Linia poleceń Windows (cmd). Pliki wsadowe (batch/.bat)

Linia poleceń systemu Windows daje znacznie większe możliwości niż jego standardowe użytkowanie. Przede wszystkim wykonywanie większości czynności administracyjnych jest znacznie szybsze niż metodą klikania w kolejnych oknach kolejnych opcji.

W obecnych wersjach (od Windows 2008/Vista) istnieją dwie linie poleceń - stara, pamiętająca jeszcze korzenie systemu oraz nowa, o nazwie PowerShell. Należy przy tym pamiętać, że chociaż pierwsza linia poleceń wywodzi się z systemu DOS, to w obecnej postaci niewiele ma z nim wspólnego. W systemach Windows aż do wersji Me interpreter ten był wersją DOS (do Windows Me graficzny wygląd był tylko nakładką systemu DOS). Od Windows NT (w wersji użytkowej jądro NT zadebiutowało wraz z 2000/XP) pomimo podobnego wyglądu, interpreter nie ma nic wspólnego ze starym systemem. Linia pozwala na wykonywanie wszystkich operacji systemowych – od uruchomienia prostego notatnika po wykonanie specjalistycznych ustawień/poleceń systemowych, które niekiedy nie mogą być inaczej wykonane. Znajomość poleceń jest szczególnie przydatna gdy wersja systemu nie posiada odpowiednich narzędzi graficznych (np. wersje niższe od Professional). Microsoft bowiem nie blokuje samej funkcjonalności w systemie, a jedynie blokuje możliwość konfiguracji i zmiany z poziomu graficznego. Dzięki poleceniom tekstowym możemy więc dokonać znacznie więcej nawet na podstawowych wersjach systemu.

1. Podstawowe polecenia

a) ver – polecenie sprawdza wersję systemu (a przy okazji interpretera)

b) cd – pozwala na zmianę aktualnie wybranego katalogu. Dodatkowo należy zaznaczyć, że w przypadku posiadania większej ilości dysków twardych ścieżkę ustawiamy dla każdego niezależnie – przy przejściu na kolejne dyski zostaje ona zapamiętana. Należy pamiętać, że samej litery dysku NIE ZMIENIAMY z tym poleceniem; aby zmienić literę dysku należy wpisać ją bezpośrednio w linii poleceń, np.

c:\>d:

zmieni obecny dysk z c na d.

Przykłady:
c:\>cd Windows
c:\>cd c:\Windows

oba polecenia spowodują przejście do katalogu Windows. Proszę zauważyć, że podczas przejścia do katalogu można pominąć literę dysku bądź folderów nadrzędnych w przypadku, gdy katalog ten jest bezpośrednim następcą (dzieckiem) danej lokalizacji. Jeżeli planujemy przejście do innego katalogu ścieżka zawsze musi być pełna (cała).

C:\Windows>cd e:\programy

spowoduje przejście do katalogu programy na dysku e. Nie zostaniemy tam jednak przeniesieni! (trzeba zmienić dysk)

ZADANIE: Proszę znaleźć zamiennik polecenia cd; Proszę sprawdzić czy można przemieszczać się pomiędzy dyskami po wpisaniu litery dysku oraz katalogu

c) mkdir – tworzenie nowego katalogu w aktualnej bądź podanej (pełna ścieżka) lokalizacji

Przykład:

c:\>mkdir d:\nowy

Utworzy nowy katalog o nazwie nowy na dysku d:.

c:\moj> mkdir inny

utworzy katalog inny w bieżącej lokalizacji

d) copy – pozwala na skopiowanie plików z jednej lokalizacji do innej. Kopiować można pojedyncze obiekty jak i całe lokalizacje. Ważne jest by pamiętać, że narzędzie kopiuje jedynie PLIKI.

Przykład:

c:\>copy c:\pierwszy * c:\drugi

skopiuje wszystkie pliki z katalogu pierwszy do katalogu drugi. Ważne jest by katalog drugi ISTNIAŁ na dysku; w przeciwnym wypadku narzędzie utworzy jeden plik o nazwie drugi i złączy w nim zawartość wszystkich plików z katalogu pierwszy!

C:\>copy d:\inny\tajny_plik.txt c:\Users\Public\

przekopiuje plik bez zmiany nazwy.

C:\>copy d:\inny\tajny_plik.txt c:\Users\Public\publiczny_plik.txt

podobnie jak w poprzednim wypadku; teraz dodatkowo zostanie zmieniona nazwa na publiczny_plik.txt w lokalizacji docelowej

ZADANIE: zapoznać się z najpopularniejszymi przełącznikami polecenia. W jaki sposób kopiować pełne zawartości katalogów (łącznie z podkatalogami)?

e) driverquery – wyświetla wszystkie zainstalowane sterowniki na wskazanym systemie Windows. Można wskazać własny komputer (bez parametrów), można też sprawdzić komputer w sieci lokalnej/firmowej/VPN. Polecenie potrafi sformatować wyjście na postać tabelaryczną, listę bądź format CSV (np. dla arkuszy kalkulacyjnych bądź programów bazodanowych)

ZADANIE: sprawdzić możliwości narzędzia przy odpytaniu komputera w sieci lokalnej (odpowiednie parametry).

f) wusa – bardziej skrypt niż osobne polecenie cmd. Pozwala operacje na pobranych aktualizacjach oraz odinstalowywanie wskazanych aktualizacji systemu Windows. Jego niepodważalną zaletą jest możliwość odinstalowania aktualizacji po podaniu jej numeru z bazy wiedzy Microsoft (kb – knowledge base).

Przykład:
wusa /uninstall /kb:980302

Spowoduje usunięcie aktualizacji o podanym numerze

ZADANIE: dowiedzieć się co jeszcze można zrobić za pomocą wspomnianego narzędzia

g) attrib – pozwala na nadawanie odpowiednich atrybutów dla plików i folderów

Przykład:

c:\>attrib +h nowy

nada atrybut 'Ukryty' dla elementu nowy

ZADANIE – jakie atrybuty możemy nadawać plikom i folderom. Czy można zmienić atrybuty elementom podrzędnym (znajdującym się np. w folderze wskazanym)?

h) netsh – dosyć potężne i przydatne polecenie systemu Windows. Pozwala ono na zarządzanie wszystkimi ustawieniami sieciowymi w systemie. Zarządzania można dokonywać zarówno lokalnie jak i zdanie (na komputerach sieci lokalnej).

Przykłady:

netsh interface ipv4 show route

Polecenie pokaże nam wszystkie znane ścieżki dla interfejsu ipv4

netsh interface ipv4 show config

Wynik będzie podobny do wydania polecenia ipconfig

netsh interface ipv4 add address <parametry>

Pozwala na konfigurowanie dowolnych interfejsów sieciowych. Po pierwsze musimy podać nazwę naszego interfejsu (musimy ją odczytać odpowiednim poleceniem), po czym można przejść do konfiguracji dowolnych parametrów adresu – IP, maski, bramy, metryki bramy (priorytet), typu zmiany (do pierwszego ponownego włączenia/na stałe) itp.

Przykład konfiguracji połączenia o nazwie Siec1:

netsh interface ipv4 add address „Siec1” address=172.18.0.2 gateway=172.18.0.1 mask=255.255.255.128

Serwery DNS zmienia się/dodaje z poleceniem dnsservers zamiast address.

Każdy poziom polecenia (kolejne jego człony) można przepatrzeć poprzez podania znaku zapytania:

netsh interface ?

Dzięki temu wyświetlone zostaną informacje jakie polecenie możemy podstawić zamiast znaku zapytania

ZADANIE: Proszę dowiedzieć się jak zmienić aktualnie ustawioną konfigurację interfejsu sieciowego. W jaki sposób można dodawać nowe interfejsy do systemu za pomocą polecenia.

i) net – polecenie, którego nazwa dawna dawno nie ma zbyt wiele wspólnego z prawdziwym (obecnym) zastosowaniem. Pierwotnie, w systemie DOS, dzięki niemu można było zarządzać siecią lub ustawieniami sieci. W obecnej chwili polecenie pozwala także na zarządzanie użytkownikami, kontami w systemie, wyświetleniem informacji o systemie, zarządzać grupami użytkowników czy uruchamianie bądź wyłączanie usług systemowych. Oczywiście wszystkie podpolecenia mają możliwość zastosowania na komputerach zdalnych – stąd ich lokalizacja (pomimo zasięgu lokalnego).

Przykłady:
net user uzytkownik /ADD

dodaje nowego użytkownika o nazwie uzytkownik

net accounts uzytkownik /forcelogoff:30

Podanemu użytkownikowi ustawia limit sesji na 30 minut. Po tym czasie zostanie on wylogowany

net user uzytkownik /times:Pn-Pt,8:00-15:00

Użytkownikowi zostanie nałożony limit; będzie mógł się logować jedynie od 8 do 15 , od poniedziałku do piątku

net stop Audiosrv

wyłącza usługę systemową Audio (od tego momentu nie będzie działać dźwięk)

ZADANIE: W jaki sposób udostępnić i zmapować udostępniony przez siebie zasób (udostępnienia proszę dokonać przez polecenie net) pod konkretną literę dysku twardego na dowolnym komputerze w sieci lokalnej? Do czego służy polecenie net computer?

j) wmic – jedno z potężniejszych poleceń konsoli. Posługiwanie się nim przypomina odpytywanie bazy danych SQL. Baza ta zawiera wszystkie konfiguracje oraz wszystkie informacje, jakie system posiada o komputerze. Pozwala na zmiany i ingerencję w dowolne z tych ustawień (z zastrzeżeniem niektórych wyłączenie dla konta systemowego).

Przykłady:

wmic useraccount get all

Pobiera wszystkie informacje o wszystkich kontach użytkowników w systemie

wmic useraccount WHERE name=”Administrator” get disabled

polecenie sprawdzi czy konto Administrator jest wyłączone (wartości prawda/fałsz)

wmic useraccount WHERE name=”Administrator” set disabled=FALSE

polecenie włączy konto Administrator (jeżeli było wyłączone)

wmic desktop get wallpaper

Poda ścieżkę docelową ustawionej tapety pulpitu

ZADANIE: W jaki sposób sprawdzić numer seryjny dysku twardego oraz wersję BIOS przy użyciu wmic? W jakiś sposób odczytać informacje o ekranach śmierci za pomocą wmic? Jak wymusić na użytkowniku zmianę hasła co 15 dni poprzez linię poleceń?

ZADANIA DO WYKONANIA:
1. Jakim poleceniem można wyczyścić aktualną zawartość konsoli?
2. Do czego służy polecenie ftp? Czym różni się od polecenei tftp?
3. Jakim poleceniem można zabić proces w systemie Windows? Czy można zabijać procesy na maszynie zdalnej?
4. Po co stosuje się sumy kontrolne? Czy system posiada dla cmd narzędzie, które pozwalałoby na sprawdzenie sumy kontrolnej wskazanego pliku?
5. Jakim poleceniem można przenosić pliki poprzez konsolę?

https://technet.microsoft.com/en-us/library/bb490954.aspx
https://msdn.microsoft.com/en-us/library/windows/desktop/aa394531(v=vs.85).aspx
http://www.computerhope.com/nethlp.htm