COmanage Dev Minutes 27-Apr-09

COmanage BoF
2009 Internet2 Spring Member Meeting
 27-Apr-09

Attending

Heather Flanagan, Stanford (chair)
Digant Kasundra, Stanford
Scotty Logan, Stanford
Michael P. Pelikan, The Penn State U.
Ken Forstmeier, The Penn State U.
Milan Sova, CESNET (Czech Republic National Research and Education Network)
Lucy Lynch, ISOC
Mark Scheible, North Carolina State U
Jorj Bauer, U. Penn
Tim Callahan U. Michigan
David Bantz, U. Alaska - Fairbanks
Satyanarayana Nanduri, Centre for Development of Advanced Computing (C-DAC),
   India
Stefan Karapetrov, Polycom
Juhani Gurney, NORDUnet
Licia Florio, TERENA
Mike Grady, U. Illinois at Urbana-Champaign
Ian Young, University of Edinburgh
IJ Kim, Internet2
Nate Klingenstein, Internet2
Emily Eisbruch, Internet2 (scribe)

Introduction

Heather welcomed the group and provided an overview of COmanage:
COmanage is a platform to enable collaborative organizations to become more effective.
It eliminates some potential domain issues and arguments over who hosts the various collaboration tools.
There is interest in COmanage from a wide variety of organizations, including science research groups, business administration folks, Ivy+ schools, and more.

Testing COmanage

A pre-configured COmanage Alpha VM instance is running as a service and available at https://spaces.at.internet2.edu/display/COmanage/Home (under "Test Drive")
To download and install the latest version of the Alpha version VM image (~1.3GB), also see https://spaces.at.internet2.edu/display/COmanage/Home (under "Test Drive")
Using the COmanage Alpha NEW
COmanage dev/unstable package Applications

Domestication

Applications that easily externalize their authentication and group information are able to be integrated into the COmanage platform. We call those types of applications "domesticated" applications.
So far, the COmanage team, at the request of early "use case" collaborations has focused on domesticating:
Drupal (content management - CM)
Confluence (wiki)
Sympa (mailing list manager - MLM)
Other applications are being considered. See the Roadmap for current thoughts on applications desired for integration into COmanage.
The COmanage team plans to talk to developers of collaborative applications of interest about how to structure their applications to make them either domesticated or easy to domesticate. The current developer team cannot scale to the level needed to do all the domestication themselves; the broader communities around each of the applications must be involved.

Future Direction

Important questions exist about the future direction for COmanage.

- Do we envision IT specialists deploying COmanage for their user community?

  or- Do we want to be able to say to a researcher who is not an IT expert, "Here's an appliance, you don't need to know anything technical to get this running and operational, and maintenance will happen behind the scenes." ?

User Interface: Discussions are planned with the people at the Fluid project regarding how the user interface and user experience should evolve for maximum ease of use. http://www.fluidproject.org/

Scalability

Q: Can the COmanage appliance host multiple VOs or is just a single VO?
A: Right now, it's setup for a single VO. Technically, could have more than one.

Q: What happens if the VO gets popular?
A: It depends upon how much memory and resources you've given it. We haven't yet gotten to the point of working on fault tolerance.

Q: Did you consider scaling out to a separate server?
A: There are potentially a couple of different methods, depending upon specific implementation details...
Scalability issues go back to how scalable Grouper and Shibboleth are.

We are taking existing applications and helping people bring them together.

Challenge: We have more interest than we have people working on the project. Potential adopters have expressed interest in having instant messaging, calendaring and other applications within the COmanage framework. The current development team can't make these work without more time and involvement. We are seeking others who want to help with development.

Group and Authentication Issues

Q: Can you make use of an institution's existing group structure?
A: If an institution uses Grouper, then yes, it is possible to have COmanage use that infrastructure.

Q: Concern: if someone leaves an institution, their Shibboleth credentials stop working. Then how do they sign onto the COmanage collaboration instance supporting the VO/CO of which they might still be a part?
A: That's a task for an authorization system, not an authentication system. Their authentication can still work (e.g. because of retirement benefits).
So if we start distributing authorization, then we need to ask "can you tie this into campus authorization system?"
Digant: If someone leaves an organization, their relationship is best managed by the VO.

Q: Is it possible to tie the COmanage authentication into the campus Grouper instance?
A: Yes.
But then what's the benefit?

What this problem space talks about is that the authentication and authorization works with the home institution, but not by extension necessarily in the case of the VO.

RL "Bob": It's a step along the path. I want to reflect that in my VO if there's no possibility of connecting to the institution. So the first hook is the link of authorization for sign on.

Applications should not own identities.

Brendan's concern: Can see little COmanage instances popping up like mushrooms around my campus. I foresee the need to have a document to say: "as cool as this is, here's what to think about before inviting all your friends..." As a default we could tell users to get a ProtectNetwork identity if they leave their institution and need to continue in the VO.

Q: Is there a document outlining the issues that make domestication possible? So an institution could domesticate, for example, Subversion?
A: Digant: we have the start of these documents. We would be happy to accept offers to help with that documentation. Domestication documentation is further along than other documentation.

Attribute Release

There is discussion within the CIC about how to deploy this, and gaining permission for IdPs to release the required attributes. We need to be able to explain this to people who control those attributes within the campuses, and be mindful of privacy policy issues.
Attribute release policy (ARP) is a stress point.

There are tools: InfoCard and uApprove.
It appears that it's very safe to do uApprove. InfoCard is getting safe too.

Need to get InCommon to provide basic information about ARPs in various contexts to their participants.
Sites need to be able to relay upon a consistent translation of attributes - controlled vocabulary is important.

We also see the need for a consistent translation of eduPerson into English. The Dutch are working on that, we understand.
Although many apps provide external identity, a lot of them have web services to do provisioning, which would be generic. The key need is for hooks to integrate.

Q: How about a generic proxy? That would allow a lot of apps to be provisioned by doing little work.
A: We have looked at that, and we should look at it more closely.

Microsoft and Sharepoint Issues

Q: what does this mean in Microsoft environment?
A: SharePoint is a highly desired service. What will it take to domesticate SharePoint?

We understand that Microsoft is keenly aware of the issues and are looking at them. More feedback will help, but they are getting there.

It appears that this web services approach would work, if we can determine what all the services are doing.
There is a federated version (via plugin) of SharePoint. The hard point is managing the authorizations. That's where it needs to come together.

Q: So what about the Microsoft platform as a domestication hub? Is that feasible?
Passing the identity appears not to be a problem, but what will Microsoft do as far as the authorization?

Q: Are they federating the tools for authorization to SharePoint sites?

A: the next version of SharePoint will have fully incorporated the identity aspects.

SharePoint is not the greatest collaboration platform. But it is the lowest common denominator. Many sites would prefer the Confluence wiki platform instead.

Q: What would licensing look like?
A: SharePoint WSS - you only need server license. But MOSS- need end point licenses.

Anecdotally we have heard of sites that have made a deal with Microsoft to solve this problem, for an identifiable and bounded community.

Heather's Take-Away from Discussion

Folks seemed to think the "appliance" is a good direction. So we will continue to go down that path.

People also seem to want the instructions on how to do this themselves, integrating in to their own environment as needed. We will pursue the documentation and policy discussions needed to make that "framework" model work.

We also need to focus on the documentation so people understand COmanage and also so people can feed into/contribute to the documentation based on their own efforts and experiences in domesticating applications, etc.

To Get Involved

Go to spaces wiki where you can view the latest documentation and downloads:https://spaces.at.internet2.edu/display/COmanage/COmanage+Product+Roadmap

Go to the COmanage website where you will find the COmanage info-sheet and instructions for joining the mailing lists:http://middleware.internet2.edu/co/

Next Call: Friday, May 15, at 2 p.m. ET