University of California Santa Cruz Project Page

UC Santa Cruz Deployed Grouper in Summer 2015. We have the unique situation where our IT Services org structure changes with some regularity. Therefore much of our design hinges on minimizing the impact of an IT Services org change while maintaining service operation. We have therefore kept the top level structure simple.

We have adopted UCLA's concept of a top level ucsc stem to allow for federated grouper across the UC-Trust mini federation. As the University of California has been encouraging campuses to create cross campus services. It may become important to understand what the authorization levels of off campus accounts are. After that we have a simple top level structure.

Stem	Friendly Name	Description
ucsc: org	ucsc: Organizations	This houses the delegation and permission structure. This is based on the current org chart. Changes here impact levels of delegation
ucsc:p	ucsc: POSIX	Posix account stem. Groups here should not change once they are established. The structure is relatively flat. The service name folder and then the groups themselves. Caution should be exercised with long names as many posix based systems can't display long group names.
ucsc: svc	ucsc: Services	This stem is used to house the effective groups. Service accounts will look at the groups here to determine access. The top level below this will contain the major organization, for example "ITS", "School of Engineering", or "Financial". Under the organization the service being provided is named as a folder, for our Data Center VPN project the following is the stem structure where the groups are located "ucsc:svc:its:dcvpn" This allows the effective groups to remain in a static place, even if the delegation of permissions change withing the ucsc:org stem.
ucsc: ref	ucsc: Reference	For any groups that have a campus wide definition, we place that group here. Some examples are "Students", "Employees", "Faculty", etc. Currently not all of these exist since global definitions are not always easy to enforce across campus. Typically services will have their own definition of what a group of people are and these will need to be constructed from primitive groups.

First use case is VPN access control.

For more info, Jeffrey Crawford

See Also

Campus Groups from UC Santa Cruz IT website