HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK

HÁLÓZATOK ALAPJAI ÉS ÜZEMELTETÉSE

Üzemeltetési és hibakezelési stratégiák

2019. május 14.

Zsóka Zoltán

BME Hálózati Rendszerek és Szolgáltatások Tanszék

zsoka@hit.bme.hu

MŰEGYETEM 1782

MA MIRŐL LESZ SZÓ?

1. Üzemeltetés - házirend
2. Hibakeresés
3. Összefoglalás

ÜZEMELTETÉSI FELADATOK

- Naprakészség biztosítása – funkcionális és biztonsági frissítések telepítése
  - Operációs rendszerek
  - A hálózat szolgáltatásait biztosító alkalmazások
  - Felhasználói programok
  - Védelmi rendszerek
- Felügyelet, szükség esetén azonnali beavatkozással
  - Számítógépek
  - Kapcsolóeszközök
  - Szolgáltatások
- Monitorozás, teljesítményadatok figyelése
- Jogosultsági rendszer karbantartása
- A felhasználó oldalán
  - Programok telepítése, beállítása
  - Munkakörnyezet karbantartása
- Hibafelismerés és -elhárítás

- A menedzsment rendszerekre alapozva látják el
- Mihez kell igazodni?
  - Felelősségi körök – jogosultsági rendszer
  - Biztonságos működés: házirend

HÁLÓZATI HÁZIREND

- Cél: egy szervezet (pl. cég) esetén szabályozni a hálózat használatát
  - Szerepkörök – hozzáférés az eszközökhöz és erőforrásokhoz
  - Szervezeti struktúra leképezése felelősségi körökre
    - Ki milyen hozzáféréseket birtokol és módosíthat
    - Pl: Gazdasági igazgató, IT biztonsági igazgató, rendszergazda
- A házirend ismerteti a
  - Veszélyeket
  - Helyes használatot
  - Szankciókat
- Hatókör – mindenkire érvényes, aki hozzáfér a hálózathoz
  - Cég alkalmazottai
  - Partnerek
  - Vendégek

HÁZIREND KÉSZÍTÉSE

- Több csoport (részleg) együttműködésével
  - Vezetőség: jóváhagyás
  - Hálózati és hálózatbiztonsági csoport: technikai részletek
  - Felhasználók: véleménynyilvánítás
  - Jogi osztály: jogszabályi megfelelés
  - Személyzeti vagy sajtó osztály: megismertetés az érintettekkel
- Előírások kikényszerítése a végpontokon – több szinten
  - Kötelező: csak akkor fér a hálózathoz, ha teljesül az előírás
  - Ajánlott: a felhasználó figyelmeztetést kap az előírásról
  - Ellenőrzés: többnyire a felhasználó tudta nélkül, az eredményt naplózzák
- Szerepkörök
  - Belső: pl. adminisztrátor, privilegizált felhasználó, általános felhasználó
  - Külső: pl. partner, vendég
- Megkülönböztetés a végpont típusa alapján
  - Pl: asztali gép, laptop, okostelefon, VPN

A HÁZIREND ELEMEI

- Szervezetenként eltérhet a cél, és így a házirend is
- Jellemző elemek
  - Áttekintés
  - Célkitűzés
  - Hatályosság
    - Érintett szervezeti egységek
    - Időbeli korlátok
  - Követelmények, feltételek, felelősségek, szankciók
  - Definíciók – szakkifejezések feloldása
  - Történeti áttekintés – változások dokumentálása, verziókövetés
- Elkülönülő részei lehetnek
  - Technikai részletek a hálózati szakembereknek
  - Használati előírások felhasználóknak

HÁZIREND SZABÁLYOK – PÉLDÁK

- Felhasználói nevek és jelszavak
  - Alapértelmezett jelszavakat meg kell változtatni
  - A jelszavaknak kellően erősnek kell lenniük
  - Rendszeres időközönként cserélni kell őket
  - A nem használt felhasználói neveket rövid időn belül törölni kell
- Biztonsági- és operációs rendszerek naprakész frissítése
  - Antivírus szoftverek rendszeres frissítése
  - Az operációs rendszerek automatikus frissítése vagy ennek tiltása
- Vendégek hozzáférése
  - Nincs hozzáférés a belső hálózathoz
  - Az Internetet elérhetik
- Hálózati (Ethernet) csatlakozók védelme
- Email-ek szűrése
  - Forráscímek alapján
  - Mellékletek típusa alapján
- Tartalomszűrés tűzfallal

MA MIRŐL LESZ SZÓ?

1. Üzemeltetés - házirend
2. Hibakeresés
3. Összefoglalás

HIBAKERESÉS CIKLUSA

- Probléma azonosítása
  - Megfigyelés, adatgyűjtés
  - Elemzés
  - Hipotézisek felállítása a lehetséges okokra
  - Célzott tesztelés
- Megoldás kidolgozása
  - Lehetséges megoldások számbavétele
  - Megoldás kiválasztása
  - Végrehajtás
- Ellenőrzés
- Dokumentáció – jobb ha nem csak utólag
  - Viszonyítási alap (baseline) – tipikus működés esete
- „A sikeres hibaelhárítás a hiba megjelenése előtt kezdődik”

HIBAKERESÉSI MÓDSZEREK

- Caveman, brute force
  - Addig állítgatunk, dugdosunk, amíg nem szűnik meg a hiba
  - Hibás eljárás
  - További hibákat okozhat
  - Elfedhet meglevő hibákat
- Elméleti megközelítés
  - A dokumentált fizikai és logikai hálózati kép alapján
  - Logikai következtetésekkel
  - Bonyolult rendszereknél nem könnyű
- **Szisztematikus eljárás**
  - Rétegről rétegre haladunk, szűkítve a lehetséges okokat
  - A hiba pontos behatárolását teszi lehetővé
- Követendő alapelv: egyszerre egy ponton avatkozunk be

SZISZTEMATIKUS HIBAKERESÉS

- Lentről felfelé – bottom-up tesztelés
  - A legalsó rétegtől felfele haladva
  - Minden rétegben ellenőrzés a hibával kapcsolatba hozható elemeknél
- Fentről lefelé – top-down tesztelés
  - Legfelső réteg: ahol a hibát tapasztaltuk
  - Rétegenként lefelé haladva
- Középutas módszer
  - Valamelyik közbülső rétegtől indulva
  - Felfelé, vagy lefelé haladva
  - A kiindulási réteg tapasztalati úton is kiválasztható
  - Tipikusan a hálózati rétegtől indulnak
  - Feltételezi a hálózat ismeretét, a tipikus hibajelenségek okainak ismeretét
- Egy-egy rétegben számos funkciót kellhet tesztelni

ESZKÖZÖK A HIBAKERESÉSHEZ

- Végpontokon alkalmazható eszközök
  - ipconfig, ifconfig, ip address
  - arp
  - route
  - ping
  - tracert, traceroute
  - netstat
  - dig, (nslookup)
  - telnet
  - Wireshark, tcpdump
- Hálózati kapcsoló-berendezések lekérdezése
  - Menedzsment felület
    - Programozható lekérdezések – NETCONF, RESTCONF
    - SNMP
  - Parancssoros lekérdezések
    - Pl. Cisco: show parancsok
    - Konfigurációra vonatkozhat, pl. show running-config
    - Aktuális állapotra vonatkozhat, pl show ip interface brief

TIPIKUS HIBÁK OKAI - IPCONFIG

- Tipikus parancs: ipconfig /all
- A kimenet üres
  - Nincs ethernet kártya, le van tiltva, nincs hozzá driver, ...
- Az IP cím 0.0.0.0
  - Valószínűleg a DHCP címkérés még folyamatban van
  - DHCP cím visszaadása: ipconfig /release
  - DHCP cím lekérése, vagy meghosszabbítása: ipconfig /renew
- Az IP cím 169.254.x.x alakú
  - A DHCP sikertelen
  - IPv4 autokonfigurációs cím (APIPA - Automatic Private IP Addressing, RFC3927)
- Default gateway címe rossz
- DNS szerver hiányzik, vagy nem a várt cím

TIPIKUS HIBÁK OKAI

- arp
  - Tipikus parancs: arp -a
  - IP címhez nem a várt MAC-cím tartozik
    - Több azonos IP cím a LANon
    - Támadásra is utalhat
  - Forgalmat indítottunk, mégsincs bejegyzés egy adott címhez
    - L2 (vagy lejjebbi) probléma valószínű, pl hibás VLAN beállítások
- route
  - Tipikus parancs: route print
  - Több különböző default gateway cím
    - Több interfész különböző beállítással, a forgalom nem arra megy ki, mint gondolnánk

TIPIKUS HIBÁK OKAI - PING

- "Destination host unreachable": a hoszt nem érhető el
  - A helyi hálózaton
    - Nincs bekapcsolva a gép
    - Nincs a hálózathoz kapcsolva
    - Rossz az IP konfiguráció
    - L2 hiba
  - Távoli hoszt esetén
    - Routing hiba
- Egyetlen válasz sem érkezik (timeout), vagy "Destination net unreachable"
  - A távoli gép vagy hálózat nem érhető el (nincs bekapcsolva)
  - Tűzfal szűri az ICMP echo request csomagokat (tipikusan a cél hálózatánál)
- Válaszok érkeznek, de vannak elmaradt válaszok is
  - Csomagvesztés az út mentén
    - Rossz kábel vagy interfész
    - Túlterhelt link
    - Routing gyakori változása (lengés)

MA MIRŐL LESZ SZÓ?

1. Üzemeltetés - házirend
2. Hibakeresés
3. Összefoglalás

MIRŐL VOLT EDDIG SZÓ?

- Hálózatok alapelemei, az Internet alapjai
- Protokoll, szerkezet és szolgáltatás
- Az Internet szerkezeti részei
- Áramkörkapcsolás és csomagkapcsolás
- Csomagvesztés, késleltetés, átbocsátóképesség

- Az Internet felépítése
- Protokollrétegek
- Hálózati alkalmazások alapjai

- A Web és a HTTP
- Fájlátvitel
- Az elektronikus levelezés protokolljai
- Doménnév-szolgáltatás az Interneten

MIRŐL VOLT EDDIG SZÓ?

- Socketek programozása
- A szállítási réteg szolgáltatásai
- Nyalábolás és nyalábbontás
- Összeköttetés nélküli szállítás: UDP

- A TCP protokoll
- Szegmensek nyugtázása
- Forgalomszabályozás
- Kapcsolatkezelés

- Torlódáskezelés a TCP-ben
- TCP átbocsátás és igazságosság
- További TCP funkciók
- A QUIC protokoll

MIRŐL VOLT EDDIG SZÓ?

- Portok besorolása
- A hálózati réteg funkciói
- IPv4
- IPv6

- Alhálózatok tervezése
- Változó hosszúságú maszkok

- CIDR
- Címkiosztás, DHCP
- Címfordítás
- Datagram továbbítás

- Irányítási tábla
- ICMP
- Statikus irányítás
- Dinamikus irányítás

- Hierarchikus routing
- RIP
- OSPF
- BGP
- Broadcast, Multicast

MIRŐL VOLT EDDIG SZÓ?

- Az adatkapcsolati réteg szolgáltatásai
- Címzés az L2 rétegben
- Lokális hálózatok (LAN-ok)
- Ethernet

- Többszörös hozzáférés
- Vezetéknélküli LAN (WLAN)
- Fizikai réteg

- Cellás rendszerek
- 2G – GSM
- 2,5G – GPRS

- 3G – UMTS
- 4G – LTE

MIRŐL VOLT EDDIG SZÓ?

- Hálózati funkciók fejlődése
- Szoftveralapú hálózatok (SDN)
- Hálózati funkciók virtualizálása (NFV)

- Felhő alapú rendszerek
- Hálózatok adatközpontokban
- A dolgok Internete (IoT)

- Hálózatmenedzsment
- SNMP
- NETCONF, YANG

- Redundancia és hatékonyság – virtualizált összefogás és szétvágás

- Üzemeltetés - házirend
- Hibakeresés

HÁLÓZATI RENDSZEREK
ÉS SZOLGÁLTATÁSOK
TANSZÉK