IBM QRadar on Cloud

Tento Popis služby stanovuje podmínky služby Cloud Service. Příslušné dokumenty objednávky poskytují podrobnosti o ceně a další podrobnosti o objednávce Zákazníka.

1. Cloud Service

1.1 IBM QRadar on Cloud

Zákazník si může vybrat z následujících dostupných nabídek.

1.1.1 IBM QRadar on Cloud 100 EPS

Nabídka IBM QRadar on Cloud přináší pokročilé řešení pro informace o zabezpečení z portfolia IBM Cloud, které využívá produkt IBM Security QRadar SIEM. Umožňuje Zákazníkovi shromažďovat, korelovat a uchovávat události generované z místních i cloudových prostředích a provádět správu zabezpečení a hrozeb stejně jako s produktem QRadar SIEM nasazeným v místě. V rámci nabídky IBM poskytuje také nepřetržité monitorování infrastruktury a používá nejnovější úrovně softwaru nebo důležité opravy, kdykoli jsou k dispozici.

Tato Služba Cloud Service zahrnuje devadesát (90) dní aktivního, prohledávatelského úložiště.

1.2 Volitelné služby

1.2.1 IBM QRadar on Cloud 1K EPS Temporary Upgrade

Upgrade služby, který poskytuje další kapacitu 1000 EPS pro shromažďování a zpracování protokolovaných událostí, ale pouze pro stanovený počet měsíců. Zákazník si může zakoupit několik jednotek tohoto upgradu, a to až do maximální úrovně EPS, kterou nabídka podporuje. Účelem této části je umožnit Zákazníkovi, který vyžaduje pokrytí během období špičky během roku, splnit tyto požadavky prostřednictvím dočasného upgradu kapacity. Na konci období budou tato dočasná navýšení kapacity z prostředí Zákazníka odebrána.

1.2.2 IBM QRadar on Cloud Data Storage 100 EPS

Upgrade datového úložiště přidává další úložiště a rozšiřuje období analýzy. Upgrade kapacity zákazníkům poskytuje až 1 úplný rok uložených dat na každý zakoupený upgrade 100 EPS.

1.2.3 IBM QRadar on Cloud Flows Add-On

Integruje se s IBM QRadar SIEM a procesory toku pro zajištění viditelnosti sítě ve vrstvě 3 a analýzu toku, které Zákazníkovi pomohou rozpoznat a zjistit aktivity prostřednictvím sítě Zákazníka a reagovat na ně.

1.2.4 IBM QRadar on Cloud Vulnerability Management Add-On

Aktivně rozpoznává a zjišťuje síťová zařízení a slabá místa zabezpečení aplikací, doplňuje kontext a podporuje stanovení priorit nápravy a činností zmírňování.

1.2.5 IBM QRadar on Cloud Log Archival

Umožňuje Zákazníkovi archivovat data událostí ze služby Cloud Service po dobu registrace. IBM bude se Zákazníkem spolupracovat na zápisu navržených událostí do úložiště objektů pro archivační účely. Na žádost Zákazníka společnost IBM obnoví až třicet (30) dní archivovaných dat o událostech do instance služby Cloud Service Zákazníka do tří (3) pracovních dní od takové žádosti. Taková data zůstanou dostupná Zákazníkovi po dobu 48 hodin před vrácením do archivačního úložiště objektů. Zákazník je oprávněn zaslat až dvě žádosti za období tří měsíců. Upgrade kapacity Zákazníkům poskytuje až 1 úplný rok uložených dat na každý zakoupený upgrade 100 EPS.

1.3 Akcelerační služby

1.3.1 IBM QRadar on Cloud Optimization Service

Pro tuto vzdáleně poskytovanou službu registrace společnost IBM uskuteční se Zákazníkem schůzku ke zhodnocení s cílem posoudit aktuální stav instance služby Cloud Service Zákazníka a výsledky poskytne

Zákazníkovi prostřednictvím sestavy QRadar on Cloud Health Status, v níž uvede případné oblasti pro zlepšení.

Společnost IBM dále poskytne Zákazníkovi na jeho žádost některou z následujících konzultačních služeb v délce až osmi (8) dní během období 1 roku:

- Pomoc s přidáním dalších zdrojů protokolu ke službě Cloud Service;
- konfigurace dalších vyhledávání, výkazů a panelů dashboard;
- provedení dodatečného ladění stávajícího nasazení QRadar; a
- poskytnutí přenosu znalostí na příslušné subjekty QRadar.

1.3.2 Služby nastavení

Na dálku jsou poskytovány následující služby nastavení, které lze objednat samostatně. Každá objednaná služby skončí (90) dní od koupě, není-li uvedeno jinak, bez ohledu na to, zda byly vyčerpány všechny (případné) hodiny. Služby budou zahrnovat jmenovaného Správce podpory IBM, který naplánuje veškeré zahajovací hovory.

1.3.3 IBM QRadar on Cloud Deployment Service

Tato služba poskytuje čtyřicet (40) hodin odborných služeb, během nichž společnost IBM poskytne některé nebo všechny následující položky:

Společnost IBM provede kontrolu architektury SIEM o rozsahu až šestnácti hodin pro definování požadavků na vykazování Zákazníka a svá zjištění poskytne Zákazníkovi formou výkazu o řešení architektury, který pomůže definovat a zaznamenat požadavky Zákazníka.

Výkaz bude zahrnovat:

- Požadavky na vykazování definované Zákazníkem, které Zákazníkovi pomohou se splněním požadavků na zajištění souladu, auditů a zpráv o zabezpečení.
- Požadavky na zprávy o zabezpečení, příklady využití a aplikace, s jejichž implementací může společnost IBM pomoci (až deset (10) případů využití a až dvě (2) aplikace).
- Základní informace o protokolu a zdrojích toku Zákazníka, které budou vyžadovány na podporu případů využití.
- Aspekty infrastruktury sítě, jako jsou firewally a porty.

Na základě výkazu o řešení architektury společnost IBM provede následující úkoly, podle toho, co zbývající čas umožní:

- Konfigurace shromažďování událostí pro až tři (3) instance až deseti (10) typů zdrojů protokolu do služby Cloud Service. Tato činnost bude zahrnovat poskytnutí znalostí příslušným pracovníkům Zákazníka, aby mohli dle potřeby přidávat další zdroje protokolů. Do této části služby budou zahrnuty pouze zdroje protokolů podporované standardními moduly QRadar Device Support Modules (DSMs).
- Úvodní ladění, které zahrnuje a) aktivaci předpřipravených zásad, uložených vyhledávání, grafů a výkazů akumulovaných časových řad; b) identifikaci a odstranění zdrojů šumu; a c) konfiguraci offline úložiště prostřednictvím NFS, CIFS nebo iSCSI.
- Implementace deseti (10) případů využití a dvou (2) aplikací z IBM QRadar App Exchange, které byly zdokumentovány v dokumentu řešení architektury.

1.3.4 IBM QRadar on Cloud Custom Parser Service

Tato služba zajistí vývoj jednoho vlastního rozboru /uDSM na podporu nestandardních typů zdrojů protokolu Zákazníka, které mají být zasílány do služby Cloud Service, a zahrnuje následující úkoly:

- vytvoření vlastního rozboru pro jeden nestandardní typ zdroje protokolu (práce prováděná na dálku);
- vytvoření, konfigurace a mapování uDSM;
- nasazení a testování vlastního uDSM; a
- rozbor až dvaceti pěti typů zpráv pro zdroj protokolu.

2. Datové listy ochrany a zpracování údajů

Dodatek o zpracování údajů (Data Processing Addendum, DPA) společnosti IBM na adrese http://ibm.com/dpa a Datový list zpracování a ochrany údajů (označováno jako Datový list nebo Dodatek DPA) v odkazech níže poskytují další informace o ochraně údajů pro služby Cloud Services a volby týkající se typů Obsahu, které lze zpracovat, využívaných činností vztahujících se ke zpracování, funkcí ochrany údajů a specifických aspektů uchovávání a vrácení Obsahu. Dodatek DPA se uplatní, pokud se na osobní údaje zahrnuté v Obsahu vztahuje Evropské obecné nařízení o ochraně údajů (EU/2016/679) (GDPR).

https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=FB0F42F0750011E6865BC3F213DB63F7

3. Úrovně služby a Technická podpora

3.1 Dohoda o úrovni služeb

IBM poskytuje Zákazníkovi následující Dohodu o úrovni služeb (SLA). IBM uplatní nejvyšší použitelnou kompenzaci vycházející ze souhrnné dostupnosti služby Cloud Service, jak je uvedeno v tabulce níže. Procento dostupnosti se vypočítá jako celkový počet minut v rámci smluvního měsíčního období minus celkový počet minut Odstávky za smluvní měsíční období, děleno celkovým počtem minut za smluvní měsíční období. Definice Odstávky, proces uplatňování nároku a jak kontaktovat IBM ohledně problémů s dostupností služby jsou uvedeny na stránkách IBM v přehledu SaaS support na adrese https://www.ibm.com/software/support/saas_support_overview.html.

Dostupnosti služeb	Dobropis (% měsíčního registračního poplatku*)
Méně než 99,9 %	2 %
Méně než 99,0 %	5 %
Méně než 95,0 %	10 %

* Registrační poplatek je smluvní cena za měsíc, za který je uplatňován nárok.

3.2 Technická podpora

Informace o technické podpoře pro službu Cloud Service, včetně kontaktních údajů na podporu, úrovní závažnosti, hodin dostupnosti podpory, dob odezvy a dalších informací a procesů podpory, lze zjistit výběrem služby Cloud Service v příručce podpory IBM support guide na adrese https://www.ibm.com/support/home/pages/support-guide/.

4. Poplatky

4.1 Metriky poplatků

Metrika poplatků za službu Cloud Service je stanovena v Transakčním dokumentu.

Na tuto službu Cloud Service se uplatní následující metriky zpoplatnění:

- Sjednaná služba je profesionální nebo trénování služba související se službami Cloud Services.
- Události za sekundu je počet výskytů specifické události za sekundu, která je zpracovávána službami Cloud Services nebo souvisí s použitím služeb Cloud Services.
- Toků za minutu je počet toků za minutu spravovaných nebo zpracovaných službami Cloud Services. Tok je záznam komunikace mezi dvěma hostiteli. Pakety obsahující stejnou zdrojovou IP, cílovou IP, zdrojový port, cílový port a protokol se spojí do jednoho záznamu Toku.
- Aktivum je jednoznačně identifikovatelný hmotný prostředek nebo položka s hodnotou, které mají být přístupné nebo spravované službami Cloud Services.

5. Dodatečné podmínky

Podmínky v případě Smluv ke službě Cloud Service (nebo ekvivalentní smlouvy k základnímu cloudu) uzavřené před 1. lednem 2019 jsou dostupné na adrese https://www.ibm.com/acs.

5.1 Aktivační software

Služba Cloud Service obsahuje následující Aktivační software:

- Brána dat – Zákazník smí nainstalovat a používat pouze maximálně deset (10) kopií Brány dat.

6. Přednostní podmínky

6.1 Použití dat zabezpečení

Dále uvedené má přednost v případě rozporu s částí Ochrana obsahu a údajů v základních podmínkách služby Cloud Service mezi stranami: IBM může z Obsahu Zákazníka získávat ukazatele potenciálně škodlivých aktivit za účelem použití v kontextech získávání informací o kybernetických hrozbách, konkrétně adresy URL, adresy IP, domény a hašování souborů. IBM může dále upozornit Zákazníka, pokud tyto ukazatele naznačují, že je u něj zvýšené riziko kybernetických hrozeb.