

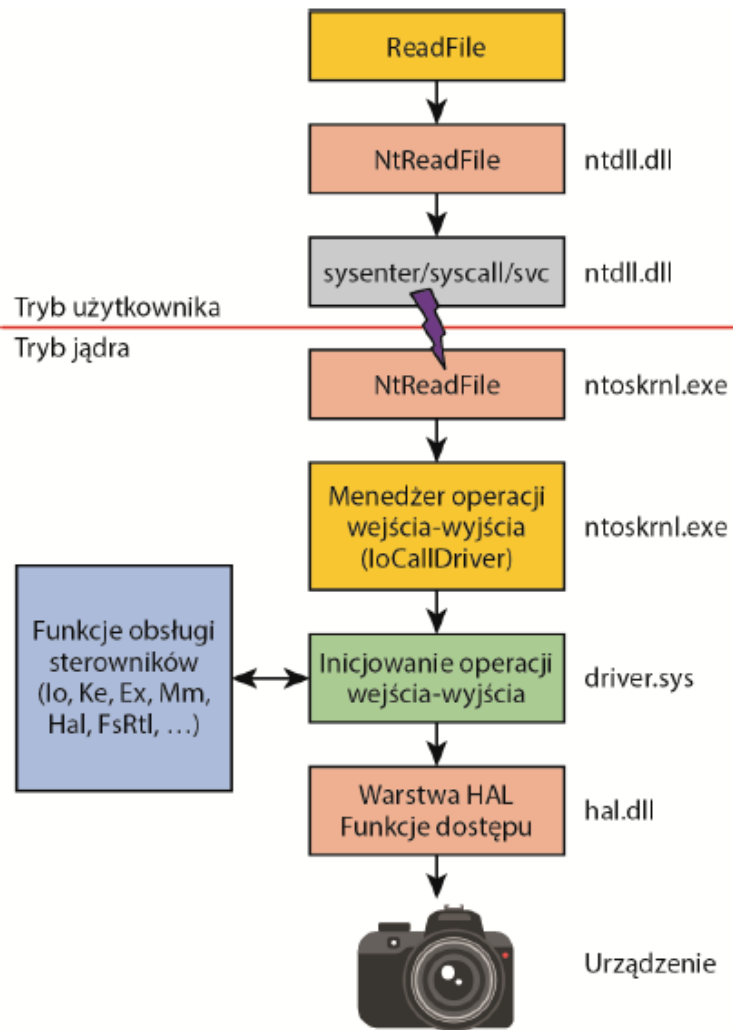
Systemy operacyjne

WYKŁAD 9 i 10

dr inż. Stanisława Plichta

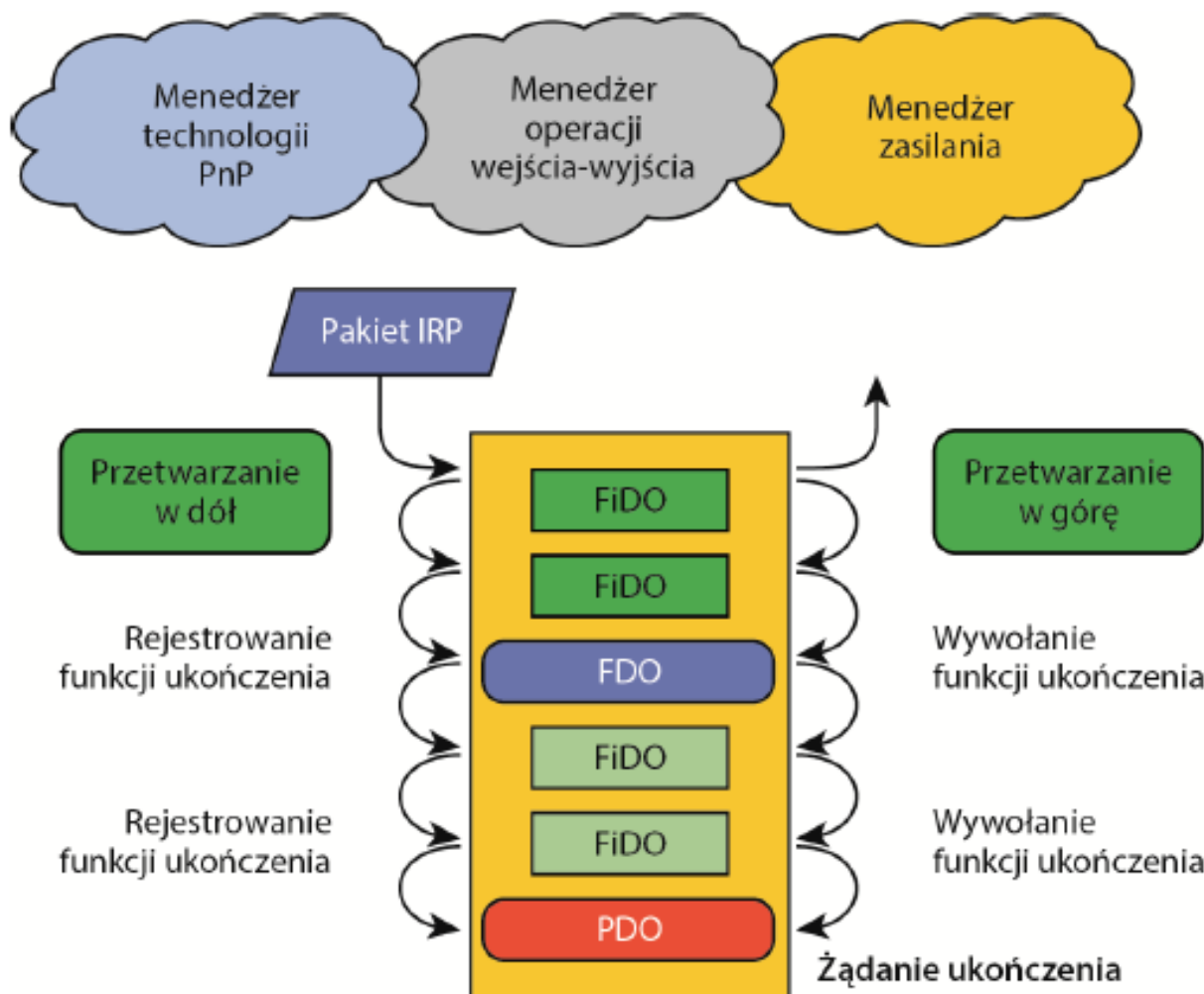
splichta@ans-ns.edu.pl

Przepływ typowego żądania operacji WE/WY



- System operacyjny dokonuje abstrakcji wszystkich żądań operacji wejścia-wyjścia jako operacji względem pliku wirtualnego, ponieważ menedżer operacji wejścia-wyjścia dysponuje informacjami wyłącznie o plikach.
- Na sterowniku spoczywa odpowiedzialność za dokonanie translacji komentarzy zorientowanych plikowo do postaci poleceń konkretnych urządzeń.

Przepływ pakietu IRP



Typy sterowników urządzeń

Klasyfikacja sterowników urządzeń:

1. Trybu jądra

- sterowniki systemu plików
- Sterowniki z obsługą technologii Plug and Play
- Sterowniki bez obsługi technologii Plug and Play

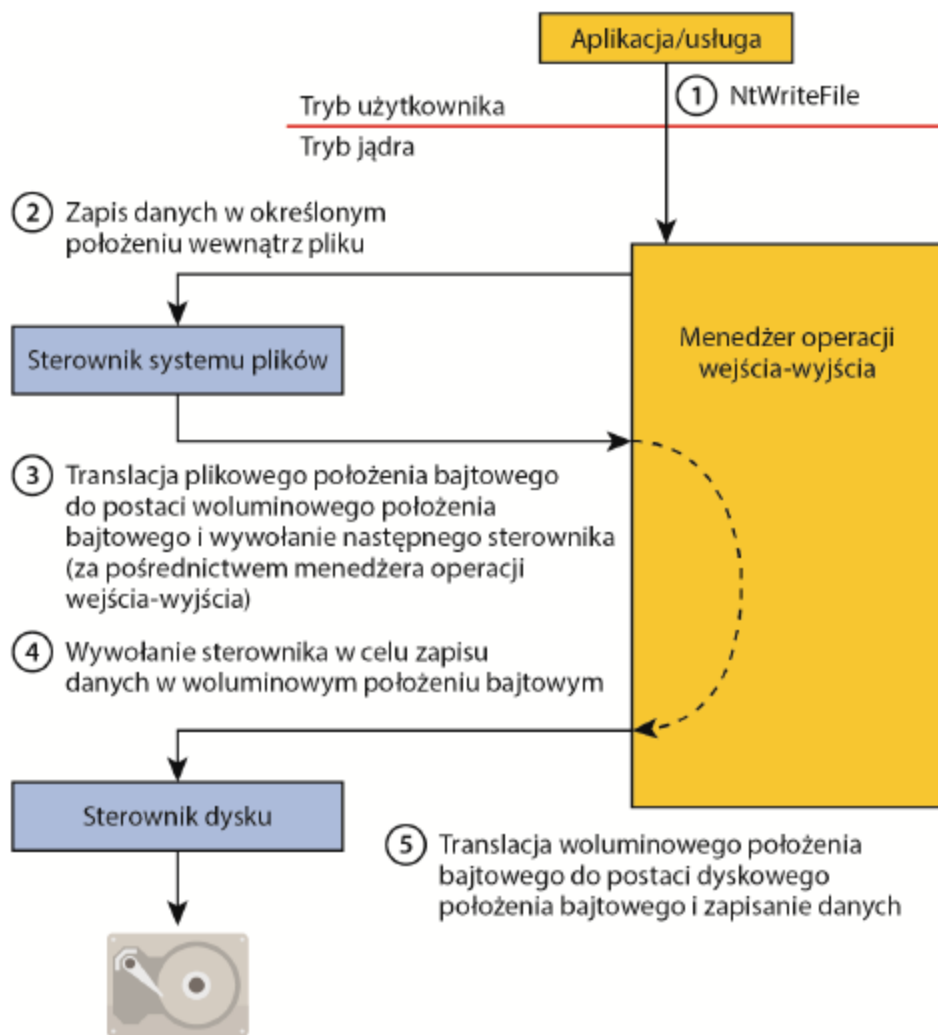
2. Trybu użytkownika

- Sterowniki drukarek podsystemu systemu Windows
- Sterowniki UMDF (User-Mode Driver Framework)

Warstwy sterowników

- Obsługa sprzętu może zostać rozdzielona między następujące komponenty:
 - Sterowniki klas.
 - Sterowniki miniklas.
 - Sterowniki portów.
 - Sterowniki miniportów.

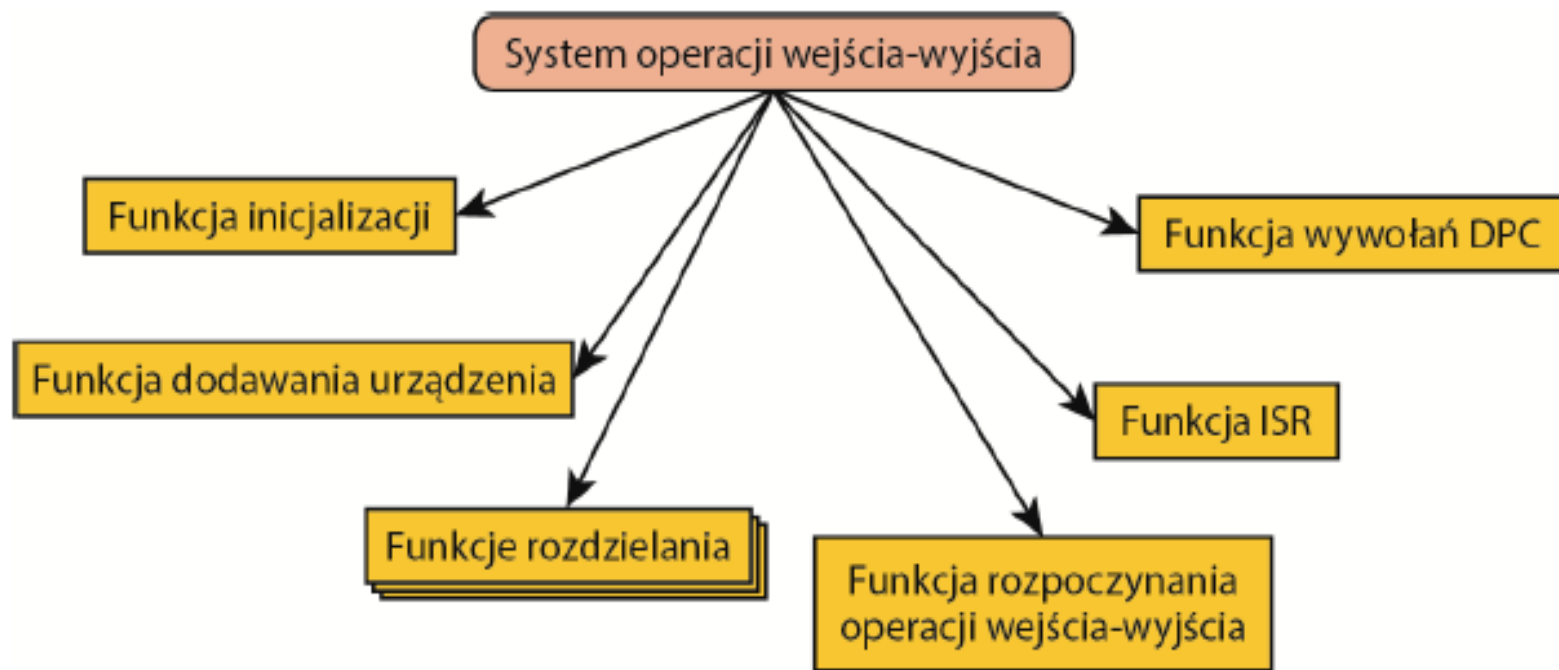
Sterownik systemu plików



1. Akceptacja żądania zapisu danych w określonym miejscu wewnątrz konkretnego pliku.
2. Translacja żądania do postaci żądania zapisującego określoną liczbę bajtów na dysku w konkretnej lokalizacji.
3. Przekazanie żądania za pośrednictwem menedżera operacji wejścia-wyjścia do sterownika dysku.
4. Sterownik dysku dokonuje translacji żądania na lokalizację fizyczną na dysku i komunikuje się w celu zapisania danych.

Warstwy sterownika systemu plików i sterownika dysku

System operacji wejścia-wyjścia nadzoruje wykonywanie funkcji sterowników urządzeń.



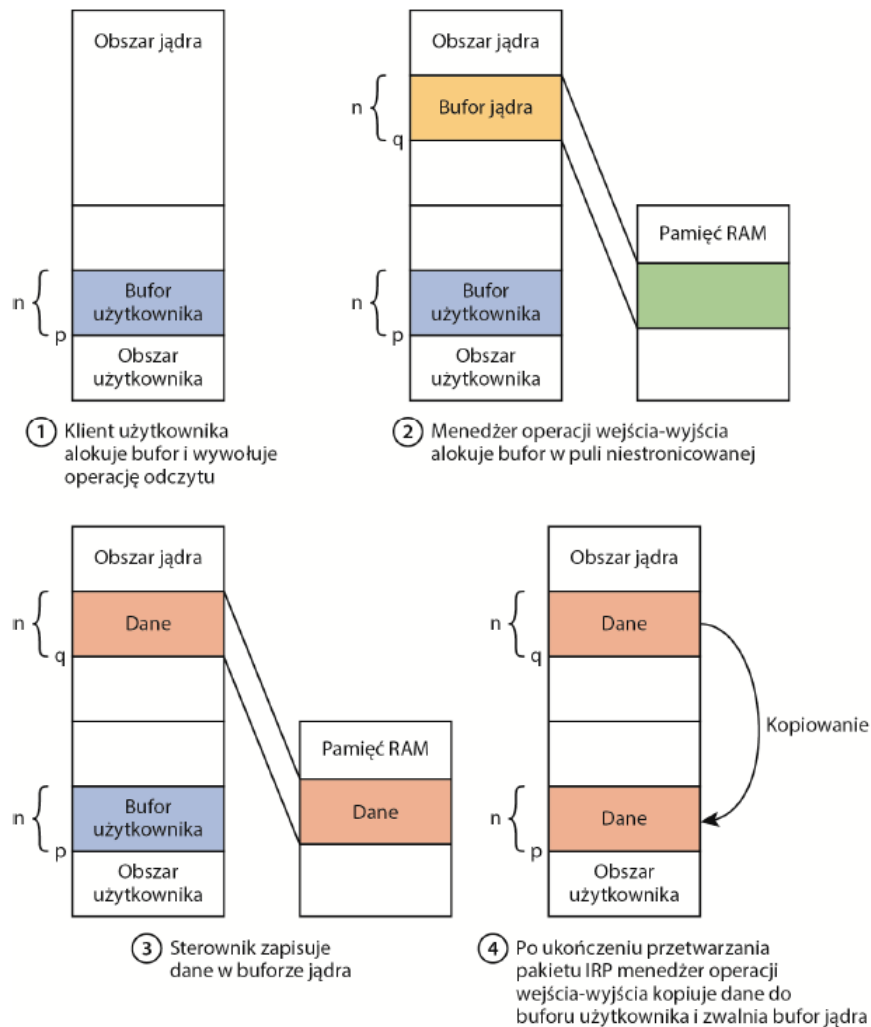
Otwieranie urządzeń

- Obiekt pliku to struktura danych trybu jądra, która reprezentuje dojście do urządzenia.
- Obiekty plików są zasobami systemowymi, które mogą być współużytkowane przez dwa lub więcej procesów trybu użytkownika.
- Obiekt pliku zawiera dane unikalne dla dojścia do obiektu, natomiast w samym pliku znajdują się dane lub tekst przeznaczony do współużytkowania.

Typy operacji wejścia-wyjścia

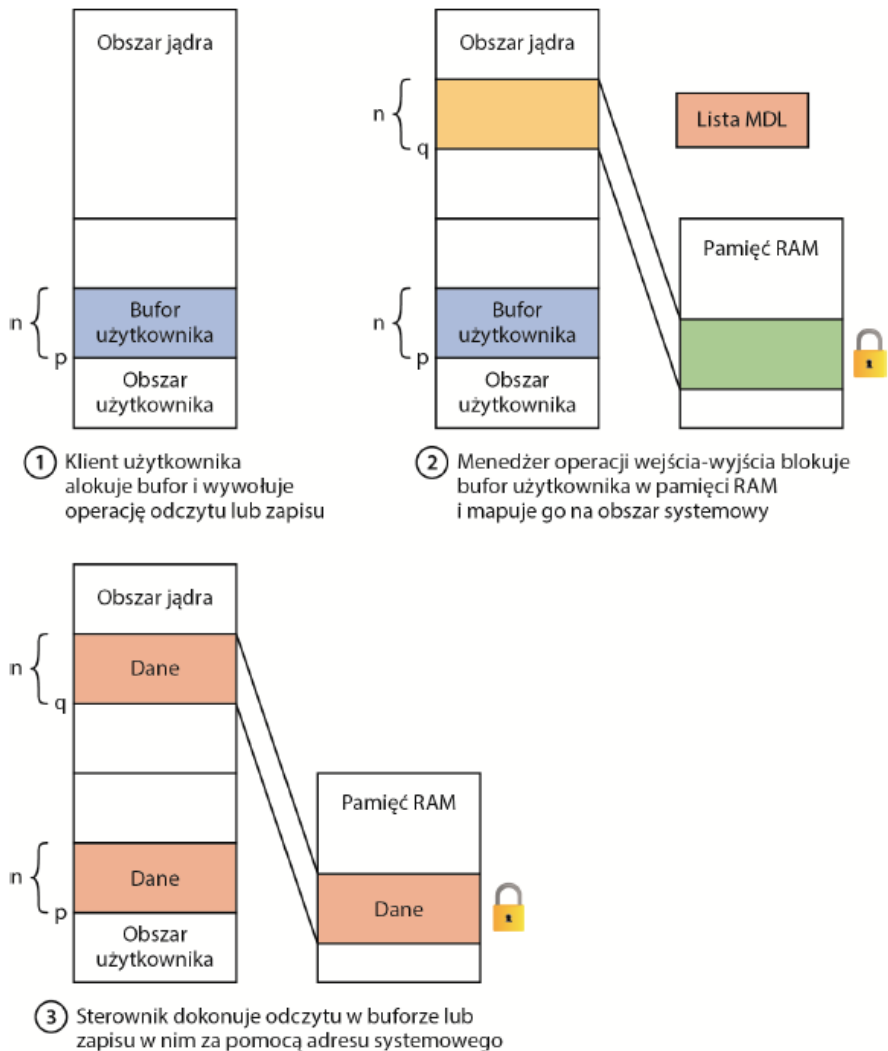
- **Synchroniczne operacje wejścia-wyjścia** - większość operacji wejścia-wyjścia wykonywanych przez aplikacje (domyślny wariant).
- **Asynchroniczne operacje wejścia-wyjścia** - umożliwia aplikacji utworzenie wielu żądań operacji wejścia-wyjścia i kontynuowanie działania w trakcie realizowania operacji wejścia-wyjścia przez urządzenie.
- **Szybka operacja wejścia-wyjścia** - pomija generowanie pakietu IRP i przechodzi bezpośrednio do stosu sterownika.

Buforowana operacja wejścia-wyjścia



- Menedżer operacji we/wy alokuje lustrzany bufor, który ma taką samą wielkość jak bufor użytkownika w puli niestronicowanej.
- Operacja zawsze wymaga kopiowania, co jest nieefektywne w wypadku dużych buforów.

Bezpośrednia operacja wejścia-wyjścia



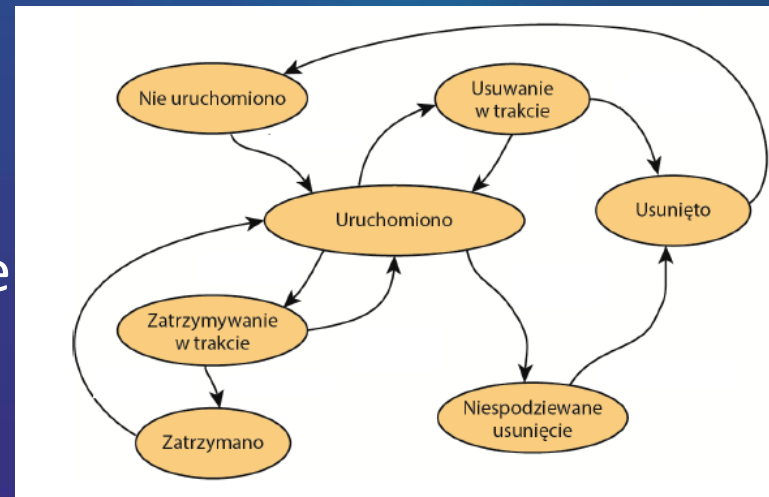
- Zapewnia sterownikowi możliwość uzyskania bezpośredniego dostępu do buforu użytkownika bez potrzeby kopiowania.
- Przydaje się w wypadku dużych buforów zwłaszcza przy transferach bazujących na funkcji DMA.

Driver Verifier

- Mechanizm, który może ułatwić znajdowanie i izolowanie typowych błędów występujących w kodzie sterowników urządzeń lub w innym kodzie systemowym trybu jądra.
- Firma Microsoft używa go do przeprowadzenia testów własnych sterowników urządzeń, a także wszystkich sterowników dostarczanych przez producentów.
- Obsługiwany jest w kilku komponentach systemowych:
 - menedżerze pamięci
 - menedżerze operacji wejścia-wyjścia
 - warstwie HAL

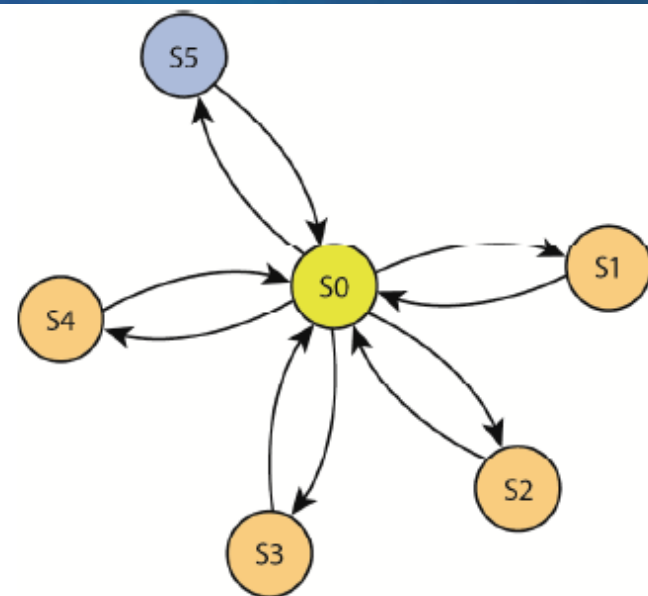
Menedżer technologii PnP

- Komponent zaangażowany w obsługę możliwości rozpoznawania i adaptowania przez system Windows zmieniających się konfiguracji sprzętowych:
 - automatycznie rozpoznaje zainstalowane urządzenia,
 - alokuje zasoby sprzętowe,
 - ładuje odpowiednie sterowniki,
 - implementuje mechanizmy służące do wykrywania zmian w konfiguracji sprzętowej,
 - obsługuje urządzenia podłączone do sieci, takie jak projektory i drukarki sieciowe.



Menedżer zasilania

Stan	Zużycie energii	Wznawianie programowe	Opóźnienie sprzętowe
S0 (pełna aktywność)	Maksymalne	Nie dotyczy	Żadne
S1 (uśpienie)	Mniejsze niż dla stanu S0 i większe niż dla stanu S2	System wznawia pracę tam, gdzie ją zakończył (powraca do stanu S0)	Mniejsze niż 2 sekundy
S2 (uśpienie)	Mniejsze niż dla stanu S1 i większe niż dla stanu S3	System wznawia pracę tam, gdzie ją zakończył (powraca do stanu S0)	Dwie lub więcej sekund
S3 (uśpienie)	Mniejsze niż dla stanu S2; procesor jest wyłączony	System wznawia pracę tam, gdzie ją zakończył (powraca do stanu S0)	Tak samo jak w wypadku stanu S2
S4 (hibernacja)	Zasilanie ograniczone do przycisku zasilania i układu aktywowania	System jest ponownie uruchamiany z zapisanego pliku stanu hibernacji i wznawia pracę tam, gdzie ją zakończył przed hibernacją (powraca do stanu S0)	Długie i nieokreślone
S5 (pełne wyłączenie)	Zasilanie ograniczone do przycisku zasilania	Ponowny rozruch systemu	Długie i nieokreślone



Bezpieczeństwo

Zabezpieczenie systemu operacyjnego obejmuje:

- Typowe mechanizmy - konta, hasła i ochrona plików.
- Uszkodzenie, uniemożliwienie użytkownikom o niższych uprawnieniach wykonywania pewnych działań.
- Niedopuszczenie do tego, aby programy użytkowników niekorzystnie wpływały na programy innych użytkowników lub na system operacyjny.

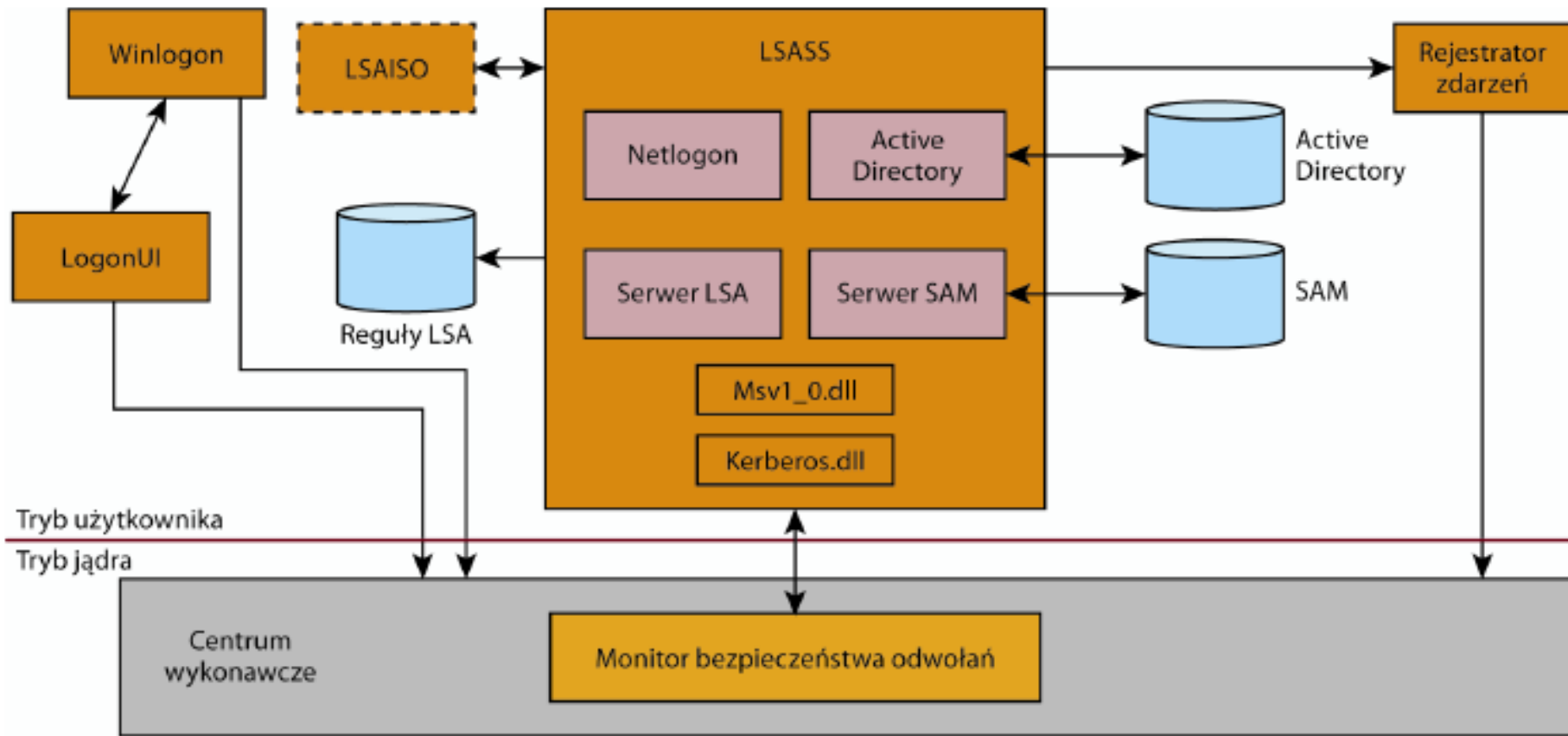
Główne wymagania klasy C2

- Istnienie mechanizmu bezpiecznego logowania.
- Uznaniowa kontrola dostępu.
- Monitorowanie zabezpieczeń.
- Zabezpieczenie przed ponownym użyciem obiektów.

System Windows spełnia również dwa wymagania zabezpieczeń z poziomu B:

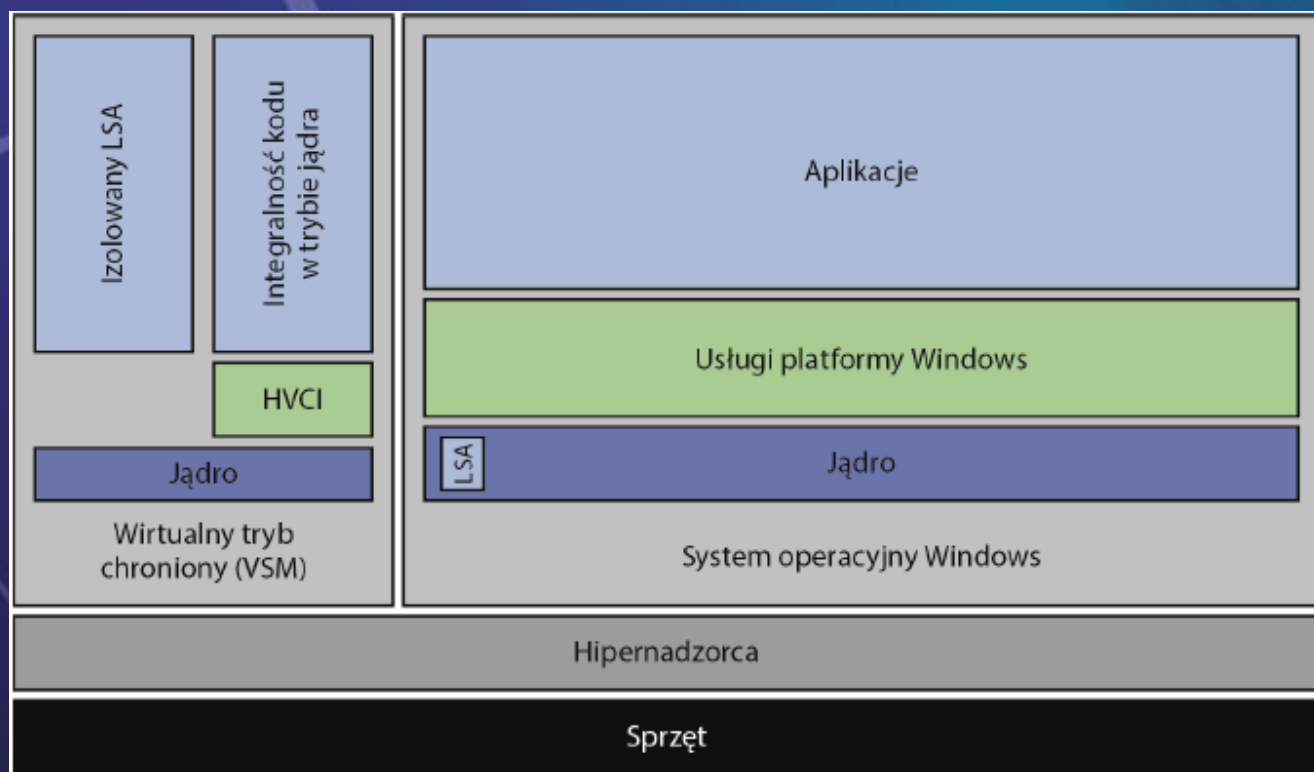
- Funkcje zaufanej ścieżki.
- Zarządzanie mechanizmami zaufanymi.

Komponenty odpowiedzialne za bezpieczeństwo systemu Windows



Bezpieczeństwo oparte na wirtualizacji

Systemy Windows 10 i Windows Server mają architekturę, której bezpieczeństwo jest oparte na wirtualizacji (VBS) z dodatkowym, wirtualnym poziomem zaufania (VTL).



Składniki uwierzytelniania

- **Hasło** - podstawowe świadectwo tożsamości użytkownika logującego się w systemie komputerowym.
- **Jednokierunkowa funkcja NT (NTOWF — *NT One-Way Function*)** - funkcja haszująca stosowana przez starsze komponenty do identyfikowania użytkownika.
- **Bilet uprawniający (TGT — *Ticket-Granting Ticket*)** - równoważny funkcji NTOWF w przypadku zastosowania nowocześniejszego protokołu uwierzytelniania o nazwie Kerberos - rozwiązanie domyślnie stosowane w domenach opartych na usłudze Active Directory, zostało przyjęte w systemie Windows Server 2016.

Ochrona obiektów

- Gdy proces otwiera istniejący obiekt za pomocą nazwy menedżer obiektów sprawdza zabezpieczenia dostępu.
- Monitor bezpieczeństwa odwołań sprawdza, czy obiekt ma zabezpieczenia domyślne.
- Obiekt, który nie korzysta z zabezpieczeń domyślnych, musi sam zarządzać informacjami o swoim zabezpieczeniu.
- Obiektami, które korzystają z zabezpieczeń domyślnych są:
 - muteksy,
 - zdarzenia,
 - semafony.
- Obiekt pliku ignoruje zabezpieczenia domyślne.

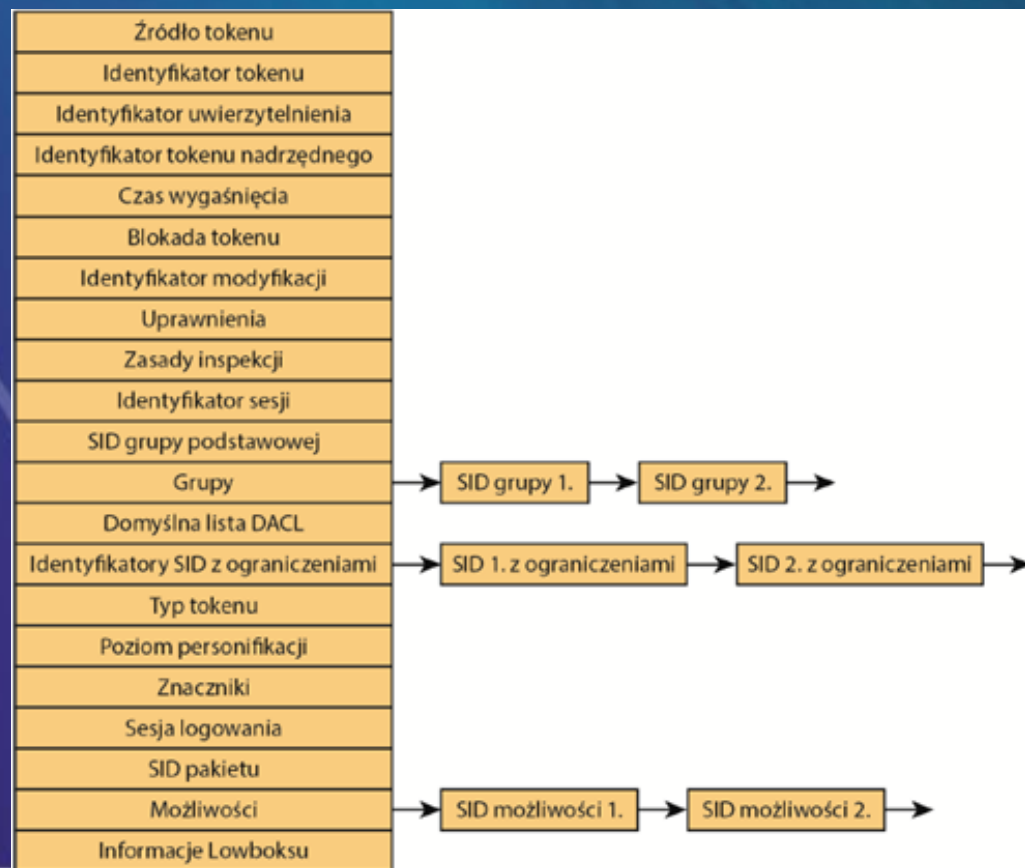
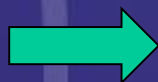
Identyfikatory zabezpieczeń

- System Windows używa identyfikatorów zabezpieczeń (SID — *Security Identifiers*) zamiast nazw.
- Identyfikatory SID posiadają użytkownicy, grupy lokalne i domenowe, komputery lokalne, domeny, członkowie domen i usługi.
- SID jest wartością numeryczną o zmiennej długości, składającą się z numeru wersji struktury SID, 48-bitowej wartości autoryzacji identyfikatora i zmiennej 32-bitowej wartości podautoryzacji lub identyfikatora względnego.

Tokeny

- Do identyfikacji kontekstu zabezpieczeń procesu lub wątku Monitor SRM wykorzystuje obiekt zwany *tokenem*.

Token dostępu



Personifikacja

- Personifikacja - ważna funkcja, używana przez system Windows w ramach modelu zabezpieczeń.
- Model programowania klient-serwer.
- Stosując personifikację, serwer tymczasowo przyjmuje profil bezpieczeństwa klienta wysyłającego żądanie.

Deskryptory zabezpieczeń i kontrola dostępu

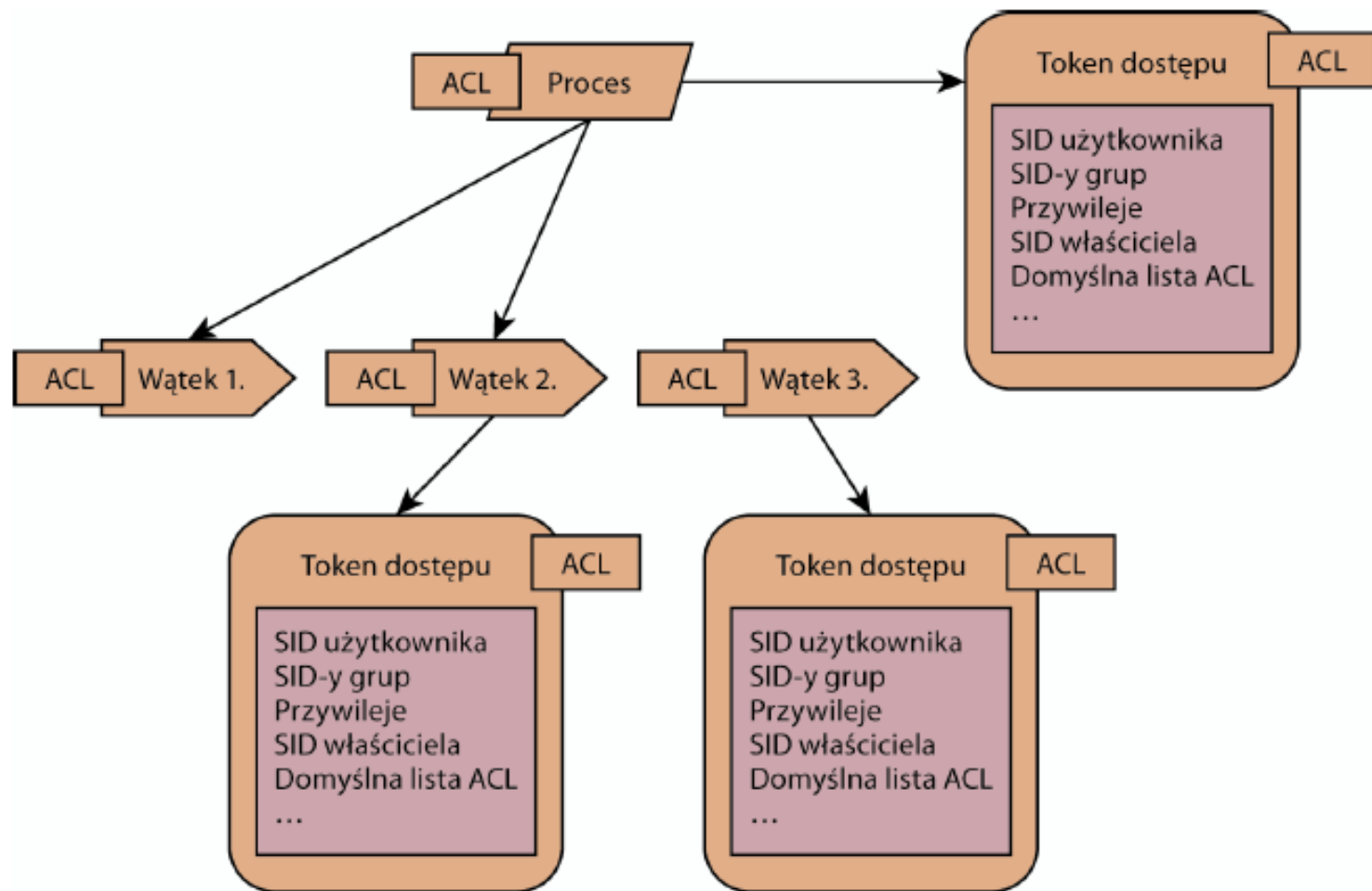
Deskryptor zabezpieczeń składa się z następujących atrybutów:

- Numer poprawki
- Znaczniki
- SID właściciela
- SID grupy
- Lista uznaniowej kontroli dostępu (DACL)
- Lista systemowej kontroli dostępu (SACL)

Prawa i przywileje konta

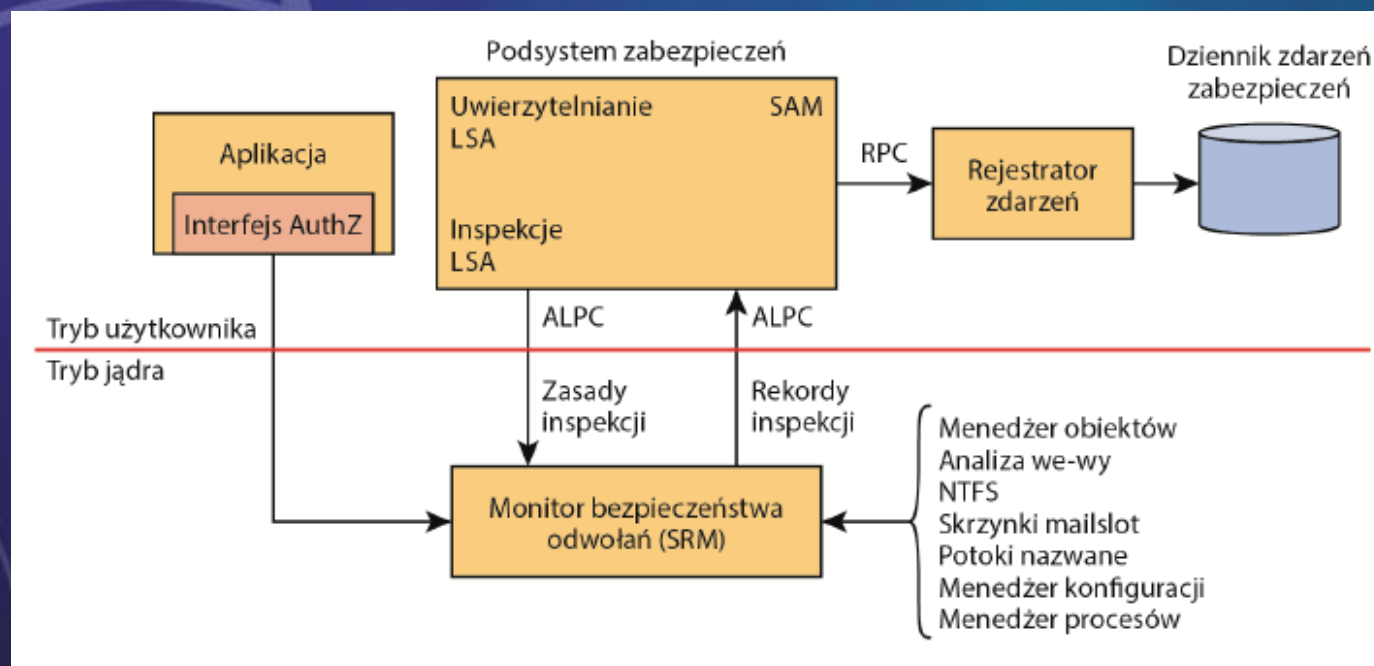
- System Windows korzysta z praw oraz z przywilejów konta.
- *Przywilej* (ang. *privilege*) jest prawem konta do wykonywania określonych operacji związanych z bezpieczeństwem, np. wyłączania komputera lub zmiany czasu systemowego.
- *Prawo konta* (ang. *account right*) zezwala na przeprowadzenie określonego rodzaju logowania na komputerze - logowania lokalnego lub interaktywnego albo odmawia takiego prawa.
- Administrator systemu przypisuje przywileje do grup i kont.

Struktury zabezpieczeń procesów i wątków

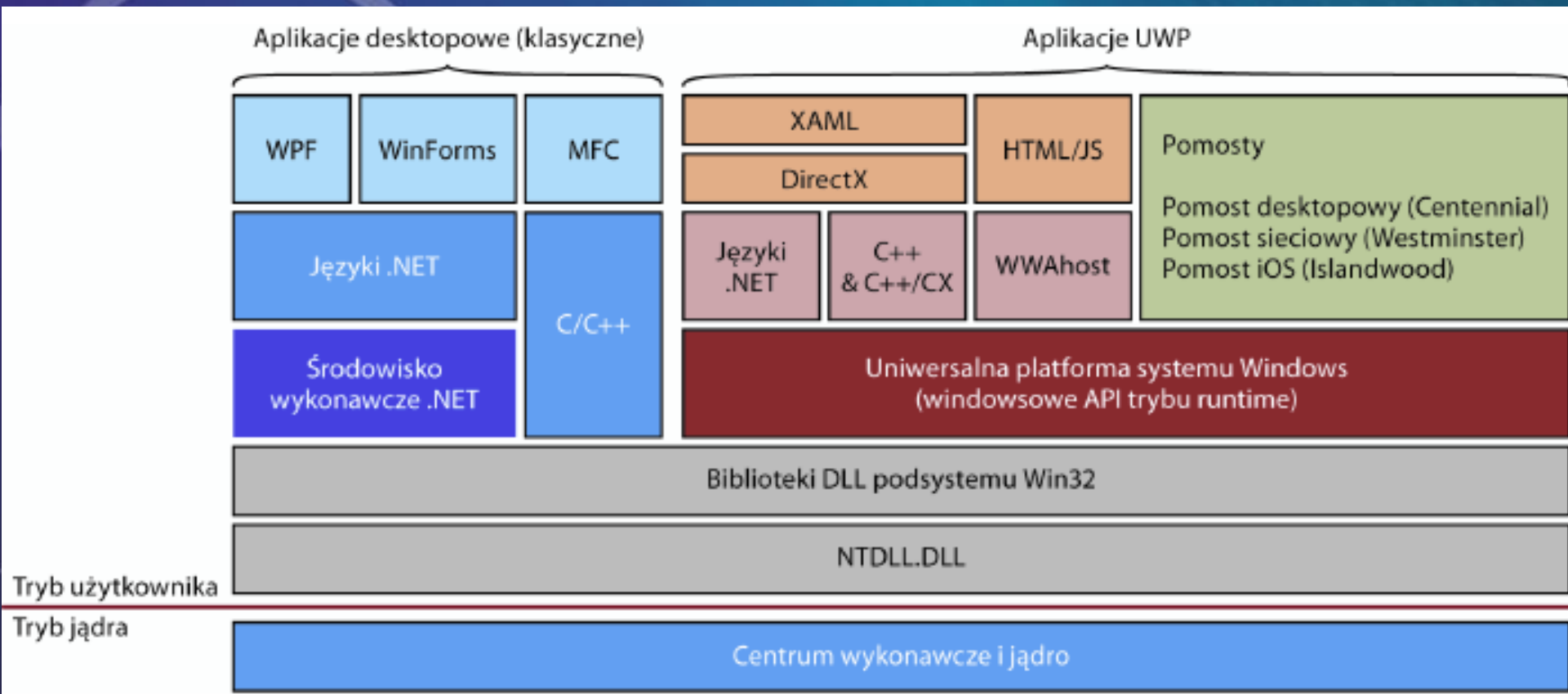


Przepływ rekordów inspekcji zabezpieczeń

- Menedżer obiektów może generować zdarzenia inspekcji w wyniku sprawdzania praw dostępu.
- Kod trybu jądra zawsze ma prawo do generowania zdarzenia inspekcji.



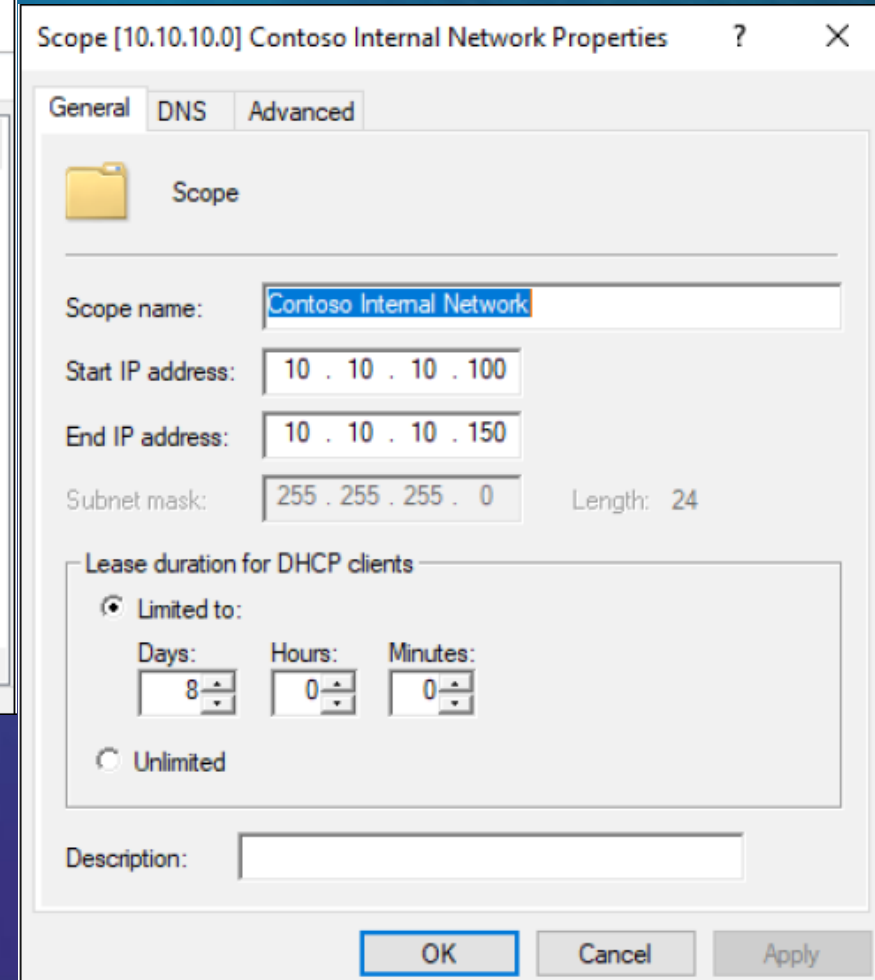
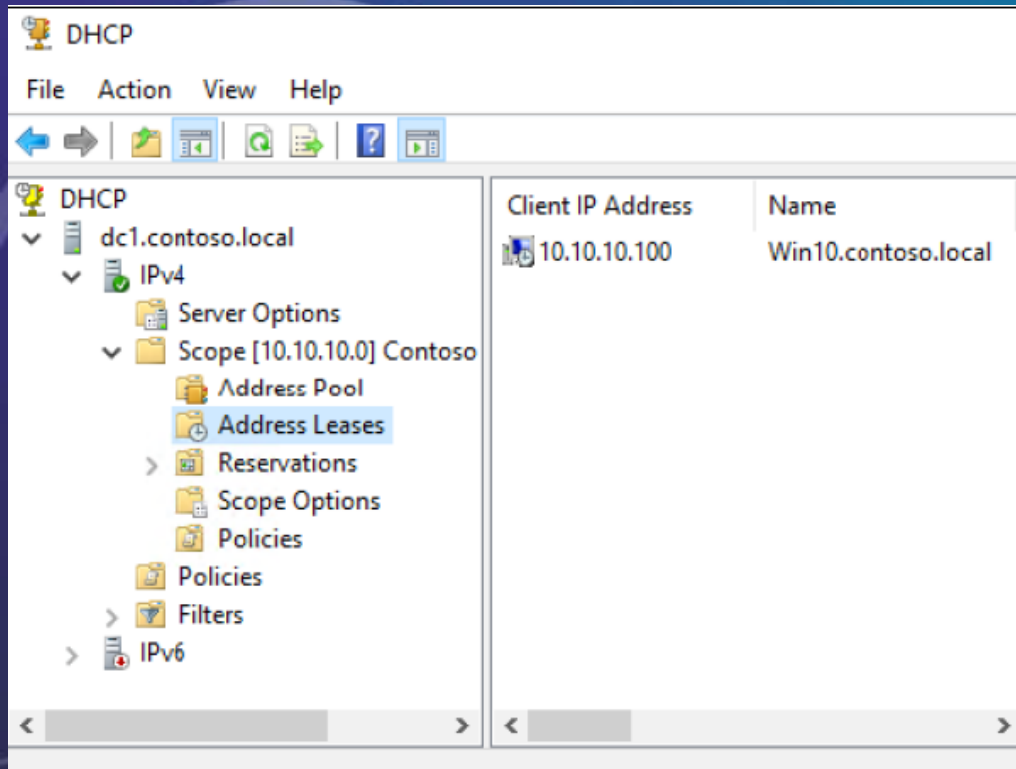
Schematyczny układ platformy Windows



Usługa DHCP

- **DHCP** (*Dynamic Host Configuration Protocol*) – protokół dynamicznego konfigurowania węzłów.
- Umożliwia komputerom uzyskanie od serwera danych konfiguracyjnych:
 - adresu IP hosta,
 - adresu IP bramy sieciowej,
 - adresu serwera DNS,
 - maski podsieci.
- Brak serwera DHCP wymaga od administratora ręcznej konfiguracji wszystkich urządzeń w sieci.

Dynamic Host Configuration Protocol



System nazw domen (DNS)

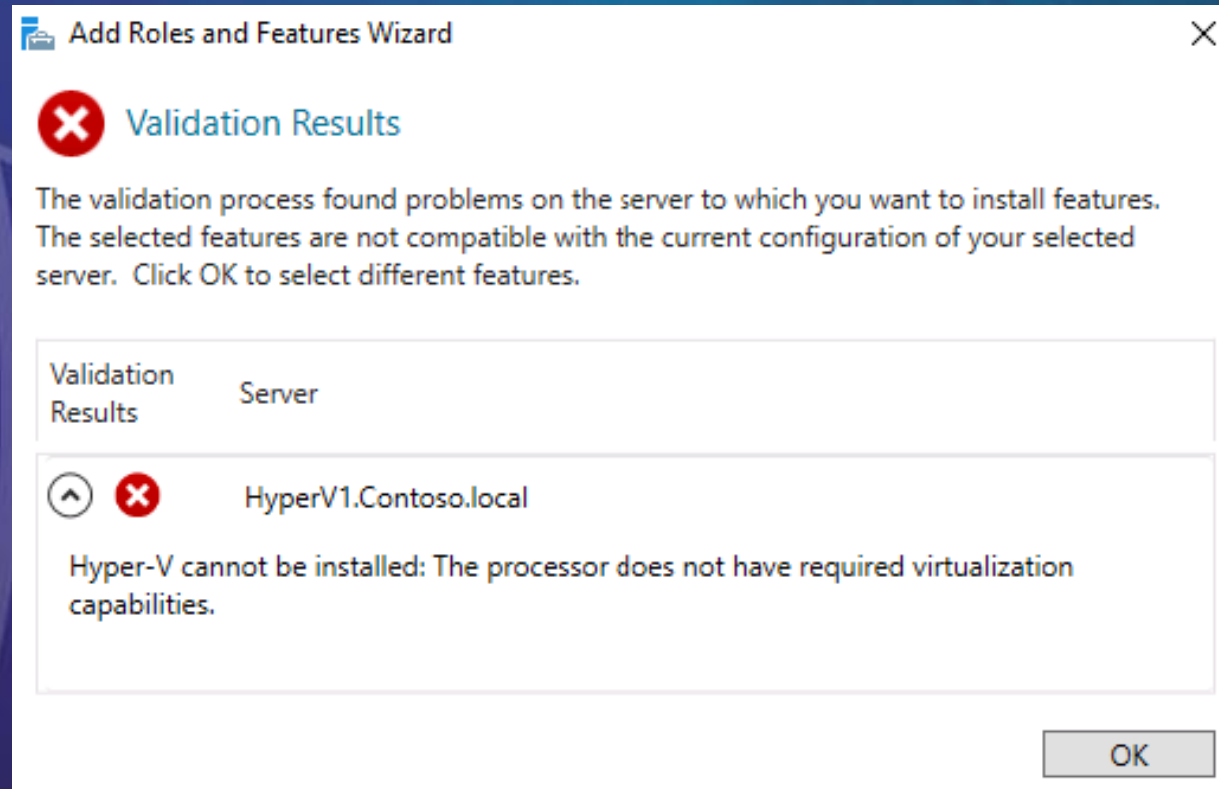
- Usługa DNS jest odpowiedzialna za przechowywanie i rozpoznawanie wszystkich nazw w sieci.
- Różne rodzaje rekordów DNS:
 - Rekord hosta (A lub AAAA).
 - Rekord aliasu (CNAME).
 - Rekord wymiany poczty (MX).
 - Rekord serwera nazw (NS).

Hyper-V

- W środowisku opartym na produktach firmy Microsoft stosuje się technologię zapewniającą możliwość uruchamiania **maszyn wirtualnych** (VM) - rola **Hyper-V**
- Możliwości wirtualizacji zapewnione przez firmę Microsoft:
 - Projektowanie i wdrażanie serwera Hyper-V.
 - Korzystanie z wirtualnych przełączników.
 - Implementacja serwera wirtualnego.
 - Zarządzanie serwerem wirtualnym.
 - Chronione maszyny wirtualne.
 - Integracja z Linuksem.
 - Serwer Hyper-V 2019.

Serwer Hyper-V

- Większość nowoczesnego sprzętu w pełni obsługuje funkcjonalność hiperwizora,
- Podczas próby zainstalowania roli Hyper-V może pojawić się komunikat o błędzie - w ustawieniach BIOS jest wyłączona opcja DEP.
- Pojedynczy serwer przeciętnie wykorzystuje 8 GB



Serwer Hyper-V

Select server roles

DESTINATION SERVER
HyperV1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Hyper-V

Virtual Switches

Migration

Default Stores

Confirmation

Results

Select one or more roles to install on the selected server.

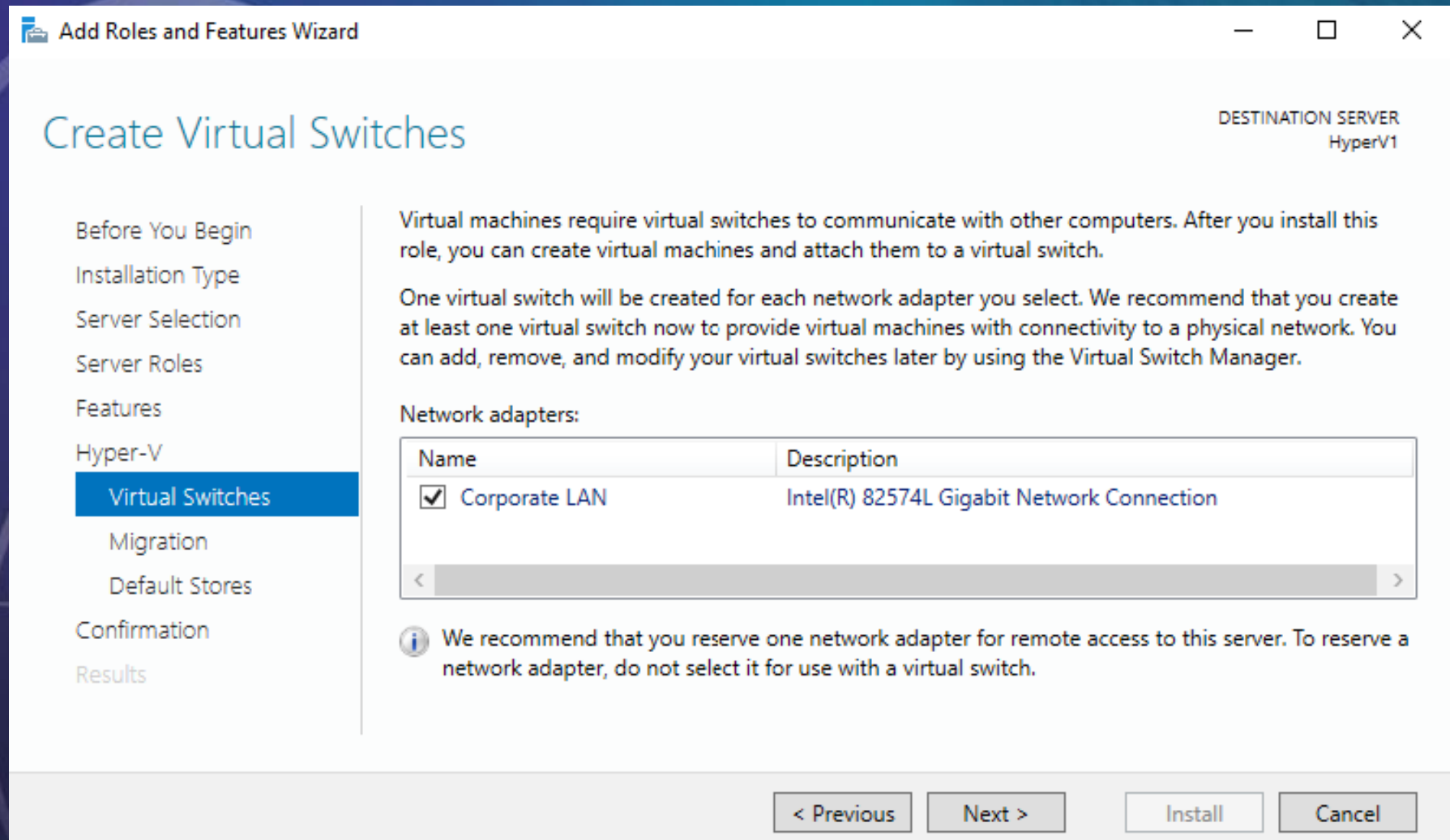
Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☐ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ☒ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☒ **Hyper-V**
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services

Description

Hyper-V provides the services that you can use to create and manage virtual machines and their resources. Each virtual machine is a virtualized computer system that operates in an isolated execution environment. This allows you to run multiple operating systems simultaneously.

Instalowanie roli Hyper-V



Instalowanie roli Hyper-V

Add Roles and Features Wizard

Virtual Machine Migration

DESTINATION SERVER
HyperV1

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Hyper-V
 Virtual Switches
 Migration
 Default Stores
Confirmation
Results

Hyper-V can be configured to send and receive live migrations of virtual machines on this server. Configuring Hyper-V now enables any available network on this server to be used for live migrations. If you want to dedicate specific networks for live migration, use Hyper-V settings after you install the role.


☐ Allow this server to send and receive live migrations of virtual machines

Authentication protocol

Select the protocol you want to use to authenticate live migrations.

☒ Use Credential Security Support Provider (CredSSP)
This protocol is less secure than Kerberos, but does not require you to set up constrained delegation. To perform a live migration, you must be logged on to the source server.

☐ Use Kerberos
This protocol is more secure but requires you to set up constrained delegation in your environment to perform tasks such as live migration when managing this server remotely.

 If this server will be part of a cluster, do not enable migration now. Instead, you will configure the server for live migration, including specifying networks, when you create the cluster.

< Previous Next > Install Cancel

Instalowanie roli Hyper-V

Default Stores

DESTINATION SERVER
HyperV1

Before You Begin

Installation Type

Server Selection

Server Roles

Features

Hyper-V

Virtual Switches

Migration

Default Stores

Confirmation

Results

Hyper-V uses default locations to store virtual hard disk files and virtual machine configuration files, unless you specify different locations when you create the files. You can change these default locations now, or you can change them later by modifying Hyper-V settings.

Default location for virtual hard disk files:

C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks

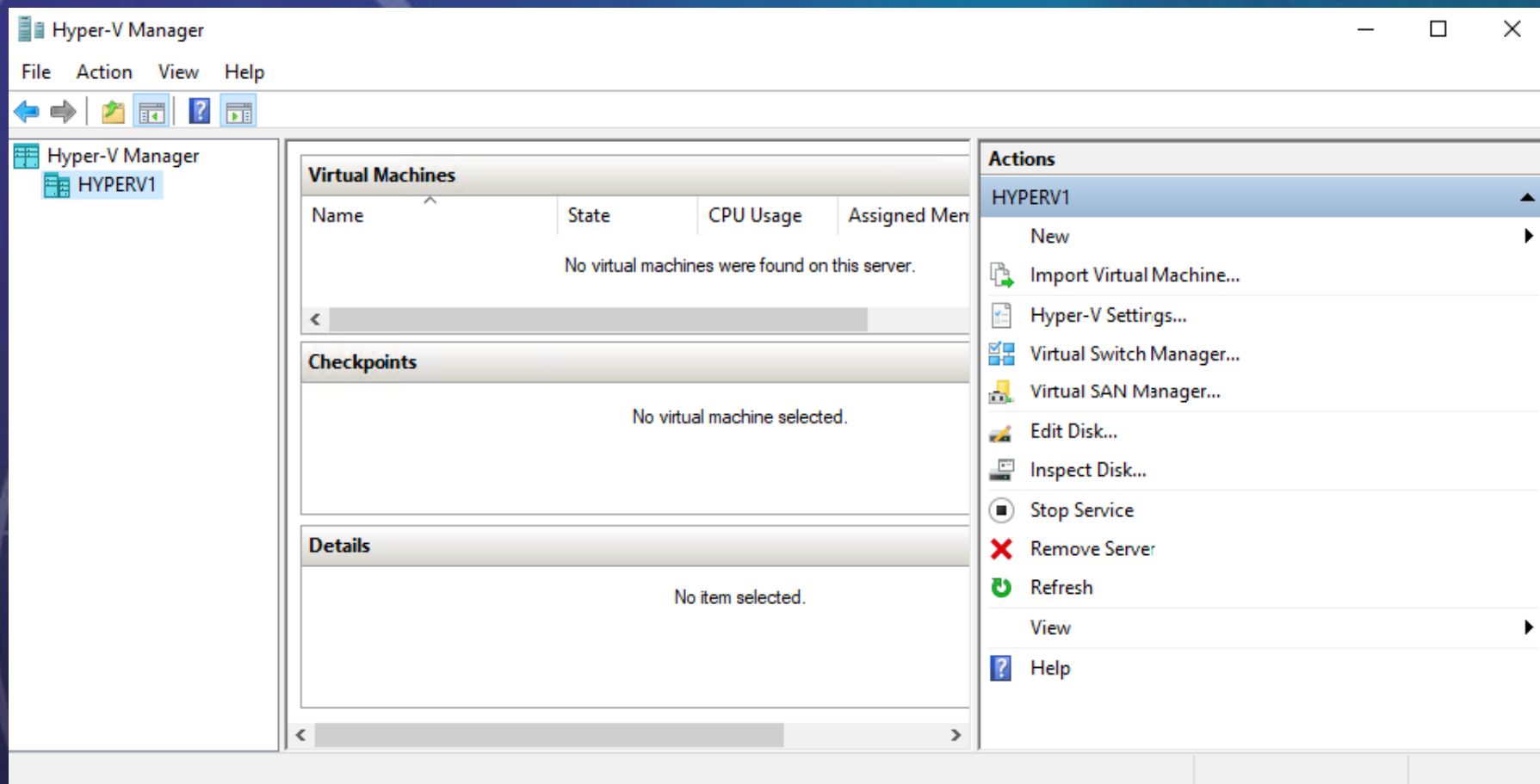
Browse...

Default location for virtual machine configuration files:

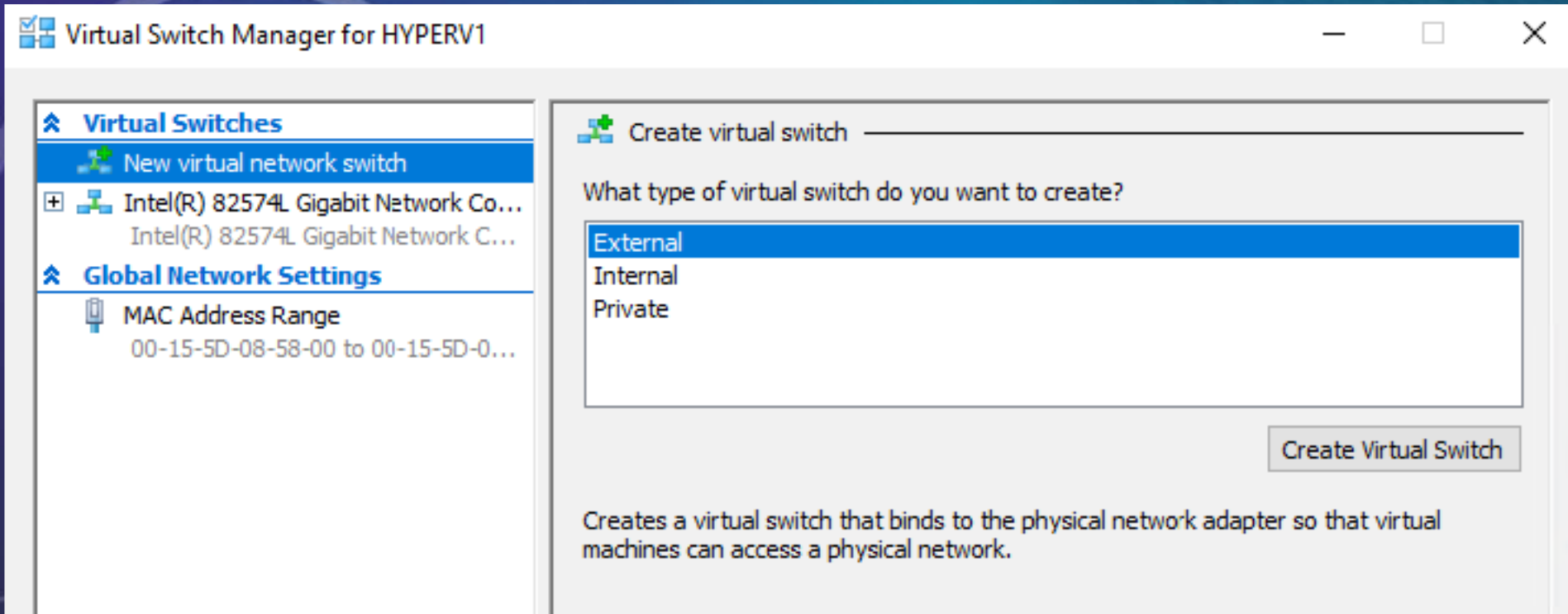
C:\ProgramData\Microsoft\Windows\Hyper-V

Browse...

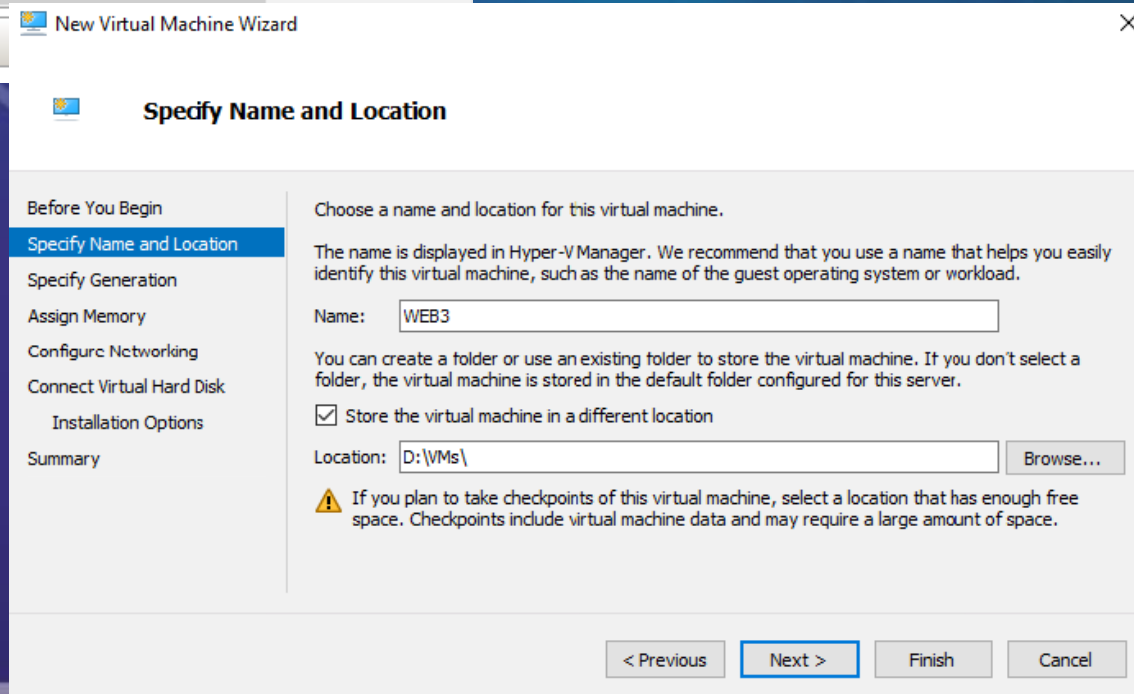
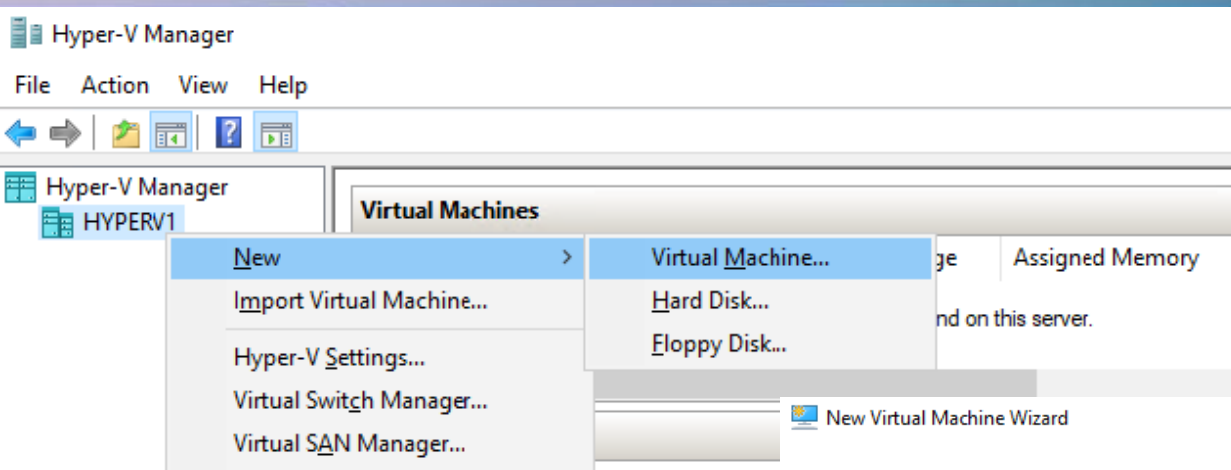
Przełączniki wirtualne



Przełączniki wirtualne



Implementacja serwera wirtualnego



Implementacja serwera wirtualnego


Choose the generation of this virtual machine.

☒ Generation 1


This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

☐ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

 Once a virtual machine has been created, you cannot change its generation.

Implementacja serwera wirtualnego


 **Assign Memory**

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: MB

☐ Use Dynamic Memory for this virtual machine.

 When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Installation Options
Summary

A virtual machine requires storage so that you can install an operating system. You can create a new virtual hard disk now or configure it later by modifying the virtual machine's properties.

☒ **Create a virtual hard disk**
Use this option to create a VHDX dynamically expanding virtual hard disk.

Name:
Location:
Size: GB (Maximum: 64 TB)

☐ **Use an existing virtual hard disk**
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

Location:

☐ **Attach a virtual hard disk later**
Use this option to skip this step now and attach an existing virtual hard disk later.

You can install an operating system now if you have access to the setup media, or you can install it later.

☒ **Install an operating system later**

☐ **Install an operating system from a bootable CD/DVD-ROM**

Media

☒ **Physical CD/DVD drive:**

☐ **Image file (.iso):**

☐ **Install an operating system from a bootable floppy disk**

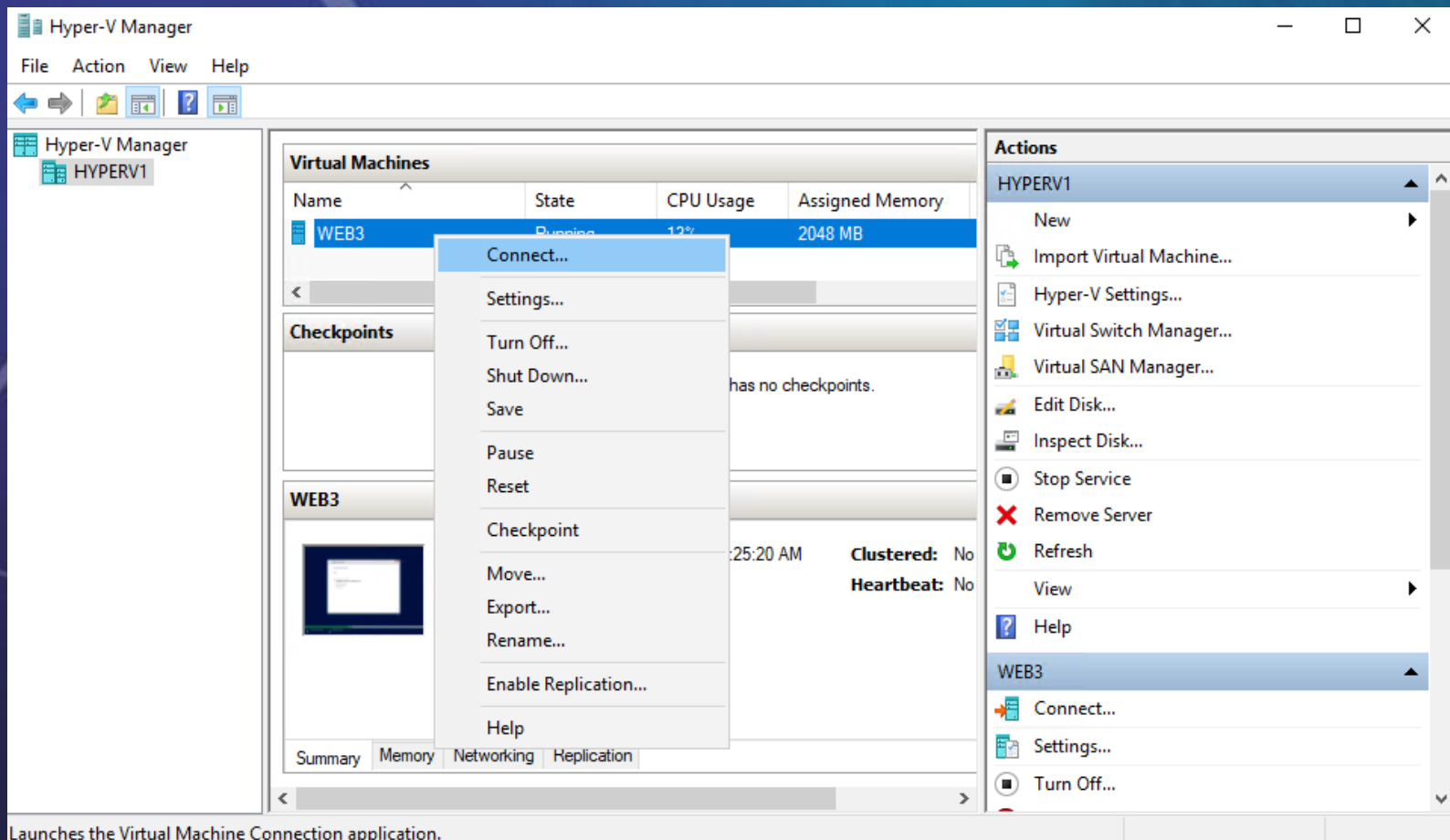
Media

☐ **Virtual floppy disk (.vfd):**

☐ **Install an operating system from a network-based installation server**

Menedżer funkcji Hyper-V

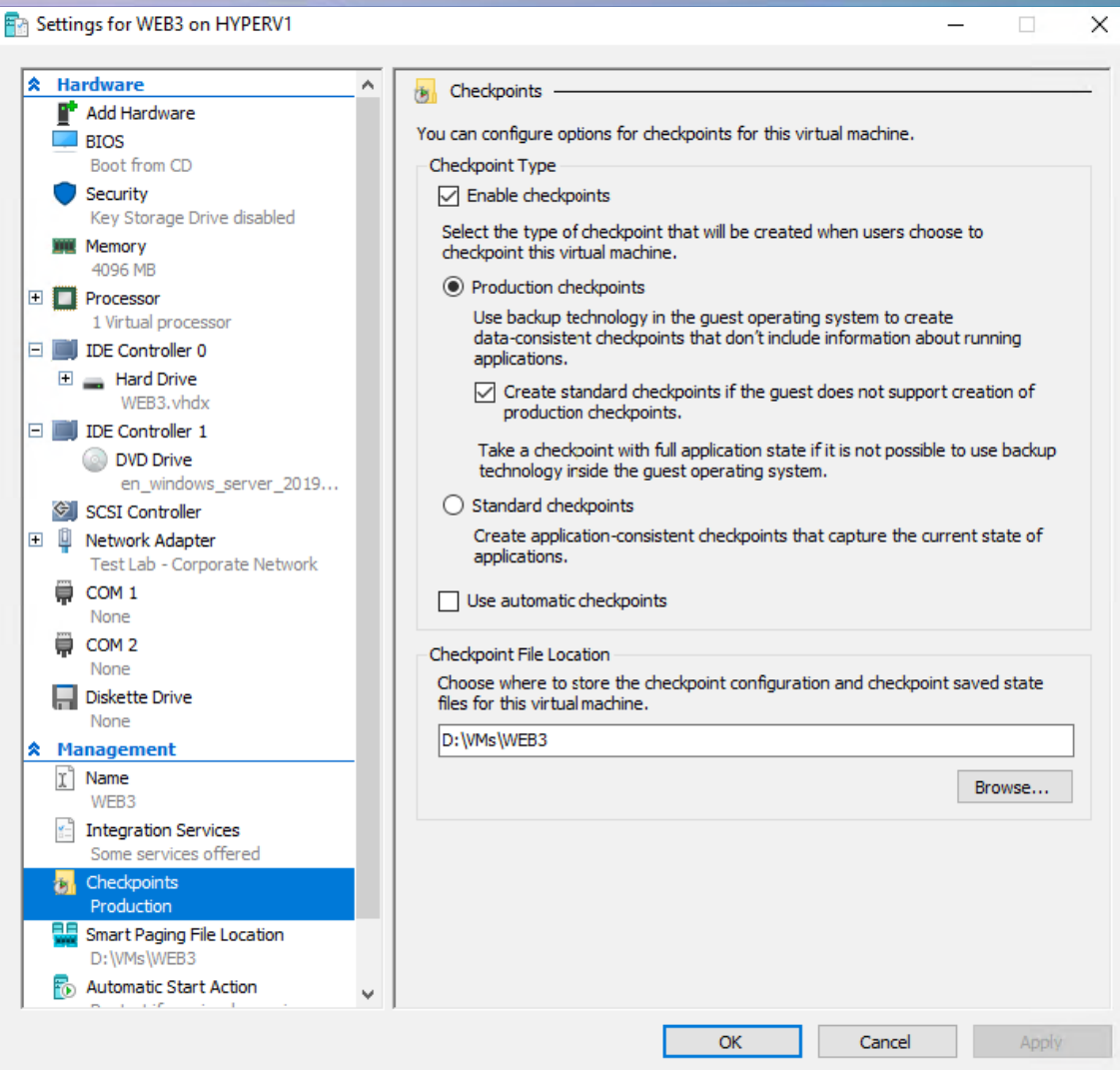
Podstawowe narzędzie służące do zarządzania serwerem Hyper-V.
Dostarcza informacji o maszynach wirtualnych i umożliwia ich wszechstronną obsługę.



Przydatne opcje menedżera funkcji Hyper-V

- Zarządzanie przełącznikami wirtualnymi.
- Możliwość utworzenia nowej maszyny wirtualnej,
- Szczegółowa modyfikacja ustawień maszyny wirtualnej jest możliwa po wybraniu opcji *Settings...* (*Ustawienia...*).
- Opcja *Memory* (*Pamięć*) - ilość pamięci RAM, którą ma wykorzystywać maszyna wirtualna.

Punkty kontrolne



- *Checkpoints (Punkty kontrolne)* - utworzenie dla maszyny wirtualnej migawki z danego momentu.
- Produkcyjne punkty kontrolne.
- Standardowe punkty kontrolne.
- PowerShell - może zarządzać maszyną wirtualną z innego serwera lub komputera stacjonarnego

Chronione maszyny wirtualne

- Firma Microsoft stworzyła technologię o nazwie BitLocker służącą do szyfrowania dysków.
- Chronione maszyny wirtualne to po prostu standardowe maszyny wirtualne Hyper-V z włączonym szyfrowaniem dysków za pomocą funkcji BitLocker.
- Zastosowanie idei chronionych maszyn wirtualnych jest o wiele ważniejsze w przypadku serwerów umieszczonych w chmurze publicznej lub prywatnej, ponieważ nie mamy wówczas dostępu do realnego sprzętu.

Integracja z systemem Linux

Metody używania maszyn wirtualnych z systemem Linux na serwerze wyposażonym w środowisko Windows Server 2019:

- Uruchamianie w środowisku Hyper-V,
- Chronione maszyny wirtualne z systemem Linux,
- Uruchamianie w kontenerach.

Usługi związane z Active Directory

1. Usługi certyfikacyjne AD CS (Active Directory Certificate Services)
2. Usługi AD DS (Active Directory Domain Services)
3. Usługi AD FS (Active Directory Federation Services)
4. Usługi AD LDS (Active Directory Lightweight Directory Services)
5. Usługi AD RMS (Active Directory Rights Management Services)

Role serwera

- Serwer DHCP
- Serwer DNS
- Serwer faksowania
- Serwer plików
- Usługi terminalowe
- Usługi kontroli dostępu przez sieć
- Serwer wydruków
- Serwer internetowy IIS
- Usługi multimedialne
- Usługi WDS
- Usługi Share Point
- Usługi UDDI

Serwer plików

- **Serwer plików** (*file server*) – serwer, który udostępnia w sieci komputerowej określone zasoby plikowe komputera.

Podstawowe typy serwerów plików:

- Oparte na protokole **SMB** (*ang. Server Message Block*).
- Serwer plików oparty o sieciowy system plików np. **NFS** (linux).
- Serwer FTP.
- SAMBA.
- Serwer wydruku.
- Serwer poczty:
 - POP3
 - SMTP
- Serwer baz danych

Rozproszony system plików

Zasady jednoczesnego dostępu wielu użytkowników do pliku:

- **Możliwość jednoczesnego odczytu bez możliwości zapisywania** – mechanizm prosty do realizacji.
- **Kontrolowanie zapisu** - wielu użytkowników otwiera jeden plik, ale tylko jeden z nich ma możliwość zapisu zmienionego dokumentu.
- **Jednoczesne zapisywanie** - daje możliwość jednoczesnego zapisu i odczytu tego samego zbioru przez kilku użytkowników - wymaga intensywnego nadzoru ze strony systemu operacyjnego.
 - klasa *stateless*
 - klasa *callback*

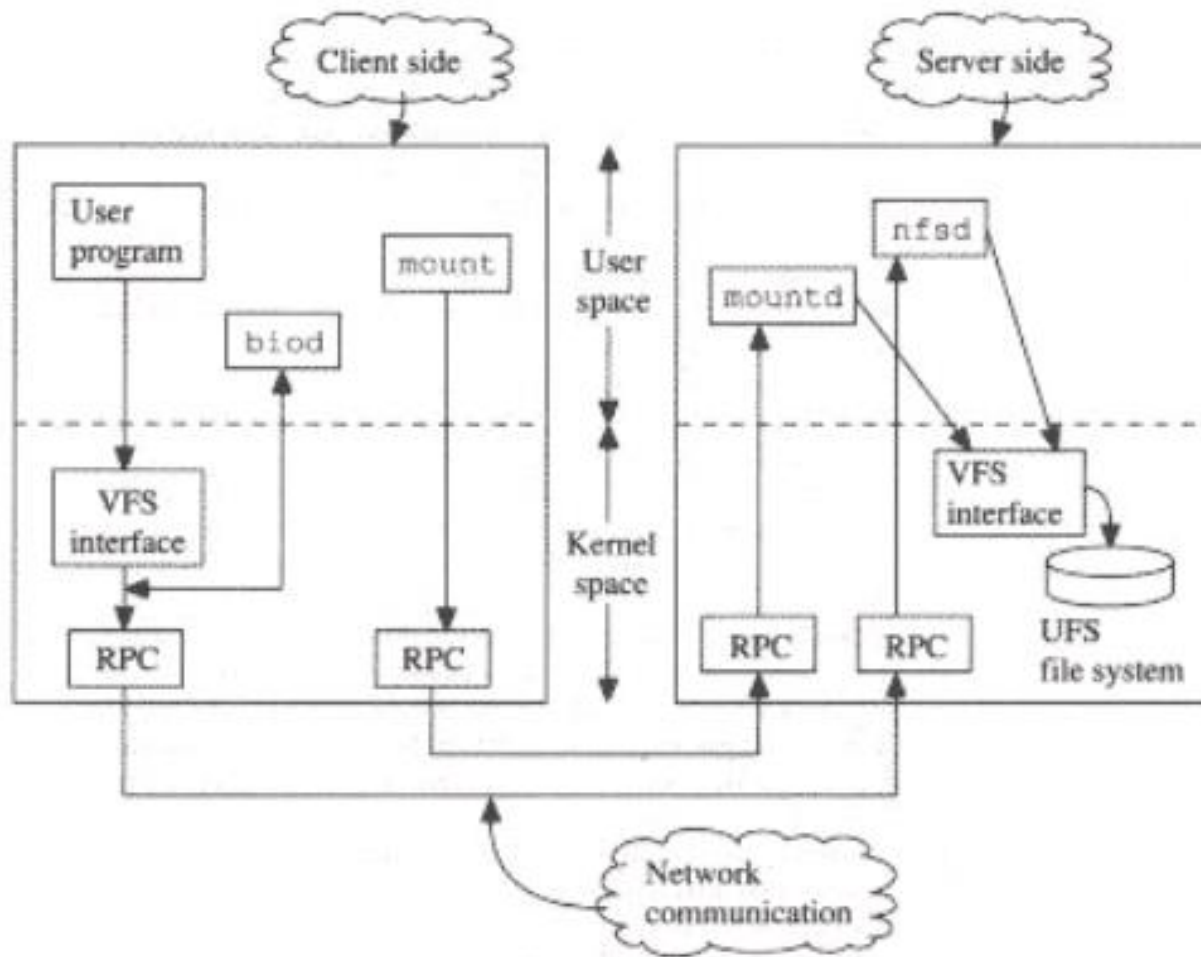
NFS (*Network File System*)

- Pierwotnie opracowany przez firmę Sun Microsystems w 1984 roku - umożliwia użytkownikowi dostęp do plików za pośrednictwem sieci na komputerze klienckim.
- Ważną cechą systemu NFS jest bezstanowy serwer - serwer NFS eksportujący katalogi nie zapamiętuje żadnej informacji o stacjach klienckich, a zajmuje się wyłącznie operacjami czytania i zapisywania.
- System NFS nie ma najlepszego modelu bezpieczeństwa.

Sieciowy system plików NFS

- Sieciowy system plików (Network File System - NFS) daje użytkownikom dostęp do danych i obiektów przechowywanych na zdalnym serwerze obsługującym NFS.
- Każdy system plików podłączony lokalnie przez NFS będzie miał cechy i ograniczenia katalogu lub systemu plików, z którego został podłączony z serwera zdalnego.
- Operacje na podłączonych systemach plików nie są wykonywane lokalnie.
- Żądania przechodzą przez połączenie do serwera i muszą być dostosowane do wymagań i ograniczeń systemu plików znajdującego się na serwerze.
- Dostęp do systemów plików NFS poprzez interfejs zintegrowanego systemu plików.

NFS (Network File System)



AFS (*Andrew File System*)

- Powstał na uniwersytecie Carnegie Mellon.
- Ma przewagę nad typowymi sieciowymi systemami plików, pod względem skalowalności i bezpieczeństwa.
- Produkcyjne instancje AFS obsługują nawet do 50 tys. klientów.
- Buforowanie po stronie klienta przyczynia się do zwiększenia wydajności systemu i umożliwia ograniczone funkcjonowanie w przypadku awarii serwera lub sieci.

