

Tues 9.45am SalonsA-D

Scribing Template --Tues., Nov 12, 2013 at 9:45am -- **Salons A-D**

TOPIC: Grouper Provisioning

CONVENER: David Langenberg

SCRIBE: Keith Hazelton

of ATTENDEES: 45

MAIN ISSUES DISCUSSED:

Grouper change-log consumers and alternatives to PSP going forward

Some discussion of fault-tolerance around processing changes coming from Grouper; The Grouper database is a single point of failure so addressing that should be a priority.

DavidL: The direction of development for Grouper is to move from monolithic PSP model to a number of small, specific changelog consumers for particular targets. AD and LDAP are core cases. It's the Unix model: Do one thing, & do it well. It was noted at one institution that there was no demand for message-based approaches, they "just" want to look at AD or LDAP or a database view. Representatives from other sites said there WERE consumers who would be glad to run their processing based on a message queue.

In addition to simple updates of identity attributes or group information, there is a common interest in change-log driven account creation.

Grouper already has ESB and XMPP change-log consumers. SCIM is coming.

You always need to run a fixer/reconciler because message-based stuff *will* fail; a daily run to check for errors

Key requirement: processing off the change log must be fast and it must scale horizontally

Real-world provisioning problems are messy: You'll ultimately need perl/python/ruby to solve them

Would be good if Grouper could also consume messages on the inbound side (call it Grouper Loader NG)

Leveraging Grouper permissions to access OAuth-protected resources (DEMO w CAS Server, Grouper and an OAuth client)

Bill Thompson demoed use of a CAS Server invoking Grouper over web services as part of handling authNZ for someone accessing a resource protected by an OAuth Authorization server. See <https://github.com/UniconLabs/cas-grouper-oauth> for the code to the proof of concept. See <https://wiki.jasig.org/display/CASUM/OAuth> for more info about CAS OAuth support.

This could be relevant to two other upcoming ACAMP sessions: [Santa Clara at 3:15 pm: Service Management and Grouper-Based Service Provisioning](#). Santa Clara at 4:15 pm: [SOA / RESTful interfaces with federated identities](#).

ACTIVITIES GOING FORWARD / NEXT STEPS:

Grouper project will continue in the direction of supporting specific changelog consumers for specific targets

It's also straight-forward to develop a custom changelog consumer, it amounts to implementing a Java interface.

If slides are used in the session, please ask presenters to convert their slides to PDF and email them to acamp-info@incommon.org