

Powershell – konsola systemu Windows

PowerShell ma za zadanie w pełni zastąpić konsolę systemową. Coraz więcej poleceń w systemie z poprzednich wersji jest wygaszane bądź blokowane. W zamian za to coraz więcej funkcjonalności pojawia się w konsoli PowerShell. Obecnie każdą opcję systemową można wykonać poprzez nowe polecenia przepisane do nowej konsoli. W poniższym materiale zostaną omówione najistotniejsze polecenia i ich możliwości.

1. Zakładanie użytkownika. Zarządzanie grupami.

a) **New-LocalUser** – polecenie tworzy nowego użytkownika. Domyślnie po jego wywołaniu otrzymamy szereg pytań, np. o nazwę użytkownika lub hasło. Polecenie można wywołać z dodatkowymi parametrami (tylko niektóre):

- Name <nazwa> - nazwa nowego użytkownika
- FullName <nazwa> - pełna nazwa użytkownika; nazwa ta będzie wyświetlana, jednak nie będzie można jej użyć np. do logowania się
- Description <opis> - pozwala na dodanie opisu użytkownika
- Disabled – użytkownik będzie wyłączony

b) **Get-LocalUser** – polecenie pozwala na wyświetlenie wszystkich użytkowników dostępnych w systemie.

c) **Rename-LocalUser** – pozwala na zmianę nazwy użytkownika

d) **Remove-LocalUser** – usuwa wskazanego użytkownika

e) **Enable-Localuser/Disable-LocalUser** – umożliwia włączenie bądź wyłączenie wskazanego użytkownika

f) **Set-LocalUser** – pozwala na zmianę poszczególnych parametrów wskazanego konta użytkownika

g) **New-LocalGroup** – tworzy nową grupę użytkowników. Możliwe parametry:

- Name <nazwa> - nazwa nowej grupy użytkowników
- Description <nazwa> - opis nowej grupy
- Confirm – parametr powoduje, że przed utworzeniem nowej grupy wyświetlone zostanie potwierdzenie operacji

h) **Rename-LocalGroup** – pozwala na zmianę lokalnej grupy

i) **Set-LocalGroup** – umożliwia zmianę parametrów grupy użytkowników; w tym wypadku można zmieniać jedynie opis grupy

j) **Remove-LocalGroup** – usuwa wskazaną grupę

k) **Get-LocalGroup** – wyświetla wszystkie dostępne grupy w systemie

l) **Add-LocalGroupMember** – dodaje do wskazanej grupy określonych użytkowników. Parametry polecenia:

-Group <nazwa> - określa grupę, do której będą dodawani użytkownicy
-Member <lista_nazw> - lista użytkowników, którzy mają zostać dodani do wskazanej grupy;
nazwy użytkowników mogą zostać oddzielone przecinkami

m) **Remove-LocalGroupMember** – usuwa wskazanych użytkowników ze wskazanej grupy;
posiada te same parametry co poprzednie polecenia

2. Operacje na komputerach.

a) **Rename-Computer** – pozwala na zmianę nazwy komputera lokalnego bądź któregośkolwiek w sieci. Parametry:

-ComputerName <nazwa> - nazwa komputera, dla którego zmieniana będzie nazwa; może zostać pominięty (wtedy operacja zadziała dla komputera lokalnego)
-NewName <nazwa> - nowa nazwa dla komputera
-PassThru – zwraca wynik polecenia; brak tego parametru powoduje brak wyświetlenia komunikatów
-Restart – powoduje zrestartowanie komputera po zamianie nazwy

b) **Add-Computer** – polecenie pozwala na dodanie komputera do grupy roboczej lub domeny

c) **Stop-Computer** – umożliwia na wyłączenie komputera lokalnego bądź zdalnego

d) **Restart-Computer** – uruchamia ponownie wskazany komputer

3. Zarządzanie usługami i procesami.

a) **New-Service** – pozwala na utworzenie nowej usługi w systemie Windows. Usługi to procesy działające w systemie i pozwalające np. na utrzymywanie systemu w dobrej kondycji (np. Windows Update, Windows Defender), aplikacje kontrolujące stan aplikacji w systemie (jej ważność, łatwość dostępu) lub czy system działa poprawnie (sprawdzanie daty i godziny systemowej, rozpoznawanie nazw sieciowych). Parametry polecenia:

-Name <nazwa> - nazwa widziana na liście usług
-BinaryPathName <ścieżka_wywołania> - pełna ścieżka do pliku wykonywalnego naszej usługi;
może zawierać dodatkowe parametry wywołania
-StartupType <Boot,System,Automatic,Manual,Disabled> - sposób uruchamiania usługi (można wybrać jeden z podanych w nawiasie)

b) **Stop-Service** – pozwala na zatrzymanie wskazanej usługi/usług (podawanych po przecinku)

c) **Start-Service** – uruchamia wskazaną usługę/usługi

d) **Resume-Service** – wznowia zatrzymaną usługę/usługi

e) **Restart-Service** – ponownie uruchamia usługę/usługi

f) **Suspend-Service** – zawiesza wskazaną usługę/usługi

g) **Get-Service** – wyświetla listę usług dostępnych w systemie lokalnym lub zdalnym

- i) **Get-Process** – pobiera i wyświetla listę procesów uruchomionych w systemie lokalnym bądź zdalnym
- j) **Start-Process** – umożliwia uruchomienie jednego bądź wielu procesów-zadań. Procesy mogą być uruchamiane z innymi poświadczeniami niż aktualne, można też ładować środowisko innych użytkowników (np. wpisy rejestru).

-WorkingDirectory <katalog> - katalog startowy aplikacji; jeżeli nie zostanie podany to domyślnym będzie ten, z którego wywołujemy aplikację

-LoadUserProfile – ładuje środowisko (rejestr) wskazanego użytkownika

-Credential <nazwa> - załadowanie programu z uprawnieniami wskazanego użytkownika

k) **Stop-Process** – zatrzymuje wskazany proces systemowy. Zatrzymanie może nastąpić po identyfikatorze, obiekcie (przekazanym z innego polecenia) lub nazwie/nazwach procesów (nazwy muszą być dokładnie podane)

l) **Wait-Process** – wysyła polecenie wyłączenia procesu jednak w sposób „łagodny”, tj. kończy aktualny proces/procesy po wykonaniu zadania (nie pozwoli np. na przyjęcie kolejnych argumentów).

4. Harmonogram zadań

Dodawanie i zarządzanie zadaniami poprzez PowerShell wymaga rozbudowanych poleceń. Zamiast opisywać poszczególne polecenia pokazana zostanie możliwość tworzenia, sprawdzania czy też ich usuwania. PowerShell pozwala także na import i eksport poszczególnych zadań.

a) celem dodania nowego zadania uruchamianego od poniedziałku do piątku, z uprawnieniami administratora systemu notatnika należy wykonać następujące polecenia:

```
$user=New-ScheduledTaskPrincipal ".\admin"  
$action=New-ScheduledTaskAction -Execute "notepad.exe"  
$settings=New-ScheduledTaskSettingsSet -DontStopIfGoingOnBatteries -WakeToRun  
$trigger=New-ScheduledTaskTrigger -DaysOfWeek Monday,Tuesday,Wednesday,Thursday,Friday -  
At 10:30am -RepetitionDuration 1h -RepetitionInterval 15mins
```

```
$task=New-ScheduledTask -Action $action -Principal $user -Trigger $trigger -Settings $settings  
Register-ScheduledTask -TaskName "NotatkiInstant" -InputObject $task
```

b) modyfikacja poprzedniego zadania poprzez

```
$Time = New-ScheduledTaskTrigger -At 12:00 -Once  
Set-ScheduledTask -TaskName "NotatkiInstant" -Trigger $Time
```

c) uruchomienie (aktywowanie) wszystkich zadań dostępnych w wybranym katalogu zadań:

```
Get-ScheduledTask -TaskPath "\MojeZadania\" | Enable-ScheduledTask
```

d) uruchomienie (natychmiastowe wykonanie) wskazanego zadania:

```
Start-ScheduledTask -TaskName "NotatkiInstant"
```

e) zatrzymanie wskazanego zadania:

Stop-ScheduledTask -TaskName "NotatkiInstant"

Zadania do samodzielnego opracowania:

- 1) przetestować przedstawione polecenia poprzez tworzenie, modyfikowanie i usuwanie użytkowników w systemie
- 2) przetestować dodawanie własnych procesów do usług; sprawdzić czy uruchamianie ich działa przy uruchomieniu systemu
- 3) uruchomić zadanie na komputerze zdalnym (np. u kolegi); przetestować możliwości restartowania/wyłączania komputera zdalnego.
- 4) wyeksportować dowolne zadanie z harmonogramu zadań
- 5) zaimportować dowolne zadanie z innego komputera (np. od kolegi)
- 6) Wskazać polecenia z linii poleceń, które zostały zastąpione poprzez polecenia z PowerShell (wskazać przynajmniej 5 grup); Czy polecenia te zyskały na funkcjonalności?
- 7) Czy istnieje możliwość zarządzania instalacją składników systemu Windows z linii poleceń? Jeżeli tak w jaki sposób można tego dokonać?
- 8) Pokazać możliwości zarządzania przestrzenią magazynową przez PowerShell. Czy istnieje dla tego rodzaju zarządzania alternatywa?

Wszelkie odpowiedzi należy odpowiednio udokumentować (np. zrzutem ekranu). Wykonane prace należy przesłać na adres piotr_dobosz@int.pl, z tematem zawierającym frazę [TEB_BCH_I] (klasa I) lub [TEB_EUTK_BCH] (klasa II) do dnia 9.11.2018

Materiały:

<https://stackoverflow.com/questions/15199321/powershell-equivalent-to-grep-f>

<https://docs.microsoft.com/en-us/powershell/module/?view=win10-ps>