers that offer critical services. Amazon EC2 openly publishes its accreditations; these are listed in Appendix A.
Appendix C that supplements this chapter illustrates the many assurance frameworks and assessments available to guage third party services.

(MTBF) provide historical data on the company's past incidents. If BI have a lower rate of failure than a competing company (or FI itself), then migration is a good move.

Security and privacy by design Establishing trustworthiness in such services and the ability to quantify them are key contributors to assessing the operational trust of Clouds.

Trustworthiness means the service performs its job as expected...security and privacy need to be integrated from within rather than to be an added option. Key proofs that FI may request are the isolation mechanisms between virtual machines (stated in the Amazon EC2 whitepaper), and the protection of integrity and confidentiality when a machine is being scaled or replicated. When scaling down, data should be non-recoverable. Also, the communication channels should be secured during such load distribution. BI can provide details of protocol encryption standards for assurance.

These descriptions are my summary and comment to a much larger resource of information: see CMS chapter 4 for fuller descriptions.

Operational trust relies on 3 factors which we have discussed above (slide 145): human factors (*are breaches revealed?*), documentation (are processes and policies well documented and followed: *is there historical evidence to verify?*) and the automation of management services (scaling, healing and accurate logging e.g. for monitoring or intrusion detection purposes). We have also discussed that featuring these properties and trust measurement metrics in the SLA, including transparent historical records and incident management processes & accounts enable FI to establish trust. These cover slide 143's techniques of establishing trust with an unknown entity: direct interaction, trust negotiation, reputation, and trust recommendation & propagation (elaborated from book sections 4.1 & 8.1).

c.3 Trusting the SLA: real world examples

We've deemed the terms of the SLA as our primary mechanism for outlining assurances and guarantees. To quote our slides that deal with trust establishment (169+).."Users have very limited control over the service deployment, have no control over the exact location of the provided services, and have no option but to trust Cloud providers to uphold the guarantees provided in the SLA." Specifically, FI will have concerns about data confidentiality and the location of data storage (for financial institution legality reasons). Therefore, we are looking at guarantees from BI present within their terms and conditions. Let's look at an existing Cloud provider to illustrate that how this is possible.

If we look at Rackspace's Cloud control panel [Appendix E], we see that when our user creates a virtual machine instance they also have the option of choosing the region. Regions are partitioned by country, and therefore we have our choice of where our data is located (a Cloud farm in a particular region). The instance can be mirrored by the user to different countries, so the user remains in control. It also reassures us that even if farms distribute the data over many resources (i.e. for storage), the resources will be of close proximity (still in the same region), so we do not suffer performance issues.

We mentioned earlier that it is also the responsibility of the customer to monitor the sites independently, in case the provider is not transparent about its breaches. Similarly, independent monitoring helps with billing disputes, although we at FI should ensure that BI has a trustworthy management data panel[5]. It is importance to discuss these properties in a business model context - terms and conditions and a guaranteed SLA are a business-class way of providing these assurances. These lead us to the importance of provenance and logging in our next question.

c.4 Privacy Policy

The protection, verification and validation of management data is crucial to preventing insider attack. A nominated Cloud provider's Privacy Policy must inherit the terms of FI's Privacy Policy. If we look at existing Privacy Policies[6] we see that these are the locations where terms for data retention and particularly,

[5] "Cloud providers would need to provide users with trustworthy tools which help them to transparently assess the trustworthiness of Clouds." Example: Rackspace Monitoring panel, Appendix E
"Cloud users do not have control over such mechanisms, and neither can they access log and audit records. Users have no option but to trust Cloud providers." Exercise 6. We discuss this in our next answer, regarding provenance.

[6] http://www.barclays.co.uk/ImportantInformation/Privacypolicy/P1242557966945, Privacy Policy of Barclays Bank Plc

precautions against insider abuse are stated. In Deutsche Bank's Privacy Policy[7] for example, point 7 (Management of Personal Information) states that DB: "has implemented appropriate measures to protect against inappropriate access" & "has implemented appropriate security measures such as protection from unauthorized access, computer viruses, etc. in order to protect Personal Information from loss, damage, falsification, leakage, etc.". Particularly significant is the statement "DeAMJ will oblige the outsourced vendors to manage the handling of Personal Information in the same manner." - and this is precisely the obligation we expect from BI on behalf of FI. Just as a client of FI expects FI's Privacy Policy agreement to be maintained under law, so too does FI delegate their terms to their outsourced party BI. Point 12 of Deutsche Bank's Privacy Policy (which FI may emulate) lists a statement regarding "Compliance with Laws, Improvements and Enhancements" (which it no doubt inherited from the Financial Services Authority, http://www.fca.org.uk/, who publish reports on the value of "Transparency" in finance and "Insider Dealings" (both May 2013)). If a breach occurs, the client may expect compensation from FI, but BI having breached their Privacy Policy will first restitute FI.

c.5 Techniques for establishing trust at hardware level

There is more to establishing trust than defining operational management properties and policies. FI can take a technical look at the infrastructure that BI provide (provided it has the expertise for such analysis). Our slides cover this in the second half of the trust in Clouds section (slides 153 - 180).

Let's quickly discuss use of TPM to provide assurance of security.

c.5.1 Hardware level assurance (with TPM and attestation)

We can use a TPM[8] to protect storage devices, which will verify integrity when scaling or duplicating. Using TPMs, FI and BI can establish and prove a chain of trust on their Cloud devices (from hardware level to the loaded volume), giving assurance that BI's Cloud infrastructure provides privacy and security within the confines of the law. This may involve the TPMs using a minimum strength of encryption to secure communicating volumes and channels[9]. This allows security to be remotely tested (CMS 8.4: Device properties), and could even utilize FI's public keys to give them assurance (i.e. to encrypt the data). Platform attestation will assure that FI (requestor) and BI (verifier) can mutually authenticate eachother (see slide 138, CMS 8.7.3: Adding devices to a domain utilizing TPMs, Authentication algorithms 8.6 & 8.7). It is particularly important due to Cloud dynamism that the chain of trust is revaluated adequately (CMS 7.3) as the Cloud scales. That is, that FI can verify their level of trust will be maintained without risk (during daily dynamic resource usage) as a result of visibly secure design.

At the end of of Appendix C there are examples of Hardware Level Assurance, including Amazon's new CloudHSM Security as a Service, and RSA's secureID TPM.

c.5.2 A Trust Framework

Our book tells us that there are numerous ways to establish trust between unknown entities (CMS chapter 8 or slide 143): in our case, FI and BI. These ways are: direct interaction, trust negotiation, reputation, and trust recommendation and propagation (CMS 4.1).

We have spoken about trust based on properties (trust negotiation). Chapter 8 offers us a trust framework, which is the "provision of a secure and trustworthy environment which assures users that Cloud providers continually enforce their requirements, do not interfere with their application data, and move the control of users' application data from the hands of Cloud providers to the users."(CMS 8.1). This applies not just to IaaS, but is adaptable to PaaS, and possibly SaaS as well (depending on how much data ownership the SaaS provider claims in their terms).

We began our answer by reviewing the pre-outsourcing steps. We have chosen the application we wish to outsource, and our deployment type. We also discussed what to include in our SLA.

[7] https://japan.db.com/en/content/privacy_policies_damj.html, Privacy Policy of Deutsche Bank Plc

[8] "A TPM security device is a tamper resistant security device that binds to a storage platform or virtual machine. Using security keys, once can verify the volume with trusted parties." CMS 8.4

[9] "OpenStack uses this security by design, and the use of security groups for filtering traffic", CMS 11.2.2

"After the organization decides on the applications to be outsourced, it defines the application requirements which includes: technical requirements, service level agreement and usercentric security and privacy requirements."

Since we mentioned earlier that a Cloud customer (FI) is dependent on BI upholding the SLA, they ideally want a tool 'enabling them to assess that the Cloud keeps meeting their requirements'. This is where our Trust Framework helps. It consists of 2 levels:

Level 1: Importantly it allows FI to protect their outsourced resources to the same standards of their internal protection policies. It requires secure, transparent protection measures at 3 phases: a) inside FI's organization b) at BI's Cloud c) for all communication between internal (a) and external (b) resources.

Level 2: Allow organizations to attest the Cloud provider's trustworthiness for managing the organization's outsourced resources (*which* if you think about it, really re-phrases the heart of our question). Here, we depend upon our Cloud provider being able to establish a chain of trust (between the organization and the Cloud infrastructural resources - that is a) a chain of trust between the organization and the VCC, and b) a chain of trust between the VCC and the Cloud's infrastructural resources. Our two chains (a, b) are depicted in Figure 8.1: Protection levels in the proposed framework, CMS p.110.

In our model of communication between the organization and Cloud provider, the VCC acts as a point of interface (a proxy) between the organization and BI's physical infrastructure - and is consequently also a point of attack. Both BI and FI therefore need to assess the trustworthiness of this proxy.

Establishing a chain of trust at a) for level 1: requires the organization to attest to the trustworthiness of VCC management agents to manage the organization resources. This is based on organization and user properties.

Establishing a chain of trust at b) for level 2: requires the provision of a trustworthy Cloud's virtual resource management using 1) VCCs and VMMs that attest to eachother the execution environment 2) the TPM which we laid out eariler, for it is a component in our framework.

c.6 Audit results

Security consultants are required by hosting companies to perform penetration testing. Evidence of published results from consultants can be used by FI to evaluate BI's trust rating. The blogs (http://www.sans.org/cloud) and (http://pen-testing.sans.org/blog/2012/07/05/pen-testing-in-the-cloud) give background information on how hosting providers can achieve PCI compliance[10] . As http://blogs.cisco.com/security/penetration-testing-in-the-cloud/ advises, FI need to be asking questions such as: "What does my contract and SLA state about penetration testing?" Does the CSP (Cloud Service Provider) already have a team of penetration testers? Is this enough to meet your security requirements or compliance objectives?" It offers current and relevant questions. The take home message, as always, is that financial and medical institutions really should not be using the public Cloud (only private and community) because they offer less assurances. It is wiser that FI have decided to outsource only one application to BI as PaaS. Another law that BI should comply with is The Cloud Compliance act of 2012[11], which aims to "improve the enforcement of criminal and civil law with respect to Cloud computing" (with particular attention to the prevention of unauthorized access). FI could use such legal statutes to regain compensation from BI (who are now subcontracted to take on the management risks - transitive trust).

[10] PCI DSS Cloud Computing Guidelines, PC Secuirty Standards Council, February 2013, https://www.pcisecuritystandards.org/security_standards/documents.php
"In our experience, PCI compliance is often expensive, difficult, time-consuming, and simply cannot be successfully tackled as a one-off project", Platform as a Service and PCI, Engineyard Cloud, http://pages.engineyard.com/rs/engineyard/images/PCIwhitepaper.pdf

[11] http://beta.congress.gov/bill/112th/senate-bill/3569/text
However, at present this Bill is controversial, as discussed by Forbes (http://www.forbes.com/sites/ericgoldman/2012/10/02/the-proposed-cloud-computing-act-of-2012-and-how-internet-regulation-can-go-awry/).

c.7 Summary of our assurance methods

We have now illustrated that assurance relies the organization trusting the Cloud provider. The trust comes from the infrastructure upwards - TPMs and keypair authentication are used for verifying that the requesting organization is retrieving data from the providers allocated hardware resources. The organization also uses the TPM for securing its hardware when scaling horizontally or vertically in accordance with the TCG design principles [8].

Secondly, we establish a trust framework to secure the VCC proxy between the organization and the provider. These two levels of configuration comprehension are necessary for a financial institution where security levels are mandated by law. And lastly, we have the SLA & Privacy Policy, an agreement between the organization and provider which ensures a statement and possible guarantee of these terms[12].

So from inspection of BI's TPM configuration at a technical hardware level (including an assurance of secure transmission with algorithms 8.6 and 8.7 in CMS p.120, or service level encryption assurances as in Amazon's whitepaper in Appendix C) right through to top level inspection of business policies and processes (combined with inspection of historical records for incident management, and customer references) FI have the ability to ascertain an assurance profile of BI's operational, data & application management abilities, to compare with other providers (including itself).

There is a lot of wisdom and good process in this book - it was my challenge to constrain it within my desired page objective! Above was the best advice that I have found for providing assurance.

[12] Appendix B gave an example of the risks of losing data control or ownership with a SaaS solution, where SaaS provider Coghead would delete all data within 2 days unless the client provided a written request.
"*The Good, Bad, and the Ugly of SaaS Terms of Service, Licenses, and Contracts*", http://peterlaird.blogspot.com/2008/06/good-bad-and-ugly-of-saas-terms-of.html

d Introduction

Automated management services are fundamental to the Cloud, and the aspect that will seperate it from current 'dedicated server' infrastructure. Auto-scaling and auto-healing will be the key to saving time in incident managment and prevention; expenditure on overinflated dedicated servers (that potentially require upgrades and migration as the service grows); automatic recovery from that single point of failure; and ultimately a reduction in the cost of human employment expenditure (which goes to the provider and customer), as well as green expenditure (no dedicated customer servers for lightweight applications).

But these auto-management features are in their infancy, and their dynamic complexity implicates efforts at prevenance.
Developments in provenence techniques and services will drive the acceptance (and trust) in self management environments.

We split this answer into 2 parts. Each subsection of each part will conclude with a discussion of the relationship to the other part.

d.1 Self-managed services

First let us discuss why self-management is a very attractive and fundamental feature of the future dynamic Cloud; but how its unguided design could hamper provenance.

The self managed Cloud consists of many various add-on services. Depending on the application type and consumer, some services may be less valuable. For example, a simple conference advertising website may not require a great investment in scalability as a service – especially if it only expects 500 attendees – but it will require perpetual global availability and resilience services. On the other hand, if we consider a company such as FI with a large consumer base, availability, scalability, reliability, adaptability, and system architect all become necessary services. We appreciate that such an application will cost us more to host, but in reward of more assured uptime, resilience at peak times and under attack, and greater assurred security and privacy by design.

For illustration, I will succinctly overview the interdependency of our available services; however, note they are here for a quick display of appreciation for a formal answer. The aim of the answer is to provide adequate discussion against our question, and not to simply regurgitate the book. For a full description, please refer to CMS chapter 5, particularly sections 5.2 and 5.4.

d.1.1 Quick descriptions

Adaptability as a virtual service concerned about adapting virtual resources, which are part of the virtual layer, to changes and incidents. If the Risk Management Application is at a time of peak access (e.g. before a holiday), it will dynamically find the resources.
Fig. 5.1 (CMS p.67) shows how incident responses to system failure or demand triggers the ADaaVS.

Adaptability as an Application Service ability to provide timely and efficient support of applications to system changes and events. Consider if the Risk Management Application inflates resource usage greatly between simply browsing the front-end, to logging in and performing user activity. Adaptability may handle this on a per-usage basis.
Figure 5.7 (CMS p.73) shows how changes from the application layer directly relate to user properties (e.g. security and privacy), and how ADaaAS cascades responses from other services (or is triggered by other services, such as scalability).

Resilience as a Virtual Service resembles system administrators who deploy the outcome of the SAaaVS at the virtual layer. The RSaaVS works with other resources and management tools to deploy the resilient design. It is also in charge of communicating failures of a resource to other services. E.g. RSaaVS would trigger AVaaVS to divert traffic to alternative routes, and ADaaVS to take further actions. Should maintain security and privacy by design.
Figure 5.2 (CMS p.69) shows how the system architect (responding to changes in user requirements or fail-

ure) triggers a response from RSaaVS (e.g. moving the VM to other servers). It must maintain security and privacy by design during this action.

Resilience as an Application Service ability of a system to maintain an application's features (e.g. serviceability and security) despite a number of component failures. High resilience is achievable by providing high resilience at the virtual layer and establishing well planned failover procedures (+ high redundancy). Tries to survive inevitable failures rather than reduce them.
ADaaAS is notified of a single point of failure event, and then it manages the event and coordinates with the RSaaAS. The RSaaAS in turn performs actions based on the event (may be cascaded).
Figure 5.8 (CMS p.73) illustrates application responses (e.g. restart or re-route) to event triggers (application or communication failure), followed by cascaded actions to services.

Scalability as a Virtual Service supports the elasticity feature of the Cloud. Actions include horizontal scalability by replicating a VM's resources and/or vertical scalability by expanding a VM's resources. Actions should always validate user properties before scaling resources and should maintain security and privacy by design (protects VM integrity and confidentiality on replication, shreds data from released resources, allocation of new virtual resources should be based on user properties). The SCaaVS should notify the Availability as a Virtual Service (AVaaVS) and Reliability as a Virtual Service (RLaaVS) when scaling up/down. FI will require this for their large consumer base.

Scalability as an Application Service providing an application with the capabilities to quickly and efficiently adapt to the addition and removal of virtual resources (e.g. on peak). ADaaVS, upon detecting a need for adding resources triggers the SCaaVS. SCaaVS then triggers ADaaAS which finally triggers SCaaAS (figures 5.9 & 5.10 in CMS p.74).

Availability as a Virtual Service maintains communication channels of available virtual services with resources at the application layer; distributes application layer requests evenly across available redundant virtual resources. The higher the resilience of a system the higher the availability and reliability. If a channel is marked unusable by the RSaaVS, the AVaaVS would immediately stop diverting traffic to that channel, and re-divert traffic to other active channels until the ADaaVS addresses the problem.

Availability as an Application Service is in charge of distributing requests coming to an application across all redundant application resources based on their current load. represents the relative time a service provides its intended functions, and high levels are the result of excellent resilient design (at a cost). Figure 5.10 (CMS p.75) provides examples of events and changes triggering the AVaaAS. The events are triggered by RSaaAS while the changes are triggered by SCaaAS. The AVaaAS in turn performs actions based on the events and changes.

System Architect as a Virtual Service resembles enterprise architect professionals. It is an indicator of resilient design and it always considers user requirements and infrastructure properties, and should maintain user security and privacy requirements by design.
E.g. if a physical domain could not serve a virtual domain for any reason (e.g. network failure), the ADaaVS would then check with the SAaaVS on where to relocate the virtual resources, without compromising user properties.
Figure 5.2 referenced earlier shows how Resilience as a Virtual Service is deployed by SAaaVS in response to a change in user requirements, or network / server failure. It takes into account infrastructure properties and policies.

d.1.2 Interdependency

These descriptions have deliberately emphasised the behaviour of services triggering or being triggered by other services. This is to show the extent of their interdependence. A review of these interdependencies, with accommodating diagrams, is well covered by CMS subsections 5.3 Virtual services interdependency (see Figure 5.6: Virtual layer self-managed services interdependency, p.71) and 5.5 Application services interdependency.

d.1.3 The result of dynamicity and interdependence: complexity in logging

> What is the implication of multiple independent service functions triggering each other (cascading) on a scalable resource?

We have established that the Cloud creates a complex dynamic environment.
This is because resources are regularly being created and destroyed as a consequence of elastic resources.
Furthermore, we have an intertwined set of services that trigger each other in a cascading nature.

Let us imagine if an instance of a virtual machine at a datacentre was compromised, and that virtual machine (belonging to a customer, but being controlled by an attacker) was used to compromise a third-party website. Then, as a consequence of operational management (scalability) that instance (in an active-passive setup) was destroyed. When the forensics teams try to locate the source, if the solution has been securely designed, surely tracing back to a destroyed resource will be impossible?

We will talk in just a moment about the solution (trust establishment and a trustworthy, fully standardized and centralized logging system), but before we do, let's consider what provenance is, and how it relates to our complex service ecosystem.

d.2 The importance of provenance

d.2.1 How it is afflicted by dynamicity and interdependence

> *"Logging, auditing and historical data are of tremendous importance for establishing trust in Clouds."* CMS 10.1, Provenance in Clouds

...and they are the key to the forensics efforts in the attack scenario described above. It is also the key to other necessities: monitoring, error resolution and of course billing the customer correctly.

All Clouds and their services will generate volumes of log data. Especially for our financial institution, we will have obligations to keep this data for a set number of years (Sarbanes-Oxley Act of 2002 mandates financial record retention for 7 years[13]. So it's likely a sensible Cloud provider will use its cheapest, largest disk volumes to archive this data[14].

We note that logs and provenance are not the same thing; whereas logs provide a sequential history of predefined actions (and hence, predefined predictable output within some set of fixed syntax and output codes), provenance refers to the history of origins. Logs may refer to a particular application, but provenance goes beyond an application to include people and machines. That said, provenance will almost certainly utilize the results of logging (as a source of provenance), and therefore any complications from intertwined, complex and unstandardized services (as a result of self-managed services with no human responsible) will implicate provenance. Logs are useful for documenting operational management issues (Exercise 6), but it does not evaluate human elements, such as managers responsible or insiders.

Logs are the data of operational management services, but provenance data for example, will be more presentable to auditors than mere log records. Provenance data provides assurances of trust to auditors, stakeholders, prospective customers, and potentially legal inquisitors. Since provenance is provided by linking together recorded log data from self-managed services (on multiple resources) to provide a complete history of an event or result, you can see that the relationship of self-managed services providing trustworthy, comprehensive and retained logs is critical to providing provenance assurances to our interested parties.

d.2.2 Additional: A trustworthy solution

It is quite simple to state this relationship. But let's also consider how we can strengthen the relationship between self-managed services and provenance for future development. If FI inquire from BI about these factors, it will have more reason to choose BI as a trustworthy provider. All potential customers should have trustworthiness and forensics capability in mind when choosing a Cloud provider.

We know that establishing trust in the Cloud requires:

[13] Dispelling Log Data Retention Myths, http://esj.com/articles/2004/05/12/dispelling-log-data-retention-myths.aspx
[14] IBM, Archiving reduces risk & costs for financial sector, http://www.ibm.com/midmarket/us/en/article_Industries1_1209.html

1. support infrastructures with trustworthy mechanisms and tools to help Cloud providers automate the process of managing, maintaining, and securing their systems;

2. developed methods to help Cloud users and providers establish trust in the operational management of the infrastructure.

How do we reach this solution?

In regard to *1.* we spoke about techniques for establishing trust quite extensively in Solution c). This included discussion about establishing trust at infrastructure level through the use of TPMs. we spoke about establishing chains of trust across distributed resources, such that self-managed services could securely exchange data, and remote attestation. We are going to discuss briefly here more about *2.* - the challenge of future provenance systems to develop trustworthy logging systems (or supply Logging as a Service (LaaS)[15]) for provenance.

Standardization -

Let's say that we have many essentially independent services cascading with each other. In order to make sense of it all, we want a standardized logging syntax. One of the challenges of the dynamic Cloud model is that our various properties and services are trying to collaborate, but may not be generating their logs in a standardized syntax. As such, creating a single interface to sift and organize these logs is a challenge. CMS section 10.1.2 describes two useful methods - to have an established process for generating log records, and also semantics that describe their meaning for an external auditor or tool. Papers establish that there is as of yet no industrially standard way for healthcare and financial systems to store their logs (A Survey of Data Provenance Techniques [8], Provenance in Agent-mediated Healthcare Systems [9]), but this author suggests that efforts are being made in this direction (IPAPI: Designing an Improved Provenance API [10], Towards a Universal Data Provenance Framework using Dynamic Instrumentation [11]), and a good approach is a logging system with an API and standardized, perhaps XML tagged logs so that tool creation is trivial. The process for generating logs could be one of the processes FI evaluate when they consider BI as a provider (as proposed in answer c). An API is one of the ways of documenting the logging syntax.

Meta data -

Identifying meta data with attributes such as application, resource and customer will assist in creating provenance tools to link associated resources to a particular incident.

The paper "Provenance from Log Files: a BigData Problem" [12] also proposes that there be a logging hierarchy: "Logging frameworks like log4j, log4net, nlog, python logger support multiple logging levels. These levels are used to rank the importance of log messages and control the amount of information to be dumped into log files". Along with historical origin, marking the importance of a log record may trigger automated incident prevention, healing and scaling events (such as the Scalability as a Virtual Service). All the papers [8-12] and CMS chapter 10.3 Log records management and requirements cite meta data as being fundamental to provenance.

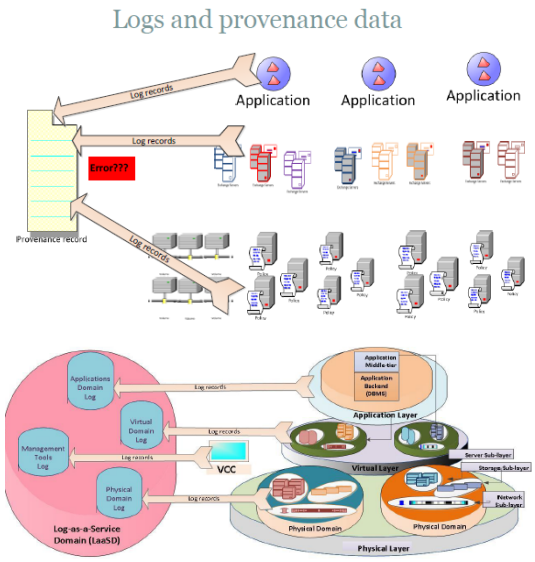
Centralization -

Ultimately we want to link together these distributed logs.

See the following 2 diagrams. To quote slide 202, our aim is to:

"Store log records in a structured, highly available, and centralized repository. This enables provenance tools to easily and quickly find log records, query them, and bind related events together.
A possible solution for some of the challenges (of) provenance record management is to Move log records from their originating distributed processes to a trustworthy centralized repository. Log records should be easily queried using standard mechanisms."

[15] Loggly.com: "The world's most popular cloud-based log management service". Parses log records from independent Cloud resources for a centralized web panel display.
UnifiedLogging.com: "provides Logging as a Service (LaaS)..Whether you are using Microsoft Windows Azure, Amazon AWS, Rackspace Cloud or another infrastructure. Define notification triggers". Also centralizes log data from independent Cloud platforms, allowing custom alerts.



Course lecture slides, pp.188 & 202

Footnote 15 listed third-party tools that achieve centralized logging. Some hosting providers have already released standalone Cloud monitoring agents on their platforms (Rackspace, May 2013 - see Appendix E for a screenshot of their beta Cloud monitoring service - subscription required after July 2013).

Security of design -

The LaaS should be well protected by security measures, and its correctness must be verified.
We need to be able to trust the results presented by the logging system (i.e. that incidents are logged correctly). We also need an assurance that the logging mechanism (which may be sent to an archiving volume at a separate data centre) is securely transmitted (through keypair authentication between data centres). Lastly, we must be confident that the logging storage platform cannot be tampered by unauthorized access (insiders looking to cover their tracks or mislead the forensics efforts following an incident). The logs are taken as given; and therefore ensuring their integrity is critical.

How the solution addresses our threats and challenges

If we look back to our solution tables from questions a) and b), we note that this centralized, tagged and standardized provenance solution assists the challenges that arise from migrating to Cloud infrastructure.

One of the main issues with the public Cloud was data isolation, and the threat of competing companies acting as insiders on a shared platform. Reading Amazon's whitepaper of Appendix A, we see that Amazon, despite providing the World's most popular public Cloud, makes assurances on ***trustworthy***, ***key managed***, ***isolated*** user environments. Establishing such accredited and protected platforms dissolves our concerns about the private Cloud being more secure than the public Cloud. We know that Amazon provides a hugely public Cloud, but since the SLA assures the solution as being trustworthy, it doesn't matter how many competitors are using the product; it is still trustworthy and protected - probably more accredited than FI's private Cloud.

Let's consider if a self-managed resource makes what the customer suspects to be a billing error. When the jobs of systems' administrators become more automated, they will also have to become more transparent to the client in order to maintain trust. Most customers that avoid moving to the Cloud have a fear that due to some resource glitch or application memory leakage, their monthly bill will exceed their expectations. A centralized monitoring solution will hopefully allay these fears, providing a standardized, itemized bill that the user can comprehend, and hopefully set upper spending caps or alerts on.

The second great concern after billing errors is the fear that automatic scaling will permanently destroy a data resource (due to fault in the SCaaVS). Again, trustworthy management and assurance that insider

viruses cannot affect user data is the key to assurance and adoption. Amazon for example, states that user accounts are "redundantly stored in multiple physical locations as part of normal operation of those services and at no additional charge" [13], which encourages customer confidence that if self-managed service errors do occur, the data will be retrievable. It is important to remember that any concerns about data destruction also apply to the existing domain of dedicated managed servers; but the advantage of the Cloud is that it mitigates the notion of common 'server breakdown' as being the reason for data loss.

Summary

The foremost issue we dealt with in question a) was isolating the data from competitors on public Cloud deployment types. A ***truly trustworthy solution*** helps to provide FI with the savings of moving chosen applications to BI's public Cloud, with assurances of secure, isolated and accredited environments at no additional in-house certification costs.

The foremost issue we dealt with in question b) was having access to a more competent management team provided by BI on SaaS, with a mitigated threat of insiders. A ***provenance accredited solution*** assures FI that in the event of insider breach (which may still occur with BI), a successful inquiry can be held to trace and remedy the root cause.

Additional final words

As a Systems' Administrator and product solutions developer that, over the last 2 years, has gradually been forced towards the Cloud by our third parties (Adobe Creative Cloud, Google Gmail & Drive, IBM[16]*, Microsoft Windows Server solutions, and our PaaS web-hosting providers Engineyard and Rackspace), I have found these exercises useful. They have broadened my understanding and appreciation in the benefits of the Cloud. They will also allow me to tailor the most cost efficient and appropriate Deployment types and Service types for our various products. Most importantly, they have helped me to reflect upon the assurances I should seek from Cloud providers, and how I can set up trusted environments that actually improve upon the security policies that we previously implemented with our dedicated servers.*

[16] "The race to buy up providers of business services over the internet intensified on Tuesday with two industry giants making acquisitions worth a combined $4.5bn, underlining how so-called cloud computing is reshaping the information technology industry...The acquisitions by IBM and Salesforce are the latest signs of a big strategic shift in the technology sector as businesses increasingly buy software and services over the internet from remote locations that were formerly run on in-house computers. Salesforce was advised by Bank of America. JPMorgan advised ExactTarget. SoftLayer was advised by Credit Suisse and Morgan Stanley.", *IBM and Salesforce strike cloud computing deals. Financial Times (4th June 2013)*

References

[1] Abbadi I. M. (2013), Clouds Management & Security (draft)

[2] Abbadi I. M. (2013), Cloud Security (CLS) Course Slides, University of Oxford

[3] Abbadi I. M. (2013), Cloud Security (CLS) Course Exercises: model answers 1-6, University of Oxford

[4] Jeffery K., Neidecker-Lutz B. (2010) The Future of Cloud Computing, European Commission.
Available from: http://cordis.europa.eu/fp7/ict/ssai/docs/cloud-report-final.pdf [accessed 1st June 2013]

[5] Microsoft Corporation (2013), Microsoft business security solutions: Relentless on security [online].
Available from: http://office.microsoft.com/en-us/business/microsoft-business-security-solutions-FX103045813.aspx [accessed 1st June 2013]

[6] Abbadi I. M., Martin A. (2011), Trust in the Cloud, Information Security Technical Report, University of Oxford.
Available from: http://www.sciencedirect.com/science/article/pii/S1363412711000513 (Athens) [accessed 1st June 2013]

[7] Trusted Computing Group (2011) Design Principles, Specification version 1.2 Revision 116.
Available from: http://www.trustedcomputinggroup.org/files/static_page_files/72C26AB5-1A4B-B294-D002BC0B8C062FF6/TPM%20Main-Part%201%20Design%20Principles_v1.2_rev116_01032011.pdf [accessed 1st June 2013]

[8] Gannon D., Plale B., Simmhan Y. L. (2005) A Survey of Data Provenance Techniques, Indiana University Computer Science Department.
Available from: ftp://ftp.cs.indiana.edu/pub/techreports/TR618.pdf [accessed 1st June 2013]

[9] Moreau L. et al. (2006) Provenance in Agent-mediated Healthcare Systems, University of Southampton ECS, Universitat Politècnica de Catalunya, Computer and Automation Research Institute.
Available from: http://www.gridprovenance.org/publications/ [accessed 1st June 2013]

[10] Hopper A. et al. (2013) IPAPI: Designing an Improved Provenance API, University of Cambridge Computing Laboratory.
Available from: https://www.usenix.org/system/files/conference/tapp13/tapp13-final4.pdf [accessed 1st June 2013]

[11] Gessiou E. et al. (2012), Towards a Universal Data Provenance Framework using Dynamic Instrumentation, Columbia University Department of Computer Science, Polytechnic Institute of NYU, Institute of Computer Science (Hellas).
Available from: http://www.cs.columbia.edu/~vpappas/papers/provenance.sec12.pdf [accessed 1st June 2013]

[12] Ghoshal D., Plale B. (2012) Provenance from Log Files: a 'BigData' Problem, Indiana University Computer Science Department.
Available from: http://www.edbt.org/Proceedings/2013-Genova/papers/workshops/a42-ghoshal.pdf [accessed 1st June 2013]

[13] Amazon (2013), Amazon Web Services: Overview of Security Processes [online].
Available from: http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf [accessed 1st June 2013]

[14] Amazon (2013), Amazon Web Services: Risk and Compliance [online].
Available from: http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf [accessed 1st June 2013]

[15] Engineyard (2013), Ten Advantages of Platform-as-a-Service [online].
Available from: http://pages.engineyard.com/rs/engineyard/images/Engine_Yard_Top_10_PaaS_Advantages.pdf [accessed 1st June 2013]

Appendices

Appendix A

External case study examples

A description of the motivations behind why FI will have chosen a private Cloud (to better utilize their existing infrastructure)
Capturing the Private Cloud: http://gcn.com/Articles/2009/07/13/Private-cloud-computing-for-government.aspx

A report on implementing realworld Cloud infrastructure security policies. *Amazon Web Services: Overview of Security Processes:* http://media.amazonwebservices.com/pdf/AWS_Security_Whitepaper.pdf

Excellent document listing the many accreditations FI should look for. *Amazon Web Services: Risk and Compliance:* http://media.amazonwebservices.com/AWS_Risk_and_Compliance_Whitepaper.pdf

Verifying Cloud compliance. Amazon EC2 may only offer IaaS, but its compliance policies are first class; possibly more accredited than FI's private Cloud. BI, specific to the financial domain, should draw its own document from this.

AWS is compliant with various certifications and third party attestations. These include:

•SAS70 Type II. This report includes detailed controls AWS operates along with an independent auditor opinion about the effective operation of those controls.

• PCI DSS Level 1. AWS has been independently validated to comply with t he PCI Data Security Standard as a shared host service provider. ISO 27001.AWS has achieved ISO 27001 certification of the Information Security Management System (ISMS) covering infrastructure, data centers, and services
•
FISMA. AWS enables government agency customers to achieve and sustain compliance with the Federal Information Security Management Act (FISMA). AWS has been awarded an approval to operate at the FISMA

It has also completed the control implementation and successfully passed the independent security testing and evaluation required to operate at the FISMA

Moderate level from government agencies. Additionally, customers have built healthcare applications compliant with HIPPA's Security and Privacy Rules on AWS.

The Amazon paper offers accreditations and processes upon the following topics, which FI can use as a template for evaluating BI's private Cloud. I have added **comments* below to chapters of interest:

Shared Responsibility Environment
* "*Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS."Users accept responsibility for setting up keys and ensuring security mechanisms"*

Control Environment
* *accreditations (excerpt above)*
Secure Design Principles
* *software development best practises*
Backup
* *all instances are backed up to redundant servers in case of scaling destruction*
Monitoring
* *instance monitoring*
Information and Communication
Employee Lifecycle
* *Enforces stringent staff background checks before employing (as does the banking industry)*
Physical Security
* *video surveillance, 2-tier authentication for access*
Environmental Safeguards
* *fire / water / temperature protection*
Configuration Management
* *Emergency, non-routine, and other configuration changes to existing AWS infrastructure are authorized, logged, tested, approved, and documented in accordance with industry norms*
Business Continuity Management
* *A popular phrase in hosting provider certification papers – Amazon defines availability, response, communication and review*
Fault Separation
* *provides customers the flexibility to place instances and store data within multiple geographic regions.*
Amazon Account Security
* *forces the user to create a private-public keypair upon set up*
Network Security
* *infrastructure incorporates automatic protection against DDoS, IP spoofing and port scanning attacks*

Appendix B

External case study examples

Our approach was to: 1. research our literary sources 2. evaluate them to our case study (verdicts) 3. tabulate the results.

To keep the answer academic (and maintain a good flow between concise answers), the verdicts were drawn from research literature alone. However, this is a very realworld problem, and I as a developer and administrator have also had to solve this issue (when migrating our Ruby on Rails application http://desaldata.com to hosting provider Engineyard as its performance was an issue). While we have left Engineyard Cloud for Hostgator dedicated servers (in our case, it was the performance of the site - not the number of clients, that has since been optimized through re-coding efforts, so the costs were unsubstantiated), we continue to use Cloud based provider Rackspace for our most popular flagship site globalwaterintel.com (which receives 30,000+ visitors a month). The latter is a site that requires scalability for high volumes of traffic, and a single dedicated server alone would struggle.

I would like to try to illustrate that the Verdicts I made hold true in the realworld.

I have researched fresh (2013) materials from Engineyard and Rackspace (both of whom provide exclusively Cloud based hosting architecture; and are great proponents and open source contributors in the field of Cloud adoption). I have referenced these quotes in the answer, and hope you will find them useful supplementary material here.

My desire was not to inflate the body of my answer into pages of marketing material, but collect real World examples from clients and hosting provider papers to support our arguments. Our book, CMS, similarly avoided quoting marketing material and kept things 'solely academic'. That is why I have created these optional appendices. They helped me to construct my verdicts.

Additional effort of IaaS:

We feature a comparison table (Ten Advantages of Platform-as-a-Service, p.5, Engineyard 2013, Bibliography: [15]) from proponent Cloud hosting provider Engineyard (IaaS vs. PaaS). Engineyard provide a customized PaaS solution on top of the Amazon EC2 IaaS.

Do-it-Yourself on EC2	Use Engine Yard PaaS
Initialize 1. Build app 2. Set up EC2 account 3. For each desired instance: a. a. Install/configure OS b. b. Install desired language version, runtime c. c. Install frameworks and other libraries/gems d. d. Install/configure application server e. e. Install/configure HTTP server f. f. Install/configure load balancer g. g. Install/configure other components (DB, cache) h. h. Debug integration of stack i. i. Install/configure application on stack 4. Get instances working together	**Initialize** 1. Build app 2. Set up Engine Yard account 3. Click several configuration choices 4. Click "Boot"
Update 1. Repeat items a-i above, per instance 2. Get instances working together	**Update** 1. Use Update Instances wizard
Scale 1. Do a-i above for new instances 2. Reconfigure application servers, load balancers, DB, etc. 3. Ensure consistent stacks 4. Get instances working together	**Scale** 1. Use Add Instances wizard

Appendix B

Above: A comparison of effort between IaaS and PaaS

In regard to effort, the table illustrates the set up process required by the customer for an EC2 IaaS vs. their customized PaaS solution. You can see from comparison of the two processes that a well developed user-interface for PaaS, or in our case SaaS, by a respected provider (whether it be Microsoft Azure for PaaS, or Engineyard PaaS, or Gmail SaaS), a higher level service solution offers us the benefit of less technical knowledge for set up (and hence, less risk of FI's systems administrators acting as insiders, or misconfiguring the environment).

Customer feedback

Clients of Engineyard are vocal about the benefits of having experts configure Cloud solutions for them, and four realworld quotations stand out that support the arguments we have made in b).

Reduced Effort

"The best thing about relying on Engine Yard for our deployments is that they are dedicated stack experts, so I can trust that they've selected battle-tested production configurations for Rails applications. Because of this, we've reduced the time we spend each week on system operations." *CTO of HealthLeap, a medical appointment booking website*

With Engine Yard, we can deploy our application in five minutes, and we know we're running on the best technology stack. If we were managing our own servers, we'd have to take resources away from development to invest in a dedicated IT/infrastructure engineer. Instead, we're able to focus on building new features." *Founder of Z2 Live, an online gaming site*

Benefit of additional expertise from outsourcing to specialists (security and intrusion mitigation)

we are a game studio, not an infrastructure company, so we were inexperienced when it came to configuring servers to scale based on changing traffic patterns. This is where Engine Yard really shines because scaling Rails applications is one of their specialties." *CEO, PlayMesh*

"Engine Yard automatically spreads your application across multiple availability zones, enhancing application resilience...As outlined above, when you build and run on a PaaS, you use technology that has been developed and refined in response to the needs of thousands of customers. But it's not just the technology that embodies that aggregated expertise. It's the people themselves. When you call Engine Yard Support, you speak to someone who has dealt with hundreds of problems in the same domain as yours." *Whitepaper body*

From personal experience, when we moved my company's site http://desaldata.com (upon which I was the developer and remain the system administrator) to the premium managed provider Engineyard, we largely did so because we were able to utilize the vast farm of human expertise from dedicated server specialists (to assist our in-house development and administration team that consisted of 2 people trying to figure out why the site was running slowly). It is common for hosting providers to recognize this; developers and administrators of established existing sites often upgrade to premium Cloud based hosts to tap the resource of scalable computation and shared administration experience. Rackspace.com for example, offer Advisory Services (http://www.rackspace.com/enterprise_hosting/advisory_services/) for companies moving to the Cloud.

We have emphasised repeatedly that we want FI to be able to benefit from the expertise provided by outsourcing to BI, as well as the potential to mitigate insider threats by choosing a more specialized set of software configuration admins with more established expertise in the domain.

The risks of losing data control or ownership with a SaaS solution

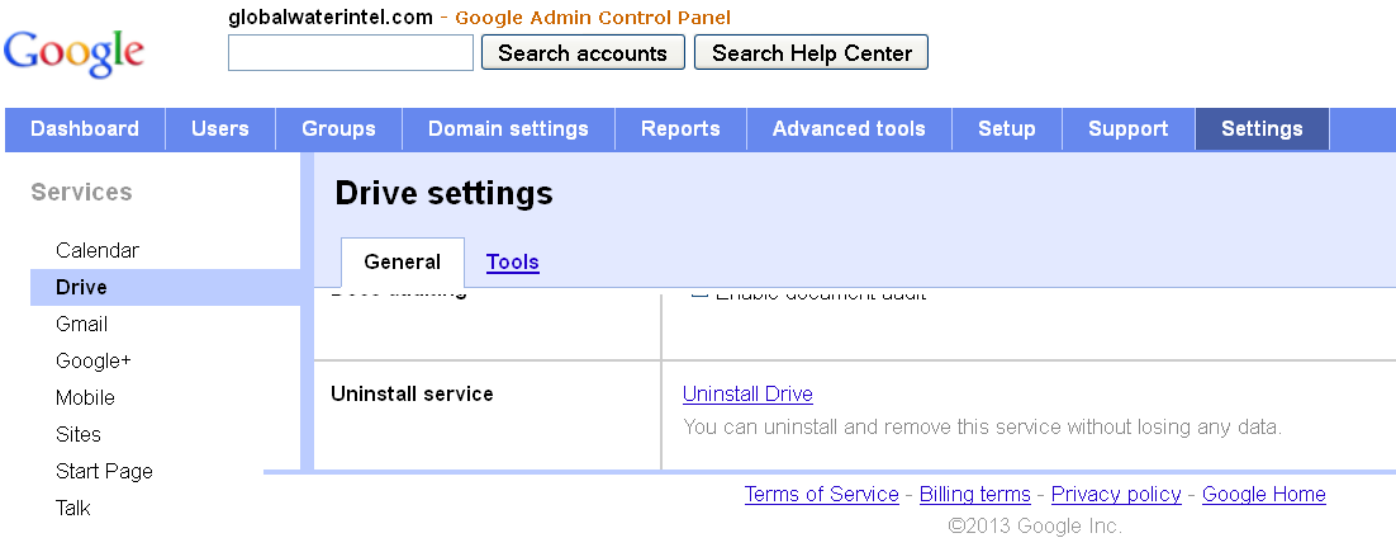
The Good, Bad, and the Ugly of SaaS Terms of Service, Licenses, and Contracts. Includes specific excerpts from user agreements dealing with the rights of users of Software as a Service who forfeit data control as a condition of using the site.

For example: "if Coghead terminates your account, you have just 2 days to send written notice to request your data. Otherwise they can permanently delete all of your data."

Appendix B

This exemplifies our point that we expect third parties to transitively comply with the terms FI has issued to its clients (and also, to legal authorities). If these change, the customers and regulatory officials will need to be informed. *For examples, see* http://peterlaird.blogspot.com/2008/06/good-bad-and-ugly-of-saas-terms-of.html

Fortunately looking at the Google Administrator panel for my own company, we see the following reassurance:



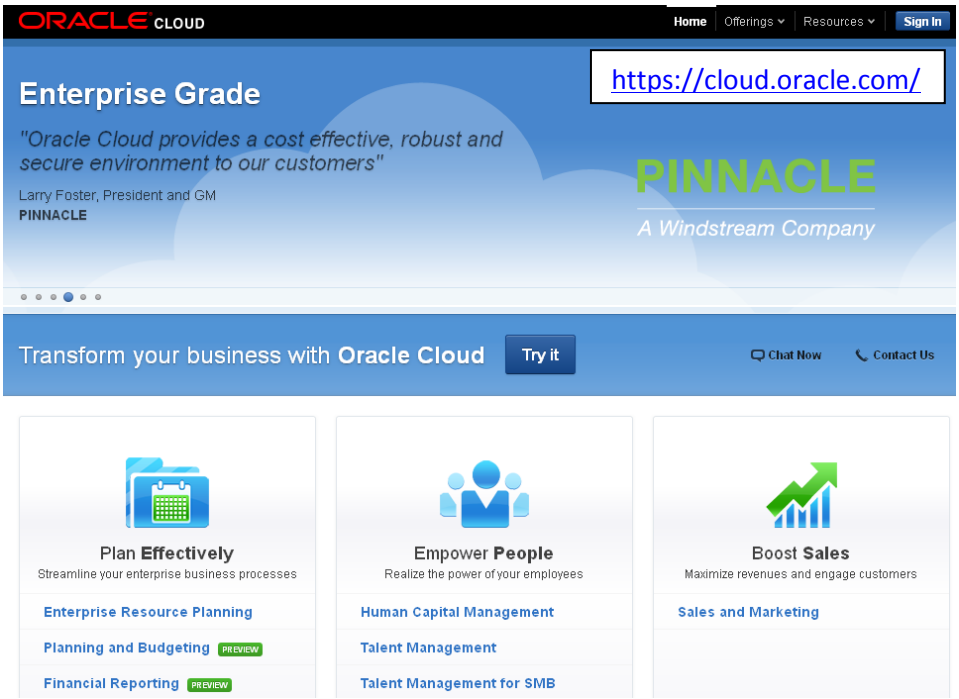
Reduced migration effort & Compatibility

Lastly, we turn to Oracle's case study. Oracle offer banking services on a range of service types.

"Oracle delivers the broadest selection of enterprise-grade cloud solutions, including software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS)."

http://www.oracle.com/us/industries/financial-services/banking/overview/index.html

Similar to BI, we find that Oracle (and also Adobe) have leveraged their vast server farms to offer customers savings on infrastructure, while also being able to incorporate banking software applications. These applications, being from one vendor, are i) designed to interoperate more seamlessly (the advantage of opting for BI's suite of programs – at a cost), and ii) designed to scale and harness the scalability and resilience of the Cloud architecture they are hosted on.



Appendix C

External case study examples

Assurance

Here are selected Cloud SLAs from the real world. Note the terms they define.

Microsoft Office 365

Assurance expectations for standard (non-financial) consumers

Office 365 asks users to move their data to online Cloud services; it specifically refers to reliability and security on its consumer level advertising page, since this is a very real concern. It is interesting to note the level of technical language now being used to assure customers of a common document presentation & spreadsheet suite.

Reliability: "Get peace of mind knowing your services are available with a guaranteed 99.9% uptime, financially backed service level agreement (SLA)."

Security : Your data is yours. We safeguard it and protect your privacy. The built-in security features available to all customers by default are: 24-hour monitored physical data centers; Logical isolation of data between tenants; Segregation of the internal datacenter network from the external network and encryption of data transmitted across the networks; Encryption of email data at rest using BitLocker 256-bit encryption and SSL/TLS encryption of data in transit ; Administrative access to Office365, controlled by a **role-based access control process**.

Applications built by following the Security Development Lifecycle. The Microsoft secure development lifecycle ensures that security and privacy are incorporated by design, from software development to service operation.

http://blogs.technet.com/b/perryclarke/archive/2012/05/16/managing-access-to-the-exchange-online-service.aspx

http://office.microsoft.com/en-us/business/microsoft-business-security-solutions-FX103045813.aspx

http://office.microsoft.com/en-us/business/office-365-small-business-small-business-software-FX103887194.aspx

Rackspace.com: http://www.rackspace.com/information/legal/cloud/sla
http://www.rackspace.co.uk/legal/cloud-sla-servers/

We have built the hosting industry's most aggressive Service Level Agreement (SLA) to cover the multiple components that keep your site up and running. Rackspace's SLA is a contract between you, the customer, and Rackspace. It defines the terms of our responsibility and the money back guaranty if our responsibilities are not met.

We guarantee that our data centre network will be available 100% of the time.. excluding scheduled maintenance.
We guarantee that data centre HVAC and power will be functioning 100% of the time... Infrastructure downtime exists when Cloud Servers downtime occurs as a result of power or heat problems.
We guarantee the functioning of all cloud server hosts including compute, storage, and hypervisor. If a cloud server host fails, we guarantee that restoration or repair will be complete within ***one hour of problem identification.***

So we see that while the original dedicated server SLA (http://www.rackspace.com/managed_hosting/support/servicelevels/managedsla/) claims 100% uptime and money back for **any** downtime, the new Cloud SLA allows a one hour restoration buffer for dynamic Cloud errors. The 1 hour restoration time is quite surprising for a premium host, and may be lifted as Cloud auto-healing and auto-scaling abilities mature.

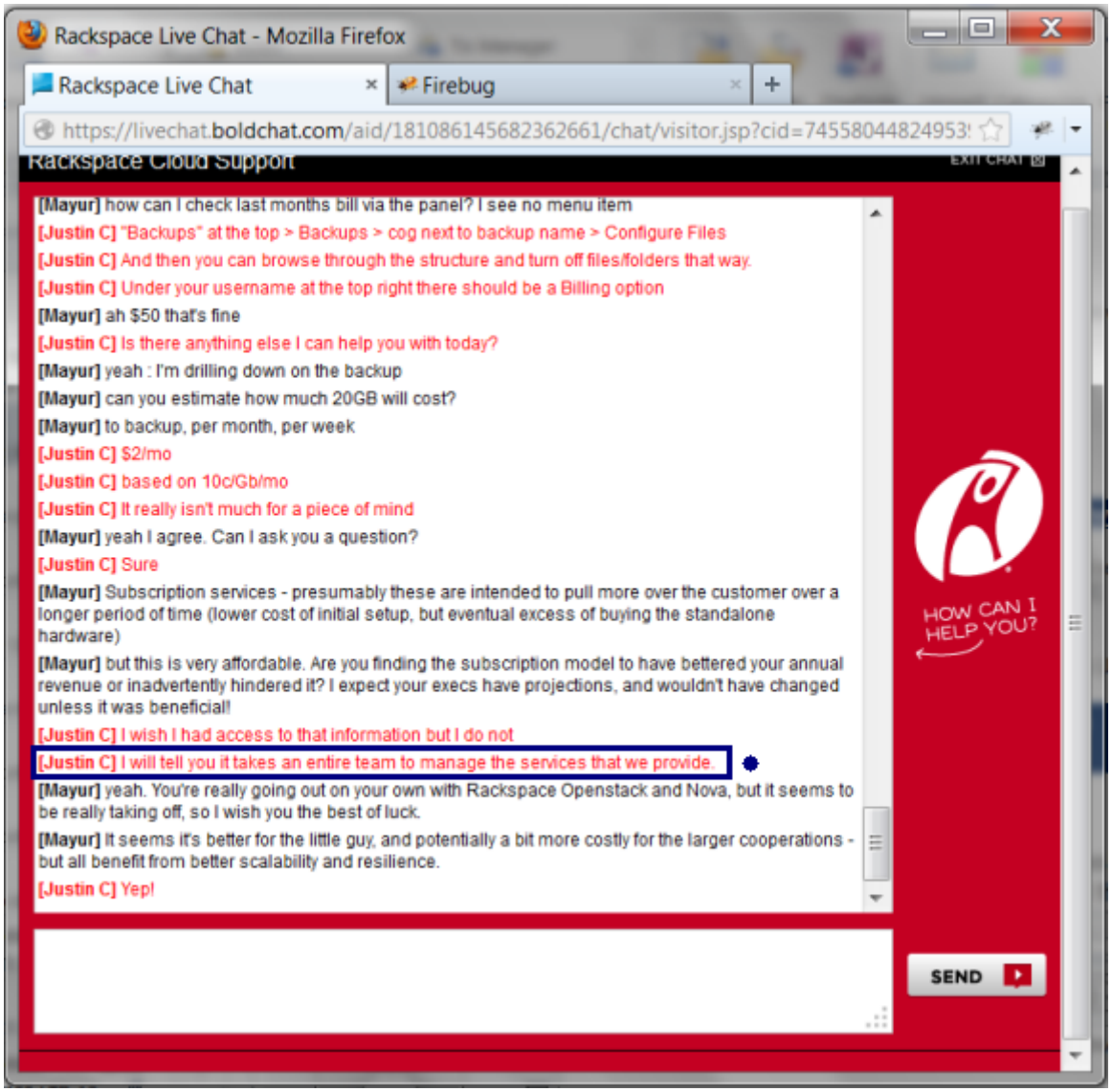
Appendix C

We also note that Rackspace offers an Alternative SLA for critical services:
http://www.rackspace.com/enterprise_hosting/critical_applications/
http://www.rackspace.com/information/legal/criticalapplicationadvanced
Critical Application Services advanced service level agreement provides a 100% production platform uptime guarantee and a 2x service level credit for businesses that demand the highest level of performance and uptime on critical applications and websites.

N.B. (Rackspace's) 100% uptime is a long-standing marketer's tactic, which simply means they will pay for any down time that does occur. Amazon on the other hand has a more realistic guarantee of 99.95%, which actually translates into just over 4.3 hours of non-scheduled downtime a year. http://www.thewhir.com/blog/exploring-cloud-slas-amazon-vs-rackspace

It could be that the above SLA is simply offering more credit as an incentive to businesses like FI; or alternatively the Cloud dynamism may be monitored and controlled by human resources instead of being automatic!

Certainly, a conversation I had with Rackspace premium support indicated this:



Rackspace's Cloud services may not yet feature automatic dynamism

Appendix C

Assurance frameworks

Many Cloud Standards bodies provide assurance frameworks. They do this to establish a structure to what is a relatively new field. Quite often this is by providing checklists or research papers.

Independent bodies

Information Systems Audit and Control Association, http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Cloud-Computing-Management-Audit-Assurance-Program.aspx

- The audit/assurance program is a tool and template to be used as a road map for the completion of a specific assurance process.
    - The governance affecting cloud computing
    - The contractual compliance between the service provider and customer
    - Control issues specific to cloud computing
- IT audit and assurance professionals are expected to customize this document to the environment in which they are performing an assurance process.

"How effective is your IT assurance approach?" COBIT 5 for Assurance: http://www.isaca.org/COBIT/Pages/Assurance-product-page.aspx/

Platform as a Service and PCI: https://pages.engineyard.com/PaaS-and-PCI.html

Cloud Security Alliance: https://cloudsecurityalliance.org/. I have compiled and uploaded a summary of their latest certifications to http://files.globalwaterintel.com/dl/csa_certifications.pdf

A particularly good checklist: Cloud Controls Matrix: https://downloads.cloudsecurityalliance.org/initiatives/ccm/CSA_CCM_v1.4.xlsx

The foundations of the Cloud Security Alliance Controls Matrix rest on its customized relationship to other industry-accepted security standards, regulations, and controls frameworks such as the ISO 27001/27002, ISACA COBIT, PCI, NIST, Jericho Forum and NERC CIP and will augment or provide internal control direction for service organization control reports attestations provided by cloud providers.

The Cloud Computing Assurance Framework

One of the most important recommendations in the ENISA's Cloud Computing Risk Assessment report is the Information Assurance Framework, a set of assurance criteria designed to assess the risk of adopting cloud services, compare different Cloud Provider offers, obtain assurance from the selected cloud providers, reduce the assurance burden on cloud providers.

http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computing-information-assurance-framework

Government bodies

Cloud Computing - Overview of Information Assurance (paper), NSA, http://www.nsa.gov/ia/_files/support/Cloud_Computing_Guidance.pdf

Overview of Information Assurance, Concerns and Opportunities, Cloud Technology Introduction

Cloud computing is an emerging trend which has progressed to the point of serious adoption in both public and private sector organizations...the information assurance aspects of cloud computing with a focus on potential security advantages and pitfalls. While many of the security concerns associated with cloud computing are shared

Appendix C

with traditional computing models, this paper will focus on those issues unique to cloud computing or that are exacerbated by it.

The "ilities": Can the cloud provider offer adequate reliability, availability, and quality of service? The cloud can complicate questions such as availability in ways perhaps wholly unexpected by those accustomed to traditional computing paradigms. Take the case of the FBI's execution of a warrant against a data center, targeting individuals suspected of fraud and confiscating computers related to the suspects, but also housing the digital presence of a dozen other businesses, at least one of which was unable to execute their business.

Data purging: Do you need a means of ensuring that deleted data is truly deleted and does not remain in an archive?

*Thoughts on the information assurance impact of cloud computing are continuing to evolve as this technological model matures. The Cloud Security Alliance's Security Guidelines for Critical Areas of Focus in Cloud Computing (*http://www.cloudsecurityalliance.org/guidance/csaguide.pdf*) delves much more deeply into many of the issues raised ... representing the census thoughts of many experts in the cloud computing and information assurance arenas.*

http://gcloud.civilservice.gov.uk/

"(The UK) Government is committed to the adoption of cloud computing and delivering computing resources."

Features many papers about how to achieve assurance certification:
http://gcloud.civilservice.gov.uk/category/accreditation/

Trust

Security as a Service

Amazon EC2 is providing Security as a Service through their webpanel, with the addition of CloudHSM (launched in March 2013).

"The AWS CloudHSM service helps you meet corporate, contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) appliances within the AWS cloud....for applications and data subject to rigorous contractual or regulatory requirements for managing cryptographic keys...CloudHSM service allows you to protect your encryption keys within HSMs designed and validated to government standards for secure key management" http://aws.amazon.com/cloudhsm/

"We are excited to announce AWS CloudHSM, a new service enabling customers to increase data security and meet compliance requirements by using dedicated Hardware Security Module (HSM) appliances within the AWS Cloud. The CloudHSM service allows customers to securely generate, store and manage cryptographic keys used for data encryption in a way that keys are accessible only by the customer." http://aws.amazon.com/about-aws/whats-new/2013/03/26/announcing-aws-cloudhsm/

Amazon just announced the launch of CloudHSM, a new service that provides Amazon Web Services users who need to meet corporate, contractual and regulatory compliance requirements for data security a way to do so by using a dedicated Hardware Security Module (the 'HSM' in CloudHSM) within the Amazon cloud. Until now, Amazon argues, the only option for many companies that use its cloud services was to store their most sensitive data – or the encryption keys to it – in their own on-premise data centers. This, of course, made it hard for these companies to fully migrate their applications to the cloud.

The new service, Amazon writes, can be used to support "a variety of use cases and applications, such as database encryption, Digital Rights Management (DRM), and Public Key Infrastructure (PKI) including authentication and authorization, document signing, and transaction processing." The actual appliances are Luna SA modules from SafeNet, Inc..The upfront cost to provision a CloudHSM is $5,000 and the hourly cost are $1.88 per hour, which comes out to $1,373 on average per month. For businesses that need this kind of security, that's probably a small price to pay.

Appendix C

Amazon Web Services Launches CloudHSM, A Dedicated Hardware Security Appliance For Managing Cryptographic Keys, March 2013, TechCrunch http://techcrunch.com/2013/03/26/amazon-web-services-launches-cloudhsm-a-dedicated-hardware-security-appliance-for-managing-cryptographic-keys/, http://aws.amazon.com/cloudhsm/pricing/

TPM hardware

FI's customers could also be sent TPMs (such as RSA's secureID dongle: http://en.wikipedia.org/wiki/SecurID)

"Developed by the Trusted Computing Group (TCG), the TPM is a standard for providing a hardware-based root of trust for computing and other systems...it has been is estimated that 200-300 million TPMs have shipped in enterprise PCs based on these standards."

"A cloud service can use the TPM binding an OpenID certificate to the TPM for strong machine authentication to their service"...No matter which cloud services or model is pursued, security improvements should be among the criteria on the "must have" list. Issues to consider include: hardware versus software-based security, hardware activation, known users, known machines, accessing both data and application services, data protection and compliance, and protecting the service provider's agreement for controlled user access. For data leakage and access control, authorization to access information from the cloud, whether it's an application or an application with data, requires a trusted endpoint to ensure strong authentication and knowledge of who is accessing the cloud service and the data hosted by the cloud service. In fact, a trusted endpoint is part of the solution for addressing all of the issues. One solution involves implementing the Trusted Platform Module (TPM), a widely available security chip that already resides in most business PCs. The layers of authentication, where the machine is known by the cloud and the machine has a relationship with the user, significantly enhance cloud security. This process provides a chain of trust for machine-to-machine connectivity so that only known machines and known users obtain access to applications and data. Unlike other hardware token security tools that are available in USB, key fob, and smart card type products, the standards-based TPM is typically an application-specific integrated circuit (ASIC)" .

http://brianberger.sys-con.com/node/1411630/mobile, and discussed in Chapter 8.4 of our course book.

Appendix D

External case study examples

Provenance in the Cloud is a topic of modern research unto itself.
The paper (Provenance for the Cloud) http://static.usenix.org/event/fast10/tech/full_papers/muniswamy-reddy.pdf highlights the need for metadata in Cloud storage volumes, and extending the Condor system for gathering provenance data. http://static.usenix.org/event/tapp11/tech/final_files/Abbadi.pdf highlights the importance of capturing provenance data from physical, virtual and application resources. At present, the only way that provenance is provided on a Cloud is through linking together log and audit data collected from multiple resources, to provide the complete history of an event or result. It is no substitute for provenance systems that already exist in Grid systems. Cloud computing therefore is a good example of a situation where the introduction of better provenance data could provide immediate benefits for system administrators as well as users.
It features examples on how day to day Cloud dynamics can result in an affect on provenance data: *"Our first example demonstrates how a simple increase in load, and the corresponding reaction from the cloud, can result in a loss of provenance data."* p.4

"Another important point which indirectly depends on cloud provenance is trust establishment. Trust establishment in cloud computing requires collaborative efforts from industry and academia. As discussed by Abbadi, establishing trust in cloud systems requires two mutually dependent elements: (a.) support infrastructures with trustworthy mechanisms and tools to help cloud providers automate the process of managing, maintaining, and securing their systems (this includes but is not limited to self-managed services as discussed earlier); and (b.) developing methods to help cloud users and providers establish trust in the operation of the infrastructure by continually assessing its operational status. An important component in both elements is establishing trustworthy cloud provenance mechanisms....One way to implement this is for cloud providers, who are interested in providing trustworthy provenance mechanisms, to support automated management services with incident provenance describing, for example, the root cause of an incident. Cloud users, on the other hand, would be interested in this to assure them that the information provided by the cloud reflects the real operation of the cloud. For example, it would enable cloud users to ensure that the billing statements reflect real usage of resources. Another example would be attesting the integrity and enforcement of cloud resource policies." Challenges for Provenance in Cloud Computing (link above).

There are lots of publications listing modern research into trusted computing at
http://www.tclouds-project.eu/index.php/component/jumi/publications
"TCLOUDS puts its focus on privacy protection in cross-border infrastructures and on ensuring resilience against failures and attacks. TCLOUDS aims to build prototype internet-scale ICT infrastructure which allows virtualised computing, network and storage resources over the Internet to provide scalability and cost-efficiency."

Author's comment: As online services become the electronic age's backbone for critical government infrastructures (medical) and corporate services (banking), a scalability, availability, security and importantly resilience needs to be achieved that matches industrial Engineering standards. Trusted computing and modern provenance efforts are the way forward. *From a futurist's perspective*, hopefully this will allow the investment into infrastructures that are hosted in non-EU countries, allowing data laws and resources to be governed across international law with the same degree of encryption security and legal protection; not to mention creating a vast single unified grid of computing power and storage for Earth's consumption.

Appendix E

Rackspace Webinar: New Cloud Control Panel: A Behind The Scenes Look

The following is taken from a Rackspace Cloud Services webinar I attended on 30th April 2013.

I took the following screenshots and notes live to illustrate what current leading Cloud developers are actively promoting. A full recording can be found at: http://www.rackspace.com/blog/tag/webinar/ along with 10 other webinar discussions about Rackspace Cloud from 2013. Having completed the course, it is nice to reflect that a lot of the *must have* focuses we mentioned in our report (auto-polling, PCI compliance, region isolation, RBAC) are what Rackspace sees as important areas of current and future development. It builds upon our course Nova experiments.

Notes (numbers mean minute progression)

new control panel built on the cloud [use github for rapid deployments, through 1000's of unit tests 1300

business goals: simply IT [customer centric approach - made a "mental model diagram": spoke to customers, made a map

Designing the control with usability control panel

Watched the customer work on it, did re-design. (Iterative UX approach)

15m : services that they offer, UI + API.

nova designed to operate at webscale nova scalability:(first gen; order of magnitude: 100'thousands: second gen : millions)

{regions+openstack abilities}: 0 day release for new distro images

create a DB instance (select size + ram) in a container

{container_based_virtualization _ not hypervisor_type1_like_vm}: light weight version partitioning scheme rather than independent VMs for each instance. Breaks a virtual OS to a virtual container of DB. RAM + disk independently - multiple DBs. Containers are fast

decoupling cloud storage from your VM (creating SSD OR databases: lower cost. Can optimize for more storage or more performance). Different volumes to attach to multiple vm's.

{polling_monitoring_service_http checks ping checks_multiple_regions_auto_actions_based on triggers_known as_pollers}: agent installable on private or public cloud. Monitoring as a service - CPU, disk, memory, RAM, bandwidth polling, can set thresholds and alerts on application availability, can choose whether to scale application up or down.

{cloud_networks_create_single_tenant_vlan_layer_networks in the cloud_control_ip_addressing_scheme_complete_network_isolation}: used for isolation: used for security, powered by quantum

41m : roadmap: "investment in security, resilience, security and distribution control...choice in scalability"

Rackspace assign different users different permissions to resources using RBAC: (files, DB containers, storage volumes are assigned to different users): rolling out this year. 45m “rollout of RBAC permissions for resources”

Need for more granular billing information

PCI compliance: their customers in the cloud have passed PCI compliance audits, but they take payments through 3rd party gateways

There are account limits (like a hairdryer circuit breaker) - like a runaway script that creates lots of cloud servers - used as a protection rather than a hardlimit (like credit card limit)

Appendix E

More investments in different flavour classes for different application requirements

create a portable IP across servers as cloud networks evolve. Each cloud account has an internal “optimized” network for *services* and external network for *public access*. 53m: Load balancing

load balancers and private networks: public network, private network for access containers of databases

57m: Cloud networks allows isolated networks

can spin up a London server from the US, or northern Virginia cloud from the UK (to hit maximum load)

rackspace knowledge center: rackspace.com fanatical support section

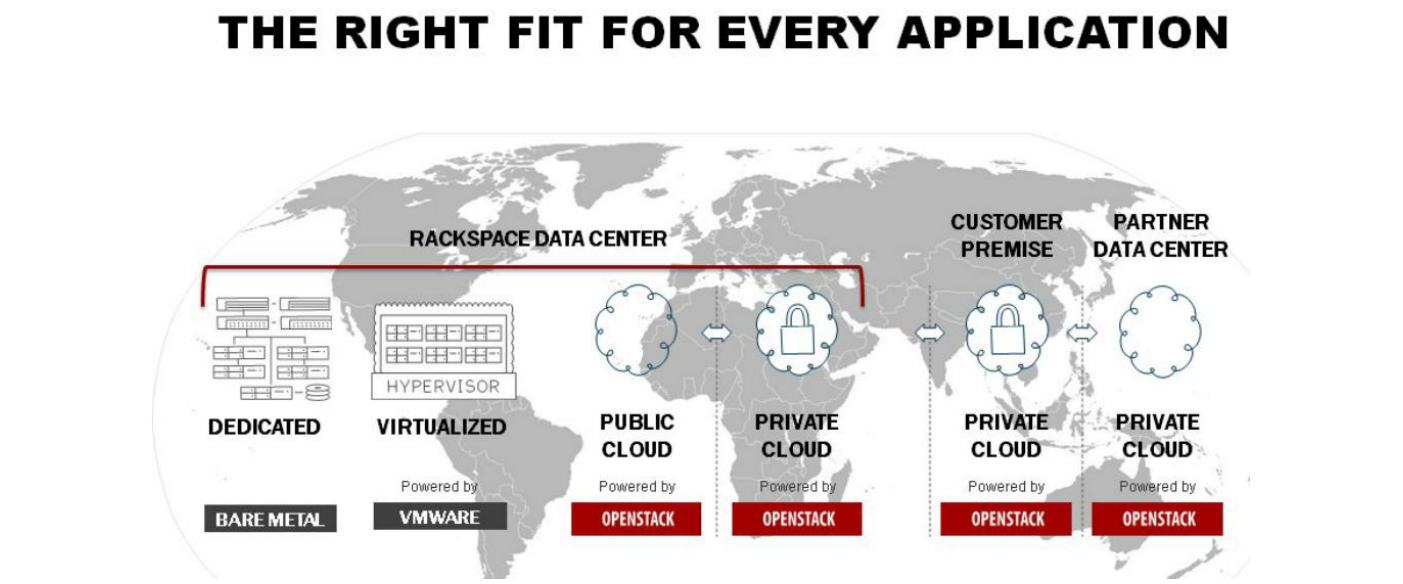
devops.rackspace.com blog tips + tricks

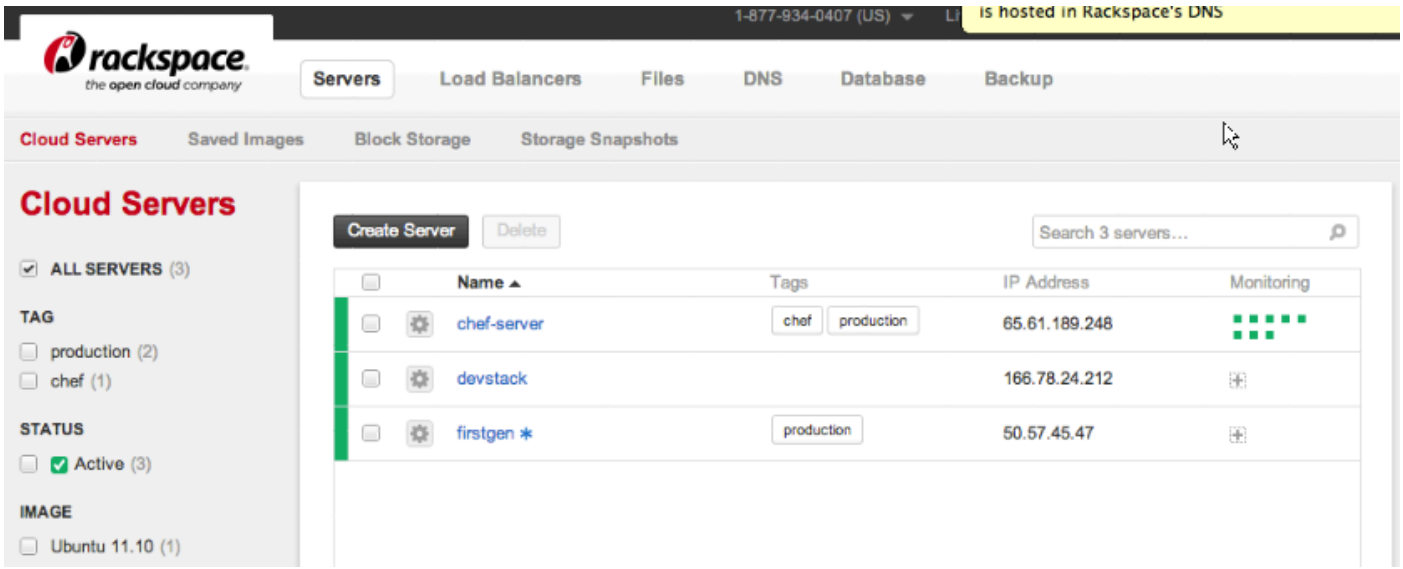
racksmon: create an entity, give it an IP address, monitor it from the command line

59m: nova monitoring client, reddwarf (CLI apps)

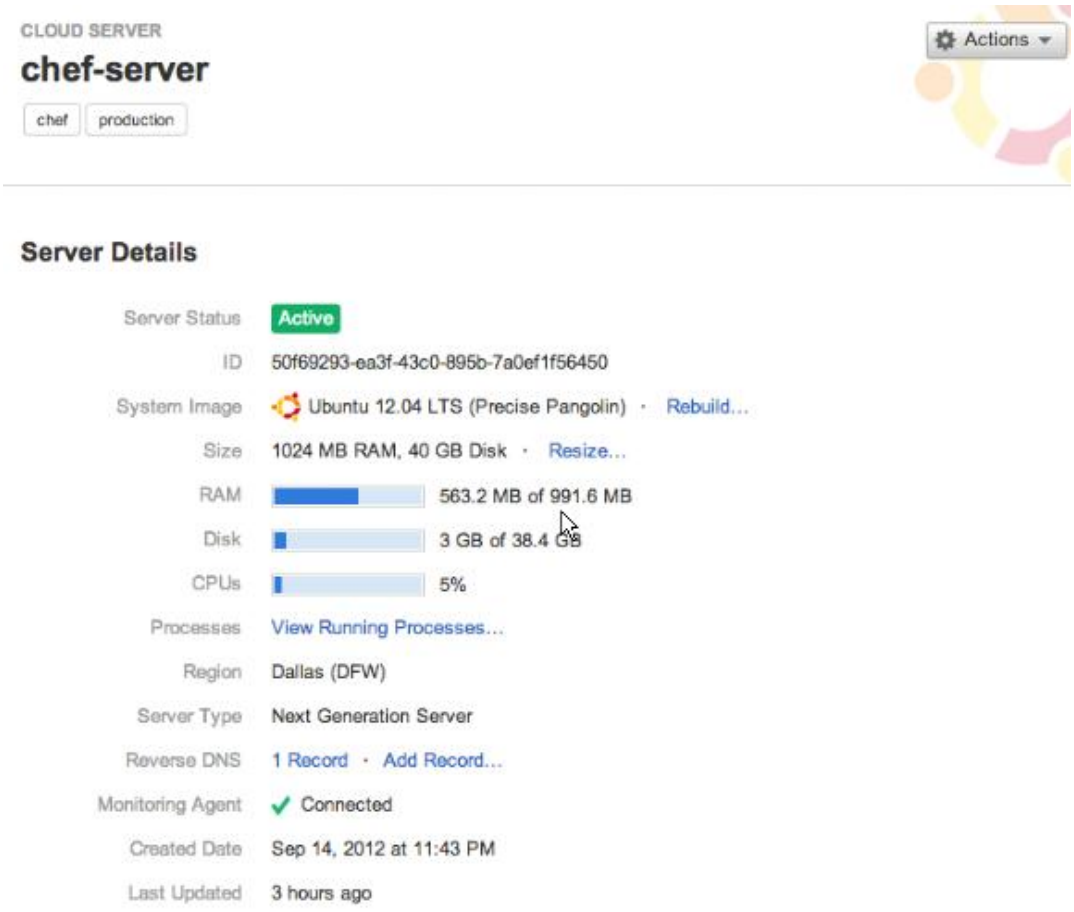
There is a cap on DBs of 150GBs (for backups)

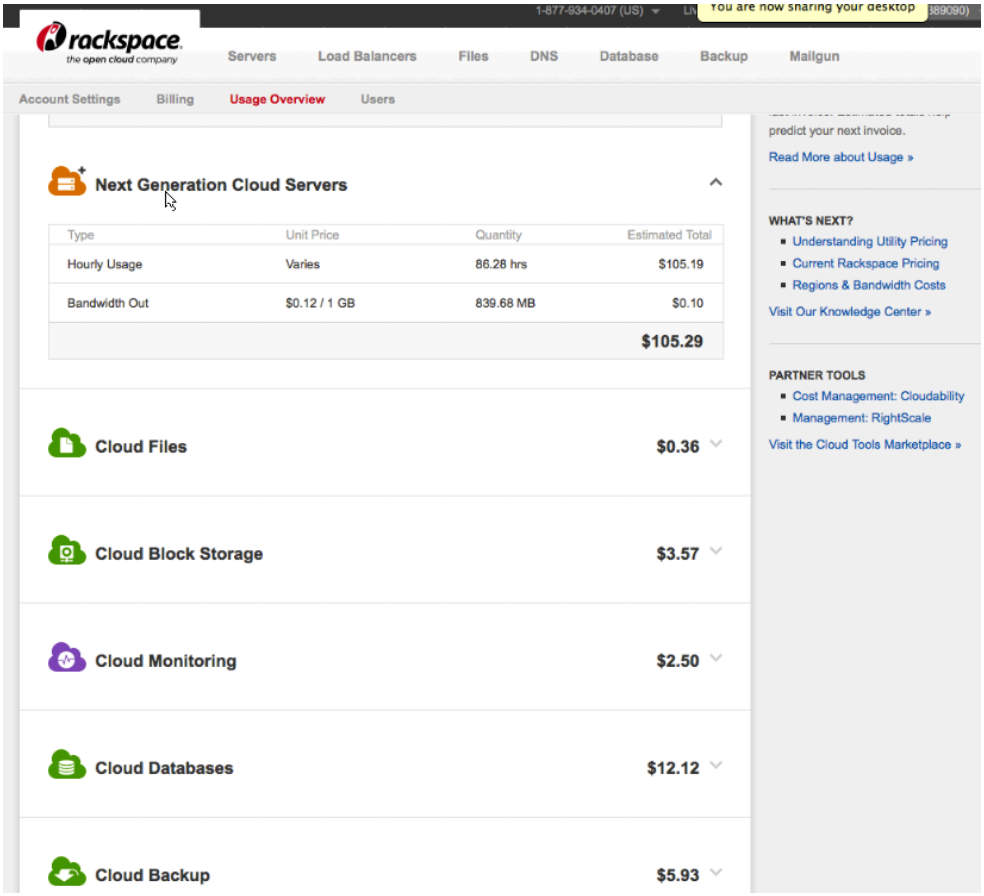
PCI or HIPAA "any hosting provider is unlikely to say that it is compliant...you need to be responsible for your data, get audited, and pass" [1h 3m]



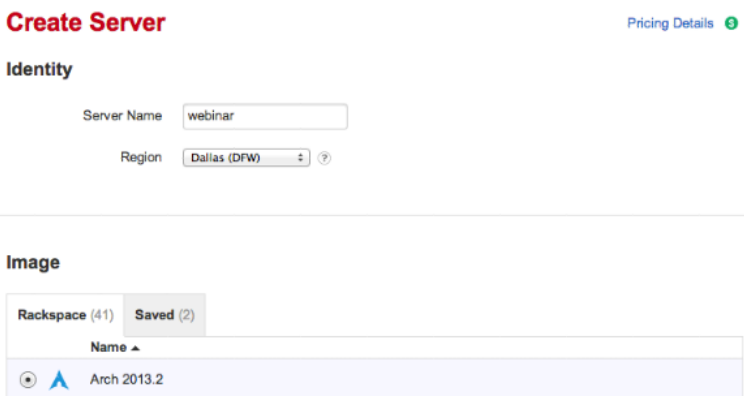


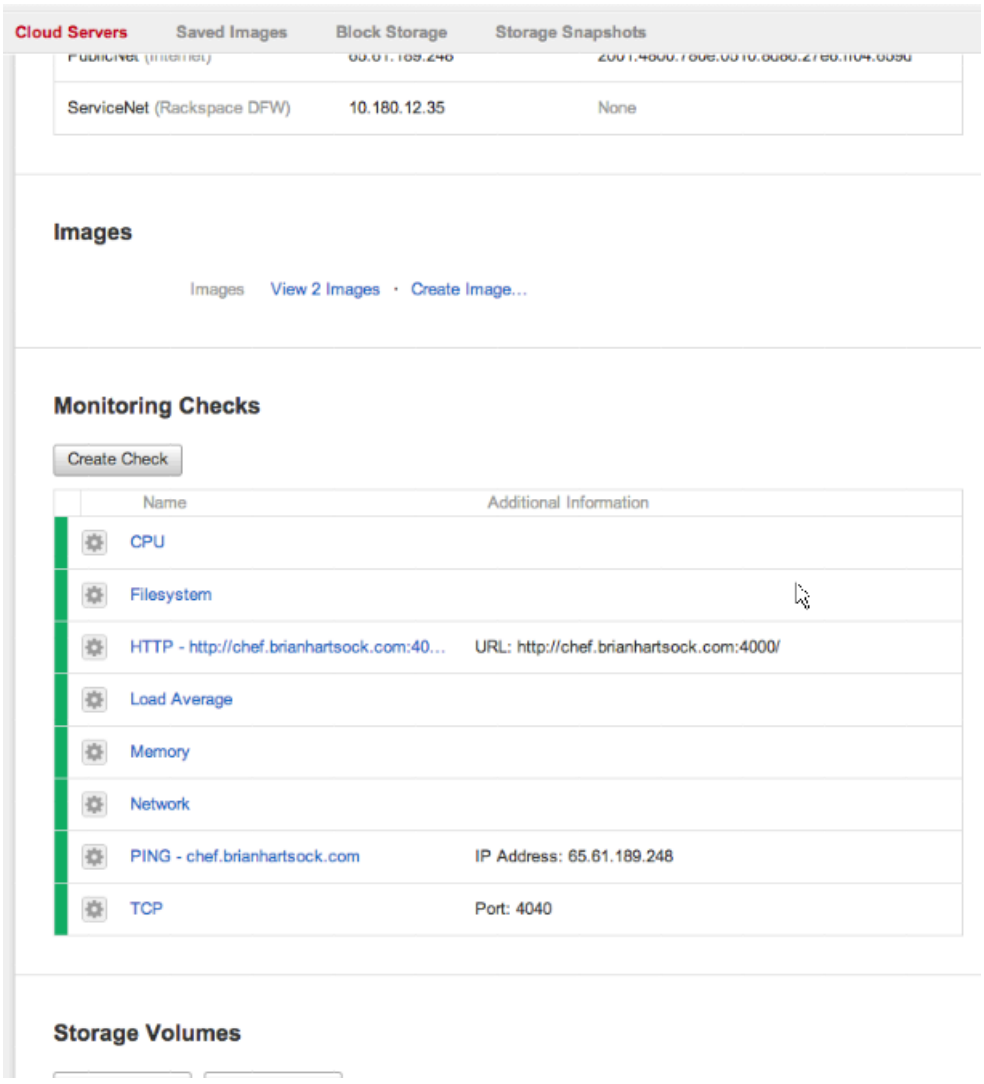
Appendix E


CLOUD SERVER
chef-server
chef
production
Actions
Server Details
Server Status
Active
ID
50f69293-ea3f-43c0-895b-7a0ef1f56450
System Image
Ubuntu 12.04 LTS (Precise Pangolin) · Rebuild...
Size
1024 MB RAM, 40 GB Disk · Resize...
RAM
563.2 MB of 991.6 MB
Disk
3 GB of 38.4 GB
CPUs
5%
Processes
View Running Processes...
Region
Dallas (DFW)
Server Type
Next Generation Server
Reverse DNS
1 Record · Add Record...
Monitoring Agent
Connected
Created Date
Sep 14, 2012 at 11:43 PM
Last Updated
3 hours ago


rackspace
the open cloud company
Servers
Load Balancers
Files
DNS
Database
Backup
Mailgun
Account Settings
Billing
Usage Overview
Users
Next Generation Cloud Servers
Type
Unit Price
Quantity
Estimated Total
Hourly Usage
Varies
86.28 hrs
$105.19
Bandwidth Out
$0.12 / 1 GB
839.68 MB
$0.10
$105.29
Cloud Files
$0.36
Cloud Block Storage
$3.57
Cloud Monitoring
$2.50
Cloud Databases
$12.12
Cloud Backup
$5.93
predict your next invoice.
Read More about Usage »
WHAT'S NEXT?
Understanding Utility Pricing
Current Rackspace Pricing
Regions & Bandwidth Costs
Visit Our Knowledge Center »
PARTNER TOOLS
Cost Management: Cloudability
Management: RightScale
Visit the Cloud Tools Marketplace »

Appendix E

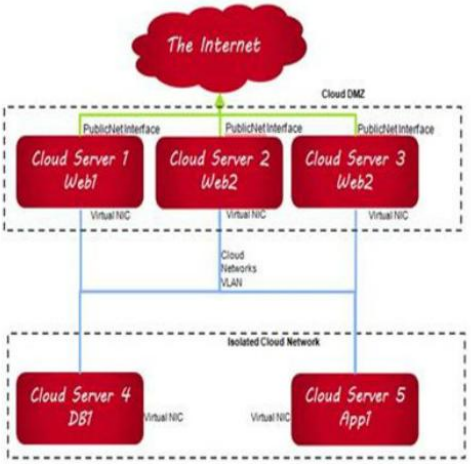

Create Server
Pricing Details
Identity
Server Name
webinar
Region
Dallas (DFW)
Image
Rackspace (41)
Saved (2)
Name
Arch 2013.2


Cloud Servers
Saved Images
Block Storage
Storage Snapshots
ServiceNet (Rackspace DFW)
10.180.12.35
None
Images
Images
View 2 Images
Create Image...
Monitoring Checks
Create Check
Name
Additional Information
CPU
Filesystem
HTTP - http://chef.brianhartsock.com:40...
URL: http://chef.brianhartsock.com:4000/
Load Average
Memory
Network
PING - chef.brianhartsock.com
IP Address: 65.61.189.248
TCP
Port: 4040
Storage Volumes

Appendix E

RACKSPACE® CLOUD NETWORKS

- API driven layer 2 network segmentation
- Virtualized network for security and isolation in the public cloud
- Powered by OpenStack Quantum



RACKSPACE® CLOUD MONITORING

- Monitor anywhere
- Scales automatically
- Flexible alerts
- Infrastructure monitoring

2013 ROADMAP THEMES

BETTER CONTROL	Giving customers more transparency and insight into their hosted applications and infrastructure.
ENHANCED SECURITY & RESILIENCY	Enabling better security and strengthening businesses.
EASIER TO SCALE	Enabling geographically distributed, mission critical applications, expansion and automation.
SERVICES	Evolving Fanatical Support®, advising, sharing best practices and collaborating with our customers.

Appendix E

RACKSPACE® CLOUD SERVERS™
POWERED BY OPENSTACK®

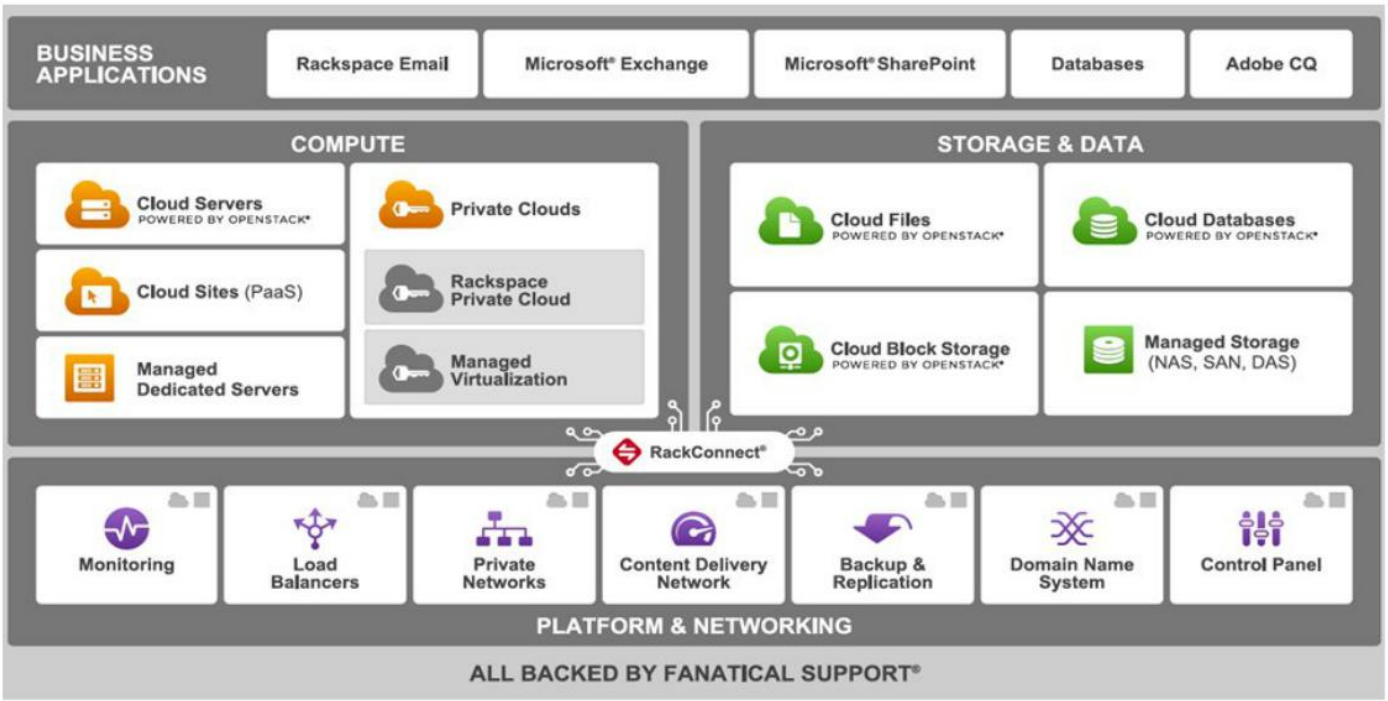
- Built on OpenStack
  - –Create hundreds of servers in minutes
- Choose your region
- Much Improved "ilities"
  - –Scalability, Reliability, Agility
- Over 40 OS and DB images
  - –Quick Releases
  - –Update Windows Images Regularly

openstack™ CLOUD SOFTWARE

rackspace the open cloud company

RACKSPACE® HOSTING | WWW.RACKSPACE.COM 13

Rackspace Portfolio



rackspace the open cloud company

RACKSPACE® HOSTING | WWW.RACKSPACE.COM 12

useful slides:

4: shows order: Cloud services
- Deployment types
- Challenges
- Components
- Management platforms
- Management services

— insiders
— trust
Assessing Trustworthiness
Assess levels of trust
Steps when outsourcing
Establishing trust
Provenance
openstack

Slides BREAKDOWN

1st week

Section | Description | Value

14–16 : 2 definitions — little

Enterprise Infrastructure

21 : Modern admins are overwhelmed by too many servers. → Now in virtualisation era. — little

26 : Adv. of virtualisation
Chall of virtualisation — little

'Cloud
28: Service + deployment types' — IaaS, PaaS, SaaS — 30: Bar chart ✓

31–35 Deployment types — Public/hybrid — useful
Scalability, adaptability, Self-healing

38–41 Operational challenges
Data management
Interoperability
Privacy, Security, Trust

42 · Forensic/provenance overview

43 Performance, Legislation, Green

(44) Ex. 1

50 Taxonomy benefits (above)

52 Components (network, vcc, storage, vm)
Horizontal vs. vertical

110 Insiders — Definition, models
114

115, 120–124 Procedure + Examples

(125) Ex. 5

123 Trust (overview, properties, establishment, relationships, challenges)
(boot authentication, platform attestation)
chain of trust

131–2 TPM (protected storage / platform state)

133–6 Structure — Root of trust
RT measurement / storage / reporting

137 chain of trust (see boot from TPM), pic

138 Platform attestation (pic)

144 Establishing trust in the cloud (properties + importance) — useful
(for users, providers, collaborating entities, auditors) — useful

144 Trust models – stakeholders — auto management services

145 operational trust (trust in infrastructure: humans, docs,

146–151 (adaptability property – reliability property

152 Pic – properties by business

153 cloud dynamics (scaling and moving based on policy)
reffect on trust relationships

157 Dynamic trust relationships (load balancing, redundancy, clustering, scaling)

1 trust challenges – composite chains, re-evaluation/transparency

5 Trust challenges with outsourcing, steps — useful

–170 User concerns (insiders, regulations etc. Control

2–176 Requirements for establishing trust (pic 173) (chain of trust)

77 Importance of self managed services

78 Protecting from insiders

79 Trusted environments and migrations (reliable infrastructure) useful

80 Key requirements for trust

(8) Ex. 5

Exercises:

61–62 Management Platforms (diagrams) Services

63 Benefits of automation (MTTD etc.)

65–66 Types of management (automated) services

(68) Ex. 2

69 Self managed services (d) — (ii)

72 Types (pic. 72)

73–80 Advanced descriptions: Adaptability, App Layer SMS
resilience, scalability, availability, reliability

81 Adaptability, Architect, Scalability — Virtual Layer SMS
Availability, Reliability, Security, Privacy (picture on 91)
Examples (92–100)

(103) Ex. 3

185 Provenance → a + b
system admin + forensic provenance

187 Difference from logs

189 Complication of sources

191 Provenance in clouds

192 Scenario

196 Use of provenance, indirect logging

199 Current big shortcomings

200 reasons for complexity

201 Requirements for establishment (standardisation)

202 solution to challenges (200)

204 Requirements for provenance

(209) Ex. 6