

Bezpečnostní opatření pro Oracle Cloud Infrastructure v podnicích

Bc. Daniel Cidl

Diplomová práce
2025



Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně

Fakulta aplikované informatiky

Ústav informatiky a umělé inteligence

Akademický rok: 2024/2025

ZADÁNÍ DIPLOMOVÉ PRÁCE

(projektu, uměleckého díla, uměleckého výkonu)

Jméno a příjmení: Bc. Daniel Cidl
Osobní číslo: A23583
Studijní program: N0613A140022 Informační technologie
Specializace: Kybernetická bezpečnost
Forma studia: Kombinovaná
Téma práce: Bezpečnostní opatření pro Oracle Cloud Infrastructure v podnicích
Téma práce anglicky: Security Measures for Oracle Cloud Infrastructure in Enterprises

Zásady pro vypracování

- Seznamte se s bezpečnostními funkcemi Oracle Cloud Infrastructure.
- Identifikujte potenciální hrozby a slabiny.
- Navrhněte opatření pro zabezpečení dle bezpečnostních zásad OCI.
- Sestavte a ověřte vhodné scénáře zabezpečení.
- Zhodnoťte účinnost navržených opatření v modelových situacích.

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam doporučené literatury:

1. KAVIS, Michael. *Architecting the Cloud: design decisions for Cloud computing service models (SaaS, PaaS, and IaaS)*. Hoboken, New Jersey: Wiley, c 2014. Wiley CIO series. ISBN 1118617614.
2. GILMAN, Evan a BARTH, Doug. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. Springfield: O'Reilly, 2017. ISBN 9781491962190.
3. SHOSTACK, Adam. *Threat Modeling: Designing for Security*. New Jersey: Wiley, c 2014. ISBN 9781118809990.
4. COCHRAN, Kodi A. Securing the Cloud: A Comprehensive Guide to Cloud Security. In: *Cybersecurity Essentials* [online]. Berkeley, CA: Apress, 2024, s. 327-363 [cit. 2024-10-17]. ISBN 979-8-8688-0431-1. Dostupné z: doi:10.1007/979-8-8688-0432-8_12.
5. EDWARDS, Dr. Jason. Cloud Security. In: *Mastering Cybersecurity* [online]. Berkeley, CA: Apress, 2024, s. 223-280 [cit. 2024-10-17]. ISBN 979-8-8688-0296-6. Dostupné z: doi:10.1007/979-8-8688-0297-3_8.

Vedoucí diplomové práce: **Ing. Peter Janků, Ph.D.**
Ústav informatiky a umělé inteligence

Konzultant diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **27. října 2024**

Termín odevzdání diplomové práce: **2. června 2025**



L.S.

doc. Ing. Jiří Vojtěšek, Ph.D. v.r.
děkan

prof. Mgr. Roman Jašek, Ph.D., DBA v.r.
ředitel ústavu

Ve Zlíně dne 17. listopadu 2024

PROHLÁŠENÍ AUTORA DIPLOMOVÉ PRÁCE

Beru na vědomí, že

- odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., v platném znění bez ohledu na výsledek obhajoby;
- diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a bude dostupná k nahlédnutí;
- jedno vyhotovení diplomové práce v listinné podobě bude ponecháno Univerzitě Tomáše Bati ve Zlíně k uložení;
- na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- podle § 60 odst. 1 autorského zákona má Univerzita Tomáše Bati ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60 odst. 2 a 3 mohu užít své dílo – diplomovou práci – nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá; neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji, že

- jsem na diplomové práci pracoval(a) samostatně a použitou literaturu jsem řádně citoval(a); v případě publikace výsledků budu uveden(a) jako spoluautor;
- odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou obsahově totožné.

Ve Zlíně, dne

.....
podpis autora

ABSTRAKT

Diplomová práce se zaměřuje na návrh, implementaci a ověření bezpečnostních opatření v prostředí Oracle Cloud Infrastructure (OCI) pro podnikové využití. Teoretická část analyzuje principy cloudové bezpečnosti, zejména model sdílené odpovědnosti a klíčové bezpečnostní funkce OCI. Praktická část popisuje metodiku testování bezpečnostních scénářů v prostředí Proof-of-Concept a hodnotí účinnost navržených opatření proti vybraným hrozbám. Práce obsahuje i praktická doporučení a shrnuje současné možnosti a limity zabezpečení OCI s návrhy na další výzkum v oblasti automatizace a optimalizace bezpečnostních procesů.

Klíčová slova: Oracle Cloud Infrastructure, cloudová bezpečnost, CIS OCI Foundations Benchmark, MITRE ATT&CK, bezpečnostní opatření, sdílená odpovědnost, testování

ABSTRACT

This thesis focuses on the design, implementation, and verification of security measures in Oracle Cloud Infrastructure (OCI) for enterprise use. The theoretical part analyzes cloud security principles, especially the shared responsibility model and key OCI security features. The practical part describes a methodology for testing security scenarios in a Proof-of-Concept environment and evaluates the effectiveness of the proposed measures against selected threats. The thesis also includes practical recommendations and summarizes the current capabilities and limitations of OCI security, with suggestions for further research in the areas of automation and optimization of security processes.

Keywords: Oracle Cloud Infrastructure, cloud security, CIS OCI Foundations Benchmark, MITRE ATT&CK, security measures, shared responsibility, testing

Velmi děkuji vedoucímu diplomové práce Ing. Peteru Janků, Ph.D., a určenému konzultantovi Ing. Davidu Malaníkovi, Ph.D., kteří mi poskytli cenné rady i podněty a především mi věnovali svůj čas.

Současně chci poděkovat všem členům své rodiny, za jejich podporu a zejména trpělivost během studia.

OBSAH

ÚVOD.....	13
I TEORETICKÁ ČÁST.....	15
1 ZÁKLADY CLOUD COMPUTINGU A JEHO BEZPEČNOSTI.....	16
1.1 DEFINICE CLOUD COMPUTINGU	16
1.2 MODEL SDÍLENÉ ODPOVĚDNOSTI (SHARED RESPONSIBILITY MODEL).....	19
1.3 NÁSTROJE K HODNOCENÍ BEZPEČNOSTI CLOUDOVÝCH POSKYTOVATELŮ	23
1.4 PŘEHLED POSKYTOVATELŮ CLOUDOVÝCH SLUŽEB A SOUČASNÉ TRENDY	24
2 PŘEDSTAVENÍ ORACLE CLOUD INFRASTRUCTURE (OCI).....	26
2.1 ORACLE PUBLIC CLOUD	26
2.2 ORACLE CLOUD INFRASTRUCTURE (OCI)	26
2.3 ORACLE CLOUD INFRASTRUCTURE (OCI) GEN2	27
2.4 TYPY ÚČTŮ DOSTUPNÝCH V OCI.....	29
3 KLÍČOVÉ BEZPEČNOSTNÍ FUNKCE V OCI.....	32
3.1 ZÁKLADNÍ PROSTŘEDKY PRO SPRÁVU ZDROJŮ V OCI	32
3.2 REGION, DOMÉNA DOSTUPNOSTI, FAULT DOMÉNA.....	33
3.3 SPRÁVA IDENTIT A PŘÍSTUPŮ (IAM).....	34
3.4 SPRÁVA KLÍČŮ A ŠIFROVÁNÍ DAT	34
3.5 SÍŤOVÁ BEZPEČNOST	36
3.6 MONITOROVACÍ NÁSTROJE A REAKCE NA INCIDENTY	40
3.7 BEZPEČNOSTNÍ ZÓNY (SECURITY ZONES)	42
4 IDENTIFIKACE HROZEB A SLABIN.....	43
4.1 FÁZE NÁVRHU INFRASTRUKTURY	43
4.2 FÁZE REÁLNÉHO PROVOZU	44
4.3 PŘEHLED SOUČASNÝCH HROZEB CLOUDOVÝCH SLUŽEB.....	44
4.4 KLASIFIKACE HROZEB POMOCÍ FRAMEWORKU MITRE ATT&CK.....	46
4.5 TRADIČNÍ MODELOVÁNÍ HROZEB VS. CSPM	48
4.6 OCI CLOUD GUARD	49
4.7 CLOUD GUARD THREAT MONITORING	52
4.8 ORACLE THREAT INTELLIGENCE SERVICE.....	53
4.9 OCI VULNERABILITY SCANNING SERVICE	55
5 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ DLE ZÁSAD OCI.....	57
5.1 CENTER FOR INTERNET SECURITY (CIS) OCI FOUNDATIONS BENCHMARK	57
5.2 PLÁN ZABEZPEČENÍ INFRASTRUKTURY	58

5.3	VIZUALIZACE ARCHITEKTURY POMOCÍ OCI DIAGRAMU	62
5.4	VYTVORENÍ TENANCY	62
5.5	VYTVORENÍ PRVKŮ ŘÍZENÍ IDENTITY A PŘÍSTUPOVÝCH OPRÁVNĚNÍ (IAM).....	63
5.6	AKTIVACE CLOUD SECURITY POSTURE MANAGEMENT (CSPM)	63
5.7	ZABEZPEČENÍ WORKLOADŮ.....	64
5.8	VYTVORENÍ A ZABEZPEČENÍ OSTATNÍCH SLUŽEB A ZDROJŮ	65
5.9	OVĚŘENÍ SOULADU S CIS OCI FOUNDATIONS BENCHMARK	66
5.10	PRŮBĚŽNÝ MONITORING AUDITNÍCH A BEZPEČNOSTNÍCH ZÁZNAMŮ	66
II	PRAKTICKÁ ČÁST.....	67
6	SESTAVENÍ NAVRŽENÝCH BEZPEČNOSTNÍCH OPATŘENÍ.....	68
6.1	PLÁN ZABEZPEČENÍ INFRASTRUKTURY	68
6.2	VIZUALIZACE ARCHITEKTURY POMOCÍ OCI DIAGRAMU	70
6.3	VYTVORENÍ TENANCY	72
6.4	UPGRADE FREE TIER TYPU ÚČTU NA PAY-AS-YOU-GO (PAYG)	74
6.5	VYTVORENÍ „CUSTOM-MANAGED“ ŠIFROVACÍHO KLÍČE (CIS LEVEL 2).....	74
6.6	VYTVORENÍ PRVKŮ ŘÍZENÍ IDENTITY A PŘÍSTUPOVÝCH OPRÁVNĚNÍ (IAM).....	75
6.7	AKTIVACE CLOUD SECURITY POSTURE MANAGEMENT (CSPM)	77
6.8	ZABEZPEČENÍ WORKLOADŮ.....	78
6.9	VYTVORENÍ A ZABEZPEČENÍ OSTATNÍCH SLUŽEB A ZDROJŮ	79
6.10	OVĚŘENÍ SOULADU S CIS OCI FOUNDATIONS BENCHMARK	83
7	OVĚŘENÍ VYBRANÝCH BEZPEČNOSTNÍCH SCÉNÁŘŮ	85
7.1	TESTOVACÍ SCÉNÁŘ – PREVENCE VYTVORENÍ VEŘEJNÉHO BUCKETU	85
7.2	TESTOVACÍ SCÉNÁŘ – PREVENCE VYTVORENÍ NEAUTORIZOVANÉ VCN.....	87
7.3	TESTOVACÍ SCÉNÁŘ – PREVENCE NEOPRÁVNĚNÉ MODIFIKACE ROLÍ	88
7.4	TESTOVACÍ SCÉNÁŘ – PREVENCE LOCKOUTU ADMINISTRÁTORA IDCS DOMÉNY	90
7.5	TESTOVACÍ SCÉNÁŘ – NOUZOVÝ PŘÍSTUP PŘES CLOUD SHELL A EPN	92
7.6	TESTOVACÍ SCÉNÁŘ – OVĚŘENÍ CLOUD GUARD RESPONDÉRU	95
7.7	TESTOVACÍ SCÉNÁŘ – GEOLOKAČNÍ OMEZENÍ PŘÍSTUPU POMOCÍ WAF	97
7.8	TESTOVACÍ SCÉNÁŘ – SPRÁVA SPOTŘEBY ZDROJŮ V OCI POMOCÍ KVÓT.....	100
8	VYHODNOCENÍ ÚČINNOSTI NAVRŽENÝCH OPATŘENÍ	103
8.1	ANALÝZA VÝSLEDKŮ TESTŮ.....	103
8.2	KVANTITATIVNÍ A KVALITATIVNÍ VYHODNOCENÍ.....	103
8.3	DOPORUČENÍ A NÁVRHY NA ZLEPŠENÍ.....	104
	ZÁVĚR.....	107

SEZNAM POUŽITÉ LITERATURY.....	109
SEZNAM OBRÁZKŮ	122
SEZNAM TABULEK.....	123
SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK.....	124
SEZNAM PŘÍLOH.....	128

ÚVOD

V posledních letech zaznamenáváme výrazný nárůst využívání cloudových technologií v podnikovém prostředí, a to napříč různými průmyslovými odvětvími. Jedním z klíčových hráčů na poli cloudových služeb je společnost Oracle se svou platformou Oracle Cloud Infrastructure (OCI). Přesun firemních systémů do cloudu přináší řadu výhod, jako je flexibilita, škálovatelnost a snížení provozních nákladů, avšak současně s sebou nese i zvýšené nároky na zabezpečení a ochranu dat. Právě tato oblast, tedy bezpečnostní opatření v prostředí OCI, se stává stěžejním tématem nejen pro samotné podniky, ale i pro akademickou a výzkumnou sféru.

Z hlediska odborného zaměření představuje problematika bezpečnosti v cloudu atraktivní a zároveň velmi aktuální výzkumné téma. Rostoucí množství publikací a studií věnovaných obecným otázkám cloudového zabezpečení dokazuje, že jde o pole intenzivního vývoje. Přesto v praxi stále často chybí ucelený a komplexní přístup k ochraně dat a služeb v konkrétním prostředí vybraného poskytovatele. Problematika OCI zůstává v porovnání s jinými platformami (např. AWS či Microsoft Azure) zkoumána méně, a proto se nabízí prostor pro detailní analýzu a návrh specifických opatření.

Cílem této diplomové práce je navrhnout a otestovat bezpečnostní opatření pro OCI v podnicích tak, aby odpovídala aktuálním bezpečnostním zásadám a doporučením společnosti Oracle i obecným principům kybernetické bezpečnosti. Mezi dílčí cíle patří:

- Seznámit čtenáře s bezpečnostními funkcemi OCI.
- Identifikovat potenciální hrozby a slabiny v prostředí OCI.
- Navrhnout opatření pro zabezpečení v souladu s bezpečnostními zásadami OCI.
- Sestavit a ověřit vhodné scénáře zabezpečení.
- Zhodnotit účinnost navržených opatření v modelových situacích.

V souladu s těmito cíli si práce klade několik pracovních hypotéz. Předpokládá například, že (1) správná implementace bezpečnostních opatření v OCI může významně snížit riziko úspěšného kybernetického útoku, (2) mnoho společností podceňuje význam auditovacích a monitorovacích nástrojů, a (3) kombinace doporučených postupů Oracle s obecně uznávanými bezpečnostními standardy (např. ISO/IEC 27001, NIST, OWASP) vede ke komplexnějšímu zabezpečení než spoléhání se na jediný rámec.

Očekávaným přínosem práce je vytvoření uceleného postupu, který bude sloužit jako vodítko při zavádění zabezpečení pro firmy využívající OCI. Navržené postupy a scénáře by měly pomoci organizacím minimalizovat rizika spojená s migrací i běžným provozem v cloudu. Kromě praktických doporučení poskytne práce také teoretické ukotvení pro hlubší porozumění problematice cloudové bezpečnosti v kontextu platformy Oracle, čímž může přispět nejen k dalšímu rozvoji výzkumných aktivit v této oblasti, ale také k informované praxi v podnicích.

I TEORETICKÁ ČÁST

1 ZÁKLADY CLOUD COMPUTINGU A JEHO BEZPEČNOSTI

Cloud computing lze obecně popsat [1, s. 223] jako poskytování výpočetních zdrojů (jako např. serverů, úložišť, databází, sítí, softwaru či analytických nástrojů) přes Internet na vyžádání, obvykle s modelováním plateb podle využití. V praxi to znamená, že namísto správy a provozu vlastních serverů v datovém centru (*on-premise*) dochází k využívání výpočetní kapacity provozované poskytovatelem cloudu (*cloud service provider*), jenž se stará o potřebnou infrastrukturu, softwarové aktualizace a celkový provoz.

Z finančního hlediska nabízí cloud computing pro firmy výhodu [2, s. 328] především při snižování a optimalizaci nákladů. Hlavní rozdíl spočívá v přechodu [3, s. 303] od kapitálových výdajů (*Capital Expenditures, CapEx*) k provozním výdajům (*Operational Expenditures, OpEx*). Organizace nemusí investovat velké částky do nákupu a údržby vlastního hardwaru (servery, datová úložiště apod.) a platí jen za to, co reálně využijí. Infrastrukturu mohou navíc jednoduše škálovat [3, s. 38] podle aktuálních potřeb. Poskytovatelé cloudu se starají o údržbu a zabezpečení, což navíc snižuje provozní náklady na vlastní odborný IT personál [3, s. 80].

Navzdory mnoha přínosům může cloud pro firmy představovat i rizika z hlediska zabezpečení a legislativních požadavků na ukládání dat [3, s. 187]. Zásadní je například otázka datové suverenity [1, s. 479] – v jaké zemi či jurisdikci jsou data reálně uložena a jaké zákony se na ně vztahují [1, s. 436], což může komplikovat dodržování předpisů [3, s. 155] [3, s. 186] jako GDPR [1, s. 246]. Dále, i když sami poskytovatelé cloudu investují do bezpečnosti, ztrácí firma přímou kontrolu nad spravovanými daty, a ty mohou být zranitelné vůči kybernetickým útokům nebo únikům způsobeným nesprávnou konfigurací. Problematická může být také závislost [3, s. 75] na konkrétním poskytovateli (*vendor lock-in*), kdy migrace do jiného cloudového prostředí znamená složitý a mnohdy nákladný proces. V neposlední řadě je potřeba pečlivě analyzovat smluvní podmínky [3, s. 237], aby byly jasně definovány standardy pro zabezpečení, dostupnost a případnou odpovědnost za porušení legislativních norem či úniky dat.

1.1 Definice cloud computingu

V literatuře i v praxi existuje celá řada definic cloud computingu. Liší se většinou v tom, na které aspekty kladou důraz – někdy více zdůrazňují technologickou stránku (virtualizace, automatizace, sdílená infrastruktura), jindy se zaměřují spíše na obchodní model (poskytnutí služeb „na vyžádání“, placení pouze za využití zdroje, flexibilita).

1.1.1 NIST 800-145

Americký Národní institut pro standardy a technologie (National Institute of Standards and Technology, NIST) definuje ve svém dokumentu „NIST Special Publication 800-145“ cloud computing jako „*model, který poskytuje všudypřítomný, pohodlný a na vyžádání dostupný síťový přístup ke sdílenému fondu konfigurovatelných výpočetních zdrojů (například sítím, serverům, úložištím, aplikacím a službám), které lze rychle alokovat a zase uvolnit, a to jen s minimálním úsilím vynaloženým na správu či komunikaci s poskytovatelem služeb.*“ [4].

NIST ve své definici [4] zdůrazňuje pět klíčových charakteristik cloudu:

- *On-demand self-service* – možnost samoobslužného objednání a řízení služeb (např. spuštění serveru) bez nutnosti komunikovat s poskytovatelem [4].
- *Broad network access* – široká dostupnost přes síť (typicky Internet), kompatibilita s různými zařízeními [4].
- *Resource pooling* – sdílený pool zdrojů (výpočetních, úložných atd.), který obsluhuje více zákazníků (multi-tenant model) [4].
- *Rapid elasticity* – rychlá a elastická škálovatelnost zdrojů dle aktuální potřeby [4].
- *Measured service* – měření a účtování [3, s. 68] podle reálného využití (pay-as-you-go) [4].

NIST dále rozeznává tři modely služeb (IaaS, PaaS, SaaS) a čtyři modely nasazení (veřejný, soukromý, komunitní a hybridní cloud).

Modely služeb podle NIST:

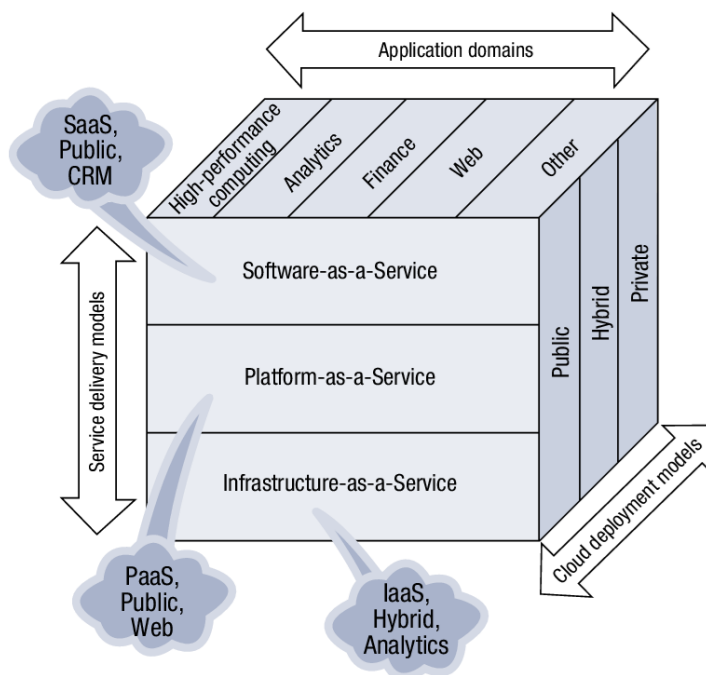
- *IaaS (Infrastructure as a Service)* je model, kde poskytovatel (CSP) nabízí základní výpočetní zdroje (servery, úložiště, síť) jako virtualizovanou infrastrukturu. Zákazník ovládá operační systémy, nasazený software i konfiguraci sítě, ale neřeší samotnou fyzickou vrstvu (datová centra) [4] [1, s. 224].
- *PaaS (Platform as a Service)* je model, kdy nad vrstvou infrastruktury je navíc k dispozici platforma pro vývoj, nasazení a správu aplikací (např. databáze, vývojová prostředí). Zákazník se tak nemusí starat o konfiguraci serverů či runtime, pouze se soustředí na samotný vývoj a provoz svých aplikací [4] [1, s. 224].
- *SaaS (Software as a Service)* je plně hotové a spravované softwarové řešení přístupné přes Internet (např. e-mailový klient, CRM systém, účetní software). Zákazník platí

zpravidla za počet uživatelů (nebo jiných metrik), přičemž se nestará o infrastrukturu ani platformu [4] [1, s. 225].

Modely nasazení podle NIST:

- *Veřejný cloud (Public Cloud)* je typ cloudu, kdy jsou služby nabízeny široké veřejnosti přes Internet. Fyzická infrastruktura patří poskytovateli, který zpravidla sdílí zdroje mezi více zákazníky (multi-tenant model) [4] [1, s. 230].
- *Soukromý cloud (Private Cloud)* bývá provozován výhradně pro jednu organizaci, ať už v jejím vlastním datovém centru, nebo ve vlastním vyhrazeném prostředí u poskytovatele. Výhodou je vyšší míra kontroly a bezpečnosti, nevýhodou vyšší náklady oproti veřejnému cloudu [4] [1, s. 230].
- *Komunitní cloud (Community Cloud)* je model, kdy je sdílené prostředí cloudu využíváno více organizacemi se společnými požadavky (např. bezpečnostní regulace, zaměření na určité odvětví, apod.). Náklady a správa se mohou dělit mezi zúčastněné subjekty [4].
- *Hybridní cloud (Hybrid Cloud)* je kombinace dvou či více modelů (např. veřejného a soukromého), které zůstávají propojené sdílenou infrastrukturou nebo aplikacemi. Tento typ umožňuje vyvážit flexibilitu a nákladovou efektivitu veřejného cloudu s bezpečností a kontrolou soukromého prostředí [4] [1, s. 230].

Na obrázku (Obrázek 1) můžeme vidět základní přehled modelů služeb cloud computingu a modelů nasazení (označovaného také jako SPI model).



Obrázek 1: SPI model cloud computingu

(zdroj: [5])

1.1.2 ISO/IEC 22123-1 a 22123-2

Mezinárodní organizace pro standardizaci (International Organization for Standardization, ISO) ve spolupráci s IEC (International Electrotechnical Commission) vydala vlastní dokumenty, které vymezují slovník [6] a definici [7] pojmů v kontextu cloud computingu. Jedná se zejména o normy ISO/IEC 22123-1 a 22123-2, které nahradily dřívější ISO/IEC 17788. Tyto dokumenty se v praxi také používají, avšak v komerční sféře se spíše setkáme s odkazem na definici NIST.

1.2 Model sdílené odpovědnosti (Shared Responsibility Model)

Z hlediska řízení bezpečnosti se cloud computing zásadně liší od tradičního (on-premise) computingu. V případě řešení on-premise (neboli *in-house*) mají zákazníci plnou kontrolu nad svou technologickou infrastrukturou – mají fyzický přístup k hardwaru a plně ovládají veškerý software v produkčním prostředí. V případě cloudu ale zákazníci používají komponenty, které jsou částečně spravovány (s výjimkou private cloudu provozovaného přímo u zákazníka v jeho vlastním data centru) poskytovateli cloudových služeb. To znamená, že odpovědnost za bezpečnost v cloudu je v tomto případě sdílena [1, s. 232] mezi zákazníky a poskytovateli těchto služeb. Tento model je znám jako *model sdílené odpovědnosti (shared responsibility model)*.

V modelu sdílené odpovědnosti se liší, za co odpovídá poskytovatel cloudové služby a za co zákazník (*tenant*). Navíc u některých činností (např. patchování operačního systému) záleží na tom, jaký model služeb [2, s. 329] (SaaS / PaaS / IaaS) a jaký model nasazení (veřejný cloud, privátní cloud, hybridní, komunitní) byl zvolen [1, s. 232]. Typický poskytovatel cloudu se stará o fyzickou bezpečnost datacenter, základní infrastrukturu a část softwarové vrstvy. Zákazník pak nese odpovědnost za správné nastavení přístupů, ochranu svých dat na aplikační úrovni a za řízení identit.

1.2.1 Primární odpovědnost poskytovatele cloudu (Cloud Service Provider)

Poskytovatel cloudové služby [2, s. 330] zpravidla odpovídá za následující typy činností:

- Fyzická bezpečnost datacenter: Zahrnuje fyzickou ostrahu objektu, zabezpečení přístupů (karty, biometrické systémy), kamerové systémy, redundantní napájení a chlazení, apod.
- Provoz a správa základní infrastruktury: Poskytovatel cloudu se stará o servery (hardware), síťové prvky (routery, switche), fyzické úložiště, hypervizory (vrstva virtualizace).
- Zajištění vysoké dostupnosti fyzických prostředků: Poskytovatel rovněž zajišťuje redundanci síťových spojení, záložní kapacity, havarijní plány pro fyzickou úroveň.
- Základní údržba a patchování hostitelů: Poskytovatel se stará o bezpečnostní záplaty a aktualizace samotné platformy (hypervizor, firmware).

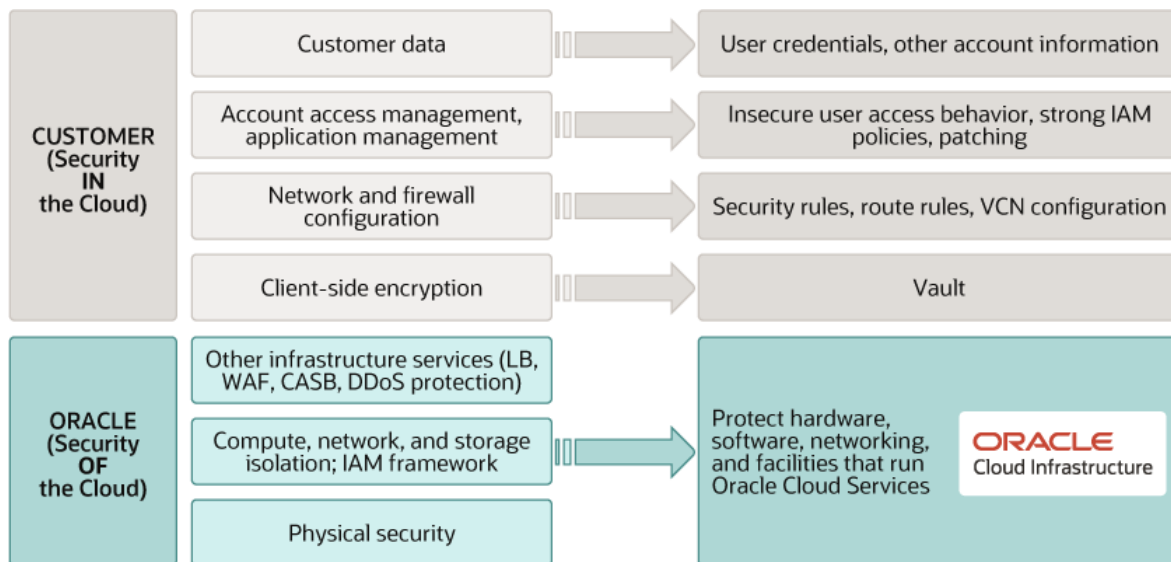
Tyto činnosti jsou v některých publikacích označovány jako *security of the cloud*, tedy jako bezpečnost samotné cloudové infrastruktury.

1.2.2 Primární odpovědnost zákazníka (Tenant)

Následující typy činností jsou v režii zákazníka [2, s. 330] cloudových služeb:

- Správa identit a přístupů k účtům: Zákazník má na starosti vytváření, správu a odstraňování uživatelských účtů (IAM), nastavování oprávnění a bezpečnost klíčů (API keys, SSH).
- Ochrana a řízení citlivých dat: Vždy spravuje svá data, provádí jejich klasifikaci (co je důvěrné, osobní údaje, atp. [1, s. 437]), má kontrolu nad tím, která data se do cloudu ukládají, šifrování na aplikační úrovni, mazání dat (*lifecycle management*) [3, s. 174].

Tyto činnosti jsou obvykle označovány jako *security in the cloud*, tedy vše, co se týká konkrétního využití a konfigurace cloudového prostředí zákazníkem. Toto rozdělení ilustruje obrázek (Obrázek 2).



Obrázek 2: Security IN the Cloud vs. OF the Cloud

(zdroj: [8])

1.2.3 Sdílené odpovědnosti podle modelu služby (SaaS, PaaS, IaaS)

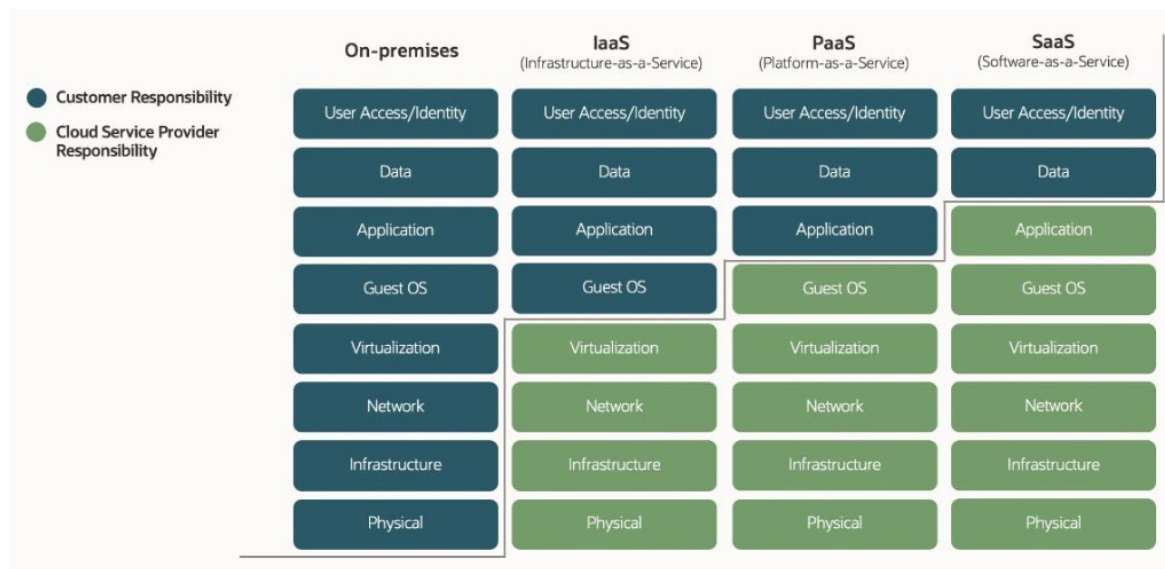
U všech ostatních odpovědností pak velmi záleží na použitém modelu služeb [3, s. 193], v němž zákazník pracuje. Někdy může být daná činnost odpovědností poskytovatele cloudu, zatímco jindy může být naprosto stejná činnost odpovědností zákazníka. Typicky:

- SaaS (Software as a Service) – U tohoto modelu je většina technického nastavení včetně zabezpečení na straně poskytovatele [3, s. 51]. Patchování aplikace je téměř vždy v odpovědnosti poskytovatele (zákazník řeší jen uživatelské nastavení, ne instalaci). Nastavení bezpečnostních funkcí v aplikaci je sdílená odpovědnost – poskytovatel dává nástroje (např. přístupová práva, šifrování dat v SaaS), ale zákazník určuje, kdo do aplikace může přistupovat a jaká data [2, s. 333] se tam ukládají. Zálohování dat je v režii poskytovatele [3, s. 122], nicméně politiky retence (jak dlouho se data uchovávají) nebo doplňkové zálohy mohou být v gesci zákazníka.
- PaaS (Platform as a Service) – Zde jsou některé činnosti rozdělené. Patchování operačního systému má na starosti poskytovatel [3, s. 154] [2, s. 332], který garantuje aktualizace OS a runtime prostředí (např. databázový server, aplikační server) [3, s. 127]. Správa a konfigurace aplikačního kódu je v odpovědnosti zákazníka (správné

nasazení kódu, aktualizace knihoven v rámci aplikace, nastavení bezpečnostních závislostí). O škálování a využití platformy se stará poskytovatel [3, s. 49], který zajišťuje mechanismus škálování (auto-scaling) [3, s. 117], zákazník následně volí, zda (a jak) škálování využije, a je také zodpovědný za náklady i za to, zda škálování nepřinese nové bezpečnostní hrozby.

- IaaS (Infrastructure as a Service) – U tohoto modelu je nejvíce technického nastavení odpovědností zákazníka [3, s. 131]. Patchování a zabezpečení virtuálních strojů (OS) je v režii zákazníka [3, s. 44], protože zákazník spravuje celý OS. Veškerá virtuální síťová konfigurace (subnety, security group, firewall) je v gesci zákazníka, který je nastavuje. Poskytovatel nabízí nástroje pro segmentaci a pravidla. Šifrování dat na úrovni disku může být zčásti v režii poskytovatele (poskytovatel nabízí šifrované úložiště) i zákazníka, který rozhoduje, zda a jak nasadí vlastní šifrovací klíče (*Bring Your Own Key, BYOK*).

Na obrázku (Obrázek 3) můžeme vidět rozdělení odpovědností podle modelu služeb.



Obrázek 3: Model sdílené odpovědnosti podle modelu služeb

(zdroj: [9])

Jak je z uvedeného patrné, model IaaS poskytuje největší volnost v konfiguraci a nastavení na míru, ovšem za cenu nejvyšší míry odpovědnosti – je nutné samostatně řešit a správně nastavit bezpečnostní opatření a konfigurace (včetně operačního systému). Naopak SaaS přenáší většinu technických a provozních aspektů na stranu poskytovatele, což však znamená méně prostoru pro vlastní úpravy a nutnost přijmout již přednastavená řešení. S

ohledem na výše uvedené neexistuje univerzální řešení, které by bylo vhodné pro každou situaci [3, s. 114]. Vždy je nutné důkladně posoudit specifické požadavky, vyhodnotit související rizika a na základě toho zvolit takový model služeb, který optimálně vyhoví konkrétním potřebám daného projektu či organizace [1, s. 233].

1.3 Nástroje k hodnocení bezpečnosti cloudových poskytovatelů

Společnost Cloud Security Alliance (CSA) vyvinula *Cloud Controls Matrix (CCM)* a dotazník *Consensus Assessments Initiative Questionnaire (CAIQ)*, což jsou dva klíčové nástroje, které mohou organizacím pomoci při hodnocení a srovnávání bezpečnostních opatření a procesů různých cloudových poskytovatelů, a to zejména v rané fázi výběru nebo při migraci z on-premise infrastruktury do cloudu [10].

1.3.1 Cloud Controls Matrix (CCM)

Cloud Controls Matrix je podrobný rámec vyvinutý organizací Cloud Security Alliance (CSA). Je sladěný se *Security Guidance for Cloud Computing* vydanými stejnou organizací a v praxi je považován za *de facto* standard pro zajištění bezpečnosti v cloudu.

Skládá se ze 197 kontrolních cílů (*controls*), které jsou uspořádány do 17 domén [11] a pokrývají všechny klíčové aspekty cloudových technologií (např. BCM-xx pro Business Continuity, IAM-xx pro řízení identit apod.). Výhodou je, že tyto cíle jsou často mapovány na mezinárodní standardy a regulace (např. ISO/IEC 27001/27002/27017/27018, AICPA TSC, CIS Controls, NIST CSF, NIST 800-53, PCI DSS aj.). Díky tomu mohou organizace, které musí splňovat určitou legislativu nebo mezinárodní normu [3, s. 172], využít rámec CCM ke sladění těchto požadavků s konkrétními kontrolami, které pro danou oblast plní příslušný poskytovatel.

1.3.2 Consensus Assessments Initiative Questionnaire (CAIQ)

Oproti tomu CAIQ (Consensus Assessments Initiative Questionnaire) představuje standardizovaný dotazník [11] typu *self-assessment*, který se váže k rámci CCM. Tento dotazník vyplňují poskytovatelé sami, případně jej mohou zpracovat na žádost zákazníka. CAIQ obsahuje sadu otázek, které vycházejí z kontrolních cílů definovaných v rámci CCM, a slouží jako strukturovaný nástroj pro posouzení toho, jak (a zda vůbec) cloudoví poskytovatelé zajišťují konkrétní bezpečnostní a provozní opatření.

Někteří [12] poskytovatelé cloudových služeb své vyplněné CAIQ dotazníky zveřejňují přímo na svých webových stránkách nebo v registru CSA (STAR Registry). Pokud z CAIQ nebo z mapování v CCM vyplyne, že poskytovatel nesplňuje [2, s. 348] některý z kritických požadavků, může to být důvodem k výběru jiného poskytovatele či ke zvážení kompenzačních opatření, například nasazení vlastních bezpečnostních nástrojů v rámci hybridního modelu.

1.4 Přehled poskytovatelů cloudových služeb a současné trendy

Pokud bychom zahrnuli všechny kategorie od největších *hyperscalerů* až po lokální či úzce specializované poskytovatele, můžeme konstatovat, že celosvětově existují tisíce společností spadajících pod široký pojem *cloudový poskytovatel*. Z praktického hlediska se proto nejčastěji používají termíny jako velká trojka (AWS, Azure, GCP) [1, s.226], případně top 5–7 poskytovatelů (doplněné o společnosti Alibaba, IBM, Oracle a případně další), kteří bývají řazeni podle tržní kapitalizace, podílu na trhu, počtu zákazníků či jiných podobných kritérií. K tomuto účelu slouží oficiální žebříčky publikované renomovanými analytickými společnostmi (např. Gartner, IDC, Canalys, Synergy Research Group). Tyto žebříčky se mohou mírně lišit vzhledem k odlišným metodikám, definicím cloudu či dalším použitým kritériím jednotlivých analytických firem.

V tabulce (Tabulka 1) je uvedeno pět největších poskytovatelů cloudové infrastruktury (IaaS/PaaS) podle tržního podílu za třetí kvartál roku 2024, a to na základě reportu CRN [13] (resp. Synergy Research [14]). Součástí tabulky je rovněž orientační odhad tržní kapitalizace mateřských společností v USD, který vychází z veřejně dostupných finančních údajů.

Tabulka 1 Největší poskytovatelé cloudu dle tržního podílu v Q3 2024

Pořadí (podle podílu)	Cloud (Společnost)	Tržní podíl (Q3 2024)	Odhad tržní kapitalizace (USD)
1.	AWS (Amazon)	34 %	~1,0–1,4 bilionu
2.	Azure (Microsoft)	22 %	~1,7–2,0 bilionu
3.	GCP (Alphabet)	13 %	~1,3–1,6 bilionu
4.	Alibaba Cloud	4 %	~200–250 miliard
5.	Oracle Cloud	3 %	~200–300 miliard

(zdroj: [13])

Podle Johna Dinsdalea [14], hlavního analytika společnosti Synergy Research Group, je umělá inteligence (AI) klíčovým faktorem akcelerace růstu trhu cloudových služeb v roce 2024. Nové služby a technologie orientované na AI vedou k nárůstu poptávky, což zvyšuje příjmy poskytovatelů a umožňuje další investice do základních technologií. Tento cyklus přispívá k výraznému růstu trhu, který ve třetím čtvrtletí 2024 dosáhl meziročního nárůstu o 23 %, což představuje čtvrtý po sobě jdoucí kvartál s rostoucím tempem růstu.

2 PŘEDSTAVENÍ ORACLE CLOUD INFRASTRUCTURE (OCI)

Před vstupem do světa cloudu se Oracle proslavil zejména jako lídr v oblasti databázových systémů a podnikových řešení. Společnost byla založena [15] v roce 1977 Larrym Ellisonem, Bobem Minerem a Edem Oatesem. Jejich produkt *Oracle Database* se brzy stal dominantním nástrojem pro správu databází ve velkých organizacích.

Na přelomu tisíciletí začaly IT sektor výrazně proměňovat nové cloudové technologie [1, s. 226]. Velcí technologičtí hráči jako Amazon či Microsoft v té době uvedli na trh rozsáhlé cloudové platformy, což vedlo mnoho společností k postupnému odklonu od tradičních on-premise infrastruktur. Společnost Oracle se rozhodla tomuto trendu přizpůsobit a rovněž rozšířila své portfolio o cloudová řešení.

2.1 Oracle Public Cloud

V roce 2011 uvedl [16] Oracle na trh Oracle Public Cloud, čímž oficiálně vstoupil na pole cloud computingu. Základní nabídka zahrnovala:

- *Oracle Database Cloud Service*: Verzi vlajkového databázového produktu provozovanou v cloudu (v modelu služeb typu PaaS) [17].
- *Oracle Java Cloud Service*: Platformu umožňující vývoj a nasazení Java aplikací (v modelu služeb typu PaaS) [17].
- *Oracle Fusion Applications*: Sadu podnikových aplikací pro finance, HR a řízení dodavatelského řetězce (v modelu služeb typu SaaS) [17].

Ve srovnání s konkurencí, kterou v té době představovaly zejména společnosti Amazon (AWS) a Microsoft (Azure), byl vstup společnosti Oracle na trh cloudových služeb poměrně pozdní. První cloudové produkty Oracle se navíc setkaly se smíšenými reakcemi. Trhu již tehdy dominovalo AWS díky široké nabídce služeb a rozsáhlé infrastruktuře. Aby společnost Oracle posílila svou pozici, musela pokračovat v investicích, zejména do rozšiřování svých datových center a vývoje nových funkcionalit.

2.2 Oracle Cloud Infrastructure (OCI)

Společnost Oracle začala nabízet své první infrastrukturní služby typu IaaS (např. *Compute Cloud Service*, *Storage Cloud Service*) již v letech 2012 a 2013 [18]. Tyto služby byly původně označovány jako *Oracle Public Cloud IaaS*, později přejmenované na *Classic*, a sdílely většinu infrastruktury se službami typu PaaS a SaaS.

Koncem roku 2016 Oracle veřejně představil [19] novou generaci IaaS služeb označovanou jako *Bare Metal Cloud Services (BMCS)*. Jednalo se o kompletně novou platformu, která byla navržena s důrazem na výkonné fyzické (*bare metal*) servery, vyšší rychlost, lepší izolaci zdrojů a vyšší flexibilitu. Již zhruba o rok dříve navíc došlo k rozšíření nabídky Oracle Cloud o službu *Exadata Cloud Service*, což je vysoce výkonná databázová platforma určená pro provoz náročných databázových úloh bez nutnosti vlastnit a spravovat fyzický a finančně nákladný Exadata rack.

Platforma Bare Metal Cloud Services byla později přejmenována na Oracle Cloud Infrastructure (OCI) a stala se základem tzv. *druhé generace* cloudových služeb Oracle (OCI Gen2), která dnes představuje hlavní platformu společnosti Oracle pro služby typu IaaS, PaaS i další cloudové produkty.

2.3 Oracle Cloud Infrastructure (OCI) Gen2

Platforma Oracle Cloud Infrastructure druhé generace (*OCI Gen2*) byla oficiálně představena Larrym Ellisonem v říjnu 2018 na konferenci Oracle OpenWorld 2018 [20]. Na rozdíl od první generace OCI (později označované jako *Classic*) se jedná o kompletně přepracovanou cloudovou platformu, jejímž primárním zaměřením je bezpečnost (koncept *Security First*) [20]. Zvýšené bezpečnosti bylo dosaženo zejména zavedením virtualizace sítí (*Virtual Cloud Network, VCN*) a definováním nových bezpečnostních modelů založených na tzv. *kompartmentech (compartments)*, tedy logických strukturách určených k organizaci a řízení přístupu ke zdrojům v OCI. Obě tato opatření významně snižují riziko potenciálních útoků na hypervizor.

Vylepšení se dále dotkla také výkonu a škálovatelnosti, což bylo klíčové především pro náročné podnikové aplikace a databázové systémy, jako například Oracle Autonomous Database. Druhá generace OCI rovněž přináší flexibilnější správu zdrojů, detailnější monitoring a snazší nasazení kontejnerových řešení. V dalším textu budeme pojmem OCI výhradně označovat druhou generaci OCI Gen2, pokud nebude výslovně uvedeno jinak.

OCI dnes představuje plně vybavenou moderní cloudovou platformu, splňující přísné bezpečnostní standardy a certifikace, mezi něž patří ISO/IEC 27001, SOC (Service Organization Control) 1, 2 a 3, PCI DSS (Payment Card Industry Data Security Standard), ISO/IEC 27017 a ISO/IEC 27018 (zaměřené specificky na ochranu osobních údajů v cloudu), HIPAA, FedRAMP (Federal Risk and Authorization Management Program), CSA STAR a mnohé další [21].

Nabídka služeb v rámci OCI zahrnuje kompletní škálu od infrastrukturních řešení (IaaS), přes platformní služby (PaaS), až po čistě softwarové produkty (SaaS), včetně specializovaných variant typu *Function as a Service (FaaS)* [22], *Identity as a Service (IDaaS)* aj. OCI dále nabízí inovativní technologie a služby zaměřené na umělou inteligenci, strojové učení, blockchain či Internet věcí (IoT). Výhodou OCI je také její flexibilita a podpora hybridních řešení, která firmám umožňuje kombinovat stávající on-premise infrastruktury s cloudovými službami společnosti Oracle. Díky tomu mohou organizace do cloudu přecházet postupně, a přitom zachovávat vysokou úroveň kontroly nad svými daty a aplikacemi [23].

Aktuálně je platforma OCI dostupná v 50 regionech a 25 zemích světa, zahrnující Severní Ameriku, Evropu, Asii, Blízký východ, Jižní Ameriku či Austrálii a Oceánii, přičemž další jsou postupně přidávány a zpřístupňovány. Kompletní seznam lze nalézt na webových stránkách *Public Cloud Regions* [24]. Oracle pojmenovává jednotlivé regiony podle lokality, např.:

- us-ashburn-1 (Ashburn, USA)
- uk-london-1 (Londýn, Spojené království)
- eu-frankfurt-1 (Frankfurt, Německo)
- ap-tokyo-1 (Tokio, Japonsko)

Aby vyhověla bezpečnostním, legislativním i provozním nárokům jednotlivých zemí, OCI dále dělí regiony do několika skupin:

- *Komerční (Commercial)* – regiony určené pro obecné komerční využití. Jde o nejběžnější a nejpočetnější skupinu.
- *Vládní (Government)* – regiony, které jsou navrženy tak, aby splňovaly přísné bezpečnostní, regulační i legislativní požadavky vládních institucí (např. US Government, US DoD, apod.) [25].
- *EU Sovereign Cloud* – regiony zajišťující plnou suverenitu dat v souladu s předpisy Evropské unie.
- *Oracle Database@Azure / Oracle Database@Google Cloud* – řešení umožňující provoz databázových služeb Oracle v prostředí Azure nebo Google Cloud, určené pro multicloudové nasazení a snadnou integraci s těmito platformami.

Na obrázku (Obrázek 4) můžeme vidět typy OCI regionů dostupných v Evropě.



Obrázek 4: Typy regionů Oracle Cloud Infrastructure (OCI) v Evropě

(zdroj: [24])

2.4 Typy účtů dostupných v OCI

OCI nabízí několik variant účtů a platebních modelů pro různé potřeby běžných uživatelů i firem – od bezplatného vyzkoušení až po flexibilní placené programy. Níže jsou přehledně popsány čtyři hlavní typy:

2.4.1 Always Free

Always Free [26] představuje sadu cloudových zdrojů v OCI, které jsou k dispozici zdarma a bez časového omezení pro všechny uživatele. Slouží k provozu menších aplikací, experimentování a vývojovým či testovacím [3, s. 78] účelům bez nákladů. Always Free zdroje jsou dostupné automaticky po zřízení účtu a lze je používat trvale (i po skončení případného trialu), aniž by bylo nutné cokoli platit.

Do programu Always Free spadají vybrané cloudové služby poskytované v omezeném rozsahu. Patří mezi ně například až dvě malé virtuální (VM) instance (AMD nebo ARM) nebo dvě autonomní databáze s kapacitou 20 GB každá, maximum 200 GB blokového úložiště, 20 GB objektového úložiště a dále služby jako load balancer, monitoring nebo VPN

v omezené kapacitě. Dále platí, že pokud používáte pouze zdroje v režimu Always Free, nemáte nárok na plnou technickou podporu od Oracle (k dispozici je jen komunitní podpora). Pro získání oficiální podpory či navýšení limitů je nutné přejít na placený účet.

2.4.2 Free Tier (trial)

Free Tier [27] je bezplatná zkušební verze účtu OCI pro nové zákazníky. Kromě Always Free zdrojů obsahuje jednorázový kredit 300 USD na dobu 30 dnů pro vyzkoušení libovolných dalších cloudových služeb, včetně výkonnějších konfigurací či většího počtu instancí, které by jinak spadaly mimo Always Free.

Během těchto 30 dnů nejsou účtovány žádné poplatky – veškerá spotřeba se odečítá z poskytnutého kreditu. Po vypršení zkušební lhůty navíc zůstávají dostupné Always Free zdroje, takže některé služby může uživatel nadále využívat zdarma i bez přechodu na placený účet.

2.4.3 Pay-As-You-Go (PAYG)

Pay As You Go [28] je průběžný (*on-demand*) platební model, kdy zákazník platí měsíčně zpětně za skutečně spotřebované služby. Umožňuje to velmi flexibilní využívání OCI – vhodné například pro menší firmy a startupy, projekty s proměnlivou nebo nejistou zátěží, nebo pro uživatele přecházející z Free Tier, kteří chtějí pokračovat v používání cloudových služeb bez dlouhodobého kontraktu. PAYG je výchozí model po upgradu z trialu, pokud si zákazník nezvolí variantu s Universal Credits.

Tento model poskytuje maximální flexibilitu, PAYG umožňuje snadno začít v malém a postupně navyšovat využití podle potřeby. Platí se pouze za to, co zákazník opravdu využije, a to podle standardního ceníku s měsíční fakturací zpětně (spotřeba je měřena a účtována po uplynutí každého období). Nevýhodou může být vyšší cena při větším nebo dlouhodobém využití – u modelu PAYG se uplatňují standardní on-demand ceny (bez objemových slev za závazek), takže při velké spotřebě může být celkový účet vyšší než v rámci programu Universal Credits s předplacenými kredity či individuální smlouvou.

2.4.4 Universal Credits

Universal Credits [29] je flexibilní předplacený model placení za cloud, vhodný hlavně pro firmy s větší či stabilní spotřebou. Zákazník se u něj zaváže k určité výši útraty na předem stanovené období (minimálně 12 měsíců) a předplatí si kredit, který pak může průběžně

čerpat používáním libovolných služeb OCI. Tento model slouží organizacím s předvídatelnou nebo trvalou zátěží – umožňuje jim získat lepší cenové podmínky a plánovat náklady na cloud dopředu (podobá se to paušálu za služby).

Předplacené Universal Credits lze uplatnit na všechny hlavní služby OCI (IaaS/PaaS) – zákazník má přístup ke stejnému portfoliu služeb jako v on-demand (PAYG) modelu, jen čerpání probíhá z předplaceného kreditu.

2.4.5 Enterprise Agreements (EA)

Kromě zmíněných běžných typů účtů (Always Free, Free Tier, Universal Credits a Pay As You Go) existují ještě další varianty platebních modelů, speciálně určené pro velké společnosti nebo organizace s rozsáhlejšími požadavky a specifickými potřebami.

Enterprise Agreement (EA) je speciální forma dlouhodobé smlouvy s Oracle, navržená především pro větší společnosti a podniky s vysokou spotřebou cloudových služeb. Slouží pro zákazníky, kteří chtějí individuální smluvní podmínky, cenové výhody a pevně stanovené podmínky na delší období (typicky 2–5 let). Tyto typy smluv zpravidla zahrnují i prémiovou technickou podporu ze strany Oracle (včetně account managementu) [30].

3 KLÍČOVÉ BEZPEČNOSTNÍ FUNKCE V OCI

Platforma OCI byla od počátku navržena tak, aby bezpečnost nebyla jen dodatečnou funkcí, ale základním stavebním kamenem celého prostředí [31]. OCI tedy kombinuje více vrstev ochrany – od hardwarové izolace a šifrování přes integrované nástroje pro správu přístupu a identit až po automatizované monitorování a implementaci opravných prostředků. Každá z těchto komponent je navržena s ohledem na principy *security by design* [1, s. 235] [2, s. 288] a vzájemně se doplňuje, čímž zajišťuje komplexní a vícestupňovou ochranu cloudových zdrojů v OCI.

V této kapitole jsou rozebrány klíčové bezpečnostní mechanismy OCI a jejich úloha v celkové bezpečnostní architektuře podniku.

3.1 Základní prostředky pro správu zdrojů v OCI

OCI poskytuje uživatelům několik způsobů [32], jak spravovat cloudové prostředí a vytvářet nové zdroje. Základní a nejprístupnější metodou je použití *OCI Console*, přehledného webového rozhraní pro ruční konfiguraci služeb.

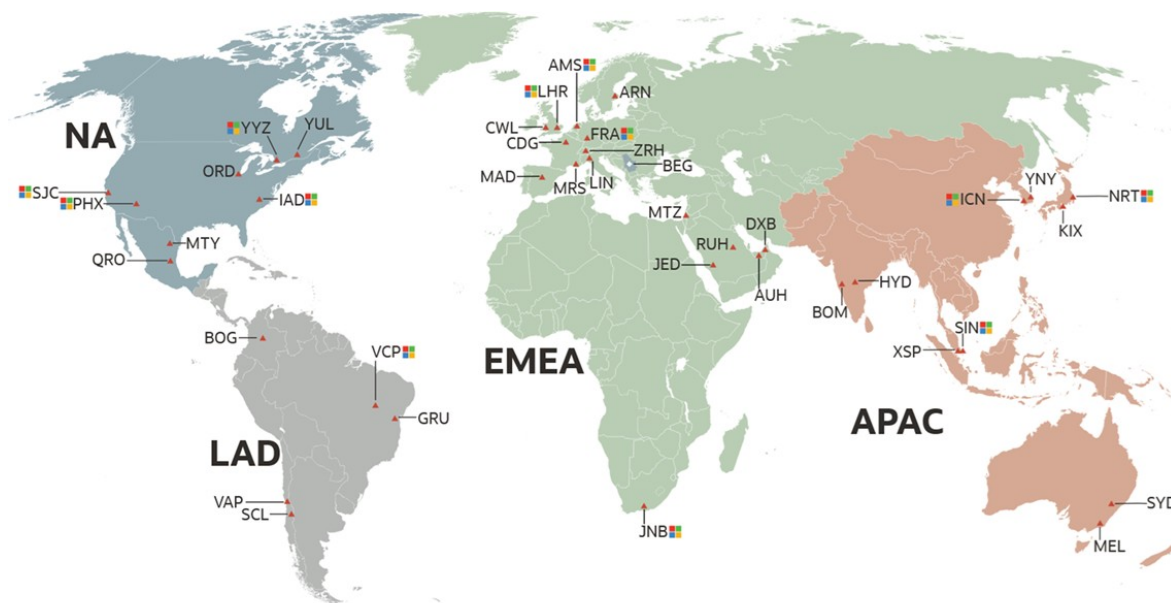
Pro automatizaci, skriptování a integraci s dalšími nástroji lze využít *OCI Command Line Interface (OCI CLI)*, což je nástroj umožňující přímou interakci s OCI prostřednictvím příkazové řádky. Jeho použití je vhodné zejména pro pokročilé uživatele, kteří potřebují provádět opakované operace, nebo pro integraci do CI/CD nástrojů. Lze jej spouštět buď lokálně, nebo v prostředí *OCI Cloud Shell*, což je integrované, předkonfigurované terminálové prostředí dostupné přímo z OCI Console, které obsahuje předinstalované nástroje jako OCI CLI, Terraform či Git, čímž výrazně zjednodušuje práci bez nutnosti nastavovat lokální prostředí. OCI Console obsahuje i vestavěný *OCI Code Editor*, který umožňuje přímo v prohlížeči upravovat skripty, Terraform šablony, nebo cloudovou konfiguraci bez nutnosti přepínání do externích nástrojů. Tento editor je integrován s Cloud Shell a je vhodný pro rychlé úpravy přímo v kontextu prostředí.

Dalšími možnostmi správy OCI zdrojů je využití *OCI SDK (Software Development Kits)* dostupných pro více programovacích jazyků (např. Python, Java, Go), nebo infrastruktura jako kód pomocí Terraformu, který umožňuje deklarativně spravovat prostředí OCI formou šablon [32].

3.2 Region, doména dostupnosti, fault doména

Region v prostředí OCI představuje nejvyšší úroveň celé infrastruktury. Každý region je samostatná geografická oblast, která zahrnuje několik vzájemně oddělených lokalit nazývaných *doména dostupnosti* (*Availability domain*) [33].

Na obrázku (Obrázek 5) můžeme vidět přehled OCI regionů ve světě.



Obrázek 5: Přehled OCI regionů ve světě

(zdroj: [34])

Doména dostupnosti (*Availability domain*, AD) je podřízeným prvkem regionu, funguje nezávisle a nabízí vysokou míru spolehlivosti. Domény dostupnosti jsou navzájem izolované, odolné vůči selhání a je vysoce nepravděpodobné, že by došlo k jejich současnému výpadku nebo že by selhání jedné domény ovlivnilo ostatní. Pro zajištění vysoké dostupnosti a minimalizaci rizik se při konfiguraci cloudových služeb doporučuje využívat více domén dostupnosti. Je však nutné vzít v úvahu, že některé prostředky – například instance a k nim připojené úložné svazky – musejí být vytvořeny v rámci téže domény dostupnosti [33].

Fault doména (FD) představuje dodatečné seskupení hardwaru a infrastruktury v rámci jedné domény dostupnosti. Každá doména dostupnosti přitom obsahuje tři fault domény. Jejich hlavním přínosem je tzv. *anti-affinita*, která umožňuje rozprostřít instance tak, aby nesdílely stejné fyzické prostředky. V důsledku toho, pokud v jedné fault doméně dojde k

hardwarovému výpadku nebo plánované údržbě, instance běžící v ostatních fault doménách zůstávají neovlivněny [33].

3.3 Správa identit a přístupů (IAM)

Služba OCI *Identity and Access Management* (IAM) [35] slouží k řízení ověřování uživatelů [2, s. 337] a autorizace přístupu k prostředkům v OCI [1, s. 237]. Umožňuje vytvářet uživatele, přiřazovat je do skupin a definovat politiky, které určují, jaké akce mohou dané skupiny provádět v rámci konkrétních oddílů neboli kompartmentů (compartments) a zdrojů.

3.3.1 Kompartmenty (Compartments)

V rámci OCI představují kompartmenty [35] základní mechanismus pro logické oddělení a správu cloudových zdrojů. Jsou navrženy tak, aby umožňovaly organizaci zdrojů (např. vývoj, testování, produkce), aplikaci bezpečnostních politik (*policies*), izolaci prostředků z hlediska bezpečnosti a souladu s regulačními požadavky (*compliance*) a jednodušší správu nákladů.

3.3.2 Řízení přístupu na základě rolí (RBAC, Groups, Policies)

Řízení přístupu ke zdrojům na základě rolí (*Role-Based Access Control, RBAC*) a princip nejmenších oprávnění v OCI znamená, že uživatelům a systémovým entitám (*principals*) jsou přidělována pouze ta oprávnění, která jsou nezbytná pro výkon jejich specifických úkolů – a nic navíc [1, s. 233] [2, s. 286].

Uživatelům v OCI nejsou přiřazována práva přímo, ale prostřednictvím členství ve skupinách (*groups*), přičemž skupina [35] představuje logické seskupení uživatelů, kteří mají vykonávat podobné role (např. administrátoři databází, síťoví inženýři, vývojáři). Přístupové politiky (*security policies*) následně definují pravidla, která určují, které skupiny mají jaká oprávnění k jakým zdrojům v rámci organizace (*tenancy*) nebo kompartmentu. Politiky se zapisují ve formě deklarativních vět v jazyce OCI Policy Language [36], např.:

```
Allow group Developers to manage instances in compartment Dev-Compartment
```

3.4 Správa klíčů a šifrování dat

Pro ochranu dat v cloudu je klíčové šifrování – a to jak dat uložených (*at rest*), tak dat přenášených (*in transit*) [1, s. 238]. OCI nabízí vestavěné mechanismy pro šifrování na všech úrovních. Všechny standardní úložiště (diskové svazky, objektové úložiště atd.) v OCI jsou

ve výchozím stavu šifrovány metodou 256-bit Advanced Encryption Standard (AES-256) za pomoci klíčů spravovaných Oracle [37].

3.4.1 Správa šifrovacích klíčů (OCI Vault, Oracle Key Management)

Pro zákazníky, kteří vyžadují vyšší úroveň kontroly nad správou šifrovacích klíčů, nabízí OCI službu *Vault* (též označovanou jako *Oracle Key Management, KMS*). Tato služba umožňuje vytváření, správu a ochranu vlastních šifrovacích klíčů prostřednictvím hardwarových bezpečnostních modulů (*HSM*), které splňují přísné bezpečnostní normy FIPS 140-2 Level 3 [38]. Uložené klíče lze následně využít k ochraně dat v široké škále služeb, včetně Object Storage, blokového úložiště (*block volumes*), databází a dalších. Významnou výhodou je možnost centrální správy životního cyklu [3, s. 208] klíčů – jejich vytváření, deaktivace, rotace – a definování přístupových politik upravujících, kdo a jakým způsobem může s klíči nakládat.

V případě zvýšených nároků na izolaci a bezpečnost kryptografických klíčů lze využít službu *Dedicated KMS*, jež nabízí vyhrazený oddíl (*partition*) v HSM zařízení [39].

3.4.2 Externí KMS (External Key Management Service)

Služba OCI KMS standardně využívá hardwarový bezpečnostní modul umístěný v datovém centru společnosti Oracle. Pro maximální zabezpečení dat a pro zákazníky, kteří musí z důvodu regulačních požadavků uchovávat kryptografické klíče zcela mimo prostředí Oracle cloudu, je k dispozici také možnost využít externí bezpečnostní modul společnosti Thales (*Thales CipherTrust Manager*) [40].

3.4.3 Šifrování komunikace

V oblasti zabezpečení komunikace podporuje OCI automaticky šifrované protokoly, konkrétně HTTPS a TLS. Standardně je využívána verze TLS 1.2 [41], přičemž pro vybrané služby je dostupná také modernější verze TLS 1.3 [42]. OCI zároveň důrazně doporučuje, aby veškerá komunikace směrem do cloudového prostředí byla zabezpečena pomocí SSL/TLS protokolů. Pro usnadnění správy digitálních certifikátů a jejich integrace s cloudovými a webovými službami poskytuje Oracle specializované nástroje, například službu *Oracle OCI Certificates*.

3.4.4 Šifrování dat v operační paměti (RAM)

S nástupem [43] nových technologií perzistentních pamětí, jako je NVDIMM, které kombinují vlastnosti operační paměti a trvalého úložiště, vznikají nové bezpečnostní výzvy. Data uložená v těchto pamětech mohou přetrvávat i po vypnutí systému, což zvyšuje riziko neoprávněného přístupu k citlivým informacím, jako jsou hesla nebo šifrovací klíče.

Platforma OCI poskytuje podporu [44] pro *Confidential Computing*, tedy technologie umožňující šifrování dat během jejich zpracování v operační paměti (označováno jako data *in-use*). Tato technologie je dostupná u vybraných virtuálních strojů (VM) a bare metal instancí, a to díky technologiím *AMD Secure Encrypted Virtualization (SEV)* a *AMD Transparent Secure Memory Encryption (TSME)*. Obě technologie umožňují hardwarově řízené šifrování operační paměti, čímž výrazně zvyšují bezpečnost a ochranu dat.

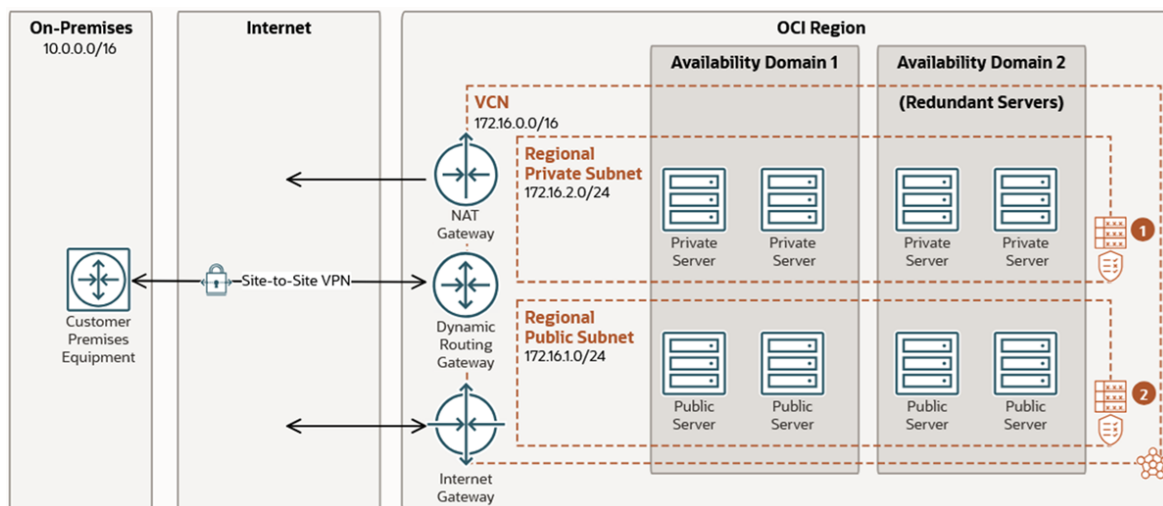
3.5 Síťová bezpečnost

Základem bezpečné architektury v OCI je Virtual Cloud Network (VCN) – virtuální softwarově spravované [1, s. 127] síťové prostředí definované zákazníkem v cloudu Oracle, analogické k tradiční firemní síti v datacentru. VCN umožňuje zákazníkovi oddělit svůj provoz od ostatních tenantů a konfigurovat adresní prostor, podsítě, směrovací tabulky a brány [45].

3.5.1 Virtual Cloud Network (VCN)

Virtual Cloud Network je soukromá síť [1, s. 247] definovaná jedním nebo více CIDR bloky (IPv4 nebo IPv6), která poskytuje logickou izolaci cloudových prostředků. Velikost VCN rozsahu může být od /16 do /30 (např. 10.0.0.0/16). Doporučuje se používat privátní IP adresní rozsahy definované v RFC 1918, s výjimkou rozsahů 10.0/8 nebo 172.16/12, které Oracle nepodporuje, místo nich lze použít 10.0/16, 172.16/16 či 192.168/16 [45].

Na obrázku (Obrázek 6) můžeme vidět příklad síťového připojení infrastruktury v OCI k privátní síti pomocí Site-to-Site VPN a veřejnému Internetu včetně příslušných zvolených IP rozsahů.



Obrázek 6: Ukázka základní síťové topologie v OCI

(zdroj: [46])

3.5.2 Security Lists

Security Lists představují seznamy síťových pravidel (funkčně obdobné *Access Control Lists*, *ACL* [1, s. 248]), které lze aplikovat na konkrétní podsítě. Tato pravidla určují, jaké typy síťového provozu (na základě IP adresy, portu a protokolu) jsou pro danou podsít' povoleny nebo zakázány. Pravidla mohou být buď *stateful* (ve výchozím nastavení) nebo *stateless*. Stateful pravidla jsou aplikována automaticky na oboustranný provoz – to znamená, že pokud je povolen příchozí provoz určitého typu, automaticky je povolen i odpovídající odchozí provoz zpět. Naopak stateless pravidla jsou aplikována pouze jednosměrně, takže je nutné výslovně definovat povolení jak pro příchozí, tak pro odchozí provoz zvlášť [47].

3.5.3 Network Security Groups (NSG)

Network Security Group (NSG) jsou flexibilnější firewallová pravidla na úrovni síťových skupin instancí. Zatímco security list se aplikuje na celou podsít' a ovlivňuje veškerý síťový provoz v rámci této podsítě, NSG umožňuje definovat síťová pravidla na úrovni skupiny jednotlivých síťových rozhraní (VNIC), například těch, které patří ke stejnému typu serveru nebo službě. Každé VNIC může být členem až pěti NSG, což zajišťuje flexibilitu při správě přístupových pravidel [47].

Kombinací Security Lists a NSG lze docílit jemnější kontroly nad síťovým provozem a důsledně tak uplatňovat princip nejmenších oprávnění i na úrovni sítě.

3.5.4 Síťové brány (Gateways)

V prostředí OCI jsou k dispozici tři základní typy síťových bran [48], které umožňují efektivní a bezpečné propojení virtuálních cloudových sítí (VCN) s externími službami a Internetem:

- *Internet Gateway* – Umožňuje přímé připojení VCN k veřejnému Internetu. Tato brána je nezbytná pro zajištění veřejného přístupu k prostředkům v rámci VCN, jako jsou například webové servery. Z hlediska bezpečnosti je nutné použít omezit pouze na nezbytné podsítě a vždy s vhodně nastavenými bezpečnostními pravidly.
- *NAT Gateway* – Umožňuje instancím v privátních podsítích přístup k veřejnému Internetu pro odchozí komunikaci, aniž by byly samy dostupné externě (lze použít například pro stahování aktualizací).
- *Service Gateway* – Umožňuje privátní přístup z VCN k interním službám OCI (jako je např. Object Storage) bez nutnosti využívat veřejný Internet.

Tyto nástroje dohromady zajišťují, že infrastruktura v OCI může být navržena jako vrstvená (zónová) síť, kde jsou citlivé části systému odděleny a chráněny více úrovněmi zabezpečení.

3.5.5 OCI Bastion

OCI Bastion [49] je plně spravovaná služba, která poskytuje bezpečný a časově omezený přístup k prostředkům umístěným v privátních podsítích bez veřejných IP adres. Umožňuje autorizovaným uživatelům navazovat SSH spojení z definovaných IP adres bez nutnosti nasazení a správy tradičních jump hostů. Služba podporuje tři typy relací:

- *Spravovaná (managed) SSH relace* – Umožňuje přímé SSH připojení k instanci s nainstalovaným Oracle Cloud Agentem a povoleným Bastion pluginem.
- *SSH port forwarding (tunelování)* – Umožňuje bezpečně přesměrovat provoz přes SSH tunel na specifický port cílového prostředku, což je užitečné například pro přístup k databázím nebo RDP.
- *Dynamické port forwarding (SOCKS5)* – Poskytuje flexibilní tunelování, kde klient rozhoduje o cílovém prostředku a portu během relace, což je vhodné pro přístup k více službám v privátní síti.

OCI Bastion je integrován s OCI Identity and Access Management (IAM), což umožňuje detailní řízení přístupu a auditování všech relací. Služba je bezplatná a dostupná ve všech komerčních regionech OCI.

3.5.6 Web Application Firewall (WAF)

OCI nabízí [50] plně spravovanou službu *Web Application Firewall (WAF)*, která slouží k ochraně webových aplikací před útoky na aplikační vrstvě sítě (Layer 7), jako jsou *SQL injection*, *Cross-Site Scripting (XSS)* a další typy zneužití zranitelností [1, s. 249] [51, s. 319-336]. WAF funguje jako bezpečnostní brána mezi klientem a webovou aplikací – veškerý příchozí provoz je nejprve analyzován a filtrován na základě definovaných bezpečnostních pravidel, a teprve poté předán aplikačnímu backendu. Klíčové vlastnosti OCI WAF:

- *Předdefinované pravidla* – OCI WAF využívá sadu více než 250 předdefinovaných pravidel [52] založených na OWASP ModSecurity Core Rule Set (CRS), které pokrývají nejběžnější webové zranitelnosti (např. SQLi, XSS, RFI, LFI aj.), včetně těch definovaných v seznamu OWASP Top 10 [1, s. 159].
- *Vlastní ochranná pravidla* – Uživatelé mohou definovat vlastní (custom) ochranná pravidla [53] pomocí jazyka ModSecurity Rule Language a přizpůsobit tak ochranu specifickým potřebám aplikace.
- *Bot management a výzvy* – Pro detekci a blokování škodlivých botů nabízí OCI WAF mechanismy jako JavaScript Challenge, CAPTCHA Challenge a Device Fingerprint Challenge, které pomáhají odlišit legitimní uživatele od automatizovaných útoků.
- *Geografické a IP filtrování* – Administrátoři mohou omezit přístup na základě geografického umístění, IP adres, URL cest a dalších atributů požadavků, což umožňuje jemné ladění přístupových politik.
- *Ochrana proti DDoS útokům* – OCI WAF poskytuje ochranu proti útokům typu *Distributed Denial-of-Service (DDoS)* na aplikační vrstvě [54], čímž zajišťuje dostupnost aplikací i při pokusech o jejich přetížení.

3.5.7 OCI (Next-Generation) Network Firewall

Kromě výše zmíněných mechanismů Oracle nabízí i pokročilejší síťové služby. Například OCI Network Firewall [55], který představuje cloudovou službu nové generace, poskytuje pokročilou ochranu síťového provozu [2, s. 218-219] v prostředí OCI. Tato služba,

postavená na technologii Palo Alto Networks, nabízí mimojiné vlastnosti jako stavovou inspekci provozu, filtrování na základě URL a FQDN (včetně podpory zástupných znaků), integraci pokročilých mechanismů detekce a prevence průniků (IDPS), inspekci šifrovaného provozu (SSL/TLS) včetně podpory pro TLS 1.2 a 1.3 a integraci s OCI Monitoring a Logging pro centralizovaný přehled. Služba je navržena tak, aby byla vysoce dostupná a škálovatelná, s možností zpracování datového toku až 25 Gb/s [56].

3.5.8 Zero Trust Packet Routing

Zero Trust Packet Routing (ZPR) je bezpečnostní služba [57] v prostředí OCI, která umožňuje organizacím definovat a vynucovat síťové přístupové politiky založené na principu tzv. "nulové důvěry", kdy se implicitně předpokládá, že žádná síťová komunikace není důvěryhodná [1, s. 254] [58]. Základem ZPR jsou tzv. *bezpečnostní atributy* (security attributes), což jsou specifické štítky, kterými jsou cloudové prostředky označeny. Pomocí jazyka ZPR Policy Language (ZPL) jsou následně definovány přístupové politiky, které určují, které zdroje a jak mohou komunikovat na základě přiřazených atributů.

ZPR tak umožňuje definovat bezpečnostní pravidla nezávisle na konkrétní síťové topologii a v praxi tak doplňuje stávající bezpečnostní seznamy (Security Lists) a skupiny (Network Security Groups), čímž poskytuje vícevrstvou ochranu.

3.6 Monitorovací nástroje a reakce na incidenty

Správné nastavení preventivních bezpečnostních opatření, jako jsou řízení přístupu (IAM), šifrování dat a síťová segmentace [1, s. 109], tvoří základ bezpečnostní architektury. Neméně důležité [1, s. 259] je však také průběžné monitorování prostředí a včasná reakce na bezpečnostní incidenty. Pro tyto účely nabízí OCI širokou škálu specializovaných nástrojů.

3.6.1 OCI Monitoring , OCI Logging

Služba *Monitoring* [59] v rámci OCI umožňuje sledování výkonových a bezpečnostních metrik [3, s. 244] různých prostředků, jako je například využití CPU, počet API volání či síťová latence. Uživatelé si mohou definovat alarmy, které se automaticky aktivují při překročení stanovených prahových hodnot. Typickým příkladem je monitorování počtu neúspěšných pokusů o přihlášení k instancím nebo neobvyklého zvýšení odchozího síťového provozu, což může signalizovat bezpečnostní incident.

Služba *Logging* [60] oproti tomu zajišťuje centralizovaný sběr [3, s. 218] logů ze široké škály OCI služeb. Uživatelé mohou vytvářet filtry a dotazy, které umožňují rychlou a automatizovanou detekci specifických událostí v systémových či aplikačních záznamech, například pro identifikaci chyb, varování nebo neautorizovaných přístupů.

3.6.2 OCI Audit

OCI *Audit* je integrovaná služba v rámci OCI, která automaticky zaznamenává veškerá volání OCI API a klíčové změny v prostředí. Každé vytvoření, úprava nebo odstranění cloudového prostředku, změna síťové konfigurace či přihlášení uživatele do konzole je evidováno jako auditní událost s přiřazeným časovým razítkem, identitou uživatele a podrobným popisem provedené akce [61].

Auditní logy jsou neměnné – nelze je upravovat ani mazat – a jsou uchovávány po dobu 365 dní [62]. Tento mechanismus významně přispívá k detekci vnitřních hrozeb (insider threats) i zneužití kompromitovaných účtů, jelikož každá interakce s prostředím zanechává auditní stopu.

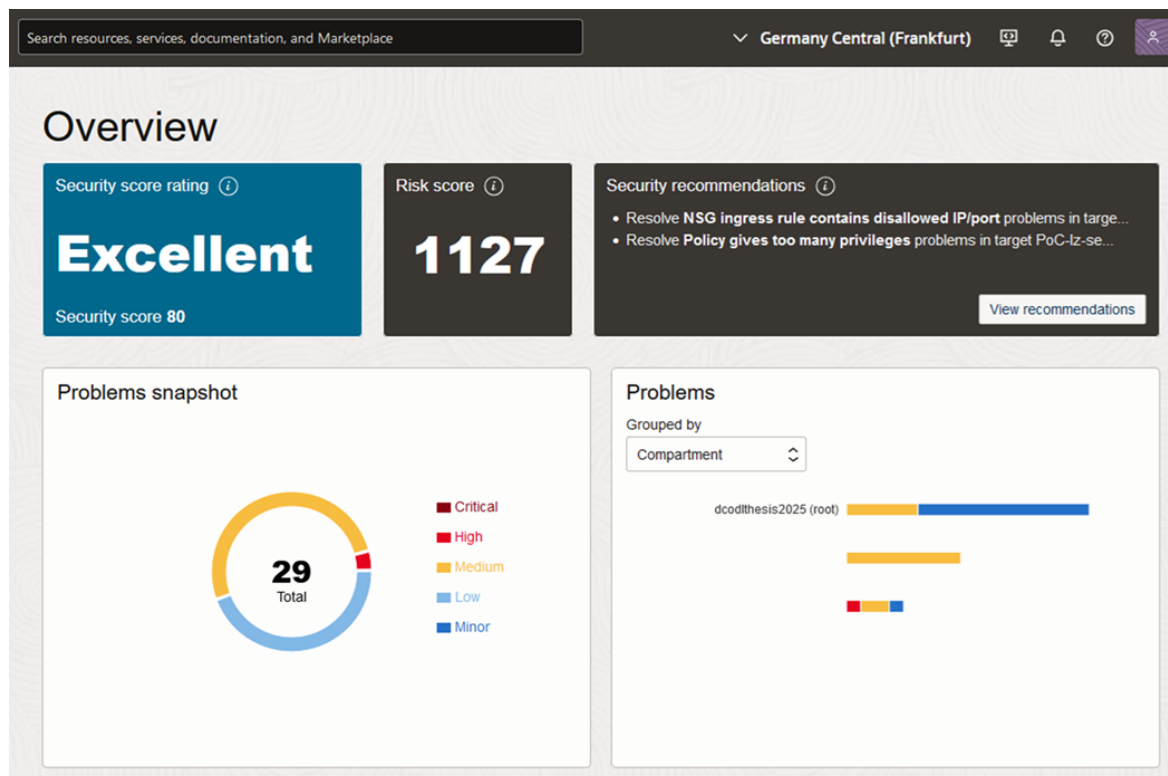
Vyhledávání a analýzu auditních záznamů lze plně automatizovat prostřednictvím OCI API nebo CLI. Například jednoduchým skriptem lze filtrovat všechny operace typu „Delete“ provedené mimo stanovenou pracovní dobu, což usnadňuje odhalování podezřelých aktivit [1, s. 499].

3.6.3 OCI Cloud Guard, Threat Intelligence

OCI nabízí [63] službu *Cloud Guard*, která slouží jako nativní nástroj pro nepřetržité monitorování bezpečnostního postavení infrastruktury v prostředí OCI. Tato služba umožňuje automaticky detekovat a reagovat na bezpečnostní incidenty napříč celou tenancy, čímž pomáhá udržovat konzistentní a bezpečné cloudové prostředí [1, s. 394].

OCI Cloud Guard je integrován [64] se službou *Oracle Threat Intelligence Service*, která poskytuje informace o aktuálních hrozbách, jako jsou známé škodlivé IP adresy nebo domény. Tyto informace jsou dále zpracovány Cloud Guard komponentou *Threat Detector*, která využívá modely chování sladěné s rámcem *MITRE ATT&CK* k identifikaci podezřelých aktivit a potenciálních útoků, což následně umožňuje efektivněji reagovat na potenciální hrozby v reálném čase.

Na obrázku (Obrázek 7) je znázorněna centrální konzole Cloud Guard.



Obrázek 7: Cloud Guard – Centrální konzole

(zdroj: vlastní)

3.7 Bezpečnostní zóny (Security Zones)

Security Zones představují nadstavbový bezpečnostní mechanismus [65] v prostředí OCI, jehož cílem je zajistit, aby vybrané cloudové prostředky byly vytvářeny a spravovány v souladu s definovanými bezpečnostními standardy. Jedná se o dodatečnou vrstvu ochrany zaměřenou na vynucení bezpečnostních politik při správě cloudových prostředků s cílem předcházet chybám v konfiguraci, které by mohly ohrozit bezpečnost infrastruktury.

Security Zone aplikuje a především vynucuje soubor předdefinovaných politik a konfigurací, jako je například povinné šifrování dat, omezení veřejného přístupu nebo používání spravovaných (customer-managed) šifrovacích klíčů. Tyto politiky se automaticky uplatňují při každém vytváření nebo úpravě zdrojů v rámci dané zóny, tj. takový OCI zdroj, který by nesplňoval podmínky dané bezpečnostní zóny vůbec není možné vytvořit (operace bude zamítnuta).

Soubor pravidel je možné přizpůsobit tak, aby odpovídal specifickým interním bezpečnostním požadavkům organizace nebo vyhověl příslušným legislativním rámcům, například GDPR, HIPAA či PCI-DSS.

4 IDENTIFIKACE HROZEB A SLABIN

Jak již bylo řečeno, bezpečnost v cloudu funguje na principu sdílené odpovědnosti mezi poskytovatelem cloudu a zákazníkem. Poskytovatel (v tomto případě Oracle) zajišťuje bezpečnost základní infrastruktury, zatímco zákazník odpovídá za zabezpečení svých aplikací, operačních systémů (v závislosti na modelu) a dat nasazených v cloudu. To znamená, že podniky musí aktivně implementovat bezpečnostní opatření v rámci svých cloudových prostředí, aby ochránily svá data před neoprávněným přístupem, narušením integrity či výpadky služeb.

Identifikace hrozeb a zranitelností v cloudovém prostředí zpravidla vychází z obecných bezpečnostních rámců (např. NIST, ISO/IEC 27001), které jsou kombinovány se specifickými metodami a nástroji vyvinutými přímo pro cloudové systémy. Tato činnost se obvykle realizuje ve dvou navazujících (a vzájemně provázaných) fázích – nejprve během návrhu cloudové infrastruktury a následně v průběhu jejího reálného provozu.

4.1 Fáze návrhu infrastruktury

V této fázi se nejprve stanoví kontext a budoucí rozsah [3, s. 102]. Je nutné určit, jaké služby a data se v cloudu nacházejí, kdo k nim má přístup a k čemu jsou využívány. Mapuje se architektura nasazení (IaaS, PaaS, SaaS) a model sdílené odpovědnosti mezi poskytovatelem cloudových služeb a zákazníkem. Provede se analýza rizik včetně identifikace aktiv (např. datové sady, aplikace, kontejnery), definují se hrozby a posuzuje se pravděpodobnost a dopad případné kompromitace.

Hrozby se často třídí podle kritičnosti (např. vysoká, střední, nízká) a na základě toho se vyhodnocují priority pro následná opatření. V rámci modelování hrozeb se využívají modely jako *STRIDE* (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*) [66, s. 61-85] nebo *DREAD* (*Damage, Reproducibility, Exploitability, Affected Users, Discoverability*) pomocí kterých se vytvářejí diagramy systémových komponent [66, s. 43-49] a definují se různé hypotetické scénáře útoku.

Na základě zjištění se definují technické (konfigurace, firewall, šifrování) i organizační (procesy, školení [1, s. 525], monitorování) opatření dle principu *secure by design* [3, s. 72].

4.2 Fáze reálného provozu

Ani sebelepší návrh bezpečnostní architektury není definitivní. Hrozby a zranitelnosti se neustále vyvíjejí [2, s. 46] – objevují se nové *CVE (Common Vulnerabilities and Exposures)* nebo nové formy útoků. Změny však často nastávají i uvnitř samotné organizace, kde správci upravují konfigurace, nasazují nové verze aplikací, mění se organizační struktura či dochází k rotaci personálu (noví pracovníci, nové přístupové role).

Z těchto důvodů je nezbytné provádět proces identifikace hrozeb a zranitelností průběžně a opakovaně – ideálně s využitím automatizovaných nástrojů [1, s. 263], jako je monitoring, alerting a detekce zranitelností (např. Vulnerability Scanning Service, Cloud Guard, analýza logů, nástroje typu SIEM apod.). Nedílnou součástí procesu by měly být i další související aktivity, jako je pravidelné (alespoň čtvrtletně) aplikování bezpečnostních záplat (tzv. *Critical Patch Updates, CPU*) k odstranění známých zranitelností [1, s. 378] [2, s. 160], provádění penetračních testů [1, s. 384] (plánovaných i ad hoc) a také reakce na bezpečnostní incidenty (*incident response*) [1, s. 677].

4.3 Přehled současných hrozeb cloudových služeb

Pro získání přehledu o aktuálních cloudových hrozbách je možné využít informace z mnoha zdrojů [66, s. 108], například dokumenty *Top Threats to Cloud Computing 2024* [67] od Cloud Security Alliance, *ENISA Threat Landscape 2024* [68] od Evropské agentury pro kybernetickou bezpečnost a *Security Guidance v5 (2024)* od Cloud Security Alliance. Ze zprávy ENISA [68] například plyne, že mezi sedm hlavních kybernetických hrozeb roku 2024 patří útoky na dostupnost (zejména odmítnutí služby / DDoS), ransomware a hrozby zaměřené na data. Dokument *Top Threats to Cloud Computing 2024* [67] zase identifikuje jako klíčové problémy mj. nesprávnou konfiguraci cloudových prostředí, slabiny v řízení identit a přístupu (IAM) a zranitelnosti rozhraní API, jak je vidět v tabulce (Tabulka 2).

Tabulka 2 CSA – Největší hrozby cloud computingu v roce 2024

Pořadí	Název hrozby	Průměrné skóre
1.	Nesprávná konfigurace a nedostatečné řízení změn (Misconfiguration & Inadequate Change Control)	8.282331
2.	Správa identit a přístupů (Identity & Access Management / IAM)	8.070780
3.	Nezabezpečená rozhraní a API (Insecure Interfaces & APIs)	7.987272

4.	Nedostatečná volba/implementace cloudové bezpečnostní strategie (Inadequate Selection/Implementation of Cloud Security Strategy)	7.620689
5.	Nezabezpečené zdroje třetích stran (Insecure Third-Party Resources)	7.582061
6.	Nezabezpečený vývoj softwaru (Insecure Software Development)	7.545801
7.	Neúmyslné zveřejnění dat v cloudu (Accidental Cloud Data Disclosure)	7.506641
8.	Systémové zranitelnosti (System Vulnerabilities)	7.462794
9.	Omezená viditelnost/pozorovatelnost v cloudu (Limited Cloud Visibility/Observability)	7.389799
10.	Neautentizované sdílení zdrojů (Unauthenticated Resource Sharing)	7.379310
11.	Pokročilé přetrvávající hrozby (Advanced Persistent Threats)	7.364326

(zdroj: [13])

Cloudové služby [2, s. 108] mohou trpět podobnými zranitelnostmi jako tradiční IT systémy [3, s. 152], ale v cloudovém prostředí se některé slabiny projevují specifickěji [2, s. 235]. Jednou z nejčastějších příčin bezpečnostních incidentů v cloudu je nesprávná konfigurace [2, s. 89] ze strany uživatele. Cloud Security Alliance uvádí nesprávnou konfiguraci a neadekvátní řízení změn jako vůbec nejzávažnější bezpečnostní problém roku 2024 v oblasti cloudu [67]. Příkladem může být veřejně přístupný objektový storage bucket obsahující citlivá data nebo bezpečnostní pravidlo povolující neomezený přístup z Internetu. Další možnou zranitelností je nedodržení *best practices* při návrhu sítě a identity – například všechny aplikace a databáze v jedné ploché síti bez segmentace [2, s. 168], nebo používání jednoho administrátorského účtu pro příliš mnoho účelů.

Z analyzovaných zpráv plyne, že mezi další známé typy slabin cloudových platforem patří například nezabezpečené APIs [67] – rozhraní, která cloud nabízí pro správu zdrojů, mohou obsahovat chyby nebo nemusí být zákazníkem správně zabezpečena (slabé autentizační metody, exponování přístupových klíčů), což otevírá dveře potenciálním útokům. Oproti tomu klesají obavy z tradičních chyb na straně poskytovatele (např. hypervizorové zranitelnosti či ztráta dat u poskytovatele) a CSA ve své zprávě Top Threats 2024 konstatuje [67], že respondenti průzkumu je řadí mezi méně pravděpodobné.

Jiným typem hrozby můžou být například útoky, které mění nebo ničí data. Typickým příkladem je ransomware v cloudovém prostředí [2, s. 162] – útočník se pokusí zašifrovat

data uložená v OCI (např. na připojených blokových svazcích) a požadovat výkupné. ENISA uvádí ransomware jako jednu z nejvýznamnějších hrozeb současnosti [68], řadí jej mezi top hrozby roku 2024. Ani cloudové prostředí není vůči ransomwaru imunní, zejména pokud má útočník přístup k virtuálním strojům nebo souborovým úložištím uvnitř tenancy.

Hrozby související s dostupností (*availability*) se nejčastěji projevují formou DoS/DDoS útoků (*Denial of Service, Distribuované Denial of Service*) [1, s. 15]. Cílem je vyřadit službu z provozu buď přetížením její infrastruktury (síťovou záplavou, vyčerpáním systémových prostředků) nebo zneužitím nějaké zranitelnosti k pádu služby. Útoky DDoS mohou směřovat na aplikace běžící v OCI (např. webové servery) nebo na samotné komponenty infrastruktury. Cloudoví poskytovatelé včetně Oracle mají robustní ochrany proti síťovým DDoS na úrovni datacenter a páteční sítě, takže útoky na infrastrukturu jsou obvykle odrazeny dříve, než dopadnou na konkrétní uživatele. Odráží to i zjištění CSA, že obavy z útoků na sdílenou infrastrukturu či DoS na úrovni poskytovatele se snížily [67]. Nicméně, aplikační DDoS (například útok zahlcující konkrétní API endpoint miliony validních požadavků) může stále způsobit výpadek služby provozované v OCI, pokud není adekvátně chráněna (např. pomocí WAF s rate limiting).

Hrozby dostupnosti zahrnují i sabotáž ze strany insidera [1, s. 19] – například administrátor zneužije přístupu a smaže kritické virtuální servery nebo zablokuje síťové spojení. Taková akce může ochromit provoz stejně účinně jako externí útok.

4.4 Klasifikace hrozeb pomocí frameworku MITRE ATT&CK

MITRE ATT&CK (zkratka znamená „Adversarial Tactics, Techniques, and Common Knowledge“) je celosvětově uznávaná databáze [69] kybernetických hrozeb a technik používaných útočníky. Byla vytvořena organizací MITRE Corporation za účelem kategorizace, dokumentace a sdílení informací o způsobech, jakými kybernetičtí útočníci pronikají do systémů, pohybují se v sítích, získávají přístup k datům a provádějí další škodlivé aktivity. MITRE ATT&CK ve své podstatě katalogizuje rozsáhlou škálu taktik, technik a procedur (TTP), které používají kybernetičtí útočníci, a nabízí strukturovaný přístup k modelování kybernetických hrozeb a tvorbě obranných strategií.

Oracle ve své službě Cloud Guard využívá modely chování sladěné s MITRE ATT&CK k detekci škodlivých aktivit [70]. Model ATT&CK IaaS Matrix [69], který se specificky zaměřuje na cloudové prostředí typu IaaS, zahrnuje následující taktiky:

4.4.1 Počáteční přístup (Initial Access):

Techniky, které útočníkům umožňují získat počáteční přístup [2, s. 138] do cloudového prostředí. Obsahuje celkem 3 techniky (např. T1078 „Valid Accounts“, popř. T1078.004 „Valid Accounts: Cloud Accounts“).

4.4.2 Spuštění (Execution)

Metody, jimiž útočníci spouštějí škodlivý kód nebo příkazy v prostředí IaaS. Obsahuje celkem 4 techniky (např. T1204 „User Execution“, popř. T1204.001 „User Execution: Malicious Link“).

4.4.3 Perzistence (Persistence)

Techniky, které útočníkům umožňují udržet si trvalý přístup [2, s. 141] v napadeném prostředí, i po potenciálních restartováních nebo změnách [2, s. 192]. Obsahuje celkem 6 technik (např. T1136 „Create Account“, popř. T1136.001 „Create Account: Local Account“).

4.4.4 Eskalace oprávnění (Privilege Escalation)

Metody, jimiž útočníci získávají vyšší úroveň oprávnění [2, s. 139], než jaké původně měli, aby mohli provádět pokročilejší operace. Obsahuje celkem 4 techniky (např. T1098 „Account Manipulation“, popř. T1098.003 „Account Manipulation: Additional Cloud Roles“).

4.4.5 Obcházení obrany (Defense Evasion)

Techniky zaměřené na vyhnutí se detekci [2, s. 143] bezpečnostními nástroji a opatřeními. Obsahuje celkem 9 technik (např. T1535 „Unused/Unsupported Cloud Regions“).

4.4.6 Přístup k přihlašovacím údajům (Credential Access)

Metody získávání přihlašovacích údajů uživatelů nebo systémů v prostředí IaaS. Obsahuje celkem 4 techniky (např. T1555 „Credentials from Password Stores“, popř. T1555.003 „Credentials from Password Stores: Credentials from Web Browsers“).

4.4.7 Průzkum (Discovery)

Techniky, které útočníkům umožňují získat informace o prostředí [2, s. 66], systémech a službách v IaaS, aby mohli plánovat další kroky. Obsahuje celkem 14 technik (např. T1580 „Cloud Infrastructure Discovery“).

4.4.8 Postranní pohyb (Lateral Movement)

Metody, jimiž se útočníci pohybují mezi systémy a službami [2, s. 140] v rámci cloudového prostředí, aby rozšířili svůj vliv. Obsahuje celkem 2 techniky (např. T1021 „Remote Services“, popř. T1021.001 „Remote Services: Remote Desktop Protocol“).

4.4.9 Sbírání dat (Collection)

Techniky zaměřené na shromažďování citlivých nebo důležitých dat z napadeného prostředí. Obsahuje celkem 4 techniky (např. T1074 „Data Staged“, popř. T1074.001 „Data Staged: Local Data Staging“).

4.4.10 Exfiltrace (Exfiltration)

Metody, jimiž útočníci přenášejí získaná data [2, s. 145] z napadeného prostředí do svého vlastního úložiště. Obsahuje celkem 2 techniky (např. T1048 „Exfiltration Over Alternative Protocol“, popř. T1048.001 „Exfiltration Over Alternative Protocol: Exfiltration Over Symmetric Encrypted Non-C2 Protocol“).

4.4.11 Dopad (Impact)

Techniky, které mají přímý negativní dopad na dostupnost, integritu nebo důvěrnost systémů a dat v prostředí IaaS. Obsahuje celkem 8 technik (např. T1485 „Data Destruction“, popř. T1485.001 „Data Destruction: Lifecycle-Triggered Deletion“).

Aktuální a kompletní výčet technik a procedur souvisejících s příslušnými uvedenými taktikami lze nalézt na stránkách popisujících matici modelu ATT&CK IaaS Matrix [69].

4.5 Tradiční modelování hrozeb vs. CSPM

Tradiční modelování hrozeb (např. metodou STRIDE) se zaměřuje na ruční nebo částečně automatizovanou analýzu potenciálních útoků, scénářů a vektorů hrozeb. Tento proces je velmi náročný, jak z hlediska času potřebného k provedení analýzy, lidských zdrojů, úrovně expertních znalostí nebo aktuálnosti informací o hrozbách. V dynamickém cloudovém

prostředí je proto pro analýzu hrozeb kvůli rychlosti, automatizaci [2, s. 121] a přehledu v reálném čase efektivnější použít tzv. systém *Cloud Security Posture Management* (CSPM).

Jedná se obecně o soubor nástrojů a postupů [71], které pomáhají organizacím automatizovaně zjišťovat, vyhodnocovat a řešit bezpečnostní hrozby a slabiny v cloudovém prostředí s cílem zabránit chybné konfiguraci cloudových služeb a minimalizovat rizika spojená s únikem dat nebo porušením legislativních předpisů. Vzhledem k tomu, že tyto systémy provádějí identifikaci a vyhodnocování neustále a opakovaně [1, s. 519], mohou také okamžitě reagovat a automaticky provést nápravu, jakmile objeví potenciálně nebezpečnou konfiguraci nebo rizikovou aktivitu. V praxi tak CSPM výrazně zjednodušuje a centralizuje správu bezpečnosti v cloudu.

OCI nabízí vestavěnou podporu systému CSPM v podobě integrovaného souboru služeb zaměřených na zabezpečení cloudu. Patří mezi ně zejména OCI Cloud Guard a jeho komponenta *Cloud Guard Threat Monitoring* pro detekci aktivních hrozeb, dále *OCI Vulnerability Scanning Service (VSS)* pro vyhledávání zranitelností a v neposlední řadě také informační zdroj *Oracle Threat Intelligence Service* poskytující agregovaná data [2, s. 126] o hrozbách.

4.6 OCI Cloud Guard

OCI Cloud Guard je nativní bezpečnostní služba cloudu OCI, která dohlíží na zdroje a aktivity v celé tenancy a dokáže průběžně prověřovat cloudové prostředky OCI z hlediska konfigurace (např. hledání slabých nastavení) a také sledovat činnost uživatelů a operátorů pro odhalení rizikových aktivit [63]. Při zjištění potenciálního problému může Cloud Guard podle nastavení buď doporučit nápravné opatření, asistovat s jeho provedením, nebo jej plně automaticky provést. K tomu využívá několik klíčových konceptů, tzv. *cíle (targets)*, *detektory (detectors)*, *recepty (recipes)*, *pravidla (rules)* a *respondéry (responders)* [72].

Cíl definuje rozsah monitorování – obvykle konkrétní kompartment (včetně jeho podkompartmentů), který Cloud Guard sleduje. Každému cíli jsou přiřazeny detektorové recepty, které určují, jaké kontroly se mají provádět. Cloud Guard disponuje čtyřmi předdefinovanými kategoriemi detektorů, z nichž každá se zaměřuje na odlišnou oblast bezpečnosti:

- *Detektor aktivity (Activity detector)* sleduje akce a operace v prostředí (API volání, změny konfigurace apod.), které by mohly představovat bezpečnostní problém (např. vytváření klíčových zdrojů neautorizovaným uživatelem) [73].
- *Detektor konfigurace (Configuration detector)* kontroluje nastavení a konfiguraci prostředků (síťové nastavení, úložiště, identity) a hledá odchylky od osvědčených postupů či bezpečnostních zásad, které by mohly vést k ohrožení [73].
- *Detektor zabezpečení instancí (Instance Security detector)* poskytuje dodatečnou ochranu běžících výpočetních instancí (virtuálních strojů a bare metal serverů) kontrolou jejich stavu a konfigurace za běhu – např. ověřuje konfigurace operačního systému a bezpečnostní nastavení hostitele [73].
- *Detektor hrozeb (Threat detector)* vyhledává jemné vzorce chování a aktivity v prostředí, které mohou naznačovat probíhající útok nebo hrozbu, i když jednotlivě nemusí být zjevné [73] [74].

Každý detektor v OCI Cloud Guard využívá sadu detekčních pravidel sdružených v tzv. *detektorovém receptu (detector recipe)*. Oracle poskytuje předdefinované (*Oracle-managed*) recepty pro každý typ detektoru s výchozí konfigurací pravidel. Tyto recepty lze podle potřeby klonovat a upravovat, čímž vznikne *uživatelsky definovaný (user-managed)* recept. Detekční pravidlo obvykle popisuje konkrétní podmínku nebo vzorec, například „object storage bucket je veřejně dostupný“ nebo „vytvoření instance s veřejnou IP adresou“.

Pokud je detekováno porušení definovaného pravidla, systém automaticky zaznamená incident nebo nesoulad s nastavenou bezpečnostní politikou. Každý takový incident obsahuje podrobné informace o typu identifikovaného rizika, jeho závažnosti a původu [74].

Na obrázku (Obrázek 8) je zobrazen seznam pravidel pro vestavěný recept detektoru konfigurace „OCI Configuration Detector Recipe (Oracle managed)“.

☐	Detector rule	Risk level	Status	Settings configured	Conditional group	
☐	Write Log access disabled for bucket	Low	Disabled	Not allowed	No	⋮
☐	VNIC without associated network security group	Minor	Enabled	Not allowed	No	⋮
☐	VCN has no inbound Security List	Medium	Disabled	Not allowed	No	⋮
☐	VCN has Local Peering Gateway attached	Low	Enabled	Not allowed	No	⋮
☐	VCN has InternetGateway attached	Low	Enabled	Not allowed	No	⋮
☐	VCN Security list allows traffic to restricted port	Critical	Enabled	Yes	No	⋮
☐	VCN Security list allows traffic to non-public port from all sources (0.0.0.0/0)	Critical	Enabled	No	No	⋮
☐	User has API keys	Low	Enabled	Not allowed	No	⋮
☐	User does not have MFA enabled	Critical	Enabled	Not allowed	No	⋮
☐	Tenancy admin privilege granted to group	Medium	Enabled	No	No	⋮
☐	Scanned host has vulnerabilities	Critical	Enabled	Yes	No	⋮
☐	Scanned host has open ports	Critical	Enabled	Yes	No	⋮
☐	Scanned container image has vulnerabilities	Critical	Enabled	Yes	No	⋮
☐	Resource is not tagged appropriately	Low	Enabled	No	No	⋮

Obrázek 8: Cloud Guard – OCI Configuration Detector Recipe (Oracle managed)

(zdroj: vlastní)

Pro reakci na zjištěné problémy nabízí Cloud Guard tzv. *respondéry* (*responders*) – tedy definované akce sloužící k nápravě. Respondér může například automaticky uzavřít veřejný port, resetovat heslo, odeslat upozornění administrátorovi nebo provést jinou nápravnou operaci. I respondéry mají své recepty a pravidla, která určují, jaká akce má být spuštěna při výskytu konkrétního typu problému. Tím je možné Cloud Guard nakonfigurovat nejen pro pasivní detekci, ale i pro aktivní obranu – a to buď plně automaticky, nebo s manuálním schválením ze strany bezpečnostního týmu [75] [76].

Cloud Guard zároveň poskytuje centrální konzoli, ve které lze sledovat všechny zjištěné problémy napříč tenancy, jejich aktuální stav (např. otevřený, vyřešený, ignorovaný) a tzv. *skóre zabezpečení* (*security score*). Toto skóre kvantifikuje celkovou úroveň zabezpečení prostředí na základě počtu a závažnosti zjištěných problémů. Cloud Guard je úzce integrován s dalšími službami OCI – například s notifikační službou (Notifications), Event Service pro správu událostí, službou Logging, Identity and Access Management (IAM) pro prosazování zásad, a dalšími bezpečnostními nástroji. Tato integrace umožňuje Cloud Guardu efektivně identifikovat rizika a udržovat prostředí v souladu s nastavenými bezpečnostními pravidly.

Cloud Guard je poskytován bezplatně pro vybrané služby [77], ovšem je dostupný pouze v upgradovaném (placeném) typu OCI účtu.

4.7 Cloud Guard Threat Monitoring

Funkce Threat Monitoring v rámci Oracle Cloud Guard je zaměřena na detekci a sledování kybernetických hrozeb v prostředí OCI v reálném čase. Cloud Guard v tomto kontextu funguje obdobně jako systém pro detekci útoků – průběžně analyzuje události a záznamy o aktivitě (zejména auditní logy OCI) a vyhledává vzorce chování nasvědčující možným škodlivým aktivitám [74]. Tato funkcionalita je realizována prostřednictvím detektorového receptu Threat detector, který využívá kombinaci pravidel, modelů strojového vyhodnocování [1, s. 561] a dat z oblasti threat intelligence k identifikaci potenciálních útoků dříve, než k nim skutečně dojde.

Proces detekce probíhá ve více fázích. V první fázi Threat detector shromáždí [74] relevantní data ze zvolených cílů, především z auditních protokolů (*audit logs*). Zároveň čerpá informace z Oracle Threat Intelligence Service, zejména o známých indikátorech kompromitace (*Indicators of Compromise, IOC*), jako jsou podezřelé IP adresy nebo domény spojené se známými útoky či malwarem. Tyto vstupy jsou dále vyhodnocovány pomocí detekčních pravidel a modelů, které jsou sladěny s rámcem MITRE ATT&CK. Každé pozorované chování je zařazeno do kontextu známých taktik a technik útočníků. Pokud některý model rozpozná podezřelý vzorec (např. opakované neúspěšné přihlášení, eskalaci oprávnění, využití API z neobvyklé geolokace nebo přístup přes síť Tor), Cloud Guard vygeneruje tzv. *sighting* – jednorázový detekovaný výskyt podezřelé aktivity.

Každý sighting je následně ohodnocen na základě dvou faktorů: závažnosti (potenciální dopad v případě, že jde o skutečný útok) a důvěryhodnosti (míra jistoty, že skutečně jde o škodlivou aktivitu). Cloud Guard zároveň koreluje jednotlivé sightings v čase i napříč regiony. Pokud jsou zaznamenány opakované podezřelé aktivity vztahující se ke stejnému prostředku (např. instance nebo uživatel), systém je sloučí do tzv. *resource profile* – souhrnného profilu daného prostředku, tvořeného posloupností detekcí. Pro tento profil Cloud Guard vypočítá [73] rizikové skóre, které zohledňuje jak závažnost možného útoku, tak jeho pravděpodobnost. Pokud skóre přesáhne stanovený práh (např. Critical), je automaticky vytvořen incident typu problem a předán k řešení bezpečnostnímu týmu.

Threat Detector využívá sadu přednastavených detekčních pravidel (tzv. *Oracle-managed Threat Detector Recipe*), které pokrývají široké spektrum typových hrozeb. Tato pravidla vycházejí z ověřených scénářů útoků a jsou průběžně aktualizována společností Oracle. Uživatelé mají možnost tato pravidla upravovat – např. definovat vlastní prahové

hodnoty, nebo vyloučit známé legitimní aktivity, aby se minimalizoval počet falešných poplachů. K tomuto účelu slouží například funkce *Managed List*, tedy uživatelsky spravované seznamy (např. důvěryhodné IP adresy, povolené porty apod.), které lze v pravidlech využít ke zpřesnění detekce.

Na obrázku (Obrázek 9) je ukázka detekce výskytu (sighting) podezřelé uživatelské aktivity včetně klasifikace skóre a severity pomocí služby Threat Monitoring.

The screenshot displays the Oracle Threat Monitoring interface. At the top, there is a search bar and a navigation menu with 'Germany Central (Frankfurt)' selected. The main content area is titled 'Persistence' and shows 'General information' and 'Additional details' tabs. The 'General information' tab is active, displaying the following data:

- OCID:** ...mqza6ch7ha [Show](#) [Copy](#)
- Tactic:** Persistence (TA0003)
- Technique:** Account Manipulation: Additional Cloud Credentials (T1098.001)
- Resource:** [alice.newman.poc.auditor@gmail.com](#)
- Resource type:** User
- First detected:** Fri, Apr 11, 2025, 03:11:17 UTC
- Last detected:** Fri, Apr 11, 2025, 03:11:17 UTC
- First occurred:** Thu, Apr 10, 2025, 09:41:00 UTC
- Last occurred:** Thu, Apr 10, 2025, 09:41:00 UTC
- Regions:** Germany Central (Frankfurt)
- Sighting score:** 4
- Severity:** Minor
- Confidence:** Minor

Below the general information, there is a section titled 'Endpoints' which contains a table with the following data:

IPV4 addresses	Type	Country	Latitude	Longitude	ASN	Regions	Service	First detected	Last detected	First occurred	Last occurred
141.143.193.50	-	nl	52.35	4.9	206209	Germany Central (Frankfurt)	UploadApikey	Fri, Apr 11, 2025, 03:11:17 UTC	Fri, Apr 11, 2025, 03:11:17 UTC	Thu, Apr 10, 2025, 09:41:00 UTC	Thu, Apr 10, 2025, 09:41:00 UTC

Obrázek 9: Threat Monitoring – Detekce výskytu a klasifikace skóre

(zdroj: vlastní)

4.8 Oracle Threat Intelligence Service

Oracle Threat Intelligence Service (OCI Threat Intel) je cloudová služba, která zajišťuje agregaci a správu dat o kybernetických hrozbách z různých zdrojů a jejich přeměnu na prakticky využitelnou inteligenci v rámci OCI [64]. Služba shromažďuje data ze širokého spektra zdrojů – využívá poznatky Oracle Security výzkumníků a interní telemetrie z Oracle cloudových služeb, veřejně dostupné otevřené zdroje (například databáze malwarových domén abuse.ch či seznamy výstupních uzlů sítě Tor) i informace od partnerských bezpečnostních společností [64]. Výsledkem je jednotná databáze hrozeb, kde má každý indikátor (např. IP adresa, doménové jméno, URL nebo hash souboru) přiřazen jednoznačný

indikátor důvěryhodnosti (*confidence score*) na základě kvality a shody napříč zdroji. Tím je výrazně omezen počet falešných poplachů – pokud například určitá IP adresa figuruje jen v jednom méně spolehlivém zdroji, dostane nízkou důvěryhodnost, zatímco adresy vyskytující se opakovaně napříč zdroji mají skóre vysoké.

V konzoli OCI je dostupná Threat Indicator Database, ve které lze vyhledávat konkrétní indikátory kompromitace (Indicators of Compromise, IOC) a získávat o nich podrobné informace. Ukázku vyhledávání lze vidět na obrázku (Obrázek 10).

Indicator	Type	Threat type	Overall confidence	First reported	Last reported
172.68.10.116	IP address	SqliInjectionattack	50	Mon, Aug 12, 2024, 06:08:23 UTC	Sat, Mar 8, 2025, 20:23:00 UTC
172.68.10.12	IP address	SqliInjectionattack	50	Wed, Jul 17, 2024, 22:07:46 UTC	Sat, Mar 8, 2025, 20:30:11 UTC
172.68.10.122	IP address	SqliInjectionattack	50	Wed, Jul 17, 2024, 22:07:46 UTC	Sat, Mar 8, 2025, 20:38:11 UTC
172.68.10.13	IP address	SqliInjectionattack	50	Wed, Jul 17, 2024, 22:07:46 UTC	Sat, Mar 8, 2025, 20:37:27 UTC
172.68.10.182	IP address	SqliInjectionattack	50	Wed, Aug 14, 2024, 16:08:20 UTC	Sat, Mar 8, 2025, 20:32:24 UTC
172.68.10.183	IP address	SqliInjectionattack	50	Wed, Aug 14, 2024, 15:08:20 UTC	Sat, Mar 8, 2025, 20:37:23 UTC
172.68.10.188	IP address	SqliInjectionattack	50	Sun, Dec 8, 2024, 13:12:55 UTC	Sat, Mar 8, 2025, 20:41:42 UTC
172.68.10.194	IP address	SqliInjectionattack	50	Wed, Jul 17, 2024, 22:07:46 UTC	Sat, Mar 8, 2025, 20:41:01 UTC
172.68.10.195	IP address	SqliInjectionattack	50	Fri, Aug 16, 2024, 21:08:52 UTC	Sat, Mar 8, 2025, 20:36:03 UTC
172.68.10.20	IP address	SqliInjectionattack	50	Thu, Feb 13, 2025, 19:07:11 UTC	Sat, Mar 8, 2025, 20:24:23 UTC

Obrázek 10: Threat Intelligence – Vyhledávání v databázi Threat Indicator

(zdroj: vlastní)

Oracle Threat Intelligence Service funguje jako podpůrná služba pro další bezpečnostní nástroje – je nativně integrována zejména se službou Cloud Guard a jejím detektorem hrozeb. Díky tomu Cloud Guard automaticky využívá threat intelligence data při analýze incidentů a rozhodování o rizicích. Současně služba poskytuje rozhraní pro bezpečnostní analytiky, kteří mohou s daty aktivně pracovat.

Služba je poskytována bezplatně [78], ovšem je dostupná pouze v upgradovaném (placeném) typu OCI účtu.

4.9 OCI Vulnerability Scanning Service

OCI Vulnerability Scanning Service (VSS) je služba [79] pro automatizované skenování zranitelností [2, s. 60] v prostředí OCI, zaměřená na virtualizované i fyzické servery a kontejnery. Jejím cílem je pomoci identifikovat a odstranit známé slabiny v cloudové infrastruktuře dříve, než je útočníci zneužijí [2, s. 90]. VSS se zaměřuje na dvě hlavní oblasti – výpočetní instance (hostitele) a kontejnerové obrazy (image) uložené v OCI Container Registry. Pro každou z nich provádí specifické kontroly:

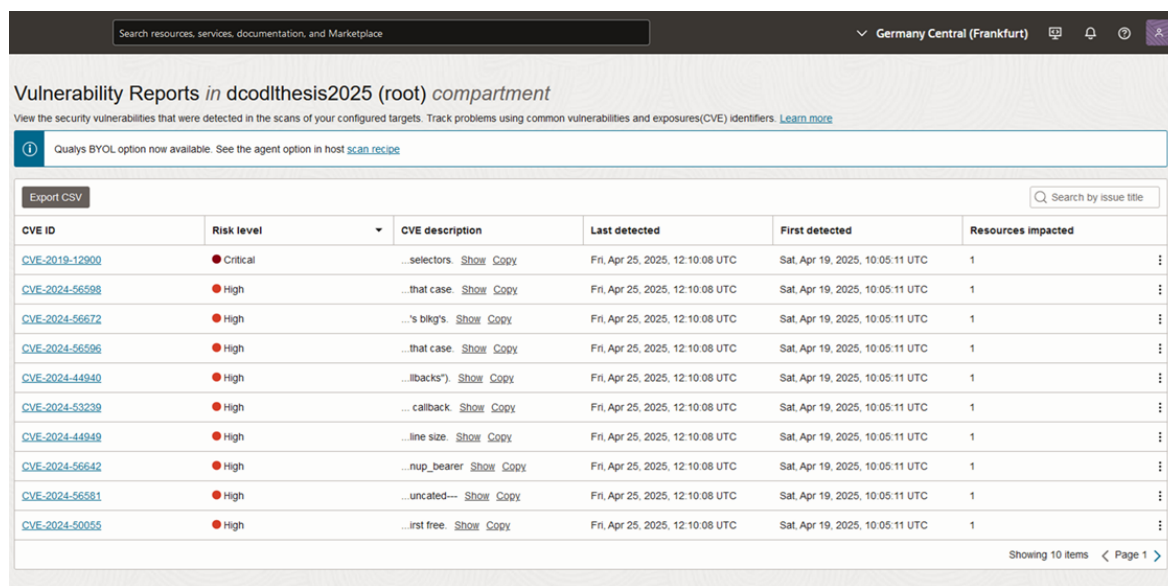
- *Skenování hostitelů (Compute instances)* – VSS analyzuje na každé aktivní instanci otevřené síťové porty [2, s. 58] a ověřuje jejich bezpečnost. Kontroluje také nainstalované OS balíčky a software vzhledem ke známým zranitelnostem podle databáze CVE (NVD) a hodnotí konfiguraci operačního systému dle bezpečnostních standardů, zejména benchmarků CIS pro Linux. Detekuje také známé zranitelné knihovny či komponenty (například *Log4Shell* nebo *Spring4Shell*). Součástí je i síťový scan veřejných IP adres, který ověřuje skutečnou dostupnost portů přes síťová pravidla [79].
- *Skenování kontejnerových obrazů (image)* – VSS je integrována s *OCI Container Registry* (OCIR) a pravidelně skenuje uložené obrazy (image) kontejnerů, zda neobsahují zranitelné balíčky či závislosti. Funguje to obdobně jako u hostitelů, služba porovnává nalezené info s databázemi známých zranitelností (CVE) a při nalezení shody reportuje, které komponenty je nutné aktualizovat. Skenování kontejnerů probíhá automaticky při vložení nového image do registru a dále v pravidelných intervalech [79].

Administrátor v OCI nastavuje VSS pomocí *receptů (scan recipes)*, přičemž Oracle poskytuje výchozí recepty a uživatelé si je mohou upravit obdobně jako u Cloud Guard. *Cíl (target)* pak určuje konkrétní prostředky, které se mají skenovat – lze zacílit celý kompartment (všechny instance v něm) a jeho podkompartmenty, nebo vybrat jen určité instance či repository v OCIR. Pro každou instanci je k dispozici *Host Scan report* uvádějící seznam nalezených zranitelností, jejich závažnost (např. podle CVSS skóre) a případně míru souladu s CIS benchmarky.

Dále služba generuje agregované *Vulnerability Reports* pro jednotlivé CVE zranitelnosti napříč prostředím – například souhrnný report ukáže všechny instance, které mají zranitelnou knihovnu OpenSSL, apod [80]. U každého nálezu VSS poskytuje detail

(CVE identifikátor, popis chyby, odkaz do NVD databáze) a často i návod k nápravě (např. verze balíčku, na kterou aktualizovat). Prioritizace nálezů vychází ze skóre CVSS – VSS převádí základní CVSS skóre zjištěných chyb do kategorií (Critical/High/Medium/Low/None) a ty odpovídají úrovním rizika používaným v Cloud Guard [79].

Na obrázku (Obrázek 11) je seznam CVE zranitelností nalezených pomocí služby Oracle Vulnerability Scanning Service.



The screenshot shows the 'Vulnerability Reports' page for the 'dcodlthesis2025 (root) compartment'. It displays a table of 10 CVEs, all with a 'High' risk level. The table includes columns for CVE ID, Risk level, CVE description, Last detected, First detected, and Resources impacted. Each row has links to 'Show' and 'Copy' the CVE details.

CVE ID	Risk level	CVE description	Last detected	First detected	Resources impacted
CVE-2019-12900	Critical	...selectors. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-56598	High	...that case. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-56672	High	...s blkg's. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-56596	High	...that case. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-44940	High	...llbacks"). Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-53239	High	... callback. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-44949	High	...line size. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-56542	High	...nup_bearer. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-56581	High	...uncated---. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1
CVE-2024-50055	High	...irst free. Show Copy	Fri, Apr 25, 2025, 12:10:08 UTC	Sat, Apr 19, 2025, 10:05:11 UTC	1

Obrázek 11: OCI Vulnerability Scanning Service – Nalezené CVE zranitelnosti

(zdroj: vlastní)

Vulnerability Scanning Service úzce spolupracuje s OCI Cloud Guard pro jednotné zobrazení bezpečnostních nálezů. Zjištěné zranitelnosti a otevřené porty jsou automaticky promítány i do Cloud Guard konzole jako problémy typu konfigurace.

Služba je poskytována bezplatně, ovšem je dostupná pouze v upgradovaném (placeném) typu OCI účtu.

5 NÁVRH BEZPEČNOSTNÍCH OPATŘENÍ DLE ZÁSAD OCI

V této kapitole navrhujeme bezpečnostní opatření pro nově vytvořenou tenancy v OCI, a to v souladu s bezpečnostními doporučeními definovanými v dokumentu CIS OCI Foundations Benchmark od organizace Center for Internet Security (CIS) a osvědčenými postupy společnosti Oracle. Navržená opatření jsou strukturována do jednotlivých oblastí, které pokrývají klíčové aspekty bezpečnosti cloudové infrastruktury – od řízení identit a přístupových oprávnění přes zabezpečení workloadů až po průběžný monitoring a audit bezpečnostních událostí.

Původní cíl této práce, tedy vytvoření a ověření vhodných bezpečnostních scénářů prostřednictvím Proof-of-Concept (PoC), jsme se rozhodli integrovat přímo do návrhu této kapitoly a následné implementace v kapitole 6. Důvodem této integrace je fakt, že – jak již bylo popsáno v kapitole 3 – platforma OCI byla od počátku navržena s bezpečností jako základním stavebním kamenem celého prostředí (security by design). Bezpečnostní funkce OCI se vzájemně doplňují a propojují, čímž vytvářejí komplexní vícevrstvou ochranu zdrojů. Proto je vhodnější demonstrovat využití bezpečnostních nástrojů a jejich vzájemnou integraci v rámci jednotného, uceleného scénáře. Tento návrh je následně prakticky implementován v kapitole 6, která detailně popisuje realizaci příslušných bezpečnostních opatření a jejich konkrétní konfiguraci v prostředí OCI.

5.1 Center for Internet Security (CIS) OCI Foundations Benchmark

Center for Internet Security (CIS) je nezisková organizace, která se zaměřuje na zlepšování kybernetické bezpečnosti prostřednictvím vývoje osvědčených postupů a standardů pro bezpečnou konfiguraci IT systémů. Tyto nástroje a doporučení umožňují organizacím efektivně zabezpečit jejich prostředí v OCI a chránit citlivá data před potenciálními hrozbami již během návrhu infrastruktury.

Ve spolupráci s Oracle vytvořila organizace CIS dokument *CIS OCI Foundations Benchmark* [81], který poskytuje konkrétní pokyny pro bezpečnou konfiguraci služeb a komponent v OCI. Patří mezi ně například pravidla typu „Zajistit, aby byli vytvořeni správci služeb (service-level admins) pro řízení zdrojů jednotlivých služeb.“, nebo „Zajistit, aby žádná síťová bezpečnostní skupina (NSG) neumožňovala příchodí přístup (ingress) z libovolné zdrojové IP adresy typu 0.0.0.0/0 na port 22.“, případně „Zajistit, aby byl Cloud Guard aktivován v kořenovém kompartmentu (root compartment) tenancy.“

Dokument také definuje konfigurační profily odpovídající důležitosti konkrétních bezpečnostních kontrol. Verze 1.1 obsahuje dvě úrovně doporučení:

- *Úroveň 1 (Level 1)*: Doporučení, která jsou praktická a rozumná pro většinu prostředí, představující bezpečnostní *best practices*.
- *Úroveň 2 (Level 2)*: Přísnější opatření, která rozšiřují úroveň 1. Jsou určena pro prostředí, kde je zabezpečení důležitější než snadná správa a použitelnost, a slouží jako opatření vícevrstvé ochrany („defense-in-depth“) [1, s. 105].

V návaznosti na dokument CIS OCI Foundations Benchmark připravil Oracle sadu referenčních terraformových šablon *OCI Landing Zone(s)* [82], které pomůžou s vytvořením základních zdrojů v OCI tak, aby splňovaly parametry CIS OCI Benchmark (jako např. oddělení odpovědností či škálovatelnost).

Zároveň byly vydány *CIS Hardened Images* [83] pro Oracle Linux. Tyto předem nakonfigurované obrazy operačních systémů jsou v souladu s CIS Benchmarks a poskytují bezpečný základ pro nasazení aplikací v OCI, čímž snižují riziko zranitelností a zvyšují celkovou bezpečnost infrastruktury.

5.2 Plán zabezpečení infrastruktury

Při plánování [84] zabezpečení nové tenancy postupujeme hierarchicky. Nejprve se zaměříme na návrh a zabezpečení základních komponent (např. strukturu kompartmentů nebo počet uživatelů s administrativním oprávněním, apod.), následně řešíme zabezpečení konkrétních zdrojů infrastruktury či workloadů.

5.2.1 Výběr domovského regionu

Domovský region (*Home region*) v OCI je hlavní region [85], který je zvolen během vytváření účtu (tenancy). Jsou zde uloženy všechny zdroje týkající se správy identity a přístupů (IAM), nastavení účtu, správy uživatelů, skupin, politik a kompartmentů. Rovněž zde jsou soustředěny klíčové audity a protokoly (logs) týkající se aktivity uživatelů a správy přístupů a údaje pro fakturaci, náklady a přehled o spotřebě cloudových zdrojů napříč všemi regiony v tenancy.

Tento region nelze po vytvoření tenancy změnit, proto je jeho prvotní volba velmi důležitá. Přestože je možné dodatečně aktivovat (metodou *subscribe*) další regiony (např.

pro potřeby obnovy po havárii, disaster recovery [1, s. 244]), veškeré definice IAM zdrojů zůstávají uloženy pouze v domovském regionu a do dalších regionů jsou replikovány.

Doporučuje se domovský region zvolit co nejbližší hlavnímu centru administrace nebo managementu organizace, pro minimalizaci latencí a lepší správu.

5.2.2 (Volitelně) Zvážení oddělených domén identity

Doména identity (Identity domain) je ve své podstatě kontejner, který umožňuje vytvářet, spravovat a organizovat uživatelské účty a skupiny v cloudu odděleně (včetně federace účtů, zabezpečení integrace aplikací využívajících jednotného přihlášení typu Single Sign-On a správu poskytovatelů identit na bázi SAML nebo OAuth).

Každá tenancy [86] obsahuje výchozí doménu identity (Default identity domain) vytvořenou v hlavním kompartmentu (root compartment). Tato doména zahrnuje výchozího administrátora a skupinu, a také výchozí politiku, která administrátorům umožňuje spravovat libovolný zdroj v rámci celé tenancy. Výchozí doména identity existuje po celou dobu existence dané tenancy a nelze ji smazat. V rámci jedné tenancy je možné vytvářet další domény podle potřeb organizace.

Oracle obecně doporučuje [87] používat výchozí doménu identity pouze pro účty administrátorů OCI a následně používat odlišné domény pro každé aplikační prostředí (např. produkční, vývojové, testovací), aby se předešlo bezpečnostním rizikům.

5.2.3 Stanovení počtu globálních administrátorů

V prostředí OCI se můžeme setkat s následujícími typy globálních administrátorů:

- *Cloud Account Administrator*: Nejvyšší role z hlediska Identity Domains. Má možnost spravovat (tvořit, mazat) všechny domény identity a přiřazovat další doménové administrátory.
- *Identity Domain Administrator*: Role omezená na jednu konkrétní doménu identity (např. Default Domain, nebo doménu Partners, apod.). V rámci této jedné domény může spravovat uživatele, skupiny, hesla, aplikace, MFA politiky, atd. Nemůže vytvářet či mazat jiné domény ani upravovat identity v jiných doménách. Nemá (automaticky) oprávnění spravovat infrastrukturní zdroje v tenancy (Compute, síť, databáze, atp.) – to je věc IAM politik.

- *Tenancy Admin*: Mohou spravovat všechny infrastrukturní zdroje v celé tenancy (Compute, Networking, Storage, Databases, atd.). Jedná se typicky uživatelé/skupiny, kteří mají v IAM politice oprávnění „*Allow group <...> to manage all-resources in tenancy*“.

Doporučeným osvědčeným postupem nejen v OCI je definovat [2, s. 166] pouze nezbytně nutný počet administrátorů – tedy co nejméně. Platí pravidlo „least privilege“ (nejméně potřebných oprávnění). Pro správu různých oblastí (např. síť, databáze, bezpečnost), je vhodné vytvořit specializované administrátorské skupiny s omezenými právy, nikoli univerzální administrátory. Současně je ovšem nutné myslet na mimořádné situace (např. kdy hlavní administrátor opustí společnost, nebo není k dispozici) a mít pro případy nouze vytvořen [87] záložní (tzv. "Break glass") administrátorský účet.

5.2.4 Definice typů plánovaných workloadů

Při plánování infrastruktury OCI je klíčové předem zvážit, jaké typy workloadů (pracovních zátěží či aplikací) budeme provozovat. Důvodem jsou zejména následující faktory:

- *Neměnnost síťových parametrů po vytvoření* – Po vytvoření VCN v OCI a definici rozsahů IP adres (CIDR bloků) nelze tyto hodnoty již později změnit. Návrh síťové topologie by proto měl správně reflektovat předpokládaný růst a potřeby infrastruktury. V případě neodhadnutí správné velikosti či struktury podsítí nebo IP rozsahů, organizace může později čelit složité migraci nebo nutnosti znovu vytvořit celé prostředí.
- *Optimalizace síťové topologie* – Různé typy workloadů (např. webové aplikace, databáze, analytické clustery, HPC, Kubernetes) mají odlišné síťové nároky – latence, propustnost, izolaci a bezpečnost.
- *Bezpečnost a soulad s předpisy* – Typ workloadu zásadně ovlivňuje bezpečnostní požadavky (například citlivá data vyžadují izolaci a speciální bezpečnostní opatření jako NSG, firewall, WAF). Při správném plánování je možné definovat odpovídající bezpečnostní mechanismy a rozdělit síťové segmenty podle rizikových profilů aplikací.

Existuje celá řada typů workloadů, z nichž každý má odlišné požadavky na síťovou topologii (velikost VCN, členění na podsítě), typ instancí a jejich úložiště, bezpečnostní

opatření (firewall, NSG, WAF) nebo integraci se specializovanými OCI službami (OKE, Data Flow, Functions). Mezi nejběžnější typy patří:

- *HPC (High-Performance Computing)* – Náročné výpočty a analýzy (např. vědecké simulace, strojové učení). Vyžadují vysoký výkon CPU/GPU, nízkou latenci a velkou šířku pásma.
- *Kontejnery a Kubernetes (OKE)* – Moderní kontejnerizované aplikace provozované v Kubernetes.
- *Big Data a Analytické workloady* – Datové sklady, datová jezera (Data Lakes), streaming, analýza dat. Potřebují velké úložiště, vysoký datový tok a integraci s analytickými službami (např. OCI Data Flow, Autonomous Database, Data Integration) [3, s. 136].
- *Disaster Recovery (DR) a zálohování* – Záložní lokalita nebo řešení obnovy po havárii. Požaduje efektivní replikaci dat, geografickou separaci a vysokou dostupnost.
- *Serverless aplikace (Functions, API Gateway)* – Aplikace založené na serverless technologiích (bez nutnosti správy serverů).
- *DevOps prostředí* – CI/CD pipeline, automatizace nasazování aplikací [3, s. 291].
- *ERP a enterprise aplikace* – Velké firemní aplikace (Oracle E-Business Suite, JD Edwards).
- *Hybridní a multicloudové workloady* – Integrace s on-premise prostředím nebo s jinými cloudy. Vyžadují speciální konfigurace sítí (např. VPN, FastConnect), zabezpečenou komunikaci a koordinaci.

Proto je důležité již při plánování infrastruktury OCI jasně definovat, jaké typy workloadů budou provozovány, a podle toho přizpůsobit návrh.

5.2.5 Návrh struktury kompartmentů

Kompartmenty (compartments) v OCI slouží k organizaci a izolaci cloudových zdrojů, což usnadňuje správu a kontrolu přístupu. Zde je možné použít několik [88] přístupů:

- *Umístění všech zdrojů do hlavního kompartmentu (root compartment)*: Lze použít jen u malých organizací nebo v dočasné testovací fázi, jinak ne příliš vhodné. Oracle v tomto případě doporučuje navíc vytvoření *sandbox* kompartmentu, aby uživatelé

měli samostatný prostor pro testování nových funkcí, zatímco zdroje v hlavním (root) kompartmentu zůstanou chráněny přísnějšími pravidly.

- *Vytvořit strukturu kompartmentů podle projektů nebo oddělení:* Tímto způsobem lze umožnit jednotlivým týmům ve firmě vytvořit si a pracovat s vlastními zdroji, které si mohou samostatně a nezávisle spravovat, aniž by získali administrátorská práva k hlavnímu (root) kompartmentu nebo jiným projektům.
- *Vytvořit strukturu kompartmentů podle bezpečnostních požadavků:* Při tomto přístupu jsou vytvořeny kompartmenty a bezpečnostní zóny pro projekty, které musí splňovat specifickou úroveň zabezpečení definovanou sadou pravidel bezpečnostní zóny („security zone recipe“).

5.2.6 Určení specializovaných administrativních rolí a oprávnění

OCI nabízí [36] nejběžnější již předdefinované bezpečnostní politiky (Common Policies), které usnadňují správu oprávnění a řízení přístupu k různým zdrojům OCI. Jsou navrženy tak, aby pokryly typické scénáře použití a pomohly administrátorům rychle a efektivně nastavit přístupová práva. Například politika „*Let the Help Desk manage users*“ pro správu uživatelů, nebo politika „*Let network admins manage a cloud network*“ pro jednotnou správu síťového nastavení, apod.

K tomuto účelu lze použít referenční architekturu CIS OCI Landing Zone [82], která poskytuje předpřipravené prostředí, jenž automaticky nastavuje kompartmenty, politiky (Common Policies), skupiny a pravidla v souladu s doporučeními CIS OCI Benchmark, a to automaticky, čímž celý proces zrychluje a výrazně snižuje riziko lidských chyb.

5.3 Vizualizace architektury pomocí OCI diagramu

Navrženou architekturu je vhodné pro lepší přehled vizualizovat formou OCI diagramu. K tomuto účelu Oracle nabízí sady [89] nástrojů pro vytváření diagramů architektury OCI ve formátech PowerPoint, draw.io a Visio. Tyto formáty obsahují ikony služeb OCI a v některých případech také připravené šablony, které lze použít.

5.4 Vytvoření tenancy

Poté, co finalizujeme plán, přistoupíme k vytvoření tenancy dle specifikovaných parametrů.

5.4.1 Zabezpečení účtu globálního administrátora pomocí MFA

Domény identity (včetně Default) používané v IAM obsahují [86] již předdefinovanou politiku pro přihlašování do OCI Console, která obsahuje pravidlo vynucující použití vícefaktorového ověřování (MFA), a to nejen pro všechny typy administrátorských účtů, ale obecně pro všechny uživatele. Doporučuje se toto ověřit a ponechat aktivované.

5.5 Vytvoření prvků řízení identity a přístupových oprávnění (IAM)

Vytvoříme mechanismy [90] pro autentizaci uživatelů a autorizaci jejich přístupu ke zdrojům v tenancy způsobem, který odpovídá principu nejnižších možných oprávnění (least-privilege). Dále vytvoříme specializované administrátorské skupiny pomocí nichž budeme provádět administraci příslušných specializovaných OCI zdrojů a workloadů (např. zabezpečení sítí, apod.). Lze využít referenční architekturu OCI Landing Zone [82].

5.6 Aktivace Cloud Security Posture Management (CSPM)

V okamžiku, kdy máme vytvořenou tenancy a nastavený IAM, je vhodné aktivovat systém pro identifikaci hrozeb a slabin v rámci fáze reálného provozu infrastruktury, tj. Cloud Security Posture Management (CSPM), a jeho komponenty.

5.6.1 (Volitelně) Vytvoření hlavního šifrovacího klíče v Oracle Vault

Oracle umožňuje pro šifrování dat v klidu (data-at-rest) použít jak šifrovací klíče spravované Oracle (Oracle-managed), tak klíče spravované přímo zákazníkem (customer-managed) uvnitř Oracle Vault. Nicméně pro data uložená uvnitř bezpečnostní zóny (Security Zone) platí [91], že musí být šifrována vždy pomocí klíčů spravovaných zákazníkem (customer-managed). Data musí být šifrována jak při přenosu (in transit), tak při uložení (at rest).

5.6.2 (Volitelně) Vytvoření bezpečnostních zón (Security Zone)

OCI Security Zone [92] je vhodné použít zejména v situacích, kdy potřebujeme zajistit nejvyšší úroveň zabezpečení a dodržování bezpečnostních standardů při správě citlivých nebo kritických cloudových zdrojů (např. z legislativních či jiných důvodů). Její použití může být vhodné (nebo dokonce nutné) v následujících případech:

- *Práce s citlivými daty:* Pro prostředí obsahující citlivé údaje (osobní data, finanční informace, zdravotnické údaje), u kterých je kritické minimalizovat riziko úniku nebo kompromitace.

- *Soulad s bezpečnostními standardy*: Pokud je nutné zajistit soulad s předpisy nebo bezpečnostními normami, jako např. CIS OCI Benchmark, GDPR, HIPAA, PCI DSS atd. [1, s. 246]
- *Izolace kritické infrastruktury*: V případech, kdy je nutné striktně kontrolovat, jak se vytvářejí a konfiguruje zdroje a kde se ukládají data, aby nebylo možné jejich nechtěné nebo nebezpečné nastavení.
- *Kontrola přístupu a konfigurace zdrojů*: Pokud je nutné zajistit, že zdroje nebudou dostupné z veřejného Internetu nebo že konfigurace budou odpovídat pouze schváleným bezpečnostním standardům Oracle.
- *Prevence lidských chyb*: Security Zone automaticky zamítá jakoukoliv operaci, která odporuje definovaným bezpečnostním pravidlům, což minimalizuje riziko chyb při konfiguraci.

5.6.3 Aktivace OCI Cloud Guard

Doporučuje se aktivovat [93] službu OCI Cloud Guard, která nepřetržitě monitoruje prostředí OCI, analyzuje konfiguraci zdrojů a detekuje možné bezpečnostní hrozby nebo nesprávně nakonfigurované zdroje.

5.6.4 Aktivace Vulnerability Scanning

Z praktického hlediska je vhodné nastavit jako cíl služby OCI Vulnerability Scanning Service (VSS) celý kompartment, což zajistí automatické oskenování všech výpočetních instancí, které jsou do tohoto kompartmentu později umístěny.

5.7 Zabezpečení workloadů

Dle typu zvolených workloadů (definovaných v sekci plánování infrastruktury) provedeme jejich vytvoření a zabezpečení.

5.7.1 Vytvoření a zabezpečení cloudové sítě (Network Configuration)

Jeden ze základních typů workloadů, se kterým se můžeme v praxi setkat, je *třívrstvá (three-tier)* aplikace používající vícevrstvý síťový model. Tři vrstvy jsou obvykle definovány jako prezentační vrstva, aplikační vrstva a datová vrstva. Každá vrstva je izolovaná ve vlastní specializované podsíti, odděleně od ostatních vrstev. V rámci OCI Landing Zone jsou tyto tři podsítě definovány následovně:

- *prezentační vrstva* odpovídá veřejné webové podsíti (Web subnet)
- *aplikační vrstva* odpovídá aplikační podsíti (App subnet)
- *datová vrstva* odpovídá databázové podsíti (DB subnet)

Součástí je rovněž vytvoření firewallových (Security list) a routovacích (Route table) pravidel a otevření příslušných portů.

5.7.2 Vytvoření a zabezpečení cloudového úložiště (Storage)

Na základě typu požadovaného workloadu vytvoříme a zabezpečíme zvolený typ úložiště. OCI nabízí několik typů úložišť, každé vhodné pro různé scénáře a požadavky:

- *Block Volume* – Síťově připojené blokové úložiště určené pro virtuální instance [94].
- *Object Storage* – Vysoce škálovatelné úložiště objektů (podobné S3 od AWS). Prakticky neomezená kapacita, dostupnost přes HTTP(S), kompatibilní API [95].
- *Archive Storage* – Cenově velmi efektivní dlouhodobé archivační úložiště (za cenu delších obnovovacích časů oproti standardnímu Object Storage) [96].
- *File Storage* – Spravované souborové úložiště s protokolem NFS [97].
- *Local NVMe Storage* – Lokální, přímo připojené SSD úložiště na instancích. Extrémně nízká latence, vysoký IOPS, není perzistentní po ukončení instance [98].
- *Database storage* – Spravované úložiště v rámci databáze OCI (např. Autonomous Database, Exadata Database Service, Database as a Service/DBaaS).

5.8 Vytvoření a zabezpečení ostatních služeb a zdrojů

V závislosti na konkrétních požadavcích je z hlediska větší úrovně zabezpečení vhodné zvážit vytvoření dalších bezpečnostních prvků, mezi které patří:

- *Notifications, Alarms* – Služba umožňující odesílání oznámení o událostech v OCI pomocí e-mailu, SMS či webhooku, v kombinaci s automaticky spouštěnými upozorněními založených na metrikách, která indikují anomálie nebo dosažení stanovených limitů.
- *Cost tracking, Budget* – Nástroje pro monitorování a analýzu nákladů na cloudové služby v OCI, včetně nastavení limitů výdajů a upozornění při jejich překročení.

- *Flow Logs* – Záznamy síťového provozu zachycující informace o datových tocích v rámci virtuální sítě (VCN).
- *Service Connector Hub* – Centrální nástroj propojující OCI služby, umožňující přesun dat mezi nimi (např. logy do úložiště, notifikace na monitoring).
- *Network Firewall* – Spravovaná firewallová služba poskytující pokročilou ochranu sítě (VCN) před hrozbami a útoky.
- *Bastion Service* – Služba umožňující bezpečný, řízený vzdálený přístup k privátním prostředkům v OCI přes SSH či RDP.
- *WAF (Web Application Firewall)* – Firewallová ochrana webových aplikací proti běžným hrozbám (např. SQL injection, XSS) [2, s. 268] [2, s. 281].
- *Zero Trust Packet Routing (ZPR)* – Přístup k síťovému směrování založený na principech nulové důvěry, kde každá komunikace musí být explicitně povolena.

5.9 Ověření souladu s CIS OCI Foundations Benchmark

Poté, co je architektura v OCI vytvořena a nastavena, je vhodné ještě ověřit, zda splňuje doporučené bezpečnostní parametry definované dle CIS OCI Foundations Benchmark.

5.9.1 CIS Compliance Checker

CIS Compliance Checker [99] je skript vyvinutý firmou Oracle, který slouží ke kontrole bezpečnostní konfigurace cloudového prostředí Oracle Cloud Infrastructure vůči CIS OCI Foundations Benchmark a osvědčenými postupy pro bezpečné nastavení služeb a zdrojů v OCI. Skript lze stáhnout z GitHubu a jednoduše spustit pro jakoukoli OCI tenancy. Jeho výstupem je podrobná zpráva o komponentách, které nejsou v souladu s CIS OCI Foundations Benchmark, společně s doporučením, jak příslušnou konfiguraci opravit.

5.10 Průběžný monitoring auditních a bezpečnostních záznamů

Součástí návrhu bezpečné cloudové infrastruktury je také pravidelný monitoring auditních a bezpečnostních záznamů [1, s. 235] prostřednictvím služeb OCI, jako jsou Audit, Logging a Cloud Guard [84]. To umožňuje včasnou detekci incidentů a podporuje rychlou reakci i zajištění souladu s interními i externími požadavky (včetně regulatorních) [1, s. 397].

II PRAKTICKÁ ČÁST

6 SESTAVENÍ NAVRŽENÝCH BEZPEČNOSTNÍCH OPATŘENÍ

V rámci této kapitoly provedeme sestavení (implementaci) bezpečnostních opatření navržených v předchozí kapitole v testovacím prostředí v OCI. V následujících kapitolách poté rovněž provedeme ověření jejich funkčnosti a efektivity v rámci vybraných bezpečnostních testů.

6.1 Plán zabezpečení infrastruktury

Pro realizaci *Proof-of-Concept* (PoC) testovacího OCI prostředí použijeme doporučenou referenční architekturu OCI Core Landing Zone dostupnou jako šablonu pro Terraform, která je volně k dispozici na GitHub [100] s vlastními parametry, jejichž souhrnný přehled obsahuje tabulka (Tabulka 3).

Tabulka 3 PoC – Návrh infrastruktury

Parametr PoC Tenancy	Hodnota
Implementovaná úroveň CIS	2
Domovský region	eu-frankfurt-1
Další aktivované regiony	žádné
Cloud Account Administrator	1 (d_codl@***)
Počet zvolených domén identity	1 (Default)
Identity Domain Administrator	1 (d_codl@***)
Tenancy Admin	1 (d_codl@***)
Plánované workloady	1 základní třívrstvá aplikační topologie
Struktura kompartmentů	(root compartment) + Security + Network + Application + Database

Seznam administrativních rolí	IAM Administrators Credential Administrators Cost Administrators Auditors Announcement Readers Security Administrators Network Administrators Application Administrators Database Administrators Storage Administrators Access Governance
Seznam dynamických skupin	Security Functions AppDev Functions Compute Agent Database KMS
Definované bezpečnostní politiky	basic_root_policy security_admin_policy security_admin_root_policy network_admin_policy network_admin_root_policy compute_agent_policy database_admin_policy database_dynamic_group_policy appdev_admin_policy iam_admin_policy iam_admin_root_policy cred_admin_policy auditor_policy announcement_reader_policy exainfra_admin_policy cost_admin_root_policy storage_admin_policy access_governance_root_policy net_fw_app_policy lz_services_policy lz_oke_clusters_policy services_policy oke_clusters_policy
Komponenty CSPM	Vytvoření „customer-managed“ hlavního šifrovacího klíče v Oracle Vault Vytvoření bezpečnostní zóny (PoC-lz-security-zone) Aktivace Cloud Guard Nastavení Vulnerability Scanning (1x týdně, každou neděli)

Návrh a zabezpečení VCN (dle workloadů)	1 třivrstvá aplikační (three-tier) VCN CIDR 192.168.0.0/16 + Web podsít' (veřejná) 192.168.0.0/24 + App podsít' (soukromá) 192.168.1.0/24 + DB podsít' (soukromá) 192.168.2.0/24
Typ úložiště	Objektové úložiště (Object Storage)
Ostatní služby	Flow Logs Object Storage logging Service Connector Hub OracleVault Notifications and Alarms + security_admin_email_endpoints (d_codl@***) + network_admin_email_endpoints (d_codl@***) Tag defaults (CreatedBy, CreatedOn) Budget + budget_alert_threshold (100%) + budget_amount (USD 100/měsíc) + budget_alert_email_endpoints (d_codl@***)

(zdroj: vlastní)

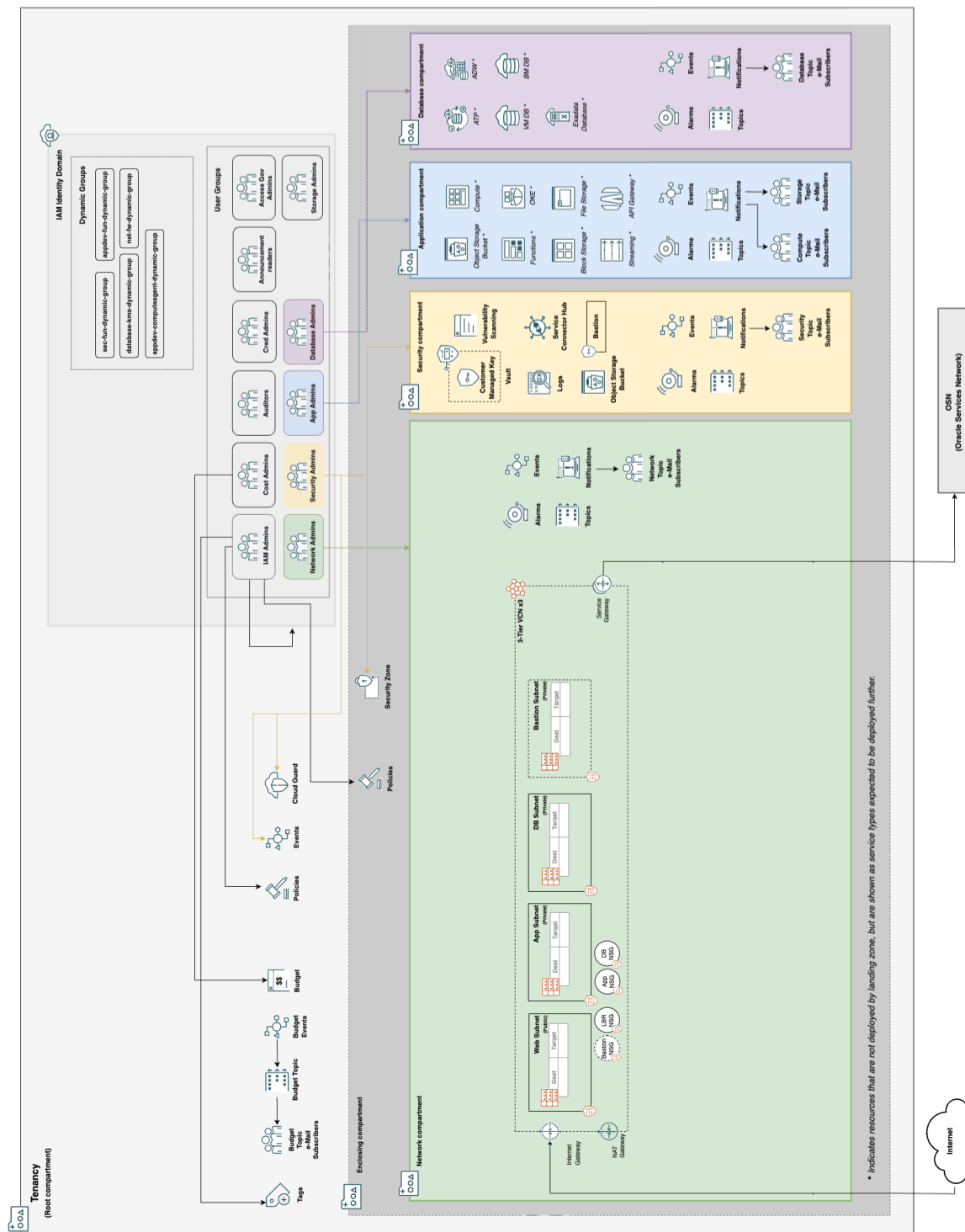
6.2 Vizualizace architektury pomocí OCI diagramu

Architektura OCI Core Landing Zone, kterou jsme pro realizaci PoC použili, obsahuje návrh struktury kompartmentů spolu s uživatelskými skupinami a pravidly IAM, která zajišťují oddělení rolí a odpovědností. Definujeme jednu VCN (typu „three-tier“) s potřebným směrováním a zabezpečením příchozí a odchozí komunikace. Součástí Landing Zone jsou také bezpečnostní služby Oracle Cloud Guard, Flow Logs, Service Connector Hub, Vault a Vulnerability Scanning.

Z pohledu governance jsou v Landing Zone nastaveny upozornění a alarmy pomocí témat a událostí, které administrátorům signalizují změny nebo překročení stanovených metrik u zdrojů. Automaticky se také používají přednastavené tagy, které umožňují identifikovat vlastníka zdroje a datum vytvoření a dále nastavení základního budgetu.

Důležitou součástí governance je i správa logování. Podle CIS OCI Benchmark jsou logy provozu VCN a logy Object Storage ve výchozím nastavení aktivovány. Landing Zone navíc umožňuje využít službu Service Connector Hub k centralizaci logů OCI do jediného cílového umístění (standardně bucket v Object Storage). Tato možnost usnadňuje potenciální integraci OCI logů do SIEM nástrojů třetích stran, jako je například Cisco

Splunk. Na obrázku (Obrázek 12) je znázorněn OCI diagram PoC architektury. Větší detail jednotlivých částí diagramu obsahuje příloha P I.



Obrázek 12: PoC – OCI diagram (třívrstvá aplikační topologie)

(zdroj: [100])

6.3 Vytvoření tenancy

Prvním krokem při realizaci Proof-of-Concept (PoC) testovacího OCI prostředí je vytvoření vlastního pronajatého prostoru (tenancy) ve zvoleném OCI regionu (eu-frankfurt-1). Níže v tabulce (Tabulka 4) jsou uvedeny detaily nově vytvořené tenancy.

Tabulka 4 PoC – Název tenancy a OCID

Název tenancy OCID	dcodlthesis2025
ocid1.tenancy.oc1..aaaaaaaahxhpeqkgsrfmtwxjfxffiofrexn7ipxh4rqm4zlvem7nn2oefyaq	

(zdroj: vlastní)

6.3.1 Zabezpečení účtu globálního administrátora pomocí MFA

Ve výchozím nastavení OCI vyžaduje [101] při přihlašování do OCI Console použití druhého faktoru (Multi-factor authentication, MFA) povinně pro všechny uživatele. Toto je implementováno prostřednictvím předem nakonfigurované sign-on politiky s názvem *Security Policy for OCI Console*, viz obrázek (Obrázek 13), která je automaticky aktivována při vytvoření nové tenancy. Tato sign-on politika obsahuje dvě hlavní pravidla:

- *MFA pro administrátory (MFA for administrators)*: Toto pravidlo je první v pořadí priorit a vyžaduje, aby všichni uživatelé ve skupině Administrators a všichni uživatelé s administrátorskou rolí museli při každém přihlášení do OCI Console použít MFA.
- *MFA pro všechny uživatele (MFA for all users)*: Toto pravidlo je druhé v pořadí priorit a vyžaduje, aby všichni uživatelé museli při každém přihlášení do OCI Console použít MFA.

The screenshot shows the OCI Console interface for the 'Security Policy for OCI Console'. At the top, there's a navigation bar with the title 'Security Policy for OCI Console' and a dropdown menu set to 'Germany Central (Frankfurt)'. Below the navigation bar, a breadcrumb trail reads 'Security > Sign-on policies > Sign-on policy details'. A blue information box at the top contains a message: 'To further improve the security posture of your tenancy, Oracle recommends that you keep multi-factor authentication (MFA) enabled for users with administrative privileges. See [OCI Security recommendations](#).' Below this, the main heading is 'Security Policy for OCI Console'. There are two buttons: 'Edit sign-on policy' and 'Deactivate sign-on policy'. A tab labeled 'Sign-on policy information' is active, showing a description: 'The Security Defaults to secure OCI Console' and a creation timestamp: 'Created: Wed, Mar 12, 2025, 12:55:19 UTC'. Below this, the 'Sign-on rules' section has three buttons: 'Add sign-on rule', 'Edit priority', and 'Remove sign-on rule'. A table lists two rules:

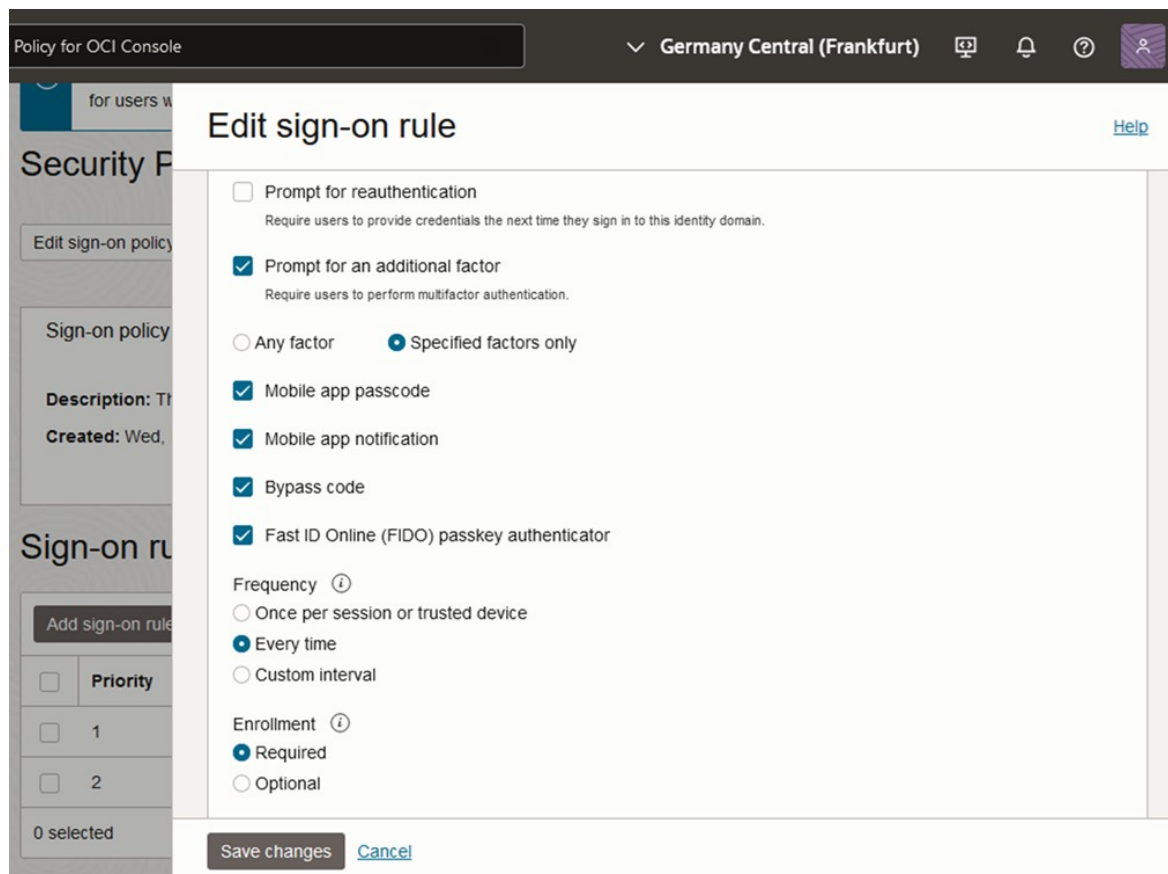
☐	Priority	Name	
☐	1	MFA for administrators	⋮
☐	2	MFA for all users	⋮

At the bottom of the table, it says '0 selected' on the left and 'Showing 2 items' on the right.

Obrázek 13: Bezpečnostní politika „Security Policy for OCI Console“

(zdroj: vlastní)

Vzhledem k tomu, že obě pravidla jsou vytvořena a aktivována automaticky, stačí v doméně identity, kterou aktuálně používáme (obvykle „Default Identity Domain“) ověřit, že obě pravidla mají aktivní volbu „Prompt for an additional factor“ v sekci „Actions“, jak je patrné na obrázku (Obrázek 14).



Obrázek 14: Editace MFA pravidla „Prompt for an additional factor“

(zdroj: vlastní)

6.4 Upgrade Free Tier typu účtu na Pay-As-You-Go (PAYG)

Vzhledem k tomu, že některé bezpečnostní funkce OCI (jako např. Cloud Guard) jsou dostupné pouze v placené verzi OCI účtu, je nutné z tohoto důvodu účet upgradovat. Pro potřeby PoC zvolíme typ placeného účtu Pay-As-You-Go (PAYG).

6.5 Vytvoření „custom-managed“ šifrovacího klíče (CIS Level 2)

Šifrování pomocí klíčů spravovaných zákazníkem („customer-managed“) je požadavkem CIS Foundations Benchmark úrovně 2. Proto je nutné tento klíč nejprve vytvořit v Oracle Vault, aby mohl být následně zadán jako parametr v rámci použití OCI Core Landing Zone (pozn. CIS Foundations Benchmark úroveň 1 vytvoření „custom-managed“ šifrovacího klíče nevyžaduje).

6.6 Vytvoření prvků řízení identity a přístupových oprávnění (IAM)

Bezpečnostní prvky pro řízení identity a přístupových práv jsou vytvořeny aplikací terraformové šablony OCI Core Landing Zone pomocí Oracle Resource Manageru. Výsledek ověříme v příslušných sekcích OCI Console, viz obrázky (Obrázek 15), (Obrázek 16), (Obrázek 17) a (Obrázek 18).



Compartments

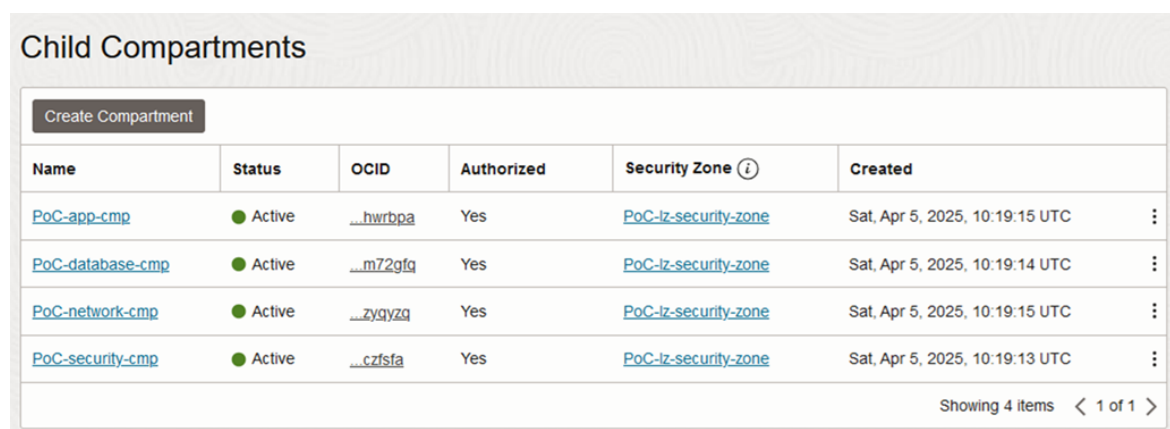
Create Compartment

Name	Status	OCID	Authorized	Security Zone ⓘ	Subcompartments	Created	
dcodithesis2025	● Active	...oefyag	Yes	-	1	-	⋮
PoC-top-cmp	● Active	...hfg4ja	Yes	PoC-lz-security-zone	4	Sat, Apr 5, 2025, 10:18:54 UTC	⋮

Showing 2 items < 1 of 1 >

Obrázek 15: PoC – Vytvořené IAM prvky (Enclosing Compartment)

(zdroj: vlastní)



Child Compartments

Create Compartment

Name	Status	OCID	Authorized	Security Zone ⓘ	Created	
PoC-app-cmp	● Active	...hwrtpa	Yes	PoC-lz-security-zone	Sat, Apr 5, 2025, 10:19:15 UTC	⋮
PoC-database-cmp	● Active	...m72gfg	Yes	PoC-lz-security-zone	Sat, Apr 5, 2025, 10:19:14 UTC	⋮
PoC-network-cmp	● Active	...zyqyzq	Yes	PoC-lz-security-zone	Sat, Apr 5, 2025, 10:19:15 UTC	⋮
PoC-security-cmp	● Active	...czfsfa	Yes	PoC-lz-security-zone	Sat, Apr 5, 2025, 10:19:13 UTC	⋮

Showing 4 items < 1 of 1 >

Obrázek 16: PoC – Vytvořené IAM prvky (Nested Compartments)

(zdroj: vlastní)

Groups *in Default Domain*

Search by group name or description.

Create group More actions ▼

☐	Name	Description	Created	
☐	PoC-app-admin-group	Core Landing Zone group for managing app development related services.	Sat, Apr 5, 2025, 10:18:57 UTC	⋮
☐	PoC-network-admin-group	Core Landing Zone group for network management.	Sat, Apr 5, 2025, 10:18:57 UTC	⋮
☐	PoC-iam-admin-group	Core Landing Zone group for managing IAM resources in the tenancy.	Sat, Apr 5, 2025, 10:18:54 UTC	⋮
☐	PoC-storage-admin-group	Core Landing Zone group for storage services management.	Sat, Apr 5, 2025, 10:18:54 UTC	⋮
☐	PoC-security-admin-group	Core Landing Zone group for security services management.	Sat, Apr 5, 2025, 10:18:54 UTC	⋮
☐	PoC-announcement-reader-group	Core Landing Zone group for reading Console announcements.	Sat, Apr 5, 2025, 10:18:54 UTC	⋮
☐	PoC-database-admin-group	Core Landing Zone group for managing databases.	Sat, Apr 5, 2025, 10:18:54 UTC	⋮

Obrázek 17: PoC – Vytvořené IAM prvky (Groups)

(zdroj: vlastní)

Policies *in PoC-top-cmp compartment*

Create Policy Delete

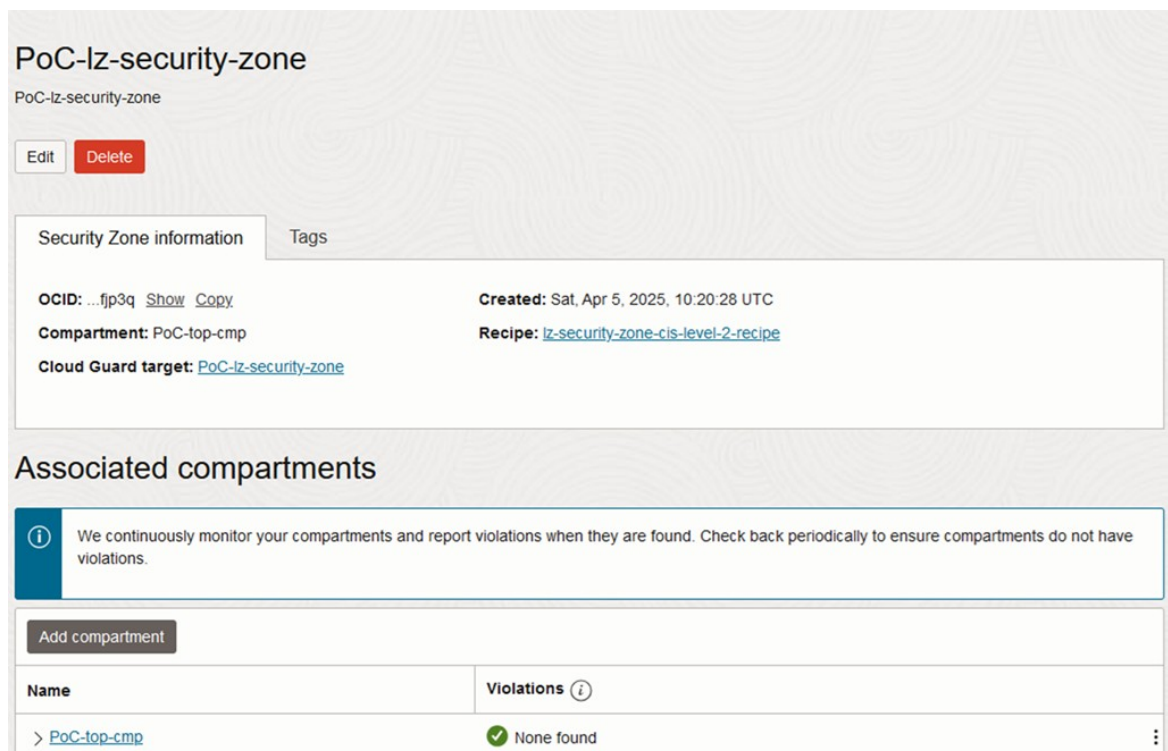
☐	Name	Description	Statements	Created	
☐	PoC-database-admin-policy	Core Landing Zone policy for PoC-database-admin-group group to manage database related resources.	39	Sat, Apr 5, 2025, 10:19:58 UTC	⋮
☐	PoC-appdev-admin-policy	Core Landing Zone policy for PoC-app-admin-group group to manage app development related services.	40	Sat, Apr 5, 2025, 10:19:58 UTC	⋮
☐	PoC-security-admin-policy	Core Landing Zone policy for PoC-security-admin-group group to manage security related services in Landing Zone enclosing compartment (compartment PoC-top-cmp).	43	Sat, Apr 5, 2025, 10:19:58 UTC	⋮
☐	PoC-network-admin-policy	Core Landing Zone policy for PoC-network-admin-group group to manage network related services.	30	Sat, Apr 5, 2025, 10:19:58 UTC	⋮
☐	PoC-database-dynamic-group-policy	Core Landing Zone policy for PoC-database-kms-dynamic-group group to use Vault service.	3	Sat, Apr 5, 2025, 10:19:57 UTC	⋮
☐	PoC-iam-admin-policy	Core Landing Zone policy for PoC-iam-admin-group group to manage IAM resources in Landing Zone enclosing compartment (compartment PoC-top-cmp).	2	Sat, Apr 5, 2025, 10:19:57 UTC	⋮
☐	PoC-storage-admin-policy	Core Landing Zone policy for PoC-storage-admin-group group to manage storage resources.	28	Sat, Apr 5, 2025, 10:19:57 UTC	⋮
☐	PoC-compute-agent-policy	Core Landing Zone policy for PoC-app-computeagent-dynamic-group group to manage compute agent related services.	3	Sat, Apr 5, 2025, 10:19:57 UTC	⋮

Obrázek 18: PoC – Vytvořené IAM prvky (Security Policies)

(zdroj: vlastní)

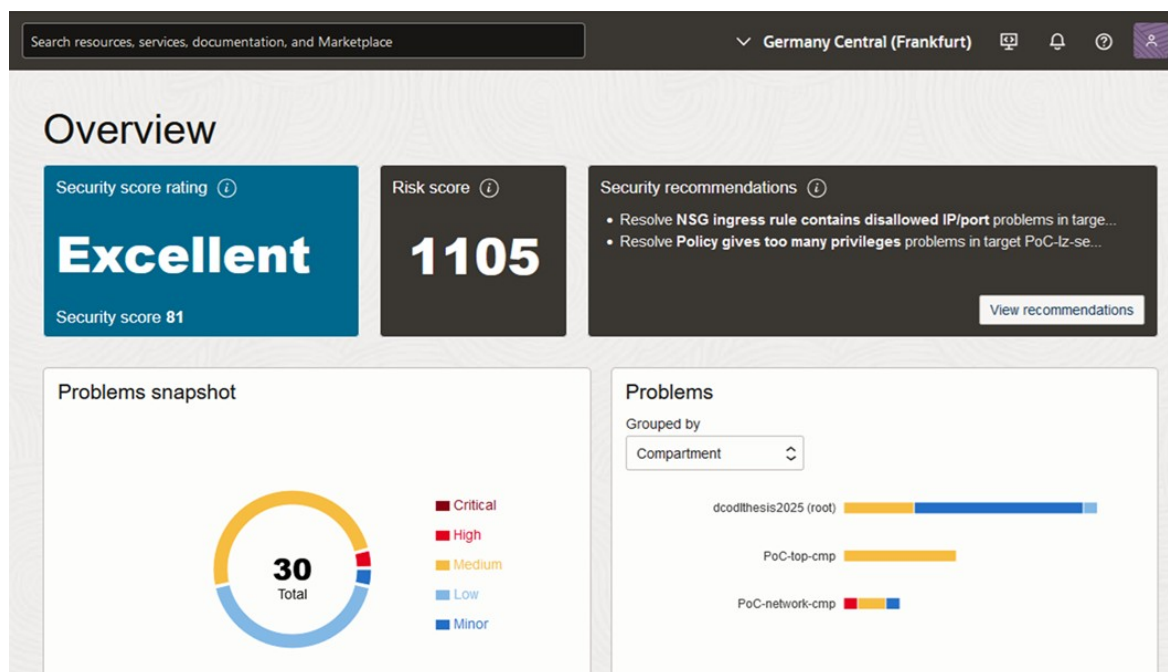
6.7 Aktivace Cloud Security Posture Management (CSPM)

Vytvoření hlavního šifrovacího klíče v Oracle Vault bylo již provedeno dříve (v rámci kroku 6.5). Zbývající bezpečnostní prvky nutné k aktivaci CSPM jsou vytvořeny aplikací terraformové šablony OCI Core Landing Zone pomocí Oracle Resource Manageru. Výsledek opět overíme v příslušných sekcích OCI Console, viz obrázky (Obrázek 19), (Obrázek 20) a (Obrázek 21).



Obrázek 19: PoC – Aktivace CSPM (Security Zone)

(zdroj: vlastní)



Obrázek 20: PoC – Aktivace CSPM (Cloud Guard)

(zdroj: vlastní)

Targets in PoC-security-cmp compartment

Create a target to enable scanning for resources in a compartment. [Learn more](#)

Qualys BYOL option now available. See the agent option in host [scan recipe](#)

Hosts Container image

Create

Name	State	Target compartment	Scan recipe	Created
PoC-network-cmp-scan-target	Active	PoC-network-cmp	PoC-default-scan-recipe	Sat, Apr 5, 2025, 10:19:31 UTC
PoC-security-cmp-scan-target	Active	PoC-security-cmp	PoC-default-scan-recipe	Sat, Apr 5, 2025, 10:19:31 UTC
PoC-app-cmp-scan-target	Active	PoC-app-cmp	PoC-default-scan-recipe	Sat, Apr 5, 2025, 10:19:31 UTC
PoC-database-cmp-scan-target	Active	PoC-database-cmp	PoC-default-scan-recipe	Sat, Apr 5, 2025, 10:19:31 UTC

Showing 4 items < Page 1 >

Obrázek 21: PoC – Aktivace CSPM (Vulnerability Scanning Service)

(zdroj: vlastní)

6.8 Zabezpečení workloadů

V rámci zabezpečení workloadů jsme vytvořili základní síťovou topologii a cloudové úložiště typu Object Storage aplikací terraformové šablony OCI Core Landing Zone pomocí Oracle Resource Manageru. Výsledek overíme v příslušných sekcích OCI Console, viz obrázky (Obrázek 22), (Obrázek 23) a (Obrázek 24).

Virtual Cloud Networks

Virtual Cloud Networks (VCNs) are private virtual networks you set up in Oracle Cloud Infrastructure. You can attach gateways, route tables, and security lists to specify routing and security rules.

To view service log metrics and additional information about service resources, click [View or manage logs](#)

Create VCNStart VCN Wizard

Name	State	IPv4 CIDR Block	IPv6 Prefix	Default Route Table	DNS Domain Name	Created
PoC-three-tier-vcn-1	● Available	192.168.0.0/16	—	Default Route Table for PoC-three-tier-vcn-1	threeertiervcn1.oraclevcn.com	Sat, Apr 5, 2025, 10:19:31 UTC

Showing 1 item < 1 of 1 >

Obrázek 22: PoC – Zabezpečení workloadů (VCN)
(zdroj: vlastní)

Subnets

Create Subnet

Name	State	IPv4 CIDR Block	IPv6 Prefixes	Subnet Access	Created
middle-subnet	● Available	192.168.1.0/24	—	Private (Regional)	Sat, Apr 5, 2025, 10:20:02 UTC
backend-subnet	● Available	192.168.2.0/24	—	Private (Regional)	Sat, Apr 5, 2025, 10:20:01 UTC
frontend-subnet	● Available	192.168.0.0/24	—	Public (Regional)	Sat, Apr 5, 2025, 10:20:01 UTC

Showing 3 items < 1 of 1 >

Obrázek 23: PoC – Zabezpečení workloadů (Subnets)
(zdroj: vlastní)

Ingress Rules

Add Ingress RulesEditRemove

☐	Stateless	Source	IP Protocol	Source Port Range	Destination Port Range	Type and Code	Allows	Description
☐	No	0.0.0.0/0	ICMP			3, 4	ICMP traffic for: 3, 4 Destination Unreachable: Fragmentation Needed and Don't Fragment was Set	ICMP type 3 code 4
☐	No	192.168.0.0/16	ICMP			3	ICMP traffic for: 3 Destination Unreachable	ICMP type 3

0 selected

Showing 2 items < 1 of 1 >

Obrázek 24: PoC – Zabezpečení workloadů (Security list)
(zdroj: vlastní)

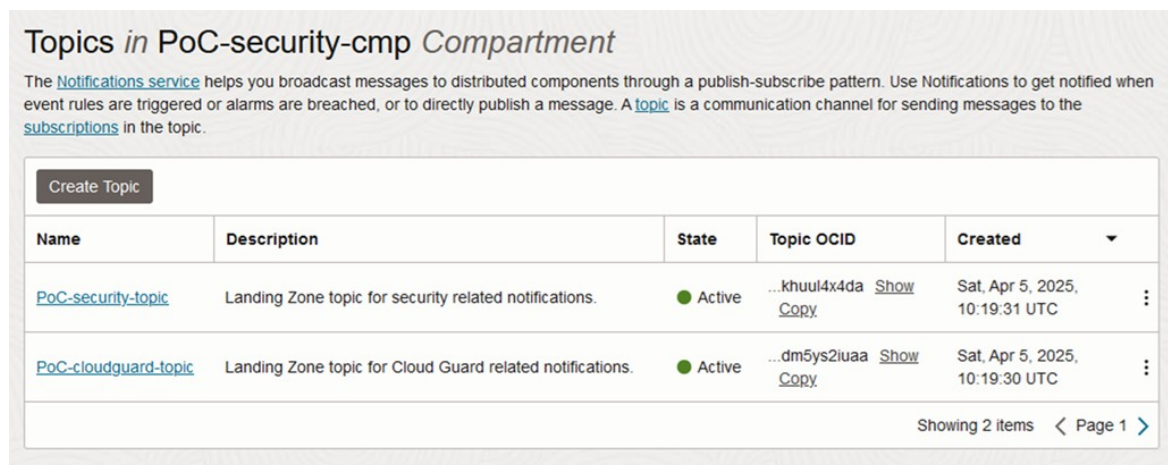
6.9 Vytvoření a zabezpečení ostatních služeb a zdrojů

Během implementace PoC jsme rovněž vytvořili dodatečné služby a zdroje k podpoře vyšší úrovně zabezpečení a kontroly, a to zejména tyto:

6.9.1 Notifications, Alarms

Landing Zone implementuje doporučení standardu CIS Benchmark prostřednictvím rámce notifikací, který zajišťuje zasílání upozornění na emailové adresy v případě změn infrastruktury. Tento rámec plně využívá služeb OCI Events a OCI Notifications. Princip spočívá v tom, že jakmile dojde k určité události, například k aktualizaci bezpečnostních politik, je zpráva automaticky zaslána na předem definované téma (topic), přičemž přihlášení odběratelé následně obdrží odpovídající notifikaci.

V rámci PoC jsme implementovali dvě témata, a to notifikace týkající se událostí změn v infrastruktuře („PoC-security-topic“) a notifikace bezpečnostních událostí reportovaných z Cloud Guardu („PoC-cloudguard-topic“). Tuto skutečnost ilustruje obrázek (Obrázek 25).



Topics in PoC-security-cmp Compartment

The [Notifications service](#) helps you broadcast messages to distributed components through a publish-subscribe pattern. Use Notifications to get notified when event rules are triggered or alarms are breached, or to directly publish a message. A [topic](#) is a communication channel for sending messages to the [subscriptions](#) in the topic.

Create Topic

Name	Description	State	Topic OCID	Created
PoC-security-topic	Landing Zone topic for security related notifications.	Active	...khuul4x4da Show Copy	Sat, Apr 5, 2025, 10:19:31 UTC
PoC-cloudguard-topic	Landing Zone topic for Cloud Guard related notifications.	Active	...dm5ys2iuua Show Copy	Sat, Apr 5, 2025, 10:19:30 UTC

Showing 2 items < Page 1 >

Obrázek 25: PoC – Ostatní služby a zdroje (Notifications)

(zdroj: vlastní)

Landing Zone dále rozšiřuje monitoring událostí o operační metriky a alarmy poskytované službou OCI Monitoring. Tento model umožňuje detekovat události na úrovni jednotlivých zdrojů, například nadměrné využití procesoru, paměti či úložiště, nebo také stavové změny spojení typu FastConnect, apod. Příklad nastavení pro síťový kompartment („PoC-network-cmp“) ilustruje obrázek (Obrázek 26).

Alarm Definitions *in PoC-network-cmp Compartment*

Use the [Monitoring service](#) to set up alarms to notify you when a condition occurs.

Create Alarm Actions Search

☐	Alarm name	Status	Severity	Metric namespace	Notifications destination	Suppressed
☐	PoC-fast-connect-status-alarm	● Disabled	Critical	oci_fastconnect	Notifications	Not suppressed
☐	PoC-vpn-status-alarm	● Disabled	Critical	oci_vpn	Notifications	Not suppressed

0 selected Showing 2 items < 1 of 1 >

Obrázek 26: PoC – Ostatní služby a zdroje (Alarms)

(zdroj: vlastní)

6.9.2 Cost tracking, Budget

Aby se předešlo neočekávaným nákladům, Landing Zone umožňuje vytvoření základního rozpočtu (budget), který zasílá upozornění na zadanou emailovou adresu v případě, že prognózované výdaje dosáhnou předem definovaného limitu. V rámci PoC jsme vytvořili základní rozpočet s měsíčním limitem USD 100,- viz obrázek (Obrázek 27).

Budgets

You can use budgets to track costs in your tenancy. After creating a budget for a compartment, you can set up alerts that will notify you if a budget is forecast to be exceeded or if spending surpasses a certain amount.

Create Budget

Name	Status	Budget Type	Budget Scope	Target	Amount	Spent	% Spent In Period	Forecast ⓘ
PoC-main-budget	● Active	Monthly	Compartment	PoC-top-cmp	US\$100	US\$0	N/A	US\$0 ⓘ

Showing 1 item < 1 of 1 >

Obrázek 27: PoC – Ostatní služby a zdroje (Budget)

(zdroj: vlastní)

Rovněž je implementována metoda automatického „tagování“ vytvořených zdrojů. Tagování zdrojů (resource tagging) představuje důležitou součást rámce správy a řízení (governance framework), jelikož umožňuje detailní identifikaci jednotlivých zdrojů bez ohledu na jejich zařazení v rámci kompartmentů. V prostředí OCI je díky tagování možné zajistit dva zásadní aspekty řízení prostředí, a to sledování nákladů a správu přístupů založenou na tagovacích politikách (tag-based policies).

Landing Zone zavádí výchozí tagy „CreatedBy“ (kým vytvořeno) a „CreatedOn“ (kdy vytvořeno) v nově vytvořeném jmenném prostoru (tag namespace). Tyto výchozí tagy zajišťují automatické označení všech následně vytvořených zdrojů a jejich použití je vyžadováno standardem CIS Foundations Benchmark.

Aktuální implementaci v rámci PoC ilustruje následující obrázek (Obrázek 28).

☐	Name	Value Type	Status	OCID	Cost Tracking	Created
☐	CreatedBy	String	● Active	...ugaoga	Yes	Wed, Mar 12, 2025, 12:55:44 UTC
☐	CreatedOn	String	● Active	...por43a	No	Wed, Mar 12, 2025, 12:55:44 UTC

0 selected Showing 2 items < 1 of 1 >

Obrázek 28: PoC – Ostatní služby a zdroje (Cost Tracking Tags)

(zdroj: vlastní)

6.9.3 Flow Logs

Každý zdroj v rámci virtuální cloudové sítě (VCN) disponuje jednou nebo více virtuálními síťovými kartami (Virtual Network Interface Cards, VNIC). Síťová služba využívá bezpečnostní seznamy (Security Lists) pro řízení, jaký provoz je povolen skrze konkrétní VNIC. Každá VNIC podléhá všem pravidlům uvedeným ve všech bezpečnostních seznamech přiřazených k subnetu, do kterého VNIC náleží. Pro účely řešení problémů spojených s bezpečnostními seznamy nebo auditu provozu VNIC lze nastavit záznamy síťových toků (VCN Flow Logs). Tyto záznamy zachycují detailní informace o provozu, který byl povolen či zamítnut na základě pravidel uvedených v bezpečnostních seznamech.

Použití Flow Logs v rámci CIS Foundation Benchmark úrovně 1 není povinné, nicméně je vyžadováno v rámci úrovně 2. Aktuální implementaci Flow Logs v PoC ilustruje obrázek (Obrázek 29).

Flow log configurations *in PoC-security-cmp Compartment*

Use flow logs to capture network traffic information that supports your monitoring and security needs. [Learn more](#).

Enable flow logs Edit Delete

☐	Name	Enablement point type	Enablement point	Capture filter	Destination	Lifecycle state
☐	TT-VCN-1-DB-SUBNET-flow-log	Subnet	backend-subnet	-	PoC-flow-logs-group	● Active
☐	TT-VCN-1-APP-SUBNET-flow-log	Subnet	middle-subnet	-	PoC-flow-logs-group	● Active
☐	TT-VCN-1-WEB-SUBNET-flow-log	Subnet	frontend-subnet	-	PoC-flow-logs-group	● Active

0 selected Showing 3 items < 1 of 1 >

Obrázek 29: PoC – Ostatní služby a zdroje (Flow Logs)

(zdroj: vlastní)

6.10 Ověření souladu s CIS OCI Foundations Benchmark

Prozatím jsme všechny kroky prováděli jako hlavní administrativní uživatel (tenancy admin). Nyní je čas začít využívat bezpečnostní architekturu a zejména RBAC (role based access control) role, které jsme si v rámci PoC nadeřinovali a vytvořili.

K ověření souladu s CIS OCI Foundations Benchmark použijeme CIS Compliance Checker skript, který spustíme jako nově vytvořený uživatel Alice v rámci role auditor („PoC-auditor-group“), která je právě pro tyto účely určena.

CIS Compliance Checker skript stáhneme z GitHubu a spustíme v prostředí Cloud Shell přímo v OCI Console viz obrázek (Obrázek 30).

```
alice_newm@cloudshell:~ (eu-frankfurt-1)$ python3 cis_reports.py -dt --obp --raw

#####
#                               Running CIS Reports - Release 2.8.8                               #
#####
Version 2.8.8 Updated on March 4, 2024
Please use --help for more info

Tested   oci-python-sdk version: 2.147.0
Installed oci-python-sdk version: 2.149.1
The command line arguments are: ['cis_reports.py', '-dt', '--obp', '--raw']

Starts at 2025-04-10T11:13:40
```

Obrázek 30: PoC – Spuštění CIS Compliance Checker

(zdroj: vlastní)

Poté, co skript skončí a vyprodukuje výslednou zprávu, prověříme nálezy, které nejsou v souladu s požadavky benchmarku nebo obecnými bezpečnostními doporučeními, a provedeme příslušné korekce, viz obrázek (Obrázek 31).

```

#####
#                               OCI Best Practices Findings                               #
#####
Category                        Compliant      Findings      Best Practices
#####
Cost_Tracking_Budgets           False          1             0
SIEM_Audit_Log_All_Comps        False          6             0
SIEM_Audit_Incl_Sub_Comp        False          1             0
SIEM_VCN_Flow_Logging           False          3             0
SIEM_Write_Bucket_Logs          False          0             0
SIEM_Read_Bucket_Logs           False          0             0
Networking_Connectivity         False          0             0
Cloud_Guard_Config              False          1             0
Certificates_Near_Expiry        True           0             0
#####
#                               Writing Oracle Best Practices reports to CSV              #
#####
CSV: OBP_Summary                --> dcodlthesis2025-2025-04-10_11-13-40/obp_OBP_Summary.csv
CSV: Cost_Tracking_Budgets_Findings --> dcodlthesis2025-2025-04-10_11-13-40/obp_Cost_Tracking_Budgets_Findings.csv
CSV: SIEM_Audit_Log_All_Comps_Findings --> dcodlthesis2025-2025-04-10_11-13-40/obp_SIEM_Audit_Log_All_Comps_Findings.csv
CSV: SIEM_Audit_Incl_Sub_Comp_Findings --> dcodlthesis2025-2025-04-10_11-13-40/obp_SIEM_Audit_Incl_Sub_Comp_Findings.csv
CSV: SIEM_VCN_Flow_Logging_Findings --> dcodlthesis2025-2025-04-10_11-13-40/obp_SIEM_VCN_Flow_Logging_Findings.csv
CSV: Cloud_Guard_Config_Findings --> dcodlthesis2025-2025-04-10_11-13-40/obp_Cloud_Guard_Config_Findings.csv

```

Obrázek 31: PoC – Revize výsledků CIS Compliance Checker

(zdroj: vlastní)

7 OVĚŘENÍ VYBRANÝCH BEZPEČNOSTNÍCH SCÉNÁŘŮ

V této kapitole ověříme úroveň zabezpečení vytvořené infrastruktury a zdrojů v OCI v rámci simulovaných bezpečnostních situací (scénářů), které mohou reálně nastat. Jednotlivé scénáře navrhujeme s ohledem na nejčastější hrozby v prostředí cloudu (diskutované v kapitole 4), a současně tak, aby z hlediska kyberbezpečnosti pokryly všechny složky tzv. *CIA triády* (Confidentiality, Integrity, Availability) [2, s. 17]. Zaměříme se na otestování různých zdrojů v OCI a oblastí infrastruktury s cílem, aby navržené scénáře pokryly co nejširší spektrum možných situací. Na závěr výsledky zhodnotíme.

Každý test bude současně označen svým jednoznačným identifikátorem ve tvaru:

SEC-[KATEGORIE]-[CIA]-[ČÍSLO]-[VOLITELNÝ_POPIS]

Kde význam položek je následující:

- SEC – prefix, že jde o bezpečnostní test
- [KATEGORIE] – typ oblasti (např. AUTH, NET, DATA...)
- [CIA] – aspekt bezpečnosti (C = Confidentiality, I = Integrity, A = Availability)
- [ČÍSLO] – pořadí testu v dané kategorii/CIA
- [VOLITELNÝ_POPIS] – stručné upřesnění

7.1 Testovací scénář – Prevence vytvoření veřejného bucketu

Technika „Data from Cloud Storage“ (T1530) v rámci frameworku MITRE ATT&CK [102] popisuje rizika spojená s neoprávněným přístupem k datům uloženým v cloudových úložištích (zejména typu IaaS). Útočníci mohou využít chybné konfigurace zabezpečení, které často vznikají neúmyslně, a získat tak přístup k citlivým informacím.

Vytvoření veřejného bucketu bez autentizace představuje klasický příklad špatně zabezpečeného cloudového úložiště a je považováno za závažnou bezpečnostní chybu, která může vést k nekontrolovanému úniku dat. Pokud je bucket nastaven jako veřejný, znamená to, že kdokoli na Internetu – bez jakéhokoli ověření identity – může získat přístup k jeho obsahu. Tento přístup je zcela mimo kontrolu IAM systému.

V prostředí OCI je v rámci tzv. bezpečnostních zón (Security Zones) zcela zakázáno [103] vytvářet veřejně přístupné Object Storage buckety. Jakékoli pokusy o vytvoření

veřejného bucketu jsou systémem automaticky zablokovány. Cílem tohoto bezpečnostního scénáře je ověřit v praxi toto opatření.

7.1.1 Příprava testovacího prostředí

Test lze provést v rámci stávající infrastruktury (vytvořené v kapitole 6) bez nutnosti vytvářet další zdroje v OCI.

7.1.2 Výsledek testu

Tabulka (Tabulka 5) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 5 Testovací scénář – Prevence vytvoření veřejného bucketu

Atribut testu	Hodnota
ID testu	SEC-DATA-C-001-PUBLIC-BUCKET-CREATE
Typ testu	Confidentiality
Název scénáře	Prevence vytvoření veřejného bucketu
Popis	Pokus o vytvoření veřejně přístupného bucketu pro možnou exfiltraci dat.
Úroveň hrozby	Critical
OCI služba	Object Storage
Kompartment	PoC-top-cmp
Uživatel a role	d_codl@*** (tenancy administrator)
Metoda provedení	OCI CLI
Příkaz/kroky k provedení	<pre>oci os bucket create \ --name muj-verejny-bucket \ --compartment-id \$(oci iam compartment list --name PoC-top-cmp --query "data[0].id" --raw-output) \ --public-access-type ObjectRead \ --storage-tier Standard</pre>
Očekávaný výsledek	Pokus o vytvoření bucketu selže s chybovou zprávou o porušení bezpečnostní politiky.
Skutečný výsledek	<pre>ServiceError: "code": "Forbidden", "message": "Security Zone Violation: Object Storage buckets in a security zone can't be public.",</pre>
Status (Pass/Fail)	 Pass
Poznámka / Komentář	Potvrzeno očekávané chování.
Datum a čas testu	13/04/2025 10:26 CET

Odkaz na OCI dokumentaci	[103]
--------------------------	-------

(zdroj: vlastní)

7.1.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

7.2 Testovací scénář – Prevence vytvoření neautorizované VCN

Tento scénář odpovídá taktice „Privilege Escalation“ (TA0004) z rámce MITRE ATT&CK [104], která popisuje techniky, jež útočníci využívají k získání vyšších oprávnění v systému nebo síti. Jedním z příkladů je situace, kdy uživatelský účet má přístup k určitým funkcím, které by mu neměly být dostupné.

V OCI je klíčovým nástrojem pro řízení přístupu služba Identity and Access Management (IAM). IAM umožňuje definovat politiky, které určují, kdo má jaký typ přístupu k jednotlivým zdrojům v konkrétních kompartmentech. Například lze vytvořit [105] politiku, která umožní skupině uživatelů pouze čtení metadat v kompartmentu pro správu síťové konfigurace, ale nikoliv vytváření nebo mazání jednotlivých zdrojů. Tímto testem ověříme, že uživatel bez oprávnění „manage virtual-network-family“ v kompartmentu „PoC-network-cmp“ nemůže vytvořit novou VCN.

7.2.1 Příprava testovacího prostředí

Test lze provést v rámci stávající infrastruktury (vytvořené v kapitole 6) bez nutnosti vytvářet další zdroje v OCI.

7.2.2 Výsledek testu

Tabulka (Tabulka 6) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 6 Testovací scénář – Prevence vytvoření neautorizované VCN

Atribut testu	Hodnota
ID testu	SEC-NET-I-001-UNAUTHORIZED-VCN-CREATION
Typ testu	Integrity
Název scénáře	Prevence vytvoření neautorizované VCN

Popis	Pokus o vytvoření nové Virtual Cloud Network (VCN) v kompartmentu „PoC-network-cmp“, aniž by měl uživatel odpovídající oprávnění podle IAM politiky.
Úroveň hrozby	High
OCI služba	Virtual Cloud Network
Kompartiment	PoC-network-cmp
Uživatel a role	alice.newman.poc.auditor@***(PoC-auditor-group)
Metoda provedení	OCI CLI
Příkaz/kroky k provedení	<pre>oci network vcn create \ --cidr-block 10.0.0.0/16 \ --compartment-id "\$(oci iam compartment list --access-level ANY --compartment-id- in-subtree true --query "data[?name=='PoC-network-cmp'].id [0]" --raw-output)" \ --display-name "Neopravnena-VCN"</pre>
Očekávaný výsledek	Pokus o vytvoření VCN selže s chybovou zprávou o porušení IAM politik.
Skutečný výsledek	<pre>ServiceError: "code": "NotAuthorizedOrNotFound", "message": "Authorization failed or requested resource not found.",</pre>
Status (Pass/Fail)	✅ Pass
Poznámka / Komentář	Potvrzeno očekávané chování.
Datum a čas testu	13/04/2025 10:34 CET
Odkaz na OCI dokumentaci	[36], [87]

(zdroj: vlastní)

7.2.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

7.3 Testovací scénář – Prevence neoprávněné modifikace rolí

Mírnou variací předchozího scénáře je situace, kdy se útočník nejprve pokusí o změnu role či oprávnění ke svému (nebo kompromitovanému) účtu v cloudovém prostředí s cílem získat větší pravomoci. Tento případ souvisí s technikou „Account Manipulation: Additional Cloud Roles“ (T1098.003), jak je definována v rámci MITRE ATT&CK [106].

Test má za cíl ověřit úspěšné zablokování takového pokusu a potvrdit správné nastavení IAM politik a dodržování principu nejmenších oprávnění.

7.3.1 Příprava testovacího prostředí

Test lze provést v rámci stávající infrastruktury (vytvořené v kapitole 6) bez nutnosti vytvářet další zdroje v OCI.

7.3.2 Výsledek testu

Tabulka (Tabulka 7) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 7 Testovací scénář – Prevence neoprávněné modifikace rolí

Atribut testu	Hodnota
ID testu	SEC-AUTH-I-002-ROLE-ASSIGNMENT-MODIFICATION
Typ testu	Integrity
Název scénáře	Prevence neautorizované modifikace rolí
Popis	Pokus o změnu přiřazených rolí uživatelem bez administrátorských oprávnění.
Úroveň hrozby	High
OCI služba	Identity and Access Management (IAM)
Kompartment	PoC-network-cmp
Uživatel a role	alice.newman.poc.auditor@*** (PoC-auditor-group)
Metoda provedení	OCI CLI
Příkaz/kroky k provedení	<pre>oci iam policy create \ --name "Allow-Auditors-to-create-VCN" \ --description "Umožňuje skupině PoC-auditor-group spravovat síťové prostředky v kompartmentu PoC-network-cmp" \ --statements "[\"Allow group PoC-auditor-group to manage virtual-network-family in compartment PoC-network-cmp\"]" \ --compartment-id "\$(oci iam compartment list --access-level ANY --compartment-id-in-subtree true --query \"data[?name=='PoC-network-cmp'].id [0]\" --raw-output) "</pre>
Očekávaný výsledek	Akce bude zamítnuta. Systém vrátí chybu, protože uživatel nemá oprávnění měnit IAM politiky.
Skutečný výsledek	<pre>ServiceError: "code": "NotAuthorizedOrNotFound", "message": "Authorization failed or requested resource not found.",</pre>
Status (Pass/Fail)	 Pass
Poznámka / Komentář	Potvrzeno očekávané chování.

Datum a čas testu	13/04/2025 10:37 CET
Odkaz na OCI dokumentaci	[36], [87]

(zdroj: vlastní)

7.3.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

7.4 Testovací scénář – Prevence lockoutu administrátora IDCS domény

Správci domény identity (Identity Domain Administrators, IDA) disponují v prostředí OCI nejvyššími oprávněními v rámci konkrétní domény. Mají plnou správu nad uživatelskými účty, skupinami, aplikacemi i systémovým nastavením, včetně možnosti přidělovat a odebírat administrátorské role ostatním uživatelům. Tato centralizovaná pravomoc z nich činí klíčové subjekty z hlediska provozní dostupnosti i bezpečnosti.

Tento scénář má své analogie i v bezpečnostním rámci MITRE ATT&CK, konkrétně v technice „Valid Accounts: Domain Accounts“ (T1078.002), která popisuje [107] zneužití doménových účtů útočníky za účelem získání nebo udržení přístupu k systému, eskalace oprávnění či vyhnutí se detekci. Právě centralizovaná moc doménových administrátorů činí jejich účty atraktivním cílem a kritickým bodem z pohledu dostupnosti i integrity prostředí.

Nejen z těchto důvodů je zásadní, aby organizace zajistila existenci více než jednoho administrátorského účtu v každé doméně identity. V opačném případě hrozí riziko zablokování přístupu do prostředí (lock-out) v případě ztráty přístupu k jedinému aktivnímu IDA (např. při odchodu zaměstnance nebo deaktivaci účtu). Test má ověřit existenci záložního účtu doménového administrátora.

7.4.1 Příprava testovacího prostředí

Test lze provést v rámci stávající infrastruktury (vytvořené v kapitole 6) bez nutnosti vytvářet další zdroje v OCI.

7.4.2 Výsledek testu

Tabulka (Tabulka 8) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 8 Testovací scénář – Prevence lockoutu administrátora IDCS domény

Atribut testu	Hodnota
ID testu	SEC-IDC-A-001-DOMAIN-ADMIN-LOCKOUT
Typ testu	Availability
Název scénáře	Prevence lockoutu administrátora IDCS domény
Popis	Test ověřuje, zda je v doméně identity (např. Default Domain v OCI) nakonfigurováno více než jedno administrátorské konto s rolí Identity Domain Administrator. Cílem je minimalizovat riziko ztráty přístupu do domény v případě ztráty nebo deaktivace jediného administrátora.
Úroveň hrozby	Critical
OCI služba	Identity Domains (IDCS)
Kompartment	Root / Default domain
Uživatel a role	d_codl@*** (Tenancy admin)
Metoda provedení	OCI Console
Příkaz/kroky k provedení	Ověření existence záložního účtu v OCI Console navigací do „Identity / Domains / Default / domain / Security / Administrators“
Očekávaný výsledek	V systému jsou minimálně 2 účty s rolí Identity Domain Administrator, aby se předešlo ztrátě přístupu.
Skutečný výsledek	Defaultní doména obsahuje pouze jednoho administrátora (d_codl@***), záložní účet nebo role nejsou přiřazeny.
Status (Pass/Fail)	✗ Fail
Poznámka / Komentář	Je nutné přidat minimálně jednoho dalšího uživatele s rolí Identity Domain Administrator jako zálohu pro krizové scénáře (např. deaktivace účtu, odchod osoby z organizace).
Datum a čas testu	13/04/2025 11:18 CET
Odkaz na OCI dokumentaci	[36], [87]

(zdroj: vlastní)

7.4.3 Opravná opatření

Opravná opatření jsou nutná, jelikož během testu bylo zjištěno, že existuje pouze jeden IDA uživatel. Chybí záložní administrátor. Jedná se o závažné riziko, proto je doporučeno neprodleně přidat druhého administrátora.

7.5 Testovací scénář – Nouzový přístup přes Cloud Shell a EPN

Technika „Valid Accounts: Cloud Accounts“ (T1078.004) z frameworku MITRE ATT&CK popisuje [108] situace, kdy útočníci zneužívají platné přihlašovací údaje cloudových účtů k získání neoprávněného přístupu, udržení přístupu, eskalaci privilegií nebo obcházení bezpečnostních opatření. V prostředí OCI může neoprávněné získání přístupu k účtu s oprávněními pro Cloud Shell a EPN umožnit útočníkovi přístup k instancím v privátní síti, které nejsou běžně dostupné z veřejného Internetu.

Tento testovací scénář je navržen k ověření schopnosti bezpečného a kontrolovaného nouzového přístupu k instanci umístěné v privátní podsíti bez veřejné IP adresy. Prostřednictvím OCI Cloud Shellu a Ephemeral Private Network (EPN) bude simulován přístup k této instanci, což umožní posoudit efektivitu a bezpečnost tohoto přístupu. Cílem testu bude demonstrovat, že na instanci mimo Security Zone (v kořenovém kompartmentu) je možné se dostat (mimojiné) za pomoci Ephemeral Private Network přístupu z Cloud Shellu, zatímco na instanci uvnitř Security Zone nikoli.

7.5.1 Příprava testovacího prostředí

V rámci přípravy si nejprve v OCI v kompartmentu „PoC-app-cmp“ vytvoříme jako uživatel „Elias Nakamura“ (s rolí „PoC-app-admin-group“) novou soukromou VM instanci:

- Shape „VM.Standard.A1.Flex“ („Always Free-eligible“), image „Oracle Linux 8 (2025.01.31-0)“, kompartment „PoC-app-cmp“, VCN „PoC-three-tier-vcn-1“, soukromá podsít' „middle-subnet“ a dále „Encrypt this volume with a key that you manage“ s parametry Vault compartment „PoC-app-cmp“ a zvoleným vaultem a šifrovacím klíčem. SSH klíče pro přihlášení si necháme vygenerovat.

Dále si vytvoříme druhou VM instanci (mimo Security Zone):

- V kořenovém (root) kompartmentu vytvoříme pomocí nástroje „Start VCN Wizard“ s volbou „Internet Connectivity“ novou VCN „PoC-bastion-vcn-1“. Použijeme výchozí navržené hodnoty pro konfiguraci, tj. rozsah VCN „10.0.0.0/16“, CIDR pro veřejnou podsít' „10.0.0.0/24“ a soukromou podsít' „10.0.0.1/24“, Internet gateway (pro veřejnou) a NAT/Service gateway (pro soukromou) a ponecháme výchozí routovací tabulku a security list.
- Dále v soukromé podsíti „10.0.0.1/24“ vytvoříme novou VM instanci s parametry shape „VM.Standard.A1.Flex“ („Always Free-eligible“), image „Oracle Linux 8

(2025.01.31-0)“, kompartment „root“, VCN „PoC-bastion-vcn-1“, podsít' „private subnet PoC-bastion-vcn-1 (regional)“. SSH klíče pro přihlášení si necháme vygenerovat. Ostatní volby ponecháme výchozí.

7.5.2 Výsledek testu

Tabulka (Tabulka 9) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 9 Testovací scénář – Nouzový přístup přes Cloud Shell a EPN

Atribut testu	Hodnota
ID testu	SEC-NW-A-002-EMERGENCY-EPN-ACCESS
Typ testu	Availability
Název scénáře	Ověření nouzového přístupu na instanci v privátní podsíti pomocí Ephemeral Private Network
Popis	Test ověřuje funkčnost Ephemeral Private Network (EPN) v OCI pro případ nouzového přístupu na instanci umístěnou v privátní podsíti (ovšem mimo Security Zone) a bez veřejné IP adresy a zároveň blokaci téhož přístupu do jiné instance uvnitř Security Zone.
Úroveň hrozby	Medium
OCI služba	Cloud Shell + Networking (Ephemeral Private Network) + Compute + Security Zone
Kompartiment	Root + PoC-app-cmp
Uživatel a role	d_codl@*** (Tenancy admin) elias.nakamura.poc.appadm@*** (PoC-app-admin-group)
Metoda provedení	OCI Console (Cloud Shell) + SSH

Příkaz/kroky k provedení	Nejprve otestujeme instanci umístěnou v kořenovém (root) kompartmentu. Po přihlášení do OCI Console spustíme Cloud Shell. V menu Network vybereme „Ephemeral private network setup“, VCN „PoC-bastion-vcn-1“, private subnet „private subnet PoC-bastion-vcn-1“. Klikneme na „Use as active network“. V Cloud Shellu se následně pokusíme připojit k dané instanci pomocí ssh a uloženého soukromého SSH klíče: <pre>ssh -i ssh-key-2025-04-18.key opc@10.0.1.32</pre> Následně provedeme totéž pro instanci umístěnou uvnitř Security Zone v kompartmentu „PoC-app-cmp“. V menu Network vybereme „Ephemeral private network setup“, VCN „PoC-three-tier-vcn-1“, private subnet „middle-subnet“. Klikneme na „Use as active network“. V Cloud Shellu se následně pokusíme připojit k dané instanci pomocí ssh a uloženého soukromého SSH klíče: <pre>ssh -i ssh-key-2025-04-18.key opc@192.168.1.128</pre>
Očekávaný výsledek	Ephemeral Private Network session umožní bezpečný přístup na instanci mimo Security Zone bez potřeby veřejné IP adresy. Přístup bude pouze přes OCI interní síť. Pro instanci uvnitř Security Zone se přístup nezdaří.
Skutečný výsledek	<pre>d_codi@cloudshell:~ (eu-frankfurt-1)\$ ssh -i ssh-key-2025-04-18.key opc@10.0.1.32</pre> Activate the web console with: systemctl enable --now cockpit.socket <pre>[opc@sec-nw-a-002-secure-bastion-connection ~]\$ hostname sec-nw-a-002-secure-bastion-connection</pre> Last login: Sat Apr 19 14:26:57 2025 from 10.0.1.167 <pre>elias_naka@cloudshell:~ (eu-frankfurt-1)\$ ssh -i ssh-key-2025-04-18.key opc@192.168.1.128</pre> ssh: connect to host 192.168.1.128 port 22: Connection timed out
Status (Pass/Fail)	 Pass
Poznámka / Komentář	Potvrzeno očekávané chování.

Datum a čas testu	19/04/2025 16:26 CET
Odkaz na OCI dokumentaci	[109], [110]

(zdroj: vlastní)

7.5.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

7.6 Testovací scénář – Ověření Cloud Guard respondéru

Cloudová matice frameworku MITRE ATT&CK popisuje specifické techniky související s rizikem přidělování veřejných IP adres compute instancím v cloudovém prostředí. Například technika „Gather Victim Network Information: IP Addresses“ (T1590.005) popisuje [111] metody, které útočníci využívají k získání informací o IP adresách cílové organizace. Získané IP adresy mohou útočníkům pomoci odhalit další detaily o oběti, například velikost organizace, fyzickou lokalitu, poskytovatele internetových služeb nebo způsob hostování veřejně přístupné infrastruktury. Jiná technika „Exploit Public-Facing Application“ (T1190) zase uvádí [112] metody, které útočníci využívají k získání počátečního přístupu do cílového systému prostřednictvím zneužití zranitelností v aplikacích, které běží na instancích s veřejnou IP adresou.

Z těchto důvodů jsme sestavili scénář s cílem ověřit schopnost Oracle Cloud Guard detekovat přiřazení veřejné IP adresy compute instanci a automaticky na tuto událost reagovat zastavením instance.

7.6.1 Příprava testovacího prostředí

Pro tento test budeme potřebovat VM instanci s veřejnou IP adresou. Vytvoříme ji v hlavním (root) kompartmentu a umístíme do veřejné podsítě „10.0.0.0/24“, kterou již máme k dispozici z předchozího scénáře. Pro VM použijeme tyto parametry:

- Shape „VM.Standard.A1.Flex“ („Always Free-eligible“), image „Oracle Linux 8 (2025.01.31-0)“, kompartment „root“, VCN „PoC-bastion-vcn-1“, podsít’ „public subnet PoC-bastion-vcn-1 (regional)“. V sekci „Public IPv4 address“ zaškrtneme volbu „Automatically assign public IPv4 address“. SSH klíče pro přihlášení si necháme vygenerovat. Ostatní volby ponecháme výchozí.

7.6.2 Výsledek testu

Tabulka (Tabulka 10) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 10 Testovací scénář – Ověření Cloud Guard respondéru

Atribut testu	Hodnota
ID testu	SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER
Typ testu	Availability + Integrity
Název scénáře	Ověření automatické reakce Cloud Guard na přidělení veřejné IP adresy compute instanci
Popis	Test ověřuje schopnost Cloud Guard detekovat situaci, kdy je compute instanci přiřazena veřejná IP adresa (pravidlo detektoru „Compute Instance has Public IP Address“), což je v rozporu s bezpečnostními zásadami. Po detekci je automaticky spuštěn respondér, který provede zastavení instance (pomocí pravidla „Stop Compute Instance“).
Úroveň hrozby	High
OCI služba	Cloud Guard + Compute + Networking
Kompartment	Root
Uživatel a role	d_codl@*** (Tenancy admin)
Metoda provedení	OCI Console
Příkaz/kroky k provedení	Upravíme recept „PoC-responder-recipe“ respondéru pro Target „PoC-cloud-guard-root-target“ („Cloud Guard / Configuration / Targets / Target details“) a vyeditujeme pravidlo „Stop Compute Instance“. Zde nejprve přidáme požadovanou bezpečnostní politiku („Allow service cloudguard to manage instance-family in tenancy“), dále v sekci „Setting“ nastavíme „Rule trigger“ na „Execute automatically“ (a potvrdíme checkbox) a nakonec v sekci „Conditional group“ nastavíme podmínku, která vždy platí (např. „Region“, „not in“, „abc“ viz [76]), jelikož chceme, aby se respondér aktivoval vždy.
Očekávaný výsledek	Cloud Guard detekuje přiřazení veřejné IP, incident se objeví v dashboardu a respondér automaticky zastaví compute instanci.

Skutečný výsledek	Časové razítko vytvoření instance: Fri, Apr 25, 2025, 15:46:25 UTC Časové razítko detekce Cloud Guard: Fri, Apr 25, 2025, 18:03:27 UTC Časové razítko aktivace respondéru: Fri, Apr 25, 2025, 18:03:41 UTC Instance byla automaticky zastavena.
Status (Pass/Fail)	✅ Pass
Poznámka / Komentář	Potvrzeno očekávané chování.
Datum a čas testu	25/04/2025 16:46 CET
Odkaz na OCI dokumentaci	[75], [76]

(zdroj: vlastní)

7.6.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

7.7 Testovací scénář – Geolokační omezení přístupu pomocí WAF

Bezpečnostní scénář zaměřený na použití služby Web Application Firewall (WAF) v prostředí OCI přímo souvisí s technikou „Exploit Public-Facing Application“ (T1190) frameworku MITRE ATT&CK, která popisuje [112] postupy, při nichž útočníci zneužívají zranitelnosti veřejně dostupných webových aplikací k získání počátečního přístupu do systému. Nasazení WAF s restrikcemi na základě geolokace nebo IP rozsahů může významně snížit riziko takového zneužití.

Test má za cíl ověřit správné fungování WAF politik v prostředí OCI a přispět tak k posouzení odolnosti infrastruktury vůči těmto typům hrozeb.

7.7.1 Příprava testovacího prostředí

Pro tento test budeme potřebovat 2 compute VM instance s veřejnou IP adresou a OCI Public Loadbalancer. Obě instance vytvoříme z poolu instancí pomocí „Instance Configurations“, kde si nadefinujeme novou společnou šablonu s následujícími parametry:

- Shape „VM.Standard.A1.Flex“ („Always Free-eligible“), image „Oracle Linux 8 (2025.04.16-0)“, kompartment „root“, VCN „PoC-bastion-vcn-1“, podsít’ „public subnet PoC-bastion-vcn-1 (regional)“. V sekci „Public IPv4 address“ zaškrtneme volbu „Automatically assign public IPv4 address“. SSH klíče pro přihlášení si necháme vygenerovat. Ostatní volby ponecháme výchozí.

Dále na obou instancích nainstalujeme a aktivujeme webový server NGINX:

```
sudo dnf install -y nginx
sudo systemctl enable --now nginx.service
sudo systemctl status nginx
```

A povolíme síťový provoz na standardním portu 80 (webserver) v NGINX firewallu a také v příslušném security listu VCN a otestujeme.

```
sudo firewall-cmd --add-service=http --permanent
sudo firewall-cmd --reload
```

Dále vytvoříme vlastní (custom) NGINX konfigurační soubor, který zobrazí veřejnou IP adresu webového serveru (abychom věděli, na který webserver jsme aktuálně připojeni).

```
vi /srv/website/index.html
vi /usr/share/nginx/html/index.html
```

Jako poslední vytvoříme OCI Loadbalancer („Networking / Load balancers / Load balancer / Create load balancer“) s těmito parametry:

- Choose visibility type „Public“, Assign a public IP address „Ephemeral IP address“, kompartment „root“, VCN „PoC-bastion-vcn-1“, podsít „public subnet PoC-bastion-vcn-1 (regional)“. Next.
- Specify a load balancing policy „Weighted round robin“, Select backend servers / Add instances „instance vytvořené v předchozím kroku“, Port „80“, Specify health check policy (ponecháme výchozí), Security list „Automatically add security list rules“, Egress/Igress security list „Default Security List for PoC-bastion-vcn-1“, Session persistence „Disable session persistence“. Next.
- Configure listener, Specify the type of traffic your listener handles „HTTP“, Specify the port your listener monitors for ingress traffic „80“. Next.

Submit.

Provedeme otestování, že loadbalancer funguje tj. pokud zadáme v internetovém prohlížeči veřejnou adresu loadbalanceru a provedeme několikrát obnovení stránky (klávesou F5), zobrazí se obsah průběžně buď z jedné nebo druhé VM instance (webserveru).

7.7.2 Výsledek testu

Tabulka (Tabulka 11) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 11 Testovací scénář – Geolokační omezení přístupu pomocí WAF

Atribut testu	Hodnota
ID testu	SEC-WAF-A-004-RESTRICT-WEB-ACCESS
Typ testu	Integrity + Availability
Název scénáře	Geolokační omezení přístupu pomocí služby Web Application Firewall (WAF)
Popis	Test ověřuje správnou funkci WAF policy s nastaveným Access Control pravidlem pro restrikci přístupu na Load Balancer pouze ze zdrojových IP adres lokalizovaných v České republice.
Úroveň hrozby	High
OCI služba	Web Application Firewall (WAF), Load Balancer, Compute Instances, Networking
Kompartiment	Root
Uživatel a role	d_codl@*** (Tenancy admin)
Metoda provedení	OCI Console
Příkaz/kroky k provedení	Vytvoříme novou WAF policy navigací do „Identity & Security / Web Application Firewall / Create WAF policy“ v hlavním „root“ kompartimentu. Next. V sekci „Access control“ zaškrtneme volbu „Enable access control“ a pomocí „Add Access Rule“ v sekci „Condition Type“ nastavíme „Country/Region“, operátor „Not in list“ a cílovou zemi „Czechia“. V sekci „Rule action“ zvolíme „Action name“ položku „Pre-configured 401 Response Code Action“. Next. Next. V sekci „Select enforcement point“ vybereme loadbalancer vytvořený v rámci přípravné fáze. Next. Na závěr klikneme na „Create WAF policy“.
Očekávaný výsledek	Přístup na webovou aplikaci bude umožněn pouze z České republiky. Přístupy z ostatních států budou odmítnuty.

Skutečný výsledek	Pro přístup z Česka: Public IP tohoto serveru je: 138.3.245.177 Pro přístup z jiné země: { "code": "401", "message": "Unauthorized" }
Status (Pass/Fail)	✓ Pass
Poznámka / Komentář	Potvrzeno očekávané chování.
Datum a čas testu	28/04/2025 15:10 CET
Odkaz na OCI dokumentaci	[113]

(zdroj: vlastní)

7.7.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

7.8 Testovací scénář – Správa spotřeby zdrojů v OCI pomocí kvót

V prostředí OCI je efektivní správa nákladů a prevence neplánovaného [3, s. 84] překročení rozpočtu klíčová pro udržení finanční kontroly nad cloudovými zdroji. Jedním z nástrojů, který OCI poskytuje pro dosažení tohoto cíle, jsou *compartment quotas* – zásady [114], které umožňují administrátorům přesně řídit spotřebu zdrojů v jednotlivých kompartmentech. Tyto kvóty umožňují nastavit limity na počet nebo kapacitu konkrétních zdrojů, jako jsou například compute instance, v rámci definovaného kompartmentu. Tímto způsobem lze zajistit, že týmy nebo projekty nepřekročí přidělené zdroje, což pomáhá předcházet neočekávaným nákladům a podporuje dodržování rozpočtových omezení.

V tomto scénáři se zaměříme na ověření funkčnosti tím, že pomocí *compartment quotas* nastavíme maximální počet povolených compute instancí v daném kompartmentu. Následně vytvoříme jednu instanci, což by mělo proběhnout úspěšně, a poté se pokusíme vytvořit druhou instanci, která by měla být zamítnuta kvůli překročení nastaveného limitu.

7.8.1 Příprava testovacího prostředí

Test lze provést v rámci stávající infrastruktury (vytvořené v kapitole 6) bez nutnosti vytvářet další zdroje v OCI.

7.8.2 Výsledek testu

Tabulka (Tabulka 12) obsahuje přehled parametrů testu, jednotlivých kroků jeho provedení a dosaženého výsledku.

Tabulka 12 Testovací scénář – Správa spotřeby zdrojů v OCI pomocí kvót

Atribut testu	Hodnota
ID testu	SEC-GOV-A-005-COMP-QUOTA-LIMIT
Typ testu	Availability
Název scénáře	Ověření řízení limitu maximálního počtu vytvořených OCI zdrojů (instancí)
Popis	Test ověřuje správnou funkčnost omezení maximálního počtu vytvořených zdrojů (instancí) pro daný OCI kompartment (pomocí Compartment Quotas) z důvodů sledování nákladů a governance.
Úroveň hrozby	Medium
OCI služba	Governance (Compartment Quotas) + Compute
Kompartment	PoC-app-cmp
Uživatel a role	d_codl@*** (Tenancy admin) elias.nakamura.poc.appadm@*** (PoC-app-admin-group)
Metoda provedení	OCI CLI + OCI Console
Příkaz/kroky k provedení	<pre>oci limits quota create \ --name "SEC-GOV-A-004-COMP- QUOTA-LIMIT" \ --compartment-id ocidl1.tenancy.oc1..aaaaaaaahxh peqkgsrftwxjfxffiofrexn7 ipxh4rqm4zlvem 7nn2oefyaq \ --description "Max 1 instance quota" \ --statements '["set compute-core quota to 1 in compartment PoC-top-cmp:PoC-app-cmp"] '</pre>
Očekávaný výsledek	První instance se vytvoří úspěšně. Pokus o vytvoření druhé instance skončí chybou kvůli překročení compartment quota limitu.
Skutečný výsledek	The following compartment quotas were exceeded: standard-a1-core-count in policy 'ocidl1.quota. oc1..a aaaaaaawm5av4ow7tx5 vvvrwt6 gxso5q6 qatjfv72hg7luwvmv6vxx 4m4a' by 1
Status (Pass/Fail)	✅ Pass
Poznámka / Komentář	Potvrzeno očekávané chování.
Datum a čas testu	26/04/2025 11:34 CET
Odkaz na OCI dokumentaci	[114]

(zdroj: vlastní)

7.8.3 Opravná opatření

Nejsou potřeba žádná opravná opatření, test byl úspěšný.

8 VYHODNOCENÍ ÚČINNOSTI NAVRŽENÝCH OPATŘENÍ

V této kapitole shrneme výsledky bezpečnostního testování provedeného v prostředí OCI a zhodnotíme účinnost navržených bezpečnostních opatření. Zaměříme se na analýzu úspěšnosti jednotlivých scénářů, identifikujeme silné i slabé stránky implementovaných kontrol včetně rychlosti a spolehlivosti detekce a reakce na incidenty. Rovněž upozorníme na technická i procesní omezení a navrhneme konkrétní zlepšení včetně doporučení vycházejících z principu sdílené odpovědnosti a oficiálních bezpečnostních standardů Oracle.

8.1 Analýza výsledků testů

V průběhu testování bylo vyhodnoceno celkem osm bezpečnostních scénářů, pokrývajících klíčové aspekty CIA triády (Confidentiality, Integrity, Availability). Všechny testy kromě jednoho byly úspěšné (status: Pass), což dokládá, že navržená opatření fungují dle očekávání. Jediný neúspěšný test 7.4 – Prevence lockoutu administrátora IDCS domény (SEC-IDC-A-001-DOMAIN-ADMIN-LOCKOUT) odhalil závažný nedostatek – přítomnost pouze jednoho administrátora domény identity, což představuje riziko lockoutu.

Falešné poplachy (false positives) nebo nedetekované incidenty (false negatives) nebyly zaznamenány. Všechny testy potvrdily správné nastavení IAM politik, Cloud Guard detektorů a responder pravidel a nastavení kvót (compartment quotas).

8.2 Kvantitativní a kvalitativní vyhodnocení

Kvantitativně bylo provedeno celkem osm scénářů, z nichž sedm bylo úspěšně detekováno a vyhodnoceno bezpečnostními službami OCI. Jediný test (SEC-IDC-A-001-DOMAIN-ADMIN-LOCKOUT) odhalil kritickou slabinu v podobě chybějícího záložního doménového administrátora.

Za pozornost stojí výsledek testu 7.6 – Ověření Cloud Guard respondéru (SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER), kde bylo zjištěno, že detektor nereaguje okamžitě na incident přiřazení veřejné IP adresy compute instanci. Ze sekce „Skutečný výsledek“ vyplývá, že instance s veřejnou IP adresou byla vytvořena v „15:46:25 UTC“, zatímco Cloud Guard tuto skutečnost detekoval až v „18:03:27 UTC“. Z toho je patrné, že došlo k více než dvouhodinové prodlevě mezi vznikem incidentu a jeho detekcí. Tento fakt může být v reálném provozu problematický, zejména u kritických systémů. Doporučuje se

zvážit podání žádosti o zlepšení (enhancement request, ER) vůči firmě Oracle pro implementaci zkrácení reakční doby Cloud Guardu na podobné incidenty.

Další omezení byla zaznamenána u samotných responder akcí, které jsou v současnosti limitovány pevně definovanými detekčními pravidly. Například akce "Stop Compute Instance" je v dokumentaci *OCI Respond Recipes Reference* [75] dostupná pouze pro detektor typu:

- Configuration, Compute: Instance has a public IP address

Nelze ji tedy využít v jiných kritických situacích, jako je například detekce známých zranitelností (např. CVE s vysokým skóre), což značně omezuje možnosti automatizované reakce. Rozšíření podpory responder akcí pro další typy detekovaných incidentů by výrazně zvýšilo flexibilitu a použitelnost Cloud Guardu v rámci komplexního řízení bezpečnostních událostí.

Celkově lze konstatovat, že testy přispěly k ověření funkčnosti navržených bezpečnostních mechanismů a odhalily praktická omezení především u automatizovaných odpovědních mechanismů. IAM segmentace, řízení kompartmentů a síťové restriktce fungují dle očekávání. Cloud Guard se ukázal jako velmi přínosný, avšak s prostorem pro vylepšení v oblasti rychlosti detekce a rozšiřitelnosti responder akcí.

8.3 Doporučení a návrhy na zlepšení

Na základě výsledků testování a zjištěných omezení navrhujeme následující opatření pro zlepšení bezpečnostní politiky a reakční schopnosti prostředí OCI:

8.3.1 Zajištění záložního administrátora domény identity

Kritický nedostatek zjištěný v testu 7.4 – Prevence lockoutu administrátora IDCS domény (SEC-IDC-A-001-DOMAIN-ADMIN-LOCKOUT) ukazuje na potřebu mít minimálně dva správce s rolí Identity Domain Administrator. Odstranění této jednostranné závislosti sníží riziko ztráty přístupu ke klíčovým nastavením domény.

8.3.2 Zrychlení reakční doby služby Cloud Guard

Výsledky testu 7.6 – Ověření Cloud Guard respondéru (SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER) ukázaly více než dvouhodinovou prodlevu mezi vznikem incidentu (přiřazení veřejné IP) a jeho detekcí. Navrhujeme podat oficiální požadavek

(enhancement request) směrem k Oracle s cílem zkrátit tuto dobu v budoucích verzích služby.

8.3.3 Rozšíření možností použití Cloud Guard responder akcí

V současnosti lze akci „Stop Compute Instance“ využít pouze u předem definovaných typů detekcí, např. přítomnost veřejné IP adresy. Není ji však možné využít při jiných kritických incidentech (např. zjištění CVE zranitelnosti). Doporučujeme navrhnout rozšíření podpory responder akcí pro další typy incidentů formou oficiálního požadavku (enhancement request) směrem k Oracle.

8.3.4 Zohlednění nákladovosti pokročilých detektorů Cloud Guardu

Během testování bylo zjištěno, že služba Oracle Cloud Guard *Instance Security Enterprise*, která umožňuje skenování instancí na známé zranitelnosti a hrozby, je zpoplatněna částkou 0.0069 USD za uzel a hodinu [115].

Přestože Cloud Guard jako služba je dostupná bez poplatku, některé pokročilé detektory vyžadují samostatnou aktivaci a mohou mít vliv na provozní náklady. Je důležité mít tuto skutečnost na paměti při návrhu bezpečnostních politik a konzultovat cenové modely s oficiální dokumentací Oracle. Zároveň oceňujeme, že tyto funkce nejsou aktivní ve výchozím stavu, ale musí být explicitně povoleny, čímž se eliminuje riziko neúmyslného účtování.

8.3.5 Napojení Cloud Guard na centrální SIEM řešení

Doporučujeme napojení prostředí OCI na centrální SIEM (např. Splunk, ELK), což umožní hlubší analýzu a korelaci událostí napříč prostředím.

8.3.6 Zavedení automatizovaného testování politik

Vytvoření skriptů či testovacích rutin pomocí OCI CLI, Terraformu nebo jiných nástrojů výrazně zefektivní opakovanou validaci bezpečnostních opatření v prostředí.

8.3.7 Využití oficiálního bezpečnostního checklistu Oracle Cloud Infrastructure

Pro systematické dosažení vyšší úrovně zabezpečení a připravenosti na potenciální hrozby v prostředí OCI doporučujeme využít oficiální [8] bezpečnostní checklist poskytovaný společností Oracle, který je strukturován do následujících dvanácti klíčových oblastí:

- Autentizace (Správa uživatelských přihlašovacích údajů)

- Autorizace (Řízení oprávnění ke cloudovým zdrojům na základě IAM politik)
- Federace identit (Podpora federace identit s externími poskytovateli)
- Izolace zdrojů (Oddělení a organizace cloudových zdrojů pomocí kompartmentů)
- Síťová bezpečnost (Zajištění síťové bezpečnosti)
- Bezpečnost výpočetních instancí (Zabezpečení přístupu k výpočetním instancím)
- Bezpečnost na úrovni služby (Bezpečnostní opatření pro jednotlivé služby OCI)
- Ochrana dat
- Správa, audit a monitoring
- Řízení a reakce na bezpečnostní incidenty (Prevence bezpečnostních incidentů)
- Soulad s regulacemi a zabezpečení aplikací
- Odolnost provozu a kontinuita podnikání (Pravidelné testování obnovy po havárii)

Níže uvedená tabulka (Tabulka 13) zahrnuje seznam kroků pro oblast autentizace.

Tabulka 13 Bezpečnostní checklist pro OCI – Autentizace

#	1. Autentizace Bezpečnostní opatření a doporučení	Hotovo?
1	Identifikujte uživatele, kteří potřebují přístup k Oracle Cloud Infrastructure.	☐
2	Používejte jedinečná a složitá hesla.	☐
3	Provádějte rotaci hesel a API klíčů každých 90 dnů nebo častěji.	☐
4	Zajistěte, aby přihlašovací údaje nebyly pevně uloženy v softwaru nebo uváděny v dokumentaci.	☐
5	Nesdílejte jeden uživatelský účet mezi více uživateli.	☐
6	Implementujte mechanismy pro okamžité zablokování přístupu k tenancy, když zaměstnanec opustí organizaci.	☐
7	Pravidelně kontrolujte členství uživatelů ve skupinách v IAM a odstraňujte uživatele, kteří přístup nepotřebují.	☐
8	Přihlašovací údaje správce tenancy používejte pouze v naléhavých případech, ne pro běžnou denní práci.	☐
9	Pravidelně kontrolujte protokoly auditu (audit logs) týkající se činnosti správců.	☐
10	Používejte vícefaktorovou autentizaci (MFA).	☐
11	Sledujte protokoly auditu pro přístupy od výchozího správce tenancy a změny ve skupině správců, abyste zachytili neoprávněné akce.	☐

(zdroj: [8])

ZÁVĚR

Tato diplomová práce se zabývala komplexním posouzením bezpečnostních opatření v prostředí Oracle Cloud Infrastructure (OCI) s důrazem na jejich efektivní implementaci v podnikové praxi. Práce propojila teoretické poznatky z oblasti cloudové bezpečnosti s praktickým ověřením v rámci navržených testovacích scénářů, přičemž vycházela z uznávaných rámců (například CIS, NIST, MITRE ATT&CK) i z konkrétních doporučení společnosti Oracle.

V teoretické části byla provedena podrobná analýza modelu sdílené odpovědnosti a hlavních bezpečnostních služeb dostupných v OCI. Byly popsány principy zabezpečení prostřednictvím kompartmentů, správné správy identit a přístupových práv, šifrování dat v různých stavech, automatizovaného monitoringu a detekce incidentů. Pozornost byla věnována i procesu řízení zranitelností, aplikaci bezpečnostních zón (Security Zones) a využití nativních nástrojů, jako je Oracle Cloud Guard.

Praktická část práce byla zaměřena na vytvoření a otestování sady bezpečnostních scénářů v prostředí Proof-of-Concept. Tyto testy ověřily účinnost navržených opatření vůči reálným hrozbám a simulovaným incidentům – například pokusům o eskalaci privilegií, vystavení instancí veřejným IP adresám, detekci zranitelností nebo automatickou reakci na bezpečnostní incidenty pomocí responderů Cloud Guardu. Výsledky prokázaly, že správně nastavená bezpečnostní opatření významně snižují riziko úspěšného útoku i rozsah dopadů případných incidentů. Během testování byla identifikována také určitá omezení – například zpoždění v detekci některých incidentů Cloud Guardem, omezená možnost automatických akcí pro vybrané typy incidentů, nebo nutnost aktivace některých pokročilých funkcí jako placených služeb (Cloud Guard Instance Security Enterprise). Tyto skutečnosti potvrzují význam pečlivého plánování bezpečnostní architektury a průběžného monitoringu nejen z hlediska technického, ale také provozního a finančního.

Některé zjištěné nedostatky, konkrétně například neúspěšný test v kapitole 7.4 (SEC-IDC-A-001-DOMAIN-ADMIN-LOCKOUT), je nutné interpretovat v kontextu principu sdílené odpovědnosti mezi poskytovatelem cloudové služby (Oracle) a jejím uživatelem (tenantem). Zatímco Oracle poskytuje nástroje a architekturu pro správu identit a řízení přístupu, odpovědnost za správnou konfiguraci účtů, včetně zajištění dostatečného počtu administrátorů domény identity, zůstává plně na straně zákazníka. Tento test tak neodhalil technický nedostatek v platformě samotné, ale spíše procesní pochybení na straně uživatele

cloudového prostředí. Výsledky testování tak ukazují, že vysoká míra bezpečnosti v cloudu je dosažitelná pouze při správném pochopení a uplatnění role zákazníka v rámci celkového bezpečnostního modelu a že pouze kombinace technických opatření, procesního řízení a pravidelného auditu může zajistit odpovídající úroveň ochrany podnikového prostředí.

Přínosem práce je nejen detailní metodika návrhu a testování bezpečnostních opatření v OCI, ale i konkrétní doporučení pro jejich efektivní implementaci, včetně odkazu na checklisty, které mohou sloužit jako základ pro bezpečnostní audity či interní směrnice.

Závěrem lze konstatovat, že Oracle Cloud Infrastructure poskytuje robustní platformu s rozsáhlými možnostmi bezpečnostní konfigurace, nicméně efektivní ochrana závisí na znalostech, pečlivosti a odpovědnosti každé organizace. Práce tak otevírá prostor pro další výzkum zaměřený například na automatizaci bezpečnostních kontrol, rozšířenou integraci s dalšími nástroji SIEM/SOAR či optimalizaci nákladů spojených s provozem bezpečnostních funkcí v cloudu.

SEZNAM POUŽITÉ LITERATURY

- [1] EDWARDS, Dr. Jason. Cloud Security. In: *Mastering Cybersecurity*. Berkeley, CA: Apress, 2024. ISBN 979-8-8688-0296-6. Dostupné z: doi:10.1007/979-8-8688-0297-3_8.
- [2] COCHRAN, Kodi A. Securing the Cloud: A Comprehensive Guide to Cloud Security. In: *Cybersecurity Essentials*. Berkeley, CA: Apress, 2024, ISBN 979-8-8688-0431-1. Dostupné z: doi:10.1007/979-8-8688-0432-8_12.
- [3] KAVIS, Michael. *Architecting the Cloud: design decisions for Cloud computing service models (SaaS, PaaS, and IaaS)*. Hoboken, New Jersey: Wiley, c 2014. Wiley CIO series. ISBN 1118617614.
- [4] MELL, Peter a Tim GRANCE. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. The NIST Definition of Cloud Computing. *Computer Security Resource Center*. Online. September 2011 [cit. 2025-01-26]. Dostupné z: <https://csrc.nist.gov/pubs/sp/800/145/final>
- [5] ISACA. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*. Online. Semantic Scholar. 2011. Dostupné z: <https://api.semanticscholar.org/CorpusID:117137649>. [cit. 2025-02-01].
- [6] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 22123-1:2023. *Information technology — Cloud computing Part 1: Vocabulary*. Online. 2023 [cit. 2025-01-26]. Dostupné z: <https://www.iso.org/standard/82758.html>
- [7] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. ISO/IEC 22123-2:2023. *Information technology — Cloud computing Part 2: Concepts*. Online. 2023 [cit. 2025-01-26]. Dostupné z: <https://www.iso.org/standard/80351.html>
- [8] ORACLE CORPORATION. *Security checklist for Oracle Cloud Infrastructure*. Online. Oracle Help Center: Solution Playbooks. 2020. Dostupné z: <https://docs.oracle.com/en/solutions/oci-security-checklist/#GUID-44B3A191-99B1-446E-BFE2-B93C6C60ED65>. [cit. 2025-03-30].
- [9] ORACLE CORPORATION. *Oracle Cloud Infrastructure (OCI) and the United Kingdom National Cyber Security Centre Cloud Security Principles (NCSC)*. Online. 2020. Dostupné z: <https://www.oracle.com/a/ocom/docs/ncsc-cloud-security-principles.pdf>. [cit. 2025-03-30].

- [10] PUMVARAPRUEK, Nuttapon a Twittie SENIVONGSE. Classifying cloud provider security conformance to cloud controls matrix. In: *2014 11th International Joint Conference on Computer Science and Software Engineering (JCSSE)*. Online. IEEE, 2014, s. 268-273 [cit. 2025-05-22]. ISBN 978-1-4799-5822-1. Dostupné z: doi:10.1109/JCSSE.2014.6841879
- [11] CLOUD SECURITY ALLIANCE (CSA). *Cloud Controls Matrix (CCM)*. CSA. Online. 2021 [cit. 2025-05-22]. Dostupné z: <https://cloudsecurityalliance.org/research/cloud-controls-matrix>
- [12] ROGACH, Yana. *Oracle Cloud Infrastructure publishes updated CAIQ v4*. Online. Oracle Cloud Infrastructure Blog. 2023. Dostupné z: <https://blogs.oracle.com/cloud-infrastructure/post/oracle-cloud-infrastructure-publishes-updated-caiq-v4>. [cit. 2025-04-27].
- [13] HARANAS, Mark. *Cloud Market Share For \$84B Q3 2024: AWS, Microsoft, Google Cloud Lead*. Online. Synergy Research. 2024. Dostupné z: <https://www.crn.com/news/cloud/2024/cloud-market-share-for-84b-q3-2024-aws-microsoft-google-lead>. [cit. 2025-02-02].
- [14] SYNERGY RESEARCH GROUP. *Cloud Market Growth Surge Continues in Q3*. Online. Growth Rate Increases for the Fourth Consecutive Quarter | Synergy Research Group. 2024. Dostupné z: <https://www.srgresearch.com/articles/cloud-market-growth-surge-continues-in-q3-growth-rate-increases-for-the-fourth-consecutive-quarter>. [cit. 2025-02-02].
- [15] CONTRIBUTORS, Wikipedia. *Oracle Corporation*. In: *Wikipedia, The Free Encyclopedia*. Online. 2025 [cit. 2025-05-22]. Dostupné z: https://en.wikipedia.org/wiki/Oracle_Corporation
- [16] METZ, Cade. Ellison Answers Benioff with Oracle Cloud. *WIRED*. Online. 2011 [cit. 2025-05-22]. Dostupné z: <https://www.wired.com/2011/10/ellison-answers-benioff-with-oracle-cloud/>
- [17] HARRISON, Guy. Oracle's Public Cloud. *Database Trends and Applications*. Online. 2012 [cit. 2025-05-22]. Dostupné z: <https://www.dbta.com/Columns/Applications-Insight/Oracles-Public-Cloud-79723.aspx>

- [18] Oracle Becomes Corporate Sponsor of OpenStack Foundation. *Database Trends and Applications*. Online. 2014 [cit. 2025-05-22]. Dostupné z: <https://www.dbta.com/Editorial/News-Flashes/Oracle-Becomes-Corporate-Sponsor-of-OpenStack-Foundation-93748.aspx>
- [19] LEUNG, Leo. *Oracle Bare Metal Cloud Services Are Now Available*. Online. Oracle Cloud Infrastructure Blog. Dostupné z: <https://blogs.oracle.com/cloud-infrastructure/post/oracle-bare-metal-cloud-services-are-now-available>. [cit. 2025-01-31].
- [20] STEELE, Colin. *Introducing the Generation 2 Cloud at Oracle OpenWorld 2018*. Online. Oracle Cloud Infrastructure Blog. 2018. Dostupné z: <https://blogs.oracle.com/cloud-infrastructure/post/introducing-the-generation-2-cloud-at-oracle-openworld-2018>. [cit. 2025-01-31].
- [21] ORACLE CORPORATION. *Oracle Cloud Compliance*. Online. Oracle. 2025. Dostupné z: <https://www.oracle.com/corporate/cloud-compliance/>. [cit. 2025-01-31].
- [22] ORACLE CORPORATION. *Overview of Functions*. Oracle Cloud Infrastructure Documentation. Online. 2025 [cit. 2025-05-22]. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Functions/Concepts/functionsoverview.htm>
- [23] CONTRIBUTORS, Wikipedia. *Oracle Cloud*. In: *Wikipedia, The Free Encyclopedia*. Online. [cit. 2025-05-22]. Dostupné z: https://en.wikipedia.org/wiki/Oracle_Cloud
- [24] ORACLE CORPORATION. *Public Cloud Regions*. Online. Oracle. 2025. Dostupné z: <https://www.oracle.com/cloud/public-cloud-regions/>. [cit. 2025-01-30].
- [25] ORACLE CORPORATION. *Government Cloud*. Online. Oracle. 2025. Dostupné z: <https://www.oracle.com/government/govcloud/>. [cit. 2025-01-30].
- [26] ORACLE CORPORATION. *Always Free Resources*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/FreeTier/freetier_topic-Always_Free_Resources.htm. [cit. 2025-03-28].
- [27] ORACLE CORPORATION. *Oracle Cloud Infrastructure Free Tier*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/FreeTier/freetier.htm>. [cit. 2025-03-28].

- [28] ORACLE CORPORATION. *OCI Price List*. Online. Oracle. 2025. Dostupné z: <https://www.oracle.com/cloud/price-list/>. [cit. 2025-03-28].
- [29] ORACLE CORPORATION. *Universal Credits*. Online. Oracle. 2024. Dostupné z: <https://www.oracle.com/cloud/universal-credits/>. [cit. 2025-03-28].
- [30] ORACLE CORPORATION. *Oracle Customer Success Services*. Oracle.. Online. [cit. 2025-05-22]. Dostupné z: <https://www.oracle.com/customer-success/>
- [31] ORACLE CORPORATION. *Oracle Cloud Infrastructure Security Architecture*. Online. 2024 [cit. 2025-05-22]. Dostupné z: <https://www.oracle.com/uk/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf>
- [32] ORACLE CORPORATION. *Accessing Oracle Cloud Infrastructure*. Oracle Cloud Infrastructure Documentation. Online. 2024 [cit. 2025-05-22]. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/baremetalintro_topic-Accessing_Oracle_Cloud_Infrastructure.htm
- [33] ORACLE CORPORATION. *Regions and Availability Domains*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/General/Concepts/regions.htm>. [cit. 2025-02-10].
- [34] ORACLE CORPORATION. *Physical Architecture Concepts*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/GSG/Concepts/concepts-physical.htm>. [cit. 2025-02-10].
- [35] ORACLE CORPORATION. *Overview of Identity and Access Management*. Oracle Cloud Infrastructure Documentation. Online. 2025 [cit. 2025-05-22]. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/overview.htm>
- [36] ORACLE CORPORATION. *Policy Syntax*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/policysyntax.htm>. [cit. 2025-04-26].
- [37] ORACLE CORPORATION. *Object Storage Data Encryption*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/Object/Tasks/encryption.htm>. [cit. 2025-03-02].

- [38] ORACLE CORPORATION. *Key Management*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.public.content.oci.oraclecloud.com/en-us/iaas/Content/KeyManagement/Concepts/keyoverview.htm>. [cit. 2025-03-02].
- [39] ORACLE CORPORATION. *Dedicated KMS*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/KeyManagement/Tasks/dedicated_kms.htm. [cit. 2025-03-02].
- [40] ORACLE CORPORATION. *External Key Management Service*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/KeyManagement/Tasks/external_key_management.htm. [cit. 2025-03-02].
- [41] ORACLE CORPORATION. *Using In-transit TLS Encryption*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/File/Tasks/intransitencryption.htm>. [cit. 2025-03-02].
- [42] WILLIAMS, Alan. *Announcing support for TLS 1.3 in Oracle Database 23ai*. Online. Oracle Database Insider. 2024. Dostupné z: <https://blogs.oracle.com/database/post/announcing--tls13>. [cit. 2025-03-02].
- [43] SUSE. *AMD Secure Encrypted Virtualization (AMD-SEV) Guide*. Online. SUSE. 2025. Dostupné z: <https://documentation.suse.com/sles/12-SP5/html/SLES-amd-sev/index.html>. [cit. 2025-03-02].
- [44] ORACLE CORPORATION. *Confidential Computing*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Compute/References/confidential_compute.htm#confidential_compute_coco_supported_shapes. [cit. 2025-03-02].
- [45] ORACLE CORPORATION. *Networking Overview*. Oracle Cloud Infrastructure Documentation. Online. [cit. 2025-02-22]. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/overview.htm>
- [46] ORACLE CORPORATION. *Scenario C: Public and Private Subnets with a VPN*. Oracle Cloud Infrastructure Documentation. Online. 2025 [cit. 2025-02-22]. Dostupné z: <https://docs.oracle.com/en->

us/iaas/Content/Network/Tasks/scenarioc.htm#Scenario_C_Public_and_Private_Subnets_with_a_VPN

- [47] ORACLE CORPORATION. *Security Rules*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/securityrules.htm#stateful>. [cit. 2025-05-22].
- [48] ORACLE CORPORATION. *Access to Oracle Services: Service Gateway*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Network/Tasks/servicegateway.htm>. [cit. 2025-05-22].
- [49] ORACLE CORPORATION. *Bastion Overview*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Bastion/Concepts/bastionoverview.htm?utm_source=chatgpt.com. [cit. 2025-04-27].
- [50] ORACLE CORPORATION. *Overview of Web Application Firewall*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/WAF/Concepts/overview.htm>. [cit. 2025-03-02].
- [51] WEIDMAN, Georgia. *Penetration testing: a hands-on introduction to hacking*. San Francisco, CA: No Starch Press, c[2014]. ISBN 1593275641.
- [52] ORACLE CORPORATION. *Supported Protection Rules*. Oracle Cloud Infrastructure Documentation. Online. 2023 [cit. 2025-05-22]. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/WAF/Reference/protectionruleids.htm#Supported_Protection_Rules
- [53] ORACLE CORPORATION. *Custom Protection Rules*. Oracle Cloud Infrastructure Documentation. Online. [cit. 2025-05-22]. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/WAF/Tasks/customprotectionrules.htm>
- [54] ORACLE CORPORATION. *Layer 7 DDoS Mitigation*. Oracle Cloud Infrastructure Documentation. Online. 2024 [cit. 2025-05-22]. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/WAF/Concepts/ddos.htm>
- [55] ORACLE CORPORATION. *Network Firewall*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/network-firewall/home.htm>. [cit. 2025-03-02].

- [56] ORACLE CORPORATION. *Network Firewall*. Online. Oracle United Kingdom. 2025. Dostupné z: <https://www.oracle.com/uk/cloud/networking/network-firewall/>. [cit. 2025-04-27].
- [57] ORACLE CORPORATION. *Overview of Zero Trust Packet Routing*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/zero-trust-packet-routing/overview.htm#overview-zero-trust-packet-routing>. [cit. 2025-04-27].
- [58] GILMAN, Evan a BARTH, Doug. *Zero Trust Networks: Building Secure Systems in Untrusted Networks*. Springfield: O'Reilly, 2017. ISBN 9781491962190.
- [59] ORACLE CORPORATION. *Overview of Monitoring*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Monitoring/Concepts/monitoringoverview.htm>. [cit. 2025-03-02].
- [60] ORACLE CORPORATION. *Logging Overview*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Logging/Concepts/loggingoverview.htm>. [cit. 2025-03-02].
- [61] ORACLE CORPORATION. *Contents of an Audit Log Event*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Audit/Reference/logeventreference.htm>. [cit. 2025-05-22].
- [62] ORACLE CORPORATION. *Audit Log Retention Period*. Online. Oracle Cloud Infrastructure Documentation. 2023. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Audit/Tasks/settingretentionperiod.htm>. [cit. 2025-03-02].
- [63] ORACLE CORPORATION. *Cloud Guard*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/cloud-guard/home.htm>. [cit. 2025-03-02].
- [64] ORACLE CORPORATION. *Overview of Threat Intelligence*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/threat-intel/using/overview.htm>. [cit. 2025-03-15].
- [65] ORACLE CORPORATION. *Overview of Security Zones*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/security-zone/using/security-zones.htm>. [cit. 2025-03-02].

- [66] SHOSTACK, Adam. *Threat Modeling: Designing for Security*. New Jersey: Wiley, c 2014. ISBN 9781118809990.
- [67] CLOUD SECURITY ALLIANCE (CSA). *Top Threats to Cloud Computing 2024*. Online. CSA. 2024. Dostupné z: <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-2024>. [cit. 2025-03-02].
- [68] EUROPEAN UNION AGENCY FOR NETWORK AND INFORMATION SECURITY (ENISA). *ENISA Threat Landscape 2024*. Online. ENISA. 2024. Dostupné z: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>. [cit. 2025-03-02].
- [69] MITRE ATT&CK. *Cloud Matrix*. Online. MITRE ATT. 2025. Dostupné z: <https://attack.mitre.org/matrices/enterprise/cloud/>. [cit. 2025-03-02].
- [70] ORACLE CORPORATION. *Cloud Guard Features*. Online. Oracle. 2024. Dostupné z: <https://www.oracle.com/security/cloud-security/cloud-guard/features/>. [cit. 2025-03-02].
- [71] ORACLE CORPORATION. *What Is Cloud Security Posture Management (CSPM)?* Online. Oracle Česká Republika. 2021. Dostupné z: <https://www.oracle.com/cz/security/cloud-security/what-is-cspm/>. [cit. 2025-03-15].
- [72] ORACLE CORPORATION. *Cloud Guard Concepts*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/cloud-guard/using/cg-concepts.htm>. [cit. 2025-05-22].
- [73] ORACLE CORPORATION. *Detector Recipe Reference*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/cloud-guard/using/detect-recipes.htm>. [cit. 2025-05-22].
- [74] ORACLE CORPORATION. *About Threat Detector*. Online. Oracle Cloud Infrastructure Documentation. 2023. Dostupné z: <https://docs.oracle.com/en-us/iaas/cloud-guard/using/threats-about.htm#threats-about>. [cit. 2025-03-02].
- [75] ORACLE CORPORATION. *Responder Recipe Reference*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/cloud-guard/using/respond-recipes-reference.htm#respond-recipes-reference>. [cit. 2025-04-26].

- [76] ORACLE CORPORATION. *Editing Responder Rule Settings in an OCI Target's Recipes*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/cloud-guard/using/targets-modify-rules-respond.htm#targets-modify-rules-respond>. [cit. 2025-04-26].
- [77] ORACLE CORPORATION. *Cloud Guard FAQ*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://www.oracle.com/uk/security/cloud-security/cloud-guard/faq/>. [cit. 2025-03-16].
- [78] ORACLE CORPORATION. *Oracle Threat Intelligence Service FAQ*. Online. Oracle Threat Intelligence Service. 2025. Dostupné z: <https://www.oracle.com/security/cloud-security/threat-intelligence-service/faq/>. [cit. 2025-03-15].
- [79] ORACLE CORPORATION. *Vulnerability Scanning Overview*. Online. Oracle Cloud Infrastructure Documentation. 2023. Dostupné z: <https://docs.oracle.com/en-us/iaas/scanning/using/overview.htm>. [cit. 2025-03-16].
- [80] ORACLE CORPORATION. *Listing Vulnerability Reports*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/scanning/using/view-host-vulnerabilities-report.htm#view_host_vulnerabilities_report. [cit. 2025-05-22].
- [81] CENTER FOR INTERNET SECURITY (CIS). *CIS OCI Foundations Benchmark*. Online. CIS. 2024. Dostupné z: https://www.cisecurity.org/benchmark/oracle_cloud. [cit. 2025-03-29].
- [82] ORACLE CORPORATION. *Deploy a secure landing zone that meets the CIS OCI Foundations Benchmark*. Online. Oracle Help Center. 2025. Dostupné z: <https://docs.oracle.com/en/solutions/cis-oci-benchmark/index.html>. [cit. 2025-03-29].
- [83] CENTER FOR INTERNET SECURITY (CIS). *CIS Hardened Images on Oracle Cloud*. Online. CIS. 2024. Dostupné z: <https://www.cisecurity.org/cis-hardened-images/oracle/>. [cit. 2025-03-29].
- [84] ORACLE CORPORATION. *Securing Your Tenancy*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Security/Tasks/securing_your_tenancy.htm. [cit. 2025-03-29].

- [85] ORACLE CORPORATION. *What is the tenancy home region? How do I find my tenancy home region?* Online. Oracle Cloud Infrastructure Documentation: Frequently Asked Questions. 2024. Dostupné z: <https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/GSG/Reference/faq.htm>. [cit. 2025-03-29].
- [86] ORACLE CORPORATION. *Managing Identity Domains*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Identity/domains/overview.htm>. [cit. 2025-03-29].
- [87] ORACLE CORPORATION. *Well-architected framework for Oracle Cloud Infrastructure*. Online. Oracle Help Center. 2024. Dostupné z: <https://docs.oracle.com/en/solutions/oci-best-practices/manage-identities-and-authorization.html>. [cit. 2025-03-29].
- [88] ORACLE CORPORATION. *Learn Best Practices for Setting Up Your Tenancy*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: <https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/GSG/Concepts/settinguptenancy.htm>. [cit. 2025-03-29].
- [89] ORACLE CORPORATION. *OCI Architecture Diagram Toolkits*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/General/Reference/graphicsfordiagrams.htm>. [cit. 2025-04-02].
- [90] ORACLE CORPORATION. *Securing IAM*. Online. Oracle Cloud Infrastructure Documentation. 2023. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Security/Reference/iam_security.htm. [cit. 2025-03-29].
- [91] ORACLE CORPORATION. *Security Zone Policies*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/security-zone/using/security-zone-policies.htm>. [cit. 2025-03-29].
- [92] ORACLE CORPORATION. *Security Services*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Security/Concepts/security_features.htm#Security_Zones_Service. [cit. 2025-03-29].
- [93] ORACLE CORPORATION. *Enabling Cloud Guard in your Tenancy*. Online. Oracle Help Center: Research. 2023. Dostupné z:

- <https://docs.oracle.com/en/programs/research/setting-up-cloud-guard/>. [cit. 2025-03-29].
- [94] ORACLE CORPORATION. *Overview of Block Volume*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Block/Concepts/overview.htm#Overview_of_Block_Volume. [cit. 2025-04-03].
- [95] ORACLE CORPORATION. *Overview of Object Storage*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Object/Concepts/objectstorageoverview.htm#overview>. [cit. 2025-04-03].
- [96] ORACLE CORPORATION. *Overview of Archive Storage*. Online. Oracle Cloud Infrastructure Documentation. 2023. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Archive/Concepts/archivestorageoverview.htm#Overview_of_Archive_Storage. [cit. 2025-04-03].
- [97] ORACLE CORPORATION. *Overview of File Storage*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/File/Concepts/filestorageoverview.htm#Overview_of_File_Storage. [cit. 2025-04-03].
- [98] ORACLE CORPORATION. *Protecting Data on NVMe Devices*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Compute/References/nvmedeviceinformation.htm>. [cit. 2025-04-03].
- [99] ORACLE CORPORATION. *Compliance Checking Script*. Online. GitHub. 2025. Dostupné z: <https://github.com/oci-landing-zones/oci-cis-landingzone-quickstart/blob/main/compliance-script.md>. [cit. 2025-03-29].
- [100] ORACLE CORPORATION. *OCI Core Landing Zone*. Online. GitHub: [oci-landing-zones/terraform-oci-core-landingzone](https://github.com/oci-landing-zones/terraform-oci-core-landingzone). 2025. Dostupné z: <https://github.com/oci-landing-zones/terraform-oci-core-landingzone>. [cit. 2025-03-31].
- [101] ORACLE CORPORATION. *Identity Domains With the "Security Policy for OCI Console" Sign-On Policy*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/Identity/Concepts/identitydomains.htm#Identity_Domains_With_the_Security_Policy_for_OCI_Console_Sign-On_Policy.

us/iaas/Content/Security/Reference/iam_security_topic-iam_mfa_identity_domains_signon_policy.htm. [cit. 2025-03-26].

- [102] MITRE ATT&CK. *T1530: Data from Cloud Storage*. Online. MITRE ATT. 2024. Dostupné z: <https://attack.mitre.org/techniques/T1530/>. [cit. 2025-04-12].
- [103] ORACLE CORPORATION. *Securing Object Storage*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: https://docs.public.oneportal.content.oci.oraclecloud.com/en-us/iaas/Content/Security/Reference/objectstorage_security.htm. [cit. 2025-04-12].
- [104] MITRE ATT&CK. *TA0004: Privilege Escalation*. Online. MITRE ATT. 2018. Dostupné z: <https://attack.mitre.org/tactics/TA0004/>. [cit. 2025-04-12].
- [105] ORACLE CORPORATION. *Access Control*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Network/Concepts/accesscontrol.htm#Policies>. [cit. 2025-04-12].
- [106] MITRE ATT&CK. *T1098.003: Account Manipulation: Additional Cloud Roles: Additional Cloud Roles*. Online. MITRE ATT. 2020. Dostupné z: <https://attack.mitre.org/techniques/T1098/003/>. [cit. 2025-04-12].
- [107] MITRE ATT&CK. *T1078.002: Valid Accounts: Domain Accounts*. Online. MITRE ATT. 2023. Dostupné z: <https://attack.mitre.org/techniques/T1078/002/>. [cit. 2025-04-13].
- [108] MITRE ATT&CK. *T1078.004: Valid Accounts: Cloud Accounts: Cloud Accounts*. Online. MITRE ATT. 2024. Dostupné z: <https://attack.mitre.org/techniques/T1078/004/>. [cit. 2025-04-19].
- [109] SERGIO J CASTRO. *How to access Compute Instances in a Private Subnet with the Oracle Cloud Shell*. Online. Oracle University Blog. 2022. Dostupné z: <https://blogs.oracle.com/oracleuniversity/post/access-compute-instances-oracle-cloud-shell>. [cit. 2025-04-19].
- [110] ORACLE CORPORATION. *Cloud Shell Networking*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/API/Concepts/cloudshellintro_topic-Cloud_Shell_Networking.htm. [cit. 2025-04-19].

- [111] MITRE ATT&CK. *T1590.005: Gather Victim Network Information: IP Addresses*. Online. MITRE ATT. 2025. Dostupné z: <https://attack.mitre.org/techniques/T1590/005/>. [cit. 2025-04-26].
- [112] MITRE ATT&CK. *T1190: Exploit Public-Facing Application*. Online. MITRE ATT. 2025. Dostupné z: <https://attack.mitre.org/techniques/T1190/>. [cit. 2025-04-26].
- [113] ORACLE CORPORATION. *Understanding Conditions*. Online. Oracle Cloud Infrastructure Documentation. 2024. Dostupné z: https://docs.oracle.com/en-us/iaas/Content/WAF/Concepts/understanding_conditions.htm. [cit. 2025-04-28].
- [114] ORACLE CORPORATION. *Overview of Compartment Quotas*. Online. Oracle Cloud Infrastructure Documentation. 2025. Dostupné z: <https://docs.oracle.com/en-us/iaas/Content/Quotas/Concepts/resourcequotas.htm>. [cit. 2025-04-26].
- [115] ORACLE CORPORATION. *Cloud Security Pricing*. Online. Oracle United Kingdom. 2025. Dostupné z: <https://www.oracle.com/uk/security/cloud-security/pricing/>. [cit. 2025-05-11].

SEZNAM OBRÁZKŮ

Obrázek 1: SPI model cloud computingu	19
Obrázek 2: Security IN the Cloud vs. OF the Cloud	21
Obrázek 3: Model sdílené odpovědnosti podle modelu služeb.....	22
Obrázek 4: Typy regionů Oracle Cloud Infrastructure (OCI) v Evropě	29
Obrázek 5: Přehled OCI regionů ve světě.....	33
Obrázek 6: Ukázka základní síťové topologie v OCI	37
Obrázek 7: Cloud Guard – Centrální konzole.....	42
Obrázek 8: Cloud Guard – OCI Configuration Detector Recipe (Oracle managed)	51
Obrázek 9: Threat Monitoring – Detekce výskytu a klasifikace skóre	53
Obrázek 10: Threat Intelligence – Vyhledávání v databázi Threat Indicator	54
Obrázek 11: OCI Vulnerability Scanning Service – Nalezené CVE zranitelnosti	56
Obrázek 12: PoC – OCI diagram (třívrstvá aplikační topologie)	71
Obrázek 13: Bezpečnostní politika „Security Policy for OCI Console“	73
Obrázek 14: Editace MFA pravidla „Prompt for an additional factor“	74
Obrázek 15: PoC – Vytvořené IAM prvky (Enclosing Compartment)	75
Obrázek 16: PoC – Vytvořené IAM prvky (Nested Compartments).....	75
Obrázek 17: PoC – Vytvořené IAM prvky (Groups).....	76
Obrázek 18: PoC – Vytvořené IAM prvky (Security Policies)	76
Obrázek 19: PoC – Aktivace CSPM (Security Zone).....	77
Obrázek 20: PoC – Aktivace CSPM (Cloud Guard).....	78
Obrázek 21: PoC – Aktivace CSPM (Vulnerability Scanning Service)	78
Obrázek 22: PoC – Zabezpečení workloadů (VCN).....	79
Obrázek 23: PoC – Zabezpečení workloadů (Subnets)	79
Obrázek 24: PoC – Zabezpečení workloadů (Security list).....	79
Obrázek 25: PoC – Ostatní služby a zdroje (Notifications).....	80
Obrázek 26: PoC – Ostatní služby a zdroje (Alarms).....	81
Obrázek 27: PoC – Ostatní služby a zdroje (Budget)	81
Obrázek 28: PoC – Ostatní služby a zdroje (Cost Tracking Tags)	82
Obrázek 29: PoC – Ostatní služby a zdroje (Flow Logs)	83
Obrázek 30: PoC – Spuštění CIS Compliance Checker	83
Obrázek 31: PoC – Revize výsledků CIS Compliance Checker.....	84

SEZNAM TABULEK

Tabulka 1 Největší poskytovatelé cloudu dle tržního podílu v Q3 2024.....	24
Tabulka 2 CSA – Největší hrozby cloud computingu v roce 2024	44
Tabulka 3 PoC – Návrh infrastruktury	68
Tabulka 4 PoC – Název tenancy a OCID	72
Tabulka 5 Testovací scénář – Prevence vytvoření veřejného bucketu	86
Tabulka 6 Testovací scénář – Prevence vytvoření neautorizované VCN.....	87
Tabulka 7 Testovací scénář – Prevence neoprávněné modifikace rolí	89
Tabulka 8 Testovací scénář – Prevence lockoutu administrátora IDCS domény.....	90
Tabulka 9 Testovací scénář – Nouzový přístup přes Cloud Shell a EPN.....	93
Tabulka 10 Testovací scénář – Ověření Cloud Guard respondéru	96
Tabulka 11 Testovací scénář – Geolokační omezení přístupu pomocí WAF.....	99
Tabulka 12 Testovací scénář – Správa spotřeby zdrojů v OCI pomocí kvót	101
Tabulka 13 Bezpečnostní checklist pro OCI – Autentizace	106

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ACL Access Control List

AD Availability Domain (v kontextu OCI)

AES-256 Advanced Encryption Standard (256bitové šifrování)

AICPA American Institute of Certified Public Accountants

AMD-SEV AMD Secure Encrypted Virtualization

API Application Programming Interface

ARM Advanced RISC Machine (typ procesorové architektury)

ATT Adversarial Tactics and Techniques (v kontextu MITRE ATT&CK)

AWS Amazon Web Services

BCM-xx Business Continuity Management (číslovaný bezpečnostní cíl v CSA CCM)

BMCS Bare Metal Cloud Services (dřívější název první generace OCI IaaS)

BYOK Bring Your Own Key (vlastní správa šifrovacích klíčů)

CAIQ Consensus Assessments Initiative Questionnaire (dotazník CSA)

CapEx Capital Expenditures (kapitálové výdaje)

CCM Cloud Controls Matrix (bezpečnostní rámec CSA)

CIA Confidentiality, Integrity, Availability (bezpečnostní triáda)

CIDR Classless Inter-Domain Routing (způsob zápisu IP adresních rozsahů)

CIS Center for Internet Security

CLI Command Line Interface

CRM Customer Relationship Management

CRN Cloud Resource Name (OCI označení zdrojů)

CRS OWASP Core Rule Set (soubor pravidel pro WAF ochranu)

CSA Cloud Security Alliance

CSF Cybersecurity Framework (např. NIST CSF)

CSP Cloud Service Provider

CSPM Cloud Security Posture Management

CVE Common Vulnerabilities and Exposures

CVSS Common Vulnerability Scoring System

DBaaS Database as a Service

DDoS Distributed Denial of Service

DevOps Development and Operations (součinnost vývoje a provozu IT systémů)

DMZ Demilitarized Zone (oddělená síťová zóna)

DoD Department of Defense (USA)

DR Disaster Recovery

DREAD Damage, Reproducibility, Exploitability, Affected Users, Discoverability

ENISA European Union Agency for Cybersecurity

EPN Ephemeral Private Network (dočasné síťové připojení)

ERP Enterprise Resource Planning

FaaS Function as a Service

FD Fault Domain (doména poruchy v rámci dostupnosti OCI)

FedRAMP Federal Risk and Authorization Management Program (USA)

FIPS Federal Information Processing Standards

FQDN Fully Qualified Domain Name

GCP Google Cloud Platform

HIPAA Health Insurance Portability and Accountability Act (USA)

HPC High-Performance Computing

HSM Hardware Security Module

IaaS Infrastructure as a Service

IAM Identity and Access Management

IDA Identity Domain Administrator (v OCI)

IDaaS Identity as a Service

IDCS	Identity Cloud Service (služba Oracle pro správu identit)
IDPS	Intrusion Detection and Prevention System
IEC	International Electrotechnical Commission
IOC	Indicator of Compromise
IOPS	Input/Output Operations Per Second
IoT	Internet of Things
ISACA	Information Systems Audit and Control Association
KMS	Key Management Service
LFI	Local File Inclusion (typ zranitelnosti)
MFA	Multi-Factor Authentication
MITRE	Nezisková organizace spravující ATT&CK a CVE (MITRE Corporation)
NAT	Network Address Translation
NCSC	National Cyber Security Centre
NFS	Network File System
NIST	National Institute of Standards and Technology (USA)
NSG	Network Security Group (např. v OCI nebo Azure)
NVD	National Vulnerability Database
NVDIMM	Non-Volatile Dual In-line Memory Module
OAuth	Open Authorization (protokol pro delegované ověřování)
OCI	Oracle Cloud Infrastructure
OCID	Oracle Cloud Identifier (jedinečný identifikátor OCI zdroje)
OCIR	Oracle Cloud Infrastructure Registry (repozitář kontejnerů)
OKE	Oracle Kubernetes Engine
OpEx	Operational Expenditure (provozní výdaje)
OWASP	Open Worldwide Application Security Project
PaaS	Platform as a Service

PAYG	Pay As You Go (platební model za cloudové služby)
PCI-DSS	Payment Card Industry Data Security Standard
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RFC	Request for Comments (technické standardy Internetu)
RFI	Remote File Inclusion (typ zranitelnosti)
SaaS	Software as a Service
SAML	Security Assertion Markup Language
SEV	Secure Encrypted Virtualization (technologie AMD)
SIEM	Security Information and Event Management
SOC	Security Operations Center
SPI	SaaS, PaaS, IaaS (tři základní modely poskytování cloudových služeb)
SQLi	SQL Injection (zranitelnost vkládání SQL příkazů)
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege (model hrozeb)
TSC	Trust Services Criteria (AICPA)
TSME	Transparent Secure Memory Encryption (AMD)
TTP	Tactics, Techniques and Procedures (v MITRE ATT&CK)
VCN	Virtual Cloud Network (např. v OCI)
VNIC	Virtual Network Interface Card
VPN	Virtual Private Network
VSS	Vulnerability Scanning Service
WAF	Web Application Firewall
XSS	Cross-Site Scripting (typ zranitelnosti)
ZPL	ZPR Policy Language (jazyk pro definici bezpečnostních pravidel pro ZPR)
ZPR	Zero Trust Packet Routing

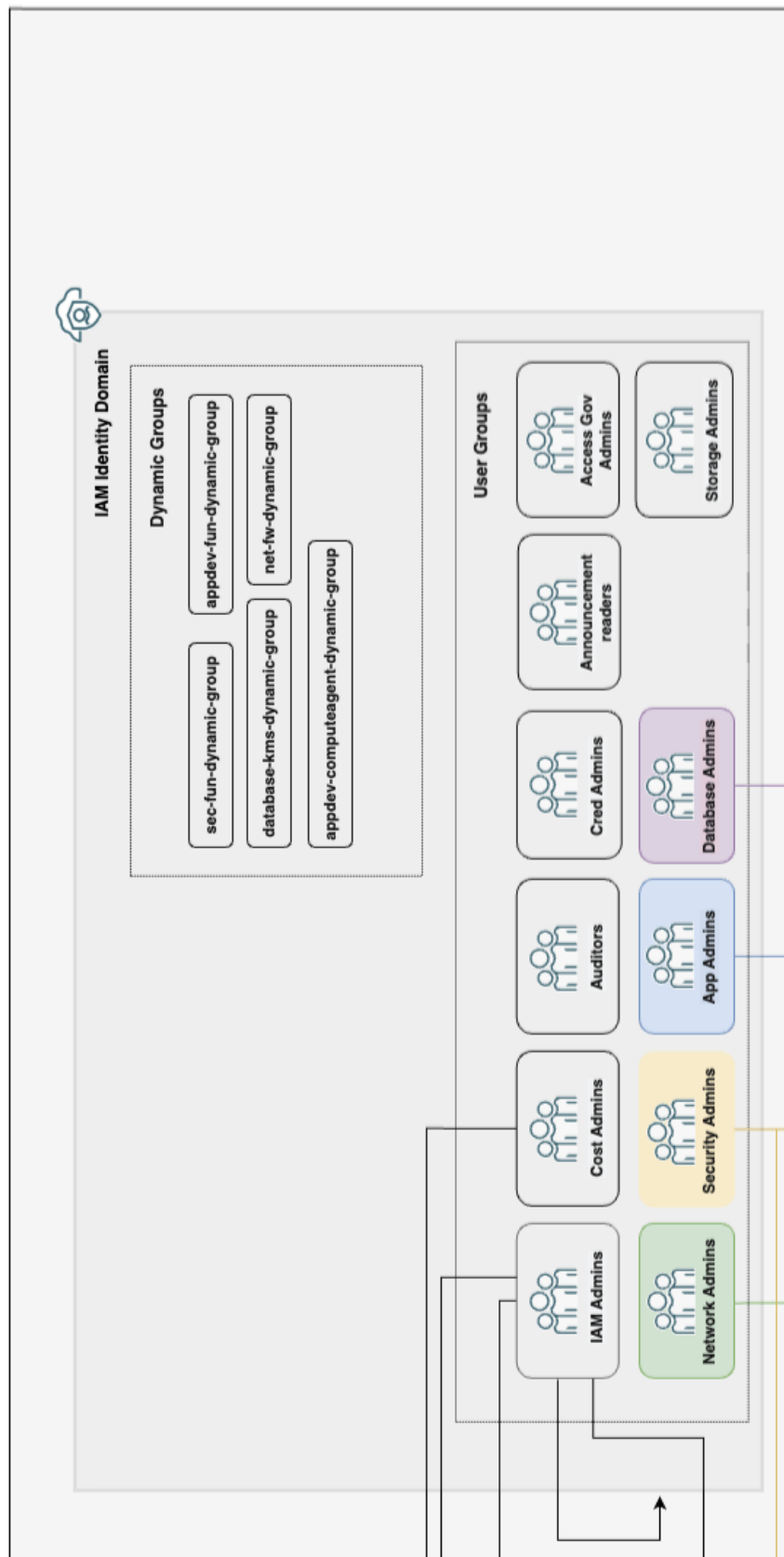
SEZNAM PŘÍLOH

Příloha P I: Detaily OCI diagramu PoC architektury

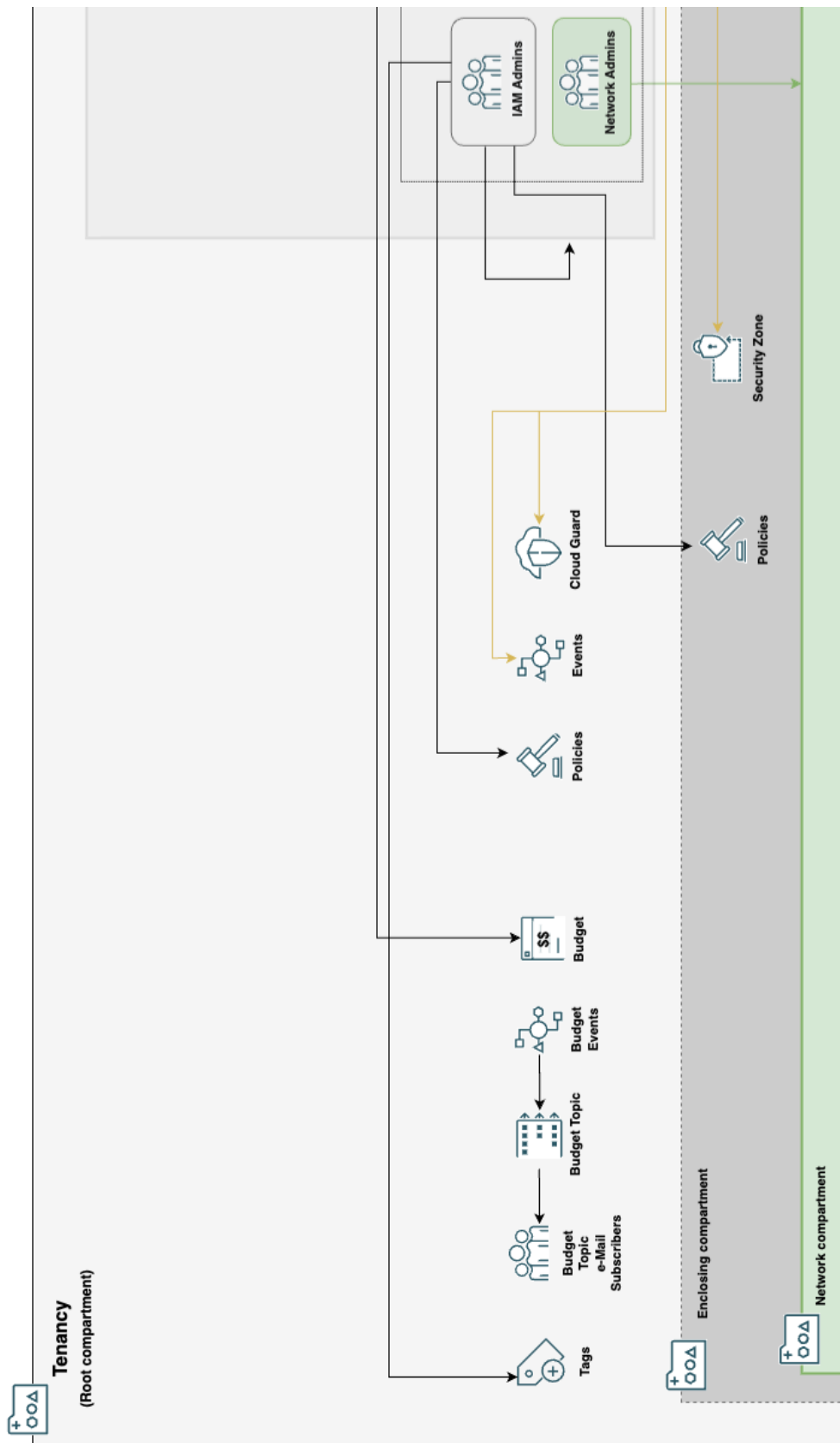
Příloha P II: Výsledky testů bezpečnostních scénářů

PŘÍLOHA P I: DETAILS OCI DIAGRAMU PoC ARCHITEKTURY

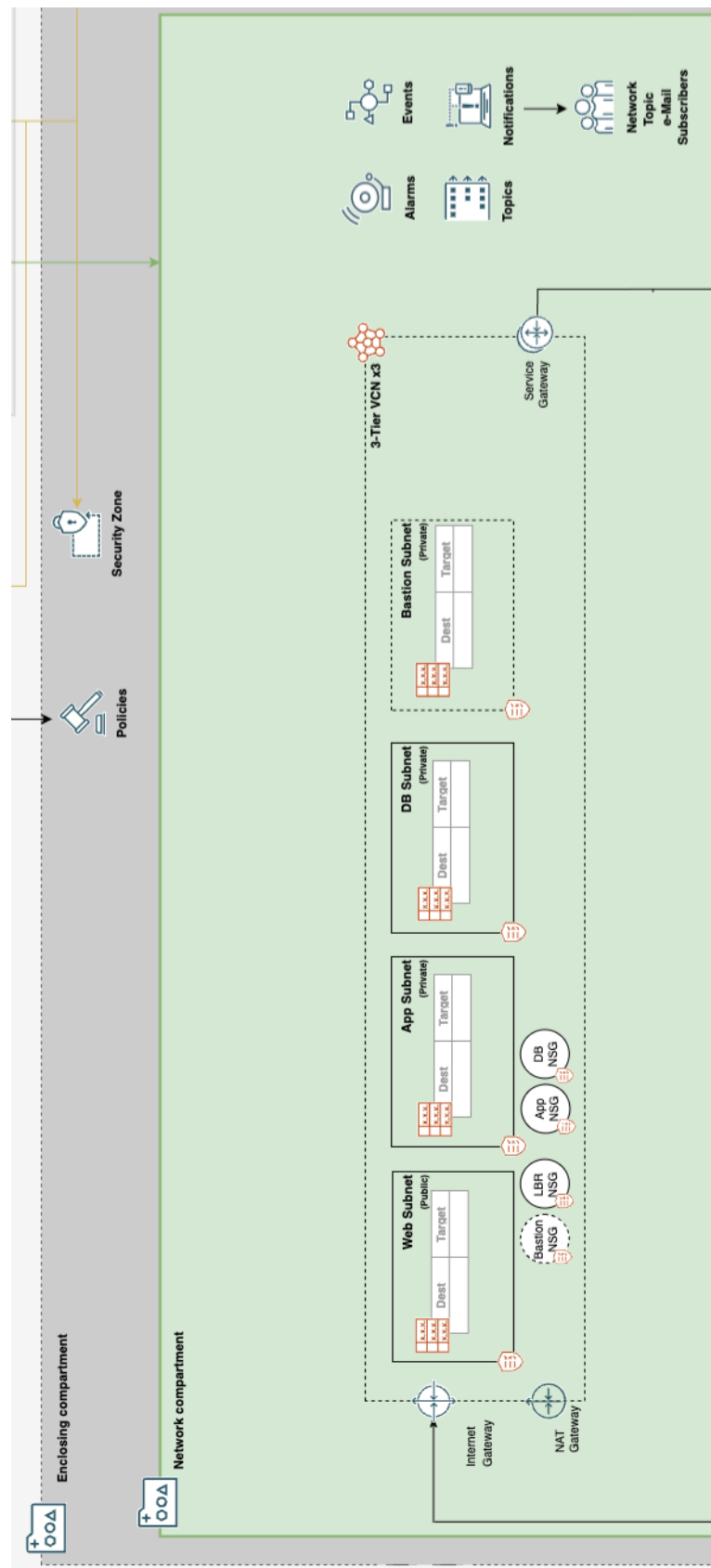
Obrázek znázorňuje výřez OCI diagramu PoC (IAM)



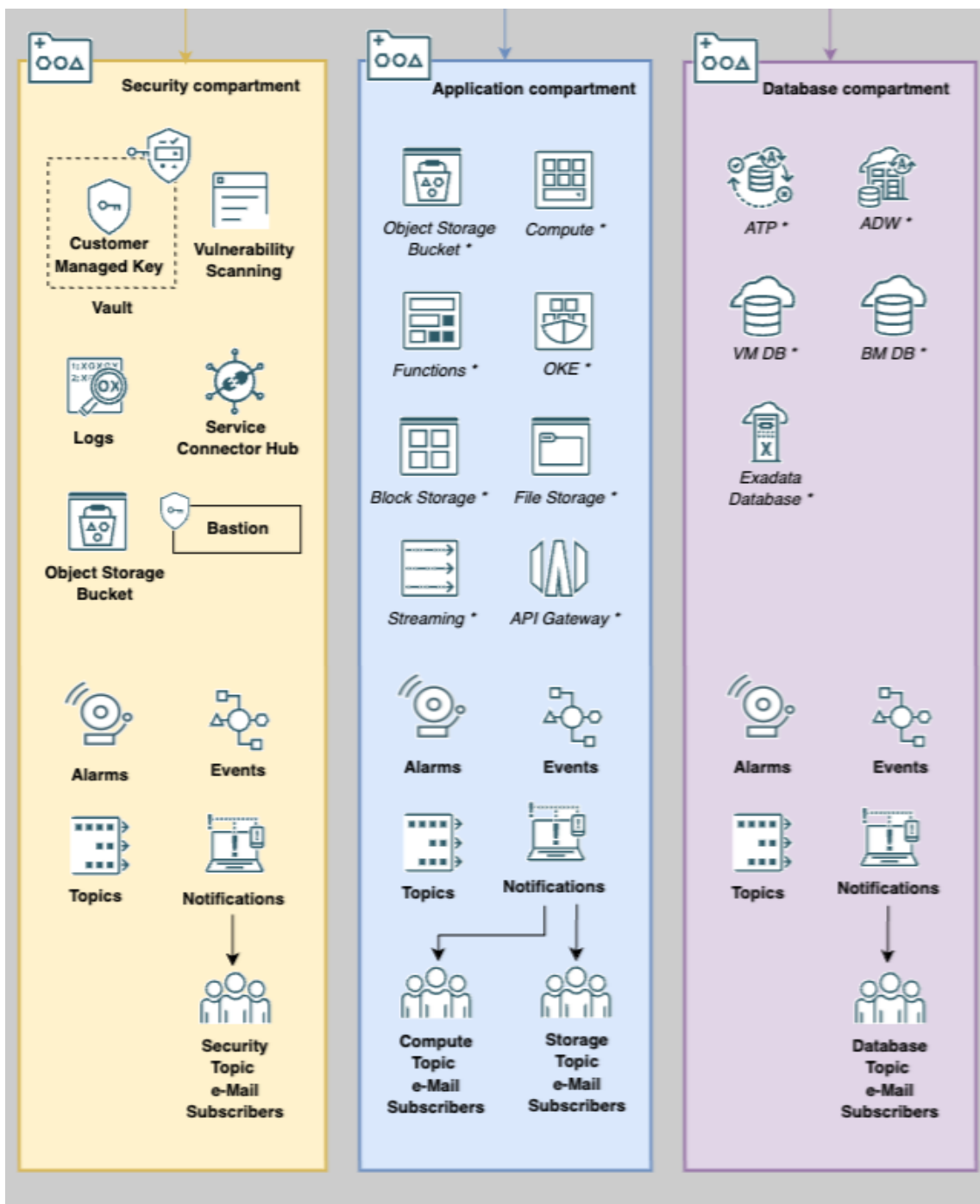
Obrázek znázorňuje výřez OCI diagramu PoC (Tenancy/Root kompartment)



Obrázek znázorňuje výřez OCI diagramu PoC (Network compartment)



Obrázek znázorňuje výřez OCI diagramu PoC (Security/App/DB kompartmenty)



PŘÍLOHA P II: VÝSLEDKY TESTŮ BEZPEČNOSTNÍCH SCÉNÁŘŮ

Obrázek znázorňuje neúspěšný pokus o vytvoření veřejného bucketu z prostředí OCI CLI Cloud Shell (ID testu „SEC-DATA-C-001-PUBLIC-BUCKET-CREATE“)

Actions	Network: Public
Cloud Shell <pre>Welcome to Oracle Cloud Shell. Cloud Shell now runs on Oracle Linux 8. For more information, see the release notes. For help, contact Oracle Support. Your Cloud Shell machine comes with 5GB of storage for your home directory. Your Cloud Shell (machine and home directory) are located in: You are using Cloud Shell in tenancy dcdlthesis2025 as OCI local user d_codl@utb.cz Type 'help' for more info. d_codl@cloudshell:~ (eu-frankfurt-1)\$ oci os bucket create \ > --name muj-verejny-bucket \ > --compartment-id \$(oci iam compartment list --name PoC-top-cmp --query "data[0].id" --raw-output) \ > --public-access-type ObjectRead \ > --storage-tier Standard ServiceError: { "client_version": "Oracle-PythonSDK/2.149.1, Oracle-PythonCLI/3.54.0", "code": "Forbidden", "logging_tips": "Please run the OCI CLI command using --debug flag to find more debug information.", "message": "Security Zone Violation: Object Storage buckets in a security zone can't be public.", "opc-request-id": "fra-1:GyqS8bo3vDJIQ5YQoJ4w0gRl3a0j6-WVneutz97XEeF3z4pUZ3GXsthGB4qzUn0F", "operation_name": "create_bucket", "request_endpoint": "POST https://objectstorage.eu-frankfurt-1.oraclecloud.com/n/frmvcqk10atk/b", "status": 403, "target_service": "object_storage", "timestamp": "2025-04-13T08:26:51.663316+00:00", "troubleshooting_tips": "See [https://docs.oracle.com/iaas/Content/API/References/apierrors.htm] for more information about resolving resolve this issue, run this CLI command with --debug option and contact Oracle support and provide them the full error message." } d_codl@cloudshell:~ (eu-frankfurt-1)\$</pre>	

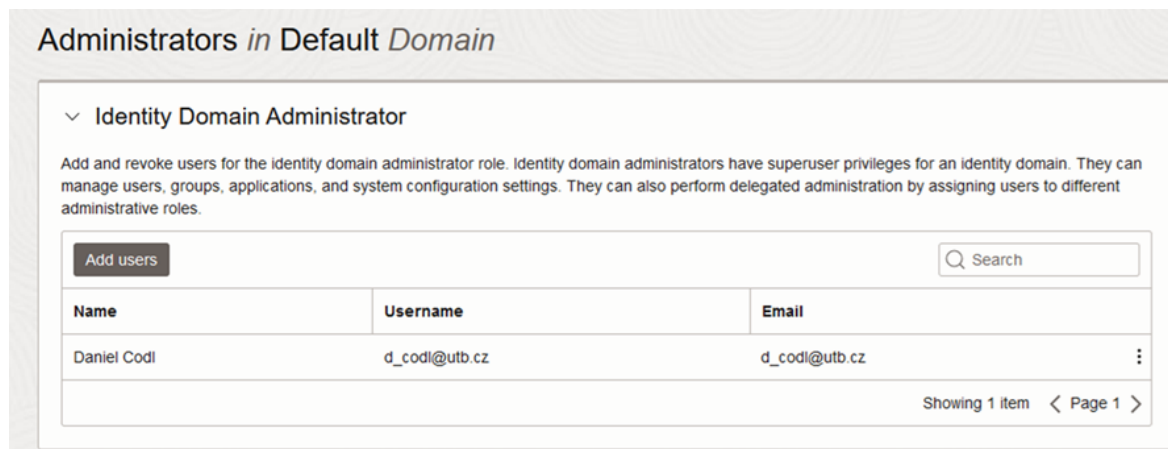
Obrázek znázorňuje neúspěšný pokus o vytvoření VCN z prostředí OCI CLI Cloud Shell (ID testu „SEC-NET-I-001-UNAUTHORIZED-VCN-CREATION“)

Actions	Network: Public
Cloud Shell <pre>welcome to Oracle Cloud Shell. Cloud Shell now runs on Oracle Linux 8. For more information, see the release notes. For help, contact Oracle Support. Your Cloud Shell machine comes with 5GB of storage for your home directory. Your Cloud Shell (machine and home directory) are located in: Germany You are using Cloud Shell in tenancy dcodlthesis2025 as OCI local user alice.newman.poc.auditor@gmail.com Type 'help' for more info. alice_new@cloudshell:~ (eu-frankfurt-1)\$ oci network vcn create \ > --cidr-block 10.0.0.0/16 \ > --compartment-id "\$(oci iam compartment list --access-level ANY --compartment-id-in-subtree true --query "data[?name=='PoC-network-cmp'].id" > --display-name "Neopravnena-VCN" ServiceError: { "client_version": "Oracle-PythonSDK/2.149.1, Oracle-PythonCLI/3.54.0", "code": "NotAuthorizedOrNotFound", "logging_tips": "Please run the OCI CLI command using --debug flag to find more debug information.", "message": "Authorization failed or requested resource not found.", "opc-request-id": "080344A0859F408082886801D4A83027/614C9A5C702062E67252548F2A34F7FC/9020F10E0AC788156290754E5D983941", "operation_name": "create_vcn", "request_endpoint": "POST https://iaas.eu-frankfurt-1.oraclecloud.com/20160918/vcns", "status": 404, "target_service": "virtual_network", "timestamp": "2025-04-13T08:34:55.941316+00:00", "troubleshooting_tips": "See [https://docs.oracle.com/iaas/Content/API/References/apierrors.htm] for more information about resolving this err run this CLI command with --debug option and contact Oracle support and provide them the full error message." } alice_new@cloudshell:~ (eu-frankfurt-1)\$</pre>	

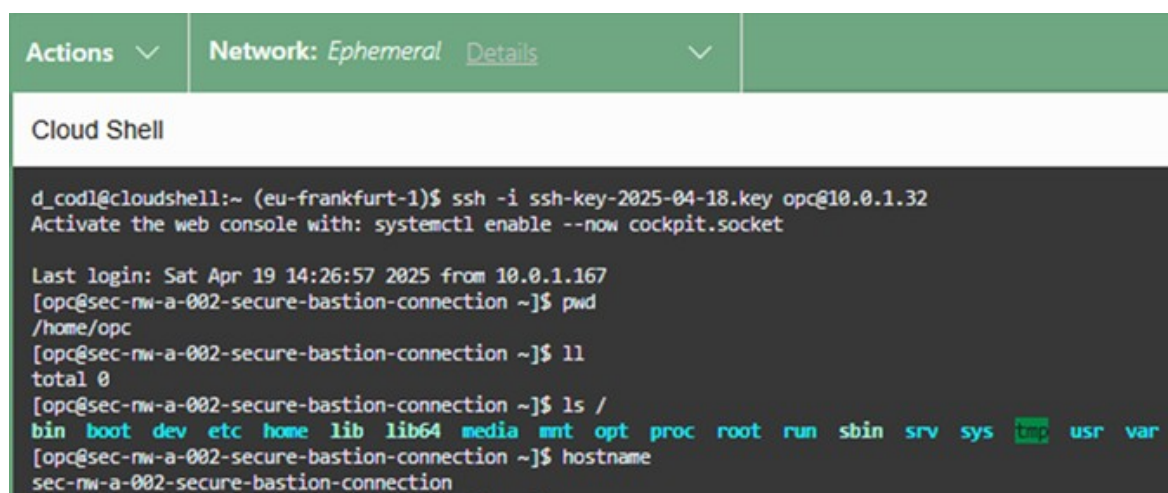
Obrázek znázorňuje neúspěšný pokus o změnu role z prostředí OCI CLI Cloud Shell (ID testu „SEC-AUTH-I-002-ROLE-ASSIGNMENT-MODIFICATION“)

Actions	Network: <i>Public</i>
Cloud Shell <pre>alice_newm@cloudshell:~ (eu-frankfurt-1)\$ oci iam policy create \ > --name "Allow-Auditors-to-create-VCN" \ > --description "Umožňuje skupině PoC-auditor-group spravovat síťové prostředky v kompartmentu PoC-network-cmp" \ > --statements "[\\"Allow group PoC-auditor-group to manage virtual-network-family in compartment PoC-network-cmp\\"]" \ > --compartment-id "\$(oci iam compartment list --access-level ANY --compartment-id-in-subtree true --query "data[?name=='PoC-network-cmp']" ServiceError: { "client_version": "Oracle-PythonSDK/2.149.1, Oracle-PythonCLI/3.54.0", "code": "NotAuthorizedOrNotFound", "logging_tips": "Please run the OCI CLI command using --debug flag to find more debug information.", "message": "Authorization failed or requested resource not found.", "opc-request-id": "DD120460850F402296BE2328D803F33A/45949A4248884E157D9C45156842A190/A0382402CD9E7437622F2ADF64478000", "operation_name": "create_policy", "request_endpoint": "POST https://identity.eu-frankfurt-1.oci.oraclecloud.com/20160918/policies", "status": 404, "target_service": "identity", "timestamp": "2025-04-13T08:37:45.593816+00:00", "troubleshooting_tips": "See [https://docs.oracle.com/iaas/Content/API/References/apierrors.htm] for more information about resolving to resolve this issue, run this CLI command with --debug option and contact Oracle support and provide them the full error message." } alice_newm@cloudshell:~ (eu-frankfurt-1)\$</pre>	

Obrázek znázorňuje chybějícího záložního administrátora výchozí domény identity v OCI Console (ID testu „SEC-IDC-A-001-DOMAIN-ADMIN-LOCKOUT“)



Obrázek znázorňuje úspěšný pokus zalogování pomocí EPN a OCI Cloud Shell do soukromé podsítě mimo Security Zone (ID testu „SEC-NW-A-002-EMERGENCY-EPN-ACCESS“)



Obrázek znázorňuje neúspěšný pokus zalogování pomocí EPN a OCI Cloud Shell do soukromé podsítě uvnitř Security Zone (ID testu „SEC-NW-A-002-EMERGENCY-EPN-ACCESS“)



Obrázek znázorňuje čas vytvoření („Launched“) compute instance s veřejnou IP adresou v prostředí OCI Console (ID testu „SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER“)

OCI Cloud

Search resources, services, documentation, and Marketplace

Compute » Instances » Instance details » Work requests

VM-SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER

Start

Stop

Reboot

Terminate

More actions

Instance information

Shielded instance

Maintenance

Oracle Cloud Agent

Notifications

RUNNING

General information

Availability domain: AD-1

Fault domain: FD-1

Region: eu-frankfurt-1

OCID: ...4j4vjq Show Copy

Launched: Fri, Apr 25, 2025, 15:46:25 UTC

Compartment: dcodithesis2025 (root)

Capacity type: On-demand

Instance details

Virtual cloud network: PoC-bastion-vcn-1

Launch mode: PARAVIRTUALIZED

Instance metadata service: Versions 1 and 2 Edit Info

Image details

Operating system: Oracle Linux

Version: 8

Obrázek znázorňuje čas aktivace detektoru („First detected“) Cloud Guard (ID testu „SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER“)

Cloud

Search resources, services, documentation, and Marketplace

Cloud Guard > Alerts > Problems > Problem details

P

RESOLVED

Instance has a public IP address

Checks public IP only [Learn more](#)

Remediate

Mark as resolved

Dismiss

Details

General information

Problem OCID: ...da6i6kipiq [Show](#) [Copy](#)

Resource ID: ...t6ix4j4vjvq [Show](#) [Copy](#)

Detector type: Configuration

Resource name: [VM-SEC-CG-A-003-INSTANCE-S...](#)

Managed: Local

Risk level: ● High

Resource type: Instance

Status: Resolved

Compartment: [dcodlthesis2025 \(root\)](#)

Regions: Germany Central (Frankfurt)

Target: [PoC-cloud-guard-root-target](#)

First detected: Fri, Apr 25, 2025, 18:03:27 UTC

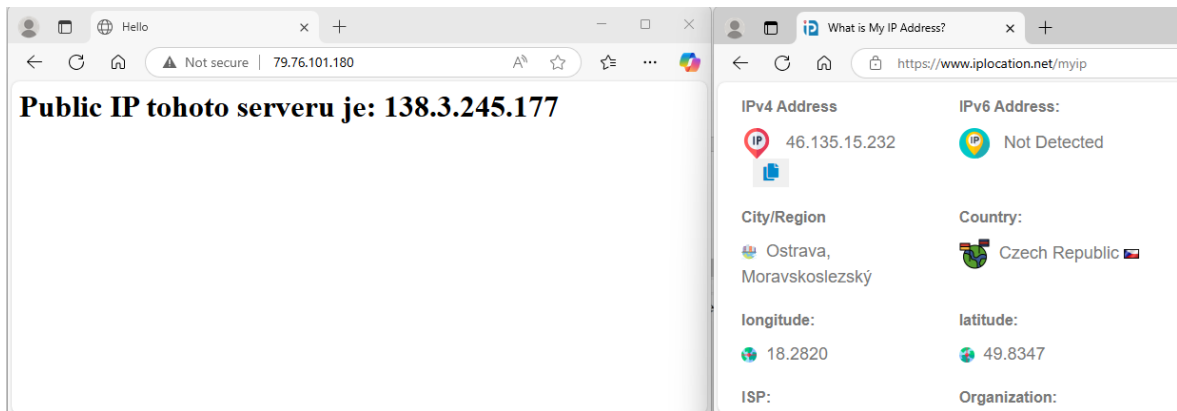
Last detected: Fri, Apr 25, 2025, 18:04:00 UTC

Labels: CIS_OCI_V1.0_NETWORK, COMPUTE, CIS_OCI_V1.1_NETWORK

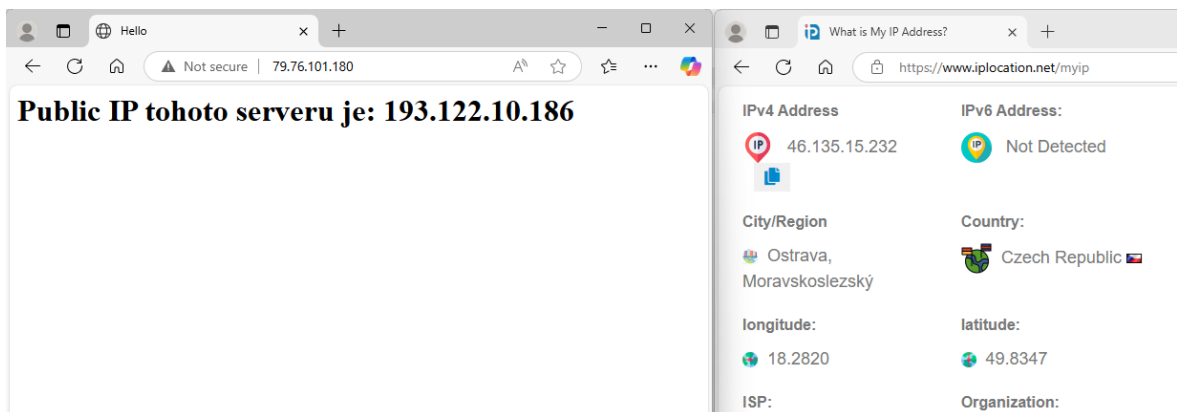
Obrázek znázorňuje čas aktivace respondéru Cloud Guardu a zastavení compute instance (ID testu „SEC-CG-A-003-INSTANCE-SECURITY-RESPONDER“)

Resources	Responder activity			
Problem history Responder activity	Responders related to this problems			
Stop Compute Instance		Fri, Apr 25, 2025, 18:03:41 UTC	Completed	● Succeeded
Stop Compute Instance		Fri, Apr 25, 2025, 18:03:41 UTC	Started	● Succeeded

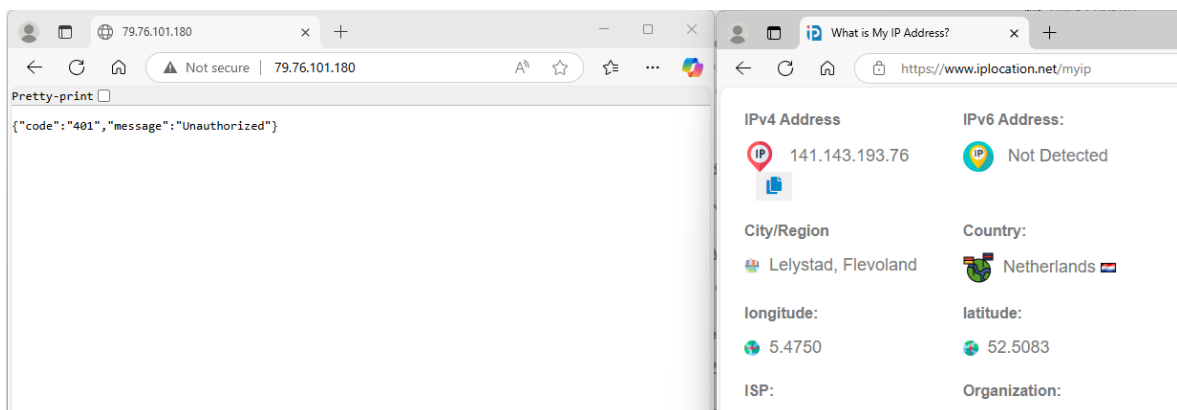
Obrázek znázorňuje povolení přístupu na VM server přes OCI Loadbalancer a WAF pro přístup z České republiky (ID testu „SEC-WAF-A-004-RESTRICT-WEB-ACCESS“)



Obrázek znázorňuje povolení přístupu na VM server přes OCI Loadbalancer a WAF pro přístup z České republiky (ID testu „SEC-WAF-A-004-RESTRICT-WEB-ACCESS“)



Obrázek znázorňuje blokaci přístupu na OCI Loadbalancer v kombinaci s WAF pro přístup mimo ČR (ID testu „SEC-WAF-A-004-RESTRICT-WEB-ACCESS“)



Obrázek znázorňuje neúspěšný pokus o vytvoření druhé compute instance při aktivní kvótě na maximální počet instancí (ID testu „SEC-GOV-A-005-COMP-QUOTA-LIMIT“)

Cloud

Search resources, services, documentation, and Marketplace

Create compute instance

Create an instance to deploy and run applications, or save as a reusable Terraform stack for creating an instance with Resource Manager.

Name

Instance-20250426-1118

Create in compartment

PoC-app-cmp

doodlthesis2025 (root)/PoC-top-cmp/PoC-app-cmp

Placement

The availability domain helps determine which shapes are available.

Availability domain

AD 1

SJJR-EU-FRANKFURT-1-AD-1

✓

AD 2

SJJR-EU-FRANKFURT-1-AD-2

AD 3

SJJR-EU-FRANKFURT-1-AD-3

Show advanced options

Security

Shielded instance: Disabled

Confidential computing: Disabled

Edit

Create

Save as stack

Cancel

The following compartment quotas were exceeded: standard-a1-core-count in policy 'ocid1_quota_oc1...aaaaaaaawm5av4ow7b5vvrw6gxxo5q6qalfva72hg7luwvm6vxx4m4a' by 1, standard-a1-core-regional-count in policy 'ocid1_quota_oc1...aaaaaaaawm5av4ow7b5vvrw6gxxo5q6qalfva72hg7luwvm6vxx4m4a' by 1. You can locate the quota policies by searching for the quota IDs in the console.