Admin Server 2 - Active Directory Services AD DS back up and restore I Anthony Adams

AD DS Backup

There are three types of backup that you can perform to back up Active Directory Domain Services (AD DS) on a domain controller.

Full Backup - Backs up everything
Partial backup - Backup a particular directory
State Backup - Backup a system state/objects (users, groups, computers)

You can also use all three backup types to restore AD DS.

A full server backup contains all volumes on the domain controller.

To back up only the files that are required to recover AD DS, you can perform either a system state backup or a critical-volumes backup

Windows Server Backup

- The Windows Server Backup utility is not installed by default

- Once installed you can use the GUI based interface or the Wbadmin.exe command-line tool

- Can perform full server backup (all volumes), selected volumes and System State backups

- Can recover volumes, folders, files and the system state

- Can be used to for system recovery,
    -Will restore a complete system onto a new hard disk, by using a full server backup and the Windows Recovery Environment

- Can perform a Non-Authoritative AD DS restore
    -Recover AD DS from a specific system state backup

Authoritative Restore

- Authoritative restores are necessary when there is more than one domain controller. (Microsoft recommends to have 2 or more domain controllers so if one fails the other can take over, if there is only one and it fails you will not be able to sign in to recover it).

- Increases the Update Sequence Number (USN) of a recovered item or subtree
    - Ensures the deletion is not replicated back again by a peer domain controller

- Accomplished using NTDSutil.exe
    -Uses the DN or Distinguished Name of the Active Directory object or Subtree to be recovered

- The DN for the Hamilton Organizational unit in the Acme.com domain is:
    OU=Hamilton,DC=Acme,DC=Com

Windows Server Backup

- A system state backup will vary depending on

the server roles installed

- Will include at least the following data

    Registry

    COM+ Class Registration database

    Boot files

    Active Directory database (Ntds.dit)

    SYSVOL directory (Scripts and keys are stored here)

    Cluster service information

    System files that are under Windows Resource Protection

In the lab

Install the Windows Server Backup feature

Create a System State backup

Modify Active Directory
    Delete an OU Container

Recover Active Directory
    Non-authoritative recovery of the AD DS from a System State backup

Authoritative recovery of an OU

Admin Server 2 - Windows Registry Backup and Recovery

Windows Registry, what is it?

The windows registry is a file containing configuration settings related to such things like:

Operating System
Hardware Devices
Installed Programs
Specific and default user accounts
Local Machine

Every windows machine has its own registry DB file.

Registry Components

There are 2 main components to a registry entry. A key and a value.

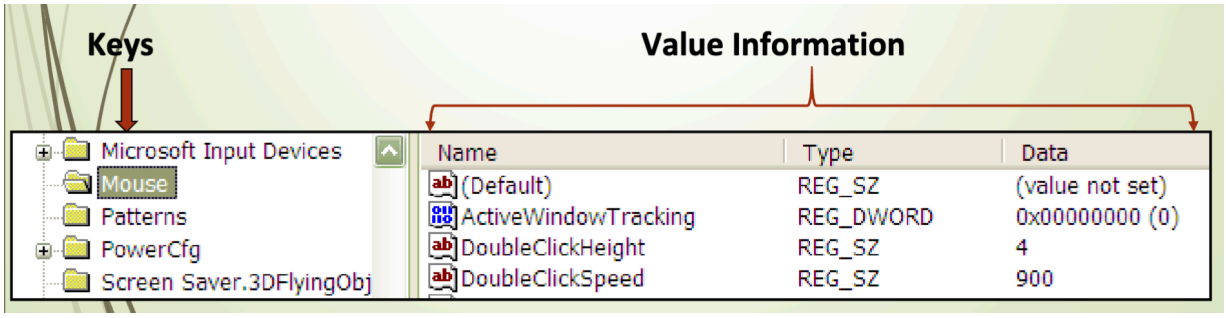
Keys - Similar to folders

Provides organizational structure

Refers to the registry item being configured

Values - Similar to files

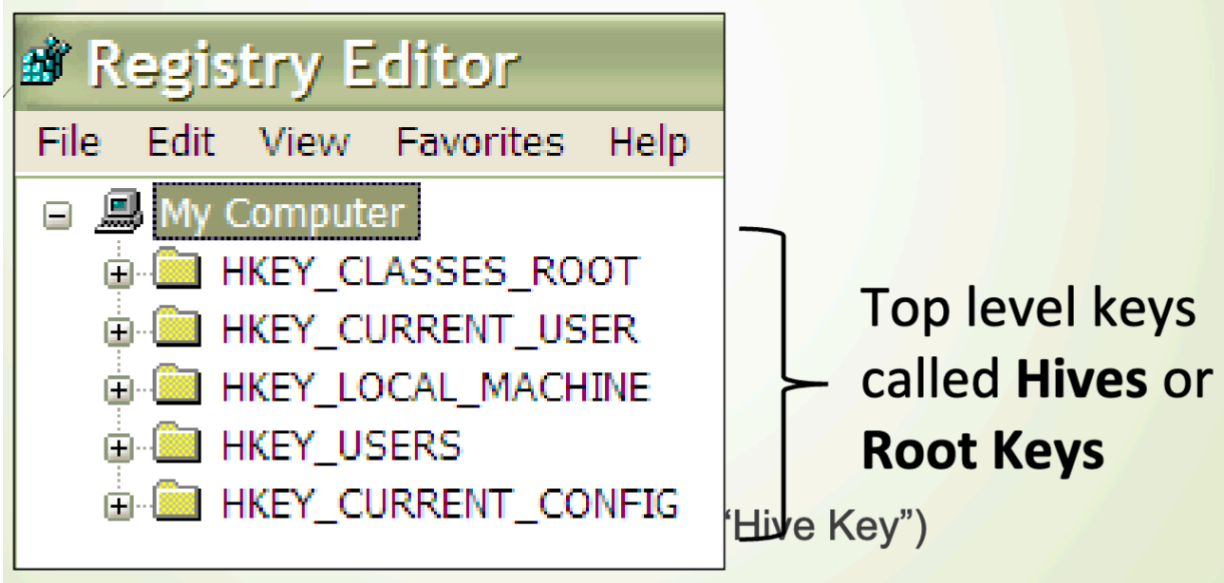
Contains the actual settings (like data in a file) for specified key



Organization Hierarchy

The top level of the hierarchy is called root keys or hives

Open regedit or regedit32 in windows start screen to open the registry.



HKCU - HKEY_CURRENT_USER
- Settings specific to currently logged in user
- Control panel settings, home directory
- Makes up the User Profile for a given user

HKU - HKEY_USERS
- Contains the information about each user

account stored on the computer and system wide user information

HKLM - HKEY_LOCAL_MACHINE
- Settings specific to the local computer
- Settings used by device drivers and applications for example (hardware installed and so on)

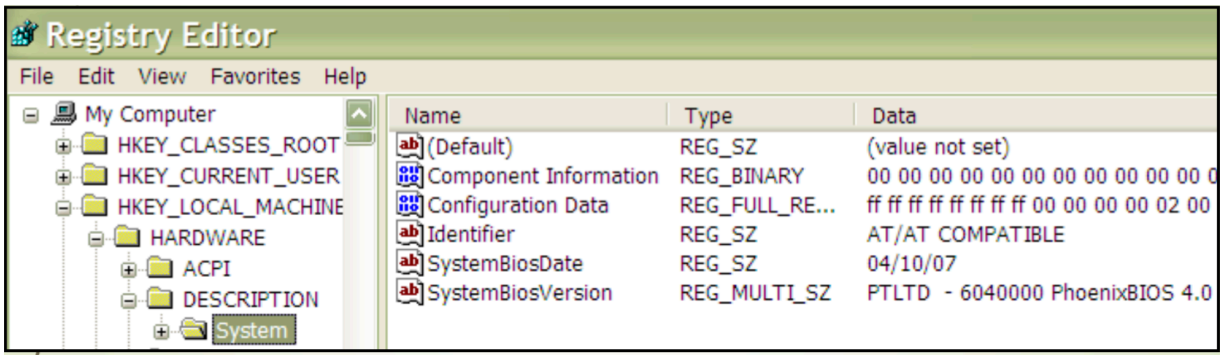
HKCR - HKEY_CLASSES_ROOT
- Information about registered applications
- File associations like .doc ~ Word, .ppt ~ Powerpoint and so on. (When you click a file what programs opens it)

HKCC - HKEY_CURRENT_CONFIG
- Information gathered at boot up identifying the computers current configuration
- Not stored permanently in the registry, recreated during each boot up
- Dynamic information unlike HKEY_LOCAL_MACHINE

Finding things - One method

Browsing through keys to the specific key is a

common method

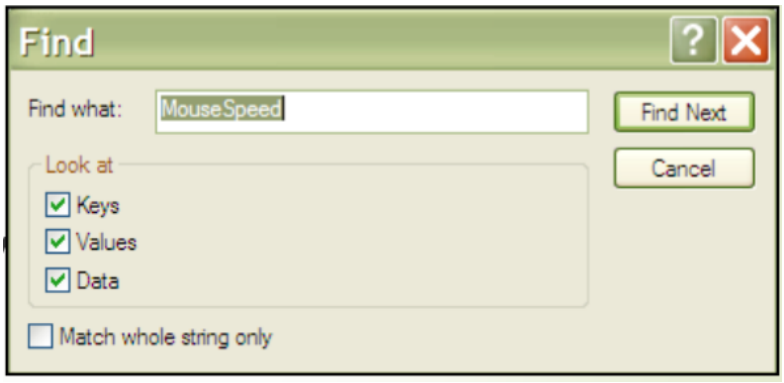


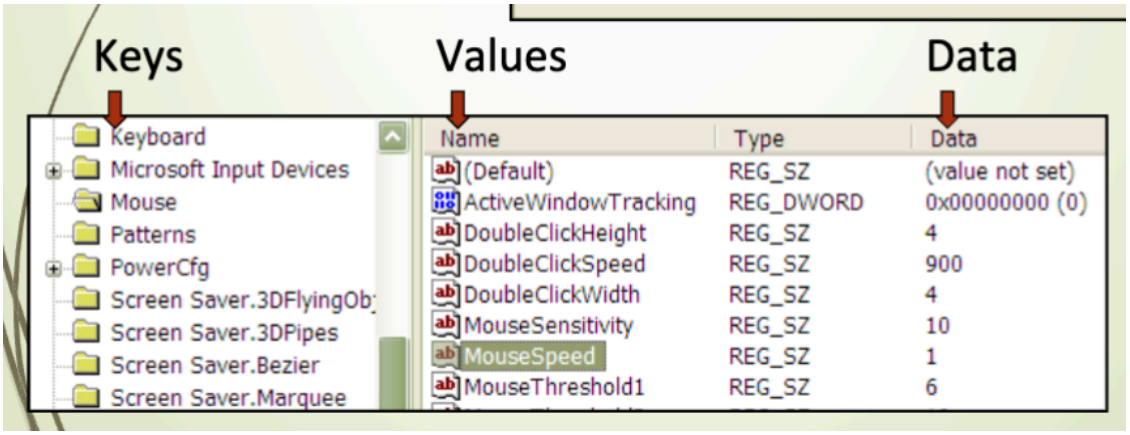
You can browse through the registry editor following the hierarchy to the system, search for a hive and then navigate within the hive, find a specific key and then its respective values

It is important to know generally what is stored in each hive in order to reduce search time

Finding things - a second method

Simply use the find function. Press CRTL + F to bring up the find tool and search for what you want





A warning to consider…

Regedit works on the registry LIVE.

Changing registry settings is technically very simple. However, incorrect changes can have unexpected consequences and can possible crash and break your system.

- There are thousands if settings to choose from
- Easy to choose the wrong value

- Even if you choose the correct value, entering the wrong data can have disastrous side effects.

How do you mitigate your risk? Registry backups.

Registry backup & Restore Options

There are 2 options built into regedit:

Export/Merge
Used when need to reset matching values and keys back to their original settings without deleting new keys and values

Export/Import
Used when you need to do a restore that is an exact match to the original registry

Registry Editor Backup: Export/Merge

Export
- Right click a registry key and choose Export
- User chooses a name for a .reg file containing everything inside that key (subkeys, values, data)

- .reg is a text file format so it can be edited (Make sure you know what you are doing here)

Merge
- Right click the .reg file and select Merge
- Automatically overwrites matching values in the correct location of the registry with the older value
- Does not touch values and keys in the current version if they are not in the merged .reg file

Registry Editor Backup: Export/Import

Export
- Right click a registry key and choose export with the registry hive file file type
- Creates a binary image file containing everything everything inside that key (subkeys, values, data)
- User specifies the extension (no default)

Import
- Right click the key location and select File/Import
- Critical to select the correct key location
- Automatically overwrites everything in the selected key with the exported files contents

Reg.exe command line tool

As regedit is a GUI, reg.exe is a CLI tool. It can also be used to create backup files.

- reg.exe
- often used in command and PowerShell scripts to create and restore registry backups

- To create and restore a .reg file:
`reg export RootKey\Subkey outputfile.reg` To make the back up
`reg import RootKey\Subkey outputfile.reg` To restore from the back up

To create and restore a registry hive file:
`reg save RootKey\Subkey outputfile.hiv`
`reg restore RootKey\Subkey outputfile.hiv`

PowerShell Registry PSProvider

- PowerShell providers are .NET programs, these programs look at areas within the windows environment through these providers

- PSProviders make special data storage areas available to PowerShell for viewing and management

- PSProvider examples include:
    - Registry
    - File System
    - Alias
    - Environment
    - Variable

CMDLET's

Get-PSProvider

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-psprovider?view=powershell-7.4

The `Get-PSProvider` cmdlet gets the PowerShell providers in the current session. You can get a particular drive or all drives in the session.

Get-PSDrive

https://learn.microsoft.com/en-us/powershell/module/microsoft.powershell.management/get-

psdrive?view=powershell-7.4

This cmdlet gets the following types of drives:

- Windows logical drives on the computer, including drives mapped to network shares.

- Drives exposed by PowerShell providers (such as the Certificate:, Function:, and Alias: drives) and the HKLM: and HKCU: drives that are exposed by the Windows PowerShell Registry provider.

- Session-specified temporary drives and persistent mapped network drives that you create by using the New-PSDrive cmdlet.

Registry Structure

The windows registry structure in terms of their file system equivalents:

Keys - Equivalent to folders/directories
Value Names - Equivalent to file names
Value Data - Equivalent to file content

Registry is a hierarchical structure like the file system

Registry Hive Key Access

PowerShell only makes the following 2 hive keys immediately accessible, by default:

HKEY_CURRENT_USER (HKCU)
HKEY_LOCAL_MACHINE (HKLM)

Other hive keys can be made accessible using the New-PSDrive cmdlet. For example:
New-PSDrive –name HKCC –PSProvider Registry -root Hkey_Current_Config

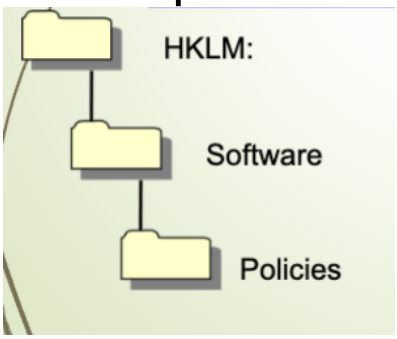
CMDLets for working with registry drives

Set-location (aliased to cd) You can navigate up and down the hierarchical structure of keys similar to folder structure using this
- Relative and absolute paths can be used

Set-Location Policies Only works if the current key contains the Policies key otherwise you would have to specify the absolute path

Set-Location HKLM:\Software\Policies

Would put us here:



CMDLets for working with the registry

Get-childitem (aliased to ls and dir)

Get-ChildItem HKLM:\Hardware
Lists names of the registry keys located in the specified location (under the name heading)
Lists the value names stored in each of these keys (under property heading)
Does NOT list sub-keys inside the listed keys

Get-ChildItem -path . –recurse
Lists all of the keys, sub-keys and their properties in the current path

Get-itemProperty
Lists the value names and their settings in the specified key
- The path must be included, however -path is optional
- List values in the current key

New-item
Creates a new registry key, eg:
New-item HKCU:\console –name TestKey

New-itemProperty
Creates a new registry value, eg:
New-ItemProperty –path HKCU:\Console\TestKey –name Test –Type String –Value “Test value”

Set-itemProperty
Changes the content of the specified registry value, eg:
Set-ItemProperty –path HKCU:\Console\TestKey –name Test –Value “New test value”

Registry / File System Equivalencies

A “:\” is used to designate the hive key root:

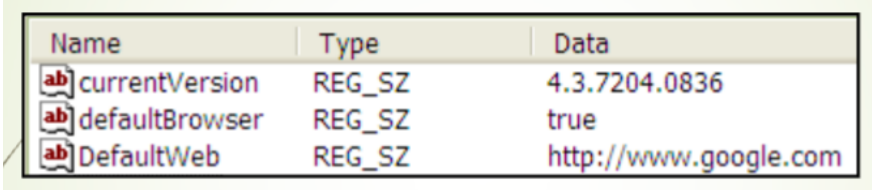
HKCU:\ is the equivalent to C:\

Multi-word keys must be places inside quotes:
Set-Location HKCU:\"Control Panel"
Is the equivalent to:
C:\"Program Files"

The . and the .. work the same way as in the file system
.\Test.ps1 refers to the Test.ps1 script located in the current directory
Set-Location .. changes the default location to the key above the current one

3 Most Common Data Types

String (Type designation: REG_SZ)
Text string but can also hold numbers



DWORD (Type designation: REG_DWORD)
32-bit or 64-bit integer in hexadecimal or decimal format

Name	Type	Data
ControllerMode	REG_DWORD	0x00000002 (2)

Binary (Type designation: REG_BINARY)
Raw binary data displayed in hexadecimal format

Name	Type	Data
PStats	REG_BINARY	f1 2a cd 48 01 00 00 00 6f 00 6f

In the Lab

Backup registry settings using regedit and reg.exe
Find and modify registry keys and values using PowerShell
Restore registry settings (Merge and Import)