Лекція 5.

Помічник по Azure (**Azure Advisor)**

Платформа Azure Well-Architected Framework описує п'ять основних аспектів архітектури:

- ✓ надійність,
- ✓ безпека,
- ✓ оптимізація витрат,
- ✓ ефективність роботи та
- ✓ ефективність продуктивності.

Помічник по Azure — це засіб, який дає попереджувальні, практичні та персоналізовані рекомендації з п'яти основних аспектів.

Помічник надає рекомендації для наступних ресурсів:

Шлюз додатків

Служби додатків

Групи доступності

Кеш Azure

Фабрика даних Azure

База даних Azure для MySQL

База даних Azure для PostgreSQL

База даних Azure для MariaDB

Azure ExpressRoute

Azure Cosmos DB

Загальнодоступні IP-адреси

Azure Azure Synapse Analytics

Сервери SQL Server

Облікові записи зберігання

Профілі диспетчера трафіку

Віртуальні машини

Типи рекомендацій(**Azure Advisor**)

Рекомендації щодо витрат - Помічник по Azure допомагає виявляти неактивні та недостатньо використовувані ресурси. Рекомендації щодо витрат можна отримати на вкладці Вартість панелі моніторингу Помічника.
Також помічник може надавати такі рекомендації:

- ❖ Завершить роботу віртуальної машини, якщо вона не використовується.
- ✓ Помічник може зробити цю рекомендацію, якщо: споживання ресурсів мережі було менше 2% протягом семи днів;
- ✓ максимального споживання ресурсів ЦП усіма ядрами не перевищує 3%;
- ✓ середнього показника ЦП за останні три дні, підсумованого по всіх ядрах, менше або дорівнює 2%.
- ❖ Змініть розмір віртуальної машини, щоб зберегти ресурси. Помічник порекомендує розмір, якщо:
- ✓ Поточне навантаження не перевищує 80 % використання робочих навантажень, які мають взаємодії з користувачем.
- ✓ Поточне навантаження не перевищує 40% використання робочих навантажень для користувачів.

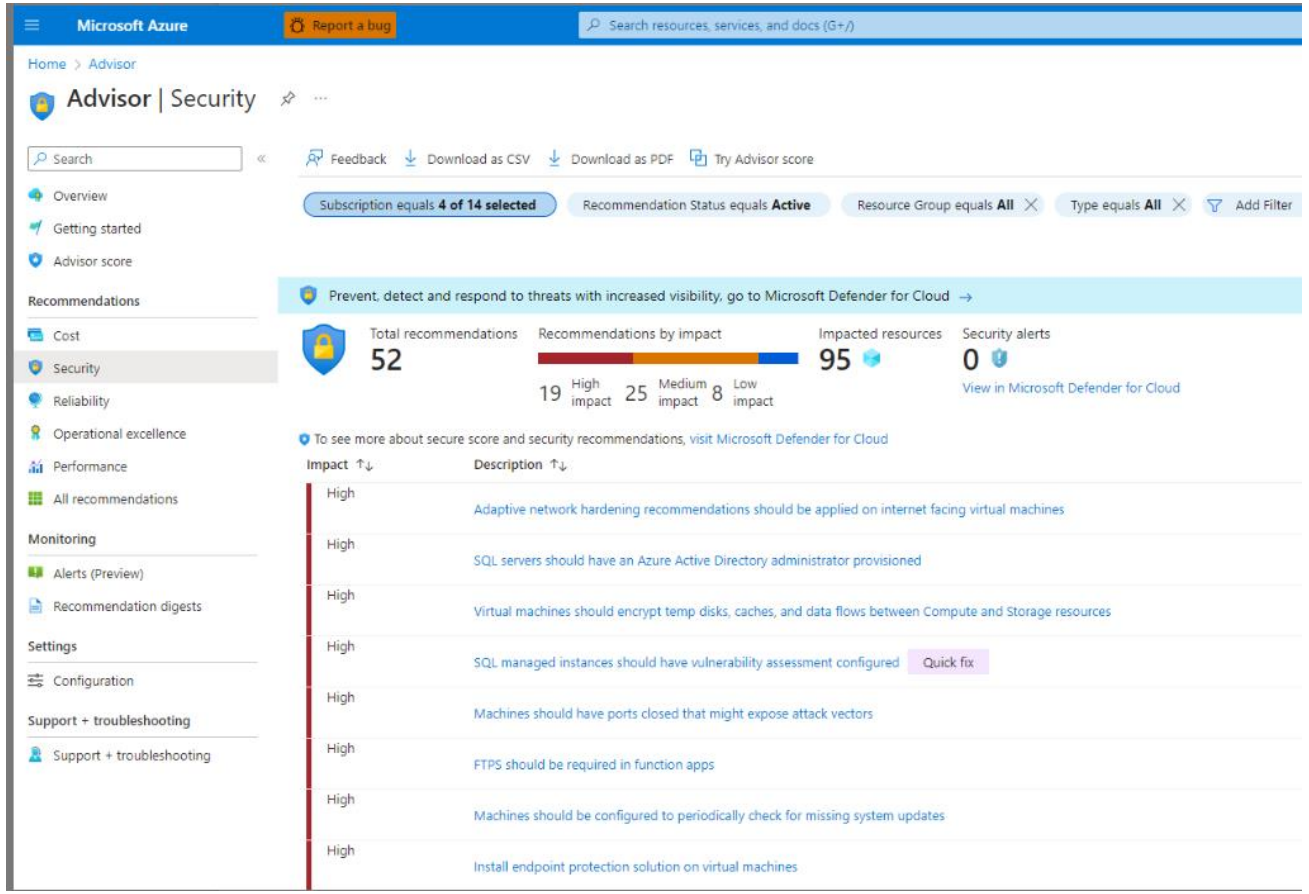
Оцінка економії буде відображатися для рекомендованих дій.

Типи рекомендацій(**Azure Advisor**)

- **Рекомендації щодо безпеки** - інтегруються з Microsoft Defender для хмари. Ці рекомендації можна отримати на вкладці Безпека панелі моніторингу Помічника.

❖ У Windows, Mac і Android Microsoft Defender можуть перевіряти файли або програми,, а також запускати сканування файлів, які вже є;

❖ У Windows, iOS і Android Microsoft Defender перевірятимуть посилання, які відкриваються, щоб спробувати виявити небезпечне.

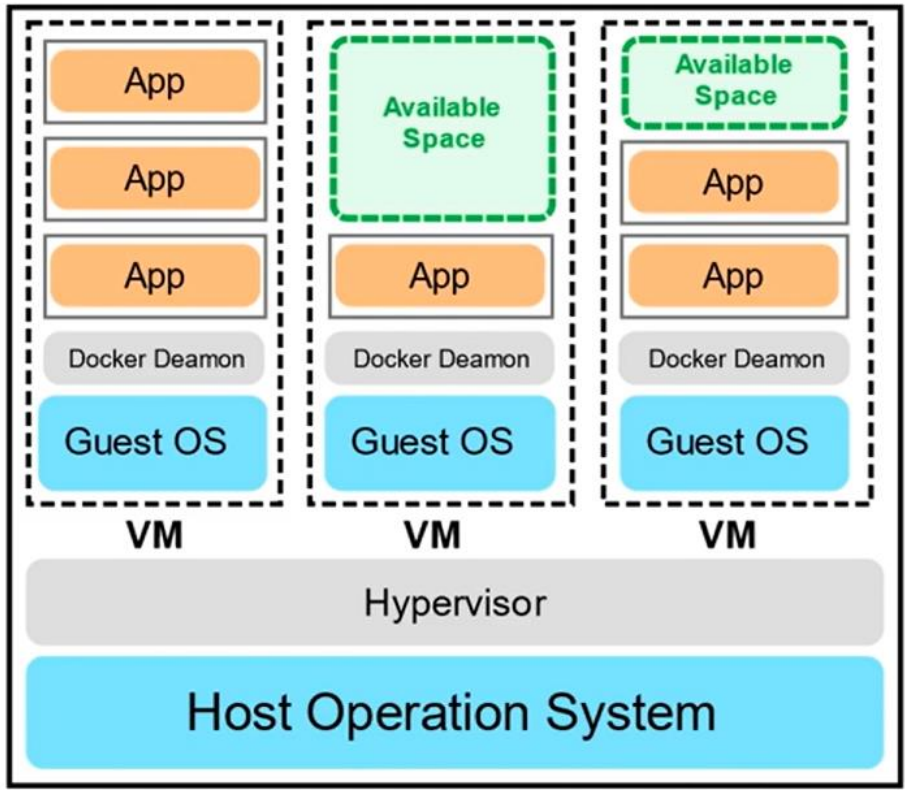


Рекомендації з надійності (Azure Advisor)

- **Рекомендації щодо надійності** - Перевірки надійності включають: Визначення чи використовує ВМ версію образу Check Point - яка є відома втратами мережного підключення під час операцій обслуговування платформи. Рекомендація Помічника допоможе виконати оновлення до новішої версії образу, що вирішує цю проблему. Ця перевірка забезпечить безперервність робочих процесів, покращивши мережне підключення.
- **Відмовостійкість шлюзу додатків** – Ця перевірка забезпечить безперервність роботи критично важливих доданків, які прослуховують шлюзи - Помічник виявляє екземпляри шлюзів додатків, для яких не налаштовано забезпечення стійкості до відмови і пропонує дії щодо виправлення, які можна виконати. Помічник виявляє середні або великі шлюзи додатків з одним екземпляром і рекомендує додати принаймні один додатковий екземпляр.
- **Віртуальні машини без увімкнення резервного копіювання** - Помічник визначає віртуальні машини, резервне копіювання на яких не увімкнене, а потім рекомендує включити резервне копіювання.
- **Рекомендації щодо відмовостійкості віртуальної машини** - Помічник виявляє віртуальні машини, які не входять до групи доступності, і рекомендує перемістити їх до групи доступності. Ця конфігурація гарантує доступність не менше однієї віртуальної машини, яка забезпечує виконання угоди про рівень обслуговування Azure у разі планового або позапланового обслуговування.

Контейнери Azure

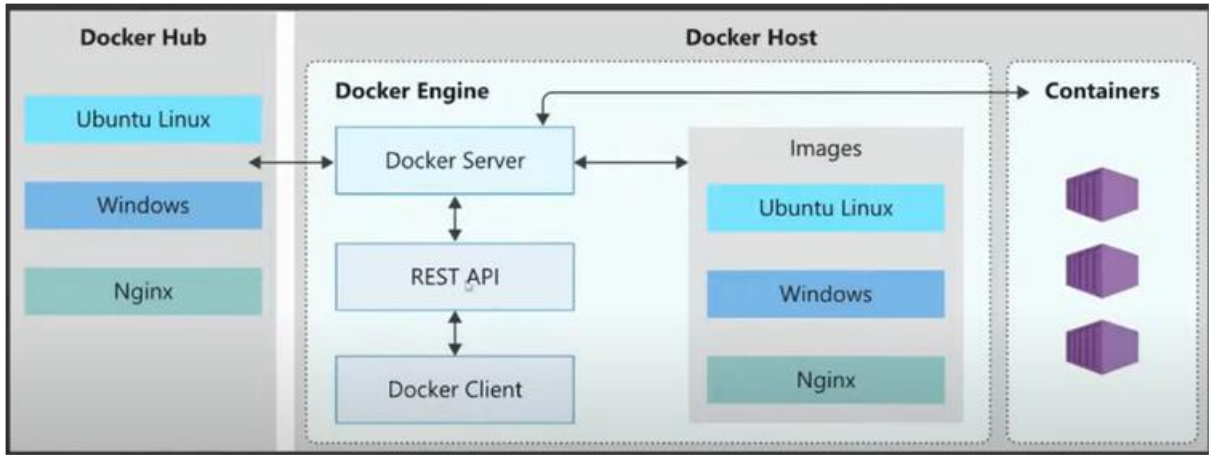
- Контейнер – це слабко ізольоване середовище, що дозволяє створювати та виконувати пакети програмного забезпечення (у тому числі ВМ). Ці пакети включають код і всі залежності, необхідні для швидкого і надійного запуску додатків у будь-якому обчислювальному середовищі. Такі пакети називаються образами контейнерів. Образ контейнера – це одиниця, яка використовується для поширення програм.
- Контейнеризація програмного забезпечення – це спосіб віртуалізації ОС, який застосовується для розгортання та виконання контейнерів без використання віртуальної машини. Контейнери можуть працювати на фізичному обладнанні, у хмарі, у віртуальних машинах та кількох ОС.
- Принципова різниця між Контейнером та ВМ – ВМ віртуалізує апаратне забезпечення (електроні та механічні пристрої). Контейнер – віртуалізує ВМ або програмний доданок.
- Таким чином, якщо потрібно запустити доданок на спеціальній ОС – для цього не завжди потрібно мати ВМ.



Клієнт – сервера архітектура Docker

Docker — це платформа контейнеризації, яка використовується для розробки, доставки та виконання контейнерів. Docker не передбачає використання гіпервізора. При розробці та тестуванні програм можна запускати Docker на настільному ПК або ноутбуці. Настільна версія Docker підтримує Linux, Windows та MacOS. У робочих системах Docker доступний для серверних середовищ, включаючи безліч варіантів Linux та Microsoft Windows Server 2016 та пізніших версій. Docker підтримує багато хмарних середовищ, включаючи Azure.

Модуль Docker складається з кількох компонентів, що реалізують клієнт-серверну архітектуру, при якій клієнт та сервер працюють на одному вузлі. Клієнт взаємодіє із сервером за допомогою REST API, що дозволяє клієнту також взаємодіяти з віддаленим екземпляром сервера.

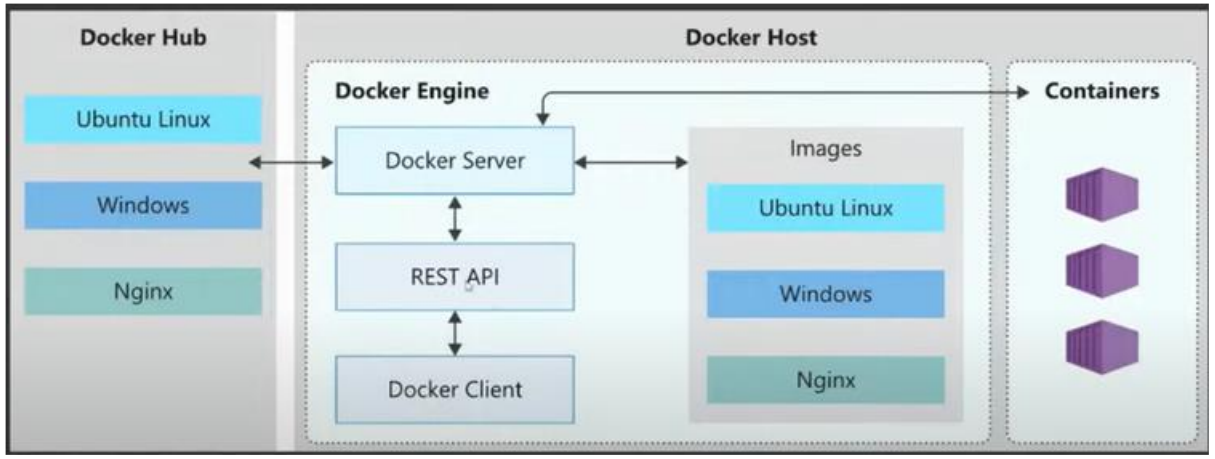


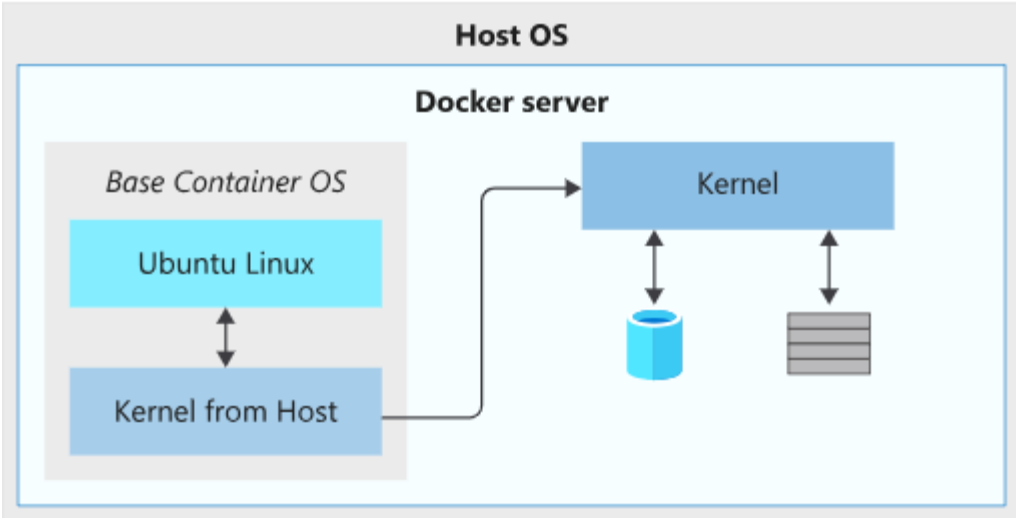
Docker Hub – це реєстр контейнерів Docker на основі моделі "програмне забезпечення як послуга" (SaaS). Реєстри Docker – це репозиторії, які служать для зберігання та розповсюдження створюваних образів контейнерів. Docker Hub є загальнодоступним реєстром Docker, який використовується за умовчанням для керування образами.

Клієнт – сервера архітектура Docker

ОС вузла — це ОС, на якій працює механізм Docker. Контейнери Docker, які працюють у Linux, спільно використовують ядро не вимагають контейнерної ОС, якщо є прямий доступ до ядра ОС. Однак для контейнерів Windows потрібна контейнерна ОС. Контейнер залежить від ядра ОС для керування такими службами, як файлова система, керування мережею, планування процесів і керування пам’яттю.

контейнерна ОС — це ОС, яка є частиною упакованого образу. Є можливість включати різні версії ОС Linux або Windows у контейнер. Ця гнучкість дозволяє отримати доступ до певних функцій ОС або встановити додаткове програмне забезпечення, яке можуть використовувати наші програми.



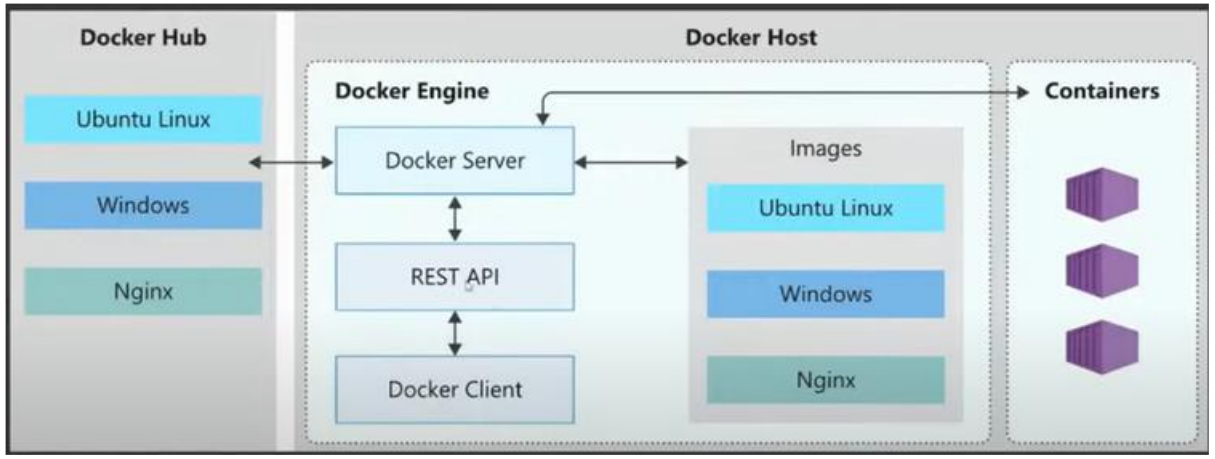


Клієнт – сервера архітектура Docker - Клієнт

Існує два варіанти для клієнта Docker: програма командного рядка з ім'ям docker або програма на основі графічного інтерфейсу користувача (GUI) з ім'ям Docker Desktop.

Команди docker з ІНТЕРФЕЙСУ командного рядка або Docker Desktop використовують REST API Docker для надсилання інструкцій на локальний або віддалений сервер і виконують функції основного інтерфейсу, який використовується для керування контейнерами.

Сервер Docker це керуюча програма, яка називається dockerd. Керуюча програма dockerd відповідає на запити клієнта за допомогою REST API Docker і може взаємодіяти з іншими програмами, що управляють. Сервер Docker відповідає за відстеження життєвого циклу контейнерів.



Клієнт – сервера архітектура Docker - Зображення контейнера

Зображення контейнера — це пакет, що містить програмне забезпечення, бібліотеки, конфігураційні файли і т.п. Під час запуску він стає контейнером. Контейнер є екземпляр зображення в пам'яті.

Зображення контейнера є незмінним. Єдиний спосіб змінити зображення – створити нове.

Зображення контейнера – може бути базовим та батьківським.

Базове зображення не створює шар файлової системи –в такому разі, доданок, який запускає контейнер має використовувати ядро ОС вузла.

Батьківський образ - це образ контейнера, з якого створюються образи. Наприклад, замість створення образа з scratch, а потім встановлювати Ubuntu, краще використовувати образ, вже заснований на Ubuntu. Можна навіть використовувати образ, у якому вже встановлено Nginx. Батьківський образ зазвичай включає ОС контейнера.

Обидва типи образів дозволяють створювати багаторазово використовувані образи. Однак базові образи дають більший контроль за вмістом підсумкового образу.

У Windows можна створювати лише образи контейнерів, що базуються на базових образах контейнерів Windows. Ці базові образи контейнерів Windows надаються та обслуговуються корпорацією Майкрософт.

Екземпляри контейнерів Azure

Azure Служба "Екземпляри контейнерів Azure" надає найшвидший і найпростіший спосіб запуску контейнера в Azure без керування віртуальними машинами та застосування додаткових служб. Екземпляр контейнера – це метод завантаження контейнерів.

Екземпляри контейнерів Azure – це пропозиція в рамках моделі "платформа як послуга" (PaaS). Екземпляри контейнерів Azure дозволяють надсилати контейнери, а потім служба запустить їх.

Коли ви розгортаєте контейнер в Azure, ви вказуєте джерело зображення в конфігурації розгортання або шаблонах. Потім середовище виконання контейнера (наприклад, Docker) використовує цю інформацію, щоб отримати вказане зображення контейнера з джерела та запустити його як контейнер у вашому середовищі Azure.

Хоча контейнер використовує ядро операційної системи сервера, контейнер не отримує необмежений доступ до ядра. Натомість контейнер отримує ізольоване, а в деяких випадках віртуалізоване уявлення системи. Наприклад, контейнер може звертатися до віртуалізованої версії файлової системи та реєстру, але будь-які зміни стосуються лише контейнера та видаляються при його зупинці. Щоб зберегти дані, контейнер може підключити постійне сховище.

Контейнери додатків мають додаткові переваги, такі як можливість балансування навантаження та масштабування.

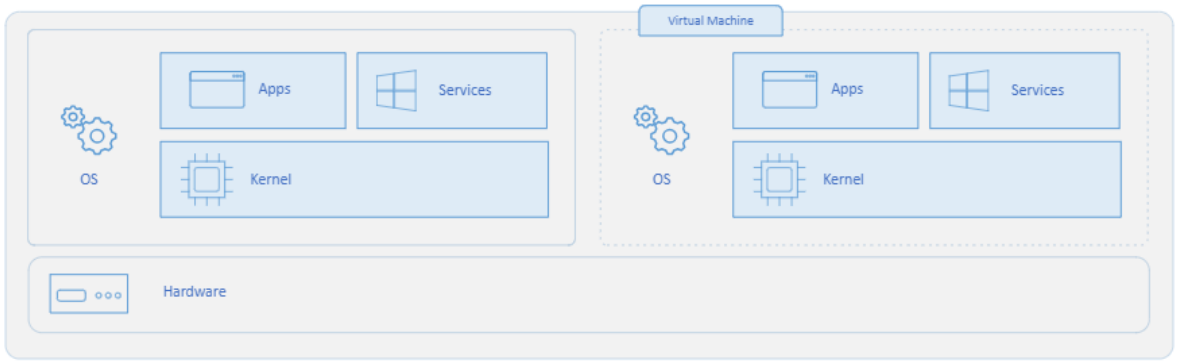
Типи програм, які не можна перемістити в контейнер Windows

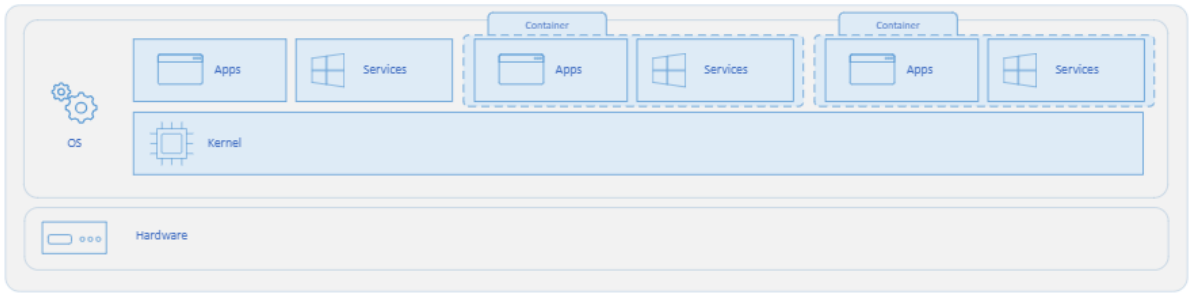
Типи програм	Причини
Додатки, для яких потрібні можливості робочого столу	Контейнери не підтримують графічний інтерфейс користувача (GUI). навіть якщо в самому додатку немає графічного інтерфейсу користувача, але є установник, який використовує його.
Програми, що використовують протокол віддаленого робочого столу (RDP)	Оскільки протокол віддаленого робочого столу (RDP) призначений для створення інтерактивного візуального сеансу, обмеження графічного інтерфейсу користувача, описане вище, застосовується і до нього.
програми з базами даних	Контейнери не передбачають збереження даних. можна контейнеризувати лише в тому випадку, якщо ви ізолюєте потрібні дані з одного сеансу в наступному та зберігаєте їх у постійному сховищі.
Програми, які використовують .NET Framework версії 2.0 або пізнішої	Для підтримки .NET Framework потрібні певні образи контейнерів, при цьому підтримуються лише пізніші версії Версії, що передують 2.0, не підтримуються в принципі

Типи програм, які «ідеальні» для контейнеризації

Типи програм	Причини
Консольні програми	Консольні програми, які не мають обмежень за графічним інтерфейсом користувача
Служби Windows	Оскільки це фонові процеси, які не потребують прямої взаємодії з користувачем
Веб-програми	Веб-програми по суті є фоновими службами, які прослуховують певний порт, і тому є відмінними кандидатами для контейнеризації, тому що вони можуть використовувати переваги масштабованості, пропоновані контейнерами.

Принципова різниця між ВМ і контейнерами





віртуальні машини працюють під керуванням повноцінної операційної системи із власним ядром (Kernel), як показано на рис зліва. З рисунку справа - бачимо, що контейнер не має власного ядра. Багато середовища контейнерів використовують віртуальні машини як операційну систему сервера, і не працюють безпосередньо на обладнанні, зокрема під час роботи з контейнерами у хмарі.

Таблиця відмінностей між ВМ і контейнерами

Функція	віртуальна машина	контейнер
Ізоляція	Забезпечує повну ізоляцію від операційної системи вузла (базова операційна система вказана при створенні ВМ) та інших віртуальних машин. Це корисно, коли важлива строга межа безпеки, наприклад, для поділу додатків від компаній, що конкурують, на одному сервері або в кластері.	Зазвичай надає спрощену ізоляцію від вузла (базова операційна система вказана при створенні) та інших контейнерів, але не надає настільки надійної межі безпеки, як у випадку віртуальних машин.
Операційна система	Містить повноцінну операційну систему, включаючи ядро, тому потребує більше системних ресурсів (ЦП, пам'яті та сховища).	Запускає частину операційної системи в режимі користувача і її можна адаптувати, щоб вона містила лише необхідні служби для програми, що дозволить використовувати менше системних ресурсів.
Сумісність з гостьовою системою	Працює практично з будь-якою операційною системою у віртуальній машині.	Працює на тій же версії операційної системи, що і вузол
Постійне сховище	Використовує віртуальний жорсткий диск (VHD) для локального сховища для однієї віртуальної машини або загальний файловий ресурс SMB для спільно використовуваного кількома серверами сховища. або серверами сховища.	Використовує диски Azure для локального сховища для одного вузла або служби файлів Azure (спільні ресурси SMB) для спільного використання кількома вузлами або серверами сховища.
Балансування навантаження	Балансування навантаження віртуальної машини переміщує віртуальні машини, що виконуються, на інші сервери у відмово стійкому кластері.	Самі контейнери не переміщуються. Натомість Orchestrator може автоматично запускати або припиняти роботу контейнерів на вузлах кластера для керування змінами навантаження та доступності.
Мережа	Використовує віртуальні мережні адаптери.	Використовує ізольоване уявлення віртуального мережного адаптера, надаючи меншу віртуалізацію

Azure DNS

Система доменних імен – це ієрархія доменів. Ієрархія починається з root домену, ім'я якого просто ".". Нижче наведені домени верхнього рівня, такі як com, net, org або ukjp. Під доменами верхнього рівня знаходяться домени другого рівня, наприклад, org.uk або co.jp. Ці домени в ієрархії DNS глобально розподілені на серверах DNS по всьому світу.

Домени DNS в Azure DNS розміщуються в глобальній мережі DNS-серверів Azure, В Azure DNS мережа організована таким чином, що на кожен запит DNS відповідає найближчий доступний DNS-сервер.

При створенні контейнера на порталі Azure для нього автоматично створюється IP-адреси. Загальнодоступна IP-адреса використовується для віддаленого доступу. Хоча портал не створює повне доменне ім'я або повне доменне ім'я, його варто додати після створення.

Реєстратор доменних імен - це організація, яка дозволяє придбати доменне ім'я, наприклад, company.com. Купуючи доменне ім'я, ви отримуєте право керувати ієрархією DNS під цим ім'ям, наприклад, налаштувати перенаправлення на веб-сайт вашої компанії при введенні адреси www.company.com. Реєстратор може розмістити домен на власних серверах імен від вашого імені або дозволить вказати альтернативні сервери доменних імен.

Зона DNS

Зона DNS використовується для розміщення записів DNS певного домену. Щоб розмістити домен в Azure DNS, необхідно створити зону DNS. Кожен запис DNS для вашого домену створюється всередині цієї зони DNS.

Наприклад, домен company.com може містити декілька записів DNS, включаючи mail.company.com (поштовий сервер) і www.company.com (для веб-сайту).

При створенні зони DNS в Azure DNS враховуйте таке.

- ✓ Ім'я зони має бути унікальним у межах групи ресурсів, а зона не має існувати. В іншому випадку операція завершиться помилкою.
- ✓ Це ж ім'я зони можна використовувати повторно в іншій групі ресурсів або іншій підписці Azure.
- ✓ Якщо кільком зонам надано одне й те саме ім'я, кожному примірнику призначаються різні адреси серверів доменних імен. За допомогою реєстратора доменних імен можна налаштувати лише один набір адрес.

Типи та набори записів

Типи записів

Кожний запис DNS має ім'я та тип. Записи поділяються на різні типи в залежності від даних, які вони містять. Найбільш поширений тип - запис A, який зіставляє ім'я з IPv4-адресою. Інший поширений тип - запис MX, який зіставляє ім'я з поштовим сервером.

Azure DNS підтримує всі загальні типи записів DNS: A, AAAA, CAA, CNAME, MX, NS, PTR, SOA, SRV та TXT. Зверніть увагу, що записи SPF представлені у вигляді записів TXT.

Набори записів

У деяких випадках необхідно створити кілька записів DNS із заданим ім'ям та типом. Наприклад, припустимо, що веб-сайт www.company.com розміщується за двома різними IP-адресами. Для цього веб-сайту потрібно два різні записи A — по одній для кожної IP-адреси: Ось приклад набору записів:

```
www.contoso.com.        3600    IN    A    134.170.185.46
www.contoso.com.        3600    IN    A    134.170.188.221
```

Типи та набори записів

Azure DNS керує всіма записами DNS за допомогою наборів записів. Набір записів (також називається набором записів ресурсів) – це колекція записів DNS у зоні, які мають одне ім'я та належать до одного типу. Більшість наборів записів містять один запис. Проте трапляються й набори з кількома записами (як у прикладі вище).

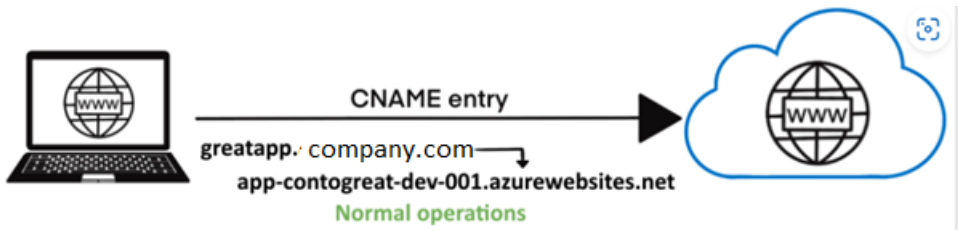
Наприклад, припустимо, що ви вже створили в зоні company.com запис A www, що вказує на IP-адресу 134.170.185.46 (перший запис вище). Щоб створити другий запис, не потрібно створювати додатковий набір записів — слід додати запис до вже наявного набору записів.

Набір записів типу SOA та CNAME є винятками. За стандартами DNS декілька записів з тим самим ім'ям для цих типів не допускаються, тому такі набори записів можуть містити лише один запис.

Захоплення піддомену

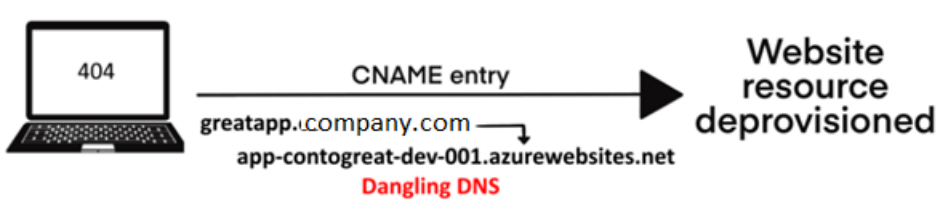
Захоплення піддоменів — поширена та серйозна загроза для організацій, які регулярно створюють та видаляють безліч ресурсів. Захоплення піддомену може відбутися, якщо у вас є запис DNS, що вказує на відкликаний ресурс Azure. Такі записи DNS називаються недійсними. Записи CNAME особливо вразливі до цієї загрози. Захоплення піддоменів дозволяє зловмисникам перенаправляти трафік, призначений для домену організації на сайт, що виконує шкідливі дії. Поширений сценарій для захоплення піддомену:

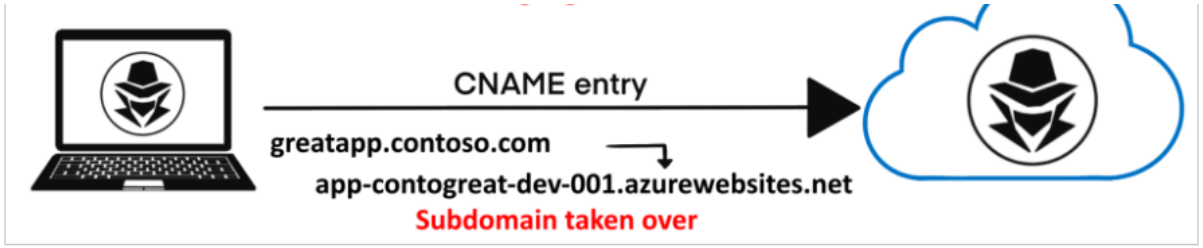
СТВОРІННЯ: Ви підготуєте ресурс Azure з повним доменним ім'ям (FQDN) app-contogreat-dev-001.azurewebsites.net. Ви призначаєте запис CNAME в зоні DNS з піддоменом greatapp.company.com, який надсилає трафік до ресурсу Azure.



Захоплення піддомену - ВІДГУК

Ресурс Azure буде відкликаний або видалений після того, як у ньому зникне потреба.





На цьому етапі запис CNAME greatapp.company.com необхідно видалити із зони DNS. Якщо запис CNAME не видалити, він оголошується як активний домен, але не надсилає трафік до активного ресурсу Azure. Це визначення "висячих" dns-записів.

Висячий піддомен (greatapp.company.com) тепер вразливий і може бути перепризначений іншому ресурсу підписки Azure.

ЗАХОПЛЕННЯ:

Використовуючи загальнодоступні методи та засоби, зловмисник виявляє "висячий" піддомен. Зловмисник готує ресурс Azure з тим самим повним доменним ім'ям раніше керованого вами ресурсу. У цьому прикладі app-contogreat-dev-001.azurewebsites.net.

Трафік, що відправляється в піддомен greatapp.company.com, тепер направляється в ресурс шкідливого суб'єкта, де вони керують вмістом.