

Popis služeb IBM Cloud Service

IBM Intelligent Operations Center on IBM SmartCloud

Níže je uveden Popis služeb pro Vaši Objednávku:

1. Cloud Service

Nabídka Cloud Service, včetně základní nabídky a dostupných volitelných komponent, je popsána níže a odpovídá výběru v Objednávce. Objednávka bude zahrnovat předkládanou Cenovou nabídku a Dokument o oprávnění (Proof of Entitlement) uvádějící datum zahájení, smluvní období pro služby Cloud Service a datum zahájení fakturace.

1.1 IBM Intelligent Operations Center Standard User on IBM SmartCloud

Standardní uživatelé (Standard User) mají k dispozici následující funkce:

- Konzole Intelligent Operations Center (IOC) – hlavní rozhraní, které uživatelům umožňuje prohlížet si události a stav událostí a geoprostorové informace (to vyžaduje integraci se službou GIS, která není dodávána v rámci služby Cloud Service) a zobrazovat reporty pro účely analýzy historických trendů a optimalizace implementace prostředků a informace o klíčových ukazatelích výkonnosti (KPI), které si uživatel vybral.
- Umožňuje uživatelům zobrazovat výsledky z analýz na základě času a místa události nebo ostatní data zpracovaná službami Cloud Services na mapě.
- Umožňuje uživatelům stahovat události na základě dat zpracovaných službou IBM Cloud Service.
- Umožňuje uživatelům prohlížet reporty o událostech nebo jiná data zachycená prostřednictvím konzole IOC.
- Poskytuje šablony Standardních provozních postupů (SOP), které si mohou uživatelé upravit pro události reakce na nouzové situace.
- Umožňuje uživatelům provádět Standardní provozní postupy (SOP), které pomáhají automatizovat standardní odezvu na událost, prahovou hodnotu KPI nebo podmínku definovanou v reportu.
- Poskytuje uživatelům přehledný souhrn informací o všech událostech ve městě.

1.2 IBM Intelligent Operations Center Premium User on IBM SmartCloud

Prémioví uživatelé (Premium User) IBM Intelligent Operations Center Standard User on IBM SmartCloud mají přístup ke všem funkcím uvedeným výše, plus k následujícím dodatečným funkcím:

- Vytváření a úpravy klíčových ukazatelů výkonnosti (KPI) a reportů.
- Vytváření a úpravy Standardních provozních postupů, včetně šablon pro odezvu na stav nouze.
- Administrace služby IBM Cloud Service přes administrativní rozhraní.
- Import dat z Vašeho systému nebo ze systémů třetích stran přes integrační rozhraní API.
- Konfigurování analýz, které v závislosti na čase a lokalitě identifikují korelace mezi událostmi ve městě.
- Definování a správa rozhraní a konfigurování reportů na portálu Citizen Collaboration Portal (definovaný níže).
- Schopnost odesílat servisní požadavky, přidávat uživatele do systému, měnit uživatelské konfigurace a přidávat nové obrazovky do uživatelského rozhraní.

1.3 IBM Intelligent Operations Center Consumer User on IBM SmartCloud

Uživatelé z řad spotřebitelů (Consumer User) smí používat portál Citizen Collaboration Portal, který představuje specializované rozhraní umožňující Uživatelům z řad spotřebitelů externí, veřejný přístup ke službě IBM Cloud Service. Prostřednictvím portálu Citizen Collaboration Portal mají Uživatelé z řad spotřebitelů možnost odesílat požadavky na služby, prohlížet stav svého požadavku a rovněž mohou prohlížet jakékoli reporty. Uživatelé z řad spotřebitelů nemají žádný přístup k funkcím IBM Intelligent Operations Center Standard User on IBM SmartCloud nebo IBM Intelligent Operations Center Premium User on IBM SmartCloud.

2. Popis zabezpečení

2.1 Zásady zabezpečení

IBM dodržuje zásady v oblasti zabezpečení a ochrany soukromí, které jsou zveřejněny a s nimiž jsou seznámeni zaměstnanci IBM. IBM vyžaduje, aby osoby na celém světě, které poskytují podporu datovým střediskům IBM, byly proškoleny v oblasti zabezpečení a ochrany soukromí. IBM disponuje vlastním bezpečnostním týmem, který se specializuje na zabezpečení informací. Zásady a standardy IBM v oblasti zabezpečení jsou každoročně přezkoumávány a přehodnocovány. Bezpečnostní incidenty IBM jsou zpracovávány v souladu s postupem reagování na incidenty.

2.2 Řízení přístupu

Přístup k datům zákazníka je umožněn pouze oprávněným zástupcům podpory IBM v souladu se zásadami oddělení rolí. Ve vztahu k hostiteli pro mezilehlého správce "brány" používají pracovníci podpory IBM dvouúrovňové ověření. Při přístupu k datům Zákazníka se pro všechna připojení používají šifrované kanály. Veškeré přístupy k datům Zákazníka a přesuny dat z nebo do hostitelského prostředí jsou zapisovány do protokolů. V rámci datových středisek IBM IOC není využívána WIFI. Protokoly přístupů jsou pravidelně kontrolovány. Postupy ukončení a změn pracovního poměru jsou zavedeny a zahrnují vrácení aktiv a odebrání přístupových práv.

2.3 Integrita a dostupnost služeb

Úpravy prostředků operačního systému (OSR - operating system resource) a úpravy aplikačního softwaru se řídí procesem řízení změn IBM. Změny v pravidlech brány firewall podléhají procesu řízení změn a před implementací jsou jednotlivě přezkoumávány bezpečnostními pracovníky IBM. Zaměstnanci IBM monitorují prostředky datových středisek IBM 24 hodin denně, 7 dní v týdnu. Na podporu detekce a řešení potenciálního ohrožení zabezpečení systému je oprávněnými administrátory a dodavateli, kteří jsou třetími stranami, prováděno pravidelné interní i externí skenování ohrožení zabezpečení. Ve všech datových střediscích IBM jsou používány systémy na detekci malwaru (antivirové programy, detekce neoprávněného vniknutí a ochrana před ním, skenování ohrožení zabezpečení). Služby datových středisek IBM podporují řadu doručovacích protokolů pro přenos dat prostřednictvím veřejných sítí. Jedná se například o HTTPS/SFTP/FTPS/S/MIME a site-to-site VPN. Zálohovaná data určená pro uložení mimo pracoviště jsou před přenosem šifrována.

2.4 Protokolování aktivit

V případech, kdy je to technicky proveditelné, udržují týmy IBM protokoly svých aktivit pro systémy, aplikace, datová úložiště, middleware a zařízení síťové infrastruktury. Aktivita je protokolována v reálném čase do centrálních úložišť protokolů, což umožňuje minimalizovat pravděpodobnost neoprávněných zásahů, umožňuje centrální provádění analýzy, zasílání výstražných zpráv a tvorbu reportů. Aby se zabránilo neoprávněným zásahům, jsou data opatřena podpisem. Analýza protokolů se provádí v reálném čase prostřednictvím pravidelných analytických reportů, v nichž je vyhledáváno jakékoli abnormální chování. Operátoři jsou upozorňováni na anomálie a v případě potřeby mohou 24 hodin denně, 7 dní v týdnu telefonicky kontaktovat bezpečnostního specialistu.

2.5 Fyzické zabezpečení

IBM dodržuje standardy v oblasti fyzického zabezpečení, jejichž účelem je omezení neoprávněného fyzického přístupu k prostředkům v datových střediscích. Přístup do datových středisek IBM je možný pouze omezenými přístupovými body, pro něž platí režim dvouúrovňového ověření a které jsou monitorovány sledovacími kamerami. Přístup je umožněn pouze oprávněným pracovníkům s povoleným přístupem. Operátoři ověří povolení k přístupu a vydají přístupovou kartu umožňující nezbytný přístup. Zaměstnanci, jimž byly vydány takové přístupové karty, musí odevzdat ostatní přístupové karty a po dobu jejich činnosti smí mít u sebe pouze přístupové karty pro přístup do datového střediska. Používání přístupových karet je evidováno. Návštěvníci, kteří nejsou pracovníky IBM, jsou při vstupu do budovy zaregistrováni a po budovách se pohybují v doprovodu. Je zavedena fyzická ochrana proti škodám způsobeným požárem, záplavami, zemětřesením, výbuchem, občanskými nepokoji a jinými formami přírodních katastrof nebo katastrof způsobených lidským faktorem. Zásobovací a nakládací oblasti a další místa, jimiž mohou do prostor vniknout neoprávněné osoby, jsou hlídány a izolovány. Případy přidání a odstranění zařízení a vybavení jsou protokolovány.

2.6 Dodržování požadavků

Vždy jednou ročně je v našich produktivních datových střediscích prováděn odvětvový audit dle SAS 70 Type II, nyní SSAE 16, nebo ekvivalentní audit. Tým IBM přezkoumává činnosti související se zabezpečením a ochranou soukromí z hlediska dodržování požadavků týkajících se obchodních aktivit IBM. Tým IBM pravidelně provádí hodnocení a prověřování, jejichž cílem je ověřit dodržování zásad zabezpečení

informací. Zaměstnanci IBM a dodavatelů každoročně absolvují školení pracovních sil zaměřené na vzdělávání a získání povědomí v oblasti zabezpečení. Zaměstnancům jsou připomínány jejich pracovní cíle a povinnosti ohledně dodržování etického obchodního chování, ochrany důvěrných informací a závazků IBM v oblasti zabezpečení.

3. Cíle v oblasti úrovně služeb

Cíle týkající se úrovně služeb pro tuto nabídku Cloud Service jsou:

- 99,5% dostupnost mimo naplánované časové úseky vyhrazené na údržbu;
- maximálně pětisekundová doba odezvy indikující aktivitu webové stránky.

Cíle týkající se úrovně služeb představují pouze cíl, nikoli záruku vůči Zákazníkovi. Zákazník nemá v případě, že IBM nesplní cíle týkající se úrovně služeb, žádný nárok na refundaci, vrácení peněz nebo jinou formu náhrady či nápravy.

4. Oprávnění a informace o fakturaci

4.1 Metriky poplatků

Služby IBM Cloud Services jsou prodávány na základě jedné z následujících metrik poplatků, jak je uvedeno v Objednávce:

- a. Souběžný uživatel je měrnou jednotkou, na jejímž základě lze získat Cloud Service. Souběžný uživatel je osoba, která kdykoli v daném časovém okamžiku přistupuje ke službě Cloud Service. Bez ohledu na to, zda daná osoba souběžně přistupuje ke službě Cloud Service vícekrát, se taková osoba počítá za jediného Souběžného uživatele. Jste povinni získat oprávnění pro maximální počet Souběžných uživatelů, kteří jakýmkoli způsobem, přímo či nepřímo (například prostřednictvím multiplexovacího programu, zařízení nebo aplikačního serveru) souběžně přistupují ke službě Cloud Service během období měření uvedeného v části Dokument o oprávnění (Proof of Entitlement) Objednávky.

4.2 Poplatky a fakturace

Výše platby za Cloud Service je specifikována v Objednávce.

4.3 Poplatky za neúplný měsíc

Poplatek za neúplný měsíc představuje poměrnou denní sazbu. Poplatky za neúplný měsíc budou vypočítány na základě zbývajících dnů neúplného měsíce, počítáno ode dne, kdy jste byli společností IBM informováni o tom, že Vám byl udělen přístup k nabídce Cloud Service.

5. Smluvní období a možnost prodloužení

5.1 Smluvní období

Smluvní období pro poskytování Cloud Service začíná datem, kdy Vám IBM oznámí, že Vám byl udělen přístup ke službě Cloud Service, jak je uvedeno v Objednávce. Smluvní a fakturační období se budou počítat až po úplném poskytnutí nabídky, což znamená, že před přístupem uživatelů ke službě Cloud Service jsou dokončeny všechny zátěže a konfigurace dat. V Dokumentu o oprávnění (Proof of Entitlement), který je součástí Objednávky, bude potvrzeno přesné datum začátku a konce smluvního období. V průběhu smluvního období jste oprávněni zvýšit Vaši úroveň užívání Cloud Service. Chcete-li tak učinit, obraťte se na IBM nebo na svého Obchodního partnera IBM. Zvýšenou úroveň užívání potvrdíme v Objednávce.

5.2 Volby prodloužení smluvního období pro služby Cloud Service

Ve Vaší Objednávce je pro smluvní období určena jedna z následujících voleb, která uvádí, zda na konci smluvního období bude služba Cloud Service prodloužena:

5.2.1 Automatické prodloužení

Jestliže je ve Vaší Objednávce uvedeno automatické prodloužení, jste oprávněni ukončit končící smluvní období pro poskytování služby Cloud Service prostřednictvím písemné žádosti zaslané přinejmenším devadesát (90) dní před datem uplynutí smluvního období, které je uvedeno v Objednávce. Neobdrží-li IBM nebo Váš Obchodní partner IBM takovou výpověď do data ukončení smluvního období, bude končící smluvní období automaticky prodlouženo o jeden rok nebo o období rovnající se původnímu smluvnímu období uvedenému v Dokumentu o oprávnění (Proof of Entitlement).

5.2.2 Pokračující fakturace

Je-li v Objednávce uvedena pokračující fakturace, budete mít po ukončení smluvního období i nadále přístup ke Cloud Service a užívání Cloud Service Vám bude fakturováno na bázi pokračující fakturace. Chcete-li ukončit užívání Cloud Service a zastavit proces pokračující fakturace, musíte zaslat IBM nebo svému Obchodnímu partnerovi IBM devadesát (90) dní předem písemnou žádost o zrušení Cloud Service.

Poté, co bude zrušen Váš přístup, budou Vám vyfakturovány jakékoli nesplacené poplatky za přístup až do měsíce, v němž zrušení nabylo účinnosti.

5.2.3 Požadavek prodloužení

Je-li v Objednávce pro prodloužení uvedena volba "ukončení", znamená to, že k datu ukončení smluvního období bude poskytování Cloud Service ukončeno a Váš přístup ke Cloud Service bude odstraněn. Chcete-li pokračovat v užívání Cloud Service i po datu ukončení, musíte svému obchodnímu zástupci IBM nebo Obchodnímu partnerovi IBM zaslat objednávku za účelem zakoupení nového registračního období.

6. Technická podpora

Technická podpora je pro službu Cloud Service a pro aktivační software (je-li to relevantní) poskytována během smluvního období služby Cloud Service. Technická podpora je součástí Cloud Service a není dostupná jako samostatná nabídka. Během období platnosti technické podpory:

- a. IBM Vám bude poskytovat asistenci v případě Vašich běžných otázek typu "jak na to" a rovněž při prošetřování jakýchkoli incidentů, jež souvisejí s funkčností a týkají se kódu.
- b. IBM Vám umožní elektronické nahlašování problémů a poskytne Vám asistenci prostřednictvím webového portálu podpory, a to v průběhu běžné pracovní doby (zveřejněná pracovní doba denní směny) příslušného střediska podpory IBM. (Tento druh asistence není dostupný pro Vaše koncové uživatele.) IBM poskytuje asistenci pro problémy se závažností 1 celoročně, 24 hodin denně.
- c. IBM může požadovat, abyste jí umožnili vzdálený přístup do Vašeho systému za účelem stanovení příčiny problému. Ve všech případech, kdy IBM s Vaším souhlasem vzdáleně přistupuje do Vašeho systému, nesete odpovědnost za adekvátní ochranu svého systému a všech dat, která jsou v něm uložena.

Technická podpora nezahrnuje asistenci týkající se 1) návrhu a vývoje aplikací, 2) Vašeho užívání služby Cloud Service v jiném než specifikovaném provozním prostředí, ani 3) selhání způsobených produkty či službami, za které IBM nenese podle tohoto Popisu služeb odpovědnost.

7. Aktivační software

Tato nabídka Cloud Service může zahrnovat aktivační software. Aktivační software smíte používat pouze ve spojení s Vaším užíváním služby Cloud Service, a to způsobem popsáním v dokumentaci, po celou dobu poskytování služby Cloud Service. V rozsahu, v němž aktivační software obsahuje vzorový kód, máte dodatečné právo vytvářet odvozená díla ze vzorového kódu a používat je v souladu s uděleným právem. Aktivační software je poskytován v souladu se Závazkem týkajícím se úrovně služeb (pokud existuje), avšak jinak je dodáván "JAK JE".

8. Soulad s Pravidly Safe Harbor

IBM se nevyjádřila, zda tato služba Cloud Service odpovídá požadavkům Pravidel Safe Harbor, která se týkají shromažďování, používání a uchovávání dat z Evropské unie a Švýcarska.

9. Další informace

9.1 Sběr dat

Jste si vědomi a vyjadřujete svůj souhlas s tím, že IBM smí v rámci své běžné obchodní činnosti a podpory služeb Cloud Service od Vás (Vašich zaměstnanců a smluvních partnerů) shromažďovat osobní údaje týkající se užívání služeb Cloud Service prostřednictvím sledovacích a jiných technologií. IBM tak činí za účelem získání statistik užívání a informací o efektivitě našich služeb Cloud Service, které umožňují zlepšit zkušenosti uživatelů a/nebo přizpůsobit interakce na míru. Potvrzujete, že získáte nebo jste získali souhlas, který IBM zmocňuje ke zpracování shromážděných osobních údajů v souladu s příslušnými právními předpisy, a to pro výše uvedené účely v rámci IBM, jiných společností náležejících IBM a jejich subdodavatelů, kdekoli IBM a její subdodavatelé provádějí obchodní činnost. IBM vyhoví požadavkům Vašich zaměstnanců a smluvních partnerů, pokud jde o přístup, aktualizaci, opravu nebo vymazání jejich shromážděných osobních údajů.

9.2 Lokality, v nichž jsou využívány výhody

V případech, kdy je to relevantní, budou daně založeny na lokalitě(ách), kterou(é) jste uvedli jako místo, kde využíváte výhod služeb Cloud Service. IBM uplatní daně na základě obchodní adresy, která byla při objednání služby Cloud Service uvedena jako primární lokalita pro využívání výhod, ledaže byste IBM poskytli doplňující informace. Nesete odpovědnost za aktualizaci takových informací a za informování IBM o jakýchkoli změnách.