

# Systemy operacyjne

## WYKŁAD 11 i 12

dr inż. Stanisława Plichta  
[splichta@ans-ns.edu.pl](mailto:splichta@ans-ns.edu.pl)

# OpenAFS

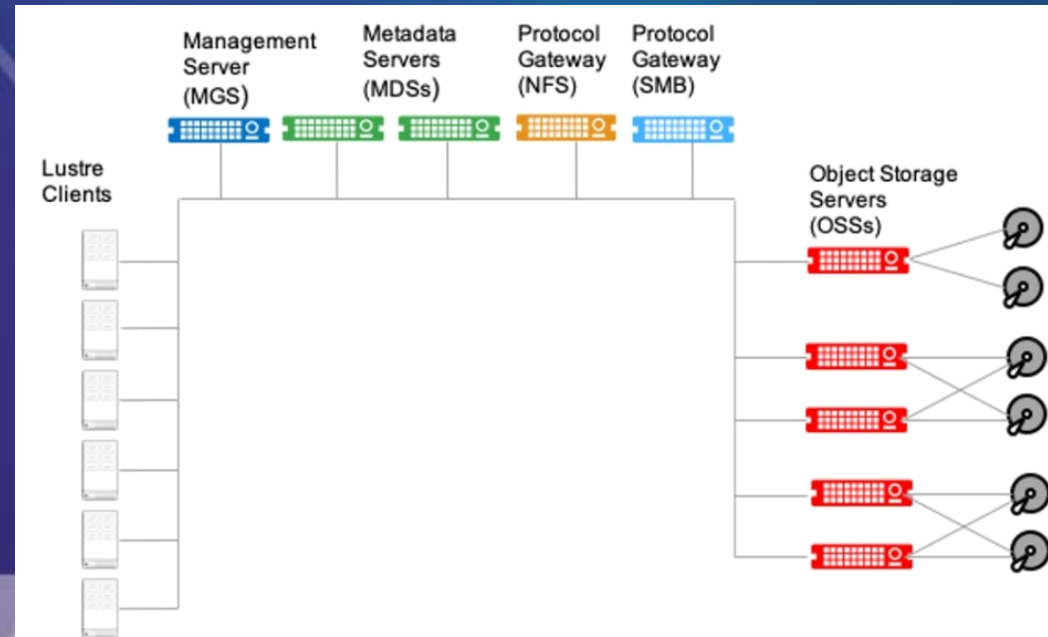
- Jest to zarazem sieciowy i rozproszony system plików.
- Ma możliwość udostępniania plików również w sieciach WAN.
- Jest całkowicie wirtualny.
- Przechowywany jest na replikowanych serwerach danych.

# GPFS (*General Parallel File System*)

- Powszechny równoległy system plików.
- Produkt komercyjny firmy IBM.
- Dane mogą być rozproszone na wiele dysków, a każdy z węzłów może uzyskać dostęp do tego samego pliku w tym samym czasie.
- Możliwe są dwie konfiguracje dostępu:
  - sieć SAN
  - bezpośrednia pamięć masowa.

# Lustre

- Lustre - klastrowy system plików używany aktualnie jedynie na platformach linux.
- Dane przechowywane w Lustre są traktowane jak obiekty.
- Metadane tych obiektów przechowywane są oddzielnie na serwerach metadanych (MDS).



# PVFS (*Parallel Virtual File System*)

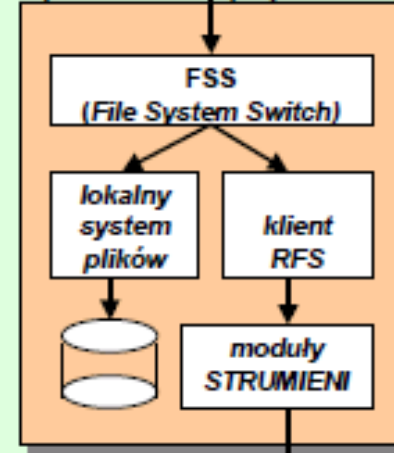
- Równoległy wirtualny system plików, który zapewnia wysoką wydajność aplikacji rozproszonych lub równoległych.
- Węzłom wejścia-wyjścia w PVFS udostępniana jest część dysków wewnętrznych.
- Przestrzeń plików tych dysków jest następnie rozpraszana na cały klaster, a dostęp do niego można uzyskać przez sieć Ethernet, moduł jądra oraz bibliotekę libpvfs zainstalowaną na komputerach klientach.
- PVFS nie zawiera obecnie środków dla redundancji danych.
- Odtworzenie uszkodzonego węzła jest również niemożliwe.

# ReFS

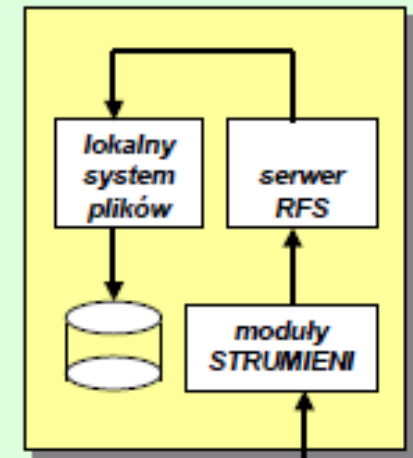
## Dziedzina RFS



## KLIENT wywołanie funkcji systemowej



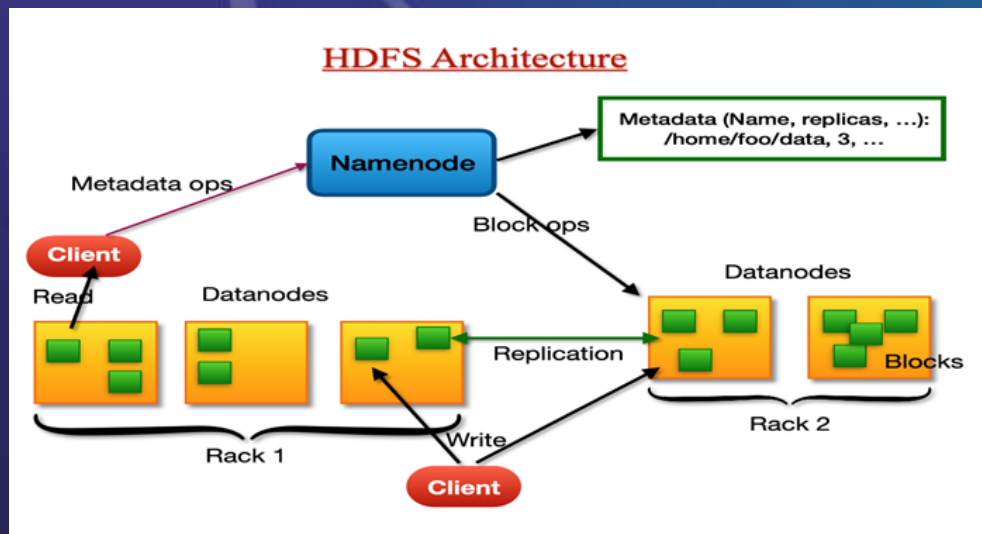
## SERWER





# Architektura systemu plików

- Apache Hadoop HDFS to rozproszony system plików Hadoop.
- Przeznaczony do przechowywania dużych plików na tanim sprzęcie.
- Odporny na błędy - zapewnia aplikacjom wysoką przepustowość.
- System plików Hadoop HDFS zapewnia architekturę Master i Slave.
- Węzeł główny uruchamia demony węzła nazwy, a węzły podrzędne uruchamiają demony węzła danych.



# Charakterystyka HDFS

- Odporność na uszkodzenia dzięki replikacji danych.
- Monitoring - istnieje ciągłe „bicie serca” komunikacji między węzłami danych do NameNode.
- Wyważanie - proces automatycznej migracji bloków danych z jednego węzła do drugiego.
- Zarządzanie integralnością - HDFS używa sum kontrolnych, które są skutecznym „podpisem cyfrowym”.
- Replikacja metadanych - pliki metadanych są podatne również na niepowodzenia, dlatego HDFS może zostać tak skonfigurowany, aby tworzyć repliki plików metadanych.



# System plików - podsumowanie

- Systemy obecnie budowane nie są wszechstronne.
- Żaden z przedstawionych systemów nie będzie rozwiązywał wszystkich potrzeb użytkowników.
- Dzięki dużej różnorodności istnieje możliwość implementacji najlepszego dla indywidualnych potrzeb.
- Oprogramowanie płatne jest stabilniejsze i bardziej skalowalne.

# Funkcje serwera

System udostępnia następujące funkcje, które można instalować za pomocą poleceń konsoli Server Manager:

- Background Intelligent Transfer Service
- Windows BitLocker Drive Encryption
- Desktop Experience
- Internet Storage Naming
- Server LPR Port Monitor
- Message Queuing

# Funkcje serwera

- Multipath I/O
- Removable Storage Manager
- Remote Assistance
- RPC over HTTP Proxy
- Simple TCP/IP Server
- SMTP Server
- Telnet Client
- Telnet Server
- TFTP Client

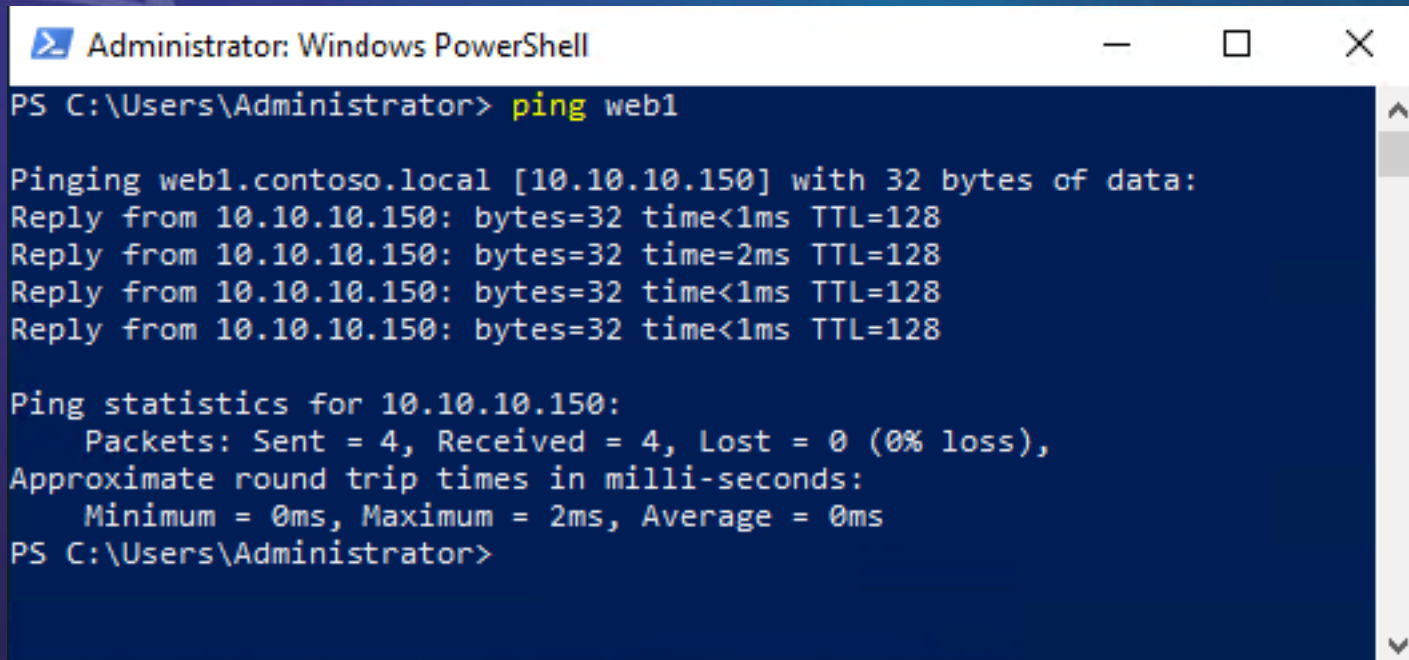
# Narzędzia sieciowe

Bezpłatne narzędzia sieciowe:

- ping,
- tracert,
- pathping,
- Test-Connection,
- telnet,
- Test-NetConnection.

# Polecenie ping

- Służy do wysłania zapytania o nazwę DNS i (lub) adres IP, po którym następuje oczekiwanie na
- Jest głównym narzędziem do testowania łączności między dwoma urządzeniami w sieci.



```
Administrator: Windows PowerShell
PS C:\Users\Administrator> ping web1

Pinging web1.contoso.local [10.10.10.150] with 32 bytes of data:
Reply from 10.10.10.150: bytes=32 time<1ms TTL=128
Reply from 10.10.10.150: bytes=32 time=2ms TTL=128
Reply from 10.10.10.150: bytes=32 time<1ms TTL=128
Reply from 10.10.10.150: bytes=32 time<1ms TTL=128

Ping statistics for 10.10.10.150:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 2ms, Average = 0ms
PS C:\Users\Administrator>
```

# Polecenie tracert

- Służy do śledzenia pakietu sieciowego

```
PS C:\WINDOWS\system32> tracert www.bing.com
```

```
Tracing route to any.edge.bing.com [204.79.197.200]  
over a maximum of 30 hops:
```

1	<1 ms	<1 ms	<1 ms	192.168.8.1
2	1 ms	<1 ms	<1 ms	192.168.128.1
3	8 ms	7 ms	5 ms	172.17.224.1
4	11 ms	9 ms	15 ms	172.19.253.1
5	10 ms	9 ms	11 ms	172.31.255.1
6	20 ms	9 ms	13 ms	htl-max1-1.iserv.net [206.114.55.1]
7	15 ms	12 ms	8 ms	69.87.144.9
8	23 ms	18 ms	19 ms	888-2.iserv.net [206.114.40.2]
9	23 ms	20 ms	15 ms	g5-0-0.core3.grr.iserv.net [206.114.51.20]
10	19 ms	11 ms	19 ms	g5-0-0.core1.grr.iserv.net [206.114.51.2]
11	21 ms	28 ms	19 ms	GigabitEthernet4-1.GW5.DET5.ALTER.NET [152.179.10.81]
12	25 ms	28 ms	28 ms	0.ae1.XL3.CHI13.ALTER.NET [140.222.225.179]
13	27 ms	37 ms	54 ms	TenGigE0-6-0-1.GW2.CHI13.ALTER.NET [152.63.65.133]
14	36 ms	34 ms	34 ms	microsoft-gw.customer.alter.net [152.179.105.130]
15	58 ms	50 ms	46 ms	104.44.81.58
16	34 ms	33 ms	36 ms	10.201.194.219
17	26 ms	29 ms	29 ms	a-0001.a-msedge.net [204.79.197.200]

```
Trace complete.
```

```
PS C:\WINDOWS\system32>
```

```
Windows PowerShell
```

```
Copyright (C) 2015 Microsoft Corporation. All rights reserved.
```

```
PS C:\Users\jkrause> tracert www.bing.com
```

```
Tracing route to any.edge.bing.com [204.79.197.200]  
over a maximum of 30 hops:
```

1	9 ms	1 ms	1 ms	192.168.8.1
2	*			192.168.8.1 reports: Destination host unreachable.

```
Trace complete.
```

```
PS C:\Users\jkrause>
```



# Polecenie pathping

- Polecenie pathping wykonuje dokładnie to samo co tracert.
- Dodatkowo - pokazuje, z którego interfejsu sieciowego komputera są wysyłane pakiety.

```
PS C:\Users\jkrause> pathping www.bing.com

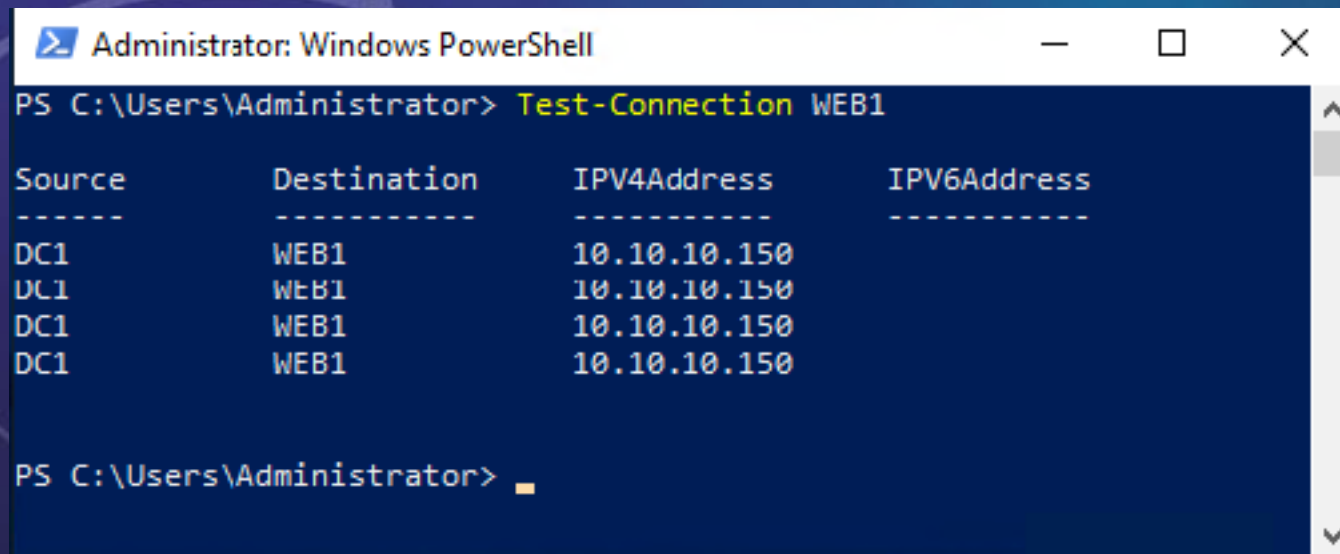
Tracing route to any.edge.bing.com [204.79.197.200]
over a maximum of 30 hops:
  0  IVO-PC-328 [192.168.8.113]
  1  192.168.8.1
  2  192.168.128.1
  3  *          192.168.8.1 reports: Destination host unreachable.

Computing statistics for 75 seconds...
Hop  RTT      Source to Here   This Node/Link   Address
    0                               Lost/Sent = Pct  Lost/Sent = Pct
  0                               0/ 100 = 0%      IVO-PC-328 [192.168.8.113]
    1    1ms      0/ 100 = 0%      0/ 100 = 0%      |
    2    ---     100/ 100 =100%  100/ 100 =100%   192.168.8.1
    3    ---     100/ 100 =100%  0/ 100 = 0%      |
    4    ---     100/ 100 =100%  0/ 100 = 0%      192.168.128.1
    5    ---     100/ 100 =100%  0/ 100 = 0%      |
    6    ---     100/ 100 =100%  0/ 100 = 0%      IVO-PC-328 [0.0.0.0]

Trace complete.
PS C:\Users\jkrause>
```

# Polecenie Test-Connection

- Nowsze narzędzie, które można wywołać tylko w powłoce PowerShell.
- Podobne do polecenia ping - bardziej przyjazne dla użytkownika z nową kolumną danych *Source*.



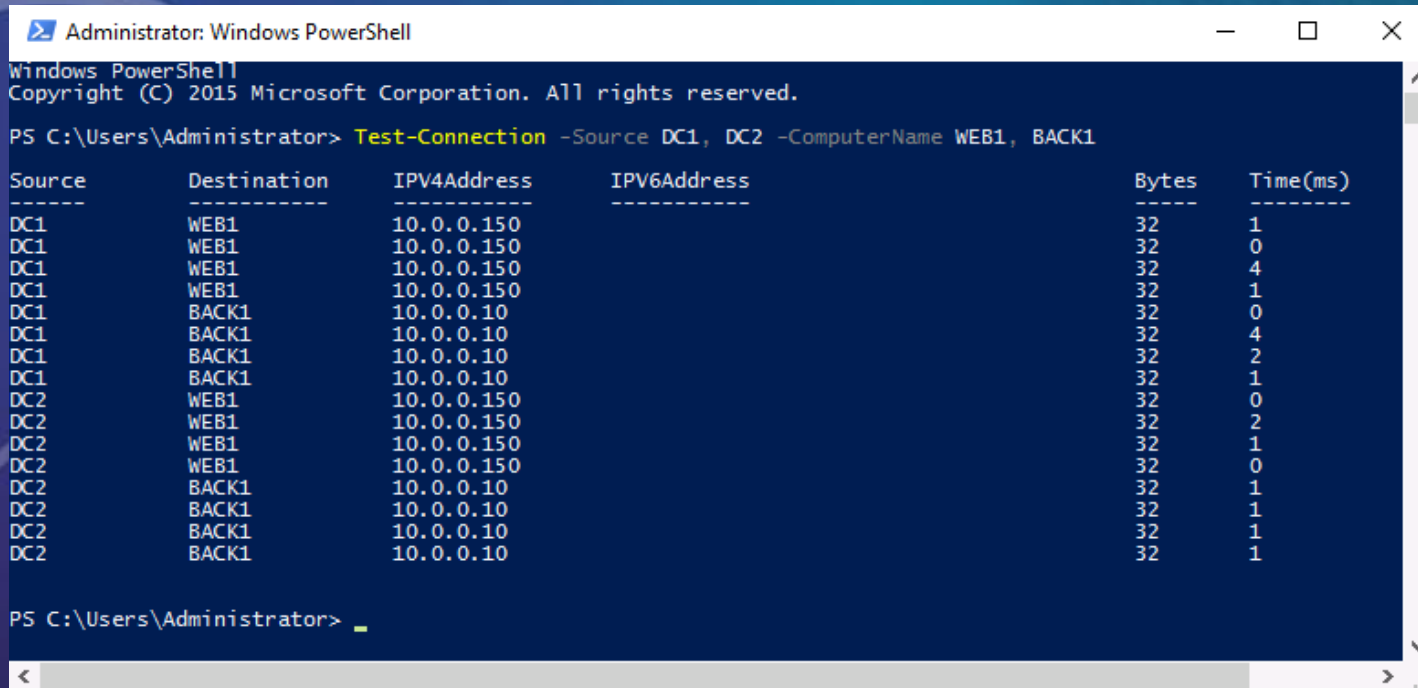
The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command `Test-Connection WEB1` has been executed. The output is a table with four columns: `Source`, `Destination`, `IPv4Address`, and `IPv6Address`. The `Source` column contains the value `DC1` for all four rows. The `Destination` column contains the value `WEB1` for all four rows. The `IPv4Address` column contains the value `10.10.10.150` for all four rows. The `IPv6Address` column is empty for all four rows.

```
PS C:\Users\Administrator> Test-Connection WEB1
```

Source	Destination	IPv4Address	IPv6Address
DC1	WEB1	10.10.10.150	
DC1	WEB1	10.10.10.150	
DC1	WEB1	10.10.10.150	
DC1	WEB1	10.10.10.150	

```
PS C:\Users\Administrator>
```

# Polecenie Test-Connection



The screenshot shows a Windows PowerShell window titled "Administrator: Windows PowerShell". The command executed is `Test-Connection -Source DC1, DC2 -ComputerName WEB1, BACK1`. The output is a table with columns: Source, Destination, IPV4Address, IPV6Address, Bytes, and Time(ms). The table lists connection statistics for DC1 and DC2 to WEB1 and BACK1.

Source	Destination	IPV4Address	IPV6Address	Bytes	Time(ms)
DC1	WEB1	10.0.0.150		32	1
DC1	WEB1	10.0.0.150		32	0
DC1	WEB1	10.0.0.150		32	4
DC1	WEB1	10.0.0.150		32	1
DC1	BACK1	10.0.0.10		32	0
DC1	BACK1	10.0.0.10		32	4
DC1	BACK1	10.0.0.10		32	2
DC1	BACK1	10.0.0.10		32	1
DC2	WEB1	10.0.0.150		32	0
DC2	WEB1	10.0.0.150		32	2
DC2	WEB1	10.0.0.150		32	1
DC2	WEB1	10.0.0.150		32	0
DC2	BACK1	10.0.0.10		32	1
DC2	BACK1	10.0.0.10		32	1
DC2	BACK1	10.0.0.10		32	1
DC2	BACK1	10.0.0.10		32	1

Statystyki dotyczące komunikowania się źródłowych serwerów DC1 i DC2 z docelowymi maszynami WEB1 i BACK1

# Polecenie telnet

- Umożliwia nawiązanie połączenia między dwoma komputerami w celu zarządzania maszyną zdalną za pośrednictwem wirtualnego połączenia terminalowego.
- Usługa Telnet nie jest domyślnie dostępna w systemie Windows Server - trzeba ją zainstalować – funkcja o nazwie *Telnet Client (Klient Telnetu)*.
- Korzystając z wiersza poleceń lub programu PowerShell możemy połączyć się ze swojego komputera do usługi zdalnej.

# Polecenie Test-NetConnection

Test-NetConnection programu PowerShell to kolejny sposób na sprawdzenie określonych portów lub usług w systemie zdalnym, przy czym uzyskane dane wyjściowe są bardziej przyjazne niż w przypadku usługi Telnet.

```
PS C:\Users\Administrator> Test-NetConnection WEB1 -Port 80  
WARNING: TCP connect to (10.10.10.150 : 80) failed
```

```
ComputerName      : WEB1  
RemoteAddress     : 10.10.10.150  
RemotePort       : 80  
InterfaceAlias    : Ethernet  
SourceAddress     : 10.10.10.10  
PingSucceeded     : True  
PingReplyDetails (RTT) : 1 ms  
TcpTestSucceeded  : False
```

```
PS C:\Users\Administrator>  
PS C:\Users\Administrator> Test-NetConnection WEB1 -Port 80
```

```
ComputerName      : WEB1  
RemoteAddress     : 10.10.10.150  
RemotePort       : 80  
InterfaceAlias    : Ethernet  
SourceAddress     : 10.10.10.10  
TcpTestSucceeded  : True
```

```
PS C:\Users\Administrator>
```

# Domena Windows

- Kontrolery domeny mogą być jednocześnie serwerami usług sieciowych.
- Domeny Windows zmieniły się wraz z rozwojem systemów operacyjnych Windows.
- Wyróżniamy 2 typy domen:
  - Domena typu NT 4
  - Domena Active Directory



# PowerShell

Wyświetlenie wszystkich dostępnych ról i funkcji

**Get-WindowsFeature**

Wyszukanie funkcji o nazwach rozpoczynających się od liter TEL

**Get-WindowsFeature -Name TEL\***

Polecenie instalacji funkcji Telnet-Client

**Add-WindowsFeature Telnet-Client**

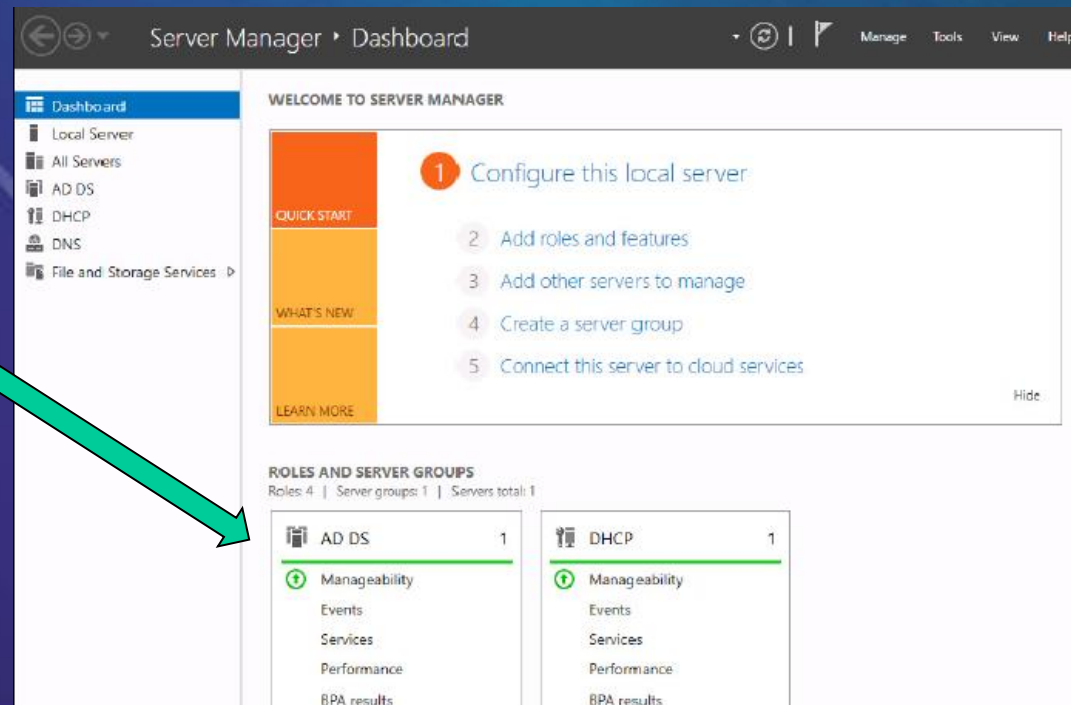
Wyświetlenie ról i funkcji zainstalowanych na serwerze

**Get-WindowsFeature | Where Installed**

# Serwer Menager

- Umożliwia szybkie sprawdzenie, co jest obecnie zainstalowane na serwerze.
- Kolumna po lewej stronie prezentuje listę ról zainstalowanych i możliwych do zarządzania.

AD DS i DHCP działają normalnie — nazwy podkreślone zieloną linią.



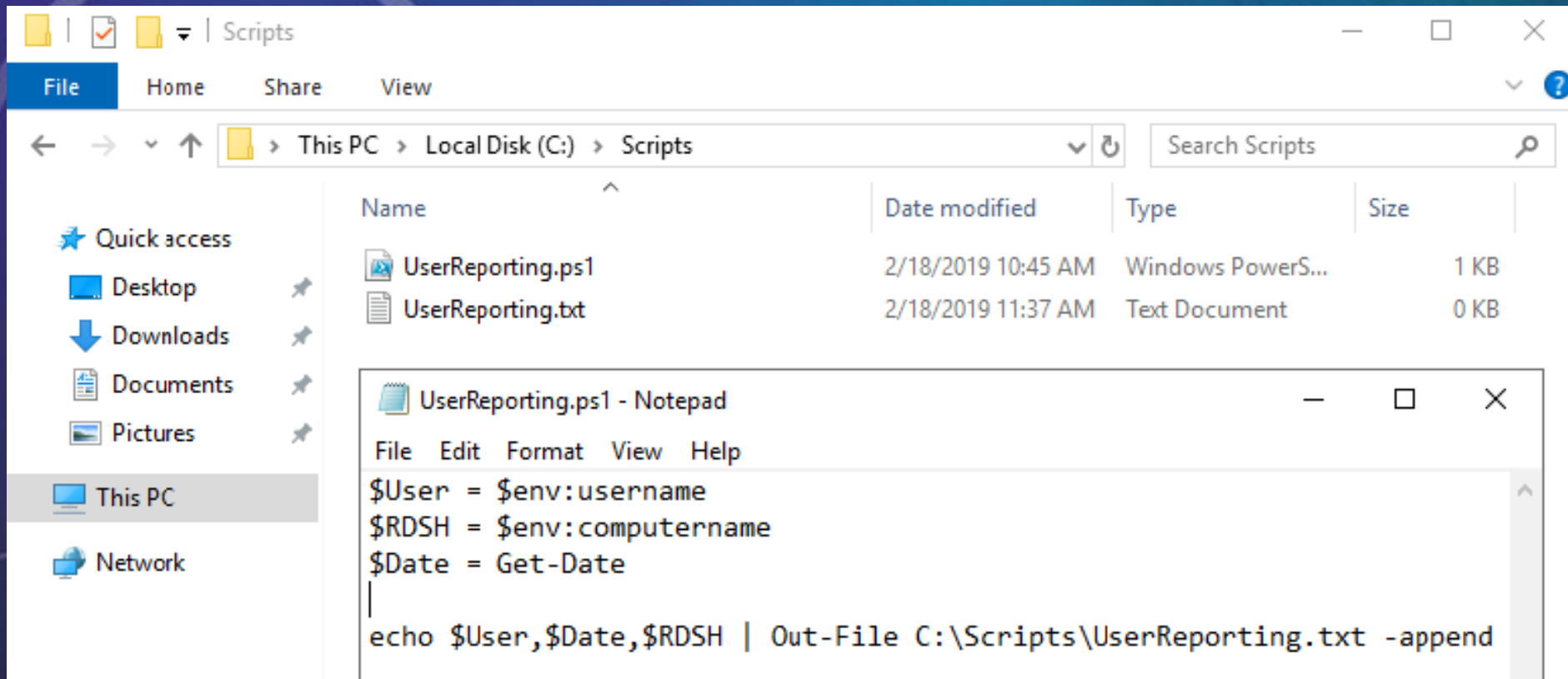
# PowerShell

- Zasady wykonywania skryptów mają pięć różnych poziomów:
  - **Restricted** - blokują wykonywanie skryptów,
  - **AllSigned** - każdy uruchamiany skrypt musi zostać podpisany przez zaufanego wydawcę,
  - **RemoteSigned** – domyślna zasada – własne skrypty mogą być uruchamiane, nawet jeśli nie będą podpisane cyfrowo,
  - **Unrestricted** - podpisane lub niepodpisane skrypty mogą być uruchamiane, ostrzeżenie podczas korzystania ze skryptów pobranych z internetu,
  - **Bypass** - nic nie jest blokowane i nie są wyświetlane żadne ostrzeżenia podczas uruchamiania skryptów.

# PowerShell

- Zasady DEP (Default Execution Policy) można dodatkowo ulepszyć przez określenie zakresu zasad wykonywania (*Execution Policy Scope*).
- Można wykorzystywać trzy zakresy:
  - Process ,
  - CurrentUser,
  - Local-Machine.
- Domyślnie zasady DEP dotyczą maszyny lokalnej.

# PowerShell



The screenshot displays a Windows File Explorer window titled 'Scripts' with the address bar showing 'This PC > Local Disk (C:) > Scripts'. The left sidebar shows 'Quick access' with links to Desktop, Downloads, Documents, and Pictures, and 'This PC' with a link to Network. The main pane shows a table of files:

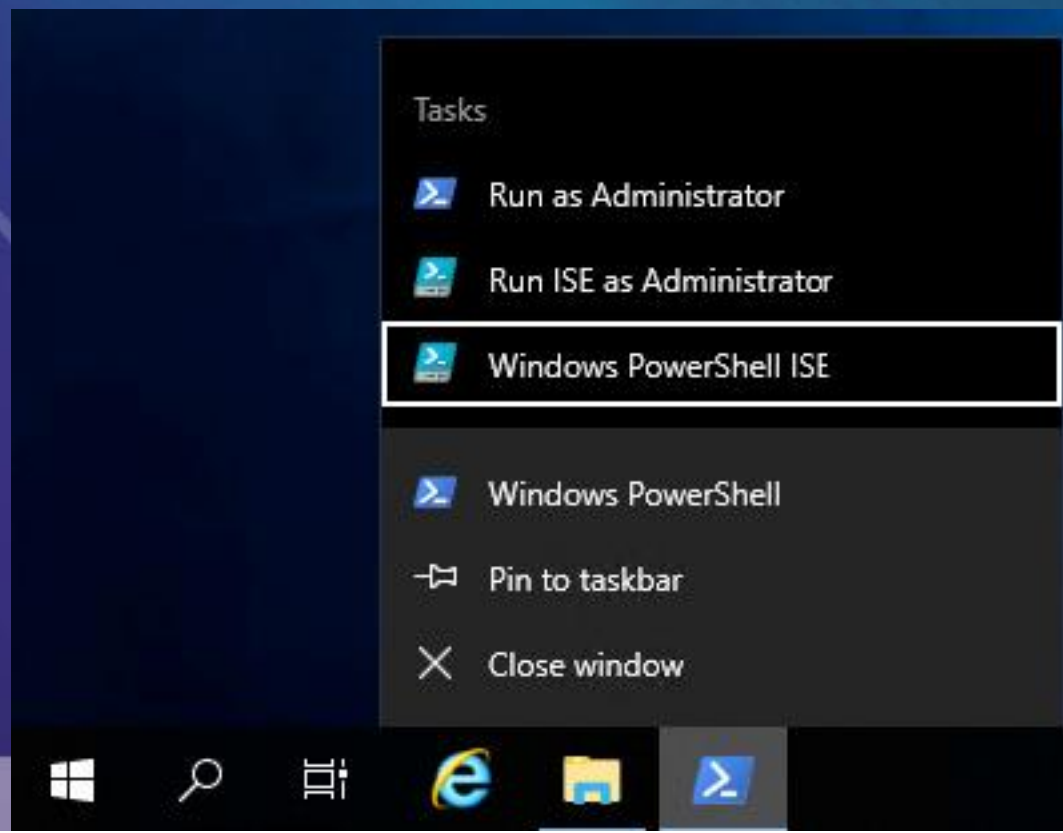
Name	Date modified	Type	Size
UserReporting.ps1	2/18/2019 10:45 AM	Windows PowerS...	1 KB
UserReporting.txt	2/18/2019 11:37 AM	Text Document	0 KB

Below the table, a Notepad window titled 'UserReporting.ps1 - Notepad' is open, showing the following PowerShell script:

```
File Edit Format View Help
$User = $env:username
$RDSH = $env:computername
$Date = Get-Date
|
echo $User,$Date,$RDSH | Out-File C:\Scripts\UserReporting.txt -append
```

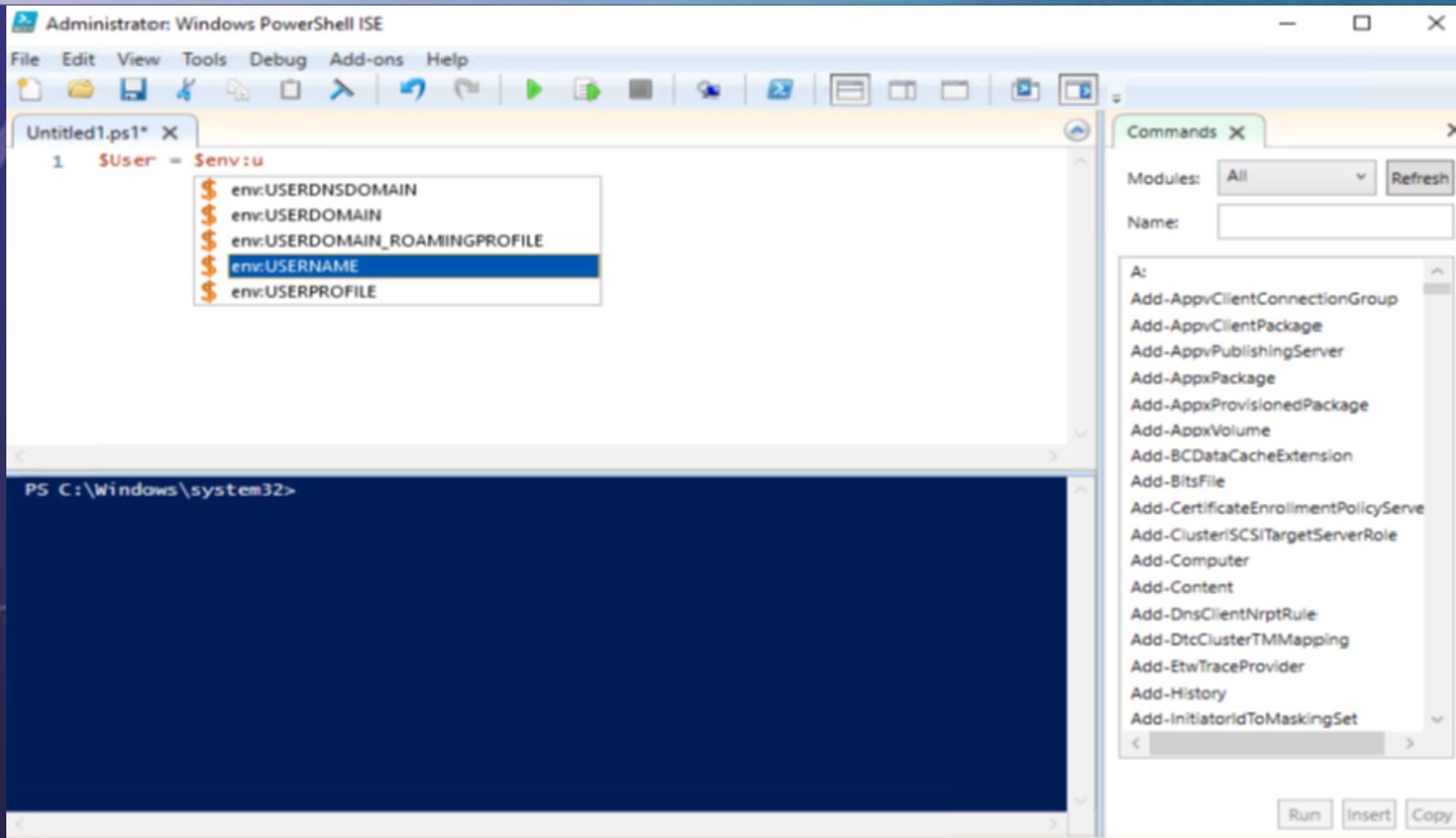
# Zintegrowane środowisko skryptowe PowerShell

- **Zintegrowane środowisko skryptowe PowerShell (ISE)** - program instalowany domyślnie w systemie Windows Server, który pozwala na tworzenie skryptów PowerShell i zapewnia odpowiednie wsparcie.

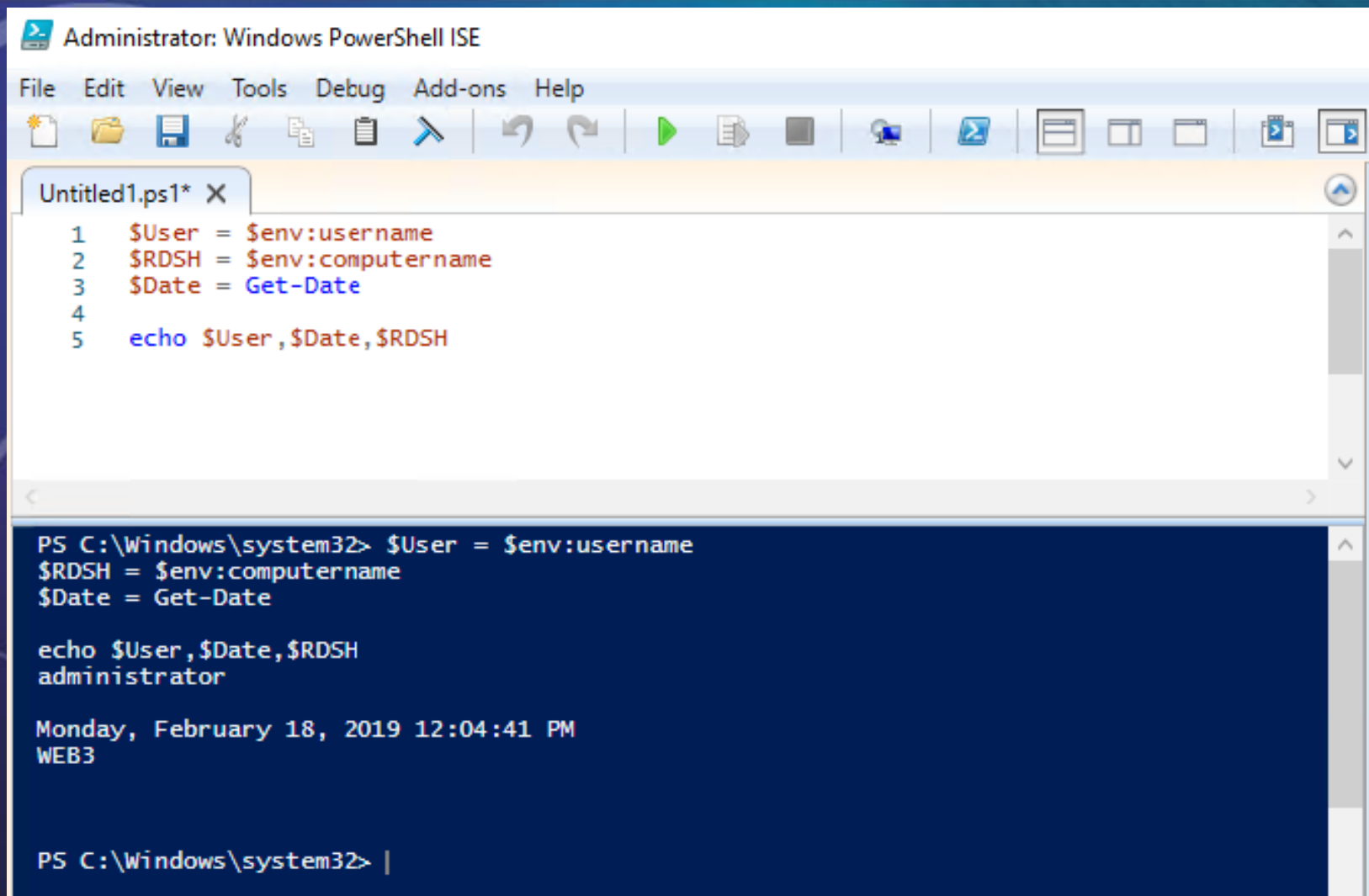




# Zintegrowane środowisko skryptowe PowerShell



# Zintegrowane środowisko skryptowe PowerShell

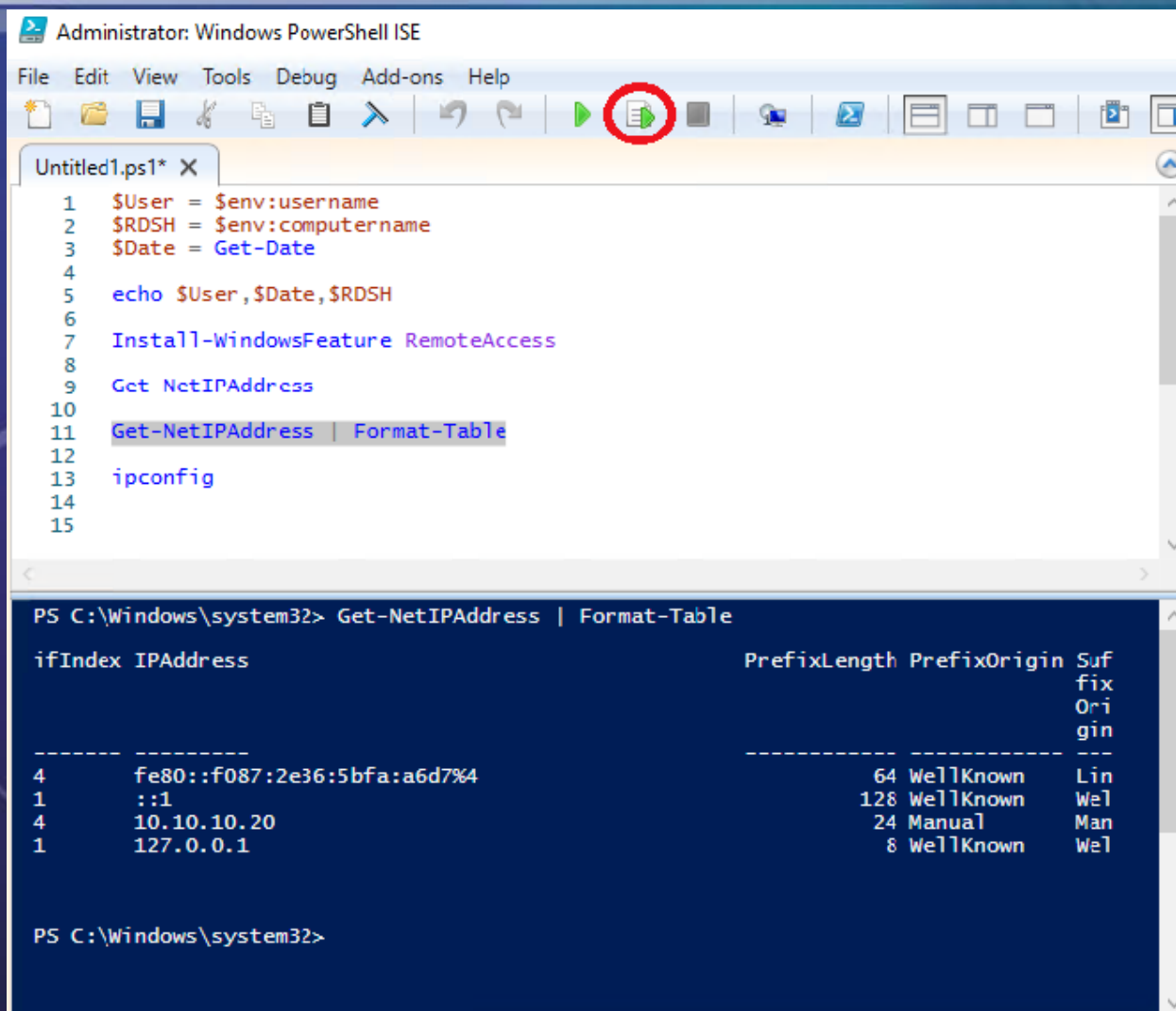


The screenshot displays the Windows PowerShell ISE (Integrated Scripting Environment) running as Administrator. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. The toolbar contains icons for file operations (New, Open, Save, Print), editing (Cut, Copy, Paste), and execution (Run, Stop, Breakpoint). The script editor shows a file named "Untitled1.ps1\*" with the following PowerShell script:

```
1 $User = $env:username
2 $RDSH = $env:computername
3 $Date = Get-Date
4
5 echo $User,$Date,$RDSH
```

The console window below the editor shows the execution of the script. The prompt is "PS C:\Windows\system32>". The script's output is displayed on three lines: "administrator", "Monday, February 18, 2019 12:04:41 PM", and "WEB3". The console prompt is now "PS C:\Windows\system32> |".

# Zintegrowane środowisko skryptowe PowerShell



The screenshot shows the Windows PowerShell ISE interface. The title bar reads "Administrator: Windows PowerShell ISE". The menu bar includes File, Edit, View, Tools, Debug, Add-ons, and Help. The toolbar contains various icons, with the Run icon (a green play button) circled in red. The script editor shows a file named "Untitled1.ps1" with the following code:

```
1 $User = $env:username
2 $RDSH = $env:computername
3 $Date = Get-Date
4
5 echo $User,$Date,$RDSH
6
7 Install-WindowsFeature RemoteAccess
8
9 Get-NetIPAddress
10
11 Get-NetIPAddress | Format-Table
12
13 ipconfig
14
15
```

The console window shows the command prompt at "PS C:\Windows\system32>". The command "Get-NetIPAddress | Format-Table" has been executed, resulting in the following output:

```
PS C:\Windows\system32> Get-NetIPAddress | Format-Table

ifIndex IPAddress                               PrefixLength PrefixOrigin SuffixOrigin
-----
4 fe80::f087:2e36:5bfa:a6d7%4 64 WellKnown   Link
1 ::1 128 WellKnown   Local
4 10.10.10.20 24 Manual     Manu
1 127.0.0.1 8 WellKnown   Local
```

The prompt "PS C:\Windows\system32>" is visible at the bottom of the console window.

# Certyfikaty w systemie Windows Server

Ogólnie używane typy certyfikatów:

- **Użytkownika** – proces uwierzytelniania użytkownika w sieci.
- **Komputera** - wspieranie interakcji między siecią a samym kontem komputera.
- **SSL** - najczęściej używane do zabezpieczenia ruchu na stronie WWW.

# Implementowanie usług certyfikatów AD

- Środowisko certyfikatów jest znane pod nazwą infrastruktury klucza publicznego (*Public Key Infrastructure*) — PKI.
- Systemu Server umożliwia utworzenie serwera urzędu certyfikacji w sieci.

Select role services

DESTINATION SERVER  
CA1.contoso.local

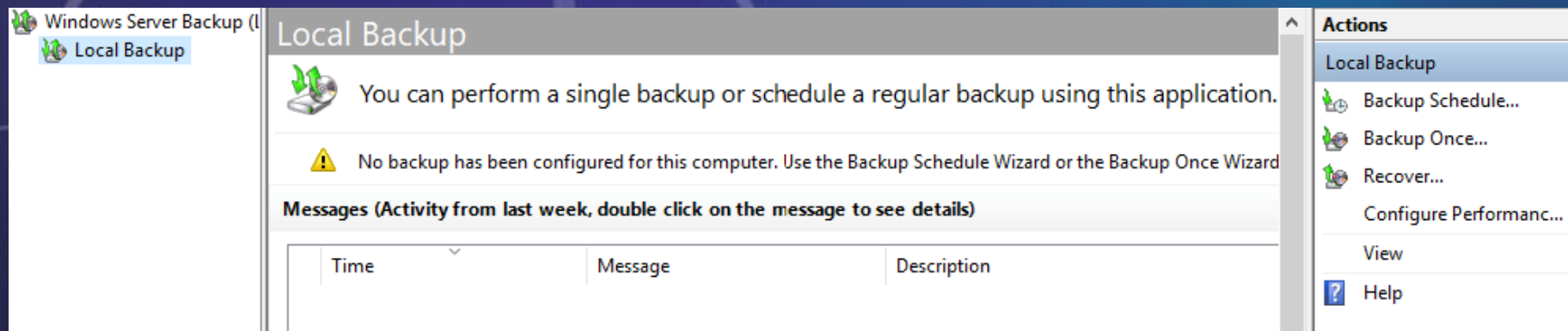
Before You Begin  
Installation Type  
Server Selection  
Server Roles  
Features  
AD CS  
Role Services  
Web Server Role (IIS)  
Role Services  
Confirmation  
Results

Select the role services to install for Active Directory Certificate Services

Role services	Description
<input checked="" type="checkbox"/> Certification Authority	Certification Authority (CA) is used to issue and manage certificates. Multiple CAs can be linked to form a public key infrastructure.
<input type="checkbox"/> Certificate Enrollment Policy Web Service	
<input type="checkbox"/> Certificate Enrollment Web Service	
<input checked="" type="checkbox"/> Certification Authority Web Enrollment	
<input type="checkbox"/> Network Device Enrollment Service	
<input type="checkbox"/> Online Responder	


# Kopia zapasowa i jej przywracanie

- System operacyjny Server udostępnia funkcje do zarządzania serwerami.
- Pozwala tworzyć odpowiedni harmonogram kopii zapasowych systemu.
- Należy pamiętać o zainstalowaniu funkcji - *Windows Server Backup*.





# Kopia zapasowa i jej przywracanie



## Specify Backup Time

Getting Started

Select Backup Configurat...

**Specify Backup Time**

Specify Destination Type

Confirmation

Summary

How often and when do you want to run backups?

☒ Once a day

Select time of day: 2:00 AM

☐ More than once a day

Click an available time and then click Add to add it to the backup schedule.

Available time:		Scheduled time:
12:00 AM	Add >	9:00 PM
12:30 AM		
1:00 AM		
1:30 AM		
2:00 AM		
2:30 AM		
3:00 AM		
3:30 AM		
4:00 AM		
4:30 AM		
	< Remove	

# Przywracanie danych z systemu Windows

- Otwórz konsolę *Windows Server Backup*.
- Wybierz akcję *Recover...(Odzyskaj...)*.
- Określ lokalizację pliku kopii zapasowej.
- Wybierz plik kopii zapasowej.



## Specify Remote Folder

Getting Started

Specify Location Type

Specify Remote Folder

Select Backup Date

Select Recovery Type

Type the Universal Naming Convention (UNC) path to the remote shared folder that contains the backup that you want to use.

Example: \\MyFileServer\SharedFolderName

# Przywracanie danych z systemu Windows



## Select Items to Recover

Getting Started

Specify Location Type

Specify Remote Folder

Select Backup Date

Select Recovery Type

Select Items to Recover

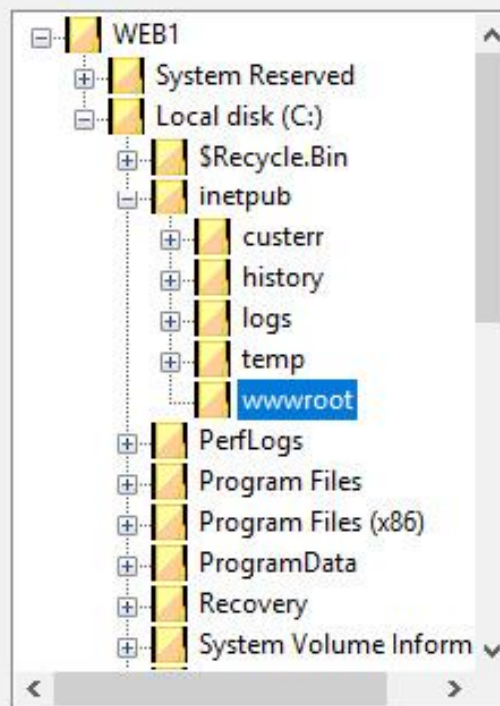
Specify Recovery Options

Confirmation

Recovery Progress

Browse the tree in Available items to find the files or folders that you want to recover. Click an item in the tree or under Name to select it for recovery.

Available items:



Items to recover:

Name	Date Modified
iisstart.htm	1/19/2019 12:...
iisstart.png	1/19/2019 12:...

# Przywracanie z płyty instalacyjnej

Choose an option



Continue

Exit and continue to Windows Server



Troubleshoot

Reset your PC or see advanced options



Turn off your PC



## Advanced options



System Image  
Recovery

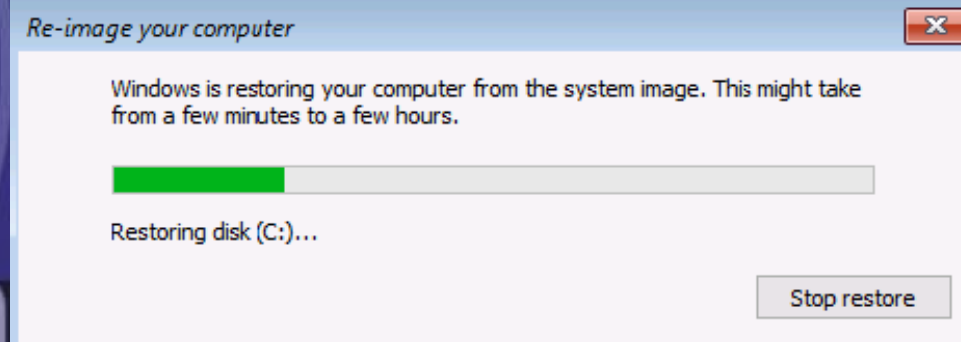
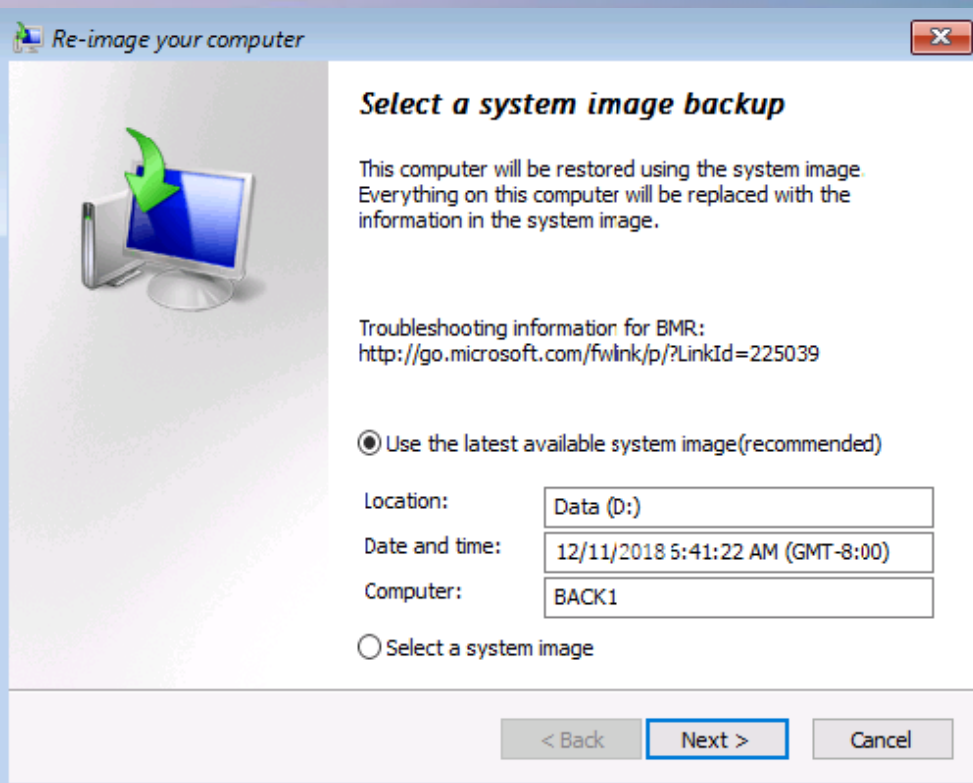
Recover Windows using a specific  
system image file



Command Prompt

Use the Command Prompt for  
advanced troubleshooting

# Przywracanie z płyty instalacyjnej



# Windows Defender Advanced Threat Protection





# Windows Defender Advanced Threat Protection

- **ATP** to rodzina produktów i systemów, które współpracują ze sobą w celu ochrony maszyn.
- Pierwszym systemem operacyjnym, który miał wbudowany antywirusowy program Defender był Server 2016.
- Program Windows Defender jest domyślnie instalowany w systemie Windows Server.
- Automatycznie wyłącza się w przypadku zainstalowania innego programu antywirusowego.

# Windows Defender ATP Exploit Guard

Podstawowe elementy rozwiązania Defender ATP Exploit Guard:

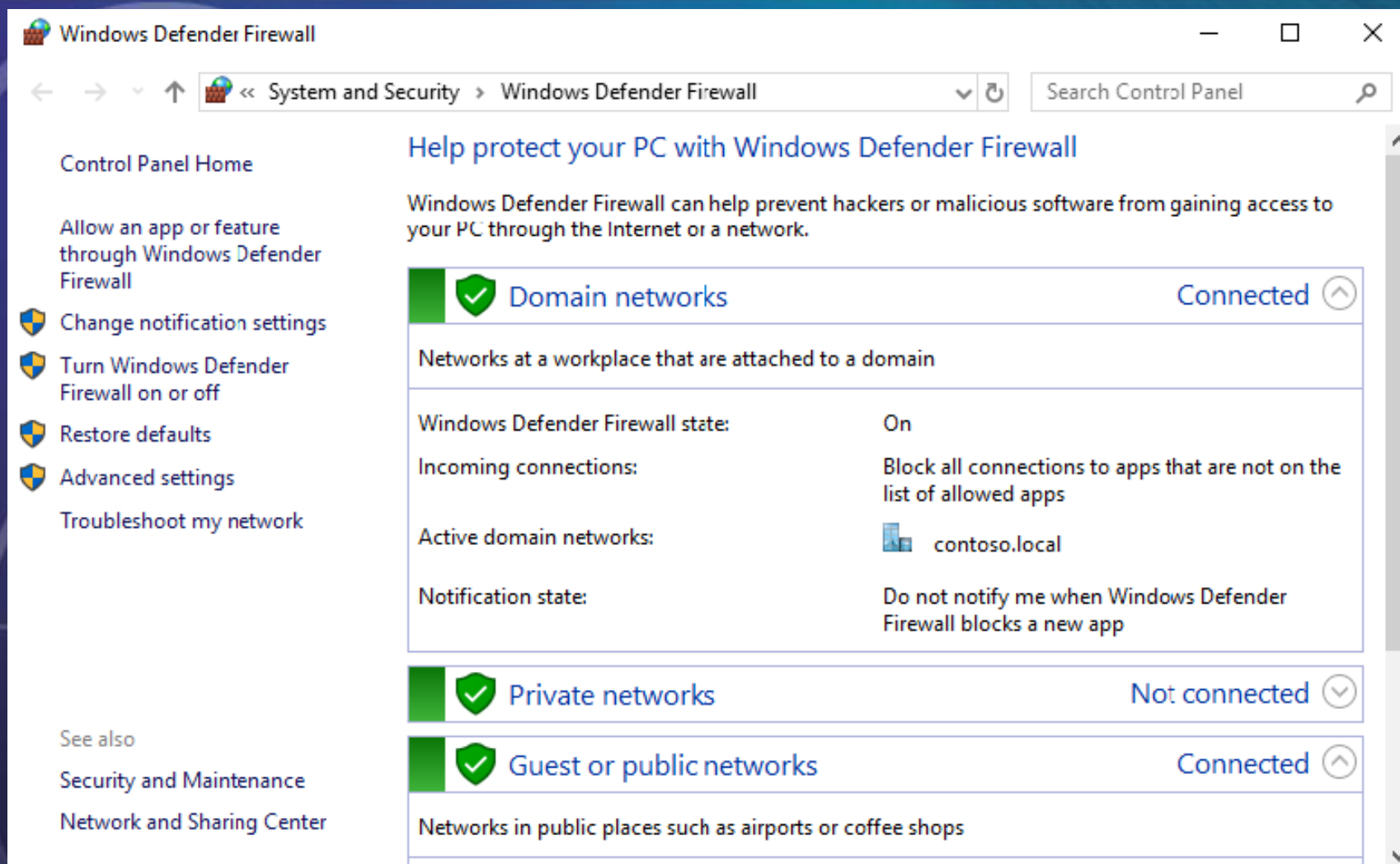
- Redukcja powierzchni ataku (*Attack Surface Reduction* - ASR).
- Ochrona sieci - włączenie filtra Windows Defender SmartScreen.
- Kontrolowany dostęp do folderu - oprogramowanie typu ransomware.
- Ochrona przed exploitami.

# Zapory systemu Windows

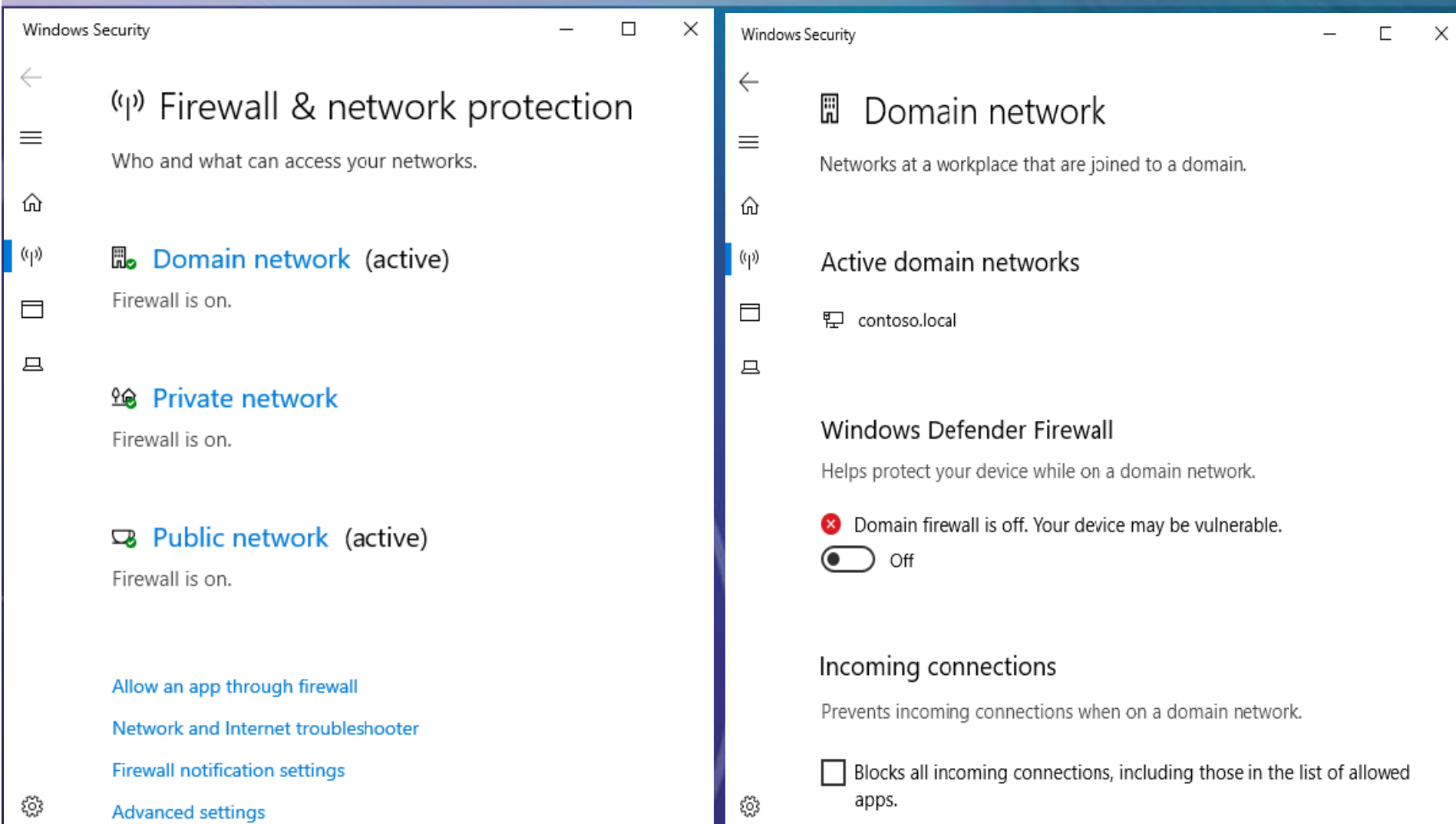
Istnieją trzy różne konsole, za pomocą których można konfigurować ustawienia zapory systemu Windows:

- Zapora Windows Defender (Panel sterowania),
- Zapora i ochrona sieci,
- Zapora Windows z zaawansowanymi zabezpieczeniami (WFAS).

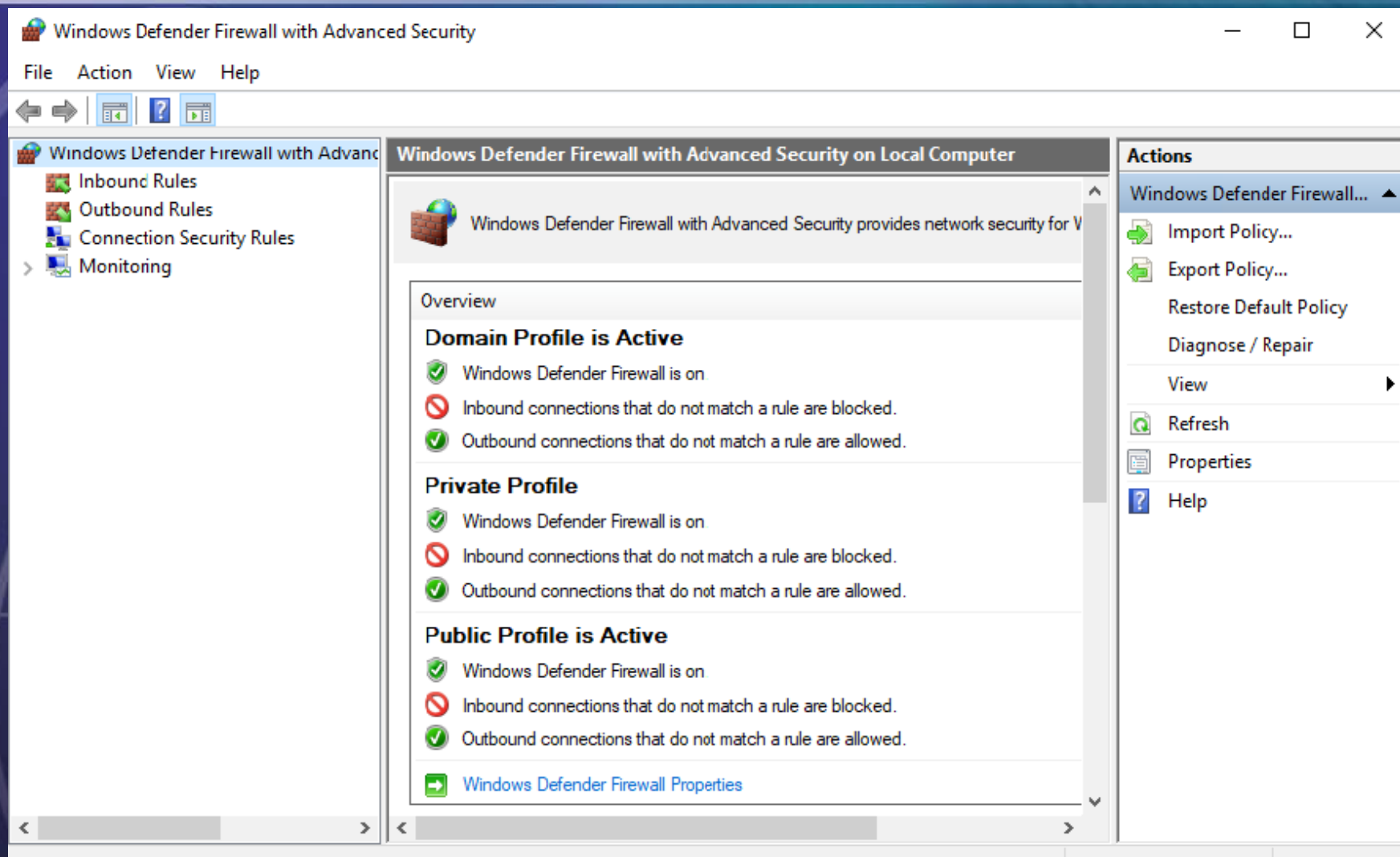
# Zapora Windows Defender (panel sterowania)



# Zapora i ochrona sieci (Ustawienia zabezpieczeń Windows)



# Zapora Windows z zaawansowanymi zabezpieczeniami (WFAS)





# Trzy różne profile zapory

Dostępne są trzy różne typy profili:

- Domain Profile
- Private Profile
- Public Profile

# Disaster recovery

- Zapasowe centrum danych - disaster recovery center, w którym przechowywane są kopie zapasowe.
- Aby stworzyć skuteczny plan działania, należy przeprowadzić dokładne analizy i kalkulacje jeszcze przed wystąpieniem awarii posługując się wskaźnikami:
  - **RPO** (Recovery Point Objective)
  - **RTO** (Recovery Time Objective)
  - **NRO** (Network Recovery Objective)
  - **MDL** (Maximum Data Loss)

# Disaster recovery

- **Disaster Recovery Plan (DRP)** obejmuje procedury i procesy, które należy uruchomić, aby przywrócić podstawowe funkcjonowanie firmy po katastrofie.
- Ważnym elementem DRP jest zapewnienie *Disaster Recovery Center*.
- Kopię zapasową można przechowywać np. w chmurze (tworząc środowisko hybrydowe).

# RTO I RPO A SKUTEKZNOŚĆ DISASTER RECOVERY

- *Recovery Point Objective (RPO)* określa częstotliwość, z jaką powinna być wykonywana kopia zapasowa danych.
- *Recovery Time Objective (RTO)* określa, ile czasu zajmie przywrócenie stanu systemu sprzed awarii.
- Dąży się aby wartości tych wskaźników były jak najniższe.
- Ustalenie optymalnych parametrów dla poszczególnych aplikacji jest najczęściej kompromisem między potrzebami biznesu, a opłacalnością.

# RTO I RPO A SKUTEKZNOŚĆ DISASTER RECOVERY

- Backup danych to za mało, aby przywrócić funkcjonowanie firmy, jeśli awarii uległa infrastruktura IT.
- Koniecznym elementem jest zapasowe centrum danych.
- Możliwe jest skorzystanie z usług:
  - *Disaster Recovery as a Service (DRaaS)* - dostawca chmurowy.
  - BaaS - własny zespół specjalizujący się w odtwarzaniu awaryjnym.