Virtualios infrastruktūros sauga

VI priežiūros ir eksploatavimo (operation) sauga

Diegimas ir valdymas

Kasdieninė veikla administruojant virtualią infrastruktūrą bendrąją prasme siejama su tam tikromis saugumo grėsmėmis. Tam tikrų darbų **greitesniam ir patogesniam** atlikimui, gali būti mažinami saugos reikalavimai. Tai aktualus klausimas kasdieninei veiklai atlikti.

Saugumo grėsmės bus nagrinėjamas atsižvelgiant į:

- Monitoringo sistemų teisingą konifgūravimą
  - Prieigos ribojimai prie fizinių mašinų
  - Prieigos ribojimai prie VM
  - Prieigos ribojimai prie duomenų saugyklų atskirų LUN
- VM administravimą.
- Rezervinio kopijavimo sistemų administravimą.

Monitoringas

Mašinos būsenos monitoringas

Kiekviena IT infrastruktūra privalo būti stebima. Paprastai tuo užsiima NOC (Network Operation Center).

Monitoringo sistemos dažniausiai veikia per agentus (kliento-serverio modelis), kurie instaliuojami į stebimą serverį (VM ar fizinį).

Fizinės mašinos monitoringas tikslai:

- Ar fizinė mašina atsako į tinklo užklausas (tinklo monitoringas)
- Aparatūrinių gedimų aptikimas (pvz. naudojant gamintojų agentais ir monitoringo sistemą – HP SMH)
- Serverio ir VM konfigūracijos pakeitimų stebėsena

SNMP

Bet kuri didesnė tinklo infrastruktūra turi būti valdoma ir dažniausiai centralizuotai. Valdymui atlikti būtina surinkti informaciją iš tinklo įrenginių ir priklausomai nuo jų būsenos atlikti atitinkamus sprendimus.

SNMP (Simple Network Management Protocol) skirtas tinkle veikiantiems įrenginiams stebėti ir valdyti. SNMP protokolas veikia TCP/IP ir IPX/SPX tinkluose. (161,162 (trap) portai)

Specifikacijos pateiktos RFC 3411 – 3418.

Informacija apie irenginius saugoma **MIB** (Management Information Base).

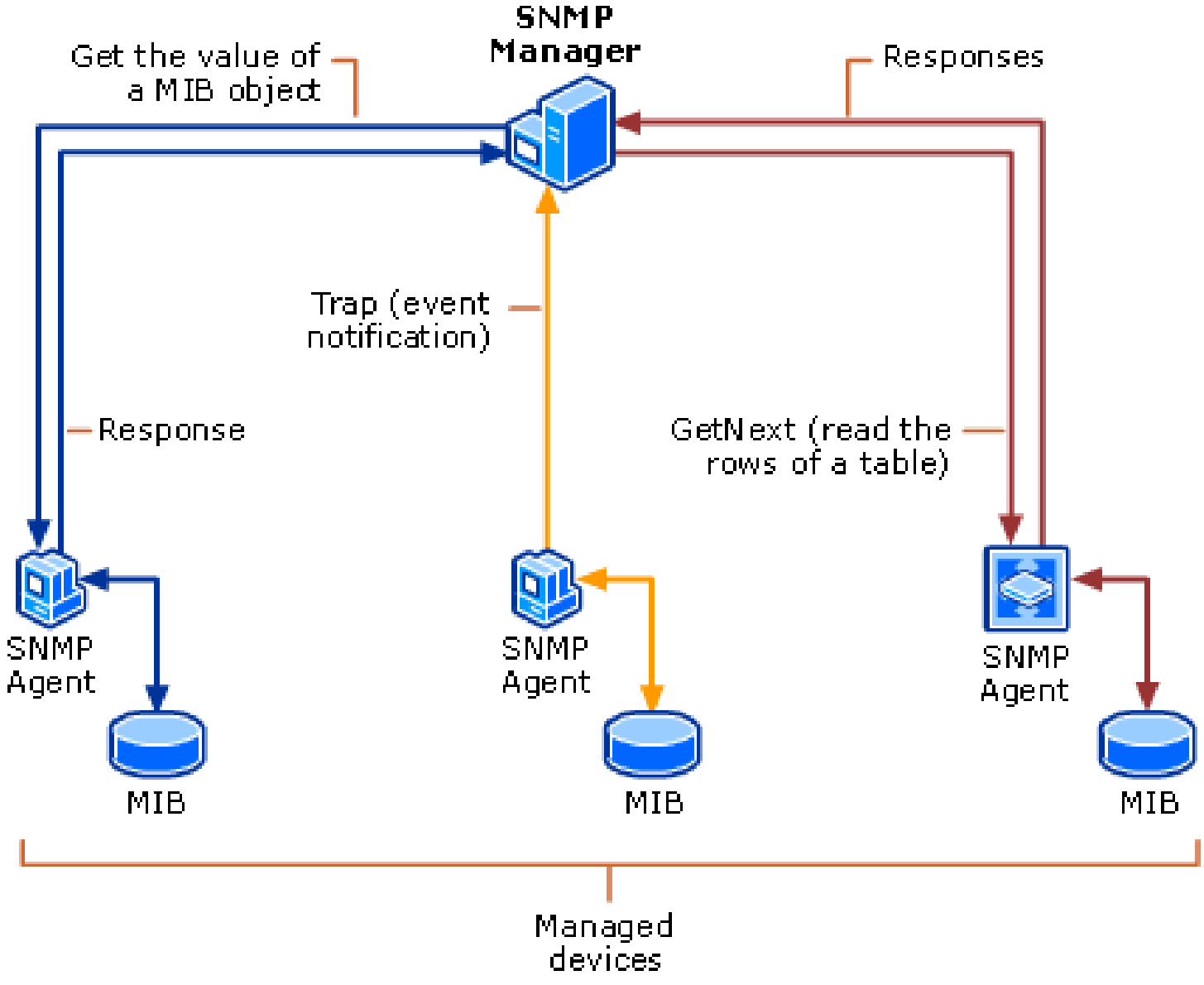
MIB modeliai ir SNMP naudoja ASN.1 notacijų kalbą.

SNMP

Tinklo valdymo struktūra, sudaryta SNMP pagrindu, susideda iš:

- **SNMP agento**. SNMP agentas atsako į valdytojo SNMP užklausas. SNMP agentas tvarko ir prižiūri kompiuterio MIB
- **SNMP valdytojo** (manager). SNMP valdytojas surenka valdymo informacija iš SNMP agentų ir ją apdoroja.
- **MIB** (*Management Information Base*). Egzistuoja keletas MIB modelių: MIB-I, MIB-II, RMON, RMON2) Per MIB pateikiami agentų prižiūrimi duomenų objektai. MIB naudoja ASN.1 notacijas.

SNMP


SNMP
Manager
Get the value of
a MIB object
Responses
Trap (event
notification)
Response
GetNext (read the
rows of a table)
SNMP
Agent
SNMP
Agent
SNMP
Agent
MIB
MIB
MIB
Managed
devices

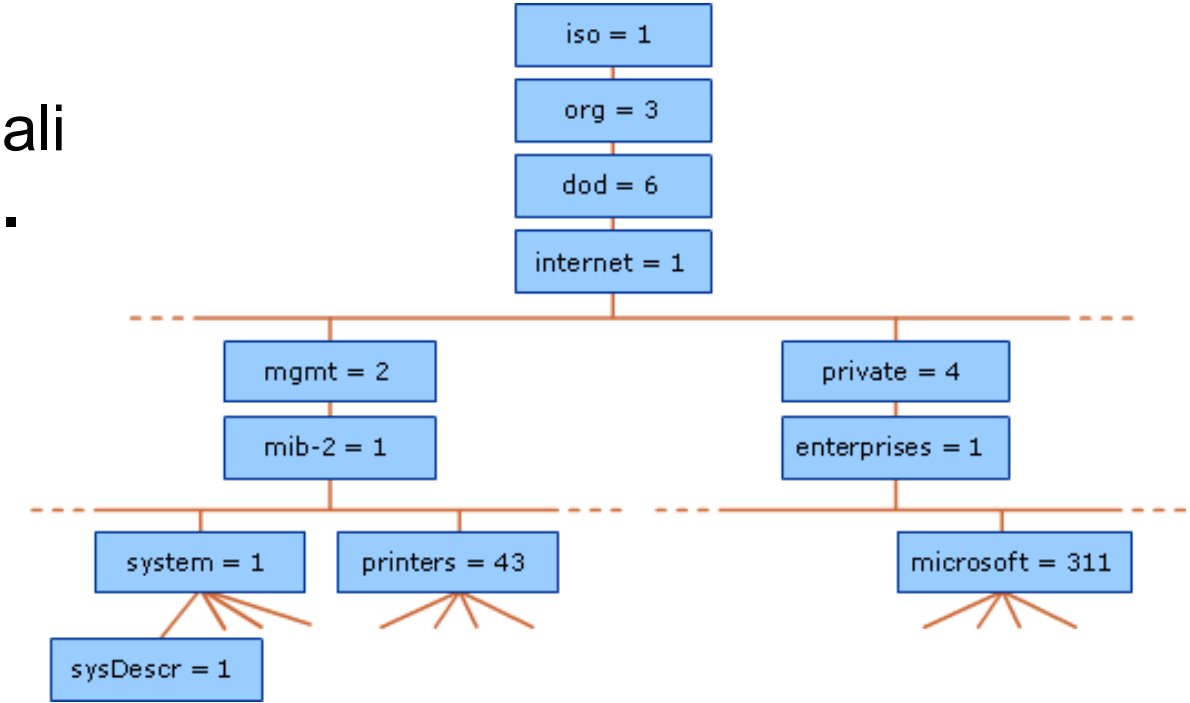
SNMP MIB

MIB apibrėžia stebimo mazgo valdomų duomenų struktūrą.

Duomenys saugomi medžio tipo duomenų bazėje, kurioje apibrėžti tam tikri **objektų identifikatoriai** (OID).

Stebimi objektai: OS versija, IP adresas, sąsaja, HDD laisvos vietos dydis, atidarytų failų skaičius.

Kiekvienas OID apibrėžia kintamąjį, kurio reikšmė gali būti nuskaityta per SNMP.



Monitoringas

SNMP – tai atviru tekstu veikiantis 7 lygmens protokolas, todėl reiktų naudoti SNMP v3, kuri palaiko šifravimą.

VMware ESXi konfigūravimas norint prijungti serverį prie bendruomenės (community) ir prie monitoringo sistemos (pvz. naudoti vCLI):

```
vicfg-snmp.pl --server host.example.com --username user --password password -c public
```

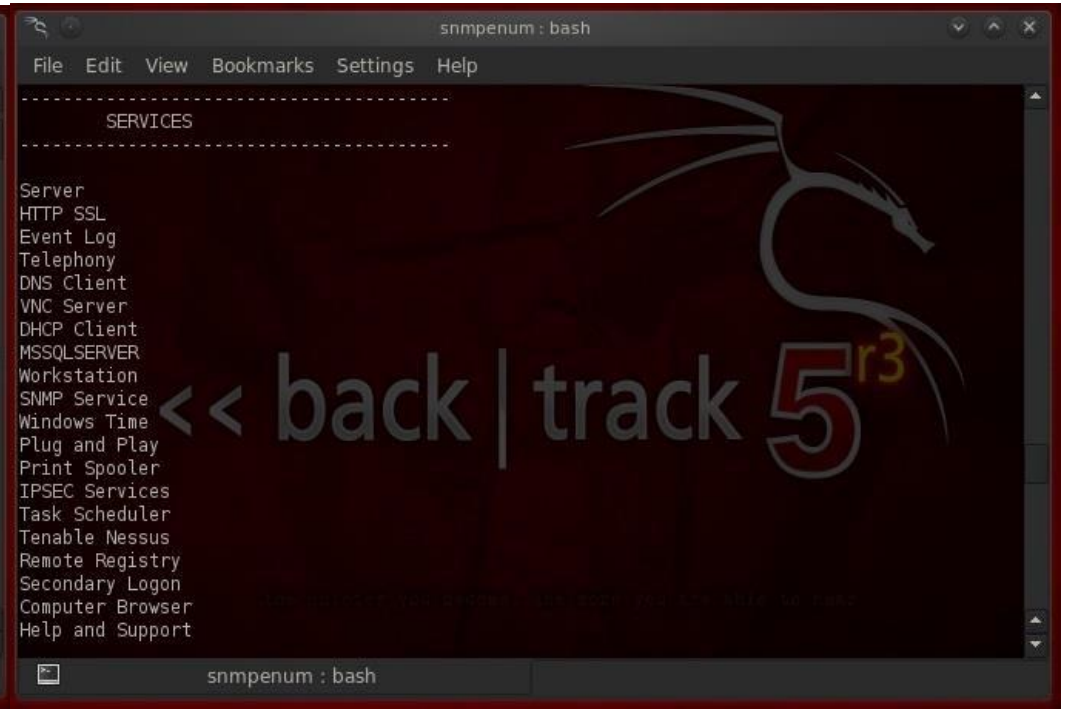
```
vicfg-snmp.pl --server host.example.com --username user --password password -t target.example.com@162/public
```

SNMP v1 hack

Naudojamas BackTrack Linux tools **snmpenum**

Komanda (laikome, kad community *public*)

./snmpenum.pl *IP_adresas* public windows.txt



Monitoringas

ESXi v.5.0 palaiko tik SNMP v1 ir v2, todėl reikia riboti prieigą prie ESXi per 161 ir 162 portus tik SNMP valdymo serveriui: (Configuration -> Security Profile ->Firewall).

ESXi v.5.5 ir vėlesnės versijos palaiko SNMP v3.

Kiekvienas SNMP v3 agentas turi „engine ID“ kuris laikomas kaip unikalus agento identifikatorius. Nustatymas atliekamas:

```
esxcli system snmp set --engineid id
```

id – tai simboliu seka (5-32 simbolių)

Monitoringas

SNMP v3 taip pat laiko autentifikacijos ir šifravimo protokolus. Tai leidžia identifikuoti vartotojus ir šifruoti SNMP pranešimus (užtikrinti duomenų konfidencialumą).

Autentifikacijai:

```
esxcli system snmp set --authentication protocol
```

protocol reikšmės none, SHA1 arba MD5.

Šifravimui:

```
esxcli system snmp set --privacy protocol
```

protocol reikšmės: none, AES128.

Monitoringas

SNMP v3 leidžia apibrėžti vartotojus, kuriems leidžiama naudotis agento teikiama informacija. Vartotojo duomenys sugeneruojami:

```
esxcli system snmp hash --auth-hash authsecret
--priv-hash privsecret --raw-secret
```

Rezultatas:

Authhash: 08248c6eb8b333e75a29ca0af06b224faa7d22d6

Privhash: 232ba5cbe8c55b8f979455d3c9ca8b48812adb97

Monitoringas

SNMP v3 vartotojo sukūrimas:

```
esxcli system snmp set –users
userid/authhash/privhash/security
```

```
esxcli system snmp set --users
user1/08248c6eb8b333e75a29ca0af06b224faa7d22d6/
232ba5cbe8c55b8f979455d3c9ca8b48812adb97/priv
```

SNMP v3 trap konfigūruojamas panašiai, kaip ir ankstesnėse SNMP versijose, tik skirtumas tame, kad galime panaudoti vartotojų autorizaciją ir šifravimą.

Monitoringas

Monitoringo agentai ESXi serveryje gali veikti per Vmware API ir SDK, todėl rekomenduojama naudoti SSL kanalą saugumui užtikrinti.

Naudojant atviro kodo monitoringo sistemas (pvz. Nagios, Munin) reikia taip pat naudoti SSL kanalą ir riboti prieigą prie SNMP portų tik atskiriems serveriams.

Našumo monitoringas

Našumo monitoringo sistemos taip pat gali įtakoti virtualios infrastruktūros saugumą. Rekomenduojama riboti prieigą prie serverių ir tinklų tik monitoringo sistemoms.

Konfigūracijos keitimai

Konfigūracijos pakeitimų monitoringas

Pakeitimų monitoringas privalo būti atliekamas siekiant išvengti problemų ir nesusipratimų ateityje.

Tikslas - žinoti, kas, kada ir ką pakeitė konfigūracijoje.

Galima naudoti specifinius įrankius iš Tripwire ir ConfigureSoft.

Pakeitimų monitoringas gali būti kaip vienas iš procesų Pakeitimų valdyme (ITIL, COBIT ir t.t.). Rekomenduojama turėti dokumentuotą konfigūraciją ir ją nuolat tvarkyti. Galima naudoti pvz. Veeam Reporter įrankį.

VM administravimas

Būtina atskirti administratorių roles ir privilegijas. Turi būti taikomas RBAC metodas.

VM administratorius – tai rolė apibrėžta VC.

VM administratoriaus pareigos:

- OS ir programų priežiūra
- Atnaujinimų priežiūra

Prieigos prie VM būdai:

- Nuotolinis prisijungimas: RDP, VNC, SSH, vSphere client.
- Prisijungimas prie konsolės: webAccess, VIC

VM administravimas

Rekomendacijos:

- VM administratoriui iš esmės nebūtinas prisijungimas prie virtualios infrastruktūros
- Prisijungimas prie VNC serverio turėtų būti atliekamas per SSH gateway, nes naudojamas stipresnis šifravimas, nei DES algoritmas naudojamas VNC.
- Naudojant VNC reikia žinoti kuriame ESXi serveryje yra VM, kas leidžia VM administratoriui žinoti apie VI konfigūraciją.
- VNC reikalauja unikalaus porto numerio kiekvienam VM, todėl tai gali sukelti sumaištį.
- Priega per konsolę, reikalauja prieigos prie VM tinklo, kas sukelia grėsmes dėl tinklo infrastruktūros.

VM „griūtis“

VM nugriuvus dėl kažkokių priežasčių yra tokios galimybės atlikti tyrimą:

- Nagrinėti VM žurnalinius (*log*) failus ESX serveryje

  `/vmfs/volumes/.../VM_name/vmware.log`

  `/var/log/vmkernel`

- Nagrinėti VM operacinės sistemos žurnalinius (*log*) failus.

Pastaba:

VM griuvimas (blue screen) dažniausiais nesusiję su virtualizacijos sluoksniu t.y. virtualia aparatūrine dalimi.

Didžiausią įtarimą dėl griuvimo turi kelti galimi virusai, kirminai ir t.t.

Kodėl reikia daryti rezervines kopijas?

Fizinio saugumo grėsmės:

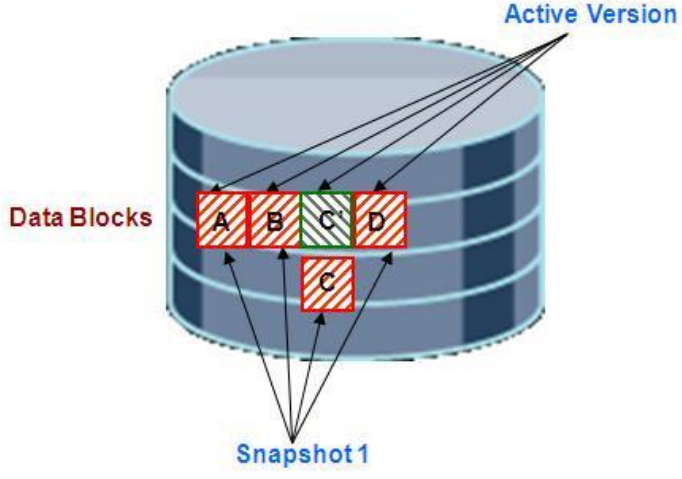
- Fizinio įrenginio gedimas
- Kenksmingas programinis kodas (virusai, kirminai ir t.t)
- Ištrinti, sugadinti failai ir katalogai
- Duomenų vagystės
- Žmogiškos klaidos kopijuojant, atstatant duomenis
- Gamtos stichijos

Backup administravimas

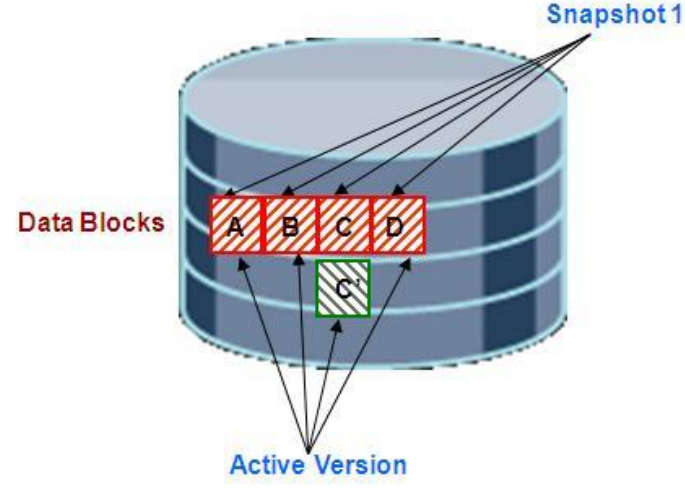
Rezervinių kopijų (backup) administratorius turi dideles teises t.y. prieiga prie VM tinklo, saugyklų tinklo, media serverio ir t.t.

VM rezervinių kopijų darymo procesas:

- Sukuriamas veikiančios VM snapshot, tuomet daroma vmdk rezervinė kopija ir užrašomi pakeitimai iš snapshot.



Copy-on-write snapshot

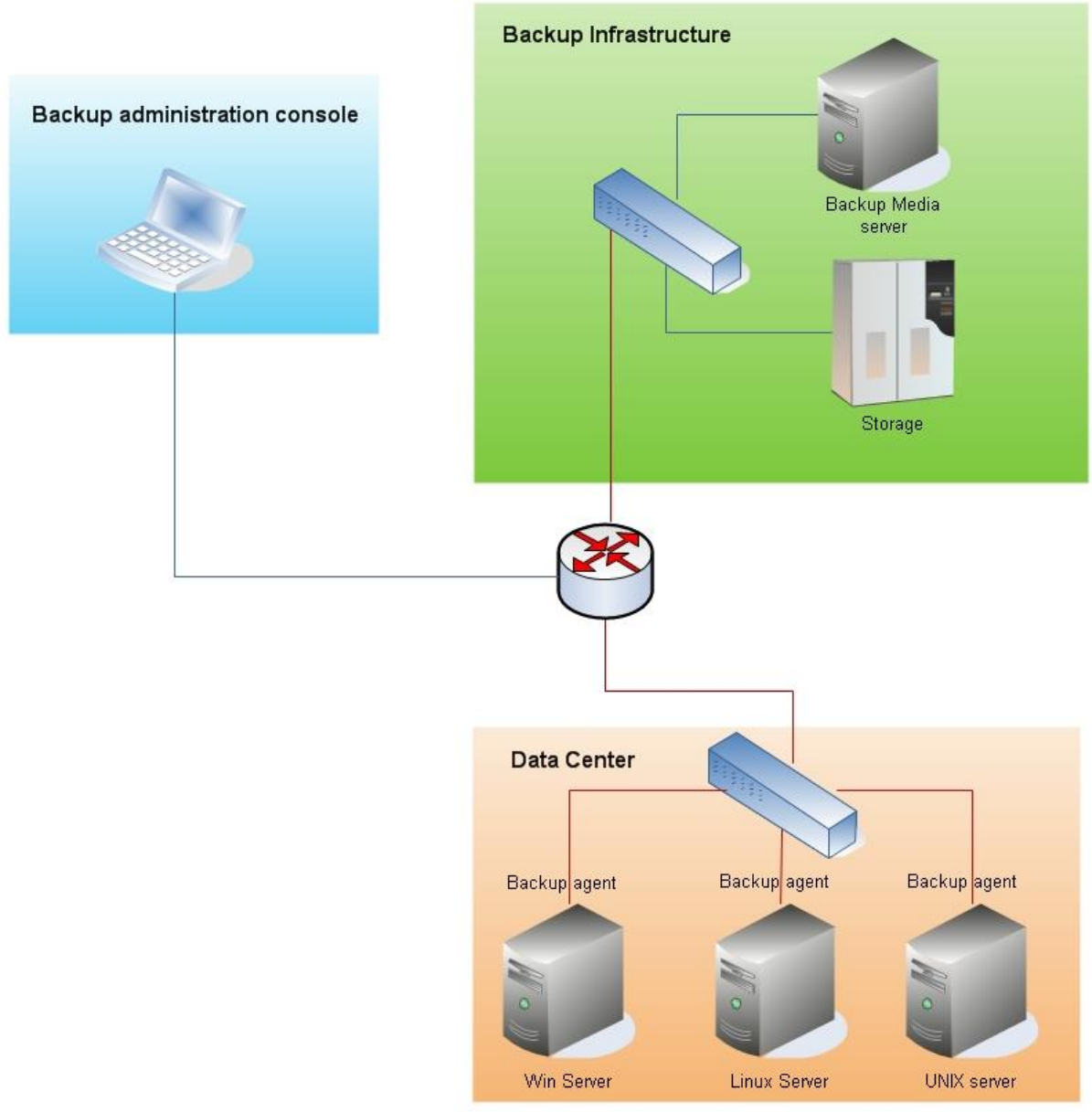


Redirect-on-write

Rezervinio kopijavimo architektūra

- Kopijavimui naudojama programinė įranga, kuri apima tokius procesus: planavimą, vykdymą, stebėjimą ir atstatymą.
- Rezervinio kopijavimo architektūra sudaryta naudojant kliento-serverio principą, kur serveris yra kopijų valdymo centras, o klientas sistema, kurios kopijos yra daromos.
- Duomenų bazių kopijavimo būdai:
  - Karštasis – kai kopijuojama veikianti DB
  - Šaltasis – kai prieš kopijavimą DB yra stabdoma ir tuomet daromos failų kopijos.

Rezervinio kopijavimo sistemos pavyzdys



Rezervinio duomenų kopijavimo politikos formavimas

Formuojant duomenų rezervinio kopijavimo politiką vertinami tokie kriterijai:

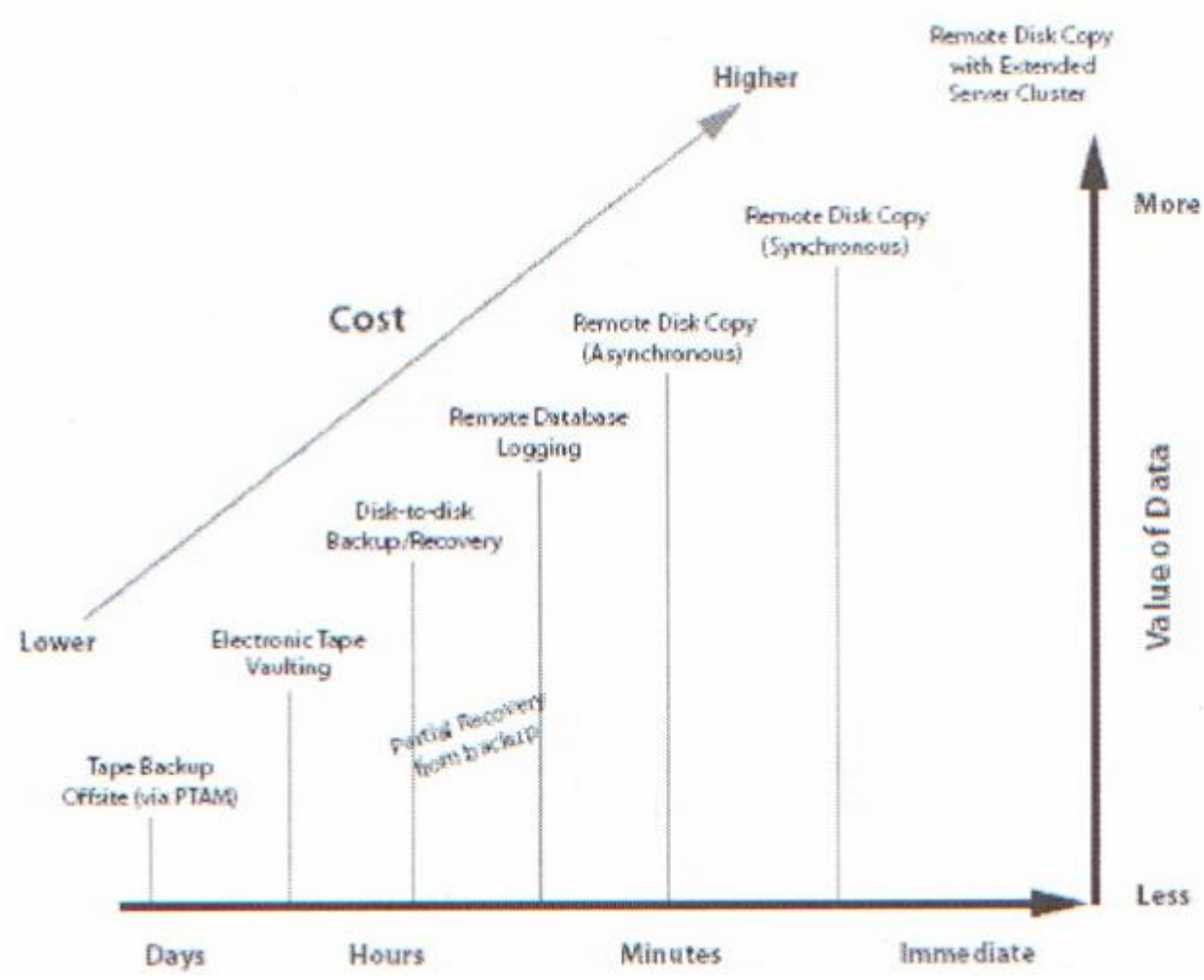
- Duomenų ir taikomųjų programų svarbumas
- Galimas duomenų praradimas (valandomis, paromis)
- Rezervinių kopijų saugojimo laikas (dienomis)
- Duomenų atstatymo iš kopijų trukmė (valandomis)
- Duomenų saugojimo vieta (diskų masyvai, magnetinės juostos)
- Duomenų suspaudimo lygis

RTO, RPO

- Svarbiausi rezervinio kopijavimo politikos rodikliai:
  - **atstatymo laikas** (Recovery Time Objective RTO)
  - **atstatymo taškas** (Recovery Point Objective RPO)
- **RTO** nurodo laiką, reikalingą veiklos funkcijų ar taikomųjų programų atstatymui.
- **RPO** nustato laiko tašką prieš nelaimingą įvykį iki kurio duomenys gali būti atstatyti.

Priklausomai nuo pasirinkto kopijavimo tipo egzistuoja darna tarp RTO, RPO ir sprendimo įgyvendinimo bei palaikymo kainos.

RTO ir RPO darna



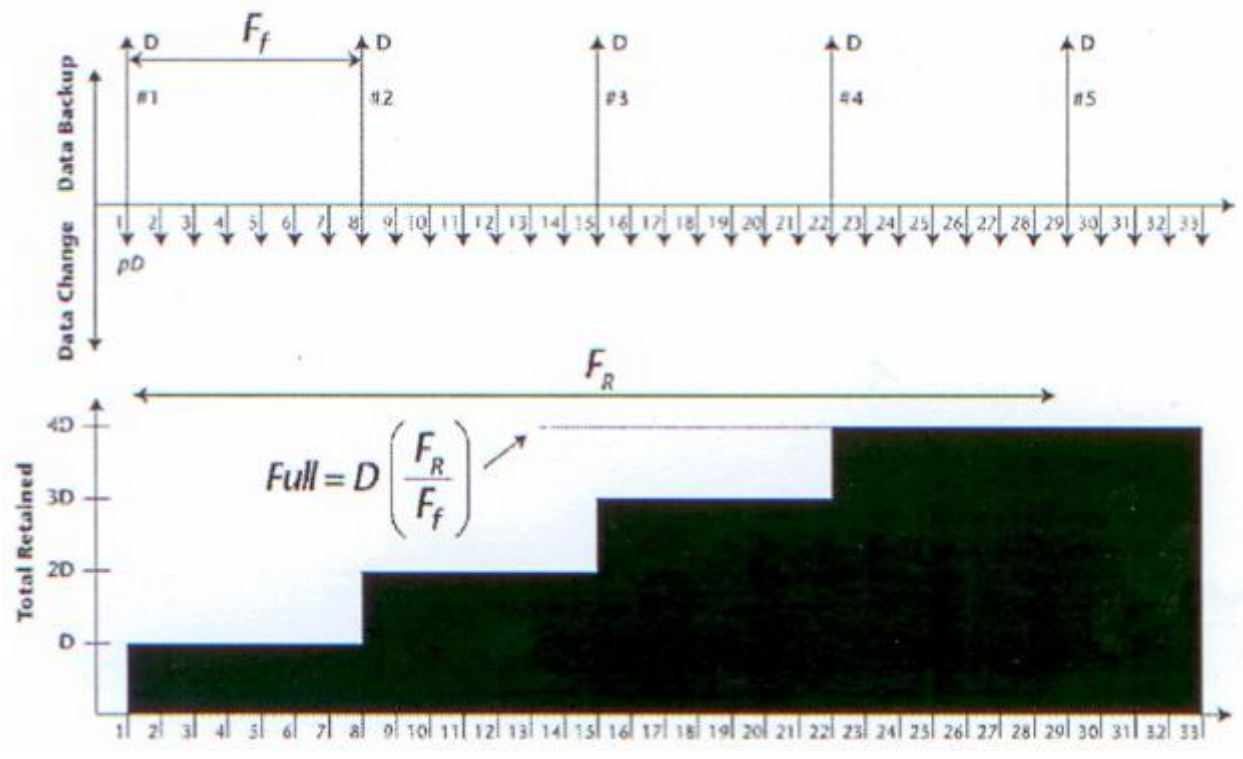
Duomenų kopijavimo modeliai

Pagal kopijuojamų duomenų ir kopijos santykį nustatomi tokie rezervinio duomenų kopijavimo modeliai:

- Pilnas (Full backup)
- Diferencinis augantis (differential-incremental backup)
- Akumuliuotas augantis (acumulative-incremental backup)

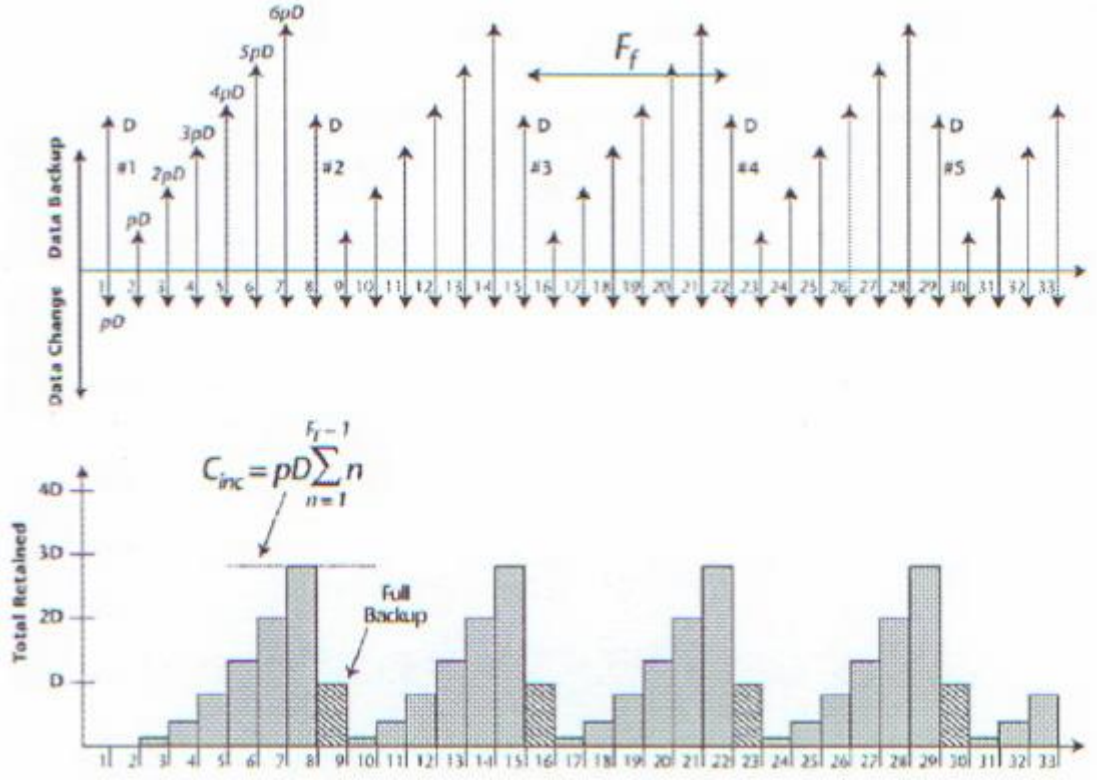
Pilnas duomenų kopijavimo modelis

- Pilno kopijavimo metu sukuriama kopija visiems pažymėtiems failams. Pav. parodyta, kad pilna kopija daroma kas 7 dienas ir atvaizduoti 4 kartai. Saugant tokį kopijų skaičių reikia 4D talpos saugyklos.



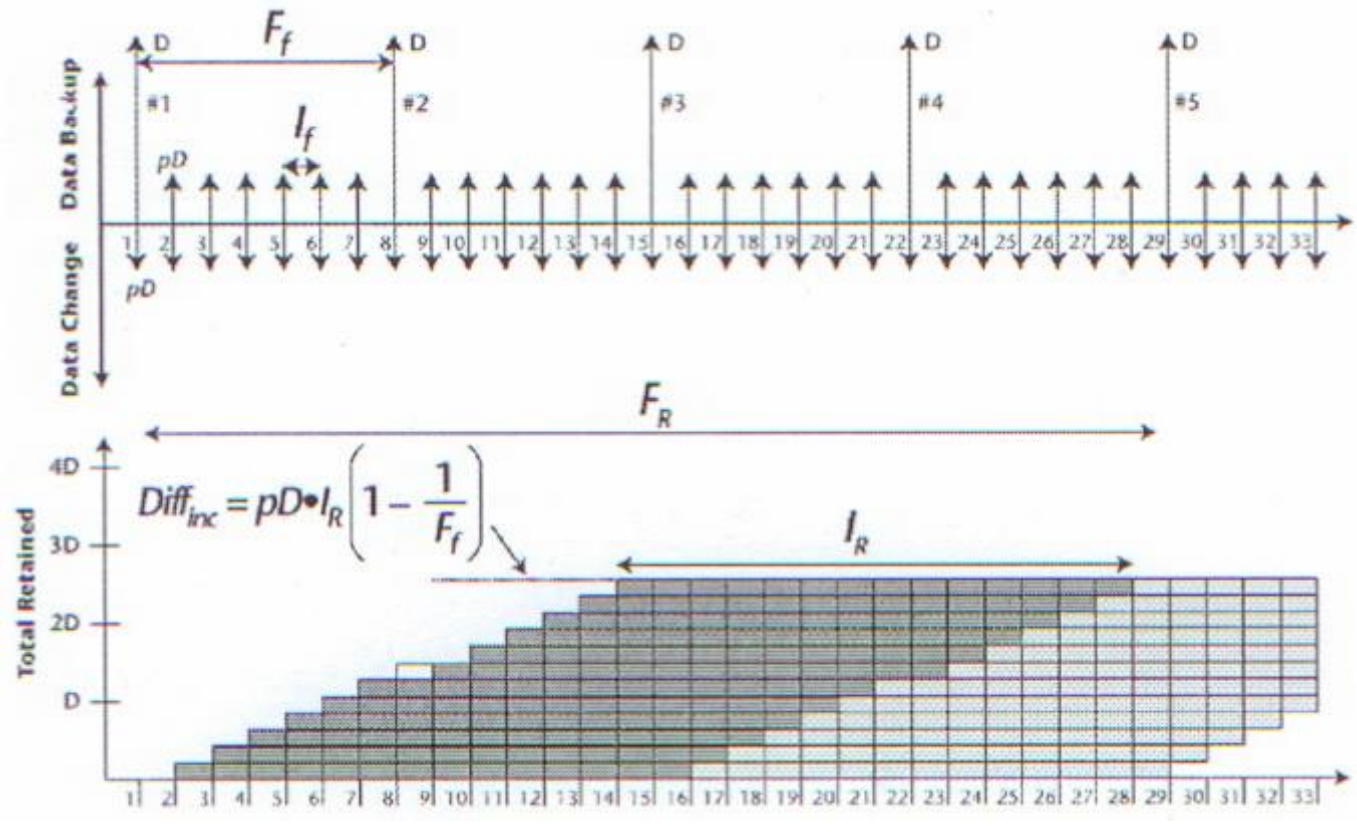
Diferencinis augantis kopijavimo modelis

Naudojant šį modelį kopijos daromos tik tiems failams, kurie buvo pakeisti nuo paskutinio pilnos duomenų kopijos. Naudojama, kai norime taupyti talpyklos vietą ir turėti tik paskutinę failo versijos kopiją.



Akumuliuotas augantis duomenų kopijavimo modelis

Naudojant šį modelį, rezervinės kopijos daromos tik tiems failams, kurie buvo pakeisti po bet kurio paskutinio rezervinio kopijavimo (pilno ar akumuliuoto).



Rezervinio kopijavimo įrenginiai

Rezervinės duomenų kopijos saugomos tokiose laikmenose:

- Magnetinėse juostose, juostų bibliotekose
- Diskuose, diskų masyvuose
- Optiniuose diskuose (CD, CD-RW, DVD, DVD+-RW)
- Trečiųjų šalių saugyklose

Backup administravimas

Rekomendacijos

- Backup įrankiuose (pvz. VCB, Veeam backup tool) naudojamus slaptažodžius saugoti šifruotus ir tik *read-only* teisėmis root vartotojui.
- Turi būti apibrėžta prieigos teisės atitinkamiems vartotojams prie kopijuojamų duomenų (pvz. backup administrator).
- Backup tinklas turi būti atskirtas nuo administravimo tinklo.
- Nepamiršti, kad snapshot tik disko ir jo spart.atminties atvaizdas, sudarytas iš nukopijuotos blokų adresų lentelės. Sugedus fiziškai diskui, atstatymas iš snapshot neįmanomas, todėl reikia daryti diskų rezervines kopijas taip pat.

3-2-1 taisyklė

Saugaus rezervinio kopijavimo taisyklė

- Turėti **3** svarbių failų kopijas (pirminė ir dvi rezervinės)
- Saugoti failų kopijas **2** skirtinguose įrenginiuose (HDD saugykla ir juostos), tam kad apsisaugoti nuo galimo įrenginio gedimo.
- Vieną kopiją laikyti fiziškai kitame duomenų centre.

Bendrieji saugos reikalavimai

- VI privalo turėti skirtingas saugumo zonas.
- Visos sistemos, naudojamas VI administravimui privalo būti viename tinkle.
- Prisijungimai prie šio tinklo turi būti stebimi monitoringo sistemomis.
- VI valdymo serveris vCenter, turi būti tame pačiame tinkle ir toje pačioje saugumo zonoje, kaip ir administravimui skirti serveriai.

Komandiniai skriptai

Kartais VI administratoriui reikia panaudoti skriptus, kurie būtų vykdomi visuose ESXi serveriuose (pvz. konfigūracijos keitimas, žurnalinių įrašų filtravimas ir t.t.)

Tokiems veiksmams atlikti reikalinga pateikti prisijungimo duomenis: vartotojo vardą ir slaptažodį.

Svarbu:

Negalima skriptuose įrašyti prisijungimo vardo ir slaptažodžių. Jie turi būti įvedami interaktyviai.

```
for x in esx1 esx2 esx3
do
   echo $x
   ssh admin@$x $*
done
```

Rolių ir teisių valdymas

Rolės ir vartotojų teisės turi būti tinkamai suprantamos ir valdomos.

- Teisės suteikiamos šakniniams objektams yra paveldimos objektams vaikams
- Suteikiant teises ESX serveriuose naudojamas principas – „*galima tik tas, kas apibrėžta, visa kita draudžiama*“
- Rolės ir jų teisės turėtų būti apibrėžiamos pagal įmonėje nustatytą saugos politiką.
- Rekomenduojama rolių ir teisių valdyme turėti patvirtinimo procesą, kuris leistų turėti aktualų sąrašą.

VM sauga

VM saugumo grėsmės kyla iš dviejų pusių:

- Hypervizoriaus (kaip virtualios aparatūros tiekėjo)
- VM OS

VM saugumas iš virtualios aparatūros pusės - tai konfigūraciniai failai hypervizoriuje. Nustatant juos būtina nagrinėti:

- Kaip bus prie VM pajungiami ir naudojami biometriniai įrenginiai, apsaugos raktai, flash drive ir kiti išoriniai įrenginiai
- Kaip pasiekiami saugyklos: per hypervizorių ar tiesiogiai per iSCSI, NFS ir t.t.?
- Kokia duomenų, saugojamų VM‘e praradimo rizika ir kaina?

Apsaugos raktai

Apsaugotos programos gali naudoti USB, COM arba LPT raktus.

Siekiant prijungti juos prie VM, galimi variantai:

- Prijungti prie hypervizoriaus serverio (problema su VM migravimu)
- Naudoti USB over IP įrenginius (panaikinama VM migravimo problema, tačiau iškyla klausimai:
  - kokiame tinkle turi būti įrenginys,
  - ar ugniasienė turi riboti prieigą prie to įrenginio,
  - ar bus naudojamas „broadcast‘as“ tinkle,
  - kas gali prisijungti prie šio įrenginio.

Biometriniai įrenginiai

Biometriniai įrenginiai suteikia papildomą saugumo lygį identifikuojant vartotoją.

Siekiant prijungti biometrinį išorinį įrenginį prie VM galimi sprendimai:

- Naudoti USB over IP įrenginius (žr. problemas anksčiau)
- Prijungti biometrinį įrenginį prie fizinės darbo vietos ir per RDP prijungti prie VM

Išoriniai įrenginiai

Prie virtualios mašinos gali būti prijungiami įvairūs išoriniai įrenginiai: HDD, FC įrenginiai, CD-ROM, IP saugyklos, IP įrenginiai.

Problemos:

- Jei pajungti prie hypervizoriaus serverio, problemos su migravimu.
- Visos išorinės laikmenos, patencialiai gali turėti kenkėjišką kodą, todėl patartina drausti prie VM prisijungti tokius įrenginius.
- Jei IP įrenginiai jungiami iš kitos saugumo zonos, galimos saugumo grėsmės.

VM testavimas

Naujos VM neturi būti testuojamos tame pačiame tinkle, resursų grupėje (pool), saugumo zonoje.

VM testavimui patartina prijungti mašiną prie atskiro vSwitch.

Nerekomenduojama leisti VM tiesiai jungtis prie tos pačios iSCSI ar NAS saugyklos, kaip kad naudoja hypervizorius.
Leidžiant VM tiesiogiai naudoti tas pačias saugyklas, gali būti prieinama prie vmkernel.

VM auditavimas

VM konfigūracijos auditavimui reikia naudoti trečių šalių įrankius: pvz. Tripwire arba Configuiresoft

VM snapshot‘ai turi būti daromi atitinkamai pagal nustatytą įmonės politiką. Jie neturi būti daromi kartu visoms VM, nes shapshot‘ai stipriai naudoja vCPU, dėl ko galima sukelti DoS.

Analogiška rekomendacija su VM antivirusinių programų skenavimo laiko nustatymu. Jis turi būti sukonfigūruotas taip, kad tai nevyktų vienu metu ir nesukeltų DoS reiškinio.