TNE10005/TNE60002

Network Administration

Lab 9

Managing Security

in

Active Directory

SWINBURNE UNIVERSITY OF TECHNOLOGY

Aims:

To improve the baseline security of a Windows Server 2016 Domain.

Virtual Machines

sWin16DC1, sWin10CL101

Preliminary settings

1. Check the Hyper-V **settings** for **sWin10CL101**. Ensure the **Network Adapter** is configured for the **Hawthorn** virtual switch.
2. Launch **sWin16DC1**, and log on to **sWin16DC1** as **Administrator.**
3. Do not launch **sWin10CL101** until being instructed.
4. On **sWin16DC1** create an OU called **ICT**.
5. On **sWin16DC1**, in the **ICT** OU create:
   A. Two user accounts **IPuser**, **ISuser**.
   B. Two global groups: **G_ICTProcurement** and **G_ICTSupport.**
   C. Two **Domain Local** groups **DL_Data_FC** and **DL_Data_R**.
   D. Nest :
      - IPuser > G_ICTProcurement > DL_Data_R
      - ISuser > G_ICTSupport > DL_Data_FC
6. On **sWin16DC1** create a shared folder called **Data**. Allocate the **Share** permissions to **Everyone = Full Control.** Give the DL groups the NTFS permissions as described by their names.
7. Create a File called **TopSecret.txt** and add some data into it.

Security settings

8. On sWin16DC1, use **Group Policy Management** to edit the **Default Domain Controllers Policy.**

9. Configure the following settings in **Computer Configuration, Policies, Windows Settings, Security Settings**:

   A. **Account Policies, Password Policy**:

   - **Enforce password history** to **12** passwords remembered
   - **Minimum password age** to **1** day. When prompted accept the default for the Maximum password age (30 days).
   - **Minimum password length** to **8** characters
   - **Password must meet complexity requirements** to **enabled**

   B. **Account Policies, Account Lockout Policy**:

   - **Account lockout threshold** to **3** invalid logon attempts
     (Accept the default 30 minutes for other policies)

10. Create a GPO called **Lab9SecSettings** and link it to the **ICT** OU.

    A. **Local Policies, User Rights Assignment:**

    - **Allow log on locally**, add the **G_ICTSupport** & **Administrators** groups
    - **Deny log on locally**, add the **G_ICTProcurement** groups

11. Test some of these settings on **sWin10CL101**.

    A. Use **gpupdate /force** on the domain controller.

    B. Launch **sWin10CL101** virtual machine.

Predict whether the user can successfully log on **sWin10CL101** as **IPuser**?

____

C. Log on as **IPuser**

Is your prediction correct? ____________

If your prediction was not correct discuss it with a fellow student.

We will now try to understand the observation by seeing which settings have applied to sWin10CL101 by using **gpresult**.

> ***Note:***
> *You may remember from the lecture we learned about having at least two user accounts for every administrator. An unprivileged account for logging on, and a privileged account that administrators use when they need to run an application with elevated privileges. We will be using* ***Run as*** *in the next section. This is how you run an app with elevated privileges.*

12. On **sWin10CL101**, launch an elevated command line console, by clicking **Start**, type ***cmd***, but do **not** press enter!

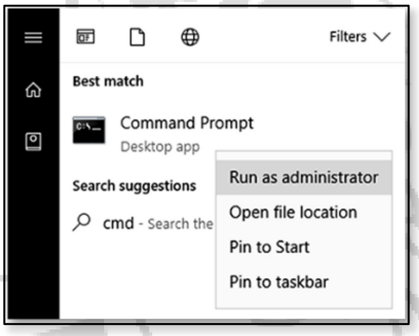
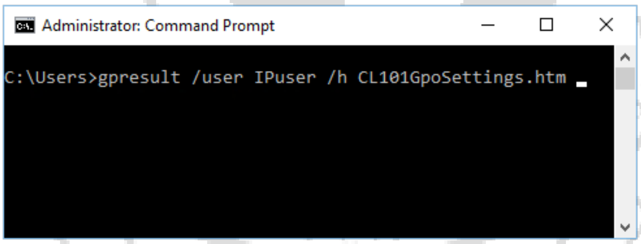


Figure 1 - Run as

- Right click the **Command Prompt** desktop app, and select **Run as administrator**.
- Enter the credentials **sWin\Administrator** with the default password.

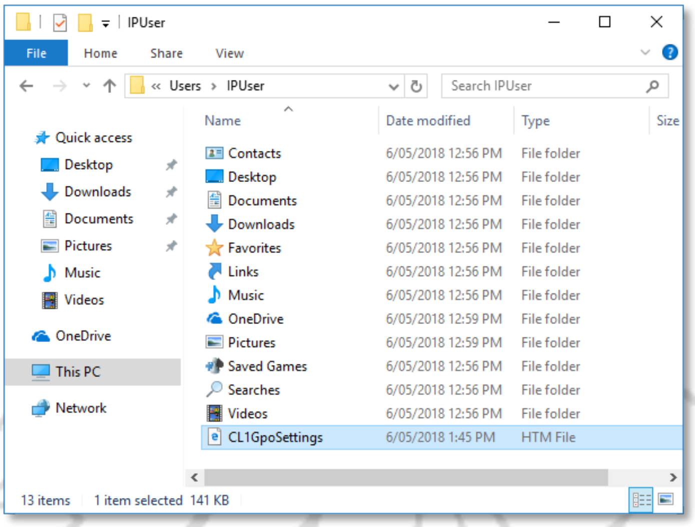
13. At the command prompt, change to the IPuser's home folder by typing: ***cd c:\users\IPuser***.
At the command prompt type the following to generate a report on which GPO settings have been applied:
***gpresult /user* IPuser */h* CL101GpoSettings.htm**, and press **Enter**.



```
C:\Users>gpresult /user IPuser /h CL101GpoSettings.htm
```

Figure 2 - GPresult

14. Using **File Explorer** browse to **C:\Users\IPuser** and double-click **CL101GpoSettings1.htm**



Name	Date modified	Type	Size
Contacts	6/05/2018 12:56 PM	File folder	
Desktop	6/05/2018 12:56 PM	File folder	
Documents	6/05/2018 12:56 PM	File folder	
Downloads	6/05/2018 12:56 PM	File folder	
Favorites	6/05/2018 12:56 PM	File folder	
Links	6/05/2018 12:56 PM	File folder	
Music	6/05/2018 12:56 PM	File folder	
OneDrive	6/05/2018 12:59 PM	File folder	
Pictures	6/05/2018 12:59 PM	File folder	
Saved Games	6/05/2018 12:56 PM	File folder	
Searches	6/05/2018 12:56 PM	File folder	
Videos	6/05/2018 12:56 PM	File folder	
CL1GpoSettings	6/05/2018 1:45 PM	HTM File	

13 items 1 item selected 141 KB

Figure 3 - GPresult Report Location

15. When the report loads, scroll down until you find the **Applied GPOs** section. Was the **Lab9SecSettings** GPO applied?

Explain your observations:

16. In **Active Directory Users and Computers**, move the **sWin10CL101** from the **Computers** container to the **ICT** OU.

Reboot **sWin10CL101**, and log in as **IPuser**

Were you successful?

Explain your observation:

Predict whether **ISuser** can log on, then log on to **sWin10CL101** as **ISuser**

17. From a command line run ***gpresult /h*** **CL101GpoSettings2.htm**

    Which of the following settings have changed? **Account Policies/Password Policy:** ____________________________

    Local Policies/User Rights Assignment ________________________

    Try to explain your observation:

    ____

    ____

    ____

    ____

Restricting Groups

Restricting Groups is a very useful policy that allows the administrator to restrict membership of privileged groups such as the Administrators group.

If a hacker or a junior administrator adds a non-authorised user account to a privileged group, the next time the group policy is applied it all non-authorised accounts are removed.

18. At the **sWin.local** domain level, create and link a GPO called **RestrictAdminGroup**. When created, **Edit** the **Computer Configuration, Policies, Windows Settings, Security Settings, Restricted Groups** policy.

19. Right-click on the **Restricted Groups** container and select **Add Group...** Browse to **Administrators** group.

20. In the Administrators **Properties**, click the **Members of this group: Add** button and add the user account **ISuser**.

Click **OK** until you are back at the Group Policy Management Editor.

21. In **Active Directory Users and Computers**, in the **Builtin** container, right-click on the Administrators group, and select the **Members** tab.

    Click on the **Add...** button and add the user account from the **ICTProcurement** Group. Click **OK**.

    Click on the **Add...** button and add the user account from the **ICTSupport** Group. Click **OK**.

22. Run **gpupdate /force**

    Go back to the **Members** tab of the **Administrators** group and verify that the user **ISuser** remains a member of the Administrators group, but the newly added user account **IPuser** has been removed.

Auditing

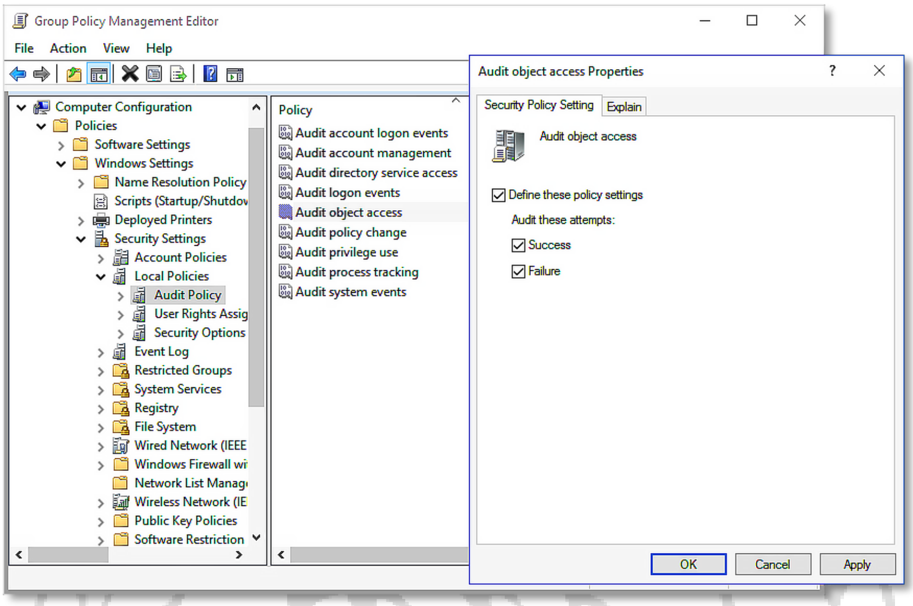
Auditing enables an administrator to keep a record of events such as: Who logs on to the network; who accesses important files. These records can be retrieved using the **event viewer** console.

23. On **sWin16DC1** in **GPMC** edit the **Default Domain Policy**.

    In **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Local Policies**, **Audit Policy**, configure the following settings:

    A. **Audit Account Logon Events** = Enabled: Success & Failure

    B. **Audit Object Access** = Enabled: Success & Failure



Audit object access Properties

Audit object access

☑ Define these policy settings

Audit these attempts:

☑ Success

☑ Failure

Figure 4 - Audit Object Access

24. Go to **C:\Data** and for **TopSecret.txt** go to the **advanced security security** settings and click on the **Auditing** tab.

25. Click **Add**, then click **Select a principal**, then enter **Authenticated Users**. In the **Type:** field select **All** (i.e. both success and failure). The click **OK** to close the Advanced Security settings, then **OK** again to close the **TopSecret** properties.

26. Reboot **sWin10CL101**. Log in as **ISuser** and browse to **\\sWin16DC1\Data** and open up the **TopSecret** file, make some changes, and then save it.

27. On **sWin16DC1**, launch the **Event Viewer** app, expand **Windows Logs** and click on the **Security** log.

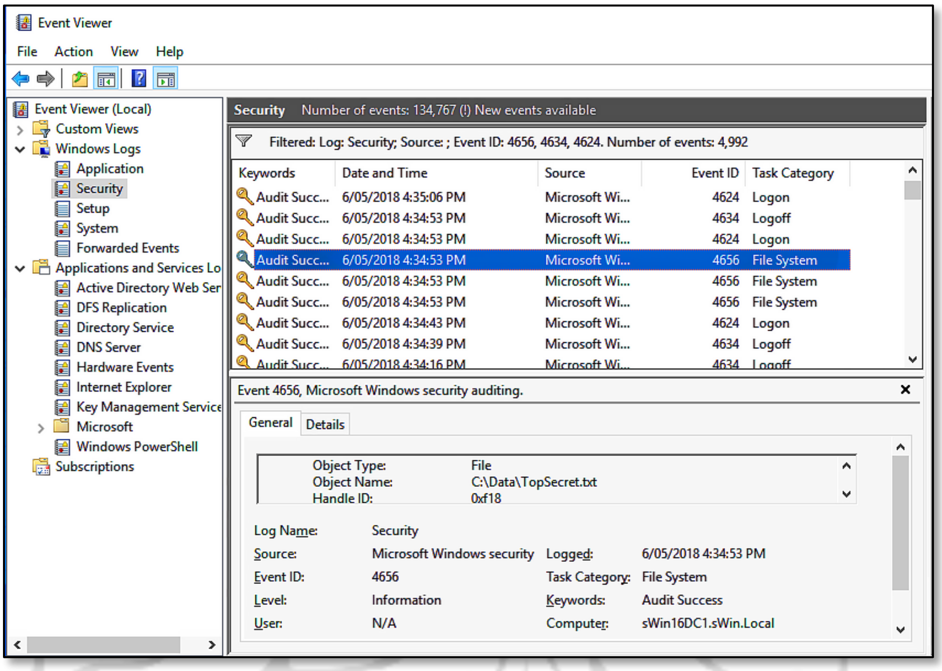
28. Look for the following event IDs:

    A. 4656 for object access events,

    B. 4624 for account logon events,

    C. 4634 for account logoff

    If you are struggling to locate the events you can **Filter Current Log…** for these event IDs, and/or you can **Find…** and enter in the user's logon name **ISuser**.



Security Number of events: 134,767 (!) New events available

Filtered: Log: Security; Source: ; Event ID: 4656, 4634, 4624. Number of events: 4,992

Keywords	Date and Time	Source	Event ID	Task Category
Audit Succ...	6/05/2018 4:35:06 PM	Microsoft Wi...	4624	Logon
Audit Succ...	6/05/2018 4:34:53 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	6/05/2018 4:34:53 PM	Microsoft Wi...	4624	Logon
Audit Succ...	6/05/2018 4:34:53 PM	Microsoft Wi...	4656	File System
Audit Succ...	6/05/2018 4:34:53 PM	Microsoft Wi...	4656	File System
Audit Succ...	6/05/2018 4:34:53 PM	Microsoft Wi...	4656	File System
Audit Succ...	6/05/2018 4:34:43 PM	Microsoft Wi...	4624	Logon
Audit Succ...	6/05/2018 4:34:39 PM	Microsoft Wi...	4634	Logoff
Audit Succ...	6/05/2018 4:34:16 PM	Microsoft Wi...	4634	Logoff

Event 4656, Microsoft Windows security auditing.

Object Type: File
Object Name: C:\Data\TopSecret.txt
Handle ID: 0xf18

Log Name: Security
Source: Microsoft Windows security
Logged: 6/05/2018 4:34:53 PM
Event ID: 4656
Task Category: File System
Level: Information
Keywords: Audit Success
User: N/A
Computer: sWin16DC1.sWin.Local

Figure 5 - Event Viewer: Audit Object Access

Using the Encrypted File System

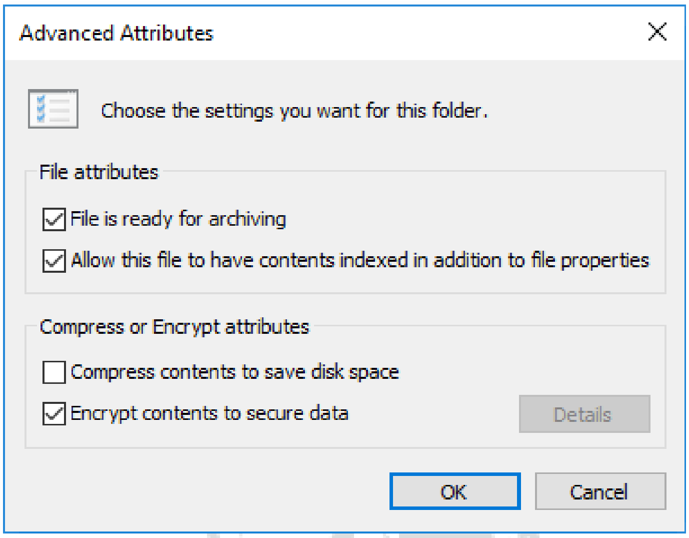
EFS encrypts a file or a folder with a symmetric key, and then encrypts the symmetric key with an asymmetric key stored in a Windows certificate. This means that everyone's copy of the encryption key is both different and secure.

29. On **sWin10CL101**, ensure that the file **TopSecret.txt** is closed.

    A. Right click the file and select **Properties**.

    B. In the default **General** tab, click on the **Advanced...** button.

    C. In the **Advanced Attributes** dialog, check **Encrypt contents to secure data** and click **OK**.



Advanced Attributes

Choose the settings you want for this folder.

File attributes

☑ File is ready for archiving

☑ Allow this file to have contents indexed in addition to file properties

Compress or Encrypt attributes

□ Compress contents to save disk space

☑ Encrypt contents to secure data

Figure 6 - Enable EFS

D. On the **TopSecret Properties** dialog, click **Apply**.

Now if you were to go back to Advanced… you would notice that the Details button is now active. If you wanted to add other user certificates, so they can access the encrypted file, you would do it here.

If you have time, log on to sWin10CL101 as IPuser, and see if you can open the encrypted file.

The remainder of this lab is ***NOT*** *dependent on the preliminary OUs, User Accounts and Groups. If you run out of time you can practice these later. They can also be assessed in Part C of the Skills Exam.*

WSUS settings with GPO

Windows Server Update Services allow administrators to both streamline and control the updates that operating systems and applications require to remain secure.

A computer needs to be configured to download the updates from the WSUS server, and this can be done by using GPOs.

30. On **sWin16DC1** edit the **Default Domain Policy**.
    In **Computer Configuration, Policies, Administrative Templates, Windows Components, Windows Update** make the following changes:

    A. In **Specify intranet Microsoft update service location:**

    - **Enabled**
    - **Set the intranet update service…** = **http://172.16.32.1**
    - **Set the intranet statistics server** = **http://172.16.32.1**

    B. In **Configure Automatic Updates:**

    - **Enabled**
    - **Config. auto. updating:** = **4 – Auto download and schedule install**
    - **Scheduled install day:** = **Every day**
    - **Scheduled install time:** = **04:00**

    C. In **Enable client-side targeting:**

    - **Enabled**
    - **Target group name for this computer**: = **TestPCs**

GPO with Firewall

31. Create a new GPO called **Firewall-AllowPing** and link it to the domain.

32. Edit the GPO by going to and expanding **Computer Configuration, Policies, Windows Settings, Security Settings, Windows Firewall with Advanced Security**

33. Keep expanding until you see **Inbound Rules**. Right click **Inbound Rules** and select **New Rule...** and configure the following as you work through the wizard:

    A. Rule Type = Custom

    B. Program = All programs

    C. Protocol and Ports = Protocol type: ICMPv4

    D. Scope = Any IP address

    E. Action = Allow the connection

    F. Profile = Domain, and Private (i.e. untick Public)

    G. Name

    - Name: = AllowPing
    - Description: = *Rule to temporarily allow pinging in the domain when troubleshooting. Technician: Kim. Job#1532*

Once this GPO has replicated to all computers in the domain you should be able to ping them all. However, once troubleshooting has completed, you should unlink this GPO to prevent ping scans being used in preparation for hacking.

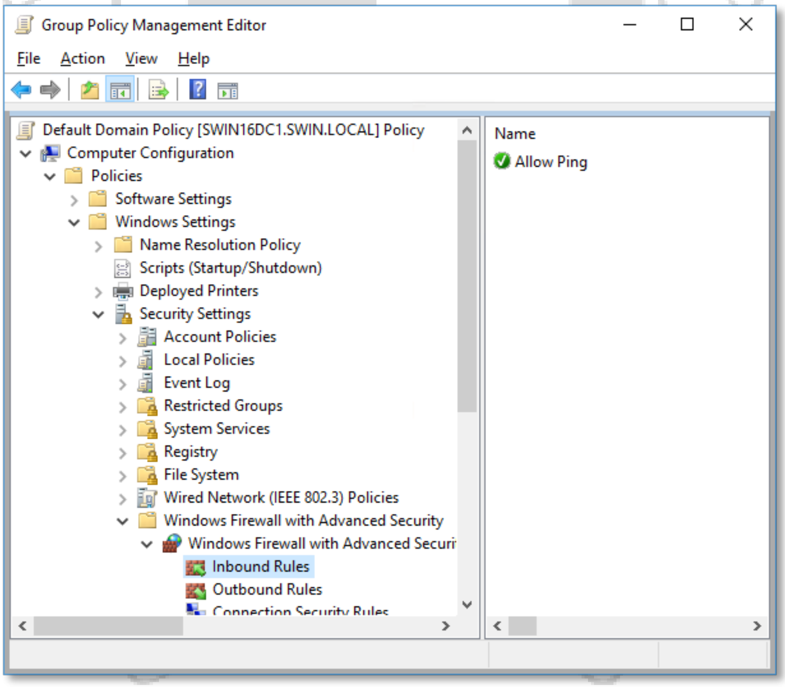


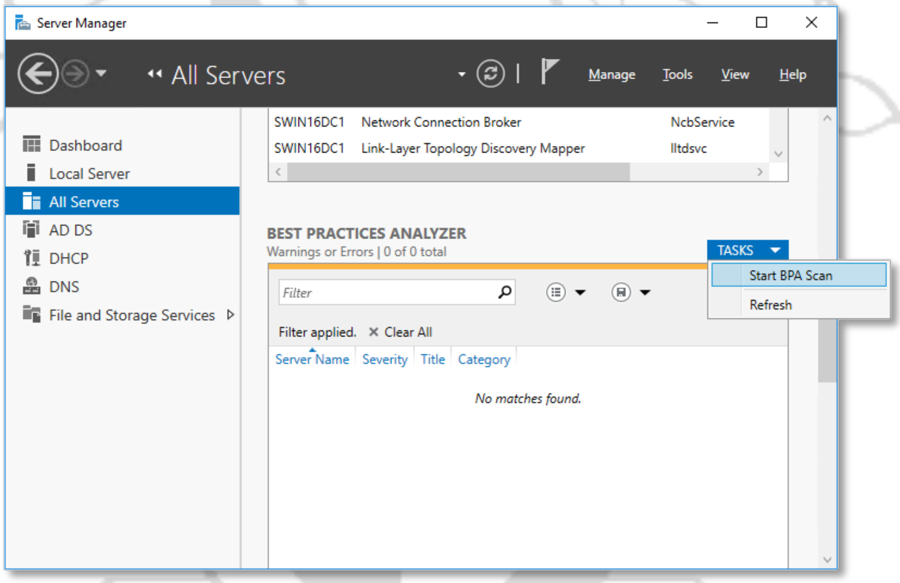
Figure 7 - Windows Firewall via GPO

Best Practices Analyzer or Security Compliance Manager

The Best Practices Analyzer (BPA) is built into Server Manager. It is a tool that scans the server for security hols, and performance improvements. It is similar to the Security Compliance Manager (SCM), which also runs as a wizard and identifies potential security holes. The report provides a list of suggested improvements, with links that either fix the issue for you or take you to a Microsoft web page that provides instructions on how to rectify the issue. For a new network administrator it is a valuable security blanket.

As the focus of this lab is security, ideally we would prefer to use SCM, but as we would need to download it and install it we will proceed with the BPA.

34. In **Server Manager**, click on **All Servers**, and make sure that **SWIN16DC1** is selected. Then scroll down until you see **Best Practices Analyzer**.
35. Click on the drop down arrow next to **TASKS**, select **Start BPA Scan**, then click the **Start Scan** button.



SWIN16DC1	Network Connection Broker	NcbService
SWIN16DC1	Link-Layer Topology Discovery Mapper	lltdsvc

BEST PRACTICES ANALYZER

Warnings or Errors | 0 of 0 total

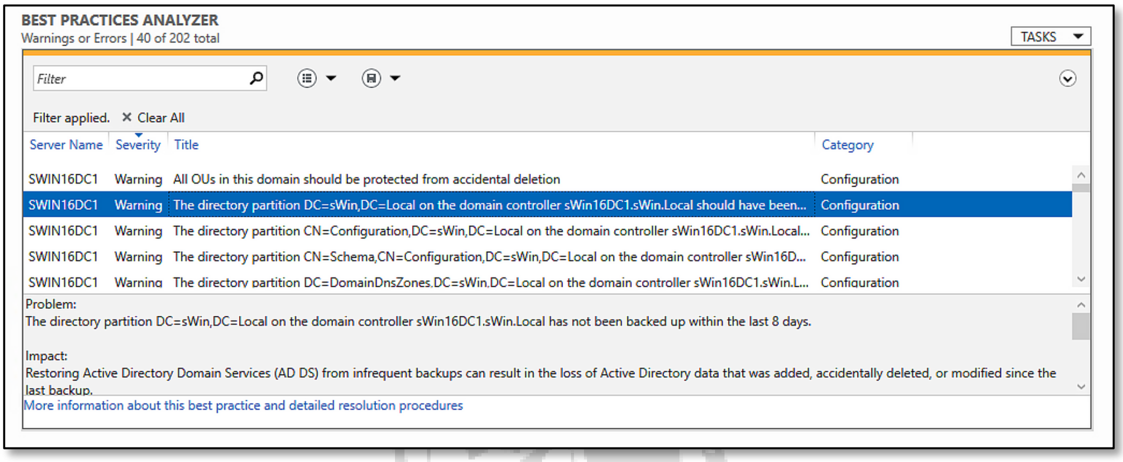
Filter applied.

No matches found.

Figure 8 - Start BPA Scan

It takes a while, so be patient.

36. When the wizard completes you will be provided with a list of warnings.



BEST PRACTICES ANALYZER
Warnings or Errors | 40 of 202 total

Server Name	Severity	Title	Category
SWIN16DC1	Warning	All OUs in this domain should be protected from accidental deletion	Configuration
SWIN16DC1	Warning	The directory partition DC=sWin,DC=Local on the domain controller sWin16DC1.sWin.Local should have been...	Configuration
SWIN16DC1	Warning	The directory partition CN=Configuration,DC=sWin,DC=Local on the domain controller sWin16DC1.sWin.Local...	Configuration
SWIN16DC1	Warning	The directory partition CN=Schema,CN=Configuration,DC=sWin,DC=Local on the domain controller sWin16D...	Configuration
SWIN16DC1	Warning	The directory partition DC=DomainDnsZones,DC=sWin,DC=Local on the domain controller sWin16DC1.sWin.L...	Configuration

Problem:
The directory partition DC=sWin,DC=Local on the domain controller sWin16DC1.sWin.Local has not been backed up within the last 8 days.

Impact:
Restoring Active Directory Domain Services (AD DS) from infrequent backups can result in the loss of Active Directory data that was added, accidentally deleted, or modified since the last backup.

More information about this best practice and detailed resolution procedures

Figure 9 - BPA Report

Clicking on one of the items will provide you with details of the problem, the impact if the problem was to eventuate and a link to where you can get instructions on how to fix the problem… but the links won't work when you are not connected to the internet. So we will leave it here for this exercise.

Pack up

1. Shut down and revert all virtual machines used in this lab.
2. Log off the Host server **ATC626-XY**
3. Push your chair in as you leave.

End of Lab