Real Life Cloud: moving a service to a cloud provider

Authors

Glenn Wearen, Anna Wilson
HEAnet, 5 George's Dock, IFSC, Dublin 1

Abstract

How do you move a service to the cloud? What problems do you face?

HEAnet recently started moving some of its long standing services from our own infrastructure to cloud providers. It's a bigger deal than it sounds - we're really familiar with running our own servers, so we're really used to having that sort of control. When you embrace elastic and ephemeral infrastructure, a lot of things change.

Elastic is building your infrastructure so that it can stretch and shrink to fit your needs in the moment. Instead of buying the biggest server you could ever possibly need, you split your service across many instances, adding more (and, more importantly, paying for them) only when they're needed.

Ephemeral is the flip side of that; in order to take advantage of elastic computing, your service needs to be ready for any single part of it to disappear at a moment's notice.

That's not usually how we work in NRENs, where reliability is foremost of our concerns.

Those are the direct changes. But there are lots of indirect changes that arise from using cloud infrastructure that aren't immediately obvious. For example, we usually control our spending on infrastructure by making sure that every purchase order for a server has to be signed off. When buying a server is done by an operator clicking a button — or even worse, an automated script triggering an event — how do we keep track of that? Can we even tell which project is spending what amount?

In 2017, HEAnet moved an Identity Provider service to a cloud provider. We chose it because it requires some compute, some custom networking, good communication between the cloud and the site (with graceful failover when that breaks) and the careful protection of some sensitive data. So it's a pretty good exemplar for other services that might move.

We ran into a lot of interesting issues on the way, and they weren't where we expected them to be. Spinning up some virtual machines in a cloud provider is pretty easy - it's "just someone else's computer", right?

But we're so used to spinning up VMs that it's easy to overlook the power you can get from doing things differently - and the complexities that come with that power, whether you use it or not. Unlike a startup, an NREN is not a green field site, so some of the biggest challenges come from integrating with our existing infrastructure, based as it is on assumptions we made many years ago.

For example, we've worked hard to get the ability to commission servers in a "HEAnet-like" manner, so that we can manage them as a fleet, and use version control to manage the configuration. But there are some subtle pitfalls. When we grant these cloud servers access to our version control infrastructure, that's like giving them access to the crown jewels. It's very easy to return a server and its IP address, but when that IP address is handed out to another user... it's much harder to keep our access control up to date at the same speed.

We went through many different models for how to make this service before we landed on the one that worked best for us, and in doing so we discovered a lot about the differences between running services in our own datacentre and running them in a cloud environment.

This is a very practical real life experience in moving a real, production service to the cloud. We're learning a lot as this project proceeds; we're most of the way through the first full implementation (with the project scheduled to end in January) and already have many lessons to share, with more to come by next June.

Keywords: cloud, identity, nren, service, virtualisation

Biographies

Glenn Wearen joined HEAnet in 2007 with responsibility for federated access. Prior to joining HEAnet, Glenn held a number of positions focusing on single-sign-on, federated access, and identity lifecycle management with HP, Baltimore Technologies and Fidelity Investments. Glenn holds a Bachelor of Science Degree in Computer Applications (Software Engineering) from DCU and is an ISC2 Certified Information Systems Security Professional (CISSP) and ICS Certified Data Protection Practitioner.

Anna Wilson is the Service Desk Manager in HEAnet, and a member of the Network Development team. She's been with the company since 1997.