LInk to 2018 ACAMP wiki

Advance CAMP Friday , Oct. 19, 2018

9:10am-10:00am

Oceana 4

COmanage Unix Support/Federating HPC

CONVENER: Kevin Hillebrand

MAIN SCRIBE: Tom Jordan

ADDITIONAL CONTRIBUTORS:

# of ATTENDEES: 15

DISCUSSION:

Anyone already doing federated SSH login for HPC clusters?

UNC Chapel Hill - requiring people to have sponsored accounts currently, want to try to get away from that. Sponsored accounts require criminal checks so take some time.

Kevin - want to be able to leverage COmanage to create a parent CO and organizational units to provision LDAP and posix groups to allow delegated access to cluster. Also want to be able to publish SSH keys into LDAP. Also exploring the idea of PAM doing a callback to a web browser. Another alternative is an ASCII QR code (Slavek).

OSC Open On Demand - can do VNC, SSH, remote job submission and monitoring.

Duke - protected research enclave deals with restricted data, has some things like On Demand but without HPC specifics. Can take a federated user with a set of attributes and push them into AD and manipulate what they can see. ProConsul - locally developed, out on github.

ECP as a possible solution? ECP to establish the session and then make a backchannel response.

Project Moonshot? Relies on GSSAPI, so need to integrate SSH with GSS-SAML.

Two tracks - what's the right solution long term vs. what's an appropriate workaround today? A simple case that's not ideal is eligibility feeds between campuses that frequently collaborate.

Problem statement - unix support in COmanage to provision users, homedirs, etc and then SSH integration. OIDC token in password field and then let everything else read it - implementation available from Globus. Globus provides a wrapper around SSH to allow it to establish an OIDC token on the client. Client side stays vanilla, but the server side needs the wrapper.

https://www.incommon.org/docs/iamonline/20170913_IAMOnline.pdf
(does someone have a better link?)

Range of solutions for federated SSH, each has their own issues - client customization, etc.

Can also use ECP to get a certificate from CILogon (transient, users do not need to be aware). Also needs custom SSH. Some folks seeing an increase in HPC users that don't know how to use SSH.

Provisioning accounts - COmanage proof of concept for provisioning to LDAP and Unix cluster. Is the right approach to have COmanage provision these accounts directly or provision to a management system that then does something with them? Design is established but has been #2 priority.

Pacific Research Platform / National Research Platform - is there a group that we could work with in this space? Ongoing calls to discuss what the national research platform should be. Could also look internationally (CERN, etc).

Consider possible conferences for discussions - PERC(?), others?
Outside of 'big iron' environment, need for federation in HPC is growing. Life sciences, etc. Where do AWS and Google fit? Still some reticence from LIGO, etc. Some concerns about changes needed for software stacks but inevitable that folks will start to explore. Might not make

sense right now for persistent compute needs, but for short-term scaling could be beneficial. Some ideas around scheduler support for bursting to cloud to deal with workload.

NIH is pushing a more cloud-focused model. Several proofs of concept (gen3 as example) to try to make cloud simpler for researchers. Globus Transfer and Globus Auth are a key part. Grouper is another case of a provisioning engine - doesn't create unix users but could deliver info into something that could. GID management and cluster permissions are things that could be accommodated either by grouper or COmanage. Could do separate LDAP servers per cluster or could leverage LDAP plugins or cluster config to filter results.

What's needed to improve the capabilities in COmanage? Money helps to drive priorities, also availability of resources. More community pressure can help the project adjust priorities.

Also some need to consider how config management fits in - Puppet, etc.

ACTIVITIES GOING FORWARD / NEXT STEPS:

1. Survey CASC members to determine priority for COmanage to support provisioning / managing Unix users, groups, etc

=====

Note: please be sure to link to or attach any key resources from this breakout session