

Supporting Group Policy

Lab 02: How Group Policy Works



V1.0 Released: February 17, 2014

# Exercise 1 User Environment Debug Logging

On one Windows XP client machine, enable user environment debug logging.

How to enable user environment debug logging in retail builds of Windows

http://support.microsoft.com/kb/221833

## Goal

By reading the uerenv.log, find line with following information

1. Get User SID
2. Get User OU name
3. Get the GUID of Default Domain Policy
4. Get the GPC and GPT version of Default Domain Policy
5. Get the line indicating that the Enforced flag is enabled.
6. Get the line indicating that the Block Inheritance is enabled.
7. Get the line indicating that User does not have sufficient permission to apply one GPO.

## Reference

Interpreting Userenv log files

<http://technet.microsoft.com/en-us/library/cc786775.aspx>

# Exercise 2 Group Policy Service Debug Logging

On one Windows 7 client machine, enable GPSVC debug logging.

Key: HKLM\Software\Microsoft\Windows NT\CurrentVersion\Diagnostics

Value Name GPSvcDebugLevel

Value Type: REG\_DWORD

Value data: 30002 (Hexadecimal)

Log File location: %Systemroot%\Debug\UserMode\gpsvc.log

## Goal

By reading the gpsvc.log, find line with following information

1. Get the GPC and GPT version of Default Domain Policy
2. Get the gpt.ini path of Default Domain Policy
3. Get the line indicating that the Enforced flag is enabled.
4. Get the line indicating that the Block Inheritance is enabled.
5. Get the line indicating that User does not have sufficient permission to apply one GPO.
6. Get the start time of Registry CSE processing.

# Exercise 3 Group Policy Template Reading

Create a new GPO, configure following computer settings:

* Windows Settings / Startup Scripts
* Windows Settings / Shutdown Scripts
* Windows Settings / Local Policies / Security Options / Interactive logon: Do not display last user name
* Windows Settings / Local Policies / Security Options / User Rights Assignment / Allow log on locally

Configure following user settings

* Administrative Templates\Desktop\Hide and Disable all items on the desktop

Find out the corresponding file within SYSVOL folder.

Note: Try to use the tool below to read registry.pol

http://gpoguy.com/free-tools/free-tools-library/registry-pol-viewer-utility/