**Microsoft Hyper-V – virtualizacijos sistema, kurį skirta x64 sistemoms hypervizoro pagrindu. Hyper-V programos beta versija buvo integruotą į Windows Server 2008, o finalinė versija išleista balandžio 26 d. 2008 metais. Seniau programa buvo žinoma kaip *Windows Server Virtualization*.**

**Atskira nemokama programos versija Hyper-V, kurį gavo pavadinimą „Microsoft Hyper-V Server 2008“ buvo išleista lapkričio 1 d. 2008 m. Programa yra baziniu *Server Core* variantu *Windows Server 2008 –* apjungia visą funkcianoluma Hyper-V. Nemokama 64 bitų *Core* versiją Hyper-V apribota komandinės eilutės sąsaja, kur konfiguravimas operacinės sitemos, aparatinės bei programinės dalies atliekamas komandinės eilutės pagalba. Naujos valdymo sąsajos menu atlieka paprastą pirminę konfuguraciją, o kai kurie nemokami, paplitę skriptai, papildo duotą koncepciją.**

 **Virtualaus serverio administravimas ir konfiguravimas atliekamas programinės įrangos pagalba, kurios įdėgtos kompiute ryje su Windows Vista, Windows 7 arba Windows Server 2008 operacine sistema su papildomomis galimybėms administruoti Hyper-V.**

**Architekrūra**

**Hyper-V atskiriamas pagal samprata „skyrius“. Skyrius- loginio vieneto riba, palaikoma hypervizoro, kuriame dirba operacinės sistemos. Kiekvienas hypervizoro egzempliorius turi vieną *pagrindinį skyrių* su Windows Server 2008 operacine sistema. Virtualizacijos stekas įjungiams *pagrindiniame skyriuje* ir turi tiesioginį priėjimą prie aparatinės dalies. *Pagrindinis skyriaus* pagalba sudaromas *atrinius skyrius,* kuriame ir laikomos virtualios operacinės sitemos. *Atrinis skyrius* gali sukurti savo *antrinius skyrius* ir jiems būti pagrindiniu. Pagrindinis skyrius sudaro antrinius hypervizoro pagalba.**

****

**Virtualizacijos skyriai ne turi priėjimo prie fizinio procesoriaus, negali valdyti realių petraukčių. Dėl to jie turi virtualų procesoriaus atvaizdo adresą, kuris priklauso nuo hypervizoro konfuguraciajos. Hypervizor gali nustatyti procesoriaus sudėtį kiekvienam skyriui. Hypervizor valdo procesoriaus pertrauktys ir siunčia jas į tam tikrus skyrius, naudodamasis *dirbtiniu petraukčių valdikliu (****Synthetic Interrupt Controller arba SynIC****).* Hyper-V gali aparatiškai didinti adresų transliaciją tarp atskirų virtualių adresinių erdvių** [IOMMU](http://ru.wikipedia.org/wiki/IOMMU) (*I/O Memory Management Unit-atminties įvedimo/išvedimo įtaisas*) pagalba, kuris dirba atskirai ir nepriklauso nuo aparatinio atminties valdymo.

Antriniai skyriai ne turi priėjimo prie aparatinių resursų, bet gauna virtualų resursų atvaizdą, kurie vadinasi virtualus įtaisai. Kiekviena užklausa skirta virtualiems įtaisams, nukreipiama per *VMBus* įtaisams pirminiame skyriuje, kurie ir apdoros duotą užklausą.

VMBus- loginis kanalas, kuris sąveikauja tarp skyrų. Atsakymas grįžta irgi per VMBus. Jeigu pirminio skyriaus įtaisai irgi virtualaus skyriaus, tai užklausa bus perduodama toliau, kol nepasieks pirminio skyriaus, kur turės prieiga prie fizinių įtaisų. Pirminiai skyriai įjungia *Virtualization Service Provider*, kuris jungiasi su VMBus ir apdoroja įtaisų priėjimo užklausas nuo antrinių skyrių. Antriniai skyriai dirba su *Virtualization Service Client (VSP),* kuris persiunčia užklausas per VMBus į pirminio skiriaus VSC.

**Pagrindinės Hyper-V apsaugos problemos**

1. **Administravimo panelės nebūvimas administravimo užduotims paskirstyti.**
* **Pagal nutylėjimą valdyti virtualias mašinas gali Hyper-V administratorius**
1. **Paprastas virtualių sistemų pernešimas į kitas fizines platformas.**
* **Konfidicialūs duomenys gali būti pavogti, kopijuojant virtualias mašinas.**
1. **Virtualios mašinos naudojasi host serverio resursais.**
* **Pagal nutylėjimą neapribotas virtualiųjų mašinų host sistemos naudojamasis.**
1. **Tinklinė sąveika**
* **Virtualus serveris turi turėti pakankamai tinklo sąsajų teisingai virtualių mašinų tinklų segmentacijai.**
1. **Serverio apsauga**
* **Administratorius turi prieiga prie visų virtualių mašinų**
* **Kadangi visas tinklo pralaidumas antrinių operacinių sitemų praeina per host serverį sąsajas, tai viena sensorius Ids host serveryje galės kontroliuoti visą trafiką antrinių operacinių sistemų.**
1. **Serverio apsauga nuo pačių virtualių mašinų**
* **Yra būtinybė izoliuoti host serverį, nuo virtualių mašinų.**

**Hyper-V saugumas**

1. ***Pagrindinės OS saugumas***

**Dėgimas.**

**Instaliuojant serverį Hyper-V rekomenduojama padaryti kelius žingsnius, kurie padidina sistemos saugumą. Galima sumažinti potencialų atakos plotą, įdiegus Hyper-V į serverį Windows 2008 R2, kuris dirbs branduolio režime be grafinio režimo. Taip pat rekomenduojama naudoti papildomus tinklo adapterius, mažiausiai dviejus, vienas iš kurių bus naudojamas darbui su virtualia mašina, kitas adminitruojant serverį su įdėgtu Hyper-V paketu.**

 **Rekomenduojama naudoti kaip pagrindinės operacinės sistemos įdėgimo variantą Server Core Windows Server 2008 R2 operacinei sistemai. Dėgimas Server Core užtrikrina minimalią atakos galimybę ir sumažina ištaisymų, atnaujinimų kiekį, kurie reikalingi aptarnavimui.**

Server Core privalumai:

* Minimali pagrindinės operacinės sistemos atakos galimybė.
* Naudojamas minimalus įtasų kiekis.
* Didesnis sistemos našumas, nes naudojama minimalus sistemos komponentų kiekis.
* Minimalus atnaujinimų kiekis-sistema minimaliai perkraunama.

Server Core trukūmai:

* Serveryje nėra grafinio valdymo.
* Kai kurie draiveriai ir programos ne palaikomos Server Core režime.
* Serveryje galima naudoti tik tuos draiverius, kurie praėjo suderinamumo patikrinimą.

**Tinklo sąsajų konfuguracija**

Tinkama tinklų sąsajų konfiguracija žymiai padidina bendrą apsaugos Hyper-V mazgų lygį. Microsoft rekomenduoja naudoti mažiausiai du tinklo adapterius Hyper-V mazge. Operainei virtualizacijos serverio sistemai naudojamas išskirtas tinklo adapteris. Pagal nutylėjimą pagrindinei virtualizacijos operacinei sistemai tinklas nekonfiguruojmas. Serverio valdymui, kur naudojamas Hyper-V, reikia naudoti išskirtą tinklo adapterį ir prijungtį jį prie patikimo potinklio, izoliuojant nuo kitų potinklių. Virtualių mašinų tinklo darbui naudojama vienas arba keli skirtingi tinklo adapateriai. Tai ledžia naudoti skirtingus tinklo saugumo lygius ir virtualių mašinų konfiguraciją.

Pavyzdžiui galima nustatyti tinklą tikiu būdu, kad priėjimas prie tinklo virtualioms mašinoms, skirtusi nuo priėjimo prie tinklo pagrindinei operacinei sitemai, įskaitant virtualių lokalių tinklų naudojimą, IP saugumą (IPSec), prieigos prie tinklo saugumą (NAP).

**Host serverio valdymas ir administravimas**

Nerekomenduojama suteikinėti virtualių mašinų administratoriams prieigos teisių prie pagrindinės operacinės sistemos. Remiantis mažiausiu privilegijų principu, virtualių mašinų administratoriams suteikiamos minimalios būtinos teisės. Reikalingų teisių valdymas visuose objektuose, kurie susiję su virtualiomis mašinomis, gali būti sudėtinga užduotis. Prie netinkamo naudojimo, gali privesti prie saugumo problemų.

1. ***Virtualių mašinų saugumas***

Virtualios mašinos saugumas iš pricnipo nieko nesisikyria nuo pagrindinės operacinės sistemos saugumo. Visi saugumo kriterijai, kurie priskiriami prie operacinės sistemos, pilnai atitinka virtualios mašinos saugumą. Rekomenduojama, kad kiekvienoje virtualioje mašinoje, būtų naudojama:

* Antivirusinė programa
* Kitos priemonės, kurios atitinka saugumo reikalavimus atitinkamai sistemai.

**Duomenų sistemų sauga**

Duomenų sistemų apsaugai reikia naudoti standartinius šaltinius- access control lists (ACLs)- virtualių mašinų prisijungmimo prie duomenų nustatymai. Toks požiūris užkirs kelią, kai įsilaužėjas bandys gauti neteisėtą prisijungimą prie virtualios mašinos duomenų tam, kad nukopijuoti juos arba pakeisti juos – variantų labai daug.

Vis dėlto, ACLs naudojamasis ne užtikrins pačios virualios mašinos nuo netesėto prisijungimo.

Hyper-V serveryje kiekviena virtuali mašina dirba vmwp.exe saugumo proceso kontekste, kuris atliekamas NETWORK SERVICE vardu ir kuris turi prieiga prie virtualios mašinos duomenų. Tai būtina tam, kad naudotis Hyper-V konsole virtualios mašinos valdymui iš naudotojo pusės, kuris be abejo turi priegos teisės prie sistemos.

Hyper-V saugomo žingsniai įtraukia ne tik ACLs naudojimą, bet ir saugumo užtikrinimo,valdymo instrumentus, tokius kaip System Center Virtual Machine manager 2008, Authorization Manager, kurie naudojami teisėms prie virtualių mašinų apriboti.

**BitLocker šifravimas**

Rekomenduojama naudoti BitLocker šifravimo mechanizmą Hyper-V resursų apsaugai. BitLocker šifravimas naudoja serverio įrangos komponentus ir mikroprogramas operacinės sitemos užkrovimo metu bei disko šifravimui, netgi jei serveryje nėra maitinimo įtampos. Tai leidžia apsaugoti duomenys, jei diskas bus pavogtas arba nukopijuotas į kitą kompiuterį. BitLocker šifravimas padeda apsaugoti duomenys netgi jei įsilaužėjas naudoja kitą operacinę sistemą arba bando neteisėtai prisijungti prie duomenų disko.

**Prisijungimo prie objekto įvykių auditas**

Saugumo funkcijos duomenų sistemoje gali užkirsti kelią neteisėtiems prisijungimams, labai svarbiems virtualių mašinų objektams, pavyzdžiui prie VHD duoemnų. Audito naudojimas priėjimui prie objektų leis aptikti neteisėtus prisijungimus. Įjunkite prisijungimo auditą Hyper-V serveryje. Po šios funcijos įjungimo bus registruojami visi prisijungimo prie duomenų įvykiai. Jeigu duomenų sudėtis bus pažeista, įvykių žurnale bus registruojamas kiekvienas prisijungimo prie duomenų bandymas.

Dažnai atsitinka, kad virualiose mašinose reikia saugoti labai svarbius, konfidicealius duomenys. Tokiais atvejais reikia užtikrinti daug didesnį saugos lygį. Vienas iš svarbesnių virtualių mašinų privalumų yra galimybė greitai pakeisti į autonominį režimą pristabdymo funkcijos Hyper-V pagalba (suspend).

1. ***Hypervizor‘o apsauga***

**Atminties apsauga: fizinės atminties prisirišimas prie virtualios mašinos.**

**Kiekviena virtuali mašina naudoja tik savo fizinę atmintį. Virtualios mašinos negali kartu naudoti tą patį atminties plotą. Hypervizor bet kuriuo momentu gali suteikti teises tam tikram atminties plotui nuskaityti, keisti bei uždrausti priėjimą.**

**Įėjimo/ išėjimo sistemų apsauga**

**Pagrindinė operacinė sistema turi galimybe valdyti virtualių mašinų įėjimo/išėjimo nustatymus. Tai leidžia apriboti prieiga prie tam tikrų įėjimo/išėjimo sistemų.**

**Realizuota prieigos sistema prie hypervizorų**

**Hypervizor ne leidžia naudoti priveligijuotas procesoriaus instrukcijas.**

**Plati integracija su Authorization Manager**

Sistema leidžia nustatyti privilegijas virtualiuose mašinuose.

**Teisių nustatymas virtualiųjų mašinų grupėms**

Leidžia nustatyti virtualių mašinų teises, jų paleidimą, įdėgimą, sukurimą, atvaizdų prijungimą.

**Bendrų resursų apsauga**

Prieiga prie visų Hyper-V resursų prieinama tik nuskaitymui.