

## **Information on Questions Submitted for Review**

After the completion of the Information Technology Needs Assessment, information was put together for a peer review of the Oklahoma State University Active Directory environment. Information was submitted to Yale University, University of Missouri System, and Southwest Missouri State University. The three questions asked of the peers were:

1. Does our environment fit best practices for an Active Directory implementation?
2. Does the implementation of all users within a single organizational unit with automated provisioning fit best practices?
3. Does the delegation of permissions in an organizational unit fit best practices?
4. Does our DNS implementation fit best practices? Is there anything in AD DNS, which needs to be modified in order to make better use of the BIND DNS and AD DNS relationship?

Below is a compilation of the information.

### **Fitting Best Practices:**

Each of the institutions was very complimentary of the environment and the documentation put together on the environment. None of the institutions saw problems with the design of the directory. They were impressed with our upfront planning. Nothing was determined to be problematic.

### **Location of User Accounts:**

Two of the three institutions (Missouri & Yale) have their User accounts in a single container. Southwest Missouri State University currently has three based on the person's primary role.

Quote from Missouri – “I'm glad to see your decision to put all the user objects in one container - I think it'll help keep your creation process a lot cleaner.”

Southwest Missouri State University – “We don't keep all of our user objects in the same OU as you do. We currently divide users into three main categories: Faculty, Staff, or Student. Each of these categories has its own OU. In the new Active Directory we will probably break into two categories: Employee, Student. We move the account objects between OU's if their primary role changes. I wouldn't call it a "Best Practice" but it is the organizing principle on our end and it works well for us.”

Quote from Yale – “The vast majority of our user accounts exist in a single OU which is actually named "Users" though the name means little. We have a user accounts office which is responsible for creating and maintaining all user accounts and other groups are

forbidden (by both university policy and limitations on AD permissions) to create users for any reason.”

Since many areas have had concerns over this topic, IT also talked with the University of Colorado, the University of Texas and the University of Kansas. All three of them have their users in a single container as well.

### **DNS Setup:**

Yale University has a similar hybrid DNS setup as ours. Quote from Yale – “Our AD lives partially in our "main" namespace (our root is yale.edu) and partially outside it (ad.yale.edu DNS zone) but also functions by delegating blocks of the namespace to Windows DDNS servers. I did a lot of work when W2K came out trying to figure out how to blend DDNS with static BIND servers and this system works very well.”

The University of Missouri System currently has a hybrid DNS set up as well. They are reviewing the possibility of removing AD DNS from their environment. They are still in the testing phases to see if this will work for them.

Quote from SWMS – “When we first implemented Active Directory we made the mistake of following the Microsoft recommendation to make the Active Directory namespace for DNS the same as the University's internet domain, SMSU.EDU. This was a huge mistake, particularly since the group that controls the Active Directory is not the same group that controls the DNS servers. As we are building our new Active Directory this summer, in conjunction with our name change, we are moving to a separate DNS namespace for the Active Directory. The campus DNS namespace is changing to MISSOURISTATE.EDU, but the Active Directory namespace is going to be EDUBEAR.NET. We will be using Active Directory integration DNS from Microsoft and only allowing secure updates. It is critical to only allow secure updates.”

Since DNS is an integral piece, research was also found at websites set up by the University of Colorado and the University of Berkeley, who also have a similar hybrid AD/BIND DNS Set up.

### **Conclusions:**

Based on the information received back from this peer review and information pulled together from ITC meetings, IT will be performing the following projects:

- AD Permission Updates – IT will be updating ITC permissions on each OU based on the matrix outlined in previous meetings. A working group has been formed to review options for login script updates. Members of the Server Administration team will meet with each ITC after the login script solution has been finalized to

review OU settings, set up the login scripts, go through the administrator's guide and discuss any questions about day to day operations.

- DNS Review – IT will review its DNS setup to maximize the usage and minimize the impact to services being provided.
- User Account Information – IT will continue to enhance Okey Admin services to provide additional functionality to ITCs to perform day to day operations. Okey will continue to serve as the authoritative identity provisioning system for the Oklahoma State University System.