Laboratorium 1: DHCP

DHCP redukuje złożoność i ilość pracy administracyjnej poprzez automatyzację procesu konfigurowania TCP/IP.

Sposób zdobywania adresu IP przez klienta:
- Klient wysyła pakiet rozgłoszeniowy DHCPDISCOVER
- Serwery DHCP wysyłają pakiety rozgłoszeniowe DHCPOFFER
- Klient DHCP wysyła pakiet rozgłoszeniowy DHCPREQUEST
- Serwer DHCP wysyła pakiet rozgłoszeniowy DHCPACK

W każdej chwili w okresie dzierżawy klient DHCP może wysłać do serwera DHCP pakiet DHCPRELEASE, aby zwolnić dane konfiguracyjne adresu IP i anulować resztę dzierżawy.

Klient DHCP będzie także próbował odnowić dzierżawę adresu IP za każdym razem, gdy komputer zostanie ponownie uruchomiony. Aby spróbować odnowić dzierżawę, klient DHCP wysyła pakiet DHCPREQUEST bezpośrednio do serwera DHCP, od którego uzyskał dzierżawę.

Uwaga Jeśli klient żąda nieprawidłowego lub zduplikowanego adresu dla sieci, serwer DHCP może wysłać w odpowiedzi komunikat odmowny DHCP (pakiet DHCPNACK). Zmusza to klienta do zwolnienia jego adresu IP i uzyskania nowego, prawidłowego adresu.

Jeśli klient DHCP zostanie ponownie uruchomiony w sieci, gdzie żaden serwer DHCP nie odpowiada na pakiet DHCPREQUEST, klient DHCP próbuje połączyć się ze skonfigurowaną bramą domyślną. Jeśli próba połączenia się z bramą domyślną nie powiedzie się, klient przestaje korzystać z dzierżawionego adresu.

Adres jest dzierżawiony na pewien okres czasowy i **po upływie połowy czasu dzierżawy klient próbuje odnawiać dzierżawę** i klient wysyła w trybie **unikastowym** .

Odnawianie adresu IP:
- Klient DHCP wysyła pakiet DHCPREQUEST
- Serwer jeśli może wysyła DHCPACK

Kolejna próba wykonywana jest po upływie 87,5% czasu dzierżawy.

Jeśli nie uda się odnowić dzierżawy klient cały proces zaczyna od początku.

Zakres jest przedziałem adresów IP udostępnionych do dzierżawy

Rezerwacja określa wybrany z zakresu adres, którego dzierżawienie jest zarezerwowane dla określonego klienta DHCP

Opcje DHCP są dodatkowymi parametrami konfiguracyjnymi, przydzielanymi klientom DHCP razem z jego adresem IP. Np.:
- adres routera IP
- adres serwera DNS
- adres serwera WINS
- nazwa domeny DNS

Klasy:
- Klasy dostawców służą do przypisania opcji DHCP na podstawie identyfikatora dostawcy
- Klasy użytkowników służą do przypisywania opcji DHCP na podstawie potrzeb użytkowników

Agentem DHCP jest komputer lub router który nasłuchuje komunikatów DHCP/BOOTP od klientów DHCP i przekazuje te komunikaty do serwera DHCP innej podsieci

Router zgodne z RFC 1542 to router który przekazuje żądania DHCP do innej podsieci.

Jak pracuje Agent DHCP:

- Klient wysyła pakiet rozgłoszeniowy DHCPDISCOVER
- Agent przekazuje komunikat DHCPDISCOVER do serwera DHCP
- Serwer wysyła komunikat DCHPOFFER do agenta DHCP
- Agent rozgłasza pakiet DHCPOFFER
- Klient rozgłasza pakiet DHCPREQUEST
- Agent przekazuje komunikat DCHPREQUEST do serwera DHCP
- Serwer wysyła komunikat DHCPACK do agent DHCP
- Agent rozgłasza pakiet DHCPACK

Próg licznika skoków (hoop count threshold) określa liczbę routerów, przez które może być transmitowany pakiet agenta zanim zostanie odrzucony.

Wartość progowa czasu od rozruchu to wyrażona w sekundach długość czasu jaki agent przekazywania DHCP będzie czekać aby lokalny serwer DHCP odpowiedział na żądania klienta, zanim prześle dalej to żądanie

Dynamiczna **baza danych usługi DHCP** zawiera dane konfiguracyjne usługi DHCP (w tym między innymi informacje o zakresach, zastrzeżeniach, opcjach, dzierżawach). Uruchomienie usługi DHCP bez bazy danych jest niemożliwe. Jest aktualizowana w momencie gdy klient DHCP uzyskuje lub zwalnia dzierżawę

Baza danych usługi DHCP składa się z następujących plików, które są przechowywane w katalogu ***\%Systemroot%\system32\dhcp***:

- **dhcp.mdb** Plik bazy danych dla usługi DHCP. Plik zawiera dwie tabele: tabelę mapowań adresów IP na identyfikatory właścicieli i tablicę mapowań nazw na adresy IP.
- **tmp.edb** Tymczasowy plik, który służy bazie danych DHCP jako plik wymiany podczas operacji związanych z obsługą indeksów bazy danych.
- **j50.log** i **j50*.log** Dzienniki wszystkich transakcji przeprowadzonych z bazą danych. W razie potrzeby usługa DHCP wykorzystuje te dzienniki do odzyskiwania danych.
- **res*.log** Zarezerwowane pliki dzienników służące do rejestrowania istniejących transakcji, jeśli w systemie zabraknie miejsca na dysku.
- **j50.chk** Plik punktu kontrolnego.

Do kompaktowania ręcznego bazy danych DHCP używamy programu Jetpack.

Domyślnie usługa DHCP co **60** minut automatycznie wykonuje kopię zapasową bazy danych usługi DHCP i związanych z nią wpisów rejestru w katalogu kopii zapasowej na dysku lokalnym. Automatycznie wykonywane kopie zapasowe są domyślnie przechowywane w katalogu \%Systemroot%\system32\dhcp\backup\new. Administrator może zmienić lokalizację kopii zapasowej.

Jeśli w momencie uruchomienia usługi DHCP okaże się, że nie można załadować oryginalnej bazy danych usługi DHCP, wtedy usługa DHCP automatycznie przywraca ją z katalogu kopii zapasowej na dysku lokalnym. W przypadku awarii bazy danych DHCP administrator może ją przywrócić albo z katalogu kopii zapasowej na dysku lokalnym, albo z innego nośnika. W przypadku, gdy serwer ulegnie awarii sprzętowej i lokalna kopia zapasowa jest niedostępna, administrator może przywrócić bazę danych tylko z innych nośników.

Uzgadnianie to proces sprawdzania zawartości bazy danych usługi DHCP przez porównanie z wartościami rejestru usługi DHCP.

Uzgodnienie bazy danych usługi DHCP jest wskazane w następujących sytuacjach:

- Gdy zawartość bazy danych usługi DHCP jest poprawna, ale nie jest poprawnie wyświetlana w konsoli DHCP.
- Jeśli po przywróceniu bazy danych usługi DHCP baza danych usługi DHCP nie zawiera aktualnych informacji.

Laboratorium 2: DNS

Rozpoznawanie nazw hostów to proces tłumaczenia nazw hostów na adres IP.

Nazwa **host** jest nazwą DNS urządzenia w sieci, która jest używana do lokalizacji komputera w sieci.

Server1. nwtraders.com
Hostname|DNS suffix

Metody rozpoznawania nazw hostów przez klienta DNS:

- Pamięć podręczna programu rozpoznawania nazw na komputerze klienckim
- Serwer DNS
- Plik hosts

Bufor resolvera gromadzi nazwy hostów które ostatnio były rozwiązywane oraz nazwy załadowane z pliku Hosts. Wyświetlanie za pomocą:
Ipconfig /displaydns

Plik hosts znajduje się w folderze **%Systemroot%\system32\drivers\etc\.** Gdy w pliku hosts zostanie utworzone mapowanie nazwy hosta na adres IP i plik zostanie zapisany, mapowanie zostanie załadowane do pamięci podręcznej programu rozpoznawania nazw na komputerze klienckim.

Domenowa przestrzeń nazewnicza (domain Namespaces):
Root Domain -> Top-Level Domain -> Second-Level Domain -> Subdomain -> Komponenty DNS -> Klienci DNS, Serwery DNS, Serwery DNS w intranecie

Obszar nazw DNS obejmuje domenę główną, domeny najwyższego poziomu, domeny drugiego poziomu i (zazwyczaj) poddomeny. Obszar nazw DNS i nazwa hosta składają się na w pełni kwalifikowaną nazwę domenową (**FQDN**).

Zapytanie/kwerenda DNS jest żądaniem rozwiązania nazwy kierowanym do serwera DNS. Rozróżniamy dwa typy zapytań: rekursywne i iteracyjne. Kwerenda DNS to żądanie adresu IP dla określonej nazwy, przesłane do serwera DNS przez program klienta DNS.

Zarówno klient DNS jak i serwer DNS mogą zainicjować żądanie rozwiązania nazwy

Serwer DNS może być autorytatywny lub nieautorytatywny dla żądanego obszaru nazw.

Autorytatywny serwer DNS to taki, który zawiera podstawową lub pomocniczą kopię strefy DNS.
Jeśli serwer DNS jest autorytatywny dla obszaru nazw, to:

- sprawdza pamięć podręczną, sprawdza strefę, a następnie zwraca żądany adres
- zwraca autorytatywne „Nie”

Jeśli serwer DNS jest **nieautorytatywny** dla obszaru nazw, to:

- przesyła dalej nierozwiązaną kwerendę do określonego serwera, nazywanego usługą przesyłania dalej
- używając znanych adresów wielu serwerów głównych, inicjuje przeglądanie drzewa DNS w celu znalezienia odpowiedzi na kwerendę. Proces ten jest również nazywany wskazówkami dotyczącymi serwerów głównych.

Zapytanie rekursywne (cykliczne) jest zapytaniem, w którym klient oczekuje od serwera DNS kompletnej odpowiedzi. Dopuszczalna jest pełna odpowiedź lub odpowiedź, że nazwa nie może zostać rozpoznana. Serwer DNS szukając odpowiedzi sprawdza strefę wyszukiwania do przodu (forward lookuop zone i bufor)

Root Hints są rekordami DNS na serwerze DNS, które przechowują adresy głównych serwerów DNS (serwerów domeny głównej). Adresy IP serwerów głównych są przechowywane w pliku Cache.dns znajdującym się w folderze **%Systemroot%\system32\Dns**.

Zapytanie iteracyjne (iterative Queries) jest zapytaniem do serwera DNS, w którym klient DNS prosi o najlepszą odpowiedź jakiej dany serwer może dostarczyć bez przeszukiwania innych serwerów DNS. Odpowiedzią jest często wskazanie na inny serwer DNS w drzewie DNS

Forwarder (usługa przesyłania dalej) jest serwerem DNS wyznaczonym do rozwiązywania nazw w odpowiedzi na zapytania innych serwerów.

Buforowanie na serwerze DNS – Buforowanie polega na tymczasowym przechowywaniu ostatnio uzyskanych informacji w celu przyspieszenia kolejnych dostępów do tej informacji

Rekord zasobu (RR) jest standardową strukturą bazy DNS zawierającą informację używaną do przygotowania odpowiedzi na zapytanie

Typy rekordów:

- **A** host
- **PTR** wskaźnik
- **SOA** adres startowy uwierzytelniania / pierwszy rekord w strefie
- **SRV** rekord usługi
- **NS** serwer nazw
- **MX** wymiennik poczty
- **CNAME** alias

Strefa jest częścią bazy DNS, która zawiera rekordy (RR) należące do ciągłej przestrzeni nazw DNS

Typy stref:

- **podstawowa** autorytatywna kopia bazy DNS (odczyt / zapis)
- **wtórna** odczytywalna kopia bazy DNS
- **bazowa / skrótowa** kopia z ograniczoną liczbą rekordów (SOA, NS, A)

Strefa wyszukiwania do przodu - wyszukiwanie proste to proces, w którym jest wyszukiwana nazwa domenowa komputera-hosta w celu znalezienia odpowiadającego jej adresu IP.

Strefa wyszukiwania wstecz - wyszukiwanie wsteczne to proces, w którym jest wyszukiwany adres IP komputera-hosta w celu znalezienia jego nazwy domenowej.

Transfer strefy (zone transfer) to mechanizm synchronizacji autorytatywnych stref DNS pomiędzy serwerami DNS

Proces transferu strefy:

- kwerenda SOA dla strefy
- odpowiedź na kwerendę SOA
- kwerenda IXFR lub AXFR (I jeżeli jest obsługa przyrostowa i chcemy tylko informacje od ostatniej aktualizacji, A jeżeli chcemy całą strefę)
- odpowiedź IXFR lub AXFR

Mechanizm powiadomienia (DNS notify) umożliwia powiadomienie serwerów pomocniczych o modyfikacji strefy. Rekord zasobu został zmodyfikowany i numer SOA został zmodyfikowany serwer podstawowy wysyła powiadomienie o zmianie strefy. A serwery zapasowe wysyłają żądanie transferu strefy.

Dynamiczna aktualizacja jest procesem w którym klient DNS dynamicznie tworzy, rejestruje lub uaktualnia swoje rekordy w strefie. Proces ten jest nadzorowany przez serwer DNS.

Ręczna aktualizacja jest procesem w którym administrator ręcznie tworzy, rejestruje lub uaktualnia rekordy zasobów. Umożliwia komputerowi klienta automatyczną współpracę z serwerem DNS w celu tworzenia, rejestracji lub uaktualnienia swoich własnych rekordów w strefie

Proces dynamicznej aktualizacji klienta DNS

- Klient wysyła zapytanie SOA
- Serwer DNS wysyła nazwę strefy i adres IP serwera
- Klient sprawdza istniejącą rejestrację
- Serwer DNS odpowiada stwierdzeniem, że nie ma rejestracji
- Klient wysyła dynamiczną aktualizację do serwera DNS

Proces dynamicznej aktualizacji rekordów na serwerze DNS

- Klient DHCP wysyła żądanie dzierżawy adresu IP
- Serwer DHCP zgadza się na dzierżawę
- Serwer DHCP automatycznie generuje FQDN
- Serwer DHCP aktualizuje rekord DNS hosta i rekord DNS wskaźnika dla klienta

Strefa DNS zintegrowana z usługą Active Directory to strefa DNS przechowywana w usłudze Active Directory. Strefy zintegrowane z AD mogą używać usług:

- przechowywania danych o konfiguracji strefy w usłudze Active Directory zamiast w pliku strefy.
- korzystania z replikacji usługi Active Directory zamiast z transferów stref.
- zezwalania tylko na zabezpieczone aktualizacje dynamiczne (zamiast na zabezpieczone i niezabezpieczone aktualizacje w strefach innych niż zintegrowane z usługą Active Directory).

W procesie **delegowania** autorytarność w stosunku do domeny podrzędnej jest przypisywana innej jednostce poprzez dodanie stosownego rekordu w bazie DNS.

Wartość TTL zawarta w rekordach i strefach DNS zwracanych w kwerendzie jest wyrażona w sekundach i określa czas po upływie którego udzielona odpowiedź staje się nieważna.

Przedawnienie to proces prowadzący do ustalenia czy stary rekord zasobu DNS powinien zostać usunięty z bazy danych DNS

Oczyszczanie to proces czyszczenia i usuwania nieaktualnych lub wygasłych danych z bazy usługi DNS

Nslookup jest narzędziem służącym do diagnozowania infrastruktury systemu DNS

DNSCmd jest narzędziem z pakietu Support Tools które umożliwia wykonywanie wielu zadań administracyjnych z wiersza poleceń

DNSLint jest narzędziem które wysyła serię zapytań w celu wspomożenia diagnostyki procesu rozwiązywania nazw

Laboratorium 3: WINS

WINS - Proces rozwiązywania nazw NetBIOS

Nazwa NetBIOS jest identyfikatorem używanym przez usługę NetBIOS pracującą na komputerze. Składa się z 15 znaków nazwy właściwej i jednego znaku (przyrostka) oznaczającego rodzaj usługi. Razem ma **16 znaków / bajtów**.

Nazwa netBIOS	Przyrostek	usługa	adres IP
Server2	00	workstation	192.168.0.39
Server2	20	Server	192.168.0.39
Server2	01	Messenger	192.168.0.39

Domyślna kolejność wysyłania kwerendy do serwera WINS:
Pamięć podręczna -> Usługa WINS -> Emisja -> Plik lmhost

Emisje lokalne to komunikaty sieciowe wysyłane z jednego komputera do pozostałych urządzeń znajdujących się w danym segmencie sieci

Readrestor NetBios rozsyła emisję lokalną

- jeśli zasób znajduje się w sieci lokalnej generowana jest odpowiedź na emisję i zwracany jest adres IP
- jeśli zasób znajduje się w sieci zdanej emisja nie zostanie przesłana przez router

Plik lmhosts – to lokalny plik tekstowy w którym są zamapowane nazwy NetBIOS na adresu IP hostów

- Plik lmhosts musi znajdować się na każdym komputerze.
- Domyślna lokalizacja pliku lmhosts to folder **%Systemroot%\system32\drivers\etc**, a plik ma rozszerzenie sam. Aby możliwe było odczytywanie tego pliku, trzeba usunąć rozszerzenie sam.
- Wpisy pliku lmhosts zawierające słowo kluczowe #PRE będą wstępnie ładowane do pamięci podręcznej nazw NetBIOS. Mapowania nazw NetBIOS oznaczone słowem kluczowym #PRE będą pozostawać w pamięci podręcznej nazw NetBIOS, dopóki mapowania ze słowem kluczowym #PRE nie zostaną usunięte z pliku lmhosts.

Typ węzła NetBIOS – określają sposób tłumaczenia nazw NetBIOS na adres IP.

- **B** – do rejestrowa i rozwiązywania nazwy jest rozgłaszanie -- 1
- **P** – do rejestrowania i rozwiązywania nazwy wykorzystywany jest serwer nazw taki jak serwer WINS --2
- **M**— kombinacja typów B i P domyślnie stosowany jest typ B – 4
- **H**—kombinacja typów P i B domyślnie stosowany jest typ P –8

Proces rejestracji i zwalniania nazwy

- Klient WINS wysyła żądanie rejestracji
- Serwer WINS zwraca komunikat rejestracyjny z wartością TTL określającą czas ważności. Domyślnie TTL = 6dni. Próba odnowienia po 3 dniach.
- Klient WINS wysyła żądanie zwolnienia nazwy
- Serwer WINS wysyła potwierdzenie zwolnienia

Obsługa serii (burst handling) oznacza reakcję serwera do dużej ilości klientów którzy jednocześnie próbują zarejestrować swoje nazwy – krótki czas wygaśnięcia. Domyślna wartość to 500.

Rozwiązywanie nazw przez serwer WINS

- Klient WINS kontaktuje się z pierwszym serwerem WINS trzy razy w celu rozwiązania nazwy przy użyciu usługi WINS.
- Jeśli pierwszy serwer WINS nie odpowie, klient kontaktuje się kolejno z pozostałymi dostępnymi serwerami WINS aż do uzyskania odpowiedzi.
- Jeśli serwer WINS rozpozna nazwę NetBIOS, zwraca adres IP do klienta. Po otrzymaniu odpowiedzi klient w oparciu o uzyskany adres nawiązuje połączenie z żądanym zasobem.
- Jeśli żaden serwer WINS nie jest w stanie rozpoznać nazwy NetBIOS, proces rozpoznawania jest kontynuowany poza usługą WINS. Typowy klient o typie węzła H próbuje użyć emisji. Jeśli emisja nie przynosi rezultatu, klient sprawdza wpisy z pliku Lmhosts.

Rekord klienta to rekord bazy danych, zawierający szczegółowe informacje o każdej usłudze zależnej od systemu NetBIOS, zainstalowanej na komputrze klienckim.

Mapowanie statyczne – oznacza ręczne wprowadzanie pozycji do bazy WINS. Administrator wprowadza pozycję określając nazwę i adres IP komputera

Replikacja WINS polega na kopiowaniu zaktualizowanych danych WINS z jednego serwera WINS na inne w celu zsynchronizowania tych danych

Replikacja wypychana / typu pchnij (PUSH) - Replikacja tego typu zapewnia wysoki poziom synchronizacji, ale wymaga szybkich łączy

- Serwer A osiąga poziom 50 zmian w bazie
- Serwer A informuje partnera że określony poziom został osiągnięty

- Serwer B odpowiada żądaniem replikacji
- Serwer A wysyła repliki nowych pozycji w bazie

Replikacja ściągana / typu ciągnij (PULL) - Ten typ replikacji ogranicza częstotliwość replikacji dla wolnych łączy szybkich łączy

- Partner typu PULL żąda replikacji na podstawie upływającego czasu

Replikacja wypychania/ściągania / typu pchnij i ciągnij (PUSH & PULL)

- Replikacja ta zapewnia że bazy na różnych serwerach WINS są niemalże w każdym momencie identyczne
- Informacje partnerów gdy w bazie osiągnięty zostanie założony poziom zmian oraz żądanie replikacji co określony czas

Właściwości partnerów replikacji WINS

- **włączanie automatycznej konfiguracji partnera** - wykrywanie serwery WINS dołączające się do sieci są dodawane jako partnerzy replikacji
- **włączania połączeń stałych** - przyśpiesza wykonywanie replikacji ponieważ serwer może natychmiast wysyłać rekordy do partnerów
- **włączanie zastępowania unikatowych mapowań statycznych na serwerze (migrowanie włączone) -** jeśli w trakcie procesu aktualizacji usługa WINS zgłasza dla tej samej nazwy zarówno wpis dynamiczny, jak i statyczny, zachowywany jest wpis statyczny. To domyślne zachowanie można jednak zmienić, zaznaczając ustawienie Zastąp unikatowe mapowania statyczne na tym serwerze (migrowanie włączone).

Aby **naprawić uszkodzoną bazę WINS** należy dysponować jej kopią zapasową

Usuwanie rekordów - operacja usuwania prostego powoduje usunięcie rekordów zaznaczonych w konsoli usługi WINS tylko z aktualnie zarządzanego lokalnego serwera WINS. Jeśli rekordy usuwane w ten sposób zostały zreplikowane na inne serwery WINS, repliki nie zostaną usunięte. Pozostaną one w bazach danych tych serwerów do czasu, aż administrator usunie je za pośrednictwem konsoli WINS, wykonując tę operację osobno dla każdego serwera.

Ukrywanie rekordów - jeśli w celu usunięcia rekordu, którego właścicielem jest wybrany serwer, zostanie użyta metoda ukrywania, operacja zostanie przeprowadzona na wszystkich serwerach WINS, do których rekord został zreplikowany. Serwer WINS będący właścicielem rekordów zmienia ich stan na ukryty. W efekcie usługa WINS traktuje rekordy jako nieaktywne i nie korzysta z nich. Gdy te rekordy zostaną ukryte lokalnie, serwer będący ich właścicielem nie odpowiada na kwerendy o nazwy NetBIOS wysyłane przez innych klientów i serwery WINS ani nie rozpoznaje tych nazw, dopóki rekordy te nie zostaną ponownie zarejestrowane przez klienta WINS. W kolejnych cyklach replikacji serwer właścicielski WINS replikuje zaznaczone rekordy jako „ukryte” do pozostałych serwerów WINS.

Zagęszczanie bazy (Compacting) - to proces odzyskiwania niewykorzystywanego miejsca w bazie danych WINS które zajmują przestarzałe rekordy. Umożliwia itrzymywanie integralności bazy poprzez:

- **zagęszczanie dynamiczne** – realizowanie automatycznie podczas wykorzystywania bazy
- **zagęszczanie offline** – administrator zatrzymuje serwer WINS i wykorzystuje polecenie **jetpack**

Oczyszczanie - proces usuwania i kasowania wygasłych wpisów bazy danych WINS. W trakcie oczyszczania usuwane są również wpisy, które zostały zreplikowane ze zdalnego serwera WINS i nie zostały usunięte z lokalnej bazy danych WINS. Proces ten jest inicjowany automatycznie w odstępach czasu ustalonych przez:

- **interwał odnawiania** - częstotliwość z jaką klient odnawia rejestracje swoich nazw na serwerze (domyślnie 6 dni)
- **interwał wygaśnięcia** - odstęp czasu między oznaczeniem wpisu jako zwolniony, a oznaczeniem go jako wygasły (domyślnie 4 dni)
- **limit czasu wygaśnięcia** - odstęp czasu między oznaczneim wpisu jako wygasły a jego wyczyszczeniem z bazy danych WINS. Wartość taka sama co interwału odnawiania.
- **interwał weryfikacji** - czas po jakim serwer sprawdza, czy nazwy, których nie jest właścicielem są nadal aktywne. Wartość minimalna 24 dni.

Sprawdzanie spójności bazy – Sprawdzanie spójności bazy danych WINS pomaga zachować integralność baz istniejących na serwerach WINS w dużej sieci

Laboratorium 4: ADMINISTRACJA SERWEREM

Zdalne administrowanie serwerem – **usługa terminalowa**

Grupy używane do **administrowania serwerem**:

- administratorzy,
- operatorzy kopii zapasowych,
- operatorzy kont,
- operatorzy serwerów,
- operatorzy drukarek.

Administratorzy zawsze powinni być członkami grupy która jest najbardziej **ograniczona / restrykcyjna**.

Polecenie „uruchom jako" służy do logowania się na koncie administracyjnym podczas pracy na koncie „nie administracyjnym" i wykonywania zadań administracyjnych. Polecenia „uruchom jako" można uruchomić za pomocą:

- **menu start**,
- **eksploratora Windows**
- **cmd** (Runas /user:nazwa_domeny\nazwa _użytkownika nazwa_programu)

Konsola Computer Management MMC jest zestawem narzędzi administracyjnych, przy pomocy których można lokalnie i zdalnie zarządzać komputerem. Oferuje interfejs dla przystawek służących do zarządzania sprzętem oprogramowaniem i usługami sieciowymi na serwerach z systemem Windows.

Przystawka *Zarządzanie komputerem*: Służy do zarządzania komputerami lokalnymi i zdalnymi (narzędzia systemowe, magazyn, usługi i aplikacje

Pulpit zdalny dla administracji – usługa bazuje na protokole **RDP**

Wymagania usługi Pulpitu zdalnego:

- usługę pulpitu zdalnego należy włączyć lokalnie na serwerze zdalnym
- usługę pulpitu zdalnego należy skonfigurować tak aby umożliwić użytkownikom zdalne łączenie się z serwerem
- Zamknięcia okna sesji nie kończy sesji

Podłączenie pulpitu zdalnego:

- Podłączenie do jednego serwera (z uruchomionym Pulpitem zdalnym) w jednej sesji
- Pulpity zdalne: Jednoczesne łączenie się z wieloma serwerami. Każde połączenie jest wyświetlane w konsoli MMC

Limity dla połączeń Pulpitu zdalnego - ustawieniu limitu czasu umożliwiają zapobieganie zużywaniu cennych zasobów serwera przez połączenie zdalne

- Zakończ sesję odłączoną (ile czasu po odłączeniu sesji)
- Limit czasu sesji aktywnych (odłączenie po określonym czasie użytkownika)
- Limit czasu bezczynności sesji

Menedżer usług terminalowych umożliwia:

- monitorowanie sesji użytkownika
- ręczne wymuszanie wylogowania użytkownika lub odłączenia sesji
- nadzorowania

Zalety wykorzystania usług terminalowych

- scentralizowana dystrybucja aplikacji biznesowych
- dostęp do pulpitu systemu Windows
- poszerzone możliwości administracji i obsługi technicznej

Usługa terminalowa wymaga licencjonowania. Typy licencji:

- dostępowa
- wbudowana
- połączenia internetowego
- tymczasowa

L2TP – złożenie protokołu PTTP i L2f

Zasada dostępu zdalnego to nazwana reguła która składa się z następujących elementów:

- warunków
- uprawnienia do dostępu zdalnego
- profili

Laboratorium 5: RADIUS, Podpis cyfrowy, PKI

Radius to szeroko rozpowszechniony protokół oparty na modelu klient/serwer, który umożliwia **centralne uwierzytelnianie, autoryzację, księgowanie dostępu do sieci**. Radius to standardowy protokół zarządzania dostępem do sieci przy użyciu łączy VPN, połączeń telefonicznych i bezprzewodowych. Przy użyciu protokołu Radius można centralnie zarządzać wieloma typami dostępu do sieci.

Serwery Radius odbierają, przetwarzają żądania połączeń lub komunikaty księgowania wysyłane przez klientów lub serwery proxy usługi Radius.

Usługa uwierzytelniania internetowego **IAS -** składnik systemu Windows Server zgodny ze standardem serwer Radius . Serwer IAS wykonuje scentralizowane uwierzytelnienie autoryzację, inspekcję i księgowanie połączeń VPN, telefonicznych i bezpośrednich.

Narzędzia:

- **monitor systemu** - umożliwia przeglądanie danych dotyczących wydajności w czasie rzeczywistym obejmuje określone składniki i usługi
- **dzienniki wydajności i alerty** - umożliwiają rejestrowanie konkretnych danych dotyczących wydajności składników i usług
- **monitor sieci bezprzewodowej** - udostępnia szczegółowe informacje o kunktach dostępu do sieci bezprzewodowej i klientach sieci bezprzewodowej

Radius:

- usługa urzędu certyfikacyjnego
- kryptografia asymetryczna

Podpis cyfrowy jest zwykle realizowany poprzez zaszyfrowanie skrótu (hash) wiadomości. Wykorzystywani jest klucz prywatny nadawcy. Proces takiego szyfrowania nazywamy podpisywaniem.

Podpis cyfrowy zapewnia:

- integralność
- uwierzytelnienie
- niezaprzeczalność

Podpis cyfrowy można dołączyć do dowolnego przesyłanego dokumentu.

Infrastruktura klucza publicznego - zbiór sprzętu oprogramowania ludzi polityki oraz procedur niezbędnych do tworzenia zarządzania przechowywania dystrybucji oraz odbierania certyfikatów opartych na kryptografii z kluczem publicznym.

Celem infrastruktury klucza publicznego (PKI) jest zapewnienie zaufanego i wydajnego zarządzania kluczami oraz certyfikatami. PKI jest zdefiniowany w dokumencie Intranet X.509 Public Key Infracture.

Urząd certyfikacyjny (CA) - jest punktem zaufania dla wszystkich elementów PKI, certyfikuje związek pomiędzy parą kluczy a identyfikatorem użytkownika.

Cechy:

- Klucz prywatny CA służy do podpisywania wszystkich certyfikatów PKI.
- Główny CA podpisuje certyfikaty przekazane do innych PKI
- Każdy element PKI musi mieć dostęp do kopii klucza publicznego CA

Unieważnienie certyfikatu

- CA podpisuje certyfikat łącząc parę kluczy z tożsamością użytkownika
- Typowe przyczyny unieważnienia to zmiana tożsamości ujawnienie klucza prywatnego lub zmiana statusu służbowego
- Musi być dostępny sposób zaalarmowania środowiska że nie można używać danego klucza dla tej tożsamości
- Taki mechanizm alarmowy nazywany w PKI unieważnieniem certyfikatu

Inne:

- Listy unieważnionych certyfikatów (CRLs)
- Listy unieważnionych certyfikatów urzędów certyfikacji (CARLs)
- Listy unieważnionych certyfikatów jednostek końcowych (EPRLs)
- Punkty dystrybucji CRL
- Mechanizm zapytań online
- Protokół OCSP
- Protokół SCVP