

Using Radiant Logic for Multi-Forest Active Directory Synchronizations

Thomas E. Board
Director, IS Architecture
Northwestern University



Agenda

- Summary
- About Higher-Education
- Situation at Northwestern
- Constraints
- Radiant Logic Solution
- Experience
- Future plans



Summary

- We are using RL to push identities into multiple AD forests
- Two links:
 - Identity and attributes
 - Password
- Privacy mandates require internal coding



About Higher-Education

- The bad-guys can be within your perimeter and domain
- The community:
 - May see security management as endangering freedoms, privacy, or as a discretionary expense
 - Is often highly decentralized – reliance on central units and even central systems may be seen to slow innovation
 - Usually does not respond well to mandates – especially if conforming costs money
 - Generally communicates poorly about the correct handling of information

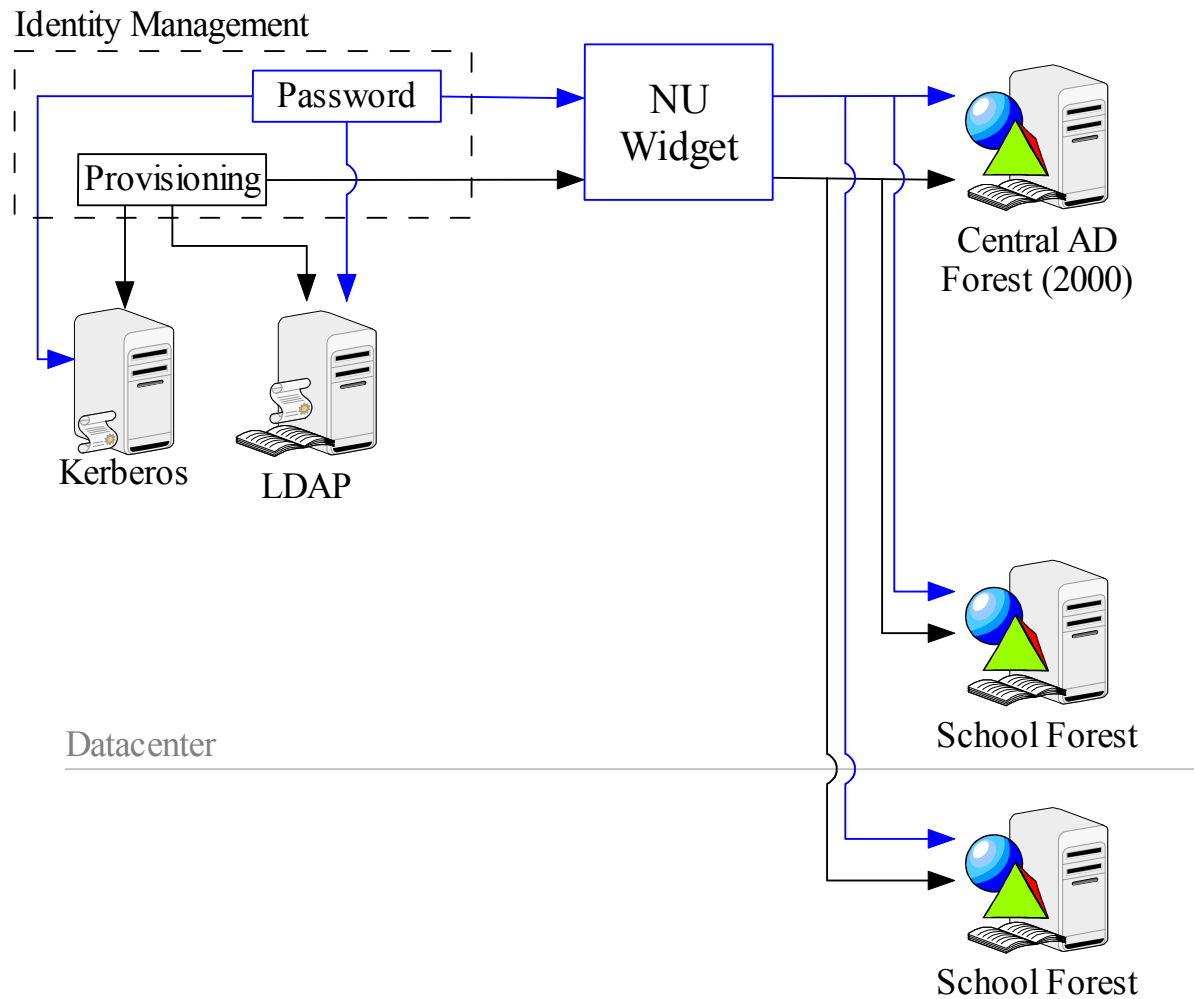


Situation at Northwestern

- Active Directory was not centrally deployed until after several schools had local instances
- Desire for single identity & password prompted development of a link from the IdM system to the AD instances
- The local link uses a now-deprecated NT4 API, and is limited to transferring name, group memberships, and password



AD Services Circa 2004



Change Drivers

- Enrich the set of attributes moved into AD instances
- End dependence upon the deprecated NT4 interface
- Maintain affordable level of customization to meet higher-education quirks
- Avoid costly technology “lock-in” to MS solutions



Constraints

- Privacy
 - Family Education Rights and Privacy Act (FERPA)
 - University policies allow blocking access to certain location information
 - AD-based LDAP services reveal too much information to searches after user bind – central IT cannot guarantee configurations in all AD forests
- Security
 - Replication of single password across multiple directory services outside of central IT direct control



Radiant Logic Solution

- Radiant Logic 4.2 on dedicated platform
- Local classes invoked by the Java “transformation scripts”
- Configuration for each target forest is cached in a persistent object to minimize the cost of reading the configuration. The last-modified time of configuration files is checked at 10 minute intervals



Radiant Logic Solution

- Our provisioning model assumes that forest administrators may move User objects into any OU.
 - We create new User objects in a default OU, and setting the common name (cn) and the short login name (SAMAccountName) to our local “NetID” username.
 - Whenever updating, we search for the a User object by SAMAccountName to determine the current DN.



Other Local Code Work

- Ignoring specific users and OUs
 - “Ignored” users are not changed in AD in any way
 - There are global and per-forest lists of usernames to ignore
 - We can ignore users based upon DN suffixes, either ignoring users in, or not in, specific OUs



Other Local Code Work

- Selecting which users are active and are sent to each forest is based on simple Boolean combinations of LDAP attribute,value tests
- Populating AD groups from LDAP attribute,value pairs (using Radiant Logic helper classes)



Other Local Code Work

- Filtering attributes to comply with AD schema restrictions (AD produces cryptic errors if schema constraints are violated)
 - discarding blank or empty values for most attributes because they aren't allowed
 - truncating attributes; for example displayName is limited to 64 characters
 - selecting a single title from several alternative locations (because the AD title is single valued)

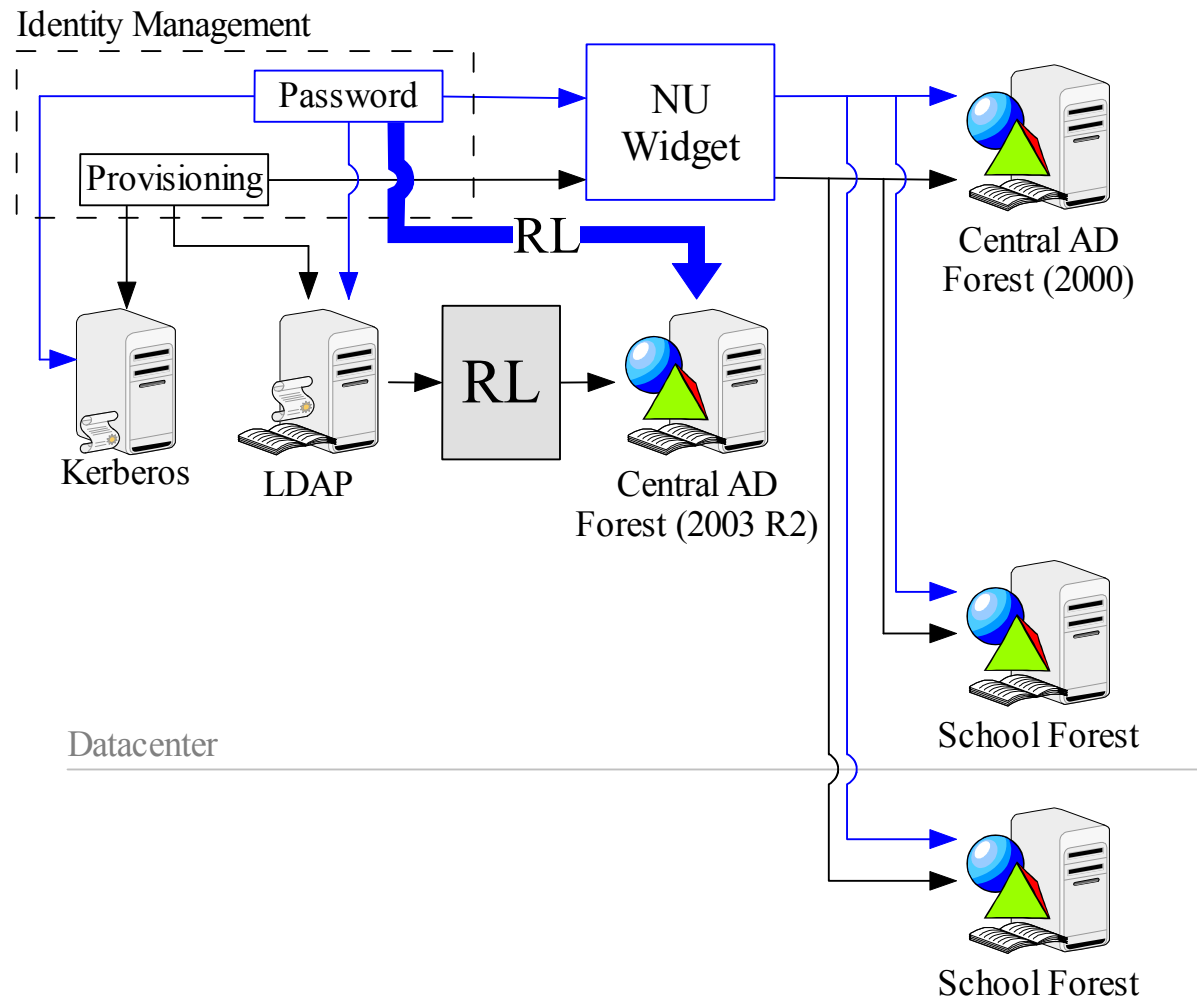


Other Local Code Work

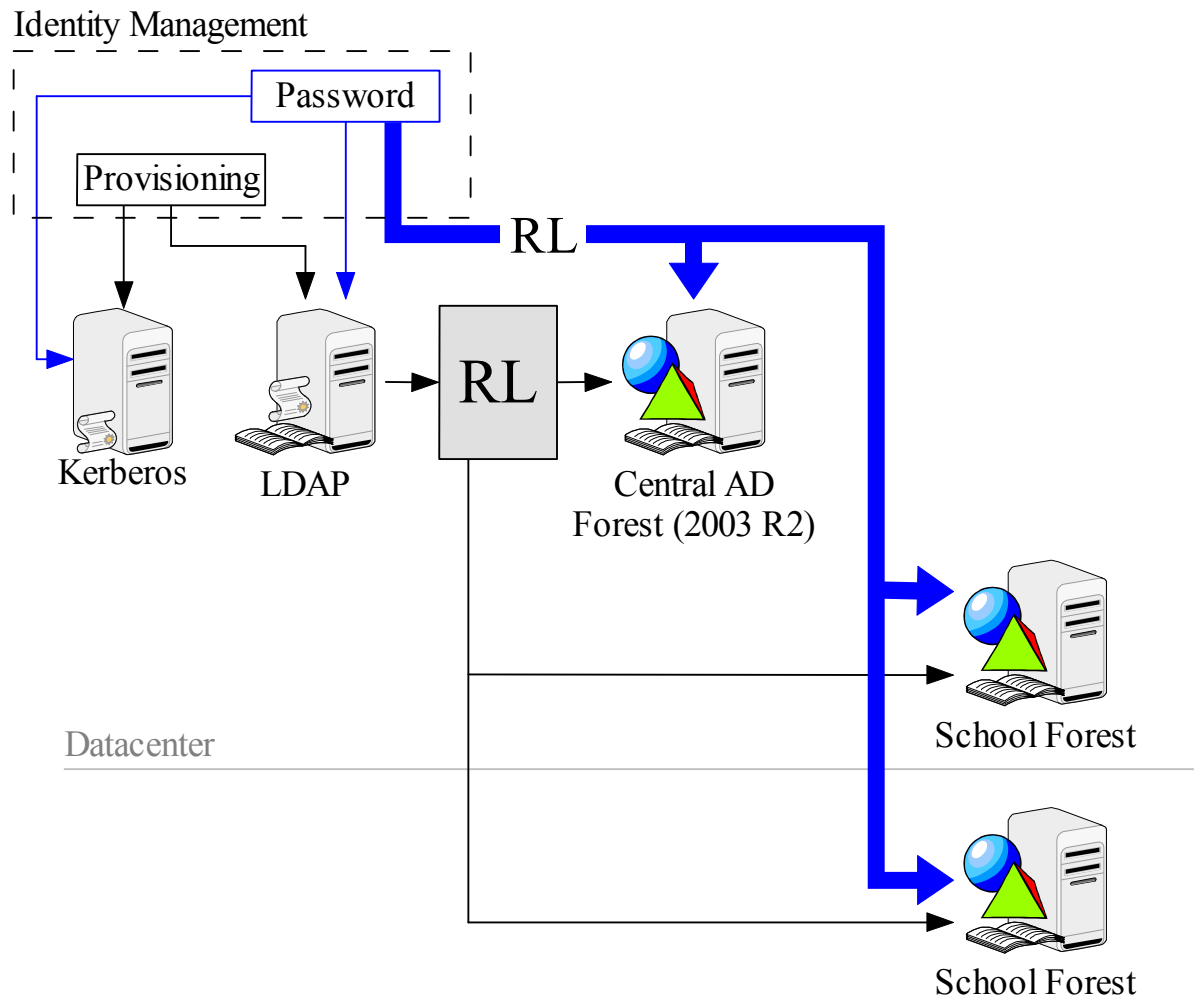
- Filtering attributes to hide users as per privacy policies (FERPA and other local policies)
 - “Hidden” users have a stub entry useful only for authentication
 - Few required attributes are changed to UNLISTED
 - Other attributes are cleared
- Making AD Users active/inactive by setting flags in in the AD attribute userAccountControl



Initial RL Deployment



Topology in 12 Months



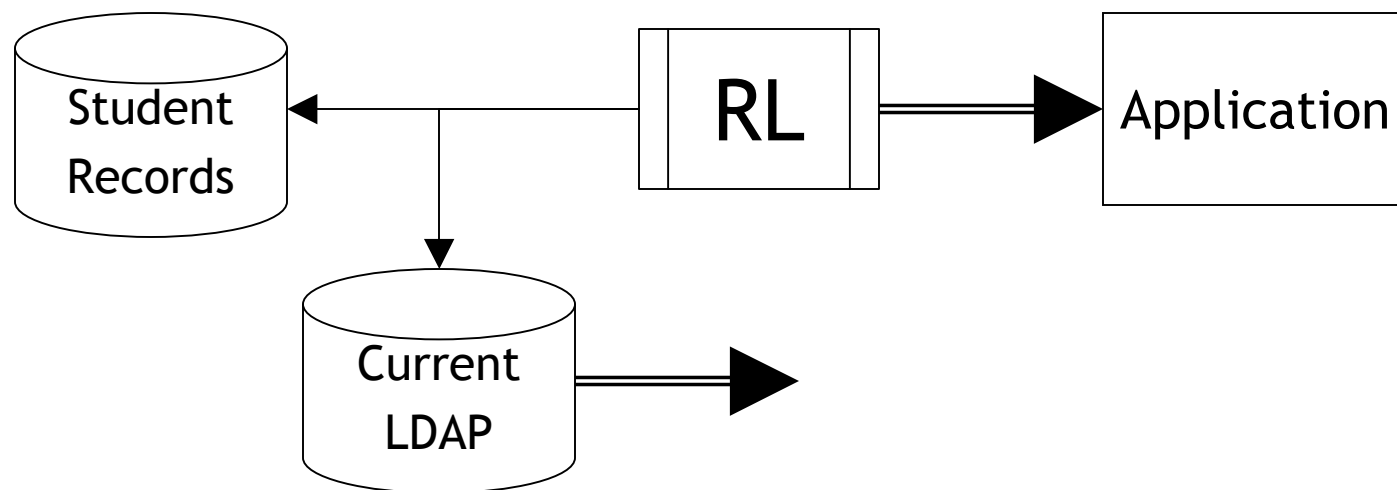
Experiences

- Most issues were traced to constraints within AD itself – were we really pushing that far into the corners?
- Technical support has been very good
 - Assisting with fringe cases
 - Decoding documentation
 - Hands-on via secure VPN
- No problems with software releases

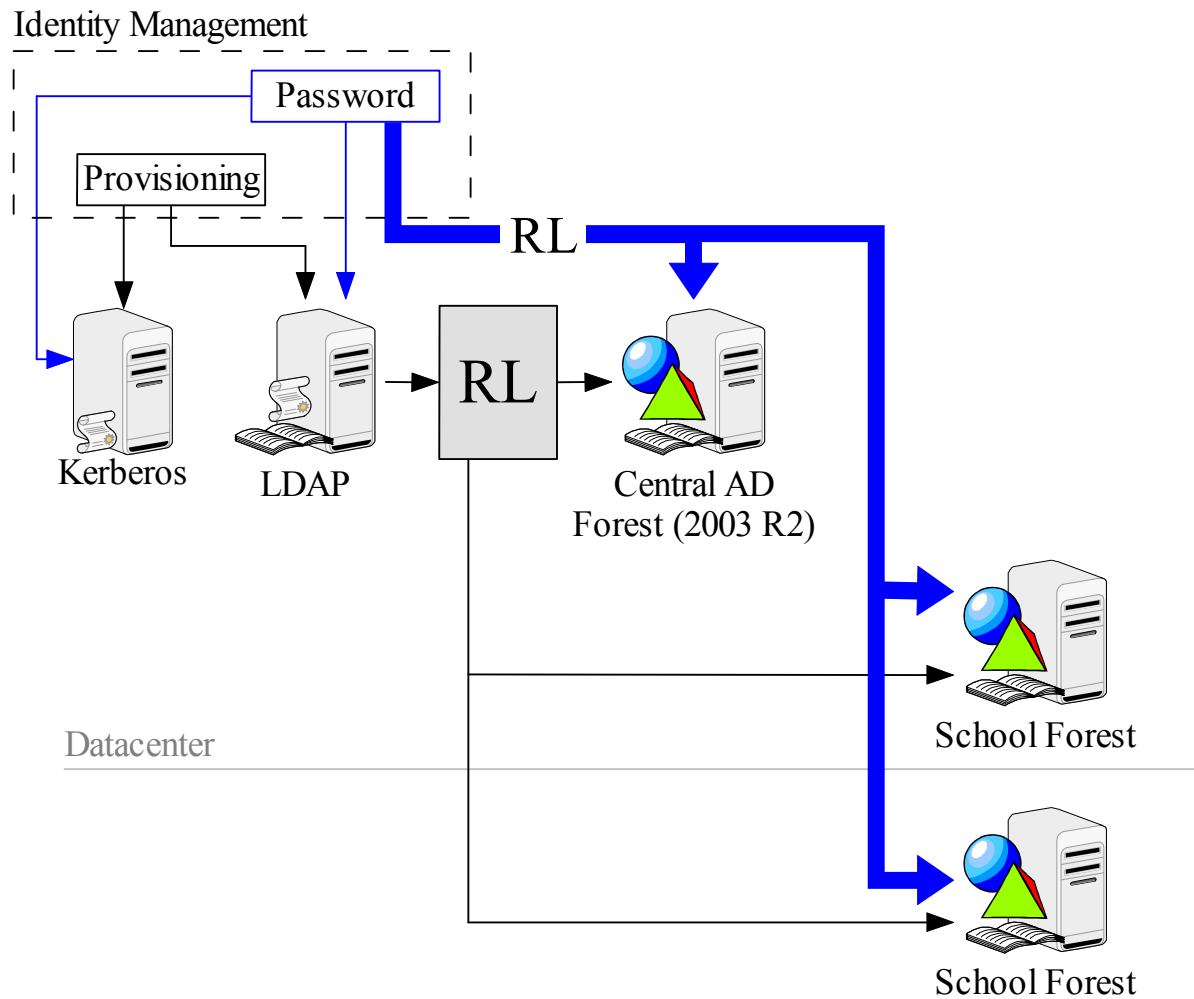


Future Plans

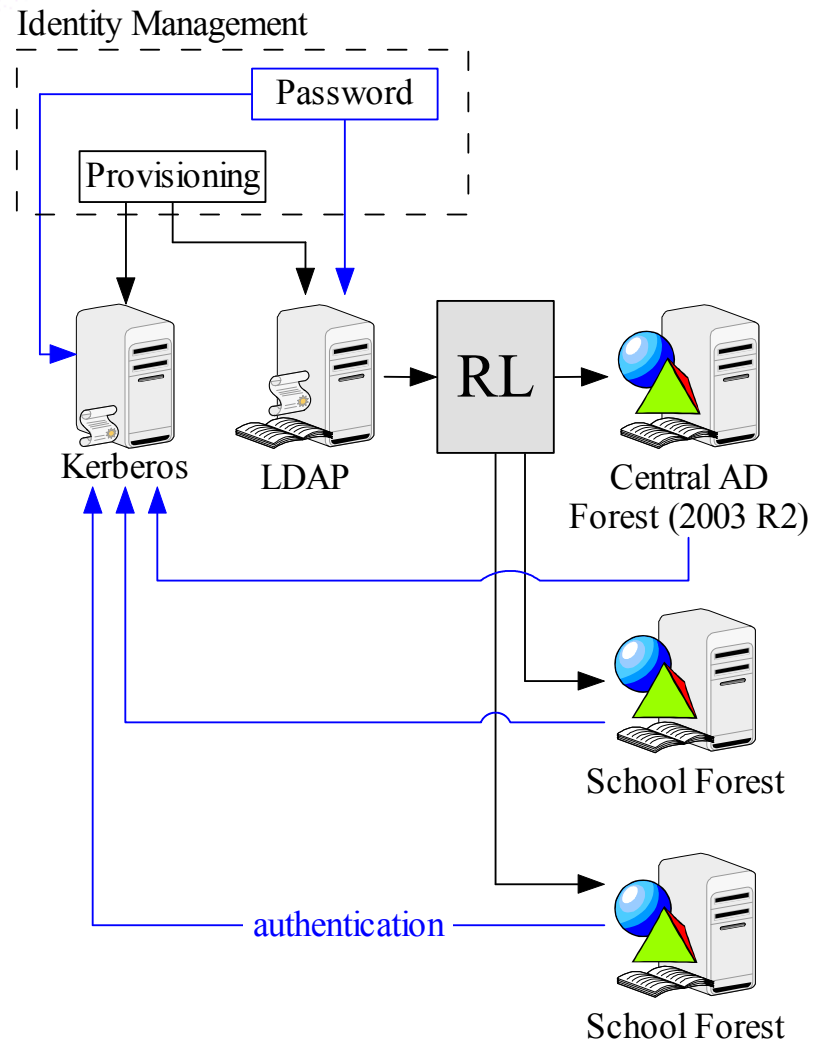
- Investigate AD password abstraction
- Investigate traditional virtual directory deployment as special LDAP service to handle protected information



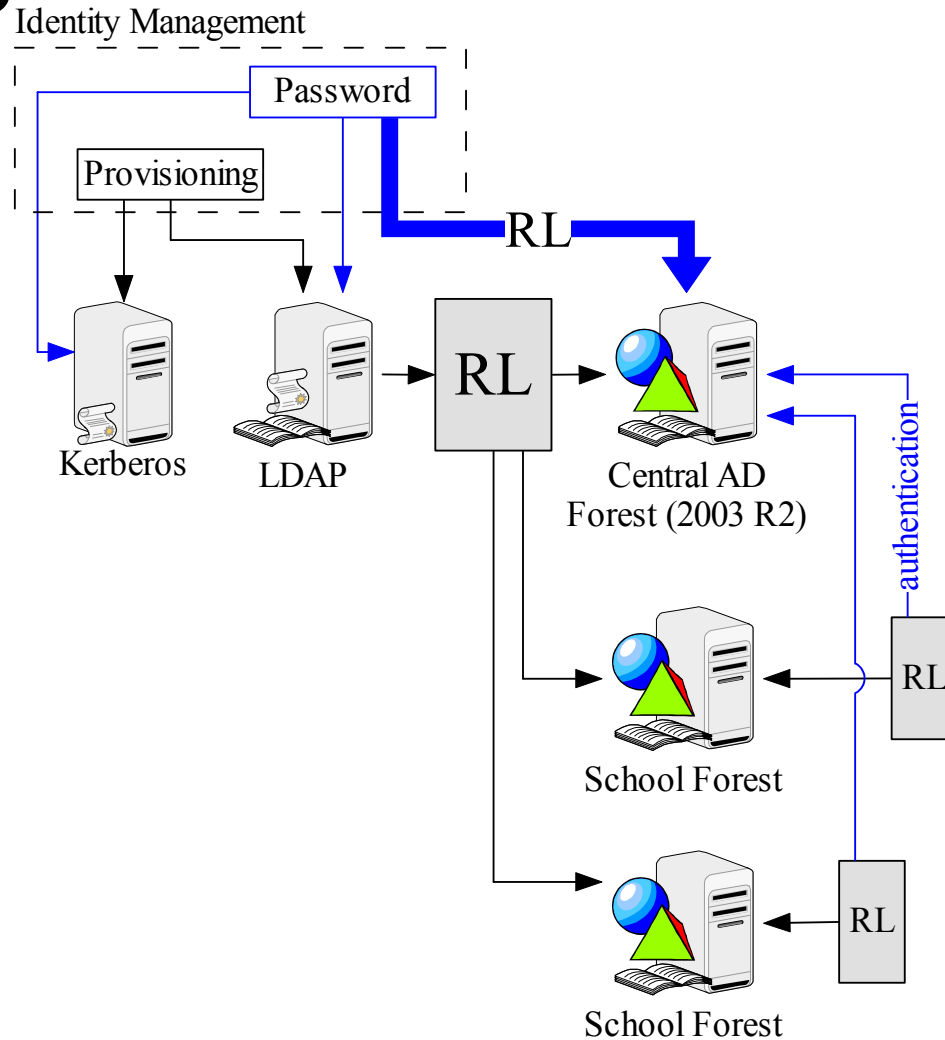
MS-Constrained Structure



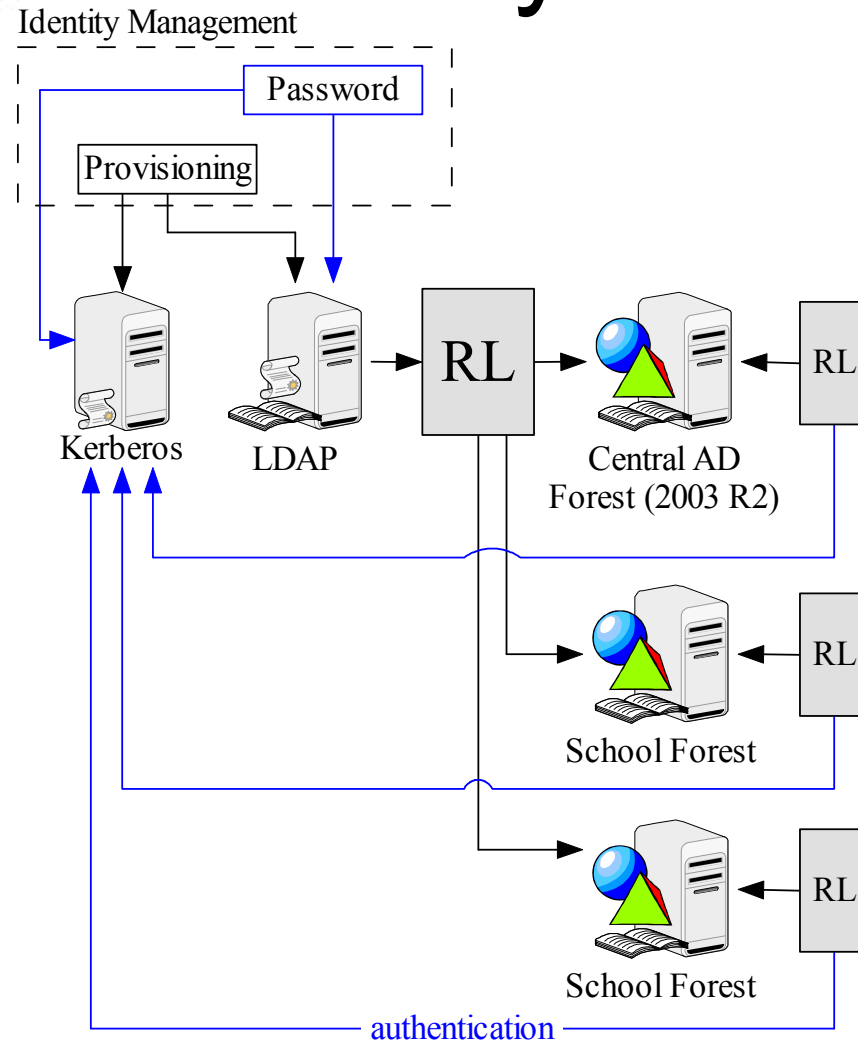
AD Password Abstraction



Single Password Instance

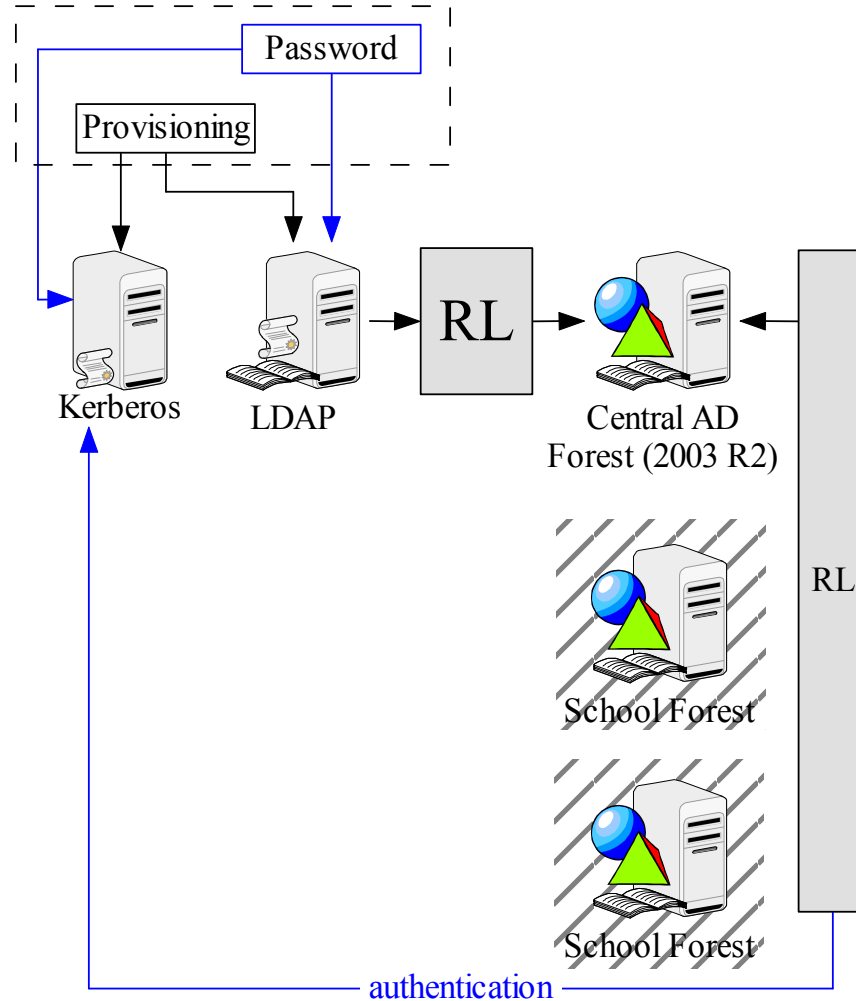


Virtual Directory Abstraction



AD Service Virtualization

Identity Management



Questions?

Q & A

