

IBM Cloud Identity

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

1. Cloud Service

IBM Cloud Identity poskytuje Jednotné přihlášení (SSO), vícefaktorové ověření a kontroly identity životního cyklu pro interní (zaměstnanci) a externí typy uživatelů.

1.1 Nabídky

Zákazník si může vybrat z následujících dostupných nabídek, přičemž všechny mají kapacitu událostí 400 událostí za sekundu.

1.1.1 IBM Cloud Identity Connect

Tato služba Cloud Service poskytuje Jednotné přihlášení (SSO) prostřednictvím ISAM and Open ID Connect (OIDC), Ověření jako službu pro cloudové ověření rozhraní API, příruční panel aplikace, reporting administrátora a analytický řídicí panel. Tato služba Cloud Service připojuje uživatele k aplikacím pomocí ověření založeného na moderních standardech a protokolech federace, včetně stovek konektorů pro běžné aplikace. Tato služba Cloud Service je úzce spojena s místním softwarovým programem IBM Security Access Management (ISAM), který je zahrnut jako aktivační software pro poskytování řešení Zákazníkovi na podporu potřeb jeho podnikání v oblasti správy přístupu zahrnující jak místní, tak cloudové aplikace.

1.1.2 IBM Cloud Identity Connect for ISAM

Tato služba Cloud Service je úzce spojena s místním softwarovým programem IBM Security Access Management (ISAM) pro poskytování řešení Zákazníkovi na podporu potřeb jeho podnikání v oblasti správy přístupu zahrnující jak místní, tak cloudové aplikace. Tato služba Cloud Service vyžaduje, aby měl Zákazník aktivní oprávnění Registrace a podpory softwaru (S&S) pro program IBM Security Access Management (ISAM), přičemž S&S musí zůstat aktivní po celou dobu trvání registrace služby Cloud Service Zákazníkem. Oprávnění Zákazníka k této službě Cloud Service musí být ekvivalentní oprávnění lokální licence ISAM Zákazníka. Ukončení S&S Zákazníkem způsobí rovněž ukončení této služby Cloud Service. Přístup k aktivačnímu softwaru stanovenému v části 5.2 není součástí této služby Cloud Service.

1.1.3 IBM Cloud Identity Essentials

Tato služba Cloud Service poskytuje Zákazníkovi funkce Jednotné přihlášení (SSO) k různým aplikacím IBM a veřejného cloudu, které Zákazník používá. Tuto službu Cloud Service lze spojit s MaaS360 od společnosti IBM pro zajištění dodatečné úrovně bezpečnostních kontrol, jako je podmíněný přístup.

1.1.4 IBM Cloud Identity Verify

Tato služba Cloud Service poskytuje vícefaktorové ověření pro aplikace chráněné pomocí Cloud Identity Connect, nebo prostřednictvím přímého vyvolání rozhraní API a pro další body vynucení včetně zákazníků RADIUS, serverů Unix/Linux a serverů Windows pro ověření jejich identity při přístupu k digitálním službám. To zahrnuje mechanismy, jako jsou e-mail, SMS a časově omezené (softwarový token) jednorázová hesla a mobilní biometrické ověření typu push založené na technologii IBM Verify. Tato služba Cloud Service je spojena s místním softwarovým programem IBM Security Access Management (ISAM) pro poskytování řešení Zákazníkovi na podporu potřeb jeho podnikání v oblasti správy přístupu zahrnující jak místní, tak cloudové aplikace. Je k dispozici samostatně nebo jako doplněk k Cloud Identity Connect, Cloud Identity Connect for ISAM a Cloud Identity Essentials.

1.1.5 IBM Cloud Identity Govern

Tato služba Cloud Service je úzce spojena s místním softwarovým programem IBM Governance and Intelligence (IGI), který je zahrnut jako aktivační software pro poskytování řešení Zákazníkovi na podporu potřeb jeho podnikání v oblasti správy přístupu zahrnující jak místní, tak cloudové aplikace. Tato služba Cloud Service poskytuje organizacím rozšířené funkce v oblasti správy životního cyklu identity v rámci cloudu a zahrnuje pracovní postup žádosti o přístup k aplikaci.

1.1.6 IBM Cloud Identity Connect and Verify

Tato služba Cloud Service nabízí Zákazníkovi funkce IBM Cloud Identity Connect a IBM Cloud Identity Verify jako jedinou nabídku.

1.1.7 IBM Cloud Identity Connect Verify and Govern

Tato služba Cloud Service nabízí Zákazníkovi funkce IBM Cloud Identity Connect, IBM Cloud Identity Verify a IBM Cloud Identity Govern jako jedinou nabídku.

1.2 Volitelné služby

1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud je samostatná instance platformy IBM Cloud Identity, kterou smí Uživatel používat výhradně pro interní neproduktivní aktivity, včetně například testování, ladění výkonu, diagnostiky chyb, interního srovnávání, fázování činností kontroly kvality a/nebo vývoje interně používaných dodatků nebo rozšíření služby Cloud Service s pomocí programovacích rozhraní zveřejněných aplikací. Tato služba Cloud Service nabízí možnost uzavřít dohodu o úrovních služeb (SLA), a to v souladu s podmínkami uvedenými v článku 3 Úrovně služeb a technické podpory. Tato služba Cloud Service má kapacitu 100 Událostí za sekundu.

1.2.2 IBM Cloud Identity Vanity Domain

Tato doména (jedna) umožňuje Zákazníkovi používat místo výchozí propůjčené domény, která je standardně poskytována platformou, doménu, kterou vlastní jeho organizace a která je pro ni relevantnější. IBM bude pro tuto doménu udržovat certifikát SSL, který bude každoročně obnovován.

1.3 Akcelerační služby

1.3.1 IBM Cloud Identity Connect Solution Planning

Tato služba poskytuje jeden (1) týden odborných služeb, během nichž společnost IBM poskytne některé nebo všechny následující položky:

- Vytvoření jednotného přihlášení pro cloudové aplikace SaaS
- Konfigurace podložky spuštění pro jednoduché vyhledání aplikace
- Propojení aplikací pomocí předpřipravených konektorů
- Plánování, architektura a návod řešení
- Doporučené přístupy a postupy IBM

1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Tato služba poskytuje tři (3) dny semináře odborných služeb zaměřených na výzvy multifaktorového ověření a zajištění aplikací Zákazníka s pomocí IBM Cloud Identity Verify. Seminář bude zahrnovat některá z následujících témat:

- Zabudování známého ověření do všech digitálních a osobních interakcí, pokud se ověření vyžaduje
- Povolení k tomu, aby aplikace vynucovaly silné ověření s pomocí rozhraní REST API přívětivého pro vývojáře
- Poskytnutí doporučení nejlepších postupů v oboru pro zabezpečení identity
- Efektivní uživatelské zkušenosti a převzetí všech provedení - telefonů, tabletů a notebooků

1.3.3 IBM Cloud Security Strategy and Planning

Tato služba poskytuje tři (3) týdny semináře odborných služeb o tom, jak uplatnit nejlepší postupy zabezpečení cloudu se zaměřením na zabezpečení infrastruktury a aplikace. Seminář bude zahrnovat některá z následujících témat:

- Vytvoření jednotného přihlášení pro cloudové aplikace SaaS
- Konfigurace podložky spuštění pro jednoduché vyhledání aplikace
- Propojení aplikací pomocí předpřipravených konektorů
- Plánování, architektura a návod řešení
- Přehled o rozvíjejících se trendech v oblasti kyber zabezpečení
- Doporučené přístupy a postupy IBM

1.3.4 IBM Cloud Identity Expert On Demand

Tato služba poskytuje dvacet (20) hodin odborných služeb dodaných ve dvou (2) hodinových relacích do třiceti (30) dní od zahájení. Služba poskytne architekta Cloud Identity, který odpoví na otázky a poskytne návody a doporučení, včetně například:

- Technických dovedností pro rozšíření implementace řešení Cloud Identity Zákazníkem
- Otázek týkajících se architektury a implementace řešení Cloud Identity Zákazníkem
- Návodu pro řešení a/nebo strategii Cloud Identity Zákazníka

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/í i) Evropské obecné nařízení o ochraně údajů (EU/2016/679) (GDPR); nebo ii) jiné zákony o ochraně údajů uvedené na adrese <http://www.ibm.com/dpa/dpl>.

<https://www.ibm.com/software/reports/compatibility/clarity-reports/report/html/softwareReqsForProduct?deliverableId=735E5650E26711E69CCD7F0385C6524D>

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 pokyny, jak kontaktovat IBM ohledně problémů s dostupností služby, jsou uvedeny na stránkách IBM v přehledu podpory pro SaaS na adrese https://www.ibm.com/software/support/saas_support_overview.html.

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

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

3.1.1 Další informace o této dohodě o úrovni služeb

Během prvních šedesáti (60) dnů doby trvání ("Počáteční doba trvání") není Zákazník oprávněn získat jakýkoli kredit v případě nedodržení minimální 99,9% dostupnosti prostředí IBM Cloud Identity dle této Dohody. Pokud před Počátečním obdobím trvání nebo během něj IBM zjistí, že stávající konfigurace, zásady, data nebo kód Zákazníka ("Předem existující komponenty") určené pro migraci ke službě IBM Cloud Identity Service by službě IBM Cloud Identity Service bránily v úspěšném dosažení procentuální dostupnosti v souladu s touto Dohodou, vyhrazuje si IBM právo informovat Zákazníka o takových Předem existujících komponentách a vyloučit je dle svého výhradního uvážení z ustanovení Dohody o úrovni služeb. V případě, že IBM Zákazníka informuje o jakýchkoli vyloučených Předem existujících komponentách, nese IBM odpovědnost za prezentaci plánu nápravy Zákazníkovi, který v rámci možností umožní, aby tyto vyloučené komponenty splnily procentuální dostupnost v souladu s touto Dohodou. Zákazník ponese výhradní odpovědnost za veškeré náklady související s touto nápravou, není-li oběma smluvními stranami dohodnuto jinak.

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 na adrese <https://www.ibm.com/support/home/pages/support-guide/>.

4. Poplatky

4.1 Metriky poplatků

Metriky poplatků za službu Cloud Service jsou uvedeny v Transakčním dokumentu.

Na tuto službu Cloud Service se uplatní následující metriky poplatků:

- Oprávněný uživatel je jedinečný uživatel, který má oprávnění pro přístup ke službám Cloud Services jakýmkoliv způsobem přímo či nepřímo (například prostřednictvím multiplexovacího programu, zařízení nebo aplikačního serveru) libovolnými prostředky.
- Zaměstnanec je jedinečná osoba, která je zaměstnána v Podniku Zákazníka, je placena Podnikem Zákazníka nebo jedná jménem Podniku Zákazníka, ať už má, či nemá udělen přístup ke službám Cloud Services.
- Vybraný účastník je každá fyzická nebo právnická osoba, která je způsobilá k účasti v jakémkoli programu poskytování služeb spravovaném nebo sledovaném prostřednictvím služeb Cloud Services.
- Instance je každý přístup ke specifické konfiguraci služeb Cloud Services.
- Sjednaná služba je profesionální nebo školicí služba související se službami Cloud Services.
- Událost je výskyt specifické události, která je zpracovávána nebo souvisí s použitím služeb Cloud Services.
 - Pro Cloud Identity Connect je Událost požadavek http vůči službě Cloud Service.
 - Pro Cloud Identity Verify je Událost vícefaktorová metoda vyvolaná službou Cloud Service.

5. Dodatečné podmínky

Na Smlouvy o službě Cloud Service (nebo ekvivalentní smlouvy o základním cloudu) uzavřené před 1. lednem 2019 se vztahují podmínky dostupné na adrese <https://www.ibm.com/acs>.

5.1 Reference Zákazníka

Zákazník souhlasí, že IBM může Zákazníka veřejně označovat jako odběratele služeb Cloud Service v reklamních nebo marketingových sděleních.

5.2 Aktivační software

Služba Cloud Service obsahuje následující Aktivační software:

Následující aktivační software se smí používat pouze se službami IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify a službami IBM Cloud Identity Connect Verify a Govern Cloud Services:

- IBM Security Access Manager Virtual Enterprise Edition

Následující aktivační software se smí používat pouze se službami IBM Cloud Identity Govern a IBM Cloud Identity Connect Verify a Govern Cloud Services:

- IBM Security Identity Governance and Intelligence Enterprise Edition
- IBM Security Identity Manager

5.3 MaxMind

Tato služba Cloud Service zahrnuje data GeoLite2 vytvořená MaxMind, dostupná z <http://www.maxmind.com>. GeoLite2 poskytuje geolokaci IP jako pomůcku při hledání geografické lokace počítače pomocí identifikace adresy IP.

5.4 Ověření

Zákazník i) povede a na vyžádání poskytne záznamy a výstupy ze systémových nástrojů v rozsahu přiměřeně potřebném pro IBM a jejího nezávislého auditora pro účely kontroly dodržování této Smlouvy ze strany Zákazníka a ii) neprodleně objedná a uhradí veškerá požadovaná oprávnění dle příslušné aktuální sazby IBM a uhradí i další poplatky a závazky stanovené na základě výsledků takového ověření, které IBM uvede na faktuře. Tyto povinnosti vzniklé v souvislosti s kontrolou dodržování podmínek jsou a budou účinné po dobu poskytování služeb Cloud Service a ještě dva roky poté.