Infrastructure - Task #3444

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

Setup a prototype IdP for identity.nceas.ucsb.edu

2013-01-02 23:15 - Ben Leinfelder

Status:	Closed	**Start date:**	2013-01-11
Priority:	Normal	**Due date:**	
Assignee:	Ben Leinfelder	**% Done:**	100%
Category:	Support Operations	**Estimated time:**	0.00 hour
Target version:	2013.10-Block.2.1		
Milestone:	None	**Story Points:**	
Product Version:	*		

Description

The is the general story for tasks related to setting up the KNB/ecoinfo LDAP as a CILogon identity provider that includes ECP support.

We've been evaluating ECP for our client tools and realize that a minority of IdPs support it. Therefore it makes sense to set up our own so that we do not strand our existing user base.

History

#1 - 2012-12-12 16:59 - Ben Leinfelder

- Target version set to 2013.2-Block.1.1

#2 - 2013-01-02 23:22 - Dave Vieglais

See also #3394

#3 - 2013-01-11 00:15 - Ben Leinfelder

- Parent task set to #3394

- Subject changed from Setup an ECP IdP for ldap.ecoinformatics.org to Setup an IdP for ldap.ecoinformatics.org

Moving to existing IdP story

#4 - 2013-01-11 00:19 - Ben Leinfelder

- Start date set to 2013-01-11

- Estimated time set to 0.00

- Status changed from New to In Progress

I have the Shibboleth IdP 2.3.8 software deployed on mn-demo-5.test.dataone.org. It is configured to use ldap.ecoinformatics.org. Internal tests show that it is correctly configured. I am awaiting instructions from CILogon on how to integrate with them for a roundtrip ECP test.

#5 - 2013-01-11 17:49 - Ben Leinfelder

We are now a (test) identity provider called "DataONE Test" -- https://test.cilogon.org/testidp/
I've tried both the browser-based and ECP-based authentication and both work great.
The identities we release are in the ou=Account tree of ldap.ecoinformatics.org so anyone with an account there should be able to authenticate via CILogon.

Next up: sociopolitical considerations for standing up an IdP "for real"

#6 - 2013-01-15 18:10 - Ben Leinfelder

- Subject changed from Setup an IdP for ldap.ecoinformatics.org to Setup an IdP for ldap.ecoinformatics.org (prototype)

- Status changed from In Progress to Closed

Marking this as the POC/prototype for what we might do in "production" (even though we are using production identities on a test IdP server right now).

#7 - 2013-01-16 21:11 - Ben Leinfelder

Deploying IdP on mn-demo-5.test.dataone.org

Installation source: /usr/share/shibboleth-identityprovider-2.3.8
$IDP_HOME: /opt/shibboleth-idp
Using SP metadata for InCommon ($IDP_HOME/conf/relying-party.xml): http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml
Upped the valid range in the filter to 30 days (from 7 days) to allow InCommon metadata. Not requiring trust of their metadata because I'm not sure where to get their credential.

Configured "IdPAuthRemoteUser" using basic apache auth with LDAP in the apache site configuration. Needed to also set tomcatAuthentication="false" in the AJP connector (Tomcat server.xml)

Configure attribute filters:
https://spaces.internet2.edu/display/InCCollaborate/Configure+a+Shibboleth+IdP+to+Support+R+and+S

Configure attribute resolver for LDAP, using the attributes in the filter above (attribute-resolver.xml). Uses ou=Account tree when communicating with LDAP server.

Use aacli.sh to test the release of attributes. Had to copy servlet-api.jar into the shibboleth lib directory and include --requester=

Secure the ECP endpoint using http basic auth like before: /idp/profile/SAML2/SOAP/ECP
https://mn-demo-5.test.dataone.org/idp/profile/SAML2/SOAP/ECP

CILogon then needed our IdP metadata to set us up on their end as an IdP (in their test area). See the "DataONE Test" idp here:
https://test.cilogon.org/testidp/

#8 - 2013-03-01 18:55 - Ben Leinfelder

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

#9 - 2013-03-06 00:36 - Ben Leinfelder

- Subject changed from Setup an IdP for ldap.ecoinformatics.org (prototype) to Setup a prototype IdP for identity.nceas.ucsb.edu

This "DataONE Test" IdP is now configured to authenticate for both ou=Account and o=unaffiliated LDAP subtrees. Care should be taken when using UIDs that exist in both trees because attributes from both accounts will be released no matter which DN actually authenticated.

#10 - 2013-04-26 18:17 - Ben Leinfelder

- Target version set to 2013.10-Block.2.1

#11 - 2013-04-26 18:17 - Ben Leinfelder

- Target version deleted (2013.10-Block.2.1)