Eloadasra jarassal (jegyzeteles nelkul), a slide-ok egyszeri elolvasasaval es az alabbi jegyzetbol keszulve osszehoztam 4-esre a vizsgat. Ettol fuggetlenul lehetnek benne hibak, konstruktiv visszajelzest szivesen fogadok, bla bla.

Sikeres vizsgazast!

1 Modellezes

- forras: 03-IRF-2009-modellezes
- modellezes: a rendszer absztrakt abrazolasa
- cel: komplexitas kezelese
- metamodell: modellezesi nyelv modellje
- kapcsolatok az egyes szintek kozott: tipusa/peldanya - metaszint, absztrakcio/konkretizacio - absztrakcios szint
- uml (csak a legalapvetobb jelolesek):
  - vonal es csillag a vegen: 1-n kapcsolat
  - ures landzsa: orokles
  - sima nyil: asszociacio (ha nem orokles akkor kell neki adni vmi nevet)

2 Folyamatmodellezes

- forras: 04-IRF-2009-folyamatkezeles
- workflow: cel erdekeben elkovetendo lepesek sorozata
- uml jelolesek
  - belepes: sotet kor
  - kilepes: lyukas kor
  - akcio: lekerekitett teglalap
  - dontes: rombusz
  - elagazas: |
  - teglalap: objektum
- soa: komplex alkalmazasok szolgaltatasokra bontasa, ezek kozott jol definialt interfesz, lazan csatolt architektura
- itil: information technology infrastructure library, best practices gyujtemeny, de nincs benne konkret megvalositasrol szo
- itil alteruletek: kapacitastervezes, rendelkezesreallas, incidenskezeles, problemakezeles, konfiguraciokezeles, valtozaskezeles, stb.
- itup: ibm tivoli unified process
- mof: microsoft operations framework
- gartner: it erettseg szintjei (0..4)
- mio: microsoft infrastructure optimization, technologiak menten lebontva az egyes szintek (pl desktopon mi kell az egyes szinteken)

3 Felhasznalo kezeles

- forras: 05-IRF-felhasznalokezeles
- biztonsag: egyre tobb problema: tervezes-implemenacio-uzemeltetes
- "leggyengebb lancszem"
- biztonsag fogalma: sertetlenseg (integrity), bizalmassag (confidentality), rendelkezesre allas (availability)
- hitelesites (authentikacio, igazolom, hogy en vagyok pisti) vs engedelyezes (authorizacio, mit csinalhat pisti)
- biztonsagi entitasok windows alatt: principal, belole user/group/machine (usernek <gep sid>-<rid> a sidje)
- azonositas: windows alatt ntlm v kerberos
- bash, powershell

4 Cimtarak

- forras: 06-IRF-cimtarak
- kozos adatter, innen tud hitelesiteni majd a webserver, vpn, ssh, stb.
- dns, nis, ldap, ad
- ldap: lightweight directory access protocol
- ldap sema → cimtar tartalom, hierarchikus
- muveletek: bind, search, update; lekerdezheto a sema is
- rdn: megmondja, hogy melyik attributum az ~ elsodleges kulcs
- gyokernel az rdn altalaban a dn, a tobbinel a cn, igy dn,cn parral egyedileg azonosithato mindenki
- az objectClass referencia mondja meg h az object melyik class peldanya
- az objectClass az egy lista! (eredmeny az attributumok unioja)
- ad: active directory, ldapon alapulo nemszabvanyos megoldas
- ds* parancs kezeli vagy powershell vagy gui

5 Engedelyezes (authorizacio)

- forras: 07-IRF-engedelyezes
- hozzaferesi matrix
- torveny: jogosultsagok szetvalasztasa, naplozas
- jogosultsagkezeles:
  - kotelezoseg: kotelezo ha kozponti jogosultsagellenorzes, belatas szerint ha tovabb lehet osztani a jogokat
  - szint: rendszer szint, eroforras szint (?)
  - fajta: ingegritas szintek (no read up, no write down - vagy forditva :P), hozzaferesi listak (acl, rbac)
- xacml (xml + acl)
- linux: bla bla, orokles csak diren exec hianya oroklodik lefele

- windows:
  - mandatory integrity control: no write up, ie hasznalja pl
  - rendszerszintu jogosultsagok: privilege (gep elallitas, driver telepites, stb) es accountright (ki lephet be, honnan lephet be, stb)
  - dacl: discretionary acl, objektumokra. owner akkor is valtoztathat rajta ha nem lenne egyebkent joga. egyebkent engedelyek unioja, de tiltasnak nagyobb prioritasa van
- group policy: gepre es felhasznalora is

6 Azonossagkezeles:

- forras: 08-IRF-identity-management
- cel: ne legyenek elfelejtett felhasznalok, ne kelljen mindent ldapbol authentikalni → lehet masolat, csak legyen rendesen szinkronizalva
- a cel rendszeren lehetnek "arva" fiokok, csak ez legyen elore megadva, es akkor normalis (pl windows everyone, stb.)
- itim: ibm tivoly identity manager. adatokat ldapban es rdbmsben is tarol.

7 Konfiguraciokezeles

- forras: 09-IRF-konfiguraciokezeles-alapok, 10-IRF-2009-konfiguraciokezeles_windows
- alapok
  - cmdb tartalma: license-ek, halozati topologia, szolgaltatasok vs eroforrasok, stb.
  - cmdb egy adatbazis, modell kell hozza, ez lesz a cim (common information model)
  - oo modell: peldanyositas (useradd), metodushivas (gep restart), stb.
  - cimom: cim object manager, modelleket kezel .mofban
  - wbem: web based enterprise managenent, (tobbek kozott) cimet hasznalja, eszkoz ra windowson: wbemtest.exe. nem konkret protokoll, az majd a cim-xml meg a ws-management lesz.
  - cim-xml: http felett, definialja a cim query language-t is
  - wbem(cim-xml) tamogatas sok helyen: openpegasus (rhel, vmware, stb), openwbem (sles), pywbem, stb
  - sblim: stanrads based linux instrumentation, ennek kereteben keszult: cim provider rpmhez, perlhez, "cim java api", stb
  - small footprint cim broker, egy cimom beagyazott rendszerekhez
  - linuxos cmdline tool: wbemcli
  - cmpi: common manageability programming interface, szabvanyos cimom provider interface. van benne peldany szolgaltato, metodus szolgaltato, stb
- windowson
  - wmi
  - cmdline tool: wmic
  - hozza wql: wmi wmi query language
  - ws-management: web services for management, ez se csak cimre jo...
  - muveletek: discover, get, put, create, delete, subscribe, execute
  - az egesz https es soap felett
  - implementacio: winrm, openwsman (cim-xmlbol fordit)
  - winrm tudja a wmit meg annal is tobbet, vista ota (hogy ne kelljen dcommal szenvedni)
  - winrm nevu cmdline tool, winrs (windows remote shell)

8 Konfiguraciokezelo adatbazisok (CMDB)

- forras: 11-IRF-2009-CMDB
- motivacio: hogy lassuk h pl hdd ledoglese mit erint, $foo szabvanynak megfelelunk-e
- cmdb: tarolja a teljes infrastrukturat
- termelo-fogyaszto: szabvanyos interfeszen tolnak bele (szenzorok) / vesznek ki belole adatokat
- felderites: agens alapu v megbizoleveles (besshzunk)
- vagy megbizolevel-mentes: nmap, ping, stb (lehet aktiv v passziv, pl wireshark)
- itil cmd: relevans infok elemekrol (ci, configuration item) es a koztuk levo kapcsolatokrol
- nagyvallalai cmdbk:
  - foderacio: nem egy db, hanem sok, es kulso kulcsok
  - osszeegyeztetes: kulonbozo dbkben levo ci-ket felismerni ha azonosak
  - szinkronizacio: eleg legyen egy helyen megvaltoztatni a user uj lakcimet
  - vizualizacio es lekepezes: lehessen reportot generalni + szurni
- cmdb resze a ci-k modellje is!
- cmdbf: ipari szabvany cmdb-k kozt
- ibm taddm (tivoli application dependency discovery manager): cmdb ibm modra
- automatikus felderitas: ping, os, portscan, server-specifikus lekerdezesek

9 Rendszermonitorozas

- forras: 12-IRF-rendszermonitorozas
- hogy ne akkor vegyuk eszre h gaz van ha szolnak a juzerek
- preventiv jelleg! :)
- szeretnenk kepet kapni a rendszer teljesitmenyerol, kihasznaltsagarol
- adatgyujtes + megjelenites + riasztas ha kell + historikus tarolas
- aganes: figyel + esetleg ertesit + egyszeru beavatkozasok
- vagy kulon process vagy builtin support
- pull/push modell. pull mint munin, pushnal az agens kezdemenyez
- szabanyok: snmp, syslog, jmx (jvm-ek monitorozasara), wbem
- szondazas (active proving): nincs kulon agens, csak userkent teszteljuk a szolgaltatast (pl monit). de itt is kell agens ha adott helyrol akarunk tesztelni.
- snmp: szabvanyos mib, agens a mib-et implementalja (mar amit..)
- kiterjesztheto, de nem kerdezheto le h milyen kiterjeszteseket hasznal a device
- muveletek: get, set, trap (ertesites feltetel teljesulese eseten async uzenetkuldessel adott ipre)
- mib es cim hasonlo, de mib kevesebbet tud, igy nem cmdb
- snmp vs wbem: binaris vs xml, configolni ne szokas snmpvel (pedig lehetne)

- gyakorlatban: peldaul mrtg, bix hasznalja
- historikus adatgyujtes: csak az "erdekes" reszeket taroljuk, az unalmas idoszakokban aggregalunk. (min/max/avg ertekek)
- munin: monitoroz, mrtghez hasonloan rrdtool oldja meg a historikus adatgyujtest, nagiossal kombinalva tud riasztani, max 50 gepig kenyelmes

10 Esemenykezeles

- forras: 14-IRF-2009-esemenykezeles
- cel: mert ertekekben a **valtozast** eszrevenni
- naplozas != esemenykezeles
- hibaok (fault), ebbol hibas allapot (error), es emiatt a user lat egy hibahatast (failure)
- windows event log, cmdline tool: wevtutil.exe
- syslogd: "pri header msg", ahol pri = 8*facility+severity
- itil: event management
- feldolgozas: szures, tovabbitas, lassitas (100% cpu fel percig nem erdekes), diplikatumok keresese
- elevules
- korrelacio: 2 esemenynek lehet u.az az oka
- ibm tivoli netcool / omnibus: probe-ok + hozza egy inmemory rdbms ami alerteket tarol

11 Szolgaltatasi szintek

- forras: 15-IRF-2009-szolgaltatasi-szintek
- szolgaltatas: onallo entitas, adminisztralni kell
- it metrikak: amit merni tudunk
- gqm: goal-question-metric
  - pelda: online erzet, mennyit kell varnia a usernek az oldalmegjelenesre, ehhez letoltesi/renderelesi ido
- sla: mit vallalunk, ezek definialva, es ezekre fix ertekek, meres mertekenek definicioja, sla-sertes kovetkezmenyei, ki mer, problemak jelentesenek folyamata

12 Virtualizacio

- bevezeto
  - forras: 16-IRF-virtualizacio-bevezeto
  - fogalma: eroforrasok elvonatkoztatasa az eroforrast nyujto elemektol
  - fajtai(5): platform (teljes gepet emulalunk), container/jaim (openvz), alkalmazas virtualizacio (fakeroot), futtatokornyezet (jvm, .net), desktop virtualizacio (rdp)
  - platform ket fajta: bare-metal (virtualizacios reteg+mgmt os;xen) vagy hosted (normal osbe epul bele a virtualizacios cucc;kvm)

  - plat. virt. def.: azonossag (u.az legyen a programok futasi eredmenye), biztonsagossag (igazi hw-t vmm - virtual machine monitor - kezeli), hatekonysag (utasitasok nagyresze modositas nelkul fusson)
  - lehet szoftveres v hardware-es virt: hw eseten mar nem lehet optimalizalni
  - paravirt: mikor a guest tud rola h virt. gepben fut, pl uml
  - trap and emulate: hogy raengedhessuk a cpura az olyan kodot amiben bizonyos utasitasokat nem engedunk lefutni
- szerver virtualizacio
  - forras: 17-IRF-virtualizacio-gyakorlat-szervervirtualizacio
  - memoriakezelesnel is a szokasos 3 eset: sw, hw es paravirt megoldasok shadow page table kezelesere
  - paravirt trukk: balooning driver
  - copy-on-write: irhatonak mutatjuk es ha vhova irni akar akkor elotte elmentjuk az eredeti adatot
  - openvz: vpseknel jo, tobb mint a chroot (pl process lista), de meg mindig kozos kernel
- virtualizacio managementje:
  - forras: 18-IRF-Virtualizacio-menedzsmentje
  - ez nemnagyon kell...

13 Incidens-, problema- es valtozaskezeles

- forras: 20-IRF-2009-Incidens_menedzsment
- service desk: ide lehet fordulnia a felhasznalonak. ticketeket nyitnak, lezarnak, torolnek, stb
- incidens: nem tervezett leallas/hiba/anomalia szolgaltatasban, formalizalt kezeles kell ra
- alfolyamatai: bejon, logoljuk, kategoriazalas, proirizalas, diagnozis, eszkalaljuk (opcionalis), megoldjuk, lezarjuk
- prioritas = surgosseg * hatas
- problema: az incidens oka.
- valtozaskezeles: valtozasok eletciklusat kezeli, hogy legyen ra terv (igy cmdb syncben lesz, hatekony eroforraskihasznalas, bla bla)

14 Kiadas es telepiteskezeles

- forras: 21-IRF-2009-kiadas-es-telepites
- release: hw, sw, doksi, folyamatok egyutt ami implemental egy rfc-t
- dsl: definitive sofrware library, ami ebben van azt lehet telepiteni
- linux: rpm, windows: msi
- msi workflow: fejlesztes, msi, msi testreszabasa, group policy, telepul
- wsus: windows server update services

15 Szolgaltatasbiztonsag

- forras: 22-irf-szolgaltatasbiztonsag
- sil: safety ingegrity level: 10 ^ -9en csak azt jelenti h x berendezesbol 15 evig csak 1 hibasodik meg, nem tobb1000 evet..
- szolgaltatasbiztonsag def: a kepesseg, hogy igazoltan bizni lehet egy szolgaltatasban (igazoltan: elemzesen, meresen alapul. bizni: kielegiteni az igenyeket)
- jellemzoi: rendelkezesreallas, megbizhatosag, biztonsagossag, bizalmassag, integritas, karbantarthatosag
- befolyasolo tenyezok hataslanca: fault (kivalto ok) → error (rendszerallapot) → failure (specifikacio megsertese)
- meghibasodasok kategoriai:
  - hw hibak
  - sw hibak
  - emberi hiba (rendszergazda, felhasznaloi artalmatlan/artalmas hiba)
  - kornyezeti hatas, pl termeszeti katasztrofa
- szolgaltatasbiztonsag eszkozei
  - hibamegelozes (tervezes)
  - hibamegszuntetes (teszteles)
  - hibatures. rendundancia tipusa: hideg (ott a polcon kikapcsolva) / langyos (be van kapcsolva csak mast csinal) / meleg tartalek (teljes duplazas)
- analizis modszerek
  - tablazat (fmea, failure mode and effect analysis)
  - hibafa: digites AND es OR kapukbol, elemi hibak korok

16 Furtozes es replikacio

- forras: 23-IRF-2009-furtozes-es-replikacio
- redundancia akkor erdemes altalaban ha 99%nal jobb rendelkezesreallast akarunk
- cluster: tobb gep virtualis kiszolgalokent jelenik meg a userek fele
- fajtai: hpc (grid, parhuzamositott), terheleseloszto, ha
- terheleseloszto:
  - alkalmazas vagy tud vagy nem tud rola
  - lehet vmi kozpont (pl szotar) vagy lehet teljesen elosztott (utobbira pelda az rr dns, vagy microsoft nlb - network load balancing - ahol a clusternek van kulon ipje)
  - session megorzese celjabol mindig u.az a node kell kiszolgalja az adott usert
- ha (feladatatveteli, omg)
  - vagy van kozos storage vagy nincs
  - felmerulo problemak (amnezia, csoportkep, stb)
- replikacio
  - szinkronizacio lehet pull vagy push
  - primary/secondary, pl bind: zero data loss (de lassabb) vagy async (de lehet adatvesztes)
  - multimaster (komplexebb, active directory tud ilyet)

17 Mentes es archivalas

- forras: 24-IRF-Backup-archivalas
- adat tobbet er mint az adathordozo
- raid: altalaban csak serveren (kerdes h mennyi ideig allhat egy szolgaltatas - a gep ne erdekes)
- backup hibaturest noveli, archivalas viszont arra megy ki, h a nemhasznalt de megorzendo adatokat biztonsagosan tarolja
- drbd: distributed redundant block device
- backup tipusok:
  - normal (torli az archive bitet)
  - copy (ro)
  - incremental
  - differential (ro incremental)
  - daily (adott napon modusult file-okat)
- data deduplication: "rossz redundancia", tehat nem tomorites, siman csak sok azonos tartalmu nagy file esetere, pl. dirvish
- mit: filerendszer, de neha kell app szintu support is hozza
- snapshot != backup, csak egy tamogato technologia backuphoz, mivel a masolas nem atomi muvelet
- virtualizacioval mindent tudunk menteni, app-level support se kell
- data destroy