Jisc
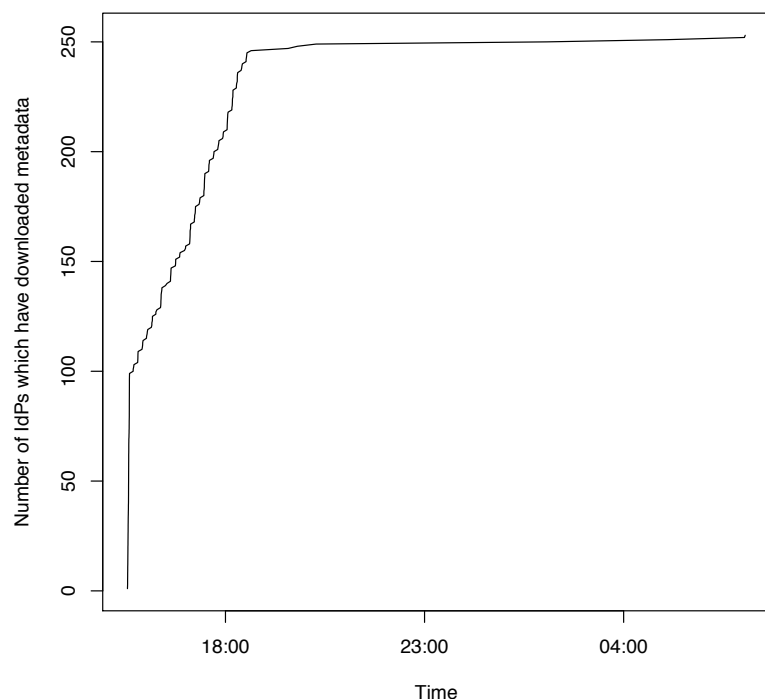
Metadata propagation in the UK federation

Presented at REFEDS 38 / TNC 2018, Trondheim.

» Service owners often ask "How long will a metadata change take to propagate to federation entities?"

» Probe using SAML 2 `AuthnRequests`

> Deploy Shibboleth SP

> Update `handlerURL` from `/Shibboleth.sso` to a UUID

> Publish updated metadata

> Send `AuthnRequest` to check whether IdP has consumed new metadata

» Shibboleth v3 IdP has MDQ client and sends HTTP 400/500 response if it hasn't refreshed metadata

Metadata propagation through the UK federation
(results/2018−05−17−output.txt.processed)

Metadata propagation through the UK federation
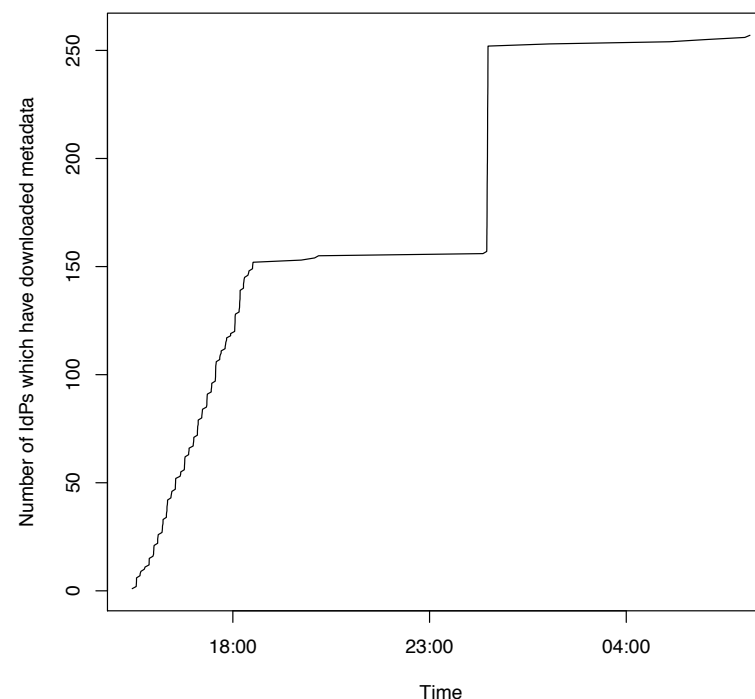**(results/2018−06−01−output.txt.processed)**

Run 1: Probe metadata out of cache

As soon as probe starts, MDQ clients read refreshed metadata.
Almost all clients using aggregates refresh in the following 4 hours.

Run 2: Probe metadata in cache

Probe starts shortly before new metadata published. Most clients using aggregates refresh within 4 hours after publication. MDQ clients refresh when probe's metadata goes out of cache

» Approximately 100 (out of 268 in test dataset) Shibboleth v3 IdPs are using MDQ to obtain metadata

» Deployers almost always use default settings or federation recommendations when configuring systems

» "just-in-time" MDQ can be slower to refresh metadata than classical aggregate refresh

» Metadata propagation is, indeed, a few hours, or overnight

» **Measuring metadata propagation from IdP to SP is harder**

  › Lower likelihood that an SP will consume metadata from the test probe

  › No analogue of AuthnRequest, use unsolicited assertion?

  › Wide range of SP implementations and potential for SPs to give a wide range of responses

» **Propagation within UK federation is part of a bigger picture.**

  › Daily / emergency metadata publications

  › Propagation through eduGAIN

Jisc

Alex Stuart
Principal Technical Specialist
(UK federation)

alex.stuart@jisc.ac.uk

github.com/alexstuart/MetadataPropagation