

Link to 2020 ACAMP wiki

Deployment Guide for TAP

Advance CAMP Wednesday Nov18,2020

12:20-1:10 am ET

Room - Docks

CONVENER: Mike Mays

MAIN SCRIBE: Chris Hubing

ADDITIONAL CONTRIBUTORS: Drew

of ATTENDEES: 33

DISCUSSION:

- Grouper, CManage and Midpoint seeing functional overlap
 - What the capabilities and overlaps are
 - What is the best solution for a given problem
 - Can be overwhelming - what to do first, how to integrate them best?
 - Mattb: Welcome to software integration working group
 - Lots of discussion around this
 - Discussion around Writing deployment guide for midpoint
 - Has around 70 pages of notes compiled while getting it into prod
 - Where to begin and where you want to get to
 - There is a banner integration group
 - Connectors are all different in the way they work
 - Keith Levalley (Davenport) is working with BES connector

- Hoping several institutions can get midpoint into production and collaborate on writing a deployment guide
 - Want to map out what goes into grouper and what goes into midpoint
 - Course rosters is “simple”/doable in Grouper, harder in midpoint
 - Then integration issues between those
- Randy Miotke: partially deployed instance of midpoint
 - Hardest concepts is how to use each of these pieces best
 - Overhead view of architecture
 - Their grouper deployment is pretty mature
 - How to best utilize Grouper while also using the provisioning of Midpoint
 - List capabilities of each tool and suggest a path. Provide support/guide.
- KeithH:
 - Making a decision tree might have too many branch points
 - But maybe case studies around places that have deployed
 - Annotate those use cases
 - e.g. “This looks best for this use case”
 - Community can/must help each other:
 - There is no “ideal” combination
 - CSP is place where we need to document successes and stumbling blocks
- Drew: there are a few integration resources (see bullet 1)
- BennO: Use case based, no one true answer
 - Maybe we can get to patterns based on use cases, eg "single SOR" vs "mult-SOR"
- Randy:
 - lifecycle rules in midpoint were useful, but there may be other ways to do that... same with other components
 - Real work isn't just deploying the solution, it's cutting over to the new one
- Matt: gradual integrations with new components, but integrate the existing useful ones
 - Starting from ground-up
 - It's not just source system, it's the target systems
 - Try to re-use
- Martin: implemented midpoint, but had to keep some of the existing systems.
 - Agree there are multiple paths forward
 - It's very situational, what are you trying to achieve
 - Having the strengths of each and pros/cons when there is overlap

- Keith: Let's keep this conversation going to identify what others are doing. Identify MVP and keep building. Who we draw from and how we choose things.
 - Venn diagram. Overlap COmanage, Grouper, etc. There will be a section in the middle to pick your product and integrate it into the right groups. Will help to identify which components you decide to pick (overlaps) and unique /exclusive features (that may or may not make sense to incorporate)
- Martin: May want to do 2 - 3 components and this could help to order them and/or find the biggest bang for the buck. This could be a great resource to get started.
- Mike M: Even picking just one will be a good place to start. Legacy systems galore.
 - Cookbook - How to accomplish in each system (COmanage/MidPoint/etc.)
 - Comparing feature richness
- Benn
 - Two products come from different backgrounds with some overlapping. Each has strengths where the other may be lacking.
 - Good starting point - data model under hood and provisioning structure.
 - COmanage started in Research and HigherEd. IDentify complicated systems of record. Provisioning side - COmanage is not designed to scale at University (500k+). midPoint better at that scale.
 - Gray area between the two
- Bill T: Venn diagram is a good start to compare functions and features, which are forever changing.
 - Capability model. How the parts of TAP can fulfill some of those capabilities. Yes, some overlap. Some can fill needs on their own and others in partnership with another component.
 - If you already have strong attribute based enterprise management you may not need Grouper.
 - Need to identify gaps/growth space in your existing architecture.
- Capability versus function/feature --
 - Feature for particular product will be in product-specific language
 - Capability more in the sense of IAM speak
 - Grouper has set math - killer feature, enterprise access management
- Keith - (claims to be an InCommon badass with training ;) -- Erin can attest he is in fact a badass (HA! =)
 - Could be a challenge using multiple components with different terminology. Asking adopters to learn all three languages and

translate between them. COmanage role, into midPoint induced role into Grouper group, etc.

- Tough to figure out.
- Trying to map them all to a common language can be even more confusing
- Idea:
 - Dashboard across components with a unified terminology
 - Conversion of functions/terminology
 - IAM console, which admittedly would be a large lift.
 - Would have to decide on the language to use and not create a 4th. ¡Esperanto!
- Thought: go back to the standards and build from there.

■ Bill T

- Products tend to take on their own vocabulary, but should revert to standards as much as possible
- Contributes to the challenge of establishing IAM as a discipline.

■ Laura

- As we're talking about various products, we're talking technical level
- Who is the audience? Where do the products shine? Let's articulate that. We're missing this piece.
- Where is there overlap? What can these tools do?
-

■ BillT

- Capabilities, not technical details of the product. These should be independent
- If higher-ed was better at articulating capabilities, it'd be easier to make a cookbook

■ Keith

- List capabilities of products but put * (star) next to the "one that shines" in that particular area
- How-to documents; help on decisions to make
- For access management, grouper has ways to express and manage that
 - It is the access management brain
 - Midpoint and comange could be the limbs, the actors that carry out what this brain says
- Any places not considering grouper? None yet

■ Mike porter: impressed with amount of data Grouper can "munch" on

- Output of munching can be input to midpoint, very powerful

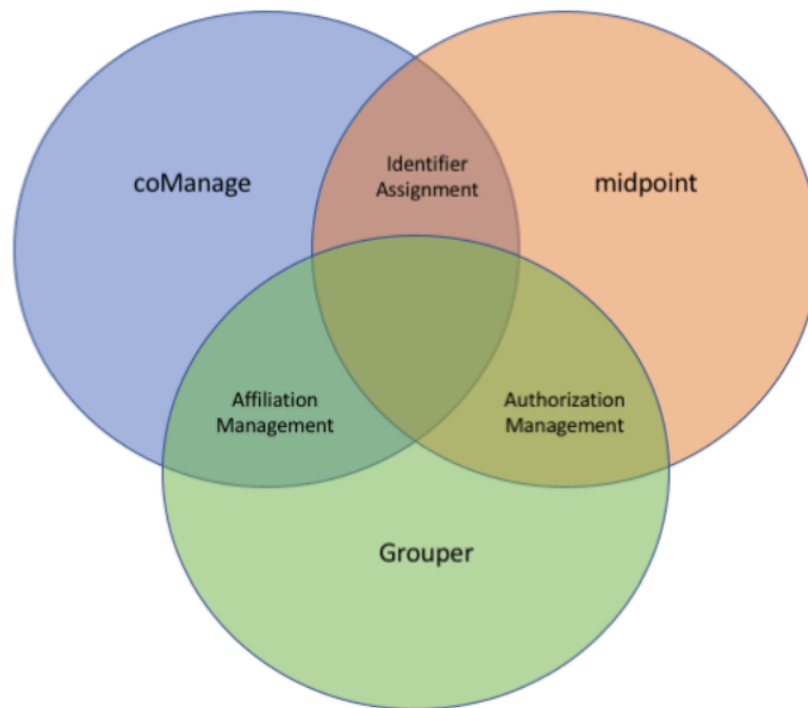
■ MattB: document how to use access controls in Grouper for lifecycle management, then do the same for midPoint and COmanage

- See what is "better" at such things

- Document these at a high level, then get into a how-to as you broaden the doc
- Mike Porter: for smaller schools, CManage might be fine and Grouper would not be needed
- What's Next?
 - Drew: establish use cases for common sized school, recommended implementations based on the type of institution
 - Steve: there's a connection between this conversation and panel yesterday. Dedra Chamberlain (from Cirrus Identity) may be able to help with this
 - To participate
 - Join the inctrust-si@incommon.org mailing list and Slack Channel (#inctrust-si DM Chris Hubing for Invite)
 - All are welcome to participate and suggest topics for our Software Integration Working Group meetings. The agenda/scribing doc is <http://bit.ly/siwg-01>. Meetings bi-weekly, Wed at 3 pm Eastern US, Fri at 10 am Eastern US
 - MattB: get those involved re-energized to do this (don't tell his supervisor that we occasionally spend too much time running down rabbit holes)

RESOURCES

1. <https://spaces.at.internet2.edu/display/CManage/CManage+midPoint+Integration+Approaches> <= Five mix and match alternatives for CManage and midPoint Integration
2. https://docs.google.com/spreadsheets/d/13HmrYwGd5QSbkjqK-TXCLTNBVZsBO_CRo9wA6gOKU6A/edit#gid=0 - TIER Provisioning Fit/Gap Worksheet (Tom Jordan - 2018?)



Core Competencies

- Identity Registration
- Provisioning
- Group Management

-
- 3. [Banner Integration Working Group](#)
- 4. [Trusted Access Platform Software Integration Working Group](#)
- 5. [COmanage Institutional Component Reference Architecture](#)
- 6. From a few years ago:
 -