



# Politechnika Śląska

Dokumentacja realizowanych zadań

## Zarządzanie systemami informatycznymi

*Infrastruktura teleinformatyczna*

Kierunek: Informatyka

Członkowie zespołu:

*Mariusz Wróbel*

*Dawid Strzyż*

Gliwice, 2022

# **Spis treści**

<b>1 Wprowadzenie</b>	<b>2</b>
1.1 Role w realizacji zadania . . . . .	2
1.2 Cel realizacji zadania . . . . .	2
<b>2 Założenia realizacji zadania</b>	<b>3</b>
2.1 System operacyjny: konfiguracja i administracja . . . . .	3
2.2 Sieci komputerowe: zadania administracyjne . . . . .	3
2.3 Stos technologiczny . . . . .	3
2.4 Oczekiwane rezultaty realizacji zadania . . . . .	3
<b>3 Realizacja zadania</b>	<b>4</b>
3.1 System operacyjny . . . . .	4
3.1.1 Identyfikacja najważniejszych zadań administracyjnych	4
3.1.2 Omówienie trzech przykładowych zadań administra- cyjnych (CMD) . . . . .	4
3.1.3 Omówienie trzech przykładowych zadań administra- cyjnych (PowerShell) . . . . .	5
3.1.4 Narzędzia firm trzecich w realizacji zadań administra- cyjnych . . . . .	5
3.2 Sieci komputerowe . . . . .	6
3.2.1 Katalog przydatnych poleceń sieciowych . . . . .	6
3.2.2 Proces diagnostyki połączenia sieciowego . . . . .	7
3.2.3 Narzędzia przydatne w administracji sieciami kompu- terowymi . . . . .	7
3.3 Szkolenie użytkowników: instalacja oprogramowania . . . . .	8
3.4 System pomocy: rozwiązywanie problemów . . . . .	9

# **1 Wprowadzenie**

## **1.1 Role w realizacji zadania**

...

## **1.2 Cel realizacji zadania**

Celem zadania jest rozpoznanie możliwości konfiguracji oraz administrowania infrastrukturą teleinformatyczną małego przedsiębiorstwa.

## **2 Założenia realizacji zadania**

### **2.1 System operacyjny: konfiguracja i administracja**

Identyfikacja najważniejszych zadań administracyjnych, które mogą być realizowane w przedsiębiorstwie z wykorzystaniem ustawień systemu operacyjnego.

Omówienie trzech przykładowych zadań administracyjnych, które mogą być realizowane z wiersza poleceń (CMD).

Omówienie trzech przykładowych poleceń, które pozwalają na realizację zadań administracyjnych z wykorzystaniem PowerShell.

Pokazanie na trzech przykładach, w jaki sposób narzędzia firm trzecich (np. WS SCC) pozwalają na realizację zadań administracyjnych.

### **2.2 Sieci komputerowe: zadania administracyjne**

Przedstawienie katalogu przydatnych poleceń sieciowych dostępnych w wierszu poleceń Microsoft Windows.

Omówienie procesu diagnostyki połączenia sieciowego (w ramach systemu operacyjnego).

Zaproponowanie zestawu trzech narzędzi (dostępnych przez Internet), przydatnych w realizacji zadań związanych z administracją sieciami komputerowymi.]

### **2.3 Stos technologiczny**

W przedsiębiorstwie znajduje się 5 stacji roboczych, a na każdej ze stacji zainstalowany jest Microsoft Windows 10.

### **2.4 Oczekiwane rezultaty realizacji zadania**

Oczekiwany rezultatem jest zaprojektowanie infrastruktury informatycznej w taki sposób aby można było ją łatwo rozwijać w przyszłości.

### **3 Realizacja zadania**

#### **3.1 System operacyjny**

##### **3.1.1 Identyfikacja najważniejszych zadań administracyjnych**

Do najważniejszych zadań administracyjnych które mogą być realizowane w przedsiębiorstwie z wykorzystaniem ustawień systemu operacyjnego możemy zaliczyć:

1. Zabezpieczenie przenośnych komputerów w których są przetwarzane dane osobowe poprzez ustawienie hasła. Ażdżanie hasłami użytkowników oraz nadzór nad przestrzeganiem procedur określających częstotliwość ich zmiany zgodnie z wytycznymi.
2. Nadzór nad ochroną systemu przed złośliwym oprogramowaniem.
3. Nadzór nad wykonywaniem kopii awaryjnych, przechowywaniem ich oraz sprawdzaniem pod kątem dalszej przydatności.
4. Nadzór nad przeglądami, konserwacjami oraz aktualniami systemów służących do przetwarzania danych osobowych.
5. nadzór nad obiegiem oraz przechowywaniem dokumentów zawierających dane osobowe generowane przez system.
6. Nadzór nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie.
7. Podjęcie działań zabezpieczających stan systemu w przypadku otrzymania informacji o naruszeniu zabezpieczeń systemu lub informacji o zmianach w sposobie działania programu lub urządzeń wskazujących na naruszenie bezpieczeństwa danych.
8. Analiza sytuacji, okoliczności i przyczyn, które doprowadziły do naruszenia bezpieczeństwa danych.

##### **3.1.2 Omówienie trzech przykładowych zadań administracyjnych (CMD)**

1. **ipconfig** - Ipconfig to narzędzie, które powinien znać każdy użytkownik systemu Microsoft Windows. Wyświetla ono informacje o bieżącej konfiguracji lokalnych interfejsów sieciowych. Ipconfig jest narzędziem

istotnym dla przeprowadzania procedury diagnostycznej sieci komputerowej. Przydaje się na przykład wtedy, gdy chcemy sprawdzić ping danego urządzenia, ale nie znamy jego adresu IP.

2. **ping** - Jest to polecenie używane w sieciach komputerowych, służące do diagnozowania połączeń sieciowych. Pozwala na sprawdzenie, czy istnieje połączenie pomiędzy hostami testującym i testowanym. Umożliwia on zmierzenie liczby zgubionych pakietów oraz opóźnień w ich transmisji.
3. **chkdsk** - Jest to bardzo przydatna komenda która umożliwia zaawansowane zarządzanie dyskami i naprawianie błędów. W zależności od użytych operatorów komenda ta może sprawdzić dysk, naprawić błędy lub lokalizować uszkodzone sektory i przywracać informacje.

### **3.1.3 Omówienie trzech przykładowych zadań administracyjnych (PowerShell)**

1. **Backup-SqlDatabase** - Wiele osób używa PowerShell do tworzenia kopii zapasowych baz danych SQL. Interfejs wiersza poleceń może wykonywać pełne kopie zapasowe bazy danych, jak i plików. Istnieje wiele sposobów tworzenia kopii zapasowej bazy danych w PowerShell, ale jednym z najprostszych jest użycie polecenia Backup-SqlDatabase.
2. **Get-Service** - Jednym z najważniejszych poleceń jest Get-Service, który udostępnia użytkownikowi listę wszystkich usług zainstalowanych w systemie, zarówno uruchomionych, jak i zatrzymanych.
3. **Get-EventLog** - Umożliwia dostęp do dzienników zdarzeń komputera (lub dzienników na komputerach zdalnych) podczas korzystania z PowerShell. Jednym z najczęstszych powodów, dla których użytkownicy przeglądają dzienniki zdarzeń, są błędy napotkane podczas pracy komputera.

### **3.1.4 Narzędzia firm trzecich w realizacji zadań administracyjnych**

W realizacji zadań administracyjnych pomocne może być użycie programów firm trzecich takich jak WSCC. Programy te umożliwiają instalowanie, aktualizowanie, uruchamianie i organizowanie narzędzi z różnych pakietów systemowych. Programy te mogą również automatycznie instalować i aktualizować obsługiwane narzędzia. Programy takie oferują również szybki dostęp

do usług i narzędzi w systemie Windows. Wśród nich warto wymienić między innymi zarządzanie użytkownikami i komputerem, CHKDISK, edytor rejestru systemowego, zapora czy dziennik zdarzeń.

Aplikacja posiada też przydatne funkcje do zarządzania procesami i aplikacjami uruchamianymi wraz ze startem systemu Windows. Oprócz tego w jego zasobach znajdziemy też programy do odczytywania najważniejszych informacji o komputerze i wszystkich w nim zainstalowanych podzespołach bazowych.

## 3.2 Sieci komputerowe

### 3.2.1 Katalog przydatnych poleceń sieciowych

Szczegóły każdej z komend można sprawdzić pod komendą help

1. **Ping** - pozwala na sprawdzenie połączenia między siecią a adresem IP
2. **Tracert** - służy do wyświetlania wszystkich adresów IP pośredniczących przy przesydle danych z maszyny lokalnej do adresu docelowego
3. **IpConfig** - pozwala na odświeżanie i wyświetlanie widoku konfiguracji sieci TCP/IP
4. **NetStat** - pozwala wyświetlić na maszynie lokalnej stan stosu TCP/IP
5. **Route** - służy do wyświetlania lub modyfikowania tablicy trasowania
6. **Arp** - służy do konwertowania IP na MAC wraz z wyświetlaniem i modyfikowaniem tablic tłumaczenia adresów IP na adresy fizyczne używane przez protokół ARP
7. **NbtStat** - możliwe jest za jego pomocą aktualizowanie pamięci podręcznej pliku Lmhosts oraz pozwala wyświetlać statystyki protokołu oraz aktualnego połączenia TCP/IP za pomocą NBT
8. **Telnet** - służy do umożliwiania dostępu do zdalnego hosta w trybie terminalu jak również służy do sprawdzania czy jakakolwiek usługa TCP jest uruchomiona na zdальnym serwerze poprzez uścielenie adresu IP i numeru portu TCP
9. **Hostname** - pokazuję nazwę maszyny
10. **Ftp** - służy do obsługi pobierania plików

11. **NsLookUp** - pozwala na wysyłanie zapytań DNS do dowolnego serwera DNS
12. **NetSh** - umożliwia konfigurację sieci w systemie Windows

### **3.2.2 Proces diagnostyki połączenia sieciowego**

Diagnoza połączenia internetowego:

- Diagnostykę zaczynamy od sprawdzenia czy sieć wifi jest włączona oraz czy tryb samolotowy jest wyłączony, by to zrobić klikamy ikonę braku połączenia internetowego. Jeżeli wifi jest wyłączone należy je włączyć oraz jeżeli tryb samolotowy jest włączony należy go wyłączyć.

- Następnie sprawdzamy czy sieć wi-fi do której chcemy się połączyć jest na liście połączeń. Jeśli znaleźliśmy naszą sieć wybieramy ją i próbujemy się z nią połączyć. Jeżeli pod nazwą sieci widnieje napis połączenia. następnie należy rozłączyć sieć i połączyć się ponownie.

- Spróbuj nawiązać połączenie z siecią na innym pasmie częstotliwości. Dla przykładu 2,4 GHz lub 5 GHz.

- Sprawdź czy jest włączony fizyczny przełącznik Wifi na komputerze przenośnym.

- Spróbuj uruchomić narzędzie do rozwiązywania problemów z siecią.

Wybierz przycisk Start, > Ustawienia> Network Internet > Status. Otwieranie ustawień stanu sieci i Internetu W obszarze Zmień ustawienia sieci wybierz opcję Narzędzie do rozwiązywania problemów z siecią.

- Ostatnim ze sposobów może być zrestartowanie modemu i routera. Postępuj następująco odłącz router od zasilania a następnie zrób to samo z modelem. Niektóre modemy mogą posiadać baterię, dlatego sprawdź czy twój takiego nie posiada, oczekaj 30 sekund a następnie podłącz modem a potem router. Na koniec spróbuj połączyć ponownie.

### **3.2.3 Narzędzia przydatne w administracji sieciami komputerowymi**

#### **1. Tcpdump i Wireshark**

Narzędzie to pozwala na przechwytywanie ruchu na karcie sieciowej i przeglądanie pakietów i ramek w czasie rzeczywistym. Wireshark pozwala rozszerzyć te funkcje o jeszcze bardziej użyteczny system do lokalizowania problemów w aplikacjach sieciowych.

Pakiety przechwycone przez Tcpdump można zachować w pliku, który może być następnie otwarty przez Wireshark do dalszej analizy. Wireshark zapewnia graficzny interfejs do sprawdzania pakietów przechwy-

conych przez Tcpdump i pozwala sortować te dane dla potrzeb bardziej dogłębnej analizy.

## 2. **Dig**

Jest to narzędzie dostarczające szczegółowej informacji o tym jak obsługiwane są kwerendy DNS użytkowników. Jądrem Dig to narzędzie CLI wykonujące kwerendy DNS. Może być bardzo użyteczne w czasie prób zdiagnozowania spowolnienia aplikacji sieciowych - pozwala np. określić, ile czasu zajmuje komputerowi uzyskanie adresu IP dla nazwy domeny serwera aplikacyjnego.

## 3. **Ntop**

Narzędzie pobiera z popularnych routerów i przełączników dane Net-Flow lub sFlow, i wyświetla je w graficznym interfejsie webowym, uzupełniając o aktywne linki rozwijające detale o poszczególnych hostach i protokołach.

Ntop podaje listę protokołów IP, posortowaną według typu protokołu, jak również listę miejsc przeznaczenia i pochodzenia ruchu. Tworzy także macierze ruchu IP, pokazujące, kto z kim się komunikuje i jakie dane są przekazywane między nimi. Dane mogą być sortowane według miejsc przeznaczenia lub pochodzenia. Pozwala to śledzić ruchy w sieci lokalnej i analizować możliwe nieprawidłowości, wynikające z usterki lub ataku hakerskiego

### **3.3 Szkolenie użytkowników: instalacja oprogramowania**

[Link do prezentacji](#)

### **3.4 System pomocy: rozwiązywanie problemów**

1. **FAQ** - frequently asked questions (często zadawane pytania) są to zbiory często zadawanych pytań i odpowiedzi, mające na celu udzielenie danemu użytkownikowi serwisu internetowego pomocy bez konieczności angażowania do tego jakichkolwiek osób. Jest to najpopularniejszy sposób otrzymywania pomocy. Jest on również najszybszy ponieważ nie jesteśmy jako klient zależni od czasu odpowiedzi na nasz problem. FAQ jest podzielony na dwa segmenty:
  - (a) Najczęstsze pytania i odpowiedzi
  - (b) Reszta danych w postaci obszernej dokumentacji
2. **Bot** - jest bardzo podobny w założeniach do FAQ lecz jest on interaktywny. Ułatwia proces wyszukiwania odpowiedzi ponieważ tym zajmuje się już komputer. Minusem takiego rozwiązania jest fakt że bot może nie zrozumieć dokładnie problemu klienta co będzie skutkowało znalezieniem błędnych odpowiedzi.
3. **Rozmowa z konsultantem** - jest to najbardziej naturalny sposób uzyskiwania pomocy. Konsultant jest odpowiednio przeszkoloną osobą która posiada szeroki zakres wiedzy o danym produkcie dzięki czemu jest w stanie szybko znaleźć odpowiedź na problem klienta. Jest to najlepszy sposób w razie nietypowego problemu. Największym minusem tego rozwiązania są ofranczone zasoby ludzkie które powodują że czas oczekiwania może być bardzo długi.