Introduced with Windows 2000 Server, Active Directory (AD) is Microsoft’s implementation of a directory service. At its most basic level, a directory service can be defined as a customizable information store used to locate and access network resources. User accounts, computers, groups, etc. are easily managed in AD because they can be organized in meaningful ways.

One of the primary benefits of AD is that it allows decentralized management of these network resources. Administrators from different departments can control and maintain their own network resources and also participate in a centralized directory service. While this is very useful for enterprise networks, care must be taken to ensure that differing policies, or lack thereof, do not impair the sustainability of the AD forest.

The purpose of this document is to create a standard set of rules and guidelines for participating in PSU’s AD forest. Adhering to this document’s recommendations will create a more straightforward, stable, and secure AD environment.

**Organizational Units:**

Organization units (OUs) are the building blocks of AD. They work in a similar fashion to file system folders. OUs can be created and deleted with ease to delegate permissions and keep AD objects organized. PSU’s OU structure looks something like this:

```
PSU.DS.PDX.EDU
    |  People
    |  Resources
        |  MyDepartment
            |  Admins
            |  Groups
            |  Printers
            |  Servers
            |  Service Accounts
            |  Test
            |  Workstations
```

**People OU**
All standard user accounts are stored in the People OU. Administrative access to this OU is restricted to Office of Information Technologies (OIT) staff only.

**Resources OU**
The Resources OU contains most other AD objects such as computer, group, and printer objects. This is where special rights can be given to individual departments if they wish to manage their own Resources sub-OU. These rights include:

1. Creating/Modifying/Deleting computer, group, printer, and shared folder objects.
2. Application of Group Policy Objects (see below for explanation of GPOs).

**MyDepartment OU**
Departmental OUs reside inside the Resources OU and contain the AD objects managed by a particular department. As a best practice, each departmental OU should contain separate sub-OUs for Admins,
Groups, Printers, Servers, Service Accounts, Testing, and Workstations. For most departments, few additional OUs are needed. In general, it is best to use security groups rather than additional OUs to apply group policy and organize AD objects.

User Objects:

Account Creation
User accounts are centrally managed. All new AD user accounts are created through the OIT account creation system (https://www.account.pdx.edu/) or by OIT staff only.

Elevated Privilege Accounts
Administrators who have elevated privileges should request a second user account from the OIT-CNS Server Team. This elevated account should never be used to logon directly to a desktop workstation. Use the elevated account for server logon and running single instances of administrative utilities such as Active Directory Users and Computers on your desktop computer.

Note: To run a single program with elevated privileges on your desktop use the “Run as…” feature. To do this, hold down the shift key and right-click on the program you would like to run. Select “Run as…” and enter your elevated account credentials.

Service Accounts
AD-only service accounts may be requested by OU administrators, and will be created at the discretion of the OIT-CNS Server Team. A service account should only be used by systems that need to perform a specific task requiring AD credentials. Service accounts should never be used by individuals. OU administrators are responsible for actions performed by their service accounts, for periodically changing service account passwords, and for disabling unused service accounts.

Test Accounts
AD-only test accounts may be requested by OU administrators, and will be created at the discretion of the OIT-CNS Server Team. OU administrators are responsible for actions performed by their test accounts, for periodically changing test account passwords, and for disabling unused test accounts.

Computer Objects:

Every AD member computer running Windows NT, Windows 2000, Windows XP, or Windows Server 2003 has an AD computer account. Similar to user accounts, computer accounts provide a means for authenticating and auditing computer access to the network and to domain resources.

Naming Convention
The PSU naming standard for computers is:

dddd-compID

  dddd  Department code (i.e. OIT or HR)

  compID  Computer’s location/function OR primary user’s name OR primary Ethernet card’s MAC address OR some other unique identification

For example, a receptionist machine in the Telecom department used primarily by John Doe and with a MAC address of 00-0C-F1-E5-5B-91 should be named:

TELE-FRONTDESK or TELE-DOE or TELE-000CF1E55B91

Page 2 of 5
Revised 5/9/2006
Joining Computers to the Domain

When computers are added to the domain they first appear in the Computers OU. Objects in this OU should be immediately moved to the appropriate Resources OU. Objects that are left in the Computers OU will be moved to the Resources\General\Computers_unidentified OU.

Each user account is allowed to join 10 computers to the domain by default. Administrators who need to join more computer objects or move objects out of the Computers OU should submit a request to the OIT-CNS Server Team.

Group Objects:

Setting up security groups is one of the most important aspects of AD administration. Improper group setup can cause serious security gaps in addition to an organizational nightmare.

Types
There are two types of groups in Active Directory: distribution groups and security groups. You can use distribution groups to create e-mail distribution lists and security groups to assign permissions to shared resources.

Distribution groups are used with applications such as Microsoft Exchange and are not currently used at PSU.

Scope
There are three group scopes: universal, global, and domain local.

UNIVERSAL GROUPS
• Should NOT be used in the PSU domain.

GLOBAL GROUPS
• Are logical groupings of people based on their location, job responsibilities, etc.
• Should be created when a logical grouping of users exists that may need to be referenced more than once
• Should never be granted access to a resource directly
• Should contain only user and other global group objects as members
• Should be named after the group of people it represents

DOMAIN LOCAL GROUPS
• Are defined to grant an explicit set of permissions to a resource
• Should be created for each resource access will be granted to and never used except for that resource
• Should generally not be nested inside another domain local group
• Should contain user and global group objects only
• Should be named after the resource and level of access granted

Naming Convention
The PSU naming standard for AD groups is:

```
dddd_groupName_accessLevel_groupType
```

- **dddd**: Department code (i.e. OIT or HR)
- **groupName**: Name that describes the global group member relationship, or the domain local group resource
**accessLevel**  Domain local groups only, access level abbreviations are:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FC</td>
<td>Full Control</td>
</tr>
<tr>
<td>Mod</td>
<td>Modify</td>
</tr>
<tr>
<td>RW</td>
<td>Read/Execute and Write</td>
</tr>
<tr>
<td>Read</td>
<td>Read/Execute</td>
</tr>
<tr>
<td>List</td>
<td>List Folder Contents</td>
</tr>
<tr>
<td>Apply</td>
<td>Read and Apply (GPO’s only)</td>
</tr>
<tr>
<td>Adv</td>
<td>All other access levels, use the description field to explain</td>
</tr>
</tbody>
</table>

**groupType**  Group type abbreviations:

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>GG</td>
<td>Global Group</td>
</tr>
<tr>
<td>LG</td>
<td>Domain Local Group</td>
</tr>
</tbody>
</table>

**Example**

**Scenario**
Computing and Network Services (CNS) has a project folder that needs to be shared amongst its employees. Management and staff need to be given full control of this folder. Student employees need read and execute access.

**Solution**

**Step 1 (create/verify global groups)**
The following three GLOBAL groups should be created if they don’t already exist:

- CNS_Management_GG
- CNS_Staff_GG
- CNS_Students_GG

**Step 2 (create domain local groups)**
The following two DOMAIN LOCAL groups need to be created:

- CNS_ProjectShare_FC_LG
- CNS_ProjectShare_Read_LG

**Step 3 (give the domain local group(s) appropriate permissions on the network resource)**
Open the properties page for the project folder and click on the Sharing tab. Share the folder and change the share permissions to allow Full Control to the Everyone group. Click on the Security tab and add the two DOMAIN LOCAL groups to the list (be sure to remove groups such as Everyone if they exists here). Give the CNS_ProjectShare_FC_LG group Full Control of the folder and give the CNS_ProjectShare_Read_LG group Read & Execute permissions.

**Step 4 (make global groups and/or individual users members of the appropriate domain local group)**
Using Active Directory Users and Computers, check to ensure that the global groups have the correct membership. Make the CNS_Management_GG and CNS_Staff_GG groups members of the CNS_ProjectShare_FC_LG group. Make the CNS_Students_GG group a member of the CNS_ProjectShare_Read_LG.

*Note: Whenever possible create global groups to define logical groupings of individuals, but do not create global groups for the sole purpose of populating a domain local group. Create global groups only if that grouping may eventually be used or referenced in some other context.

**Benefits**
Using the example above as a template for setting up access to network resources makes it extremely easy for administrators to see exactly who has access to what. Simply open a user or group object and trace the group memberships to reveal the precise access level and resource.
**Group Policy Objects:**

Group policy objects (GPOs) are used to define default settings that will be automatically applied to user and computer objects in AD. Policy settings can be used to manage desktop appearance, assign scripts, redirect folders, set security options, deploy software, etc.

**New GPOs**
Requests for new GPOs should be directed to the OIT-CNS Server Team.

**Naming Convention**
The PSU naming standard for GPOs is:

```
dddd function
```

```
dddd       Department code (i.e. OIT or HR)
function    The GPOs function or purpose
```

For example, if OIT User Support Services (USS) wanted to create a group policy to restrict access to desktop display settings, the GPO could be called “USS Restrict Display Settings”.

**Loopback Feature**
The group policy loopback setting (located at “Computer Configuration\Administrative Templates\System\Group Policy\User Group Policy loopback processing mode”) is very useful in our environment. Because PSU’s user objects are centrally managed, User Configuration settings cannot be directly applied to user objects by OU administrators. The loopback option gets around this issue by allowing User Configuration settings to be applied based on the workstation a user logs on to. See the “User Group Policy loopback processing mode” explanation tab for more details on this feature.

**Miscellaneous**

**Tips**

1. Add good descriptions to all AD objects whenever possible.
2. Use standard abbreviations carefully. Make them obvious enough to be recognized by the entire campus and be consistent in their use.
3. Consider creating a security group called DepartmentName_Workstations_FC_LG and add it to the local Administrators group on all your workstations. By populating/editing the members of this group, you’ll be able to centrally control which users in your environment have administrative access to your workstations.

**OIT-CNS Server Team Contact Information**
E-Mail: cns-server@lists.pdx.edu
Phone: x5-9566

**Author**
Ryan Bass
Active Directory Administrator
Computing and Network Services
Office of Information Technologies
Portland State University