Standardowa aktualizacja systemu produkcyjnego (Windows)

□□ Typ: procedura **□□ Dotyczy: Windows Server 2016+**

□ Czas: ~45–90 min na serwer, plus czas trwania restartu

Efekt: serwer ma zainstalowane bieżące aktualizacje, jest po restarcie, wszystkie usługi wróciły do stanu sprzed prac, a ewidencja serwerów odzwierciedla nową datę patchowania. Odpowiednik dla Linuksa opisuje strona Standardowa aktualizacja systemu produkcyjnego.

□□ Skróty użyte na tej stronie (2)

Skrót	Co znaczy
CMDB	Configuration Management Database: baza konfiguracji, czyli spis elementów, z których składają się usługi, i ich powiązań; w Zielonej rolę tę pełni NetBox
GUI	Graphical User Interface: okienka i myszka zamiast komend

Zanim zaczniemy

> **□□ Z ŻYCIA WZIĘTE**
>
> Zgłoszenie na wtorek po Patch Tuesday obejmuje sql01, bo księgowość kończy akurat miesiąc i pani Halina prosiła o przesunięcie okna serwisowego na później niż zwykle. Robimy snapshot maszyny bez zrzutu pamięci, sprawdzamy wolne miejsce na dysku systemowym i dopiero wtedy zaczynamy pobieranie aktualizacji, żeby samo okno ograniczyć do instalacji i restartu.

Sprawdzamy zgłoszenie i okno serwisowe, w którym wykonujemy prace — patchowanie produkcyjnego serwera poza umówionym oknem jest wyjątkiem, nie regułą.

Wykonujemy snapshot maszyny wirtualnej przed jakąkolwiek zmianą. Przy tworzeniu snapshotu odznaczamy opcję zrzutu pamięci maszyny (*include virtual machine memory*), chyba że mamy konkretny powód, żeby ją zostawić — domyślnie zostaje odznaczona, bo istotnie wydłuża czas tworzenia i kasowania snapshotu bez realnej korzyści dla samego patchowania.

Sprawdzamy ilość wolnego miejsca na dysku systemowym — pobrane pliki aktualizacji w `SoftwareDistribution\Download` potrafią zająć kilka gigabajtów, a instalacja dużej aktualizacji kumulatywnej wymaga dodatkowego zapasu na dysku na czas samej operacji.

Spisujemy listę usług, które przed patchowaniem trzeba zatrzymać ręcznie — zwykle agent antywirusowy/EDR (część z nich blokuje pliki systemowe w trakcie instalacji poprawek) oraz usługi własnej aplikacji, jeśli aplikacja nie radzi sobie z restartem w trakcie swojej pracy. Włączamy tryb konserwacji w systemie monitoringu na patchowany serwer, żeby restart nie wygenerował fałszywych alertów.

Sprawdzamy, czy przy okazji restartu nie warto podnieść wersji VMware Tools albo wirtualnego sprzętu (compatibility/hardware version) maszyny — restart i tak nastąpi, więc to naturalna okazja, żeby zrobić to bez dodatkowego przestoju.

Przebieg



Piec etapow standardowej aktualizacji: snapshot, pobranie, instalacja w oknie, restart, weryfikacja (kliknięcie otwiera pełny rozmiar)

1. Instalacja i import modułu PSWindowsUpdate

Uruchamiamy okno PowerShell jako administrator. Jeśli moduł nie jest jeszcze zainstalowany:

```
Set-ExecutionPolicy –ExecutionPolicy RemoteSigned -Force
Install-Module -Name PSWindowsUpdate -Force
```

Instalujemy moduł nawet wtedy, gdy wygląda na już zainstalowany — polecenie przy okazji dociąga jego nowszą wersję, jeśli jest dostępna.

Na starszych wersjach Windows Server automatyczne pobranie modułu z PowerShell Gallery bywa niedostępne (brak zaufanego źródła, brak dostępu do internetu z serwera). W takiej sytuacji instalujemy moduł ręcznie: pobieramy go na innej maszynie z dostępem do internetu, kopiujemy katalog modułu na docelowy serwer i importujemy z lokalnej ścieżki.

```
Save-Module –Name PSWindowsUpdate –Path C:\ps\
```

Skopiowaną zawartość umieszczamy w `%WINDIR%\System32\WindowsPowerShell\v1.0\Modules` na serwerze docelowym, a następnie:

```
Import-Module PSWindowsUpdate
```

2. Pobranie aktualizacji przed oknem serwisowym

Żeby skrócić samo okno serwisowe, aktualizacje warto pobrać wcześniej — w oknie zostaje wtedy tylko instalacja i restart.

Przed pobraniem czyścimy katalog `Download`, żeby nie kumulować starych, częściowo pobranych plików, i sprawdzamy wolne miejsce na dysku C:

```
Remove-Item -Path "$env:windir\SoftwareDistribution\Download\*" -Recurse -Force
```

Pobieramy aktualizacje bez instalowania ich od razu:

```
Get-WindowsUpdate -AcceptAll -Download
```

3. Instalacja w oknie serwisowym

W umówionym oknie serwisowym instalujemy wcześniej pobrane aktualizacje. Instalację można wykonać przez GUI albo przez PowerShell — z moich obserwacji aktualizacje instalują się przez PowerShell nieco szybciej, ale GUI ma tę przewagę, że rzetelnie odświeża swój stan po restarcie (więcej w sekcji *Gdy coś nie zadziała* niżej).

```
Install-WindowsUpdate -MicrosoftUpdate -AcceptAll -IgnoreReboot
```

4. Restart serwera

```
Restart-Computer -Force
```

Weryfikacja

Sprawdzamy, czy usługi, które zatrzymywaliśmy ręcznie przed pracami (agent antywirusowy/EDR, usługi aplikacji), wróciły do działania po restarcie — część z nich trzeba włączyć ręcznie, jeśli nie były skonfigurowane na automatyczny start.

```
Get-Service NazwaUslugi
```

Sprawdzamy, czy aplikacja działająca na serwerze odpowiada — w zależności od aplikacji jest to test end-to-end, sprawdzenie portu nasłuchu, albo zapytanie do endpointu health-check.

Przeglądamy dziennik zdarzeń w poszukiwaniu błędów, które pojawiły się dopiero po restarcie:

```
Get-WinEvent -FilterHashtable @{LogName='System','Application'; Level=1,2; StartTime=(Get-Date).AddHours(-2)} | Format-Table TimeCreated, LogName, Id, LevelDisplayName, Message -Wrap
```

Sprawdzamy, czy dalej nie jest wymagany kolejny restart (bywa, że jedna aktualizacja kumulatywna wymaga dwóch cykli restartu):

```
Get-WURebootStatus
```

Jeśli po pomyślnej instalacji i restarcie zabrakło miejsca na dysku, czyścimy ponownie katalog pobranych plików — są już zbędne:

```
Remove-Item -Path "$env:windir\SoftwareDistribution\Download\*" -Recurse -Force
```

Aktualizujemy datę wykonania patchowania i status serwera w ewidencji (CMDB / arkusz utrzymania), zdejmujemy tryb konserwacji w systemie monitoringu.

Wycofanie zmian

Jeśli konkretna aktualizacja jest przyczyną problemu, odinstalowujemy tylko ją, bez przywracania całego serwera:

```
Remove-WindowsUpdate -KBArticleID NumerKB -NoRestart
```

Jeżeli problem jest głębszy niż jedna poprawka — usługa nie startuje, aplikacja nie działa mimo poprawnie zainstalowanych aktualizacji — wracamy do snapshotu wykonanego przed rozpoczęciem prac, zamiast szukać przyczyny na produkcji pod presją czasu.

Gdy coś nie zadziała

Objaw	Przyczyna	Naprawa
GUI Windows Update pokazuje, że aktualizacje nie zostały zainstalowane, mimo że instalacja przez PowerShell zakończyła się sukcesem	znany błąd odświeżania panelu GUI po instalacji przez CLI	sprawdzamy stan przez `Get-HotFix` / `Get-WUHistory`, a w GUI wystarczy raz kliknąć *Sprawdź aktualizacje*, żeby dane się odświeżyły
Instalacja wisi na etapie pobierania	uszkodzony cache Windows Update	czyścimy cache zgodnie z procedurą na stronie Windows Update z wiersza poleceń
Po restarcie usługa aplikacji się nie uruchamia	usługa nie była ustawiona na automatyczny start, albo zależy od usługi wciąż się podnoszącej	sprawdzamy typ uruchomienia (`Get-Service` / `Set-Service -StartupType Automatic`), w razie potrzeby startujemy ręcznie po odczekaniu na zależności
Brakuje miejsca na dysku w trakcie instalacji	nie wyczyszczono katalogu `Download` przed pobraniem, albo aktualizacja kumulatywna wymaga większego zapasu niż zwykle	czyścimy `SoftwareDistribution\Download`, w razie potrzeby tymczasowo podłączamy dodatkowy dysk pod hypervisorem
Po aktualizacji system działa niestabilnie, przyczyna niejasna	aktualizacja wprowadziła regresję niewidoczną od razu w dzienniku zdarzeń	przywracamy snapshot wykonany przed pracami, zgłaszamy problem, nie próbujemy diagnozować pod presją czasu na aktywnej produkcji

Powiązane: Windows Update z wiersza poleceń · WSUS: czyszczenie i utrzymanie · Standardowa aktualizacja systemu produkcyjnego (odpowiednik dla Linuksa)

Źródła: notatki własne

Revision #38
Created 2026-09-25 06:44:55 UTC by Tomasz Konieczny
Updated 2026-10-26 14:07:03 UTC by Tomasz Konieczny