IBM Security Verify

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

1.1.1 IBM Security Verify

IBM Security Verify pomáhá Zákazníkům zajistit produktivitu uživatelů pomocí cloudového, jednotného přihlášení (SSO), vícefaktorového ověření, řízení životního cyklu, adaptivního ověření, analýzy identity a řízení identity v rámci jediného dílu. Tato služba Cloud Service rovněž podporuje tisíce předem vytvořených konektorů, které pomohou poskytovat, zajistit přístup k populárním cloudovým aplikacím služeb a předem vytvořeným šablonám, které pomohou s integrací interních aplikací.

- Jednotné přihlášení

  Tato služba Cloud Service poskytuje Jednotné přihlášení (SSO) a 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 Verify Access a IBM Security Verify Application Gateway, 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.

- Vícefaktorové ověření

  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 mechanizmy, 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 Verify Access pro poskytování řešení Zákazníkovi na podporu potřeb jeho podnikání v oblasti správy přístupu zahrnující jak místní, tak cloudové aplikace.

- Adaptivní přístup

  Tato služba Cloud Service vyžaduje kombinaci Informační služby o hrozbách a umělé inteligence (AI), aby organizacím pomáhala přesně rozlišovat škodlivé a skutečné uživatele, když se uživatel pokouší o přístup k aplikaci chráněné službou. Služba využívá přehledy uživatelů, jejich zařízeních a vzorcích chování pro určení akce na zmírnění rizika v reálném čase: umožnění přístupu, vynucení ověření nebo zablokování přístupu. Tato služba využívá stovky datových bodů a kontextuálních informací získaných ze zařízení koncového uživatele pro vytvoření otisku prstu daného zařízení a výpočet holistické úrovně rizika relace. Zásady přístupu založené na riziku definované v pravidlech přístupu využívají úroveň rizika relace a další parametry pro stanovení akce systému. Tato služba je úzce propojena s hlášeními správce Security Verify, editorem zásad a pravidel přístupu a službou vícefaktorového ověření.

- Správa životního cyklu a řízení

  Tato služba Cloud Service úzce spolupracuje s místními softwarovými programy IBM Security Identity Governance and Intelligence (IGI) a IBM Security Identity Manager (ISIM), které jsou součástí aktivačního softwaru, aby Zákazníkům zajistila řešení na podporu jejich požadavků podnikání z hlediska řízení identity, a to jak místně, tak v cloudových aplikacích. Tato služba Cloud Service poskytuje organizacím rozšířené možnosti správy životního cyklu identity v cloudu, které

zahrnují synchronizaci účtu, pracovní postup požadavku na přístup do aplikace, certifikaci přístupu, zajišťování cloudových a místních aplikací. Zákazníci mohou zahrnout IBM Security Verify Account Synchronization jako doplňkovou službu.

- Analýzy

  Tato služba Cloud Service rozšiřuje stávající řešení IBM, jako jsou IBM Security Identity Governance and Intelligence (IGI) a IBM Security Identity Manager (ISIM), aby poskytovala holistický rizikový profil spravovaných uživatelů. Tato služba Cloud Service zahrnuje místní víceúčelový generátor analýz, který zpracovává data o činnosti a oprávnění z různých zdrojů, které poskytují komplexní přehled o přístupových rizicích s možností podniknout kroky na základě přehledu o těchto rizicích.

1.1.2 IBM Cloud Identity Connect

Tato služba Cloud Service poskytuje Jednotné přihlášení (SSO) a 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.

1.1.3 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.

1.1.4 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.

1.1.5 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 mechanizmy, 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.

1.1.6 IBM Cloud Identity Govern

Tato služba Cloud Service je úzce spojena s místním softwarovým programem IBM Security Identity Governance and Intelligence (IGI) a IBM Security Identity Manager (ISIM), 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 zahrnující pracovní postup žádosti o přístup k aplikaci.

1.1.7 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.

1.1.8 IBM Cloud Identity Analyze

Tato služba Cloud Service rozšiřuje stávající řešení IBM, jako jsou IBM Security Identity Governance and Intelligence (IGI) a IBM Security Identity Manager (ISIM), aby poskytovala holistický rizikový profil spravovaných uživatelů. Tato služba Cloud Service zahrnuje místní víceúčelový generátor analýz, který zpracovává data o činnosti a oprávnění z různých zdrojů, které poskytují komplexní přehled o přístupových rizicích s možností podniknout kroky na základě přehledu o těchto rizicích.

1.1.9 IBM Cloud Identity Adaptive Access

Tato služba Cloud Service využívá kontextuální přehledy o uživatelích, jejich zařízeních a vzorcích chování na bázi Umělé inteligence (AI), které pomáhají s uplatňováním správných zásad ověřování.

1.1.10 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 Security Verify Non-Production

IBM Security Verify Non-Production Environment on Cloud je samostatná instance platformy IBM Security Verify, 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 Security Verify 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.

1.2.3 IBM Security Verify Application Gateway Hosted

Brána aplikace poskytuje Zákazníkům, kteří hledají podporu pro nestandardní nebo starší mechanizmy ověřování lehké zařízení hostované a spravované IBM. Tyto mechanizmy zahrnují ověření na základě LTPA a záhlaví HTTP. Průběžné monitorování a údržbu spravuje IBM.

1.2.4 IBM Security Verify SMS and Email One-time Password

Služba poskytuje jednorázová hesla doručovaná e-mailem nebo SMS jako druhý faktor mechanizmu ověření.

1.2.5 IBM Security Verify Account Synchronization

Synchronizace účtu je proces, jehož prostřednictvím jsou účty z cílových aplikací konfigurovaných pro zajištění vzaty a přeneseny do Security Verify. Proces provádí ověření stávajících podrobností o účtu, uplatňuje zásady přizpůsobení a nápravy, aby byl systém zachován ve stavu odpovídajícím cílové aplikaci.

1.2.6 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.

1.2.7 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.

1.2.8 IBM Cloud Identity Application Gateway Hosted

Brána aplikace poskytuje Zákazníkům, kteří hledají podporu pro nestandardní nebo starší mechanizmy ověřování lehké zařízení hostované a spravované IBM. Tyto mechanizmy zahrnují ověření na základě LTPA a záhlaví HTTP. Průběžné monitorování a údržbu spravuje IBM.

1.3 Akcelerační služby

1.3.1 IBM Security Verify 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 Security 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 Identify 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 Security Verify 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 Security Verify 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 IBM Security Verify, který odpoví na otázky a poskytne návody a doporučení, včetně například:

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

1.3.5 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

1.3.6 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 Identify 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

1.3.7 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

1.3.8 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://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 za sjednaný měsíc minus celkový počet minut Odstávky služby za sjednaný měsíc děleno celkovým počtem minut za sjednaný měsíc a toto je specifické pro dotčenou oblast a počet registrovaných uživatelů daného regionu. 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 Cloud Service 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 Cloud Service by službě Cloud 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:

- 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 Security Verify SMS a Jednorázová hesla je Událost e-mail nebo SMS s doručeným jednorázovým heslem.
    - Pro Cloud Identity Connect je Událost požadavek http vůči službě Cloud Service.
- Pro Cloud Identity Verify je Událost vícefaktorová metoda vyvolaná službou Cloud Service. 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.
- Jednotka prostředku je nezávislé měření prostředků spravovaného či zpracovaného nebo souvisí s použitím služby Cloud Service.

Využití jednotlivých funkčních možností vyžaduje specifický počet oprávnění Zdrojových jednotek k předplatnému této služby Cloud Service:

		Funkční možnost je vázena Zdrojovými jednotkami nezbytnými pro Uživatele				
Odstupňovaná vrstva	**Maximální měsíční počet aktivních uživatelů**	**Jednotné přihlášení**	**Vícefaktorové ověření**	**Adaptivní přístup**	**Správa životního cyklu a řízení**	**Analýzy**
1	500	0,1000	0,1000	0,1000	0,2900	0,1200
2	5 000	0,0800	0,0800	0,0800	0,0750	0,1000
3	10 000	0,0600	0,0600	0,0600	0,0500	0,0750
4	100 000	0,0080	0,0080	0,0080	0,0050	0,0200
5	500 000	0,0025	0,0025	0,0025	0,0020	0,0150
6	1 000 000	0,0020	0,0020	0,0020	0,0010	0,0010
7	5 000 000	0,0015	0,0015	0,0015	0,0005	0,0005
8	10 000 000	0,0015	0,0015	0,0015	0,0002	0,0002
9	50 000 000	0,0010	0,0010	0,0010	0,0001	0,0001
10	999 999 999	0,0005	0,0005	0,0005	0,0001	0,0001

Poznámka: Všechny výpočty budou zaokrouhleny na celé číslo.

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:

- IBM Security Verify Bridge
- IBM Security Verify
- IBM Security Verify SDK (iOS)
- IBM Security Verify SDK (Android)
- IBM Security Verify SDK for JavaScript
- IBM Security Verify Bridge for Directory Sync
- IBM Application Gateway
- IBM Security Verify Hosted Application Gateway
- IBM Security Verify Gateway for Windows Login
- IBM Security Verify Gateway for PAM (on AIX)
- IBM Security Verify Gateway for PAM
- IBM Security Verify Gateway for RADIUS
- IBM Security Verify Credentials

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 Security Verify a 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