Infrastructure - Task #3513

Task # 3394 (Closed): Deploy Shibboleth provider for KNB LDAP accounts

Task # 3395 (Closed): Deploy Shibboleth instance at UCSB

Determine accounts to include for KNB IdP

2013-01-23 17:50 - Ben Leinfelder

Status:	Closed	**Start date:**	2013-01-23
Priority:	Normal	**Due date:**	
Assignee:	Matthew Jones	**% Done:**	100%
Category:		**Estimated time:**	0.00 hour
Target version:	2013.10-Block.2.1		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

We manage many accounts for many different kinds of users with different organizational affiliations and institutional agreements. When we set up one (or more) IdP services against these accounts we need to determine which accounts should be used where and what kind of migration strategy we want to employ.

History

#1 - 2013-01-23 17:50 - Ben Leinfelder

Trees to consider:

ou=Account (1000+ users)
o=NCEAS (469)
o=KU (32)
o=MSU (14) -- recommend ignoring these accounts
o=NAPIER (4)
o=OBFS (66)
o=OSUSB (7)
o=SDSC (27)
o=unaffiliated (5000+)
o=UVM (3)

Referrals:

o=LTER -- they have set up their own IdP and those users should use that for authentication
o=PISCO -- consult with them about direction to go. Perhaps they would like to become an IdP as well.
o=SANParks -- perhaps roll them into our larger "KNB" IdP. Need to consider international policy here.
o=SAEON -- similar to SANParks. Consult with Judith and Victoria about this
o=UCNRS (126) -- they may be using these accounts for other operations within their organization

#2 - 2013-01-23 17:59 - Ben Leinfelder

- Assignee changed from Ben Leinfelder to Matthew Jones

Proposal for preparing NCEAS IdP:

Use ou=Account as the root for the NCEAS IdP

Move accounts from o=XXX into ou=Account where uid does not collide and the user should continue to have affiliated status with NCEAS.

If account from o=XXX exists in ou=Account use the latter and reset password

Map all ou=Account accounts to the old o=XXX identities using a pre-computed CILogon DN (from them)

Other considerations:

Maintain additional IdPs for each distinct organization we wish to support so that we keep them distinct and can provide identities at different levels of assurance (basic vs silver, etc).

Notably, o=unaffiliated contains the bulk of our accounts but with no assurance that they are real people with useable email addresses. This is very different than the o=NCEAS tree which is well-curated and contains people with which we largely have first-name familiarity.

By maintaining o=unaffiliated as an independent IdP we let our existing user base continue to access their account, but via a different mechanism.

Referrals:
TBD

#3 - 2013-03-01 18:55 - Ben Leinfelder

- Target version changed from 2013.2-Block.1.1 to 2013.10-Block.2.1

#4 - 2013-03-09 20:16 - Ben Leinfelder

- Parent task changed from #3394 to #3395

#5 - 2013-04-26 18:17 - Ben Leinfelder

- Target version set to 2013.10-Block.2.1

#6 - 2013-04-26 18:17 - Ben Leinfelder

- Target version deleted (2013.10-Block.2.1)

#7 - 2013-08-29 22:51 - Ben Leinfelder

- Status changed from New to Closed

- translation missing: en.field_remaining_hours set to 0.0