Active Directory Setup
IN719 Systems Administration

Introduction

Active Directory Domain Services (AD DS) is, at its heart, a database that stores information about users, groups, computers, and other entities in a network. It's a complex and powerful tool for managing networks and we will only get a small taste of its functionality in this paper. We're primarily interested in it because it will provide us with a centralised database of users for our web application later in the semester. You already have some experience with this. Have you noticed that you can log into a variety of services on campus with the same user name and password? That's AD DS. On the other hand, have you been annoyed by the fact that you have to supply the same username and password multiple times? AD DS could probably solve that, but it's complicated.

1 The problem

Today our goal is to configure our AD DS Domains and add a few users to it. We'll also crack open PowerShell briey to see a little bit about how it works with AD DS.

2 Configure AD DS

Carry out the following steps:

1. Log into your ad server and open the server manager.

2. Install Active Directory Domain Services by selecting Add Roles and Features, selecting the AD DS option, and following the installation wizard.

3. Choose to add a new forest. Use "directory.foo.org.nz" as your domain name. Click next.

4. Click the little yellow triangle at the top right and select "Promote this server to a domain controller".

5. Set your functional levels to Windows Server 2012 R2. We don't need to maintain compatibility with any older servers.

6. Select the DNS server option. (We may not even need it, but just in case.)

7. Choose and note your restore password. Click next.

8. Don't worry about the DNS delegation. It's not a problem for us. Click next.

9. The default NetBIOS name is fine. Click next.

10. The default paths are ok, but note that this is where your AD DS data will be stored. That's important when we plan backups. Click next.

11. Use the "View Script" option to save a script that can be used for an unattended install if you need to estore your domain. This script is the kind of thing that should go in your source code repo.

12. Run the prerequisites check, you'll see some messages but your setup should pass. The click install. Your server will require a reboot (?!). That's the kind of event that you should document on your wiki.

After the reboot:

1. Use the Active Directory Users and Computers tool to add domain accounts for everyone on your team. Make those users members of the Domain Admins group. Note that these new accounts are distinct from the local system accounts you created earlier.

2. Create a new Organizational Unit in your domain called "OwnCloud Users."

3. Add a new domain account for a user named Joe Bloggs inside the organizational unit.

N.B.: The purpose of the organizational unit is to hold the user information for users of the web application we'll set up later in the semester. We want an easy way to identify the users of our web app without including all of the other kinds of users in our domain.

3   View our users with PowerShell

Open Powershell and run the following command:

```
Get-ADUser -Filter * -SearchBase ''dc=directory,dc=foo,dc=org,dc=nz"
```

This should produce a list of all the user accounts in your domain. Note especially the value of the dc (domain component) items in the *Distinguished name*. Now run the following:

```
Get-ADUser -Filter * -SearchBase "ou=OwnCloud Users,dc=directory,dc=foo,dc=org,dc=nz"
```

What's the difference in the lists? Do you see why? Now experiment with other SearchBase strings. Can you write a query that returns only your user account? The purpose of this is to get a sense of the LDAP structure of AD DS.