

EZproxy at UChicago

Motivation

EZproxy has been central to the University of Chicago's plan to adopt Shibboleth. We see a Shibboleth-enabled EZproxy as a way to provide three key values:

1. ***A consistent single sign-on method for remote electronic resources while the resources themselves will be split between Shibboleth and IP-based authentication.*** This is accomplished by relying on the EZproxy configuration to contain only those resources requiring proxied IP address access, and letting ILS technologies such as SFX continue to produce URLs with the EZproxy prefix for all resources. For Shibboleth-protected resources not appearing in EZproxy's configuration, EZproxy redirects the user browser directly to the resource, and the Shibboleth transaction proceeds without further involvement of EZproxy. It is also possible to tune the EZproxy configuration so that on-campus access can be proxied without requiring a login, provided the resource provider continues to offer IP address-based access protection in addition to any Shibboleth access protection.
2. ***Incorporation of access to remote electronic resources within the campus single sign-on domain, along with other Library services and services offered by other parts of the campus.*** This is accomplished by protecting the campus Shibboleth IdP with the campus web integrated sign-on service (webISO), so that the union of local webISO, local Shibboleth, and remote Shibboleth resources form a single logical single sign-on domain.
3. ***Ability to conditionally proxy access to an IP address-protected remote electronic resource depending on the affiliation or other attributes of the user.*** This is accomplished by configuring a Shibboleth Attribute Release Policy to provide EZproxy with appropriate attributes about authenticated users. These attributes are used in EZproxy configuration declarations to associate users with groups of resources, enabling central management of which classes of users are enabled to access which sets of remote resources. This is also an aspect of value #1, in that as a resource becomes Shibbolethized, user attribute information will continue to determine conditional access to the resource. The difference is that with IP address based access, the campus EZproxy does the policy enforcement, and with Shibboleth the resource provider does the enforcement.

Maintenance

The University of Chicago has 438 entries in its EZproxy configuration file at this writing. We have more than that number of electronic subscriptions, but many subscriptions coexist on the same platform. For most services, proxying occurs at the domain level, but a few are proxied at the host level.

Of the 438 entries, 365 entries require no special configuration. 73 entries have some special configuration directives, mostly minor tweaks. There are just a handful of entries that have major configuration requirements. To our knowledge, all databases are currently fully functional; granted a correct configuration, none are hobbled by going through EZproxy.

Most of the solutions to configuration problems come from the EZproxy website or, if our Electronic Materials Assistant cannot figure it out, the EZproxy mailing list. The most common problem is that a service provider may use an internal domain that is not already in our configuration file.

All of the configuration entries are maintained by the Electronic Materials Assistant. Most entries are simply domain names or host names that are exported from a database of subscriptions into a CSV file. More complex configurations are maintained in EZproxy configuration syntax, a key-value text file. These two feeds are exported in CSV format and sent to central IT, which runs EZproxy. These two feeds are merged with other configuration elements from other parts of campus to produce the actual configuration file.

Tom Barton
Tod Olson