

IBM Cloud Identity

Ta opis storitve opisuje storitev v oblaku. Ustrezni dokumenti o naročilu nudijo cene in dodatne podrobnosti o naročnikovem naročilu.

1. Storitve v oblaku

IBM Cloud Identity zagotavlja enotno prijavo, večkratno preverjanje pristnosti ter kontrolnike za življenjski cikel identitete za notranje (uslužbence) in zunanje vrste uporabnikov.

1.1 Ponudbe

Naročnik lahko izbira med naslednjimi razpoložljivimi ponudbami, ki imajo vse zmogljivost dogodkov 400 dogodkov na sekundo.

1.1.1 IBM Cloud Identity Connect

Ta storitev v oblaku zagotavlja enotno prijavo prek ISAM in Open ID Connect (OIDC), preverjanje pristnosti kot storitev za pooblaščenje prek API-ja v oblaku, lansiranje aplikacij, poročanje skrbnika in nadzorno ploščo za analitiko. Ta storitev v oblaku poveže uporabnike z aplikacijami s sodobnimi standardi na osnovi preverjanja pristnosti in protokolov federacije, vključno s stotinami spojnikov do pogostih aplikacij. Ta storitev v oblaku se tesno integrira s sistemom programske opreme IBM Security Access Management (ISAM) na mestu uporabe, ki je vključen kot podporna programska oprema, pri čemer zagotavlja rešitev za naročnike v obliki podpore za poslovne zahteve naročnikov glede upravljanja dostopa do aplikacij na mestu uporabe in aplikacij v oblaku.

1.1.2 IBM Cloud Identity Connect za ISAM

Ta storitev v oblaku se tesno integrira s sistemom programske opreme IBM Security Access Management (ISAM) na mestu uporabe za zagotavljanje rešitve za naročnike v obliki podpore za poslovne zahteve glede upravljanja dostopa do aplikacij tako na mestu uporabe kot tudi aplikacij v oblaku. Zahteva za to storitev v oblaku je, da ima naročnik aktivno naročnino Software and Support (S&S) oz. upravičenost za sistem IBM Security Access Management (ISAM) in da ostane naročnina S&S aktivna v času trajanja naročnikove naročnine na storitev v oblaku. Naročnikovo upravičenje do te storitve v oblaku mora biti enakovredno naročnikovemu upravičenju licence ISAM na mestu uporabe. Prekinitev naročnikove S&S pomeni tudi prekinitev te storitve v oblaku. Dostop do podporne programske opreme, določene v razdelku 5.2, ni vključen v to storitev v oblaku.

1.1.3 IBM Cloud Identity Essentials

Ta storitev v oblaku naročnikom zagotavlja zmožnosti enotne prijave v različne IBM-ove aplikacije in aplikacije v javnem oblaku, ki jih naročniki uporabljajo. To storitev v oblaku je mogoče povezati z IBM-ovo rešitvijo MaaS360 za zagotavljanje dodatnih ravni varnostnih kontrol, kot je pogojni dostop.

1.1.4 IBM Cloud Identity Verify

Ta storitev v oblaku zagotavlja večkratno preverjanje pristnosti za aplikacije, zaščitene s Cloud Identity Connect ali prek neposrednega poziva API-ja, in za druge točke uveljavljanja, vključno z odjemalci RADIUS, strežniki Unix/Linux PAM in strežniki Windows, z namenom preverjanja njihovih identitet pri dostopanju do digitalne storitve. To vključuje mehanizme, kot so enkratna gesla po e-pošti, SMS-ih in s časovno omejitvijo (žeton programske opreme), ter preverjanje pristnosti s potisno mobilno biometriko, ki jo omogoča IBM Verify. Ta storitev v oblaku se integrira s sistemom programske opreme IBM Security Access Management (ISAM) na mestu uporabe za zagotavljanje rešitve za naročnike v obliki podpore za poslovne zahteve glede upravljanja dostopa do aplikacij tako na mestu uporabe kot tudi aplikacij v oblaku. Na voljo je samostojno ali kot dopolnitev za Cloud Identity Connect, Cloud Identity Connect for ISAM in Cloud Identity Essentials.

1.1.5 IBM Cloud Identity Govern

Ta storitev v oblaku se tesno integrira s sistemom programske opreme IBM Governance and Intelligence (IGI), ki je vključen kot podporna programska oprema, pri čemer zagotavlja rešitev za naročnike v obliki podpore za poslovne zahteve naročnikov glede upravljanja dostopa do aplikacij na mestu uporabe in

aplikacij v oblaku. ta storitev v oblaku zagotavlja organizacijo upravljanja naprednih identitet življenjskega cikla znotraj oblaka, in vključuje zahtevo za dostop do aplikacij delovnega toka.

1.1.6 IBM Cloud Identity Connect and Verify

Ta storitev v oblaku naročniku zagotavlja funkcionalnost izdelkov IBM Cloud Identity Connect in IBM Cloud Identity Verify v eni sami ponudbi.

1.1.7 IBM Cloud Identity Connect Verify and Govern

Ta storitev v oblaku naročniku zagotavlja funkcionalnost izdelkov IBM Cloud Identity Connect, IBM Cloud Identity Verify in IBM Cloud Identity Govern v eni sami ponudbi.

1.2 Izbirne storitve

1.2.1 IBM Cloud Identity Non-Production

IBM Cloud Identity Non-Production Environment on Cloud je ločeni primerek platforme IBM Cloud Identity, ki ga lahko naročnik uporablja samo za notranje neprodukcijske dejavnosti, ki med drugim vključujejo preizkušanje, nastavljanje zmogljivosti, diagnosticiranje napak, notranje primerjalne analize, uprizarjanje, dejavnosti zagotavljanja kakovosti in/ali razvijanje notranje uporabljenih dodatkov ali razširitev za storitev v oblaku prek objavljenih aplikacijskih programerskih vmesnikov. Ta storitev v oblaku lahko vsebuje pogodbo o ravni storitev za razpoložljivost (SLA) pod pogoji iz razdelka 3 Ravni storitev in tehnična podpora. Ta storitev v oblaku ima zmogljivost 100 dogodkov na sekundo.

1.2.2 IBM Cloud Identity Vanity Domain

Osebna domena (ena domena) naročniku omogoča, da namesto privzete najemniške domene, ki jo vnaprej pripravljeno ponuja platforma, uporablja domeno, ki je v lasti njegove organizacije in je bolj relevantna za to organizacijo. Potrdilo SSL bo za to domeno vzdrževal IBM in se bo obnavljalo vsako leto.

1.3 Pospeševalne storitve

1.3.1 IBM Cloud Identity Connect Solution Planning

Ta storitev zagotavlja en (1) teden strokovnih storitev, med katerimi bo IBM izvedel nekaj ali vse od spodaj naštetega:

- Vzpostavitev enotne prijave za aplikacije SaaS v oblaku
- Konfiguracija odskočne deske za preprosto lokacijo aplikacij
- Povezava aplikacij z že pripravljenimi spojniki
- Načrtovanje rešitev, arhitektura in vodenje
- IBM-ov priporočeni pristop in prakse

1.3.2 IBM Cloud Identity Verify Workshop for Multi-Factor Authentication

Ta storitev zagotavlja tridnevno (3) delavnico s strokovnimi storitvami, ki se osredotoča na izzive večkratnega preverjanja pristnosti in zaščito naročnikovih aplikacij z IBM Cloud Identity Verify. Delavnica bo zajemala nekaj ali vse od spodaj naštetega:

- Vdelava poznanega preverjanja pristnosti v vse digitalne in osebne interakcije, kjer je preverjanje pristnosti zahtevano
- Omogočanje, da aplikacija uveljavi močno preverjanje pristnosti s pomočjo razvijalca prijaznega API-ja REST
- Zagotovitev priporočil glede najboljših praks v panogi o zaščiti identitete
- Boljša uporabniška izkušnja in uvedba v vseh oblikah - telefonih, tabličnih računalnikih in prenosnikih

1.3.3 IBM Cloud Security Strategy and Planning

Ta storitev zagotavlja tritedensko (3) delavnico strokovnih storitev, kako uveljaviti najboljše prakse zaščite v oblaku s poudarkom na zaščiti infrastrukture in aplikacije. Delavnica bo zajemala nekaj ali vse od spodaj naštetega:

- Vzpostavitev enotne prijave za aplikacije SaaS v oblaku
- Konfiguracija odskočne deske za preprosto lokacijo aplikacij

- Povezava aplikacij z že pripravljenimi spojniki
- Načrtovanje rešitev, arhitektura in vodenje
- Vpogledi v nove trende v kibernetiki varnosti
- IBM-ov priporočeni pristop in prakse

1.3.4 IBM Cloud Identity Expert On Demand

Ta storitev zagotavlja dvajset (20) ur strokovnih storitev, ki se izvajajo v dvehurnih (2) sejah v tridesetih (30) dneh od začetka. Storitve bodo zagotovile arhitekta za Cloud Identity, ki bo na voljo za odgovore na vprašanja ter pomoč in priporočila, kar med drugim vključuje:

- Tehnične veščine za pomoč pri uvedbi naročnikove rešitve Cloud Identity
- Vprašanja glede arhitekture in uvedbe naročnikove rešitve Cloud Identity
- Svetovanje o naročnikovi rešitvi Cloud Identity in/ali strategiji

2. Podatkovni listi za obdelavo in varstvo podatkov

IBM-ov dodatek k obdelavi podatkov <http://ibm.com/dpa> (DPA) in podatkovni list za obdelavo in varstvo podatkov (podatkovni list) podaja dodatne informacije o varstvu podatkov za storitve v oblaku in možnosti v zvezi z vrstami vsebine, ki se lahko obdeluje, vključene delavnosti obdelave, funkcije varstva podatkov in podrobnosti glede hrambe in vračila vsebine. DPA velja za osebne podatke, ki jih zajema vsebina, če in v obsegu, v katerem veljajo i) Splošna uredba EU o varstvu podatkov (EU/2016/679) (GDPR); ali ii) drugi zakoni o varstvu podatkov, navedeni na spletni strani <http://www.ibm.com/dpa/dpl>.

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

3. Ravni storitve in tehnična podpora

3.1 Ravni storitve in tehnična podpora

IBM naročniku zagotavlja naslednjo pogodbo o ravni storitev za razpoložljivost ("SLA"). IBM bo priznal najvišje veljavno nadomestilo na podlagi zbirne razpoložljivosti storitve v oblaku, kot je prikazano v spodnji tabeli. Razpoložljivost, izražena v odstotkih, se izračuna kot skupno število minut v pogodbenem mesecu, zmanjšano za skupno število minut nerazpoložljivosti v pogodbenem mesecu, deljeno s skupnim številom minut v pogodbenem mesecu. Definicija nerazpoložljivosti storitve, postopek in kako kontaktirati IBM v zvezi z razpoložljivostjo storitve, so za uveljavljanje zahtevka v IBM-ovem pregledu podpore SaaS na naslovu https://www.ibm.com/software/support/saas_support_overview.html.

Razpoložljivost	Dobropis (% mesečne naročnine*)
Manj kot 99,9 %	10 %

* Naročnina je pogodbeno cena za mesec, za katerega velja zahtevka.

3.1.1 Druge informacije o pogodbi o ravni storitev

V prvih šestdesetih (60) dneh naročniškega razmerja ("obdobje začetnega preskušanja") naročnik ni upravičen do nobenega dobropisa v primeru, če okolje IBM Cloud Identity ne doseže minimalnega 99,9-odstotnega neprekinjenega delovanja, kot ga določa ta pogodba. Če IBM pred ali med obdobjem začetnega preskušanja zazna obstoječe naročnikove konfiguracije, pravilnike, podatke ali kode ("prej obstoječe komponente"), ki naj bi bile premaknjene v storitev IBM Cloud Identity in ki bi preprečile, da bi storitev IBM Cloud Identity Service uspešno dosegla zahtevan odstotek neprekinjenega delovanja iz te pogodbe, si IBM privzema pravico, da naročnika obvesti o takšnih prej obstoječih komponentah in jih po lastni presoji izvzame iz določb pogodbe o ravni storitev. Če IBM obvesti naročnika o morebitnih izvzetih prej obstoječih komponentah, mora IBM naročniku predstaviti načrt za sanacijo, kolikor je to mogoče, kar omogoča, da takšne izvzete komponente dosežejo zahtevan odstotek neprekinjenega delovanja iz te pogodbe. Naročnik je edini odgovorni za tako sanacijo, razen če se stranki ne dogovorita drugače.

3.2 Tehnična podpora

Tehnično podporo za storitev v oblaku, vključno s kontaktnimi podatki podpore, stopnjami resnosti, odzivnimi časi podpore, časom odgovora in drugimi informacijami in procesi, naročnik najde tako, da

izbere storitev v oblaku v storitvi IBM Support, ki je na voljo na <https://www.ibm.com/support/home/pages/support-guide/>.

4. Stroški

4.1 Metrike zaračunavanja

Metrike zaračunavanja za storitev v oblaku so podane v transakcijskem dokumentu.

Za to storitev v oblaku se uporabljajo naslednje metrike zaračunavanja:

- Pooblaščen uporabnik je edinstveni uporabnik, ki lahko dostopa do storitve v oblaku na kateri koli posreden ali neposreden način, prek katerega koli sredstva (na primer prek multipleksirnega programa, naprave ali aplikacijskega strežnika).
- Zaposleni je edinstvena oseba, ki je zaposlena v naročnikovem podjetju oziroma je drugače plačana z njegove strani ali deluje v njegovem imenu, ne glede na to, ali ima dostop do storitev v oblaku ali ne.
- Upravičeni udeleženec je posameznik ali subjekt, upravičen do sodelovanja v katerem koli programu za dobavo storitev, ki ga upravljajo ali mu sledijo storitve v oblaku.
- Primerek je vsak dostop do določene konfiguracije storitev v oblaku.
- Engagement je profesionalna ali izobraževalna storitev, povezana s storitvijo v oblaku.
- Dogodek je primer določenega dogodka, ki ga obdelajo storitve v oblaku ali je povezan z uporabo teh storitev.
 - Pri Cloud Identity Connect je dogodek zahteva HTTP za storitev v oblaku.
 - Pri Cloud Identity Verify je dogodek metoda večkratnega preverjanja, ki se pokliče prek storitve v oblaku.

5. Dodatna določila

Za pogodbe o storitvi v oblaku (ali enakovredne osnovne pogodbe), podpisane pred 1. januarjem 2019, veljajo pogoji, ki so na voljo na <https://www.ibm.com/acs>.

5.1 Omembe naročnika

Naročnik soglaša, da ga lahko IBM v oglaševalskih ali tržnih komunikacijah javno imenuje kot naročnika na storitve v oblaku.

5.2 Podporna programska oprema.

Storitev v oblaku vsebuje naslednjo podporno programsko opremo:

Naslednja podporna programska oprema se lahko uporablja samo s storitvami v oblaku IBM Cloud Identity Connect, IBM Cloud Identity Connect and Verify in IBM Cloud Identity Connect Verify and Govern:

- IBM Security Access Manager Virtual Enterprise Edition

Naslednja podporna programska oprema se lahko uporablja samo s storitvami v oblaku IBM Cloud Identity Govern in IBM Cloud Identity Connect Verify and Govern:

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

5.3 MaxMind

Ta storitev v oblaku vključuje podatke GeoLite2, ustvarjene s storitvijo MaxMind, ki je na voljo na spletnem mestu <http://www.maxmind.com>. GeoLite2 zagotavlja geolokacijo naslova IP, ki je v pomoč pri lociranju geografske lokacije računalnika prek identifikacije naslova IP.

5.4 Preverjanje

Naročnik bo i) hranil in na zahtevo posredoval zapise in produkte sistemskih orodij, kot je v razumni meri potrebno, da IBM in njegovi neodvisni revizorji preverjajo naročnikovo spoštovanje te pogodbe, ter bo ii) nemudoma naročil in plačal morebitna zahtevana pooblastila (vključno s povezano naročnino in podporo ali vzdrževanjem) po IBM-ovih tedaj veljavnih tarifah ter druge stroške in obveznosti, ugotovljene

na podlagi takega preverjanja, kot jih IBM navede na računu. Te obveznosti v zvezi s preverjanjem skladnosti ostanejo v veljavi med obdobjem trajanja storitev v oblaku in dve leti po tem.