Operating Systems Management

An introductory course on the basics of how operating systems work, and how to manage users on Windows and GNU / Linux systems from both GUI and CLI.

> Note: *PDF version may be out of date.*

Virtual machines

To avoid making unwanted changes and / or damaging our systems, virtual machines should be used to probe operating systems.

A virtual machine makes use of a tool called a *hypervisor*. The hypervisor is a layer virtualising an OS and software from hardware. It virtually splits the hardware and allocates resources on a 'need-to-know' basis to machine simulations called *guest machines*. Virtualised environments should strictly only be aware of virtual resources allocated to them.
Some antiviruses use virtualisation to sandbox files and analyse their behaviour, however malicious processes can overcome this by detecting the virtualisation layer and masking their behaviour, for example by delaying execution. Virtualisation can for example be detected using clipboard contents (are the empty?) or core count.

Virtual Box (VB)

Virtual Box is a tool to create and manage virtual machines. It can create machines located on one file to allow for portability. Its proprietary format *OVA* includes additional info on the machines, such as links to other machines and networks.

Note: *by default, VB uses USB version 1.1.*

Virtual drives

Virtual machines make use of *virtual drives*, which simulate physical drives. They are stored in a virtual drive format, *VDI* being VB native.

Virtual hard drives can be of two types: *fixed size* and *dynamically allocated*.
Fixed size disks are often used when equal (specific) space needs to be allocated for multiple users, as the full specified space is allocated upon creation. Dynamically allocated drives simulate the filesize specified at creation, however they occupy only the actual used space on disk, with the potential of growing to the specified size.

Configuration settings

Virtual machines themselves have many possible customisation options. The user can control the number of allocated cores (logical) with their maximal load, the amount of virtual memory, and video memory. If not enough video memory is allocated, screen flickering may occur.

Virtual networks

VB allows up to 4 virtual network adapters to be configured for various needs. The virtual networks can be of the following types:

- (virtual) NAT: outside networks cannot connect to the machines, however the machines can connect to outside networks
- NAT network mode: NAT + configuration of virtual switch / router (IP scope and mask), DHCP, allowing / disallowing IPv6
- bridged: VMs can be reached from external networks, host and VM are equal within the subnet
- host only: guest and host can only communicate within the subnet, no host network adapter to internet connection
- internal network mode: virtual router and virtual machines connected to it, no outside network access

These network and adapter settings can be changed while the machine is running, and require no restarts.

Note: *when cloning VMs, one should make sure the MAC address is changed unless preservation is needed for authentication or other specific needs. This option is labeled as "change MAC address policy*".

Powering off the machine

When powering off the machine, opting for *save state* will preserve the contents of the machine's operating memory. Relaunching the machine will resume it exactly where it was left. The saved state can be cleared without re-launching the machine UI.
Send shutdown signal will attempt to turn the machine off just as a normal shutdown from within the OS would work. *Turn off* is equivalent to a "hard shutdown", such as a power-loss, giving the guest OS no option to properly complete a power-off sequence.

Note: *when the machine state is saved, the machine configuration options are limited. The save state needs to be cleared to access configuration options again.*

Guest additions

Guest additions enable additional features for the guest machine, such as proper scaling, shared folder and clipboard with the host machine, security features, ...

Clones

A virtual machine can be *cloned*, i.e. an exact copy of it can be made. There are two types of clones:

- Full clone: one to one copy of the base machine.
- Linked clone: pointers to the clone *base*. Upon changes to the base, the changed initial data is carried over to the clone. Linked clones however need the base machine to function.

Full clones should be used if full autonomy is required, in other cases, linked clones are preferred. An example usage case is a base OS for a server.

Snapshots

Snapshots save the state of a machine, allowing for returning to a previous / initial state. However snapshots can grow and add up over time, and should thus be monitored, with obsolete snapshots removed.

Windows

NTFS can be opened in read only in UNIX and macOS systems. FAT(32) allows for full access to files by any OS.

Windows + F: feedback hub.

(Display file icons on thumbnail: no cache).

Logs

There are multiple types of logs, also known as memory dumps: system records its state for future analysis. They are by default stored in system root except for small memory dump (256kb minidump).

- small memory dump
- kernel dump
- full memory dump

https://blog.simplix.info/minidumper/

Windows specific files:

- pagefile: allows for reduction of workload of physical memory
- swapfile: unified windows programs location
- hyberfil: hibernation, dumps active memory to ram

Task scheduler

The task scheduler can make calls to event viewer (`eventvwr.msc`). `script.bat` to start notepad minified:

```
start /min notepad
```

Networking

Servers can be set not to respond to pings, however pinging is a good way to check internet connection.

DNS: translates domain names to IP addresses.
WINS: Windows Internet Name Service
Net Bios: System for devices to recognise themselves in the network

- TCP: Transmission Control Protocol
- UDP: User Datagram Protocol
- ICMP: Internet Control Message Protocol

Firewall

Filters that controls and filters in and outbound data traffic according to preset rules. Can be both hardware or software implemented.
They can be used to prevent unauthorised access to networks or network resources. All network data passes through the firewall, which then analyses the connection and makes a decision based on security policies and heuristics.

Filters can be IP based, application based, port based (incoming: all of them vs outcoming: not 80, 443). Peer to Peer networks might necessitate incoming port access (torrents), SSH, remote assistance (teamviewer). Remote desktop is an outgoing one. Other options include time, packet and protocol based.
Time based access is set in Parental Control.

Filtering rules

Skype (no longer P2P) and software might connect to people in the network without using an external server. Upon login, authentication happened on the server, however other information was spread out over the network. Connections were later still made directly, without going through the server. After Microsoft bought Skype, all was made client to server. Skype for business could be self-hosted.

Blocking rules have higher priority than allow rules.

Domain network based on the domain controller. Private networks: computer isn't visible.

Rules can be either inbound and outbound.

Remote and local addresses: specific IP addressess the are allowed to connect or be connected to.

Remote and local port: computer connection to other server.

Firewall can't have different rules for each type of network adapter.

ICMPv4 (file and printer sharing) echo request active: no response to ping requests. | Internet Control Message Protocol : supporting protocol used to send error messages and operational information.

Changing ports saves users from automated scans.

Allow connection if it is secure: if it uses IPSEC, and authentication is present, then the connection is "secure".

Windows Update

To decrease server load, peer to peer may be used. Some information can be exchanged by computers who have already downloaded the updates. Game update launches also work in the same way.

Setup

Shield icon: administrator privileges required. Content may be seen but not changed.

User Management (win10)

No granular permissions can be granted for each individual user without a domain network (domain controller), we can only target groups of users, and have limited disk quota management.

- User account allows the OS to identify the user
- OS: "single user" (DOS, nologin, cars) or "multi-user"
- Username formats: "testuser", "testuser@domain.com", "domain\testuser"
- Protected by credentials (password, key)
- Used to assign privileges in the system
- Assigned some resources (home folder, disk quota) in the system

By defalt, system and other users's folders aren't accessible, even to an administrator.

User groups

- consist of users
- users can belong to one or several groups, can be in a group created solely for the particular user
- the primary purpose of user groups is to simplify access control to computer systems
- users inherit permissions of groups

Primary use

- access control
- accounting
- default profiles
- relevancy of content

User management utility (win10)

User manager

`Wind+R [-> cmd] -> lusrmgr.msc` gives access to the local user and groups manager.

- defaultAccount: processes launched by the system attributed to that user
- Administrator and Guest accounts are disabled by default (+WDAG)
- DefaultAccount: account used by system processes

User creation dialog

- User must change password at next logon: disabled for shared accounts. Administrators can then remotely reset the password.

Local Security Policy

`Win+R [-> cmd] -> secpol.msc`.

Password policies

- Password history prevents password reuse (0-24)
- Days before user will be prompted to change password (0-999)
- Days user must use password before it can be changed (0-998)
- Minimum length

Default 10: standard computers, 7: domain controllers, 0: standalone server. Max length: 20 symbols.

Default complexity: no less than 6 chars, uppercase/lowercase, digits & nonalphabetic, not include username.

The decryption key is stored on the same machine.

Group Security Policy

Includes Local Security policy + additional settings.

`Win+R [-> cmd] -> gpedit.msc`.

Disk quotas and file permissions

- quotas are available only on NTFS volumes (journal file system, on the fly compression, permissions)
- Unless AD policies are applied quoteas are configured per volume, not folder or computer altogether
- Quotas cannot be set for groups
- If the amount of user's files already on the drive exceeds quota, it will be disabled for that user

Zip bomb: contents are highly compressed

User account control

4 levels that can be set after windows 7.

Must be a signed, verified publisher. Yellow: package not signed by the developer.
If a program requires administrator privileges, execution will be halted.

Secure desktop: only system owned system are allows to use CreateWindow() API call. It can be disabled from security policies.

System time shouldn't be changed due to certificate validities.

View event logs: shows errors and system / application logs. Scanning error logs gives information about vulnerabilities and potentially private data.
There is an Audit log containing information about system access and users.

UAC isn't a security boundary, simply a convenience feature.

Windows users addendum

Command to run commands as someone else:

```
runas /user:username[@domain]
```

Disk management

Partitions are logical divisions on a disk. They can be used to shield parts of the system (mounting and umounting), run multiple operating systems in parallel, and have different filesystems / shared drives.

Windows diskmanager displays partitions using logarithmic scale.

Default allocation unit size: size of an addressable block: 512kb. The smaller the unit, the larger the table.

NTFS

NTFS can host multiple mounted drives.

Increased security

- ACL-based security: permissions on files and/or folder based. Access type can be specified, and also set per user / group.
- BitLocker support: TPM enabled computers encrypts user data
- Suppport for large volumes: support for volumes up to 256TB. The maximum cluster number support is 2^32 -1

File name and paths

- Support for long file names, backward compatibility: storage of 8.3 alias on disk
- Supports filesizes up to 16TB
- Support for extended-length paths: >260char
- Clustered storage: NTFS volumes can be accessed by multiple cluster nodes simultaneously
- Distributed Link Tracking: shell shortcuts and links continue to work even after moving or renaming the target file
- Guarantees consistency of the volume and file system recoverability.

Flexible allocation

- Disk quotas
- File System Compression
- Increase size adding unallocated space
- Mounting of empty folders
- Sparse files: files marked as sparse will have NTFS allocate clusters only for the data specified by the application

Master Boot Record

Journal keeping track of changed on the disk. It indexes what is bootable. There is one MBR on a drive, which only allows for 4 partitions at most.
Extended partitions subdivide into more partitions however they cannot be bootable.

- Hard disk: Contains one or more partitions.
- Master Boot Record: Contains executable code that the system BIOS loads into memory. The code scans the MBR to find the partition table to determine which partition is the active, or bootable, partition.
- Boot sector: Bootable partition that stores information about the layout of the volume and the file system structures, as well as the boot code that loads Ntdlr.
- Ntldlr.dll: Switches the CPU to protected mode, starts the file system, and then reads the contents of the Boot.ini file. This information determines the startup options and initial boot menu selections.
- Ntfs.sys: System file driver for NTFS.
- Ntoskrnl.exe: Extracts information about which system device drivers to load and the load order.
- Kernel mode: The processing mode that allows code to have direct access to all hardware and memory in the system.
- User mode: The processing mode in which applications run.

Default NTFS cluster sizes

A cluster (or allocation unit) is the smallest amount of disk space that can be allocated to hold a file.

- 7 - 512 MB : 512b
- 1024: 1KB
- 2GB: 2KB
- 2TB: 4KB (above which no file compression)

Structure of an NTFS volume

- NTFS Boot sector: Contains bootcode, layout of volume and system file structure
- Master File Table: information required to retrieve files from the NTFS partition.
- File System Data: data not in MFT
- MFT copy: essential recovery

Boot sectors

On MBR disks, the boot sector contains executable code and the data required by the code, including information that the file system uses to access the volume. Ends with a 2byte signature word.

GUID partition table (GPT) disks are similar to MBR disks, except they use primary and backup partition structures to provide redundancy. These structures are located at the beginning and the end of the disk. GPT identifies these structures by their logical block address (LBA) rather than by their relative sectors.

To prevent the MFT from becoming fragmented, NTFS reserves 12.5 percent of volume by default for exclusive use of the MFT. This space, known as the MFT zone, is not used to store data unless the remainder of the volume becomes full.

File record attributes

Every allocated sector on an NTFS volume belongs to a file. Even the file system metadata is part of a file. NTFS views each file (or folder) as a set of file attributes.

Startup

Master Boot Code

1. Scans the partition table for the active partition.
2. Finds the starting sector of the active partition.
3. Loads a copy of the boot sector from the active partition into memory.
4. Transfers control to the executable code in the boot sector.

Boot sector

1. POST
2. BIOS finds boot device
3. BIOS loads first physical sector of boot device into memory, transfers CPU execution to the address

Global Unique IDentifier Partition Table (GUID, GPT)

Only compatible with UEFI, has larger disk size support, as well as more partitions.

RAID

Redundant Array of Independent (Inexpensive) Disks. There exist both hardware and software implementations. Raid controllers have their own calculation capabilities and one isn't OS reliant.

Raid 0 - striped volume

Information is split one to one: each hard drive contains an even part of the info, and the drives become dependant of each-other. It offers no redundancy but does offer speed gains.

Raid 1 - mirror volume

Also called mirroring, everything has a copy saved on every drive. The price of each byte multiplies, for no additional storage space cost. File system: REFS after breaking mirror.

Raid 4 & 5

Minimum 3 disks: redundancy disk, using XOR. Capacity = total - 1. The redundancy drive has a higher load, an shorter lifespan. R/W speed may also bottleneck. For Raid5, redundancy issue is spread across all drives. Hardware array may go into read-only mode, and upon hard-drive swap, info is restored.

Raid 6

It has two redundancy disks, and using different algorithms.

Nested raids

Usually Raid10 or Raid01, giving you both speed and redundancy.

Windows Update - categories

There are various different types as well as different rules on how to download and apply them:

- critical update: serious non-security related bug fixes
- security updated: fixes security vulnerabilities
    - critical: vulnerabilities whose exploitation can cause system infection without user action
    - important: vulnerabilities that can compromise integrity or confidentiality of data or the system itself
    - low
    - moderate
    - unspecified
- service pack & update rollup: cumulative set of hotfixes, security, critical and various updates

Service packs may contain new features and customer requested features.

- definition updates: additions to product definition databases
- feature pack: new product functionalities

LTSC

Long Term Stable Channel versions of Windows are destined for usage in areas needing a reliable backbone, such as servers. LTSC versions only get security and other critical upgrades, but no feature updates.