

Pendrive serwisowy 2.0 i narzędzia ratunkowe

Czas: 2 × 45 min

praca indywidualna, testy na laptopie w parach

Cel: Rozbudowanie pendrive'a Ventoy o zestaw narzędzi ratunkowych, sprawdzenie autentyczności pobranych obrazów sumą SHA-256 i przetestowanie każdego narzędzia na komputerze stacjonarnym i laptopie.

Po zajęciach potrafisz:

- pobiera obrazy narzędzi serwisowych wyłącznie z oficjalnych źródeł
- oblicza sumę SHA-256 pliku i porównuje ją z sumą podaną przez producenta
- uruchamia narzędzia z pendrive'a Ventoy w trybie UEFI i rozpoznaje problemy z Secure Boot
- dobiera narzędzie ratunkowe do typowej usterki komputera

Sprzęt i materiały

- komputer stacjonarny (stanowisko w pracowni)
- laptop szkolny (bez otwierania obudowy)
- własny pendrive ≥ 16 GB z Ventoy (z zadania 1, rok 1); przy braku miejsca — drugi pendrive lub obrazy z udziału szkolnego

Oprogramowanie

- **Ventoy (aktualizacja)** — opcja „Update” nie usuwa plików ISO z pendrive'a
ventoy.net/en/download.html
- **Hiren's BootCD PE** — środowisko Windows PE z narzędziami serwisowymi
hirensbootcd.org/download
- **MemTest86 Free (PassMark) lub Memtest86+** — test RAM; Memtest86+ (otwarty, obraz ISO):
<https://www.memtest.org/memtest86.com/download.htm>
- **GParted Live** — partycjonowanie poza systemem
gparted.org/download.php
- **Clonezilla Live (stable, amd64)** — obrazy i klonowanie dysków
clonezilla.org/downloads.php
- **SystemRescue** — ratunkowy Linux z narzędziami konsolowymi
system-rescue.org/Download
- **Ubuntu Desktop (aktualne wydanie LTS)** — tryb live; sumy kontrolne: plik SHA256SUMS na releases.ubuntu.com
ubuntu.com/download/desktop

Przygotowanie przed zajęciami

- Pobierz obrazy w domu albo skopiuj je z udziału szkolnego wskazanego przez nauczyciela (razem ok. 10–12 GB) — pobieranie w czasie lekcji nie zmieści się w 90 minutach.
- Przy każdym pobieranym pliku zapisz z oficjalnej strony sumę SHA-256 (albo pobierz plik z sumami).

- Zrób kopię ważnych plików z pendrive'a — aktualizacja Ventoy nie powinna ich usuwać, ale pomyłka przy wyborze opcji „Install” wymaże pendrive.

Bezpieczeństwo

- Pobieraj obrazy wyłącznie z oficjalnych stron producentów. Obraz z niezweryfikowaną lub niezgodną sumą SHA-256 usuń i nie uruchamiaj.
- W Ventoy2Disk wybieraj „Update”, nie „Install” — „Install” formatuje pendrive. Sprawdź, czy w polu „Device” jest Twój pendrive, a nie dysk komputera.
- W narzędziach ratunkowych tylko przeglądaj — nie uruchamiaj partycjonowania, klonowania ani wymazywania dysków. Te operacje wykonamy w kolejnych zadaniach na drugim dysku.
- Na laptopach nie zmieniaj ustawień BIOS/UEFI (Secure Boot, kolejność rozruchu). Korzystaj tylko z jednorazowego menu rozruchu; rejestrację klucza Ventoy (MOK) wykonaj wyłącznie za zgodą nauczyciela.

Przebieg zadania

1 Aktualizacja Ventoy i kopiowanie obrazów

1. Uruchom Ventoy2Disk, sprawdź wersję Ventoy na pendrivie („Ventoy In Device”) i w programie („Ventoy In Package”). Jeśli program jest nowszy, kliknij „Update”.
2. Sprawdź wolne miejsce na pendrivie. Skopiuj obrazy na partycję Ventoy (możesz utworzyć foldery, np. `ratunkowe`, `systemy`).

2 Weryfikacja sum SHA-256

Suma kontrolna potwierdza, że plik nie został uszkodzony ani podmieniony.

1. W wierszu poleceń oblicz sumę pierwszego obrazu: `certutil -hashfile plik.iso SHA256`.
2. W PowerShell oblicz sumę pozostałych obrazów: `Get-FileHash E:\ratunkowe\*.iso -Algorithm SHA256 | Format-List` (podaj własną literę pendrive'a).
3. Porównaj każdą sumę z wartością z oficjalnej strony (możesz użyć porównania w PowerShell: `(Get-FileHash plik.iso).Hash -eq 'SUMA_ZE_STRONY'`). Wpisz wynik do tabeli; jeśli producent nie podaje sumy, zanotuj to.
4. Celowo zmień jeden bajt w kopii małego pliku tekstowego i porównaj sumy oryginału i kopii — zapisz obserwację.

3 Testy na komputerze stacjonarnym

Uruchom każde narzędzie z menu Ventoy w trybie UEFI.

1. Wejdź do jednorazowego menu rozruchu (klawisz podaje nauczyciel lub instrukcja płyty) i wybierz pendrive w trybie UEFI.
2. Uruchom kolejno: Hiren's BootCD PE, MemTest86 lub Memtest86+, GParted Live, Clonezilla Live, SystemRescue, Ubuntu (live). Dla każdego zapisz czas uruchomienia i czy widzi oba dyski twarde oraz sieć.
3. W MemTest86 uruchom test tylko na ok. 1 minutę i przerwij; w Clonezilli dojdź do wyboru trybu i wyjdź bez wykonywania operacji.
4. Jeśli obraz .img MemTest86 nie uruchamia się z Ventoy, zapisz to i użyj obrazu ISO Memtest86+.

4 Testy na laptopie

Laptopa nie otwieramy i nie zmieniamy jego ustawień.

1. Uruchom laptop z pendrive'a przez jednorazowe menu rozruchu. Odczytaj w ustawieniach (bez zmian), czy Secure Boot jest włączony.
2. Przetestuj co najmniej Hiren's BootCD PE, Ubuntu live i SystemRescue. Zanotuj komunikaty o Secure Boot, jeśli się pojawiają.
3. Sprawdź w Hiren's BootCD PE lub Ubuntu, czy działa Wi-Fi, touchpad i czy widać dysk wewnętrzny.

5 Tabela zastosowań

1. Dla każdego narzędzia wpisz do tabeli dwie typowe usterki, przy których go użyjesz (np. „system się nie uruchamia, trzeba skopiować dane”).
2. Zrób zdjęcie menu Ventoy ze wszystkimi narzędziami.

W sprawozdaniu umieść

- ☐ wersja Ventoy oraz lista obrazów z wersjami i rozmiarami
- ☐ tabela sum SHA-256: obliczona, podana przez producenta, wynik porównania
- ☐ tabela testów uruchomienia na stacjonarce i laptopie
- ☐ tabela zastosowań narzędzi
- ☐ zdjęcie menu Ventoy i zrzut porównania sum
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Przed czym chroni sprawdzenie sumy SHA-256, a przed czym nie chroni, jeśli sumę pobierasz z tej samej strony co plik?
2. Dlaczego zmiana jednego bajtu w pliku zmienia całą sumę kontrolną?
3. Co to jest Secure Boot i dlaczego niektóre narzędzia z Ventoy nie uruchamiają się przy jego włączeniu?
4. Które narzędzie wybierzesz, gdy Windows się nie uruchamia, a trzeba szybko skopiować dokumenty użytkownika? Uzasadnij.

Kryteria oceny

Kryterium	Punkty
Pendrive z kompletem działających narzędzi (sprawdzenie na stanowisku)	5
Weryfikacja sum SHA-256 wszystkich obrazów	4
Tabela testów na stacjonarce i laptopie	4
Tabela zastosowań narzędzi	3
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

PowerShell — inwentaryzacja sprzętu skryptem

Czas: 2 × 45 min

praca indywidualna

Cel: Napisanie skryptu PowerShell, który zbiera dane o sprzęcie stanowiska i zapisuje je jako raport CSV i HTML, oraz porównanie raportów komputera stacjonarnego i laptopa.

Po zajęciach potrafisz:

- odczytuje dane sprzętu poleceniami Get-CimInstance, Get-ComputerInfo i Get-PhysicalDisk
- wybiera i przelicza właściwości obiektów (Select-Object, właściwości obliczane)
- eksportuje wyniki do CSV i HTML
- bezpiecznie uruchamia skrypt .ps1 z ustawieniem zasad wykonywania tylko dla bieżącej sesji
- porównuje konfiguracje dwóch komputerów na podstawie raportów

Sprzęt i materiały

- komputer stacjonarny z Windows 11
- laptop szkolny z Windows 11 (bez otwierania obudowy)
- pendrive (przeniesienie skryptu i raportów)

Oprogramowanie

- **Windows PowerShell 5.1 (wbudowany w Windows 11)** — uruchamiaj jako zwykły użytkownik; nie wymaga administratora
- **Visual Studio Code z rozszerzeniem PowerShell (opcjonalnie)** — wygodny edytor; wystarczy też Notatnik lub PowerShell ISE
code.visualstudio.com/download
- **HWiNFO (portable)** — kontrola poprawności danych ze skryptu
hwinfo.com/download

Przygotowanie przed zajęciami

- Przypomnij sobie z zadania 2 (rok 1), jakie dane zapisuje się w karcie inwentaryzacyjnej komputera.

Bezpieczeństwo

- Nie zmieniaj zasad wykonywania skryptów dla całego komputera (`-Scope LocalMachine`). Używaj wyłącznie `-Scope Process` — ustawienie znika po zamknięciu okna.
- Uruchamiaj tylko skrypty, które napisałeś sam lub których treść przeczytałeś i rozumiesz. Plików .ps1 z internetu nie odblokowuj bez sprawdzenia.
- Raport zawiera numery seryjne sprzętu szkoły — przechowuj go na pendrivie lub udziale szkolnym, nie publikuj w internecie.

Przebieg zadania

1 Polecenia w konsoli

Najpierw sprawdź polecenia ręcznie, potem przeniesiesz je do skryptu.

1. Uruchom PowerShell i wpisz `Get-ComputerInfo -Property CsName, OsName, OsVersion, CsManufacturer, CsModel`.
2. Odczytaj procesor: `Get-CimInstance Win32_Processor | Select-Object Name, NumberOfCores, NumberOfLogicalProcessors, MaxClockSpeed`.
3. Odczytaj pamięć: `Get-CimInstance Win32_PhysicalMemory | Select-Object BankLabel, Manufacturer, PartNumber, @{n='GB';e={$_.Capacity/1GB}}, ConfiguredClockSpeed`.
4. Odczytaj dyski i BIOS: `Get-CimInstance Win32_DiskDrive | Select-Object Model, SerialNumber, @{n='GB';e={[math]::Round($_.Size/1GB)}} , Get-PhysicalDisk | Select-Object FriendlyName, MediaType, BusType, HealthStatus` oraz `Get-CimInstance Win32_BIOS | Select-Object Manufacturer, SMBIOSBIOSVersion, ReleaseDate, SerialNumber`.
5. Sprawdź, jakie inne właściwości ma obiekt: `Get-CimInstance Win32_Processor | Get-Member -MemberType Property`. Wybierz jedną dodatkową, przydatną właściwość.

2 Skrypt raport.ps1

Zapisz skrypt na pendrivie jako `raport.ps1`.

1. Na początku skryptu ustaw folder i nazwę raportu: `$nazwa = $env:COMPUTERNAME` i `$folder = Join-Path $PSScriptRoot 'raporty'`, a następnie utwórz folder: `New-Item -ItemType Directory -Path $folder -Force | Out-Null`.
2. Zapisz wyniki poleceń z kroku 1 do zmiennych (`$cpu`, `$ram`, `$dyski`, `$bios`, `$os`).
3. Wyeksportuj listę modułów RAM i dysków do CSV: `$ram | Export-Csv "$folder\$nazwa-ram.csv" -NoTypeInformation -Delimiter ';' -Encoding UTF8` (analogicznie dla dysków).
4. Zbuduj raport HTML z fragmentów: `$html = @($os, $cpu, $ram, $dyski, $bios) | ForEach-Object { $_ | ConvertTo-Html -Fragment }, potem ConvertTo-Html -Title "Raport $nazwa" -PreContent "<h1>$nazwa</h1><p>$(Get-Date)</p>" -PostContent $html | Out-File "$folder\$nazwa.html" -Encoding UTF8.`
5. Dodaj nagłówki sekcji (`-PreContent '<h2>Procesor</h2>'` przy każdym fragmencie) i komentarze `#` opisujące każdą część skryptu.

3 Uruchomienie i kontrola

1. Sprawdź bieżące zasady: `Get-ExecutionPolicy -List`. Zapisz wynik.
2. Ustaw zasady tylko dla tej sesji: `Set-ExecutionPolicy -Scope Process -ExecutionPolicy RemoteSigned` i uruchom skrypt: `.\raport.ps1`. Jeśli plik pochodzi z innego komputera i jest blokowany, sprawdź jego treść i użyj `Unblock-File .\raport.ps1`.
3. Otwórz raport HTML w przeglądarce, a CSV w arkuszu. Porównaj trzy wartości (procesor, RAM, model dysku) z HWiNFO.

4 Laptop i porównanie

1. Uruchom ten sam skrypt na laptopie (z pendrive'a, w ten sam sposób).
2. Porównaj raporty w tabeli: procesor, pamięć (liczba modułów, pojemność, taktowanie), typ i magistrala dysku (`MediaType`, `BusType`), wersja BIOS.
3. Zapisz, których danych skrypt nie odczytał (puste pola) i dlaczego mogło tak się stać.

W sprawozdaniu umieść

- ☐ pełny kod skryptu `raport.ps1` z komentarzami
- ☐ zrzuty raportu HTML ze stacjonarki i laptopa

- ☐ tabela porównawcza obu komputerów
- ☐ porównanie z HWiNFO i opis pustych lub błędnych pól
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różni się `Format-Table` od `Select-Object` i dlaczego przed `Export-Csv` nie używa się `Format-Table`?
2. Co oznacza ustawienie `RemoteSigned` i dlaczego zmieniamy je tylko z `-Scope Process`?
3. Dlaczego pojemność pamięci dzielimy przez `1GB` i co by się stało bez tego przeliczenia?
4. Do czego w serwisie lub w firmie przydaje się automatyczny raport stanowiska zamiast ręcznej karty?

Kryteria oceny

Kryterium	Punkty
Działający skrypt tworzący CSV i HTML	7
Czytelny kod z komentarzami i sekcjami raportu	3
Raport z laptopa i tabela porównawcza	4
Kontrola danych z HWiNFO i analiza braków	3
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

PowerShell — automatyzacja diagnostyki

Czas: 2 × 45 min

praca indywidualna

Cel: Napisanie skryptu, który codziennie sprawdza stan komputera (miejsce na dyskach, stan dysków, błędy w dziennikach, czas pracy, usługi) i zapisuje wynik do logu z datą, uruchamianego automatycznie przez Harmonogram zadań.

Po zajęciach potrafisz:

- sprawdza w skrypcie wolne miejsce, stan SMART i błędy systemowe
- stosuje instrukcję warunkową do generowania ostrzeżeń
- zapisuje wyniki do pliku logu z datą i godziną
- tworzy i testuje zadanie w Harmonogramie zadań, a po zajęciach je usuwa

Sprzęt i materiały

- komputer stacjonarny z Windows 11 na drugim dysku (z zadania 13, rok 1) — tam masz konto administratora; alternatywnie maszyna wirtualna Windows 11 (z zadania 26, rok 1)
- pendrive ze skryptem z zadania 2

Oprogramowanie

- **Windows PowerShell 5.1 (wbudowany)** — część poleceń (stan SMART) wymaga uruchomienia jako administrator
- **Harmonogram zadań (taskschd.msc, wbudowany)**
- **Visual Studio Code (opcjonalnie)** — lub PowerShell ISE / Notatnik
code.visualstudio.com/download

Przygotowanie przed zajęciami

- Przy uruchamianiu komputera wybierz Windows z drugiego dysku. Sprawdź, czy możesz uruchomić PowerShell jako administrator.

Bezpieczeństwo

- Skrypt ma tylko odczytywać dane — nie umieszczaj w nim poleceń usuwających pliki ani zatrzymujących usług.
- Zadanie w Harmonogramie twórz wyłącznie w systemie z drugiego dysku lub w maszynie wirtualnej. Przed końcem zajęć usuń je (krok 5), chyba że nauczyciel poleci inaczej.
- Zasady wykonywania skryptów ustawiaj tylko dla procesu (`-ExecutionPolicy Bypass` w argumentach zadania), nie dla całego komputera.

Przebieg zadania

1 Polecenia diagnostyczne

Uruchom PowerShell jako administrator i przetestuj polecenia.

1. Wolne miejsce: `Get-CimInstance Win32_LogicalDisk -Filter 'DriveType=3' | Select-Object DeviceID, @{n='WolneGB';e={[math]::Round($_.FreeSpace/1GB,1)}}, @{n='Procent';e={[math]::Round($_.FreeSpace/$_.Size*100,1)}}`.
2. Stan dysków: `Get-PhysicalDisk | Select-Object FriendlyName, HealthStatus, OperationalStatus` oraz liczniki: `Get-PhysicalDisk | Get-StorageReliabilityCounter | Select-Object DeviceId, Temperature, Wear, ReadErrorsTotal, PowerOnHours`.
3. Błędy z ostatnich 24 godzin: `Get-WinEvent -FilterHashtable @{LogName='System'; Level=1,2; StartTime=(Get-Date).AddDays(-1)} -MaxEvents 10 -ErrorAction SilentlyContinue`.
4. Czas pracy: `(Get-Date) - (Get-CimInstance Win32_OperatingSystem).LastBootUpTime` oraz stan usług: `Get-Service -Name WinDefend, wuauserv, Spooler, EventLog | Select-Object Name, Status, StartType`.

2 Skrypt diagnostyka.ps1

Zapisz skrypt w `C:\Diag\diagnostyka.ps1`.

1. Utwórz ścieżkę logu z datą: `$log = "C:\Diag\logi\diag_$(Get-Date -Format 'yyyy-MM-dd_HH-mm').log"` i folder `C:\Diag\logi`.
2. Napisz funkcję zapisu: `function Zapisz($tekst) { "$(Get-Date -Format 'HH:mm:ss') $tekst" | Out-File $log -Append -Encoding UTF8 }`.
3. Dla każdego dysku logicznego dodaj warunek: jeśli procent wolnego miejsca jest mniejszy niż 15, zapisz `OSTRZEŻENIE: mało miejsca na C:`, w przeciwnym razie `OK`.
4. Zapisz stan dysków fizycznych; jeśli `HealthStatus` jest inny niż `Healthy`, zapisz ostrzeżenie. Dopisz temperaturę i liczbę błędów odczytu (gdy są dostępne).
5. Zapisz liczbę błędów z dziennika System z ostatnich 24 godzin i treść trzech najnowszych (`TimeCreated`, `ProviderName`, `Id`). Dopisz czas pracy komputera w dniach i godzinach oraz usługi, które nie są uruchomione.
6. Na końcu dopisz podsumowanie: liczbę ostrzeżeń (licznik zwiększany w każdym warunku).

3 Test skryptu

1. Uruchom: `powershell.exe -NoProfile -ExecutionPolicy Bypass -File C:\Diag\diagnostyka.ps1` i otwórz log.
2. Przetestuj ostrzeżenie: tymczasowo zmień próg z 15% na 99% i sprawdź, czy w logu pojawiają się ostrzeżenia. Przywróć próg 15%.

4 Harmonogram zadań

1. Otwórz `taskschd.msc` → Biblioteka Harmonogramu zadań → Utwórz zadanie. Nazwa: `Diagnostyka_<nazwisko>`, zaznacz „Uruchom z najwyższymi uprawnieniami”.
2. Wyzwalacz: codziennie o wybranej godzinie oraz drugi — „Przy logowaniu”. Akcja: program `powershell.exe`, argumenty: `-NoProfile -ExecutionPolicy Bypass -File C:\Diag\diagnostyka.ps1`.
3. Uruchom zadanie ręcznie (prawy przycisk → Uruchom). Sprawdź kolumnę „Wynik ostatniego uruchomienia” (0x0 = sukces) i czy powstał nowy log.
4. Wyloguj się i zaloguj ponownie — sprawdź, czy powstał kolejny log.

5 Porządki

1. Skopiuj skrypt i logi na pendrive.
2. Usuń zadanie z Harmonogramu (lub poleceniem `Unregister-ScheduledTask -TaskName Diagnostyka_<nazwisko>`) i pokaż nauczycielowi, że go nie ma.

W sprawozdaniu umieść

- ☐ pełny kod skryptu `diagnostyka.ps1` z komentarzami
- ☐ przykładowy log z prawidłowym działaniem i log z testem ostrzeżeń
- ☐ zrzut właściwości zadania w Harmonogramie (wyzwalacze i akcja) oraz wyniku ostatniego uruchomienia
- ☐ interpretacja wyników: stan dysków, znalezione błędy systemowe
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego `Get-StorageReliabilityCounter` wymaga uprawnień administratora i dlaczego część jego pól bywa pusta?
2. Po co w nazwie pliku logu umieszcza się datę i godzinę w formacie rok-miesiąc-dzień?
3. Co oznacza wynik 0x0 w Harmonogramie zadań i jak sprawdzisz przyczynę, gdy wynik jest inny?
4. Jakie inne sprawdzenia warto dodać do takiego skryptu w szkolnej pracowni?

Kryteria oceny

Kryterium	Punkty
Skrypt sprawdza wszystkie wymagane elementy	6
Warunki i ostrzeżenia działają (test progu)	3
Log z datą, czytelny format	3
Zadanie w Harmonogramie uruchomione i usunięte po zajęciach	4
Interpretacja wyników i odpowiedzi na pytania	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Linux — diagnostyka sprzętu z terminala

Czas: 2 × 45 min

praca indywidualna

Cel: Poznanie poleceń systemu Linux do odczytu informacji o sprzęcie, stanie dysków, temperaturach i błędach oraz porównanie wyników z programem HWiNFO.

Po zajęciach potrafisz:

- odczytuje parametry procesora, pamięci, dysków i urządzeń PCI/USB poleceniami terminala
- sprawdza stan SMART dysku programem smartctl
- odczytuje temperatury czujników (lm-sensors)
- wyszukuje błędy w dziennikach jądra i systemu (dmesg, journalctl)
- zapisuje wyniki poleceń do plików raportu

Sprzęt i materiały

- komputer stacjonarny z Ubuntu z podwójnego rozruchu (z zadania 15, rok 1) albo Ubuntu live z pendrive'a
- laptop szkolny — wyłącznie Ubuntu live z pendrive'a
- pendrive z Ventoy

Oprogramowanie

- **Ubuntu (aktualne wydanie LTS)** — zainstalowane lub w trybie live („Wypróbuj Ubuntu”)
ubuntu.com/download/desktop
- **smartmontools, lm-sensors (pakiety Ubuntu)** — instalacja: `sudo apt install smartmontools lm-sensors`
smartmontools.org
- **HWiNFO (wyniki z Windows)** — porównanie; możesz użyć raportu z zadania 2
hwinfo.com/download

Przygotowanie przed zajęciami

- Przynieś raport HWiNFO lub raport skryptu z zadania 2 dla swojego stanowiska.

Bezpieczeństwo

- Używaj tylko poleceń odczytu. Nie uruchamiaj `fdisk`, `mkfs`, `dd` ani testów SMART na żadnym dysku — dziś niczego nie zmieniamy.
- Polecenie `sudo` daje pełne uprawnienia. Przed naciśnięciem Enter sprawdź, czy przepisałeś polecenie dokładnie.
- W trybie live nie montuj i nie otwieraj partycji Windows — szczególnie na laptopie i na szkolnym dysku systemowym.

Przebieg zadania

1 Przygotowanie terminala

1. Uruchom Ubuntu, otwórz terminal (Ctrl+Alt+T). Utwórz folder raportu: `mkdir ~/raport && cd ~/raport`.
2. Zainstaluj narzędzia: `sudo apt update && sudo apt install smartmontools lm-sensors`. W trybie live instalacja trwa do wyłączenia komputera.
3. Każdy wynik zapisuj do pliku poleceniem `tee`, np. `lscpu | tee lscpu.txt`.

2 Procesor, pamięć, płyta główna

1. Procesor: `lscpu` — odczytaj model, liczbę rdzeni i wątków, rozmiary pamięci podręcznej i obsługiwane rozszerzenia wirtualizacji (VT-x lub AMD-V).
2. Pamięć: `free -h` oraz moduły: `sudo dmidecode -t memory | tee ram.txt` — znajdź liczbę gniazd, rozmiar, typ, prędkość i producenta modułów.
3. Płyta i BIOS: `sudo dmidecode -t baseboard` i `sudo dmidecode -t bios`. Zestawienie całości: `sudo lshw -short | tee lshw.txt`.

3 Urządzenia i dyski

1. Urządzenia PCI i USB: `lspci` i `lsusb`. Znajdź kartę graficzną, kontroler sieci i kontroler SATA/NVMe. Sterownik karty sieciowej: `lspci -k`.
2. Dyski: `lsblk -o NAME,SIZE,TYPE,FSTYPE,MOUNTPOINTS,MODEL` oraz zajętość: `df -h`. Ustal, który dysk jest pierwszy, a który drugi.
3. SMART każdego dysku: `sudo smartctl -i /dev/sda`, potem `sudo smartctl -H -A /dev/sda | tee smart_sda.txt` (dla NVMe: `/dev/nvme0`). Odczytaj stan ogólny, Power_On_Hours, Reallocated_Sector_Ct, Current_Pending_Sector i temperaturę.

4 Czujniki i dzienniki

1. Wykryj czujniki: `sudo sensors-detect --auto`, potem odczytaj temperatury: `sensors | tee sensors.txt`.
2. Komunikaty jądra: `sudo dmesg --level=err,warn | tee dmesg.txt`. Wyjaśnij co najmniej dwa komunikaty (wyszukaj ich znaczenie).
3. Błędy z bieżącego uruchomienia: `journalctl -p err -b | tee journal.txt`.

5 Laptop i porównanie

1. Uruchom laptop z Ubuntu live (jednorazowe menu rozruchu, bez zmian w BIOS). Wykonaj `lscpu`, `sudo dmidecode -t memory`, `lsblk`, `sudo smartctl -H -A` dla dysku wewnętrznego i `sensors`.
2. Skopiuj folder `~/raport` na pendrive (np. `cp -r ~/raport /media/$USER/Ventoy/`).
3. Porównaj w tabeli wyniki Linuksa z HWiNFO (procesor, RAM, dysk, godziny pracy dysku, temperatura).

W sprawozdaniu umieść

- ☐ tabela poleceń: polecenie → jakie informacje daje
- ☐ najważniejsze wyniki stacjonarki i laptopa (fragmenty plików z folderu `raport`)
- ☐ interpretacja SMART obu dysków stacjonarki
- ☐ wyjaśnienie dwóch komunikatów z `dmesg` lub `journalctl`
- ☐ tabela porównania z HWiNFO
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego `dmidecode` i `smartctl` wymagają `sudo`, a `lscpu` nie?
2. Czym różni się `lsblk` od `df -h`?
3. Które atrybuty SMART świadczą o zbliżającej się awarii dysku twardego?
4. Dlaczego dyski w Linuksie mają nazwy `sda`, `sdb`, `nvme0n1` i czy kolejność nazw jest zawsze taka sama po każdym uruchomieniu?

Kryteria oceny

Kryterium	Punkty
Komplet plików wyników ze stacjonarki	5
Wyniki z laptopa	3
Interpretacja SMART i komunikatów dzienników	4
Porównanie z HWiNFO	4
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Linux — dyski, partycje i montowanie

Czas: 2 × 45 min

praca indywidualna

Cel: Utworzenie i sformatowanie partycji na drugim dysku z poziomu Linuksa, skonfigurowanie trwałego montowania przez UUID w `/etc/fstab` oraz nadanie uprawnień i sprawdzenie systemu plików.

Po zajęciach potrafisz:

- tworzy partycje programem `fdisk` lub `parted` w wolnej przestrzeni dysku
- formatuje partycje w systemach `ext4` i `exFAT`
- montuje partycje ręcznie i trwale przez UUID w `/etc/fstab` z opcją `nofail`
- ustawia właściciela i uprawnienia katalogów (`chown`, `chmod`)
- sprawdza system plików poleceniem `fsck` na odmontowanej partycji

Sprzęt i materiały

- komputer stacjonarny z Ubuntu zainstalowanym w podwójnym rozruchu na drugim dysku (zadanie 15, rok 1)
- na drugim dysku co najmniej 10 GB nieprzydzielonego miejsca (albo partycja testowa z zadania 12, rok 1, którą wolno usunąć)
- alternatywa: maszyna wirtualna z Ubuntu i dodatkowym dyskiem wirtualnym 10 GB

Oprogramowanie

- **Ubuntu (aktualne wydanie LTS)** — `fdisk`, `parted`, `mkfs.ext4` są wbudowane
ubuntu.com/download/desktop
- **exfatprogs (pakiet Ubuntu)** —
`mkfs.exfat`; jeśli brak: `sudo apt install exfatprogs`
github.com/exfatprogs/exfatprogs
- **VirtualBox 7 (tylko wariant w VM)**
virtualbox.org/wiki/Downloads

Przygotowanie przed zajęciami

- Jeśli na drugim dysku nie ma wolnego miejsca: w Windows z drugiego dysku otwórz Zarządzanie dyskami i zmniejsz partycję danych (Zmniejsz wolumin) o ok. 10 GB. Systemowej partycji Windows nie ruszaj.
- Zapisz model i rozmiar obu dysków (np. z zadania 4), żeby bez wahania rozpoznać drugi dysk.

Bezpieczeństwo

- **Najpierw rozpoznaj dysk.** Polecenie `lsblk -o NAME,SIZE,MODEL,FSTYPE,MOUNTPOINTS` pokaż nauczycielowi i zapisz, który dysk jest drugi. Pomyłka litery (`sda` / `sdb`) zniszczy szkolny system.
- Twórz partycje wyłącznie w wolnej przestrzeni. Nie usuwaj i nie zmieniaj istniejących partycji Windows, EFI ani Ubuntu. W `fdisk` przed poleceniem `w` wyświetl tabelę (`p`) i sprawdź ją; w razie wątpliwości wyjdź bez zapisu (`q`).
- Przed restartem sprawdź `/etc/fstab` poleceniem `sudo findmnt --verify` i `sudo mount -a`. Błędny wpis bez `nofail` może zatrzymać uruchamianie systemu.
- Polecenie `fsck` uruchamiaj tylko na odmontowanej partycji.

Przebieg zadania

1 Rozpoznanie i partycjonowanie

W przykładach drugi dysk to `/dev/sdX` — wpisz właściwą nazwę.

- Wykonaj `lsblk -o NAME,SIZE,MODEL,FSTYPE,MOUNTPOINTS` i `sudo fdisk -l /dev/sdX`. Zrób zrzut tabeli partycji przed zmianami.
- Uruchom `sudo fdisk /dev/sdX`. Polecenie `F` pokaże wolną przestrzeń. Utwórz partycję `n` o rozmiarze `+5G` (domyślny numer, domyślny początek w wolnym miejscu).
- Utwórz drugą partycję `n` na resztę wolnego miejsca (do 5 GB). Wyświetl tabelę `p`, sprawdź, że stare partycje są nienaruszone, i zapisz `w`.
- Sprawdź wynik tym samym narzędziem z innej strony: `sudo parted /dev/sdX print free`.

2 Systemy plików i montowanie ręczne

Nowe partycje oznaczamy dalej jako `/dev/sdXA` (ext4) i `/dev/sdXB` (exFAT).

- Sformatuj: `sudo mkfs.ext4 -L DANE /dev/sdXA` oraz `sudo mkfs.exfat -L WYMIANA /dev/sdXB`.
- Utwórz punkty montowania: `sudo mkdir -p /mnt/dane /mnt/wymiana` i zamontuj: `sudo mount /dev/sdXA /mnt/dane`, `sudo mount /dev/sdXB /mnt/wymiana`.
- Sprawdź `df -hT` i `findmnt /mnt/dane`. Utwórz plik testowy na każdej partycji.

3 Trwałe montowanie przez UUID

- Odczytaj identyfikatory: `sudo blkid /dev/sdXA /dev/sdXB`.
- Zrób kopię: `sudo cp /etc/fstab /etc/fstab.bak`, a potem edytuj `sudo nano /etc/fstab` i dopisz dwa wiersze: `UUID=<uuid-ext4> /mnt/dane ext4 defaults,nofail 0 2` oraz `UUID=<uuid-exfat> /mnt/wymiana exfat defaults,nofail,uid=1000,gid=1000,umask=022 0 0`.
- Odmontuj obie partycje (`sudo umount /mnt/dane /mnt/wymiana`), sprawdź plik: `sudo findmnt --verify`, a potem zamontuj według fstab: `sudo mount -a`. Gdy nie ma błędów — uruchom komputer ponownie (Ubuntu z drugiego dysku) i sprawdź `df -hT`.

4 Uprawnienia

- Na partycji ext4 utwórz katalog `sudo mkdir /mnt/dane/projekt`, zmień właściciela: `sudo chown $USER:$USER /mnt/dane/projekt` i ustaw uprawnienia `chmod 750 /mnt/dane/projekt`. Sprawdź `ls -ld`.
- Utwórz testowego użytkownika `sudo adduser test2` i sprawdź: `sudo -u test2 ls /mnt/dane/projekt`. Zapisz wynik i wyjaśnij go.
- Spróbuj wykonać `chmod 700` na pliku w `/mnt/wymiana`. Zapisz, co się stało, i wyjaśnij różnicę między ext4 a exFAT.

5 Sprawdzenie systemu plików i porządki

- Odmontuj partycję ext4 i sprawdź ją: `sudo umount /mnt/dane`, `sudo fsck.ext4 -f /dev/sdXA`. Zapisz wynik i zamontuj ponownie (`sudo mount -a`).
- Usuń testowego użytkownika: `sudo deluser --remove-home test2`. Partycje i wpisy w fstab zostaw albo usuń — zgodnie z poleceniem nauczyciela.

W sprawozdaniu umieść

- ☐ tabela partycji drugiego dysku przed i po zmianach
- ☐ użyte polecenia i dopisane wiersze `/etc/fstab`
- ☐ wynik `df -hT` po ponownym uruchomieniu
- ☐ test uprawnień i wyjaśnienie różnicy ext4/exFAT
- ☐ wynik `fsck`

☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego w /etc/fstab używa się UUID zamiast nazwy `/dev/sdb1`?
2. Co robi opcja `nofail` i co by się stało bez niej, gdyby dysk został odłączony?
3. Co oznaczają uprawnienia 750 i kto ma jaki dostęp do katalogu?
4. Dlaczego nie wolno uruchamiać fsck na zamontowanym systemie plików?
5. Kiedy wybierzesz exFAT, a kiedy ext4?

Kryteria oceny

Kryterium	Punkty
Bezpieczne partycjonowanie bez naruszenia istniejących partycji	5
Formatowanie i poprawne wpisy fstab (montowanie po restarcie)	5
Uprawnienia i ich test	3
Sprawdzenie fsck i dokumentacja poleceń	3
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Klonowanie i obraz dysku — Clonezilla

Czas: 2 × 45 min

praca w parach (jedna osoba wykonuje, druga kontroluje wybór dysków; zamiana ról przy przywracaniu)

Cel: Wykonanie obrazu partycji systemowej Windows 11 programem Clonezilla, przywrócenie go po celowej zmianie danych i porównanie obrazu z klonowaniem dysk-dysk.

Po zajęciach potrafisz:

- rozpoznaje dyski i partycje w Clonezilli po rozmiarze, modelu i numerze seryjnym
- wykonuje obraz partycji do repozytorium na innej partycji
- weryfikuje obraz i przywraca go na partycję źródłową
- porównuje klon dysk-dysk z obrazem dysku pod względem zastosowań, czasu i miejsca

Sprzęt i materiały

- komputer stacjonarny z Windows 11 na drugim dysku
- na drugim dysku lub na pendrive partycja na obraz z wolnym miejscem co najmniej równym zajętości partycji Windows (zwykle 20–30 GB); może to być partycja danych z zadania 12 (rok 1) lub partycja ext4 z zadania 5
- pendrive z Ventoy i Clonezilla Live

Oprogramowanie

- **Clonezilla Live (stable, amd64)** — z pendrive'a Ventoy (zadanie 1)
clonezilla.org/downloads.php
- **Windows 11 na drugim dysku** — z zadania 13 (rok 1)

Przygotowanie przed zajęciami

- W Windows z drugiego dysku sprawdź (`manage-bde -status`), czy partycja C: nie jest zaszyfrowana BitLockerem (np. po zadaniu 31, rok 1). Jeśli jest — wyłącz szyfrowanie przed zajęciami (trwa długo).
- Zapisz model, rozmiar i numer seryjny obu dysków (z zadania 2 lub 4) oraz zajętość partycji Windows na drugim dysku.

Bezpieczeństwo

- **Pomylenie dysków przy przywracaniu zniszczy szkolny system.** Na każdym ekranie wyboru dysku lub partycji para głośno porównuje rozmiar, model i numer seryjny z notatką. Przed potwierdzeniem pokaż ekran nauczycielowi.
- Używaj tylko trybów `saveparts` (zapis obrazu partycji) i `restoreparts` (przywracanie partycji). Nie używaj `savedisk / restoredisk` ani trybu klonowania `device-device`.
- Clonezilla dwukrotnie pyta o potwierdzenie nadpisania („Are you sure...?”). Czytaj komunikaty do końca — odpowiedź `y` jest nieodwracalna.
- Repozytorium obrazów nie może leżeć na partycji, którą zapisujesz lub przywracasz.

Przebieg zadania

1 Plik testowy w Windows

1. Uruchom Windows z drugiego dysku. Na pulpicie utwórz `test_obraz.txt` z imieniem, datą i godziną. Oblicz jego sumę: `Get-FileHash test_obraz.txt` i zapisz.
2. Odczytaj w Zarządzaniu dyskami zajętość partycji C: i układ partycji drugiego dysku. Wyłącz Windows (pełne zamknięcie: `shutdown /s /t 0`).

2 Obraz partycji (saveparts)

Uruchom Clonezillę z pendrive'a w trybie UEFI, język: English, klawiatura: bez zmian.

1. Wybierz `device-image`, następnie `local_dev`. Gdy pojawi się lista dysków, porównaj ją z notatką (rozmiar, model, numer seryjny) i przejdź dalej Ctrl+C.
2. Jako repozytorium wybierz partycję na obraz (inną niż partycja Windows). Utwórz w niej katalog na obrazy zgodnie z pytaniem programu.
3. Wybierz tryb `Beginner`, potem `saveparts`. Nazwij obraz `win11-<nazwisko>-<data>` i zaznacz (spacją) tylko partycję Windows (NTFS) z drugiego dysku.
4. Wybierz sprawdzenie zapisanego obrazu (`Yes, check the saved image`) i brak szyfrowania obrazu. Zapisz czas rozpoczęcia i zakończenia oraz prędkość pokazywaną przez Partclone.
5. Po zakończeniu wybierz `cmd` i sprawdź rozmiar obrazu: `du -sh /home/partimag/win11-*`.

3 Celowa zmiana danych

1. Uruchom Windows z drugiego dysku i usuń `test_obraz.txt` (opróżnij też Kosz). Utwórz nowy plik `po_obrazie.txt`.
2. Wyłącz komputer.

4 Przywrócenie obrazu (restoreparts)

Zamieńcie się rolami w parze.

1. Uruchom Clonezillę, wybierz `device-image` → `local_dev` → to samo repozytorium → `Beginner` → `restoreparts`.
2. Wybierz obraz i partycję docelową. Sprawdź z partnerem, że to partycja Windows na drugim dysku (rozmiar i nazwa urządzenia zgodne z notatką). Pokaż ekran nauczycielowi i potwierdź.
3. Zapisz czas przywracania. Po zakończeniu uruchom Windows z drugiego dysku.

5 Weryfikacja i porównanie

1. Sprawdź, że `test_obraz.txt` wrócił, a `po_obrazie.txt` zniknął. Porównaj sumę SHA-256 pliku z zapisaną wcześniej.
2. Uzupełnij tabelę porównania: klon dysk-dysk (`device-device`) i obraz (`device-image`) — kiedy który stosować, czego wymaga, ile miejsca zajmuje.

W sprawozdaniu umieść

- ☐ układ partycji drugiego dysku i dane identyfikujące oba dyski
- ☐ parametry obrazu: zajętość partycji, rozmiar obrazu, współczynnik kompresji, czasy zapisu, sprawdzenia i przywracania
- ☐ zdjęcia kluczowych ekranów Clonezilli (wybór partycji źródłowej i docelowej)
- ☐ wynik weryfikacji pliku testowego (sumy SHA-256)
- ☐ tabela porównania klonu i obrazu
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego obraz zajmuje mniej miejsca niż rozmiar partycji, a nawet mniej niż jej zajętość?
2. Dlaczego Windows trzeba wyłączyć całkowicie (a nie hibernować lub używać szybkiego uruchamiania) przed wykonaniem obrazu?
3. W jakiej sytuacji lepszy jest klon dysk-dysk, a w jakiej obraz do pliku?
4. Dlaczego obraz kopii zapasowej należy przechowywać na innym nośniku niż dysk źródłowy?

Kryteria oceny

Kryterium	Punkty
Bezpieczna praca: poprawne rozpoznanie dysków, kontrola w parze	5
Obraz wykonany i sprawdzony	4
Przywrócenie i weryfikacja pliku testowego	4
Pomiary czasu i rozmiaru, tabela porównania	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Odzyskiwanie systemu po awarii — obraz do maszyny wirtualnej

Czas: 2 × 45 min

praca w parach

Cel: Przeniesienie działającego systemu Windows 11 z komputera fizycznego do maszyny wirtualnej przez obraz partycji wykonany w Hiren's BootCD PE — jako sposób odzyskania środowiska pracy po awarii sprzętu.

Po zajęciach potrafisz:

- analizuje układ partycji dysku z systemem w trybie UEFI/GPT
- wykonuje obraz partycji wymaganych do rozruchu Windows w środowisku Windows PE
- tworzy i podłącza dysk wirtualny VHD jako nośnik obrazu
- przywraca obraz na pusty dysk maszyny wirtualnej i uruchamia system
- rozpoznaje i usuwa typowe problemy po przeniesieniu systemu (EFI/BIOS, sterowniki, aktywacja)

Sprzęt i materiały

- komputer stacjonarny z Windows 11 na drugim dysku (zadanie 13, rok 1) i VirtualBox 7 w systemie szkolnym
- partycja danych na drugim dysku z wolnym miejscem co najmniej 40 GB (na plik VHD z obrazem); alternatywnie dysk zewnętrzny od nauczyciela
- pendrive z Ventoy i Hiren's BootCD PE (zadanie 1); obraz ISO Hiren's BootCD PE także na dysku komputera (dla VM)

Oprogramowanie

- **Hiren's BootCD PE** — zawiera Macrium Reflect PE i AOMEI Backupper
hirensbootcd.org/download
- **Oracle VirtualBox 7** — obsługuje dyski VHD
virtualbox.org/wiki/Downloads
- **Zarządzanie dyskami (diskmgmt.msc, wbudowane)** — tworzenie i odłączanie VHD

Przygotowanie przed zajęciami

- W Windows z drugiego dysku sprawdź `manage-bde -status`. Jeśli dysk C: jest zaszyfrowany, wyłącz szyfrowanie przed zajęciami — obrazu zaszyfrowanej partycji nie uruchomisz w VM bez klucza odzyskiwania.
- Sprawdź, czy na partycji danych drugiego dysku jest co najmniej 40 GB wolnego miejsca.

Bezpieczeństwo

- Obraz wykonuj tylko z partycji Windows na **drugim dysku**. Przywracanie odbywa się wyłącznie na dysk maszyny wirtualnej — w Hiren's BootCD PE uruchomionym na komputerze fizycznym nie używaj funkcji przywracania.
- W VM przywracaj na pusty dysk wirtualny (rozmiar ustawiony w kroku 3). Rozpoznaj go po rozmiarze; dysk VHD z obrazem ma inny rozmiar i nie może być celem.
- Plik VHD odłącz w Windows przed podłączeniem do VirtualBox — ten sam dysk używany jednocześnie przez dwa systemy może zostać uszkodzony.
- Obraz zawiera całe Twoje środowisko (konta, przeglądarkę). Po zajęciach usuń VHD z obrazem lub przechowuj go w miejscu wskazanym przez nauczyciela.

Przebieg zadania

1 Nośnik obrazu — dysk VHD

Wykonaj w systemie szkolnym (pierwszy dysk).

1. Otwórz Zarządzanie dyskami → Akcja → Utwórz wirtualny dysk twardy. Lokalizacja: partycja danych drugiego dysku, plik `obrazy-<nazwisko>.vhd`, rozmiar 40 GB, format VHD, typ: dynamicznie rozszerzany.
2. Zainicjuj nowy dysk (GPT), utwórz prosty wolumin NTFS z etykietą `OBRAZY`.
3. Odłącz dysk VHD (prawy przycisk na „Dysk N” → Odłącz wirtualny dysk twardy). Wyłącz komputer.

2 Diagnostyka i obraz w Hiren's BootCD PE

Uruchom komputer z pendrive'a, wybierz Hiren's BootCD PE.

1. Otwórz Zarządzanie dyskami (w HBCD: menu Start → Windows Administrative Tools lub skrót na pulpicie). Zrób zrzut układu partycji drugiego dysku: partycja EFI (FAT32, ok. 100–300 MB), MSR, C: (NTFS), partycja odzyskiwania. Zapisz zajętość C:.
2. Podłącz VHD: Akcja → Dołącz wirtualny dysk twardy → `obrazy-<nazwisko>.vhd`. Sprawdź, że pojawił się wolumin `OBRAZY`.
3. Uruchom Macrium Reflect (lub AOMEI Backupper, gdy Macrium nie działa). Przy drugim dysku kliknij „Image this disk...” i zaznacz tylko partycje EFI, MSR, C: i partycję odzyskiwania. Oznacz partycję danych, na której leży plik VHD.
4. Jako miejsce zapisu wskaż wolumin `OBRAZY`. Uruchom tworzenie obrazu, zapisz czas trwania i rozmiar pliku. Po zakończeniu odłącz VHD i wyłącz komputer.

3 Maszyna wirtualna

W systemie szkolnym uruchom VirtualBox.

1. Utwórz maszynę `Odtworzony-W11`: typ Windows 11 (64-bit), bez instalacji nienadzorowanej, 4 GB RAM, 2 procesory. W ustawieniach System → Płyta główna włącz **EFI**.
2. Utwórz pusty dysk VDI o rozmiarze nie mniejszym niż rozmiar partycji C: na drugim dysku plus 1 GB (Macrium pozwala zmniejszyć partycję, jeśli zajętość jest mała — wtedy wystarczy np. 60 GB).
3. W Ustawienia → Pamięć podłącz: napęd optyczny z ISO Hiren's BootCD PE oraz istniejący dysk `obrazy-<nazwisko>.vhd` jako drugi dysk twardy.

4 Przywrócenie w VM

1. Uruchom VM z ISO HBCD. W Macrium Reflect wybierz zakładkę „Restore” → wskaż plik obrazu z woluminu `OBRAZY`.
2. Jako dysk docelowy wybierz pusty dysk wirtualny (rozpoznaj po rozmiarze). Przeciągnij lub skopiuj wszystkie partycje z obrazu; partycję C: dopasuj do miejsca na dysku. Uruchom przywracanie.
3. Wyłącz VM, odłącz ISO i dysk VHD z obrazem. Uruchom VM.

5 Weryfikacja i problemy

1. Zrób zrzut ekranu logowania lub pulpitu. Sprawdź w Menedżerze urządzeń, które urządzenia mają wykrzyknik, i porównaj z komputerem fizycznym.
2. Sprawdź Ustawienia → System → Aktywacja i zapisz stan aktywacji. Zapisz, co zrobiłbyś, gdyby VM nie uruchomiła się (np. brak EFI, „No bootable medium”, błąd 0xc000000e — naprawa `bcdboot C:\Windows` z HBCD).
3. Dla chętnych: zainstaluj w VM dodatki gościa VirtualBox i porównaj działanie przed i po.

W sprawozdaniu umieść

- ☐ zrzut układu partycji drugiego dysku z opisem funkcji każdej partycji

- ☐ parametry obrazu: wybrane partycje, rozmiar, czas tworzenia i przywracania
- ☐ konfiguracja VM (EFI, dyski) — zrzut ustawień
- ☐ zrzut uruchomionego systemu w VM, lista urządzeń bez sterowników, stan aktywacji
- ☐ opis napotkanych problemów i sposobu ich rozwiązania
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego obraz samej partycji C: nie wystarczy, żeby system uruchomił się na nowym dysku w trybie UEFI?
2. Co się stanie, jeśli w VM nie włączysz EFI, a obraz pochodzi z dysku GPT?
3. Dlaczego Windows po przeniesieniu do VM uruchamia się, mimo że „sprzęt” jest zupełnie inny, i dlaczego może stracić aktywację?
4. W jakiej sytuacji serwisowej takie przeniesienie systemu do maszyny wirtualnej jest przydatne dla klienta?

Kryteria oceny

Kryterium	Punkty
Analiza układu partycji i poprawny wybór partycji do obrazu	4
Utworzenie obrazu na dysku VHD	4
Konfiguracja VM i przywrócenie obrazu	4
Uruchomienie i weryfikacja systemu albo udokumentowana diagnoza problemu	4
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Miejsca do magazynowania Windows (RAID programowy) w VM

Czas: 2 × 45 min

praca indywidualna

Cel: Utworzenie puli magazynu z trzech dysków wirtualnych, skonfigurowanie miejsc z dublowaniem i parzystością, zasymulowanie awarii dysku oraz jego wymiana — i porównanie tego rozwiązania z klasycznymi poziomami RAID.

Po zajęciach potrafisz:

- dodaje dyski wirtualne do maszyny w VirtualBox
- tworzy pulę magazynu oraz miejsca do magazynowania z dublowaniem dwukierunkowym i parzystością
- symuluje awarię dysku i odczytuje stan puli w panelu i w PowerShell
- wymienia uszkodzony dysk i naprawia miejsce do magazynowania
- porównuje poziomy RAID 0, 1, 5 i 10 pod względem pojemności, wydajności i odporności

Sprzęt i materiały

- komputer stacjonarny z VirtualBox 7
- maszyna wirtualna Windows 11 z zadania 26 (rok 1) albo nowa; ok. 50 GB wolnego miejsca na dyski wirtualne (dynamiczne)

Oprogramowanie

- **Oracle VirtualBox 7**
[virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)
- **Windows 11 w VM (Panel sterowania → Miejsca do magazynowania, PowerShell)**
— obraz ISO, gdy trzeba utworzyć nową VM
[microsoft.com/software-download/windows11](https://www.microsoft.com/software-download/windows11)

Przygotowanie przed zajęciami

- Sprawdź, czy maszyna wirtualna z zadania 26 (rok 1) uruchamia się, i wykonaj jej migawkę „przed_RAID”.
- Przypomnij sobie definicje RAID 0, 1, 5 i 10 (podręcznik INF.02).

Bezpieczeństwo

- Wszystkie operacje wykonuj wyłącznie w maszynie wirtualnej. W Windows komputera fizycznego nie otwieraj Miejsca do magazynowania — utworzenie puli kasuje dyski, które się do niej doda.
- Przy dodawaniu dysków do puli zaznacz tylko trzy nowe, puste dyski wirtualne. Dysku systemowego VM nie da się dodać, ale sprawdź listę przed kliknięciem.
- Dyski wirtualne odłączaj tylko przy wyłączonej maszynie (chyba że port ma zaznaczone „Podłączanie na gorąco”).

Przebieg zadania

1 Dyski wirtualne

1. Przy wyłączonej VM otwórz Ustawienia → Pamięć. Do kontrolera SATA dodaj trzy nowe dyski VDI, dynamicznie przydzielane, po 10 GB: `R1.vdi`, `R2.vdi`, `R3.vdi`.
2. Uruchom VM i sprawdź w Zarządzaniu dyskami, że widać trzy nowe, niezainicjowane dyski. Nie inicjuj ich.

2 Pula i miejsca do magazynowania

1. Otwórz Panel sterowania → System i zabezpieczenia → Miejsca do magazynowania → Utwórz nową pulę i miejsce do magazynowania. Zaznacz trzy nowe dyski i utwórz pulę.
2. Utwórz pierwsze miejsce: nazwa `Lustro`, litera M; typ odporności „Dublowanie dwukierunkowe”, rozmiar 4 GB.
3. Utwórz drugie miejsce (Utwórz miejsce do magazynowania): nazwa `Parzystosc`, litera P; typ „Parzystość”, rozmiar 4 GB.
4. Sprawdź w PowerShell (jako administrator): `Get-StoragePool -IsPrimordial $false`, `Get-VirtualDisk | Select-Object FriendlyName, ResiliencySettingName, Size, FootprintOnPool, HealthStatus` oraz `Get-PhysicalDisk`. Zapisz, ile miejsca w puli zajmuje każde miejsce (FootprintOnPool).
5. Skopiuj na M: i P: po kilka plików (np. folder `C:\Windows\Web`) i oblicz sumy kontrolne: `Get-ChildItem M:\Web -Recurse -File | Get-FileHash | Export-Csv C:\sumy_M.csv` (analogicznie dla P:).

3 Symulacja awarii

1. Wyłącz VM. W Ustawienia → Pamięć odłącz dysk `R2.vdi` (Usuń podłączenie — nie usuwaj pliku). Uruchom VM.
2. Sprawdź stan w panelu Miejsca do magazynowania i w PowerShell (`Get-VirtualDisk`, `Get-PhysicalDisk`, `Get-StoragePool -IsPrimordial $false | Select-Object FriendlyName, HealthStatus, OperationalStatus`). Zrób zrzuty.
3. Sprawdź, czy pliki na M: i P: są dostępne. Porównaj sumy z zapisanymi: `Compare-Object (Import-Csv C:\sumy_M.csv).Hash (Get-ChildItem M:\Web -Recurse -File | Get-FileHash).Hash` — brak wyniku oznacza zgodność.

4 Wymiana dysku i naprawa

1. Wyłącz VM, dodaj nowy dysk 10 GB `R4.vdi`, uruchom VM.
2. W panelu Miejsca do magazynowania dodaj dysk do puli („Dodaj dyski”). Brakujący dysk usuń z puli („Usuń” przy dysku z ostrzeżeniem) albo w PowerShell: `Get-PhysicalDisk | Where-Object OperationalStatus -ne 'OK' → Remove-PhysicalDisk` z nazwą puli.
3. Napraw miejsca: `Get-VirtualDisk | Repair-VirtualDisk`, obserwuj postęp `Get-StorageJob`. Sprawdź końcowy stan (`HealthStatus` = `Healthy`) i ponownie sumy kontrolne.

5 Teoria RAID

1. Uzupełnij tabelę porównania RAID 0, 1, 5, 10 dla czterech dysków po 1 TB.
2. Porównaj Miejsca do magazynowania z kontrolerem RAID sprzętowym: gdzie wykonywane są obliczenia, co dzieje się po awarii komputera, przenośność dysków.

W sprawozdaniu umieść

- ☐ konfiguracja dysków VM i puli (zrzuty)
- ☐ tabela miejsc do magazynowania: typ, rozmiar, zajętość w puli
- ☐ stan puli przed awarią, po awarii i po naprawie (zrzuty z PowerShell)

- ☐ wynik porównania sum kontrolnych po awarii i po naprawie
- ☐ tabela porównania poziomów RAID i porównanie z RAID sprzętowym
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego miejsce z dublowaniem dwukierunkowym o rozmiarze 4 GB zajmuje w puli około 8 GB, a miejsce z parzystością mniej?
2. Ile dysków może ulec awarii w dublowaniu dwukierunkowym i w parzystości przy trzech dyskach?
3. Dlaczego RAID (także programowy) nie zastępuje kopii zapasowej?
4. Które rozwiązanie wybierzesz dla domowego serwera z trzema dyskami, a które dla bazy danych wymagającej szybkich zapisów? Uzasadnij.

Kryteria oceny

Kryterium	Punkty
Pula i dwa miejsca do magazynowania poprawnie utworzone	5
Symulacja awarii i udokumentowany stan puli	4
Wymiana dysku, naprawa i weryfikacja sum	4
Tabela RAID i porównanie z RAID sprzętowym	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

RAID w Linuksie — mdadm

Czas: 2 × 45 min

praca indywidualna

Cel: Zbudowanie programowej macierzy RAID1 w Linuksie narzędziem mdadm, utrwalenie jej konfiguracji oraz przećwiczenie awarii dysku i odbudowy macierzy.

Po zajęciach potrafisz:

- przygotowuje dyski z partycjami typu Linux RAID
- tworzy macierz RAID1 poleceniem mdadm i zakłada na niej system plików
- utrwała konfigurację macierzy (mdadm.conf, initramfs, fstab) i sprawdza ją po restarcie
- symuluje awarię, usuwa i dodaje dysk oraz odczytuje postęp odbudowy w /proc/mdstat
- wyjaśnia rolę dysku zapasowego (spare)

Sprzęt i materiały

- komputer stacjonarny z VirtualBox 7
- maszyna wirtualna z Ubuntu (Server lub Desktop, aktualne LTS) — gotowa VM od nauczyciela (plik .ova z udziału) albo zainstalowana przed zajęciami

Oprogramowanie

- **Oracle VirtualBox 7**
[virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)
- **Ubuntu Server (aktualne wydanie LTS)** — lub Ubuntu Desktop; pakiet `mdadm` (`sudo apt install mdadm`)
ubuntu.com/download/server

Przygotowanie przed zajęciami

- Przygotuj maszynę wirtualną z Ubuntu: zaimportuj plik .ova od nauczyciela (Plik → Importuj urządzenie wirtualne) albo zainstaluj Ubuntu w VM w domu lub na początku zajęć. Sprawdź, czy możesz się zalogować i używać `sudo`.
- Wykonaj migawkę VM „przed_RAID”.

Bezpieczeństwo

- Całe zadanie wykonuj w maszynie wirtualnej. Polecenia `fdisk`, `mdadm --create` i `mkfs` uruchomione na komputerze fizycznym zniszczyłyby dane.
- W VM dysk systemowy to zwykle `/dev/sda`. Przed każdym `fdisk` i `mdadm --create` sprawdź `lsblk` — używaj tylko nowych, pustych dysków 5 GB.
- Przed restartem sprawdź wpis w fstab poleceniem `sudo findmnt --verify` i `sudo mount -a`. Wpis zawsze z opcją `nofail`.

Przebieg zadania

1 Dyski i partycje

1. Przy wyłączonej VM dodaj w Ustawienia → Pamięć trzy dyski VDI po 5 GB (`md1.vdi`, `md2.vdi`, `md3.vdi`). Uruchom VM.
2. Rozpoznaj dyski: `lsblk -o NAME,SIZE,TYPE,MOUNTPOINTS` i `sudo fdisk -l`. Zapisz nazwy nowych dysków (np. `sdb`, `sdc`, `sdd`).
3. Na każdym nowym dysku utwórz partycję typu Linux RAID: `sudo fdisk /dev/sdb` → `g` (nowa tabela GPT) → `n` (cała przestrzeń) → `t` → typ `raid` (lub numer „Linux RAID” z listy `L`) → `p` → `w`. Powtórz dla `sdc` i `sdd`.
4. Zainstaluj `mdadm`, jeśli go nie ma: `sudo apt install mdadm`.

2 Macierz RAID1

1. Utwórz macierz: `sudo mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdb1 /dev/sdc1`. Potwierdź pytanie o metadane (`y`).
2. Obserwuj synchronizację: `cat /proc/mdstat` (lub `watch -n1 cat /proc/mdstat`, wyjście Ctrl+C). Szczegóły: `sudo mdadm --detail /dev/md0`.
3. Utwórz system plików i zamontuj: `sudo mkfs.ext4 -L RAID1 /dev/md0`, `sudo mkdir -p /mnt/raid1`, `sudo mount /dev/md0 /mnt/raid1`.
4. Utwórz plik testowy: `sudo dd if=/dev/urandom of=/mnt/raid1/test.bin bs=1M count=200` i zapisz jego sumę: `sha256sum /mnt/raid1/test.bin`.

3 Utrwalenie konfiguracji

1. Dopisz macierz do konfiguracji: `sudo mdadm --detail --scan | sudo tee -a /etc/mdadm/mdadm.conf`, potem `sudo update-initramfs -u`.
2. Odczytaj UUID systemu plików: `sudo blkid /dev/md0` i dopisz do `/etc/fstab`: `UUID=<uuid> /mnt/raid1 ext4 defaults,nofail 0 2`. Sprawdź: `sudo findmnt --verify`.
3. Uruchom ponownie VM (`sudo reboot`). Sprawdź, że macierz nazywa się `md0` (a nie `md127`) i jest zamontowana: `cat /proc/mdstat`, `df -h /mnt/raid1`.

4 Awaria i odbudowa

1. Oznacz dysk jako uszkodzony: `sudo mdadm /dev/md0 --fail /dev/sdc1`. Sprawdź `/proc/mdstat` (oznaczenie `[U_]` i `(F)`) oraz `sudo mdadm --detail /dev/md0`.
2. Sprawdź, że dane są dostępne: `sha256sum /mnt/raid1/test.bin` i porównaj z zapisaną sumą.
3. Usuń dysk z macierzy: `sudo mdadm /dev/md0 --remove /dev/sdc1`, a następnie dodaj go z powrotem: `sudo mdadm /dev/md0 --add /dev/sdc1`. Obserwuj odbudowę (`watch -n1 cat /proc/mdstat`) i zapisz, ile trwała.
4. Dodaj trzeci dysk jako zapasowy: `sudo mdadm /dev/md0 --add /dev/sdd1`. Zasymuluj awarię `sdb1` (`--fail`) i obserwuj, że odbudowa na `sdd1` startuje automatycznie. Zaktualizuj `mdadm.conf` (usuń stary wiersz `ARRAY` i dopisz nowy z `--detail --scan`) oraz wykonaj `sudo update-initramfs -u`.
5. Dla chętnych (RAID5): przywróć migawkę „przed_RAID”, dodaj trzy nowe dyski 5 GB, utwórz na nich partycje jak w kroku 1 i utwórz `sudo mdadm --create /dev/md0 --level=5 --raid-devices=3 /dev/sdb1 /dev/sdc1 /dev/sdd1`. Porównaj pojemność z RAID1 (`df -h`).

W sprawozdaniu umieść

- ☐ wynik `lsblk` z nowymi dyskami i partycjami
- ☐ użyte polecenia z krótkim opisem
- ☐ zawartość `/proc/mdstat` i `mdadm --detail` w stanach: synchronizacja, praca normalna, awaria, odbudowa, z dyskiem zapasowym

- ☐ wpisy w `mdadm.conf` i `/etc/fstab` oraz dowód działania po restarcie
- ☐ porównanie sum SHA-256 pliku testowego przed i po awarii
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Co oznaczają zapisy `[2/2] [UU]` i `[2/1] [U_]` w `/proc/mdstat`?
2. Dlaczego bez wpisu w `mdadm.conf` i `update-initramfs` macierz po restarcie może się nazywać `md127`?
3. Czym różni się dysk zapasowy (spare) od trzeciego dysku w macierzy RAID1?
4. Ile pojemności użytkowej da RAID5 z trzech dysków 5 GB, a ile RAID1 z dwóch takich dysków?
Który poziom jest bardziej odporny na awarię?

Kryteria oceny

Kryterium	Punkty
Partycje i macierz RAID1 utworzone poprawnie	5
Konfiguracja trwała (mdadm.conf, initramfs, fstab) — działa po restarcie	4
Awaria, usunięcie, dodanie i odbudowa udokumentowane	5
Dysk zapasowy i weryfikacja sum	2
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Ubuntu Server w maszynie wirtualnej

Czas: 2 × 45 min

praca indywidualna

Cel: Zainstalowanie Ubuntu Server w maszynie wirtualnej, skonfigurowanie sieci ze stałym adresem, zdalnego dostępu SSH, kont użytkowników, aktualizacji i zapory — tak, aby serwer był gotowy do dalszych zadań.

Po zajęciach potrafisz:

- instaluje Ubuntu Server LTS w VirtualBox z serwerem OpenSSH
- konfiguruje karty sieciowe VM i stały adres IP przez netplan
- łączy się z serwerem z Windows przez SSH
- zarządza użytkownikami i uprawnieniami sudo
- aktualizuje system, włącza zaporę ufw i wykonuje migawkę VM

Sprzęt i materiały

- komputer stacjonarny z VirtualBox 7, ok. 25 GB wolnego miejsca w folderze maszyn wskazanym przez nauczyciela
- dostęp do internetu (aktualizacje)

Oprogramowanie

- **Ubuntu Server (aktualne wydanie LTS)** — obraz ISO; sprawdź sumę SHA-256 (zadanie 1)
ubuntu.com/download/server
- **Oracle VirtualBox 7**
[virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)
- **Klient SSH: OpenSSH w Windows 11 (Terminal) lub PuTTY** — OpenSSH jest wbudowany — polecenie `ssh`
chiark.greenend.org.uk/~sgtatham/putty/la-test.html

Przygotowanie przed zajęciami

- Pobierz obraz Ubuntu Server LTS (ok. 3 GB) na pendrive lub skopiuj z udziału szkolnego.
- Zapytaj nauczyciela, czy w pracowni wolno używać sieci mostkowanej, i zapisz adres IP, który przydzielił Ci dla sieci izolowanej (host-only).

Bezpieczeństwo

- Ustaw silne hasło administratora serwera (co najmniej 12 znaków) i nie zapisuj go w sprawozdaniu. Nie używaj haseł ze szkolnych kont.
- Przed włączeniem zapory zezwól na SSH (`ufw allow OpenSSH`) — inaczej odetniesz sobie dostęp zdalny.
- Instalator Ubuntu formatuje tylko dysk wirtualny VM — sprawdź, że instalujesz w VirtualBox, a nie z pendrive'a na komputerze fizycznym.
- Sieć mostkowana wystawia serwer w sieci szkolnej — używaj jej tylko za zgodą nauczyciela i przy włączonej zaporze.

Przebieg zadania

1 Maszyna wirtualna

1. Utwórz VM `srv-<nazwisko>`: obraz ISO Ubuntu Server, zaznacz pominięcie instalacji nienadzorowanej (Skip Unattended Installation), 2 GB RAM, 2 procesory, dysk VDI 25 GB (dynamiczny).
2. Ustawienia → Sieć: Karta 1 — „Mostkowana karta sieciowa” (gdy nauczyciel pozwoli) albo NAT. Karta 2 — włącz i wybierz „Karta sieci izolowanej (host-only)”.
3. Jeśli Karta 1 to NAT: Zaawansowane → Przekierowanie portów → reguła TCP, port hosta 2222, port gościa 22.

2 Instalacja

Instalacja trwa ok. 10–15 minut.

1. Uruchom VM, wybierz język English (komunikaty serwera łatwiej wyszukać), układ klawiatury Polish.
2. Na ekranie sieci sprawdź, że obie karty otrzymały adresy (zapisz je). Pozostaw automatyczny podział dysku (cały dysk wirtualny, LVM).
3. Utwórz konto administratora (nazwa serwera `srv-<nazwisko>`). Zaznacz „Install OpenSSH server”. Dodatkowych pakietów (snap) nie wybieraj.
4. Po instalacji wybierz „Reboot Now”, zaloguj się i sprawdź adresy: `ip -br a`.

3 Aktualizacje, użytkownicy i SSH

1. Zaktualizuj system: `sudo apt update && sudo apt upgrade -y`. Sprawdź wersję: `lsb_release -a` i `uname -r`.
2. Utwórz użytkownika `serwis`: `sudo adduser serwis`, dodaj go do grupy sudo: `sudo usermod -aG sudo serwis`. Sprawdź: `groups serwis`. Utwórz też użytkownika `gosc` bez sudo i sprawdź, że `sudo` mu odmawia (`su - gosc`, potem `sudo ls /root`).
3. Z Windows (Terminal) połącz się: `ssh serwis@<adres IP>` (przy NAT: `ssh -p 2222 serwis@127.0.0.1`). Zaakceptuj odcisk klucza serwera i porównaj go z wynikiem `ssh-keygen -lf /etc/ssh/ssh_host_ed25519_key.pub` na serwerze.
4. Sprawdź logowanie także z PuTTY lub z drugiego komputera (tylko przy sieci mostkowej).

4 Stały adres IP (netplan)

Stały adres ustawiamy na karcie sieci izolowanej (zwykle `enp0s8` — sprawdź `ip -br a`).

1. Obejrzyj istniejącą konfigurację: `ls /etc/netplan` i `sudo cat /etc/netplan/*.yaml`.
2. Utwórz plik `sudo nano /etc/netplan/60-hostonly.yaml` z treścią: `network: {version: 2, ethernet: {enp0s8: {dhcp4: false, addresses: [192.168.56.X/24]}}}` (X — od nauczyciela). Ustaw uprawnienia: `sudo chmod 600 /etc/netplan/60-hostonly.yaml`.
3. Zastosuj: `sudo netplan try` (zatwierdź Enter w ciągu 120 s), sprawdź `ip -br a` i z Windows `ping 192.168.56.X` oraz `ssh serwis@192.168.56.X`.

5 Zapora i migawka

1. Włącz zaporę: `sudo ufw allow OpenSSH`, `sudo ufw enable`, sprawdź `sudo ufw status verbose`.
2. Sprawdź usługę SSH: `systemctl status ssh` i ostatnie logowania: `last -n 5`.
3. Wyłącz serwer (`sudo poweroff`) i wykonaj migawkę `serwer-bazowy` (VirtualBox: Migawki → Zrób). Zapisz nazwę VM i jej lokalizację — serwer będzie potrzebny w zadaniu 11.

W sprawozdaniu umieść

- ☐ konfiguracja VM (zrzut ustawień sieci)

- ☐ wersja systemu i jądra po aktualizacji
- ☐ lista utworzonych użytkowników z grupami i wynik testu sudo
- ☐ treść pliku netplan i wynik `ip -br a`
- ☐ zrzut udanego logowania SSH z Windows i porównanie odcisku klucza
- ☐ wynik `ufw status verbose`
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różnią się w VirtualBox tryby sieci NAT, mostkowany i sieć izolowana (host-only)?
2. Po co przy pierwszym połączeniu SSH porównuje się odcisk klucza serwera?
3. Dlaczego serwer powinien mieć stały adres IP?
4. Dlaczego do administracji używa się zwykłego konta z sudo, a nie logowania bezpośrednio na konto root?
5. Co by się stało po `ufw enable` bez wcześniejszego `ufw allow OpenSSH`, gdy jesteś połączony przez SSH?

Kryteria oceny

Kryterium	Punkty
Serwer zainstalowany i zaktualizowany	4
Działające logowanie SSH z Windows	4
Użytkownicy i sudo, test uprawnień	3
Stały adres IP przez netplan i zaporę ufw	4
Migawka i kompletna dokumentacja	2
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Serwer plików Samba

Czas: 2 × 45 min

praca indywidualna, test z laptopa w parach

Cel: Uruchomienie na Ubuntu Server serwera plików Samba z udziałem tylko do odczytu i udziałem prywatnym, nadanie uprawnień oraz sprawdzenie dostępu z Windows (stacjonarka i laptop).

Po zajęciach potrafisz:

- instaluje i konfiguruje usługę Samba (smb.conf, testparm)
- tworzy konta Samba i ustawia uprawnienia katalogów w Linuksie
- łączy się z udziałem z Windows i mapuje go jako dysk sieciowy
- sprawdza stan usługi, połączenia i logi (systemctl, smbstatus, log.smbd)
- wyjaśnia współdziałanie uprawnień Samby i systemu plików

Sprzęt i materiały

- komputer stacjonarny z maszyną wirtualną Ubuntu Server z zadania 10
- laptop szkolny z Windows 11 (test dostępu przez sieć, jeśli serwer ma kartę mostkowaną)

Oprogramowanie

- **Samba (pakiet Ubuntu)** — instalacja: `sudo apt install samba`
[samba.org](https://www.samba.org)
- **Ubuntu Server z zadania 10** — migawka `server-bazowy`
ubuntu.com/download/server
- **Eksplorator plików i wiersz poleceń Windows 11** — polecenie `net use`

Przygotowanie przed zajęciami

- Uruchom serwer z zadania 10 i sprawdź logowanie SSH z Windows. Przed zmianami wykonaj migawkę `przed_samba`.

Bezpieczeństwo

- Nie włączaj w Windows niezabezpieczonego logowania gościa ani nie wyłączaj podpisywania SMB — dostęp zapewniamy kontami Samba.
- Hasła kont Samba ustaw inne niż hasło administratora serwera i nie wpisuj ich do sprawozdania.
- W zaporze otwieraj tylko usługę Samba (`ufw allow Samba`); nie wyłączaj ufw.
- Po zajęciach odłącz zmapowane dyski na laptopie i usuń zapisane poświadczenia (`net use *` `/delete`, Menedżer poświadczeń).

Przebieg zadania

1 Instalacja i katalogi

Pracuj przez SSH z Windows.

1. Zainstaluj Sambę: `sudo apt update && sudo apt install samba`. Sprawdź usługę: `systemctl status smbd`.
2. Utwórz katalogi: `sudo mkdir -p /srv/samba/publiczny /srv/samba/prywatny`.
3. Utwórz użytkownika bez logowania do powłoki: `sudo adduser --no-create-home --shell /usr/sbin/nologin uczen`.
4. Ustaw właścicieli i uprawnienia: `sudo chown serwis:serwis /srv/samba/publiczny`, `sudo chmod 755 /srv/samba/publiczny`, `sudo chown uczen:uczen /srv/samba/prywatny`, `sudo chmod 700 /srv/samba/prywatny`. Umieść w udziale publicznym plik `regulamin.txt`.

2 Konfiguracja Samby

1. Zrób kopię: `sudo cp /etc/samba/smb.conf /etc/samba/smb.conf.bak`, otwórz `sudo nano /etc/samba/smb.conf` i dopisz na końcu sekcję `[publiczny]` z wierszami: `path = /srv/samba/publiczny`, `read only = yes`, `write list = serwis`.
2. Dopisz sekcję `[prywatny]`: `path = /srv/samba/prywatny`, `read only = no`, `valid users = uczen`, `browseable = no`.
3. Sprawdź składnię: `testparm` i zapisz wynik. Utwórz konta Samby: `sudo smbpasswd -a uczen` oraz `sudo smbpasswd -a serwis`. Lista kont: `sudo pdbedit -L`.
4. Uruchom ponownie usługę: `sudo systemctl restart smbd` i otwórz zaporę: `sudo ufw allow Samba`, sprawdź `sudo ufw status`.

3 Dostęp z Windows (stacjonarka)

Używaj stałego adresu serwera z zadania 10.

1. W Eksploratorze wpisz `\\<adres_serwera>\publiczny`, zaloguj się jako `uczen`. Otwórz `regulamin.txt` i spróbuj utworzyć nowy plik — zapisz komunikat.
2. W wierszu poleceń zmapuj udział prywatny: `net use Z: \\<adres_serwera>\prywatny /user:uczen` (hasło podasz po zapytaniu). Utwórz na Z: folder i plik. Sprawdź `net use`.
3. Spróbuj otworzyć ten sam serwer jako `serwis` w drugim oknie. Zapisz komunikat (błąd 1219 — jedno konto na serwer). Odłącz połączenia: `net use * /delete`, połącz się jako `serwis` i sprawdź, czy możesz zapisywać w udziale publicznym, a czy masz dostęp do prywatnego.
4. Na serwerze sprawdź właściciela utworzonych plików: `ls -l /srv/samba/prywatny`.

4 Test z laptopa

Tylko gdy serwer ma kartę mostkowaną (adres w sieci szkolnej).

1. Na laptopie otwórz `\\<adres_mostkowany_serwera>\publiczny` i zmapuj udział prywatny jako `uczen`. Sprawdź odczyt i zapis.
2. Bez karty mostkowanej: zapisz, dlaczego laptop nie może połączyć się z siecią izolowaną (host-only), i wykonaj test z drugiego okna Windows na stacjonarce.
3. Odłącz dyski na laptopie: `net use * /delete` i usuń poświadczenia w Menedżerze poświadczeń.

5 Status i logi

1. Podczas aktywnego połączenia wykonaj na serwerze `sudo smbstatus` — odczytaj użytkownika, adres klienta, udział i wersję protokołu SMB.
2. Przejrzyj log: `sudo tail -n 30 /var/log/samba/log.smbd` oraz `journalctl -u smbd -n 20`. Znajdź wpis o nieudanym logowaniu (wywołaj go, podając złe hasło). Jeśli wpisu nie ma, dodaj w sekcji `[global]` wiersz `log_level = 1 auth_audit:3`, uruchom ponownie `smbd` i powtórz próbę.

W sprawozdaniu umieść

- ☐ dopisane sekcje smb.conf i wynik `testparm`
- ☐ uprawnienia katalogów (`ls -ld /srv/samba/*`) i lista kont Samba
- ☐ tabela testów dostępu dla kont `uczen` i `serwis` w obu udziałach
- ☐ zrzuty z Eksploratora i wynik `net use`
- ☐ wynik `smbstatus` i wpis z logu o nieudanym logowaniu
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego użytkownik `uczen` mimo wpisu `read only = no` nie mógłby zapisywać w katalogu z uprawnieniami 755 należącym do innego użytkownika?
2. Czym różni się konto systemowe Linuksa od konta Samba i dlaczego trzeba utworzyć oba?
3. Co daje opcja `browseable = no` i czy zabezpiecza ona udział?
4. Dlaczego Windows 11 blokuje dostęp gościa do udziałów SMB i jakie zagrożenie by powstało po jego włączeniu?

Kryteria oceny

Kryterium	Punkty
Samba zainstalowana, smb.conf poprawny (testparm bez błędów)	5
Konta i uprawnienia katalogów zgodne z założeniami	4
Testy dostępu z Windows (stacjonarka i laptop lub uzasadnienie)	5
Status usługi i analiza logów	2
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Serwer multimedialny Jellyfin na Ubuntu Server

Czas: 2 × 45 min

praca indywidualna (test z drugiego urządzenia w parach)

Cel: Uruchomienie w maszynie wirtualnej serwera multimedialnego udostępniającego filmy i muzykę w sieci lokalnej oraz zbadanie, jak transkodowanie obciąża procesor serwera.

Po zajęciach potrafisz:

- instaluje serwer Jellyfin z oficjalnego repozytorium i zarządza jego usługą (systemctl)
- przygotowuje katalogi multimedialnych z poprawnymi uprawnieniami dla usługi
- kopiuje pliki z udziału sieciowego na serwer Linux
- konfiguruje biblioteki i konta użytkowników w panelu WWW
- mierzy obciążenie CPU podczas odtwarzania bezpośredniego i transkodowania

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i maszyną Ubuntu Server z zadania 10
- laptop lub telefon w tej samej sieci (test odtwarzania)
- słuchawki (opcjonalnie)

Oprogramowanie

- **Jellyfin Server** — skrypt `install-debuntu.sh` z repo.jellyfin.org
jellyfin.org/docs/general/installation/linux
- **Emby Server (alternatywa)** — pakiet `.deb`; część funkcji płatna (Emby Premiere)
emby.media/linux-server.html
- **htop, cifs-utils** — z repozytorium Ubuntu (`apt`)
- **Przykładowe multimedia na wolnej licencji** — lub pliki z udziału szkolnego wskazanego przez nauczyciela
studio.blender.org/films

Przygotowanie przed zajęciami

- Sprawdź, że maszyna Ubuntu Server z zadania 10 uruchamia się, ma statyczny IP i działa logowanie przez SSH. Zapisz jej adres IP.
- Zwiększ RAM maszyny do co najmniej 2 GB i przydziel 2 procesory (VM wyłączona → Ustawienia → System).

Bezpieczeństwo

- Przed instalacją wykonaj migawkę maszyny wirtualnej — w razie problemu wrócisz do działającego serwera.
- Nie uruchamiaj skryptów z internetu z `sudo` bez sprawdzenia sumy kontrolnej i źródła (tylko repo.jellyfin.org).
- Udostępniaj wyłącznie pliki, do których masz prawa (wolne licencje, materiały szkolne). Udostępnianie filmów komercyjnych innym osobom narusza prawo autorskie.
- Dane logowania do udziału szkolnego wpisuj tylko w poleceniu montowania — nie zapisuj ich w sprawozdaniu ani w plikach na serwerze.
- Konto administratora Jellyfin zabezpiecz hasłem innym niż hasło do systemu; nie przekierowuj portu 8096 do internetu.

Przebieg zadania

1 Przygotowanie serwera

Pracuj przez SSH z Windows (Terminal) — łatwiej kopiować polecenia.

1. Wykonaj migawkę VM „przed-jellyfin” (VirtualBox → Migawki → Zrób).
2. Zaloguj się przez SSH i zaktualizuj system: `sudo apt update && sudo apt upgrade -y`.
3. Utwórz użytkownika i katalogi: `sudo adduser media`, `sudo mkdir -p /srv/media/filmy /srv/media/muzyka`, `sudo chown -R media:media /srv/media`, `sudo chmod -R 755 /srv/media`.

2 Instalacja Jellyfin

Według oficjalnej instrukcji (lub Emby z pakietu .deb — wtedy usługa nazywa się `emby-server`).

1. Pobierz skrypt i jego sumę: `curl -s https://repo.jellyfin.org/install-debuntu.sh -O` oraz `curl -s https://repo.jellyfin.org/install-debuntu.sh.sha256sum -O`.
2. Sprawdź sumę: `sha256sum -c install-debuntu.sh.sha256sum` — wynik musi brzmieć „OK”. Dopiero wtedy uruchom `sudo bash install-debuntu.sh`.
3. Sprawdź usługę i port: `systemctl status jellyfin` oraz `sudo ss -tlnp | grep 8096`.
4. Otwórz port w zaporze: `sudo ufw allow 8096/tcp`, sprawdź `sudo ufw status`.
5. Dodaj użytkownika usługi do grupy media: `sudo usermod -aG media jellyfin`, potem `sudo systemctl restart jellyfin`.

3 Kopiowanie multimedialów

Ścieżkę udziału i dane logowania podaje nauczyciel.

1. Zainstaluj klienta: `sudo apt install cifs-utils -y` i utwórz punkt montowania `sudo mkdir -p /mnt/szkola`.
2. Zamontuj udział tylko do odczytu: `sudo mount -t cifs //SERWER/UDZIAŁ /mnt/szkola -o username=LOGIN,ro` (hasło wpisz po pytaniu).
3. Skopiuj przykładowy film i kilka utworów do `/srv/media/filmy` i `/srv/media/muzyka` (`sudo cp`), popraw właściciela (`sudo chown -R media:media /srv/media`) i odmontuj udział: `sudo umount /mnt/szkola`.

4 Konfiguracja i odtwarzanie

1. W przeglądarce na komputerze-gospodarzu otwórz `http://IP_SERWERA:8096` i przejdź kreator: język, konto administratora, biblioteki Filmy (`/srv/media/filmy`) i Muzyka (`/srv/media/muzyka`).
2. Poczekaj na skanowanie biblioteki, sprawdź, czy pobrały się metadane i okładki.
3. W panelu administracyjnym (Dashboard → Użytkownicy) utwórz konto „uczen” bez praw administratora z dostępem tylko do biblioteki Muzyka. Zaloguj się nim i sprawdź, co widzi.
4. Odtwórz film z innego urządzenia (laptop lub telefon kolegi) w tej samej sieci.

5 Pomiar obciążenia przy transkodowaniu

Odtwarzanie bezpośrednio (Direct Play) prawie nie obciąża serwera, transkodowanie — bardzo.

1. W drugim oknie SSH uruchom `htop` (zainstaluj, jeśli brak).
2. Odtwórz film w jakości oryginalnej i zapisz obciążenie CPU oraz tryb odtwarzania (ikona ustawień odtwarzacza → informacje o odtwarzaniu).
3. W ustawieniach odtwarzacza zmień jakość na niższą (np. 720p, ok. 2 Mb/s), odczekaj minutę i znów zapisz CPU, tryb oraz proces `ffmpeg` widoczny w `htop`.
4. Zrób zrzuty ekranu `htop` w obu przypadkach.

W sprawozdaniu umieść

- ☐ adres IP serwera, wersja Ubuntu i Jellyfin (Dashboard → Ogólne), wynik sprawdzenia sumy SHA-256
- ☐ polecenia użyte do utworzenia katalogów i nadania uprawnień oraz wynik `ls -l /srv/media`
- ☐ zrzuty: biblioteka z okładkami, widok konta „uczen”, odtwarzanie z drugiego urządzenia
- ☐ tabela pomiaru obciążenia CPU i zrzuty htop
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego usługa Jellyfin nie widziała plików, dopóki nie dodano jej użytkownika do grupy media (lub nie nadano uprawnień do odczytu)?
2. Czym różni się odtwarzanie bezpośrednio od transkodowania i kiedy serwer musi transkodować?
3. Dlaczego katalogi multimediów umieszczono w /srv, a nie w /media?
4. Jakie zagrożenia niesie wystawienie serwera multimediów do internetu i jak bezpiecznie korzystać z niego spoza domu?

Kryteria oceny

Kryterium	Punkty
Instalacja z weryfikacją sumy, działająca usługa i port w zaporze	5
Katalogi i uprawnienia, skopiowane multimedia	4
Biblioteki, konto ograniczone, odtwarzanie z drugiego urządzenia	4
Pomiar transkodowania i wnioski	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

NAS w maszynie wirtualnej — OpenMediaVault

Czas: 2 × 45 min

praca indywidualna

Cel: Zbudowanie w maszynie wirtualnej sieciowego serwera plików NAS z macierzą RAID1 i udziałem SMB oraz sprawdzenie, jak NAS reaguje na awarię dysku.

Po zajęciach potrafisz:

- instaluje OpenMediaVault w maszynie wirtualnej z osobnym dyskiem systemowym i dyskami danych
- tworzy w panelu WWW macierz RAID1, system plików i folder współdzielony
- konfiguruje użytkowników, uprawnienia i udział SMB oraz łączy się z nim z Windows
- odczytuje stan macierzy i SMART oraz wyjaśnia ograniczenia SMART w maszynie wirtualnej
- porównuje NAS programowy z gotowym urządzeniem NAS

Sprzęt i materiały

- komputer stacjonarny z VirtualBox 7 (ok. 30 GB wolnego miejsca na dysku z maszynami wirtualnymi)
- laptop (test dostępu do udziału z innego komputera, opcjonalnie)

Oprogramowanie

- **OpenMediaVault 8 (obraz ISO amd64)** — oparty na Debianie 13; obraz z oficjalnej strony
openmediavault.org/download.html
- **Wtyczka openmediavault-md** — obsługa RAID programowego (Storage → Multiple Device)
docs.openmediavault.org/en/8.x/plugins/available/md.html
- **Oracle VirtualBox 7**
virtualbox.org/wiki/Downloads

Przygotowanie przed zajęciami

- Pobierz obraz ISO OpenMediaVault na pendrive lub dysk z maszynami wirtualnymi i zapisz jego sumę SHA-256 ze strony pobierania.
- Przeczytaj, czym różni się RAID1 od kopii zapasowej (zadanie 8 i 9).

Bezpieczeństwo

- Wszystkie operacje na dyskach wykonuj tylko na dyskach wirtualnych VM. Instalator OMV formatuje cały wybrany dysk — przy instalacji wybierz dysk systemowy VM (8–16 GB), nie dysk danych.
- Domyślne hasło administratora panelu WWW zmień natychmiast po pierwszym logowaniu.
- Nie wyłączaj VM „na twardo” podczas tworzenia lub odbudowy macierzy — używaj zamykania z panelu (Power → Shutdown).
- Nie wpisuj w powiadomieniach e-mail prawdziwego hasła do swojej poczty — konfigurację SMTP tylko pokaż lub użyj konta testowego od nauczyciela.

Przebieg zadania

1 Maszyna wirtualna i instalacja

1. Utwórz VM: typ Linux, Debian 64-bit, 2 GB RAM, 2 procesory, dysk systemowy 16 GB. Karta sieciowa: mostkowana (lub zgodnie z poleceniem nauczyciela). Oznacz instalację nienadzorowaną.
2. W ustawieniach VM (Pamięć → kontroler SATA) dodaj dwa nowe dyski VDI po 10 GB: `dane1` i `dane2`.
3. Uruchom instalator z ISO: język, klawiatura polska, nazwa hosta `nas-NAZWISKO`, hasło roota. Jako dysk instalacji wybierz dysk 16 GB.
4. Po restarcie zapisz adres IP wyświetlany na konsoli i zaloguj się w przeglądarce Windows na `http://IP` (konto admin, hasło domyślne z dokumentacji OMV). Od razu zmień hasło (ikona użytkownika → Change Password).

2 Macierz RAID1 i system plików

1. Zaktualizuj system (System → Update Management) i zainstaluj wtyczkę `openmediavault-md` (System → Plugins).
2. Storage → Disks: sprawdź, że widzisz oba dyski 10 GB, i wyczyść je (Wipe → Quick).
3. Storage → Multiple Device → Create: poziom Mirror, zaznacz oba dyski danych. Zastosuj zmiany (przycisk zatwierdzenia u góry) i obserwuj synchronizację.
4. Storage → File Systems → Create: ext4 na urządzeniu `/dev/md...`, zamontuj go i zatwierdź zmiany.

3 Użytkownicy i udział SMB

1. Users → Users: utwórz konta `jan` i `anna` (hasła zapisz tylko na kartce dla siebie).
2. Storage → Shared Folders: utwórz folder `dokumenty` na systemie plików z RAID1. W Permissions nadaj `jan` odczyt/zapis, `anna` tylko odczyt.
3. Services → SMB/CIFS → Settings: włącz usługę; w Shares dodaj udział `dokumenty`. Zatwierdź zmiany.
4. W Windows otwórz `\\IP\dokumenty`, zaloguj się jako `jan` i skopiuj kilka plików. Wyloguj połączenie (`net use * /delete`) i sprawdź, że `anna` może tylko czytać.

4 SMART, awaria i odbudowa

Dyski wirtualne nie mają prawdziwego SMART — sprawdź, co pokazuje OMV.

1. Storage → S.M.A.R.T. → Devices: spróbuj włączyć monitorowanie i odczytać informacje. Zanotuj wynik.
2. System → Notification: obejrzyj ustawienia powiadomień i listę zdarzeń, o których OMV może powiadamiać (bez wpisywania prawdziwego hasła).
3. Zamknij OMV z panelu. W ustawieniach VM odłącz dysk `dane2` i uruchom VM. Sprawdź stan macierzy (Multiple Device) i czy pliki w udziale są dostępne.
4. Wyłącz VM, dodaj nowy dysk 10 GB `dane3`, uruchom, wyczyść go i użyj Multiple Device → Recover. Zapisz czas odbudowy i stan końcowy (clean).

W sprawozdaniu umieść

- ☐ konfiguracja VM (dyski, RAM, sieć) i adres IP NAS
- ☐ zrzuty: macierz RAID1 po utworzeniu, system plików, uprawnienia folderu, udział otwarty w Windows
- ☐ wynik testu uprawnień dla kont jan i anna
- ☐ przebieg awarii i odbudowy: stan macierzy przed, w trakcie i po
- ☐ wyjaśnienie, co OMV pokazał w zakładce S.M.A.R.T. i dlaczego

☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego system OMV instaluje się na osobnym dysku, a nie na macierzy z danymi?
2. Dlaczego RAID1 nie zastępuje kopii zapasowej? Podaj dwie sytuacje, w których RAID1 nie uratuje danych.
3. Dlaczego dyski wirtualne VirtualBox nie udostępniają rzeczywistych danych SMART?
4. Wymień dwie zalety i dwie wady gotowego NAS (np. Synology, QNAP) w porównaniu z NAS zbudowanym na OMV.

Kryteria oceny

Kryterium	Punkty
Instalacja OMV na właściwym dysku, zmiana hasła admina	3
Macierz RAID1 i system plików	4
Użytkownicy, uprawnienia i udział SMB sprawdzony z Windows	4
Symulacja awarii i odbudowa macierzy	4
Odpowiedzi na pytania kontrolne i porównanie z gotowym NAS	5
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Kopie zapasowe 3-2-1 i automatyzacja

Czas: 2 × 45 min

praca indywidualna

Cel: Zaprojektowanie strategii kopii zapasowych według zasady 3-2-1 oraz zautomatyzowanie kopii w Windows (robocopy) i Linux (rsync z kopiami przyrostowymi na twardych linkach) z testem odtworzenia.

Po zajęciach potrafisz:

- rozróżnia kopię pełną, przyrostową i różnicową oraz dobiera je do potrzeb klienta
- tworzy kopię robocopy z logiem i uruchamia ją w Harmonogramie zadań
- tworzy kopie przyrostowe rsync z --link-dest i planuje je w cron
- odtwarza wybrany plik z kopii i sprawdza jego zgodność
- stosuje zasadę retencji, usuwając najstarsze kopie

Sprzęt i materiały

- komputer stacjonarny z Windows 11 (drugi dysk lub VM z zadania 26 roku 1) i maszyną Ubuntu Server z zadań 10–11
- pendrive (opcjonalnie — druga lokalizacja kopii)

Oprogramowanie

- **robocopy, Harmonogram zadań (taskschd.msc)** — wbudowane w Windows
learn.microsoft.com/windows-server/administration/windows-commands/robocopy
- **rsync, cron** — w Ubuntu Server (podręcznik rsync)
download.samba.org/pub/rsync/rsync.1
- **Samba na Ubuntu Server** — udział prywatny z zadania 11 jako miejsce docelowe kopii z Windows

Przygotowanie przed zajęciami

- Upewnij się, że udział prywatny Samby z zadania 11 działa i znasz nazwę konta oraz hasło.
- Przypomnij sobie różnicę między kopią pełną, przyrostową i różnicową (zadanie 24 roku 1).

Bezpieczeństwo

- Parametr `/MIR` robocopy usuwa w miejscu docelowym pliki, których nie ma w źródle. Zawsze najpierw uruchom polecenie z `/L` (tylko lista) i sprawdź ścieżki — pomyłka źródła z celem kasuje dane.
- Kopiuj tylko katalogi testowe (`C:\DaneTest` , `/home/UŻYTKOWNIK/dane`), nie cały profil ani dysk szkolnego systemu.
- Polecenie usuwania starych kopii (`rm -rf`) najpierw uruchom z `echo` zamiast `rm` , żeby zobaczyć, co zostanie usunięte.
- Hasła do udziału nie wpisuj w skrypcie — zapisz poświadczenia w Menedżerze poświadczeń Windows lub zaloguj się przed uruchomieniem zadania.

Przebieg zadania

1 Plan 3-2-1

Klient: mała firma, dwa komputery, ok. 50 GB dokumentów, serwer plików (Samba).

1. W sprawozdaniu zaprojektuj dla klienta: 3 kopie, 2 różne nośniki, 1 kopia poza firmą. Dla każdej kopii podaj nośnik, rodzaj (pełna/przyrostowa/różnicowa), częstotliwość i retencję.
2. Zaznacz, która kopia jest odłączona od sieci (offline) lub niezmienna — i wyjaśnij, przed czym chroni.

2 Windows — robocopy na udział Samby

1. Utwórz `C:\DaneTest` z kilkoma plikami i podkatalogiem. W udziale Samby utwórz katalog `kopia-NAZWISKO`.
2. Sprawdź polecenie na sucho: `robocopy C:\DaneTest \\IP\udział\kopia-NAZWISKO /MIR /R:1 /W:1 /L`.
3. Wykonaj kopię z logiem: to samo bez `/L`, z dopiskiem `/LOG+:C:\Logi\kopia.log /NP /TEE` (utwórz wcześniej `C:\Logi`). Odczytaj podsumowanie w logu.
4. Zapisz polecenie w pliku `C:\Skrypty\kopia.cmd`. W Harmonogramie zadań utwórz zadanie podstawowe uruchamiające ten plik codziennie o wybranej godzinie (opcja „Uruchom tylko wtedy, gdy użytkownik jest zalogowany”).
5. Zmień jeden plik, dodaj nowy i usuń inny, uruchom zadanie ręcznie (prawy przycisk → Uruchom). Sprawdź w logu, co zostało skopiowane, a co usunięte.

3 Linux — rsync z twardymi linkami

Każda kopia wygląda jak pełna, ale niezmienione pliki są tylko twardymi linkami do poprzedniej kopii.

1. Na Ubuntu Server utwórz `~/dane` z kilkoma plikami (np. `cp -r /etc/ssh ~/dane/`) i katalog `/backup` (`sudo mkdir /backup && sudo chown $USER /backup`).
2. Utwórz skrypt `~/kopia.sh`: `D=$(date +%F_%H%M)`, `rsync -a --delete --link-dest=/backup/ostatnia ~/dane/ /backup/$D/`, `ln -sf /backup/$D /backup/ostatnia` (pierwsza linia: `#!/bin/bash`). Nadaj prawo wykonania `chmod +x`.
3. Uruchom skrypt, zmień jeden plik, odczekaj minutę i uruchom ponownie. Porównaj rozmiar każdej kopii mierzony osobno (`du -sh /backup/KATALOG`) z rozmiarem całości (`du -sh /backup`) oraz liczbę dowiązań niezmienionego pliku (`stat -c %h`).
4. Dodaj zadanie cron (`crontab -e`): `* /5 * * * * /home/UŻYTKOWNIK/kopia.sh >> /home/UŻYTKOWNIK/kopia.log 2>&1`. Po 10 minutach sprawdź, czy powstały nowe kopie.

4 Odtworzenie i retencja

Kopia, której nie sprawdzono, nie jest kopią.

1. Windows: usuń plik z `C:\DaneTest` i odtwórz go z udziału. Porównaj sumy: `Get-FileHash` dla pliku odtworzonego i kopii.
2. Linux: odtwórz plik w wersji sprzed zmiany z najstarszej kopii (`cp /backup/STARA/plik ~/dane/`), sprawdź `sha256sum`.
3. Retencja: pozostaw 3 najnowsze kopie. Najpierw wyświetl kandydatów: `ls -ld /backup/20* | head -n -3`, potem dodaj `| xargs echo rm -rf`, a gdy lista jest poprawna — usuń `echo`.
4. Usuń zadanie cron po zakończeniu testu (`crontab -e`).

W sprawozdaniu umieść

- ☐ plan 3-2-1 dla klienta (tabela)
- ☐ treść `kopia.cmd` i `kopia.sh`, wpis crontab, zrzut zadania w Harmonogramie
- ☐ fragment logu robocopy z podsumowaniem po zmianach plików

- ☐ wynik porównania `du` i `stat -c %h` z wyjaśnieniem twardych linków
- ☐ wynik testu odtworzenia (sumy kontrolne) i retencji
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różni się kopia przyrostowa od różnicowej? Która szybciej się wykonuje, a która szybciej odtwarza?
2. Dlaczego robocopy z `/MIR` nie chroni przed przypadkowym usunięciem pliku, jeśli kopia wykonana się po usunięciu?
3. Dlaczego kilka kopii rsync z `--link-dest` zajmuje niewiele więcej miejsca niż jedna?
4. Dlaczego kopia na dysku stale podłączonym do komputera nie chroni przed ransomware?

Kryteria oceny

Kryterium	Punkty
Plan 3-2-1 dla klienta	3
Kopia robocopy z logiem i zadaniem w Harmonogramie	5
Skrypt rsync z <code>--link-dest</code> i cron	5
Test odtworzenia i retencja	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Instalacja nienadzorowana Windows 11 (autounattend.xml)

Czas: 2 × 45 min**praca w parach (jedna osoba instaluje ręcznie, druga nienadzorowanie — równolegle)**

Cel: Przygotowanie pliku odpowiedzi autounattend.xml i przeprowadzenie w maszynie wirtualnej instalacji Windows 11 bez udziału użytkownika oraz porównanie jej czasu z instalacją ręczną.

Po zajęciach potrafisz:

- generuje plik autounattend.xml z wybranymi ustawieniami (język, strefa czasowa, konto lokalne, partycjonowanie)
- odczytuje i objaśnia najważniejsze sekcje pliku odpowiedzi (przebiegi konfiguracji)
- przeprowadza instalację nienadzorowaną w VM VirtualBox z EFI, TPM 2.0 i Secure Boot
- mierzy i porównuje czas instalacji ręcznej i nienadzorowanej
- ocenia ryzyko użycia pliku odpowiedzi z automatycznym partycjonowaniem

Sprzęt i materiały

- komputer stacjonarny z VirtualBox 7, min. 8 GB RAM i ok. 70 GB wolnego miejsca na dwie VM
- stoper (telefon)

Oprogramowanie

- **Obraz ISO Windows 11 (polski)** — lub kopia z udziału szkolnego wskazanego przez nauczyciela
microsoft.com/software-download/windows11
- **Generator plików odpowiedzi (Christoph Schneegans)** — pobranie pliku .xml lub .xml w obrazie .iso (unattend.iso)
schneegans.de/windows/unattend-generator
- **Windows System Image Manager (Windows ADK) — dla chętnych** — narzędzie Microsoftu do tworzenia plików odpowiedzi
learn.microsoft.com/windows-hardware/get-started/adk-install
- **Oracle VirtualBox 7**
virtualbox.org/wiki/Downloads

Przygotowanie przed zajęciami

- Sprawdź, że masz obraz ISO Windows 11 w języku polskim (język w pliku odpowiedzi musi zgadzać się z obrazem).
- Przypomnij sobie ustawienia VM Windows 11 z zadania 26 roku 1 (EFI, TPM 2.0, Secure Boot, 4 GB RAM, 2 procesory).

Bezpieczeństwo

- Plik odpowiedzi z automatycznym partycjonowaniem czyści dysk bez pytania. Używaj go **wyłącznie w maszynie wirtualnej**.
- Nie kopiuj `autounattend.xml` na pendrive Ventoy ani żaden inny nośnik — Instalator Windows szuka tego pliku na podłączonych nośnikach i uruchomiony na komputerze w pracowni wymazałby dysk szkolnego systemu.
- Nie wpisuj w pliku odpowiedzi swoich prawdziwych haseł — hasło jest w nim zapisane jawnie lub łatwo odwracalnie. Użyj hasła testowego.
- System w VM pozostaje nieaktywowany (klucz ogólny służy tylko do wyboru edycji). Po zajęciach usuń VM, jeśli nauczyciel nie poleci inaczej.

Przebieg zadania

1 Przygotowanie pliku odpowiedzi

Osoba B w parze. Osoba A w tym czasie zakłada VM do instalacji ręcznej.

1. Otwórz generator. Ustaw: język wyświetlania polski, klawiatura polski (programisty), lokalizacja Polska, strefa czasowa (UTC+01:00) Warszawa.
2. Edycja: Windows 11 Pro (klucz ogólny do instalacji). Zaznacz pominięcie sprawdzania wymagań sprzętowych tylko, jeśli nauczyciel poleci; konto lokalne `uczen` z hasłem testowym, w grupie Administratorzy.
3. Partycjonowanie: automatyczne, GPT, dysk 0 — rozumiesz, że skasuje on cały dysk VM. Zaznacz instalację dodatków gościa VirtualBox (VM options).
4. Pobierz plik `.xml` (do analizy) oraz wersję w obrazie `.iso` (`unattend.iso`). Otwórz XML w Notatniku i znajdź sekcje `windowsPE`, `specialize` i `oobeSystem` oraz miejsca z nazwą konta i strefą czasową.

2 Dwie instalacje równolegle

Osoba A — instalacja ręczna, osoba B — nienadzorowana. Obie VM mają takie same parametry.

1. Utwórz VM: Windows 11 64-bit, EFI, TPM 2.0, Secure Boot, 4 GB RAM, 2 procesory, dysk 64 GB. Wybierz ISO Windows i **wyłącz** instalację nienadzorowaną VirtualBox (zależnie od wersji: zaznacz „Skip Unattended Installation” albo odznaczyć „Proceed with Unattended Installation”) — tu jej nie używamy.
2. Osoba B: w ustawieniach VM dodaj drugi napęd optyczny z `unattend.iso` (oraz trzeci z `VBoxGuestAdditions.iso` z katalogu programu VirtualBox).
3. Obie osoby: uruchom VM i stoper w tej samej chwili. Osoba A przechodzi instalację i OOBE ręcznie, wybierając konto lokalne, jeśli to możliwe (inaczej opisz, co wymusił instalator).
4. Zatrzymaj stoper, gdy pojawi się pulpit. Zanotuj czas i liczbę czynności (kliknięć/ekranów), które wykonał człowiek.

3 Weryfikacja

1. W obu VM sprawdź: nazwę konta, strefę czasową, układ klawiatury, nazwę komputera (`hostname`) i układ partycji (Zarządzanie dyskami).
2. Sprawdź, czy w VM B zainstalowały się dodatki gościa (zmiana rozdzielczości okna, `Programy i funkcje`).
3. Porównaj wyniki z ustawieniami w pliku odpowiedzi. Jeśli coś się nie zgadza, znajdź przyczynę w XML.
4. Po udokumentowaniu usuń obie VM (prawy przycisk → Usuń → Usuń wszystkie pliki) i plik `unattend.iso`, chyba że nauczyciel poleci inaczej.

W sprawozdaniu umieść

- ☐ lista ustawień wybranych w generatorze
- ☐ fragmenty XML z sekcjami windowsPE, specialize i oobeSystem z krótkim opisem
- ☐ tabela czasów i liczby czynności obu instalacji
- ☐ wyniki weryfikacji ustawień w obu VM
- ☐ ocena ryzyka: gdzie wolno, a gdzie nie wolno używać takiego pliku
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. W jakich sytuacjach serwisowych instalacja nienadzorowana oszczędza najwięcej czasu?
2. Co dzieje się w przebiegach windowsPE, specialize i oobeSystem?
3. Dlaczego plik autounattend.xml na pendrivie podłączonym do komputera może doprowadzić do utraty danych?
4. Jakie dane wrażliwe może zawierać plik odpowiedzi i jak go chronić?

Kryteria oceny

Kryterium	Punkty
Poprawny plik odpowiedzi z wymaganymi ustawieniami	5
Analiza sekcji XML	3
Przeprowadzone instalacje i pomiar czasu	5
Weryfikacja ustawień i ocena ryzyka	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Menedżery pakietów: winget i apt

Czas: 2 × 45 min

praca indywidualna

Cel: Zautomatyzowanie instalacji i aktualizacji oprogramowania za pomocą menedżerów pakietów w Windows (winget) i Linux (apt, snap, flatpak).

Po zajęciach potrafisz:

- wyszukuje, instaluje, aktualizuje i odinstalowuje programy poleceniem winget
- eksportuje listę programów do pliku JSON i odtwarza ją na innym komputerze
- pisze skrypt instalujący zestaw programów dla stanowiska
- instaluje programy w Linux przez apt, snap i flatpak i porównuje te mechanizmy

Sprzęt i materiały

- komputer stacjonarny z Windows 11 na drugim dysku (zadanie 13 roku 1) lub VM Windows 11 (zadanie 26 roku 1)
- Ubuntu na drugim dysku (zadanie 15 roku 1), w VM lub uruchomione live z pendrive'a

Oprogramowanie

- **winget (Instalator aplikacji)** — wbudowany w Windows 11; aktualizacja przez Microsoft Store („Instalator aplikacji”) learn.microsoft.com/windows/package-manager/winget
- **apt, snap** — wbudowane w Ubuntu ubuntu.com/server/docs
- **Flatpak i repozytorium Flathub** — instrukcja dla Ubuntu flathub.org/setup

Bezpieczeństwo

- Instaluj programy tylko w Windows na drugim dysku lub w VM — nie w szkolnym systemie na pierwszym dysku.
- Przed instalacją sprawdź w `winget show` wydawcę i stronę programu — nazwy podobne do znanych programów mogą należeć do innych autorów.
- Polecenia z `sudo` i `winget upgrade --all` zmieniają cały system — uruchamiaj je świadomie, z czytaniem komunikatów.

Przebieg zadania

1 winget — podstawy

Terminal Windows (PowerShell) jako zwykły użytkownik — winget poprosi o uprawnienia, gdy będą potrzebne.

1. Sprawdź wersję: `winget --version`. Wyświetl zainstalowane programy: `winget list`.
2. Wyszukaj programy: `winget search 7zip`, `winget search vlc`, `winget search notepad++`, `winget search libreoffice`, `winget search xampp`. Wpisz do tabeli identyfikatory (Id) i źródło.
3. Sprawdź szczegóły pakietu: `winget show --id 7zip.7zip` (wydawca, licencja, adres instalatora).
4. Zainstaluj 7-Zip: `winget install --id 7zip.7zip -e` i sprawdź, że pojawił się w menu Start.
5. Sprawdź dostępne aktualizacje: `winget upgrade`, a następnie zaktualizuj wszystko: `winget upgrade --all`.

2 Skrypt instalacyjny i eksport

1. Utwórz skrypt `instaluj.ps1`, który w pętli instaluje VLC, Notepad++, LibreOffice i XAMPP (identyfikatory z tabeli) z opcjami `-e --silent --accept-package-agreements --accept-source-agreements`.
2. Uruchom skrypt: `powershell -ExecutionPolicy Bypass -File .\instaluj.ps1` i zmierz łączny czas (`Measure-Command`).
3. Wyeksportuj listę: `winget export -o C:\Skrypty\pakiety.json`. Otwórz plik i sprawdź jego strukturę.
4. Przenieś `pakiety.json` do drugiej VM lub kolegi i odtwórz zestaw: `winget import -i pakiety.json --accept-package-agreements --accept-source-agreements`. Zanotuj, które pakiety się nie zainstalowały i dlaczego.
5. Odinstaluj VLC: `winget uninstall --id VideoLAN.VLC -e`.

3 Linux — apt, snap, flatpak

1. Odśwież listę i zaktualizuj: `sudo apt update`, `apt list --upgradable`, `sudo apt upgrade`.
2. Zainstaluj VLC z apt: `sudo apt install vlc`, sprawdź `apt show vlc` (wersja, rozmiar, zależności).
3. Sprawdź snapy: `snap list`, `snap find vlc`, zainstaluj inny program jako snap (np. `sudo snap install hello-world`) i sprawdź `snap info`.
4. Dodaj Flatpak według instrukcji z flathub.org/setup (`sudo apt install flatpak`, `flatpak remote-add --if-not-exists flathub https://dl.flathub.org/repo/flathub.flatpakrepo`), zainstaluj jeden program z Flathub i porównaj rozmiar pobierania.
5. Usuń jeden program w każdym menedżerze (`apt remove`, `snap remove`, `flatpak uninstall`).

W sprawozdaniu umieść

- ☐ tabela identyfikatorów pakietów winget
- ☐ treść skryptu `instaluj.ps1` i czas jego wykonania
- ☐ fragment pliku `pakiety.json` i wynik importu na drugim komputerze
- ☐ porównanie apt, snap i flatpak (tabela)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Jakie są zalety instalacji programów przez winget w porównaniu z pobieraniem instalatorów ze stron WWW?
2. Dlaczego eksport z winget nie zawsze odtwarza wszystkie programy na innym komputerze?
3. Czym różnią się pakiety snap i flatpak od pakietów .deb instalowanych przez apt?
4. Jak menedżer pakietów pomaga technikowi utrzymać bezpieczeństwo pracowni?

Kryteria oceny

Kryterium	Punkty
Wyszukiwanie, instalacja i aktualizacja w winget	4
Działający skrypt instalacyjny z pomiarem czasu	5
Eksport i import listy pakietów	3
apt, snap, flatpak i ich porównanie	5
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Systemy do gier: Bazzite kontra Windows 11

Czas: 2 × 45 min

praca w parach na dwóch identycznych stanowiskach (A — Bazzite, B — Windows 11)

Cel: Porównanie wydajności tych samych gier i testów graficznych w dystrybucji Linux przeznaczonej do gier i w Windows 11 na tym samym sprzęcie.

Po zajęciach potrafisz:

- instaluje Bazzite na drugim dysku z obsługą Secure Boot
- uruchamia gry i testy na Linux natywnie lub przez warstwę Proton
- mierzy średni FPS i 1% low w porównywalnych warunkach
- przedstawia wyniki w tabeli i na wykresie i formułuje wnioski

Sprzęt i materiały

- dwa komputery stacjonarne o identycznej konfiguracji; na stanowisku A drugi dysk przeznaczony do wymazania (za zgodą nauczyciela)
- pendrive Ventoy z obrazem Bazzite lub osobny pendrive ≥ 16 GB
- mysz i klawiatura, słuchawki

Oprogramowanie

- **Bazzite (obraz ISO)** — wybierz wariant dla karty graficznej w stanowisku; wersja pulpitu KDE
bazzite.gg
- **Unigine Superposition (Basic) i Heaven** — darmowe, wersje Windows i Linux; Heaven:
<https://benchmark.unigine.com/heaven>
benchmark.unigine.com/superposition
- **Steam** — darmowa gra wybrana przez nauczyciela; w Bazzite preinstalowany
store.steampowered.com/about
- **MangoHud (Linux)** — nakładka FPS i rejestrowanie czasów klatek; w Bazzite wbudowana
github.com/flightsmango/MangoHud
- **MSI Afterburner z RivaTuner Statistics Server (Windows)** — nakładka i pomiar FPS, 1% low
msi.com/Landing/afterburner/graphics-cards

Przygotowanie przed zajęciami

- Sprawdź model karty graficznej (zintegrowana czy dedykowana, producent) i pobierz odpowiedni obraz Bazzite. Sprawdź sumę SHA-256 obrazu.
- Ustal z nauczycielem, który dysk na stanowisku A wolno wymazać, i zapisz jego model i pojemność.

Bezpieczeństwo

- W instalatorze Bazzite wybierz **wyłącznie drugi dysk** — rozpoznaj go po modelu i pojemności zapisanej przed zajęciami. Jeśli masz wątpliwości, wyłącz komputer i odłącz przewód SATA pierwszego dysku (przy odłączonym zasilaniu).
- Po wejściu do UEFI zmieniaj tylko kolejność rozruchu; Secure Boot zostaw włączony i zarejestruj klucz MOK zgodnie z instrukcją Bazzite.
- Nie loguj się na Steam własnym kontem z zapamiętanym hasłem na komputerze szkolnym — użyj konta wskazanego przez nauczyciela i wyloguj się po zajęciach.
- Testy obciążające trwają krótko (3–5 min) — obserwuj temperatury GPU i CPU; przy przekroczeniu 90°C przerwij test.

Przebieg zadania

1 Instalacja Bazzite (stanowisko A)

Stanowisko B w tym czasie przygotowuje Windows 11 z drugiego dysku: aktualne sterowniki GPU, Steam, benchmarki, MSI Afterburner.

1. Uruchom komputer z pendrive'a (menu rozruchu), wybierz instalator Bazzite.
2. Wybierz język i klawiaturę, a jako miejsce instalacji — drugi dysk (sprawdź model i pojemność). Zatwierdź usunięcie jego zawartości.
3. Po zakończeniu i restarcie wybierz na niebieskim ekranie „Enroll MOK” i wpisz hasło podane w instrukcji Bazzite (układ klawiatury US).
4. Zaloguj się do pulpitu, podłącz sieć i sprawdź aktualizacje (Bazzite pobiera je w tle).

2 Ustalenie warunków testu

Porównanie ma sens tylko przy identycznych ustawieniach.

1. Uzgodnij w parze: rozdzielczość, jakość grafiki, tryb pełnoekranowy, wyłączona synchronizacja pionowa. Zapisz te ustawienia.
2. Zainstaluj na obu stanowiskach Superposition (preset 1080p Medium lub niższy, jeśli sprzęt jest słaby), Heaven i grę wybraną przez nauczyciela.
3. Na Bazzite włącz nakładkę MangoHud (w grach Steam: Właściwości → Opcje uruchamiania `mangohud %command%`), na Windows — nakładkę RivaTuner.

3 Pomiary

Każdy test powtórz 2 razy i zapisz wynik lepszy lub średnią.

1. Superposition: uruchom test i zapisz wynik punktowy oraz min/średni/maks FPS z ekranu wyników.
2. Heaven: uruchom tryb Benchmark (klawisz F9 lub przycisk w menu) i zapisz średni FPS i min FPS.
3. Gra: wybierz powtarzalną scenę (np. ten sam fragment mapy), graj 2 minuty i zapisz średni FPS i 1% low z nakładki lub logu. Jeśli 1% low jest niedostępny, zapisz min FPS i zaznacz to.
4. Podczas każdego testu zanotuj maksymalną temperaturę GPU i zużycie RAM.
5. Zapisz wersje: jądra Linux (`uname -r`), sterownika GPU na obu systemach, Windows (`winver`).

4 Opracowanie

1. W arkuszu wykonaj wykres słupkowy: średni FPS i 1% low dla każdego testu, dwie serie — Bazzite i Windows.
2. Oblicz różnicę procentową średniego FPS dla każdego testu.
3. Po zajęciach (decyzja nauczyciela) przywróć stan dysku lub zostaw Bazzite do zadania 18.

W sprawozdaniu umieść

- ☐ konfiguracja sprzętu (CPU, GPU, RAM) i wersje systemów oraz sterowników
- ☐ ustalone warunki testu
- ☐ tabela wyników i wykres słupkowy
- ☐ opis instalacji Bazzite z rejestracją MOK
- ☐ wnioski: który system i dlaczego wypadł lepiej, co wpływa na wynik (sterowniki, Proton, procesy w tle)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym jest Proton i dlaczego gry przeznaczone dla Windows mogą działać na Linux?
2. Dlaczego 1% low lepiej opisuje płynność gry niż średni FPS?
3. Do czego służy rejestracja klucza MOK przy instalacji Bazzite i co by się stało bez niej przy włączonym Secure Boot?
4. Jakie gry mogą nie działać na Linux mimo Protona (np. ze względu na zabezpieczenia antycheat)?

Kryteria oceny

Kryterium	Punkty
Bezpieczna instalacja na właściwym dysku i rejestracja MOK	4
Porównywalne warunki testu i kompletne pomiary	6
Tabela i wykres	3
Wnioski	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Dobór systemu dla starszego komputera

Czas: 2 × 45 min

praca w parach

Cel: Zmierzenie zużycia zasobów przez Windows 11 i lekkie dystrybucje Linux oraz przygotowanie uzasadnionej rekomendacji systemu dla klienta ze starszym komputerem.

Po zajęciach potrafisz:

- mierzy zużycie RAM, zajętość dysku i czas startu systemu
- uruchamia dystrybucje Linux w trybie live na komputerze i laptopie bez instalacji
- ocenia płynność pracy w typowych zastosowaniach biurowych
- sprawdza zgodność komputera z wymaganiami Windows 11
- przygotowuje rekomendację dla klienta z uzasadnieniem technicznym i kosztowym

Sprzęt i materiały

- komputer stacjonarny (Windows 11 — szkolny system lub drugi dysk)
- laptop szkolny (tylko uruchomienie live z pendrive'a)
- pendrive Ventoy z obrazami Linux Mint Xfce i Ubuntu
- stoper (telefon)

Oprogramowanie

- **Linux Mint 22.3 Xfce** — lub nowsze wydanie, jeśli dostępne
linuxmint.com/download.php
- **Lubuntu (aktualne wydanie LTS)** — alternatywnie Xubuntu:
<https://xubuntu.org/download/lubuntu.me/downloads>
- **Aplikacja Kontrola kondycji komputera (PC Health Check)** — sprawdzenie zgodności z Windows 11; można też odczytać wymagania ręcznie
support.microsoft.com/windows/how-to-use-the-pc-health-check-app-9c8abd9b-03ba-4e67-81ef-36f37caa7844

Przygotowanie przed zajęciami

- Pobierz obrazy Linux Mint Xfce i Lubuntu na pendrive Ventoy i sprawdź ich sumy SHA-256.
- Przeczytaj na stronie Microsoft minimalne wymagania Windows 11 (procesor, RAM, TPM, Secure Boot) i zapisz je.

Bezpieczeństwo

- Systemy Linux uruchamiaj tylko w trybie live (bez instalacji) — na laptopie i stacjonarce nie wybieraj w menu opcji instalacji.
- W trybie live nie loguj się do prywatnych kont (poczta, media społecznościowe) — po wyłączeniu wszystko znika, ale w trakcie dane są w pamięci.
- Na laptopie zmieniaj tylko kolejność rozruchu (jednorazowe menu startowe) — nie zmieniaj innych ustawień UEFI.

Przebieg zadania

1 Pomiar Windows 11

Używaj tych samych czynności dla każdego systemu — inaczej wyniki są nieporównywalne.

1. Zmierz czas od włączenia komputera do pojawienia się pulpitu gotowego do pracy (po zalogowaniu). Powtórz 2 razy.
2. Odczekaj 2 minuty po starcie i odczytaj w Menedżerze zadań → Wydajność → Pamięć zużycie RAM oraz liczbę procesów (zakładka Procesy).
3. Odczytaj zajętość partycji systemowej (Eksplorator → Ten komputer) i rozmiar folderu `C:\Windows`.
4. Otwórz przeglądarkę z tym samym zestawem 5 stron (lista od nauczyciela) i zapisz zużycie RAM oraz subiektywną płynność (skala 1–5).
5. Uruchom Kontrolę kondycji komputera lub sprawdź ręcznie zgodność z wymaganiami Windows 11 (msinfo32: model procesora, tryb BIOS, stan Bezpiecznego rozruchu; `tpm.msc`).

2 Pomiar Linux Mint Xfce i Ubuntu (live)

System live działa z pendrive'a i część plików trzyma w RAM — uwzględnij to w ocenie.

1. Uruchom komputer z pendrive'a, wybierz Linux Mint Xfce. Zmierz czas od wyboru w menu Ventoy do pulpitu.
2. Odczekaj 2 minuty i w terminalu wykonaj `free -h` oraz `ps -e | wc -l`. Zapisz wartość „used”.
3. Otwórz Firefox z tymi samymi 5 stronami, zapisz `free -h` i oceń płynność.
4. Zapisz zajętość dysku po instalacji podaną w dokumentacji dystrybucji lub odczytaj rozmiar obrazu ISO (wartość szacunkowa — zaznacz źródło).
5. Powtórz pomiary dla Ubuntu.

3 Test na laptopie

1. Uruchom laptop z pendrive'a (jednorazowe menu startowe) z Linux Mint Xfce.
2. Sprawdź działanie: Wi-Fi, touchpad, dźwięk, regulacja jasności, kamera, wskazanie baterii. Zapisz wyniki w tabeli.
3. Wyłącz laptop i upewnij się, że uruchamia się normalnie ze swojego dysku.

4 Rekomendacja dla klienta

Klient: emerytka, komputer z 2015 r. (4 GB RAM, dysk HDD), używa przeglądarki, poczty, wideorozmów i edytora tekstu. Nauczyciel może podać inny scenariusz.

1. Na podstawie pomiarów i wymagań Windows 11 wybierz system dla klienta.
2. Zaproponuj taną modernizację, która najbardziej poprawi komfort (np. dysk SSD, RAM) — podaj orientacyjne ceny z dwóch sklepów.
3. Napisz rekomendację (5–8 zdań) językiem zrozumiałym dla klienta: co zyskuje, z czym musi się oswoić, jak długo system będzie otrzymywał aktualizacje.

W sprawozdaniu umieść

- ☐ tabela porównawcza systemów (RAM, procesy, czas startu, zajętość dysku, płynność)
- ☐ wynik sprawdzenia zgodności komputera z Windows 11
- ☐ tabela działania podzespołów laptopa w trybie live
- ☐ rekomendacja dla klienta z kosztorysem modernizacji
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego pomiar RAM w systemie live nie odpowiada dokładnie systemowi zainstalowanemu?

2. Co bardziej przyspieszy starszy komputer: lżejszy system czy wymiana HDD na SSD? Uzasadnij.
3. Dlaczego nie należy zostawiać klientowi systemu bez wsparcia (np. Windows 10), nawet jeśli działa?
4. Na co zwrócić uwagę przy przenoszeniu klienta na Linux (programy, dane, przyzwyczajenia)?

Kryteria oceny

Kryterium	Punkty
Rzetelne pomiary Windows 11	4
Pomiary obu dystrybucji live	4
Test laptopa w trybie live	3
Rekomendacja z uzasadnieniem i kosztorysem	6
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Laptop — ocena stanu i wycena serwisu

Czas: 2 × 45 min

praca w parach

Cel: Ocena stanu technicznego laptopa bez otwierania obudowy oraz przygotowanie dla klienta wyceny serwisu i rekomendacji: naprawa czy wymiana.

Po zajęciach potrafisz:

- analizuje raport baterii i wyznacza stopień jej zużycia oraz trend
- przeprowadza test termiczny z rejestrowaniem danych i przedstawia go na wykresie
- odczytuje parametry SMART dysku NVMe/SATA i przelicza ilość zapisanych danych
- sprawdza wersję BIOS i dostępność aktualizacji u producenta bez ich instalowania
- przygotowuje kosztorys naprawy i uzasadnioną decyzję naprawa/wymiana

Sprzęt i materiały

- laptop szkolny (nie wolno go otwierać) z zasilaczem
- pendrive z programami przenośnymi, słuchawki z mikrofonem (opcjonalnie)
- urządzenie do testu portów: mysz USB, monitor/projektor z HDMI (jeśli laptop ma złącze)

Oprogramowanie

- **powercfg (wbudowany)** — raport baterii /batteryreport
learn.microsoft.com/windows-hardware/design/device-experiences/powercfg-command-line-options
- **HWiNFO (portable)** — czujniki, zapis do CSV (Logging)
hwinfo.com/download
- **CrystalDiskInfo (portable)** — SMART dysku
crystalmark.info/en/software/crystaldiskinfo
- **Cinebench 2026** — obciążenie CPU
maxon.net/en/downloads/cinebench-downloads
- **Arkusze kalkulacyjne** — wykres temperatur

Przygotowanie przed zajęciami

- Zabierz wyniki zadania 20 roku 1 (raport baterii, temperatury) — posłużą do oceny trendu zużycia.
- Wgraj programy przenośne na pendrive.

Bezpieczeństwo

- Nie otwieraj obudowy laptopa i nie odkręcaj żadnych śrub.
- BIOS/UEFI tylko odczytuj. Nie instaluj aktualizacji BIOS ani sterowników — przerwana aktualizacja BIOS może trwale uszkodzić płytę.
- Test termiczny prowadź na twardej, płaskiej powierzchni z odstąpionymi otworami wentylacyjnymi; przerwij przy 95°C lub nieprzyjemnie gorącej obudowie.
- Raporty zapisuj na pendrive. Numer seryjny laptopa jest daną serwisową — nie publikuj go poza sprawozdaniem.

Przebieg zadania

1 Bateria

1. W Terminalu wykonaj `powercfg /batteryreport /output E:\bateria.html` (E: — litera pendrive'a) i otwórz raport.
2. Odczytaj pojemność projektową (Design Capacity), pojemność pełnego naładowania (Full Charge Capacity) i liczbę cykli. Oblicz zużycie: $(1 - FCC/DC) \cdot 100\%$.
3. Z sekcji „Battery capacity history” odczytaj pojemność sprzed kilku miesięcy i porównaj z wynikiem z zadania 20 roku 1. Oszacuj spadek pojemności na miesiąc.

2 Test termiczny z wykresem

Laptop podłączony do zasilacza, plan zasilania zrównoważony.

1. Uruchom HWiNFO (Sensors-only) i włącz zapis do pliku (przycisk Logging) na pendrive, plik CSV.
2. Po 1 minucie spoczynku uruchom Cinebench 2026 w trybie wielowątkowym na ok. 10 minut.
3. Zakończ test, odczekaj 2 minuty i zatrzymaj zapis. Zanotuj maksymalną temperaturę CPU, taktowanie i flagi dławienia (Thermal/Power Limit).
4. W arkuszu z pliku CSV utwórz wykres: oś X — czas, osie Y — temperatura CPU i taktowanie.

3 Dysk i BIOS

1. W CrystalDiskInfo odczytaj model, interfejs, stan zdrowia, czas pracy, liczbę uruchomień i — dla NVMe — Percentage Used oraz Data Units Written.
2. Przelicz Data Units Written na terabajty (1 jednostka = $1000 \cdot 512$ B) i porównaj z wytrzymałością TBW dysku z karty katalogowej producenta (jeśli ją znajdziesz).
3. Odczytaj wersję BIOS (`msinfo32` → Wersja/data systemu BIOS) i model laptopa. Na stronie wsparcia producenta sprawdź, jaka jest najnowsza wersja BIOS i od kiedy. Nic nie pobieraj.

4 Porty i podzespoły

1. Przetestuj każdy port USB (mysz lub pendrive), wyjście HDMI, gniazdo audio, kamerę (aplikacja Aparat), mikrofon (Ustawienia → System → Dźwięk), Wi-Fi i Bluetooth.
2. Sprawdź klawiaturę (wszystkie klawisze w Notatniku lub testerze online), touchpad, zawiasy i stan ekranu (jednolite tło w 4 kolorach).

5 Wycena i decyzja

1. Na podstawie wyników zaplanuj czynności serwisowe (np. wymiana baterii, dysku, czyszczenie układu chłodzenia z wymianą pasty).
2. Znajdź ceny części dla tego modelu w dwóch sklepach i przyjmij koszt robocizny podany przez nauczyciela.
3. Sprawdź cenę porównywalnego laptopa używanego i nowego. Napisz decyzję dla klienta: naprawa czy wymiana, z uzasadnieniem.

W sprawozdaniu umieść

- ☐ dane laptopa (model, procesor, RAM, dysk, wersja BIOS — aktualna i najnowsza)
- ☐ analiza baterii z obliczonym zużyciem i trendem
- ☐ wykres testu termicznego z opisem dławienia
- ☐ parametry SMART z przeliczeniem zapisanych danych
- ☐ tabela testu portów i podzespołów
- ☐ kosztorys i decyzja dla klienta
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Co oznacza Percentage Used w SMART dysku NVMe i czy 100% oznacza natychmiastową awarię?
2. Dlaczego bateria traci pojemność także wtedy, gdy laptop stale pracuje na zasilaczu?
3. Jakie objawy z testu termicznego wskazują na potrzebę czyszczenia układu chłodzenia?
4. Dlaczego aktualizacji BIOS nie wykonuje się „na wszelki wypadek” i jakie warunki trzeba spełnić, gdy jest potrzebna?

Kryteria oceny

Kryterium	Punkty
Analiza baterii i trendu zużycia	3
Test termiczny z wykresem i interpretacją	4
SMART dysku i sprawdzenie BIOS	3
Test portów i podzespołów	3
Kosztorys i decyzja naprawa/wymiana	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Złośliwe oprogramowanie — analiza autostartu i procesów

Czas: 2 × 45 min

praca w parach (zamiana VM: jedna osoba ukrywa wpis, druga go szuka)

Cel: Nauczenie się wyszukiwania podejrzanych programów w autostarcie, procesach i połączeniach sieciowych narzędziami Sysinternals oraz usuwania ich i sprawdzania systemu skanerami drugiej opinii.

Po zajęciach potrafisz:

- analizuje wpisy autostartu w Autoruns z weryfikacją podpisów cyfrowych i VirusTotal
- ocenia procesy w Process Explorer (drzewo, ścieżka, podpis, wydawca)
- wiąże procesy z połączeniami sieciowymi w TCPView
- wykrywa i usuwa przygotowany „podejrzany” wpis autostartu
- przeprowadza skanowanie skanerem drugiej opinii i skanowanie offline Microsoft Defender

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i VM Windows 11 z zadania 26 roku 1 (z migawką)

Oprogramowanie

- **Autoruns (Sysinternals)**
learn.microsoft.com/sysinternals/downloads/autoruns
- **Process Explorer (Sysinternals)**
learn.microsoft.com/sysinternals/downloads/process-explorer
- **TCPView (Sysinternals)**
learn.microsoft.com/sysinternals/downloads/tcpview
- **Malwarebytes Free** — skaner drugiej opinii; alternatywa: ESET Online Scanner
<https://www.eset.com/int/home/online-scanner/>
malwarebytes.com/mwb-download
- **Microsoft Defender (Zabezpieczenia Windows)** — wbudowany; skanowanie offline

Przygotowanie przed zajęciami

- Uruchom VM Windows 11 i wykonaj migawkę „przed-malware”. Wszystkie ćwiczenia wykonujesz tylko w VM.

Bezpieczeństwo

- Nie pobieraj prawdziwego złośliwego oprogramowania ani „próbek” z internetu. „Podejrzany” program to Twój własny, nieszkodliwy skrypt.
- Autoruns i Process Explorer pozwalają wyłączać i usuwać wpisy systemowe — w szkolnym systemie i na laptopach tylko przeglądaj, zmiany wykonuj wyłącznie w VM.
- Sprawdzanie w VirusTotal wysyła tylko skróty (hash) plików. Nie używaj opcji wysyłania nieznanych plików — mogą zawierać dane prywatne.
- Po zajęciach przywróć migawkę „przed-malware”.

Przebieg zadania

1 Przygotowanie „podejrzanego” autostartu

Osoba A w swojej VM. Osoba B w tym czasie odwraca się od ekranu.

1. Utwórz plik `%APPDATA%\upd.cmd` z treścią `start notepad.exe` (Notatnik: Zapisz jako, typ „Wszystkie pliki”).
2. Dodaj wpis do rejestru w Wierszu polecenia (`cmd` — w PowerShell zmienna `%APPDATA%` nie zostanie rozwinięta): `reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v Aktualizator /t REG_SZ /d "%APPDATA%\upd.cmd"`.
3. Dla chętnych drugi wpis: zadanie w Harmonogramie zadań uruchamiane przy logowaniu, o mylącej nazwie.
4. Uruchom ponownie VM i sprawdź, że po zalogowaniu otwiera się Notatnik. Zamieńcie się miejscami.

2 Analiza autostartu — Autoruns

Osoba B szuka wpisów w VM kolegi.

1. Uruchom Autoruns jako administrator. W Options → Scan Options zaznacz weryfikację podpisów (Verify code signatures) i sprawdzanie w VirusTotal.com, przeskanuj ponownie.
2. Włącz Options → Hide Microsoft Entries. Przejrzyj zakładki Logon, Scheduled Tasks i Services.
3. Znajdź podejrzany wpis: zapisz lokalizację w rejestrze, ścieżkę pliku, stan podpisu i wynik VirusTotal. Wyjaśnij, co wzbudziło podejrzenie.
4. Najpierw wyłącz wpis (odznacz pole), uruchom ponownie i sprawdź efekt. Potem usuń wpis (Delete) i plik `upd.cmd`.

3 Procesy i połączenia

1. Uruchom Process Explorer. Dodaj kolumny Verified Signer i VirusTotal (View → Select Columns lub Options). Znajdź procesy bez podpisu.
2. Uruchom ręcznie `upd.cmd` i znajdź w drzewie procesów jego łańcuch (`cmd.exe` → `notepad.exe`). Sprawdź właściwości procesu: ścieżkę, wiersz polecenia, proces nadrzędny.
3. Uruchom TCPView. Otwórz przeglądarkę i znajdź jej połączenia: adres zdalny, port, stan. Znajdź proces nasłuchujący na porcie (Listening) i ustal, czym jest.

4 Skanery drugiej opinii

1. Zainstaluj Malwarebytes Free (bez okresu próbnego wersji Premium, jeśli instalator pozwala), wykonaj skanowanie i zapisz wynik.
2. Uruchom skanowanie offline: Zabezpieczenia Windows → Ochrona przed wirusami i zagrożeniami → Opcje skanowania → skanowanie offline Microsoft Defender → Skanuj teraz. VM uruchomi się ponownie (ok. 15 min) — w tym czasie opracowuj sprawozdanie.
3. Po restarcie sprawdź wynik w Historii ochrony. Przywróć migawkę „przed-malware”.

W sprawozdaniu umieść

- ☐ opis przygotowanego wpisu (lokalizacja, treść) — przez osobę A
- ☐ zrzut Autoruns z odnalezionym wpisem i opis cech, które go zdradziły — przez osobę B
- ☐ zrzut drzewa procesów i właściwości procesu z Process Explorer
- ☐ tabela połączeń z TCPView (2–3 pozycje)
- ☐ wyniki skanowania Malwarebytes i Defender Offline
- ☐ procedura postępowania przy podejrzeniu infekcji (5–7 kroków)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Jakie cechy wpisu autostartu powinny wzbudzić podejrzenie (lokalizacja, podpis, nazwa)?
2. Dlaczego najpierw wyłącza się wpis w Autoruns, a dopiero potem go usuwa?
3. Dlaczego skanowanie offline wykrywa zagrożenia, których nie widzi zwykłe skanowanie?
4. Dlaczego nie należy instalować dwóch programów antywirusowych działających jednocześnie w czasie rzeczywistym?

Kryteria oceny

Kryterium	Punkty
Przygotowanie wpisu i poprawne usunięcie wpisu kolegi	5
Analiza Autoruns z podpisami i VirusTotal	4
Process Explorer i TCPView	4
Skanowanie drugą opinią i offline, procedura postępowania	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Process Monitor — co robi program?

Czas: 2 × 45 min

praca indywidualna

Cel: Nauczenie się śledzenia operacji plikowych i rejestru programów w Process Monitor oraz wykorzystania go do znalezienia ustawień programu i przyczyny błędu.

Po zajęciach potrafisz:

- rejestruje zdarzenia Process Monitor i zawęża je filtrami
- ustala, jakie pliki i klucze rejestru tworzy instalator programu
- znajduje miejsce, w którym program zapisuje swoje ustawienia
- diagnozuje błąd wynikający z brakującego pliku (wynik NAME NOT FOUND)
- zapisuje wyniki do plików PML i CSV

Sprzęt i materiały

- komputer stacjonarny z VM Windows 11 (zadanie 26 roku 1) z migawką lub Windows 11 na drugim dysku

Oprogramowanie

- **Process Monitor (Sysinternals)** — wymaga uprawnień administratora learn.microsoft.com/sysinternals/downloads/procmon
- **Instalator 7-Zip (64-bit)** 7-zip.org
- **Notepad++ — wersja przenośna (zip)** — pakiet .zip, bez instalacji notepad-plus-plus.org/downloads

Przygotowanie przed zajęciami

- Wykonaj migawkę VM. Pobierz do VM Process Monitor, instalator 7-Zip i paczkę zip Notepad++.

Bezpieczeństwo

- Process Monitor rejestruje bardzo dużo zdarzeń — zatrzymaj przechwytywanie (Ctrl+E), gdy nie jest potrzebne, inaczej VM zwolni i zabraknie pamięci.
- Zapisane pliki PML/CSV mogą zawierać nazwy Twoich plików, ścieżki i dane z rejestru. Nie przesyłaj ich poza sprawozdanie, a z komputera szkolnego usuń po zajęciach.
- Nie zmieniaj i nie usuwaj kluczy rejestru znalezionych w Process Monitor poza przygotowanym ćwiczeniem.

Przebieg zadania

1 Pierwsze kroki i filtr

1. Uruchom `Procmon64.exe` jako administrator. Zatrzymaj przechwytywanie (Ctrl+E) i wyczyść listę (Ctrl+X).
2. Otwórz Filter → Filter... i dodaj warunek: Process Name — is — `notepad.exe` — Include. Zatwierdź.
3. Włącz przechwytywanie, uruchom Notatnik, wpisz tekst, zapisz plik `test.txt` na pulpicie i zamknij. Zatrzymaj przechwytywanie.
4. Znajdź operacje zapisu pliku `test.txt` (Operation: CreateFile, WriteFile). Sprawdź w Tools → Process Tree, jaki proces uruchomił Notatnik.

2 Co robi instalator?

1. Zmień filtr: Process Name — begins with — `7z` (nazwa instalatora). Wyczyść listę i włącz przechwytywanie.
2. Uruchom instalator 7-Zip, zainstaluj program z ustawieniami domyślnymi i zatrzymaj przechwytywanie.
3. Dodaj filtr Operation — is — `WriteFile`, a potem zamień go na `RegSetValue`. Zapisz, w jakich katalogach powstały pliki i jakie klucze rejestru zostały utworzone (Tools → File Summary i Registry Summary pomogą).
4. Zapisz zdarzenia: File → Save → Events displayed using current filter — jako PML oraz jako CSV.

3 Gdzie program trzyma ustawienia?

1. Rozpakuj Notepad++ do `C:\Narzedzia\npp`. Ustaw filtr Process Name — is — `notepad++.exe`.
2. Włącz przechwytywanie, uruchom Notepad++, zmień jedno ustawienie (np. Ustawienia → Preferencje → motyw lub język) i zamknij program.
3. Znajdź plik, do którego zapisano ustawienia (Path contains `config.xml`). Porównaj z instalowaną wersją: gdzie zapisywałyby ustawienia (wskazówka: zmienna `%APPDATA%`)?

4 Diagnoza błędu — brakujący plik

Symulujesz program, który nie działa, bo brakuje mu pliku konfiguracyjnego.

1. Utwórz `C:\Test\ustawienia.ini` z dowolną treścią i skrypt `C:\Test\aplikacja.cmd` z treścią: `type C:\Test\ustawienia.ini || echo BLAD: program nie moze sie uruchomic` i w kolejnej linii `pause`.
2. Uruchom skrypt — działa. Zmień nazwę `ustawienia.ini` na `ustawienia.old` i uruchom ponownie — pojawia się błąd.
3. W Process Monitor ustaw filtr Process Name — is — `cmd.exe` oraz Result — is — `NAME NOT FOUND`. Uruchom skrypt i znajdź zdarzenie wskazujące brakujący plik.
4. Zamknij Notepad++, zmień nazwę jego `config.xml` i uruchom go z przechwytywaniem. Opisz, jak program poradził sobie z brakiem pliku (zdarzenia NAME NOT FOUND, a potem zapis nowego pliku). Przywróć migawkę VM.

W sprawozdaniu umieść

- ☐ zrzut filtrów i drzewa procesów
- ☐ tabela plików i kluczy rejestru utworzonych przez instalator 7-Zip
- ☐ lokalizacja ustawień Notepad++ w wersji przenośnej i instalowanej
- ☐ zrzut zdarzenia NAME NOT FOUND z diagnozą błędu
- ☐ fragment pliku CSV (kilka wierszy)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego bez filtra praca z Process Monitor jest prawie niemożliwa?
2. Co oznaczają wyniki SUCCESS, NAME NOT FOUND i ACCESS DENIED? Który z nich zwykle wskazuje problem z uprawnieniami?
3. Dlaczego wersja przenośna programu zapisuje ustawienia w swoim katalogu, a instalowana w profilu użytkownika?
4. Jak technik może wykorzystać Process Monitor, gdy program po aktualizacji przestał się uruchamiać i nie wyświetla komunikatu?

Kryteria oceny

Kryterium	Punkty
Poprawne filtry i przechwytywanie	3
Analiza instalatora — pliki i rejestr	5
Lokalizacja ustawień programu	3
Diagnoza brakującego pliku	5
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Monitor wydajności — liczniki i raporty

Czas: 2 × 45 min

praca indywidualna

Cel: Zebranie danych o wydajności komputera licznikami Monitora wydajności podczas zaplanowanego obciążenia i wskazanie na ich podstawie wąskiego gardła systemu.

Po zajęciach potrafisz:

- dodaje i interpretuje liczniki procesora, pamięci, dysku i sieci w Monitorze wydajności
- tworzy zestaw modułów zbierających dane i rejestruje przebieg obciążenia
- generuje i odczytuje raport diagnostyki systemu (perfmon /report)
- korzysta z Monitora zasobów do znalezienia procesu obciążającego zasób
- wskazuje wąskie gardło na podstawie pomiarów

Sprzęt i materiały

- komputer stacjonarny z Windows 11 na drugim dysku (konto administratora) lub VM Windows 11 z zadania 26 roku 1
- dostęp do udziału szkolnego z dużym plikiem testowym (ścieżkę podaje nauczyciel)

Oprogramowanie

- **Monitor wydajności (perfmon.msc), Monitor zasobów (resmon)** — wbudowane w Windows
- **Cinebench 2026** — obciążenie CPU maxon.net/en/downloads/cinebench-downloads
- **Arkusze kalkulacyjne** — opcjonalnie — wykres z pliku CSV

Przygotowanie przed zajęciami

- Przypomnij sobie Monitor zasobów i Menedżer zadań z zadania 22 roku 1.

Bezpieczeństwo

- Pracuj na koncie administratora tylko w Windows z drugiego dysku lub w VM — nie w szkolnym systemie.
- Zestaw modułów zbierających dane ustaw z limitem czasu (np. 10 min) — pozostawiony bez limitu zapełnia dysk plikami dziennika.
- Kopiuj z udziału tylko plik testowy wskazany przez nauczyciela; po pomiarze usuń jego kopię.

Przebieg zadania

1 Liczniki na żywo

Nazwy liczników w polskim Windows mogą różnić się od podanych w nawiasach odpowiedników angielskich.

1. Uruchom `perfmon.msc` → Narzędzia monitorowania → Monitor wydajności. Usuń licznik domyślny.
2. Dodaj liczniki (zielony plus): Procesor(_Total) → % czasu procesora (% Processor Time); Pamięć → Dostępna pamięć (MB) (Available MBytes); Dysk fizyczny(_Total) → Średnia długość kolejki dysku (Avg. Disk Queue Length) i % czasu dysku; Interfejs sieciowy → Bajty razem/s (Bytes Total/sec).
3. Zmień skalę liczników tak, aby wykresy były czytelne (Właściwości → Dane → Skala). Uruchom Cinebench na 1 minutę i obserwuj zmiany.
4. Przełącz widok na Raport (Ctrl+G) i zanotuj wartości w spoczynku.

2 Zestaw modułów zbierających dane

1. Zestawy modułów zbierających dane → Zdefiniowane przez użytkownika → prawy przycisk → Nowy → Zestaw modułów zbierających dane. Nazwa `Obciążenie-NAZWISKO`, utwórz ręcznie, zaznacz Licznik wydajności.
2. Dodaj te same liczniki co wyżej, interwał próbkowania 1 s. W ustawieniach zestawu (Właściwości → Warunek zatrzymania) ustaw czas trwania 10 minut.
3. Uruchom zestaw. Według planu: min 0–1 spoczynek; min 1–4 Cinebench; min 4–7 kopiowanie dużego pliku z udziału na dysk; min 7–9 Cinebench i kopiowanie jednocześnie; min 9–10 spoczynek. Zapisuj godziny zmian.
4. Po zakończeniu otwórz raport: Raporty → Zdefiniowane przez użytkownika → `Obciążenie-NAZWISKO`. Odczytaj wartości średnie i maksymalne. Opcjonalnie zapisz dane jako CSV (prawy przycisk na wykresie → Zapisz dane jako).

3 Monitor zasobów i raport systemu

1. Podczas ponownego kopiowania pliku otwórz `resmon` → zakładka Dysk i Sieć. Znajdź proces, który generuje ruch, i plik, do którego zapisuje.
2. Uruchom w Terminalu jako administrator `perfmon /report`. Po ok. 60 s odczytaj raport diagnostyki systemu: ostrzeżenia, sekcję Przegląd zasobów (CPU, sieć, dysk, pamięć).
3. Zapisz najważniejsze ostrzeżenia i zalecenia z raportu.

4 Interpretacja

1. Dla każdej fazy obciążenia wskaż, który zasób był najbardziej obciążony i czy był wąskim gardłem.
2. Zaproponuj modernizację lub zmianę konfiguracji, która usunęłaby wąskie gardło w fazie z jednoczesnym obciążeniem.

W sprawozdaniu umieść

- ☐ lista użytych liczników i ich znaczenie
- ☐ zrzut wykresu z zestawu modułów zbierających dane z zaznaczonymi fazami obciążenia
- ☐ tabela wartości średnich i maksymalnych w poszczególnych fazach
- ☐ wyniki z Monitora zasobów i najważniejsze ostrzeżenia z raportu systemu
- ☐ wskazanie wąskiego gardła i propozycja modernizacji
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Jakie wartości licznika % czasu procesora i długości kolejki dysku świadczą o przeciążeniu tych zasobów?
2. Dlaczego niska wartość „Dostępna pamięć (MB)” może spowolnić komputer, nawet gdy procesor nie jest obciążony?
3. Czym różni się obserwacja na żywo od zestawu modułów zbierających dane i kiedy użyć każdego z nich?
4. Jakie liczniki dodałbyś, gdyby klient zgłaszał wolne działanie serwera plików w sieci?

Kryteria oceny

Kryterium	Punkty
Poprawne liczniki i ich opis	3
Zestaw modułów zbierających dane wykonany według planu obciążenia	5
Monitor zasobów i raport systemu	3
Interpretacja wąskiego gardła i propozycja modernizacji	6
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Zużycie energii i koszty eksploatacji

Czas: 2 × 45 min

praca w parach; watomierz rotacyjnie (ok. 15 min na parę)

Cel: Zmierzenie lub oszacowanie poboru mocy komputera i laptopa w różnych stanach pracy oraz obliczenie rocznego kosztu energii pracowni i oszczędności z planów zasilania i usypiania.

Po zajęciach potrafisz:

- mierzy pobór mocy watomierzem lub szacuje go na podstawie czujników HWiNFO
- porównuje pobór mocy w stanach: bezczynność, praca biurowa, pełne obciążenie, uśpienie
- konfiguruje plany zasilania i czas usypiania oraz sprawdza dostępne stany uśpienia
- oblicza roczny koszt energii pracowni i oszczędność z usypiania
- porównuje efektywność energetyczną laptopa i komputera stacjonarnego

Sprzęt i materiały

- komputer stacjonarny (stanowisko w pracowni) i laptop szkolny
- watomierz gniazdkowy — jeden na klasę (rotacja według harmonogramu nauczyciela)
- stoper (telefon)

Oprogramowanie

- **HWiNFO (portable)** — CPU Package Power, GPU Power, moc rozładowania baterii
[hwinfo.com/download](https://www.hwinfo.com/download)
- **Cinebench 2026** — pełne obciążenie CPU
maxon.net/en/downloads/cinebench-downloads
- **powercfg (wbudowany)** — plany zasilania i stany uśpienia
learn.microsoft.com/windows-hardware/design/device-experiences/powercfg-command-line-options
- **Arkusze kalkulacyjne** — obliczenia kosztów

Przygotowanie przed zajęciami

- Znajdź na rachunku za prąd w domu lub w aktualnej taryfie sprzedawcy energii cenę 1 kWh brutto (wraz z opłatami dystrybucyjnymi). Na zajęciach nauczyciel poda cenę obowiązującą szkołę.
- Przygotuj w arkuszu tabelę stanów pracy z kolumnami na moc z watomierza i z HWiNFO.

Bezpieczeństwo

- Watomierz podłącza i odłącza się przy wyłączonym komputerze; nie podłączaj do niego listwy z wieloma urządzeniami i nie przekraczaj jego dopuszczalnego obciążenia.
- Nie dotykaj watomierza i wtyczek mokrymi rękami; nie używaj watomierza z uszkodzoną obudową.
- Laptopa nie otwieraj; zmiany planu zasilania na szkolnym komputerze przywróć do stanu wyjściowego po zajęciach.

Przebieg zadania

1 Pomiar stacjonarki

Każdy stan utrzymuj co najmniej 2 minuty i zapisuj wartość ustaloną (typową), nie chwilowy szczyt.

1. Uruchom HWiNFO (Sensors-only) i znajdź CPU Package Power oraz GPU Power (jeśli jest).
2. Bezczynność: pulpit po 2 minutach spokoju. Zapisz moc z watomierza (jeśli masz go w tej chwili) i z HWiNFO.
3. Praca biurowa: przeglądarka z 3 kartami, edytor tekstu, film w serwisie wideo. Zapisz moc.
4. Pełne obciążenie: Cinebench 2026 wielowątkowo. Zapisz moc.
5. Uśpienie i wyłączenie: tylko z watomierzem — uśpij komputer, zapisz moc; wyłącz (zamknij system) i zapisz moc w stanie wyłączonym.
6. Bez watomierza: przyjmij moc całego komputera jako sumę odczytów HWiNFO i stałej na pozostałe podzespoły ustalonej z pomiaru watomierzem na innym stanowisku (podaje nauczyciel). Zaznacz w tabeli, które wartości są szacunkiem.

2 Laptop

1. Naładuj laptop powyżej 80% i odłącz zasilacz. W HWiNFO odczytaj moc rozładowania baterii (Charge Rate / Discharge Rate) w bezczynności, pracy biurowej i pod obciążeniem.
2. Jeśli watomierz jest dostępny, zmierz pobór zasilacza laptopa przy pełnej baterii w tych samych stanach.

3 Plany zasilania i uśpienie

1. Wyświetl plany: `powercfg /list` i stany uśpienia dostępne w komputerze: `powercfg /a`. Zapisz, czy dostępne są S3 lub Modern Standby (S0) oraz hibernacja.
2. Sprawdź ustawienia usypiania: Ustawienia → System → Zasilanie i bateria → Ekran, uśpienie i hibernacja. Zapisz obecne czasy.
3. W bezczynności porównaj moc w planie „Zrównoważony” i najbardziej oszczędnym dostępnym trybie (Tryb zasilania). Przywróć ustawienia wyjściowe.

4 Koszty pracowni

Przyjmij: 16 stanowisk, 8 h pracy dziennie, 190 dni nauki w roku. Nauczyciel może podać inne założenia.

1. Oblicz energię roczną: $E \text{ [kWh]} = P \text{ [W]} \cdot t \text{ [h]} / 1000$. Przyjmij profil: 50% czasu praca biurowa, 30% bezczynność, 20% obciążenie.
2. Wariant A: komputery włączone 8 h, bez usypiania. Wariant B: usypianie po 15 min bezczynności (połowa czasu bezczynności w uśpieniu). Wariant C: komputery pozostawione włączone na noc (dodatkowe 16 h bezczynności dziennie).
3. Oblicz roczny koszt każdego wariantu i oszczędność wariantu B względem A oraz koszt wariantu C.
4. Porównaj roczny koszt energii jednego stanowiska stacjonarnego i jednego laptopa w tym samym profilu pracy.

W sprawozdaniu umieść

- ☐ tabela mocy w stanach pracy (stacjonarka i laptop) z oznaczeniem pomiarów i szacunków
- ☐ wyniki `powercfg /a` i opis ustawień usypiania
- ☐ obliczenia rocznego kosztu dla wariantów A, B, C (z wzorem i ceną kWh)
- ☐ porównanie laptop – stacjonarka
- ☐ zalecenia dla dyrekcji dotyczące oszczędzania energii w pracowni
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego odczyt CPU Package Power z HWiNFO nie jest poborem mocy całego komputera z gniazdka?
2. Czym różni się uśpienie od hibernacji pod względem poboru energii i czasu powrotu do pracy?
3. Dlaczego sprawność zasilacza wpływa na koszty eksploatacji? Co oznaczają certyfikaty 80 PLUS?
4. Dlaczego komputer „wyłączony” nadal może pobierać energię z sieci?

Kryteria oceny

Kryterium	Punkty
Pomiary stacjonarki w czterech stanach (z oznaczeniem metody)	5
Pomiary laptopa	3
Plany zasilania i stany uśpienia	3
Poprawne obliczenia kosztów wariantów A, B, C	5
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Zasady grupy i ograniczenia dla użytkowników

Czas: 2 × 45 min

praca indywidualna

Cel: Skonfigurowanie lokalnych zasad grupy i zasad zabezpieczeń w Windows 11 Pro tak, aby konto standardowe miało ograniczony dostęp do systemu, a konto administratora działało bez ograniczeń.

Po zajęciach potrafisz:

- konfiguruje zasady haseł i blokady konta w `secpol.msc` i sprawdza je poleceniem `net accounts`
- blokuje dostęp do nośników wymiennych i Panelu sterowania za pomocą zasad grupy
- stosuje zasady tylko do użytkowników niebędących administratorami
- weryfikuje zastosowane zasady poleceniami `gpupdate` i `gpresult`
- wyjaśnia różnicę między lokalnymi zasadami grupy a zasadami domenowymi w szkolnej sieci

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i maszyną wirtualną Windows 11 Pro (z zadania 26, rok 1) albo Windows 11 Pro na drugim dysku
- pendrive (do testu blokady nośników)

Oprogramowanie

- **Windows 11 Pro (VM lub drugi dysk)** — edytor zasad grupy nie występuje w wersji Home
microsoft.com/software-download/windows11
- **Oracle VirtualBox 7** — przekazywanie pendrive'a do VM: Urządzenia → USB
virtualbox.org/wiki/Downloads
- **Narzędzia wbudowane** — `gpedit.msc`, `secpol.msc`, `mmc`, `gpresult`, `gpupdate`, `net accounts`

Przygotowanie przed zajęciami

- Uruchom maszynę wirtualną Windows 11 Pro i sprawdź, że masz w niej konto administratora oraz konto standardowe `uczen` (jeśli go nie ma, utwórzysz je w kroku 1).
- Przed zajęciami wykonaj migawkę maszyny wirtualnej o nazwie „przed zasadami”.

Bezpieczeństwo

- Pracuj wyłącznie w maszynie wirtualnej lub na Windows z drugiego dysku — nie zmieniaj zasad w szkolnym systemie na pierwszym dysku.
- Ustawień z „Konfiguracji komputera” nie można wyłączyć dla administratora — przed zmianą sprawdź, kogo zasada dotyczy, żeby nie odciąć się od systemu.
- Zapisz hasła kont testowych w sprawozdaniu tylko jako „ustalone” — nie wpisuj tam swoich prawdziwych haseł.
- W razie zablokowania systemu przywróć migawkę „przed zasadami”.

Przebieg zadania

1 Konta i stan wyjściowy

Przygotowanie kont testowych i zapis domyślnych ustawień.

1. Na koncie administratora otwórz Terminal (administrator) i, jeśli trzeba, utwórz konto standardowe: `net user uczen * /add` (hasło wpiszesz dwa razy).
2. Wykonaj `net accounts` i zapisz w tabeli domyślne wartości: minimalna długość hasła, próg blokady, czas blokady.
3. Zaloguj się na konto `uczen`, sprawdź, że działają: Panel sterowania, Ustawienia, pendrive (podłącz go przez Urządzenia → USB). Wyloguj się.

2 Zasady haseł i blokady konta

Zasady zabezpieczeń dotyczą wszystkich kont na komputerze.

1. Uruchom `secpol.msc` → Zasady konta → Zasady haseł. Ustaw minimalną długość hasła na 12 znaków i włącz wymaganie złożoności.
2. Przejdź do Zasady konta → Zasady blokady konta. Ustaw próg blokady na 5 nieudanych prób i czas blokady na 5 minut.
3. Wykonaj `gpupdate /force` i ponownie `net accounts` — porównaj z wartościami wyjściowymi.
4. Spróbuj zmienić hasło konta `uczen` na krótkie (`net user uczen *`) — zanotuj komunikat.
5. Wyloguj się i 5 razy wpisz złe hasło konta `uczen`. Zrób zdjęcie komunikatu o blokadzie.

3 Ograniczenia tylko dla ucznia

Lokalne zasady dla „Użytkowników niebędących administratorami” (nazwy mogą się nieznacznie różnić — w nawiasach podano nazwy angielskie).

1. Na koncie administratora uruchom `mmc` → Plik → Dodaj/Usuń przystawkę → Edytor obiektów zasad grupy → Przeglądaj → karta Użytkownicy → „Użytkownicy niebędący administratorami” (Non-Administrators).
2. W tej przystawce: Konfiguracja użytkownika → Szablony administracyjne → Panel sterowania → włącz „Zabroń dostępu do Panelu sterowania i ustawień komputera” (Prohibit access to Control Panel and PC settings).
3. Konfiguracja użytkownika → Szablony administracyjne → System → Dostęp do magazynu wymiennego (Removable Storage Access) → włącz „Wszystkie klasy magazynu wymiennego: odmowa dostępu” (All Removable Storage classes: Deny all access).
4. Konfiguracja użytkownika → Szablony administracyjne → Pulpit → Pulpit → „Tapeta pulpitu” (Desktop Wallpaper): włącz i podaj ścieżkę do obrazu, np. `C:\Windows\Web\Wallpaper\Windows\img0.jpg`.
5. Zapisz konsolę jako `zasady_uczen.msc` na pulpicie administratora.

4 Weryfikacja

1. Zaloguj się na konto `uczen` (po upływie blokady). Sprawdź Panel sterowania, Ustawienia, pendrive i zmianę tapety. Zrób zrzuty komunikatów.
2. Na koncie `uczen` wykonaj `gpresult /r` i zapisz, jakie obiekty zasad zostały zastosowane.
3. Wróć na konto administratora i sprawdź, że jego Panel sterowania i pendrive działają normalnie.
4. Wygeneruj raport `gpresult /h C:\raport_gp.html` (jako administrator) i obejrzyj go w przeglądarce.
5. Przywróć migawkę „przed zasadami” albo wyłącz ustawione zasady (stan „Nie skonfigurowano”).

W sprawozdaniu umieść

- ☐ tabela ustawień przed i po zmianie (wyniki `net accounts`)

- ☐ lista skonfigurowanych zasad z pełną ścieżką i wynikiem testu na obu kontach
- ☐ zrzuty: blokada konta, komunikat o zablokowanym Panelu sterowania i pendrivie, fragment `gpresult /r`
- ☐ opis, jak podobne ograniczenia działają w szkolnej pracowni (zapytaj nauczyciela, czy komputery są w domenie)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różni się Konfiguracja komputera od Konfiguracji użytkownika w zasadach grupy?
2. Dlaczego ograniczenia dla ucznia ustawiono w przystawce „Użytkownicy niebędący administratorami”, a nie bezpośrednio w `gpedit.msc`?
3. Jakie zagrożenie ogranicza blokada nośników wymiennych, a jakie próg blokady konta?
4. Jak w szkole lub firmie z wieloma komputerami wdraża się zasady grupy centralnie?

Kryteria oceny

Kryterium	Punkty
Poprawnie ustawione zasady haseł i blokady konta (sprawdzone na stanowisku)	5
Ograniczenia działające tylko na koncie standardowym	6
Weryfikacja <code>gpresult</code> i komplet zrzutów	4
Opis odpowiednika w szkolnej pracowni	2
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Uprawnienia NTFS, przydziały i udziały

Czas: 2 × 45 min

praca indywidualna, test sieciowy w parach

Cel: Zaprojektowanie i sprawdzenie uprawnień do folderów firmowych: uprawnienia NTFS, uprawnienia udziału sieciowego, przydziały dyskowe i kompresja NTFS.

Po zajęciach potrafisz:

- nadaje i odbiera uprawnienia NTFS, wyłącza dziedziczenie i stosuje jawną odmowę
- zapisuje i przywraca listy ACL poleceniem `icacls`
- wyznacza uprawnienia efektywne przy dostępie lokalnym i przez sieć
- konfiguruje przydziały dyskowe i sprawdza ich działanie
- porównuje rozmiar i rozmiar na dysku plików skompresowanych NTFS

Sprzęt i materiały

- komputer stacjonarny z maszyną wirtualną Windows 11 Pro (karta sieciowa w trybie mostkowanym) albo Windows 11 Pro na drugim dysku
- laptop lub komputer sąsiada w tej samej sieci (do testu dostępu przez sieć)

Oprogramowanie

- **Windows 11 Pro** — VM z zadania 26 (rok 1) z dodatkowym dyskiem wirtualnym 2 GB microsoft.com/software-download/windowss11
- **Oracle VirtualBox 7** — Ustawienia → Pamięć → dodaj dysk; Sieć → Karta mostkowana virtualbox.org/wiki/Downloads
- **Narzędzia wbudowane** — `icacls`, `net user`, `net localgroup`, `runas`, `fsutil`, `compact`, `Get-SmbShareAccess`

Przygotowanie przed zajęciami

- Dodaj do maszyny wirtualnej nowy dysk VDI 2 GB, w Zarządzaniu dyskami zainicjuj go (GPT) i sformatuj jako NTFS z etykietą `DANE` i literą `D:` (lub inną wolną).
- Wykonaj migawkę maszyny wirtualnej.

Bezpieczeństwo

- Pracuj na dysku `DANE` w maszynie wirtualnej albo na drugim dysku fizycznym — nigdy nie zmieniaj uprawnień na dysku systemowym `C:` (np. `C:\Windows`, `C:\Users`).
- Przed każdą większą zmianą zapisz ACL poleceniem `icacls ... /save` — to Twoja kopia bezpieczeństwa.
- Udział testowy usuń po zajęciach; nie udostępniaj folderów z prawem zapisu dla „Wszyscy” w sieci szkolnej na stałe.
- Hasła kont testowych ustal tylko na czas zajęć.

Przebieg zadania

1 Konta, grupy i foldery

Wszystkie polecenia wykonuj w Terminalu uruchomionym jako administrator.

1. Utwórz konta: `net user uczen * /add` i `net user ksiegowa * /add`. Utwórz grupę `net localgroup Ksiegowosc /add` i dodaj do niej konto `ksiegowa`.
2. Utwórz foldery `D:\Firma\Wspolny`, `D:\Firma\Ksiegowosc` i plik `D:\Firma\Wspolny\regulamin.txt` z dowolną treścią.
3. Zapisz uprawnienia domyślne: `icacls D:\Firma\* /save D:\acl_przed.txt /t /c` i obejrzyj wynik `icacls D:\Firma\Ksiegowosc`.

2 Uprawnienia NTFS

S-1-5-32-544 to grupa Administratorzy, S-1-5-32-545 — Użytkownicy.

1. Folder Ksiegowosc: wyłącz dziedziczenie i nadaj dostęp tylko administratorom i grupie: `icacls D:\Firma\Ksiegowosc /inheritance:r /grant:r *S-1-5-32-544:(OI)(CI)F Ksiegowosc:(OI)(CI)M`.
2. Plik regulamin.txt: ustaw jawną odmowę zapisu dla ucznia: `icacls D:\Firma\Wspolny\regulamin.txt /deny uczen:(W)`.
3. Folder Wspolny: nadaj Użytkownikom prawo modyfikacji: `icacls D:\Firma\Wspolny /grant *S-1-5-32-545:(OI)(CI)M`.
4. Przetestuj jako uczeń: `runas /user:uczen cmd`, w nowym oknie spróbuj wejść do `D:\Firma\Ksiegowosc`, utworzyć plik w `Wspolny` i dopisać tekst do `regulamin.txt` (`echo test>>D:\Firma\Wspolny\regulamin.txt`). Powtórz jako `ksiegowa`.
5. W Eksploratorze: Właściwości folderu Ksiegowosc → Zabezpieczenia → Zaawansowane → Dostęp efektywny — sprawdź uprawnienia obu kont i zrób zrzut.
6. Zapisz ACL po zmianach (`icacls D:\Firma\* /save D:\acl_po.txt /t /c`), następnie przywróć stan wyjściowy `icacls D:\Firma /restore D:\acl_przed.txt`, sprawdź efekt i przywróć zmiany z `acl_po.txt`.

3 Udział sieciowy

Uprawnienia udziału i NTFS działają razem — obowiązuje bardziej restrykcyjne.

1. Udostępnij folder `D:\Firma` jako `Firma`: Właściwości → Udostępnianie → Udostępnianie zaawansowane → Uprawnienia: grupa „Wszyscy” tylko Odczyt.
2. Sprawdź uprawnienia udziału w PowerShell: `Get-SmbShareAccess -Name Firma`.
3. Z laptopa lub komputera sąsiada otwórz `\\<IP VM>\Firma` i zaloguj się jako `ksiegowa`. Spróbuj zapisać plik w folderze Ksiegowosc. Zanotuj wynik.
4. Zmień uprawnienie udziału dla „Wszyscy” na Zmiana i powtórz test. Porównaj z dostępem lokalnym w tabeli.

4 Przydziały i kompresja

1. Właściwości dysku D: → Przydział → Pokaż ustawienia przydziałów: włącz zarządzanie, zaznacz „Odmów miejsca na dysku użytkownikom przekraczającym limit przydziału”, limit 100 MB, poziom ostrzeżenia 80 MB.
2. Jako `uczen` (Eksplorator po przełączeniu konta lub `runas`) skopiuj do `D:\Firma\Wspolny` plik lub pliki większe niż 100 MB. Zanotuj komunikat i sprawdź Wpisy przydziałów (`fsutil quota query D:`).
3. Skompresuj folder Wspolny: `compact /c /s:D:\Firma\Wspolny`. Porównaj w Właściwościach „Rozmiar” i „Rozmiar na dysku” przed i po kompresji.
4. Usuń udział, a po wypełnieniu sprawozdania przywróć migawkę maszyny wirtualnej.

W sprawozdaniu umieść

- ☐ projekt uprawnień w tabeli (kto, który folder, jakie prawo, dziedziczone czy jawne)
- ☐ wyniki testów dostępu lokalnego i sieciowego dla obu kont
- ☐ zrzut karty „Dostęp efektywny” i fragment pliku `acl_po.txt`
- ☐ wyniki testu przydziału i porównanie rozmiarów po kompresji
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Konto ma przez grupę prawo Modyfikacja, a bezpośrednio jawną Odmowę zapisu. Co może zrobić z plikiem i dlaczego?
2. Udział daje Odczyt, NTFS daje Modyfikację. Jakie są uprawnienia efektywne przez sieć, a jakie lokalnie?
3. Po co wyłączać dziedziczenie i czym różni się opcja „Konwertuj” od „Usuń”?
4. Czy kompresja NTFS pozwala uczniowi zmieścić więcej danych w przydziale 100 MB? Sprawdź i uzasadnij.

Kryteria oceny

Kryterium	Punkty
Poprawne uprawnienia NTFS i testy na dwóch kontach	6
Zapis i przywrócenie ACL <code>icacls</code>	3
Udział sieciowy i wyznaczenie uprawnień efektywnych	4
Przydział dyskowy i kompresja	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Zdalna pomoc i zarządzanie

Czas: 2 × 45 min

praca w parach (role: pomagający i użytkownik, potem zamiana)

Cel: Skonfigurowanie bezpiecznego zdalnego dostępu do komputerów: Pulpit zdalny z NLA, pomoc zdalna przez internet oraz SSH z uwierzytelnianiem kluczem i przesyłanie plików.

Po zajęciach potrafisz:

- włącza i konfiguruje Pulpit zdalny z uwierzytelnianiem na poziomie sieci oraz ogranicza krąg użytkowników
- udziela pomocy zdalnej programem RustDesk lub Pomoc szybka
- generuje parę kluczy SSH, instaluje klucz publiczny na serwerze i wyłącza logowanie hasłem
- przesyła pliki programem WinSCP z użyciem klucza
- wyjaśnia zagrożenia związane z wystawieniem RDP do internetu

Sprzęt i materiały

- dwa komputery stacjonarne z VirtualBox: maszyna wirtualna Windows 11 Pro i Ubuntu Server (karty sieciowe w trybie mostkowanym)

Oprogramowanie

- **Podłączanie pulpitu zdalnego (`mstsc`)** — wbudowany w Windows; serwer RDP tylko w wersjach Pro, Education, Enterprise
- **RustDesk** — darmowy, open source; pobieranie z GitHub: <https://github.com/rustdesk/rustdesk/releases>
rustdesk.com
- **Pomoc szybka (Quick Assist)** — opcjonalnie — pomagający musi zalogować się kontem Microsoft
apps.microsoft.com
- **OpenSSH (klient w Windows, serwer w Ubuntu)** — `ssh`, `ssh-keygen` są wbudowane w Windows 11
ubuntu.com/server/docs
- **WinSCP** — przesyłanie plików SFTP
winscp.net/eng/download.php

Przygotowanie przed zajęciami

- Sprawdź, że obie maszyny wirtualne uruchamiają się i mają adresy IP z sieci pracowni (`ipconfig`, `ip a`). Wykonaj migawki.
- Pobierz RustDesk (wersja dla Windows, x64) i WinSCP na pendrive.

Bezpieczeństwo

- Zdalny dostęp konfiguruje tylko w maszynach wirtualnych — nie włączaj Pulpitu zdalnego ani RustDesk na stałe w szkolnym systemie.
- Nigdy nie podawaj nikomu identyfikatora i hasła RustDesk ani kodu Pomocy szybkiej poza ćwiczeniem — tak działają oszuści podający się za serwis.
- Klucz prywatny SSH (`id_ed25519`) zostaje tylko u Ciebie — nie kopiuj go na serwer ani do sprawozdania.
- Przy zmianie konfiguracji SSH nie zamykaj działającej sesji, dopóki nie sprawdzisz w drugim oknie, że logowanie kluczem działa.
- Po zajęciach wyłącz Pulpit zdalny i usuń RustDesk z VM albo przywróć migawki.

Przebieg zadania

1 Pulpit zdalny (RDP)

Na maszynie wirtualnej Windows 11 Pro partnera.

1. Partner: Ustawienia → System → Pulpit zdalny → włącz. Rozwiń ustawienia i sprawdź, że włączone jest wymaganie uwierzytelniania na poziomie sieci (NLA).
2. Partner: dodaj konto standardowe `uczen` do grupy uprawnionych: w PowerShell (administrator) `Add-LocalGroupMember -SID S-1-5-32-555 -Member uczen` (SID grupy Użytkownicy pulpitu zdalnego).
3. Ty: sprawdź dostępność portu `Test-NetConnection <IP> -Port 3389`, uruchom `mstsc`, połącz się jako `uczen`. Zrób zrzut i zanotuj, co widzi w tym czasie partner.
4. Wpisz celowo złe hasło jeden raz. Partner odszukuje w Podglądzie zdarzeń → Dzienniki systemu Windows → Zabezpieczenia zdarzenia 4624 i 4625 i zapisuje adres źródłowy.

2 Pomoc zdalna przez internet

Symulacja: „użytkownik” prosi o pomoc w zmianie ustawienia.

1. Użytkownik uruchamia RustDesk (bez instalacji) i podaje pomagającemu identyfikator i jednorazowe hasło.
2. Pomagający łączy się, zmienia u użytkownika wskazane przez nauczyciela ustawienie (np. ikonę pulpitu albo rozdzielczość) i przesyła mu plik przez okno przesyłania plików.
3. Użytkownik kończy sesję i zamyka program. Zanotujcie, jakie uprawnienia (klawiatura, schowek, pliki) można odebrać pomagającemu.
4. Opcjonalnie: powtórzcie test Pomocą szybką i porównajcie oba narzędzia w tabeli.

3 SSH z kluczem

Na Ubuntu Server partnera (z zadania 10), z Windows (komputer lub VM).

- Połącz się hasłem: `ssh <użytkownik>@<IP> serwera` i zaakceptuj odcisk klucza serwera. Zapisz go.
- Na Windows wygeneruj klucze: `ssh-keygen -t ed25519 -C "imie-nazwisko"` (ustaw hasło do klucza).
- Skopiuj klucz publiczny na serwer w PowerShell: `type $env:USERPROFILE\.ssh\id_ed25519.pub | ssh <użytkownik>@<IP> "mkdir -p ~/.ssh && chmod 700 ~/.ssh && cat >> ~/.ssh/authorized_keys && chmod 600 ~/.ssh/authorized_keys"`.
- Sprawdź logowanie kluczem (system pyta o hasło do klucza, nie do konta).
- Na serwerze utwórz `sudo nano /etc/ssh/sshd_config.d/10-tylko-klucze.conf` z liniami `PasswordAuthentication no` i `KbdInteractiveAuthentication no`. Sprawdź `sudo sshd -t` i `sudo sshd -T | grep -i passwordauthentication`, potem `sudo systemctl restart ssh`.
- W nowym oknie spróbuj zalogować się bez klucza: `ssh -o PubkeyAuthentication=no <użytkownik>@<IP>` — oczekiwany wynik: `Permission denied (publickey)`.

4 Przesyłanie plików WinSCP

- W WinSCP utwórz sesję SFTP do serwera. W Zaawansowane → SSH → Uwierzytelnianie wskaż plik klucza prywatnego (WinSCP zaproponuje konwersję do formatu .ppk — zgódź się).
- Prześlij na serwer plik tekstowy, a z serwera pobierz `/etc/os-release`. Zrób zrzut okna WinSCP.
- Wyłącz Pulpit zdalny w VM Windows i zamknij RustDesk.

W sprawozdaniu umieść

- ☐ zrzuty: połączenie RDP, zdarzenia 4624/4625, sesja RustDesk, odmowa logowania hasłem SSH, okno WinSCP
- ☐ tabela porównania narzędzi zdalnego dostępu
- ☐ zawartość pliku `10-tylko-klucze.conf` i wynik `sshd -T`
- ☐ krótka notatka: zasady bezpiecznej pomocy zdalnej dla użytkownika (3–5 punktów)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

- Dlaczego nie należy udostępniać portu 3389 (RDP) bezpośrednio do internetu i jak bezpiecznie dać pracownikowi dostęp z domu?
- Co daje uwierzytelnianie na poziomie sieci (NLA)?
- Dlaczego logowanie kluczem SSH jest bezpieczniejsze od hasła i co się stanie, gdy ktoś ukradnie klucz prywatny bez hasła?
- Czym różni się RDP (osobna sesja) od pomocy zdalnej typu RustDesk/Pomoc szybka (wspólny ekran) i kiedy wybrać każde z nich?

Kryteria oceny

Kryterium	Punkty
RDP z NLA, uprawnienia i analiza dziennika zdarzeń	5
Sesja pomocy zdalnej i porównanie narzędzi	3
SSH z kluczem i wyłączone logowanie hasłem (sprawdzone na stanowisku)	6
Przesyłanie plików WinSCP	2
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Docker na Ubuntu Server

Czas: 2 × 45 min

praca indywidualna

Cel: Zainstalowanie Docker Engine z oficjalnego repozytorium, uruchomienie kontenerów z mapowaniem portów i wolumenami oraz porównanie kontenerów z maszynami wirtualnymi.

Po zajęciach potrafisz:

- instaluje Docker Engine i wtyczkę Compose z oficjalnego repozytorium Dockera
- uruchamia kontener z mapowaniem portu i katalogiem podpiętym z hosta
- wdraża aplikację z pliku `compose.yaml` z trwałym wolumenem
- diagnozuje kontenery poleceniami `docker ps`, `docker logs`, `docker stats`
- aktualizuje kontener bez utraty danych i porównuje kontener z maszyną wirtualną

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i maszyną wirtualną Ubuntu Server LTS (z zadania 10): min. 2 rdzenie, 2 GB RAM, 20 GB dysku, karta sieciowa w trybie mostkowanym

Oprogramowanie

- **Docker Engine (instrukcja dla Ubuntu)** — metoda „Install using the apt repository” docs.docker.com/engine/install/ubuntu
- **Uptime Kuma** — obraz `louislam/uptime-kuma:2`, port 3001 github.com/louislam/uptime-kuma
- **Obraz nginx (Docker Hub)** — oficjalny obraz serwera WWW hub.docker.com/_/nginx
- **Klient SSH (Terminal Windows)** — praca na serwerze przez SSH ułatwia kopiowanie poleceń

Przygotowanie przed zajęciami

- Uruchom VM Ubuntu Server, zaktualizuj system (`sudo apt update && sudo apt full-upgrade`) i wykonaj migawkę „przed dockerem”.
- Przeczytaj na stronie Dockera akapit o usuwaniu pakietów konfliktowych (Uninstall old versions).

Bezpieczeństwo

- Instaluj Dockera tylko w maszynie wirtualnej. Polecenia kopiuj wyłącznie z oficjalnej dokumentacji docs.docker.com.
- Przynależność do grupy `docker` daje w praktyce uprawnienia administratora (root) — dodawaj do niej tylko zaufanych użytkowników.
- Używaj tylko obrazów oficjalnych lub od znanych autorów; sprawdź na Docker Hub, kto publikuje obraz.
- Nie wystawiaj paneli administracyjnych kontenerów poza sieć pracowni; po utworzeniu konta w Uptime Kuma ustaw silne hasło.

Przebieg zadania

1 Instalacja Docker Engine

Wykonuj polecenia z oficjalnej instrukcji i zapisuj je w sprawozdaniu.

1. Usuń ewentualne pakiety konfliktowe zgodnie z dokumentacją (np. `docker.io`, `docker-compose`, `podman-docker`).
2. Dodaj klucz GPG Dockera do `/etc/apt/keyrings/docker.asc` i plik repozytorium `/etc/apt/sources.list.d/docker.sources` dokładnie według instrukcji, następnie `sudo apt update`.
3. Zainstaluj pakiety: `sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin docker-compose-plugin`.
4. Sprawdź `sudo systemctl status docker`, `docker --version`, `docker compose version` i uruchom `sudo docker run hello-world`. Przeczytaj, co wypisał kontener.
5. Dodaj się do grupy: `sudo usermod -aG docker $USER`, wyloguj się i zaloguj ponownie; `docker ps` działa bez `sudo`.

2 Serwer WWW w kontenerze

1. Utwórz katalog `~/www` z plikiem `index.html` zawierającym Twoje imię i nazwisko.
2. Uruchom: `docker run -d --name www -p 8080:80 -v ~/www:/usr/share/nginx/html:ro nginx:stable`.
3. Otwórz w przeglądarce na komputerze `http://<IP VM>:8080`. Zmień plik `index.html` na serwerze i odśwież stronę.
4. Sprawdź `docker ps`, `docker logs www` (widać Twoje żądania) i `docker exec -it www sh -c "cat /etc/os-release"` — porównaj system w kontenerze z systemem VM.

3 Aplikacja z docker compose

Uptime Kuma przyda się w zadaniu 28.

1. Utwórz katalog `~/kuma` i w nim plik `compose.yaml` z usługą: obraz `louislam/uptime-kuma:2`, `restart: unless-stopped`, port `3001:3001`, wolumen nazwany `kuma-data` zamontowany w `/app/data`.
2. Uruchom `docker compose up -d`, sprawdź `docker compose ps` i `docker compose logs --tail 20`.
3. Otwórz `http://<IP VM>:3001`, utwórz konto administratora i dodaj monitor HTTP strony nginx z kroku 2.
4. Sprawdź trwałość danych: `docker compose down`, potem `docker compose up -d` — monitor nadal istnieje. Odszukaj wolumen: `docker volume ls`, `docker volume inspect`.

4 Aktualizacja i porównanie z VM

1. Zaktualizuj aplikację: `docker compose pull`, `docker compose up -d`, a następnie `docker image prune`. Sprawdź, że dane zostały.
2. Uruchom `docker stats --no-stream` i zapisz zużycie RAM kontenerów. Porównaj z `free -h` całej VM i z rozmiarem obrazów (`docker images`).
3. Zatrzymaj i usuń kontener nginx: `docker rm -f www`. Kontener Uptime Kuma zostaw — będzie potrzebny w zadaniu 28.

W sprawozdaniu umieść

- ☐ lista wykonanych poleceń instalacji i wynik `docker run hello-world`
- ☐ zawartość pliku `compose.yaml`
- ☐ zrzuty: strona z nginx, panel Uptime Kuma, wynik `docker stats --no-stream`
- ☐ tabela porównania: kontener a maszyna wirtualna
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różni się obraz od kontenera i co dzieje się z danymi w kontenerze po `docker rm`, jeśli nie użyto wolumenu?
2. Co oznacza zapis `-p 8080:80` i `-v ~/www:/usr/share/nginx/html:ro`?
3. Dlaczego kontener zużywa mniej zasobów niż maszyna wirtualna i czego kontener nie zapewnia (np. inny system operacyjny, izolacja jądra)?
4. Dlaczego nie instaluje się Dockera skryptem znalezionym na przypadkowym blogu?

Kryteria oceny

Kryterium	Punkty
Instalacja z oficjalnego repozytorium i weryfikacja	5
Kontener nginx z mapowaniem portu i katalogu	4
Uptime Kuma w docker compose z trwałym wolumenem	5
Aktualizacja i porównanie kontener — VM	3
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Monitorowanie komputerów w pracowni

Czas: 2 × 45 min

praca w parach

Cel: Zbudowanie prostego systemu monitorowania dostępności komputerów i usług, przetestowanie powiadomień na symulowanej awarii i opracowanie procedury reakcji na awarię.

Po zajęciach potrafisz:

- konfiguruje monitory typu ping, port TCP i HTTP w Uptime Kuma
- tworzy stronę stanu usług i konfiguruje powiadomienie
- symuluje awarię usługi, mierzy czas wykrycia i przywraca działanie
- odczytuje bieżące obciążenie serwera w Glances
- opracowuje procedurę reakcji na awarię

Sprzęt i materiały

- komputer stacjonarny z VM Ubuntu Server (z zadań 10–12 i 27; tryb mostkowany)
- maszyna wirtualna Windows 11 lub komputer partnera jako monitorowane urządzenie
- telefon (opcjonalnie — odbiór powiadomień)

Oprogramowanie

- **Uptime Kuma** — kontener z zadania 27, panel `http://<IP VM>:3001`
github.com/louislam/uptime-kuma
- **Glances** — `sudo apt install glances`;
tryb WWW: `glances -w`
github.com/nicolargo/glances
- **ntfy** — **opcjonalnie** — powiadomienia na telefon; aplikacja Android/iOS, bez zakładania konta
ntfy.sh
- **Netdata** — **opcjonalnie** — rozbudowane wykresy wydajności; dla chętnych
netdata.cloud

Przygotowanie przed zajęciami

- Sprawdź, że w VM Ubuntu Server działa kontener Uptime Kuma (`docker compose ps` w `~/kuma`) oraz usługi `ssh`, `smbd` i Jellyfin (jeśli instalowałeś go w zadaniu 12).
- Zapisz adresy IP: VM Ubuntu Server, VM Windows lub komputera partnera.

Bezpieczeństwo

- Monitoruj tylko własne maszyny wirtualne i komputer partnera za jego zgodą — skanowanie i odpytywanie cudzych urządzeń w sieci szkolnej jest zabronione.
- Regułę zapory zezwalającą na ping włączaj tylko w maszynie wirtualnej.
- W ntfy publiczny temat może odczytać każdy, kto zna jego nazwę — wybierz trudną do odgadnięcia nazwę i nie wysyłaj w powiadomieniach haseł ani adresów spoza pracowni.
- Awarię symuluj tylko zatrzymaniem usługi w swojej VM — nie wyłączaj sprzętu sieciowego ani serwera szkolnego.

Przebieg zadania

1 Monitory w Uptime Kuma

1. W VM Windows włącz odpowiedź na ping: w PowerShell (administrator) `Enable-NetFirewallRule -Name FPS-ICMP4-ERQ-In`.
2. Dodaj monitor „Ping” dla VM Windows (lub komputera partnera) z interwałem 20 s.
3. Dodaj monitory „Port TCP”: SSH (22) i Samba (445) na VM Ubuntu Server, oraz monitor HTTP Jellyfin `http://<IP VM>:8096` (jeśli działa).
4. Dla każdego monitora ustaw liczbę ponowień przed zgłoszeniem awarii na 1. Zanotuj konfigurację w tabeli.

2 Strona stanu i powiadomienia

1. Utwórz stronę stanu (Strony statusu → Nowa) o nazwie „Pracownia — stanowisko <nr>” i dodaj do niej wszystkie monitory.
2. Skonfiguruj powiadomienie: ntfy (temat o trudnej nazwie, aplikacja na telefonie) albo kanał wskazany przez nauczyciela. Przypisz je do wszystkich monitorów.
3. Wyślij powiadomienie testowe przyciskiem „Test” i zrób zrzut odebranej wiadomości.
4. Wstrzymaj na chwilę jeden monitor (Pauza) i sprawdź, jak zmienia się strona stanu; wznów monitor.

3 Symulacja awarii

Partner zatrzymuje usługę, a Ty wykrywasz awarię tylko na podstawie monitoringu.

1. Partner zapisuje godzinę i zatrzymuje jedną usługę, np. `sudo systemctl stop smbd`, nie mówiąc której.
2. Zapisz godzinę powiadomienia i oblicz czas wykrycia. Na podstawie panelu ustal, która usługa nie działa.
3. Zaloguj się przez SSH, sprawdź `systemctl status smbd` i `journalctl -u smbd --since "10 min ago"`, uruchom usługę i potwierdź powrót do stanu „Up”.
4. Powtórz scenariusz z zamianą ról: wyłączenie VM Windows lub odłączenie jej karty sieciowej (Urządzenia → Sieć).

4 Zasoby serwera i procedura

1. Zainstaluj Glances (`sudo apt install glances`) i uruchom go w terminalu. Odczytaj obciążenie CPU, RAM, dysku i najbardziej obciążający proces.
2. Opcjonalnie uruchom tryb WWW `glances -w` i otwórz `http://<IP VM>:61208`. Zakończ go klawiszami Ctrl+C.
3. Napisz procedurę reakcji na awarię (wykrycie → ocena → powiadomienie → diagnoza → naprawa → weryfikacja → wpis do dziennika) dla jednej z monitorowanych usług.

W sprawozdaniu umieść

- ☐ tabela monitorów z typem, adresem, portem i interwałem
- ☐ zrzuty: strona stanu, powiadomienie testowe, monitor w stanie „Down” i ponownie „Up”
- ☐ przebieg dwóch symulacji awarii z czasem wykrycia
- ☐ procedura reakcji na awarię
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego udany ping do serwera nie oznacza, że działa udział Samba lub serwer Jellyfin?
2. Od czego zależy czas wykrycia awarii i dlaczego zbyt krótki interwał i brak ponowień mogą dawać fałszywe alarmy?

3. Co się stanie z monitoringiem, gdy awarii ulegnie sam serwer z Uptime Kuma? Jak temu zaradzić?
4. Jakie informacje powinien zawierać wpis w dzienniku awarii?

Kryteria oceny

Kryterium	Punkty
Poprawnie skonfigurowane monitory (min. 4, trzy typy)	5
Strona stanu i działające powiadomienie	3
Dwie symulacje awarii z diagnozą i czasem wykrycia	5
Procedura reakcji na awarię	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Inwentaryzacja i helpdesk — GLPI

Czas: 2 × 45 min

praca indywidualna

Cel: Uruchomienie systemu GLPI w kontenerach, wprowadzenie sprzętu pracowni do inwentarza oraz obsłużenie zgłoszenia serwisowego od utworzenia do zamknięcia.

Po zajęciach potrafisz:

- uruchamia aplikację wielokontenerową (GLPI + MariaDB) w docker compose
- zabezpiecza nową instalację, zmieniając domyślne hasła kont
- dodaje komputery do inwentarza ręcznie i agentem GLPI
- obsługuje zgłoszenie w roli użytkownika, administratora i technika
- odczytuje historię zmian zasobu i zgłoszenia

Sprzęt i materiały

- komputer stacjonarny z VM Ubuntu Server z Dockerem (z zadania 27): min. 2 GB RAM, tryb mostkowany
- maszyna wirtualna Windows 11 (do instalacji agenta)
- karta inwentaryzacyjna komputera z zadania 2 (rok 1)

Oprogramowanie

- **GLPI — instrukcja uruchomienia w Dockerze** — obraz `glpi/glpi`
help.glpi-project.org/tutorials/procedures/running_glpi_on_docker
- **MariaDB (obraz Docker)** — np. `mariadb:11.4` (wersja LTS)
hub.docker.com/_/mariadb
- **GLPI Agent** — instalator MSI dla Windows x64
github.com/glpi-project/glpi-agent/releases

Przygotowanie przed zajęciami

- Wykonaj migawkę VM Ubuntu Server. Sprawdź, że port 8080 jest wolny (kontener nginx z zadania 27 został usunięty).
- Przynieś kartę inwentaryzacyjną z zadania 2 (rok 1).

Bezpieczeństwo

- GLPI tworzy konta z hasłami domyślnymi (`glpi`, `tech`, `normal`, `post-only`) — zmień je zaraz po pierwszym logowaniu.
- Hasła bazy danych trzymaj w pliku `.env` z uprawnieniami `chmod 600` i nie wklejaj ich do sprawozdania.
- Agentu GLPI instaluj tylko w maszynie wirtualnej, nie w szkolnym systemie — wysyła on pełny spis sprzętu i oprogramowania.
- W zgłoszeniach nie wpisuj danych osobowych prawdziwych osób — używaj fikcyjnych.

Przebieg zadania

1 Uruchomienie GLPI

W katalogu `~/glpi` na VM Ubuntu Server.

1. Utwórz plik `.env` z liniami `GLPI_DB_HOST=db`, `GLPI_DB_PORT=3306`, `GLPI_DB_NAME=glpi`, `GLPI_DB_USER=glpi`, `GLPI_DB_PASSWORD=<własne hasło>` i nadaj mu `chmod 600`.
2. Utwórz `compose.yaml` z dwiema usługami: `db` (obraz `mariadb:11.4`, zmienne `MARIADB_RANDOM_ROOT_PASSWORD: "yes"`, `MARIADB_DATABASE`, `MARIADB_USER`, `MARIADB_PASSWORD` z pliku `.env`, wolumen `db_data:/var/lib/mysql`) oraz `glpi` (obraz `glpi/glpi:latest`, `env_file: .env`, `depends_on: [db]`, port `8080:80`, wolumen `glpi_data:/var/glpi`). Wzoruj się na instrukcji GLPI.
3. Uruchom `docker compose up -d` i obserwuj `docker compose logs -f glpi` aż do zakończenia automatycznej instalacji (kilka minut).
4. Zaloguj się na `http://<IP VM>:8080` jako `glpi / glpi`. Zmień hasła czterech kont domyślnych (komunikat na stronie głównej wskaże, które jeszcze mają hasło domyślne). Zapisz wersję GLPI.
5. Sprawdź `docker compose ps` — oba kontenery mają stan „running”. Zapisz, którego portu bazy danych nie wystawiono na zewnątrz i dlaczego to dobrze.

2 Inwentarz

1. Dodaj lokalizację: Ustawienia → Listy rozwijane → Lokalizacje → „Pracownia <nr sali>”.
2. Dodaj ręcznie komputer z karty inwentaryzacyjnej: Zasoby → Komputery → Dodaj (nazwa, producent, model, numer seryjny, lokalizacja). Dodaj komponenty: procesor, pamięć, dysk oraz monitor jako osobny zasób połączony z komputerem.
3. Włącz inwentaryzację: Administracja → Inwentarz → zaznacz włączenie inwentarza i zapisz.
4. W VM Windows zainstaluj GLPI Agent; w kreatorze podaj adres serwera `http://<IP VM>:8080/`. Otwórz `http://127.0.0.1:62354` i wymuś inwentaryzację.
5. Sprawdź w GLPI nowy komputer, porównaj dane z danymi wpisanymi ręcznie i zanotuj, co agent zebrał dodatkowo (np. oprogramowanie).

3 Zgłoszenie serwisowe

Przelogowuj się między kontami albo użyj okna prywatnego przeglądarki.

1. Jako `post-only` utwórz zgłoszenie: „Stanowisko <nr>: komputer nie uruchamia się, słychać sygnały dźwiękowe”, powiązane z komputerem z inwentarza.
2. Jako `glpi` przypisz zgłoszenie technikowi `tech`, ustaw pilność i kategorię.
3. Jako `tech` dodaj kontynuację (pytanie do użytkownika), zadanie z czasem pracy 30 min i rozwiązanie (np. „Dociśnięto moduł RAM, test pamięci bez błędów”).
4. Jako `post-only` zatwierdź rozwiązanie — zgłoszenie przechodzi w stan Zamknięte.
5. Otwórz kartę Historia zgłoszenia i komputera. Zrób zrzuty.

W sprawozdaniu umieść

- ☐ zawartość pliku `compose.yaml` (bez haseł) i wersja GLPI
- ☐ zrzuty: lista komputerów z dwoma wpisami (ręcznym i z agenta), karta komputera z komponentami
- ☐ porównanie danych z inwentarza ręcznego i agenta
- ☐ przebieg zgłoszenia: zrzut osi czasu i historii
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Jakie korzyści daje szkole lub firmie centralny inwentarz sprzętu w porównaniu z arkuszem kalkulacyjnym?
2. Czym różnią się profile Self-Service, Technician i Super-Admin w GLPI?
3. Dlaczego baza danych działa w osobnym kontenerze z własnym wolumenem i co trzeba uwzględnić w kopii zapasowej GLPI?
4. Jakie informacje powinno zawierać dobrze opisane zgłoszenie usterki?

Kryteria oceny

Kryterium	Punkty
GLPI i MariaDB uruchomione w docker compose, zmienione hasła domyślne	5
Komputer dodany ręcznie z komponentami i lokalizacją	4
Komputer zinwentaryzowany agentem i porównanie danych	3
Pełna obsługa zgłoszenia w trzech rolach	5
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Bezpieczne usuwanie danych i utylizacja

Czas: 2 × 45 min

praca indywidualna

Cel: Sprawdzenie w praktyce, które metody usuwania danych pozwalają je odzyskać, a które je niszczą, oraz przygotowanie protokołu zniszczenia danych przed przekazaniem sprzętu do utylizacji.

Po zajęciach potrafisz:

- odzyskuje usunięte pliki programem PhotoRec i ocenia skuteczność odzysku
- nadpisuje wolne miejsce (`cipher /w`) i cały dysk (`diskpart clean all` , `nwipe`)
- wyjaśnia, dlaczego na dyskach SSD stosuje się Secure Erase lub Sanitize zamiast nadpisywania
- sporządza protokół zniszczenia danych zgodny z zasadami RODO
- wskazuje prawidłową drogę utylizacji zużytego sprzętu (WEEE)

Sprzęt i materiały

- komputer stacjonarny z VirtualBox i maszyną wirtualną Windows 11
- pendrive z Ventoy (tylko jako źródło obrazu ShredOS — nie jest wymazywany)

Oprogramowanie

- **TestDisk & PhotoRec** — wersja dla Windows; `qphotorec_win.exe` ma interfejs graficzny
cgsecurity.org/wiki/TestDisk_Download
- **ShredOS (nwipe)** — obraz .iso — do VM lub na pendrive z Ventoy
github.com/PartialVolume/shredos.x86_64/releases
- **Narzędzia wbudowane Windows** — `cipher` , `diskpart` , Zarządzanie dyskami
- **NIST SP 800-88 rev. 2 (wytyczne usuwania danych)** — metody Clear, Purge, Destroy
csrc.nist.gov/pubs/sp/800/88/r2/final

Przygotowanie przed zajęciami

- Dodaj do VM Windows 11 dwa nowe dyski VDI po 1 GB. W Zarządzaniu dyskami utwórz na nich woluminy NTFS z etykietami `TEST1` i `TEST2`.
- Przygotuj zestaw plików testowych: po 3 pliki jpg, docx (lub pdf) i txt — bez danych osobowych.
- Pobierz PhotoRec (Windows) i obraz ShredOS (.iso).

Bezpieczeństwo

- `diskpart clean all` i `nwipe` nieodwracalnie niszczą cały wybrany dysk. Przed wykonaniem sprawdź `detail disk` (rozmiar 1 GB, etykieta TEST) i pokaż ekran nauczycielowi.
- W ShredOS wybieraj wyłącznie dysk testowy — nigdy dysk systemowy, pendrive z Ventoy ani pierwszy dysk komputera.
- Wymazywanie drugiego dysku fizycznego w ShredOS tylko za zgodą nauczyciela i po odłączeniu pierwszego dysku (kabel SATA przy wyłączonym zasilaniu).
- Pliki odzyskane zapisuj na dysk `C:` maszyny wirtualnej, nigdy na dysk, z którego odzyskujesz.
- Nie odzyskuj danych z cudzych nośników — dotyczy to także pendrive'ów znalezionych w pracowni.

Przebieg zadania

1 Scenariusz 1 — zwykłe usunięcie

Na woluminie TEST1.

1. Skopiuj pliki testowe na TEST1. Zapisz ich liczbę i rozmiar.
2. Usuń je klawiszami Shift+Delete, a następnie wykonaj szybkie formatowanie woluminu TEST1.
3. Uruchom `qphotorec_win.exe` jako administrator, wybierz dysk 1 GB (TEST1), system plików Other/NTFS, przeszukiwanie całego woluminu, folder docelowy `C:\odzysk1`.
4. Policz odzyskane pliki każdego typu i otwórz po jednym — oceń, czy są kompletne. Zwróć uwagę, że nazwy plików nie zostały odzyskane.

2 Scenariusz 2 — nadpisanie wolnego miejsca

Na woluminie TEST2.

1. Skopiuj pliki testowe na TEST2 i usuń je (Shift+Delete).
2. Nadpisz wolne miejsce: `cipher /w:<litera TEST2>:\` w Terminalu (administrator). Zanotuj czas działania i co wypisuje program.
3. Uruchom PhotoRec na TEST2 (folder `C:\odzysk2`) i porównaj wynik ze scenariuszem 1.

3 Scenariusz 3 — wymazanie całego dysku

Ponownie na dysku TEST1.

1. Skopiuj pliki testowe na TEST1 jeszcze raz. Uruchom `diskpart`, wykonaj `list disk`, `select disk <nr dysku 1 GB>`, `detail disk` — pokaż ekran nauczycielowi.
2. Wykonaj `clean all` i zanotuj czas. Sprawdź dysk w Zarządzaniu dyskami.
3. Uruchom PhotoRec na tym dysku (folder `C:\odzysk3`) i zapisz wynik.
4. Opcjonalnie: wyłącz VM, w VirtualBox zamontuj obraz ShredOS jako napęd optyczny i uruchom z niego VM. W `nwipe` zaznacz tylko dysk TEST2 (1 GB), wybierz metodę i weryfikację, uruchom wymazywanie i zrób zdjęcie podsumowania.

4 Dyski SSD, protokół i utylizacja

Część teoretyczna na podstawie wytycznych NIST SP 800-88 i dokumentacji producenta dysku SSD z Twojego stanowiska.

1. Sprawdź na stronie producenta dysku SSD (lub dysku z laptopa), jakim narzędziem wykonuje się Secure Erase/Sanitize. Zapisz nazwę narzędzia i warunki (np. odblokowanie dysku, zasilanie).
2. Przyporządkuj metody z zajęć do kategorii Clear, Purge, Destroy.
3. Wypełnij protokół zniszczenia danych dla fikcyjnego komputera księgowości przekazywanego do utylizacji.
4. Sprawdź, gdzie w Twojej gminie można oddać zużyty sprzęt elektroniczny (punkt selektywnej zbiórki, sklep przy zakupie nowego) i zapisz źródło.

W sprawozdaniu umieść

- ☐ tabela wyników trzech scenariuszy (pliki usunięte, odzyskane, kompletne)
- ☐ zrzuty: wynik PhotoRec, praca `cipher /w`, ekran `detail disk` przed `clean all`
- ☐ przyporządkowanie metod do kategorii NIST oraz opis metody dla SSD
- ☐ wypełniony protokół zniszczenia danych
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego po usunięciu pliku i szybkim formatowaniu dane nadal da się odzyskać?
2. Dlaczego wielokrotne nadpisywanie nie jest pewną metodą dla dysków SSD i pendrive'ów, a co robi polecenie Sanitize?
3. Czym różni się `cipher /w` od `diskpart clean all` — kiedy użyć każdego z nich?
4. Jakie obowiązki wynikają z RODO, gdy szkoła lub firma pozbywa się komputera z danymi osobowymi?

Kryteria oceny

Kryterium	Punkty
Trzy scenariusze wykonane bezpiecznie (właściwy dysk, sprawdzone przez nauczyciela)	6
Rzetelna tabela wyników i porównanie skuteczności	4
Kategorie NIST i metoda dla SSD	3
Protokół zniszczenia danych i utylizacja	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Systemy plików w praktyce: NTFS, ext4, exFAT, Btrfs

Czas: 2 × 45 min

praca indywidualna

Cel: Porównanie w praktyce funkcji systemów plików NTFS, exFAT, ext4 i Btrfs: dowiązań, atrybutów, kompresji, migawek, kronikowania, wydajności dla wielu małych plików i dostępu z innego systemu operacyjnego.

Po zajęciach potrafisz:

- tworzy i formatuje woluminy NTFS, exFAT, ext4 i Btrfs na dyskach wirtualnych
- tworzy dowiązania symboliczne i twarde w Windows (`mklink`) i Linux (`ln`)
- wykonuje migawkę Btrfs i przywraca z niej usunięty plik
- mierzy czas zapisu wielu małych plików i porównuje wyniki
- sprawdza dostęp do NTFS i exFAT z Linuksa oraz do ext4 z Windows

Sprzęt i materiały

- komputer stacjonarny z VirtualBox, maszyną wirtualną Windows 11 i maszyną wirtualną Ubuntu Server LTS (z zadania 10)

Oprogramowanie

- **Oracle VirtualBox 7** — Narzędzia → Nośniki → Utwórz (format VHD lub VDI)
[virtualbox.org/wiki/Downloads](https://www.virtualbox.org/wiki/Downloads)
- **btrfs-progs (Ubuntu)** — `sudo apt install btrfs-progs`
btrfs.readthedocs.io
- **Narzędzia wbudowane** — Windows: `mklink`, `attrib`, `compact`, `fsutil`, PowerShell; Linux: `mkfs`, `ln`, `lsblk`, `dumpe2fs`
- **DiskInternals Linux Reader** — **opcjonalnie** — odczyt ext4 w Windows; przed instalacją sprawdź warunki licencji wersji darmowej
diskinternals.com/linux-reader

Przygotowanie przed zajęciami

- W VirtualBox utwórz dysk `wspólny.vhd` 1 GB (format VHD) i podłącz go do VM Windows. Do VM Ubuntu Server podłącz dwa nowe dyski VDI po 1 GB.
- Wykonaj migawki obu maszyn wirtualnych.

Bezpieczeństwo

- Formatuj wyłącznie nowe dyski 1 GB. W Linuksie przed `mkfs` zawsze sprawdź `lsblk` — nazwy (`/dev/sdb`, `/dev/sdc`) zależą od kolejności podłączenia.
- Nagłe wyłączenie zasilania testuj tylko w maszynie wirtualnej — na prawdziwym komputerze grozi utratą danych.
- Gdy Windows zaproponuje sformatowanie dysku z ext4, wybierz Anuluj.
- Dysku nie podłączaj do dwóch maszyn jednocześnie — przełączaj go przy wyłączonych VM.

Przebieg zadania

1 Windows: NTFS i exFAT

Na dysku `wspolny.vhd` w VM Windows (Terminal jako administrator).

1. W Zarządzaniu dyskami zainicjuj dysk (GPT) i utwórz dwa woluminy po ok. 500 MB: NTFS (etykieta `NTFS`) i exFAT (etykieta `EXFAT`; jeśli kreator nie oferuje exFAT, utwórz wolumin bez formatowania i wykonaj `format <litera> /FS:exFAT /Q /V:EXFAT`). Zapisz rozmiar jednostki alokacji (`fsutil fsinfo ntfsinfo <litera>` dla NTFS, Właściwości dla exFAT).
2. Na każdym woluminie utwórz `plik.txt` i spróbuj: `mklink link.txt plik.txt`, `mklink /H twardy.txt plik.txt`, `attrib +h +r plik.txt`, `compact /c plik.txt`. Zapisz, co działa, a co kończy się błędem.
3. Porównaj kartę Zabezpieczenia we Właściwościach pliku na obu woluminach.
4. Zmierz czas zapisu 2000 małych plików: `Measure-Command { 1..2000 | % { Set-Content "<litera>\male\p$.txt" "test $_" } }` (najpierw utwórz folder `male`). Porównaj „Rozmiar” i „Rozmiar na dysku” folderu `male`.
5. Spróbuj nadać plikowi na exFAT uprawnienie poleceniem `icacls <litera>\plik.txt /grant uczen:R` (lub dowolnym istniejącym kontem) i zanotuj wynik.

2 Linux: ext4 i Btrfs

W VM Ubuntu Server. Przykład zakłada dyski `/dev/sdb` i `/dev/sdc` — sprawdź w `lsblk`.

1. Zainstaluj `btrfs-progs`. Sformatuj: `sudo mkfs.ext4 -L EXT4 /dev/sdb`, `sudo mkfs.btrfs -L BTRFS /dev/sdc`. Zamontuj w `/mnt/ext4` i `/mnt/btrfs`, nadaj sobie właściciela (`sudo chown $USER /mnt/ext4 /mnt/btrfs`).
2. Na obu: utwórz plik, dowiązanie symboliczne (`ln -s`) i twarde (`ln`), sprawdź `ls -li` — porównaj numery i-węzłów.
3. Btrfs: `sudo btrfs subvolume create /mnt/btrfs/dane`, skopiuj tam kilka plików, wykonaj migawkę `sudo btrfs subvolume snapshot -r /mnt/btrfs/dane /mnt/btrfs/dane_snap1`, usuń plik z `dane` i przywróć go z migawki.
4. Sprawdź listę podwoluminów i migawek: `sudo btrfs subvolume list /mnt/btrfs`.
5. Zmierz czas zapisu 2000 plików: `mkdir /mnt/ext4/male && time bash -c 'for i in $(seq 1 2000); do echo "test $i" > /mnt/ext4/male/p$i.txt; done'` i to samo dla Btrfs. Porównaj `du -sh` i `df -h`.
6. Kronikowanie: sprawdź `sudo dumpe2fs -h /dev/sdb | grep -i features` (szukaj `has_journal`). Uruchom pętlę zapisu na ext4 i w trakcie wyłącz VM (Maszyna → Wyłącz zasilanie). Po starcie zamontuj dysk i odszukaj w `sudo dmesg | grep -i ext4` informację o odtworzeniu kroniki.

3 Dostęp z innego systemu

1. Wyłącz obie VM. Odłącz `wspolny.vhd` od VM Windows i podłącz go do VM Ubuntu.
2. W Ubuntu: `lsblk -f`, zamontuj wolumin NTFS (`sudo mount -t ntfs3 /dev/sdX1 /mnt/ntfs`) i exFAT (`sudo mount /dev/sdX2 /mnt/exfat`). Sprawdź, czy widać pliki, dowiązania i atrybut ukryty. Utwórz plik z poziomu Linuksa.
3. Odmontuj, wyłącz VM, podłącz dysk ext4 (VDI) do VM Windows. Zapisz, co pokazuje Zarządzanie dyskami i Eksplorator (nie formatuj!). Opcjonalnie odczytaj go programem Linux Reader.
4. Przywróć dyski do pierwotnych maszyn albo przywróć migawki.

W sprawozdaniu umieść

- ☐ tabela porównania funkcji czterech systemów plików (wynik testu, nie z podręcznika)
- ☐ tabela czasów zapisu 2000 plików i zajętości miejsca

- ☐ zrzuty: przywrócenie pliku z migawki Btrfs, komunikat o odtworzeniu kroniki ext4, widok dysku ext4 w Zarządzaniu dyskami
- ☐ rekomendacja: jaki system plików dla pendrive'a, dysku systemowego Windows, serwera Linux z migawkami
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Czym różni się dowiązanie twarde od symbolicznego i dlaczego twardego nie można utworzyć między dwoma woluminami?
2. Dlaczego 2000 plików po kilka bajtów zajmuje na dysku znacznie więcej miejsca niż ich łączny rozmiar?
3. Co chroni kronikowanie (journaling), a czego nie chroni — czy zastępuje kopię zapasową?
4. Dlaczego exFAT jest dobrym wyborem dla pendrive'a używanego w różnych systemach, a nie dla dysku systemowego?
5. Czym migawka Btrfs różni się od kopii zapasowej?

Kryteria oceny

Kryterium	Punkty
Testy NTFS i exFAT w Windows	4
Testy ext4 i Btrfs, migawka i kronikowanie	6
Test dostępu z innego systemu	3
Pomiary wydajności i rekomendacja	3
Odpowiedzi na pytania kontrolne	4
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Usterki sprzętowe — diagnostyka POST i metoda wykluczania

Czas: 2 × 45 min

zespoły 2–3 osobowe; zespoły przygotowują usterki dla siebie nawzajem

Cel: Rozpoznawanie typowych usterek sprzętowych na podstawie objawów, sygnałów POST i diod diagnostycznych oraz systematyczne wykluczanie przyczyn z dokumentowaniem diagnozy.

Po zajęciach potrafisz:

- odczytuje sygnały dźwiękowe i diody POST na podstawie dokumentacji płyty głównej
- stosuje metodę wykluczania: od objawu, przez hipotezę, do testu i wniosku
- rozpoznaje usterki pamięci, zasilania, dysków, ustawień UEFI i panelu przedniego
- opracowuje schemat blokowy diagnozy komputera, który się nie uruchamia
- dokumentuje diagnozę i naprawę w karcie serwisowej

Sprzęt i materiały

- komputery stacjonarne (jeden na zespół), opaska antystatyczna, śrubokręt krzyżakowy
- dokumentacja płyt głównych (PDF ze strony producenta — model z zadania 4, rok 1)
- koperty lub kartki na „karty usterek”

Oprogramowanie

- **Instrukcja płyty głównej** — strona wsparcia producenta płyty (ASUS, Gigabyte, MSI, ASRock itd.) — rozdział o sygnałach POST lub diodach Q-LED/EZ Debug LED
- **HWiNFO** — sprawdzenie po naprawie: pamięć, tryb dwukanałowy, dyski [hwinfo.com/download](https://www.hwinfo.com/download)
- **diagrams.net (draw.io)** — schemat blokowy (może być też na papierze) app.diagrams.net

Przygotowanie przed zajęciami

- Pobierz instrukcję płyty głównej swojego stanowiska i odszukaj tabelę sygnałów dźwiękowych lub opis diod diagnostycznych. Sprawdź, czy płyta ma głośniczek (buzzer) — jeśli nie, poproś nauczyciela o głośniczek do złącza SPEAKER.
- Zapisz stan wyjściowy: kolejność rozruchu w UEFI, rozmieszczenie RAM i dysków, i zrób zdjęcia wnętrza.

Bezpieczeństwo

- Każdą zmianę w sprzęcie wykonuj przy odłączonym przewodzie zasilającym i po naciśnięciu przycisku zasilania (rozładowanie). Używaj opaski antystatycznej.
- Dozwolone są tylko usterki z listy w kroku 1. Zakazane: odłączanie chłodzenia procesora, wyjmowanie procesora, przełączanie napięcia zasilacza, zmiana haseł UEFI, wkładanie elementów na siłę.
- Wtyczki i moduły RAM wkładaj zgodnie z wycięciami — nigdy nie odwracaj złącza.
- Nie zwieraj pinów panelu przedniego narzędziami — gdy podejrzewasz panel, zgłoś diagnozę nauczycielowi.
- Po zajęciach przywróć stanowisko do stanu ze zdjęć; nauczyciel sprawdza uruchomienie systemu.

Przebieg zadania

1 Przygotowanie usterek

Lista dozwolonych usterek: brak RAM; RAM w niezalecanym gnieździe lub jeden moduł z dwóch; odłączona wtyczka EPS (4/8 pin CPU); odłączony przewód SATA danych lub zasilania dysku; wyłączony port SATA/dysk w UEFI; zła kolejność rozruchu; odłączony przewód panelu przedniego (POWER SW).

1. Zespół wybiera dwie usterki na rundę 1 (jedna) i rundę 2 (dwie naraz) i zapisuje je na karcie usterek, którą oddaje nauczycielowi.
2. Nauczyciel akceptuje kartę. Zespół wprowadza usterkę z rundy 1 na swoim stanowisku i zamienia się stanowiskami z innym zespołem.
3. Zrób zdjęcie stanowiska po wprowadzeniu usterki — posłuży do kontroli przy przywracaniu.

2 Runda 1 — jedna usterka (do 15 min)

Pracuj metodą: objaw → hipoteza → test → wniosek. Każdy test zapisuj w tabeli.

1. Przed włączeniem obejrzyj komputer z zewnątrz i wewnątrz (bez dotykania elementów) — zapisz, co zauważyłeś.
2. Włącz komputer i opisz objawy: diody, wentylatory, sygnały dźwiękowe (liczba i długość), diody diagnostyczne, obraz, komunikaty.
3. Odszukaj znaczenie sygnałów lub diod w instrukcji płyty i postaw hipotezę.
4. Sprawdzaj hipotezy od najprostszej i najtańszej: przewody, ustawienia UEFI, moduły. Po każdym teście zapisz wynik.
5. Usuń usterkę, uruchom system i potwierdź działanie (np. RAM w HWiNFO — pojemność i tryb dwukanałowy). Zgłoś diagnozę nauczycielowi.

3 Runda 2 — dwie usterki naraz (do 20 min)

Wróćcie na własne stanowisko, wprowadźcie usterki z rundy 2 i ponownie zamieńcie się stanowiskami.

1. Powtórz procedurę z rundy 1. Zwróć uwagę, że usunięcie jednej usterki może ujawnić następną (np. po naprawie RAM pojawia się brak dysku rozruchowego).
2. Zapisz kolejność, w jakiej ujawniały się objawy.
3. Po zakończeniu porównaj swoją diagnozę z kartą usterek autorów.
4. Zapisz, ile testów potrzebowałeś i które z nich okazały się zbędne.

4 Schemat diagnozy i karta serwisowa

1. Narysuj schemat blokowy diagnozy komputera, który nie uruchamia poprawnie systemu: zasilanie → POST → obraz → wykrycie dysków w UEFI → rozruch → system. Przy każdym rozgałęzieniu wpisz typowe przyczyny i test.
2. Wypełnij kartę serwisową dla jednej z usterek (wzór z zadania 32, rok 1).
3. Przywróć swoje stanowisko do stanu wyjściowego i zgłoś je do sprawdzenia.

W sprawozdaniu umieść

- ☐ model płyty głównej i tabela sygnałów POST lub diod z instrukcji (tylko te, które wystąpiły)
- ☐ tabele przebiegu diagnozy z obu rund
- ☐ schemat blokowy diagnozy
- ☐ karta serwisowa jednej usterki
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego te same sygnały dźwiękowe mogą oznaczać co innego na płytach różnych producentów?
2. Komputer włącza się, wentylatory pracują, ale nie ma obrazu ani sygnałów dźwiękowych. Jakie trzy przyczyny sprawdzisz najpierw i w jakiej kolejności?
3. Po czym poznasz, że problem dotyczy ustawień UEFI, a nie uszkodzenia dysku?
4. Dlaczego w metodzie wykluczania zmienia się tylko jeden element naraz?

Kryteria oceny

Kryterium	Punkty
Poprawne i bezpieczne przygotowanie usterek oraz przywrócenie stanowiska	4
Diagnoza i usunięcie usterek w obu rundach	6
Udokumentowany przebieg metody wykluczania	3
Schemat blokowy diagnozy	4
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Projekt końcowy cz. 1: przygotowanie stanowiska dla klienta

Czas: 2 × 45 min

praca w parach (para = firma serwisowa); każda para dostaje inną kartę zlecenia

Cel: Przeanalizowanie zlecenia klienta, dobranie i wycenienie rozwiązania oraz zainstalowanie i skonfigurowanie systemu zgodnie z wymaganiami.

Po zajęciach potrafisz:

- analizuje zlecenie i zapisuje wymagania klienta w formie mierzalnej listy
- dobiera system operacyjny i oprogramowanie z uwzględnieniem licencji i kosztów
- sporządza kosztorys (sprzęt, licencje, robocizna) i harmonogram prac
- instaluje system na drugim dysku i konfiguruje go zgodnie z wymaganiami
- dokumentuje wykonane prace w dzienniku projektu

Sprzęt i materiały

- komputer stacjonarny — instalacja na **drugim dysku**
- pendrive z Ventoy z obrazami Windows 11 i Ubuntu LTS
- karta zlecenia od nauczyciela (np. stanowisko biurowe dla księgowej, stanowisko ucznia, mini-serwer domowy)

Oprogramowanie

- **Windows 11** — na zajęciach bez aktywacji; w kosztorysie uwzględnij licencję microsoft.com/software-download/windows11
- **Ubuntu Desktop / Server LTS** — np. dla mini-serwera domowego ubuntu.com/download
- **winget / apt** — instalacja programów z listy wymagań (zadanie 16) learn.microsoft.com/windows/package-manager/winget
- **Arkusz kalkulacyjny** — kosztorys i harmonogram

Przygotowanie przed zajęciami

- Przejrzyj materiały z zadań: 33 (rok 1 — kosztorys), 16 (winget i apt) i 16 (rok 1 — konfiguracja Windows po instalacji).
- Przygotuj na pendrivie aktualne obrazy Windows 11 i Ubuntu LTS.

Bezpieczeństwo

- Instaluj system wyłącznie na drugim dysku. Przed instalacją sprawdź model i pojemność dysków w UEFI i w instalatorze; w razie wątpliwości odłącz pierwszy dysk (przy wyłączonym zasilaniu).
- Nie przekraczaj zakresu zlecenia — zmiany poza wymaganiami uzgodnij z „klientem” (nauczycielem).
- Używaj tylko legalnego oprogramowania: darmowego, próbnego lub wycenionego w kosztorysie. Nie stosuj aktywatorów ani kluczy z nieznanych źródeł.
- Hasła kont klienta zapisz w dzienniku projektu tylko jako „przekazane klientowi w zamkniętej kopercie” — nie w treści sprawozdania.

Przebieg zadania

1 Analiza zlecenia

Na podstawie karty zlecenia i krótkiej rozmowy z klientem (nauczycielem).

1. Przeczytaj kartę zlecenia i przygotuj 5–8 pytań do klienta (np. jakie programy, ilu użytkowników, jakie dane, kopia zapasowa, budżet, termin).
2. Przeprowadź rozmowę (3–5 min) i zapisz odpowiedzi.
3. Spisz wymagania w tabeli w formie sprawdzalnej, np. „konto standardowe dla użytkownika, bez praw administratora”, a nie „ma być bezpiecznie”. Każde wymaganie otrzymuje numer W1, W2...
4. Przedstaw listę wymagań klientowi i popraw ją po jego uwagach.

2 Dobór rozwiązania i kosztorys

1. Sprawdź, czy sprzęt na stanowisku spełnia wymagania (inwentaryzacja jak w zadaniu 2, rok 1). Jeśli nie — zaproponuj modernizację.
2. Dobierz system i programy; przy każdym zapisz rodzaj licencji i koszt (darmowy, subskrypcja, licencja jednorazowa).
3. Sporządź kosztorys: sprzęt (jeśli potrzebny), licencje, robocizna (godziny × stawka podana przez nauczyciela). Ceny podawaj z nazwą sklepu i datą sprawdzenia.
4. Przygotuj harmonogram prac na zajęcia 33 i 34 i przedstaw kosztorys klientowi do akceptacji.
5. Zapisz w dzienniku decyzję klienta (akceptacja lub zmiany w kosztorysie).

3 Instalacja i konfiguracja

Na drugim dysku.

1. Zainstaluj wybrany system na drugim dysku. Zapisz w dzienniku projektu godzinę rozpoczęcia i zakończenia.
2. Po instalacji sprawdź w Zarządzaniu dyskami (lub `lsblk`), że system jest na drugim dysku, a pierwszy dysk pozostał bez zmian.
3. Utwórz konta zgodnie z wymaganiami (administrator serwisowy + konto użytkownika standardowego).
4. Zainstaluj programy z listy (winget lub apt), sterowniki i aktualizacje.
5. Skonfiguruj ustawienia z wymagań (np. drukarka, udział sieciowy, plan zasilania, przeglądarka, prywatność).
6. Zaznacz w tabeli wymagań, które zostały już spełnione, a które przechodzą na zadanie 34.

W sprawozdaniu umieść

- ☐ karta zlecenia (lub jej opis), pytania do klienta i odpowiedzi
- ☐ tabela wymagań W1, W2... ze stanem realizacji
- ☐ uzasadnienie wyboru systemu i oprogramowania z rodzajami licencji
- ☐ kosztorys i harmonogram
- ☐ dziennik projektu (data, godzina, czynność, osoba)
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego wymagania klienta zapisuje się w formie sprawdzalnej i kiedy się to przyda?
2. Czym różni się licencja OEM, detaliczna (retail) i subskrypcja? Którą wybrałeś i dlaczego?
3. Jak wyliczyłeś koszt robocizny i jakie czynności zajęły najwięcej czasu w porównaniu z harmonogramem?
4. Jakie ryzyka mogą opóźnić wdrożenie i jak im zapobiec?

Kryteria oceny

Kryterium	Punkty
Analiza zlecenia i sprawdzalna lista wymagań	4
Uzasadniony dobór systemu i oprogramowania z licencjami	3
Kosztorys i harmonogram	4
Instalacja i konfiguracja zgodna z wymaganiami (sprawdzona na stanowisku)	6
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).

Projekt końcowy cz. 2: wdrożenie, testy i dokumentacja

Czas: 2 × 45 min

praca w parach (te same pary co w zadaniu 33)

Cel: Dokończenie wdrożenia stanowiska z zadania 33: kopia zapasowa, zabezpieczenia, testy akceptacyjne, dokumentacja dla użytkownika i przekazanie rozwiązania klientowi.

Po zajęciach potrafisz:

- konfiguruje i sprawdza kopię zapasową z odtworzeniem pliku
- zabezpiecza stanowisko zgodnie z wymaganiami klienta
- przeprowadza testy akceptacyjne na podstawie listy wymagań
- pisze zwięzłą instrukcję dla użytkownika i protokół odbioru
- prezentuje rozwiązanie w 5 minut i odpowiada na pytania

Sprzęt i materiały

- komputer stacjonarny z systemem zainstalowanym w zadaniu 33 na drugim dysku
- nośnik lub udział na kopię zapasową (pendrive, drugi wolumin albo udział na serwerze szkolnym — ścieżkę podaje nauczyciel)
- rzutnik lub ekran do prezentacji

Oprogramowanie

- **Narzędzia kopii zapasowej** — Windows: Historia plików / Kopia zapasowa systemu Windows; Linux: np. `rsync` lub Déjà Dup — zgodnie z zadaniem 14
- **Zabezpieczenia Windows i BitLocker** — BitLocker tylko w Windows 11 Pro/Education/Enterprise
learn.microsoft.com/windows/security/operating-system-security/data-protection/bitlocker
- **Edytor tekstu i program do prezentacji** — LibreOffice lub pakiet szkolny
libreoffice.org/download/download-libreoffice

Przygotowanie przed zajęciami

- Przejrzyj tabelę wymagań z zadania 33 — wypisz wymagania oznaczone „zad. 34”.
- Przygotuj szkic prezentacji (4–6 slajdów): klient i wymagania, rozwiązanie, koszt, testy, wnioski.

Bezpieczeństwo

- Pracuj nadal tylko na drugim dysku — sprawdź po uruchomieniu, że to system z zadania 33.
- Klucz odzyskiwania BitLocker zapisz w pliku na nośniku wskazanym przez nauczyciela (lub wydrukuj) — nie zapisuj go na szyfrowanym dysku ani w sprawozdaniu publicznym.
- Kopia zapasowa na udziale szkolnym nie może zawierać danych osobowych — używaj fikcyjnych plików klienta.
- W instrukcji dla użytkownika nie podawaj haseł; opisz tylko, jak je zmienić.

Przebieg zadania

1 Kopia zapasowa

1. Skonfiguruj kopię danych użytkownika zgodnie z wymaganiami (co, gdzie, jak często). Zapisz konfigurację w dzienniku projektu.
2. Wykonaj pierwszą kopię, usuń jeden plik testowy i odtwórz go z kopii. Zrób zrzut odtworzenia.
3. Opisz, jak rozwiązanie realizuje (lub nie) zasadę 3-2-1 i co klient powinien dokupić lub robić samodzielnie.

2 Zabezpieczenia

Tylko te, które wynikają z wymagań i rodzaju stanowiska.

1. Sprawdź aktualizacje, ochronę antywirusową i zaporę (Windows: Zabezpieczenia Windows; Linux: `sudo apt update && sudo apt upgrade`, `sudo ufw status`).
2. Sprawdź, że użytkownik pracuje na koncie standardowym, a konto administratora ma silne hasło.
3. Wdróż pozostałe zabezpieczenia z wymagań (np. BitLocker, blokada nośników USB, ograniczenia zasadami grupy, logowanie SSH kluczem).

3 Testy akceptacyjne i dokumentacja

1. Przygotuj listę kontrolną testów: dla każdego wymagania W1, W2... opis testu i oczekiwany wynik.
2. Wykonaj testy na koncie użytkownika (nie administratora) i zapisz wynik: spełnione / niespełnione / uwagi.
3. Każdy niespełniony test popraw i powtórz; zapisz w dzienniku, co zmieniłeś.
4. Napisz instrukcję dla użytkownika (1–2 strony): logowanie, gdzie zapisywać pliki, jak działa kopia, co zrobić w razie problemu, kontakt do serwisu. Pisz prostym językiem.
5. Wypełnij protokół odbioru i przekaz go klientowi (nauczycielowi) do podpisu.

4 Prezentacja

5 minut na parę, potem 1–2 pytania z sali.

1. Przećwicz prezentację w parze z zegarem — zmieść się w 5 minutach.
2. Przedstaw: zlecenie i wymagania, wybrane rozwiązanie, koszt, wyniki testów, problemy i ich rozwiązania.
3. Pokaż na żywo jedną funkcję stanowiska (np. odtworzenie pliku z kopii).
4. Odpowiedz na pytania i zanotuj uwagi klasy oraz nauczyciela.

W sprawozdaniu umieść

- ☐ konfiguracja kopii zapasowej i zrzut odtworzenia pliku
- ☐ lista wdrożonych zabezpieczeń
- ☐ lista kontrolna testów akceptacyjnych z wynikami
- ☐ instrukcja dla użytkownika (1–2 strony) jako załącznik
- ☐ podpisany protokół odbioru i plik prezentacji
- ☐ odpowiedzi na pytania kontrolne

Pytania kontrolne

1. Dlaczego testy akceptacyjne wykonuje się na koncie użytkownika, a nie administratora?
2. Kopia zapasowa „działa”, ale nikt nie próbował odtworzyć danych. Jakie jest ryzyko?
3. Co powinien zawierać protokół odbioru i do czego przyda się firmie serwisowej w przypadku reklamacji?

4. Które z wdrożonych zabezpieczeń najbardziej utrudni codzienną pracę klienta i jak to wyjaśnisz klientowi?

Kryteria oceny

Kryterium	Punkty
Kopia zapasowa z udanym odtworzeniem	3
Zabezpieczenia zgodne z wymaganiami	3
Lista kontrolna i rzetelne testy akceptacyjne	4
Instrukcja dla użytkownika i protokół odbioru	4
Prezentacja i odpowiedzi na pytania z sali	3
Odpowiedzi na pytania kontrolne	3
Razem	20

Sprawozdanie przygotuj na wzorze dołączonym do zadania (plik .docx o tym samym numerze).