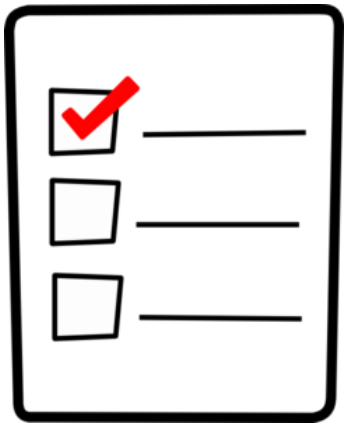
09/12/2018

Managed services for access management

Mark Williams

Agenda

- Jisc
  - Network & infrastructure
    - Janet 6, Eduroam, eduGAIN
  - Resources
    - Journal licenses
  - Services and apps
    - Data analytics



A bit of background

- Jisc: UK federation
  - 2007
  - Most commercial federation
  - Level Playing field for participation

  But a decade old…..

Agenda

- A change in requirements, a change in direction
  - Membership heavily moving towards out-sourcing and cloud
  - Accelerated in the last year or so
  - Drivers such as organisation mergers
  - Market Failure 3rd party providers for UKf okay, but expensive
- Managed Services
  - for our membership
  - for ourselves and our peers

Drivers

- Many members (esp. smaller) members:
  - Cannot devote the time and effort for such specialised services
  - Are consequently running old/out of date or unsuitable software
  - Can't take advantage of new features and initiatives

- Many members asking "why can't you do this for us?"

Jisc Managed Services for our Membership: Jisc Liberate

- Jisc Liberate - a set of cloud-based, managed, Access Management services

- And a URL re-writing web proxy (no logo!)
- Single management interface, shared configuration

Why are we doing this?

- Responding to customer demand
- Increase take-up of services
  - When it's easy to deploy, more will join and use
- Increase quality level of services
  - If we're running stuff, we can keep it **up to date** and **secure**, and help customers implement things like **Sirtfi & R&S**
- Reduce sector cost
  - Liberate has already reduced the cost of outsourcing as other providers have dropped prices after we launched

» As easy as…

1. Subscribe
2. Deploy VPN (optional)
3. Use web portal to configure connection to LDAP, configure services
4. Relax

Liberate Portal

- Simple interface to manage:
  - LDAP connection
  - Service specific settings
    - SAML IdP - consent, logos, MD…
    - eduroam – VLANs, Groups, APs and Controllers..
  - VPN connection
  - Log viewing

Secure by Design

- VPN back to home network
  - Optional, but recommended
  - OpenVPN based
    - Client on the network, connects to server on the managed VMs
  - Download appliance or config
    - Appliance is ~6MB
    - OpenWrt/LEDE VM
    - VMWare, VirtualBox, Hyper-V
- (If no VPN, we require LDAPS)

Liberate Portal – SAML IdP

- Shibboleth v3 instance
  - Updates managed centrally, latest version.
- Consent option
- Partly customisable login page (*more options soon)
- Configure extra local MD
- Configure attributes and attribute release
  - Currently support simple, scoped and mapped attributes. Scripted in the future.

Liberate Portal – (edu|gov)roam

- All the basic stuff (incl. Upstream servers)
- Manage:
  - Realms
  - VLANs
  - VLAN mappings
    - Map to a VLAN based on realm or LDAP group
  - APs and wireless controllers

Behind the scenes of Liberate

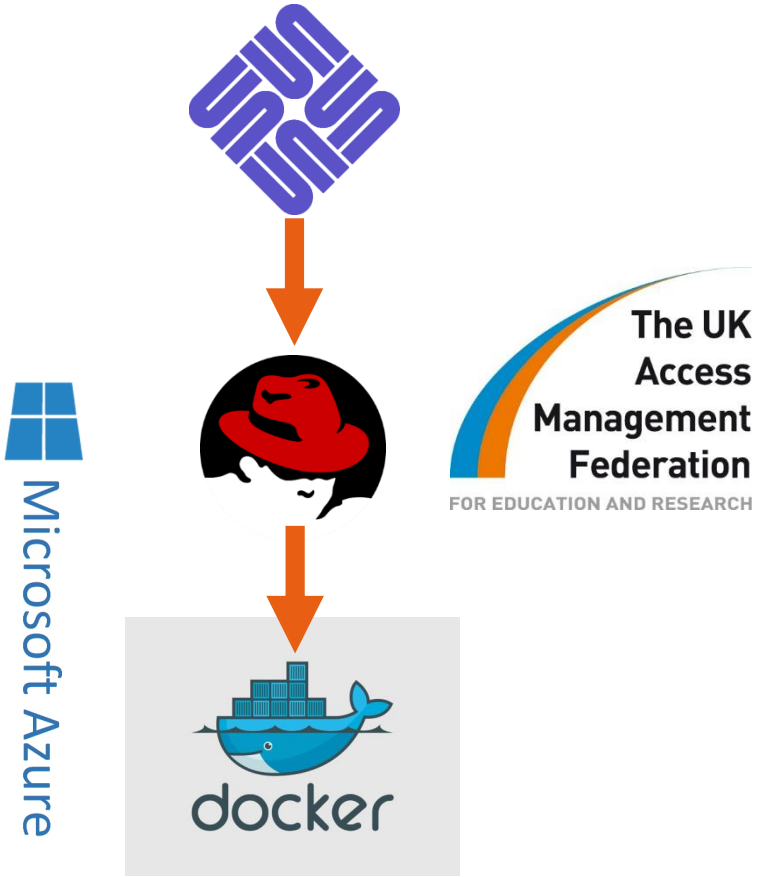
- Custom built portal
- Portal interacts with AWS APIs
  - Each new service spins up an AWS VM from a custom Debian AMI
    - Portal pushes config to VMs via custom management daemon
  - Designed to be zero touch
    - Configuration gets pushed
    - Minor updates happen automatically
    - Major updates, we simply update the AMI and then rebuild
      - Elastic IP – no downtime
        - (well, almost… VPN needs to reconnect)

Up a level in the stack: Managed Federation Service

- So managed services for users of the infrastructures
- Can we apply the lessons and design patterns of managed services to the infrastructures themselves?
- We can… so we're rebuilding the UKf to be a managed service for our own use

A bit of background (again)

- 2004 - 2015 – all infrastructure on Sun h/w and Solaris
- 2015- All rebuilt manually (to a deadline) on RHEL on Azure
- 2018 – Rebuilding again in a much more manageable way – docker based microservices



Splitting the federation into two

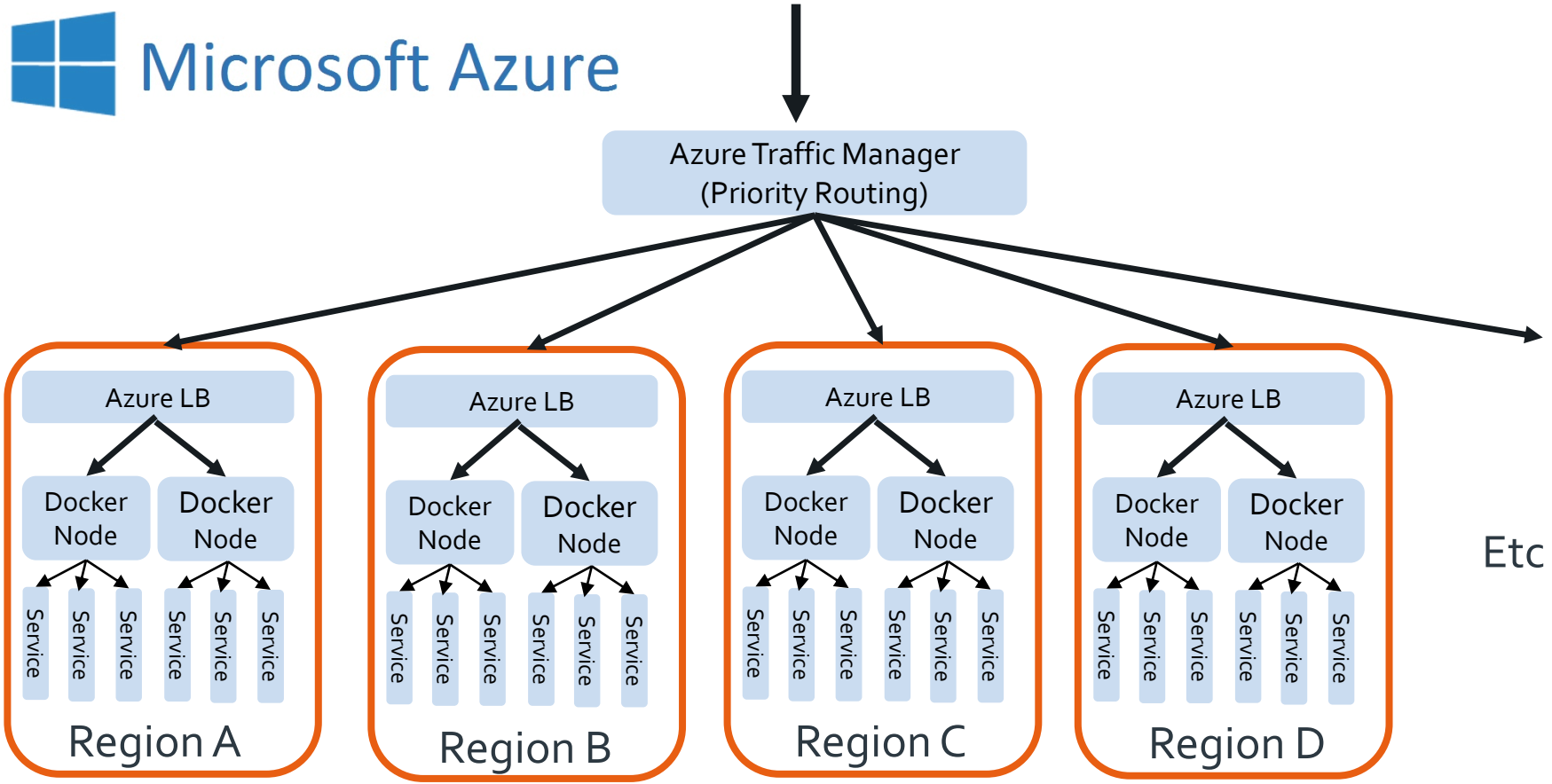
- Frontend – distribution Infr
  - MD & MDQ distribution
  - CDS
  - Management portal
  - Test IdP/SP
  - WUGEN
  - etc

- Backend – management Infr
  - Entity Repository
  - MD aggregate & MDQ creation
  - Orchestration
  - Signing
  - etc

Under the hood - Frontend

- Global distribution platform built on Azure
- Traffic manager fronting multiple (4+ initially) regions
- Multiple docker hosts per region, load balancer in front
- Individual docker nodes – no swarm, etc. Each host managed via docker-machine and docker-compose
  - Resiliency
  - Zero touch CI – build/test/release/deploy
- IPv4 & IPv6 support

MFS Frontend – Global Footprint

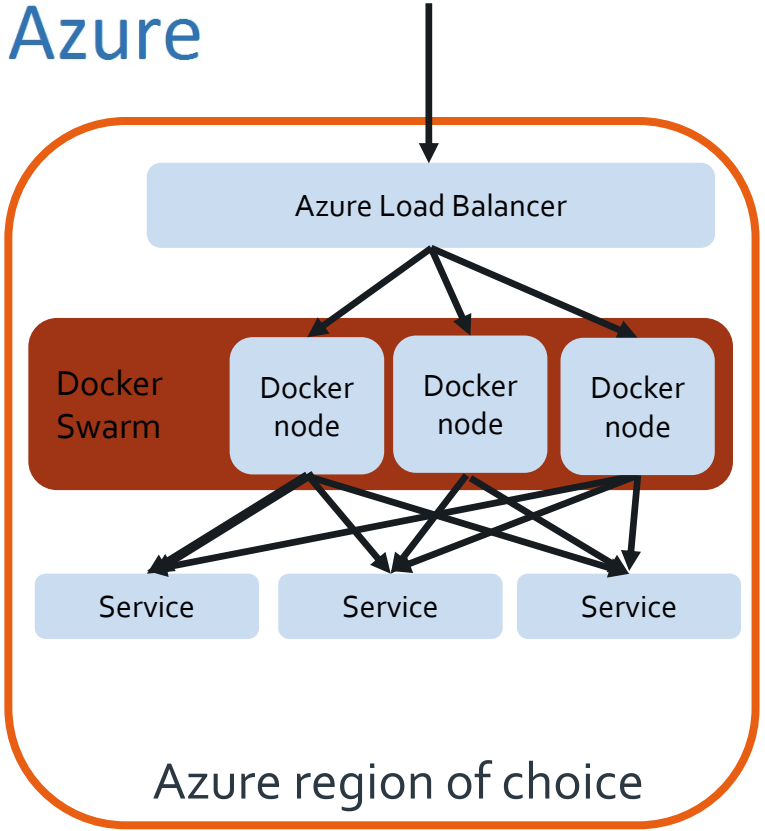


Under the hood - Backend

- Docker engine swarm mode for backend
  - Resiliency within swarm for each service
  - cloudstor:azure driver for volume portability across nodes
- Running
  - Gitlab
  - Jenkins
  - Management API (based on Shibboleth MDA)
  - Shibboleth MDA to create aggregates/MDQ
- All backed up to AWS

MFS Backend – for each MFS instance

Microsoft Azure



Managed Federation offering - technical

- **Jisc Managed Federation**
  - A collection of open source tools and orchestration routines that can run a federation the size of the UKf
- Primarily aimed at helping smaller federations get world-class tooling quickly, cheaply, and easily
  - Letting them concentrate on interacting with their customers
- Note: signing expected to be done locally in first instance
- **Managed Federation** user chooses (local) Azure DC

Non-technical aspects

- Support
  - For federation operator only
  - Offering a set of managed tooling, not running the federation
- Considering shared support with participants (follow the sun)
- Currently piloting, about to start technical pilots with Hong Kong & New Zealand
- Costs come down with more participants

A side effect…Managed Federation

- So
  - We'll have an infrastructure that we can spin up an instance of pretty quickly and easily, and that largely manages itself
- So
  - Why not offer that service to others for their own use?

What do we gain from this?

- We're doing it anyway
  - Might as well offer to others at cost + a fairly small margin
- Increase the quality of MD worldwide
  - Newer and smaller edugain participants often have problems
    - Steep learning curve!
  - Good, strict, tooling and a low cost might alleviate this
  - So we have to block fewer entities!

http://tinyurl.com/jiscliberate

Mark Williams

UK federation Manager

Mark.williams@jisc.ac.uk

jisc.ac.uk