Performance

Create a cloud experience your business can depend on

orange™ Business Services

Introduction

Cloud computing has become the norm for most companies. IDG's 2016 Cloud Computing survey reveals that 70% of organizations have at least one application in the cloud today[1]. Nevertheless, using the cloud as a platform to enable business-wide digital transformation presents several organizational and technical challenges.

Enterprises often find the promise of low-cost public cloud services is elusive when they layer on the data privacy, security and application performance capabilities that are necessary to ensure regulatory compliance and deliver the desired end-user experience.

Discrete cloud application deployments are a good way for IT teams to build expertise. But to truly make cloud computing part of their DNA, enterprises need to be able to integrate business and data workflows across multiple cloud environments.

This Orange Business Services ebook outlines best practices that enterprises can adopt when moving applications and workflows to the cloud.

We look at how to overcome six key challenges in cloud projects, including:

- **Defining your multi-cloud strategy** (page 3)
- **Ensuring you have the skills to handle a cloud migration** (page 5)
- **Creating a great end-user experience in a cloud environment** (page 7)
- **Protecting data in compliance with multiple regulations** (page 9)
- **Managing cloud service levels** (page 11)
- **Controlling the total costs of cloud** (page 13)

Defining your multi-cloud strategy

Challenge

The first step in any cloud strategy is deciding on the most appropriate cloud model to adopt – software as a service (SaaS), platform as a service (PaaS) or infrastructure as a service (IaaS) – and how it is delivered – private, public or hybrid – for each application workload. The choice of model is based on several factors:

- **Financial considerations:** what is the total the cost of ownership of the end-to-end cloud service and data lifecycle? Think about the choice, suitability, and granularity of different charging models.
- **Functional and service level requirements:** which features and services do you need? Consider the volume of traffic you expect and the service level agreements and objectives (SLAs/SLOs) required.
- **Data security and privacy regulatory compliance:** how should you protect customer and employee data, keep valuable intellectual property secure, and comply with regulatory requirements?

Multi-cloud has become the dominant IT transformation strategy to meet these goals according to industry analysts. It involves the use of multiple cloud models to meet the diverse range of business needs in an organization. A hybrid cloud uses a mix of on-premises, private cloud and third-party, public cloud services with orchestration between the two platforms. It empowers IT to be a broker of cloud services, providing the control and visibility they need and the on-demand self-service capabilities that developers and application users expect.

Why adopt a multi-cloud strategy?

A multi-cloud strategy enables:

- **Choice:** allows multiple cloud models and applications, eliminating the need to be tied to a single provider and easing data sovereignty and security compliance challenges
- **Cost savings:** by consolidating IT workloads onto virtualized servers and using cloud solutions at different pricing tiers you can meet a diversity of business, security and performance needs
- **Flexibility:** inter-cloud data flows to support multiple business functions
- **Resiliency:** use multiple cloud providers to prevent single points of failure

Match workloads to cloud services and accommodate line-of-business procurement preferences, along with merger and acquisition needs.

It's important to design cloud infrastructure with flexibility in mind so that they can grow to support new digital initiatives, such as big data analytics and IoT platforms, which will impose new infrastructure requirements.

Map application workloads to the right cloud model

Minimize costs
A public cloud is ideally suited to standardized, itinerant or highly variable demand-based applications. It's a good choice for adding incremental capacity during peak times and it delivers low upfront costs.

Data privacy, security and regulatory compliance
A private cloud provides more specific security controls and can be customized to enterprise policies, operational procedures and regional needs. Most enterprises adopt a private cloud to meet data privacy or regulatory needs for a specific application. Having this resource on tap for future use cases is beneficial to the business to increase agility.

After making this initial investment, IT teams need to maximize private cloud's utilization with other applications to realize its full benefits. A hybrid cloud provides the best of both worlds, allowing data processing in a public cloud and storage in a private cloud.

Data traffic volumes
If an application generates a lot of traffic or data needs to be encrypted, the WAN bandwidth costs and performance risks of a public cloud are likely to be high. However, some public cloud providers offer low-network latency solutions at a higher cost that may be suitable for your needs.

Reversibility
The potential complexity and costs of retrieving your business data from any chosen cloud service provider needs to be considered. This is a point often overlooked at the time of planning a migration to cloud. For some public cloud platforms, these costs can be considerable.

Maintaining existing IT standards
If similar server, storage, and/or data protection platforms are used in your legacy platform and the proposed cloud model, fewer application architecture and configuration changes will be required. A private cloud may be preferable to reduce migration risks.

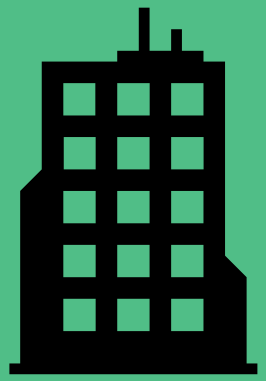
Ensuring you have the skills to handle a cloud migration

Challenge

Migrating applications is a key step in your cloud journey. Enterprises need to know what changes in the application architecture are needed and how to ensure the continuity of IT services during the change-over process.

Many applications are cloud-ready. But legacy applications are still widely used and remain essential for mission-critical business processes. They may not support x86-based shared resource environments used in the cloud and they often run on older operating systems. Bespoke software may have been developed using code that is difficult to re-architect. In many cases, the original developers have left, documentation may be poor and the risk of change uncertain.

This makes legacy applications difficult to update. It can also increase maintenance costs as it is uneconomic for vendors to support applications with few customers. For such cases, a skilled team is essential to support an effective cloud migration plan.



37%

of companies worry that they lack the right skill sets to manage cloud environments and derive the maximum benefits from them according to an IDG survey.[3]

Five must-have application migration skills

Role	Responsibilities
1. Architect	Collaborates with other IT functions to drive an effective cloud migration roadmap, overseeing infrastructure, data storage and security requirements.
2. Transition manager	Co-ordinates the cloud transformation project, minimizing downtime for business critical applications.
3. Application and data manager	Provides in-depth knowledge of the applications intended for use and advise on ETL (Extract, Transform and Load) data warehousing tasks.
4. Migration specialist	Selects the tools to migrate unstructured and structured application data and virtual machine images securely and undertakes data format conversions if required. This expert assesses whether to migrate applications online to avoid downtime or offline with an initial data copy and delta synchronization later – the pre-copy process – which is less risky.
5. Project manager	Manages the migration, assessing how long it will take to migrate data with the bandwidth that is available, and dealing with complexity of bandwidth-heavy applications that are sensitive to network latency.

Four steps for migrating applications safely to the cloud

1. **Know your assets:** use an asset management database to determine the scope of your application portfolio, the version numbers and configuration details.
2. **Prioritize:** understand the application-to-application data flows and any privacy and security implications, as well as the business impact of downtime. Move non-critical applications first, focusing on those with fewer connections to third-party applications. Use in-flight data encryption where required.
3. **Choose your migration method:** this depends upon the application or database tolerance for downtime, the size and complexity of the database, and the bandwidth of the connection to the cloud.
4. **Consider transformation:** legacy applications may need to be re-architected or completely rewritten to support a cloud environment.

Adapting quickly when migrating applications

Orange works with a healthcare provider, which was hosting sensitive patient information in-house in a database. This data is used to map required medical services against a database of providers.

Maintaining this legacy application took up the majority of the enterprise's IT budget, especially as different versions were in use in different regions. Orange helped the company to consolidate the application and retire older versions by identifying data workloads and flows before planning and executing the right cloud migration path.

Along the way, Orange found elements of the solution that wouldn't function well in a cloud environment. It moved these to Orange's cloud facility, eliminating the management overhead and freeing up availability in the customer's datacenter.

"Companies undertaking a cloud transformation program need a diverse range of skills in place."

Creating a great end-user experience in a cloud environment

Challenge

In the legacy world, applications are often distributed across multiple servers on a global basis to minimize network latency, which is determined by the distance to the user. In contrast, most cloud applications are implemented as a single active global instance, closest to where the majority of employees are based.

This means employees further away from these locations can experience long delays waiting for SaaS solutions to load data or save updates, in addition to systems that freeze or crash. For enterprises that depend on effective information flows to thrive, this is clearly unacceptable.

Most enterprises will combine multiple cloud connectivity options, balancing performance, reliability, security and cost constraints to overcome this challenge. In each case, the network needs to be adequately designed, provisioned, implemented and performance managed.

Technologies to improve the cloud application experience

Existing local internet connections to the global highways are not good enough for most cloud usage scenarios as performance varies by time of day, depending on unmanageable issues such as local usage conditions and the level of contention.

There are a range of different technologies that can help you improve your cloud application experience.

Distributed internet access
The use of local internet access at the branch site is typically selected where SLA needs are moderate, the user base and SaaS provider are based in a single country, and the local internet infrastructure is robust.

Distributed internet access with enhanced backbone
It's also possible to use a variety of enhanced internet services to improve performance by controlling the paths taken and caching the traffic.

Cloud interconnect services
A cloud interconnect service eliminates the variable performance of the internet and allows IT teams to prioritize key applications to receive a higher quality of service (QoS).

Direct connectivity to the SaaS provider
For bandwidth-heavy applications that are sensitive to network latency, cloud providers offer dedicated network connections, which are more expensive.

Traffic optimization
Virtualized or on-premise optimization software de-duplicates and compresses data sent over wide area network (WAN) links, minimizing congestion by reducing the amount of data that must be transferred.

Four steps to optimizing cloud application performance

1. Model anticipated usage
Use a bandwidth modelling tool that takes into account usage patterns for various categories of users, typical file sizes and peak usage times.

2. Choose your connectivity per application and category of user
Address latency, packet loss and network reliability through your choice of connectivity and how you configure any optimization tools that are required. In some situations, it's possible to deploy a SaaS application in hybrid mode with some components hosted globally and others in your own datacenters or with a third-party provider to overcome performance and security issues. A managed service provider can guide you through the best combination of options to meet your needs.

3. Think about hard-to-reach places
In some parts of the world, the internet may suffer consistently poor performance due to government filtering of content. A private WAN connection may be your best option here. Bandwidth may be unavoidably constrained for remote workers using cellular or satellite links or because it is expensive. WAN optimization can dramatically reduce band-width requirements.

4. Measure the user experience
Service teams shouldn't wait for helpdesk complaints to tell them employees are suffering cloud application performance problems. Network performance and application performance monitoring (NPM/APM) technologies are useful both for capacity management and troubleshooting. Together with client level tools, they enable you to observe actual performance for individual cloud users, including packet loss, and provide an enterprise-wide quality dashboard.

Optimizing application performance at peak times

Every success brings a new challenge. Lane Crawford, a Chinese retailer selling designer label luxury goods, had been experiencing a strong growth in online sales. But it faced problems scaling its Oracle retail management system during major annual sales events.

Orange migrated the solution onto a highly scalable Orange cloud service, adding performance optimization. The implementation team used a workload generator to test the system against projected workflows. Pleased with the result, the customer later migrated further ecommerce modules into Orange's cloud service.

"Ensuring high levels of cloud application performance is key to ensure employee productivity and customer satisfaction."

€608k

Large European organizations lose €608,000 every year due to performance-related problems with cloud-based applications.[4]

Protecting data in compliance with multiple regulations

Challenge

Companies face a dual challenge when addressing risk. Attackers are becoming increasingly aggressive in their pursuit of enterprise data, while security regulations are growing more stringent. These dangers, along with the potential fallout if companies get it wrong, make security one of the biggest cloud challenges.

Companies need to adopt a proactive cybersecurity and compliance program to protect employee, customer and business data stored in the cloud.

53%

Security tops the list of cloud computing concerns for 53% of decision makers.[5]

Four security and compliance challenges in the cloud

1. Jurisdictional issues
Countries across the world – from Australia to Russia and France to China – have imposed strict data protection regulations. Many governments require companies to store personal information about their residents within their borders.

2. Sector-specific requirements
Regulations also vary by industry vertical. Healthcare organizations face strict data privacy mandates, while retailers must contend with constantly-evolving credit card processing rules under the PCI-DSS standard.

3. General Data Protection Regulation (GDPR)
Any company that employs staff in the EU or handles data on citizens from the region will need to comply with GDPR. Coming into effect in May 2018, it imposes strict penalties with fines of up to €20 million or 4% of global revenue for violations, whichever is greater.

4. Rising security incident volumes
Enterprises are collecting and storing more system usage data than ever before. This makes spotting security incidents difficult for cybersecurity teams without the right solutions to help them.

Building a secure cloud environment

Encrypt what's important to you
Assess how data needs to be locked, unlocked, and moved around. Manage encryption keys effectively and make sure your cloud service provider does not have access to them. More secure connectivity options will be important for business-critical customer or financial data.

Manage cloud access
Use two-factor authentication and enforce the use of a strong password at all times on all devices. Restrict access to people who need it and ban shared accounts. Assess IP addresses and maintain audit trails as part of your policy enforcement process. You may wish to isolate cloud instances that store highly-sensitive data.

Focus on threat prevention and detection
A security operations center (SOC) provides the specialist expertise you need to monitor your entire cloud environment. This includes server activity, user activity, device activity and data in motion. Powered by a security information and event management (SIEM) system and advanced analytics tools, the SOC enables you to spot patterns in network traffic and mitigate threats before they can do damage.

Prepare for threat remediation
Organizations need a fast and effective incident response plan in response to successful attacks. Avoid fragmented cloud security monitoring and responsibility across your application, platform, network and device layers.

Source skills appropriately
With cybersecurity skills in high demand and a fast-evolving threat landscape, companies may need to turn to a third party with expertise in threat management to help protect themselves.

Enforce contractual obligations
It's important to embed the right contractual clauses into your agreements with your cloud service providers. Enterprises have a responsibility to ensure their suppliers are meeting their data privacy and security legal obligations in many jurisdictions.

Using private cloud for sensitive information

The European Space Agency has stricter security requirements than most. The organization deals with highly sensitive data. Orange implemented a private cloud for the ESA, including role-based access control to help protect the organization from account misuse.

"Some governments require companies to store personal information about their citizens within their borders in compliance with strict guidelines."

Managing cloud service levels

Challenge

Enterprises often need to manage a range of cloud and traditional IT services. They must ensure diverse service level agreements (SLA) are met, including service availability, service restoration, system utilization and application response times.

Change management is crucial. In the past, companies faced periodic reorganizations and technology upgrades. Today, they live in a digital era where technology platforms are in a continuous state of renewal and iterative, agile ways of working are key.

For successful service management, formal management change boards – supported by rigorous procedures – are essential.

Four steps to effective cloud IT service management

1. Set your metrics
Real-time monitoring tells enterprises what is happening with their applications right now. Are they up and running? How close is the enterprise to saturation level when performance starts to degrade significantly?

Historical and real-time performance metrics are vital to understand how applications perform over time and solve complex performance interactions. This enables proactive steps to be taken to prevent service incidents.

2. Manage your services
It's important to be able to capture and correlate service and infrastructure events across multiple tools. An IT service management framework enables IT teams to:

- Schedule cloud deployments, upgrades and data replication activities.
- Manage and monitor OS, applications and middleware, as well as cloud compute, storage, and network resources and orchestrate inter-cloud workloads and load balancing.
- Secure data by enforcing security policies and providing alerts.

3. Adapt to a world of continuous change
A change advisory board assesses, approves and schedules changes to the IT infrastructure. It reduces the risks with formal risk reviews, assessments, and mitigation processes for all planned changes, looking at the potential impact on business services.

A change catalog is a documented list of changes that have a history of success. It provides controlled, repeatable, and auditable service processes.

4. Enhance self-service and automation
You need to be able to automatically provision and configure cloud services and manage costs. Automation is also critical to remediate service issues more quickly. This reduces the manual workload on the IT team and reduces the risk of human error.

Building a reliable and robust cloud-based service

Enhance visibility
Ensure you have a single and comprehensive system of record for your cloud and traditional IT services and infrastructure to create an effective service management framework.

Enhance interlocks
Manage end-to-end cloud services, rather than technology silos. The enterprise and service provider need to work together in unison to achieve this goal.

Maximize operational agility
Automate and accelerate remediation, improving governance and enhancing self-service.

Use a continuous improvement process
Continuously adapt the service delivery and support model to the fast changing cloud technologies.

Capacity management for mergers and acquisitions

Orange works with an enterprise that is aggressive in acquiring other companies to drive global growth. The customer's IT team was experiencing capacity planning challenges. It wasn't able to anticipate the IT resources that newly acquired employees would need and integrate additional software applications into its portfolio post-acquisition.

By working with Orange to develop its capacity planning skills, the customer was able to anticipate these requirements earlier and begin the procurement processes to scale its highly customized private cloud without any service disruptions.

56%

of companies using cloud are relying on multiple SaaS vendors today according to private equity firm North Bridge.[6]

"Design cloud infrastructure with flexibility in mind so that they can grow to support new projects."

Controlling the total costs of cloud

Challenge

A cloud strategy is often the foundation for digital transformation. Moving to the cloud can deliver savings compared on a like-for-like basis with legacy IT systems. However other activities rolled up in digital transformation can often make this difficult to measure.

Companies pursue cloud projects to shed capital and management expenses. But if they don't fully assess their end-to-end data migration, cloud application performance and security needs, they end up with some nasty surprises.

42%

of companies view lower total cost of ownership as a driver for cloud computing projects according to IDG.[7]

Five tips to maximize ROI for cloud computing projects

1. Project costs
Encourage experimentation and then fully adopt solutions that deliver real business benefits. Prioritize features that matter most, define your architectural prescriptions, and recycle successful cloud deployments for new projects.

2. Infrastructure overheads
Decommission cloud development and test environments when they are not needed to right-size your infrastructure, in addition to any non-cloud environments. The cost of maintaining legacy IT systems and fixing flaws can then be eliminated.

Select storage with "just good enough" performance for the task at hand. If you need to batch process non-business critical data, use low-cost commodity cloud storage. Whereas, real-time analytics workloads require more expensive high-capacity, low-latency data processing resources. Data that streams non-stop may be better processed locally. Virtualization enables mixed workloads to run on the same infrastructure, minimizing costs.

Compare the cost of protecting or regenerating data. While source data needs to be protected in a more secure, higher cost environment, post-processed data can be reproduced inexpensively by re-running the process. Move inactive data to a lower-cost archive infrastructure.

3. Migration costs
Using the cloud provider's import/export service to transfer large amounts of data across the Internet can be time and cost prohibitive. Temporarily using higher price connectivity to migrate large databases allows you to reduce the migration time – which means less application downtime and lower network usage charges.

4. Skills
Work with a seasoned service provider. They can provide insights into the end-to-end capabilities that are required to deliver a positive cloud experience, from the application migration all the way through to connectivity provisioning.

Use pilot projects. They enable design and deployment teams to practice migrating select IT services to the cloud. Retrain some infrastructure managers as service managers to manage cloud provider performance.

5. Consumption
Ensure accountability by creating workflows that balance user flexibility with cost management in a service culture. Chargeback mechanisms are a good way to make business departments accountable for what they use.

Enforce a cloud-first policy for new applications wherever possible to get benefits of working at scale. Discourage too many exceptions to reduce the complexity of managing multiple environments. Using "eligibility criteria" should help this decision-making.

Reduce routine configuration costs using a self-service portal and automation.

Bringing third party expertise to bear

Cloud service contracts often involve shared responsibility between the cloud service provider and the enterprise. One enterprise wanted to manage its own operating system, applications and middleware on top of infrastructure provided by Orange. It suffered application performance problems with a lag in response times for online users. This looked like a networking problem, but in reality, things were more complex.

Orange troubleshooters found the cause of the problem: the customer's antivirus update procedure was running at the same time as peak server usage for data processing in the cloud. The antivirus solution was quickly reconfigured and employees found opening the application and saving data was fast and efficient.

This avoided unnecessary spending upgrading connectivity, helping to minimize the end-to-end cloud costs.

"Pilot projects provide a practice mechanism for design and deployment teams by migrating select IT services to the cloud."

Take action now

Cloud is no longer an *if* but *how fast* for most organizations. Enterprises today want to adopt multi-cloud services to remain competitive, but need to overcome a range of technical hurdles along the way and balance business needs and costs.

A trusted service provider like Orange Business Services, with the ability to offer end-to-end cloud services, global coverage and security expertise can provide the integrated solution that enterprises need.

A cloud experience you can depend on

Accelerate your digital transformation with better end-to-end control over legacy and cloud application lifecycles, performance and security.

Explore the potential of Orange Cloud for Business:
http://www.orange-business.com/en/cloud-computing

From inspiration to transformation. Together.

Let's bring your business ambition to life – with our human-centric approach, multi-vendor partnerships and global deployment resources.

http://www.orange-business.com/en/digital-transformation

Sources:
1. https://www.idgenterprise.com/resource/research/2016-idg-enterprise-cloud-computing-survey
2. http://www.idc.com/getdoc.jsp?containerId=prUS42464417
3. https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#download&from_embed
4. http://www.cbronline.com/news/mobility/security/cloud-performance-issues-costing-firms-600000-a-year-survey/
5. http://www.businesswire.com/news/home/20160517005583/en/Report-Reveals-Cloud-Security-Concerns-Rise-Investment
6. https://www.slideshare.net/North_Bridge/2016-future-of-cloud-computing-study
7. https://www.scribd.com/document/329518100/IDG-Enterprise-2016-Cloud-Computing-Survey#download&from_embed

For more information, contact info.cloud@orange.com

orange™ Business Services