IS 404 - Lab 8: Microsoft Active Directory

This lab will introduce you to Microsoft’s flagship permissions management suite - Active Directory. You will learn how to create your own Domain, configure a server to be a Domain Controller, and set up Users and Groups within your Domain.

# Before you begin

As a reminder, your network configuration should be the same as last lab.

Today, you will setup an active directory account. This will use the following naming convention:

* Your Active Directory (AD) Domain will be
  + *<Lab Session#> - <Station>*.404labs.islab.**local** where
    - <Lab Session#> This is the number of your assigned lab session; Use the following numbers depending on which lab you regularly attend
      * Thursday Morning – 1
      * Thursday Afternoon – 2
      * Friday Morning – 3
      * Friday Afternoon – 4
      * Some Other time – 5
    - <Station> is your workstation number
    - **E.g., If you are in the Thursday afternoon lab session on station 15 your active directory domain is 2-15.404labs.islab.local**

# Lab Setup

1. Start your Virtual Machines (VMs). **Hint**: make sure there are no other 404 VMs running or you will get IP address conflicts. If other 404 VMs are running suspend them (Action **🡪** Save)
2. *Load your configuration on your ASA firewall*
   1. Copy your saved configuration to the startup configuration.
      1. Use dir to see the files on your ASA
      2. Use the copy command to copy your configuration to the startup-config.
         1. e.g. copy flash:<filename> startup-config
   2. Reboot your firewall (reload)
   3. After your firewall boots, test connectivity between your firewall and all your VMs.
3. Verify that each computer can access the internet by browsing to Google (or any other site).
   1. NOTE: If you get an error trying to connect to the web site that says you are blocked because of IE Enhanced Security, turn off IE Enhanced Security using the Server Manager.

# Exercise 1: Create an Active Directory Domain & Primary Domain Controller

### Overview

In this exercise you will install Microsoft’s Active Directory server and create a primary domain controller to allow resource sharing across your network.

### Objectives

* Install and configure Active Directory
* Create Primary Domain Controller
* Change domain password policies and allow for local login to the domain controller

### Installing Active Directory on your Corporate server

General Steps

* Install Active Directory on your Corporate Server
* After you finish installing active directory, you still will not be able to start active directory. Why not? \_\_LS1\_\_

Detailed Steps

1. Active Directory is a role that you add to your **Corporate Server**. You can add the role from the **Server Manager**. Look for the **Roles Summary** section then click the **Add Roles** link.
2. Follow the Add Roles Wizard to add the **Active Directory Domain Services** software. Add required features. You can find more information about Active Directory at the active directory link (<http://go.microsoft.com/fwlink/?LinkId=93715>).
   1. It will require .NET Framework 3.5.1, which is fine.
3. Click the **Next** button.
4. Click the **Next** button. The installation will take a few minutes, so this is a good chance to catch up on your XKCD comics.
5. After you finish installing active directory, you still will not be able to start active directory. Why not? \_\_LS1\_\_

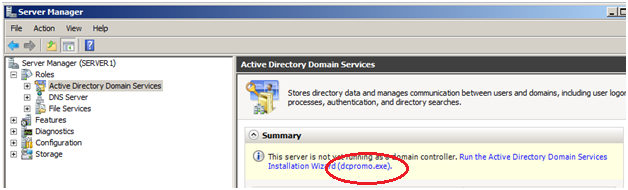
### Creating a domain and a primary domain controller

General Steps

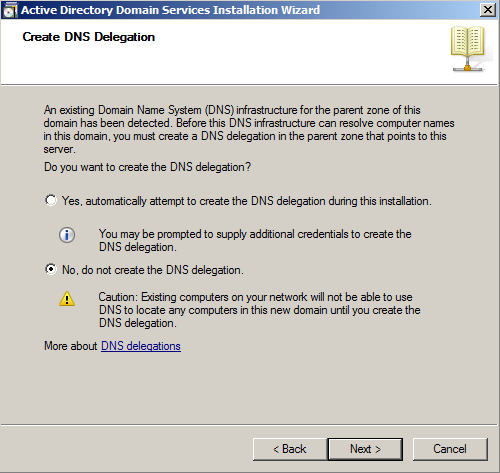
* Create a new domain for your primary domain controller, with <yourdomain>.local in the FQDN text field.
* Select **Windows Server 2008 R2** as the type of server allowed to become a domain controller.
* Do not create the DNS Delegation.
* If you are successful, you should see your domain name in the login window after your virtual machine reboots.

Detailed Steps

1. Now that you have installed active directory, you will need to configure it to be able to create a primary domain controller. Navigate to the **dcpromo.exe** link in the active directory services. Alternatively, you may navigate to Start 🡪Run 🡪 **dcpromo.exe**



1. Check the **Use Advanced Mode Installation** checkbox and click the **Next** button.
2. Click the **Next** button.
3. Select the **new domain in a new forest** button to create a new domain for your primary domain controller.
4. Type <yourdomain>**.local** in the FQDN text field (e.g., 3-15.404labs.islab.local).
   1. REMINDER: Last lab we created <yourdomain>. If you still need help, look on your Corporate Server under the DNS settings and you’ll see your domain in the Forward Lookup Zones.
   2. ***If you get an error message, you probably typed “.com” instead of correctly typing “.local”***
5. Click **Next**.
6. Verify the domain name and click **Next**.
7. Verify the domain NetBIOS name and click **Next.**
8. Select **Windows Server 2008 R2** from the dropdown menu to select the type of server allowed to become a domain controller and then click **Next**.
9. Click **Next**.
10. When prompted, click **Yes** in the warning box regarding dynamic addressing.



1. Click **No** when warned about the DNS delegation.
2. Leave the defaults for the location of the Database, log files, and SYSVOL folders.
3. Enter a recovery mode password. **Typically this password is something very secure** because it is used by an administrator to restore settings, but you should stick with something easy to remember (e.g. Password1). You will need to verify the password and then click **Next**.
4. Check your settings and press **Next.**
5. Check the **Reboot on completion** checkbox and wait for Active Directory to finish the configuration.
6. If you were successful, you should see your domain name in the login window after your virtual machine reboots.
7. Log back in as administrator with your normal password. Notice that your Administrator username and password was migrated to the domain (although your password may have expired, if so change it to Password2).

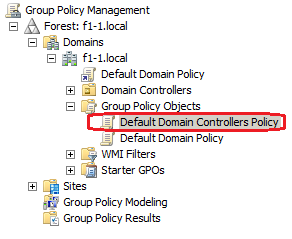
### Configuring local password policies

general steps

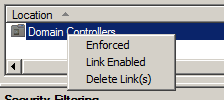
* Verify that both your **Default Domain Controllers Policy** and the **Default Domain Policy** are **Link Enabled.**
* Edit the **Password Policy** of the **Default Domain Policy** to match the following:
  + Enforce password history = 5 (number of previous passwords stored)
  + Maximum password age = 30
  + Minimum password age = 1
  + Minimum password length = 5
  + Password must meet complexity requirements = Disabled
  + Store password using… = Disabled
* Why is disabling complexity requirements in a typical network environment wise or unwise? \_\_LS2\_\_
* Allow domain users to be able to log on locally.
  + How is that different from logging onto a machine as a domain user? \_\_LS3\_\_
  + Why might we not allow this ability in a typical corporate network? \_\_LS4\_\_
  + Add **Domain Users** in the **Local Policies** under **Default Domain Controllers Policy**.
* Refresh the domain settings in cache.

Detailed Steps

1. Now that you have created a domain and domain controller, you may want to configure the local security policies for your domain. To accomplish this task, navigate to **Start** 🡪 **Administrative Tools** 🡪**Group Policy Management**.
2. Expand the **Forest** on the left, then **Domains**, then the domain you just created, then **Group Policy Objects**.
3. Double Click on the **Default Domain Controllers Policy**



* 1. Right-click on the folder icon (under “Location”), labeled: **Domain Controllers** and verify that it is **Link Enabled**. (There should be a check mark)



1. Now go to the navigation pane on the left and Click on the **Default Domain Policy**.
   1. Right-click on the icon (under “Location”) labeled: “**<yourdomain>.local”** and verify that it is **Link Enabled**. (There should be a check mark).
2. Right click on **Default Domain Policy** and select **“Edit…”**
3. Navigate to **Computer Configuration** 🡪 **Policies** 🡪 **Windows Settings** 🡪 **Security Settings.**
4. Expand **Account Policies**, and then click on **Password Policy**.
5. Double click on **various properties** to make changes and see an explanation of what the setting does.

9

Confused? 🡪Notice, as you make changes, Windows will Explain what each setting does!

1. Take a moment to explore the password settings in the local policy before changing the policy requirements to the following:

Enforce password history = 5 (number of previous passwords stored)

Maximum password age = 30

Minimum password age = 1

Minimum password length = 5

Password must meet complexity requirements = Disabled

Store password using… = Disabled

1. Why is disabling complexity requirements in a typical network environment wise or unwise? \_\_LS2\_\_
2. Finally, we will want to allow domain users to be able to log on locally. (Steps 12-18)
   1. How is that different from logging onto a machine as a domain user? \_\_LS3\_\_
   2. Why might we not allow this ability in a typical corporate network? \_\_LS4\_\_
3. Close the window to return to Group Policy Management
4. Right Click on **Default Domain Controllers Policy (not Default Domain Policy)** and select “Edit.”
   1. What’s the difference? The Default Domain Policy applies to all the computers on the domain. The Default Domain Controllers Policy applies to all the domain controllers. In this setting we only have one domain controller, which is YOUR server.
5. Expand **Computer Configuration** 🡪 **Policies** 🡪 **Windows Settings** 🡪 **Security Settings** 🡪 **Local Policies.**
6. Double-click on **User Rights Assignment** to open the properties.
7. Double-click on **Allow log on locally** to change this domain policy.
8. Click **Add User or Group** and enter **Domain Users** in the text box.
9. Click **OK**.
10. Finally, you will need to refresh the domain settings in cache. Typically, a domain controller will check for policy updates every couple of hours, but we don’t want to wait that long. Open a command prompt and type the following command: **gpupdate /force**.

# Exercise 2: Adding computers and users to the domain

### Overview

In this exercise you will create domain and local users and add computer resources to the domain.

### Objectives

* Create various domain users and groups
* Add your two Win7 virtual machines to the domain
* Create local users for your computers

### creating new users for your active directoy domain

Now that you have successfully installed and configured active directory, you will want to add users and groups to organize your resource sharing.

general steps

* Examine the Guest account in the **Users** subfolder in your **Corporate Server VM**. Why would this account be disabled by default? \_\_LS5\_\_
* Create a new User with the following information:
  + First Name = Leslie
  + Last Name = Knope
  + User Logon Name = Leslie
  + Password = manager
  + Uncheck the “User must change…” box and click **Next** and **Finish**.
* Add Leslie to the Administrators group and the Domain Admins group
* Create the following Users from your Primary Domain Controller
* Use “Password1” for all the passwords, and uncheck the “Must change password…” box.

**Group** **User(s)**

Domain AdminsRon Swanson, Andy Dwyer

Remote Desktop Users April Ludgate

DomainUsers (default) Ann Perkins

Detailed Steps

1. From your **Corporate** **Server VM**, navigate to your Server Manager. C:\Users\tmeservy\Desktop\8-3.PNG
2. Expand the roles column on the left until you can see **Active Directory Users and Computers**. Alternatively, you may navigate to this dialog by going to Start 🡪 Administrative Tools 🡪 **Active Directory Users and Computers**.
3. Continue expanding to navigate to your domain and click on the **Users** subfolder to view all the pre-configured user accounts that are created in a standard installation. Notice that the “Administrator” user name that you’ve been using to login to your Servers is a built-in account with Active Directory.
4. Examine the Guest account. Why would this account be disabled by default? \_\_LS5\_\_
5. Right-click the Administrator account and view its properties. Click the “Member Of” tab to view which Groups it belongs to, and notice that it has Administrative access through membership to that group. When you are done, close out of the properties dialog.
6. Create a new User by right-clicking the Users folder, and select **New** 🡪 **User**.
7. Enter the following information:

* First Name = Leslie
* Last Name = Knope
* User Logon Name = Leslie
* Password = manager
* Uncheck the “User must change…” box and click **Next** and **Finish**.

1. You have now created a new User in your Domain. Users must be a member of a sufficiently privileged Group to logon to the Domain. By default, all newly-created Users are added to the Domain Users group, which has sufficient privileges to logon.
2. Add the Leslie user to the Administrators group by right-clicking the Leslie user, choose Properties, Member Of (notice the Groups it’s already a member of…) and click Add. Enter the object name of “Administrators” and click “Check Names” to make sure the Server understood the Group you intended – if it recognizes the group, it will appear underlined and you can click OK.
   1. Also add Leslie to the Domain Admins group.
3. Test this account by trying to login to your Corporate Server VM as Leslie Knope.
4. Create the following Users from your Primary Domain Controller.
   1. Use “Password1” for all the passwords, and uncheck the “Must change password…” box.

**Group** **User(s)**

Domain AdminsRon Swanson, Andy Dwyer

Remote Desktop Users April Ludgate

DomainUsers (default) Ann Perkins

### Adding a Computer to a Domain

In this step you will add your other two VMs to your domain, so you can access shared resources across the network. Since your Corporate Server is the Domain Controller, it is automatically a member of your Domain. Your Windows 7A and 7B, however, are not, so the Leslie account you just created will not work on those machines until they are members of the Domain and can communicate with your Domain Controller.

general steps

* Add your Win7B VM to the domain.
* Add your Win7A VM to the domain.

Detailed Steps

1. Verify connectivity between your machines now if you have not already done so by sending a ping to YOUR Corporate Server from your Windows 7A and 7B virtual machines.
2. From your **7B** VM, add your VM to the domain by clicking the **Start** Menu, and right-clicking **Computer** and choosing **Properties**. Click the **Change Settings** button under the “computer name, domain, and workgroup settings” area. Notice that the VM is a member of the local Workgroup, not a domain.
3. Click the **Change** button, and select **Member Of: Domain** and enter your fully-qualified domain name, i.e., **<yourdomain>.local**, and click OK.
   1. If you have issues verify you can ping the server and verify your IP/DNS settings are correct.
4. In order to Add / Remove a computer to / from a Domain, your User account must be a member of the Domain Administrators group. The Administrator account you’ve been logging into has already been made a member of that group – when prompted, use Leslie’s account (**username:** “Leslie” **password:** “manager”) and click OK and restart the machine when prompted.
5. Your **7B** VM should now be a member of your Domain, which means all Active Directory Users (unless otherwise prohibited,) are be valid on your7B VM. Test this by logging onto your 7B VM with the Leslie account – make sure you click the **Switch User >>** button and log in to your Domain, not the Local machine.
6. Also, verify that the 7B VM has been added to the Domain by opening the Active Directory panel on your Corporate Server VM, expand your Domain, and expand the Computers folder – The **7B** VM should be listed.
7. Repeat this process for your Win7A machine.

### Creating Groups in a Domain

To simplify user account management, you can create Groups within Active Directory, add Users to Groups as desired, and give Groups permissions over individual resources in an enterprise.

general steps

* From your Corporate Server VM, open the **Active Directory Users and Computers** panel.
  + What is the difference between the Guest group and the Users group? \_\_LS6\_\_
  + What about the difference between the Administrators and the Account Operators? \_\_LS7\_\_
* Add a new Group named “**Pawnee**”, with a **Global** Scope and **Security** Type.
* Add Leslie to the Pawnee group.
* Create the following groups and add these Users in them.

**Group** **User(s)**

Directors Leslie, Ron, Andy

Nurses Ann

Detailed Steps

1. From your Corporate Server VM, open the **Active Directory Users and Computers** panel.
2. Click on the Built-In folder, and notice the Groups that come pre-configured in Active Directory.
3. Notice the Description of each Group.
4. What is the difference between the Guest group and the Users group? \_\_LS6\_\_
5. What about the difference between the Administrators and the Account Operators? \_\_LS7\_\_
6. Right-click the Users folder and choose **New** 🡪 **Group**. Group Name = “**Pawnee**”, and leave the Group Scope = **Global** and Group Type = **Security**. Now the Group should appear in the Users folder as a Security Group object.
7. Add the Leslie account to the Pawnee group by double-clicking Leslie, selecting the “**Member Of**” tab and entering the Pawnee group name. (Click “Check Names” to make sure it finds the Group, and click OK.)
8. View the Properties of the Pawnee group, and verify that the Leslie account is now a member.
9. Create 2 more groups with the following information (leave the defaults for the scope and type):
   1. Short Cut: Try selecting more than one at a time and then right click on one of them

**Group** **User(s)**

Directors Leslie, Ron, Andy

Nurses Ann

### Saving User Profiles

In many companies, users might log onto multiple servers and workstations throughout the enterprise. It is possible to configure a profile folder for each user, store it on a central server, and map the user’s Active Directory account to their individual profile folder. Thus a user’s profile settings and documents will be readily available from any machine in the Domain.

general steps

* In your Corporate Server, create two folders in the C drive, titled “**user**” and “**profile**”, respectively. Share these files with **Everyone** and give them **Read/Write** permission level.
* Map each User to their respective Profile Folder.
  + User Profile 🡪 Profile path: \\Server(LabStation#)\profile\Leslie
  + Home Folder 🡪 Connect – Z, To: \\Server(LabStation#)\user\Leslie
* Create Profile Folder settings for the Ron and April accounts. Make trivial changes to their personal settings (such as desktop wallpaper, icon size, nonsense folders, etc.). Verify that their changes have taken place by logging into the other VMs with both of their accounts.
* Why is it when you change the desktop wallpaper, icon size, display resolution, etc. on the Ron, April, and Leslie accounts, it effects all the other VMs in the domain? \_\_LS8\_\_

Detailed Steps

1. In your Corporate Server, create two folders in the C drive, titled “**user**” and “**profile**”, respectively. Right-click each folder, select **Share with**… **Specific People** and then select **Everyone** from the dropdown menu. Click the **Add** button and select **Read/Write** in the permission level.
2. Click **Share** and then **Done**. Make sure you do this on both folders.
3. The “user” and “profile” folders will be the central location for all User/Profile settings. Now you need to map each User to their respective Profile folder.
4. Open the **Active Directory Users and Computers** panel and expand the **Users** folder under your domain, and view the **Properties** for the **Leslie** account. Set the fields on the **Profile** tab as follows:

* User Profile 🡪 Profile path: \\Server(LabStation#)\profile\Leslie
* Home Folder 🡪 Connect – Z, To: \\Server(LabStation#)\user\Leslie
  + The Home Folder is just a drive that is automatically mapped to your computer which allows you to store files on the server and access them from any computer you logon to.

1. Click **OK**.
2. Test your new profile settings by
   1. Logging into your Win7A VM with the Leslie account, and go to **Computer**.
   2. Your personal Leslie folder should now be listed as the drive you mapped in the steps above.
   3. Create a folder on the desktop of Win7A, titled “Eagleton Destruction Plan”.
   4. **Log out** of your Win7A (the User Profile service only updates on logout).
   5. **Log on** to your Win7B VM with the Leslie account – the “Eagleton Destruction Plan” folder should be on the desktop, and your personal folder should still be mapped in the Computer drives.
3. Now create profile folder settings for the Ron and April accounts.
4. Create individual documents for the Ron and April accounts, and change any of their personal settings (desktop wallpaper, icon size, display resolution, etc.)
5. Verify that their changes have taken place by logging into the other two VMs with both of their accounts.
6. Why is it when you change the desktop wallpaper, icon size, display resolution, etc. on the Ron, April, and Leslie accounts, it effects all the other VMs in the domain? \_\_LS8\_\_

# Exercise 3: Auditing General System Events

### Overview

Windows Server has a rich range of auditing tools, but the audit policies are not defined by default, due to the amount of hard disk resources auditing consumes. To enable auditing you must define an Audit Policy in a Group Policy Object. We will modify the Default Domain Security Policy and the Default Domain Controller Security Policy.

### Objectives

* Create an audit policy for the Domain Controllers to track Logons and Object access.
* Enable the Global Audit Policy using Group Policy Management
* Set up a default domain Audit Policy using Group Policy Management

### Create a Local audit policy

general steps

* In your Corporate Server as Administrator, enable the following options:
  + Audit account logon events—Define for Success and Failure
  + Audit account management—Define for Success
  + Audit object access—Define for Success and Failure
* Update the global policy in the command line.
* Open the Event Viewer now and look at the types of events. What types of events exist? \_\_LS9\_\_
* In the Summary of Administrative Events pane, click the Error event type category and open the first item. What is the Event ID? \_\_LS10\_\_
* What executable or service created the error? Hint: look at Source or double click the error to get more details \_\_LS11\_\_
* Expand **Windows Logs** in the left pane**.** How many categories of errors exist? \_\_LS12\_\_
* How many items are in the security category? \_\_LS13\_\_

Detailed Steps

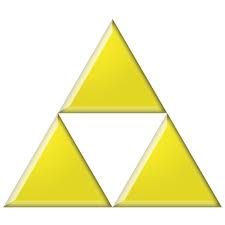
1. Log out of your Corporate Server and Log back in as Administrator.
2. Navigate to the Domain Controller Security Policy Editor, found at **Start** **🡪Administrative Tools** **🡪Local Security Policy**. Then expand **Local Policies 🡪Audit Policy**.
3. Enable the following options:
4. Audit account logon events – Define for Success and Failure
5. Audit account management – Define for Success
6. Audit object access – Define for Success and Failure
7. Once these Audit Policy objects have been defined, close the policy editor. Update the global policy in the command line to immediately update policy changes (Hint: gpupdate /force).
8. Server 2008 keeps an audit trail at **Administrative Tools** **🡪Event Viewer**. Open the Event Viewer now and look at the types of events. What types of events exist? \_\_LS9\_\_
9. In the Summary of Administrative Events pane, click the Error event type category and open the first item. What is the Event ID? \_\_LS10\_\_
10. What executable or service created the error? Hint: look at Source or double click the error to get more details \_\_LS11\_\_
11. Expand **Windows Logs** in the left pane**.** How many categories of errors exist? \_\_LS12\_\_
12. Open the Security category. Double click the first item listed there – note the date, time, user, computer, and description.
13. How many items are in the security category? \_\_LS13\_\_.
    1. You can see how easy it is to quickly fill a hard drive with audit trail items, as well as how easy it could be to find unauthorized activity perpetrated on any computer in a Domain.
14. It is possible to clear the Audit Trail, but the Server makes a note whenever the trail has been cleared. Right-click the “Security” category on the left, choose “Clear Log...” and click “Clear” when it asks you to save, (but if you wanted to do so, you could save the audit trail and archive it for future reference by clicking Save and Clear).
15. Close Event Viewer.

### Configure audit policy in group policy management

general steps

* Edit the **Default Domain Controllers Policy** in your Domain.
  + Under **Audit Policy**, enable the following options:
    - Audit account logon events—Define for Success and Failure
    - Audit account management—Define for Success
    - Audit object access—Define for Success and Failure
    - Audit directory service access—Define for Success
* Repeat the process for the **Default Domain Policy**.
* Ensure that both the Default Domain Controllers Policy and Default Domain Policy are Enforced and Link Enabled for your domain.
* Update the global policy

Detailed Steps

1. Click **Start**, point to **Administrative Tools**, and then **Group Policy Management**.
2. In the console tree, expand **Forest** (It looks like the tri-force  from Zelda… see [0](http://zelda.wikia.com/wiki/Triforce))
3. Continue to expand **Domains** **🡪**your domain **🡪** and **Domain Controllers**.
4. Right-click **Default Domain Controllers Policy** and then click **Edit**.
   1. Note: If it is disabled (greyed out), then you probably logged in with an account other than the administrator account
5. Under **Computer Configuration**, expand **Policies🡪Windows Settings** **🡪** **Security Settings** **🡪Local Policies 🡪**and **Audit Policy**.
6. Enable the following options (right click on them and select policies; then select “Define these policy settings”):
7. Audit account logon events – Define for Success and Failure
8. Audit account management – Define for Success
9. Audit object access – Define for Success and Failure
10. Audit directory service access – Define for Success
11. You can close the Group Policy Editor.
12. Now repeat this process for the **Default Domain Policy**
    1. Found under **Forest** **🡪Domains** **🡪**your domain **🡪**and **Group Policy Objects.**
13. Ensure that both the Default Domain Controllers Policy and Default Domain Policy are Enforced and Link Enabled for your domain.
    1. Right click on GPO (i.e. “Default Domain Policy” with the little shortcut arrow, **not the one under the “Group Policy Objects” folder**), and make sure that **Enforced** and **Link Enabled** are selected. Do this for **both policies** or else the audit policy will not be applied
14. Update the global policy (hint: it’s the command line thingy).

# Exercise 4: Setting permissions across the domain

### Overview

In this exercise, you will learn how to set basic permissions on network resources.

### Objectives

* Learn how to set basic permissions using a bottom-up administration approach

### Setting folder permissions

Now we will specify different access to the **Eagleton Destruction Plan** folder for the Andy and April accounts (you should have created this folder and these accounts in the first AD lab).

general steps

* Make the **Eagleton Destruction Plan** folder available to all Users by moving it to C:\Users\Public\Public Desktop\
* Create a User **Andy** and give him Full Control in the Security Properties of the **Eagleton Destruction Plan** folder.
* Add the **April** user, with only Read permissions.
* Test the permissions by logging on as **Andy**. The **Eagleton Destruction Plan** folder should be on the Desktop – open the folder, and attempt to make changes to the file and save it. Were you able to make changes? Why or why not? \_\_LS14\_\_
* Repeat the process as **April**. Are you able to save changes? Why or why not?\_\_LS15\_\_

Detailed Steps

1. Open the **Eagleton Destruction Plan** folder on your desktop on your Win7A machine (logged in as Leslie), and in it create a new text file called **Pawnee** **Office**.**txt**
2. Open the file and populate it with a description of your favorite prank that Andy and April played on Ron (or any other text you would like). Save and close the file.
3. We want the **Eagleton Destruction Plan** folder to be available to all Users on the Win7A VM, so move the **Eagleton Destruction Plan** folder to the following location: C:\Users\Public\Public Desktop\. (The folder is hidden so you can type it in the address bar in Windows Explorer)
4. View the Security Properties of the **Eagleton Destruction Plan** folder and add the **Andy** user.
5. AllowFullControl, click Apply.
6. Now add the **April** user, and only allow Read permissions. Apply and click OK. By default, any “child” objects in a folder will inherit the permissions of the parent folder.
7. Test the permissions by logging on as **Andy**. The **Eagleton Destruction Plan** folder should be on the Desktop – open the folder, and attempt to make changes to the file and save it. Were you able to make changes? Why or why not? \_\_LS14\_\_
8. Repeat the process as **April**. Are you able to save changes? Why or why not?\_\_LS15\_\_

# Exercise 5: auditing files and folders

### Overview

In this exercise you will learn how to use the auditing on individual files and folders, and use the audit trail to monitor access to network resources.

### auditing files and folders

general steps

* In your Win7A VM, logged on as Leslie, add a new audit group **Everyone.**
* Check **Full Control** for both Successful and Failed. What do you think will checking this box do? \_\_LS16\_\_.
* Enforce the audit policy via command prompt.
* Log in and out as April and attempt to edit/save the **Pawnee Office.txt** file. Repeat the process for Andy.
* Log in as Leslie, and find the audit entry of Andy’s and April’s object access of **Pawnee Office.txt**
  + What’s the Event ID when April opened the object? \_\_LS17\_\_

Detailed Steps

1. While still logged in as Leslie on the Win7A VM, open the “**Eagleton Destruction Plan folder”**, and view the **Properties** of the **Pawnee Office.txt** file.
2. Click **Security**, and then **Advanced**. Open the **Auditing** tab.
3. Back in Exercise 1 you enabled Audit Object Access, which means you can now enable Auditing on a User/Group basis for any file on your computer. Click **Continue** and then **Add** to create a new audit entry, and add the **Everyone** group.
4. Check **Full Control** for both Successful and Failed. What do you think will checking this box do? \_\_LS16\_\_
5. Click OK several times to exit.
6. In order to enforce this audit policy, do **gpupdate /force** from the command prompt.
7. To generate audit trail items, log off and log in as April and attempt to both read and edit/save the **Pawnee** **Office**.**txt** file (It should fail to save as April). Repeat the process as Andy. Make sure you log off April before logging on as Andy.
8. Now to view the results of your audit policy
   1. Log off and log back in as Leslie
   2. Look at the Event Viewer on your Win7A VM by going to Start 🡪 Control Panel 🡪System and Security 🡪Administrative Tools 🡪Event Viewer
   3. Select the Security category under Windows Logs.
   4. Can you find the audit entry of Andy’s and April’s object access of Pawnee Office.txt.
   5. What’s the Event ID when April opened the object? \_\_LS17\_\_
      1. If you have a difficult time finding it due to the number of events, use the Find… option in the right panel and type in Andy or April. Alternatively, you could clear the log and retry.

# Exercise 6: Group Policies & Log-In Options

### Overview

Administrators can control how users and groups log in to their computers and the options that are available. You will notice that when you log in to a computer on the BYU network that some options are not available – you will do the same thing with your Domain.

### Setting group policies across the domain

general steps

* In your Coporate Server as Administrator, create a GPO (named something like Login Policy).
* Remove the **Authenticated Users** group.
* Add the **Domain Users** group
* Advance your GPO policy to the top of the list and enforce it. Why do we need to do this? \_\_LS18\_\_
* Accept and enable the following settings: **Remove Documents icon…, Remove Run menu…, Remove and prevent access to the Shut Down … commands,** and **Do not allow Windows Messenger to be run.**
* Enforce this policy via command line.
* Log into one of your Win7 VMs as Leslie. Describe the changes that you now see. (You may need to review the description of what the above changes did). \_\_LS19\_\_

Detailed Steps

1. If not already logged in as Administrator, log into your Corporate Server VM as Administrator and open the **Group Policy Management** panel.
2. Find your domain in the left panel, right-click, and click **Create a GPO in this domain, and Link it here...**
3. Name your GPO (perhaps something like Login Policy) and click **OK**.
4. Click on your new policy, select the **Authenticated Users** group in the **Security Filtering** section, and click **Remove**. When prompted, click **OK**.
5. Click **Add** and add the **Domain Users** group.
6. In the left pane, click on your domain. Then, in the right pane, click the **Up** **arrow** on your new GPO to advance your policy to the top of the list. Why do we need to do this? \_\_LS18\_\_
7. Right-click on your policy and enforce the policy. When prompted, select **OK**.
8. Select your new policy, right-click, and click **Edit**.
9. On the left side of the window under the **User Configuration** folder, and the **Policies** subfolder, expand the **Administrative Templates** folder.
10. Open the **Start Menu and Taskbar** folder, double-click the **Remove Documents icon…** setting, select **Enabled** and click **OK**.
11. At this point you may want to maximize or expand the width of your window to be able to see the “State” column (to the right of the “Setting” column) change from “Not configured” to “Enabled.”
12. In similar fashion, enable **Remove Run menu…** and **Remove and prevent access to the Shut Down … commands.**
13. Click the **Windows Components** folder (beneath Administrative Templates), click Windows Messenger, and enable **Do not allow Windows Messenger to be run.**
14. You have just modified the group policy object for your domain. Put this policy into effect by using the **gpupdate /force** command on all your VMs. (If it asks you to log off, type “y” and hit enter, and then log back on as Administrator.)
15. Now log into one of your Win7 VMs as Leslie. Describe the changes that you now see. (You may need to review the description of what the above changes did). \_\_LS19\_\_

# Exercise 7: Disable Firewall Using Group Policies

### Overview

We want all computers that join our domain to disable the built-in Windows firewall.

1. Open the Group Policy Management console, and edit the “Default Domain Policy.”
2. Drill down into the computer security policy and disable the built-in Windows firewall.

# exercise 8: discovering new tools

### Overview

For the final exercise, you are required to research and implement two (2) additional features of Active Directory and Group Policies, specifically related to User and Group management or Computer management. You will explore two features of your choice and actually implement them / configure them / activate them. **DO NOT** simply disable more features; you need to select options in other categories besides the ones you’ve done in the above scenario. Some examples include: loading a program upon login, loading a web page upon login, further customization of the Start menu, remapping the “My Documents” folder to a network drive on the server, etc. Make a note of the **two additional features** you implemented and their **exact location** within the Group Policy Object Editor. **WARNING:** *It is possible to disable your computer sufficiently that you cannot continue with the next couple of labs, so please think about what you are disabling before you do so.*

What two features did you choose?

* 1. Explain the 2 features you changed in Active Directory and explain how a company would use them.
     1. Feature 1 - What did you change, where is it located, and how would a company use that feature?\_\_LS20\_\_
     2. Feature 2 - What did you change, where is it located, and how would a company use that feature?\_\_LS21\_\_

# Wrap UP

1. **Save or shut down your VMs**
2. Answer all questions thoroughly on Learning Suite.

# Big Picture

Congratulations, you did it! Did what, exactly? Well, one sec let me think… Oh yeah! You learned how to implement Active Directory, which is the main way to manage Microsoft’s permissions. You then created a domain and its primary controller. With this domain, you acquired the important skill to configure password settings, add other computers to the domain, and set policies across the domain, as well as auditing files and folders. Basically you learned how to get your domain functional. Good job!