

# CACTI Public Meeting Notes of 1-Sept-2020

## CACTI Call Sept. 1, 2020

### Attending

#### Members

- Tom Jordan, University of Wisc - Madison (chair)
- Jill Gemmill, Clemson (vice chair)
- Marina Adomeit, SUNET
- Margaret Cullen, Painless Security
- Michael Grady, Unicon
- Karen Herrington, Virginia Tech
- Christos Kanellopoulos, GEANT
- Chris Phillips, CANARIE
- Bill Thompson, Lafayette College

#### Internet2

- Ann West
- Steve Zoppi
- Nic Roy
- Jessica Fink
- Emily Eisbruch
- Dean Woodbeck
- Sara Jeanses

#### Regrets

- Matthew Economou, InCommon TAC Representative to CACTI
- Nathan Dors, U Washington
- Rob Carter, Duke
- Les LaCroix, Carleton College
- Kevin Morooney, Internet2

### New Action items from this call:

- Al TomJ - add more questions to the proposed container / packaging survey on configuration management, secrets management, deployment automation and sustainment practice, and share with the CACTI email list
- Al TomJ - ask Ken for more clarity around the goal of the proposed consent survey
- Al TomJ - add the cloud services topic to a future agenda

### Older Action item:

- Jessica - help coordinate a quarterly update from CACTI to community on best practices, trends and directions (coordinate with other InCommon governance groups)

## Discussion

- Consensus on "higher ed registry"
  - See these notes for overview and discussion of the HE registry topic:
    - [CACTI Public Meeting Notes of 26-May-2020](#)
    - [CACTI Public Meeting Notes of 9-June-2020](#)
    - [CACTI Public Meeting Notes of 7-July-2020](#)
  - Tom's proposed response to Kevin was shared and discussed on the CACTI email list
  - See Tom's email of August 11, 2020
  - Proposed email summarizes the risks around running a HE registry
  - Agreed it's OK for Tom to forward email to Kevin
- **Proposed packaging survey** - Report out from CACTI/Component Architects/Trusted Access Platform Software Integration discussion (Tom)
  - CACTI discussion of Aug 4, 2020 emphasized the need to capture in the packaging survey those who don't have strong devops /containerization practice.
  - See [CACTI Public Meeting Notes of 4-Aug-2020](#)
  - Tom shared this feedback with the [Software Integration Working Group](#)
  - The survey will be tweaked accordingly.
  - TomJ volunteered ChrisP and Matt to the Software Integration Working Group as a reference if needed

- Annual Trust and Identity committee **nomination and voting process** kicks off now, Tom, Jill and Nic working on an announcement. (Nic/Jessica)
  - [Wiki page with nomination process is here](#)
  - First step is working on blurb for overall announcement to community about Trust and Identity advisory group opportunities
  - Nic will officially notify CACTI members whose terms end in Dec 2020
  - The following people are scheduled to rotate off CACTI this year, please let Jessica (jfink@internet2.edu) know if you intend to self-re-nominate:
    1. Nathan Dors
    2. Jill Gemmill, Vice Chair
    3. Karen Herrington
    4. Tom Jordan, Chair
    5. Christos Kanellopoulos
    6. Les LaCroix
    7. Chris Phillips
- **NET+ Service Providers and Identity** - (Sara Jeanes)
  - There are opportunities for CACTI to work with NET+ CSTAAC, a NET+ advisory group looking at Cloud Architecture
  - CSTAAC (Cloud Services Technology Architecture Advisory Committee, pronounced C-stack)
  - <https://spaces.at.internet2.edu/pages/viewpage.action?pageId=154766601>
  - Jill Gemmill, CACTI vice-chair, serves on CSTAAC
  - CSTAAC Reports up through the NET+ PAG
  - CSTAAC reviewed Internet2 File Sender service (now sunsetted)
  - Reviewing Cloud Connect Service, how it can grow, and fit better with Trusted Access Platform
  - <https://www.internet2.edu/products-services/advanced-networking/networking-for-cloud/>
  - Looking at how broader HE community engages with Google and Gsuite for Education
  - Hope to encourage Google in community architected direction
  - There is increasing interest in scaling group structures, syncing LDAP groups and in deprovisioning
  - There is a demand for support around implementing tools we've developed as a community
  - Need for scaling identity grouping mechanisms
  - Passing information to cloud technology
  - Trend towards consolidation of services into a couple of hubs
  - Cloud Checker is a utility under service evaluation <https://cloudcheckr.com/>
  - Hosted by reseller partner DLT, also work with DLT on AWS
  - BillT: echo the Gsuite pressure on campus regarding groups and authorization.
  - Lafayette had project to create group for every class being offering.
  - Brought into Grouper as reference groups per Grouper Deployment Guide.
  - Then provisioned to Google. Much flexibility in Google Groups.
  - The pattern of access policy in Grouper and provisioning to cloud services has worked well.
  - How to best manage interface with Google groups, and make things easy to use, is an open question.
  - TomJ: how to best engage with cloud providers to integrate with multi lateral federation and "be a good citizen"?
  - Sara: Cloud providers are in 2 buckets:
    - 1. New and emerging cloud providers, who don't have strong opinions yet.
      - There are a few in that pipeline.
      - Conversation can take 2 years. Willing to implement multilateral federation in the way we ask.
    - 2. With large, established cloud providers,
      - it's hard to get traction around requests for a multilateral federation approach.
      - Challenges around mapping to user permission structures.
      - More interest in less complex market dynamics.
      - Higher Ed is seen as a visibility driver, perhaps not a revenue driver for the large cloud providers. We may need to help bridge the gap with a linking mechanism
- - TomJ: is a service at federation level needed? Proxies perhaps as a federation bridge.
  - Nic: cloud provider as IDP is being requested by the community
  - TomJ: seeing interest in Azure as IDP platform
  - ChrisP: Canadian Federation has been working to engage Microsoft around multilateral federation,
  - eduroam is also an important service
  - Access management paradigm. AWS and Google have their own "rules" and approach. Microsoft/O365/Azure is releasing a new approach. <https://docs.microsoft.com/en-us/schooldatasync/what-do-azure-ad-connect-and-sds-do-and-how-can-they-work-together>
  - Al TomJ - add the cloud services topic to a future agenda
- **Surveys - Packaging and Consent** (Tom)
  - Dean Woodbeck, Internet2 stated that two surveys being considered:
  - **Container/Packaging** Survey and **Attribute release/ Consent** survey
  - Dean coordinates communications with the community. We don't want to overwhelm the community, Can we combine these? Probably not
  - For container/packaging survey, a good audience are people who have been to one of the InCommon training programs and CSP alumni campuses
  - **Container / Packaging** survey
    - The software integration WG will be tweaked as discussed above, to include those less experienced w containers

- Al TomJ - add more questions to the proposed container / packaging survey on configuration management, secrets management, deployment automation and sustainment practice, and share with the CACTI email list
- **Attribute Release/Consent survey**
- Comes out of Ken Klingenstein's work with Duke University
- CAR project, Consent and Attribute release <https://spaces.at.internet2.edu/display/CAR/CAR:+Consent-informed+Attribute+Release+system>
- Suggestion we need more concrete questions for this survey
- Not clear what questions we are trying to answer with the survey,
- Includes both policy questions and technical questions
- There are many open questions on the survey, for example the attributes we are asking about should likely be listed
- Perhaps interviews or discussion groups is another way to gather the info being sought
- Nic: there is group called the CAR drivers, includes Ken, Duke, perhaps U of Illinois Urbana-Champaign
- TomJ can summarize this feedback for CAR drivers
- ChrisP: from what is available from Azure, consent is there
- "I am using consent" checkbox
- What is the yardstick on consent that we are advocating for?
- Do we need this survey on consent?
- Should we propose a certain implementation of consent?
- Nic: a deployment or implementation profile around consent would be helpful to the community, good to have something normative
- Karen: CAR model is comprehensive, but at Virginia Tech it seemed like overkill for what was needed. Drivers would be audit requirements and user experience. Virginia Tech Implemented something to satisfy the base requirements and not "go overboard"
- ChrisP: perhaps the CAR team can do an environment scan, assess the various consent techniques being used by Azure, AWS, Google, and create a scorecard. Then suggest improvements needed. For implementation of consent, there is the issue of how many consent hoops exist as a user moves from tool to tool
- Al TomJ - ask Ken and other for more clarity around the goal of the proposed consent survey
- **Quarterly Update to Community** - Are there new technologies / issues to which we should be calling the community's interest? (All)
  - Password lists in the cloud are coming
  - CISCO open roaming, how it may impact eduroam
  - Fastfed (doing some dangerous things with SAML) <https://openid.net/wg/fastfed/>
- May dive into these at future CACTI calls

#### **Parking Lot**

1. (From June 9, 2020 call) TomJ - Add as an agenda item for a future CACTI call: Operationalizing containers

**Next Meeting:** Tuesday, September 15th, 2020