НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

До захисту допущено:

Завідувач кафедри
_____ Сергій СТІРЕНКО

“___”_____2020 р.

Дипломний проект

на здобуття ступеня бакалавра

за освітньо-професійною програмою «Комп’ютерні системи та мережі»

спеціальності 123 «Комп’ютерна інженерія»

на тему: «Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Intel Virtualization Technology»

Виконав:
студент IV курсу, групи ІО-61
Даніїл ТРЕГУБОВ-УС _____

Керівник:
Доцент, к.т.н.,
Олександр ДОЛГОЛЕНКО _____

Консультант з нормоконтролю:
Професор, д.т.н.,
Валерій СІМОНЕНКО _____

Рецензент:

_____

Засвідчую, що у цьому дипломному проекті немає запозичень з праць інших авторів без відповідних посилань.
Студент _____
(підпис)

Київ – 2020 року

НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ
імені ІГОРЯ СІКОРСЬКОГО»
Факультет інформатики та обчислювальної техніки
Кафедра обчислювальної техніки

Рівень вищої освіти – перший (бакалаврьский)

Спеціальність – 123 «Комп'ютерна інженерія»

Освітньо-професійна програма «Комп'ютерні системи та мережі»

ЗАТВЕРДЖУЮ

Завідувач кафедри

_____ Сергій СТІРЕНКО

«___» _____2020 р.

ЗАВДАННЯ
на дипломний проект студента

Трегубова-Ус Даніїла Олексійовича

1. Тема проекту *«Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Intel Virtualization Technology»*
керівник проекту Долголенко Олександр Миколайович, к.т.н., доцент
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом по університету від «07» травня 2020 року №1081-с
2. Термін здачі студентом закінченого проекту
_____
3. Вихідні дані до проекту *технічна документація*
4. Зміст розрахунково-пояснювальної записки (перелік питань, які розробляються)
Опис предметної області, дослідження структури Intel Virtualization Technology, розробка серверної платформи Moodle, що орієнтована на вивчення можливостей технологій Intel® vPro™ , можливості віртуалізації ЦП, пам'яті та системи безпеки і мережевих функцій, функції віртуалізації введення-виведення.
5. Перелік графічного матеріалу

Принципова схема, функціональна схема та структурна схема

6. Консультанти проекту, з вказівкою розділів роботи, які до них вносяться

Розділ	Консультант	Підпис, дата	
		Завдання видав	Завдання прийняв
нормоконтроль	д.т.н., проф. Сімоненко В.П.		

7. Дата видачі завдання_____

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів дипломного проекту	Строк виконання етапів проекту	Примітки
1.	*Затвердження теми роботи*	*1.09.2019*	
2.	*Вивчення та аналіз завдання*	*2.09.2019-14.03.2020*	
3.	*Розробка архітектури та загальної структури програми*	*14.03.2020-25.03.2020*	
4.	*Розробка структур окремих Інтерфейсів програми*	*25.03.2020-2.04.2020*	
5.	*Програмна реалізація*	*2.04.2020-13.04.2020*	
6.	*Оформлення пояснювальної записки*	*13.04.2020-21.05.2020*	
7.	*Захист програмного продукту*	*21.05.2020 – 25.05.2020*	
8.	*Передзахист*	*26.05.2020*	
9.	*Захист*		

Студент Даніїл ТРЕГУБОВ-УС

Керівник Олександр ДОЛГОЛЕНКО

ВІДОМІСТЬ ДИПЛОМНОГО ПРОЕКТУ

№ з/п	Формат	Позначення	Найменування	Кількість листів	Примітка
1.	А4		Завдання на дипломний проект	2	
2.	А4	ІАЛЦ.467200.002 ТЗ	Технічне завдання	4	
3.	А4	ІАЛЦ.467200.003 ПЗ	Пояснювальна записка	73	
4.	А4	ІАЛЦ.467200.004 А1	Принципова схема алгоритму	1	
5.	А4	ІАЛЦ.467200.005 А2	Функціональна схема	1	
6.	А4	ІАЛЦ.467200.006 А3	Структурна схема	1	

Технічне завдання до дипломного проекту

ЗМІСТ

1. НАЙМЕНУВАННЯ ТА ОБЛАСТЬ ЗАСТОСУВАННЯ

Назва розробки: Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Intel Virtualization Technology.

Область застосування: Навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Intel Virtualization Technology.

2. ПІДСТАВИ ДЛЯ РОЗРОБКИ

Підставою для розробки є завдання на виконання роботи кваліфікаційно-освітнього рівня «бакалавр комп'ютерної інженерії», затверджене кафедрою обчислювальної техніки Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського».

3. МЕТА ТА ПРИЗНАЧЕННЯ РОЗРОБКИ

Метою даного проекту є дослідження можливостей технології Intel® vPro™: Intel Virtualization Technology та розробка програмних засобів навчання використанню можливостей цієї технології у віртуальному навчальному середовищі Moodle.

4. ДЖЕРЕЛА РОЗРОБКИ

Джерелом розробки є науково-технічна література, публікації в виданнях, довідники, публікації в Інтернеті по опису архітектури і принципу роботи Intel® vPro™: Intel Virtualization Technology.

5. ТЕХНІЧНІ ВИМОГИ

5.1. Вимоги до програмної моделі серверної платформи Moodle

Програмна система має мати наступний функціонал:

- Створювати лекції, тести і завдання у вбудованому редакторі;
- Запрошувати і імпортувати користувачів, об'єднувати їх в групи, записувати їх на курси;
- Переглядати статистику активності на платформі;
- Зміна дизайну, інтеграція з іншими сервісами, візуалізація звітів.

5.2. Вимоги до програмного забезпечення серверної платформи Moodle

- Операційна система Microsoft Windows Server 2019;
- Віртуальне навчальне середовище Moodle;
- Мова сценаріїв PHP;
- Працюючий сервер баз даних.

5.3. Розглянути можливість підключення до серверної платформи Moodle баз даних

MySQL 5.6+ ;

- PostgreSQL 9.4+ ;
- MariaDB 5.5.31+ ;
- Microsoft SQL Server 2008+ ;
- Oracle Database 11.2+ ;

5.4 Вимоги до апаратного забезпечення серверної платформи Moodle

- Два процесора типу Intel Xeon;
- Оперативна пам’ять - 64 GB з можливістю розширення до 128 GB;
- Відеоадаптер – інтегрований;
- Дискові накопичувачі - 2 накопичувача не гірше, ніж SAS 8TB 7200RPM rpm;
- Контролер SAS - не менш ніж 8 каналів з можливістю побудови RAID 0, 1, 5, 6 и 10;
- Мережний контролер –1 Gb/s (2 шт. інтегровані в материнську плату); мережний контролер - 10 Gb/s Fibre Channel (2 шт.);
- Серверний корпус rackmount (висота – не більше 2U);
- Два блока живлення з функцією «гарячої» заміни (1 основний + 1 резервний);
- Резервування системних вентиляторів, можливість здійснення «гарячої»» заміни системних вентиляторів;
- Оптичний накопичувач - DVD-RW;
- Монтажний комплект – телескопічний комплект для монтажу сервера в стійку/шафу.

6. ЕТАПИ РОЗРОБКИ

Назва етапу	Дата
Вивчення джерел за тематикою роботи	10.01.2020
Розроблення і узгодження технічного завдання	20.02.2020
Моделювання структури програмного забезпечення	03.03.2020
Розробка програмного забезпечення	25.03.2020
Тестування системи	01.05.2020
Виправлення помилок	15.05.2020
Оформлення документації дипломної роботи	25.05.2020

Анотація

В бакалаврській *дипломній* роботі досліджені можливості технології Intel® vPro™: Intel Virtualization Technology та реалізовані програмні засоби навчання по використанню її можливостей у віртуальному навчальному середовищі Moodle.

Реалізовано серверну платформу Moodle, що орієнтована на вивчення персоналізованої навчальної програми по використанню можливостей технологій Intel® vPro™.

Abstract

The bachelor's thesis explores the capabilities of Intel® vPro ™ technology: Intel Virtualization Technology and implements training tools, using its capabilities in the Moodle virtual learning environment.

The Moodle server platform has been implemented, which focuses on the study of a personalized training program on using the capabilities of Intel® vPro ™ technologies.

ПОЯСНЮВАЛЬНА ЗАПИСКА

до дипломного проекту

на тему: «Intel® vPro™: Intel Virtualization Technology»

Київ – 2020

ЗМІСТ

					ІАЛЦ.467200.003 ПЗ		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розробив		*Трегубов-Ус Д.О*			*Програмні засоби навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Intel Virtualization Technology.*	Літ.	Аркуш 1 / Аркушів 73
Перевір.		*Долголенко О.М.*					
Н. контр.		Сімоненко В.П.			*Пояснювальна записка*	НТУУ "КПІ" ФІОТ, ІО-61	
Затверд.							

ПЕРЕЛІК ТЕРМІНІВ ТА СКОРОЧЕНЬ

(TXT) - Trusted Technology Execution Technology

(AMT) - Intel Active Management Technology;

(Intel VT-x) - Intel Virtualization Technology;

(Intel VT-d) - Intel Virtualization Technology for directed I/O;

(DMA) - Direct memory access;

(SDN) - Software-defined networking;

(NAP) - Network Access Protection;

(WOL) - Wake-on-LAN;

(SOL) – Serial Over LAN;

(UUID) - Universally unique identifier;

(DHCP) - Dynamic Host Configuration Protocol;

(BOOTP) - Bootstrap Protocol;

(VNC) - Virtual Network Computing;

(KVM) - Kernel-based Virtual Machine;

(WLAN) - Wireless Local Area Network;

(S0) - комп'ютер увімкнено і працює;

(Intel ISM) - Intel Standard Manageability;

(Intel SBT) - Intel Small Business Technology;

(PCH) - Platform Controller Hub;

(SMB) - Small Medium Business;

(HW) - HardWare;

(POST) - Power On Self Test;

(TPM) - Trusted Platform Module;

(PXE) - Preboot Execution Environment;

(VMM) - Virtual Machine Manager;

(VM) - Virtual Machine;

(ОС) - Операційна система;

(GPA) - Guest Physical Address;

(HPA) - Host Physical Address;

(PCI SIG) - Peripheral Component Interconnect - Special Interest Group;

(NIC) - Network Interface Card;

(LVMM) - Level Virtual Machine Manager;

(BIOS) - Basic Input-Output System;

(PCI) - Peripheral Component Interconnect;

(EAC) - Endpoint Access Control;

(PDP) - Policy Decision Point;

(PEPs) - Policy Enforcement Points;

(ACPI) - Advanced Configuration and Power Interface;

Вступ

Технологія Intel vPro – це маркетинговий термін, використовуваний Intel для великої колекції комп'ютерних технологій. Платформа Intel® vPro ™ складається з апаратного забезпечення і технологій, які утворюють будівельні блоки для бізнес-обчислень. Специфікація платформи регулярно оновлюється для забезпечення безперервних інновацій, а також пропонує оптимізовані архітектури для настільних і мобільних пристроїв. Кожне наступне покоління Intel® vPro ™ націлене на забезпечення запасу продуктивності для бізнес-процесів при одночасній реалізації гнучких форм-факторів для різних обчислювальних середовищ.

Intel® vPro ™ призначена для керованих IT-середовищ, де бізнес прагне забезпечити дотримання корпоративних політик у своїй обчислювальної інфраструктурі. Ці політики можуть включати створення призначених для користувача образів, включення служб безпеки, підготовку пристроїв або обслуговування комп'ютерів протягом їх життєвого циклу. Цей тип управління активами може принести користь підприємствам будь-якого розміру, незалежно від того, управляється обчислювальна інфраструктура внутрішньо або постачальником послуг.

Повністю реалізована платформа Intel® vPro ™ об'єднує верхню частину лінійки процесорів Intel з високошвидкісними дротовими і бездротовими мережами, жорсткими дисками Intel® і пам'яттю Intel® Optane ™ для швидкого доступу до даних. Системи, сумісні з Intel® vPro ™, доступні в різних форм-факторах. Сюди входять тонкі і легкі мобільні системи з великим часом автономної роботи, настільні ПК малого форм-фактора для елегантних робочих місць і робочі станції, що підтримують насичену візуальну обчислювальну середу.

Однією із важливих технологій, що реалізовані на платформі Intel® vPro™, є Intel Virtualization Technology. Разом з цим, існує дуже невелика кількість джерел де описані можливості цієї платформи, майже всі вони є англомовними. Учбові посібники по вивченню можливостей цієї платформи відсутні взагалі. У зв’язку з цим розробка програмних засобів навчання в системі Moodle системних адміністраторів

використанню можливостей Intel Virtualization Technology – однієї із головних технологій платформи Intel® vPro™ є дуже актуальною і може знайти попит на навчання у співробітників багатьох IT компаній.

РОЗДІЛ 1.

Огляд технології Intel® vPro ™

1.1 Технологія Intel® vPro ™

Технологія Intel vPro - це зонтичний маркетинговий термін, який використовується Intel для великої колекції комп'ютерних апаратних технологій, включаючи Hyperthreading, Turbo Boost 3.0, VT-x, VT-d, Trusted Technology Execution Technology (TXT), Intel Active Management Technology (AMT) та інших. Коли бренд vPro був запущений (близько 2007 року), він був ідентифікований головним чином з AMT, тому деякі журналісти все ще вважають AMT суттю vPro.

1.2 Функції vPro ™

Intel vPro - торгова марка для набору апаратних функцій ПК. Комп'ютери, що підтримують vPro, в якості основних елементів мають процесор з підтримкою vPro, чипсет із підтримкою vPro та BIOS з підтримкою vPro.

ПК vPro включає:

• Багатоядерні, багатопотокові процесори або процесори Xeon, чи процесор Core з підтримкою vPro.

• Провідне та бездротове підключення до мережі.

• Технологію Intel AMT - набір апаратних функцій, орієнтованих на бізнес, що дозволяють отримати віддалений доступ до ПК для виконання завдань управління та безпеки, коли ОС не працює або вимкнено живлення ПК. Зауважте, що AMT - це не те саме, що Intel vPro; AMT - це лише один елемент vPro ПК.

•Технологію Intel Virtualization, включаючи Intel VT-x для процесора та пам'яті, і Intel VT-d для вводу / виводу для підтримки віртуалізованих середовищ. Intel VT-x прискорює апаратну віртуалізацію, що дозволяє створювати ізольовані регіони пам’яті для запуску критичних додатків на апаратних віртуальних машинах з метою підвищення цілісності запущеного додатка та конфіденційності конфіденційних даних. Intel VT-d відкриває захищені адресні простори віртуальної пам’яті

периферійним пристроям DMA, підключеним до комп'ютера через шини DMA, зменшуючи загрозу, яку створюють шкідливі периферійні пристрої.

• Технологію віддаленої конфігурації для AMT із захистом на основі сертифікатів. Віддалену конфігурацію можна виконати на системах, навіть до встановлення ОС та / або агентів управління програмним забезпеченням.

• Технологію Intel Trusted Execution (Intel TXT), яка перевіряє середовище запуску та встановлює корінь довіри, що, в свою чергу, дозволяє програмному забезпеченню будувати ланцюжок довіри для віртуалізованих середовищ. Intel TXT також захищає секрети під час переходу живлення як для впорядкованого, так і для безладного відключення (традиційно вразливий період для облікових даних безпеки).

• Підтримку IEEE 802.1X, мережі самозахисту Cisco (SDN) та захисту доступу до мережі Microsoft (NAP) на ноутбуках та підтримка 802.1x та Cisco SDN на настільних ПК. Підтримка цих технологій безпеки дозволяє Intel vPro зберігати позицію безпеки ПК, щоб мережа могла аутентифікувати систему перед завантаженням ОС і додатків та перед тим, як ПК буде дозволений доступ до мережі.

• Біт відключення виконання (Execute disable bit), який при підтримці ОС може запобігти атакам переповнення буфера.

1.3 Віддалене управління

Intel AMT - це набір функцій управління та безпеки, вбудованих в vPro ПК, що спрощує системному адміністратору моніторинг, обслуговування,

безпеку та обслуговування ПК. Intel AMT (технологія управління) іноді її помилково ототожнюють з Intel vPro (платформою ПК), але вона є тільки однією з найбільш відомих технологій ПК на базі Intel vPro.

Intel AMT включає:

Зашифроване віддалене підключення / зменшення живлення (через пробудження та локальну мережу або WOL);

Віддалене / перенаправлене завантаження (за допомогою інтегрованого перенаправлення електронного пристрою.)

Перенаправлення консолі (через послідовне використання та локальну мережу або SOL);

Попереднє завантаження доступу до налаштувань BIOS;

Програмована фільтрація для вхідного та вихідного мережевого трафіку;

Перевірка присутності агента;

Попередження на основі політики поза межами діапазону.

Доступ до системної інформації, такої як універсальний унікальний ідентифікатор ПК (UUID), інформація про апаратні засоби, стійкі журнали подій та інша інформація, яка зберігається у виділеній пам'яті (не на жорсткому диску), де вона доступна, навіть якщо ОС не працює або ПК вимкнено.

Наразі апаратне управління було доступне в минулому, але воно обмежувалося автоматичною конфігурацією (для комп’ютерів, які це вимагають) за допомогою DHCP або BOOTP для динамічного розподілу IP-адреси та бездискових робочих станцій, а також для безвідмовної локальної мережі віддалено, живлення систем.

1.4 Пульт дистанційного керування KVM на базі VNC

Починаючи з vPro з AMT 6.0, ПК із процесорами i5 або i7 та вбудованою графікою Intel, тепер містять вбудований VNC сервер Intel. Ви можете використовувати позадіапазонне віддалене підключення до ПК своєї регіональної мережі, використовуючи спеціалізовану технологію перегляду, сумісну з VNC, та мати повну здатність KVM (клавіатури, відео та миші) протягом усього циклу живлення - включаючи безперебійне управління робочим столом при завантаженні операційної системи. Такі клієнти, як VNC Viewer Plus від RealVNC, також надають додаткову функціональність, яка може полегшити виконання (і перегляд) певних операцій Intel AMT, таких як вимкнення та ввімкнення комп'ютера, налаштування BIOS та встановлення віддаленого зображення (IDER).

Не всі процесори i5 та i7 з vPro можуть підтримувати KVM. Це залежить і від параметрів BIOS OEM та наявності дискретної відеокарти. Тільки інтегрована HD-графіка підтримує здатність KVM.

1.5 Бездротовий зв’язок

Intel vPro підтримує зашифрований дротовий та бездротовий зв'язок локальної мережі для всіх функцій віддаленого керування для ПК, що знаходяться всередині корпоративного брандмауера. Intel vPro підтримує зашифровану комунікацію для деяких функцій віддаленого управління для дротових та бездротових локальних ПК за межами корпоративного брандмауера.

Ноутбуки з vPro включають гігабітне мережне підключення та підтримують бездротові протоколи IEEE 802.11 a / g / n.

Комп'ютери Intel vPro підтримують бездротове спілкування з функціями AMT.

Для бездротових ноутбуків, що живляться від акумулятора, зв’язок із функціями AMT може відбуватися, коли система підключена до корпоративної мережі. Цей зв’язок доступний, навіть коли ОС не працює, або відсутні агенти управління.

Позадіапазонна комунікація AMT та деякі функції AMT доступні для бездротових чи дротових ноутбуків, підключених до корпоративної мережі через віртуальну приватну мережу (VPN) на базі ОС, коли ноутбуки пробуджені та працюють належним чином.

Бездротове з'єднання працює на двох рівнях: інтерфейс бездротової мережі (WLAN) та драйвер інтерфейсу, що виконується на хості платформи. Мережевий інтерфейс управляє зв'язком радіочастотного зв'язку.

Якщо користувач вимикає бездротовий передавач / приймач за допомогою апаратного перемикача, Intel AMT не може використовувати бездротовий інтерфейс ні за яких умов, поки користувач не включить бездротовий передавач / приймач.

Intel AMT Release 2.5 / 2.6 може надсилати та отримувати трафік управління через WLAN лише тоді, коли платформа знаходиться в режимі живлення S0 (комп'ютер увімкнено і працює). Він не отримує бездротовий трафік, коли хост спить або вимикається. Якщо стан живлення дозволяє, Intel AMT Release 2.5 / 2.6 може продовжувати надсилати та отримувати позаполосний трафік, коли платформа знаходиться в стані Sx, але лише за допомогою дротового з'єднання локальної мережі, якщо така існує.

Версія 4.0 та пізніші версії підтримують можливість керування бездротовим бездіапазонним режимом у станах Sx, залежно від налаштування живлення та інших параметрів конфігурації.

Випуск 7.0 підтримує керованість бездротовим зв'язком на настільних платформах.

Коли бездротове з'єднання встановлено на хост-платформі, воно базується на бездротовому профілі, який встановлює імена, паролі та інші елементи захисту, що використовуються для автентифікації платформи до бездротової точки доступу. Користувач або IT-організація визначає один або декілька профілів за допомогою інструмента, такого як Intel PROSet / Wireless Software. У випуску 2.5 / 6 Intel AMT повинна була мати відповідний бездротовий профіль для отримання позадіапазонного трафіку по тому ж бездротовому каналу зв'язку. API мережевого інтерфейсу дозволяє визначати один або кілька бездротових профілів, використовуючи ті самі параметри, що і програмне забезпечення Intel PROSet / Wireless. Під час живлення хоста Intel AMT спілкується з драйвером бездротової локальної мережі на хості. Коли драйвер і Intel AMT знаходять відповідні профілі, драйвер спрямовує трафік, адресований пристрою Intel AMT для обробки керованості. З певними обмеженнями, Intel AMT Release 4.0 / 1 може надсилати та приймати позаполосний трафік без бездротового профілю, налаштованого Intel AMT, якщо активний драйвер хоста і платформа знаходиться всередині підприємства.

У версії 4.2 та на версії 6.0 бездротових платформ WLAN включено за замовчуванням як до, так і після конфігурації. Це означає, що можна настроїти Intel

AMT через WLAN, доки у головного драйвера WLAN є активне з'єднання. Intel AMT синхронізується з активним профілем хоста. Він передбачає, що сервер конфігурації налаштовує бездротовий профіль, який Intel AMT використовує в станах живлення, відмінних від S0.

Якщо виникає проблема з драйвером бездротового зв’язку, а хост все ще працює (лише в режимі живлення S0), Intel AMT може продовжувати отримувати трафік керування поза діапазоном безпосередньо з інтерфейсу бездротової мережі.

Щоб Intel AMT працював з бездротовою локальною мережею, він повинен ділитися IP-адресами з хостом. Це вимагає наявності сервера DHCP для розподілу IP-адрес, а Intel AMT повинен бути налаштований для використання DHCP.

1.6 Зашифрований зв’язок під час роумінгу

Комп'ютери Intel vPro підтримують зашифроване спілкування під час роумінгу.

vPro ПК версії 4.0 або вище підтримує захист мобільного зв’язку шляхом встановлення захищеного тунелю для зашифрованого зв'язку AMT з керованим постачальником послуг під час роумінгу (працює у відкритій, дротовій локальній мережі за межами корпоративного брандмауера). Безпечне спілкування з AMT можна встановити, якщо ноутбук вимкнений або ОС відключена. Шифрований тунель зв'язку AMT розроблений таким чином, щоб системним адміністраторам можна було отримати доступ до ноутбука або настільного ПК у супутникових офісах, де немає проксі-сервера або пристрою сервера управління.

Безпечні комунікації за межами корпоративного брандмауера залежать від додавання до мережевої інфраструктури нового елемента - сервера присутності управління (Intel називає це "шлюзом з підтримкою vPro"). Для цього потрібна інтеграція з виробниками мережевих комутаторів, постачальниками брандмауерів та постачальниками, які розробляють консолі управління для створення інфраструктури, яка підтримує зашифровані роумінгові комунікації. Таким чином, хоча зашифрований роумінговий зв’язок увімкнено як функцію в vPro ПК версії 4.0 і

новіших, ця функція не буде повною мірою працювати, поки інфраструктура не буде створена і не запрацює.

1.7 vPro безпека

Технології та методології vPro безпеки забезпечуються чипсетом ПК та іншим системним обладнанням. Під час розгортання ПК vPro, облікові дані безпеки, ключі та інша важлива інформація зберігаються в захищеній пам'яті (не на жорсткому диску) і стираються, коли вони більше не потрібні.

1.8 Питання безпеки та конфіденційності

За даними Intel, відключити AMT можна через налаштування BIOS, проте, мабуть, більшість користувачів не можуть виявити зовнішній доступ до свого ПК за допомогою апаратної технології vPro. Більше того, Sandy Bridge та наступні чіпи мають "... можливість віддаленого знищення та відновлення втраченого чи викраденого ПК через 3G".

У травні 2017 року Intel опублікувала рекомендації щодо безпеки щодо вразливості мікропрограмного забезпечення в певних системах, що використовують Intel AMT, Intel Standard Manageability (Intel ISM) або Intel Small Business Technology (Intel SBT). Уразливість потенційно є дуже серйозною і може дати можливість мережевому зловмиснику віддалено отримати доступ до бізнес-ПК та робочих станцій, які використовують ці технології. Ми закликаємо людей та компанії, що використовують бізнес-комп’ютери та пристрої, в яких вбудовані Intel AMT, Intel ISM або Intel SBT, застосувати оновлення мікропрограмного забезпечення від виробника обладнання, коли це можливо, або дотримуватися кроків, щодо пом'якшення наслідків.

Багато функцій vPro, включаючи AMT, реалізовані в Intel Management Engine (ME), окремому процесорі в чипсеті під управлінням спеціалізованої ОС MINIX 3, який, як було виявлено, має численні вразливості. На відміну від AMT, зазвичай немає офіційного документально підтвердженого способу відключення ME; вона завжди увімкнена, якщо її не вимкнено OEM.

1.9 Особливості безпеки

Intel vPro підтримує стандартні галузеві методології та протоколи, а також інші функції безпеки постачальників:

- Industry-standard Trusted Platform Module version 1.2 (TPM);
- Support for IEEE 802.1x, Preboot Execution Environment (PXE), and Cisco Self Defending Network (SDN) in desktop PCs, and additionally Microsoft Network Access Protection (NAP) in laptops;
- Execute Disable Bit;
- Intel Virtualization Technology (Intel VT(Vt-x+Vt-d));
- Intel VMCS-Intel Virtual Machine Control Structure Shadowing;
- Intel Platform Trust Technology-PTT;
- Intel Data Protection Technology;
- Intel Identity Protection technology;
- Intel Secure key;
- Intel Anti-Theft Technology;
- Intel Boot Guard;
- Intel OS Guard;
- Intel Active Management Technology-Intel AMT;
- Intel Stable Image Platform Program-SIPP;
- Intel Small Business Advantage-Intel SBA;
- Intel Trusted Execution;
- Technology (Intel TXT).

1.10 Intel Boot Guard

Intel Boot Guard - це процесорна функція, яка заважає комп'ютеру створювати зображення прошивки, не випущені виробником системи. Після ввімкнення процесори перевіряють підпис, що міститься в зображенні вбудованого програмного забезпечення, перед тим, як виконати його, використовуючи хеш публічної половини

ключа підпису, який виробник системи зливає в концентратор платформи (PCH) системи, виробленої не Intel.

Intel Boot Guard - додаткова функція процесора, що означає, що її не потрібно активувати під час виготовлення системи. Як результат, Intel Boot Guard при активації не дає можливість кінцевим користувачам встановлювати замінні вбудовані програми, такі як Coreboot.

1.11 Технології та методології

Intel vPro використовує декілька стандартних технологій та методологій безпеки для захисту віддаленого каналу зв'язку vPro. Ці технології та методології також покращують безпеку доступу до критичних системних даних ПК, налаштувань BIOS, функцій управління Intel AMT та інших чутливих функцій або даних; та захистити облікові дані та іншу важливу інформацію під час розгортання (налаштування та конфігурація Intel AMT) та використання vPro.

Протокол безпеки транспортного рівня (TLS), включаючи загальнодоступний ключ TLS (TLS-PSK) для захисту зв'язку через позадіапазонний мережевий інтерфейс. Реалізація TLS використовує 128-бітове шифрування AES та ключі RSA з довжиною модуля 2048 біт.

Протокол автентифікації дайджесту HTTP. Консоль управління автентифікує IT-адміністраторів, які керують ПК на Intel AMT.

- Одноразовий вхід на Intel AMT за допомогою автентифікації домену Microsoft Windows на основі протоколів Microsoft Active Directory та Kerberos.
- Генератор псевдовипадкових чисел (PRNG) у прошивці ПК AMT, який генерує якісні сеансові ключі для безпечного зв'язку.
- Завантажувати та виконувати можуть лише зображення цифрового програмного забезпечення (підписані Intel).
- Зберігання критичних даних щодо управління, захищених від несанкціонованого доступу, через захищене, стійке (енергонезалежне)

сховище даних (область пам’яті, що не знаходиться на жорсткому диску) в апаратному забезпеченні Intel AMT.

- Списки контролю доступу до діапазону Intel AMT та інших функцій управління.

1.12 Можливості технології vPro в умовах SMB та Enterprise компанії

Технологія vPro значно розширює можливості по управлінню парком ПК в умовах сучасної компанії, причому як невеликий (SMB - small medium business) так і великої (enterprise). Технологія дозволяє зменшити число викликів технічних фахівців на робочі місця користувачів, так як більшість завдань з vPro можна вирішувати віддалено. Інтеграція технології vPro можлива в уже існуючу IT-інфраструктуру, звичайно з поправкою на те, що можливості технології будуть застосовні тільки для ПК з підтримкою vPro.

Щоб відповідати технології vPro комп'ютер повинен обов'язково відповідати наступним вимогам:

- Процесори Intel Core i5 і Core i7 з підтримкою технології віртуалізації;
- Системна логіка Intel Q77;
- Гігабітний мережевий адаптер Intel (82578DM) з підтримкою технології Intel Active Management 6.

Технологія vPro використовує власну підмережа для управління комп'ютерами, при цьому зв'язок забезпечується за існуючою фізичної інфраструктурою. Системний BIOS ПК з підтримкою vPro містить розширений розділ із спеціальним ПЗ, яке дозволяє або отримувати IP-адресу від DHCP сервера (без участі ОС на ПК) або встановити його вручну. Адміністрування vPro-ПК може здійснюватися не тільки при працюючому ПК, але і на ПК, що знаходиться в сплячому, або вимкненому (!) станах. Це, наприклад, дозволяє проводити всі сервісні роботи з комп'ютерами користувачів по закінченні робочого дня та виключенні простоїв.

Технологія vPro передбачає два основних рівня свого використання:

1. Режим SMB;

2. Режим Enterprise.

1.13 Режим SMB

Застосується в малому офісі. Для базової функціональності не вимагає додаткових витрат на придбання спеціального ПО з підтримкою технології vPro. При такому сценарії використання забезпечуються такі функції:

- Віддалення управлінням живленням;
- Перегляд даних про основне обладнання (інвентаризація);
- Перегляд енергонезалежного журналу подій;
- Віддалене оновлення AMT Firmware;
- Вбудований апаратний KVM.

Даний функціонал забезпечується простим керуванням з консолі управління до клієнта vPro через web-інтерфейс на порт 16992 (див. рис. 1.1 та рис. 1.2):

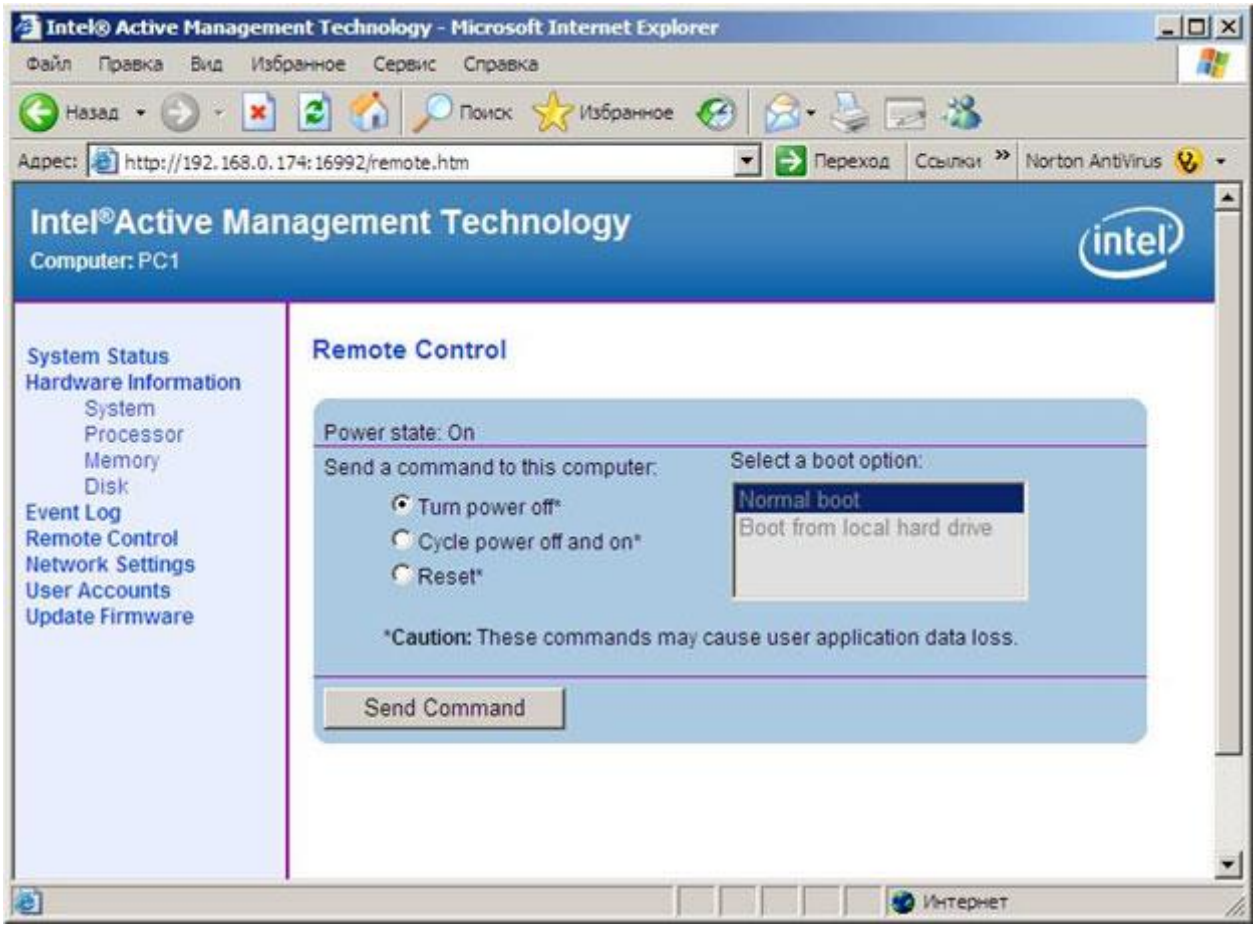


Рис. 1.1 - Дистанційне керування

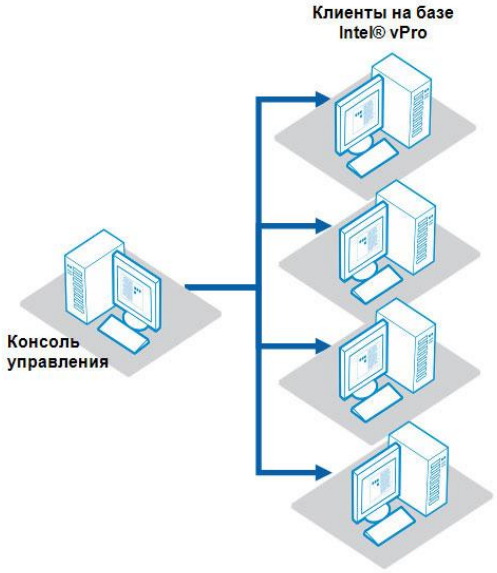


Рис. 1.2 - Консоль управління

У разі використання додаткового ПЗ (Система централізованого управління з підтримкою AMT: SyAM Desktop Monitor Local + SyAM Server Monitor Central або LANDesk Management Suite) функціональність рішення значно зростає:

- Налаштування системи оповіщень на основі апаратних датчиків платформи (повідомлення про несправності устаткування, зависання ОС і т. п.);
- Віддалене завантаження (IDE-перенаправлення) - завантаження vPro-клієнта на диск на сервері. Ця функція може бути використана, наприклад, в разі неможливості завантажити ОС на клієнтському комп'ютері, тоді можна скористатися чинним на сервері для відновлення і діагностики (див. рис. 1.3);

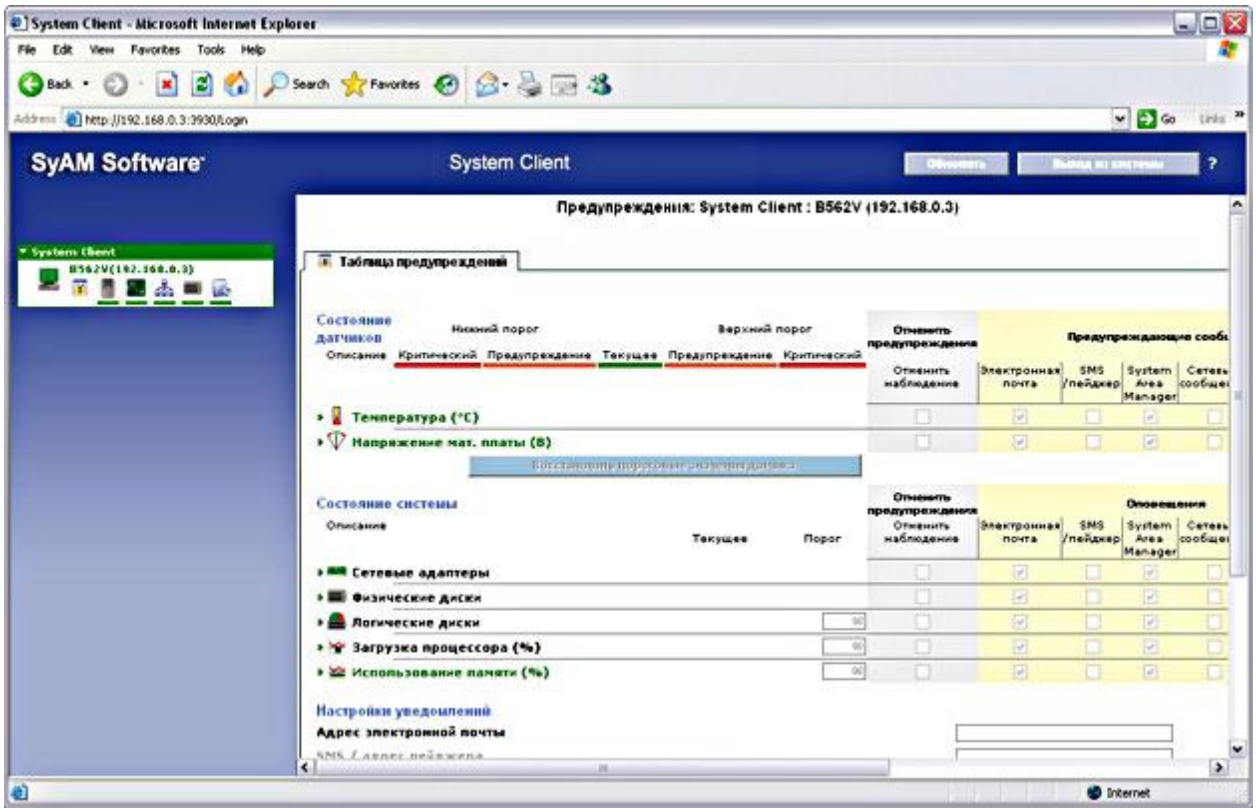


Рис. 1.3 – Таблиця попереджень

- Переадресація консолі функція SOL (Serial-over-LAN) - призначена для перенаправлення текстової консолі з робочої станції на центральну консоль управління. В рамках SOL-сесії можливий віддалений доступ до BIOS і робота з текстовими операційними системами і додатками;
- Перевірка наявності агенту управління;
- Захист системи: a). фільтрація вхідного і вихідного трафіку ОС (вбудовані апаратні фільтри для перевірки усередінісмугового і позасмугового мережевого трафіку); b). ізоляція заражених ПК (апаратне блокування мережевого трафіку);
- Оновлення антивірусного і анти шпигунського ПО у віддаленому режимі (див. рис. 1.4);

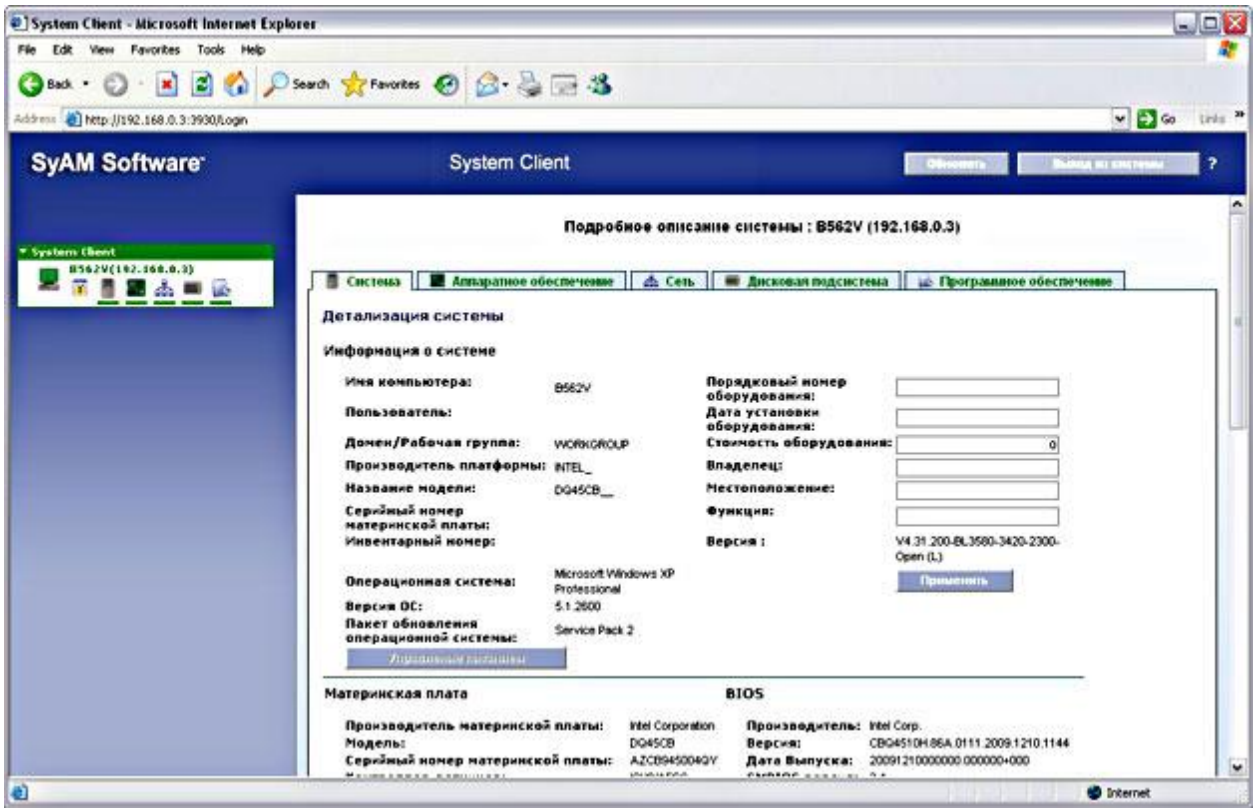


Рис. 1.4 – Деталізація системи

Більшість функцій vPro в режимі SMB тепер можна використовувати за допомогою безкоштовної утиліти Intel System Defence Utility, якої комплектується кожен ПК Team Office b583V (див. рис. 1.5, 1.6 , 1.7).

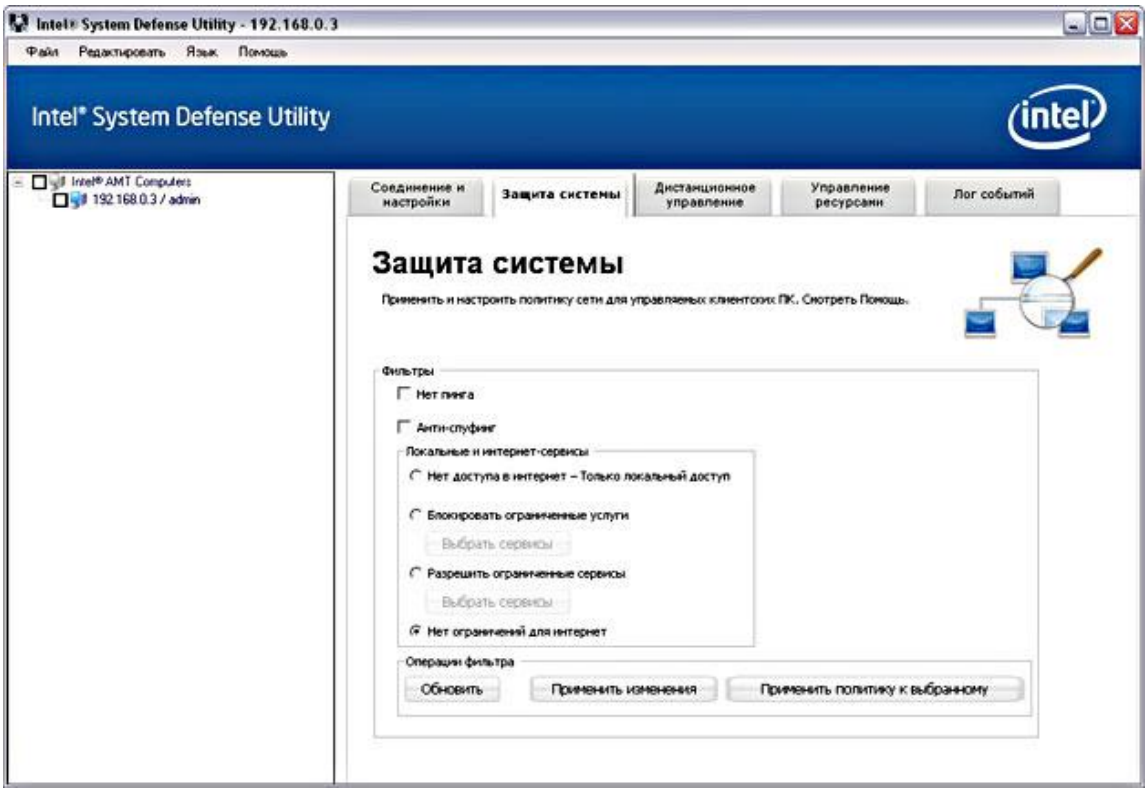


Рис. 1.5 – Захист системи

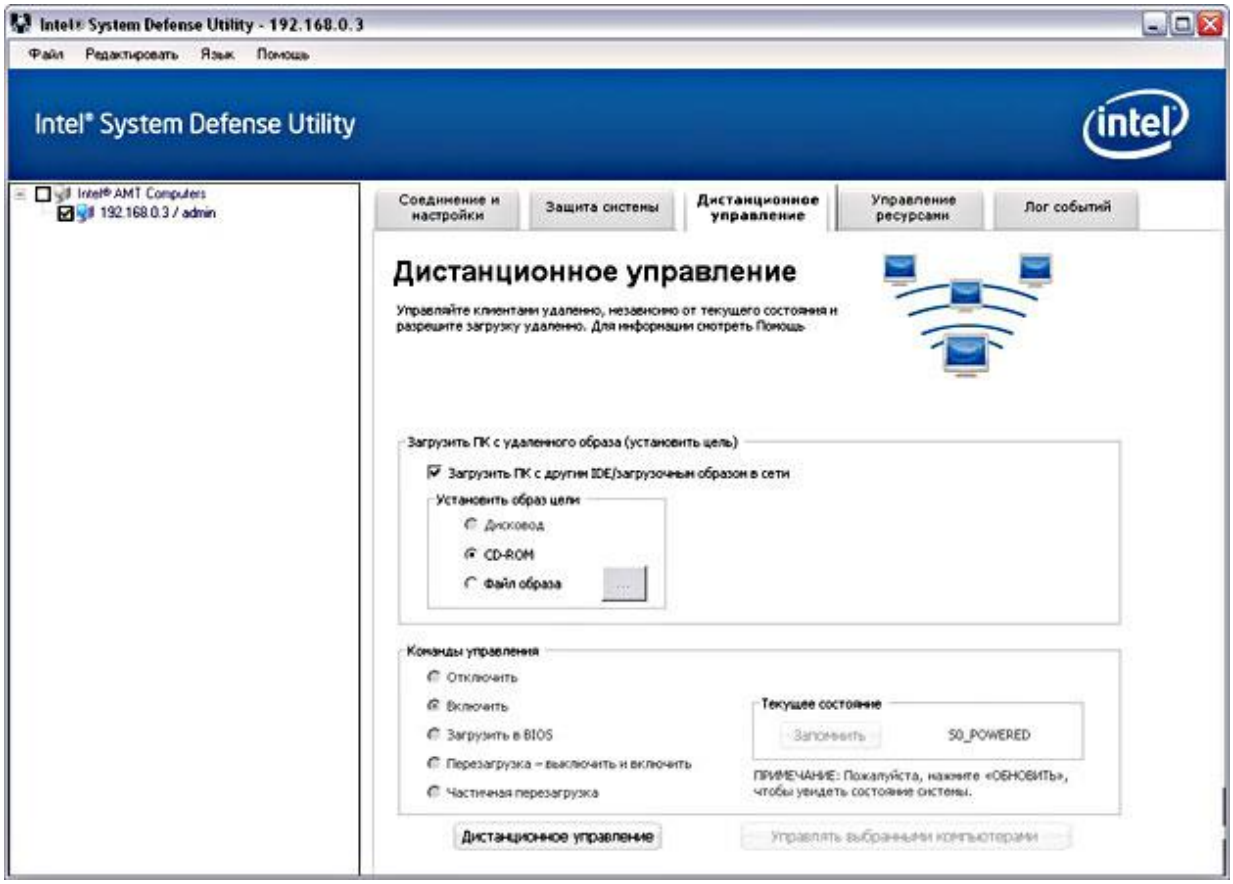


Рис. 1.6 – Дистанційне керування

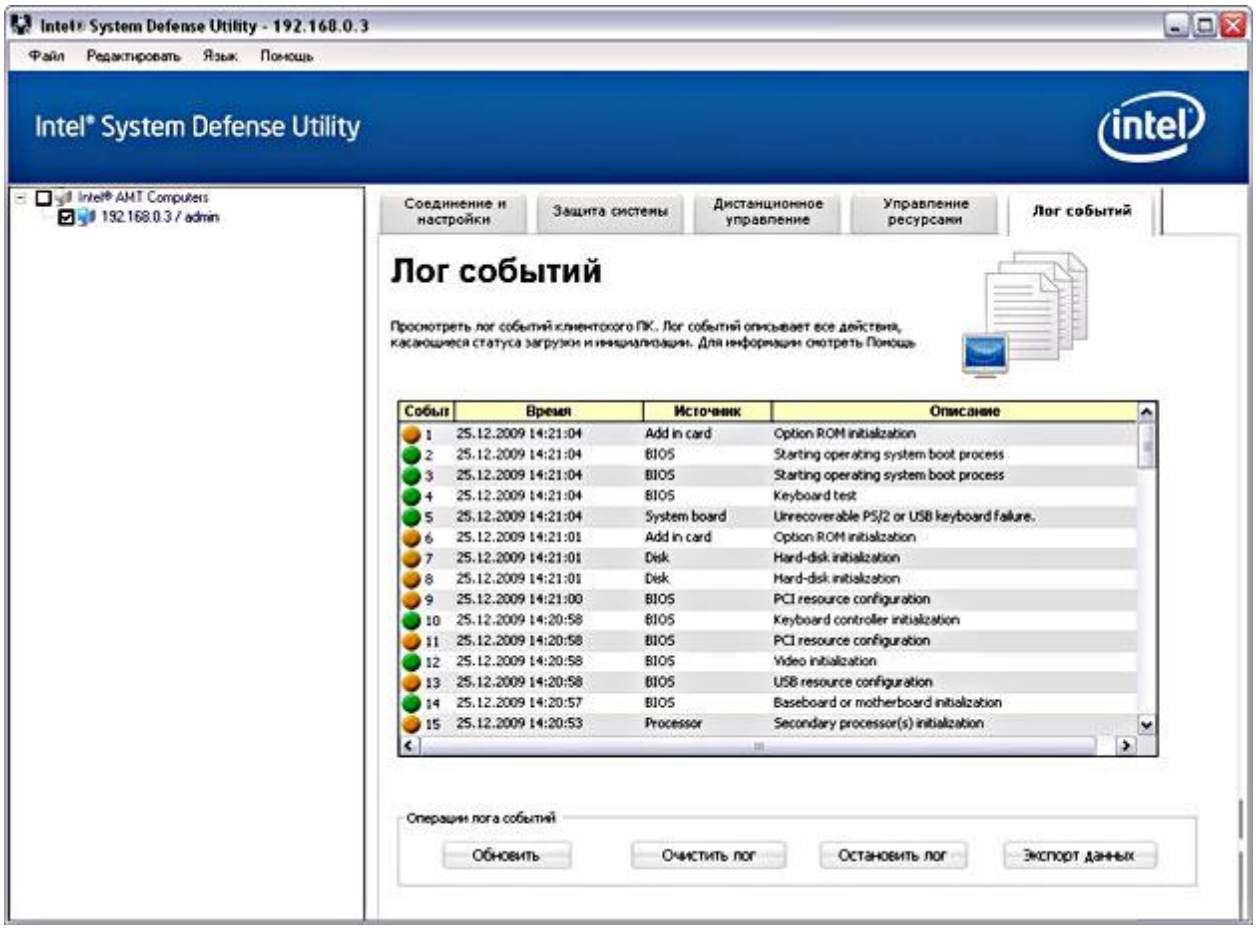


Рис. 1.7 – Лог подій

1.14 Режим Enterprise

У цьому режимі для кожної vPro-системи створюється унікальний обліковий запис, генеруються ключі безпеки, які потім переносяться на клієнтські ПК на медіа носіях (USB-flash). Після цього адміністрування клієнтів можливо тільки після взаємної аутентифікації і конфігурації. При використанні технології vPro в режимі enterprise використовуються протоколи шифрування TLS w / AES 128-bit або TLS w / RC4 128-bit, що значно підвищує рівень безпеки.

Режим Enterprise рекомендується для великих підприємств, оскільки передбачає велику трудомісткість і складність в розгортанні.

Завдяки технології vPro спрощується можливість адміністрування парку ПК сервісною службою, що знаходиться поза організацією (див. рис. 1.8):

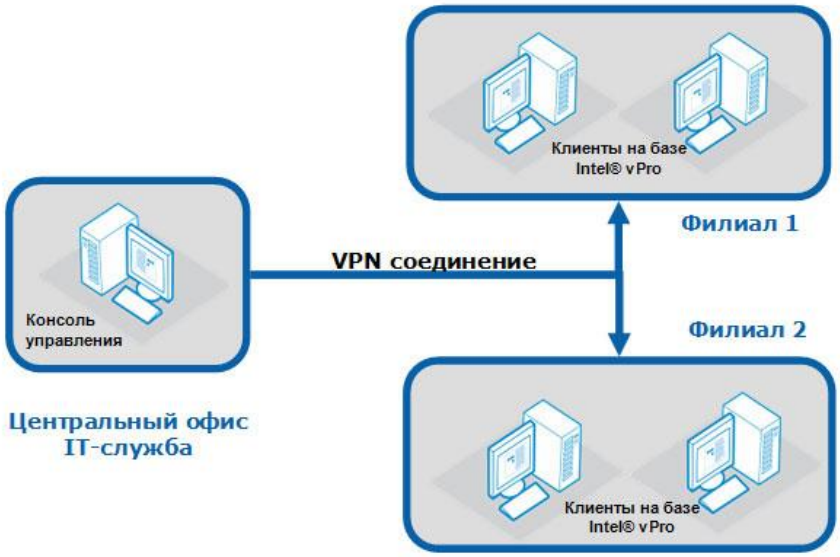


Рис. 1.8 – Парк ПК сервісної служби

Таким чином, інтегровані програмно-апаратні засоби vPro дозволяють централізовано вирішувати завдання на двох основних напрямках:

1. Управління:

- Віддалене завантаження з консолі управління;
- Віддалене управління ПК навіть при відсутності агентів управління;
- Енергонезалежний журнал подій (event log);
- Функції Serial over LAN та IDE-перенаправлення ;
- Налаштовується гнучка система оповіщень на основі апаратних датчиків платформи (повідомлення про несправності устаткування, зависання ОС і т. п.)

2. Безпека:

- Фільтрація вхідного і вихідного трафіку ОС;
- Ізоляція заражених ПК;
- Оновлення антивірусного і анти шпигунського ПО у віддаленому режимі.

Вартість ліцензії SyAM System Area Manager на сервер, що дозволяє реалізувати можливості vPro в розширеному обсязі, становить $ 179 і $ 39 на кожен настільний

ПК. Вартість альтернативного продукту LAN Desk Management Suite 105 $ на один керований пристрій.

Навіть без придбання спеціалізованого ПЗ (Системи централізованого управління з підтримкою iAMT) користувач комп'ютера Team Office b583V може скористатися перевагами технології vPro відразу "з коробки": в комплект поставки b583V входить пробна 14-ти денна версія SyAM System Area Manager (+ Client & Utilities), яка дозволяє оцінити можливості розширеного функціоналу vPro. Для тих же користувачів, які в даний момент не планують використовувати технологію vPro, її підтримка буде приємним "доважком", що не збільшує вартість Team Office b583V.

Технологія Intel vPro на ПК дозволяє скоротити навантаження на технічних фахівців завдяки можливості віддаленого моніторингу, діагностики та відновлення ПК навіть у ситуаціях, коли комп'ютер вимкнений або на ньому не працює операційна система. Крім того, переклад IT-інфраструктури на ПК з підтримкою vPro допоможе уникнути збільшення витрат, пов'язаних з підтримкою старого програмного і апаратного забезпечення, а також скоротити час простоїв системи. Нова енергоефективна конструкція дозволяє скорочувати витрати на електроенергію, а вбудовані засоби захисту допомагають знизити витрати на усунення загроз безпеки.

1.15 Програмно-апаратні функції новітніх версій AMT

Функціональні можливості AMT, починаючи з версії 6.0:

- Включення / вимикання / перезавантаження бізнес-комп'ютера, в т. ч. за розкладом;
- Базова інвентаризація HW (HardWare) на основі POST (Power On Self Test);
- Доступ до BIOS;
- Контроль роботи додатків бізнес-комп'ютера;
- Фільтри мережевої активності;
- Доступ до ПК за запитом користувача;
- Вбудований апаратний KVM (див. рис. 1.9).

Рис. 1.9 - Вбудований апаратний KVM

На відміну від заснованих на програмному забезпеченні рішень KVM, процесори Intel Core vPro з 2010 року дозволяють IT-персоналу отримати повний контроль над комп'ютерами для бізнесу. Апаратний KVM, починаючи з AMT 6.0, дає можливість технічному персоналу бачити інформацію на моніторі користувача, включаючи випадки краху ОС (так званий "блакитний екран смерті").

Вбудований апаратний KVM в складі AMT дозволяє службам технічної підтримки віддалено вирішувати такі завдання:

- Взаємодія з BIOS`ом під час перезавантаження комп'ютера. Персонал технічної підтримки може бачити зображення на екрані комп'ютера для бізнесу починаючи з повідомлень BIOS і може легко увійти в режим редагування як BIOS, так і ОС.

- Скидання паролів (в тому числі у BIOS), коли службовці забувають їх. Приблизно 60 відсотків запитів користувачів, пов'язані з шифруванням, відбуваються через необхідність введення пароля, який вони забули. Без віддаленого управління KVM скидання пароля може зайняти 25 - 40 хвилин. За нашою оцінкою, рішення цієї проблеми з KVM, зайняло б не більше трьох хвилин.

- Віддалене виконання стандартних налаштувань клієнта. Оскільки для цього потрібен повноекранний режим, тільки апаратний KVM дозволяє

дистанційно керувати комп'ютером для бізнесу, що було неможливо до появи процесорів Intel Core 2010 року. Це означає, що користувачі, при відсутності локальної підтримки, більше не повинні відправляти свої бізнес-комп'ютери в сервіс-центр і можуть повернутися до своєї роботи набагато швидше.

- Неправильне налаштування мережевого адаптера і пошкоджені або видалені системні файли. Як правило, в цих випадках телефонна розмова користувача з фахівцем технічної підтримки триває більше півгодини і не завжди з позитивним результатом. За допомогою віддаленого управління KVM інженер служби техпідтримки може взяти на себе керування машиною користувача та одразу ж побачити проблему на власні очі.

- Запуск комп'ютера і повноекранний режим самодіагностики. До появи процесорів Intel Core 2010 з віддаленим керуванням KVM, персонал служби техпідтримки в якості діагностичних інструментів був обмежений текстовими блоками, які не пропонували глибини і широти варіантів відновлення, доступних з інструментами повного екрану.

З застосуванням апаратних засобів віддаленого управління KVM з'являється можливість спростити обладнання робочих місць інженерів служби техпідтримки та знизити витрати на цю службу.

1.16 vPro, як частина Intel Stable Image Platform

Важливим моментом є й те, що технологія Intel vPro є частиною програми Intel Stable Image Platform. Програма гарантує доступність комплексу ПО та драйверів Intel протягом тривалого періоду часу з моменту випуску продукції.

1.17 Переваги експлуатації комп'ютерів для бізнесу з технологією Intel vPro + консоль управління

Проведенні дослідження, виявили наступні переваги:

- Скорочення втрат часу співробітників: при програмних несправностях - на 83-98%, при апаратних - на 65-70%;

- Скорочення кількості виходів на місце збою: при програмних несправностях - на 91%, при апаратних - на 56%;

- Скорочення часу на оновлення ПЗ: при установці на 1000 ПК - на 85%, для досягнення прийнятного рівня захисту - на 94%.

Таким чином, комп'ютери для бізнесу з технологією Intel vPro - це ПК, що володіють можливостями, які не зустрічаються в бізнес-ПК попередніх поколінь або програмних рішеннях. Комп'ютери з технологією Intel vPro надають те, що дійсно важливо для підприємствах:

- Скорочення витрат на IT-управління та захист ПК і даних за допомогою вбудованих технологій забезпечення інформаційної безпеки, що перешкоджають поширенню таких загроз, як віруси, мережеві черв'яки і інше шкідливе програмне забезпечення;
- Скорочення витрат на підтримку за допомогою вбудованих засобів управління, що дозволяють технічному персоналу дистанційно керувати системами і відновлювати їх навіть при непрацюючій ОС;
- Підвищена продуктивність системи дозволяє виконувати кілька бізнес-додатків, навіть в тих випадках, коли у фоновому режимі запущені завдання, щоб забезпечити управління системою та її інформаційну безпеку. Скорочення витрат на телефонні переговори і розширення можливостей зв'язку, використовуючи служби VoIP на ПК, спеціально оптимізованих для бізнесу.

ВИСНОВОК ДО РОЗДІЛУ 1

В цьому розділі були досліджені можливості технологій Intel® vPro™. Це платформа, що інтегрована в найновіші процесори фірми Intel. Вміле використання цієї платформи може забезпечити продуктивність бізнес-класу, апаратні засоби безпеки, сучасні можливості дистанційного керування та стабільність роботи.

РОЗДІЛ 2.

Розробка серверної платформи Moodle

2.1 Що таке Moodle?

Moodle (*Modular Object-Oriented Dynamic Learning Environment*, вимовляється «Мудл») - це модульне об'єктно-орієнтоване динамічне навчальне середовище, яке називають також системою управління навчанням, системою управління курсами, віртуальним навчальним середовищем або просто платформою для навчання, яка надає викладачам, учням та адміністраторам великий набір інструментів для комп'ютеризованого навчання, в тому числі дистанційного.

Тобто, ця платформа містить велику кількість різноманітних навчальних елементів (так званих «модулів»), які забезпечують діалог та співпрацю між викладачем та студентами. За допомогою платформи викладач може обирати будь-який з модулів, розміщувати його на сайті, редагувати, оновлювати, використовувати для інформування, навчання та оцінювання студентів. Платформа дозволяє використовувати в межах навчальної дисципліни форуми, слідкувати за активністю студентів, містить зручний для користування електронний журнал оцінок.

Moodle можна використовувати не лише в навчанні школярів, студентів, але також при підвищенні кваліфікації, бізнес-навчанні тощо. Moodle – це безкоштовна система, яка не потребує для своєї роботи жодного платного програмного забезпечення.

Обмежень щодо використання Moodle немає. Цю систему можна встановити на домашньому комп'ютері, в локальній мережі навчального закладу та глобальній мережі Інтернет.

2.2 Чи складно навчитись користуватись Moodle самостійно?

Навчитись використовувати Moodle самостійно нескладно. Для впевненого користувача комп'ютера система проста і зрозуміла навіть на інтуїтивному рівні.

Однак не зашкодить детальніше ознайомитися з її особливостями за допомогою спеціальної літератури та інтернет-ресурсів. Найкращим ресурсом є сайт Moodle, де можна знайти та завантажити навчальні матеріали українською мовою, наприклад про те як встановити Moodle на персональний комп'ютер, безкоштовно завантажити посібник для роботи з Moodle та ін. Для тих, хто добре володіє англійською мовою корисною буде книга Moodle for dummies («Мудл для початківців»), у якій просто і доступно пояснюються основні особливості роботи з цією платформою.

2.3 Як створити курс?

Для того, щоб створити курс достатньо увійти в Moodle та натиснути кнопку «Додати новий курс». В університетах є багато факультетів, тому процедура створення курсу буде складнішою. Зазвичай потрібно скористатись кнопкою «керування курсом», тоді відкриється перелік факультетів і кафедр. У цьому переліку потрібно буде знайти свій факультет і кафедру, а тоді вже скористатись кнопкою «Додати новий курс».

Після цього відкриється вікно з параметрами курсу, які необхідно заповнити.

Всі параметри поділені на групи:

- загальне;
- опис;
- формат курсу;
- вигляд;
- файли і завантаження;
- доступ для гостя;
- групи;
- перейменування ролі.

Особливої уваги заслуговує параметр «формат курсу», завдяки якому буде відображатися його зміст. Є чотири види формату курсу:

• *тижневий* – використовується, якщо навчання на курсі організовується потижнево, з точною датою початку та кінця, чітко визначеними строками;

• *тематичний* – розділяє курс на теми. Такий формат зручний для курсів, які тривають протягом семестру або навчального року;

• *форумний формат* – навчання проходить у вигляді форуму, який може оцінювати викладач;

• *формат єдиної діяльності* – на сторінці курсу буде показано тільки один елемент або ресурс.

2.4 Скільки часу займає розробка електронного курсу в Moodle?

Час необхідний для розробки навчального курсу в Moodle залежить від цілей та пріоритетів, які ставить перед собою розробник. Якщо є потреба у розробці повноцінного складного курсу, який буде включати лекційний матеріал, плани практичних занять, електронні ресурси, матеріали для самостійної роботи, тестові завдання тощо, то розробка може зайняти досить багато часу – від кількох тижнів (якщо є готові напрацювання, які здебільшого можна скопіювати), до кількох місяців (якщо усі матеріали потрібно розробляти з нуля).

У випадку обмеженого часу, коли потрібно швидко організувати дистанційне навчання, можна створити спрощений варіант курсу, робота над яким триватиме від кількох годин до кількох днів. При цьому не обов’язково одразу розміщувати усі модулі, спочатку достатньо розмістити лише найважливіші, які дозволяють надавати студентам навчальний матеріал та оцінювати їхню роботу. Кількість модулів у курсі можна поступово збільшувати, їхній зміст ускладнювати, змінювати способи оцінювання студентів та ін.

Позитивною рисою платформи є те, що модуль можна «приховати» на той час, поки він не завершений. У такому випадку його буде бачити лише викладач. Також модулі по наступних темах можна приховувати до тих пір, поки студенти не виконають завдання з попередніх тем. І лише після цього зробити їх видимими.

2.5 За допомогою яких модулів відбувається співпраця викладача з студентами?

Співпраця викладача зі студентами відбувається за допомогою двох типів модулів: «Види діяльності» та «Ресурси». Перша група модулів – *види діяльності* – передбачає можливість створення завдань для оцінювання студентів. Ці об’єкти надають можливості для спілкування зі студентами (наприклад, об’єкти «Форум», «Чат», «Зворотній зв’язок»), їхнього тестування (модуль «Тести»), виконання завдань, що передбачають завантаження файлів з результатами роботи (наприклад, модулі «завдання» чи «семінар»), розміщення елементів для спільної роботи (модуль «Вікі») та ін.

Ресурс у системі Moodle – це група об’єктів, які дозволяють додати до курсу будь-який вміст. Наприклад, це можуть бути веб-сторінки, текстові сторінки, написи, посилання на файли (модуль «Файл»), веб-сторінки (модуль «URL-веб посилання»), каталог із файлами (модуль «Тека»), текстові сторінки у форматі книги (модуль «Книга»).

Викладач сам обирає, які з цих об’єктів розміщувати на курсі, виходячи з мети та завдань навчальної дисципліни.

2.6 Як встановити Moodle на локальний комп'ютер

Moodle - переважно серверна платформа. Тільки сервер дозволяє без обмежень реалізувати весь потенціал системи, якщо не брати до уваги платні хостинги. У сервера сховище обмежена лише вашим місцем на диску, можна запрошувати скільки завгодно користувачів і впроваджувати будь-які розробки.

Табриця 1 – Мінімальні вимоги до ПК при встановленні Moodle

Мінімальні вимоги до сервера	**Встановлено такі бази даних**
Процесор: 2-х ядерний, 2ГГц; ОЗУ: 1 ГБ Місце на диску: 5ГБ	MySQL 5.6+ PostgreSQL 9.4+ MariaDB 5.5.31+ Microsoft SQL Server 2008+ Oracle Database 11.2+

Перед установкою потрібно переконатися, що комп'ютер відповідає мінімальним вимогам (див табл. 1).

Серверний формат підійде компаніям і установам, які хочуть створити локальне простір для навчання без інтернету. До такої Moodle зможуть підключитися лише користувачі з локальної мережі комп'ютера, на який встановлена система.

2.7 Що треба зробити для установки ?

Крок 1. Скачайте діструбітів Moodle

Установчий пакет можна завантажити з сайту Moodle. Всі версії можна знайти в розділі Downloads, підтримується як Windows, так і Mac OS. Безпечніше буде вибрати останню стабільну версію (Stable). Так ви завантажте інсталяційний архів на свій комп'ютер.

Крок 2. Розархівуйте дистрибутив окрему папку

Система готова до установки, але перед цим варто підготувати папку для файлів системи. Так ви зможете зберігати всі файли Moodle в одному місці.

Створивши папці, розархівуйте архів в неї.

Крок 3. Запустіть інсталятор

Запустіть Start Moodle.exe. Це відкриє cmd-вікно (інтерпретатор командного рядка Windows), і система зробить попередню настройку, як показано на рис. 2.1.

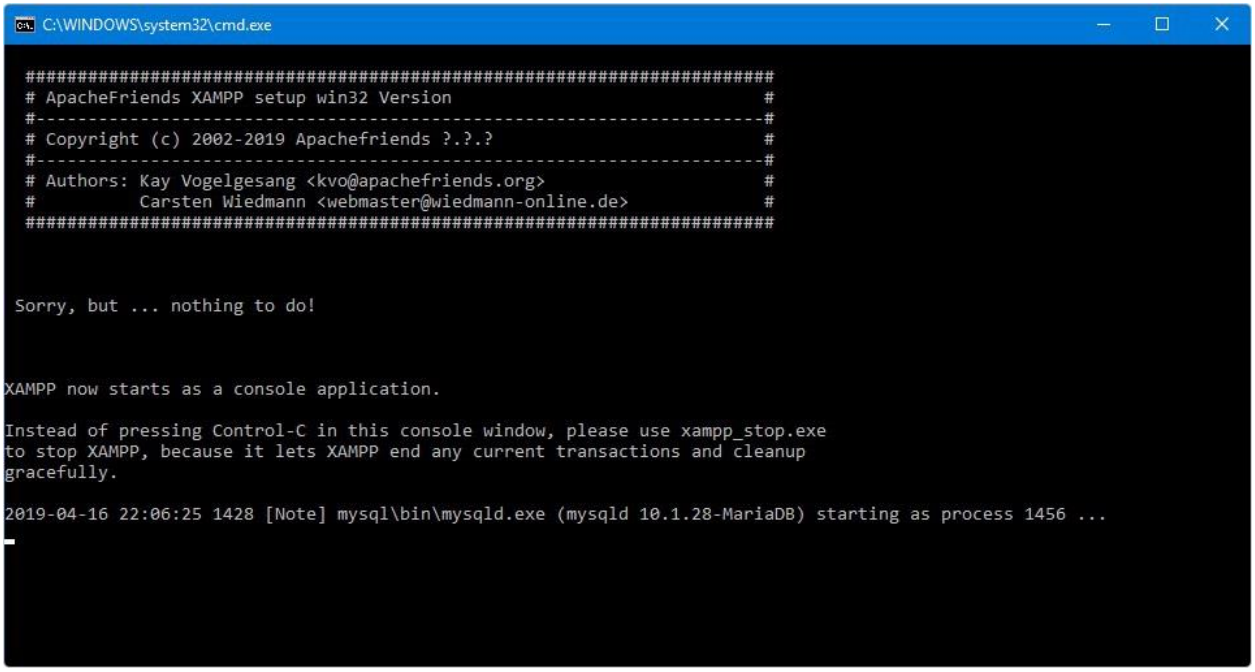


Рис. 2.1 – Вигляд cmd-вікна (інтерпретатор командного рядка Windows)

Крок 4. Відкрийте Moodle в браузері

Працювати в Moodle ви будете через браузер. Відкрийте улюблений браузер і наберіть localhost: це універсальний локальну адресу вашого комп'ютера, для цього не потрібно підключення до інтернету.

Крок 5. Встановіть Moodle

Встановіть Moodle, виконуючи вказівки в керівництві. Вас попросять придумати пароль і назву для бази даних, потім база даних почне генеруватися, а в кінці буде потрібно створити ім'я та пароль адміністратора, який стане першим користувачем платформи.

Moodle готова до роботи.

2.8 Що може початкова версія ?

Після установки ви потрапляєте на початкову сторінку Moodle. Це «нульова» система. Тут вже є деякі модулі, що дозволяють здійснювати базові дії, на кшталт створення курсів і записи користувачів, так що з нею вже можна працювати (див рис. 2.2).

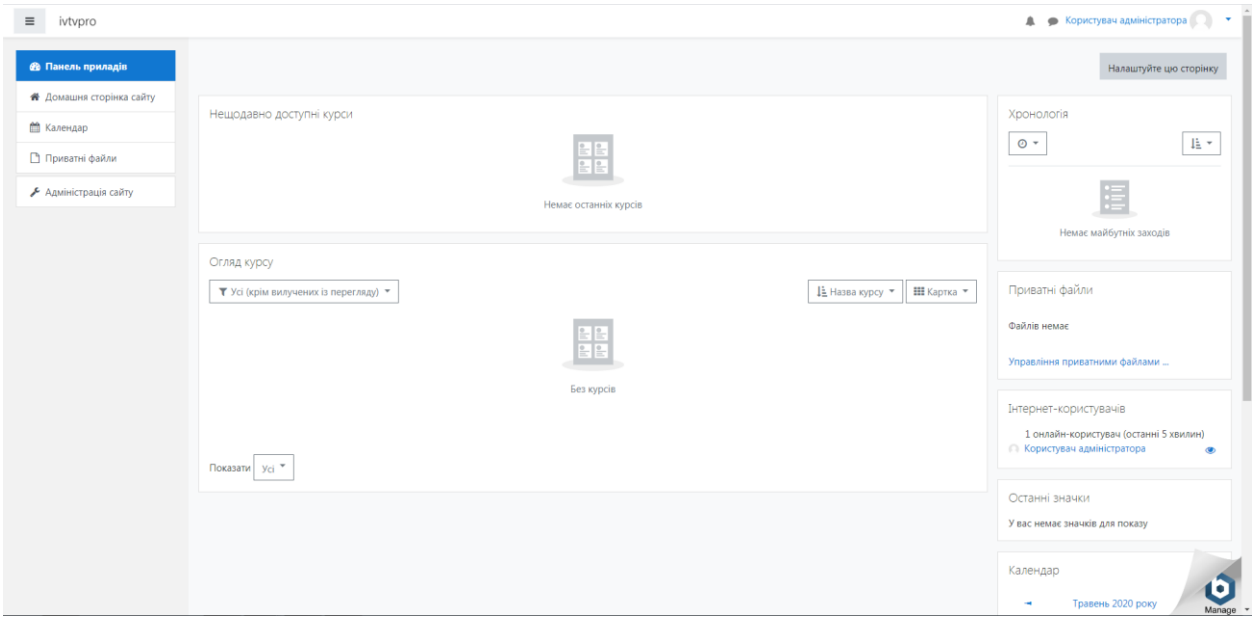


Рис. 2.2 – Початкова сторінка Moodle

Moodle повністю управляється через панель «Адміністрування». Функцій тут не так багато, але достатньо для першого встановлення. У «нульовий» Moodle можна:

- Створювати лекції, тести і завдання у вбудованому редакторі;
- Запрошувати і імпортувати користувачів, об'єднувати їх в групи, записувати їх на курси;
- Переглядати статистику активності на платформі.

Зміна дизайну, інтеграція з іншими сервісами, візуалізація звітів та інші функції настроюються за допомогою плагінів. Це архіви з настройками, які викачуються з інтернету і встановлюються на платформу. Наприклад, можна додати можливість влаштовувати вебінари, чого в «нульовий» Moodle немає.

2.9 Розробка серверної платформи для встановлення веб-серверу Moodle.

Можливі два підходи до розміщення веб серверу Moodle: використовувати або власний веб сервер, або ж розмістити його на хостингу. Розміщення на хостингу це більш дешевий варіант, але якщо у організації чи компанії є потреба в розміщені також і інших серверів, крім сервера Moodle, то більш доцільним і солідним є використання власного сервера.

За допомогою спеціального ПЗ в сервер можливо перетворити любий ПК. Таким шляхом зазвичай і обмежуються невеликі організації. З ростом популярності веб ресурсу і збільшенням його користувачів в Інтернет все замітніше будуть обмеження такого технічного рішення. У зв'язку з цим, для розгортання веб серверу Moodle є більш доцільним використання спеціалізованого комп'ютера, в котрому для якісного функціонування інформаційної системи в масштабі Інтернет використовується ряд особливих рішень. Такими рішеннями є, відмовостійкість, масштабованість, підвищена надійність та функціональне керування. Тільки повноцінний сервер може забезпечити одночасне і швидке обслуговування великої кількості користувачів.

Неможливо розробити сервер, котрий міг би задовільнити одночасно велику кількість його потенційних користувачів, бо в залежності від фінансового стану компанії, вона може виставляти різні вимоги до основних характеристик сервера. У зв'язку з цим було прийнято рішення розробити не сервер, а серверну платформу.

Серверна платформа - це рішення сервера, що має максимально можливу гнучкість. Її корпус повинен не тільки мати стоїчне виконання, але також мати максимально можливу гнучкість по встановленню всіх необхідних компонентів на визначені для них місця. При цьому блок живлення повинен відрізнятися підвищеною надійністю та широким розкидом параметрів по електричній мережі. Оптимальним чином повинна бути продумана вентиляція корпусу.

Відносно до ТЗ, сформуємо завдання по розробці серверної платформи таким чином, щоб серверна платформа могла задовільнити як найбільшу кількість потенційних користувачів:

- Вибрати необхідне обладнання для збирання сервера в наступному складі: 2 процесора типу Intel Xeon; оперативна пам'ять - 64 GB з можливістю

розширення до 128 GB; відеоадаптер – інтегрований; дискові накопичувачі - не гірше, ніж SAS 4TB 7200RPM rpm; контролер SAS - не менш ніж 8 каналів з можливістю побудови RAID 0, 1, 5, 6 и 10; мережний контролер –1 Gb/s; серверний корпус rackmount (висота – не більше 2U); два блока живлення з функцією «гарячої» заміни (1 основний + 1 резервний); резервування системних вентиляторів, можливість здійснення «гарячої»» заміни системних вентиляторів; монтажний комплект – телескопічний комплект для монтажу сервера в стойку/шафу.

- Виконати розрахунок потрібної потужності блоків живлення.

Основою розроблюваної платформи є процесори та материнська плата. Найсучаснішим рішенням є використання нового сімейства серверних процесорів фірми Intel: Xeon Gen 2 Bronze, Silver, Gold, або Platinum. В якості материнської плати була вибрана Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2), що може містити 2 таких процесори. Вона продається, як окремо, так і вже вбудованою в серверний корпус Lenovo ThinkSystem SR650. Все обладнання серверної платформи зведено в табл. 2.1.

Таблиця 2.1 – Обладнання серверної платформи.

Тип компонента	Назва	TDP, Вт	Ціна (у. о.)
Процесори	2 x Xeon Gen 2 Bronze, Silver, Gold, або Platinum: • Від 16 до 56 ядер (з частотою від 1.9 GHz до 4.5 GHz); • Кількість потоків від 32 до 112; • Загальний розмір кеш LLC 22MB -77MB.	170 - 330 W	600-7900
Материнська плата	Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2)	60W	790

	• RAID 0/1/10/5/50/6/60		
Тип компонента	Назва	TDP, Вт	Ціна (у.о.)
Оперативна пам’ять	4, 8 x 16GB Optane 2666 MT/s, DDR4	4,8 - 9,6 W	1260-2520
Дискові накопичувачі	2, 4, 6, 8 x Dell 2.4TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drive	7.8 W x 2, 4, 6, 8	1412-11296
Корпус	Lenovo ThinkSystem SR650 2U	-	1200
Блоки живлення	2x hot swap/redundant 750W PLUS Platinum	-	300
Кулери	6x be quiet! BL067	15 W	180
Операційна система	Microsoft Windows Server 2019		230
Сумарно	-	265,4-477W	5972-24416

Зовнішній вигляд корпусу Lenovo ThinkSystem SR650 показаний на рисунку 2.3.

Рис. 2.3 - Зовнішній вигляд корпусу Lenovo ThinkSystem SR650

На рисунку 2.4 приведена структурна схема материнської плати Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2).

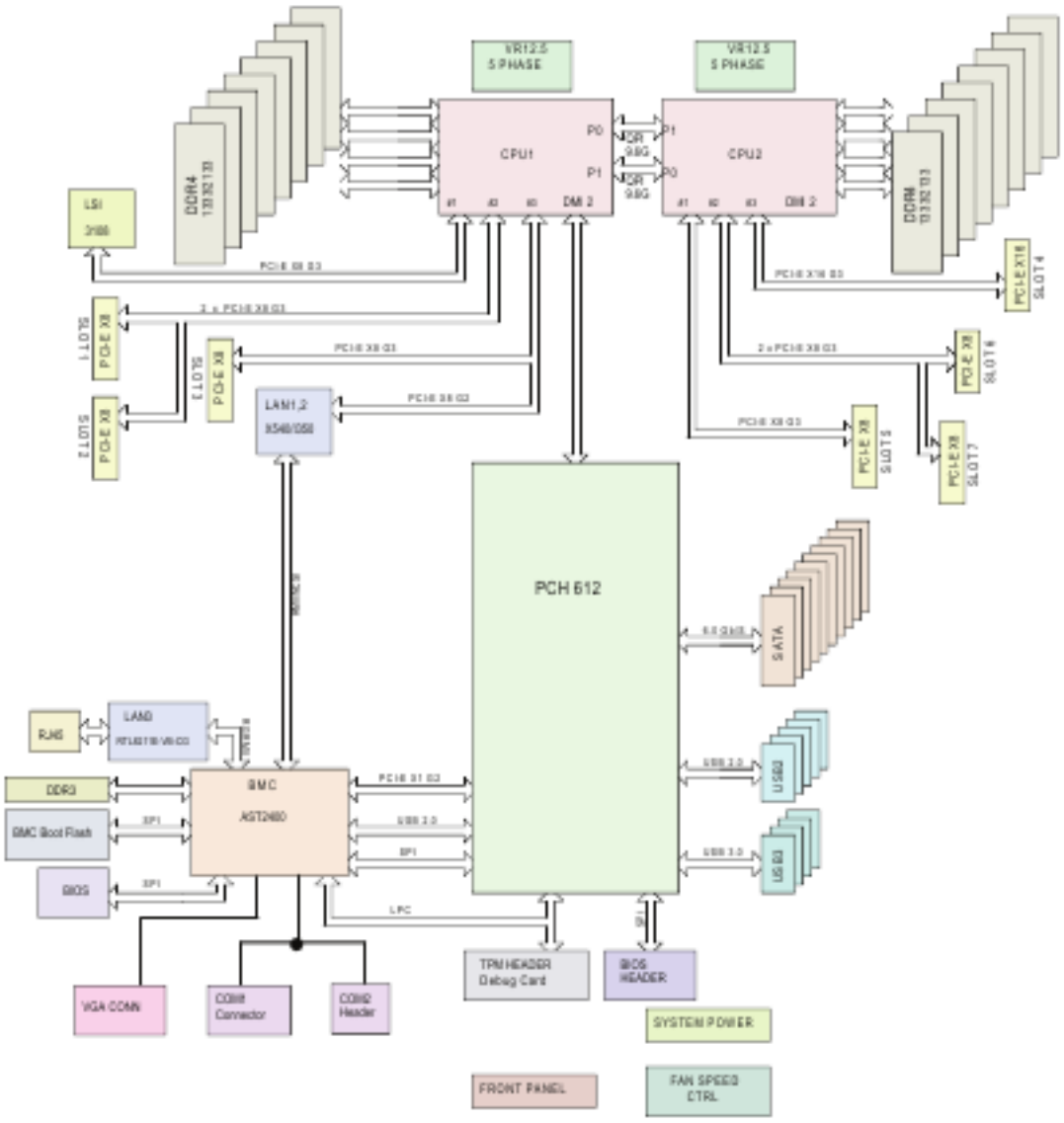


Рис. 2.4 - Структурна схема материнської плати Lenovo ThinkSystem SR650 Server (Xeon SP Gen 2)

ВИСНОВОК ДО РОЗДІЛУ 2

В цьому розділі було зібрано та систематизовану всю необхідну інформацію для створення програмних засобів навчання системних адміністраторів використанню можливостей технологій Intel® vPro™: Intel Virtualization Technology, розроблена серверна платформа Moodle, встановлено необхідне програмне забезпечення для реалізації учбового курсу на розробленій платформі.

РОЗДІЛ 3

Можливості технології Intel® Virtualization Technology VT-d

3.1 Призначення технології Intel VT-d.

Для створення віртуальних машин (або гостей) монітор віртуальної машини (VMM) aka гіпервізор виступає в якості хоста і має повний контроль над апаратним забезпеченням платформи. VMM представляє гостьове програмне забезпечення (операційну систему та прикладне програмне забезпечення) з абстракцією фізичної машини і здатне зберігати вибіркове управління ресурсами процесора, фізичною пам'яттю, керуванням перериваннями та введеннями / виведеннями даних.

VMM підтримує віртуалізацію запитів вводу / виводу від гостьового програмного забезпечення. Це робиться в програмному забезпеченні, використовуючи будь-яку з двох відомих моделей: Емуляція пристроїв або Паравіртуалізація. Загальна вимога надійності та захисту для цих або будь-яких моделей віртуалізації пристроїв вводу / виводу - це можливість ізолювати та містити доступ до пристрою лише до тих ресурсів, які призначені пристроєм VMM.

Intel VT-d - це остання частина апаратної архітектури Intel Virtualization Technology. VT-d допомагає VMM краще використовувати апаратне забезпечення за рахунок поліпшення сумісності та надійності додатків та надання додаткових рівнів керованості, безпеки, ізоляції та продуктивності вводу / виводу. Використовуючи апаратну допомогу VT-d, вбудовану в чіпсети Intel, VMM може досягти більш високого рівня продуктивності, доступності, надійності, безпеки та довіри.

Технологія віртуалізації Intel® для спрямованого вводу / виводу надає програмному забезпеченню VMM такі можливості:

- Підвищити надійність та безпеку за допомогою ізоляції пристрою, використовуючи апаратне допоміжне переміщення;
- Поліпшення продуктивності та доступності вводу / виводу шляхом прямого призначення пристроїв.

3.2 Забезпечення апаратним розподіленням для захисту

Intel VT-d забезпечує захист, обмежуючи прямий доступ до пам'яті (DMA) пристроїв до попередньо призначених доменів або областей фізичної пам'яті. Це досягається за рахунок апаратних можливостей, відомих як переназначення DMA. Логічна апаратна логіка для перезавантаження VT-d у чіпсеті знаходиться між периферійними пристроями вводу / виводу, що працюють через DMA, та фізичною пам'яттю комп'ютера. Вона працює під керуванням системного програмного забезпеченням комп'ютера system. У середовищі віртуалізації системним програмним забезпеченням є VMM. У рідному середовищі, де немає програмного забезпечення для віртуалізації, системне програмне забезпечення є нативним ОС. Переназначення DMA переводить адресу вхідного запиту DMA на правильну адресу фізичної пам’яті та здійснює перевірку дозволів на доступ до цієї фізичної адреси на основі інформації, наданої системним програмним забезпеченням.

Intel VT-d дозволяє системному програмному забезпеченню створювати кілька доменів захисту DMA. Кожен домен захисту - це ізольоване середовище, що містить підмножину фізичної пам'яті хоста. Залежно від моделі використання програмного забезпечення, домен захисту DMA може представляти пам’ять, виділену віртуальній машині (VM), або пам'ять DMA, виділену драйвером гостьової ОС, що працює в VM або як частина самого VMM. Архітектура VT-d дозволяє системному програмному забезпеченню призначати один або декілька пристроїв вводу / виводу до захисного домену. Ізоляція DMA досягається обмеженням доступу до фізичної пам'яті домену захисту від пристроїв вводу-виводу, не призначених їй, за допомогою таблиць трансляції адрес. Це забезпечує необхідну ізоляцію для забезпечення розділення між комп'ютерними ресурсами кожної віртуальної машини.

Коли будь-який даний пристрій вводу / виводу намагається отримати доступ до певного місця пам'яті, апаратне забезпечення для перезавантаження DMA шукає таблиці перекладу адрес для дозволу доступу цього пристрою до цього конкретного домену захисту. Якщо пристрій намагається отримати доступ поза межами діапазону, до якого йому дозволено отримати доступ, апаратне забезпечення для

перезавантаження DMA блокує доступ та повідомляє про помилку програмному забезпеченню системи, як показано на рис. 3.1.

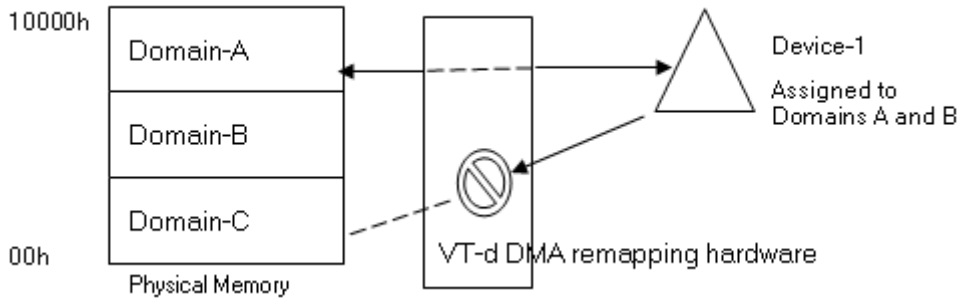


Рис. 3.1 – Повторне відтворення DMA VT-d. Пристрій-1 не призначений для Domain-C, тому коли він намагається отримати доступ до цього діапазону, він обмежується апаратним забезпеченням VT-d.

3.3 Підвищення продуктивності вводу / виводу за допомогою прямого призначення

Віртуалізація дозволяє створювати на одному сервері кілька віртуальних машин. Ця консолідація максимально використовує апаратне забезпечення сервера, але серверні програми вимагають значної продуктивності вводу / виводу. На основі програмного забезпечення методів віртуалізації вводу / виводу використовується емуляція пристроїв вводу / виводу. За допомогою цього рівня емуляції, VMM забезпечує послідовний вигляд апаратного пристрою для VM, і пристрій може бути спільним для багатьох віртуальних машин. Однак це також може сповільнити продуктивність пристроїв вводу / виводу. VT-d може вирішити втрату нативної продуктивності або природних можливостей віртуалізованого пристрою вводу / виводу шляхом безпосереднього присвоєння пристрою VM.

У цій моделі VMM обмежується функцією керування для включення прямого присвоєння пристроїв своїм розділам. Замість виклику VMM для всіх (або більшості) запитів вводу / виводу з розділу, VMM викликається лише тоді, коли гостьове програмне забезпечення має доступ до захищених ресурсів (таких як доступ до конфігурації вводу-виводу, управління перериванням тощо), які впливають на функціональність системи та ізоляцію.

Для підтримки прямого призначення пристроїв вводу / виводу у VM, VMM повинен забезпечити ізоляцію запитів DMA. Пристрої вводу / виводу можуть бути призначені доменам, а апаратне перезавантаження DMA може використовуватися для обмеження DMA з пристрою вводу / виводу до фізичної пам'яті, яка зараз належить його домену.

Коли VM або гість запускається над VMM, адресний простір, який надається гостьовій ОС як фізичний діапазон адрес, відомий як фізична адреса гостя (GPA), не може бути такою, як реальна фізична адреса хоста (HPA) . Пристрої, що підтримують DMA, потребують HPA для передачі даних до та з фізичної пам'яті. Однак у моделі прямого присвоєння гостьовий драйвер пристрою ОС керує пристроєм і надає GPA замість HPA, необхідного пристрою, сумісному з DMA. Для відповідного перетворення можна використовувати апаратне перезавантаження DMA. Оскільки GPA надається VMM, він знає перехід від GPA до HPA. VMM програмує обладнання для перезавантаження DMA з інформацією про перетворення GPA в HPA, щоб апаратне забезпечення для перезавантаження DMA могло виконати необхідну трансляцію. За допомогою перенастроювання, дані тепер можна передавати безпосередньо у відповідний буфер гостей, а не проходити через проміжний емуляційний рівень програмного забезпечення.

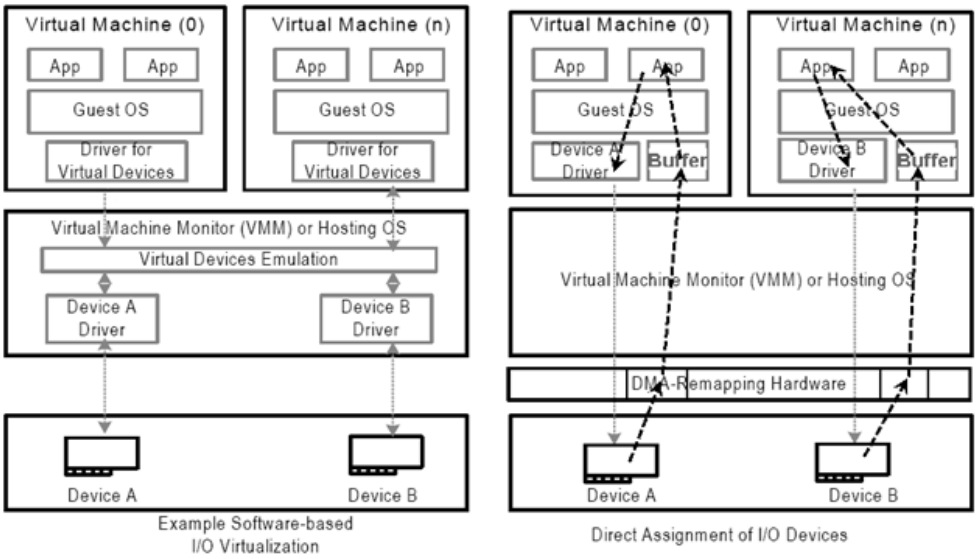


Рис. 3.2 - Введення-виведення на основі програмної емуляції і апаратне введення-виведення з прямим призначенням.

Рисунок 3.2 ілюструє програмне введення / виведення на основі емуляції програмного забезпечення порівняно з апаратним прямим призначенням на основі вводу / виводу В емуляції на основі вводу / виводу проміжний програмний рівень управляє всім введенням / виводом між VM та пристроєм. Дані передаються через рівень емуляції до пристрою та від пристрою до рівня емуляції.

У моделі прямого присвоєння немодифікований гостьовий драйвер ОС керує пристроєм, якому він призначений. На шляху прийому апаратне забезпечення для перезавантаження DMA перетворює GPA, наданий гостьовим драйвером ОС, у правильний HPA, таким чином, що дані передаються безпосередньо в буфери гостьової ОС (замість того, щоб проходити через рівень емуляції). Підтримка перестановки переривання в архітектурі VT-d дозволяє керувати перериванням також безпосередньо присвоюватися VM, додатково зменшуючи накладні витрати VMM.

3.4 Моделі використання Intel VT-d

Увімкнені ОС та VMM можуть використовувати функціонал VT-d управління пам'яттю вводу / виводу для ізоляції пристроїв до доменів захисту, що не дозволяють пристроям виконувати будь-які деліктні DMA, які можуть вплинути на функціонування системи.

VT-d може стати основою для створення захищених та ізольованих робочих розділів на серверах, робочих станціях та новому класі комбінованих пропозицій апаратного та програмного забезпечення під назвою віртуальні пристрої. Віртуальний прилад - це автономне рішення середовища виконання, оптимізоване для заздалегідь заданого набору додатків та / або служб, таких як пристрій для сканування вірусів і брандмауер або апаратний апарат управління.

Віртуальні машини у віртуальному середовищі можуть бути розділені на різні області захисту від кінця програми до кінця пристрою. Таким чином, проблема з одним пристроєм вводу-виводу в одному домені ізольована від впливу на інші домени та забезпечує ІТ-користувачам кращу надійність системи та час роботи.

Середовища випробувань та розробок, що використовують сервери з декількома широкоформатними віртуальними машинами, робочі станції з декількома спільно існуючими ОС, що працюють у віртуалізованих середовищах, все може отримати вигоду з ізольованих робочих розділів.

3.5 Моделі використання сервера

Багато серверних додатків є інтенсивним введенням / виведенням, особливо для мереж та зберігання. Основні вимоги вводу / виводу в центрі обробки даних - масштабованість та продуктивність. Вони забезпечують консолідацію сервера, надійність та доступність, оскільки критично важливі програми переміщуються на віртуалізовані сервери та інфраструктури центрів обробки даних.

3.6 Підвищення продуктивності

Віртуалізація дозволяє консолідувати робочі навантаження на недостатньо використаний сервер. У міру збільшення обсягу робочих навантажень вимоги щодо використання вводу / виводу та пропускної здатності збільшуються, а продуктивність вводу / виводу може стати вузьким місцем. Для підвищення продуктивності виділений високопродуктивний пристрій вводу / виводу може бути призначений безпосередньо VM, який потребує підвищення продуктивності вводу / виводу. Віртуалізація вводу / виводу на базі Intel VT-d дозволяє високопродуктивним пристроям вводу / виводу, таким як багатопортовий гігабіт і 10-гігабітовий мережевий адаптер, призначатися певним VMs, де продуктивність вводу-виводу є критичною, без побоювань, що інші VMs на платформі вплине на їх роботу. Intel є активним учасником специфікації віртуалізації вводу / виводу, керованої PCI-SIG, яка працює над тим, щоб мати один пристрій, що використовувався в основному серед декількох віртуальних машин.

3.7 Підвищення надійності і безпеки - власна ОС і консолідація серверів

Зростає використання декількох пристроїв вводу / виводу на консолідованих віртуалізованих серверах: до чотирьох мережевих пристроїв на віртуалізованому

сервері не рідкість. Intel VT-d може допомогти VMM покращити надійність та безпеку, виділивши ці пристрої в захищені домени.

Керуючи доступом пристроїв до певних діапазонів пам'яті, VMM може домогтися ізоляції від кінця до кінця (VM для пристрою). Це допомагає підвищити безпеку, надійність та доступність.

Ізоляція пристрою може бути досягнута і в невіртуальних платформах. Розробники драйверів пристроїв можуть використовувати ізоляцію пристрою до певних діапазонів пам'яті для налагодження апаратного забезпечення або DMA драйвера пристрою, який отримує доступ до небажаних діапазонів пам'яті.

3.8 Обхід умов "Буфер відмов"

Системне програмне забезпечення, що використовує Intel VT-d для перекомпонування можливостей DMA, покращує продуктивність, уникаючи умов буфера. Коли буфери відмов використовуються між 32-розрядним пристроєм, що виконує DMA, і фізичним діапазоном пам'яті, який недоступний через обмеження 32-бітної адреси, програмне забезпечення системи може використовувати можливість перенаправлення даних Intel VT-d DMA для перенаправлення даних у верхню пам'ять, а не виконання буферних копій.

3.9 Моделі використання клієнтів

Технологія віртуалізації Intel® (Intel® VT) дозволяє розгорнути автономні віртуальні пристрої від сторонніх постачальників для виконання життєво важливих служб безпеки та управління для таких заходів, як глибока перевірка пакетів та дотримання політики на настільних ПК із технологією Intel® vPro ™. Ці віртуальні пристрої, захищені від несанкціонованого захисту, забезпечують більш безпечне та стабільне середовище для критичних послуг та включають все необхідне програмне забезпечення в єдиний пакет для більшої зручності та ефективності. Використання VT-d з розділом послуг або керованого розділу забезпечує ізольоване, контрольоване та захищене середовище для підтримки клієнтської платформи, забезпечуючи захист пам’яті та оптимізацію вводу / виводу для віртуальних машин.

3.10 Віртуальний прилад на базі VT-d

Віртуальний пристрій - це автономне середовище віртуального виконання, оптимізоване до заздалегідь заданого набору додатків та / або послуг. Легкий монітор віртуальної машини (LVMM) - це монітор віртуальної машини (VMM), що використовує Intel VT для розділення клієнтської платформи на два середовища виконання. Один - це VM користувача, який може запускати ОС, наприклад Windows 10, та додатки, необхідні користувачеві, такі як програми для відео чи рендерінгу, програми для розробки та тестування та типові офісні програми. Другий - сервісний розділ (або Service VM), який запускає службову ОС (SOS) в ізольованому середовищі виконання. У розділі користувача є всі пристрої платформи, крім (у цьому прикладі) контролерів мережевого інтерфейсу. Їм належить сервісний розділ, який надає можливість контролювати та / або фільтрувати мережевий трафік та віртуалізувати мережеві пристрої для інших віртуальних машин на клієнтській платформі. Програми управління, що працюють у розділі служб, надають віддаленій консолі можливість адмініструвати клієнтську систему в ізоляції від решти платформи та середовища користувача.

Архітектура, що зображена на рисунку 3.3, показує, що мережевий трафік протікає через драйвер фізичної інтерфейсної картки (NIC), що належить службовому розділу. Потім драйвер мосту маршрутизує пакети між стеком мережі розділів послуг та стеком мережі розділів користувача. У розділі користувача віртуальний драйвер NIC посилає всі вихідні пакети з розділу користувача драйверу мосту, а драйвер мосту пересилає їх у фізичний NIC.

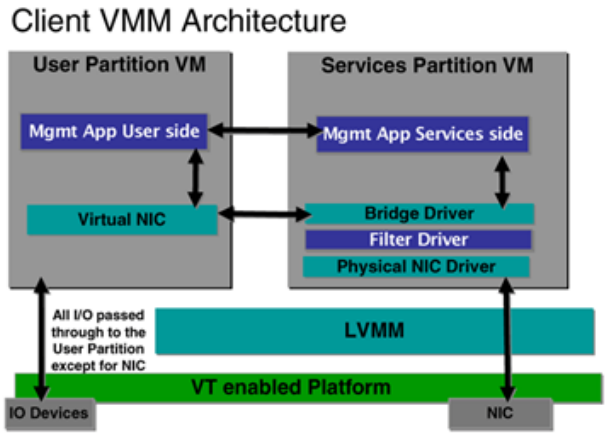


Рис. 3.3 - Архітектура VMM клієнта.

Ця мережева архітектура забезпечує більш високий рівень захисту від шкідливого мережевого трафіку. Це також створює можливість ізолювати шкідливі атаки на один розділ та призначені йому ресурси за допомогою використання VT та VT-d. VT-d створює основу для нового класу додатків, заснованих на архітектурі «Virtual Appliance». Він працює краще, ніж схема віртуалізації, яка виставляє модель пристрою NIC до розділу користувача. У цій схемі всі користувацькі розділи доступу до пристрою NIC перехоплюються та імітуються для захисту від розповсюдження шкідливого коду.

LVMM і сервісний розділ повинні бути захищені від пристроїв, що управляють шиною DMA, відображених на розділі користувача. Ці пристрої, що підтримують DMA, можуть отримувати доступ до всієї системної пам’яті та можуть навмисно чи ненавмисно отримувати доступ (читати / записувати) сторінки пам'яті, на яких розміщуються код LVMM та розділи служб та структури даних. Такий доступ може призвести до компрометації IT-секретів або зробити платформу марною від пошкодження пам'яті. VT-d використовується для запобігання цих проблем з DMA пристрою.

Як було сказано раніше, VT-d дозволяє два перегляди системної пам'яті: фізична адреса гостя (GPA) та фізична адреса хоста (HPA). LVMM зберігає вигляд HPA, фізичний адресний простір системи та розділи користувачів та служб надаються відповідним представленням GPA. LVMM підтримує таблиці тіньових сторінок для

трансляції GPA на HPA для доступу з процесора. Аналогічно, використовуючи перезавантажувальні двигуни VT-d DMA та відповідні таблиці трансляції, LVMM підтримує відображення GPA-HPA для всіх пристроїв вводу / виводу, здатних DMA. Рисунок 3.4 ілюструє цю модель використання.

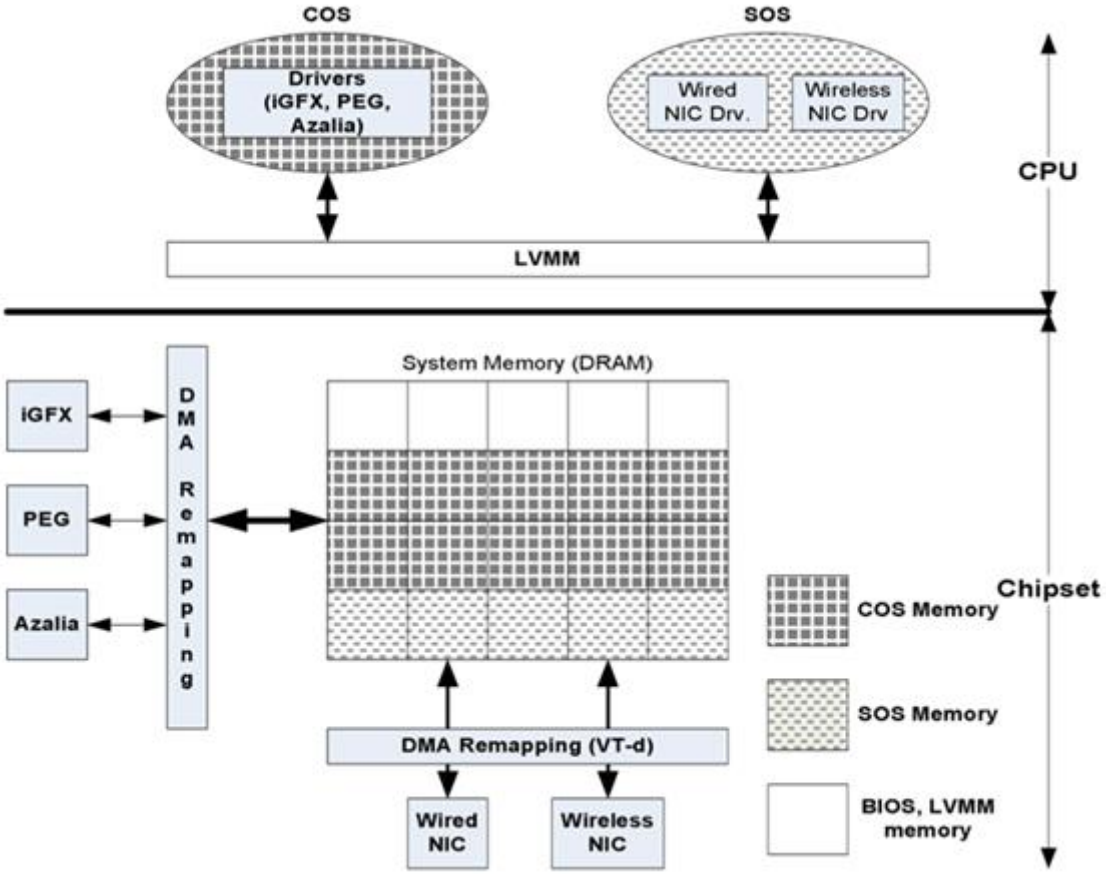


Рисунок 3.4 - Модель використання VT-d у клієнтській VMM.

Відображення DMA виконується наступним чином:

- Всі сторінки пам’яті розділів служби додаються в один домен, таким чином, лише ті пристрої DMA, які відображені в розділі служб (NIC), можуть отримати доступ до цих сторінок.
- Усі решта сторінок (крім LVMM та BIOS зарезервовані) додаються до домену розділів користувача, і всі пристрої, крім тих, які відображені на розділі служб, можуть отримувати доступ до цих сторінок (наприклад, картки додатків iGFX, PCI / PCIe тощо).
- Зарезервовані регіони LVMM та BIOS захищені від доступу до DMA через відсутність у таблицях сторінок перекладу VT-d.

Це картографування пристрою до домену має такі переваги:

- Пристрої вводу / виводу, відображені на одному домені, не можуть отримати доступ до пам'яті іншого домену. Наприклад, картки розширень PCI / PCIe в розділах користувачів не можуть отримати доступ до LVMM або сервісного розділу.
- Драйвери пристроїв у службах та розділах користувачів запускаються без змін, щоб зрозуміти відображення GPA-HPA. Ця трансляція прозоро виконується апаратним забезпеченням VT-d, коли пристрій видає запит вводу / виводу за допомогою GPA.
- Якщо пристрій погано поводиться, намагаючись отримати доступ до адреси за межами відображеного домену, апарат VT-d генерує помилку. Ця несправність фіксується LVMM і вказує на сервісний розділ. Необов'язковий додаток управління в розділі послуг може обробляти ці помилки, вживаючи відповідних дій, таких як показ повідомлення про помилку або ініціювання перезавантаження платформи, залежно від тяжкості несправності.

3.11 Використання VT-d у моделях використання клієнтів.

ІТ-відділи стикаються з багатьма проблемами в управлінні активами і, водночас, підтримці безпеки. Ось кілька прикладів використання VT-d у моделях використання клієнтів.

3.11.1 Ізоляція та відновлення клієнта

ІТ-підрозділи виграють від можливості ізолювати ключові керовані послуги та служби безпеки від доступу кінцевих користувачів, зберігаючи однаковий рівень гнучкості та продуктивності послуг для кінцевих користувачів. Служби управління та безпеки ізольовані до віртуального пристрою управління або сервісного розділу, отже, захищаючи ІТ-сервіси. Ще одна перевага користувачів і розділів служб полягає в тому, що якщо в користувацькому розділі виникне критична проблема, сервісний розділ або ІТ-розділ має можливість віддаленого та незалежного відновлення розділу користувача.

3.11.2 Кінцева точка контролю доступу

Використання VT-d для віртуалізації пристроїв дозволяє забезпечити більш безпечний контроль доступу до кінцевої точки (EAC - Network Access Control). Це дозволяє підвищити захист доступу клієнтів до підприємства, створюючи кращу керованість точок доступу. Підприємство визначає параметри прийнятності, виражені у формі політики доступу. Політика тлумачиться пунктом рішення про політику (PDP), який контролює точки виконання політики (PEPs), які контролюють доступ. Контроль доступу може включати будь-яке з наступного:

- Необмежений доступ.
- Умовний доступ на основі фільтрації трафіку.
- Обмежений доступ там, де доступні лише конкретні ресурси.

EAC дотримується методології, яку можна розділити на наступні загальні етапи:

- Збір - моніторинг, зчитування та зберігання вимірювань безпеки клієнтської системи.
- Звітність - форматування зібраних вимірювань для споживання PDP.
- Оцінка - тлумачення звітів та організаційної політики.
- Забезпечення виконання - застосовує правила контролю доступу.
- Усунення - застосовуються правила конфігурації, призначені для приведення платформи у відповідність.

3.11.3 Стримування спалаху

ІТ-відділи продовжують стикатися з проблемою, що містить уразливі місця. Віруси можуть входити на ПК та намагатися отримати доступ до конфіденційних даних або пошкодити їх чи можуть поширюватися по всьому підприємству. Захист від спалаху забезпечує стримування загрози після її виявлення. Intel® VT і VT-d можуть допомогти виявити та містити віруси швидше, обмежуючи експозицію в атакованих системах, а також інших підключених системах. Процес завантаження Virtual Appliance або Service Partition контролюється, щоб запобігти завантаженню

пошкодженого або несанкціонованого програмного забезпечення, якщо інша VMM, програма Virtual Appliance, драйвери або ОС намагаються завантажити. Отже, пошкоджений розділ можна зупинити та повідомити IT, дозволяючи завантажувати некорумповане середовище, ОС та SW.

Пошкоджений розділ може бути переключений на приватну мережу для полегшення виправлення або, за відомим сценарієм загрози; клієнт оновлюється патчем, щоб захистити його від спалаху. При більш серйозній ситуації клієнт може вимкнутись для захисту його та іншої мережі.

3.12 Наслідки для безпеки VT-d

На ПК створені надійні розділи та захист пам’яті, що дозволяє компаніям та IT краще захищати конфіденційні дані. Віртуальний пристрій або сервісний розділ управляє декількома захищеними розділами та полегшує надійне передавання інформації на основі потреб та політик бізнес-сегменту, створює безпечніше середовище виконання та вдосконалює можливості виявлення та запобігання атакам.

Системи з підтримкою VT та VT-d дозволяють завантажувати лише код, затверджений IT-персоналом. Якщо в системі присутній код зловмисного програмного забезпечення, процедура завантаження, підтверджена IT, виявить модифікацію та застосує відповідне виправлення, таке як перезавантаження безпечного резервного копіювання віртуального зображення.

Мережеві атаки протидіють моніторингу сторінок пам'яті, які не повинні змінюватися. Агенти моніторингу повідомляють VMM про спробу недійсного доступу до сторінки, і VMM може реагувати, блокуючи такі звернення. Агенти цілісності самі захищені межею VM, де прямий доступ між розділами заборонений.

Механізми захисту IT базуються на здатності створювати ізольовані середовища виконання, які менш сприйнятливі до атак. Технологія Intel VT і VT-d є важливою для створення таких надійних середовищ, які можуть діяти у разі зловмисної атаки або збоїв у апаратному забезпеченні.

ВИСНОВОК ДО РОЗДІЛУ 3

Архітектура VT-d забезпечує апаратні механізми для побудови віртуалізованого середовища з повною ізоляцією передачі даних на пристрій введення / виведення. Це дає змогу створити віртуальне середовище з більшою доступністю, надійністю та безпекою. За допомогою VT-d розробники програмного забезпечення можуть розробляти та розвивати свої архітектури, які забезпечують повний захищений обмін ресурсами вводу / виводу.

Підтримка VT-d на платформах Intel для віртуалізації пристроїв вводу / виводу доповнює існуючі можливості Intel VT для віртуалізації процесорних ресурсів та ресурсів пам'яті. Разом ця дорожня карта технологій VT пропонує повне рішення для забезпечення повної апаратної підтримки для віртуалізації платформ Intel. Віртуалізація ресурсів вводу / виводу є важливим кроком до створення значного набору нових моделей використання в центрі обробки даних, на підприємстві та вдома.

РОЗДІЛ 4.
Використання можливостей технологій VT-d в Xen та VT-x

VT-d - технологія віртуалізації введення / виведення, запропонована Intel. Ця технологія дозволяє забезпечити монопольне виділення пристрою HVM-домену, в той час як без її допомоги (або аналогічної технології IOMMU від AMD) це можливо тільки для паравіртуальних доменів.

В цьому розділі докладніше розглядаються питання застосування технології VT-d в Xen, які переваги вона дає, а також як правильно її використовувати. Xen — багатоплатформовий гіпервізор, розроблений в комп'ютерній лабораторії Кембриджського університету і поширюваний на умовах ліцензії.

4.1 Організація введення / виведення в домені Xen

Існує три основних способи забезпечення введення / виведення (і, фактично, доступу до обладнання) для гостьової операційної системи, що працює всередині домену Xen:

1. Емуляція пристроїв з боку домену 0 і використання традиційних драйверів в гостьовій системі;
2. Монопольне виділення пристроїв гостьовій системі;
3. Використання паравіртуальних драйверів.

На даний момент найбільш поширеним є перший спосіб, тобто емуляція пристроїв. Xen використовує для емуляції, так званий QEMU Device Model (qemu-dm). Це спеціальний процес, який працює в просторі користувача (userlevel) в домені 0 і надає віртуальні пристрої гостьового домену.

Повною протилежністю до цього підходу є другий підхід - монопольне виділення пристрою гостьовій системі. У цьому випадку ніяких витрат на емуляцію не потрібно. Гостьовий домен працює з пристроєм безпосередньо, без будь-якого посередництва домену 0. Він бачить пристрій "як є", і використовує стандартні драйвери від цього пристрою. Робота з пристроєм здійснюється на повній швидкості.

У третьому способі застосовуються спеціальні драйвери, які виконують введення / виведення не через емульовані пристрої, а за допомогою спеціального паравіртуального інтерфейсу, що надається системою віртуалізації і хост-системою.

Далі буде докладніше розглянуто другий спосіб, тобто монопольне виділення пристроїв гостьовим доменам.

4.2 Монопольне виділення пристроїв гостьовому домену

На даний момент такий спосіб працює з паравіртуальними доменами - їм можна виділяти пристрої в монопольне використання без всяких проблем. Що стосується HVM-доменів (доменів, що використовують апаратну віртуалізацію), це:

1. Вимагає апаратної підтримки;
2. Реалізовано в Xen, починаючи з версії 3.2.0, яка вийшла на початку 2008 року.

Зараз майже всі плати виробництва Intel, підтримують власну реалізацію апаратної віртуалізації введення / виведення відому як Intel VT-d (не плутати з Intel VT-x і Intel VT-i, які займаються віртуалізацією процесора!).

В AMD теж ведеться робота над власною реалізацією апаратної віртуалізації введення / виведення, IOMMU.

При використанні VT-d можна організувати живу міграцію доменів, яким монопольно виділені пристрої.

4.3 Як включити підтримку VT-d в Xen

- cd xen-unstable.hg
- make install
- make linux-2.6-xen-config CONFIGMODE = menuconfig
- змінити XEN -> "PCI-device backend driver" з "M" на "*".
- make linux-2.6-xen-build
- make linux-2.6-xen-install
- depmod 2.6.18.8-xen

- mkinitrd -v -f --with = ahci --with = aacraid --with = sd_mod --with = scsi_mod initrd-2.6.18-xen.img 2.6.18.8-xen
- cp initrd-2.6.18-xen.img / boot
- lspci - вибрати ідентифікатори пристроїв, які ви хочете призначити гостьовим системам
- приховати PCI-пристрої від домену 0 (dom0) за допомогою такого запису в GRUB:

```
title Xen-Fedora Core (2.6.18-xen)
  root (hd0,0)
      kernel /boot/xen.gz com1=115200,8n1 console=com1 vtd=1
      module /boot/vmlinuz-2.6.18.8-xen root=LABEL=/ ro console=tty0 console=ttyS0,115200,8n1 pciback.hide=(01:00.0)(03:00.0) pciback.verbose_request=1 apic=debug
      module /boot/initrd-2.6.18-xen.img
```

- перезавантажити операційну систему
- додати рядок "pci" в файл /etc/xen/hvm.conf

```
pci = [ '01:00.0', '03:00.0' ]
```

- запустити гостьовий HVM-домен і за допомогою команди lspci подивитися, перекидається цей пристрій чи ні. Якщо це мережевий пристрій, спробувати попрацювати з ним, наприклад, за допомогою ifconfig.

  Якщо ви хочете щоб кидок PCI-пристроїв всередину PV-доменів також виконувався за допомогою VT-d, то потрібно вказати параметр

```
iommu=pv
```

в числі аргументів командного рядка Xen при його завантаженні.

Інші можливі значення параметра iommu (з файлу xen / drivers / passthrough / iommu.c):

```
/*
 * The 'iommu' parameter enables the IOMMU.  Optional comma separated
 * value may contain:
 *
 *   off|no|false|disable       Disable IOMMU (default)
 *   pv                         Enable IOMMU for PV domains
 *   no-pv                      Disable IOMMU for PV domains (default)
 *   force|required             Don't boot unless IOMMU is enabled
 *   passthrough                Enable VT-d DMA passthrough (no DMA
 *                              translation for Dom0)
 *   no-snoop                   Disable VT-d Snoop Control
 *   no-qinval                  Disable VT-d Queued Invalidation
 *   no-intremap                Disable VT-d Interrupt Remapping
 */
```

4.4 Підтримка операційних систем

- Хост-система: PAE, 64-bit
- Гостьова система: 32-bit, PAE, 64-bit

Зараз Xen не підтримує MSI, тому для тих гостьових систем, які за замовчуванням використовують MSI, потрібно додати опцію ядра

```
pci=nomsi
```

в завантажувач (GRUB).

4.5 Перевірені комбінації

- 64-бітний хост: 32 / PAE / 64 Linux / Win7 / Win10
- PAE хост: 32 / PAE Linux / Win7 / Win10

4.6 Апаратні системи з підтримкою VT-d

Материнські плати, в яких точно є підтримка VT-d (список повний):

- DH87MC, DH87RL, DQ87PG
- DB85FL
- DX79SI, DX79SR, DX79TO
- DH77DF, DH77EB, DH77KC, DQ77CP, DQ77KB, DQ77MK, DZ77BH-55K, DZ77GA-70K, DZ77RE-75K, DZ77SL-50K
- DB75EN, DZ75ML-45K
- DQ67EP, DQ67OW, DQ67SW
- DH61AGL
- DQ57TM, DQ57TML
- DQ45CB, DQ45EK
- DQ35JO, DQ35MP

Системи, в яких точно є підтримка VT-d (список не повний):

- Dell: Optiplex 755 [2]
- HP Compaq: DC7800 [3]

Підтримка VT-d присутня у всіх комп'ютерах, що підтримують технологію Intel vPro. Технологія vPro базується на двох технологіях: AMT (Active Management Technology) для віддаленого управління залізом і VT (VT-x + VT-d) для віртуалізації процесора і систем введення / виведення.

Hi, I have been doing some significant experimentation with Intel's IOMMU (VT-d) so I can answer your questions.

* Yes, real IOMMUs (at least Intel's VT-d) are available on the market today, both as loose motherboards and in OEM systems. For details see /docs/misc/vtd.txt in the Xen source. To repeat what is in that file:

1) For VT-d enabling work on Xen, we have been using development systems using following Intel motherboards:

- DH87MC, DH87PG, DZ87KLT-75K

2) As far as we know, following OEM systems also has vt-d enabled. Feel free to add others as they become available.

c=us&cs=555&l=en&s=biz

- HP Compaq: DC7800

This is very recent...I think the motherboards only became generally available this spring. Anyway I ordered a Dell Optiplex 755 and it does indeed have VT-d and it works with Xen.

* I'm not sure about AMD's IOMMU...my impression is that it is currently not generally available, and/or there is less support in Xen.

* If your motherboard/chipset supports VT-d, you will see it in the BIOS configuration (it will probably be turned off by default). Again, unless you motherboard is very new or acquired in a non-standard way, it will _not_ have VT-d.

* Support in Xen was introduced by Intel in 3.2, which is just now getting ready to release. On 3.2 (unstable) I've been able to get a PCI NIC to pass through, but not a PCI Express graphics card (that story is on another thread). There _does_ seem to be testing of a PCI Express NIC so I guess PCI Express is in general supported.

* You are correct that open-source PV drivers for Windows DomUs are just now under development and of course are being developed on a per-device type basis. IOMMU allows you to pass through an arbitrary PCI device so you need neither PV drivers nor qemu emulation. This will presumaby perform well as you suggest, and more importantly it

allows you to use device types that qemu doesn't emulate!

Далі розглядається процедура підготовки і запуску домену з Windows в системі віртуалізації Xen на платформі з апаратною підтримкою віртуалізації (HVM).

4.7 Попередні вимоги

В першу чергу, для установки Windows 10, як і будь-який іншій системі з закритим кодом, необхідна підтримка центральним процесором технології віртуалізації Intel © Virtualization Technology (VT) або Pacifica (AMD). Підтримка апаратної віртуалізації повинна бути і у Xen. При складанні з вихідних текстів знадобиться встановити в систему:

- dev86 - Асемблер і компонувальник для реального режиму 80x86. Цей пакет необхідний для збірки коду BIOS, що запускається в (віртуальному) реальному режимі. Якщо пакет dev86 недоступний для x86_64, то можна використовувати i386 версію.
- LibVNCServer - немодифікований VGA дисплей, клавіатуру і мишу можна віртуалізувати за допомогою бібліотеки vncserver.
- SDL-devel, SDL - Якщо пакети SDL і SDL-devel були встановлені за замовчуванням, то взяти їх можна з системи портів або скомпілювавши з вихідних текстів.

При виконанні вищезазначеної процедури на Debian GNU Linux необхідно врахувати, що пакет dev86 в Debian розбитий на два пакети - bin86 і bcc - і перед компіляцією Xen з архіву вихідних текстів повинні бути встановлені обидва ці пакета.

4.8 Конфігураційний файл домену

У термінології Xen гостьові домени, виконуються в режимі апаратної віртуалізації, називаються HVM-доменами. Для полегшення процесу конфігурації існує приклад конфігураційного файлу такого домену (при установці з вихідних він називається / etc / xen / xmexample .hvm; при установці з пакетів шлях може бути

іншим). У ньому, крім опцій, які використовуються в паравіртуальних доменах є і суто специфічні:

- kernel - VMX firmware loader, / nsr / lib / xen / boot / vinxloader
- builder - Функції збірки домену. VMX-домени використовують vinx builder
- acpi - Задіє ACPI VMX-домену, але замовчуванням дорівнює "0" (вимкнено)
- apic - Задіє A PIC VMX-домену, але замовчуванням дорівнює "0" (вимкнено)
- pae - Задіє PAE VMX-домену, за замовчуванням дорівнює "0" (вимкнено)
- vif - Опціонально визначає MAC адресу і / або режим моста для мережевого інтерфейсу. Якщо значення MAC не вказано, то призначається випадкова адреса. Є можливість задати параметр type = ioemu для використання ioomu в VMX NIC. Якщо це значення не визначене, то vbd використовується як в паравіртуальних ("нормальних", з модифікованим ядром) доменах.
- disk - Визначає носії пам'яті, до яких гостьовий домен повинен мати доступ. Якщо для домену використовується фізичний носій в якості диска, то він повинен бути описаний рядком типу:

phy: UNAME ioemu: DEV, K0DE,

де UNAME - ім'я пристрою, DEV - ім'я диска, як його бачить домен і MODE приймає значення r для read-only і w для read-write. Якщо це значення не визначене, то ioemu використовується як паравіртуальих доменах.

Якщо використовується образ диска, то рядок приймає вигляд:

file: FILEPATH, ioemu: DEV, MODE

Якщо використовується більше одного диска, то вони розділяються комою.

Наприклад:

disk = ['file: / var / images / imagel. img , ioemu: hda, w ', \
'file: / var / images / image2. img , ioemu: hdb, w ']

- cdrom - Образ CD-ROM. За замовчуванням, для Domain0 це значення дорівнює / dev / cdrom. Усередині VMX-домену CD-ROM буде видно як / dev / hdc.
- boot - Завантаження з floppy (a), hard disk (c) або CD-ROM (d).
- device_model - Інструмент емуляції пристроїв для VMX-домену. Можуть бути змінені параметри, наведені нижче.
- sdl - Задействует бібліотеку SDL для відображення графіки, за замовчуванням дорівнює "0" (вимкнено).
- vnc - Задіє бібліотеку VNC для відображення графіки, по умовчанню дорівнює "0" (вимкнено).
- vneviewer - Якщо vnc = l і vncviewer = 0, користувач може використовувати vneviewer для підключення до VMX-домену.

Наприклад:

$ vncviewer domainO_IP_address: VMX_domain_id

- ne2000 - Задіє режим сумісності ne2000, за замовчуванням дорівнює "0" (відключено, використовується pcnet)
- serial - Перенаправлення послідовних портів гостьового домена на реальний пристрій.
- Usb - Включення підтримки USB без вказання специфічного пристрою. За замовчуванням ця функція відключена, в разі ж визначення параметра usbdevice, її необхідно задіяти.
- usbdevice - Включення підтримки конкретних пристроїв. Наприклад, підтримка миші PS / 2 через USB:

usbdevice = 'mouse'

- localtime - Установка локального часу. За замовчуванням дорівнює “0”, тобто UTC
- enable-audio - Підтримка звуку. Знаходиться в розробці.
- full-screen - Підтримка повноекранного режиму. Знаходиться в розробці.

- nographic - Інший спосіб перенаправити висновок па послідовний порт. В цьому випадку опції ‘sdll’ або ‘vnc’ не працюють. Використання даного режиму не рекомендується.

4.9 Перевірка на підтримку VMX

Після завантаження самого Dom0 переконаємося в наявності підтримки VMX (процесори Intel):

```
# Xm dmesg | grep VMX
(XEN) VMXON is done
(XEN) VMXON is done
…
 (XEN) VMXON is done
(XEN) VMXON is done
(XEN) VMXON is done
#
```

Якщо використовується процесор AMD:

```
# xm dmesg | grep -i svm
(XEN) AMD SVM Extension is enabled for cpu 0.
(XEN) AMD SVM Extension is enabled for cpu 1.
```

У загальному випадку:

```
# xm info | grep caps
hw_caps: 178bfbff: ebd3fbff: 00000000: 00000010: 00 . . . .
xen_caps: xen-3.0-x86_32p hvm-3.0-x86_32 hvm-3.0-x86_32p
```

hvm-3.0-x86_32 говорить про те, що XEN успішно виявив процесор, який підтримує технології Intel VT або AMD-V.

Якщо у вас ще одне повідомлення, то перевірте налаштування BIOS і задійте підтримку апаратної віртуалізації, якщо вона вимкнена.

4.10 Створення дискового розділу для гостьової системи

Створюємо образ диска Xen:

mkdir -p / root / xenimages

cd / root / xenimages

dd if = / dev / zero of = WS128.img bs = 1M count = 4096

Також необхідно створити iso-образ системи Win10 - ServicePack2. В даному випадку, розмістимо його в каталозі / root / xenimages.

На основі еталонного файлу конфігурації створимо свій власний:

cat / etc / xen / win10 128

kernel = "/ usr / lib / xen / boot / hvmloader"

builder = 'hvm'

memory = 512

name = "Win10128"

vcpus = l

pae = 0

acpi = 0

apic = 0

cpus = ""

vif = ['type = ioemu, bridge = xenbr0']

```
disk = [
'file: /root/xenimages/win10128.img,ioemu: hda, w',
'file: /root/xenimages/en_win10_pro_with_sp2.iso,ioemu: hdc: cdrom, r'
]
on_poweroff = 'destroy'
on_reboot = 'destroy'
on_ crash = 'destroy'
device_model = '/ usr / lib / xen / bin / qemu-dm'
boot = 'd'
sdl = 0
vnc = 1
vncviewer = 0
stdvga = 0
serial = 'pty'
ne2000 = 0
```

Зверніть увагу на те, що зазначений параметр boot = d, що необхідно для установки. Згодом його необхідно замінити на boot = 'c'. Доступ до гостьового домену буде здійснюватися через VNC, використання SDL не передбачається.

4.11 Запуск домену та інсталяція гостьової системи

Починаємо установку і під'єднуємося до домену за допомогою VNC – відразу після створення домену підключаємося до нього за допомогою vncviewer.

```
# xm create -c / etc / xen / win10128
Using config file "/ etc / xen / win10128".
```

Started domain Win10128

Підключення до VNC:

% $ vneviewer localhost: 0

З установкою можуть бути проблеми. Можна спробувати вирішити проблему так: на екрані установки, що пропонує натиснути F6 для установки SCSI або RAID контролера, треба натиснути F5 і вибрати пункт Standard PC із запропонованого меню.

ACPI Multiprocessor PC

ACPI Uniprocessor PC

Advanced Configuration and Power Interface (ACPI) PC

Compaq SystemPro Multiprocessor or 100% Compatible PC

MPS Uniprocessor PC

MPS Multiprocessor PC

Standard PC

Other

Після того, як програма установки Windows відформатує диск і скопіює на нього необхідні файли, виконується перезавантаження. Згідно з нашим файлу конфігурації, віртуальна машина буде закрита і нам буде надана вдала можливість відредагувати параметр boot = 'c', після чого запускаємо віртуальну машину і єднаємося з консоллю:

% # xm create / etc / xen / win10128

Using config file "/ etc / xen / win10128 ".

Started domain Win10128

VNC:

% $ vncviewer localhost: 0

4.12 Запуск вже встановленої Windows в домені Xen

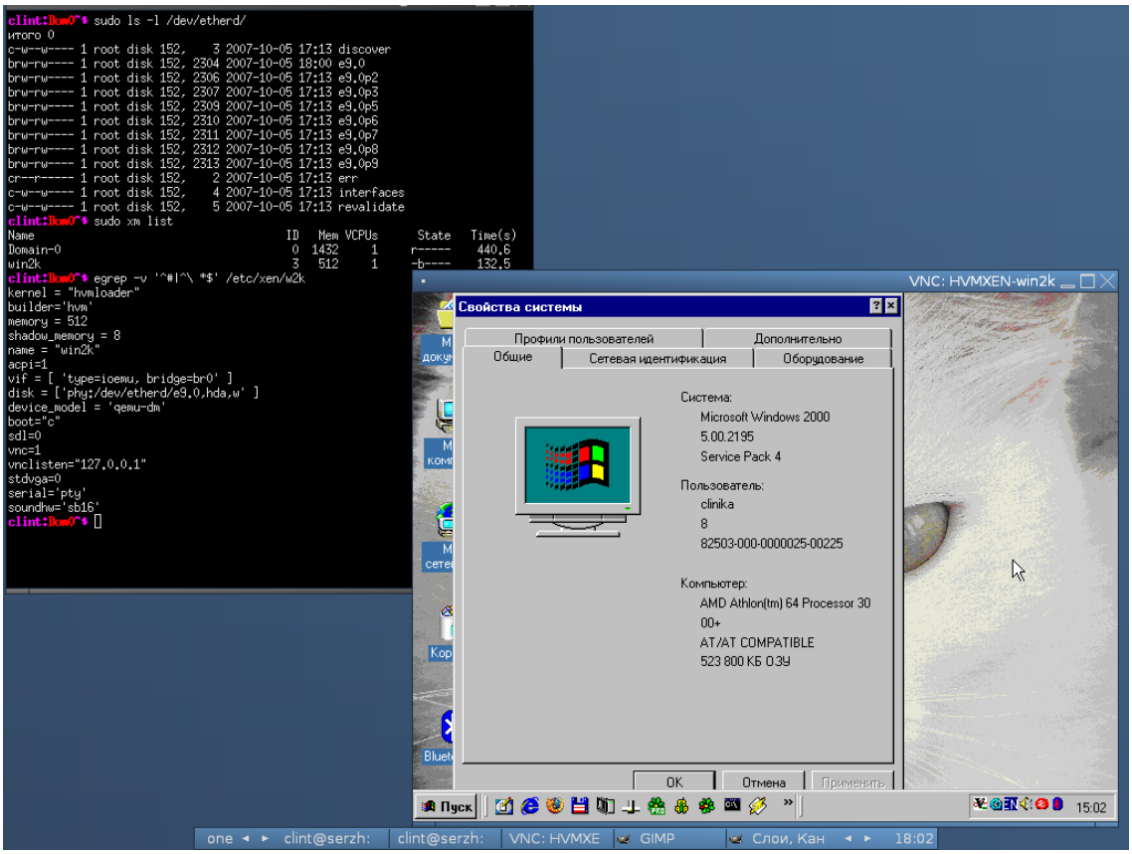


Рис. 4.1 - Операційна система Windows одного хоста, запущена в домені Xen на іншому хості

Якщо на комп'ютері встановлено дві операційні системи, і одна з них це Xenolinux (Xen + Linux), то другу можна запустити як користувальницький домен Xen. Якщо операційна система встановлена не локально, а на іншому комп'ютері, її теж можна запустити в домені Xen, тільки для цього необхідно якось дати можливість доступу системі віртуалізації до образу встановленої системи, так щоб, грубо кажучи, віртуальний домен побачив диск. Це можна зробити, наприклад, за допомогою AoE або iSCSI.

4.13 Паравіртуальні драйвери

Рис. 4.2 - Вікно Device Manager в Windows з встановленими вільними паравіртуальнимі драйверами

Апаратна віртуалізація бере на себе основні труднощі з переключення контекстів гостьових операційних систем і хост-системи, але вона нічого (поки що) не робить для прискорення введення / виведення. Як тільки завдання вимагає введення / виведення будь-яка система віртуалізації (але не паравіртуалізації!) істотно сповільнює свою роботу.

Одна з головних причин розробки і використання паравіртуальних драйверів - можливість істотного підвищення продуктивності роботи гостьових систем, що працюють в режимі повної віртуалізації.

У другій половині 2007 року з'явилися перша реалізація вільних паравіртуальних драйверів під Windows, зроблена Джеймсом Харпером (James Harper).

В кінці 2007 року вийшла версія 0.5.0 драйверів, які можна розглядати як експериментальні. Їх можна ставити в віртуальну машину і гратися з ними, але їх поки що ні в якому разі не варто використовувати на виробничих системах.

На даний момент вільні паравіртуальні драйвери Xen для Windows знаходяться в украй сирому стані і можуть використовуватися виключно в експериментальних цілях.

4.14 Переміщення PCI-пристроїв всередину домену Windows

Починаючи з Xen 3.2.0 при наявності у системі апаратної підтримки віртуалізації введення / виведення Intel VT-d (не плутати з віртуалізацією процесора VT-x!) існує можливість виконувати монопольне виділення PCI- пристрою домену Xen. Раніше це було можливо для паравіртуальних доменів, але було неможливо для HVM-доменів, а саме в такому виповнюється Windows.

При виконанні переміщення PCI-пристроя, Windows працює з ним безпосередньо, на повній швидкості, і використовуючи власні драйвера. Це дозволяє обійти проблеми з продуктивністю, які є при емуляції пристроїв, а також задіяти всі можливості пристрою, про які знає драйвер.

При виділенні пристрою гостьовому воно стає недоступним для домену 0 і використовується гостьовим доменом монопольно.

Наразі, в наш час, є дуже потужні графічні адаптери, що вбудовані в мікропроцесори Intel, монопольне виділення яких підтримується. Це означає, що запускати якусь гру, всередині гостьового домена Xen і при цьому безпосередньо використовувати графічну карту можливо.

ВИСНОВОК ДО РОЗДІЛУ 4

В цьому розділі було детально досліджено як включити підтримку технологій VT-d та VT-x в домені Xen. Було розглянуто всю послідовність дій, необхідних для включення підтримки VT-d та VT-x в домені Xen і використанню можливостей, що забезпечують ці технології.

Отримані матеріали були використані для створення уроку з учбового курсу на Moodle по вивченню можливостей Intel Virtualization Technology.

ВИСНОВКИ

Метою дипломного проекту було дослідження можливостей технології Intel vPro: Intel Virtualization Technology та розробка програмних засобів навчання використанню можливостей цієї технології у віртуальному навчальному середовищі Moodle.

Для досягнення цієї мети мною була розглянута архітектура і основні механізми роботи технології Intel Virtualization Technology. Були визначені основні можливості технології, та визначені системні елементи, котрих потребує ця технологія для своєї роботи.

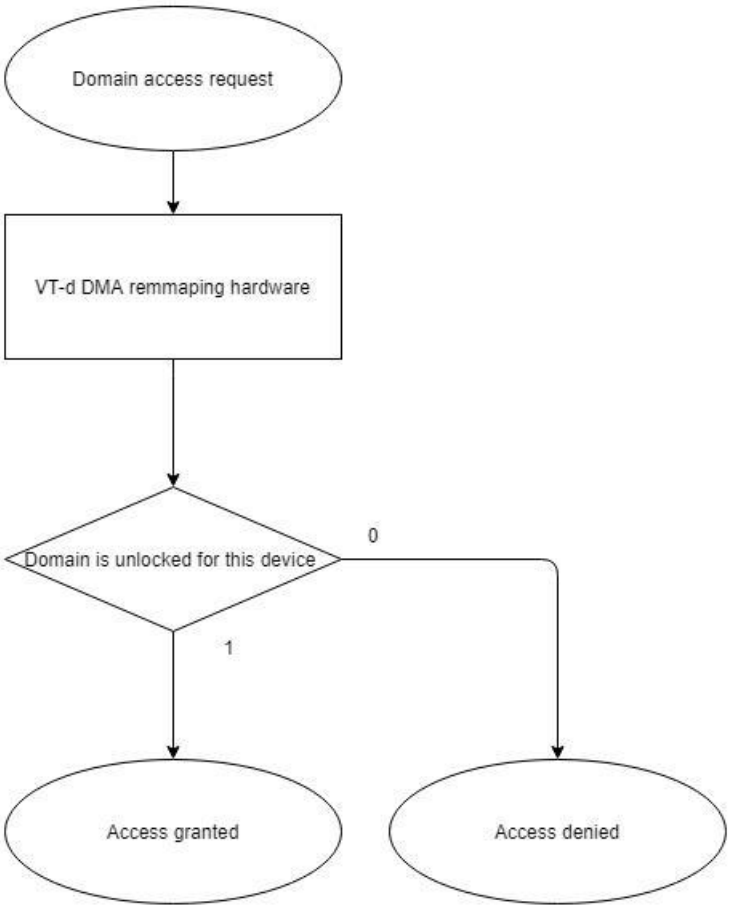
Було реалізовано серверну платформу Moodle, що орієнтована на вивчення персоналізованої навчальної програми по використанню можливостей Intel Virtualization Technology.

Було детально досліджено як включити підтримку технологій VT-d та VT-x в домені Xen та розглянуто послідовність дій, необхідних для використання можливостей, що забезпечують ці технології. Отримані матеріали були використані для створення уроку з учбового курсу на Moodle по вивченню можливостей Intel Virtualization Technology.

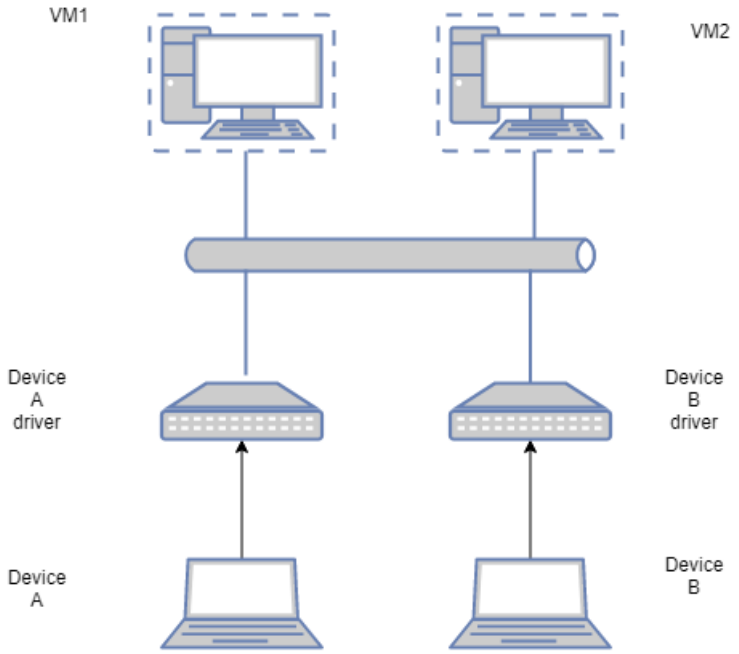
Intel Virtualization Technology є однією із головних технологій платформи Intel® vPro™, що зараз є доступною в різних форм-факторах. ЇЇ впровадження може принести користь підприємствам будь-якого розміру. У зв'язку з цим створення дистанційного курсу на Moodle ро освоєнню можливостей цієї технології є актуальною і може знайти великий попит на навчання у співробітників багатьох ІТ компаній.

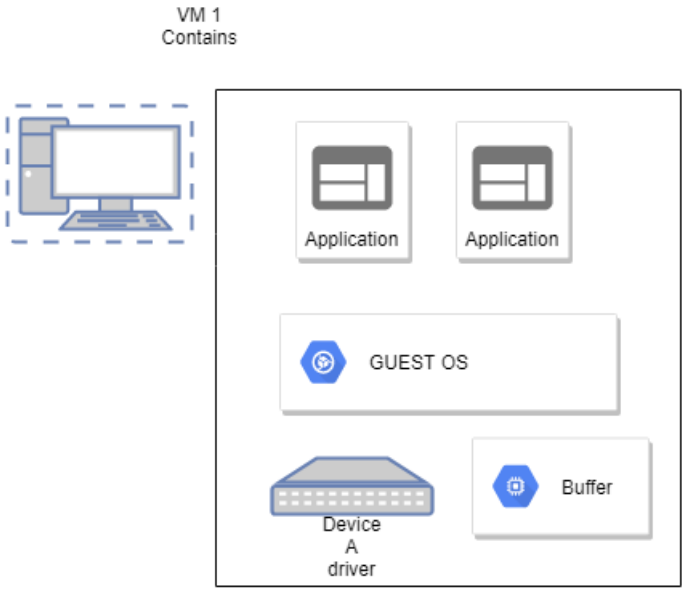
Список використаної літератури

1. Як встановити Moodle [Електронний ресурс] – Режим доступу до ресурсу: https://www.ispring.ru/elearning-insights/moodle/install.
2. Що таке Moodle? [Електронний ресурс] – Режим доступу до ресурсу: https://ru.osvita.ua/vnz/high_school/72285/.
3. Технологія Intel® vPro [Електронний ресурс] – Режим доступу до ресурсу: https://www.arbyte.ru/nastolnye-sistemy-arbyte/vpro.html.
4. Технологія Intel® vPro [Електронний ресурс] – Режим доступу до ресурсу: http://www.team.ru/lab/intel_vpro.shtml.
5. Платформа Intel® vPro [Електронний ресурс] – Режим доступу до ресурсу: https://www.intel.ru/content/www/ru/ru/architecture-and-technology/vpro/vpro-platform-general.html.
6. Intel® Virtualization Technology для напрямленого вводу / виводу (VT-d) [Електронний ресурс] – Режим доступу до ресурсу: https://software.intel.com/content/www/us/en/develop/articles/intel-virtualization-technology-for-directed-io-vt-d-enhancing-intel-platforms-for-efficient-virtualization-of-io-devices.html.
7. Використання VT-d та VT-x в Xen [Електронний ресурс] – Режим доступу до ресурсу: http://xgu.ru/wiki/%D0%98%D1%81%D0%BF%D0%BE%D0%BB%D1%8C%D0%B7%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5_VT-d_%D0%B2_Xen#.D0.A2.D0.B5.D1.85.D0.BD.D0.BE.D0.BB.D0.BE.D0.B3.D0.B8.D0.B8_VT-d_.D0.B8_VT-x_.D0.B8_.D0.B8.D1.85_.D0.B8.D1.81.D0.BF.D0.BE.D0.BB.D1.8C.D0.B7.D0.BE.D0.B2.D0.B0.D0.BD.D0.B8.D0.B5.
8. Вимоги щодо технології віртуалізації Intel® [Електронний ресурс] – Режим доступу до ресурсу: https://www.intel.ru/content/www/ru/ru/support/articles/000005758/boards-and-kits/desktop-boards.html.

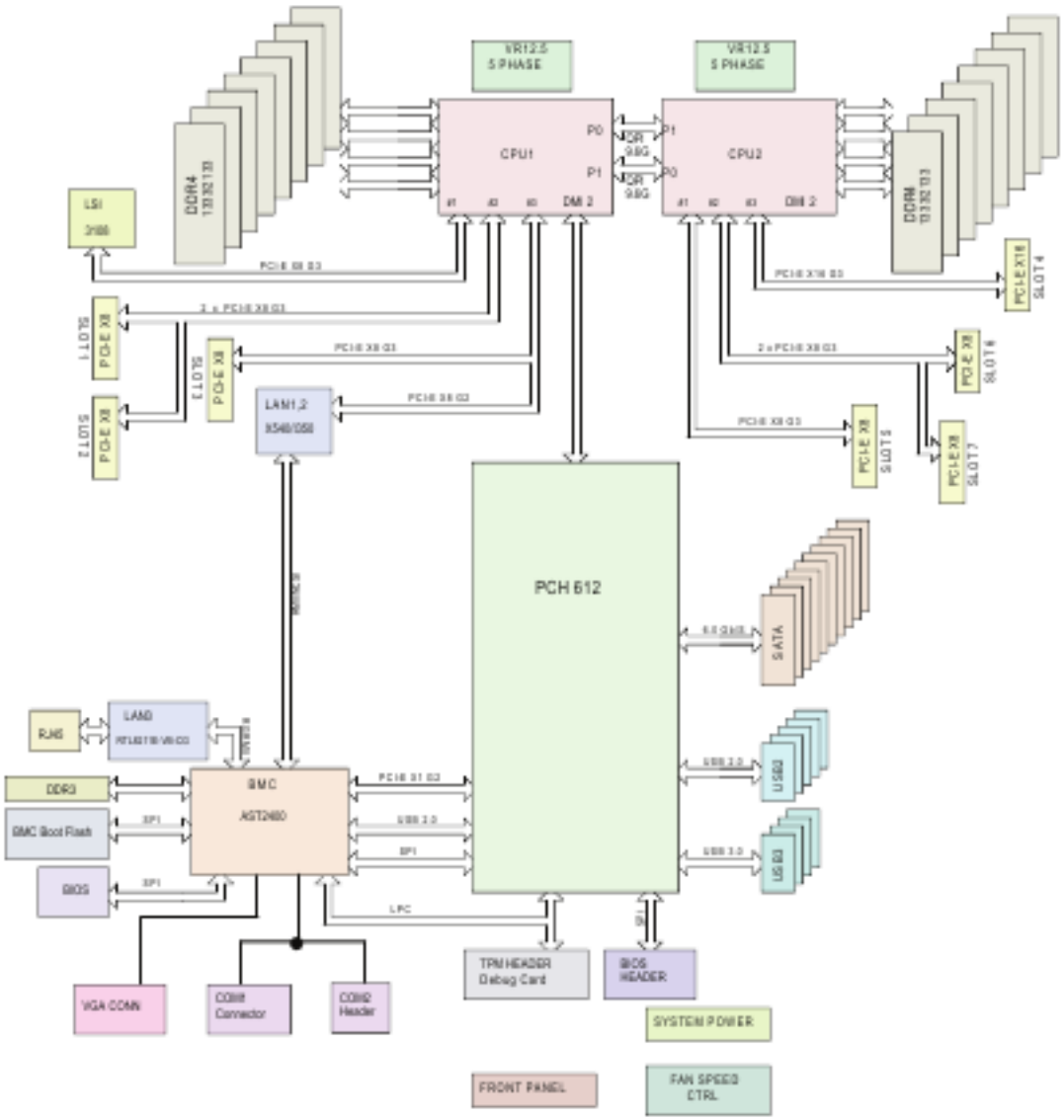


					ІАЛЦ.467200.004 А1		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розробив		*Трегубов-Ус Д.О.*			*Принципова схема алгоритму*	Літ.	Аркуш 1 / Аркушів 1
Перевірив		*Долголенко О.М.*					
Реценз.						*НТУУ «КПІ», ФІОТ, ІО-61*	
Н. Контр.		*Сімоненко В.П.*					
Затвердив							





					ІАЛЦ.467200.005 А2		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розробив		*Трегубов-Ус Д.О.*			*Функціональна схема*	Літ.	Аркуш 1 / Аркушів 1
Перевірив		*Долголенко О.М.*					
Реценз.						*НТУУ «КПІ», ФІОТ, ІО-61*	
Н. Контр.		*Сімоненко В.П.*					
Затвердив							



					ІАЛЦ.467200.006 А3		
Зм.	Арк.	№ докум.	Підпис	Дата			
Розробив		*Трегубов-Ус Д.О.*			*Структурна схема*	Літ.	Аркуш 1 / Аркушів 1
Перевірив		*Долголенко О.М.*					
Реценз.						*НТУУ «КПІ», ФІОТ, ІО-61*	
Н. Контр.		*Сімоненко В.П.*					
Затвердив							