JumpCloud platforma za IT sustave

Mršić, Patrik

VELEUČILIŠTE SUVREMENIH INFORMACIJSKIH TEHNOLOGIJA

STRUČNI PRIJEDIPLOMSKI STUDIJ INFORMACIJSKIH TEHNOLOGIJA

Patrik Mršić

ZAVRŠNI RAD

JUMPCLOUD PLATFORMA ZA IT SUSTAVE

Zagreb, listopada 2024.

Veleučilište suvremenih informacijskih tehnologija
10000 Zagreb, Ulica Vjekoslava Klaića 7

Studij:	Stručni prijediplomski studij informacijskih tehnologija smjer računalni sustavi i mreže
Student:	**Patrik Mršić**
Matični broj:	2019003

Zadatak završnog rada

Predmet:	Multimedijske mreže i sustavi
Naslov:	**JumpCloud platforma za IT sustave**
Zadatak:	Opisati proces IT administracije, konfiguracije, održavanja i nadzora uređaja na IT mreži. Objasniti način SSO i korištenje LDAP protokola na JumpCloud IT platformi. Prikazati neke osnovne funkcionalnosti na JumpCloud IT platformi.
Mentor:	Saša Punčikar, pred.
Zadatak uručen kandidatu:	8.7.2024.
Rok za predaju rada:	23.10.2024.
Rad predan:	_____

Povjerenstvo:

Dražen Novina, pred.	član predsjednik	_____
Saša Punčikar, pred.	mentor	_____
Dubravko Žižak, pred.	član	_____

SADRŽAJ

POPIS SLIKA

POPIS KODOVA

1. UVOD

Upravljanje identitetima i pristupom – IAM postaje sve važnija komponenta u modernim IT rješenjima, posebno u svijetu tehnologija u oblaku, gdje sve više organizacija, ne samo u IT sektoru već i u drugim industrijama, prelazi na oblak radi optimizacije resursa i smanjenja troškova. Ovaj prelazak na oblak donosi niz prednosti, uključujući bržu implementaciju aplikacija, skalabilnost i fleksibilnost u odgovoru na promjenjive potrebe korisnika. Međutim, prelazak na oblak također povećava kompleksnost IT sustava i otvara nove sigurnosne izazove koji zahtijevaju napredna rješenja za upravljanje korisničkim identitetima i kontrolu pristupa.

U složenom okruženju suvremenih IT sustava, sigurnost i zaštita podataka postaju ključni aspekti svakodnevnog poslovanja. IT administracija igra ključnu ulogu u očuvanju integriteta, povjerljivosti i dostupnosti podataka. Organizacije su sve svjesnije da prelazak na oblak nije samo pitanje tehničke migracije, već i stvaranje sigurnog okvira za upravljanje identitetima korisnika i njihovim pravima pristupa. To uključuje osiguravanje da ovlašteni korisnici mogu pristupiti potrebnim resursima, dok se neovlašteni pristupi moraju učinkovito blokirati kako bi se spriječili sigurnosni incidenti.

Oblak je postao jedan od najpopularnijih oblika IT infrastrukture jer omogućava organizacijama značajne uštede na troškovima hardvera, održavanja, te brzinu i fleksibilnost operacija. Oblak ne samo da pojednostavljuje upravljanje resursima, već omogućuje bržu prilagodbu novim tehnološkim zahtjevima i promjenama na tržištu. Ipak, prelazak na oblak nosi sa sobom i nove izazove u pogledu zaštite podataka i upravljanja korisničkim pravima. Upravo iz tih razloga, potreba za robusnim i fleksibilnim IAM rješenjima postaje sve veća. Ova rješenja omogućuju organizacijama centralizirano upravljanje korisnicima, uređajima, pravima pristupa i aplikacijama, čime osiguravaju veću sigurnost i kontrolu nad svojim IT resursima. Jedno od vodećih IAM rješenja u oblaku je JumpCloud, platforma koja omogućava organizacijama jednostavno i centralizirano upravljanje korisnicima, uređajima, te resursima u IT sustavu. JumpCloud je dizajniran kao sveobuhvatan alat za IT administratore, omogućujući im da s jedne točke upravljaju svim korisničkim identitetima u organizaciji, bez obzira na to koriste li korisnici različite uređaje ili operativne sustave. Osim toga, JumpCloud nudi funkcionalnosti poput višefaktorske autentifikacije – MFA, jedinstvene prijave – SSO, sinkronizacije s Active Directoryjem, kao i mogućnost integracije s različitim aplikacijama putem LDAP-a (eng. Lightweight Directory Access Protocol) ili drugih standardnih protokola.

Sve ove mogućnosti čine JumpCloud izuzetno fleksibilnim i moćnim alatom za organizacije

koje traže načine za unaprjeđenje sigurnosti i pojednostavljivanje IT administracije. Pored upravljanja korisnicima, JumpCloud omogućuje daljinsko slanje komandi za ažuriranje uređaja, instalaciju softvera, te kontrolu nad resursima putem administrativnog sučelja. To omogućava IT administratorima da brzo i učinkovito implementiraju potrebne promjene u cijeloj organizaciji, bez obzira na fizičku lokaciju korisnika ili uređaja.

U ovom radu, detaljno su obrađeni ključni segmenti JumpCloud platforme, uključujući upravljanje korisnicima, integraciju s Active Directoryjem, implementaciju višefaktorske autentifikacije, te daljinsko upravljanje uređajima. Također su objašnjene tehnologije poput SSO-a (eng. Single Sign-On), DaaS-a (eng. Directory-as-a-Service), te LDAP-a, koje omogućuju fleksibilnu i skalabilnu implementaciju unutar organizacija. Kroz praktični dio, izvršena je analiza mrežnih paketa s pomoću Wiresharka, što će omogućiti detaljan uvid u način na koji JumpCloud agent komunicira sa serverom, te kako se putem mreže prenose i obrađuju podaci o korisnicima i uređajima.

Ova analiza prikazuje kako JumpCloud ne samo da olakšava upravljanje velikim brojem korisnika i uređaja, već i poboljšava sigurnost cjelokupne IT infrastrukture organizacije. Sve ovo čini JumpCloud ključnim alatom u modernim IT okruženjima koja su sve više orijentirana prema oblaku i udaljenom radu, gdje sigurnost i efikasnost upravljanja resursima igraju ključnu ulogu u uspjehu organizacije.

2. IT ADMINISTRACIJA I NJEZINA ULOGA

Kako bi se približila tema JumpCloud Open Directory platforme, oslonac se stavlja na samu ulogu IT administracije uz opise ključnih točaka koje sadrži i sami JumpCloud. U IT sektoru unazad nekoliko godina dogodile su se jake dinamične promjene i donijele su napredne tehnologije koje sada već iziskuju stručno znanje za njihovo održavanje. Globalna digitalna transformacija omogućuje tvrtkama i organizacijama da odgovornost održavanja informatičkog sustava prebace na IT specijaliste i administratore. Te usluge pružaju centralizirani i efikasni IT menadžment same tvrtke. Tu spada uvođenje i održavanje IT opreme, njezin popravak i razne konfiguracije te vodi do toga da IT administratori sada vode čitavu informatičku brigu o samoj tvrtki.

2.1. IT administracija

IT administracija uključuje savjetodavne usluge, tehničku podršku te udaljeno spajanje na korisnička računala u svrhu bržeg rješavanja problema. IT administratori su ključne osobe odgovorne za procese konfiguracije, održavanja cjelokupne IT opreme što uključuje softverske, hardverske, operacijske, mrežne sustave i strukture.

Vrste IT usluga su:

- instalacija i održavanja računala i ostalih uređaja
- održavanje mrežne strukture i servera
- informatička podrška
- nadzor i izvještaj o stanju IT sustava
- usluge savjetovanja
- menadžment i povrat podataka

IT administracija se može podijeliti na sistemsku i mrežnu IT administraciju. Sistemska stvara zaduženje za računalne sisteme, njihovo održavanje i upravljanje serverima, dok se mrežna IT administracija bavi konfiguriranjem, testiranjem, upravljanjem i dijagnosticiranjem kvarova same mreže i mrežne opreme u organizaciji. Uključuje i kibernetičku zaštitu, usluge cloud servisa, te vođenje *backup* baze podataka klijenata i same organizacije. Sveukupno, IT podrška obuhvaća i serversku i mrežnu IT podršku gdje se sistem administratori usredotočuju i na operacijske sustave, softverske platforme ali, i servere te ostale mrežne komponente. U današnje se vrijeme organizacije češće prebacuju na IT okruženja u oblaku. Ključni razlog je

jednostavnije i brža prilagodba poslovnim potrebama. Premještanje elektroničke pošte, softvera za produktivnost poput Microsoft Officea i Google Workspacea te pohrane podataka u virtualna okruženja znatno je olakšano zahvaljujući uslugama u oblaku. Oblak omogućuje organizacijama smanjenje troškova ulaganja u fizičku IT infrastrukturu, povećanje fleksibilnosti rada, kao i lakše upravljanje sigurnosnim i operativnim izazovima. Različite opcije i rješenja koja se nude u oblaku omogućuju integraciju svih ključnih funkcija u jedinstveno okruženje, što olakšava održavanje IT sustava i poboljšava učinkovitost poslovanja.

2.2. Upravljanje uređajima

Kada se govori o upravljanju uređajima, u širem smislu riječi, govori se o procesu kontrole, konfiguracije, nadgledanja i održavanja svih uređaja koji pripadaju jednoj IT infrastrukturi organizacije. Proces obuhvaća različite vrste uređaja od računala, mobilnih uređaja, mrežnih uređaja i sl. I jedan je od najbitnijih stavki IT administracije.

Ključni elementi u upravljanju uređajima:

- konfiguracija uređaja
- nadgledanje uređaja i dijagnostika
- sigurnost sustava
- ažuriranje i održavanje softvera i operativnih sustava
- udaljena podrška

2.2.1. Konfiguracija uređaja

Proces konfiguracije uređaja uključuje postavljanje, instalaciju i prilagodbu hardverskih i softverskih značajki uređaja. Ovaj proces može obuhvaćati različite korake, a konfiguracija ovisi o vrsti uređaja i njegovoj namjeni. IT administrator mora biti upoznat s poslovnom svrhom korištenja uređaja, njegovim specifikacijama te kontekstom unutar organizacije. Osnovni dio konfiguracije je instalacija operativnih sustava (kao što su Windows, macOS, Linux, iOS, Android). Priprema uređaja se odvija u najkraćem mogućem roku, a osim instalacije operativnog sustava uključuje i podešavanje regionalnih postavki, jezičnih opcija, mrežnih parametara i drugih ključnih značajki. Sukladno navedenom instalira se i konfigurira potrebni softver i aplikacije na uređaju. U to spadaju alati za upis podataka i produktivnost (*Microsoft Office*), antivirusni alati, aplikacije i alati potrebni za upravljanje projektima ili specifične industrijske aplikacije, sve što je stvoreno za potrebu jedne organizacije. Postavljaju se sigurnosni parametri kako bi se osigurali da je uređaj potrebno zaštićen od potencijalnih

prijetnji, u to spadaju postavljanje lozinki, izrada posebnog korisničkog računa za pojedinu osobu u organizaciji što omogućuje i upravljanje pristupom, šifriranje diska i sl. Konfiguriraju se mrežne postavke, da bi uređaj bio potpun u mrežnoj infrastrukturi organizacije u kojoj se nalazi, da bi mogao pristupiti internetu te lokalnoj mreži same organizacije. Namještaju se VPN (eng. Virtual Private Network) postavke, postavke IP (eng. Internet Protocol) adrese, DNS (eng. Domain Name System) servera i drugih mrežnih parametara. Sama konfiguracija uređaja je ključan korak u implementiranju i uporabi unutar organizacije jer omogućuje da uređaji budu spremni za produktivnu upotrebu, da su isto tako osigurani od sigurnosnih rizika i prilagođeni potrebama korisnika i njegovog rada u organizaciji.

2.2.2. Nadgledanje uređaja i dijagnostika

Jedan je od ključnih aspekata upravljanja uređajima koji omogućuje organizacijama i IT administratorima da prate performanse svojih uređaja, lakše identificiraju kvarove i probleme te tako brzo reagiraju na otklanjanju istih da bi se održala stabilnost i funkcionalnost same IT infrastrukture. Praćenje performansi obuhvaća širok spektar, od resursa procesora i memorije (radne ili memorije pohrane uređaja) do pregleda mrežnog prometa po potrebi. Pregledava se i mrežni promet uređaja po potrebi. To su ugrubo najčešći parametri koje nadgledaju IT administratori u organizaciji. U tom slučaju su najbitniji oni parametri koji se iščitavaju iz logova, posebnih "prijevoda" informacija koje se mogu izvaditi iz odgovarajućih aplikacija u službi nadgledanja statusa performansi. Nadgledanje statusa hardvera i softvera obuhvaća sve od praćenja zdravlja hardvera, uključujući temperaturu, stanja diskova, baterije, ventilatora i drugih komponenti u cilju sprječavanja hardverskih kvarova do praćenja verzija operativnog sustava, provjera ažuriranja drivera, aplikacija i drugog softvera te osiguranost jesu li uređaji ažurni i sigurni što se softvera tiče.

Dijagnostika i rješavanje problema se vrši identifikacijom i analizom problema nastalima na uređajima, od pada performansi, neočekivanog gašenja aplikacija, gubitka veze na mreži ili slični problemi u organizaciji. Takvi procesi i poslovi obuhvaćaju popravljanje softvera, zamjenu ili popravak hardverskih komponenti ili primjenu ostalih rješenja kako bi se osigurao nesmotreni rad svih uređaja. Ključni dio održavanja stabilne i pouzdane IT infrastrukture u organizaciji je omogućavanje brze identifikacije i otklanjanje problema IT administratorima, pogotovo prije nastajanja većih kvarova uređaja. Nužno je osigurati i nesmotren rad bez prekida za organizaciju.

2.2.3. Sigurnost sustava

Sigurnost je jedna od najvažnijih sastavnica upravljanja uređajima u okviru IT infrastrukture organizacije. Osiguravanje sigurnosti uređaja je ključno za zaštitu podataka, očuvanje privatnosti korisnika i sprečavanje neovlaštenog pristupa ili napada na IT sisteme. Autentifikacija i autorizacija korisnika se vrši kako bi se osiguralo da samo ovlašteni korisnici mogu pristupiti uređajima i resursima. Ovo najčešće uključuje korištenje različitih načina autentifikacije, poput lozinke, biometrijskih podataka ili tokena za jednokratnu upotrebu (OTP – eng. One-time Password). Također je važno da se pravilno konfiguriraju prava pristupa kako bi se ograničio pristup određenim resursima samo ovlaštenim korisnicima. To se odnosi na dijelove organizacije gdje je bitno treba li korisniku pristup resursima u lokalnoj mreži, podatcima na serveru ili jednostavno pristup nekakvom ovlaštenom uređaju. Šifriranje podataka se koristi u svrhu zaštite podataka prilikom prijenosa preko mreže, kao i podaci koji se skladište na uređajima. Šifriranje diska je posebice važna jer osigurava da podaci budu zaštićeni ako uređaj dospije u neovlaštene ruke ili ako dođe do pokušaja provale u uređaje preko mreže i sl. Ažuriranja softvera se koristi prilikom održavanja operativnih sustava, aplikacija i sigurnosnih alata kako bi se zatvorile poznate sigurnosne rupe i ranjivosti. Ovo je važan korak u sprječavanju eksploatacije sigurnosnih propusta od strane napadača. Sigurnosne politike jasno definiraju i primjenjuju određene politike i procedure kako bi se osiguralo da korisnici prate sigurnosne standarde i pravila u upotrebi uređaja. Ovo može uključivati pravila za upotrebu lozinki, ograničenja pristupa, korištenje sigurnosnih alata i druge smjernice za sigurno korištenje uređaja u organizaciji. Upravljanje prijetnjama obuhvaća implementaciju sistema za otkrivanje i reagiranje na prijetnje (IDS/IPS) koji nadgledaju mrežni promet i aktivnosti na uređajima kako bi identificirali sumnjive ili zlonamjerne aktivnosti i poduzeli odgovarajuće korake za njihovo suzbijanje. Ovi elementi zajedno doprinose stvaranju sveobuhvatnog pristupa sigurnosti uređaja, osiguravajući da organizacija bude zaštićena od različitih sigurnosnih prijetnji i rizika. Održavanje visokog nivoa sigurnosti je ključno za zaštitu poslovnih podataka, očuvanje ugleda organizacije i osiguravanje povjerenja korisnika.

2.2.4. Ažuriranja i održavanje softvera i operativnih sustava

To su ključni aspekti upravljanja uređajima koji se odnose na proces redovnog održavanja softvera, operativnih sustava i aplikacija kako bi se osigurala njihova stabilnost, sigurnost i funkcionalnost. Redovno ažuriranje operativnih sustava (kao što su Windows, macOS, Linux, iOS, Android) služi da bi se ispravile poznate greške ranjivosti i propusti u sigurnosti. Proizvođači operativnih sustava redovno objavljuju ispravke i nadogradnje kako bi riješili ove

probleme sigurnosti, i važno je da se ažuriranja instaliraju čim postanu dostupna. Ažuriranje različitih aplikacija i softverskih alata koji se koriste na uređajima ključno je za osiguranje od potencijalnih prijetnji i ranjivosti. To uključuje aplikacije za produktivnost i uredske zadatke (poput Microsoft Office Suitea, Adobe Creative Clouda), sigurnosne alate (antivirusne programe, firewall-ove, alate za šifriranje podataka), internetske preglednike, multimedijske softvere te druge aplikacije. Redovita ažuriranja aplikacija omogućuju korisnicima pristup najnovijim funkcijama, ispravcima grešaka i sigurnosnim zakrpama, što pomaže u otklanjanju sigurnosnih propusta na vrijeme. Poseban značaj u ovom kontekstu imaju CVE (eng. Common Vulnerabilities and Exposures) identifikatori, koji služe za prepoznavanje i praćenje poznatih sigurnosnih ranjivosti u softveru. Korištenjem CVE sustava, IT stručnjaci mogu brzo identificirati ranjivosti koje pogađaju određene aplikacije ili sustave te poduzeti odgovarajuće mjere za ažuriranje i zaštitu. Redovitim primjenjivanjem sigurnosnih ažuriranja smanjuje se rizik od eksploatacije ranjivosti koje bi mogle dovesti do krađe podataka, neovlaštenog pristupa ili drugih sigurnosnih incidenata. Sistematska održavanja služe za redovno održavanje uređaja radi očuvanja njihove performanse i funkcionalnosti. Ovo uključuje čišćenje operativnog sustava od privremenih datoteka, optimizaciju radne memorije, defragmentaciju tvrdih diskova (u slučaju tradicionalnih mehaničkih diskova), provjeru integriteta podatkovnog sistema i druge aktivnosti koje poboljšavaju performanse uređaja. Sigurnosna ažuriranja služe da bi se otklonile poznate ranjivosti i propusti u sigurnosti. Ovo je ključno za sprječavanje hakerskih napada, malicioznih kodova i drugih sigurnosnih prijetnji koje mogu ugroziti podatke i funkcionalnost uređaja. Isto tako je bitno planiranje ažuriranja. Razvijanje strategije za ažuriranje i održavanje koja uključuje planiranje redovnih provjera i ažuriranja, raspore ažuriranja u odgovarajućem vremenu kako bi se minimalno ometao rad korisnika, i da se osigura da su svi uređaji ažurirani i održavani na dosljedan način. Ažuriranje i održavanje je ključno za održavanje sigurnosti, stabilnosti i performansi uređaja, osiguravajući da organizacija ima pouzdane i efikasne IT resurse za podršku u svojim operacijama.

2.2.5. Udaljena podrška

Poanta udaljene podrške je da se s lakoćom utemelji i otkloni problem na bilo kojem uređaju u organizaciji. U prijašnje vrijeme najčešće korišten način udaljene podrške je bio telefonski ili prijavom preko organizacije te bi se probalo doći do izvora problema telefonski pa bi se otklonilo po mogućnosti uživo ili bi se uređaj vozio na servis. U današnje vrijeme se udaljena podrška radi na vrlo jednostavnije načine, omogućujući efikasnije, brže reakcije administratora

jer se putem mreže i odgovarajućih aplikacija vrlo lako spoje na korisnički uređaj te mogu upravljati njime ako je uređaj funkcionalan. Najčešće aplikacije za udaljeno spajanje su TeamViewer, AnyDesk, Chrome Remote Desktop, Microsoft Remote Desktop i sl. Putem udaljene podrške se isto tako može odraditi detaljnija analiza kvara uređaja i u stvarnom vremenu se otklanja kvar, što je puno brža tehnika od samog čitanja logova ili komunikacije s korisnikom gdje korisnik mora objasniti svoj kvar što bolje da bi olakšao saznanje o kvaru jednog IT administratora.

3. JUMPCLOUD PLATFORMA

JumpCloud je platforma za usluge direktorija u oblaku koja omogućava organizacijama da upravljaju i osiguraju korisnički pristup sistemima, aplikacijama i mrežama. Pruža centralno mjesto za čuvanje i upravljanje korisničkim identitetima i omogućuje IT timovima jednostavno dodjeljivanje i povlačenje pristupa resursima. Također nudi značajke poput višefaktorske autentifikacije i upravljanja lozinkama, što ih čini sveobuhvatnim rješenjem za upravljanje korisnicima i sigurnošću sustava. JumpCloud mijenja način na koji IT administratori upravljaju svojim organizacijama iz takoreći samo jednog prozora i tako lakim putem mogu osigurati apsolutno svaki operativni sustav koji se nalazi u organizaciji. To je ujedno i prvi DaaS (eng. Directory-as-a-Service) sustav u oblaku. DaaS sustav efektivno uzima i prebacuje mrežni protokol za dohvaćanje informacija iz imenika – LDAP ili Microsoftov Active Directory u oblaku i onda ga upravlja kao servis. Kao jedna od značajka, DaaS nije pokazao da je samo Active Directory baziran u oblaku, nego je ujedno i kombinacija oba alata i nudi veliku modernizaciju Directoryja i Cloud servisa.

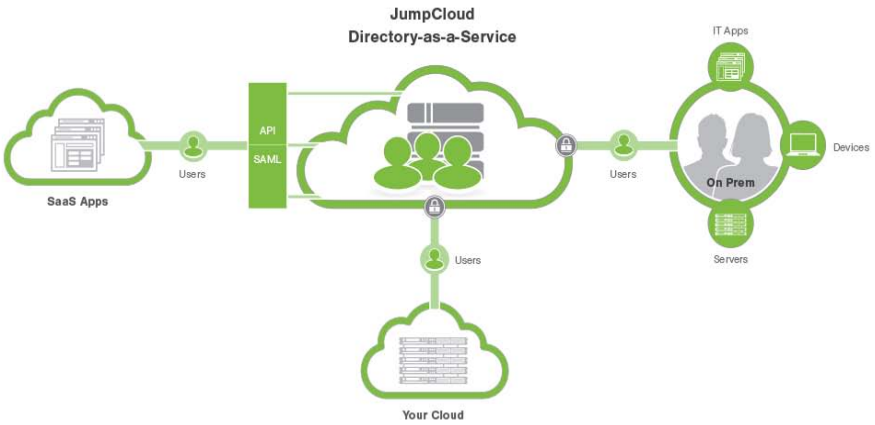
3.1. Directory-As-a.Service - DaaS

DaaS je definiran tako da omogućuje sigurnu povezanost i upravljanje korisnicima i IT resursima jedinstvenim Directoryjem korisnika i uređaja u oblaku. Directory korisnika i uređaja radi u oblaku i sastavljen je kao jedina točka za upravljanje korisnicima i pristupima uređajima i aplikacijama u organizaciji. Moguće je postaviti DaaS odmah putem samog poslužitelja u oblaku, ali je odlična opcija jer je moguća direktna migracija iz postojećih LDAP sustava na novi DaaS sustav. Olakšava upravljanje različitim vrstama IT resursa, uključujući radne površine, prijenosna računala, ručne jedinice i ostale uređaje. DaaS koristi distribuirano daljinsko izvršavanje, ovisno o vrsti implementacije. Isplativa je alternativa uobičajenim informatičkim rješenjima i koriste ga organizacije koje zahtijevaju visoku razinu performansi i dostupnosti. Uz to, DaaS služi kao idealno rješenje za male organizacije s ograničenim resursima. Prednosti DaaS-a uključuju:

- minimiziranu složenost
- oporavak od katastrofe
- neprekidnu povezanost
- povećane performanse
- personalizaciju
- pouzdanost

- sigurnost podataka
- jednostavnu migraciju platforme

Svi podaci o korisnicima, uređajima i njihovim pravima pristupa pohranjeni su u jednoj sigurnoj, bazi podataka baziranoj u oblaku. Tako je cijeli sustav centraliziran u oblaku te iz njega proizlaze svi potrebni podaci prema korisnicima koji imaju pristup. Nije razgranan na različite sustave, nego se sve odvija iz centralne točke u oblaku (Slika 1).



Slika 1. Prikaz rada JumpCloud Directory-as-a-Service sustava (JumpCloud, 2014.)

3.2. SSO metoda autentifikacije

SSO je metoda autentifikacije koja omogućuje korisnicima da sigurno i efektivno pristupe različitim varijantama IT resursa kao što su mreže, uređaji, serveri, aplikacije i ostali servisi sa samo jednim setom kredencijala. Moderni SSO se referira kao True Single Sign-On (u prijevodu: Istinska jedinstvena prijava) te ne koriste se tradicionalnom i zastarjelom verzijom autentifikacije na web aplikacijama. Razlika je u tome što SSO kod web aplikacija omogućuje samo sigurnost kod određene aplikacije i kod određenog servisa dok JumpCloudov True SSO omogućuje korisnicima spajanje na skoro svaki IT resurs preko SSO-a povezujući različite otvorene protokole. S time se pokazuje da je jako pouzdano i vrlo dobro rješenje za IT administratore koji mogu pratiti svaki resurs i upravljati svakim identitetom i pristupom uživo unutar svog IT ekosistema. Prednost je ujedno i povećanje sigurnosti sustava, povećana produktivnost u infrastrukturi, smanjuje se "zamor lozinke" - fenomen gdje se zbog povećanog

broja servisa u oblaku, raznih web aplikacija i stvaranja mnogo različitih računa i kredencijala za te aplikacije dolazi do pojednostavljenja lozinka kod korisnika te se povećava mogućnost kibernetičkog napada. Također poboljšava korisničko iskustvo i sprječava nesmotreno korištenje vanjskih uređaja unutar sistema (npr. privatna računala, mobiteli i sl.).

3.2.1. Funkcija SSO autentifikacije

Jedinstvena prijava omogućuje korisnicima autentifikaciju na različite IT resurse s kombinacijom korisničkog imena i lozinke baziranom na povjerljivom odnosu između svakog resursa i pružatelja identiteta (idP – eng. Identity Provider). Taj se odnos tipično bazira na certifikatu povezanim resursom ili pružateljem usluge (SP – eng. Service Provider) i idP-om kada se radi konfiguracija SSO-a. Svrha tog certifikata je stvoriti povjereni odnos između SP-a i idP-a da se verificira integritet informacija koje se prenose. Tijekom procesa jedinstvene prijave, podatci o identitetu se šalju od idP-a do SP-a u obliku tokena koji sadrže djeliće informacije o tom korisničkom identitetu. Kada se korisnik prijavi u portal SSO pružatelja, tada pružatelj identiteta prati korisničku aktivnost i vidi da je korisnik izvršio autentifikaciju, najčešće preko sesijskog kolačića u HTTP kodu. Od tog trenutka, bilo koji resurs spojen na SSO će se provjeriti preko SSO pružatelja kada se korisnik pokuša prijaviti u taj resurs. Ako idP verificira korisnika bazirano na njegovom prvom prijavljivanju kroz portal, tada će se taj isti token poslati na taj resurs. Međutim, ako se korisnik nije spojio na glavni SSO portal ili je njihova sesija istekla, korisnik će se morati ponovno prijaviti kako bi pristupio bilo kakvim resursima sa spojenim SSO-om. To se najčešće radi u obliku nekakvog vremena zastoja (eng. downtime) gdje ako prođe neko određeno vrijeme bez aktivnosti, korisnik će automatski biti odjavljen sa SSO resursa.

3.2.2. Različiti SSO autentifikacijski protokoli

Autentifikacijski tokeni su najbitniji dio procesa jedinstvene prijave, oni omogućuju da se verifikacija identiteta provede odvojeno od drugih servisa u oblaku. Ti tokeni mogu imati različite oblike dok prate različite komunikacijske standarde da bi osigurali svoju valjanost. Jedan najčešći standard kod autentifikacijskih tokena iliti autentifikacijskih protokola je SAML (eng. Security Assertion Markup Language), to je standardizirani format za razmjenu podataka između SP-a i idP-a te je najraširenij zbog toga što omogućuje korisnicima da se prijave na jedan sustav (npr. neku *web* aplikaciju) te mogu pristupiti ostalim povezanim sustavima bez potrebe za ponovnom prijavom. To uvelike olakšava upravljanje pristupom te olakšava

korisničko iskustvo.

3.2.3. Funkcija JumpCloud SSO autentifikacije

JumpCloud je izgradio svoj *directory* u oblaku tako da funkcionira kao glavni pružatelj identiteta u oblaku koji usmjerava IAM i SSO i pruža sve to u istoj platformi, uključujući i Cloud LDAP, Cloud RADIUS, SAML, SCIM i JIT protokole i više. JumpCloud isto tako ima i široku biblioteku od stotine predkonfiguriranih SAML konektora te se tako integracija ili prvobitna konfiguracija uvelike olakšava. JumpCloud omogućuje organizacijama da koriste glavne IAM protokole (LDAP, SAML, OAuth2, RADIUS i više) u autentifikaciji korisnika na bilo kojem IT resursu koristeći SSO. Uvelike smanjuje opseg rada zbog jednostavne konfiguracije i manjka održavanja jer sve bitne stavke autentifikacije drži na jednom mjestu. Tako se omogućuje da individualnim korisnicima ili grupama korisnika vrlo lako daje pristup odabranim resursima. SSO se može konfigurirati preko Windows, Mac i Linux uređaja, omogućuje Cross-OS SSO što znači da se Single Sign-On može provesti na sve operativne sustave u spojenom okruženju.

3.2.4. Rad OAuth2 sa SSO

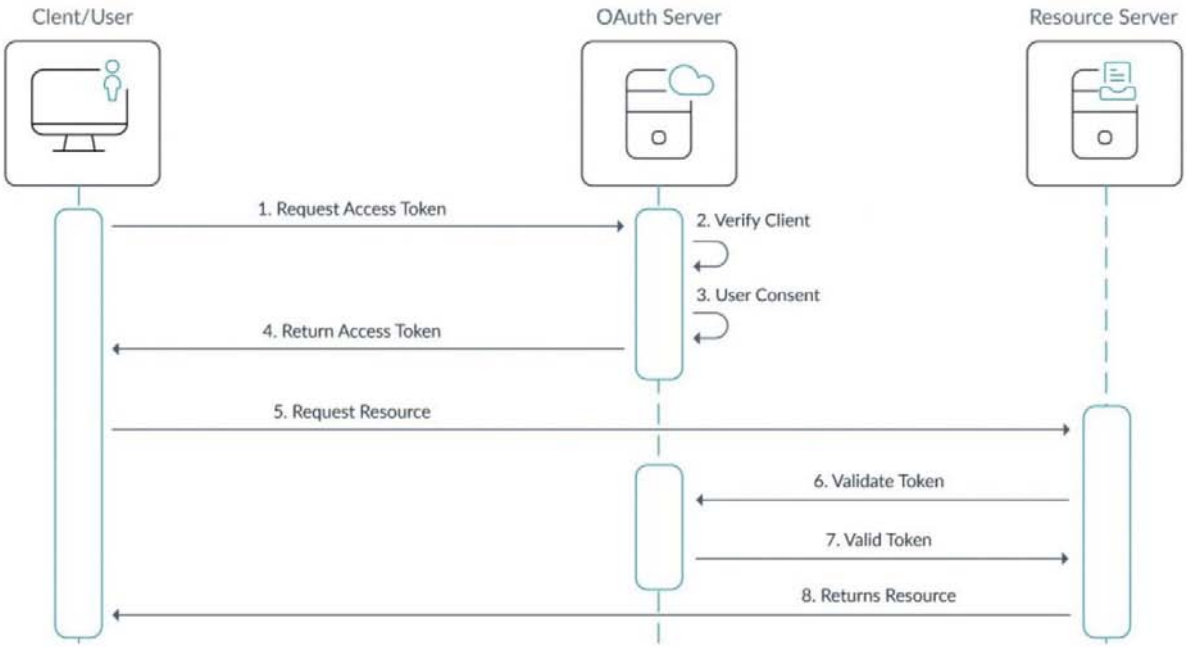
Razlika između autentifikacije i autorizacije se ovdje može prikazati na način da autentifikacija predstavlja korisnički identitet, dok autorizacija prikazuje korisničke privilegije u nekom sustavu. Tu zapravo stoji razlika između OAuth2 i ostalih protokola. Dok SAML širi korisničke podatke na oblak i ostale web aplikacije koristeći XML (eng. Extensible Markup Language) format, OAuth2 je autorizacijski protokol koji je skrojen više prema opsegu dopuštenja, što znači da pušta samo minimum pristupa u nekom resursu ili aplikaciji koje identitet treba nakon što se verificira. OAuth2 je posebno idealan za web i mobilne aplikacije i koristi se općenito u samim aplikacijama u direktnoj vezi s IdP-om. OAuth2 isto dopušta mehanizma prijave kao naprimjer “Prijava s pomoću Googlea” ili “Prijava s pomoću Microsofta” što zapravo produljuje proces prijave još više. Tako direktno spaja glavne resurse sa samim korisničkim identitetom u prijavi.

Proces autentifikacije OAuth2 protokolom (slika 2):

- korisnik zatraži pristup resursu: korisnik želi pristupiti nekom resursu (npr., nekom organizacijskom resurs) putem neke aplikacije (npr., mobilne aplikacije koja sadrži pristup tom resursu). Aplikacija (klijent) šalje zahtjev OAuth serveru za pristup tokenom
- OAuth server provjeri klijenta: OAuth server provjerava identitet aplikacije kako bi se

uvjerio da je to legitimna aplikacija koja ima pravo zatražiti pristup korisnikovim resursima

- korisnik daje suglasnost: ako je aplikacija legitimna, OAuth server preusmjeri korisnika na stranicu gdje korisnik mora dati svoj pristanak za dijeljenje svojih podataka s aplikacijom
- OAuth server izdaje pristupni token: nakon što korisnik da svoj pristanak, OAuth server izdaje pristupni token aplikaciji. Ovaj token je poput digitalnog ključa koji omogućuje aplikaciji da pristupi određenim resursima u ime korisnika
- aplikacija zatraži resurs: aplikacija koristi pristupni token za slanje zahtjeva resursnom serveru (npr., serveru organizacijskog resursa) kako bi dobila pristup željenom resursu
- resursni server provjeri token: resursni server provjerava valjanost pristupnog tokena kako bi se uvjerio da je aplikacija ovlaštena za pristup traženom resursu.
- resursni server vraća resurs: ako je token valjan, resursni server vraća traženi resurs aplikaciji
- aplikacija prikazuje resurs korisniku: aplikacija prikazuje resurs korisniku, na primjer, prikazuje fotografije koje je korisnik odabrao za uređivanje



Slika 2. Proces autentifikacije OAuth2 protokolom (Jumpcloud, 2021.)

3.3. JumpCloudov protokol za pristup imeniku – LDAP u oblaku

LDAP (eng. Lightweight Directory Access Protocol) servis predstavlja temelj Directory sustava. Njegova primarna funkcija je omogućiti pristup i održavanje distribuirane imeničke informacijske usluge preko IP mreže. Tradicionalno, LDAP okruženja, nastala od OpenLDAP-a ili Microsoft Active Directory servisa raspoređena su lokalno. Što znači da se moraju distribuirati preko fizičkih servera pa to utječe na značajne troškove u smislu održavanja, skalabilnosti i integracije s modernim uslugama u oblaku. JumpCloudov LDAP u oblaku zato nudi moderniziranu premisu stvaranja LDAP sustava u oblaku.

3.3.1. Značajke i funkcionalnosti JumpCloud LDAP-a u oblaku

LDAP servis je samo dio cjelokupnog JumpCloud DaaS sustava koji cilja pri centralizaciji i pojednostavljenju upravljanja identitetima i njihovim pristupom u organizaciji preko različitih platformi, aplikacija i mreža. Ključne značajke JumpCloudovog LDAP sustava su izvorna arhitektura u oblaku koja za razliku od tradicionalnih LDAP okruženja, je izvorno građena u oblaku za JumpClou sustav. Tako se eliminira potreba za lokalnim fizičkim hardverom i njegova potreba za održavanje i tako se pruža fleksibilnije i skalabilnije rješenje. Više-platformska kompatibilnost u JumpCloudu podržava visok raspon operativnih sustava i okruženja, uključujući Windows, macOS i Linux, također i platforme u oblaku kao što su AWS, Azure, Google Cloud i sl. Tim činom osigurava besprijekornu komunikaciju i integraciju u razne IT ekosisteme. Centralizirano upravljanje identitetima omogućuje administratorima jednostavno upravljanje korisničkim identitetima kao što su korisnička imena, lozinke te korisničke uloge, grupe i politike kroz jedinstvenu centraliziranu platformu što pojednostavljuje IT administraciju i pojačava sigurnost organizacije. Poboljšane opcije sigurnosti IT sustava u koje je JumpCloud ukomponirao snažne mjere sigurnosti u svom sustavu koji se primjenjuju na organizaciju i u to spadaju stavke kao više-faktorska autentifikacija (MFA), odredba kompleksnosti lozinke korisničkog računa te evidentiranje događaja kod pristupa mrežama, pristupa uređajima i slično. Takve značajke pomažu organizacijama održavati visoki stupanj osiguranja i usklađenosti s regulatornim standardima. API (eng. Application Programming Interface) u JumpCloudu pruža opsežan set API ključeva i unaprijed izgrađenih integracijskih protokola koji omogućuju organizacijama da spoje već svoje postojeće LDAP Directoryje sa širim spektrom aplikacija i servisa. Takva proširivost je ključna stavka za moderna IT okruženja pogotovo ako se oslanjaju na raznolik skup alata i usluga. Prisvajanje JumpCloudovog Cloud LDAP-a nosi razne prednosti organizacijama kao što je smanjenje operativnih troškova gdje se

servisom baziranom u oblaku, smanjuju vrijeme i resursi koji se troše na održavanje lokalne *Directory* infrastrukture pa se tako IT timovi mogu usredotočiti na obavljanja ostalih poslova u svojem polju u organizaciji. Isto tako se povećava fleksibilnost i skalabilnost gdje se servis Directoryja skalira po potrebi u vrlo kraćem roku. Mogu se lakše planirati resursi jer je sve u oblaku, JumpCloud servis se može vrlo jednostavno rekonfigurirati po potrebi. Poboljšanim pristupom korisnici mogu koristiti IT resurse kao što su web aplikacije, servise organizacije i sl. Bilo gdje imaju mogućnost interneta i ta stavka igra ulogu jer je u današnje vrijeme rad od doma puno zastupljeniji u IT-u nego ikad prije. JumpCloudove ugrađene značajke za sigurnost uvelike pomažu organizacijama da osiguraju korisnike u IAM praksi te u centraliziranom sustavu olakšava provođenje pravila usklađenih s regulacijama u industriji. Sama fleksibilnost i proširivost JumpCloudovog LDAP-a u oblaku omogućuje besprijekornu integraciju s drugim servisima u oblaku i aplikacijama te pomažu u stvaranju kohezivnog i efektivnog IT ekosistema.

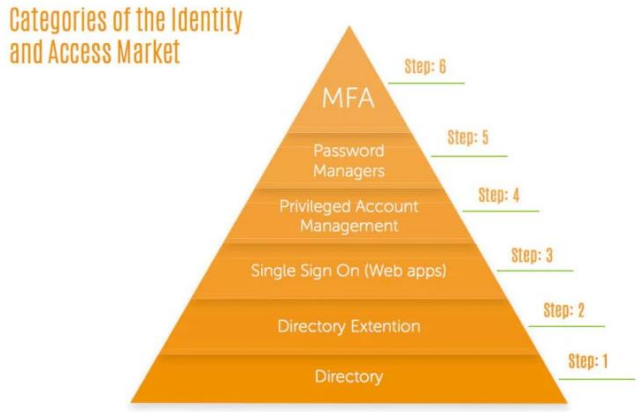
3.3.2. Rad LDAP-a u SSO okruženju

LDAP protokol je originalno dizajniran za on-Prem autentifikaciju koja se koristi u sustavu lokalne unutarnje infrastrukture organizacije i pruža puno veću sigurnost jer se ne oslanja na sustave bazirane na oblaku te pruža maksimalnu kontrolu nad sigurnošću i privatnošću jer organizacija ima potpunu kontrolu nad autentifikacijskim podatcima i infrastrukturom. Naime, kada se LDAP i SSO koriste zajedno, korisnik unosi svoje podatke za prijavu te se detalji korisničkog identiteta šalju na sigurnosni poslužitelj za autentifikaciju. Nakon toga, sigurnosni poslužitelj šalje informaciju o prijavi na LDAP poslužitelj koji koristi dane podatke da pokuša identificirati korisnika. LDAP je tu općenito autentifikacijski protokol samo pri provjeri informacije prijave na serverskoj strani.

3.4. Upravljanje identitetima i pristupom - IAM u JumpCloudu

IAM je sustav koji omogućuje upravljanje korisničkim identitetima i kontrolu pristupa informacijama unutar organizacije. IAM rješenja pomažu tvrtkama da osiguraju da samo ovlaštene osobe imaju pristup određenim resursima, te osiguravaju da se korisnički podaci sigurno pohranjuju i koriste. IAM sustavi uključuju različite komponente kao što su provjera autentičnosti (Single Sign-On, Cloud LDAP, Cloud RADIUS), upravljanje lozinkama, višefaktorska autentifikacija i upravljanje uvjetnim pristupom. Ovi sustavi također integriraju uređaje (npr. upravljanje uređajima koji koriste različite operacijske sustave) te omogućuju automatsko uključivanje i isključivanje korisnika (eng, onboarding i offboarding) kako bi se

pojednostavnilo upravljanje korisnicima. IAM sustavi su ključni za osiguravanje usklađenosti sa sigurnosnim standardima i pravilnicima, kao i za smanjenje rizika od neovlaštenog pristupa i potencijalnih sigurnosnih prijetnji. Kategorije rada IAM sustava su prikazani dijagramom te koracima objašnjeni kako upravljanje identiteta i sigurnost u organizaciji radi u JumpCloud sustavu (Slika 3).



Slika 3. Rad IAM sustava u koracima (JumpCloud, 2021.)

3.4.1. Prednosti IAM sustava

Upravljanje identitetom i pristupom predstavlja savršeno spajanje produktivnosti, sigurnosti i pristupa najboljim alatima u svojoj klasi. Uz IAM, zaposlenici koriste unaprijed određeni "identitet" kako bi dobili siguran pristup IT resursima koji su im potrebni za obavljanje posla. Primarna je prednost za ove korisnike krajnje to što su procesi racionalizirani i glatki, omogućavajući im brzi pristup novim resursima putem jednog seta kredencijala kako bi se posao obavio brže. Više ne moraju pamtiti (ili što je još gore, ponovno koristiti) lozinke za svaki resurs do kojeg pristupaju, a iskustvo prijave je dramatično poboljšano. S druge strane, IAM daje IT-u jedno centralno mjesto za kontrolu nad tim sredstvima. Administratori današnjih IT sustava moraju biti u stanju održavati vidljivost i kontrolu nad Windows, Mac i Linux krajnjim točkama, povezivati korisnike s velikim brojem lokalnih i web resursa te se integrirati s oblakom, sve uz održavanje sigurnosti podataka. SaaS rješenja za IAM, poput Identity-as-a-Service (DaaS) sljedeće generacije, pružaju administratorima jedinstvenu platformu za kontrolu upravljanja svim tim faktorima na jednom mjestu. Administrator se može udaljeno prijaviti na svoju IAM platformu i omogućiti ili onemogućiti korisnike, stvoriti ili uređivati identitete korisnika, stvoriti politike za pristup i pojačanu autentifikaciju te upravljati rješavanjem problema, sve bez napuštanja aplikacije. Rješenja za upravljanje identitetom i pristupom zasnovana na oblaku također poboljšavaju sigurnost podataka i podržavaju inicijative za

usklađenost s identitetom poput GDPR-a, PCI-a i HIPPA-a. Navodi se da 60% malih i srednjih poduzeća (MSP – eng. managed services provider) propadne u roku od šest mjeseci od kibernetičkog napada, što čini sigurnost važnijom nego ikada prije. IAM daje IT administratorima kontrolu nad zaštitom digitalnih sredstava i zaštitom njihove tvrtke od kibernetičkih napada.

3.4.2. Izazovi IAM sustava

Radno mjesto s nedavno diversificiranom radnom snagom s udaljenim radnicima koji rade na više platformi zakompliciralo je krajolik IAM-a. U prošlosti su bili IAM sustavi lakši za upravljanje jer su korisnicima bila potrebna samo dva ili tri resursa za obavljanje posla, a na radnom mjestu su dominirali Windows sustavi koji su se svi nalazili na lokaciji. Korisnici su također dolazili u fizički ured gdje je IT mogao kontrolirati mrežu i ukupno okruženje. IAM je počeo evoluirati kako su macOS i Linux stekli popularnost na radnom mjestu kao alternative Windowsu. Zatim su došli Salesforce, Google Apps (alias Google Workspace) i druge web aplikacije koje bi mogle zamijeniti lokalne Windows aplikacije. Nakon toga su stigle alternative lokalnom pohranjivanju datoteka, poput Samba File servera i NAS uređaja, ili rješenja za pohranjivanje u oblaku od dobavljača poput Boxa ili Dropboxa. Čak se i sama mreža razvila sa žične veze na bežičnu preko Wi-Fija. Sve su ove promjene učinile IAM nevjerojatno složenim. Zastarjela rješenja poput Microsoft Active Directory (AD) i dalje su glavno rješenje za upravljanje identitetom u većini IT organizacija, ali AD nije dizajniran za podršku IT resursa koji nisu Windows ili koji su zasnovani na oblaku. Kao rezultat toga, IT tim mora ili samostalno upravljati resursima koji nisu Windows, što zahtijeva dodatno vrijeme i trud za uspostavljanje i održavanje odvojenih sustava ili koristiti dodane funkcije za AD od treće strane (npr. SSO za web aplikacije, ekstenzije Directoryja, što samo dodaje dodatnu složenost već i tako kompleksnom sustavu). Na sreću, postoje noviji direktoriji zasnovani na oblaku i moderna rješenja za IAM koja mogu lako zamijeniti lokalni IAM program baziran na AD, omogućavajući jednostavniji i sveobuhvatniji pristup.

3.4.3. Implementacija IAM sustava

Tradicionalni IAM sastoji se od pet komponenti koje se nadograđuju jedna na drugu kako bi se stvorila sveobuhvatna strategija. Povezivanje ovih sustava u sekvencijalnom redoslijedu pomaže u izbjegavanju propusta u upravljanju, što može ometati sigurnost. Međutim, važno je napomenuti da moderniji IAM ponuditelji integriraju druge aspekte IT administracije, poput upravljanja uređajima i mrežom, s tradicionalnim IAM komponentama. Ove moderne

platforme direkcija nude kompletnije rješenje koje IT administratorima omogućava da osiguraju siguran pristup i upravljaju jednim identitetom za gotovo sve IT resurse. IAM sustav osigurava siguran i kontroliran pristup IT resursima unutar organizacije. Građevni blokovi IAM sustava uključuju sljedeće komponente:

- usluge direkcija
- ekstenzije direkcija
- upravljanje privilegiranim pristupom - PAM
- implementacija SSO-a u IAM sustavu
- pojačanje procesa prijave višefaktorskom autentifikacijom - MFA

Usluge direkcija predstavljaju osnovnu komponentu IAM sustava, odgovorne za pohranjivanje i autentifikaciju korisničkih podataka. Kada korisnik pristupi aplikaciji ili web servisu, usluga direkcija verificira njegov identitet i odobrava pristup. Direkcije omogućuju IT administratorima da organiziraju identitete u logičke grupe te primjenjuju politike pristupa i sigurnosne konfiguracije. Ove interakcije se bilježe radi osiguravanja poštivanja zakona o usklađenosti. U modernim IAM sustavima, usluge direkcija često uključuju dodatne funkcije, kao što je upravljanje uređajima i mrežnim resursima, čime se stvara centralizirana platforma za sigurno upravljanje identitetima.

Ekstenzije direkcija su stvorene da popune praznine konvencionalnih usluga direkcija. To je najčešći primjer kod zastarjelih aplikacija koje nemaju sve funkcionalnosti potrebne za udaljenu podršku i upravljanje identitetom. Ekstenzije dopunjuju funkcionalnost postojeće direkcije, omogućavajući joj povezivanje s platformama, uređajima i aplikacijama do kojih inače ne bi mogla. Ekstenzije također povećavaju funkcionalnost usluga direkcija integriranjem usluga upravljanja uređajima i MDM sustavom te kontroliranjem pristupa korisnika. Ako se i dalje radi sa uslugama direkcija, ekstenzija je onda najlakši prvi korak za dovršetak IAM procesa. Međutim, moderna rješenja poput platformi direkcija u oblaku nude racionaliziran pristup upravljanju pristupom i kontroli resursa IT-a koji nisu bazirani na Windowsu, eliminirajući potrebu za ekstenzijama.

Dok usluge direkcija povezuju korisnike s tim resursima, PAM određuje čemu korisnik može ili ne može pristupiti unutar ovih vrjednijih i kritičnijih aplikacija i IT sustava. Na primjer, dvije osobe imaju pristup istom sustavu u organizaciji, ali PAM osigurava da svaka osoba isključivo

može vidjeti dio sustava koji su postavili IT administratori u tom sustavu ili nekoj aplikaciji. S obzirom na to da se sve više kritične infrastrukture premješta na platforme za infrastrukturu kao uslugu - IaaS bazirane na oblaku, PAM je važniji nego ikada. Siguran pristup digitalnim aplikacijama i temeljnim sustavima koji upravljaju organizacijama nalazi se na vrhu liste IT zadataka.

SSO povezuje jedan identitet, kojim upravlja osnovna usluga direkcija, s različitim web-baziranim aplikacijama kojima korisnik treba pristup, umjesto da korisnik treba stvoriti više identiteta. Sa stajališta korisnika, oni se moraju prijaviti samo u jednu aplikaciju s jednim korisničkim imenom i lozinkom da bi dobili pristup svim svojim web-baziranim aplikacijama. SSO također smanjuje rizik od sigurnosnih incidenata povezanih s lošim praksama lozinki, kao što su korištenje slabih ili ponavljajućih lozinki. Automatizirano provizioniranje korisnika unutar SSO sustava dodatno optimizira upravljanje životnim ciklusom korisnika i unaprjeđuje sigurnost sustava. Najveća prednost za IT administratore s modernim rješenjima za jedinstveno prijavljivanje i automatizirano provizioniranje korisnika, što se često naziva upravljanjem životnim ciklusom korisnika. Uz to, vrhunska rješenja za jedinstveno prijavljivanje dodaju funkcije kao što su uvjetni pristup i višefaktorska autentifikacija kako bi se unaprijedila sigurnost ukupne implementacije SSO-a.

Višefaktorska autentifikacija - MFA je završni element sigurnosti IAM-a i omogućava što sigurnije prijave. MFA poboljšava sigurnost tako što za autentifikaciju pristupa zahtijeva dodatne informacije iznad i pored korisničkog imena i složene lozinke. Općenito, MFA zahtijeva od korisnika da unese informacije koje oni znaju (kao što su korisničko ime i lozinka) i drugi faktor poput nečega što imaju (kao što je pametni telefon ili YubiKey) ili nečega što jesu (kao što je otisak prsta ili skeniranje mrežnice) kako bi se prijavili. Dok se korisničko ime i lozinka mogu lako ugroziti u procuri podataka ili nekom drugom kibernetičkom napadu, MFA je praktički neprobojna i može se lako implementirati, što ju čini jednom od najkritičnijih komponenata za osiguravanje IAM-a. MFA je postala još pristupačnija zahvaljujući *push* notifikacijama i jednostavnom korisničkom iskustvu.

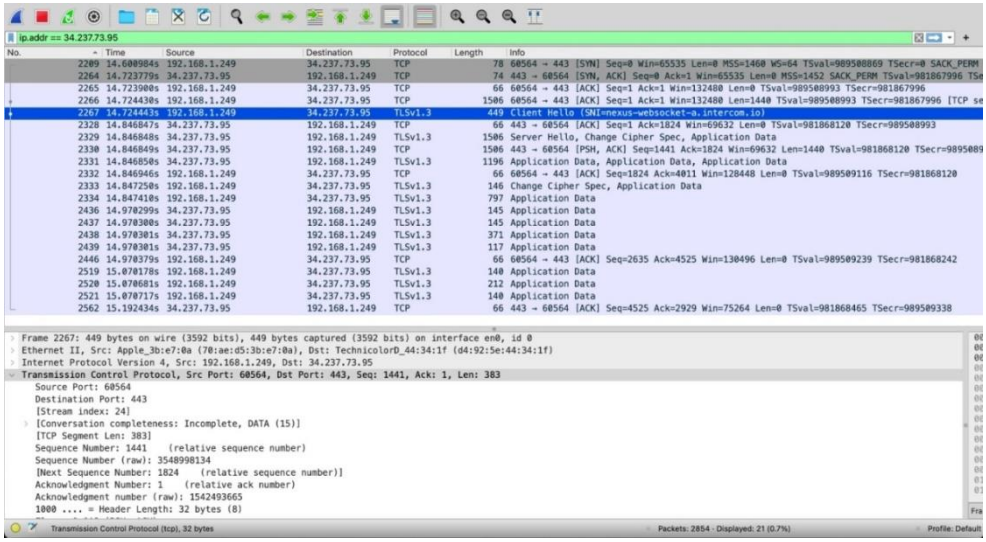
4. PRAKTIČNI RAD – ANALIZA RADA JUMPCLOUD SUSTAVA U WIRESHARKU I PRIKAZ KORISNIČKOG SUČELJA

Kao praktični dio rada prikazana je analiza paketa pri spajanju i slanju komandi na drugo računalo preko JumpCloud-a, uz prikaz korisničkog sučelja prilikom stvaranja novog korisnika. Također je prikazan postupak sinkronizacije s postojećim Active Directoryjem, kao i standardne postavke koje se koriste za dodavanje JumpCloud sustava u organizaciju.

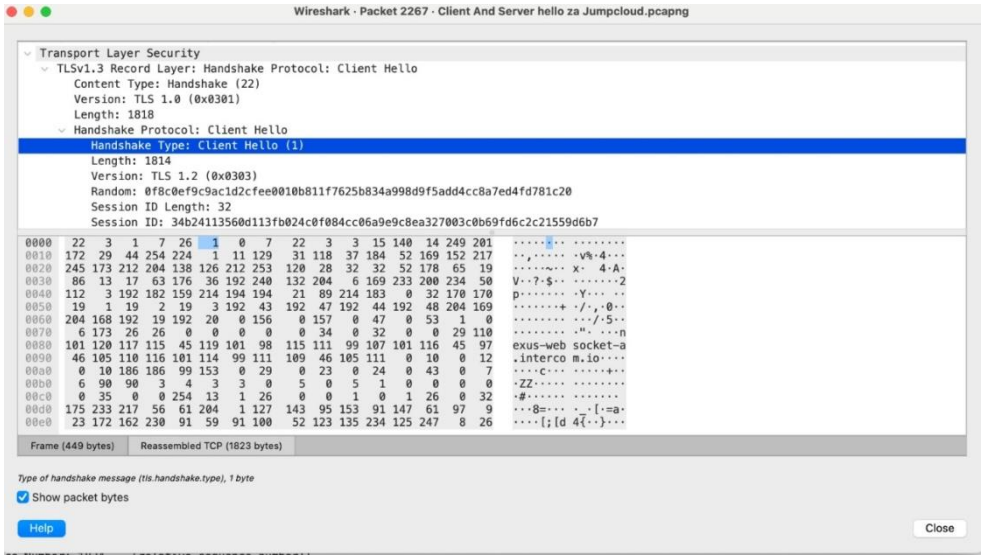
4.1. Analiza Wireshark paketa pri spajanju na JumpCloud konzolu

Pri spajanju na JumpCloud konzolu odvaja se komunikacija između računala s IP adresom 192.168.1.249 i IP adrese 34.237.73.95. Ta IP adresa se odnosi na jedan od Amazon AWS servera koje koristi JumpCloud. Paketi 2209 i 2264 - 2266 su dio trostranog rukovanja. Računalo šalje SYN paket serveru te server obrađuje točnost IP adrese i vraća SYN, ACK paket računalu te računalo vrati ACK paket da bi potvrdio TCP komunikaciju između računala i servera. Promet radi pod portovima 443 i 60654 gdje je port 443 standardni port za HTTPS (eng. *Hypertext Transfer Protocol Secure*) promet. To je sigurna verzija HTTP protokola i služi za komunikaciju između računala i servera što znači da se ona pokreće putem korisnika iz JumpCloud sustava u web pregledniku. Port 60654 je u rangu dinamičnih i privatnih portova što može inducirati da JumpCloud koristi taj port za slanje paketa pod privatnom domenom.

Slijedeći je *Client Hello* TLS paket koji prikazuje da je uspostavljena komunikacija između računala i JumpCloud servera na nexus-websocket-a.intercom.io adresu koja označava zaštićenu komunikaciju između računala i servera te osigurava da bilo koja komunikacija postane šifrirana za svakoga tko pokušava otkriti i presresti pakete. Paketi 2328-2334 i 2436-2521 su TLS paketi koji sadrže šifrirane podatke aplikacija koje se izmjenjuju između dva uređaja, u ovom slučaju računala i JumpCloud servera (Slika 4). Taj *websocket* je prikazan kao SNI (Server Name Indication) ekstenzija na paketu 2267 i pokazuje da je nexus-websocket-a.intercom.io zapravo poveznica prema JumpCloud serveru. Prikaz paketa pri spajanju na JumpCloud server i prikaz paketa *Client Hello* te primjer šifriranja WebSocketa prikazani su na sljedećim primjerima (Slika 5).



Slika 4. Prikaz paketa pri spajanju na JumpCloud server

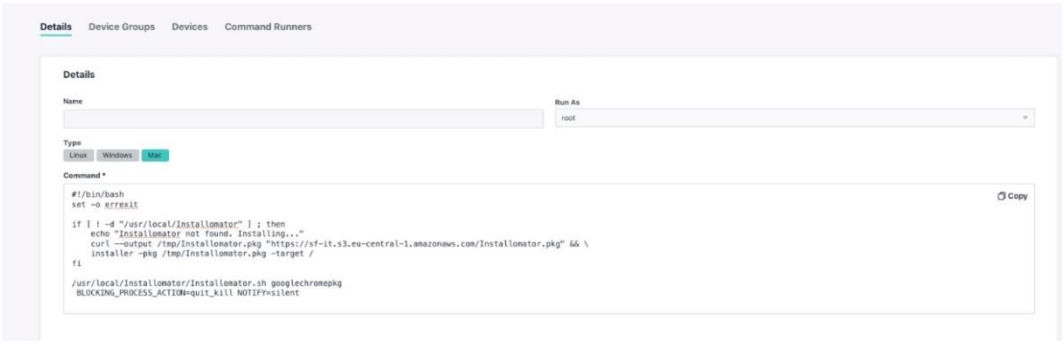


Slika 5. Prikaz paketa *Client Hello* i primjer šifriranja WebSocketa

4.2. Slanje komande za instalaciju programa na drugo računalo putem JumpClouda i analiza putem Wiresharka

Primjerom slanja komande za instalaciju programa, u ovom slučaju Google Chromea, prikazan je JumpCloudov Commands sustav koji pruža razne opcije za izvršavanje skripti na skupine uređaja unutar organizacija koristeći JumpCloudov agent. Mogu se izvršiti skripte u PowerShellu, Bashu, Shellu i ostalim varijantama. U ovom slučaju se koristi Bash skripta Installomator koja je stvorena za specijalno za MDM rješenja za Apple uređaje. Time se olakšava raspoređivanje i udaljeno upravljanje istih. Opcije se sastoje od nekoliko osnovnih podataka, kao što su ime komande, koji korisnik pokreće komandu, te kada i na koji način se

komanda pokreće. Budući da je pokrenuta komanda s administratorskog sučelja, odabire se *Run As Root* jer *Root* znači pokretanje skripte s najvećim privilegijama na sustavu. Druga stavka je odabir tipa sustava na koji se komanda šalje i pisanje same komande. Prikaz opcija za komande u JumpCloud administratorskom sučelju prikazan je na sljedećim primjerima (Slika 6).



Slika 6. Opcije za komande na JumpCloud administratorskom sučelju

Postoje i dodatne opcije kao što je raspored kada će se komanda izvršiti. Može izvršiti ručno svaki put kada se odabere u izborniku, može se namjestiti da se automatski izvršava po rasporedu dnevno, tjedno ili mjesečno. Imamo i TTL (*Time to Live*), vrijeme koje označava koliko se dugo u milisekundama izvršava komanda (Slika 7).

Slika 7. Opcije za komande na JumpCloud administratorskom sučelju

Ova Bash skripta omogućuje instalaciju Google Chromea putem JumpCloud sustava koristeći alat Installomator. Na početku skripte, korištenje #!/bin/bash osigurava da se skripta izvršava pomoću Bash ljuske, dok naredba set -o errexit postavlja opciju da se skripta automatski prekida ako neka naredba rezultira greškom. Prvi korak skripte uključuje provjeru postoji li direktorij /usr/local/Installomator. To se postiže naredbom if [! -d "/usr/local/Installomator"], gdje ! -d

označava da se provjerava nepostojanje direktorija. Ako direktorij ne postoji, skripta ispisuje poruku "*Installomator not found. Installing...*" kako bi obavijestila korisnika da alat Installomator nije pronađen i da slijedi njegova instalacija. Zatim se koristi curl naredba za preuzimanje instalacijskog paketa Installomatora s poveznice https://sf-it.s3.eu-central-1.amazonaws.com/Installomator.pkg. Ovaj paket se sprema u privremeni direktorij /tmp pod imenom Installomator.pkg. Nakon preuzimanja, koristi se naredba installer za instalaciju paketa na sustav s ciljnim direktorijem /. Nakon što je Installomator instaliran ili ako je već bio prisutan, skripta koristi Installomator za instalaciju Google Chromea pozivom /usr/local/Installomator/Installomator.sh googlechromepkg. Dodatne postavke koje prate ovu instalaciju uključuju BLOCKING_PROCESS_ACTION=quit_kill, koja osigurava da se svi procesi koji ometaju instalaciju prisilno zatvore, te NOTIFY=silent, što znači da se tijekom instalacije ne prikazuju obavijesti korisniku. Skripta tako omogućuje automatizirani i tihi postupak instalacije Google Chromea putem JumpCloud sustava, s minimalnom interakcijom korisnika i maksimalnom efikasnošću u slučaju postojećih procesa koji bi mogli ometati instalaciju (kôd 1).

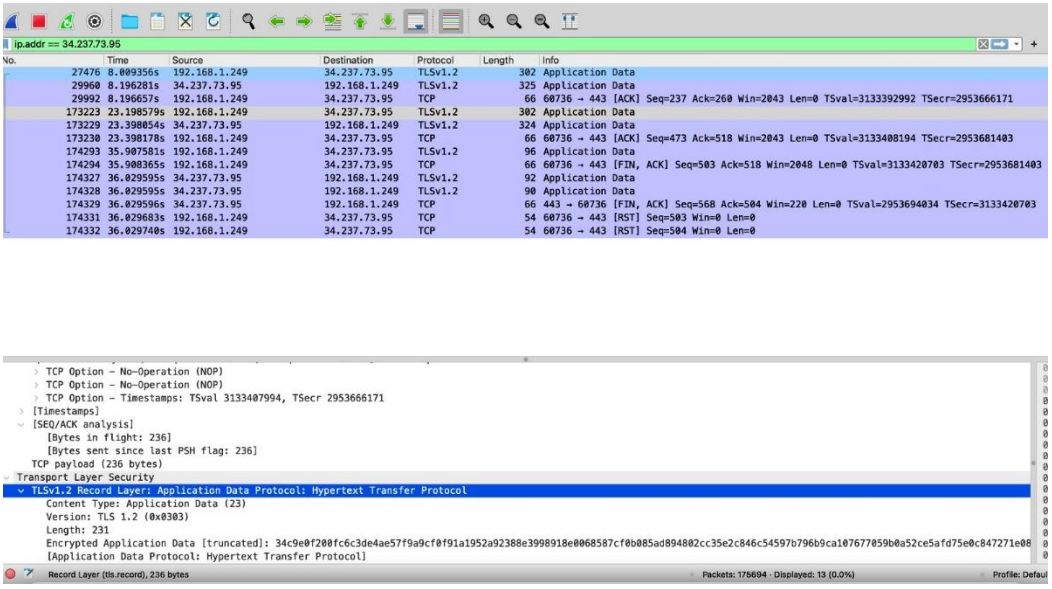
```
#!/bin/bash
set -0 errexit
If [ ! –d „/usr/local/Installomator“ ] ; then
     echo „Installomator not found. Installing...“
     curl – output /tmp/Installomator.pkg https://sf-it.s3.eu-
     central-1.amazonaws.com/Installomator.pkg && \ installer - pkg
     /tmp/Installomator.pkg –target /
fi
/usr/local/Installomator/Installomator.sh googlechromepkg
BLOCKING_PROCESS_ACTION=quit_kill NOTIFY=silent
```

Kôd 1. Bash skripta za instalaciju Google Chromea putem Installomatora

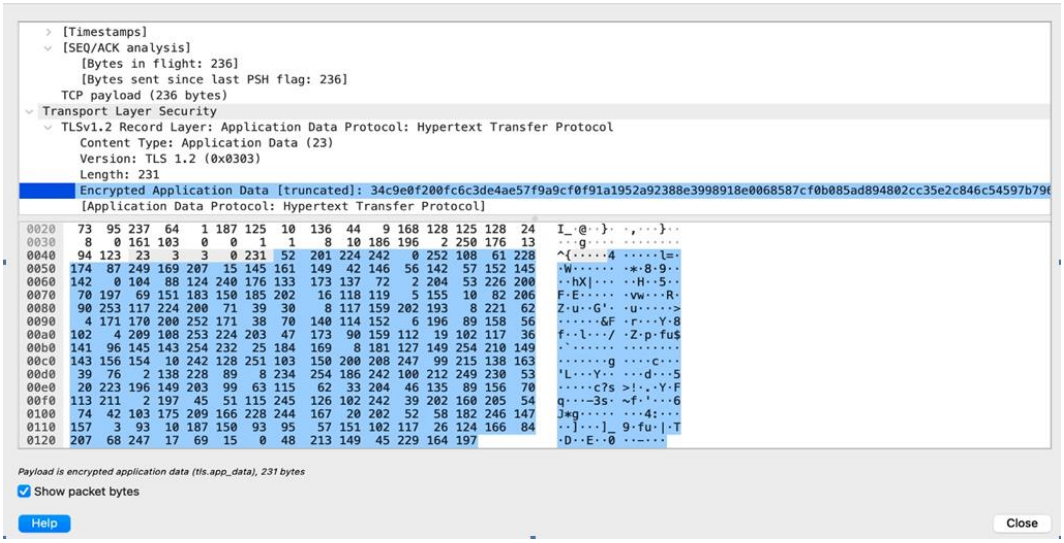
Dobiveni rezultat instalacije u JumpCloud administratorskom sučelju je prikazan u JumpCloud administratorskom sučelju putem poruke kojoj se može pristupiti u statusnoj traci komandi za određeni uređaj (Slika 8).

Slika 8. Rezultat poslane komande za instalaciju aplikacije u JumpCloud administratorskom sučelju

Analiza Wireshark paketa prikazuje komunikaciju između lokalnog računala (192.168.1.240) i JumpCloud servera (34.237.73.95). Na slici se vidi korištenje protokola TLSv1.2, što označava sigurnu komunikaciju između uređaja. *Application Data* unutar ovog protokola je šifrirana (označeno kao "*Encrypted Application Data*"), što znači da sadržaj podataka nije dostupan za pregled, ali protokol i metapodaci pokazuju da je riječ o HTTPS komunikaciji (Slika 9). U paketu broj 173223, podaci unutar segmenta "Application Data" su zaštićeni šifriranjem. Koristi se TLSv1.2, što ukazuje na sigurnu i pouzdanu razmjenu podataka. Iako sadržaj samih podataka nije čitljiv, prisutnost ovog protokola potvrđuje sigurnost prijenosa. Donji dio prikaza analizira pojedini paket, uključujući detalje poput Transport Layer Security (TLS) protokola, vrste sadržaja (*Application Data*), duljine i strukture paketa. Duljina šifriranih podataka iznosi 231 bajt, dok su ostali dijelovi paketa specifični za TCP prijenos. Na drugoj slici vidi se niz paketa, uključujući TCP pakete koji služe za uspostavu i održavanje veze. Uočene su ACK i FIN poruke koje potvrđuju uspješan prijenos podataka i zatvaranje sesije, što ukazuje na uspješno uspostavljenu vezu s JumpCloud serverom. Ova analiza prikazuje slanje komandi za instalaciju putem JumpCloud administratorskog sučelja. Iako su podaci zaštićeni šifriranjem, metapodaci i protokoli jasno pokazuju uspješan prijenos i sigurnu komunikaciju tijekom slanja komandi na server (Slika 10).



Slika 9. Prikaz paketa pri slanju komande za instalaciju preko JumpCloud admin sučelja



Slika 10. Prikaz paketa Application Data u trenutku slanja komande za instalaciju Softwarea putem JumpCloud komande

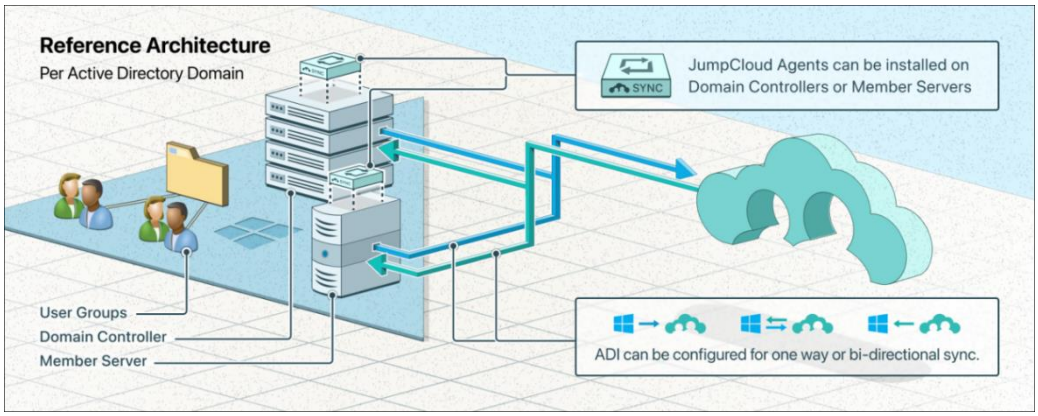
4.3. Sinkronizacija Postojećeg Active Directory sustava s JumpCloudom

JumpCloud se može integrirati s Active Directoryem koristeći JumpCloudovu ADI (eng. JumpCloud Active Directory Integration) opciju ugrađenu u samom sustavu. ADI omogućuje sinkronizaciju korisničkih informacija i grupa između JumpClouda i lokalnog ili udaljenog Active Directory sustava i koristi iste korisničke podatke za prijavu za sve resurse upravljive Active Directory i JumpCloud sustavom. ADI može biti raspoređen u raznim fleksibilnim konfiguracijama koje pašu za različite organizacije, ciljeve te Active Directory okruženja.

Postoje tri najčešća oblika ADI raspoređivanja:

- Proširivanje Active Directory okruženja da podrži dodatne mogućnosti u oblaku i veću fleksibilnost sustava.
- Smanjenje broja resursa koji su upravljani sa strane Active Directorya bez zamjene originalnog Active Directory okruženja.
- Kompletna migracija s Active Directory okruženja da cijeli sustav bude isključivo pod JumpCloud okruženjem.

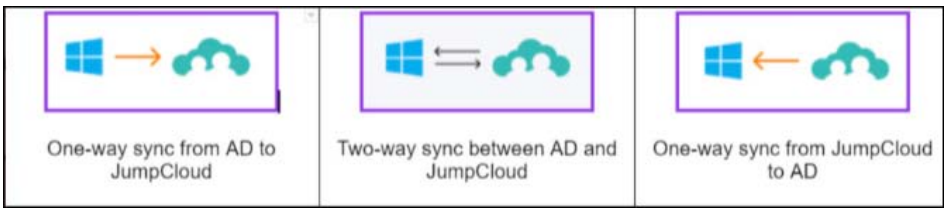
Prikaz referentne arhitekture sinkronizacije lokalnog Active Directory sustava i JumpCloud sustava u oblaku u kontekstu korisničkih grupa, domenskih upravljača te korisničkog poslužitelja (Slika 11).



Slika 11. Arhitektura sinkroniziranog Active Directory sustava s JumpCloudom

Isto tako postoji i tri moguće konfiguracije raspoređivanja i sinkronizacije podataka između Active Directorya i JumpClouda (Slika 12).

- Jednosmjerna sinkronizacija iz Active Directorya prema JumpCloudu opisuje situaciju gdje se bilo koja promjena u Active Directory sučelju isključivo jednosmjerno ažurira u JumpCloud sučelju.
- Dvosmjerna sinkronizacija znači da će se sustav ažurirati ako se napravi promjena i u Active Directory i u JumpCloud sučelju.
- Jednosmjerna sinkronizacija iz JumpClouda prema Active Directoryu znači da se ažuriranje sustava isključivo iz JumpClouda odražava na Active Directory.

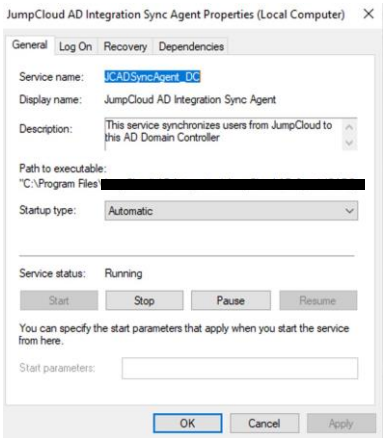


Slika 12. Grafički prikaz sinkronizacije između Active Directory i JumpCloud sustava

U postojećem sustavu integracija funkcionira pomoću JumpCloud sinkronizacijskog agenta. Njegova instalacija na poslužitelju omogućuje spajanje Active Directorya s JumpCloudom i spaja sve korisnike, korisničke grupe i podatke, pravila grupe pa čak i postavke adresa elektroničke pošte svih korisnika i sigurnosnih grupa. Agent je u Active Directoryu instaliran pomoću dobivene datoteke iz JumpCloud sučelja i mora se definirati u postavkama Active Directorya. Radi kao proces u Services aplikaciji za Windows Server programsko sučelje (Slika 13).

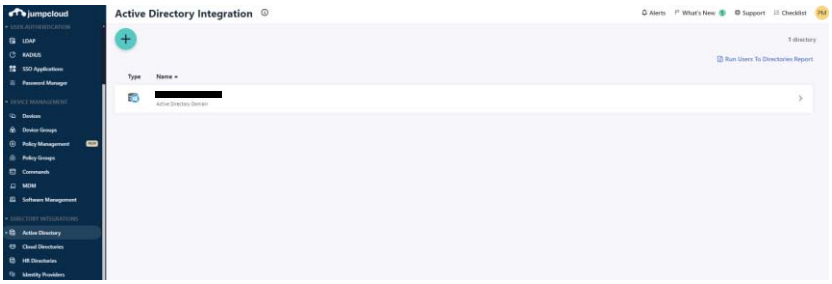
Slika 13. JumpCloud Sync i Import agenti u Windows Server okruženju

Sync agent mora raditi kontinuirano kako bi sinkronizacija između JumpClouda i Active Directoryja bila uspješna. U slučaju bilo kakvih poteškoća tijekom sinkronizacije, moguće je putem Windows Server okruženja pristupiti svojstvima servisa i ponovno pokrenuti Sync agenta. Ako ponovno pokretanje ne otkloni problem, može se izvršiti ponovna instalacija agenta (Slika 14).

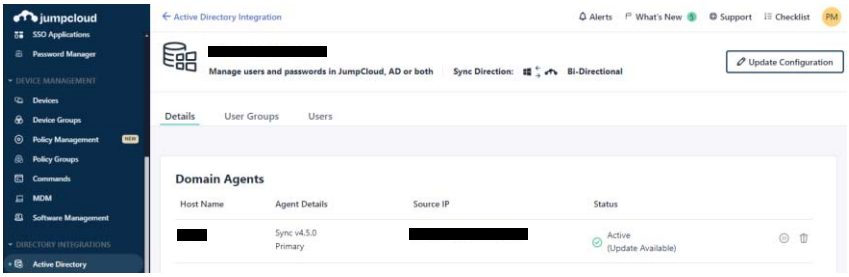


Slika 14. Svojstva JumpCloud Sync agenta u okruženju Windows Server

U JumpCloud administratorskom sučelju pod Directory Integrations – Active Directory je vidljiv popis svih mogućih Active directory integracija, broj korisnika i broj korisničkih grupa (Slika 15). U kontekstu organizacije vidljivi su prikazi agenta koji su trenutno aktivni i u procesu sinkronizacije, prikazana je njihova verzija, prikaz stanja u kojem mogu biti (Slika 16).



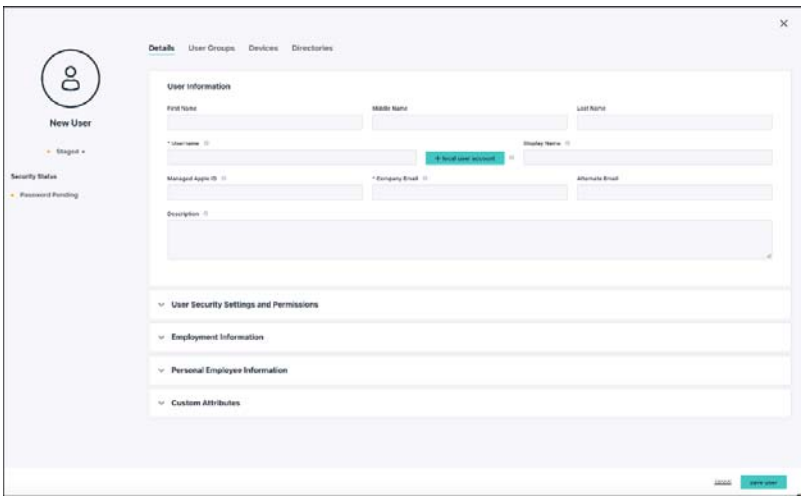
Slika 15. Popis Active Directory integracija u JumpCloud administratorskom okruženju



Slika 16. Prikaz popisa agenta za sinkronizaciju u JumpCloud administratorskom okruženju

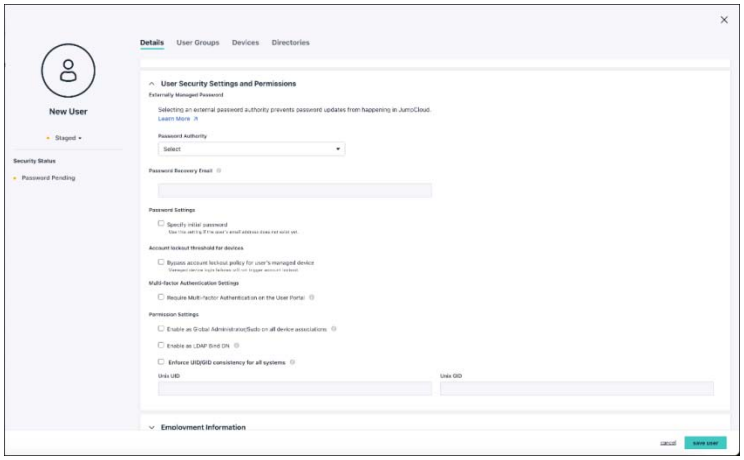
4.4. Dodavanje korisnika u JumpCloudu i osnovne značajke korisničke administracije

Korisnici se mogu dodati na mnogobrojne načine, uključujući ručno, putem očitanja CSV datoteke, putem API-ja ili iz druge aplikacije ili directoryja. Moguće su i razne integracije pomoću SCIM sustava. Ručno dodavanje korisnika u JumpCloud administratorskom sučelju, kao i u bilo kojem okruženju za upravljanje korisnika ima sustav upisa osnovnih informacija o korisniku kao što su puno ime i prezime, korisničko ime, adresa elektroničke pošte vezana za organizaciju, alternativna adresa elektroničke pošte i sl. Iz JumpCloudovog sučelja se uz osnovne informacije mogu odmah za korisnika postaviti razna pravila u grupaciji, sigurnosne postavke (npr. postavljena lozinka korisničkog računa u organizaciji), može se odmah korisnik povezati na određeni pretpodešeni uređaj ako je podešen prije dodavanja korisnika (Slika 17).



Slika 17. *New User* sučelje u JumpCloudovom administratorskom portalu

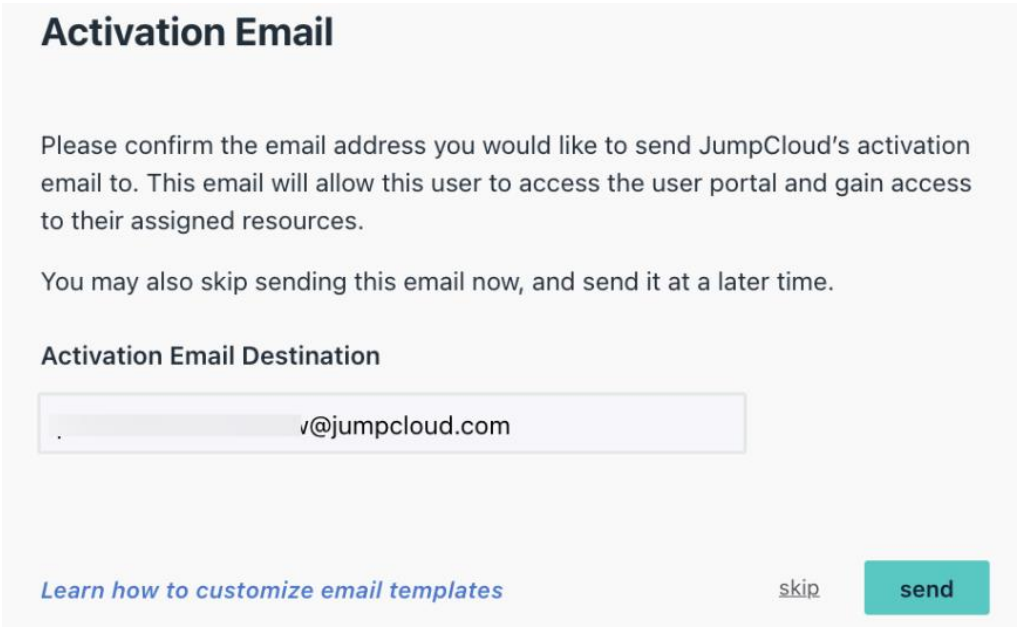
Zelenim gumbom označeno *Local User Account* je zapravo stavka koja je bitna kod povezivanja korisnika s podešenim uređajem. To znači da ako želimo da taj korisnik preuzme ovlasti nad uređajem, korisničko ime u JumpCloudu i korisničko ime na tom uređaju moraju biti jednaki. Ako se pretpodesi uređaj za korisnika tada se na tom uređaju može postaviti korisničko ime u istome formatu kako bi željeli da bude u JumpCloud sustavu (npr. ime.prezime, prezimeime i sl.). Korisničko ime se određuje ovisno o standardima organizacije. Elektronička pošta tvrtke naravno isto spada u definirane postavke tvrtke te se mora podudarati sa formatom korisničkog imena. Nakon upisa osnovnih podataka o korisniku, ispunjuju se korisničke sigurnosne postavke i dozvole (Slika 18).



Slika 18. Prikaz korisničkih sigurnosnih postavki i dozvole

Lozinkom koju upravlja vanjska platforma se zapravo zaustavlja promjena lozinke unutar

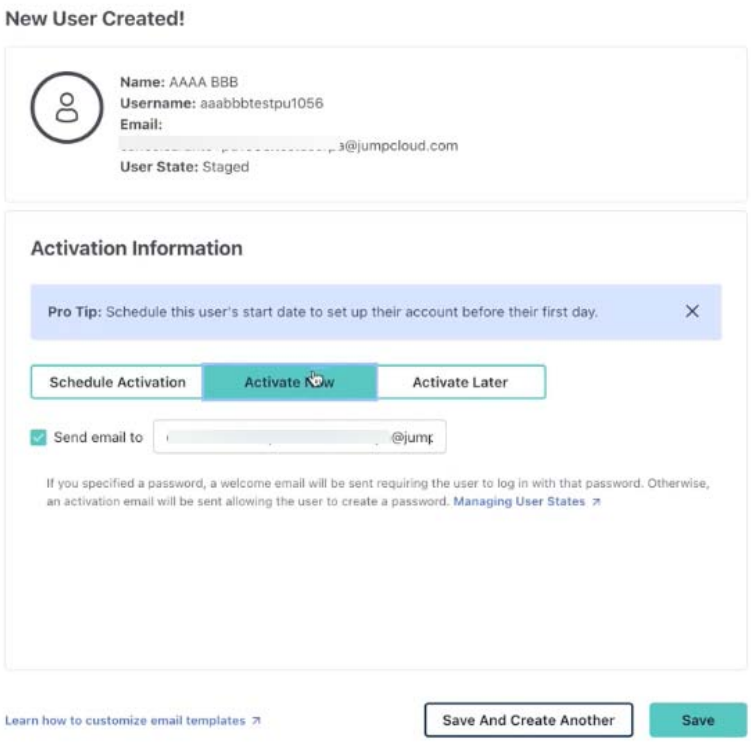
JumpCloud sustava sa strane korisnika i administratora. Kada je korisnička lozinka vanjski namještena, tada ne postoji istek lozinke, te korisnici neće dobivati obavijesti o zamjeni svoje lozinke unutar organizacije. Ova postavka se upotrebljava kada korisničkom lozinkom upravlja pomoću IdP-a. Elektronička pošta za obnovu lozinke se upisuje ako je definirano kao opcija za promjenu lozinke. Opcije lozinke postoje u slučaju kako bi se specificirala inicijalna lozinka za novog korisnika. Ova opcija se koristi ako korisnik još nema postavljenu adresu E-pošte u organizaciji. U slučaju da administrator postavi početnu lozinku na JumpCloudu, korisnik ne dobiva nikakvu obavijest, nego ta lozinka stupa na snagu istog trenutka. Može se postaviti da se korisnički račun ili uređaj koji je spojen s računom ne zaključaju u slučaju previše neuspjelih pokušaja upisa lozinke, postoje i postavke višefaktorske autentifikacije gdje se pri inicijalnoj registraciji korisnika može zahtijevati postavljanje autentifikacije ili se može odrediti neki točan period do kada korisnik mora obaviti spajanje višefaktorske autentifikacije sa svojim računom. Mogu se isto tako postaviti globalne administratorske ovlasti na uređaje što je bitno kada tvrtka ima ograničenja kod korištenja poslovne opreme. Kada se ispune sve osobne i poslovne informacije za korisnika, odabere se opcija da se korisnik spremi i tada je korisnik službeno kreiran u organizaciji. Ovisno o postavkama, korisnik može automatski biti postavljen u aktivno stanje, pri spremanju korisnika se pojavljuje prozor za slanje aktivacijske E-pošte na adresu koja je određena pri kreaciji samog korisnika (Slika 19).



Slika 19. Prozor za slanje aktivacijske E-pošte pri kreiranju novog korisnika

Isto tako ako je stanje korisnika postavljeno kao prirađeno, pri spremanju korisnika se dobije

prozor da se postavi točan datum aktivacije korisnika što može biti korisno ako se unaprijed zna trenutak kada korisnički račun treba biti aktiviran za tvrtku i olakšava dodatnu provjeru kod same aktivacije za IT administratore (Slika 20).



Slika 20. Prozor za postavke točnog datuma aktivacije korisnika pri kreaciji

5. ZAKLJUČAK

Nakon temeljitog istraživanja DaaS sustava u oblaku , utvrđene su prednosti i nedostaci tih sve popularnijih sustava u IT industriji. Bogata dokumentacija dostupna na internetu omogućuje detaljno razumijevanje funkcionalnosti i pogodnosti udaljenog upravljanja IT sustavima u organizacijama različitih veličina. Analiza paketa u Wiresharku omogućila je uvid u komunikaciju između računala i administrativnog web sučelja JumpClouda. Prikazom šifriranih paketa može se razumjeti kako se odvija komunikacija s udaljenim web serverom prilikom spajanja na web sučelje. Dodatno, pojašnjena je uloga interkoma u osiguravanju komunikacije, čime se onemogućava jednostavan pristup podacima putem alata poput Wiresharka. To dodatno potvrđuje da su DaaS sustavi u oblaku sigurni te da učinkovito štite organizacije od potencijalnih kibernetičkih napada. Zaključak je da implementacija sustava za udaljeno upravljanje i organizaciju može značajno unaprijediti IT infrastrukturu u organizacijama svih veličina. S obzirom na sve češći rad na daljinu, ovakvi sustavi predstavljaju budućnost jer smanjuju troškove opreme, kontinuirano se unapređuju, te znatno olakšavaju posao IT administratorima u sadašnjosti i bližoj budućnosti. Osim tehničkih aspekata, primjena tih sustava ima značajan utjecaj na poslovanje organizacija. Korištenje ovih tehnologija omogućava smanjenje operativnih troškova putem centraliziranog upravljanja uređajima i aplikacijama, što smanjuje potrebu za fizičkom infrastrukturom. Ovaj aspekt je posebno koristan za male i srednje tvrtke koje možda nemaju dovoljno resursa za održavanje kompleksnih IT sustava. Istovremeno, velike organizacije mogu upravljati uređajima i korisnicima na globalnoj razini, smanjujući vrijeme potrebno za rješavanje problema i optimizaciju performansi. Sigurnosni aspekti također su ključni. Šifriranje podataka i komunikacija putem sigurnih protokola, kao što je prikazano u analizi Wiresharka, osiguravaju zaštitu podataka u svakom trenutku. Kako se kibernetičke prijetnje nastavljaju razvijati, implementacija naprednih sigurnosnih mjera unutar ovih sustava postaje sve važnija za zaštitu organizacija od napada koji mogu ugroziti poslovanje i povjerenje klijenata. Uvođenje DaaS sustava u oblaku donosi i povećanu fleksibilnost poslovanja. U dinamičnim okruženjima gdje zaposlenici rade na daljinu ili koriste vlastite uređaje (BYOD – eng. Bring Your Own Device), ovi sustavi omogućavaju sigurno upravljanje i pristup IT resursima bez obzira na lokaciju. Ovo je ključno u suvremenim organizacijama koje se sve više oslanjaju na rad na daljinu i suradničke platforme za podršku poslovnim procesima. Osim toga, dugoročna prednost ovih sustava ogleda se u njihovoj skalabilnosti. Organizacije mogu brzo proširiti ili smanjiti opseg upravljanja uređajima i korisnicima prema svojim trenutnim potrebama, čime se osigurava prilagodljivost promjenama u poslovnom okruženju. To omogućava brže odgovore na

tehnološke izazove te doprinosi efikasnijem poslovanju. Na temelju ovog istraživanja može se zaključiti da implementacija DaaS-a donosi višestruke prednosti u upravljanju IT resursima, povećanju sigurnosti i optimizaciji operativnih procesa. Ubrzan razvoj tehnologije i rastući trendovi digitalne transformacije usmjeravaju organizacije prema sve većoj upotrebi ovakvih rješenja, čime se omogućava lakše održavanje IT sustava, bolja zaštita podataka i povećanje operativne efikasnosti. Zaključno, može se reći da su DaaS sustavi u oblaku i ključni alati u modernom IT okruženju. Njihova implementacija postaje neophodna za organizacije koje žele osigurati fleksibilnost, sigurnost i skalabilnost svojih IT operacija, a pritom smanjiti troškove i optimizirati radnu učinkovitost. Kako se tehnološki ekosustavi nastavljaju razvijati, ove tehnologije će i dalje igrati značajnu ulogu u upravljanju organizacijama, posebno u kontekstu sve veće digitalizacije i globalizacije poslovanja. Implementacija ovakvih rješenja omogućava organizacijama da se prilagode izazovima budućnosti, osiguravajući stabilan i siguran IT temelj za rast i razvoj.

LITERATURA

1. Jumpcloud.com, (2014.), https://jumpcloud.com/blog/what-is-daas-directory-as-a-service (pristupljeno 27. 3. 2024.)
2. Jumpcloud.com, (2019.), https://jumpcloud.com/blog/iam-vs-idp (pristupljeno 30. 3. 2024.)
3. Jumpcloud.com, (2022.), https://jumpcloud.com/support/use-cloud-ldap (pristupljeno 5. 4. 2024.)
4. Jumpcloud.com, (2021.), https://jumpcloud.com/blog/single-sign-on-actually-works (pristupljeno 5. 4. 2024.)
5. Ansys.com (2023.), https://developer.ansys.com/product/Tools-for-Ensight-Post-Processing/group__websocketserver.xhtml (pristupljeno 15. 6. 2024.)
6. Accuenergy.com, https://www.accuenergy.com/support/reference-directory/tls-transport-layer-security-protocol/ (pristupljeno 17. 6. 2024.)
7. Jumpcloud.com (2021.) https://jumpcloud.com/support/add-users-to-admin-portal (pristupljeno 30. 8. 2024.)

SAŽETAK

Ovaj završni rad temelji se na analizi rada postojećeg sustava za udaljeno upravljanje IT sistemima te njegove analize kroz istraživanje i mrežnu analizu sustava s ciljem da se prikaže funkcionalnosti i pogodnosti ciljanog Directory sustava kao usluga i da se dokaže koliko jedan unificirani sustav u oblaku olakšava svakodnevne poslove u današnjem svijetu IT administracije i koje sve načine koristi da bi se poboljšao sustav i osiguranje u organizacijama i njihovim IT sistemima svih veličina.

Ključne riječi: višefaktorska autentifikacija, jedinstvena prijava, IT administracija, upravljanje sustavom, centralizirani sustav, sinkronizacija sustava, Active Directory, konfiguracija, sigurnost sustava

SUMMARY

This final thesis is based on the analysis of the existing system for remote and mobile device management for IT systems and its analysis through research and network analysis of the systems is aiming to show the functionality and benefits of the Directory-As-A-Service systems and it's implementation on the organization. It proves how much a unified Cloud system facilitates everyday tasks in today's world of IT administration and using all means improves various system management and security in organizations and their IT systems of all sizes.

Keywords: Multi-Factor authtentication - MFA, Single Sign-On – SSO, IT adminstration, system management, centralized system, synchronization, Active Directory, system configuration, system security