LDAP Options Subtrees and Composite attributes for Identity

LDAP Options, Subtrees and Composite attributes for Identity

DATE and TIME: Friday 26 May 2001, 10:00 - 11:00 am

CONVENER: Roland Hedberg, Michael Gettes

SCRIBE: Keith Hazelton

# of ATTENDEES: 10

Attendee	Institution
Roland Hedberg	Umea University
Benn Oshrin	Internet2 Middleware
Todd Piket	UMN
Michael Gettes	CMU
Billy Cook	Clemson U
Jeremy Grieshop	Clemson U
Jim Green	Michigan State
Michael Pelikan	Penn State
Emily Eisbruch	Internet2
Keith Hazelton	UW-Madison

MAIN ISSUES DISCUSSED

Take email address: (the "attribute option" specifies the intended use or purpose of each value of email address)

We agreed to call these structured attribute values "Guises", which is the term that Roland Hedberg popularized in Scandinavia

MichaelP We took a vote: Implement a separate DB that has same data as directory, use DB to provide "operational data store" services

KeithH: What about the Subentry approach, putting subtrees under the person object?

Roland, MichaelG: attribute options are SO much easier for the app developer; it also works with LDAP Browswer

Keith: Python module to get/set guises? The essential RESTfulness of subentries

MichaelP: person orgUnitDN, orgUnitPrimaryDN pointers to entries in the organizational hierarchy

Todd: I appreciate that...but

MichaelG: DSGW in 389directory; templating file for options...

Todd: ePPA from 8 institutions in the system

eduPersonScopedPrimaryAffiliation ? New eP attribute??

Billy Cook: The CU Vault at Clemson University

RolandH: we've been running directory services for 23 years. Sweden ended up with some not-very-specific guidelines on how to implement. Everyone does it differently still today. Lots of apps have very specific views of what should be in the LDAP directory. App-specific LDAP directories. We did it, but apps are becoming more intelligent, and don't assume they can dictate what is in the directory nowdays. Our LDAP directory is read-only except for SuperAdmins. Our ADs are provisioned from same source as LDAP. That's where writes happen.

JeremyG: Plugins to OpenLDAP seems to work well for transformation of attribute values

MichaelG: Big fan of 389; OpenLDAP is riddled with problems in a production env. Indices that get broken; Multi-master replication doesn't work. It's the code and not doing the proper locks, etc. 389 is open source. There's a plug-in that does Kerberos right.

389 Directory Server, descended from Fedora Directory (Red Hat), descended from AOL, iPlanet, netscape, Dixie (Howes, Smith, Good). 389DS implementation is very close to Sun LDAP implementation.

KeithH: I'll ask RobCarter for permission to publish that Kerberos plugin for 389DS that he and Michael did.

Benn: Ordering of multivalued attributes would be a win, too.

MichaelG: Do you really want to standardize on the values or do you want people to pay attention to the capabilities and let them come up with their own solutions

Benn and Michael argue about standards and their value.

SUMMARY FROM REPORT OUT TO THE LARGER GROUP : Multiple approaches for handling structured data in LDAP, including composite attributes. OpenLDAP v. 389 v. others, and comparisons will be written up for reference...

ACTIVITIES GOING FORWARD / NEXT STEPS

[ACAMPScribe:Todd Piket] Send writeup of issue statement for eP{Scoped}PA

[ACAMPScribe:Roland, MichaelG, Keith] Writeup The Options: 1) Why would you ever want to do this in LDAP? attr. options, composite attributes, sub-entries, ... Start with use cases. Bake-off.

[ACAMPScribe:Keith] Ask Rob Carter for permission to use the 389DS plugin that he & Michael Gettes wrote to handle Kerberos "the right way".

REQUESTS

RESOURCES