input to software projects breakout session notes

TomD's Notes from Breakout session -- providing input to perMIT and Grouper projects

Scenario - We have an IDM application but not a centralized AD, we are looking at bringing up a central AD to support sso and file sharing.

Do we want folks to use the Identity Manager or some other way?

a/Hill- We have been running enterprise group management at MIT for sometime and feeds AD. The groups are mostly adhoc and managed by end users . There are over 200,000 groups with about 24,000 active users.

If you wanted to use institutional data use ldappc to push the data into AD.

a/hyzer - Grouper has three ways of pulling data : sql-loader, web service interface and ldappc

For pushing data, it is the upcoming Grouper notification / change log for incremental provisioning out (or read from ldap or web service)

There are other ways like permit to solve a set of problems other than simply group membership e.g. MIT perMIT

a/Hill - in perMIT "canwrite to file share" " filesharename" these can be flattened to a group name for groups based access

a/hyzer - attributes will connect to groups, folders, memberships, or subjects. We will be able to support hierarchies of roles, permissions, and of course group memberships so you can have as elegant (or complicated) a structure as you want create long names groups , to minimize having to create long names

a/hyzer- for small groups , less than 500 , doing ad hoc groups is not much of a burden.

a/hyzer - begins to talk to a use case with two classes sharing a fngileshare, one reading and one reading and writing

function = (can create video, can read video, can write critique, can read critique)

1. get data from lms and populate subjects into permits

a/hyzer-Grouper would populate groups with the memberships of the two classes and add an attribute to designate the "verb"/function

a/Hill- with a well developed application they are likely going to use for example AD security descriptors for all authorization, you can set a registry key so that group membership are not passed in kerberos tickets

q; What will most linux kinds of applications do?

a: java acegi or ldap calls

q: we have a master admin accounts system , users are mapped to role and sources(secondary identified source) how can perMIT support roles?

q: Are you talking about traditional rbac roles?

a: yes

a: perMIT has some role concepts : primary authorizer, principle investigator,

q: Do you support workflow?

a: Not really, the roles maybe be part of the authorization system

Discussion about precalculating memberships in nested groups

q: Does the permit have to know about a subject before it can be assigned or can users type a random but unique string

a: in general folks felt this was unwise and the subject name had to be verified

q: Should group information be kept in saml assertion?

a: No particular needs expressed except a desire from CMU's KS implementation to have the option given their web services implementation

q: Have you looked at implementing Kuali authorization services on top of perMIT

a: yes and for the KS service definitions we think we can implement it as a layer

q: How do you support Confluence?

a: Confluence has an ldap plugin but you had to do authenication via ldap at one point, an option can allow you to use shib for authentication. There ldap connector doesn't support ldap mods .