What is Multi-Cloud?

Benefits

∙ Picking the Right Tools for the job
∙ Avoiding Vendor Lock-in
∙ Better Protection from DDoS Attacks
∙ Data Management

Choosing Between Different Cloud Providers

∙ Make use of Independent Industry Advice and Standards
∙ Vendor Performance
∙ Vendor Lock-in

Considering Cloud Service Models

∙ SaaS
∙ Building a Hosting Environment

Putting it all Together: What does a Cloud Management Platform do?

∙ General Services
∙ Service Management
∙ Financial Management
∙ Resource Management
∙ Governance and Policy
∙ Security

Conclusion: Use the Right Tool for the Job
At its most basic, multi-cloud describes an environment formed from two or more cloud computing services. No single provider offers the solution to completely satisfy a customer’s needs, so developers often look to several cloud service providers to build in further redundancy or maximise processing power. This also eliminates over-reliance on one vendor, enabling greater flexibility throughout an enterprise environment.

Multi-cloud is often confused with hybrid cloud, but there are two key differences. Firstly, the elements of a hybrid environment usually work together, while in multi-cloud different clouds are used for different tasks. Data and processes interact extensively in a hybrid cloud – in a multi-cloud usage is more contained to each independent cloud.

Secondly, multi-cloud always comprises several public clouds and can also include virtual and physical infrastructure, including private clouds. Hybrid, however, is always formed of both private and public.

So far, most multi-cloud approaches have investigated the IaaS layer, overlooking the rest of the cloud stack. However, an increasing number of powerful SaaS and PaaS configurations are beginning to emerge.

Multi-cloud is set for explosive growth over the next few years. According to MarketsandMarkets, the multi-cloud management market size is expected to expand to USD 4,492.7 million by 2022 (from USD 1,169.5 million in 2017). And a recent study from analyst firm 451 Research also suggests the future of IT is hybrid and multi-cloud, with 69% of respondents planning to have some form of multi-cloud environment by 2019.
Benefits

The four main benefits of adopting multi-cloud are:

1. Picking the Right Tools for the job

Businesses are starting to withdraw from “one-size-fits-all” software solutions. Usually built by the big vendors, these tools still have their place (and a large market share) but are, ultimately, generalist solutions which compromise in various areas.

Companies now want specific technologies to help them get the best from each area of their business. For example, while high performance might be crucial for one application, another – one processing strictly-regulated confidential data, say – might need a cloud service that runs in a specific region. These requirements could be met by the applications running on different IaaS platforms – each one catering to a particular need.

Multi-cloud is becoming increasingly popular because it provides organisations with the ability to merge different best-of-breed platforms together, forming one powerful overall solution.

2. Avoiding Vendor Lock-In

One of the big advantages of multi-cloud is that you can avoid being tied to the specific standards, protocols, and tools of one vendor. In fact, multi-cloud fosters a more agnostic way of building software, as the fundamental infrastructure is typically kept independent of the application software stack.

Reducing dependency on one provider puts you in a much stronger position to act if, say, a vendor suddenly pushes up prices or stops meeting the uptime levels you need.

Cloud computing evolves quickly, so the ability to respond to market fluctuations is vital. And businesses that aren’t tied to a specific vendor can adapt their strategy in response to industry changes much more quickly, since they don’t have to re-architect their entire infrastructure.
3. Better Protection from DDoS Attacks

If all the resources powering your applications are housed on one cloud, a DDoS attack can not only take those applications down but keep them down. And, according to ITIC, an hour of downtime costs more than $100,00 for 98% of organisations.

With multi-cloud architecture powering your applications, even if one cloud is compromised, others remain available to manage the load until the service recovers.

4. Data Management

You probably know that “not all data is created equal”. While some parcels might be part of computations 100 times a day for a year, others will just sit in a database for their entire lifecycle. By sharing data across multiple clouds, you can use the best service for each function.

For example, your HR or legal department might need to store huge volumes of sensitive records but not actually process the data. Security features will be key in the storage of this data. However, when data needs to be uploaded, examined, and downloaded back to a local intranet, processing power and speed are crucial. A cloud provider that caters for this, more than your IT’s security system, is a valuable ally.
Choosing Between Different Cloud Providers

When evaluating different vendors, there are three things to bear in mind:
1. Independent industry advice and standards
2. Vendor performance
3. The risk of vendor lock-in

Every cloud provider has different strengths, and understanding them can help you choose the best tools for the job.

Gartner provides one example of worthwhile industry analysis with their Magic Quadrant and Critical Capabilities services.

For example, the below represented the status of the PaaS market in 2016:

Source: Gartner
Unsurprisingly, Microsoft and Salesforce were shown to be leading the way. Analysing the cluster of visionaries is more interesting – here’s an extract from the Gartner Magic Quadrant report:

In the PaaS market, the visionary vendors include many of the classic enterprise software vendors as they invest to reinvent themselves for the next generation of application developers. Generally, visionary vendors are investing in leading-edge enterprise aPaaS services not yet readily adopted by mainstream enterprise customers; thereby adding support for capabilities such as big data and stream analytics, IoT, event-driven and in-memory platforms, and offline mobile computing. Other Visionaries excel in understanding enterprise demands on the road to cloud adoption and support: high productivity for LOB users; polyglot high-control and continuous integration/continuous delivery (CI/CD) through containers for IT developers; integration, orchestration and API management for composite application services; and self-service management for hybrid application deployments.

Critical Capabilities reports complement Magic Quadrants by providing deeper independent insight into a vendor’s product and service offerings, which can be compared against a set of critical differentiators. You can also compare products and services based on the specific use cases needed by your business.

Industry standards can provide added confidence when evaluating different vendors. The following are most likely to be useful:

- **ISO/IEC 27017:2015**: This is a code of practice for information security controls applicable to the provision and use of cloud services.

- **The Cloud Data Management Interface (CDMI)**: This is a SNIA standard that specifies a protocol for self-provisioning, administering, and accessing cloud storage. It defines the functional interface that applications will use to create, retrieve, update and delete data elements from the cloud.
2. Vendor Performance

It’s a good idea to seek information about vendors’ past availability and platform performance levels when beginning procurement. And service level agreements and compensation levels for service downtime are an essential part of any contract. The performance level of the company itself is also important, since any provider that goes bankrupt or gets acquired will substantially disrupt their customers’ businesses. So it’s a good idea to obtain information about the company’s ownership and audited financial statements.

3. Vendor Lock-in

As mentioned, not being tied to a specific vendor is a powerful benefit of multi-cloud, but some contracts can make flexibility hard to achieve. To ensure you don’t find yourself locked in, consider the following questions when evaluating providers:

- What happens if you need to move provider – is there a migration service or any support?
- Exactly how will company data be stored, used, backed up, and how can it be extracted?
- Does the vendor have a data extraction utility, and what formats does it support?
- What will be the cost of data transfer?

These are all areas that can reveal whether there’s a high risk of lock-in with any vendor.
Multi-cloud environments are generally composed of some, or all, of the following elements:

- The main three cloud service models:
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
  - Infrastructure as a service
- On-premises environments

After we’ve looked at how to approach the question of SaaS adoption, we’ll consider the alternative – building a hosting environment (as PaaS, IaaS or on-premises). As there are so many ways in which software can be installed on a hosting environment, rather than skim over technical pros and cons, we focus on the risks that come with each choice. This is the line of inquiry used in a paper by ICAEW: Cloud adoption: a risk-based approach to choosing a cloud platform.

**SaaS**

The decision of whether to adopt SaaS can be divided into two phases:

1. Does the SaaS provider and platform meet the due diligence requirements of your business?
2. Are there strategic or commercial benefits that would be lost by adopting SaaS?

---

**Due Diligence Requirements**

To mitigate the risk of software lock-in, ask yourself the following when considering SaaS:

- Is it possible to trial the service before committing to a contract?
- Is migrating data to other platforms feasible, or will it be stored in a supplier-specific format?
- Does the vendor offer a private version of the software in case you want to adopt an on-premises instance?

Check the following data security issues:

- If the provider has responsibility for backing up data, how often do they do it, how quickly can it be restored, and where is it backed up?
- What SLAs are in place for data loss or periods of software inaccessibility?
- Is there any insurance in place for cyber-attacks?

Finally, think about business continuity and disaster recovery:

- How long could you potentially go without access to the software before it becomes a critical issue for your business?
- If data is compromised or lost completely, how long will it take to rebuild data sets and at what cost?
Strategic and commercial considerations

SaaS applications can’t be customised, which can substantially weaken how much a company can leverage its USP or competitive advantage. As noted by ICAEW:

*Software that is revenue-generating is often customised in some way to gain a competitive advantage. If all businesses use the same software there will be little differentiation in the experience, which means they can only compete by dropping prices (and lowering margins), or increasing service (which usually results in dropping margins). If software is key to revenue generation, many companies will continually refine their software to provide efficiencies that give them an edge that allows them to compete on price or service without sacrificing their margins.*

One of the biggest problems with SaaS is that it’s just not practical for businesses that require full, simple integration to their active directory and domains, and integration with other systems (e.g. a CRM system that links to an order system, finance, customer records etc).

Since most software is not ‘standalone’ within a company and will need to synchronise with other programs and applications, SaaS offerings that can’t closely integrate with internal systems are often an unrealistic long-term solution.

Of course, interacting with SaaS applications via API lookups can be an option, but this isn’t always possible. And performing bespoke development costs time and usually money, especially when a new version of the SaaS tool is released, meaning the work has to be potentially amended or redone.
**Building a Hosting Environment**

If the following is true, a SaaS solution is a probably a good fit:

- A SaaS model exists for the software in question
- It passes the due diligence of your organisation
- There aren’t significant commercial or strategic benefits from controlling the application on your own hosting platform

However, when the answer is ‘no’ to any of the above points, a hosting environment becomes the better option.

The adoption of cloud services is essentially an outsourcing decision, in which a business figures out the assets they are able/willing to manage themselves and which will rest with a cloud provider:

<table>
<thead>
<tr>
<th>On Premises</th>
<th>IaaS</th>
<th>PaaS</th>
<th>SaaS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
<td>Applications</td>
</tr>
<tr>
<td>Data</td>
<td>Data</td>
<td>Data</td>
<td>Data</td>
</tr>
<tr>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
<td>Runtime</td>
</tr>
<tr>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
<td>Middleware</td>
</tr>
<tr>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
<td>O/S</td>
</tr>
<tr>
<td>Virtualisation</td>
<td>Virtualisation</td>
<td>Virtualisation</td>
<td>Virtualisation</td>
</tr>
<tr>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
<td>Servers</td>
</tr>
<tr>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
<td>Storage</td>
</tr>
<tr>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
<td>Networking</td>
</tr>
</tbody>
</table>

Source: hanussoftware
What Does a Cloud Management Platform do?

A cloud management platform (CMP) is a technical cloud broker that can evaluate the variety of available cloud service options. It simplifies management, enables visibility and optimises resource-usage in a multi-cloud environment.

The Cloud Standards Customer Council splits the functional capabilities of a CMP into six categories:

1. General Services

CMPs need to integrate with both dedicated and on-premises private clouds, as well as existing enterprise systems, and public cloud platforms. They include a self-service interface, which caters for a variety of different user needs. Gartner gives the following two examples:

1. Some users will need a clearly defined, finite set of services drawn from a service catalogue. This user group might be infrastructure and operations staff that need to provision IaaS resources.

2. Other users will require a service interface that lets them interact with native capabilities within a public cloud platform. They might be software developers that need to utilise a full suite of public cloud services.

2. Service Management

Service management is the end-to-end monitoring of the application to check that agreed availability and performance service levels are achieved. Areas for monitoring include business logic, the user interface, and data persistence. CMPs assess the capacity levels of storage, memory, and CPU to optimise private and public cloud workload placement.

3. Financial Management

The metering functionality in a CMP monitors consumption of cloud resources and displays service usage statistics. Consumption-based invoicing can then be produced.

Extensive analysis and reporting is often possible in CMPs to enable budgeting and the optimisation of cloud expenses. Many tools have forecasting features, whereby techniques such as “what-if” analysis can determine the cost implications of scaling deployed resources up or down.
4. Resource Management

CMPs should be able to display how virtual resources (e.g. servers, applications, and storage) are being used in both private and public cloud environments and provide an accurate inventory. They should support the provisioning and management of cloud resources from a single portal (usually via API connections).

Service blueprinting can rapidly accelerate network design via templates that have fully supported, vendor-validated blueprints and designs. It also offers the ability to quickly swap out or upgrade assets to right-size the environment.

With the amount of infrastructure required for multi-cloud, CMP solutions should include a control panel for corporate asset management. This allows IT teams to catalogue and manage hundreds to thousands of assets, potentially across the world. The platform should also include change management processes, user permissions and reporting capabilities.

5. Governance and Policy

A key function of cloud management platforms is to enable governance and enforce policies aligned to the business. The Cloud Standards Customer Council gives three examples:

- These policies can range from preventing the porting of confidential data to a public cloud to limiting the purchase options (on-demand, reserved, spot) for test servers to applying quotas for project spend and geographic placement of infrastructure and information.

6. Security

Security features within cloud management platforms themselves tend to be fairly limited. Instead, they connect with existing Active Directories or security systems built from, for example SAML (Security Assertion Markup Language).

CMPs also need to manage the encryption and cryptographic keys of the connected cloud services. Finally, CMPS provide role-based access control, with the appropriate privileges for developers, administrators, managers, etc.
Conclusion

Use the Right Tool for the Job

You don’t use a screwdriver to hammer nails, and you don’t use a hammer to drive in screws. Multi-cloud enables you to pick the right platform for each application to be run in the business, then link the data between them securely.

Software API development allows for communication between applications, and the development of secure network links between platforms allows for the secure, encrypted and low-latency transmission between platforms and networks.

Multi-cloud:
- Avoids vendor lock in
- Provides options for supplier, network, and platform redundancy
- Lowers cost
- Ensures applications are housed on the most suitable environment
To find out more about how Happi can support your technology needs during a digital transformation, try the world’s first IaaS tool for free.

happi

Happi stands for ‘Highly Automated Procurement and Provisioning of Infrastructure’. It’s a visual composer and marketplace for finding and deploying your hosting environment. With the world’s first true IaaS tool, Happi users can design, buy, and deploy hosted infrastructure anywhere in the world. Completely free to use, Happi is ready and waiting to revolutionise your infrastructure provisioning.