ДЕРЖАВНИЙ УНІВЕРСИТЕТ ТЕЛЕКОМУНІКАЦІЙ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ЗАХИСТУ ІНФОРМАЦІЇ

КАФЕДРА ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ

Пояснювальна записка

до магістерської роботи
на тему:

«ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ НА БАЗІ ORACLE CLOUD INFRASTRUCTURE»

Виконала студентка 6 курсу, групи БСДМ-62
спеціальності 125 Кібербезпека
освітньо-професійної програми «Інформаційна та кібернетична безпека»
(шифр і назва спеціальності)
Алекеєнко О. А.
(прізвище та ініціали)
Керівник Гахов С. О.
(прізвище та ініціали)
Рецензент
(прізвище та ініціали)
Нормоконтролер Чумак Н. С.
(прізвище та ініціали)

КИЇВ – 2023

РЕФЕРАТ

Текстова частина магістерської роботи: сторінки 65, рисунків 24, джерел 26.

Об'єкт дослідження – забезпечення безпеки хмарної інфраструктури організації.

Предмет дослідження – технологія забезпечення безпеки хмарної інфраструктури організації.

Мета роботи – розробка варіанту технології забезпечення кібербезпеки хмарної інфраструктури для організації та рекомендацій щодо використання технології для захисту хмарної інфраструктури організації.

Методи дослідження – опрацювання літератури за даною темою, аналіз експлуатаційної документації обраної системи, робота з міжнародними стандартами та їх порівняння, моделювання процесу забезпечення захисту хмарної інфраструктури організації.

В роботі проведено аналіз проблеми захисту хмарних інфраструктури організації, визначено мету та завдання забезпечення захисту хмарних інфраструктур. Проаналізовано існуючі методи та засоби забезпечення захисту хмарних інфраструктур в організації на базі Oracle Cloud Infrastructure.

Досліджено методи та засоби забезпечення безпеки хмарних інфраструктур на базі Oracle Cloud Infrastructure. Визначено призначення, основні функції та склад засобів забезпечення захисту Oracle Cloud Infrastructure.

На основі досліджень проведених в роботі розроблено рекомендації та технологію забезпечення безпеки хмарної інфраструктури організації на базі Oracle Cloud Infrastructure

Галузь використання – кібербезпека хмарної інфраструктури організації.

ХМАРНА ІНФРАСТРУКТУРА, КІБЕРБЕЗПЕКА, ЗАХИСТ ХМАРНИХ СИСТЕМ, МЕТОДИ ТА ЗАСОБИ ЗАБЕЗПЕЧННЯ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ, ТЕХНОЛОГІЯ ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ

ABSTRACT

Master’s thesis: pages 64, figures 24, sources 28.

Object of research – the process of ensuring the protection of the organization’s cloud infrastructure.

Subject of research – the technology for ensuring the protection of the organization’s cloud infrastructure.

The aim of research – to develop a variant of the technology for the cybersecurity of organization’s cloud infrastructure and to develop recommendations on use of technology for protection of cloud infrastructure of organization.

Research methods – elaboration of literature on the topic, analysis of operational documentation of the selected system, work with international standards and their comparison, modeling of the process of securing the cloud infrastructure of the organization.

The paper analyzes the problem of ensuring the protection of the organization's cloud infrastructures, defines the purpose and task of ensuring the protection of cloud infrastructures. The existing methods and means of ensuring the protection of cloud infrastructure in an organization based on Oracle Cloud Infrastructure are analyzed.

The methods and means of ensuring the security of cloud infrastructures based on Oracle Cloud Infrastructure have been studied. Purpose, main functions and composition of Oracle Cloud Infrastructure protection tools are defined.

Based on the research carried out in the work, recommendations and technologies for ensuring the security of the organization's cloud infrastructure have been developed based on Oracle Cloud Infrastructure using the legal framework and direct recommendations of Oracle.

Field of use – cybersecurity of cloud infrastructure.

CLOUD INFRASTRUCTURE, CYBERSECURITY, CLOUD SYSTEM PROTECTION, METHODS AND MEANS OF SECURITY OF CLOUD INFRASTRUCTURE, TECHNOLOGY FOR PROTECTING CLOUD INFRASTRUCTURE

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

БД – база даних

КІД – керування ідентифікацією та доступом

OCI – Oracle Cloud Infrastructure

ПЗ – програмне забезпечення

ХІ – хмарна інфраструктура

ХС – хмарний сервіс

IaaS – Infrastructure as a Service

ВСТУП

Актуальність дослідження. Цифрова трансформація сучасного світу за останні роки набрала неймовірних обертів за рахунок швидкого та глобального розвитку ІТ-галузі, яка торкнулась великої кількості приватних підприємств, державних установ та інших організацій різного рівня, а також і життя будь-якої людини окремо. Це призводить до ще більшого множення, ускладнення і у той же час прискорення багатьох цифрових процесів життєдіяльності людства, що у свою чергу потребує ще більших та значніших ресурсів та «території» для її зберігання, обробки та існування. Хмарні технології – один з основних майданчиків, де в повній мірі може розвиватися сучасний світ.

Унікальні у своєму роді хмарні технології – надання користувачу ресурсів та потужностей у вигляді інтернет-сервісу – на разі є однією з провідних галузей розвитку ІТ. Її актуальність цілком і повністю вийшла з її можливості зменшити витрати, бути здатною до масштабування та гнучкістю, що дозволяють компаніям значно оптимізувати свої ресурси. Окрім цього, це значно зменшує піклування клієнта про капітальні витрати, про адміністрування та часто вирішує питання забезпечення безпеки.

Безпека завжди буде гострим питанням, коли мова йде про ІТ та цифрову трансформацію. Хмарні сервіси, як їх частина, вже давно активно існують в життєдіяльності бізнесу та державних установ західних країн, та дедалі більше охоплюють ті ж зони тут, в Україні. Будь-яка установа, чи то приватне підприємство, чи медична система, чи державний сервіс послуг, містять сотні тисяч вразливих даних, виток, модифікація чи втрата яких може призвести не лише до колосальних фінансових та ресурсних збитків, а й стати загрозою життю людини.

Тому можливість, знання та вміння забезпечувати захист хмарних сервісів є пріоритетом для фахівців з кібербезпеки. Проблема безпеки зараз потребує розробки якісних та дійсно працюючих технологій, які б могли значно полегшити

вирішення цієї задачі та надавали вже готову систему, що була б здатна підходити до цього питання комплексно.

Вищенаведені причини та аргументи актуалізують тему даної магістерської роботи, у якій проведено дослідження щодо технологій забезпечення захисту хмарних інфраструктур організації на базі Oracle Cloud Infrastructure.

Метою дослідження є розробка варіанту технології забезпечення кібербезпеки хмарної інфраструктури для організації та рекомендацій щодо використання технології для захисту хмарної інфраструктури організації.

Об'єкт дослідження – процеси захисту хмарної інфраструктури організації.

Предмет дослідження – технологія захисту хмарної інфраструктури організації.

Наукові завдання:

дослідити сутність проблеми забезпечення захисту хмарної інфраструктури організації;

визначити сутність завдань забезпечення захисту хмарної інфраструктури організації;

проаналізувати існуючі та актуальні технології забезпечення захисту хмарної інфраструктури організації;

проаналізувати методи та засоби забезпечення захисту хмарної інфраструктури організації;

проаналізувати основні функції та принципи реалізації забезпечення захисту хмарної інфраструктури організації.

Методи дослідження – робота з відповідної до даної теми літератури, аналіз експлуатаційної документації обраної системи, робота з міжнародними стандартами та їх порівняння, моделювання процесу забезпечення захисту хмарної інфраструктури організації.

Практичне значення одержаних результатів полягає в розробці варіанта технології забезпечення захисту хмарної інфраструктури організації на базі Oracle Cloud Infrastructure, а також у розробці рекомендацій щодо застосування створеної технології забезпечення захисту хмарної

інфраструктури в організації.

Апробація результатів магістерської роботи було оприлюднено на всеукраїнській науковій конференції «Актуальні проблеми кібербезпеки», яка відбулася 27 жовтня 2022 року в Державному університеті телекомунікацій, м. Київ; в журналі «Сучасний захист інформації» №1(49), 2022 р., в статті «Методики фішингу в мобільних системах».

1 АНАЛІЗ ПРОБЛЕМИ ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ

1.1 Призначення, архітектура та функції хмарної інфраструктури

Дана робота буде присвячена технології, що базується на хмарних обчисленнях, а саме являється підтипом хмарних можливостей – хмарна інфраструктура (далі – ХІ). Відповідно до ISO/IES 17788 є три типи хмарних можливостей, що принципово відрізняються один від одного видами ресурсів та функціями, якими оперують та які пропонують користувачеві. Але найважливішим є те, що кожна з трьох класифікацій слідує принципу розподілення проблеми, що мінімізує дублювання функціоналу кожного з типу:

тип можливостей додатку – тип хмарної можливості, який дозволяє використовувати клієнту хмари програми, що надаються постачальником послуги хмари;

тип можливостей інфраструктури – тип, який надає клієнту хмари доступ до використання її ресурсів зберігання, обробки даних та можливостей її мережі;

тип можливостей платформи – тип можливості, що дозволяє клієнту хмари розробляти, керувати та використовувати створенні самим клієнтом додатки та програми використовуючи більше однієї мови програмування та більше одного середовища виконання, які підтримуються самою платформою.

Можливості є окремою класифікацією хмарних обчислювань, але активно впливають на формування категорії хмари. Категорія хмарних сервісів (далі – ХС) – це група сервісів хмари, яких об’єднує деякий спільний набір функцій та якостей та може включати характеристики однієї з хмарних можливостей [1]. Проте, не дивлячись на свою відмінність, архітектурно ХС побудовані однаково.

NIST (National Institute of Standards and Technology*)* – Національний інститут стандартів та технологій, що керується Комерційний департаментом США та встановлює стандарти й рекомендації для багатьох технологічних сфер [13].

У свої спеціальній публікації 500-291, де NIST зібрали максимальну ознайомчу інформацію щодо хмарних обчислювань, розробили також архітектуру хмарних обчислювань, на основі загальних знань та розумінь щодо хмари, яка містить п’ять базових учасників з відповідними до них ролями. Для подальшого аналізу, є доцільним розглянути цю архітектуру.

Архітектура хмарних обчислювань від NIST складається з п’яти основних учасників: користувач хмари, провайдер хмари, хмарний аудитор, хмарний брокер та хмарний оператор (рис 1.1). Саме ці об’єкти хмари виступають її ключовими учасниками та виконують основні функціональні ролі ХС.

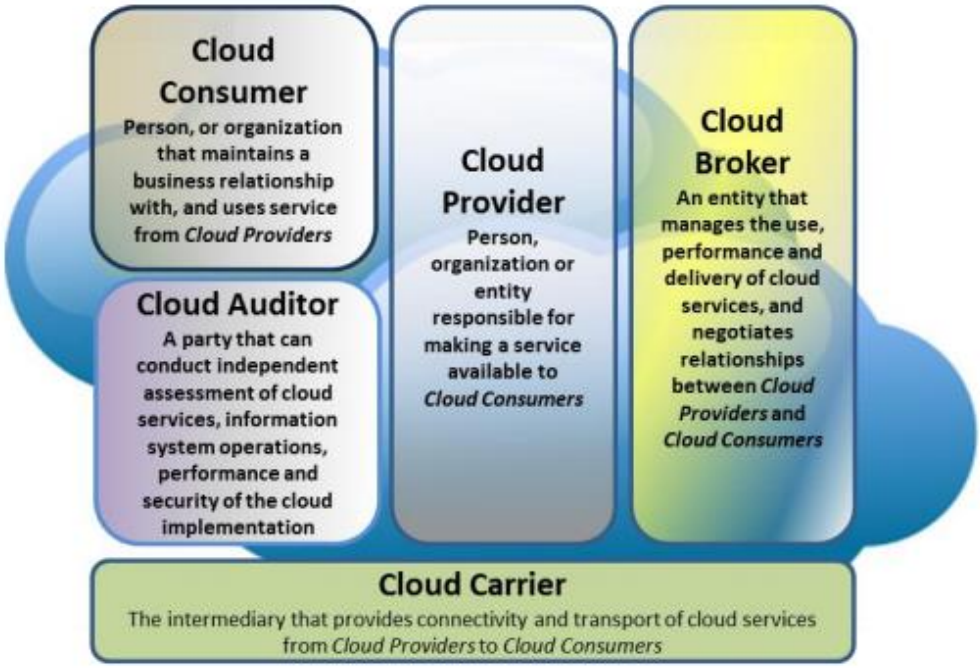


Рис 1.1 Учасники хмарних обчислювань відповідно до архітектури хмарних обчислювань NIST [6]

Клієнт хмари – суб'єкт, людина або організація, який отримує хмарні послуги від провайдера хмари. *Провайдер хмари* – людина або організація, яка надає послуги хмари клієнту хмари. Через відмінність між можливостями хмари та їх вплив на категорію хмарних обчислювань, які були згадані раніше та більше детально будуть розглянуті пізніше, провайдер хмари може надавати різний рівень

послуг, який буде формувати різні ступені відповідальності над контролем, безпекою та конфігураціями між постачальником хмари та її клієнтом [6].

Хмарний брокер – посередник між клієнтом хмари та її постачальником. Він забезпечує клієнта необхідною та зрозумілою йому інформацією, роз'яснює складні аспекти хмарних обчислювання та запропонованих послуг. *Хмарний аудитор* виступає незалежним суб'єктом моніторингу безпеки та ефективності ХС. А *хмарний оператор* є зазвичай організацією, що несе відповідальність за транзит даних [6].

Взаємодія цих п'яти учасників архітектури хмарних обчислювань добре та зрозуміло зображена на Рис. 1.2 з спеціальної публікації NIST, де лініями зображають взаємодію між суб'єктами хмарного сервісу – клієнт, аудитор, брокер та провайдер хмари, в той час як зелене поле виступає зоною впливу саме хмарного оператора.

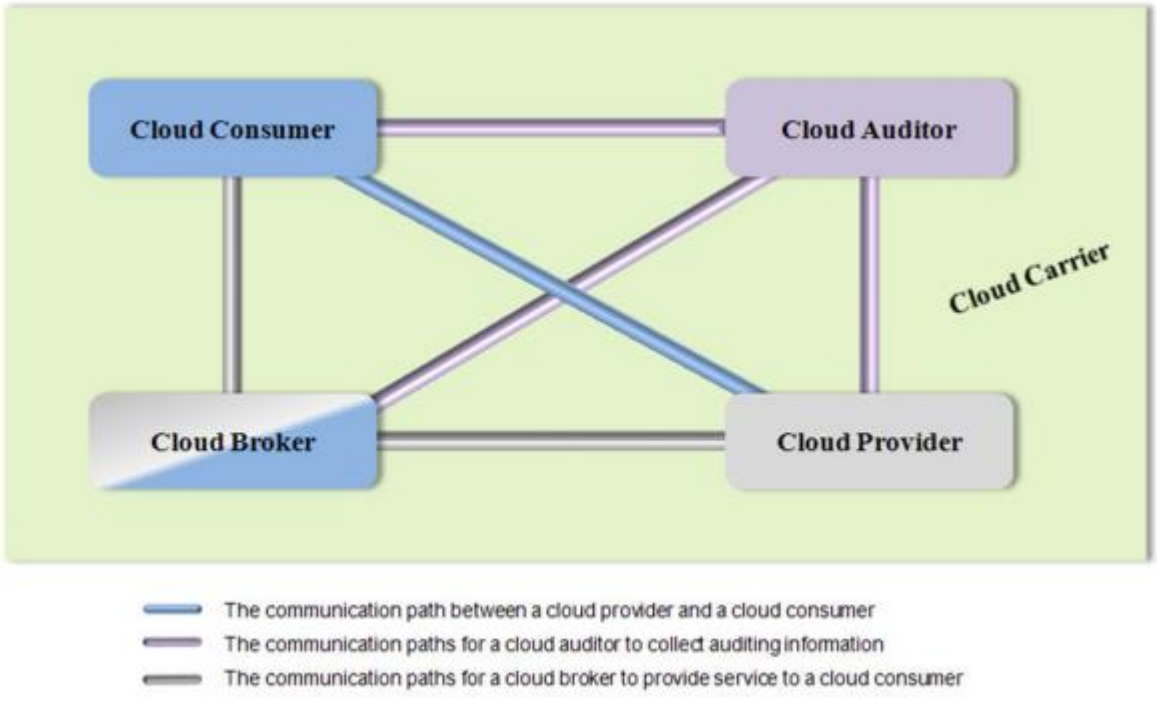


Рис 1.2 взаємодія учасників архітектури хмарних обчислень NIST [6]

І саме взаємодія між клієнтом та провайдером хмари, функції, які отримує користувач від постачальника (рис. 1.3), а також розподілення їх обов'язків відносно хмари є однією з характеристик ХС, яка ділить їх на різні категорії.

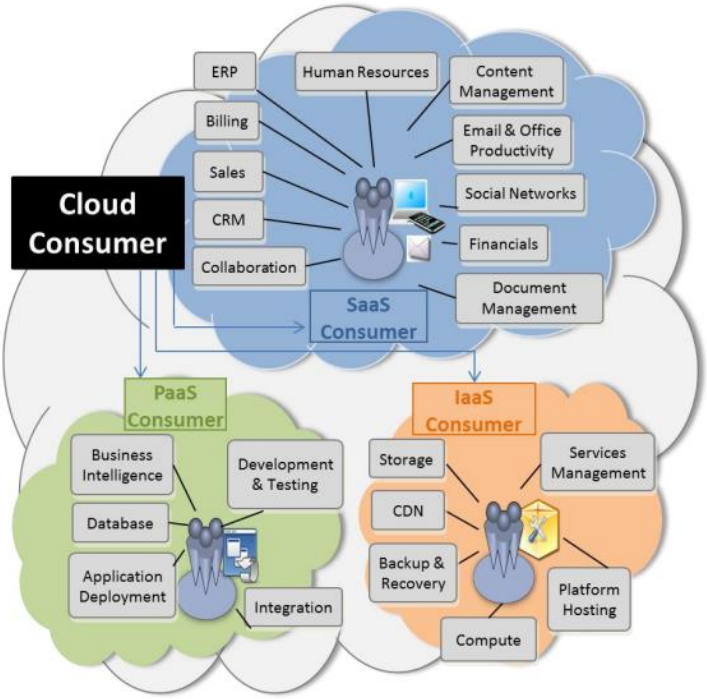


Рис. 1.3 Функціональні можливості різних категорій ХС відносно клієнта хмари [6]

В стандарті та рекомендаціях ISO/IES 17788 розрізняють декілька категорій ХС*: Communications as a Service (CaaS), Compute as a Service (CompaaS), Data Storage as a Service (DSaaS), Infrastructure as a Service (IaaS), Network as a Service (NaaS), Platform as a Service (PaaS), Software as a Service (SaaS)*. Всі вони надають різну комбінацію можливостей хмари і мають різне розповсюдження серед організацій та користувачів, але в цій роботі доречно більш детально розглянути лише декілька з них.

Software as a Service (SaaS) – це ХС, який надає функціонал типу можливостей додаток [1]. Це спосіб доставки додатку через Інтернет – як послуга. Тобто, замість того аби самостійно завантажувати, розгортати та обслуговувати ПЗ, клієнт отримує до нього доступ через інтернет уникаючи багаторівневого та складного керування ПЗ та обладнання. В такому ХС безпечність, доступність та виробничу потужність додатку забезпечує провайдер ХС. Окрім цього, ПЗ, яке використовує клієнт, базується в публічні хмарі [1]. Приклад: клієнт використовує додаток, а базові налаштування коригує провайдер – електронна пошта чи будь-

який інший офісний додаток (Рис 1.4).

Такі ХС часто додатково надають послуги, як: автоматизація бізнес процесів, поштовий маркетинг, керування співвідношеннями з клієнтами (CRM) тощо [3]. Прикладами SaaS можуть бути Dropbox, Google Applications, Salesforse тощо.

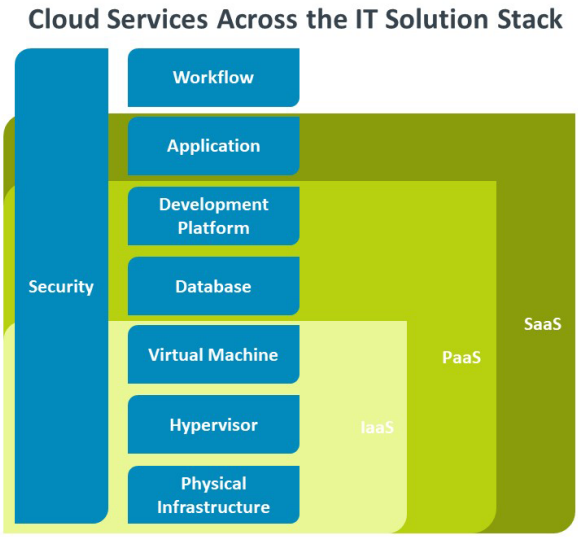


Рис. 1.4 Хмарна послуга SaaS в співвідношенні до інших ІТ-рішень

Platform as a Service (PaaS) – це ХС, який надає функціонал типу можливостей платформа [1]. Така ХС по своїй суті надає доступ користувачеві до ІТ-платформи, як то ОС, СУБД, об'єднуючі ПЗ та системи розробки та тестування, якими володіє провайдер ХС. PaaS не просто надає клієнту можливість використовувати ПЗ, але й вирішує питання апаратного забезпечення.

Тобто, на відміну від SaaS, що видно на рис. 1.5, де повністю все налаштовується менеджерами ХС і клієнту залишається лише користуватися обраним ПЗ, в PaaS клієнт має бути розробником або системним адміністратором, аби правильно розгорнути та налаштувати обране ним ПЗ на наданому йому апаратному забезпеченню, аби користуватись ним у подальшому. Такий сервіс базується не на публічній хмарі [1]. Приклад: клієнт керує додатками, а ОС бере на себе провайдер – база даних чи веб-сервер.

Така ХС додатково може надавати такі функції, як: фаєрволл, інтегроване середовище розробки (IDE), HTTP-сервери тощо [3]. Прикладами PaaS є: AWS

Elastic Beanstalk, Windows Azure, Google App Engine та інші.

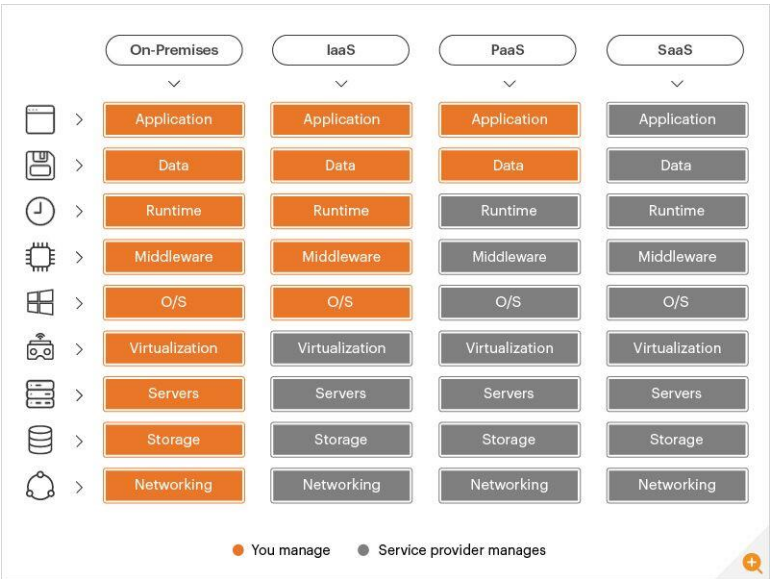


Рис 1.5 Хмарний сервіс PaaS в співвідношенні до інших IT-рішень

Infrastructure as a Service (IaaS) – це ХС, який надає функціонал типу можливостей інфраструктура [1]. ХС категорії IaaS надає користувачеві через третю сторону автоматизовану та масштабовану IT-інфраструктуру – сховище, хостування, обчислення та мережу – беручи ресурси з власних глобальних центрів даних (рис. 1.6).

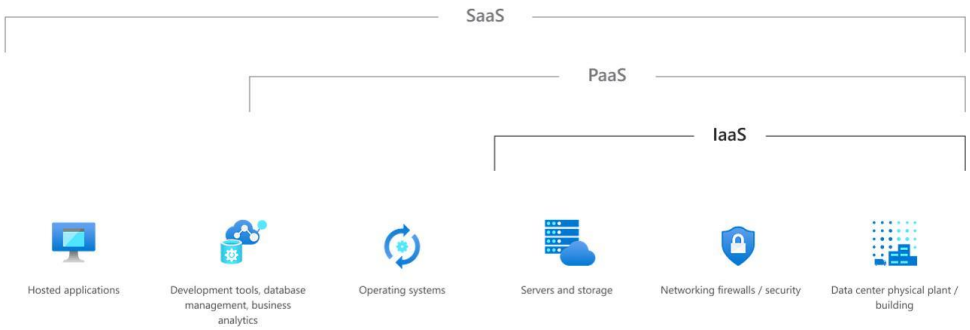


Рис 1.6 Хмарний сервіс IaaS в співвідношенні до інших IT-рішень

Особливістю IaaS є те, що клієнти такої ХС оплачують лише те, чим користуються по факту. Вона ж вирішує питання небажання організацією володіти всіма активами, як то ліцензії, ПЗ та сервери, а просто надає можливість брати в оренду ці ресурси. Приклад: клієнт розгортає будь-яке ПЗ та додатки – віртуальні сервери та віртуальні мережі. Такий сервіс може базуватись у приватній, публічній

та гібридні хмарі [1].

Така ХС надає наступні можливості: мережа, обчислення, зберігання, балансування навантаження [3]. Найпоширенішими прикладами IaaS є Amazon Web Services (AWS), Microsoft Azure та Oracle Cloud (Рис. 1.7). Останній приклад буде розглянутий в даній роботі.

Рис. 1.7 Рейтинг хмарних систем від Gartner за першу половину 2022 року

Відносно IaaS виділяють такі переваги:

Динамічне масштабування – провайдери IaaS надають можливість швидко надавати необхідну ємність та зменшувати її за потреби клієнта;

Підвищена безпека - провайдери IaaS вкладають значні ресурси та засоби в технології та знаннях аби забезпечувати якісну безпеку;

Самообслуговування – доступ до системи через просте інтернет-підключення;

Скорочення періодів простою – IaaS надає можливість швидко та ефективно відновлюватись після перебоїв;

Покращення швидкості – IaaS доступна для розробки нових проектів на ній,

одразу як усі засоби системи будуть забезпечені;

Скорочення капітальних витрат – зазвичай IaaS орієнтується на помісячну оплату;

Плати за те, чим користуєшся – розрахунки сплат робляться на основі метрик використання функцій IaaS [7].

Це робить IaaS найбільш доцільною організаціям, які мають постійне робоче навантаження, проте бажають його розподілити, вирішуючи питання рутинних задач та обслуговування інфраструктури; організаціям, які швидко розвиваються, але не мають відповідного капіталу, аби забезпечити себе необхідним апаратним забезпеченням. Тобто IaaS найкраще забезпечує масштабуванням та швидким наданням послуг.

Але, подібна система, заснована на наданні в більшості саме апаратних ресурсів має наступні недоліки:

Керування доступністю – навіть найбільші провайдери IaaS можуть мати простої;

Залежність від широкосмугового доступу – допоки підключення забезпечує якісне Інтернет-з’єднання – усе працює;

Обмеженість налаштувань та конфігурацій – публічні хмари мають обмежений доступ та можливість до унікальних налаштувань;

Складність SLA – угода про рівень послуг (SLA) зазвичай є доволі складною для розуміння;

Неочікувані витрати – помісячна сплата може збільшуватись та/або пікова активність використання, на якій будуються розрахунки, виявиться більшою за очікувану;

Ризики безпеки – IaaS провайдери забезпечують лише фізичну безпеку інфраструктуру, її апаратну частину, в той час як за ПЗ відповідальність несуть лише користувачі;

Ризик безпеки – при втраті прямого доступу до інфраструктури можуть та виникають нові уразливості [7].

Саме ризики безпеки буде розглянуто в наступному підрозділі.

Отже, загалом будь-який хмарний сервіс є доцільною системою організації робочого процесу будь-якого типу організації, адже має чітко розподілені функції та можливості, а тому здатна бути підібраною відповідно до потреб та ресурсів того чи іншого підприємства. Окрім цього і сам ринок ХС має десятки представників різного рівня, формату та доступності, завдяки чому будь-який бізнес має змогу обрати найбільш влучний для себе варіант провайдера. Завдяки ХС організації здатні більш швидко розвиватись та автоматизувати свої робочі процеси, що прискорює їх подальше розширення, а також зменшує їх капітальні витрати, необхідність в самостійному адмініструванні та вирішує питання забезпечення безпеки та резервного зберігання.

1.2 Аналіз проблеми забезпечення захисту хмарної інфраструктури організації

Для хмарних провайдерів Інтернет став комунікаційною інфраструктурою, що використовує добре відомий TCP/IP протокол – ідентифікатор користувачів у павутині. І подібно до звичайного комп'ютера в мережі, віртуальна машина, якою являється ХС, має свій власний IP-адрес. І як у випадку з IP комп'ютера, зловмисник, не важливо: внутрішній чи зовнішній, - може цю адресу знайти. А це у свою чергу може надати йому інформацію про фізичні сервери, які використовує жертва, та інтегрувати в них свою власну віртуальну машину і з них розпочати свою атаку.

Хмарний сервіс складається з десятків однотипних віртуальних машин клієнтів, і у випадку, коли зловмисник отримує доступ до однієї з них, він автоматично здатен отримати доступ і до усіх інших, де містяться вразливі дані, виток, зміна та знищення яких може призвести до значних збитків. А для того, щоб отримати доступ до системи, зловмиснику потрібно лише аби провайдер ХС чи його клієнт допустили ряд помилок в конфігуруванні та налаштуванні цієї системи апаратно чи програмно.

Відповідно до McAfee 2019 Cloud Adoption and Risk Report 65% організацій по всьому світу використовують IaaS у своїй роботі, при тому, що її якісне

налаштування є деякою проблемою через значну кількість та складність конфігурацій, які має такий ХС. При цьому *21%* файлів у хмарі містять вразливу інформацію (рис. 1.8), що робить доступ неавторизованих осіб до системи ще більш шкідливим, ніж можна очікувати. Серед цих вразливих даних, окрім паролів, інформацій електронної пошти і т.п., є конфіденційна інформація – *27%* (бізнес плани, фінансові звіти, алгоритми продажів тощо), – яка може стати особливо цікавою для спроб злочинного доступу до неї.

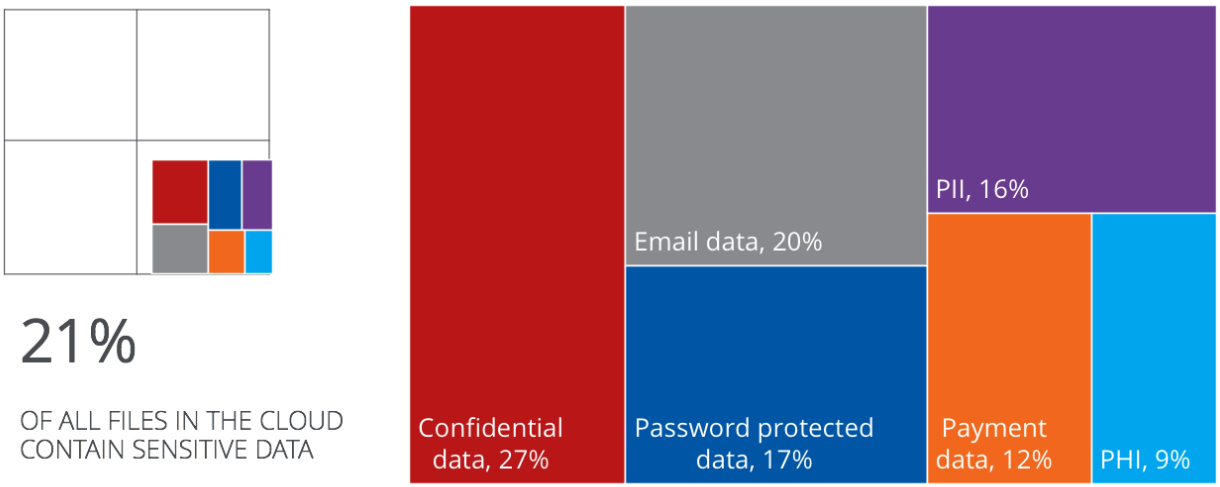


Рис. 1.8 Процентна діаграма вразливих даних в хмарі відносно до всіх даних всередині неї відповідно до звіту McAfee 2019 Cloud Adoption and Risk Report [8]

Хоч само по собі, розміщення вразливої інформації у хмарі не є обов'язково чимось негативним, проте ризик її пошкодження, викрадення або неавторизованої зміни зростає через не відповідне використання цих даних всередині системи чи спільного користування ними поза політикою цієї системи. В своєму дослідженні McAfee зазначають, що поширення чутливих даних відкритими каналами зросло на *23%* - дуже зручно поділитись необхідним файлом чи архівом за допомогою короткого посилання на нього в середині хмари. Проте подібний підхід є проблематичним, через те, що посилання надає доступ до папки/файлу будь-кому, хто має дане посилання. Тобто поділившись один раз посиланням, зростає ризик його повторного поширення вже іншій особі. І подібних ланцюжків може

трапитись значна кількість, що робить їх розслідування та вивчення неймовірно складним для фахівців з кібербезпеки.

Раніше у цьому підрозділі вже зазначалось, що налаштування такої ХС, як IaaS, через свою багаторівневість, може стати серйозним випробуванням для розробників та спеціалістів організації. «Організації мають в середньому 14 неправильно налаштованих IaaS/PaaS конфігурацій, що працюють за один раз, в результаті чого в середньому 2,269 окремих інцидентів існують у системи кожного місяця» - відзначається у звіті McAfee. Так, наприклад, виникає проблема відсутності шифрування у S3 блоках AWS, що робить дані, які вони містять, публічно-доступними.

В цілому відзначаються такі *проблеми конфігурацій* в IaaS:

Не ввімкнене шифрування блоків S3;

EBS шифрування даних не ввімкнене;

Відсутній розподіл доступу через ролі IAM;

Відключені журнали VPC Flow;

Відсутня двофакторна аутентифікація користувачів IAM.

Окрім ризиків безпеки, що виникають від неякісного налаштування XI, відповідно до дослідження McAfee, кожний 12,2 інцидент в організації кожного місяця – є НД третіх лиць до корпоративних даних, що зберігаються в хмарі, за рахунок попередньо викрадених облікових даних. Подібні інциденти стосуються 80,3% організацій, що були опитані. 92% з організацій, що приймали участь в аналізі McAfee, мали витік облікових даних, які тепер доступні для продажу в Darknet, тобто у Тіньовій павутині.

Symantec, щодо зазначеного вище, відзначає, що більшість подібних інцидентів – викрадення облікових даних – відбувається для подальшого встановлення зловмисником своїх власних командно-контрольних (C&C) серверів, шкідливих сайтів. Це призводить до того, що клієнти, які мають довіру до хмари, можуть скористатися чи зайти на шкідливий сайт/сервер і потрапити у руки зловмисникам. Також подібний витік облікових даних дає змогу зловмисникам використовувати отримані ресурси хмари для майнінгу (здобуття) криптовалют чи

для запуску DDoS-атаки на інші свої жертви.

Але найбільшою проблемою витоку даних є доступ зловмисників до вразливої чи конфіденційної інформації клієнтів хмари, що є проблемою як для самих клієнтів (бізнес-підприємства, медичні та державні установи тощо) так і для провайдерів ХС. Доступ авторизованого користувача може надати можливість не лише читати та видаляти дані, а й модифікувати їх та знімати на власні накопичувачі для подальших маніпуляцій чи розповсюдження.

До того ж у звіті SailPoint зазначається, що підприємства, які намагаються підтримувати безперервність свого бізнесу, зазвичай, упускають контроль тих, хто має доступ до ХІ. З цього ж дослідження видно, що **45%** атак відбулися через відсутність видимості та контролю доступу. Причиною є використання декількох IaaS, що призводить до очевидних проблем з відповідним керуванням доступами. Спроби покладатись на різні інструменти управління ХІ ще більше ускладнюють це питання, тому на виході **97%** опитуваних компаній відчувають проблему на собі і являються вразливими до потенційних кібератак [11].

Gartner – дослідницька та консалтингова компанія, що спеціалізується у сфері IT – у свої публікації «Well-known Gartner's Seven Security Issues Which Cloud Clients Should Advert» визначає 7 наступних проблем безпеки в хмарі:

Привілейований доступ користувачів: конфіденційні дані, що оброблюються за межами організації, вже є зоною ризику, адже аутсорсингові послуги по факту обходять усі рівні контролю, які клієнти хмари використовують над внутрішніми програми.

Відповідність нормативним вимогам: у відносинах між ХС та клієнтом основну та остаточну відповідальність за безпеку та цілісність несе саме клієнт, навіть якщо їх зберіганням займається провайдер. Останні несуть відповідальність за доступність до даних, що вони зберігають та забезпечення лише зовнішнього аудиту.

Розташування даних: використання хмари надає доступ до ресурсів, місцезнаходження яких зазвичай мало турбує клієнта, що зменшує контрольованість даних, які розміщуються на цих ресурсах.

Розподілення даних: в одній хмарі зазвичай знаходяться дані одразу кількох клієнтів, що вже створює деяку проблему розмежування та правильного шифрування. І хоч останній метод є ефективним, проте він не забезпечує 100% безпеки від витоку даних.

Відновлення: у випадку збою, простою, пошкодження чи знищення серверу хмари, що чекає на дані, що там зберігались? Питання забезпечення відновлення даних у подібному випадку стоїть доволі гостро, і рішення відрізняється від провайдера до провайдера. Також важливо брати до уваги, що клієнти віддають перевагу не наданню третім особам доступу до контролю їх даних, тримаючи відносини щодо контролю та безпеки виключно між ними та провайдером хмари.

Розслідування: для фахівців з безпеки є особливо складним питання досліджувати ХС, оскільки усі логи, дані та журнали декількох клієнтів можуть бути розташовані разом та розподілені по різним наборам, що часто змінюються.

Довгострокова життєздатність: клієнт має бути впевнений, що його дані залишаться доступними та фізично захищеними не в залежності від того, чи буде розорена компанія провайдера, чи він буде поглинутий кимось іншим, хто має відмінну політику [12].

Отже, серед основних проблем забезпечення захисту XI, відповідно до досліджень, можна виділити:

проблеми з відповідним налаштуванням параметрів хмари, що може призвести до витоку даних з інформаційних «бакетів» (розподілених буферів даних), невідповідного розподілу доступу, відкриття облікових даних в публічних сховищах;

вразливість до таких атак як DoS чи DDoS, які здатні призвести до недоступності системи протягом значного часу і принести вражаючі втрати для будь-якої компанії;

складність з керуванням доступами, що може призвести до витоку даних через аутсорсингові канали, через невдоволеного працівника чи зловмисника, що отримав доступ до облікових даних одного з працівників;

зниження інфраструктурної видимості XI через модель спільної

відповідальності – між клієнтом та провайдером ХС – ускладнює можливість якісно та детально підійти до питань налаштування та забезпечення відповідної захисту для системи, адже в цьому питанні задіяні дві окремі сторони, одна з яких може допустити критичні для безпеки помилки;

можливість самообслуговування всередині хмари IaaS, що робить останню дуже привабливою в питанні ціни і значно легшою в використанні, може призвести до утворень тіньового ІТ або до тіньового використання ІТ ресурсів, за чим може слідувати витік даних, порушення законодавства, витрата несанкціонованих ресурсів, що збільшують ціну за оренду ХІ.

1.3 Аналіз існуючих методів захисту хмарної інфраструктури організації

Так як в IaaS провайдер забезпечує користувача апаратними ресурсами, то зі своєї сторони саме він керує їх захистом, в той час як клієнт бере на себе відповідальність за програмну безпеку своєї хмари. Ця самообслуговання та відсутність інфраструктурної видимості, про які говорилось в минулому підрозділі, часто стають значними проблемами в питанні забезпечення якісного захисту.

В процесі забезпечення захисту інформації обидві сторони приймають неопосередковану участь, але їх прямі обов’язки чітко визначаються у угодах про надання послуг, які у свою чергу базуються на міжнародних напрацюваннях та рекомендаціях, якім слід приділити увагу перед тим, як розглянути існуючі технологічні рішення у різних IaaS.

Розглянемо основні методики та рекомендації щодо забезпечення безпеки хмари, які надають такі організації як ISO/IES та NIST.

Щодо забезпечення безпеки та приватності хмари, В. Янсен та Т. Гренс розробили настанови, які були видані в спеціальній публікації 800-144 від NIST. Далі ми розглянемо лише декілька частин даного документу, для попереднього ознайомлення з ним та розкриття теми розділу.

В настановах публікації 800-144 рекомендації поділені на 9 зон: управління, відповідність, довіра, архітектура, керування ідентифікацією та доступом (КІД), ізоляція ПЗ, захист даних, доступність, реагування на інциденти.

Управління. Щодо керування рекомендовано розширити зону організаційних практик, які відносяться до політик, процедур та стандартів всередині організації та відносяться до розробки додатків та надання послуг у хмарі, а також охоплюють моніторинг використання та реалізації розгорнутих та задіяних служб. Окрім цього доречним буде впровадження механізмів аудиту, які будуть слідкувати за дотриманням визначених організацією практик протягом життєвого циклу системи.

Відповідність. У розділі про відповідність головними рекомендаціями будуть звертання уваги на деталі законодавства та контракту, який надає провайдер XI. Доцільним при організації захисту хмари звернути увагу на законодавство держави, її нормативні акти, які охоплюють питання хмарних обчислень. Важливо виявити які зобов'язання ці закони та норми накладають на саму організацію, особливо щодо місцезнаходження даних, конфіденційності та безпеки цих даних, правил керування записами. Не останнє місце займає уважне вивчення пропозицій провайдера хмари щодо організаційних вимог, які необхідно виконати і сам контракт відповідає законодавчим нормам. Також проаналізуйте чи не порушує електронне виявлення провайдера конфіденційність та безпеку даних і програм.

Довіра. Зона довіри охоплює керування доступами всередині організації, які мають забезпечити конфіденційність та захищеність вразливих даних. Необхідно переконатись, що механізми обслуговування від постачальника здатні забезпечити видимість процесів та елементів керування безпекою, а також їх здатність бути актуальними в довгостроковій перспективі. Чітко окреслити права власності на дані. Підібрати та інтегрувати програму управління ризиками, яка здатна бути достатньо гнучкою, аби мати змогу адаптуватись до мінливого ландшафту небезпек на увесь час життєвого циклу системи. Не нехтувати актуалізацією даних щодо безпеки всієї системи, аби підтримувати доцільність рішень щодо управління ризиками.

Архітектура. Публікація 800-144 також рекомендує зрозуміти та базово вивчити основні технології, які використовує обраний провайдер хмари, в тому числі які наслідки можуть нести ті чи інші засоби контролю на безпеку та конфіденційність системи протягом усього її циклу.

Керування ідентифікацією та доступом. Щодо КІД клієнт має переконатись, що встановив якісні та відповідні засоби забезпечення безпеки правильної автентифікації, авторизації та ідентифікації і відповідним доступом. І ці налаштування мають відповідати умовам організації.

Ізоляція ПЗ. Оцініть ризики безпеки ваших ПЗ на основі аналізу того, яку віртуалізацію використовує провайдер хмари, якими логічними методами ізоляції він керується всередині своє системи на велику кількість користувачів.

Захист даних. Щодо захисту даних публікація 800-144 рекомендує проаналізувати якими рішеннями провайдер даних керується при контролі доступу до даних в стані їх спокою, під час транспортування, використання та дезінфекції. Оцініть ризик від інших користувачів хмари обраного вами провайдера. Вивчити та зрозуміти як працюють методи шифрування у обраного вами провайдера та визначити які ризики він за собою несе.

Доступність. Важливими будуть питання резервного копіювання та відновлення даних. Як організовано цей процес у обраного провайдера, чи є у нього процес аварійного відновлення. Переконайтесь, що ці процеси відповідають вимогам організації щодо безперервності роботи та планам у випадку екстрених ситуацій. Також визначить, чи здатний провайдер забезпечити негайне відновлення робочих процесів та за які терміни він може їх організовано відновити у випадку непередбачуваної та/або серйозної катастрофи.

Реагування на інциденти. Важливо ознайомитись та узгодити положення контракту з провайдером та його процедурами реагування на інциденти, оцінити їх відповідність вимогам та очікуванням організації. Доцільним є упевнитись, що провайдер хмари має прозорий процес реагування та має якісно організований процес для обміну інформацією до та після інциденту з організацією. Також треба переконатись, що організація також в змозі реагувати на інциденти відповідно до

свої вимог та вимог провайдера хмари, враховуючі їх відповідні ролі та обов’язки щодо обчислювального середовища.

Також, доволі цікавим у Публікація 800-144 від NIST є список вимог безпеки від клієнта до провайдера хмари, що мають допомогти обрати найбільш підходящого організації постачальника XI. В цей список входять наступні вимоги:

вимоги до персоналу, що включає в себе також дозволи, ролі та обов’язки;

нормативні вимоги;

доступність наданої послуги;

сповіщення про актуальні проблеми, процедура їх перегляду та підходи до їх вирішення;

правила, угоди та процедури щодо оброки та розкриття інформації;

контроль фізичного та логічного доступу, якими керується провайдер хмари;

як відбувається процес контролю доступу до мережі, фільтрація трафіку, процес підключення;

які параметри захисту даних використовує провайдер;

конфігурація системи та керування виправленнями;

резервне копіювання та відновлення даних;

протоколи зберігання та очищення даних;

сканування безпеки та вразливостей системи;

процес управління ризиками;

процес звітування, регулювання та вивчення інцидентів;

безперервність операцій

керування ресурсами;

наявність відповідних сертифікацій та акредитацій;

відповідні гарантій;

незалежний аудит надаваних послуг.

Окрім загальних рекомендацій щодо організаційного забезпечення безпеки, публікація містить доцільні пропозиції щодо організації аутсорсингової активності, які поділені на три зони: попередні дії, початкова та супутня діяльність, підсумкова діяльність. У свої суті вони максимально підсумовують і вимоги до провайдера

вище, і основні задачі для забезпечення безпеки, які розглядались на початку підрозділу.

Попередні дії. Визначити вимоги до безпеки, конфіденційності тощо, яким має відповідати провайдер ХІ, вони стануть критеріями відбору. Проаналізуйте елементи керування безпекою та конфіденційністю, які надає постачальник хмари, та оцініть їх ризики в контексті контролю цілей організації. Оцініть, чи здатен постачальник хмари надавати хмарні послуги в обіцяному та відповідному вигляді протягом життєвого циклу, при цьому забезпечуючи очікуванні рівні безпеки та конфіденційності.

Початкова та супутня діяльність. Важливим є переконатись, що всі вимоги та зобов'язання обох сторін, в тому числі про забезпечення конфіденційності та безпеки, чітко прописані в угоді про надання послуг і що вони схвалені обома сторонами. Доцільним буде залучення юридичного консультанта для оцінки угоди про надання послуг і його присутності під час будь-яких переговорів щодо надання цих послуг. Час від часу доречним є оцінка продуктивності провайдера хмарних послуг і якості надання послуг, аби забезпечити відповідне до контракту виконання усіх зобов'язань , що також є частиною керування ризиками та зменшування їх ймовірності.

Підсумкова діяльність. Завжди важливо нагадувати провайдеру послуг, у випадку розірвання угоди чи завершення партнерства, про будь-які договірні вимоги, які мають бути виконати опісля. Скасувати усі можливі та попередньо доступні фізичні та електронні доступи, що були надані провайдеру хмари, і вчасно оновити фізичні маркери та ярлики. І на останок упевнитись, що провайдер притримується умов угоди, щодо наданих та архівованих ресурсів організації, відповідно повертає їх та відновлює у стані, що буде придатним до використання, а також належним чином видаліть її зі своїх ресурсів.

ISO (International Organization for Standardization) та IES (International Electrotechnical Commission) – дві найвідоміші міжнародні технологічні організації, які займаються розробкою стандартів.

Для стандартизації рекомендацій щодо захисту ХС ISO/ IES взяли за основу

один зі свої ранніх документів ISO/IEC 27002, який є значущою базою у питанні забезпечення інформаційного захисту у ІТ-системах. У даній роботі ми розглянемо лише деякі уточнення, що були додані в цей документ, для його стандартизації саме відносно захисту хмари.

Перші корективи вносять у питання політики ІБ, де одразу відбувається розподіл обов'язків між клієнтом та провайдером хмари, про які говорилось раніше. Відповідно до ISO/IEC 27017.

Зі сторони клієнта. При розробці власної політики ІБ, організація має, по-перше, спиратися на визначенні допустимі рівні ризиків ІБ відносно інформаційних та інших активів організації, і, по-друге, брати до уваги наступне:

можливість доступу до інформації, що зберігається в ХС, та керування нею зі сторони провайдера ХІ;

наявність можливості обслуговування активів в ХС (приклад: ПЗ);

можливість виконання процесів в багатотенатному віртуалізованому ХС;

користувачів ХС та середовище, в якому вони будуть використовувати політику ІБ;

адміністраторів ХС зі сторони користувача ХС, тобто наявність доступу з привілеями;

географічне місцезнаходження організації провайдера ХС та країни, в яких провайдер може зберігати дані о користувачі ХС [15].

При створенні політики ІБ клієнту хмари завжди треба пам'ятати що створена ним політика охоплює лише інформаційні та бізнес-процеси користувача ХС і не має відношення до тих самих процесів, але зі сторони провайдера хмари.

Зі сторони постачальника. Провайдеру хмари, при створенні чи редагуванні політики ІБ, рекомендовано враховувати наступні положення:

базові вимоги до ІБ, що мають відношення до проєктування та інтеграції ХС;

ризики, які можуть бути викликані інсайдерами з відповідними доступами;

багатокористувацьке середовище та ізоляцію користувачів, що включає в себе і віртуалізацію;

наявність доступу до активів користувача ХС для провайдера послуг хмари;

взаємодія з користувачем під час керування змінами;

безпечність віртуалізації;

доступ до даних користувача ХС та їх відповідний захист;

керування життєвим циклом облікових записів користувачів хмари;

інформування про порушення та провідні принципи в питанні обміну інформацією та даними у разі допомоги під час розслідування та криміналістичного дослідження [15].

Загалом, безпечність віртуалізації в хмарі складається з декількох аспектів, які включають в себе зберігання та контроль доступу до віртуалізованних образів, обробку неактивних та відключених віртуальних систем, керування їх життєвим циклом, моментальних знімків та захист гіпервізору і засобів керування безпекою використання точок самообслуговування.

Відносно ролей та обов'язків ISO/IEC 27017 зазнає високу важливість чіткого розподілення та документування ролей і обов'язків у процесі взаємодії користувача та провайдера ХС. Так, при неоднозначному розподіленні ролей, не коректному визначенню права власності даними, обов'язків, щодо керування доступом та обслуговуванням інфраструктури, можуть призвести до комерційних і юридичних суперечок. Окрім цього дуже важливо визначати відповідального за безперебійність процесів, резервне копіювання та відновлення даних у випадку збою, аби уникнути витоку даних через непорозуміння між обома сторонами.

Зі сторони клієнта. Користувач має узгодити з провайдером ХС відповідне розподілення ролей та обов'язків в області ІБ, та упевнитись, що він здатен виконувати визначені для нього обов'язки та ролі. Ці ролі та обов'язки мають бути задокументованими. Також клієнт ХС має визначити порядок взаємодії з функцією клієнтської підтримки та обслуговування провайдера ХС, і бути здатним керувати цією взаємодією .

Зі сторони провайдера. Провайдер ХС має затвердити та задокументувати відповідний розподіл ролей та обов'язків відносно ІБ з усіма своїми користувачами, постачальниками ХС та іншими постачальниками.

Також, доволі важливої частиною забезпечення ІБ, в незалежності від

системи, типу організації тощо вона існує, є правильне навчання працівників, що взаємодіють з обраною системою.

Зі сторони клієнта. Тренінги, щодо користування хмарою, проводяться в першу чергу для тих, хто буде найбільше взаємодіяти з системою, або несе за неї відповідальність зі сторони користувача. Серед цих людей можуть/мають бути керівництво, менеджери, адміністратори, інтегрувальники та інші користувачі ХС. Це забезпечить координовану дію зі сторони працівників у питанні забезпечення ІБ. В ці учбові програми мають входити:

стандарти та процедури використання ХС;

ризики ІБ, що будуть пов'язанні з ХС, та способи керування цими ризиками;

ризики системного чи мережевого середовища при використанні ХС;

використання нормативно-правової бази [15].

Зі сторони провайдера. Провайдер ХС має забезпечити проходження учбових та інформаційних програм своїми працівниками, а також вимагати від них навчання відносно коректного користування з інформацією користувачів ХС, та даними загалом, що надходять з хмари. Адже такі дані можуть нести в собі вразливу, конфіденційну інформацію користувачів ХС, або взагалі такі дані можуть мати обмежений доступ до них [15].

ISO/IEC 27017 також розглядає менеджмент активів і має щодо них окремі рекомендації для сторін взаємодії ХС. Адже саме визначення даних, що були отримані з хмари, як активів та їх відповідний облік якісно впливає на покращення ситуації з ІБ.

Зі сторони клієнта. Інвентаризація активів користувача має враховувати інформацію та відповідні активи, що знаходяться в середовищі хмари. Має бути чіткий розподіл та тегування (вказування) їх місцезнаходження в цій хмарі.

Зі сторони провайдера. Інвентаризація активів постачальника ХС має чітко визначати: данні користувачів ХС та дані, що отримані з хмари.

Важливими також стануть рекомендації щодо криптографії, яка має забезпечувати безпечність даних у хмарі. Так, відносно політики використання криптографічного захисту загалом можна відзначити, що деякі типи даних, як то

медичні картки, номера паспортів тощо, по факту мають бути захищені шифруванням, але є деякі інші визначення, що будуть відноситись окремо до клієнта хмари та постачальника.

Зі сторони клієнта. Користувач ХС має реалізувати криптографічний захист інформації відносно визначених ним ризиків, і обрані міри мають бути достатньо ефективними для усунення ризиків, в незалежності від того, хто надає ці міри захисту: клієнт чи провайдер ХС. Окрім цього, користувач має упевнитись, що криптографічний методи захисту, які надає йому провайдер (якщо це обумовлено типом ХС та угодою між клієнтом та провайдером), відповідає наступним мірам:

вони відповідають вимогам політики щодо користувача ХС;

ці методи є сумісні з іншими криптографічними засобами захисту, які використовує клієнт хмари;

вони можуть бути застосовані до даних у їх стані спокою чи під час транзиту в хмарну службу – як всередині неї так и поза її рамками [15].

Також клієнт ХС має визначити криптографічні ключі до кожної хмарної служби та бути здатним реалізувати керування ними. Тому, у разі використання власної системи керування ключами або окрему службу, користувач ХС не повинен надавати провайдеру хмари дозвіл на зберігання ключів шифрування для криптографічних операцій та керування ними.

У випадку, якщо провайдер ХС надає функцію керування ключами зі своєї сторони, тоді клієнт хмари має упевнитись у процедурах керування ключами, на основі наступних параметрів:

які типи ключів використовуються;

якою є специфікація системи управляння ключами, що включає в себе процедури на кожному життєвому етапі існування ключа (генерація, зміна та оновлення, зберігання, видалення, виведення, архівування та знищення);

рекомендовані клієнту ХС процедури щодо керування ключами [15].

За сторони провайдера. Постачальним має надати користувачу інформацію про випадки, коли криптографічний захист застосовується відносно інформації, що він оброблює. І також є важливим надання інформації клієнту ХС щодо методів

криптографічного захисту, яку використовує провайдер, аби той мав розуміння щодо використання власних криптографічних методів захисту.

ISO/IEC 27017 також надає інформацію щодо менеджменту ІБ.

Так, провайдер ХС має упевнитись, що клієнт ХС отримає відповідну до нього інформацію ІБ про:

перелік інцидентів ІБ, які відносяться до клієнта ХС;

опис ступеню розкриття виявлених інцидентів та які методи реагування було вжито;

терміни направлення сповіщень щодо виявлених інцидентів ІБ;

процедуру сповіщення;

контактними даними відповідальних за рішення питань щодо інцидентів;

методиками вирішення виникаючих інцидентів [15].

Також ISO/IEC 27017 містить індивідуальну рекомендацію щодо безпечного використання та експлуатації (куди входить керування виробничою силою системи, резервного копіювання, реєстрації та моніторингу, в тому числі щодо журналів аудиту адміністратора та оператора), безпечності комунікацій, розробка, підтримка та здобування системи, взаємодія з провайдером, відповідність.

В цьому розділі уло визначені призначення, архітектури та функцій хмарної інфраструктури, проаналізовано проблеми забезпечення її безпеки та розглянуто існуючі методики захисту. Окрім цього була наведена та описана термінологія, розглянуті нормативно-правові документи відносно проблем безпеки хмарної інфраструктури та методики їх рішення.

2 АНАЛІЗ МЕТОДІВ ТА ЗАСОБІВ ЗАХИСТУ ХМАРНОЇ ІНФРАСТРУКТУРИ НА БАЗІ ORACLE CLOUD INFRASTRUCTURE

2.1 Призначення, основні функції та рішення хмарної інфраструктури Oracle Cloud Infrastructure

Oracle Cloud Infrastructure (OCI) – це платформа ХС, яка надає можливість розгортати та запускати широкий спектр ПЗ зберігаючи при цьому стале високопродуктивне середовище [19]. В її арсеналі є: реляційні, OLAP, JSON та NoSQL бази даних, контейнери, Kubernetes, потокове передавання інформації, безсерверні функції, Spark, VMware, блокноти Jupyter – все, що є необхідним та важливим практично в будь-якій роботі. За рахунок розробки платформи з нуля, OCI здатна приймати на собі всі п’ять головних типів додатків, серед яких є додатки з реляційними БД, відомчі та технічні додатки (рис. 2.1). І окрім цього має широкий спектр SaaS, що покривають значну кількість відомчих та галузевих сфер. В тому числі OCI перша запровадила віртуалізації 2-ого рівня, що дозволяє користувачам хмари запускати VMware прямо під корпоративними ПЗ всередині самої OCI.

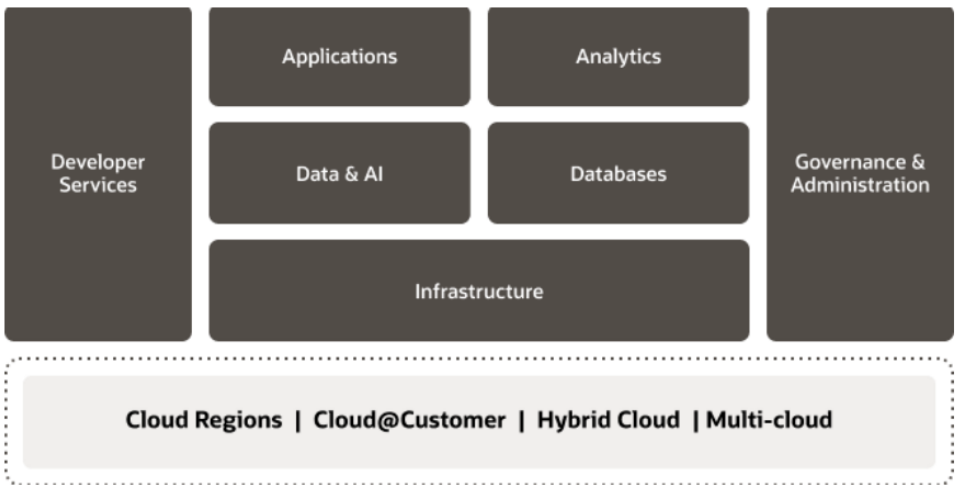


Рис. 2.1 Хмарні служби OCI [19]

Серед цих додатків OCI має: додатки, що використовують релятивні БД, додатки високопродуктивних обчислень (HPC - High Performance Computing),

сховище даних та Data Lake, веб- та хмарні додатки, VMware в хмарі або гібридні хмарні налаштування.

Додатки, що використовують релятивні БД. Багато існуючих корпоративних додатків (E-Business Suite, SAP тощо) використовують БД Oracle, адже вона надає високу продуктивність, широкий функціонал та висока доступність. Oracle Real Application Clusters (RAC) (Рис. 2.2) – функція БД Oracle, яка надає декільком кластеризованим екземплярам Oracle одночасно отримати доступ до спільної БД [19]. Іона забезпечує низьку затримку, високу доступність та онлайн доступність, яка важлива для багатьох стандартних корпоративних додатків. Ця функція використовує Oracle Clusterware у свої інфраструктурі, яка забезпечує поєднання взаємопов'язаних серверів в одну систему, зручну для кінцевого користувача. Але самостійне встановлення RAC є доволі дорогим та ресурсозатратним процесом, який можна замінити використанням сервісу Oracle Cloud Infrastructure Database – двохвузловий управляємий RAC-екземпляр.

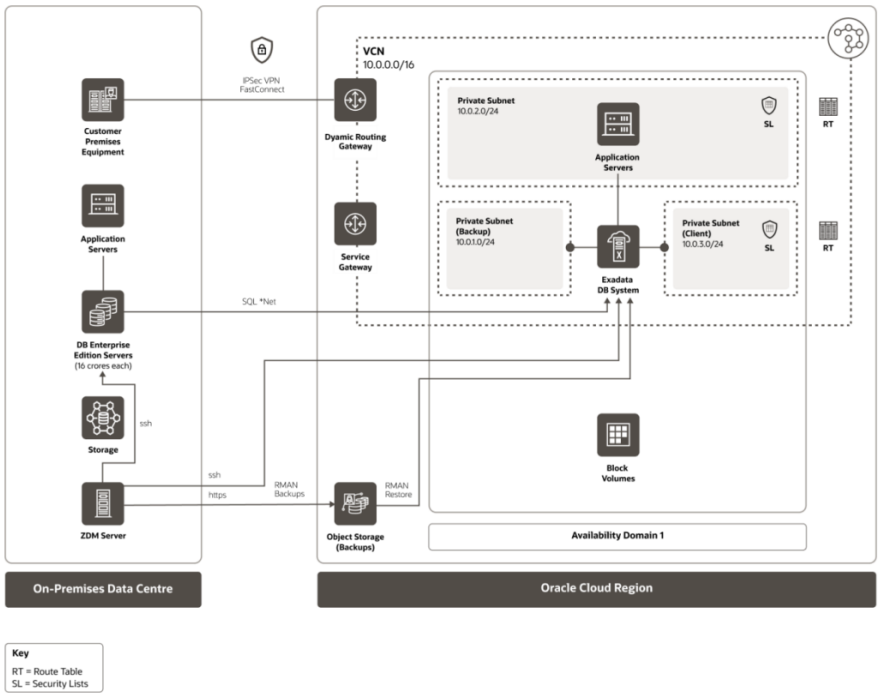


Рис. 2.2 Oracle Exadate Cloud Service та RAC в інфраструктурі OCI [19]

Додатки високопродуктивних обчислень. Навантаження високопродуктивних обчислень (HPC), такі як моделювання аварій, моделювання ризиків, визначення цифрових двійників, для аналізу великих наборів даних

потребують високої виробничої сили, високої пропускної здатності та низької варіативності. Для них важко підібрати правильне локальне середовище, легко створити умови для надмірного використання, високопродуктивні мережі складні в обслуговувані та графічні процесори, які приймають в аналізі значну участь, можуть швидко застаріти. Oracle налаштовує та розробляє кластери HPC відповідно до вимог та потреб клієнта або надає таку можливість як послугу, що здатна сприйняти навантаження MPI (Message Passing Interface – інтерфейс передачі повідомлень), яка початково була доступна лише для локального розміщення. Схематично HPC можна розглянути на рис. 2.3 нижче:

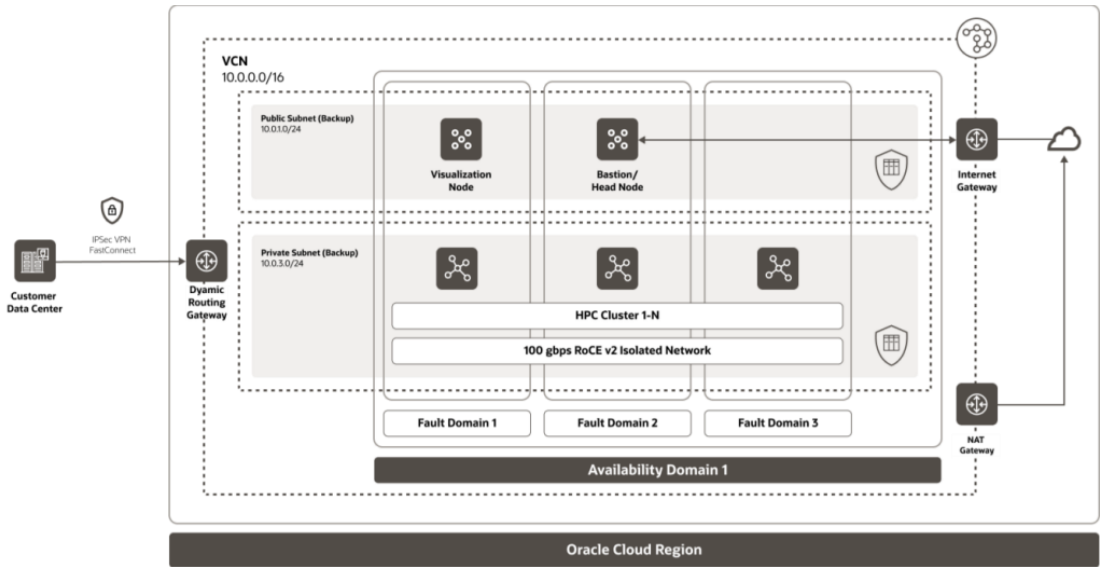


Рис. 2.3 HPC в інфраструктурі OCI [19]

Сховище даних та Data Lake. OCI надає можливість клієнту розгортати програми з великими даними у великих масштабах. Вона сприймає велику варіацію форматів даних у свої БД, у службі інтеграції даних OCI та для потокового передавання OCI з підтримкою Kafka Connector. Надає можливість утворити конвеєр даних, для їх подальшого зберігання та обробки, за допомогою зручної для користувача комбінації OCI Object Storage, OCI Data Flow (Spark), Oracle Big Data (Hadoop) або Oracle Autonomous Data Warehouse. На основі цих даних Oracle може допомогти з аналізом чи навчанням моделей за допомогою додатків Oracle Analytics Cloud, OCI Data Science, Oracle Machine Learning чи на основі інструментів від ряду інших виробників. У наведеній нижче еталонній архітектурі

(рис. 2.4) показано конвеєр даних із використанням служб Data Flow (Spark), Object Storage та Autonomous Data Warehouse.

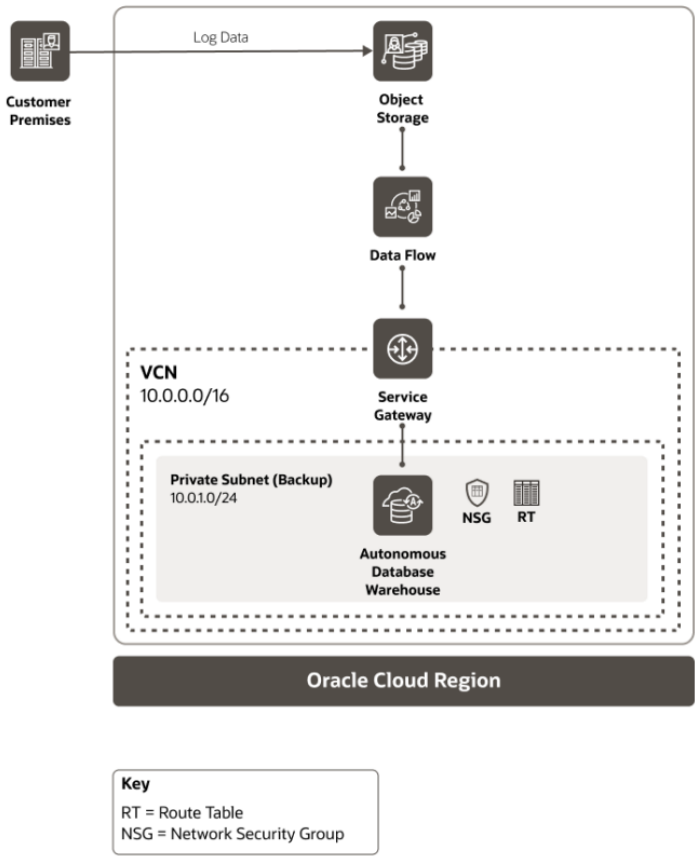


Рис. 2.4 Обробка лог-даних за допомогою OCI Data Flow (Spark) та Autonomous Data Warehouse на інфраструктурі OCI [19]

Веб- та хмарні додатки. Не завжди є легкою задачею попередньо визначити очікуваний трафік для веб-програм та додатків, що може призвести до надмірної пропускної здатності та фактичного низького використання обраного дорого обладнання та ресурсів. OCI в свою чергу надає безліч інфраструктурних додатків, такі як: віртуальні машини, контейнери, функції з великою кількістю налаштувань часу виконання та збереження даних та серверних платформ типу «голий метал» - платформа без ОС, яка надає прямий доступ ПЗ до апаратної частини. Окрім цього OCI є масштабованою, високо доступною та економічно ефективною платформою для будь-якого веб-додатку. Еталонна архітектура на рис. 2.5 демонструє масштабовану та високодоступну веб-програму, що працює на Oracle Cloud Infrastructure.

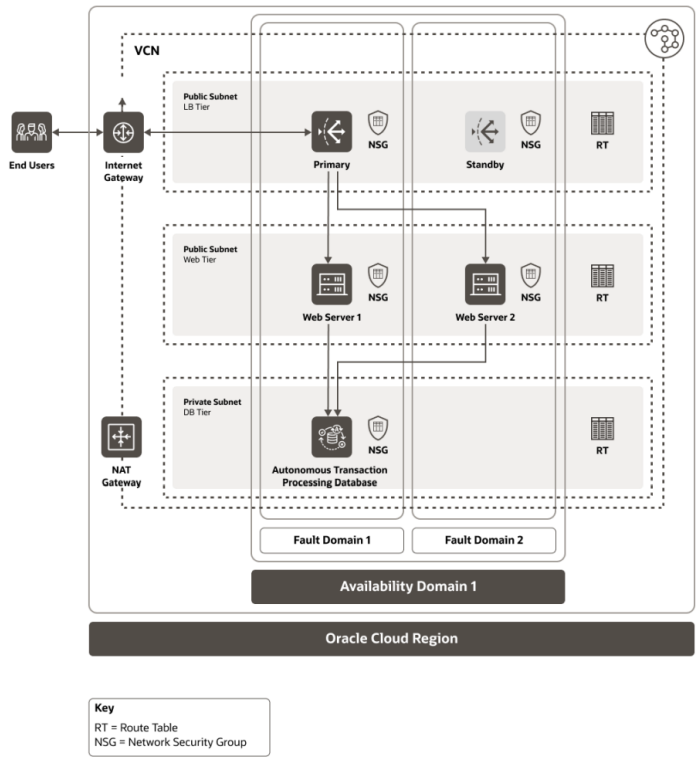


Рис. 2.5 Масштабований та високо доступний веб-додаток на платформі OCI [19]

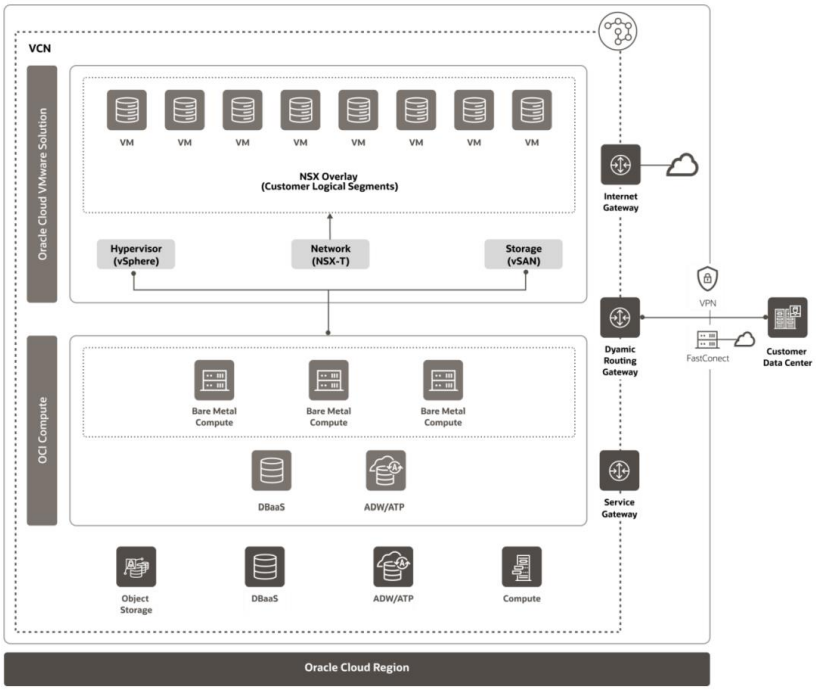


Рис. 2.6 Oracle Cloud VMware Solution на платформі OCI [19]

VMware в хмарі або гібридні хмарні налаштування. Зазвичай великі компанії, та і більшість інших, використовують VMware vSphere аби запускати та керувати програмами в свої центрах обробки даних. Але перехід з фізичного до хмарного

використання подібної системи несе за собою великі витрати та ризики, що викликані зміною архітектури та зміною знайомих IT-процесів. Для уникнення цих проблем OCI надає можливість користувачеві повний контроль над версією VMware, циклом виправлення та безпекою, за допомогою рішення Oracle Cloud VMware, яке виконує свої обіцянні функції за рахунок еластичної інфраструктури та прямого доступу до решти служб OCI. На рис. 2.6 можна побачити архітектуру VMware та рекомендації щодо її розгортання на платформі OCI.

Також OCI надає широкий спектр хмарних сервісів, деякі з яких згадувались трохи раніше, але в цій роботі будуть розглянути лише деякі з них окремо до кожної зони хмарних служб (рис. 2.7).

Рис. 2.6 Зони хмарних сервісних служб OCI [19]

Обчислення та контейнери. OCI Compute надає можливість клієнтові розгортати та керувати однокористувацьким сервером (виділений сервер типу «голий метал»), багатокористувацькими віртуальними машинами, віртуальними машинами з виділеним хостом, що використовує той самий набір API. Еластичність послуг та можливість OCI дає змогу обрати як і самообслуговуванні хости з погодинною оплатою або гнучкі VMware, для яких клієнт має можливість за короткий час визначити необхідну для своїх потреб кількість ядр та розмір пам’яті. Серед апаратних можливостей є процесори від Intel і AMD X86, процесори Ampere Arm і графічні процесори Nvidia [19]. OCI Infrastructure Container Engine for

Kubernetes – окрема служба, що надає можливість повного контролю, масштабування та високої доступності для розгортання контейнерів програм у хмарі. Для цієї служби користувач має лише вказати необхідні для його програм обчислювальні ресурси, на основі яких отримує їх повний комплект на OCI яку орендує.

Підключення та мережа. OCI Networking надає можливість створити та управляти програмно визначеною мережею, тобто віртуально хмарною мережею (VCN). VCN – віртуальна версія класичної локальної мережі, де є змога обрати власні IP-адреси RFC 1918 [19], визначити підмережі, маршрути, шлюзи та правила брандмауера, який буде підтримувати маршрутизацію приватного та публічного трафіку в мережі. Oracle Cloud Infrastructure Load Balancing в свою чергу допомагає розподіляти навантаження в утвореній клієнтом VCN, надає можливість його збільшення або зменшення. Швидку передачу даних між об’єктами інфраструктури OCI забезпечує за допомогою OCI FastConnect, яка надає швидкість від 1 до 10 Гбіт/с через більше ніж 50 глобальних мережевих провайдерів [19]. І унікальна можливість підключитись до Microsoft Azure через OCI також є, маючи на увазі, що обіцяна затримка близько 2 мілісекунд.

Зберігання. OCI Block Volumes – служба OCI, яка надає високоефективне мережеве сховище з підтримкою інтенсивного та широко спектру робочих навантажень типу введення та виведення. Служба використовує блокові томі, що надає змогу користувачеві збільшувати за потреби ємність обчислювальних екземплярів, забезпечити їх довговічність та постійність навіть для мультипоєднання обчислювальних екземплярів. OCI Object Storage направлене на високопродуктивне зберігання з майже нескінченною ємністю для неструктурованих даних типу журналів, зображень та відео. Такі програми, як Spark, можуть використовувати Object Storage для збереження великого масштабу даних.

Бази даних. Oracle Autonomous Database – автоматизовані бази даних від Oracle, які вже оптимізовані для обробки документоорієнтованих робочих навантажень (JSON), транзакцій та зберігання даних. Ці БД забезпечують

найвищий рівень безпеки та мають оптимальний досвід завдяки можливостям самовиправленню, самоналаштуванню та автоматичному масштабуванню без додаткових пристроїв. БД OCI була розроблена на основі Oracle Exadata за рахунок чого має спільні з ним або виділені варіанти свого розгортання – ізолює базові ресурси інфраструктури для окремого користувача. OCI Database і Exadata Cloud здатні до легкого створення, масштабування та захисту за допомогою ціноутворення за ліцензією або Bring Your Own License (BYOL) [19]. Також Oracle пропонує керовані БД MySQL і NoSQL.

Платформа даних, data science та аналіз. OCI Streaming та інтеграція даних OCI, як низка деяких інших інструментів, дозволяють використовувати майже будь-які формати даних з локальних і хмарних джерел. OCI Data Catalog дає можливість користувачу відслідковувати свої дані в декількох сховищах даних OCI. За допомогою OCI Data Science вчені мають подібний каталог інструментів на основі Python, який можна використовувати для створення, навчання та керування моделями машинного навчання. Oracle Analytics Cloud буде доцільним для бізнес- та IT-аналітикам, яка надає керовану службу для самостійної аналітики даних у середовищі OCI або з зовнішніх джерел даних.

Інтеграція та додатки. Oracle Integration Cloud надає можливість інтеграції додатків всередині самої OCI і сторонніх SaaS, і локальних додатках та галузевих стандартах, таких як FTP. Окрім хмари клієнт Oracle може скористатися широким спектром бізнес-ПЗ: сервісні програми, планування ресурсів підприємства, керування людським капіталом, взаємодія з клієнтами, керування ланцюжком поставок та інше. Також Oracle може забезпечувати рішеннями у банківський справі, підтримці клінічних випробувань, виставлення рахунків, керування ризиками тощо.

Сервіси розробки. Oracle DevOps сервіси та інструменти допомагають в оптимізації життєвому циклі розробки ПЗ (SDLC), інфраструктурних операціях, листуванні розробників та спостережливості. Користувачам надається можливість використовувати популярні open-source інструменти, по типу Jenkins, Terraform, Grafana та Spinnaker, які можна інтегрувати в OCI. Для отримання доступу до OCI

клієнт може скористатися інтуїтивним графічним інтерфейсом, REST APIs, SDKs, CLI (інтерфейс командної строки) або браузерним терміналом Cloud Shel [19]l.

Безпека та управління. IAM (Identity and Access Management) надає доступ до керування групами доступу користувачів до окремих ресурсів. Oracle спрощує керування за допомогою функції розмежовування та політик з синтаксисом типу SQL, що робить цей процес більш легким до розробки та управління. OCI Vault централізує менеджмент шифрування даних та секретів. Клієнт може використовувати систему керування ключами для створення та імпортування ключів, для їх генерації, включення чи відключення в криптографічних процесах, прив'язувати ключі до відповідних ресурсів та використовувати ключі для шифрування та дешифрування. OCI Audit надає прозорості та видимості активностей відносно ресурсів клієнта. Ця функція записує у логи всі події, що можуть бути використання для аудиту безпеки та їх відповідності до встановлених стандартів та правил. Oracle Cloud Observability and Management (OCOM) надає широкий набір сервіси з управління, діагностики та аналітики, що відкриває можливість для легкого діагностування встановлених традиційних та хмарних технологій як в середині хмари так і на фізичній основі. OCOM використовує заснований на стандартах підхід, який є відкритим і не залежить від постачальника, тому ця платформа завжди готова для взаємодії зі Slack, Twilio, PagerDuty тощо.

2.2 Служби та сервіси захисту Oracle Cloud Infrastructure

У минулому підрозділі було поверхнево розглянуто основні функції та служби OCI, окремо від кожну сферу платформи: інтеграція, сховище, БД, інтеграція тощо. Безпека і управління були останньою зоною, що було оглянуто, але для подальшого розкриття теми цієї роботи, саме цю зоні слід розкрити глибше.

Так, для забезпечення захисту та аудиту, OCI має декілька інструментів: Identity and Access Management, Vault, Audit та Oracle Cloud Observability and Management. Саме їх і буде розкрито в цьому підрозділі.

OCI Audit. Oracle Cloud Infrastructure Audit – система, що автоматично записує в журнали логів OCI усі події та виклики, що відбуваються у всіх

підтримуваних кінцевих точках API інфраструктури. В ці події входить: виклики API, здійснені консоллю OCI, інтерфейсом командного рядка (CLI), комплектами розробки програмного забезпечення (SDK), клієнтами користувача хмари або іншими службами Oracle Cloud Infrastructure. Керуються ці журнали також через Audit. Служба Oracle Storage ділить журнали логів за обраним сегментом, але не за обраним об’єктом.

Логи OCI Audit включають в себе: час дії API, джерело та мета діяльності, тип дії, тип відповіді, зміни стану ресурсів, дані про усунення несправностей в журналі (останні два активні з осені 2019 року). Кожна подія в журналі має визначену структуру запису, яка включає ідентифікатор заголовку, цільові ресурси, позначку часу записаної події, параметри запиту та відповіді. Доступ до цих логів можна отримати через API або SDK для Java. Завдяки таким записами більш детально можна проводити діагностику, відслідковувати реальне використання ресурсів, моніторити відповідність та збирати ці події для їх подальшого використання для забезпечення безпеки. Приклад логу аудиту можна розглянути в Додатку А.

OCI Vault. Oracle Cloud Infrastructure Vault – це один з основних сервісів керування, який зберігає та керує ключами шифрування та секретами для забезпечення безпечного доступу до ресурсів. Відповідно до обраного типу захисту, ключі сховища можуть зберігатись як на сервері, так і на надійних апаратних модулях безпеки (HSM), які відповідають FIPS 140-2 безпеки рівня 3. Схематичне зображення OCI Vault можна розглянути на рис. 2.7.

OCI Vault підтримує декілька типів шифрування ключів: AES, RSA, алгоритм цифрового підпису на основі еліптичних кривих ECDSA. Їх можна комбінувати відповідно до свої вимог: шифрування симетрично або асиметричного ключа, для підпису документів цифровим підписом.

Сховище OCI можна використовувати для створювання та зберігання сховищ, ключів та секретів. Для них служба надає наступні можливості контролю [20]:

створення сховищ;

створювання та імпортування криптографічного розрахунку для головного ключа;

створення секретів та зберігання секретів облікових даних;

перевертання ключів для генерації нового криптографічного розрахунку;

експорт метаданих ключа чи сховища в резервну копію, для її подальшого відновлення та використання;

налаштування правил для керування та використання секретів;

видалення сховища, ключів чи секретів;

надавання метаданих до ресурсів;

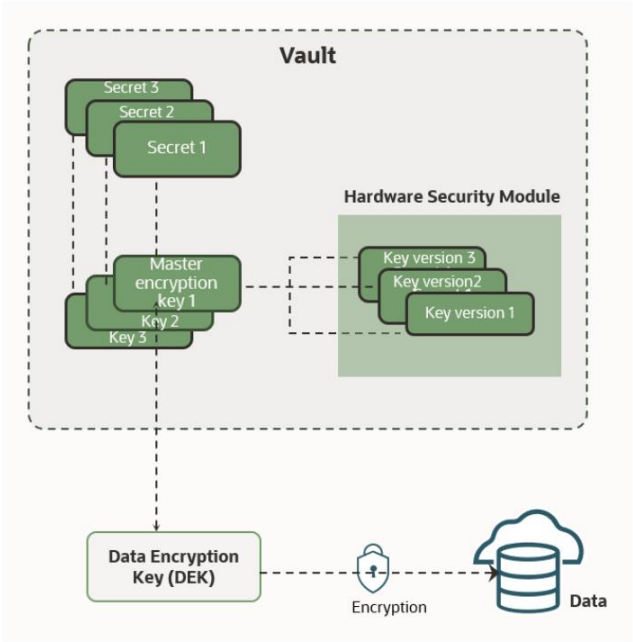


Рис. 2.7 Схематичне зображення OCI Vault Key Management System [20]

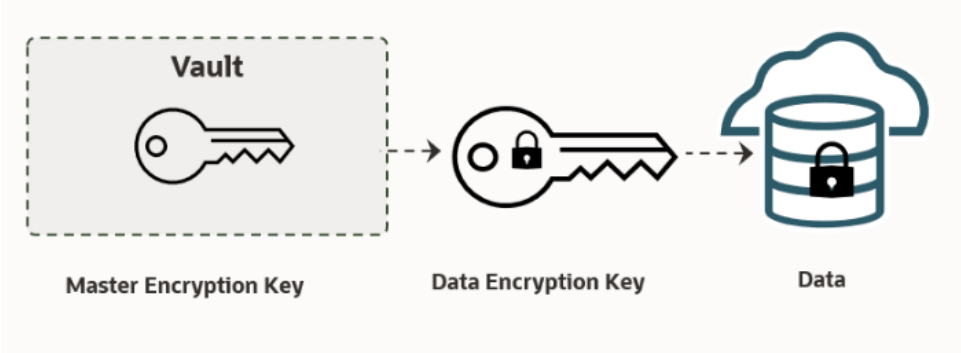


Рис. 2.8 Ієрархія ключів в OCI Vault Key Management System [20]

Щодо ключів шифрування користувач може виконувати наступні дії:

використання ключів для підпису повідомлень та перевірки підпису;

використання ключів для шифрування та дешифрування даних як у стані спокою, так і під час їх передачі;

створення ключів шифрування даних;

призначення ключів до підтримуваних OCI ресурсів;

Також OCI Vault можна інтегрувати з іншими сервісами OCI, завдяки чому створені ключі можна буде використовувати і для цих сервісів. Так, для інтеграції готові наступні сервіси: OCI Block Volume, OCI Container Engine for Kubernetes, OCI Database, OCI File Storage, OCI Object Storage, OCI Streaming.

Але головна можливість OCI Vault – це взаємодія Сховища з IAM, що дозволяє врегульовувати та контролювати доступи користувачів OCI до сховища ключів, секретів. OCI Audit спрощує моніторинг ключів та використання секретів Сховища, а також дає можливість відслідковувати адміністративні дії щодо сховища, ключів та секретів.

OCI Identity and Access Management. Oracle Cloud Infrastructure Identity and Access Management (Рис. 2.9) дозволяє контролювати розмежування доступу користувачів платформи до її ресурсів.

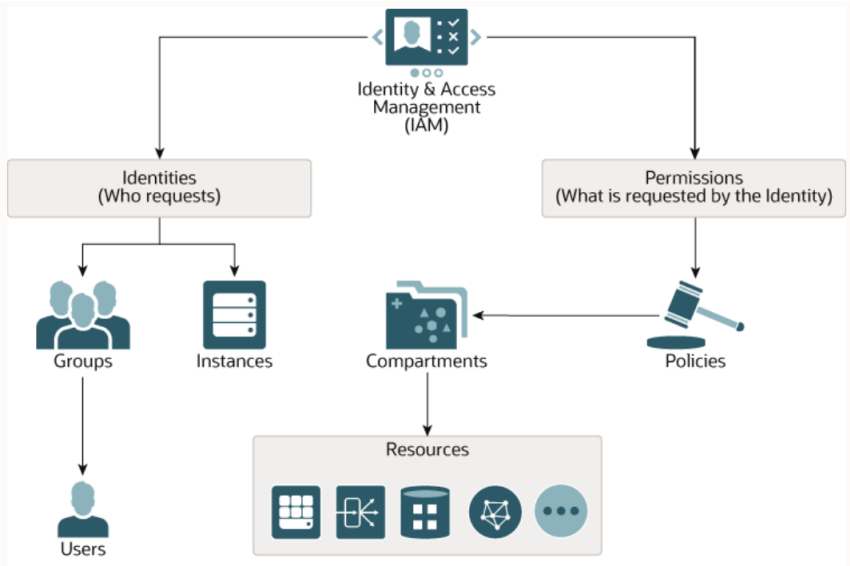


Рис. 2.9 Модель IAM в OCI [25]

IAM складається з декількох компонентів: ресурси, користувачі, групи та динамічні групи, ресурси мережі, політики, відділи, володіння, федерації, домашній регіон.

Ресурси представляють собою усі об’єкти хмари, які були створені компанією користувача під час взаємодії з OCI. Сюди входять: підмережі, таблиці маршрутів, блокові томи, обчислювальні екземпляри тощо.

Користувачі – окремі працівники чи системи, що потребують використання чи взаємодії з ресурсами OCI, які отримує компанія-клієнт хмари. Користувачі можуть запускати екземпляри, працювати з віртуальною хмарною мережею тощо, і вони зазвичай не виступають кінцевими користувачами IAM.

Група є колекцією користувачів, які мають необхідність в одному виді доступу до деякого набору ресурсів та відділів.

Динамічні групи – спеціальна група, яка складається з ресурсів, таких як обчислювальні екземпляри, доступи в які відповідають впровадженим в компанії правилами. Тому членство в такій групі є динамічним через мінливість відведених їм ресурсів. Такі суб’єкти системи мають змоги виконувати дії в API до служб відповідно до політик, які були визначені компанією.

Джерело мережі представляє собою групу IP-адрес, яким виділений доступ до ресурсів платформи користувача. IP-адреси можуть бути як публічними адресами так і адресою з VCN в межах платформи. Як тільки джерело буде створено, користувач може використати політику аби обмежити доступ для запитів, що надходять не з IP-адреси джерела мережі.

Відділ – це набір відповідних ресурсів. Вони є фундаментальними компонентами OCI для організації та ізоляції хмарних ресурсів користувача. Саме виокремлення цих відділів допомагає в визначенні фактичного використання ресурсів і подальшого розрахування оплати оренди, визначенні доступу (через політики) та ізоляції (відокремлення ресурсів одного проекту чи підрозділу від іншого). На відділах будується виокремлення головних частин організації клієнта.

Володіння є корінним автоматично створеним провайдером відділом, що складається з усіх ресурсів OCI, які орендує користувач. Так, в їх межах знаходяться усі об’єкти IAM, а саме: користувачі, групи, відсіки та політики. У відсіках зі свого боку розміщуються усі інші типи хмарних ресурсів, по типу віртуальних мереж чи блокових томів.

Політики виступають у вигляді документу, який визначає доступи користувачів платформи до її ресурсів. Ці дозволи надаються для груп та відсіку, що дозволяє прописати політики доступу однієї групи в межах певного відділу чи в межах платформи. Надаючи групі доступ до володіння, вона одразу отримує той самий рівень доступу і до усіх відділів в середині володіння.

Домашній регіон – це регіон в якому розміщені ресурси IAM користувача хмари. Усі ресурси IAM є глобальними та доступними в усіх регіонах, але базовий набір знаходиться саме в домашньому регіоні. Тому для поширення змін в IAM, важливо це зробити саме в середині домашнього регіону, аби ці зміни поширились і на інші регіони.

Федерація представляє собою відносини між адміністратором клієнта хмари та постачальниками ідентифікаційної інформації та послуг. При об’єднанні OCI з постачальником ідентифікації інформації, саме в другому буде відбуватись керування користувачами та групами. OCI та Oracle Identity Cloud Service об’єднані між собою за замовчуванням.

В IAM завжди існує попередньо утворена група «адміністратори», яка містить обліковий запис адміністратора за замовчуванням. Саме цей суб’єкт стане першим користувачем IAM компанії та буде відповідальним за стартове налаштування додаткових адміністраторів в цій групі. Цю групу не можна видалити і вона завжди має містити хоча б одного користувача.

«Адміністратори» за замовчуванням, відповідно до попередньо створеної політики, мають доступ до всіх API операцій OCI та ресурсів хмари всередині володіння. Тобто серед можливостей є створення та керування: групами, політиками, відділами (в межах IAM) та VCNs, блоковими томами тощо (в межах ресурсів хмари). Ця політика не може бути зміненою чи видаленою.

2.3 Підхід, компоненти та основні рекомендації щодо захисту, на яких базується безпека Oracle Cloud Infrastructure

Підхід OCI щодо забезпечення захисту платформи базується на семи засадах, що будуть розглянуті далі, на основі яких було розроблено декілька рішень для

покращення захисту та відповідності хмарної інфраструктури. Про деякі інструменти, що реалізують ці засади, було обговорено в попередньому підрозділі.

Клієнтська ізоляція. OCI надає можливість розгортати додатки та активи даних в середовищі, що повністю ізольовано як від працівників Oracle, так і від інших клієнтів хмари. Тобто ізоляції підлягають: додатки, інформація, ресурси хмари. Ізоляція забезпечуються за рахунок серверів типу «голий метал», VMware, VCN, IAM та відділів.

Шифрування даних. Завдяки алгоритмам шифрування та управлінню ключів, дані користувачів забезпечені захистом та відповідністю і у стані спокою, і під час транзиту. Захист даних за допомогою шифрування забезпечується за допомогою шифрування сховищ за замовчуванням, Сховище для керування ключами, DB шифрування.

Контроль безпеки. Розподіл операційних обов'язків, обмеження доступу впливають на зменшення ризику шкідливого впливу та від випадкових дій користувачів. За контроль безпеки відповідають: автентифікація та авторизація користувачів, контроль безпеки мережі, мережеві екрани та керування екземплярами.

Видимість. OCI забезпечує надання повного журналу логів та аналітики безпеки перевірки та моніторингу подій відносно ресурсів платформи. Завдяки цьому, адміністратори безпеки мають широкий спектр можливостей для аналізу та подальшого забезпечення захисту платформи зі своєї сторони. Так, видимість забезпечують аудит логів, CASB моніторинг та протидія.

Захист гібридної хмари. OCI надає можливість самостійно визначати активи безпеки, такі як облікові записи користувачів та політики. Також завжди є легальна можливість використовувати рішення безпеки від сторонніх постачальників для захисту даних та активів у хмарі. Для захисту гібридної хмари слід звернути увагу на: IPSes VPN, рішення безпеки сторонніх постачальників, Identity Federation та FastConnect.

Висока доступність. Надання користувачу хмари повністю незалежні центри даних, які є повністю доступними, масштабованими та є готовими протидіяти

атакам з мережі. Високу доступність забезпечують: SLA, незалежні від збоїв ЦОД та домени.

Верифікована безпечна інфраструктура. Усі сервісі Oracle відповідають широкому спектру стандартів та вимог, де FedRAMP, FIPS 140-2, GDPR, HIPAA, PCI DSS і SOC 1/2/3 лише деякі з них. За верифікацію безпеки інфраструктури відповідають: відповідність сертифікації та атестації, penetration-and-vulnerability тестування, операції безпеки.

Для забезпечення відповідної безпеки інфраструктури, Oracle керується моделлю спільної безпеки. Так, зі своєї сторони постачальник забезпечує безпеку XI та операцій, типу, контроль доступу оператора хмари та оновлення безпеки інфраструктури. В той час, як користувач відповідає за безпечне налаштування свої хмарних ресурсів.

На рис. 2.9 візуально зрозуміло зображено розподіл відповідальності, за яким видно, що клієнт відповідає за безпеку даних свої клієнтів (такі як облікові дані користувачів орендаря хмари), керування доступом та своїми додатками (IAM політики тощо), налаштування мережі та мережевих екранів (наприклад, налаштування VCN), шифрування зі сторони клієнта (Сховище). Постачальник хмари в свою чергу піклується про ізоляцію мережі, обчислювань та зберігання, про забезпечення фізичного захисту, захист інших інфраструктур типу CASB, DDoS тощо.

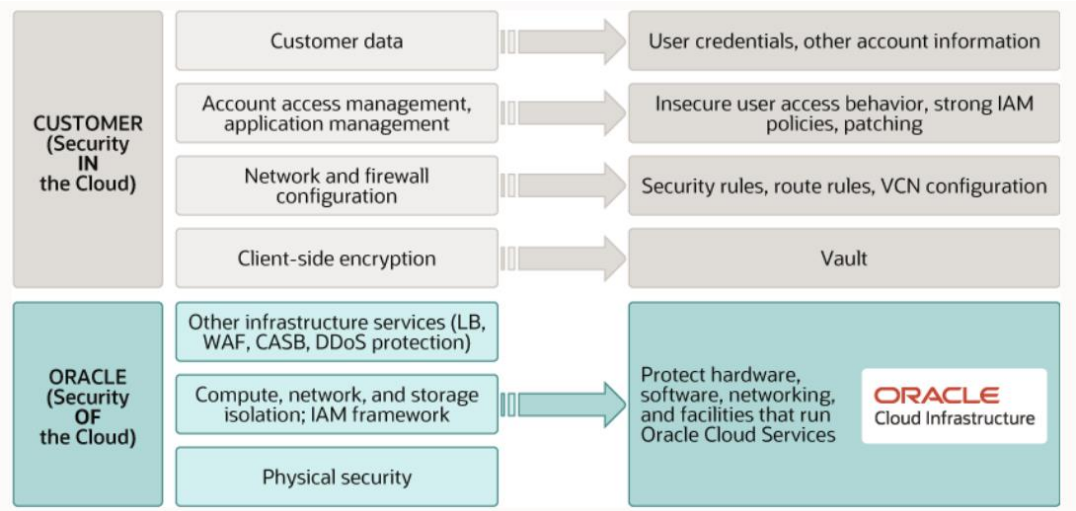


Рис. 2.10 Модель спільної безпеки для OCI

Тобто зі своєї сторони Oracle відповідає за всі аспекти фізичної безпеки доменів. В той же час, постачальник та користувач одночасно відповідають за безпеку інфраструктурного апаратного забезпечення, ПЗ та відповідних конфігурацій та елементів керування. Клієнт окремо відповідає за платформу, яку розгортає на хмарі, ПЗ, яке використовує в ній, дані, які використовує та зберігає, та за загальне керування ризиками, безпекою.

Спільна відповідальність також поширюється серед усіх існуючих доменів хмари: контролювання доступу, захист робочих процесів, класифікація даних та їх відповідність, безпека інфраструктури, ідентифікація та безпека мережі.

IAM. Oracle надає усі необхідні служби IAM: ідентифікація, автентифікація, авторизація та аудит. Клієнт зі своєї сторони має створити облікові записи користувачів хмари та захистити їх доступи. Також клієнт хмари має завжди переглядати ці дозволи для обґрунтування їх актуальності та, при необхідності, змінювати ці доступи відповідно до свої міркувань.

Безпека робочого навантаження. Зі своєї сторони Oracle забезпечує надання безпечних образів та спрощує можливість використання сторонніх рішень захисту на своїй платформі. Від користувача OCI потребується забезпечення захистом ОС та ПЗ, які розгортаються на наданій йому платформі. Так, у цей список доречним є вирішення питання зі своєчасним оновленням ПЗ та ОС, проведення правильного налаштування їх конфігурацій.

Класифікація та відповідність даних. Користувачеві є доцільним правильно класифікувати та маркувати свої дані, що буде відповідати очікуваному рівню безпеки та відповідності.

Безпека інфраструктури хоста. Аби забезпечувати відповідну захищеність, клієнт має піклуватись за безпечне налаштування свої обчислювальних ресурсів (віртуальні машини, голі екземпляри та контейнери), ресурсами зберігання свої даних (об’єктне та локальне сховище, блокові томи) та служби даних. Зі своє сторони Oracle відповідає за оптимальне налаштування та захист служб, які надає. Сюди входить безпека гіпервізора, налаштування дозволів та елементів керування доступу до мережі, що впливають на правильність обміну даними між хостами та

забезпечує надійне підключення та встановлення пристроїв зберігання даних.

Безпека мережі. Провайдер несе відповідальність за фізичну безпеку мережевої інфраструктури, коли клієнт має забезпечити її правильними конфігураціями безпеки віртуальну мережу, балансування, шлюзи та DNS.

Безпека кінцевих точок. Важливо налаштувати відповідну безпеку кінцевих точок, які мають доступ до OCI.

Фізична охорона. Oracle відповідає за захист глобальну фізичну інфраструктури (апаратне забезпечення, ПЗ, мережі та засоби), які несуть пряме відношення до запуска OCI.

Також Oracle пропонує 4 зони відповідальності, на яких можна розгортати відповідне забезпечення доступності, цілісності та конфіденційності:

Безпека та відповідність вимогам. Забезпечення захисту своїх системи та інформаційних ресурсів в хмарі. Сюди входять: автентифікація користувачів, ізоляція ресурсів та контролювання доступу, захист обчислень, захист БД, захист інформації, захист мережі.

Надійність і відмовостійкість. Створення надійних додатків, розробляючи стійку хмарну інфраструктуру. Сюди входить: відмовостійка архітектура, ліміти обслуговування, резервне копіювання та масштабування.

Оптимізація продуктивності та витрат. Ефективне використання ресурсів інфраструктури покращує продуктивність та зменшує потенційні витрати. Сюди входить: розрахування розміру, моніторинг та налаштування мережі, відстеження та керування витратами, стратегія зберігання.

Операційна ефективність. Керування та контроль додатків та ресурсів інфраструктури, аби покращити їх продуктивність та результати. Сюди входить: стратегія розгортання, моніторинг навантажень, підтримка та керування ОС.

Окрім цього, для якісного розгортання OCI Oracle рекомендує наступних фахівців:

архітектор додатків – розробник та керівник розробки користувацьких додатків, що будуть розміщуватись на хмарі. Такий фахівець має розуміти набір інструментів, що надається, вміння безпечно та ефективно використовувати

платформу та забезпечити її стабільність. Відповідає за безпеку та відповідальність, надійність та стійкість;

архітектор хмари – відповідальний за потреби та вимоги робочого навантаження та середовища, вибирає необхідні послуги та рішення для розгорнутого стану хост-платформи. Відповідає за безпеку та відповідальність, операційна ефективність, надійність та стійкість;

архітектор DevOps – визначає користь інструментів віртуалізації та автоматизації з боку операцій та за процес і набір з боку розробки. Займається розробкою та керуванням інструментів автоматичного реагування, збирає та застосовує дані моніторингу та сповіщень для створення динамічного реактивного середовища, а також визначає інструменти та програми, які найкраще впливають та відповідають робочому навантаженню. Відповідає за операційна ефективність, безпеку та відповідальність, надійність та стійкість;

архітектор підприємства – визначає загальну технологічну стратегію, тобто відповідає за бюджет, доступність та інші бізнес-метрики. Також може впливати за вибір постачальника хмари, спонсурування хмарного офісу та узгодження організаційної структури розгортання хмари. Відповідальний за операційна ефективність, безпеку та відповідальність, надійність та стійкість, ефективність та оптимізація витрат;

архітектор інфраструктури – відповідає за узгодженість між вимогами програми з наявними обчислювальними та зберігальними можливостями. Визначає стратегію життєвого циклу обладнання ЦОД (гіпервізор, контейнеризація, фізичні сервери, блокове та файлове сховище, ОС). Відповідає за надійність та стійкість, операційна ефективність, безпеку та відповідальність;

архітектор мережі – забезпечує стійкість, продуктивність та безпеку підключення додатків. Займається підключенням до гібридної хмари, локальне чи WAN підключення, вхідне-вихідне та бокове підключення, розгортанням хмарної мережі VCN, конфігурацією балансувальника навантажень, підключення до FastConnect тощо. Забезпечує доступність ємності для робочих навантажень як у стабільному стані, так і під час «стрибків» активності. Відповідає за безпеку та

відповідальність, надійність та стійкість;

архітектор безпеки – відповідає за безпечне розгортання компонентів програми, визначає стратегію для систем виявлення вторгнень, їх запобіганню, розробляє плани та алгоритми реагування на інциденти тощо. Може також займатись IAM у хмарі, забезпеченням безпеки мережі, шифруванням та керуванням секретами. Відповідає за безпеку та відповідальність, ефективність та оптимізація витрат операційна ефективність [23].

У цьому розділі було визначені призначення, основні функції та рішення хмарної інфраструк-тури Oracle Cloud Infrastructure, проаналізовано служби OCI, що відповідають за забезпечення хмарної інфраструктури організації та розглянуто підходи, компоненти та основні рекомендації щодо забезпечення захисту. Окрім цього була наведена та описана термінологія, розглянуті керівництва та технічні документи Oracle Cloud Infrastructure.

3 ТЕХНОЛОГІЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕКИ ХМАРНОЇ ІНФРАСТРУКТУРИ ОРГАНІЗАЦІЇ НА БАЗІ ORACLE CLOUD INFRASTRUCTURE

3.1 Технологія забезпечення безпеки хмарної інфраструктури на базі Oracle Cloud Infrastructure

Як було визначено з розділу 1 цієї роботи, основною загрозою безпечності даних в хмарі та самої хмарної інфраструктури є невідповідне та неякісне налаштування хмари. Тому дуже важливо на кожному етапі підготовки захисту врахувати усі можливі деталі та уважно підійти до налаштування служб, додатків та ПЗ які надає провайдер хмари, та які використовує сам клієнт хмари. Ця технологія буде враховувати рекомендації Oracle та міжнародні нормативно-правові документи, а також поетапно охоплювати 11 зон безпеки Oracle Cloud Infrastructure.

Автентифікація. В OCI користувач потребує облікові дані для отримання доступу до конкретних зон та можливості XI. Так, платформа надає можливість користувачам генерувати, змінювати свої облікові дані, а адміністратор системи має доступ до їх скидання. Рекомендації до налаштувань автентифікації наступні:

визначити працівників (користувачі), які потребують доступу до OCI;

використовувати для їх облікових даних унікальні та складні паролі, спираючись на міжнародні рекомендації та тенденції (наприклад, NIST SP800-63B, ISO/IEC 27002:2013, CIS Password Policy Guide тощо);

ввести в практику примусову зміну ключів та API кожні 90 днів;

упевнитись, що жодні облікові дані не були hard-code в жодне ПЗ та не фігурують в документаціях організації;

не поширювати облікові дані між працівниками;

впровадження автоматичного механізму анулювання облікового запису та його доступу, у випадку, коли відповідний користувач залишає організацію;

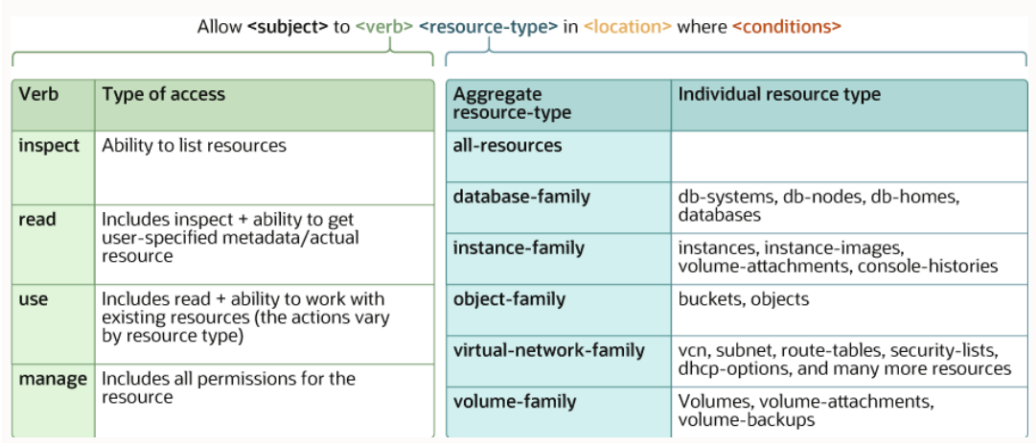
проводити аналіз та моніторинг членства користувачів в групах IAM, для подальшого видалення користувачів, яким наданий доступ більше не є необхідним;

не зловживати доступами адміністратора оренди та використовувати їх лише в екстрених випадках;

перевіряйте активність адміністратора з деякою періодичність у журналах аудиту;

використовуйте багатофакторну автентифікацію (MFA).

Авторизація. Запити на доступ в OCI автентифікуються на основі наданих облікових даних і авторизуються відповідно до попередньо створених політик IAM, які створюються на основі наступного синтаксису на рис. 2.11:


Allow <subject> to <verb> <resource-type> in <location> where <conditions>

Verb	Type of access
inspect	Ability to list resources
read	Includes inspect + ability to get user-specified metadata/actual resource
use	Includes read + ability to work with existing resources (the actions vary by resource type)
manage	Includes all permissions for the resource

Aggregate resource-type	Individual resource type
all-resources	
database-family	db-systems, db-nodes, db-homes, databases
instance-family	instances, instance-images, volume-attachments, console-histories
object-family	buckets, objects
virtual-network-family	vcn, subnet, route-tables, security-lists, dhcp-options, and many more resources
volume-family	Volumes, volume-attachments, volume-backups

Рис. 2.11 Синтаксис політик IAM в OCI [25]

Рекомендації до керування авторизацією наступні:

зіставте групи IAM з функціональними ролями в середині вашої організації;

створіть та організуйте групи IAM відповідно до дозволів, що плануєте надати;

розробіть та припишіть політику IAM для створених в ній груп;

обов’язково додайте користувачів в групу з відповідними доступами, які бажаєте їм надати;

призначаючи дозволи IAM для користувачів, дотримуйтесь принципу найменшого привілею та розподілу обов’язків.

Identity Federation. OCI підтримує об’єднання з Oracle Identity Cloud Service, Microsoft Active Directory через Active Directory Federation Services (AD FS), Microsoft Azure Active Directory, Okta та іншими постачальниками

ідентифікаційних даних, які підтримують протокол Security Assertion Markup Language (SAML) 2.0. Рекомендації до керування Identity Federation наступні:

створіть групу об'єднаних адміністраторів, яка буде відповідати групі IdP адміністраторів і буде працювати по тім самим політикам IAM, як і група IdP адміністраторів;

аби запобігти обходу безпеки, створіть політику безпеки IAM, яка буде забороняти групі IdP адміністраторів IAM додавати чи змінювати членство в групі адміністраторів хмари за замовчуванням;

координуйте та узгоджуйте обов'язки та ролі з інформаційної безпеки в OCI відповідно до наданих ролей та вимог.

Ізоляція ресурсів. Відсіки – фундаментальна частина OCI, яка дозволяє створювати різноманітний набір ресурсів для організації, безпечної ізоляції та контрою доступу. Правильне створення та організація відсіків, відповідно до найголовніших частин організації, допомагає в подальших вимірах використання ресурсів системи, контролю доступу та ізоляції ресурсів (Рис. 2.12).

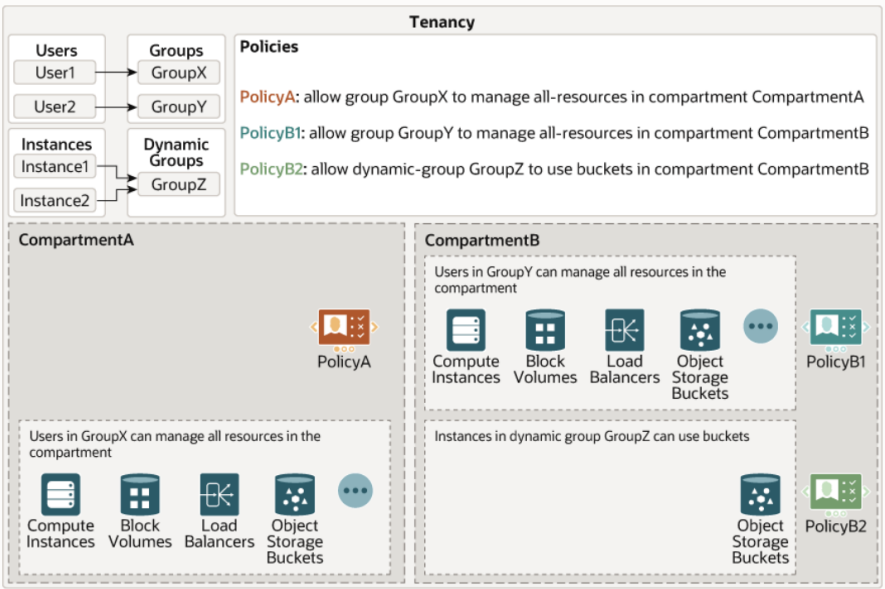


Рис. 2.12 Контролювання доступу через політики та відсіки в OCI [25]

Рекомендації для керування відсіками наступні:

ізолюйте основні відділи організації у відсіки;

визначайте відсіки та політики IAM, щоб надавати доступи лише тим користувачам, у яких є необхідність в доступі до певних ресурсів;

створюючи дочірні відсіки, прописуйте їх політики IAM, для правильного збільшення організаційних рівнів;

визначайте лише необхідний ліміт ресурсів для відсіків, для попередження надмірного зловживання;

уникайте прописування політик IAM на рівні кореневого відділу;

прописати політики, що будуть обмежувати доступ до переміщення дочірніх чи батьківських відсіків неавторизованим користувачам.

Безпека мережі. Мережа OCI надає можливість створення віртуальних хмарних мереж VCN та підмереж, які ізолюють ресурси клієнта хмарина рівні мережі.

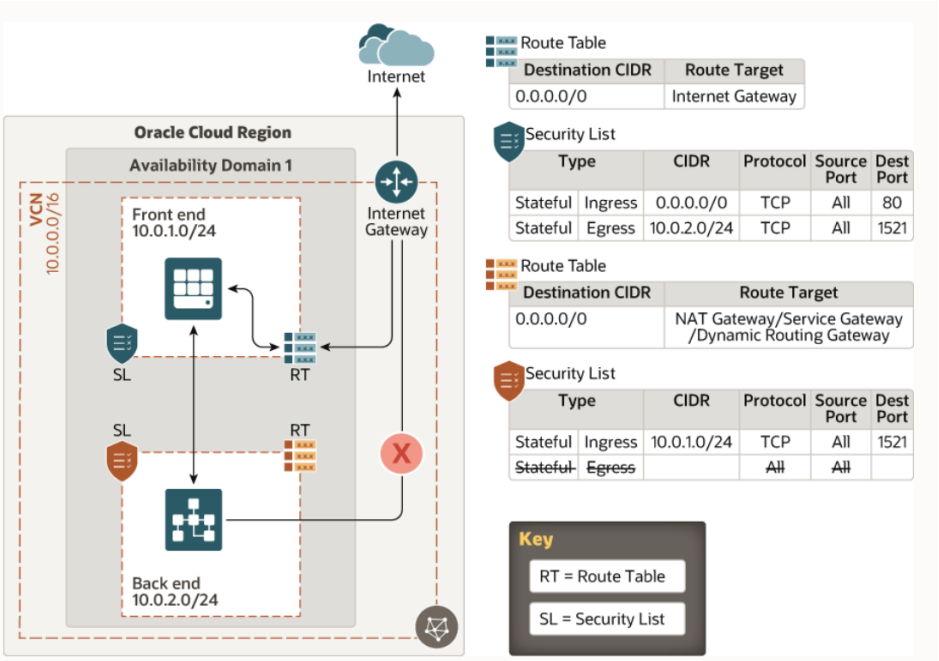


Рис. 2.13 Приклад використання підмережі, таблиць маршрутів та список безпеки для забезпечення захисту мережі [25]

VCN можна підключити до інтернету або локальних ЦОД за допомогою служби FastConnect чи з'єднань IPSec VPN. Для контролювання потоку трафіку в середині створеної мережі доцільно використовувати двонаправлені правила брандмауера – зі збереженням та без збереження стану, – шлюзи зв'язку та таблиці маршрутів. Списки контрою (ACL) та брандмауери, що були призначені для мережі, поширюються по всі її топології та зоні керування, задля забезпечення

багаторівневої реалізації захисту. На рис. 2.13 зображено архітектури віртуального брандмауера з використанням списків безпеки, задля забезпечення захисту мережі. Встановивши правила у списку безпеки, вони одразу розповсюджуються на всі VNIC в підмережах, до яких був доданий цей список. А для більш детального брандмауера рекомендовано використовувати групи безпеки мережі (NSG), які будуть застосовуватись лише для тих VNIC, що були обрані користувачем, та допоможуть виокремити архітектуру підмережі від безпеки робочого навантаження. Приклад порівняння списку безпеки та NSG групи можна розглянути на рис. 2.14.

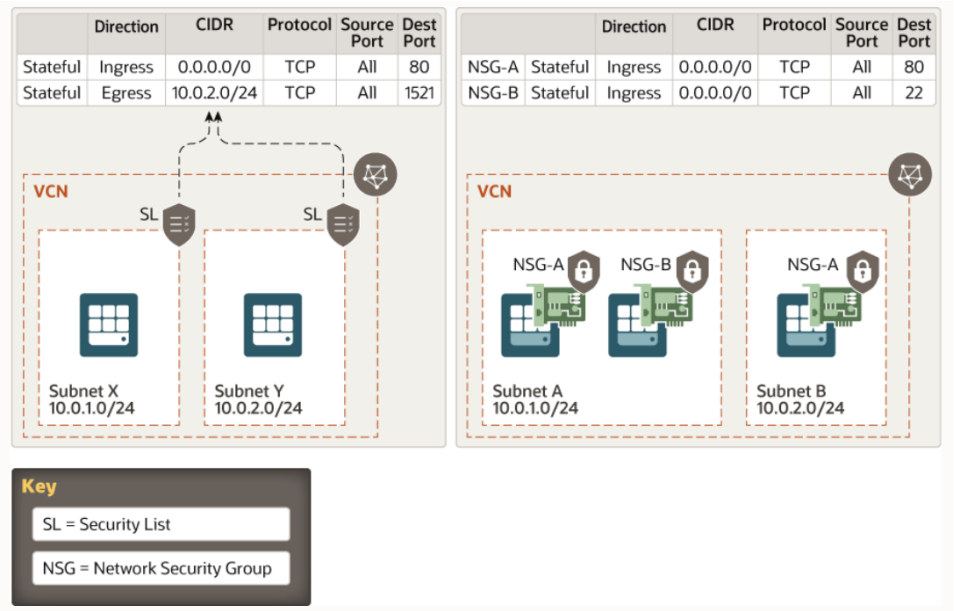


Рис. 2.14 Порівняльне зображення списків безпеки та NSG [25]

Рекомендації для забезпечення безпеки мережі:

розділіть VCN на приватну та публічну підмережу;

визначте правила брандмауера для контролю доступу до екземплярів;

використовуйте політики IAM для обмеження доступу до мережевих ресурсів групам, яким не дозволено керувати ними;

створіть та налаштуйте балансувальники навантаження для високої доступності та безпеки транспортного рівня (TLS);

для контролювання доступу до мережі, доцільно використовувати стратегію багаторівневої підмережі VCN (підмережа DMZ для балансувальників

навантаження, публічна підмережа для зовнішніх хостів, як веб-сервери, приватна мережа для внутрішніх хостів, як БД);

налаштувати системи IDS/IPS – виявлення та захист від вторгнень;

для підключення до Інтернету з приватних комп'ютерів використовуйте шлюз NAT;

для підключення до мережі служб Oracle використовуйте service gateway;

використовуйте WAF – брандмауери веб-програм;

налаштуйте та використовуйте детальні правила безпеки для доступу до мережі VCN, зв'язку з Інтернетом, для доступу до інших VCN мереж через peering gateways (однорангові шлюзи), та для доступу до локальних мереж через IPSec VPN і FastConnect.

створить зони DNS, використовуйте для забезпечення безпеки балансувальників навантаження клієнтські сертифікати TLS.

Безпека обчислювальних екземплярів. Для захисту обчислювальних екземплярів доцільно використовувати SSH на основі ключів доступу до екземплярів. Адже SSH на основі паролю не є стійким до атак «грубого підбору». Рекомендації до безпеки обчислювальних екземплярів:

стабільно оновлюйте встановленні на обчислювальних екземплярах ОС;

відключіть вхід за допомогою пароля та root-вхід;

використовуйте системи IDS/IPS на основі хосту;

використовуйте брандмауери на основі хостів, як приклад iptables, для обмеження доступу до мережі екземплярі, зокрема портами, протоколами та типами пакетів;

змініть порт SSH на нестандартний;

керуйте ключами SSH та їх ротацією;

обмежте доступ до метаданих екземпляру для всіх, окрім привілейованих користувачів;

використовуйте принципи екземпляру та динамічні групи IAM.

Безпека на рівні обслуговування. Важливо впроваджувати алгоритми, підходи, практики та елементи керування безпекою для всіх окремих служб OCI.

Рекомендації до керування безпекою на рівна обслуговування:

забезпечте безпеку блокових томів (впровадження контролю доступу за допомогою IAM, забезпечення шифрування та конфіденційності за допомогою системи ключів, систематичне резервне копіювання, виконання аудиту безпеки);

забезпечення захисту обчислень (впровадження контролю доступу за допомогою IAM, забезпечення шифрування та конфіденційності за допомогою системи ключів, регулярні оновлення, виконання аудиту безпеки);

забезпечення захисту каталогу даних (впровадження правила найменшого доступу для користувачів та груп IAM до відповідних типів ресурсів, обмежити доступ до видалення даних до кількох користувачів, наприклад, адміністратору оренди хмари чи відділу, надавати доступ користувачам лише для читання даних);

забезпечення захисту БД (впровадження автентифікації користувачів для доступу до БД, впровадження найменшого доступу через групи безпеки чи списки безпеки в VCN, обмежити доступ до видалення даних до кількох користувачів, наприклад, адміністратору оренди хмари чи відділу, систематичні резервні копіювання, наприклад, на основі RMAN, який шифрує кожну копію за допомогою ключа-шифрування, регулярні оновлення, виконання аудиту безпеки);

забезпечення захисту транспортування даних;

забезпечення захисту електронного листування (створити окремого користувача SMTP, що буде надавати дозволи для схвалених відправників і буде блокувати підозрілих);

забезпечення захисту сховищ файлів (використання списків безпеки VCN, обмежити доступ до видалення даних до кількох користувачів, наприклад, адміністратору оренди хмари чи відділу, періодично робити знімки файлової системи, використовувати добре відомі методі безпеки NFS, такі як опція all_squash для відображення всіх користувачів у nfsnobody та списки ACL NFS для примусового контролю доступу до змонтованої файлової системи);

забезпечення захисту IAM (створіть адміністраторів рівня обслуговування для найменших привілеїв, обмежити можливість змінювати членство в групі адміністраторів оренди хмари, обмежити доступ до видалення та зміни в політиках

безпеки, заборона на отримання доступу чи зміни облікових даних користувачів адміністраторами);

забезпечення захисту мережі (розбити мережу на сегменти-підмережі – приватна мережа для внутрішніх хостів, публічна мережа для NAT, IDS та серверів веб-додатків, DMZ для балансувальників навантаження, встановлення фаерволу для контролю доступу до мережі, налаштування фаерволів на основі хосту, наприклад iptables, встановлення правил безпеки для зв'язку хостів в публічні мережі, розміщення вразливих хостів (бази даних, наприклад) в приватній мережі);

забезпечення захисту даних інтеграції (впровадження правила найменшого доступу для користувачів та груп IAM до відповідних типів ресурсів, обмежити доступ до видалення даних до кількох користувачів, наприклад, адміністратору оренди хмари чи відділу, надавати доступ користувачам лише для читання даних);

забезпечення захисту контейнерного двигуна для Kubernetes (не запускати взаємно ненадійні робочі процеси в одному кластері, забезпечення шифрування та конфіденційності за допомогою системи ключів, встановлення контролю доступу на основі ролей (RBAC), впровадження політики безпеки модулів, блокування доступу контейнера до метаданих екземплярів, впровадження політик для мережі);

забезпечення захисту сховища об'єктів (впровадження контролю доступу за допомогою IAM, забезпечення шифрування та конфіденційності за допомогою системи ключів, забезпечення цілісності даних під час їх транспортування чи копіювання, регулярні оновлення, виконання аудиту безпеки);

забезпечення захисту менеджера ресурсів (впровадження контролю доступу за допомогою IAM, обмежити використання вразливих даних в конфігураційних та вихідних файлах, виконання аудиту безпеки).

Захист даних. Рекомендації для захисту даних:

використовуйте службу Vault для керування ключами;

шифрування даних у стані спокою (наприклад, за допомогою Vault) та під час транзиту;

впровадити класифікацію даних за типом, цінністю, чутливістю, конфіденційністю та критичністю;

впровадження резервного копіювання та відновлення відповідно до SLA та вимог організації;

впровадження керуванням життєвого циклу даних;

впровадження процесу обертання ключів;

реалізувати захищений доступ до секретів.

Аудит, моніторинг та управління. Рекомендації до аудиту, моніторингу та управлінню:

встановити процедуру аудиту хмари;

встановити процедуру перевірки та аналізу журналу подій;

реалізувати процес обробки аналізу загроз;

використовуйте систему тегів та класифікації ресурсів;

визначте та впровадьте правила іменування ресурсів;

запровадити системи та процеси для аналізу та об'єднання даних моніторингу та реєстрації.

Управління та реагування на інциденти. Рекомендації для управління та реагування на інциденти:

використовуйте системи типу Oracle CASB для визначення ризиків, вразливих місць, ймовірності та впливи, що будуть пов'язані з безпекою OCI;

розгорнути та налаштувати центр безпеки SOC та групу реагування на інциденти;

розгорнути та налаштувати систему керування інформацією та подіями безпеки SIEM;

запровадити процес виявлення, реагування, звітування та рішення інцидентів;

запровадити процес пост-інциденту та навчання.

Відповідність та безпека програм. Рекомендації до відповідності та безпеки програм:

визначте та класифікуйте дані, що використовуються програмами організації;

визначити та запровадити елементи керування даними відповідно до

розробленої класифікації даних;

налаштуйте автентифікацію, авторизацію, контроль доступу на рівні програм для користувачів;

налаштуйте елементи керування мережею на рівні програми;

налаштуйте моніторинг, аудит та логування на рівні програми;

налаштуйте WAF для веб-додатків;

визначте та розгорніть усі засоби контролю відповідності нормативним вимогам.

Операційна стійкість та безперервність бізнесу. Рекомендації:

впровадити захист та управління API;

встановити політику безпеки та процедури щодо керування зовнішніми партнерами та постачальниками;

розробити план безперервності діяльності;

встановити політику безпеки та процедури щодо змін у діяльності;

впровадити перевірку цілісності ПЗ, файлів та даних (наприклад, інструмент Tripwire);

встановити політику безпеки та процедури управління ризиками щодо застосування змін до ПЗ, проектів і конфігурацій API і компонентів інфраструктури;

встановити та контролювати базову лінію потоків даних користувачів і систем.

3.2 Рекомендації щодо забезпечення безпеки хмарної інфраструктури організації

Тенденція на використання хмарних сервісів серед організацій приватного чи державного типу активно набирає оберти, через їх можливість прискорити розвиток, життєдіяльність та робочі процеси, при цьому залишаючись гнучкими та значно доступнішими. Проте, використання будь-якої ХС пов’язано зі значними ризиками безпеки даних у хмарі, і відповідальність за забезпечення їх захисту завжди залежить від клієнта хмари, в незалежності від типу ХС, чи то SaaS, PaaS

чи IaaS. Тому важливо саме на рівні організації, яка бере той чи інший тип хмари в оренду, попіклуватись про створення видимості процесів в хмарі та їх контролю. Наступні рекомендації, розроблені у вигляді етапів та кроків, є узагальненими практиками, що направленні на покращення ситуації з безпечністю хмари та створення впевненого фундаменту для підтримки цього стану захищеності протягом усього життєвого циклу хмари.

Етап 1. Розуміння використання хмари та ризики, що пов'язані з нею. Цей етап направлений на створення розуміння щодо поточного стану хмари та оцінки її ризиків, використовуючи хмарні рішення постачальника хмари, що був обраний організацією.

Крок 1. Визначення вразливих та потребуючих контролю даних. Створення, узгодження та використання системи класифікації даних, допоможуть визначити який потенційний ризик безпеки мають ті чи інші дані вашої організації. Бо саме втрата, модифікація чи виток даних, які є найбільш важливими для функціонування організації, можуть призвести до штрафних санкцій, втрати інтелектуальної власності, юридичних проблем тощо.

Крок 2. Визначити політики та правилами, за якими має отримуватись доступ до вразливих даних. Навіть тримаючи дані у захищеному середовищі, важливо розуміти хто та як отримує до неї доступ, та що відбувається з цією інформацією далі. Проведіть оцінку дозволів до усіх файлів та папок у хмарі, та визначте їх контекст, тобто які ролі мають це доступ, де знаходяться користувачі, що отримали до даних доступ, який пристрій використовували тощо.

Крок 3. Перевірте наявність тіньового IT, тобто невідомого використання хмари. Не завжди звичайні користувачі клієнта хмари повідомляють IT-команду про конвертування файлів у PDF чи підписки на хмарне-сховище. Тому вкрай важливим є використання веб-проксі, журналу SIEM та брандмауера для виявлення хмарних служб, що не були офіційно зафіксовані. Після виявлення подібних тіньових процесів, доцільно провести оцінку їх ризику.

Крок 4. Аудит конфігурацій для IaaS. Середовище IaaS є багаторівневим та

складним, і має безліч критичних конфігурацій, які без відповідного налаштування можуть стати вразливостями для всієї системи. Тому доцільно провести повний аудит усіх конфігурацій, особливо тих, що відповідають за ідентифікацію, керування доступом, мережу та шифрування.

Крок 5. Виявіть шкідливі дії користувачів. Недобросовісне та необережні дії користувачів клієнта хмари, зовнішні чи внутрішні дії зловмисниками можуть демонструвати поведінку, яка вказує на шкідливе використання хмарних даних. Аби попередити подібні ризики, можна проводити аналітику поведінки користувачів (UBA), яка здатна відстежити аномалії та зменшити потенційні внутрішні та зовнішні витоки даних.

Етап 2. Захист хмари. Після визначення ризиків безпеки, можна перейти до стратегічного розроблення захисних процесів та підходів до ХС відповідно до їх рівня ризику.

Крок 1. Застосування політики захисту даних. Після впровадження класифікації даних, доцільним є прикладання до них відповідних політик, які будуть визначати де і як ті чи інші типи даних мають зберігатись, які дані треба поміщати в карантин чи видаляти з хмари. Відповідно до розробленої політики треба проводити навчання користувачів клієнта хмари, для попередження помилкових чи небезпечних дій з їх сторони щодо даних в хмарі.

Крок 2. Шифрування конфіденційних даних з використанням власних ключів. Провайдери хмари надають можливість шифрування в свої хмарі, які надають для оренди, завдяки чому, дані не будуть доступні стороннім особам. Проте постачальник хмари все одно буде мати доступ до цих ключів шифрування, бо сам їх клієнту і надає. Через це доцільно використовувати власні ключі, аби мати повний контроль доступу до власних даних.

Крок 3. Обмеження способів обміну даних. Як тільки дані опиняються у хмарі, застосовуйте своїх політики контролю доступу і одній чи одразу в декількох службах. В ці дії входять: налаштування користувачів та груп для перегляду чи редагуванню, контроль розповсюдження інформації (наприклад, дозвіл на

розповсюдження через спільні посилання).

Крок 4. Заборона на розповсюдження даних на некеровані та невідомі пристрої. ХС дає змогу отримувати доступ д хмари з будь-якого пристрою, що має підключення до Інтернету. Але доступ з некоровайного пристрою, на кшталт особистого телефону користувача клієнта хмари, створює сліпу зону для безпеки. Тому важливо блокувати завантаження на такі некеровані пристрої та вимагати проводити їх перевірку на безпечність.

Крок 5. Використання розширеного захисту від зловмисного ПЗ до IaaS. В середовищі IaaS саме клієнт хмари відповідає за забезпечення безпеки ОС, ПЗ та мережевого трафіку. Технології anti-malware можна застосовувати і до ОС і до віртуальної мережі, як раз для забезпечення захисту інфраструктури. Також доцільно буде розгорнути білі списки для додатків та технології захисту на основі machine-learning для загальних процесів та файлових сховищ.

Етап 3. Реагування на інциденти безпеки хмари. Як і в будь-якому іншому IT-середовищі, в хмарі також трапляються інциденти безпеки, які будуть потребувати або керованого, або автоматичного виправлення.

Крок 1. Впровадьте додаткову перевірку сценаріїв доступу з високим ризиком. Наприклад, якщо користувач клієнта хмари намагається отримати доступ до конфіденційних даних у хмарі через девайс, що не є зареєстрованим у системі, має автоматично запускатись двофакторна автентифікація.

Крок 2. Підганяйте налаштування політики доступу в міру появи нових хмарних служб. Інтегрувавши в хмарну БД ризиків захищений веб-шлюз та брандмауер, можна досягнути автоматизації оновлення політики для веб-доступу.

Крок 3. Видаляйте шкідливе ПЗ з хмарної служби. Зловмисне ПЗ здатне скомпрометувати спільну папку, яка автоматично синхронізується з хмарним сховищем, тим самим навіть без участі користувачів відтворюючись вже у хмарі. Використовуйте anti-malware сканування для уникнення ransomware та атак крадіжки даних.

Для досягнення найкращих результатів з безпеки на основі попередніх

розроблених кроків, доцільно використовувати наступні ключові технології у поєднанні з функціями безпеки, які надає провайдер хмари.

Cloud Access Security Broker (CASB) – захищає дані в хмарі за рахунок попередження втрати даних та використовує аналіз поведінки користувачів. Також часто використовується доя моніторингу конфігурацій в IaaS та виявлення тіньових IT. Приклади: Netskope CASB, Skyhigh Security (McAfee's MVISION Cloud) Zscaler [26].

Cloud Workload Protection (CWP) – виявляє робочі навантаження та контейнери, надає захист від шкідливого ПЗ та спрощує управління безпекою в IaaS. Приклади: Trend Micro Deep Security, VMware Carbon Black App Control.

Virtual Network Security (VNS) – сканування мережевого трафіку між віртуальними екземплярами IaaS разом з точками ходу та виходу.

В розділі було розроблено практичну технологію забезпечення захисту хмарної інфраструктури на основі Oracle Cloud Infrastructure, надані детальні рекомендації щодо кожного аспекту безпеки в інфраструктурі. Також були розроблені загальні рекомендації, у вигляді етапів та кроків, щодо підходу до забезпечення захисту хмарної інфраструктури організації.

ВИСНОВКИ

Темою магістерської роботи було дослідження та розробка технології і рекомендації щодо забезпечення захисту хмарної інфраструктури організації.

Для розкриття теми було проведено аналіз актуальності хмарних сервісів, як середовище розвиту організацій приватного чи державного рівня. Також було визначено тенденцію сучасних проблем та ризиків безпеки хмарних інфраструктур. Так, найбільш великою проблемою є складність та непослідовність налаштувань основних конфігурацій хмарного сервісу типу «інфраструктура-як-послуга», через її багаторівневість та складність.

Було досліджено методи та засоби захисту хмарної інфраструктури організації на базі Oracle Cloud Infrastructure. Так, під час дослідження було визначено структуру та архітектуру Oracle Cloud, функції її сервісів та додаткових послуг. Основними службами, що забезпечують безпеку OCI, стали Identity and Access Management, Vault, Audit та Oracle Cloud Observability and Management.

На основі проведеної роботи була розроблена технологія забезпечення захисту хмарної інфраструктури, яка включає детальний підхід до налаштувань 11 зон безпеки Oracle Cloud Infrastructure. Так, ця технологія може бути настільною книгою детальних рекомендацій щодо побудови якісної та захищеної інфраструктури зі сторони клієнта хмари.

Окрім цього були розроблені та підготовлені узагальнюючі рекомендації щодо забезпечення захисту хмарної інфраструктури організації, що стануть у нагоді для побудови захисту IaaS в незалежності від обраного провайдера.

Таким чином, розроблені технологія та рекомендації стануть у нагоді фахівцям адміністратору оренди хмари, архітектору додатків, архітектору хмари, архітектору DevOps, архітектору підприємства архітектору інфраструктури, архітектору мережі, архітектору безпеки, працівникам та керівнику відділу інформаційної та кібербезпеки, аналітикам з інформаційної та кібербезпеки.

ПЕРЕЛІК ПОСИЛАНЬ

1. Information technology – Cloud computing – Overview and vocabulary. ISO/IEC 17788:2014 / Joint Technical Committee ISO/IEC JTC 1, 2014 – 16 с.

2. New to SaaS? Welcome! [Електронний ресурс] – Режим доступу: https://www.salesforce.com/in/saas/#:~:text=What%20is%20SaaS%3F,complex%20software%20and%20hardware%20management

3. SaaS vs PaaS vs IaaS: Choosing the Right Model for Your Application [Електронний ресурс] / Arun Aravamudhan – Режим доступу: https://www.eginnovations.com/blog/saas-vs-paas-vs-iaas-examples-differences-how-to-choose/

4. PAAS vs SAAS [Електронний ресурс] / Priya Pedamkar – Режим доступу: https://www.educba.com/paas-vs-saas/

5. В чем разница между IaaS, SaaS и PaaS?[Електронний ресурс] – Режим доступу: https://senior.ua/articles/v-chem-raznica-mezhdu-iaas-saas-i-paas

6. NIST Special Publication 500-291. Recommendations of the National Institute of Standards and Technology [Електронний ресурс] – Режим доступу: https://www.nist.gov/system/files/documents/itl/cloud/NIST_SP-500-

7. What Is IaaS? [Електронний ресурс] – Режим доступу: https://www.comptia.org/content/articles/what-is-iaas

8. 5 Key Findings from 2019 Cloud Adoption and Risk Report/ McAfee Cloud BU [Електронний ресурс] – Режим доступу: https://www.mcafee.com/blogs/enterprise/cloud-security/5-key-findings-from-2019-cloud-adoption-and-risk-report/

9. Well-known Gartner's Seven Security Issues Which Cloud Clients Should Advert [Електронний ресурс] / Greater Noida – Режим доступу: https://www.ripublication.com/aeee_spl/aeeev4n4spl_15.pdf

10. The Most Common Cloud Security Threats and How to Avoid Them [Електронний ресурс] / Elizabeth Fichtner – Режим доступу:

https://www.datto.com/blog/the-most-common-cloud-security-threats-and-how-to-avoid-them

11. Survey: 45% Of Cyber Security Attacks Fuelled By Lack Of Visibility Over IaaS Cloud Infrastructure [Електронний ресурс] / ISBuzz Staff - Режим доступу: https://informationsecuritybuzz.com/survey-45-of-cyber-security-attacks-fuelled-by-lack-of-visibility-over-laas-cloud-infrastructure/

12. Building the Infrastructure for Cloud Security/ A Solutions view [Електронний ресурс] / Raghu Yeluri, Enrique Castro-Leon – 240 с.

13. Guidelines on Security and Privacy in Public Cloud Computing. Special Publication 800-144 of the National Institute of Standards and Technology [Електронний ресурс] W. Jansen, T. Millar, T. Grance – Гейтерсберг, Мериленд: Natl. Inst. Stand. Technol. Spec. Publ., 2012. – 79 с. – Електрон. дан. – Гейтерсберг, Мериленд: National Institute of Standards and Technology – 2021.

14. Information technology — Cloud computing — Guidance for policy development ISO/IEC TR 22678:2019 [Електронний ресурс] / Joint Technical Committee ISO/IEC JTC 1, 2019 – 42 с.

15. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services [Електронний ресурс] / Joint Technical Committee ISO/IEC JTC 1, 2015 – 44 с.

16. What is IaaS? [Електронний ресурс] – Режим доступу: https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-iaas/#:~:text=Infrastructure%20as%20a%20service%20(IaaS,(PaaS)%2C%20and%20serverless

17. Three Key Findings from SailPoint’s State of IaaS Report [Електронний ресурс] – Режим доступу: https://www.sailpoint.com/blog/three-key-findings-from-sailpoints-state-of-iaas-report/

18. Cloud Security For Dummies®, Oracle 3rd Special Edition [Електронний ресурс] / Lawrence Miller – Режим доступу: https://www.oracle.com/explore/security/cloud-security-for-dummies?topic=Cloud%20Security&lb-

mode=overlay&source=:ow:o:p:mt:::RC_WWMK210806P00057:CloudSecurityForDummies&intcmp=:ow:o:p:mt:::RC_WWMK210806P00057:CloudSecurityForDummies

19. Oracle Cloud Infrastructure Platform Overview [Електронний ресурс] – Режим доступу: https://www.oracle.com/a/ocom/docs/cloud/oracle-cloud-infrastructure-platform-overview-wp.pdf

20. Overview of Identity and Access Management [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm

21. Security Overview [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_overview.htm

22. Security Best Practices [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en-us/iaas/Content/Security/Reference/configuration_security.htm#Security_Best_Practices

23. Best practices framework for Oracle Cloud Infrastructure [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en/solutions/oci-best-practices/index.html#GUID-5F2D2745-934E-409A-A7BA-D0976F727845

24. A Step-By-Step Guide to Cloud Security Best Practices [Електронний ресурс] – Режим доступу: https://www.skyhighsecurity.com/en-us/cybersecurity-defined/cloud-security-best-practices.html

25. Security checklist for Oracle Cloud Infrastructure [Електронний ресурс] – Режим доступу: https://docs.oracle.com/en/solutions/oci-security-checklist/toc.htm

26. A 2022 Gartner® Magic Quadrant™ Leader for Security Service Edge [Електронний ресурс] – Режим доступу: https://www.skyhighsecurity.com/en-us/solutions/lp/gartner-magic-quadrant-for-sse.html

27. Теза

28. Статья

ДОДАТКИ

Додаток А

Приклад запису в журналі-логів аудиту


```
{
    "eventType": "com.oraclecloud.ComputeApi.GetInstance",
    "cloudEventsVersion": "0.1",
    "eventTypeVersion": "2.0",
    "source": "ComputeApi",
    "eventId": "<unique_ID>",
    "eventTime": "2019-09-18T00:10:59.252Z",
    "contentType": "application/json",
    "data": {
        "eventGroupingId": null,
        "eventName": "GetInstance",
        "compartmentId": "ocid1.tenancy.oc1..<unique_ID>",
        "compartmentName": "compartmentA",
        "resourceName": "my_instance",
        "resourceId": "ocid1.instance.oc1.phx.<unique_ID>",
        "availabilityDomain": "<availability_domain>",
        "freeformTags": null,
        "definedTags": null,
        "identity": {
            "principalName": "ExampleName",
            "principalId": "ocid1.user.oc1..<unique_ID>",
            "authType": "natv",
            "callerName": null,
            "callerId": null,
            "tenantId": "ocid1.tenancy.oc1..<unique_ID>",
```

```
                "ipAddress": "172.24.80.88",
                "credentials": null,
                "userAgent": "Jersey/2.23 (HttpUrlConnection 1.8.0_212)",
                "consoleSessionId": null
        },
        "request": {
                "id": "<unique_ID>",
                "path": "/20160918/instances/ocid1.instance.oc1.phx.<unique_ID>",
                "action": "GET",
                "parameters": {},
                "headers": {
                        "opc-principal": [

"{\"tenantId\":\"ocid1.tenancy.oc1..<unique_ID>\",\"subjectId\":\"ocid1.user.oc1..<unique_ID>\",\"claims\":[{\"key\":\"pstype\",\"value\":\"natv\",\"issuer\":\"authService.oracle.com\"},{\"key\":\"h_host\",\"value\":\"iaas.r2.oracleiaas.com\",\"issuer\":\"h\"},{\"key\":\"h_opc-request-id\",\"value\":\"<unique_ID>\",\"issuer\":\"h\"},{\"key\":\"ptype\",\"value\":\"user\",\"issuer\":\"authService.oracle.com\"},{\"key\":\"h_date\",\"value\":\"Wed, 18 Sep 2019 00:10:58 UTC\",\"issuer\":\"h\"},{\"key\":\"h_accept\",\"value\":\"application/json\",\"issuer\":\"h\"},{\"key\":\"authorization\",\"value\":\"Signature headers=\\\"date (request-target) host accept opc-request-id\\\",keyId=\\\"ocid1.tenancy.oc1..<unique_ID>/ocid1.user.oc1..<unique_ID>/8c:b4:5f:18:e7:ec:db:08:b8:fa:d2:2a:7d:11:76:ac\\\",algorithm=\\\"rsa-pss-sha256\\\",signature=\\\"<unique_ID>\\\",version=\\\"1\\\"\",\"issuer\":\"h\"},{\"key\":\"h_(request-target)\",\"value\":\"get /20160918/instances/ocid1.instance.oc1.phx.<unique_ID>\",\"issuer\":\"h\"}]}"

                        ],
                        "Accept": [
```

```
                "application/json"
            ],
            "X-Oracle-Auth-Client-CN": [
                "splat-proxy-se-02302.node.ad2.r2"
            ],
            "X-Forwarded-Host": [
                "compute-api.svc.ad1.r2"
            ],
            "Connection": [
                "close"
            ],
            "User-Agent": [
                "Jersey/2.23 (HttpUrlConnection 1.8.0_212)"
            ],
            "X-Forwarded-For": [
                "172.24.80.88"
            ],
            "X-Real-IP": [
                "172.24.80.88"
            ],
            "oci-original-url": [
        "https://iaas.r2.oracleiaas.com/20160918/instances/ocid1.instance.oc1.phx.<unique_ID>"
            ],
            "opc-request-id": [
                "<unique_ID>"
            ],
            "Date": [
                "Wed, 18 Sep 2019 00:10:58 UTC"
```

```
            ]
        }
    },
    "response": {
        "status": "200",
        "responseTime": "2019-09-18T00:10:59.278Z",
        "headers": {
            "ETag": [
                "<unique_ID>"
            ],
            "Connection": [
                "close"
            ],
            "Content-Length": [
                "1828"
            ],
            "opc-request-id": [
                "<unique_ID>"
            ],
            "Date": [
                "Wed, 18 Sep 2019 00:10:59 GMT"
            ],
            "Content-Type": [
                "application/json"
            ]
        },
        "payload": {
            "resourceName": "my_instance",
            "id": "ocid1.instance.oc1.phx.<unique_ID>"
        },
```

```
            "message": null
        },
        "stateChange": {
            "previous": null,
            "current": null
        },
        "additionalDetails": {
            "imageId": "ocid1.image.oc1.phx.<unique_ID>",
            "shape": "VM.Standard1.1",
            "type": "CustomerVmi"
        }
    }
}
```