Office 365 Rollout Cardiff University

Philip Smart & Lyn Rees

Overview

1. Cardiff University and email
2. Drivers for change
3. Why Cloud
4. Challenges of Cloud
5. Implementing Office365 in Cardiff
6. Rollout status

Existing Email Infrastructure

- Prior to migration, Lotus Notes Domino was deployed in house across the university.
  - 15,000 staff mailboxes (users and shared).
  - 35,000 student mailboxes.
  - 6 staff servers
  - 14 student servers
  - 14TB of email data (attachments!)

Drivers For Change

- Those who know Domino know that it's not cost effective as an email/groupware only solution.
- We Originally purchased/implemented as part of a suit of applications from IBM, but only to deliver email/groupware services.
- Domino/Notes not a cost effective solution when only delivering groupware services due to high admin overhead.
- Mobile support was late to come and had limited scalability (claimed improved now).
- Poor fit for the organization. e.g. ID files a pain!

Office 365?

- Exchange is still market leader for groupware.
- Good desktop client support, cross-platform (to a point).
- Good cross-platform mobile support (active sync).
- MS Office integration (Students now getting Pro Plus).
- Welsh and Local government using Office 365.
- Welsh Language support is good (Cymru am byth! Iechyd da!)
- MS are giving us free licences for staff and students.
  - No servers
  - no storage
  - no software upgrades.

What is Office 365?

- Software as a service. Reduce IT support costs by outsourcing hardware and software maintenance.

- Provides Exchange online, Lync and Sharepoint services (OneDrive, Project online, Office Web Apps). All based around Windows Azure Active Directory.

- For Email, we're given a blank Exchange environment that we need to set-up, configure and administer ourselves.

- Can either create remote-mailbox, then licence, or simply assign licence and 365 will do the rest.

Challenges of Cloud

- Can't change freeze
  - We have a stringent change process.
- Can only delay big upgrades for a short time (3 months?)
- Continuously changing with small increments every 2 weeks (with no real change-log)
- Everything over the internet
- Backend monitoring/reporting - lack of
  - There is a dashboard of outages – only reported by MS when enough people complain
- Microsoft support - dependency. Free support quality not good. Premier support has been very good, but isn't cheap.

Technical Challenges

- No Active Directory in Cardiff.
- Integration of user provisioning into existing Identity Management Systems.
- Migration of users from Domino.
- Mail routing - MS make Exchange hybrid routing pretty straight forward for their own stack, more difficult using different platforms.
  - Will eventually move most (all?) domains to the cloud but maintain some Linux mail hubs on campus (outbound mostly).
  - Currently, MX still on campus, routing through Linux (Exim) hubs.
- Migrating data over the internet is slower that on-site. It's also an unknown quantity, could be fast this week, slow the next (though, in our experience it's been reasonably consistent).

Integration With Our Identity Management

- All Cardiff User accounts are managed centrally in our Identity Vault (eDirectory).
- Accounts in our identity vault come from three data authorities
  - HR (Core)
  - Student Records (SITS)
  - Web Interface
- As accounts are input, they are transformed through a series of business logic rules (Drools), where:
  - Mail type is added based on Affiliation and School.
  - We add MSCLOUD as a mailtype for those on 365.
  - Some departments still set to Domino.

Integration With Our Identity Management

- For Office 365, we required an onsite Active Directory.
  - Users are synchronised (by dirXML) from our eDirectory instance to our Active Directory Instance.
  - DirSync then synchronises these users to the cloud Azure AD instance.
    - We do not use FIM - although dirSync part of FIM.
    - We do set some dirSync properties e.g. 1 hour sync, exclude some users.
- This does not cover our shared mailboxes.
- We use ADFS for authentication.

Integration With Our Identity Management

- Users therefore are synchronised to the Cloud, but require licences.
- During processing, if mailtype set to MSCLOUD and the user has a mailbox entitlement (set by our Member Entitlement policies) then:
  - Queue an XML message on our AMQP RabbitMQ message queue server.
    - Message contains UPN, Affiliation and item to licence e.g. MAIL
  - Powershell .net adaptor then takes messages from the queue every 1 minute, constructs powershell cmdlets and assigns the users licences in the cloud.
    - According to type e.g. FACULTY license or STUDENT.
    - We can also group different licence assignments e.g. Lync and Exchange.

Integration With Our Identity Management

- When a user leaves or is suspended, their account is hidden in AD for up to a year.
  - They are synched to the cloud, but can not authenticate via ADFS.
  - Separate container, allows us to easily recover mailboxes as we do not really get rid of them.
  - After a year, we then remove from onsite AD - deletes them in the cloud - with one month mailbox retention.

Integration With Our Identity Management

- Shared mailboxes
  - We do not synchronise our shared mailboxes into our AD.
  - We create them as Cloud managed objects using powershell - which we do licence and set certain default policies on.
  - Again, if a shared mailbox is created in our Identity Managment system, we queue an XML AMQP message that is picked up by our powershell .net adaptor and actioned.
    - Full SMB lifecycle needs to be included - e.g. update and delete needs to be queued and handled by our powershell adaptor.

Integration With Our Identity Management

- Office 365 ProPlus
  - We give the Office 365 ProPlus license to our 'entitled' students (pretty much all on accredited courses).
  - For this, our identity management system identifies those entitled during account creation and queues another XML AMQP message.
    - As opposed to Powershell, we action this using the GraphAPI.
    - This gives us much better assurance the licence has taken (the object is returned immediately)
    - Can be slotted into our existing Java based identity management suite - as Restful API.

Migration

- SMTP mail routing (sub domain to push to cloud) – no specialist tools
- Quest for data migration only – mail, calendaring, tasks
  - 5 workstations running both outlook and notes libraries (including Quest tool)
  - 10 threads on each, 50 parallel user migrations.
  - XX users per night, still learning experience for us and Quest
    - Quest supplying regular tool updates.

Rollout

- All students moved over to 365
  - Switchover teams out on campus
- Staff around 75% have moved over
  - Also switchover teams
  - Staff more involved usage e.g. calendaring, rooms and resources, shared mailboxes (permissions)
- Not much resistance to the change
  - Not much love for Notes.