HOW TO BUILD
TAILORED CLOUD SOLUTIONS

LEARNING FROM 100 CLOUD JOURNEYS

GIUSEPPE PATERNÒ

Learnings from over 100 Cloud Journeys

How to build tailored cloud solutions

ISBN: 9798665550602

Foreword

I've worked on over 100 cloud projects and no two were exactly alike. Cloud solutions can be complex and each project has to meet specific business needs and work within specific parameters. They can range from building large private clouds to moving everything to the cloud, and even implementing organisational changes.

In this paper I set out what I learned in my career, sharing with you three different case histories that show how every business should have its own tailored journey to the cloud.

I hope that -going through these stories- I can truly inspire you in finding your own path to help to increase your business agility, lower or rationalise your costs and better focus on the core business.

-- Giuseppe Paternò

Acknowledgements

I'm lucky, I know. I was able to travel through Europe and part of the world and play a key role in creating something unique. This experience is a privilege granted only to a few people.

Unfortunately, the price to pay is to be away from my loved ones for most of my time. I can tell you that having my heart split between countries is probably the most challenging part of my life.

I can't thank my wife Maria enough for supporting me and my friends who were there when I needed to talk to someone. I can't name all of them, but special thanks to Ezio and Gianluca.

About the Author

Giuseppe Paternò is an IT infrastructure architect, security expert, and cloud solution guru with over 25 years of international experience.

His clients are companies who are either at the start of their cloud journey, or want to build their own cloud infrastructure.

He works with CEOs and board directors to make sure the business gets real long-term benefits from its IT spend. Giuseppe has worked with Deutsche Telekom, eBay, Etisalat, IBM, Pirelli, RedHat, Sun Microsystems, TomTom, Vodafone, and Volvo.

info@gpaterno.com

www.gpaterno.com

https://www.linkedin.com/in/gpaterno/

Index

Preface

In February 2020, Covid-19 forced almost everyone to work from home. Most IT infrastructures weren't ready for this, and the pandemic put systems under heavy stress. Suddenly, businesses had a good reason to embrace the cloud: moving applications to the cloud reduced the strain on existing infrastructure.

The cloud helped many businesses cope. Businesses that had wondered if all the talk about "the cloud" was just marketing spin found it could deliver real business value.

Every business needs a tailored journey – and an experienced guide

Moving applications to the cloud is a start point for many businesses on their journey to the cloud. But every business should have its own tailored journey.

I've worked on over 100 cloud projects and no two were exactly alike. Cloud solutions can be complex and each project has to meet specific business needs, and work within specific parameters.

Choose your cloud architect carefully. Take care to choose the right individual rather than a big consultancy brand. Experienced cloud architects

have to combine a business focus with technical and project experience – and more than a dash of inspiration.

A good architect adds some art to the architecture.

Six pillars for successful cloud projects

Keeping these rules top of mind will help your cloud project deliver results:

1. Use open standards and open source. You will have fewer update nightmares, more security, less vendor lock-in, and better portability across systems.

2. Keep it simple when you can. Over-engineering will create solutions that are difficult to manage.

3. Move everything non-strategic to the cloud if it reduces total cost of ownership.

4. Automate whatever you can. This makes it easier to move applications across clouds or back on-premise.

5. Take a zero-trust approach to security. Trust nothing that's crossed public or semi-public networks, and apply security as close as possible to applications.

6. Keep multiple backups in open formats. If you have a copy of everything, and you automated everything, disaster recovery is a piece of cake.

Three cloud journeys tailored to business

The three case histories in this paper show how tailored solutions should fit the business and deliver real benefits:

- An investment bank that needed to cut ties with its IT partner – suddenly, secretly. The bank got real control, better security, and lower costs.
- A telco that had to cope with 400’000 new subscribers. The project increased capacity, boosted reliability, and cut license costs
- A manufacturer that needed its own IT solution. The business became more agile, cut costs, and established a more effective approach to IT projects.

The cloud is more than marketing

Given all the talk, you could be forgiven for thinking “the cloud” is an annoying marketing buzzword. It certainly annoys me when it’s used in a vague way. Because without context, the cloud is rather vague.

The cloud can mean a solution with real business benefits, or something that brings little real value – and even adds extra risk.

Cloud is far more than virtualization

In the early days, the cloud was pretty much a synonym for virtualization, and in some ways it still is. But more and more, cloud means pay-as-you-use services.

And don’t be distracted by those t-shirts that say “the cloud is just someone else’s computer”. That’s a fun t-shirt, if you’re a certain kind of tech nerd, but it’s a long way from reality.

Letting go of your physical servers

There’s been a lot of confusing talk about the cloud, and some people still tell me they don’t completely trust the idea of the cloud – they want a server they can touch.

I usually overcome their objections with this question: Do you generate your own electricity or buy it from a power company?

The same idea applies to the cloud.

In some situations you might want to keep a critical application on your own servers and infrastructure – the equivalent of generating your own electricity. But most of the time it makes more business sense to rent cloud servers and infrastructure – the equivalent of buying electricity from a power company.

Private clouds for larger companies

Larger companies spend eye-watering sums on cloud services. I've met clients who hand over $2m a month – a substantial annual overhead by any measure – to a famous cloud-service provider.

A private cloud would slash these costs. But many companies prefer to shoulder the cost burden rather than take on architecting, building, and running their own private cloud.

A tailored approach to cloud

When I was 19, I got a valuable lesson in IT consulting. I was working with IBM on a project for an Italian company that made bathroom fittings. I was trying to convince their IT manager to invest in faster connections to their mainframe computer in Paris. It seemed obvious to me that a fast connection was better than the pitifully slow one they had. “We make toilets here”, the manager said. “We’ll only spend money on IT if it helps us make toilets more efficiently, or helps us save money”.

I learnt my lesson: technology is a business tool – it has to deliver value for the business.

I keep this lesson in mind when I talk to clients about their cloud journey.

Cloud journeys need to take several factors

I haven’t counted how many cloud projects I’ve worked on, but I know it’s way more than 100. And no two projects were the same: embracing the cloud is a unique journey that requires a tailored approach.

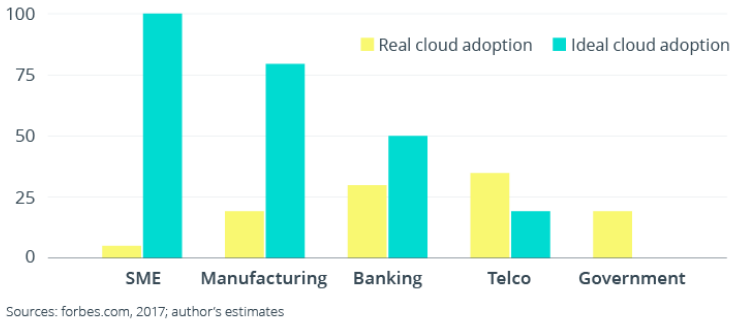
There are certainly some common patterns, but each project depends on a range of factors.

- Business strategy, the company's industry, sector, and market segment – and any special legal or compliance requirements.
- Company structure, and the kind of workforce they employ.
- The current IT department's workload and available skills.
- Cultural and political factors. For example, some countries don't like American-owned companies; other countries insist on keeping data local, or be bound by more stringent data processing laws.
- Physical location – the "digital divide". Internet speeds are slower North of the UK and South of Italy, so cloud architecture should minimise the exchange of data.

The cloud-adoption paradox

The chart below shows actual cloud adoption by market sector and company type, compared to what I believe is ideal cloud adoption. The data for real cloud adoption is from a 2017 forbes.com review. The ideal adoption rates are my estimates, based on my experience.

My gut feeling, from working with European clients, is that cloud adoption in other sectors – for example energy and utilities – is even higher than the forbes.com data.



Average rates of cloud adoption (yellow) vs ideal cloud adoption (green)

Low adoption by SMEs and manufacturing

Companies that would get the most benefit from the cloud, such as small to medium sized enterprises (SMEs) and manufacturing have low adoption rates.

They still have most of their systems and application on-premises, probably with no disaster recovery plan. In the worst case scenarios, they have no backups and no safety net. In my opinion they should focus on what they do best – embracing cloud services would relieve the business of many unnecessary IT tasks.

For these businesses, embracing the cloud requires specialist skills and probably 1-2 years of work. This will deliver significant long-term benefits, but requires a high upfront consultancy cost.

Not all companies should go for an all-out

At the other end of the adoption scale, large companies go all-out for cloud solutions. They can afford private clouds and can potentially save a huge amount of money.

But not all big companies should take this path. Telecommunication companies, or telcos, and government agencies are a case in point. A telco's main business is operating a broadband or voice

network. So telcos shouldn't rely on someone else to provide those services.

Government agencies should also think twice before they use other countries' datacentres – for obvious reasons.

High adoption rates can be a side effect

Some large companies may have made a big move to cloud services because they use software-as-a-service (SaaS) solutions like Salesforce – and telcos are often a case in point. Salesforce is a great CRM tool, but if your business spends 10 million euros a year on Salesforce, you could probably create a tailored CRM for far less.

High cloud-adoption rates can be driven by the urge to delegate. I've found that this is often how management sees the cloud: an outsourcer you can delegate business responsibilities to.

This kind of delegation may reduce risks for management, but it can increase costs – and add security risks.

Transforming the IT culture

The cloud is just a technology – but you'll get much more out of it if you embrace its philosophy. This requires a company to make deep changes to how it sees IT. Changes that will help the business become more productive and agile. If you're not willing to change your internal processes and department divisions, you won't enjoy the full benefits of the cloud.

If you truly understand and embrace cloud philosophy, the cloud is a huge shift in your organisation. It will change your way of working on IT projects forever, dramatically improve your IT, and cut costs.

A new kind of IT manager

The IT manager's mission should be to empower a democratic approach to IT in all the business units. IT managers should act as a system integrator, and a central coordinator of resources. They should set strategy, provide common resources – like identity management – and make sure security standards are met.

In a cloud-philosophy model, each department would have an IT ambassador who is both a domain expert and tech savvy – a kind of distributed IT model. They liaise with their peers

to ensure that IT best practices are met when selecting a product or service, or developing a new application.

Extended development teams

If you develop your own applications and decide to embrace the cloud in full, then you need to shift the way you think about developing your application.

You'll need to be able to modify source code – often only 15-20 lines – so that you can run applications in containers.

Secondly, to be able to scale, you need to mix internal developers with external developers (contractors) and form extended development teams. These teams will allow you to retain internal knowledge and skills on the application, while scaling with external developers.

Thirdly, you might consider how to restructure how your software developers work with IT operations, and use what's become known as a DevOps approach. FaceBook, for example, don't have a distinction between developers and system administration, they are all product engineers responsible for the entire lifecycle of applications.

The detail of how to use extended development teams, agile methodologies, and DevOps is outside the scope of this paper – but these strategies will help you fully embrace the cloud philosophy.

Six pillars for a successful cloud

I've found that keeping these rules top of mind helps focus the project on the right solution, and deliver results for the business.

1. Use open standards and open source.

Embrace open source and open standards as much as you can in your applications. Most open source products (excluding some databases or caches) can be automated and this makes them portable. If you choose a database-as-a-service, make sure it uses common protocols such as MySQL or Postgres, so that you can export data and import elsewhere.

You will have fewer update nightmares, more security, less vendor lock-in, and better portability across systems.

2. Move everything non-strategic to the cloud if it reduces total cost of ownership

For example, a good first step is to move collaboration (mail, documents, VoIP, drive sync) to cloud services and ensure high security standards. Embracing cloud collaboration also gives you the option of cloud identity management, and this will ease cloud migrations.

Ensure SaaS providers will let you export the data in an open format. Check prices and the fine print before you buy – and only embrace SaaS products only if they cut costs.

Applications with tight hardware integrations or with highly confidential data should remain on-premise.

3. Keep it simple when you can

Over-engineering will create solutions that are difficult to manage. I cannot stress this enough. I know that many applications are complex, but don't fall into the temptation of making things more complicated. It's an easy mistake to make.

Only make things complicated if the extra effort will deliver real economic or competitive advantage.

4. Automate whatever you can

Open standards for data and open source will help you avoid any lock-in and give you freedom of choice. Using containers to distribute and run the applications, along with an automation system, will create a process for quickly moving your application makes it easier to move applications across clouds or back on-premise.

If you can't re-engineer your application, just shift and lift virtual machines (VMs) with legacy

workloads to an infrastructure as a software (IaaS) provider.

Understanding how much uptime your applications need will help you save money – don't pay for service levels you don't need. You may be surprised to find that basic SLAs will work for most internal applications.

5. Take a zero-trust approach to security

Trust nothing that's crossed public or semi-public networks. Nowadays there is no clear divide between an internal office network and the Internet. In the most extreme cases, an office network is just a transit network, just a bit more secure than a home network.

Traditional firewalls are no longer effective, and you should apply protection as close as possible to the application.

But the work-anywhere model has some upside. The office will just be a meeting place and users will be able to work from anywhere. Looking a bit further ahead, new devices like the iPad Pro, with a keyboard and embedded trackpad, can replace PCs for standard users. These devices are easier to manage with a mobile device management (MDM) and less vulnerable to viruses and malware. The keyboard and the trackpad can be fantastic

when using a remote terminal with two factor authentication to connect to legacy applications.

PCs and workstations will only be for advanced users who need proper computing power – for example, developers, or those who run local scripts or financial excel formulas with external data.

6. Keep multiple backups in open formats

Last but not least, have one or many backups or replicas of all cloud data in an open format. I'm really paranoid about this. If you have a copy of everything, and you automated everything, you will be able to rebuild your entire infrastructure easily. Disaster recovery will be a piece of cake: you will be able to restore either to another cloud or rebuild on-premise.

Three very different cloud journeys

Each of these journeys to the cloud comes from a different market segment and takes a different approach.

The first one is a central London investment bank, a fast-track project that relied on speed and secrecy. This project is about a two-month sprint to move the bank's entire IT system away from an outsourcer with poor security standards.

The second one is about a satellite operator offering broadband services. Their cloud journey consisted of two projects that delivered higher availability and lower licence costs and allowed the IT team to focus on business-critical tasks.

The last one is a project that gave a global manufacturer a way to unlock its IT system's potential to be a business enabler – rather than a drain on costs and innovation.

I hope they'll give you some ideas about how to make your cloud journey.

The investment bank

One day the CEO and co-owner of an investment bank in central London invited me for a coffee. A friend of a friend said he was in desperate need. The chat felt very friendly, like we were getting to know each other.

Out of the blue he said, 'We've been hacked and they stole 8 million pounds. We have outsourced everything and need to get out of there – ideally in two weeks or one month. Can you help?"

I was astonished, and literally couldn't breathe for 30 seconds.

But I love challenges. So be it. Challenge accepted.

A fast and secret move

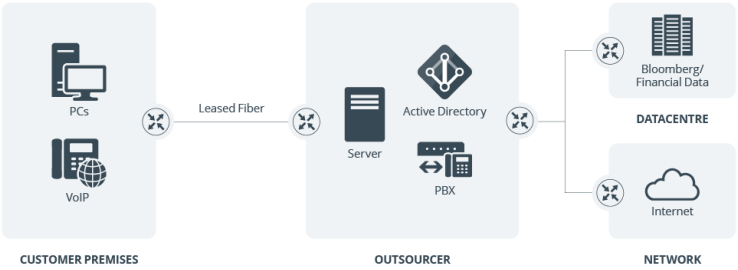
An analysis showed that the severe data breach was due to total lack of privilege management. It was also possible that an employee of the outsourcing company was bribed to copy some data. The bank had a false sense of security: the outsourcer used old firewalls with few rules, and no security was enforced inside the bank network perimeter.

The result of this event was a total loss in confidence in the outsourcing company. The

bank needed to move away as quickly as possible – without letting them know what was going on.

The big issue was that the bank had no in-house skills and no IT personnel. Everything was outsourced.

Money was not an issue – we had an almost unlimited budget – but time was a key element.



Existing bank architecture

The bank had outsourced all its IT

Everything was outsourced to a company that specialised in banks. The bank only had workstations and phones on their premises. With leased fibre lines to the outsourcer datacentres, traditional infrastructure with Microsoft Active Directory and applications as virtual machines (mostly Windows), voice over internet (VoIP) PBX on an old unsupported Avaya.

Internet access, Bloomberg and other financial data providers were only available from the outsourcer location. Workstations, phones, and all the licenses – even desktops – were rented from the outsourcer. The bank's only on-site engineering was on an on-call basis, with no real internal IT. We needed to consider these factors when we planned the migration.

The quickest way to "get out" of the outsourcer was to embrace the cloud – any hardware and datacentre colocation would have taken too long.

A phased approach for the emergency

We needed to act as quickly as possible – before the outsourcer got wind of the bank's decision.

Our top priority was secure company communication. First of all, we created an emergency internet access from the central location. We bought the quickest line we could get, with a plan to have a full redundant internet connection in one month. We immediately ordered a dedicated line to Bloomberg and the other financial data providers, while using their internet backup at the start of the project.

We created an empty virtual private cloud (VPC) on Amazon Web Services (AWS) London Region. We knew this wasn't the strongest region, but we needed to comply with regulations. We created

an Active Directory (AD) replica and started syncing the AD to Azure AD, so that we could have started creating the mailboxes on Office365.

Protect banks' confidential information

Then we migrated all the mail to Office365, along with other collaboration tools. We moved around 5TB of personal confidential files to OneDrive – and set up policies that were far more secure than the ones the bank had in place. There was no filer to maintain and files are fully replicated on the personal workstations or laptops. This carved out the main problem of protecting confidential files.

We couldn't trust the workstations because they were still managed by the outsourcer. So we added an extra workstation for the core trading and operations team but managed it through a mobile device manager. Using iPad Pros and Microsoft Surface was a great help. Windows was required at the start of the project for some applications, mostly Bloomberg terminals.

The CEO suspected that some calls were secretly wiretapped, so we moved the communication to a hosted VoIP PBX, and reused the existing ISDN phone lines, eventually porting them to VoIP.

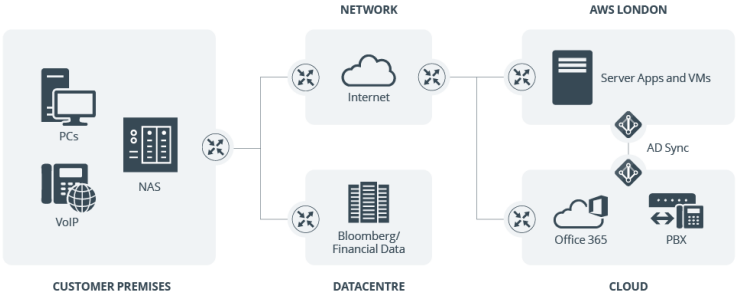
The pressure eased

We relaxed a bit as communication was secured, and bought a local network attached storage server (NAS) and started replicating the data for disaster recovery purposes, and the file archive. We shifted and lifted key VMs to AWS and reduced the number of VMs as many applications were consumed through SaaS. We secured access to the core applications through remote terminals protected by two factor authentication and geolocation. Geolocation was also enforced on Microsoft Office 365 through the use of conditional access features.

Licenses were no longer an issue: Windows licenses were provided by OEM, Office was provided though the Office365 subscription and Windows Server was provided by AWS as part of their offering.

When things were stabilised, we rebuilt the local networks and rolled out our own workstations and devices, with the brand new redundant internet connection.

Then we cut the connection with the former outsourcer.



New bank architecture after outsourcer cut-off

A two-month sprint to move the core IT

It was really hard work, but I kept my promises: I remember finishing at 5am and going back at 9am for meetings. But we produced a miracle – we moved the bank's core technology in just two weeks. It took another two months to carve out the rest of the IT. And optimising everything lasted almost one year – mostly due to contractual obligations or lead times on physical equipment.

With fewer systems to maintain, we drastically reduced the need for IT support, apart from regular management and security patching activities on AWS. Even with standard configurations, the bank's security got a big boost. The core systems were now accessed through terminal services (Citrix) and two factor authentication, without the possibility of copying or extracting data.

A nice side effect was that the bank was spending a fraction of what the outsourcer had been charging. It was a great journey and I really enjoyed the team I worked with.

The satellite operator

You remember a peculiar project where Mark Zuckerberg, the owner of FaceBook, wanted to use solar powered drones to bring the internet to emerging countries. They were supposed to fly low orbit and downstream connections to fixed stations in Africa.

Well, it turned out that it wasn't that easy. So FaceBook turned to a famous satellite broadband operator to launch satellites and cover the emerging countries. The satellite operator, which behaves in the same way a telco does, was focused on providing data to ships, airplanes, and places where no fixed or mobile data was available. They weren't ready to handle the first stage of the project – an extra 400'000 subscribers.

Scale up to availability and keep costs low

The plan was that more customers would sign up as new generation satellites with high-speed beams launched. This would mean more log data to process – about 50TB per day. And more customers would mean a bigger burden on IT operations.

The company only had 10-15 people handling operations between network and the system. They did a great job automating every single

aspect of the solution, but they weren't confident they could handle these new services.

Two projects to handle the new services

We decided to go for two projects to be able to cope with the new services.

The first project focused on customer, and partner-facing applications. The goal was to reduce the IT team's workload, increase availability of services, and keep costs low.

We moved all customer and partner-facing applications to the cloud. Customer-facing applications had been available through resellers. With the new services, the customer portal would be offered by the telco, along with a partner portal that would provision new customers.

The second project was about increasing high availability, avoiding vendor lock-in and reducing costs in the datacentre that provide physical termination of the satellite links and core services. The telco had a bad experience with the enterprise storage arm of a famous brand. An update had failed, bringing down all the virtual machines in that datacentre. The telco had to move to disaster recovery and eventually bring back the VMs once the issue was solved. No data was lost, but the telco had lost confidence in the

brand and wanted the freedom to implement their own open solution.

A savvy management

The telco was a big VMware shop, but I was lucky – the management were also Open Source enthusiasts who understood the value of automation.

They had a refreshingly sensible view on technology: use the tools that make the most sense.

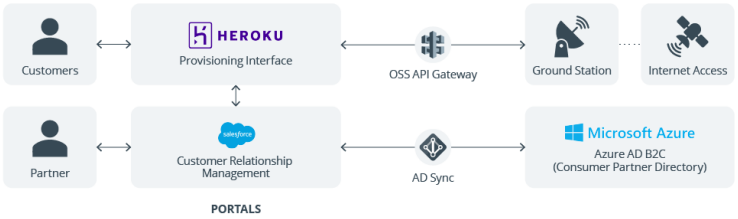
Integrating Salesforce with our solution

Salesforce was a top-management decision and something we had to live with. We evaluated providing authentication and integration services internally but decided the complexity of providing these high availability services through the two main datacentres was probably not worth the effort.

For example, we evaluated running our own identity management through the open source project Keycloak. That would have meant at least three front-ends and three mySQL master replicas. Plus maintaining availability, upgrades, and making sure we could replicate almost live in another datacentre. This looked challenging, given typical database replication problems – and

Azure AD B2C offered 50'000 users for free, and additional users for a few cents.

So we decided to go for Azure AD B2C to manage identities for consumers and partners – a no-brainer. We linked the Partner Portal, hosted by Salesforce as a Community, to the Azure AD B2C. Salesforce also uses the company corporate Azure AD to grant access to corporate users and assign proper roles.



Customer/Partner Facing Application

We more or less did the same evaluation on running the application internally or through Heroku. We chose Heroku as a platform as a service because they are owned by Salesforce and have special APIs and replication to interact with Salesforce data. We linked the consumer identities to Azure B2C.

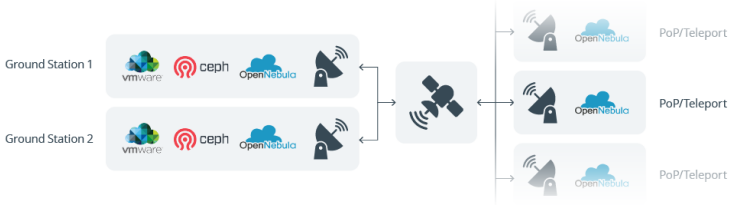
The only gateway to the local datacentres is through an operational support system (OSS) API that the internal developers made available.

Provisioning/deprovisioning of users and any modification to subscriptions will be handled on Heroku and Salesforce, and eventually propagated to the OSS systems through these APIs. These are now the only on-premise systems. This means the IT team has fewer systems to take care of and can focus on the business' critical operations support systems.

Optimising the datacentre

We're currently working on optimising the telco's datacentres. At the end of the day, satellites aren't that different from a standard national telecommunication provider: the signal's relayed through satellites instead of wires.

Instead of standard telco points of presence (POPs), teleports convert the satellite signal into a standard landline connection. This will create a geographically dispersed termination, provide extra redundancy, and retain control of the two main datacentres.



Operator new datacentres' architecture (Main Ground Stations and Teleports)

Combining VMware and open source

Up to now the telco was (and still is) a big VMware shop, with classical Storage Area Networks. But the failure during the upgrade of an enterprise storage solution, increasing license costs, and the need for better and cheaper disaster recovery, meant the telco was ready for open source ideas.

First, we decided to embrace Ceph as Software Defined Storage, which is pretty much a standard in the open source space. We used Ceph as alternate storage for VMware to work along the traditional SAN. The good thing about Ceph is that it gives you the flexibility to create your own tailored SAN, optimising it for the workload you need, with the hardware you choose. This doesn't mean you save money, because Ceph only helps you save money when you scale a lot – over a

petabyte. But Ceph gives you the unbeatable flexibility of rolling out newer hardware on-line, without any potential downtime.

With Ceph as a foundation, we rolled out OpenNebula, another open source product, as cloud infrastructure software. We can argue on OpenNebula vs OpenStack, as I was a big part of the OpenStack community, but the OpenStack project can be too complex for simple use cases. OpenNebula is perfectly fine for specific use cases.

Automated workloads and infrastructure

In this project there were two objectives. On one side, we needed to be able to roll-out repeatable workloads on the central datacentres, in virtual machines with containers orchestrated by Ansible. Using this kind of automated workload is a waste of precious licenses under VMware.

On the other side, teleports just need two hardware nodes for redundancy, which means a fairly straightforward infrastructure. For these edge deployments, OpenNebula turned out to be really flexible as we could automate the deployment of virtual machines with radio equipment software, and even create images in the central locations – an easy and cheap disaster recovery capability.

Delivering results

The telco's core issue was to reduce the pressure on internal IT. Although customer-facing applications are important, it's not the core business. Moving applications from on-premise to the cloud cut costs by 85% and reduced the IT team's workload.

On the datacentre side, Software Defined Storage through Ceph avoids any vendor lock-in. Cost is not the real factor here, as Ceph is only cost effective when you really go over 1 Petabyte of storage. But Ceph gives you the freedom to choose the hardware or perform hardware refreshes on-line. And if you're familiar with the cattle vs pets computing approach, OpenNebula is a great tool to deploy cattle-like workload – repeatable virtual machines that can easily be thrown away.

The great automation work by the telco IT team created the perfect foundation for this part of the project. As a side effect, OpenNebula brought a better disaster recovery and savings on VMware licensing.

The global manufacturer

This manufacturer is a spin-off of a larger global manufacturer with 26 factories across the globe. The parent and the breakaway company split the market segments and the new company took over five factories.

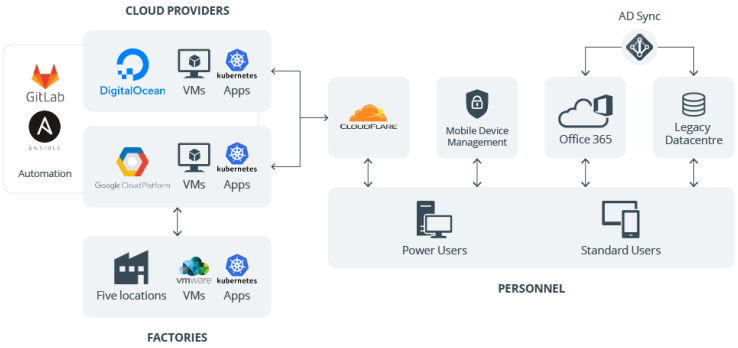
Legacy combined high cost and low service

At first the relationship was great. The parent company provided all the spin-off's IT under a two-year contract. The new company's IT manager's job was to keep the relationship with the parent company's IT team.

Then things went sour. As time passed, the parent company decided to stick to the letter of the IT contract: splitting systems, maintaining the as-is with no modifications or improvements – and no software upgrades or new projects.

To make matters worse, the parent company hosted the new company's legacy applications at an expensive datacentre – but moved its own systems to a cheaper, more effective provider. The parent also charged high fees for simple IT work and forced the new company to use expensive consulting companies.

Last but not least, when the new company decided to commission a project from the parent to provide digital services to their big customers. The parent and its consultants burned through 2 million Euros but failed to deliver the project.



A clever solution for an agile manufacturing business

Choosing the perfect combination

Many projects didn't embrace Google Cloud or Office 365. So we started synchronising the internal directory with Office 365.

This was mainly so we could move the collaboration suite, but it also established a cloud identity provider that feeds data from the local Active Directory or LDAP. A cloud identity provider is important when you want to embrace cloud

applications and ease integration with third party services and custom-developed applications.

Before we chose a cloud provider, we decided to take a close look at the SLAs for the applications we wanted to move to the cloud. We found out that DigitalOcean was granting 99.99% of uptime under their SLA, which is far more than what we need for the average intranet application. Only a few critical applications needed more, so we decided to go for Google Cloud to ensure a higher SLA, some of their tools were also closer to our philosophy than AWS.

Setting a strategy for the future

Micro-services and application containerization were key. Everything was deployed through Ansible or Kubernetes. We adopted Gitlab to create CD/CI pipelines for us and third-party contractors to build internal software that automatically deploys to the development and QA environments. Software promotion in production was still manual, to control the release cycle, but required almost zero touch.

We chose Cloudflare to protect our new dispersed infrastructure. It gives great protection through WAF and GeoFencing, as some applications are only available in given countries. With their Access solution, along with Cloud Identity management

provided by Azure, we are able to automatically protect intranet resources with little effort. We did all this at a fraction of what the parent company had charged for the poorly maintained local datacentre.

Then we started the testing phase in the factories. Our goal was to replace the old monolithic software that collects data from machines into a standard database – and build a modular microservice approach that runs on Kubernetes on VMWare.

Organisational changes were the key

This project is one of my favourites as it illustrates all the cloud adoption techniques I advocate. I was lucky to find an enlightened Head of Digital who really loved the approach, and a CEO who is willing to accept the challenge and listen to everybody. The Head of Digital and I were both lucky in that we didn't have to deal with any company politics.

In my opinion, the biggest achievement was organisational rather than technical: we deeply changed the role of IT. We created IT ambassadors in each department and fostered the internal IT community. This empowered the business to deliver their own projects and gave the IT team a way to control over mission-critical data.

Office365 and Azure AD were a great relief to the IT team. Collaboration really matters to this company, especially in the days of the Covid-19 pandemic. Fewer things to manage, and central cloud identity that can be used on all projects.

The savvy use of multi-cloud, especially when applying the right SLA strategy, helped us negotiate a datacentre spend that was 25% of what we'd budgeted. CloudFlare turned out to be around 2% of the existing solution, with better security.

We're still in an early phase of adopting bring your own device (BYOD) and commodity desktops, but it looks that they'll be much cheaper than a custom Windows build in the long run. And more reliable, with flexibility that allows for new devices.

Cloud: every journey matters

Businesses, especially in these unprecedented times, are facing budget challenges and skill shortages. The market is putting more and more pressure on the IT department to deliver projects fast with low resources.

Employees and partners should be able to access information anywhere, anytime, and with new devices to be able to compete on a global market. Up to now, traditional IT departments struggle to cope with those requirements and scale.

The savvy use of the cloud can help companies in finding a smart way to overcome these issues. On the other end, wrong decisions can lead to wasting even more time and budget, not mentioning that vendor lock-in is just around the corner. Experience is crucial: IT is a magic combination of business with technical, and project experience from a professional can add some real value.

In this publication, I shared three examples that best summarised the common patterns I found in my projects. By cherry-picking the right cloud resources, optimising the existing infrastructure, automating and embracing open-source, you'll be able to reduce costs up to 80%, reduce the

burden to the IT department and have the freedom to move your applications and data from one provider to the other. Such wise use of the cloud means negotiating better tariffs with the providers and having the side effect of disaster recovery and business continuity plan.

At the beginning of 2020, I spoke at a conference about my consulting experience, and I borrowed Transport for London's famous motto "every journey matters". I couldn't find any other catchphrase that can fit totally: every project is a unique journey.

I genuinely hope that, by sharing my experience, you can find the right path for you.

LEARNING FROM

100 CLOUD JOURNEYS

Giuseppe Paternò has worked on over 100 cloud projects and no two were exactly alike. Moving applications to the cloud is a start point for many businesses on their journey to the cloud. But every business should have its own tailored journey.

Cloud solutions can be complex and each project has to meet specific business needs and work within specific parameters. They can range from building large private clouds to moving everything to the cloud, and even implementing organisational changes.

In this paper Giuseppe set out what he learnt in 25+ years of IT, sharing three different case histories that show how every business should have its own tailored journey to the cloud. The author also shares in the publication his own six pillars for delivering successful cloud projects.

The author aims to inspire businesses in finding their own path to increase their business agility, lower or rationalise their costs and better focus on the core business.

Giuseppe is an IT infrastructure architect, security expert, and cloud solution guru with over 25 years of international experience.

His clients are companies who are either at the start of their cloud journey, or want to build their own cloud infrastructure.

He works with CEOs and board directors to make sure the business gets real long-term benefits from its IT spend. Giuseppe has worked with Deutsche Telekom, eBay, Etisalat, IBM, Pirelli, RedHat, Sun Microsystems, TomTom, Vodafone, and Volvo.

✉ info@gpaterno.com
🌐 www.gpaterno.com