Domestication Guide

How to Integrate Domesticated Applications with COmanage

Introduction

The domestication of an application involves the proper installation of the application on the COmanage server and proper use of COmanage infrastructure to externalize authentication, group membership, and privilege management. This document will guide developers in all of those aspects.

Installation

Native Debian Package

Installation in the form of a Debian package is preferred. Detailed information on creating Debian packages can be found at:

- Create Debian Linux packages
- Official Debian Packaging documentation

In the process of the post-install, the package should make use of the COmanage Perl module to request LDAP and MySQL accounts.

Tarball Installation

NOTE: Tarball installation is NOT preferred because it makes inventorying, auditing, and security patching difficult.

Tarballs will be extracted into /opt. They should provide a bootstrapping script that COmanage can run to finish the installation after the tarball is expanded. This script should make use of the COmanage Perl module to request LDAP and MySQL accounts.

Authentication

To externalize authentication, domesticated applications should rely on Shibboleth. Shibboleth is an Internet2 project that allows federated authentication with minimal release of information. Domesticated applications should look for eduPersonPrincipalName in the headers. Additional information about this user, including displayName can be gathered from the LDAP directory by searching for eduPersonPrincipalName in cn=people,cn=comanage.

Authorization/Privilege Management

As in the general case, authentication should never imply authorization. Authorization into the application and within the application should ideally be externalized to Signet. An application should use the Signet API to access the privilege information stored on the COmanage infrastructure.

> Is this really our answer for authorization? Is Java the only version of the Signet API? Is there a document that shows how the Signet information is expressed in LDAP so additional APIs can be developed?

Group Membership

Membership in groups is maintained by Grouper. This information can be accessed by direct searches in the LDAP directory under cn=groups, cn=comanage. Entries under this branch will have objectClass groupOfNames and multivalued attribute member which will contain the distinguished name (dn) of each member of the group. To translate this into a list of eduPersonPrincipalNames, the dn can be parsed to isolate that value. To expand this into a list of displayNames, the LDAP directory can be queried for displayName for each DN that is a member of that group.

> Is there an API for accessing this information? If grouper is doing anything besides a flat tree in cn=groups using the groupOfNames objectclass with enumeration of member, than we should document that here.