Windows Server 2008 Configuration

Part 2

Lab Manual

Presented by

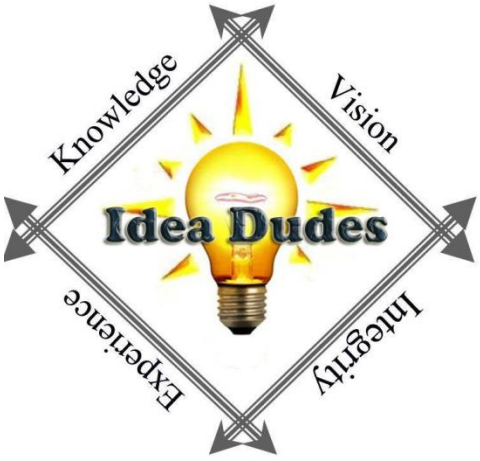

Table of Contents

Module 2 – Implementing Group Policy

Requirements

Use the DC1
First Level Employees, Groups
A global security group in the Groups OU named Sales
Scott Milner
Toya Jackson
Mary Star

Exercise 1: Create, Edit and Scope a Group Policy Object

1. Logon to DC1 with Administrator permissions
2. Open Group Policy Management console from Administrative Tools
3. Expand Forest, Domains, finalvision.com domain and the Group Policy Objects container
4. Right-Click the Group Policy Objects Container and choose New
5. Name box type **FinalVision standards** click OK
6. Right-Click FinalVision Standards GPO and select Edit
7. Right-Click the root node of the console and select Properties
8. Click the Comment Tab and **type FinalVision coroporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO: (type your name)** then click OK
9. Expand User Configuration\Policies\Administrative Templates
10. Check out the policies and settings
11. Right-Click Administrative Templates in the Users Configuration and Choose Filter
12. Select Enable Keyword Filters check box
13. Filter for Words type **screen saver**
14. Choose Exact in the drop-down box
15. Click OK
16. Browse to examine the screen saver policies that you have found
17. Control Panel\Display node, click the policy settings Screen Saver Timeout.
18. Double-click the policy setting Screen Saver Timeout
19. Read the Explanation
20. Click the Settings Tab and select Enabled
21. In the Seconds box, type **600**
22. Comments tab type **Corporate IT Security Policy implemented with this policy in combination with the Password Protect the Screen Saver.**
23. Click OK
24. Double-Click the Password Protect The Screen Saver policy setting
25. Select Enabled
26. Comment tab type **Corporate IT Security Policy implemented with this policy in combination with Screen Saver Timeout**
27. Click OK
28. Close GPME
29. Right-Click finalvision.com domain and choose Link An Existing GPO
30. Select the FinalVision Standards GPO and click OK

Exercise 2: View the Effects of Group Policy Application

1. Right-click the desktop and choose properties on DC1
2. Click Screen Saver
3. Notice you can change the settings
4. Open a command prompt and type **gpupdate.exe /force /boot /logoff**
    a. This will refresh the group policy
5. Return to the Screen Saver Settings and you should not be able to change settings

Exercise 3: Explore a GPO

1. In the Group Policy Management Console, select the FinalVision Standards GPO in the Group Policy Container
2. Scope Tab, notice that GPO reports its links in the Links section
3. Click the Settings tab to see a report of the policy settings in the GPO
4. Click Show All link at the top of this settings report and this will display all of the settings that have been configured
5. Point at the text for the policy Screen Saver Timeout. This is a hyperlink that will give you a detailed explanation of the policy settings
6. Click Details tab. This will show the Comments from the Comments tab
7. Write down the Unique ID on the Details tab
8. Open the following \\finalvision\SYSVOL\finavision.com\Policies
9. Double-click the folder with the recorded folder number this is the GPT of the GPO

Exercise 4: Explore Administrative Templates

1. Open the %SystemRoot%\PolicyDefintions folder
2. Open en-us folder or folder for your region
3. Double-Click ContorPanelDisplay.adml. Open it up in Notepad.
4. Turn on Word Wrap from the format menu
5. Search for the ScreenSaverIsSecure text
6. Note the label and the explanatory text
7. Close the file and navigate to the PolicyDefinitions folder
8. Double-Click ControlPanelDisplay.admx and open in Notepad
9. Search for the text shown here

```
<policy name=”ScreenSaversIsSecure” class=”User”
displayName=”$(string.ScreenSaverIsSecure)”
explainText=”$(string.ScreeenSaverIsSecure_Help”)
key=”Software\Policies\Microsoft\Windows\Control Panel\Dekstop”
valueName=”ScreenSaverIsSecure”>
        <parentCategory ref=”Display” />
        <supportedOn ref=”windows:SUPPORTED_Win2kSP1” />
        <enabledValue>
                <string>1</string>
        </enabledValue>
        <dsiabledValue>
                <string>1</string>
        </disabledValue>
</policy>
```

10. Identify the parts of the template that define the following
    a. The name of the policy settings that appears in the GPME
    b. Explanatory text
    c. Registry Key and value affected by the policy setting
    d. The data put into the registry if the policy is enabled
    e. The data put into the registry if the policy is disabled

Exercise 5: Creating a Central Store

1. In Group Policy Management Console, right-click FinalVision Standards and choose Edit
2. Expand User Configuration\Policies\Administrative Templates
3. Definitions are ADMX
4. Close GPME
5. Open the following folder \\finalvision.com\SYSVOL\finalvision.com\Policies
6. Create a folder called PolicyDefinitions
7. Copy the contents of %SystemRoot%\PolicyDefinitions to the folder
8. Right-Click FinalVision Standards and select Edit
9. Expand User Configuration\Policies\Administrative Templates
10. Notice that the node reports Policy Definitions (ADMX files) Retrieved From The Central Store

Module 3 – Configuring Group Policy Scope

Requirements

Use the DC1
First Level Employees, Groups
A global security group in the Groups OU named Sales
Scott Milner
Toya Jackson
Mary Star

Exercise 1: Create a GPO with a Policy Setting That Takes Precedence over a Conflicting Setting

1. Logon to DC1 with the Administrator
2. Open ADUC and create a first-level OU called **Engineers**
3. Open GPMC
4. Right-Click the Engineers OU and choose Create A GPO In This Domain, And Link It Here
5. Enter the name **Engineering Application Override** and click OK
6. Expand the Engineers OU, right-click the GPO and Choose Edit
7. Expand the User Configuration\Policies\Administrative Templates\Control Panel\Display
8. Double-Click the Screen Saver Timeout policy setting
9. Click Disabled, and then click OK
10. Close the GPME
11. In the GPMC select Engineering Application Override and then click the Group Policy Inheritance tab
12. Notice that the Engineering Application Override GPO has precedence over the FinalVision Standards GPO

Exercise 2: Configure the Enforced Option

1. In the GPMC right-click finalvision.com and choose Create A GPO In This Domain and Link It Here
2. Enter the name **Enforced Domain Policies** and click OK
3. Right-Click the GPO and choose Edit
4. Expand Computer Configuration\Policies\Administrative Templates\System\Logon
5. Double-click that Always Wait For The Network At Computer Startup And Logon policy setting
6. Select Enabled and click OK
7. Close GMPE
8. Right-Click the Enforce Domain Policies GPO and choose Enforced
9. Select the Engineers OU, and then click the Group Policy Inheritance tab
    a. Notice that your enforce domain GPO has precedence even over GPOs linked to the Engineers OU

Exercise 3: Configure Security Filtering

1. Open ADUC and create global security group named GPO_FINALVISION Standards_Exceptions
2. In the GPMC, select the Group Policy Objects container
3. Right-click the Engineering Application Override GPO and choose Delete. Click Yes to confirm your choice
4. Select the FINALVISION Standards GPO in the Group Policy Objects container
5. Click the Delegation tab
6. Click the Advanced button
7. In the Security Settings dialog box, click the Add button
8. Type the name of the group and click OK
9. In the permissions list, scroll down and select the Deny permission for Apply Group then click OK
10. Click Yes to confirm your choice
11. Note the entry shown on the Delegation tab in Allowed Permissions column for the GPO_FINALVISION Standards_Exceptions group
12. Click the Scope tab and examine the Security Filtering section

Exercise 4: Loopback Policy Processing

1. Open ADUC and create global security group called **Sales Laptops** in the Groups OU
2. In the GPMC, right-click the Group Policy container and choose New
3. Name Box type **Sales Laptop Configuration** and click OK
4. Right-Click the GPO and choose Edit
5. Expand User Configuration\Policies\Administrative Templates\Desktop\Desktop
6. Double-Click the Desktop Wallpaper policy setting
7. Click the Explain tab and review the explanatory text
8. Click the Comment tab and type **Corporate standard wallpaper for sales laptops**
9. Click the Settings tab
10. Select Enabled
11. In the Wallpaper Name Box type **c:\windows\web\Wallpaper\server.jpg**
12. Click OK
13. Expand Computer Configuration\Policies\Administrative Templates\System\Group Policy
14. Double-click the User Group Policy Processing Mode policy setting
15. Click Enabled and, in the Mode drop-down list, select Merge
16. Click OK and close GPME
17. In the GPMC, select the Sales Laptop Configuration GPO in the Group Policy container
18. On the Scope tab, in the Security Filtering section, select the Authenticated Users group and click the Remove button. Click OK to confirm your choice
19. Click the Add button in the Security Filtering section
20. Type the group name. **Sales Laptops**, and click OK
21. Right-click the Desktops OU and choose Link an Existing GPO
22. Select Sales Laptop Configuration and Click OK
    a. Sales Laptops group has been filtered by Security filtering to apply the Sales Laptop Configuration GPO

Module 4 – Configuring Group Policy Scope

Requirements

Use the DC1
First Level Employees, Groups
A global security group in the Groups OU named Sales
Scott Milner
Toya Jackson
Mary Star
Module 3 OUs and Groups

Exercise 1: Use the Group Policy Results Wizard

1. Logon to DC1 with Administrator
2. Open a command prompt and type **gpupdate /force /boot** (record the system time for later exercise)
3. Logon to DC1 with Administrator
4. Expand Forest
5. Right-click Group Policy Results and choose Group Policy Results Wizard
6. Click Next
7. On the Computer Selection page, select This Computer and click Next
8. On the User Selection page, select Display Policy Settings For, select a Specific User and Select FinalVision\Administrator then Click Next
9. On the Summary of Selections page , review the settings and click Next
10. Click Finish
11. On the Summary tab, click the Show All link at the top of the report
12. Review the Group Policy Summary results
13. Click the Settings Tab and click the Show All Link at the top of the page
14. Click the Policy Events tab and locate the event that logs the policy refresh and compare the times
15. Click the Summary tab, right-click the page, and choose Save Report and HTML
16. Open the saved RSoP report from your Documents folder

Exercise 2: Use the Gpresult.exe Command

1. Open a command prompt
2. Type **gpresult /r** and press ENTER
3. Type **gpresult /v** and press ENTER
4. Type **gpresult/z** and press ENTER
5. Type **gpresult /h:"%userprofile%\Documents\RSOP.html"** and press ENTER
6. Open the saved RSOP report from your Documents folder.

Exercise 3: View Policy Events

1. Open the Event View console from the Administrative Tools menu
2. Expand Windows Logs\System
3. Locate events with GroupPolicy as the Source.
4. Review the information associated with GroupPolicy events
5. Click the Application node in the console tree underneath Windows logs
6. Sort the Application log by the Source column
7. Review the logs by Source and identify the Group Policy events that have been entered in this log
8. In the console tree, expand Application and Services Logs\Microsoft\Windows\GroupPolicy\Operational
9. Locate the first event related in the Group Policy refresh you accomplished in Exercise 1

Exercise 4: Perform Group Policy Modeling

1. Open ADUC
2. Create a user account Elmer Fudd in the Employee OU
3. Create an OU called Laptops in the Disney OU
4. Create a computer account called LAPTOP101 in the Laptops OU
5. Add LAPTOP101 and Domain Users to Sales Laptops group
6. In the GPMC (Group Policy Management Console), expand Forest
7. Right-Click Group Policy Modeling and choose Group Policy Modeling Wizard
8. Click Next
9. On the Domain Controller Selection page, click Next
10. On the User and Computer Selection page, in the User Information section, click the User button, click Browse and then click Elmer Fudd
11. In the Computer Information section, click the Computer button, click Browse, select LAPTOP101
12. Click Next
13. Select Loopback Processing and select Merge on the Advanced Simulation Options page
14. Click Next
15. On the Alternate Active Directory Paths page, click Next
16. On the User Security Groups, page click Next
17. On the Computer Security groups page, click Next
18. On the WMI Filters for Users page, click Next
19. On the WMI filters for Computer page, click Next
20. Review your settings on the Summary Of Selections page, click Next and then click Finish
21. Examine the Report produced

Module 5 – Delegating Membership Using Group Policy

Requirements

Use the DC1
A first level named Admins with a Sub-OU named Admin Groups
A global security group named Help Desk in the Admins\Admins Groups OU
A global security group named Miami Support in the Admins\Admins Groups OU
A first-level OU named Laptops
An OU named Miami in the Laptops OU
A computer object named DESKTOP101 in the Miami OU

Exercise 1: Delegate the Administration of All Clients in the Domain

1. Logon to DC1 as an Administrator
2. In the GPMC, expand Forest\Domain\finalvision.com. Select the Group Policy Objects container
3. Right-Click the Group Policy Objects and choose New
4. In the name box type **Corporate Help Desk** and click OK
5. Right-click the GPO and select Edit
6. In GPME navigate to Computer Configuration\Policies\Windows Settings\Security Settings\Restricted
7. Right=Click Restricted Groups and choose Add Group
8. Click the Browse button and, in the Select Groups dialog box type **finalvision\Help Desk** and click OK
9. Click OK to close the Add Group dialog box
10. Click the Add button next to the This Group Is A Member of sections
11. Type **Administrators** and click OK
12. Click OK again to close the Properties dialog box
13. Close the GPME
14. In the GPMC, right click the Laptops OU and choose Link An Existing GPO
15. Select the Corporate Help Desk GPO

Exercise 2: Delegate the Administration of a Subset of Clients in the Domain

1. In the GPMC, expand Forest\Domains\finalvision.com
2. Right-Click the Group Policy Objects container and choose New
3. In the Name box, type **New York Support** and click OK
4. Right-click the GPO and choose Edit
5. Repeat 5-12 of Exercise 1 except type **finalvision\Miami Support** in step 7
6. In the GPMC, Right-click the LapTops\Miami OU and choose Link An Existing GPO
7. Select Miami Support GPO and click OK

Exercise 3: Confirm the Cumulative Application of Member Of Policies

1. In the GPMC, expand Forest and Select Group Policy Modeling node
2. Right-click Group Policy Modeling node and select Group Policy Modeling Wizard
3. Click Next
4. On the Domain Controller Selection page, click Next
5. On the User and Computers Selection page, in the Computer Information section, click the Browse button
6. Expand the domain and the LapTops OU and then select Maimi OU
7. Click OK
8. Select Skip To The Final Page Of This Wizard Without Collecting Additional Data check box
9. Click Next
10. On the Summary Of Selections page, click Next
11. Click Finish
12. Click the Settings tab
13. Double-click Security Settings
14. Double-click Restricted Groups
    a. Help Desk and Miami Support should be listed

Module 6 – Managing Security Settings

Requirements

Use the DC1
A first-level OU Disney
Admins OU located under Disney
An OU named Admin Groups under Admins OU
Global security group SYS_DC Remote Desktop in Admin Groups OU is a member of Remote Desktop Users Group

Exercise 1: Configure the Local Security Policy

1. Logon to DC1 with Administrative Permissions
2. Open the Local Security Policy from the Administrative Tools Folder
3. Expand Security Settings\Local Policies\User Rights Assignment
4. In the details pane, double-click Allow Log On Through Terminal Services
5. Click Add User or Group
6. Type finalvision\SYS_DC Remote Desktop and click OK
7. Click OK again
    a. This will allow the SYS_DC Remote Desktop group access through Terminal Services
8. Double-click Allow Log On Through Terminal Services
9. Select finalvision\SYS_DC Remote Desktop
10. Click Remove
11. Click OK

Exercise 2: Create a Security Template

1. Click Run from the Start Menu
2. Type **mmc** and press ENTER
3. Choose Add/Remove Snap-in from the File Menu
4. Select Security Templates from the Available Snap-ins and click the Add Button and Click OK
5. Choose Save from the File menu and save the console with the name Security Management
6. Right-click C:\Users\Administrator\Documents\Security\Templates and choose New Template
7. Type **DC Remote Desktop** and click OK
8. Expand DC Remote Desktop\Local Policies\User Rights Assignments
9. In the details, double-click Allow Log On Through Terminal Services
10. Select Define These Policy Settings In the Template
11. Click Add User or Group
12. Type **finalvision\SYS_DC Remote Desktop** and click OK
13. Right-click DC Remote Desktop and choose Save

Exercise 3: Use the Security Configuration and Analysis Snap-In

1. Choose Add/Remove Snapin from the File menu
2. Select Security Configuration Analysis from the Available Snap-Ins and click the Add button, click OK
3. Right-click the same node and choose Open Database
4. Type **DC1Test** and click Open
5. Select DC Remote Desktop template and click OK
6. Right-click Security Configuration and Analysis and choose Analyze Now
7. Click OK
8. Expand Local Policies and select User Rights Assignment
9. Notice that the Allow Log On Through Terminal Services policy is flagged with a red-circle and an X. This indicates a discrepancy between the database setting and the computer setting.
10. Double-click Allow Log On Through Terminal Service
11. Click the checkbox next to Administrators under Database Setting, and then click OK
12. Right-click Security Configuration and Analysis and choose Save
13. Right-click Security Configuration and choose Explore Template
14. Select DC Remote Desktop and click Save
15. Close and reopen your Security Management console
16. Expand c:\users\Administrator\Documents\Security\Templates\DC Remote Desktop\Local Policies\User Rights Assignment
17. In the details pane, double-click Allow Log On Through Terminal Services
18. SYS_DC Remote Desktop and Administrators are present
19. Right-click Security Configuration and Analysis and choose Configure Computer Now
20. Click OK and confirm the error path
21. Open the Local Security Policy console
22. Expand Security Settings\Local Policies\User Rights Assignment. Double-click Allow Log On Through Terminal Services
23. Confirm that both Administrators and SYS-DC Remote Desktop are listed

Exercise 4: Use the Security Configuration Wizard

1. Open the Security Configuration Wizard from the Administrative Tools Folder
2. Click Next
3. Select Create A New Security Policy and click Next
4. Accept the default server name, DC1 and click Next
5. On the Processing Security Configuration Database, view the Configuration Database (explore it)
6. Close the Configuration View
7. Click Next and on the Role Based Service Configuration page, click Next
8. On the Select Server Roles, Select Client Features, Select Administration and Other Options, Select Additional Servers, and Handling Unspecified Services pages, examine the settings , click Next on each page
9. Click Next on the Confirm Service Change page
10. On the Network section introduction page, click Next
11. On the Network Security page, click Next (Do Not Change Any Settings)
12. On the Registry Settings section introduction page, click Next
13. Click through pages but do not change any settings
14. On the Audit Policy intro page, click Next
15. On the System Audit Policy page, examine but do not make changes and click Next
16. Audit Summary page, examine, click Next
17. On the Save Security Policy click Next
18. Type **DC Security Policy** click Include Security Templates and click Add
19. Browse and locate DC Remote Desktop template

20. Click OK
21. Click View Security Policy to examine the settings of the security policy
22. Accept the Apply Later default setting and click Next
23. Click Finish

Exercise 5: Transform a SCW Security Policy to a Group Policy

1. Open a command prompt
2. Type **cd c:\windows\security\msscw\policies** and press ENTER
3. Type **scwcmd transform /?** and press ENTER
4. Type **scwcmd transform /p:"DC Security Policy.xml" g:/"DC Security Policy"** and press ENTER
5. Open GPMC
6. Expand the console tree Forest\Domains\finalvision.com\Group Policy Objects
7. Select DC Security Policy
8. Click Settings tab to examine the settings of the GPO
9. Click the Show Link next to Security Settings
10. Click the Show link next to Local Policies\User Rights Assignment
11. Confirm that the BUILTIN\Administrators and finalvision\SYS_DC Remote Desktop groups are give the Allow Log On Through Terminal Services user right

Module 7– Managing Software with Group Policy Installation

Requirements

Use the DC1
Create a first-level OU named Groups and create a OU called Applications
Create a global security group named APP_XML Notepad to represent the users and computers to which XML Notepad is deployed
Create a folder named Software on C Drive
Create a folder named XML Notepad
Give APP_AML Notepad Read and Execute permission
Share the Software folder with the Share name Software and grant Everyone group the Allow Full Control share permission
Download XML Notepad from the Microsoft downloads http://www.microsoft.com/downloads

Exercise 1: Create a Software Deployment GPO

1. Log on to DC1 as Administrator
2. Open the GPMC
3. Right-click the Group Policy Container and choose New
4. In the Name box, type name **XML Notepad**, and then click OK
5. Right-click the XML Notepad GPO and choose Edit
6. Expand User Configuration\Policies\Software Settings
7. Right-click Software Installation, choose New and then select Package
8. In the File Name text box, type **\\DC1\software** select the Windows Installer package
9. In the Deploy Software dialog box, Select Advanced and click OK
10. On the General tab, note that the name of the package includes the version
11. Click the Deployment Tab
12. Select Assigned
13. Select the Install This Application At Logon check box
14. Select Uninstall This Application When It Falls Out Of The Scope Of Management
15. Click OK
16. Close GPME
17. In the GPMC, select XML Notepad GPO in the Group Policy Objects container
18. Click the Scope tab
19. In the Security Filtering section, select Authenticated Users and click Remove
20. Click OK
21. Click the Add button
22. Type **APP_XML Notepad**
23. Click OK
24. Right-click the domain finalvision.com and choose Link An Existing GPO
25. Select XML Notepad and Click OK

Exercise 2: Upgrade and Application

1. Open GPMC
2. Right-click the XML Notepad GPO in the Group Policy Container and choose Edit
3. Expand User Configuration\Policies\Software Settings
4. Right-click Software Installation, choose New and then select Package
5. In the File Name text box, enter **\\dc1\software** select the XMLNotepad.msi and click Open
6. Click Open
7. Click the Advanced option and click OK
8. On the General tab, change the name of the package type **XML Notepad 2010**
9. Click the Deployment tab
10. Select Assigned
11. Select the Install This Application At Logon check box
12. Click the Upgrades tab
13. Click Add Button
14. Select the Current Group Policy Object (GPO) option
15. Package To Upgrade List, select the package for the simulated earlier version, XML Notepad 2007
16. Select Uninstall The Existing Package, and select Then Install The Upgrade Package
17. Click OK
18. Click OK again
19. Right-click the package that you just created , choose All Tasks, and then click Remove
20. Select Immediately Uninstall The Software From Users and Computers Option
21. Click OK

Module 8– Auditing

Requirements

Use the DC1
Create a folder called Confidential Data on the C Drive
Create a global security group called Consultants
Add the Consultants to the Print Operators Group
Create a user name Robert Newton and add the user to the Consultants group

Exercise 1: Configure Permissions and Audit Settings

1. Logon to DC1 as Administrator
2. Open the properties of the C:\Confidential Data folder and click the Security tab
3. Click Edit
4. Click Add
5. Type **Consultants** and click OK
6. Click the Deny check box for the Full Control permission
7. Click OK to close the Permissions dialog box
8. Click Advanced
9. Click Auditing tab
10. Click Edit
11. Click Add
12. Type **Consultants** and click OK
13. In the Audit Entry dialog box, select the check box under Failed next to Full Control
14. Click OK

Exercise 2: Enable Audit Policy

1. Open GPMC and select Group Policy Objects container
2. Right-click the Domain Controller Security Policy and choose Edit
3. Expand Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy
4. Double-click Audit Object Access
5. Select Define These Policy Settings
6. Select the Failure check box
7. Click OK
8. Open command prompt
9. Type **gpupdate /force** and press ENTER

Exercise 3: Generate Audit Events

1. Logon on to DC1 as Robert Newton
2. Attempt to open C:\Confidential Data
3. Create a text file on the desktop and cut it and attempt to paste it the C:\Confidentail Data folder

Exercise 4: Examine the Security log

1. Logon to DC1 as Administrator
2. Open the Event Viewer
3. Expand Windows Logs\Security
4. Click the Filter Current Log link in the Actions pane
5. Configure the filter as narrow as possible
6. Click OK
7. Click the Save Filter Log File As link in the Action pane
8. Choose text and type **Audit Log Export**
9. Click Save
10. Open the resulting text file in Notepad and search for instances of C:\Confidential Data

Exercise 5: Use Directory Services Changes Auditing

1. Open ADUC
2. Click View menu and Ensure that the Advanced Features us selected
3. Select the Users container
4. Right-click the Domain Admins and choose Properties
5. Click the Security tab and then click Advanced
6. Click the Auditing tab and click Add
7. Type **Everyone** and then click OK
8. In the Audit Entry dialog box click the Properties tab
9. Select the check box below Successful and next to Write Members
10. Click OK
11. Click OK
12. Click the Members tab
13. Add the user Robert Newton and click Apply
14. Select Robert Newton, click Remove and then click Apply
15. Click OK to close the Domain Admins Properties dialog box
16. Open the Security Log and located the events that are generated when you added Robert Newton
    a. 4662
17. Open a command prompt and type **auditpol /set /subcategory: "directory service changes" /success:enable**
18. Open the properties of Domain Admins and add Robert Newton to the group
19. Return to the Event Viewer snap-in and refresh the view of the Security log
    a. Event ID 5136
20. Examine the information in the Directory Services Changes event

Module 9– Configuring Password and Lockout Policies

Requirements

Use the DC1

Exercise 1: Configure the Domain's Password and Lockout Policies

1. Logon to DC1 as an Administrator
2. Open GPMC
3. Expand Forest\domains\finalvision.com
4. Right-click Default Domain Policy and choose Edit
5. Click OK
6. Expand Computer Configuration\Policies\Security Settings\Account Policies and then select Password Policy
7. Double-click the following
    a. Maximum Password Age: 90 days
    b. Minimum Password Length: 10 characters
8. Select Account Lockout Policy in the console tree
9. Double-click the Account Lockout Threshold policy setting and configure it for 5 Invalid Logon Attempts then click OK
10. Click OK
11. Close the GPME

Exercise 2: Create a Password Settings Object

1. Open ADSI Edit from the Administrative tools folder
2. Right-click ADSI Edit and choose Connect to
3. In the Name box , type **finalvision.com** click OK
4. Expand finalvision.com and select DC=finalvision, DC=Com
5. Expand CN=System and select CN=Password Settings Container
6. Right-click the PSC, choose New and then select Object
7. Click Next
8. Configure each attribute as indicated in the following
    a. Common Name **My Domain Admins PSO**
        i. This is the friendly name
    b. msDS-PasswordSettingsPrecedence : **1**
        i. PSO has the highest because it is closest to 1
    c. msDS-PasswordReversibleEncryptionEnabled : **False**
        i. Password is not stored in clear text
    d. msDS-PasswordHistoryLength: **30**
        i. User cannot use same password for 30 times
    e. msDS-PasswordComplexityEnabled : **True**
        i. Complexity rules are enforced
    f. msDS-PasswordLength: **15**
        i. Length of the password
    g. msDS-MinimumPasswordAge: **1:00:00:00**
        i. How long user has to wait before changing password
    h. msDS-MaximumPasswordAge: **45:00:00:00**
        i. Password must be changed every 45 days
    i. msDS-LockoutThreshold: **5**
        i. How many attempts before lockout
    j. msDS-LockoutObservationWindow: 0:01:00:00
        i. 5 failed logons will cause account to be locked
    k. msDS-LockDuration: **1:00:00:00**
        i. Account will remain locked for 1 day unless unlocked manually
9. Click the More Attributes button
10. Edit attributes box, type CN=DomainAdmins, CN=Users, DC=finalvision,DC=Com
11. Click OK
12. Click Finish

Exercise 3: Identify the Resultant PSO for a User

1. Open ADUC
2. Click View menu and make sure Advanced Features is selected
3. Expand finalvision.com and click Users container
4. Right-click the Administrators account and choose Properties
5. Click the Attribute Editor tab
6. Click the Filter button and make sure that Constructed is selected
7. In the Attributes list, locate msDS-ResultantPSO
8. Identify the PSO that affects the user

Exercise 2: Enable Audit Policy

1. Repeat steps 1-6 of Exercise 2 to select the Password Settings container in ADSI Edit
2. In the console details pane, select CN=My Domain Admins PSO
3. Press Delete
4. Click Yes

Module 10– Auditing Authentication

Requirements

Use the DC1

Exercise 1: Configuring Auditing of Account Logon Events

1. Logon to DC1 as an Administrator
2. Open GPMC
3. Expand Forest\Domains\finalvision.com\Domain Controllers
4. Right-click Default Domain Controllers Policy and select Edit
5. Expand Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies and select Audit Policy
6. Double-click Audit Account Logon Events
7. Select the Define These Policy Settings check box
8. Select both Success and Failure check boxes and click OK
9. Double-click Audit Logon Events
10. Select the Define These Policy Settings check boxes and click OK
11. Close GPME
12. Click Start and click Command Prompt
13. Type **gpupdate /force**

Exercise 2: Generate Account Logon Events

1. Log off of DC1
2. Attempt to log on as Administrator with an incorrect password (repeat this once or twice)
3. Log on to DC1 with correct password

Exercise 2: Generate Account Logon Events

1. Open Event Viewer
2. Expand Windows Logs, and then select Security
3. Identify the failed and successful events

Module 11– Configuring Read-Only Domain Controllers

Requirements

Use the DC1

Install a Second Server called RODC1
- IP Address: 10.10.0.30
- Subnet Mask: 255.255.0.0
- Default Gateway: 10.10.0.1
- DNS Server: 10.10.0.10

Create the following objects
- Global security group called Branch Office Users
- Users Robert Newton, Kathy Bayes and are members of Branch Office Users
- Michael Douglas
- Add the Domain Users group as a member of the Print Operators group

Exercise 1: Install an RODC

1. Logon to RODC1
2. Click Start and click Run
3. Type **dcpromo** and click OK
4. Click Next
5. On the Operating System Compatibility page, click Next
6. On the Choose a Deployment Configuration page, Select the Existing Forest option and select Add a Domain Controller to An Existing Domain Click Next
7. On the Network Credentials page, type **finalvision.com**
8. Click the Set button
9. In the Username type **Administrator**
10. In the Password box, type **Pa$$w0rd**
11. Click OK
12. Click Next
13. On the Select A Domain page, select finalvision.com and click Next
14. On the Select A Site page, select Default-First-Site-Name and click Next
15. On the Additional Domain Controller page, select Read-Only Domain Controller and select Next
16. On the Delegation of RODC Installation and Administration page, click Next
17. On the Location for Database, Log Files, and SYSVOL click Next
18. On the Directory Service Restore Mode Administrator password type **Pa$$w0rd** and confirm then click Next
19. On the Summary Page click Next
20. In the progress window, select the Reboot On Completion check box

Exercise 2: Configure Password Replication Policy

1. Logon to DC1
2. Open ADUC
3. Expand the domain and select the Users container
4. Examine the default membership of the Allowed RODC Password Replication Group
5. Open the properties of the Denied RODC Password Replication Group
6. Add the DNS Admins group as a member of the Denied RODC Password Replication Group
7. Select the Domain Controllers OU
8. Open the properties of RODC1
9. Click the Password Replication Policy tab
10. Identify the PRP settings for the Allowed RODC Password Replication Group and Denied RODC Password Replication Group
11. Click Add button
12. Select Allow Passwords for the Account To Replicate To This RODC and click OK
13. In the Select Users, Computers or Groups dialog box type **Branch Office Users** and click OK
14. Click OK

Exercise 3: Monitor Credential Caching

1. Logon to RODC1 as Robert Newton and then log off
2. Logon to RODC1 as Kathy Bayes and the logoff
3. Log on the DC1
4. Open ADUC
5. Open properties of RODC1
6. Click the Password Replication Policy tab
7. Click Advanced button
8. On the Policy Usage tab, select Accounts Whose Passwords Are Stored On this Read-Only Domain Controller from the drop-down menu
9. Locate the entry for Robert Newton
10. Locate the entries for Robert Newton and Kathy Bayes
11. Click Close and then Click OK

Exercise 4: Prepopulate Credentials Caching

1. Log on to DC1 with Administrator
2. Open ADUC
3. Open properties of RODC1
4. Click Password Replication Policy tab
5. Click the Advanced Button
6. Click the Prepopulate Passwords button
7. Type **Donald Duck** and click OK
8. Click Yes to confirm you want to send credentials to the RODC
9. On the Policy Usage select Accounts Whose Passwords Are Stored On The Read-Only Domain Controller
10. Locate Donald Duck
11. Click OK

Module 12– Install the DNS Service

Requirements

Three Windows 2008 Servers

Server01 (10.10.0.40,255.255.0.0 DNS-10.10.0.40)
Server02(10.10.0.50,255.255.0.0 DNS-10.10.0.50)
Server03(10.10.0.60,255.255.0.0 DNS-10.10.0.60)

Exercise 1: Install a Primary DNS Server

1. Logon to DC1 as an Administrator
2. In the Server Manager, right-click the Roles node and Select Add Roles
3. Review the information in the DNS Server page and Click Next
4. Review your choices and click Cancel
5. Examine the installation results and click OK
6. Move to the DNS Server node in the Server Manager and expand all its sections
7. Explore the DNS server container

Exercise 2: Install AD DS and Create a New Forest

1. Logon to Server01 with the local administrator account
2. In the Server Manager, right click node and select Add Roles
3. On the Roles page select Active Directory Domain Service and click Next
4. Review the information and click Next
5. Confirm your choices and click Install
6. Examine the installation results and click Close
7. Click the Server Manager Active Directory node in the Server manager
8. Click Run the Active Directory Domain Services Installation Wizard in the details pane
9. Click Next
10. Review the information and click Next
11. On the Choose A Deployment Configuration page, choose Create A New Domain In A New Forest and click Next
12. On the Name The Forest Root Domain page, type **NewInnovations.com** and click Next
13. On the Set Forest Functional Level page, select Windows 2008 Server from the drop-down list and click Next
14. On the Additional Domain Controller Options page, verify that DNS and Global Catalog are both selected and click Next
15. Click Yes
16. Click Yes for Delegation
17. On the Location for Database, Log Files, and SYSVOL accept the default locations and click Next
18. Confirm your settings on the Summary Page and click Next
19. Select the Reboot On Completion check box and wait for the operation to complete
20. Logon to Server01
21. Examine the DNS after Reboot

Exercise 3: Create a Manual Zone Delegation

1. Logon to Server01 with the local administrator account
2. In the Server Manager, Expand DNS Server node and click Forward Lookup Zones node
3. Right-click Forward Lookup Zones and Select New Zone
4. Click Next
5. On the Zone Type page, select Primary Zone and make sure the Store The Zone In Active Directory check box is selected and click Next
6. On the Active Directory Zone Replication Scope page, To All DNS Servers In This Zone: newinovations.com and click Next
7. On the Zone Name page, type **ideadudes.biz** and click Next
8. On the Dynamic Update page, select Allow Only Secure Updates and click Next
9. Click Finish to create the Zone
10. Move to the ideadudes.biz zone and select it
11. Right-click the ideadudes.biz zone and select New Delegation
12. Click Next
13. On the Delegated Domain Name page, type Server02, and click Next
    a. Server02.ideadudes.biz
14. On the Name Server page, click Add and Type **server02.ideadudes.biz**
15. Move to the IP Addresses Of This NS Record section of the dialog box and type **10.10.0.50** and click OK
16. Click Next and then Finish to create the delegation

Exercise 4: Install AD DS and Create a New Domain Tree

1. Logon to Server02 with the local administrator account
2. In the Server Manager, Add Role
3. Click Next
4. Install Active Directory Domain Services and click Next
5. Review the information click Next
6. Confirm your choices and click Install
7. Examine the installation results and click Close
8. Click the Active Directory Domain Services node in Server Manager
9. Click Run The Active Directory Domain Services Installation Wizard
10. Review the information and click Next
11. Select an Existing Forest, select Create a New Domain in an Existing Forest, Select A New Domain Tree Root Instead Of A New Child Domain check box, and click Next
12. On the Network Credentials type **newinnovations.com** and click Set on enter alternate credentials type **newinnovations\administrator** enter **Pa$$w0rd** and confirm click OK and then Next
13. Type **ideadudes.biz** on the Name The New Domain Tree Root page, and click Next
14. Click Next
15. Click Next
16. Click Yes
17. Select No for the DNS Delegation
18. On Location for Database, Log Files and SYSVOL accept default and click Next
19. Type **Pa$$w0rd** for password and confirmation
20. Confirm your settings and click Next
21. Select the Reboot On Completion check box
22. Review the DNS Changes

Exercise 3: Create a Manual Zone Delegation

1. Logon to Server03 with the local administrator account
2. In the Server Manager, Add Role
3. Click Next
4. Install Active Directory Domain Services and click Next
5. Review the information click Next
6. Confirm your choices and click Install
7. Examine the installation results and click Close
8. Click the Active Directory Domain Services node in Server Manager
9. Click Run The Active Directory Domain Services Installation Wizard
10. Review the information and click Next
11. Select an Existing Forest, select Create a New Domain in an Existing Forest and Create A New Domain In An Existing Forest click Next
12. On the Network Credentials type **newinnovations.com** and click Set on enter alternate credentials type **newinnovations\administrator** enter **Pa$$w0rd** and confirm click OK and then Next
13. Name Domain type **newinnovations.com** as FQDN of the parent domain, type **intranet** in the single label of the child domain field and click Next
14. Click Next
15. Click Next
16. Click Yes
17. Click Next
18. Type **Pa$$w0rd** and confirm the password and click Next
19. Select the Reboot on Completion check box
20. Logon to the new created domain and open the DNS Server node in Server Manager
21. Review the changes within the DNS

Module 13– Finalizing a DNS Server Configuration in a Forest

Requirements

Three Windows 2008 Servers

Server01 (10.10.0.40,255.255.0.0 DNS-10.10.0.40)
Server02(10.10.0.50,255.255.0.0 DNS-10.10.0.50)
Server03(10.10.0.60,255.255.0.0 DNS-10.10.0.60)

Exercise 1: Single-Label Name Management

1. Logon to Server01 as an Administrator
2. In the Server Manager, select the Forward Lookup Zone in the DNS role
3. Right-click Forward Lookup Zone to select New Zone from the context menu
4. Review the information and click Next
5. Select Primary Zone and ensure that it is saved in Active Directory
6. Select To All DNS Servers In This Forest:newinnovations.com and click Next
7. On the Zone Name page, type **GlobalNames** and click Next
8. On the Dynamic Update page, select Do Not Allow Updates and click Next
9. Click Finish to create the zone
10. Open a command prompt with Administrative privileges
11. Type the following **dnscmd /config /enableglobalnamessupport 1** and press ENTER
12. Repeat steps 10-12 on Server02, Server03
13. Return to Server01 to add the single-label names

Exercise 2: Create Single-Label Names

1. Logon to Server01 as an Administrator in finalvision.com domain
2. In the DNS console select GlobalNames FLZ
3. Right-click GlobalNames to select New Alias (CNAME) from the context menu
4. Type **Server01**, FQDN field **Server01. newinnovations.com**
5. Do not select Allow Any Authenticated User To Update All Records With The Same Name
6. Click OK
7. Open a command prompt
8. Type the following
    a. **Dnscmd server01.finalvision.com /recordadd globalnames webserver cname server02.newinnovations.com**
    b. **Dnscmd server01.finalvision.com /recordadd globalnames OWA cname server02.newinnovations.com**
9. Close the command prompt and return to GlobalNames to view the new records.

Exercise 3: Modify a Global Query Block List

1. Logon to Server01 as an Administrator in finalvision.com domain
2. Open a command prompt with Administrative permissions
3. Type **dnscmd /config /globalqueryblocklist wpad isatap manufacturing**
4. Close the command prompt