**UC Davis IT Infrastructure Futures
Access Subgroup Recommendations**

**Members: Curtis Bray, Bob Brewer, Paul Drobney, Adam Getchell, Roger Hess, Chip Mrizek, Hemang Patel, Mark Redican, Larry Ross, Uwe Rossbach, Gary Sharpe, Jatinder Singh, Paul Singh, Lowell Valiant.**

**The IT Infrastructure Futures Access subgroup prioritized six discussion topics:**

|  |  |
| --- | --- |
| Category | DiscussionPriority |
| DNS | 5+ |
| LDAP | 5 |
| Active Directory | 5 |
| Certificates | 5 |
| IAM | 4 |
| DHCP | 0 |

**Recommendations and Discussion Summary**

**DNS:** This workgroup recommends moving the existing bind-based Unix DNS servers to a mix of both bind-based DNS for external (public) DNS queries and access with the Microsoft DNS servers for internal DNS queries and access, with the root of Active Directory (AD) using the ucdavis.edu DNS namespace.

The existing campus Infoblox infrastructure can be used to manage Microsoft DNS (Infoblox is a Microsoft Gold Partner).

A risk assessment and evaluation on the business impact of changing the core campus DNS servers to a Microsoft-centric DNS should be conducted.

**LDAP:** There is an existing campus LDAP service while uConnect Active Directory also provides this functionality. The ITIF Access workgroup recommends updating any attributes within uConnect AD to match that of campus LDAP in the short-term. For the long-term LDAP recommendation, the ITIF Access workgroup does recommend the campus begin looking at integrating Microsoft LDAP through attrition of services and as product life-cycles are reaching end-of life, for those applications or services using the campus LDAP. This will allow us to safely phase-out the redundant campus LDAP service.

**Active Directory:** Since the DNS of uConnect AD is recommended to be rooted at ucdavis.edu top-level domain (see DNS above), the existing uConnect AD Forest will have to be modified or migrated to assume this higher namespace, as it is currently rooted at a sub-domain level, ad3.ucdavis.edu.

A risk assessment and evaluation on the business impact of changing or migrating the existing AD3 Forest structure should be conducted. Also, a review of other Universities which have gone through a similar migration should be conducted.

**Certificates:** The ITIF Access workgroup recommends a method for obtaining personal certificates, such as for email, should be provided by campus. Workstation certificates for IPSec security along with can be utilized by a certificate service integrated with uConnect AD.

The workgroup recommends having the uConnect certificate services become an intermediary Certificate Authority (CA) service, which then has a trusted-chain with a public CA. This will prevent any non-trusted certificate errors for those clients/applications requiring a public CA certificate.

**IAM:** The group felt the Identity and Access Management (IAM) project was too far along and the campus deeply involved financially for this group to provide any additional input on its direction. Most everyone in the group is not involved in the IAM project and do not feel they have enough information to provide a valuable contribution. The suggestion from the group for the IAM discussion is more information should be disseminated, as most in the group did not know the status of this project.

**DHCP:** The group felt an adequate campus DHCP solution was already in place and further discussion on this topic is not warranted.