TNE10005/TNE60002

Network Administration

Lab 7

Increasing Object Security Using AD Groups

Aims:

- Install a child domain
- Create resources to share throughout the forest
- Deploy a secure and scalable group strategy.

Virtual Machines

sWin22DC1, sWin22RTR, sWin22SVR2, sWin22SVR3, sWin10CL101, sWin10PC203.

First, launch and log on to sWin22DC1. Then launch sWin22RTR. When sWin22RTR is loaded, launch and login to the following virtual machines in this order: sWin22SVR2, sWin22SVR3.

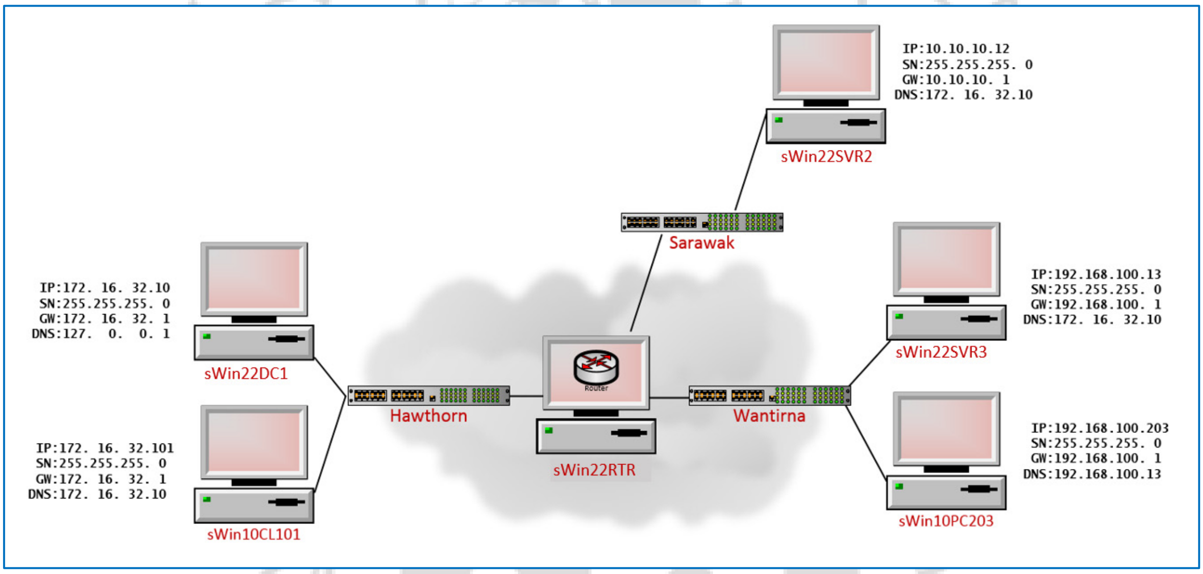


Figure 1 - Lab 07 Topology

Preliminary settings:

> ***Note:***
> *This lab assumes that you have taken adequate notes and mastered key steps from past labs. If you find that your notes are missing key steps, make sure you update them before you leave.*

Check to see if sWin22SVR3, sWin10CL101 and sWin10PC203 are connected to the correct virtual switches and have the IP configuration that matches Figure 1 - Lab 07 Topology.

This should not take longer than 10 minutes.

Lab Exercises

Create a Child Domain

1. Verify that the DNS server address is properly configured on **sWin22SVR3** by ensuring you can successfully ping ***sWin.local***. If you cannot successfully ping, see if you and a fellow student can troubleshoot the error. Call for assistance from the tutor if you have not resolved the problem in five minutes.
2. Add the **Active Directory Domain Services** role to **sWin22SVR3** (refer to Lab 06 if you cannot remember how to do this).
3. Once the installation is complete, on **sWin22SVR3**, in **Server Manager**, click on the alert and select **Promote this server to be a domain controller**.

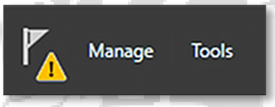
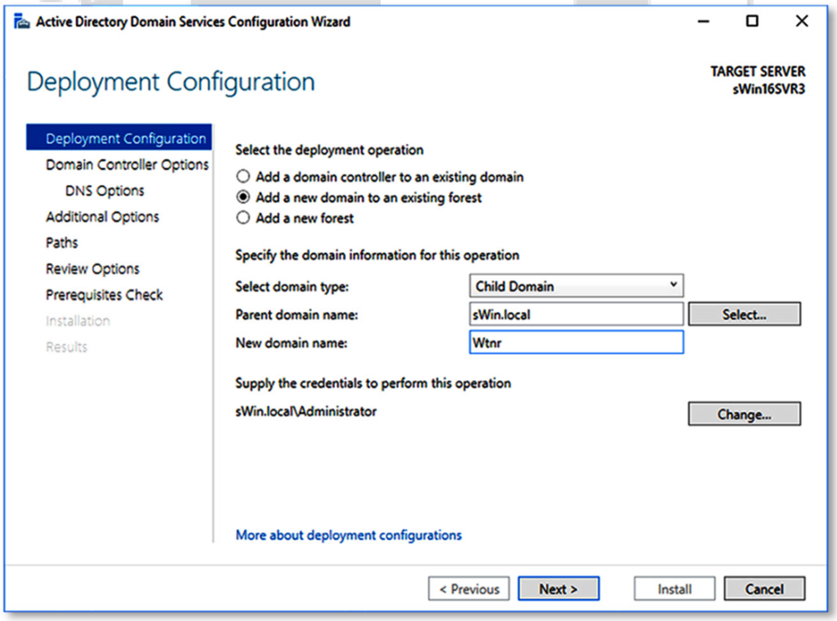


Figure 2 - Promote Server

4. On the wizard page **Deployment Configuration**:
   a. Select the deployment operation **Add a new domain to an existing forest**,
   b. Click the **Select...** button to provide the Enterprise Administrator's credentials and enter:
      i. ***sWin.local\Administrator*** as the User name, and
      ii. ***Pa55w.rd*** as the password.
   c. Fill out the rest of the page as given in Figure 3 - Child Domain Creation, and click **Next**.



Select the deployment operation

○ Add a domain controller to an existing domain
● Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

Select domain type: Child Domain

Parent domain name: sWin.local

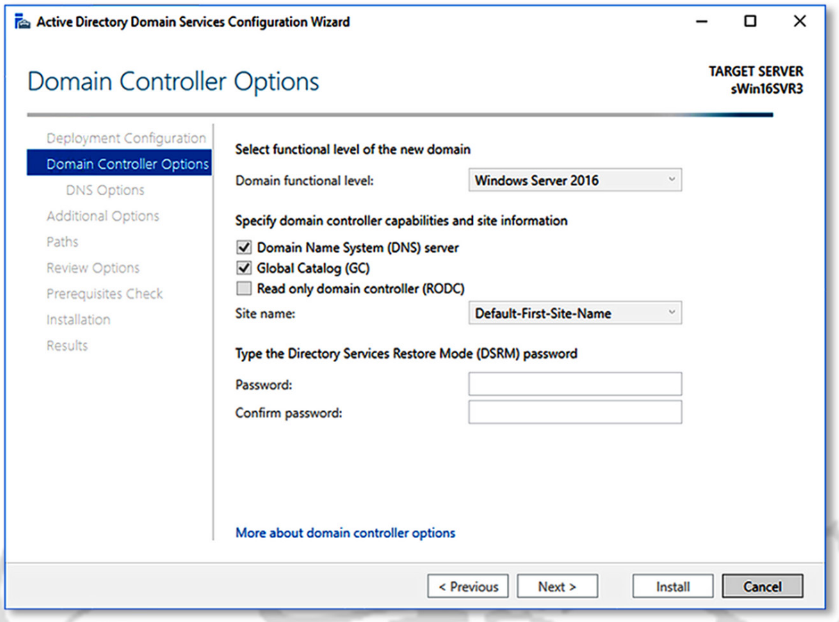
New domain name: Wtnr

Supply the credentials to perform this operation

sWin.local\Administrator

Figure 3 - Child Domain Creation

5. On the **Domain Controller Options** page of the wizard, ensure that the options selected match those given in Figure 4 - Domain Controller Options



Domain Controller Options

Select functional level of the new domain

Domain functional level: Windows Server 2016

Specify domain controller capabilities and site information

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

Site name: Default-First-Site-Name

Type the Directory Services Restore Mode (DSRM) password

Password:

Confirm password:

Figure 4 - Domain Controller Options

6. Enter the standard lab password as the **DSRM** password and click **Next.**

7. On the **DNS Options** wizard page, ensure **Create DNS delegation** is ticked and that the Credentials for delegation creation is **sWin.local\Administrator**, and click **Next**.

   Click **Next** for the next three pages of the Wizard.

   On the **Prerequisites Check** page, ignore the alert about *cryptography algorithms*, this is beyond the scope of this course, and does not create a serious threat, and click **Install**.

   sWin22SVR3 will now be promoted as the primary DC in a new child domain. In order to do this a DNS server for the child domain needs to be installed and all of the relevant forest information must be copied across from sWin22DC1.

   This all takes some time, so we will use this time to create some user accounts and network resources.

> *Only if you receive an error message of failing to promote sWin22VR3, perform the following steps on both sWIn22DC1 and sWinSVR2:*
>
> - *Launch Windows PowerShell*
> - *Within the Windows PowerShell, type **repadmin /syncall** and press **<Enter>***

Group Strategy

We will now try to create the following objects and resources:

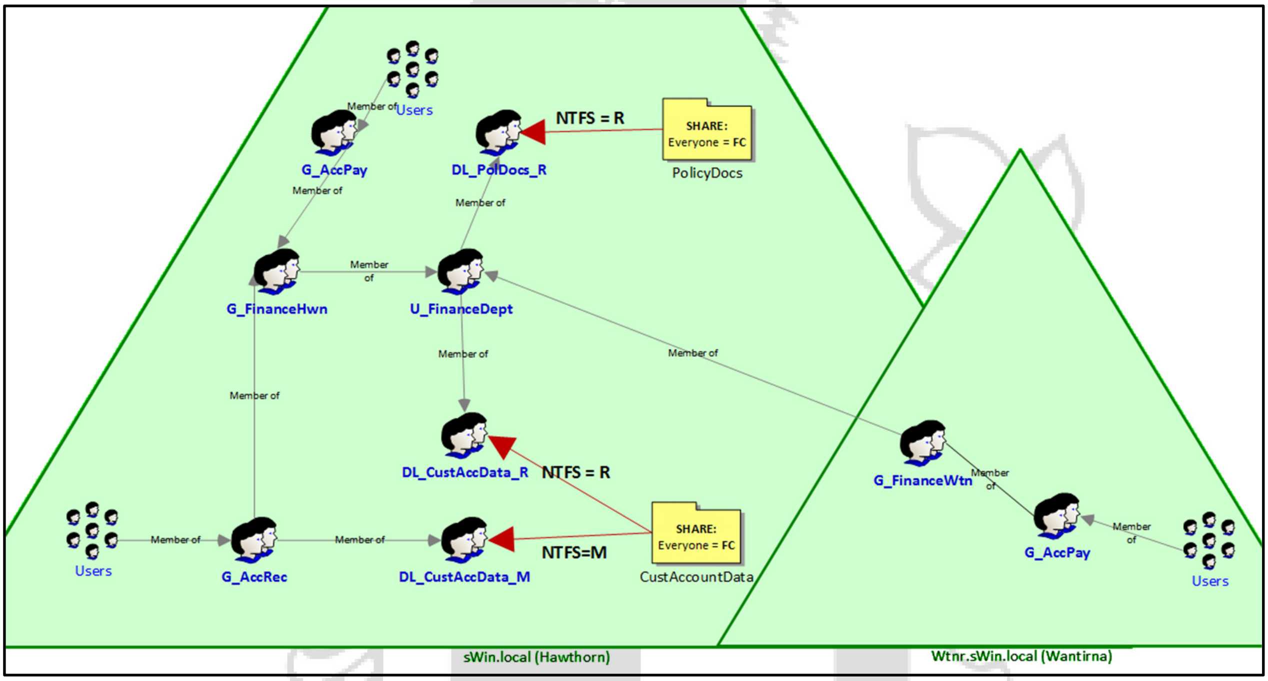


Figure 5 - Group Strategy for Lab 07

Creating Network Resources

8. On **sWin22DC1:**
   a. Create the folders:
      i. **C:\Policy_Docs**
      ii. **C:\CustAccountData**
      iii. **C:\Home**
   b. Share these folders with the **share** permissions **Everyone = Full Control**.
   c. Create some sample files in both the **Policy_Docs** and **CustAccountData** folders
   d. On the folders Policy_Docs and CustAccountData, following the steps from the ***Removing Inherited Permissions*** from last week's lab, remove all permissions for the **Users** group (and no other group).

Create an OU

9. On **sWin22DC1** launch **Active Directory Users and Computers**, right click on **sWin.local** and select **New** > **Organizational Unit**. Name the new OU **Finance**.

Create sWin.local Groups

10. Right click on the new OU **Finance**, and select **New** > **Group**.
    a. Name the group **G_FinanceHwn**.
    b. Ensure that the Group scope **Global** is selected and that the Group type is **Security**.

***NOTE:** We will only be using the **Security** Group type in Network Admin. You cannot allocate permissions with Distribution groups. Distribution groups are effectively e-mail lists.*

NOTE: Second Level Account Groups

Occasionally we face the need to group account groups. For example, a department may have a number of teams within the department such as Accounts Receivable and Accounts Payable or Maintenance Electrical, Maintenance Building and Maintenance Plumbing. In some circumstances the administrator needs to give one team access to a resource, but not the other teams. Then in different circumstances the administrator may need to give the whole department access to a resource.

The most efficient, flexible and scalable way of doing this is to create a second level account group where we make the first level account group a member of the second level account group.

For example in the Accounts department we may want to create the first level account groups G_Acc_Rec and G_Acc_Pay. We would make the user accounts members of the appropriate group according to which team they are allocated to. We then create a second level account group call G_Acc_Dept and add the G_Acc_Rec and G_Acc_Pay group's members. This way we only need to give the G_Acc_Dept access to a resource and the member groups also get access. This approach is sometimes called the I G G DL A group strategy.

In a multi-domain forest, we cannot use Global groups as second level account groups if we want to provide access to resources in different domains. This is due to the fact that the Global group scope can only have accounts from its local domain as members. Thus in situations where we need to create a second level account group in a multi-domain forest we need to use the Universal group scope.

Taking the Swinburne campuses as an example. Assuming that we have domains at each campus and together they form a forest. We would create global groups at each campus e.g. G_Accounts_Hwn, G_Accounts_Swk, etc. For our second level account group we would create the Universal group U_Acc_Dept, and make each of the G_Acc… groups from each domain members. This approach is called the I G U DL A group strategy.

11. Repeat the process to create the following groups:

Name	Scope
G_AccPay	Global
G_AccRec	Global
U_FinanceDept	Universal
DL_CustAccData_R	Domain Local
DL_CustAccData_M	Domain Local
DL_PolicyDocs_R	Domain Local

NOTE: *When creating groups the default scope is **Global**. This can be a potential problem if you are creating many groups in a rush and forget to change the default group to Domain Local. If you do make this mistake you cannot directly change a Domain Local group into a Global group. However you can change either type to a Universal group, and from a universal group you can change to either Global or Domain Local. So if you accidentally create the wrong scope, don't panic, just change to a Universal group, make sure that you click OK, then you can change back to the correct scope.*

We will nest the groups later on.

Creating sWin.local User Accounts and Templates

In last week's lab we used **Active Directory Users and Computers** to create user accounts. In this section we are going to create a user account template.

Users in the same team generally need to access the same resources. They generally need to use the same computers, same printers and same data, hence need to be members of the same groups. Now you could configure all of these attributes every time you create a new user... or you can create a **User account template**. A user account template is just a user account that we copy every time we need to create a new user account for that team.

NOTE: When you copy a user account template the following attributes are copied to the new user account:

- *Group Memberships*
- *Home Directories*
- *Profile Settings*
- *Logon Scripts*
- *Logon Hours*
- *Password Settings*
- *Department Name*
- *Manager*

12. On **sWin22DC1** launch **Active Directory Users and Computers**. Right click on the OU **Finance** and select **New** > **User**

    a. Enter _***UsrTmpAccPay*** as both the **First name**, and **User logon name**, and click **Next**.

    b. As this account will not be used by any user we do not need to add a password, but we need to ensure that **User must change password at next logon**, and **Account is disabled**. Ensure both are ticked then click **Next**, then **Finish**.

13. We now need to configure the attributes that we want copied to each new user account for this team:

    Right click on **_UsrTmpAccPay** and select **Properties**
    *(Note: If you are behind schedule only configure **a** & **b**)*

    a. On the **Profile** tab:

        i. **Home folder** to **Connect**, **H:**,
        To: **\\sWin22DC1\Home\%username%**

    b. On the **Member Of** tab:

        i. **Add**, **G_AccPay**

    c. On the **Account** tab, set:

        i. **Logon Hours…** to Monday to Friday

        ii. **Log On To…** to **sWin10CL101**

        iii. **Account expires** = the last day of the current year.

    Then click **OK**

14. To copy this template, right click the **_UsrTmpAccPay** account and select **Copy…**

    a. Enter the First name ***Doug***, the Last name ***Pirahna*** and the User logon name ***dpirahna***, and click **Next**.

    b. Enter the Password ***Pa55w.rd*** and remove the ticks **User must change password**, and **Account is disabled**.
    (Note: In the real world we not do this, this is to speed up the lab)

    c. Duplicate this template again for another new user **Luigi Vercotti**.
    After duplicating, on the user's Member Of tab, remove the current group, and make Luigi a member of the G_AccRec group.

    Note: You should now be able to observe new user folders in the C:\Home\ folder.

We will now change back to the Wantirna domain to finalise its configuration.

Verifying Successful Child Domain Creation

15. On **sWin22SVR3**, type Pa55w.rd to log on as WTNR\Administrator. In Server Manager, from Tools select **Active Directory Domains and Trusts**. Expand **sWin.local** and verify that **Wtnr.sWin.local** has been added as a child domain. It should appear similar to Figure 6 - Active Directory Domains and Trusts.

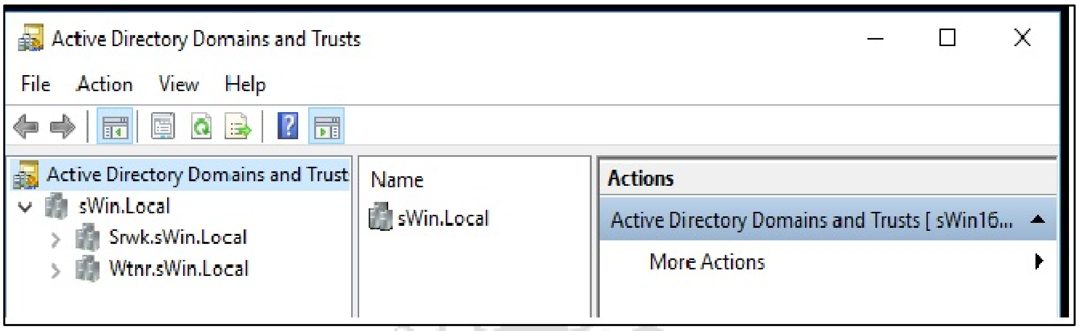

Active Directory Domains and Trusts
File Action View Help
Active Directory Domains and Trust
sWin.Local
Srwk.sWin.Local
Wtnr.sWin.Local
Name
sWin.Local
Actions
Active Directory Domains and Trusts [sWin16...
More Actions

Figure 6 - Active Directory Domains and Trusts

Create Wtnr.sWin.local Objects

Create an OU in PowerShell

16. On **sWin22SVR3**, load **PowerShell** and type:

```
new-ADOrganizationalUnit -name Finance -path "
dc=Wtnr,dc=sWin,dc=local"
```

and press **Enter**

Create a New User Account Using PowerShell

17. Enter the following to create a new user account for Kim:

```
New-AdUser -name "Kim" -Path "ou=Finance,dc=Wtnr,dc=sWin,dc=local" -
accountPassword (ConvertTo-SecureString -AsPlainText "Pa55w.rd" -
Force) -enable $True
```

Create Groups Using PowerShell

18. Enter the following to create the groups for the Wantirna domain.

a.
```
New-ADGroup -name G_FinanceWtn -GroupCategory Security –
GroupScope Global -path "ou=Finance,dc=Wtnr,dc=sWin,dc=local"
```

b.
```
New-ADGroup -name G_AccPay -GroupCategory Security -GroupScope
Global -path "ou=Finance,dc=Wtnr,dc=sWin,dc=local"
```

19. Use the following to set the membership and nesting of the Wantirna groups:

a.
```
Add-ADGroupMember G_AccPay Kim
```

b.
```
Add-ADGroupMember G_FinanceWtn G_AccPay
```

Join sWin10PC203 to the New Domain

By default, new computer accounts are created in the Computer container in AD. If we want a Computer Account to be created in a specific OU we can just right click on that OU and select New, Computer…

But this does not help when an Administrator joins from a computer without an account to the domain. To change the default location for Computer Accounts we need to use **redircmp**.

20. On **sWin22SVR3**, in **PowerShell** type the following:

```
redircmp "ou=Finance,dc=Wtnr,dc=sWin,dc=local"
```

We will now join **sWin10PC203** to the Wantrina domain.

21. On **sWin10PC203**, test whether DNS is working by successfully pinging the new child domain **Wtnr.sWin.local**

    If successful, join **sWin10PC203** to the **Wtnr.sWin.local** domain, as covered in Lab 6, section "Joining a Domain" (i.e. System Info > Change settings).

    a. Use the credentials **Wtnr\Administrator** and the password **Pa55w.rd**. (Skip the *Add an account* prompt)

    b. After **sWin10PC203** has rebooted, verify that its Computer account is appearing in the **Finance** OU in the Wantirna domain.

Nesting the Groups in the Forest

***Note:** We have already completed the nesting for the Wantirna domain using PowerShell.*

Nesting Within the Hawthorn Domain

22. On **sWin22DC1**, in **Active Directory Users and Computers**, in the **Finance** OU, nest the groups according to the Group Strategy in Figure 5.
    ***Hint:** You can double-click a group name from within the member/member-of properties will load the properties of the next group.*

    In summary:

    a. **Doug Pirahna** is a member of **G_AccPay**.
    G_AccPay is a member of **G_FinanceHwn**.
    G_FinanceHwn is a member of **U_FinanceDept**.
    U_FinanceDept is a member of **DL_CustAccData_R**.
    Assign **DL_CustAccData_R** the permissions,
    Read and **List folder contents** to the **CustAccountData** folder.

    b. **Luigi Vercotti** is a member of **G_AccRec**.
    G_AccRec is a member of **G_FinanceHwn**.
    G_FinanceHwn is a member of **U_FinanceDept**.
    G_AccRec is a member of **DL_CustAccData_M**.
    Assign **DL_CustAccData_M** the permissions,
    Modify to the **CustAccountData** folder.

    c. **U_FinanceDept** is a member of **DL_PolicyDocs_R**
    DL_PolicyDocs_R the permissions,
    Read and **List folder contents** to the **PolicyDocs** folder.

Nesting Groups between Domains

23. Staying on **sWin22DC1** in **Active Directory Users and Computers**, double-click on **U_FinanceDept**, and click on the **Members** tab. Then click the **Add...** button.

24. On the **Select Users, Contacts...** dialog box, click the **Locations...** button.
    Expand the **sWin.local** domain, and scroll down and select the **Wtnr.sWin.local**, and click **OK**.

25. In the **Enter the object names...** field type ***G_***, and then click the **Check Names** button. Notice that all of the Wantirna groups are listed. Select the **G_FinanceWtn**, and click **OK**.

Testing the Access Permissions

> *Work around – If you get an error stating Kim cannot log in remotely do one of the followings:*
> 1. *Log on to sWin10PC203 as Wtnr\Administrator, or*
> 2. *On sWin22SVR3 make the Everyone group a member of the Remote Desktop Users group.*

26. On **sWin10PC203** log on as **Kim**. From Windows File Explorer (📁), enter the UNC for **sWin22DC1** and press enter, i.e.

```
\\sWin22DC1.sWin.local\CustAccountData
```

27. Kim is a member of the G_AccPay team. She should only have read access. Verify that this is the case.

28. On **sWin10CL101**, log on as **Luigi Vercotti**. Connect over the network to the **CustAccountData** folder. Verify that you can save changes and create new files.

> *Before you change the memberships of any groups, remember that a Group's SID must appear in the Access token of the user. If you change group membership after a user has logged on, the new group's SID will not yet appear in the users Access token. In other words you must log the user off, then log back on in order to generate a new Access token.*

Extension *(Optional)*

Create two more DL groups for CustAccountData. One to have Full Control permissions and the other to have Deny Write permission.

Add the U_FinanceDept as a member of the new Full Control DL.
What are the differences? *(once you have generated a new Access token :)*
Add the U_FinanceDept as a member of the new Deny Write DL.

What are the differences?

See if you can explain your observations using the theory covered in the lecture (i.e. cumulate NTFS..., cumulate Share..., most restrictive applies)

Pack up

1. Shut down all guest VMs.
2. **Sign out** from the Host virtual machine and make sure that it is **Stopped** otherwise it will run in the background and use up your quota.
3. If on campus, **log off from the ATC626 lab PC,** and push your chair in as you leave.

End of Lab