IBM Security Verify

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

1. Storitev 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.

1.1.1 IBM Security Verify

IBM Security Verify pomaga naročnikom, da zagotovijo storilnost uporabnikov z v oblaku zagotovljenim, večkratnim preverjanjem pristnosti z enotno prijavo, upravljanjem življenjskega cikla, prilagodljivim preverjanjem pristnosti, analitiko identitete in upravljanjem identitete pod eno samo številko dela. Ta storitev v oblaku podpira tudi tisoče vnaprej zgrajenih spojnikov, ki pomagajo zagotoviti dostop do priljubljenih aplikacij storitve v oblaku in vnaprej zgrajenih predlog za pomoč pri integraciji internih aplikacij.

- Enotna prijava

  Ta storitev v oblaku zagotavlja enotno prijavo in Open ID Connect (OIDC), preverjanje pristnosti kot storitev za pooblaščanje prek API-ja v oblaku, lansirnik 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 Verify Access na mestu uporabe in IBM Security Verify Application Gateway, 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.

- Večkratno preverjanje pristnosti

  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 Verify Access 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.

- Prilagodljiv dostop

  Ta storitev v oblaku uporablja kombinacijo obveščanja o grožnjah in umetne inteligence (UI), s katero organizacijam pomaga natančno razlikovati med zlonamernimi in pravimi uporabniki, ko poskuša uporabnik dostopati do aplikacij, ki jo varuje storitev. Ta storitev v oblaku uporablja vpoglede v uporabnike, njihove naprave in vedenjske vzorce, s katerimi v realnem času določi ukrep za zmanjševanje tveganja: dovoli dostop, vsili preverjanje pristnosti ali blokiraj dostop. Storitev uporablja na stotine podatkovnih točk in kontekstualnih informacij, zbranih iz naprave končnega uporabnika, s katerimi naredi prstni odtis naprave in izračuna raven celostnega tveganja seje. Pravila za dostop na osnovi tveganja, določena v pravilniku za dostop, uporabijo raven tveganja seje z dodatnimi parametri za določanje sistemskega dejanja. Ta storitev je tesno povezana s poročili skrbnika Security Verify, urejevalnikom pravil pravilnika za dostop in storitvijo večkratnega preverjanja pristnosti.

- Upravljanje življenjskega cikla

  Ta storitev v oblaku se tesno integrira s sistemom programske opreme IBM Security Identity Governance and Intelligence (IGI) in IBM Security Identity Manager (ISIM) 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 identitete, tako za aplikacije na mestu uporabe kot aplikacije v oblaku. Ta storitev v oblaku organizacijam zagotavlja napredne zmožnosti upravljanja življenjskega cikla identitete v oblaku, ki vključuje sinhronizacijo računov, delovni tok zahteve za dostop do aplikacije, potrjevanje dostopa, preskrbo v oblak in aplikacije na mestu uporabe. Naročniki lahko IBM Security Verify Account Synchronization vključijo kot dodatno storitev.

- Analitika

  Ta storitev v oblaku dopolni obstoječe IBM-ove rešitve, kot sta IBM Security Identity Governance and Intelligence (IGI) in IBM Security Identity Manager (ISIM), ter tako zagotovi celosten profil tveganja upravljanih uporabnikov. Ta storitev v oblaku vključuje večnamenski mehanizem za analitiko na mestu uporabe, ki obdeluje podatke o dejavnosti in upravičenju iz različnih virov, ki zagotavlja 360-stopinjski pregled nad tveganji dostopa z možnostjo ukrepanja na osnovi vpogledov v ta tveganja.

1.1.2 IBM Cloud Identity Connect

Ta storitev v oblaku zagotavlja enotno prijavo in Open ID Connect (OIDC), preverjanje pristnosti kot storitev za pooblaščanje prek API-ja v oblaku, lansirnik 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.

1.1.3 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.

1.1.4 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.

1.1.5 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.

1.1.6 IBM Cloud Identity Govern

Ta storitev v oblaku se tesno integrira s sistemom programske opreme IBM Security Identity Governance and Intelligence (IGI) in IBM Security Identity Manager (ISIM) 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. Ta storitev v oblaku organizacijam zagotavlja napredne zmožnosti upravljanja življenjskega cikla identitete v oblaku, ki vključuje delovni tok zahteve za dostop do aplikacije.

1.1.7 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.

1.1.8 IBM Cloud Identity Analyze

Ta storitev v oblaku dopolni obstoječe IBM-ove rešitve, kot sta IBM Security Identity Governance and Intelligence (IGI) in IBM Security Identity Manager (ISIM), ter tako zagotovi celosten profil tveganja upravljanih uporabnikov. Ta storitev v oblaku vključuje večnamenski mehanizem za analitiko na mestu uporabe, ki obdeluje podatke o dejavnosti in upravičenju iz različnih virov, ki zagotavlja 360-stopinjski pregled nad tveganji dostopa z možnostjo ukrepanja na osnovi vpogledov v ta tveganja.

1.1.9 IBM Cloud Identity Adaptive Access

Ta storitev v oblaku uporablja kontekstualne vpoglede z umetno inteligenco (UI) v uporabnike, njihove naprave in vedenjske vzorce, s pomočjo katerih lahko organizacije izvajajo prave pravilnike preverjanja pristnosti.

1.1.10 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 Security Verify Non-Production

IBM Security Verify Non-Production Environment on Cloud je ločeni primerek platforme IBM Security Verify, 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 Security Verify 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.

1.2.3 IBM Security Verify Application Gateway Hosted

Prehod aplikacije zagotavlja poenostavljeno napravo, s katero upravlja in jo gosti IBM in ki je namenjena naročnikom, ki želijo podpreti nestandardne ali podedovane mehanizme za preverjanje pristnosti. Ti mehanizmi vključujejo preverjanje pristnosti na osnovi LTPA in glave HTTP. Stalen nadzor in vzdrževanje izvaja IBM.

1.2.4 IBM Security Verify SMS and Email One-time Password

Storitev zagotavlja enkratna gesla, dostavljena prek e-pošte in storitve kratkih sporočil (SMS), kot mehanizem preverjanja pristnosti drugega faktorja.

1.2.5 IBM Security Verify Account Synchronization

Sinhronizacija računa je proces, v katerem se račune iz ciljnih aplikacij, konfiguriranih za preskrbo, pridobi in vpelje v Security Verify. Proces izvede preverjanje pristnosti obstoječih podrobnosti računa ter uvede pravilnike uvedbe in sanacije, da se sistem ohrani v skladnem stanju s ciljno aplikacijo.

1.2.6 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.

1.2.7 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.

1.2.8 IBM Cloud Identity Application Gateway Hosted

Prehod aplikacije zagotavlja poenostavljeno napravo, s katero upravlja in jo gosti IBM in ki je namenjena naročnikom, ki želijo podpreti nestandardne ali podedovane mehanizme za preverjanje pristnosti. Ti mehanizmi vključujejo preverjanje pristnosti na osnovi LTPA in glave HTTP. Stalen nadzor in vzdrževanje izvaja IBM.

1.3 Pospeševalne storitve

1.3.1 IBM Security Verify 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 Security 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 Identify 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 razvijalcem 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 Security Verify 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 kibernetski varnosti
- IBM-ov priporočeni pristop in prakse

1.3.4 IBM Security Verify Expert On Demand

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

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

1.3.5 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

1.3.6 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 Identify 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 razvijalcem 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

1.3.7 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 kibernetski varnosti
- IBM-ov priporočeni pristop in prakse

1.3.8 IBM Cloud Identity Expert On Demand

Ta storitev zagotavlja dvajset (20) ur strokovnih storitev, ki se izvajajo v dvournih (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) podajata dodatne informacije o varstvu podatkov za storitve v oblaku in možnosti v zvezi z vrstami vsebine, ki se lahko obdeluje, vključene dejavnosti 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://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 Pogodba o ravni storitev

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, in je specifična za prizadeto regijo in za število naročenih uporabnikov v tej regiji. 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 pogodbena cena za mesec, na katerega se nanaša zahtevek.

3.1.1 Druge informacije o pogodbi o ravni storitev

V času prvih šestdesetih (60) dni naročnikovega obdobja veljavnosti ("obdobje burn-in") naročnik ni upravičen do nobenega dobropisa, če okolje storitve v oblaku ne doseže minimalno 99,9 % časa delovanja po tej pogodbi. Če pred ali v obdobju Burn-In IBM identificira obstoječe naročnikove konfiguracije, pravilnike, podatke ali kodo ("obstoječe komponente"), ki bodo preseljene v storitev v oblaku in ki bi storitvi v oblaku preprečevale, da uspešno doseže odstotek časa delovanja iz te pogodbe, si IBM pridrži pravico, da obvesti naročnika o teh 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, časom razpoložljivosti podpore, odzivnim časom in drugimi informacijami ter 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:

- 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 Security Verify SMS and One-Time Password je dogodek enkratno geslo, dostavljeno prek e-pošte ali storitve kratkih sporočil (SMS).
    - Pri Cloud Identity Connect je dogodek zahteva HTTP za storitev v oblaku.
- Pri Cloud Identity Verify je dogodek katerakoli večkratna metoda, ki je poklicana prek storitve v oblaku. Pooblaščeni 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.
- Enota vira je neodvisna mera vira, ki jo upravlja ali obdela storitev v oblaku oz. je povezana z uporabo storitev v oblaku.

  Uporaba vsake funkcionalne zmožnosti zahteva določeno število pooblastil za enoto sredstva za to naročnino na storitev v oblaku:

		Funkcionalna zmožnost v uteženih enotah sredstva, potrebnih na uporabnika				
Stopnjevana plast	**Maksimum mesečnih aktivnih uporabnikov**	**Enotna prijava**	**Večkratno preverjanje pristnosti**	**Prilagodljiv dostop**	**Upravljanje življenjskega cikla**	**Analitika**
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

Opomba: Vsi izračuni se zaokrožijo navzgor na celo število.

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:

- 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

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 Security Verify and IBM Cloud Identity Govern and IBM Cloud Identity Connect Verify and Govern:

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