AWS Migration Update

Sponsor: Anthony Brigginshaw

Author: Rob Thompson

Board/Authority/Group: UC Programme Board

Date: 27th March 2017

Paper For Information Only

UCPB060417 – Paper 5

OFFICIAL SENSITIVE

Main objective

- Provide an overview of the scope of the migration.
- Update on significant achievements, progress to date and associated high level plan leading to a go-live at the end of May ‘17.
- Assess key risk areas and approaches to mitigation.

UC

Scope of the SCC to AWS Migration

- The UC FS application has already been developed and implemented to support the ability to scale and meet the programmes roll-out plans.
- The final step to realise this scalable architecture is through the migration to a commodity cloud infrastructure provider which will allow UC FS to scale its infrastructure, quickly and efficiently.
- This will be achieved by moving from Specialist Computer Centre (SCC) to Amazon Web Services (AWS), providing a number of day 1 benefits:
  - Increased resilience by running the service over 3, independent 'Availability Zones'.
  - Ability to scale the service on demand very quickly and easily.
  - Potential for the service to heal itself.
  - AWS' excellent reliability record & feature capability.
  - 70% cost reduction on an 'as is' basis with opportunity for further cost optimisation.

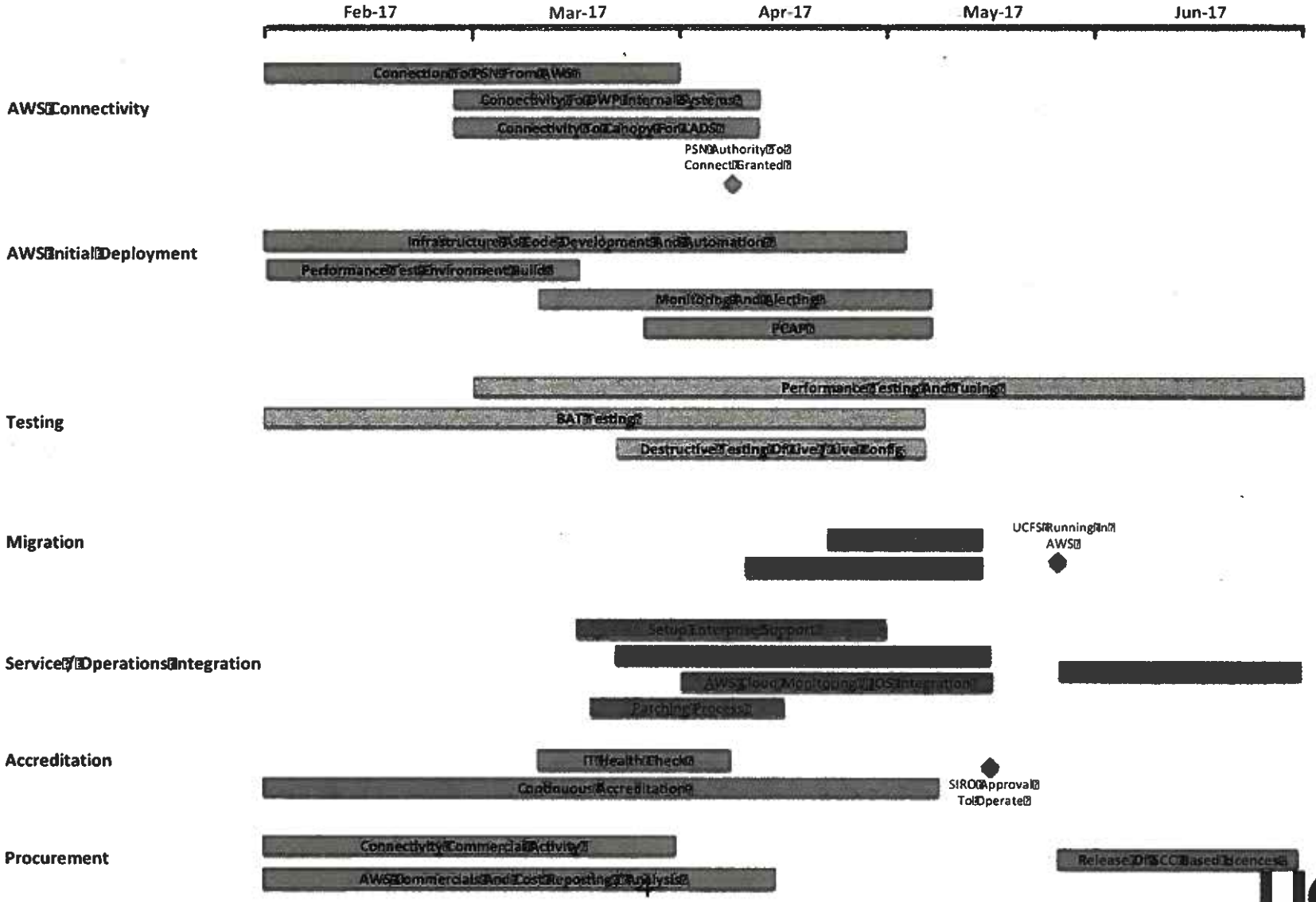
UC

AWS Migration – Progress To Date

- Architecture review: Successful review by Amazon and Slalom.
- High availability design: Functional testing in progress.
- Automation: Software developed to allow the automated creation of infrastructure for all environments (Prod, Staging, Performance, Dev/Test).
- Performance testing for October scaling: In progress, based upon UC FS rolling load testing programme, forecasting volumes 6 months in advance.
- Failure/OAT Testing: Key pieces of application infrastructure successfully tested under common cloud failure scenarios (Database, Messaging).
- Security: IT Health Check completed with no major issues identified.
- Network: AWS have been granted certification by GDS allowing connection to the Government approved network (PSN) from systems hosted on their platforms

UC

AWS Migration – High Level Plan



AWS Migration – Key Risks and Mitigations (1)

Area & Risk	Mitigation
Network connectivity: Not available in time to meet a migration in May '17	A decision was made in late February to use a PSN connection from AWS to the DWP network as a contingency option whilst the strategic network solution is built, commissioned and made available. This removes the strategic network connection from the critical path.
System Performance: UC FS load and response times degrade.	Comprehensive performance testing of October '17 loads on both agent and claimant services using the current synthetic tests give assurance that AWS infrastructure characteristics meet our current benchmarks for system performance.
Functional Performance: UC FS functionality is compromised as a result of the migration	The same test frameworks & structure used for the weekly releases to SCC are also being used for the AWS migration, ensuring we are validating functional performance from a known good state.
Architecture: The architecture of the service on AWS is compromised.	UC FS and Digital-IOS teams commissioned Amazon and Slalom (specialist AWS consultancy) to review the architecture of the service. This healthcheck was positive and the only key areas identified for redress are already on the development backlog.

UC

AWS Migration – Key Risks and Mitigations (2)

Area & Risk	Mitigation
Security: The service becomes less secure in moving to AWS	The service has been designed to be more secure with greater degrees of encryption applied to data using improved key management. IT Healthchecks have been carried out and specific AWS security risks assessed by DWP CSO.
Migration: The migration itself introduces problems for the service through data corruption.	The nature of the migration means we have the ability to build UC FS as a greenfield environment on AWS and move the majority of the data in advance with the remaining data copied once the service is taken offline. We can then test the service behind closed doors before enabling the network access. Before network access is enabled we have the option to cut back to SCC. Once external access is granted, fix forward would be the strategy to remedy any issues.
Resilience: The service becomes less resilient in AWS than currently experienced in SCC.	Key components in the UC FS stack (database and messaging) have been built and tested at component level to ensure they are resilient under common cloud failure scenarios. Service level failure testing under load is planned to exercise more realistic failure modes.

UC

Summary

- This paper has been brought to this meeting because:

- Providing Information Only

Decision	Approved
For Information Only	

UC

BACKUP

UC

UC FS Architecture in AWS