



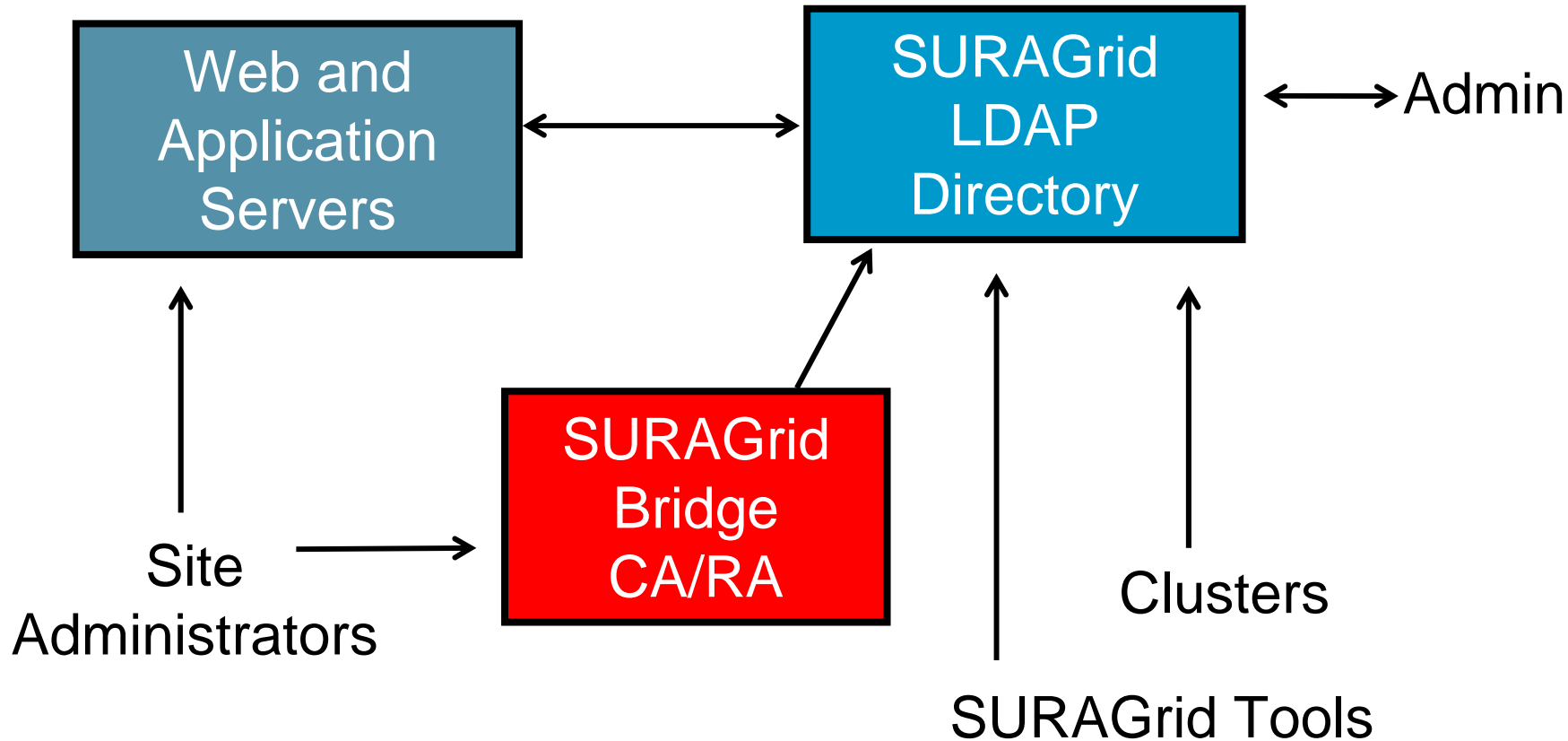
SURAGrid AuthN & AuthZ Background & Tools

Jim Jokl

September 22, 2006

University of Virginia

Tools Infrastructure Components



Background and Level Setting

- SURAGrid's [PKI Bridge infrastructure](#) supports Grid Authentication
 - Technology validation
 - Anticipated future interactions with HEBCA, Federal Bridge, Commercial, etc
 - Globus does not use bridge-aware PKI path validation logic (it uses OpenSSL)
 - Requires pre-loading of cross-certificates
 - Pre-loading of signing policy files
 - [Hand configuration](#)

Tools #1 & #2: Basic PKI Automation

- A [script](#) that handles the proper installation of your CA certificate, its associated policy file, and certificate hash symbolic link
- Cross-certificates are stored in the [site record](#) of the SURAGrid LDAP server
- A [tool](#) was developed to automatically retrieve the correct set of cross-certificates, build the appropriate symbolic links, and generate the policy files

Background and Level Setting

- The Globus Toolkit uses PKI for authentication of users and resources
 - Sites new to Globus often have difficulty creating and operating their PKI Certification Authority
- Cross-certification of a site's CA is also often a stumbling point that leads to delayed implementations

Tool #3: Campus Grid CA Creation

- [Documentation and automation](#) of the setup of the Globus SimpleCA package for use on SURAGrid
 - How-to documentation
 - Scripts that automate the work
 - Handle the PKI cross-certification tasks

Background and Level Setting

- Globus maps PKI Subject Distinguished Names (DNs) to local Unix IDs
 - “/C=US/O=University of Virginia/OU=UVA Standard PKI User/emailAddress=jajatvirginia.edu/CN=James A. Jokl 82" jaj
 - Maintained in the grid-mapfile
 - Cumbersome to maintain
 - Prone to typo's
 - Must be maintained on each Globus gatekeeper

Tools #4 - #6: Grid Mapfile Automation

- SURAGrid user management [web interface](#)
 - Creates and maintains [user entries](#) in the SURAGrid LDAP directory

- SURAGrid Globus LDAP [callout module](#)
 - Direct Globus integration for fully automated site
 - Can be used in conjunction with a grid-mapfile
 - Must compile source code in your Globus environment – source code based on NMI

- SURAGrid grid-mapfile integration [tool](#)

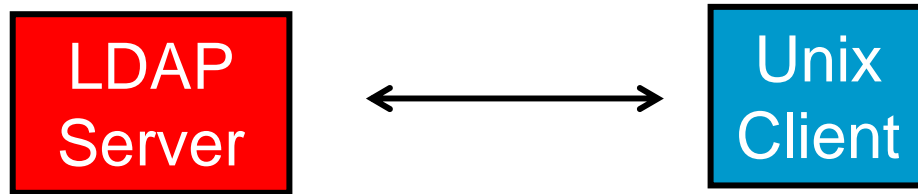


Background and Level Setting

- Globus assumes that standard Unix user accounts exist on all systems
 - Password file entries
 - Name, UID, GID, shell, etc
 - Home Directories
- This can be painful to manage in a large inter-institutional system
 - Researchers come and go
 - Scalability to dozens of sites, large number of researchers and students

Tools #7 & #8: User Account Automation

- SURAGrid LDAP server contains posixAccount schema data
 - [Automate](#) replacement of Unix password files via nsswitch.conf



- A tool could also be written to synchronize other password file databases with the LDAP server
- A Home Directory creation [Perl script](#) is also available to complete the automation package

Background and Level Setting

- SURAGrid's AuthN/AuthZ plans evolved over several years via in-person meetings and conference calls
 - Initial focus was on a PKI Bridge for AuthN
 - Solving the complexity of cross-cert distribution
 - Operating the process and helping sites
 - Site automation and scalability came next
 - Global namespace for automation & accounting
 - Coordinated Unix UIDs & GIDs (NFS, perm, etc)
 - Multiple levels of site automation

What tools should my site use?

- The tools were created to enable
 1. Fully automated sites that simply use the web management interface
 2. Intermediate sites that just want to use the certificates and grid-mapfile automation systems
 3. Sites that do not wish to participate in the automation (accept root certs and Subject DNs for users manually)
 - Could still leverage naming and LDAP as a

Some Future Possibilities

- LDAP replication
- Use of additional authorization attributes
- Integration with UMich (or other) accounting package
- Two-tier assurance PKI
- Other directions
 -



Questions and comments?

Thank You