Teragrid Gateway Authentication Directions

Tony Rimovsky

Dane Skow

Current Authentication

- Primary method of access is interactive shell
  - Accounts are created based on allocation award
  - Special type of allocation called Roaming which allows users to roam between resources
  - An implication of roaming is that user accounts are created on all resources
  - There are currently approximately 4000 Teragrid users and 20 resources
  - Teragrid, in combination with the resource providers, is responsible for administrating all of the accounts, including handling applications and vetting of users

Current Authentication (cont)

- Gateways
  - Each gateway is given a “community account” and by default jobs for that gateway are run through that account and allocation.
  - The gateway is responsible for managing their own users
  - The gateway is responsible for tracking usage and being able to tie it back to users for reporting and troubleshooting.
  - The gateway is required to provide the ability to backtrack to users in the event of a security incident.
  - Anticipate that most of the targeted growth in users (doubling) will be through the gateways.

Issues with current system

- Roaming
  - Creating accounts for every user on every resource
    - Increases number of idle accounts - isn't safe
    - Doesn't scale
    - Is inefficient
  - Some resources aren't well suited to open roaming
- Gateways
  - Security issues with arbitrary code via community accounts
  - Accountability dependencies for TeraGrid
  - Single community account for each gateway is rarely ideal.

TeraGrid™

New Directions

- Move towards attribute based authentication for:
  - Gateways
  - Roaming

Charlie Catlett: “We want to improve the ability of campus researchers and students to access TeraGrid services. In a nutshell, I'd like to see campus credentials used to access TeraGrid services, meaning that obtaining a TeraGrid allocation involves, among other things, adding a new authorization attribute to the user's existing credentials (or in their credential mapping server, etc.).”

New Directions (cont)

- Authentication
  - Use campus authentication mechanism such as Shibboleth
    - Some questions of trust here. We are at the point where campuses rely on these services for financial transactions for their students. This seems like a reasonable point to begin trusting them.
  - TeraGrid RPs will likely continue their own services initially as translator and/or because campus auth services are not universally available or robust.
  - Accept authentication credentials from peer grids (GIN agreements)

New Directions (cont)

- Gateway changes
  - Gateways would pass attributes through to TeraGrid resources
  - Gateway usage would map to accounts based on research project rather than an entire portal behind one account
  - Attributes would be passed through to system instrumentation to allow TeraGrid staff to associate users to activities (for diagnostic purposes as well as forensic).
  - Addresses arbitrary code problem because it is essentially back to the same level of accountability we use today.
- Roaming changes
  - Roaming usage would move from interactive shell to GRAM submission