Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Pece Adjievski

Postavitev privatnega oblaka z VMware vCloud

diplomsko delo
na univerzitetnem študiju

Mentor: prof. dr. Matjaž Branko Jurič

Ljubljana, 2013

Besedilo je oblikovano z urejevalnikom besedil LaTeX.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Tržaška 25
1001 Ljubljana, Slovenija
telefon: 01 476 84 11
01 476 83 87
faks: 01 426 46 47
01 476 87 11
www.fri.uni-lj.si
e-mail: dekanat@fri.uni-lj.si

Št. naloge: 01865/2012
Datum: 04.09.2012

Univerza v Ljubljani, Fakulteta za računalništvo in informatiko izdaja naslednjo nalogo:

Kandidat: **PECE ADJIEVSKI**

Naslov: **POSTAVITEV PRIVATNEGA OBLAKA Z VMWARE VCLOUD**
PRIVATE CLOUD DEPLOYMENT USING VMWARE VCLOUD

Vrsta naloge: Diplomsko delo univerzitetnega študija

Tematika naloge:

Proučite področje računalništva v oblaku, koncepte in lastnosti privatnih in hibridnih oblakov. Predstavite osnovne koncepte virtualizacije v kontekstu računalništva v oblaku. Proučite rešitev VMware vCloud za postavitev IaaS (Infrastructure as a Service – infrastruktura kot storitev) privatnih in hibridnih oblakov ter analizirajte ključne komponente in funkcionalnosti. Raziščite dobre prakse načrtovanja arhitektur privatnih oblakov. Zasnujte in implementirajte arhitekturo privatnega oblaka s pomočjo rešitve VMware vCloud. Razširite arhitekturo privatnega oblak s pomočjo komponente vCloud Connector za implementacijo hibridnega oblaka.

Mentor:

prof. dr. Matjaž B. Jurič

Fakulteta za računalništvo in informatiko • UNIVERZA V LJUBLJANI • 2

Dekan:

prof. dr. Nikolaj Zimic

Izjava o avtorstvu diplomskega dela

Spodaj podpisani Pece Adjievski, z vpisno številko **63060409**, sem avtor diplomskega dela z naslovom:

Postavitev privatnega oblaka z VMware vCloud

S svojim podpisom zagotavljam, da:

- sem diplomsko delo izdelal samostojno pod mentorstvom prof. dr. Matjaža Branka Juriča
- so elektronska oblika diplomskega dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko diplomskega dela
- soglašam z javno objavo elektronske oblike diplomskega dela v zbirki "Dela FRI".

V Ljubljani, dne 6. marca 2013 Podpis avtorja:

Zahvalil bi se prof. dr. Matjažu Branku Juriču za strokovno pomoč in vodenje pri izdelavi diplomskega dela. Zahvala gre tudi staršema, za moralno in finančno podporo v teku študija.

Kazalo

Povzetek

Računalništvo v oblaku spreminja področje IT in poslovnim organizacijam prinaša številne prednosti in priložnosti, ki lahko prispevajo k bolj učinkovitemu poslovanju. Diplomska naloga obravnava računalništvo v oblaku in se pri tem osredotoča na področje privatnih in hibridnih oblakov, kjer želimo vzpostaviti okolje z obstoječimi in uveljavljenimi tehnologijami. Cilj tako vzpostavljenega okolja je omogočiti in zagotoviti samooskrbovanje infrastrukturnih - IaaS storitev. V uvodnem delu diplomske naloge smo naslovili osnovne koncepte virtualizacije kot tehnologijo, ki je ključnega značaja za računalništvo v oblaku. Spoznali smo tudi osnovne koncepte računalništva v oblaku in izpostavili bistvene značilnosti. V nadaljevanju smo si bolj podrobno ogledali rešitev VMware vCloud, kjer smo opisali posamezne komponente ter analizirali ključne funkcionalnosti in gradnike rešitve. Sledila je bolj podrobna obravnava vzpostavitve arhitekture privatnega oblaka, v okviru katerega smo analizirali dobre prakse. Podali smo tudi načrt ter izvedli implementacijo s pomočjo rešitve vCloud. V zadnjem poglavju smo si ogledali koncepte in prednosti hibridnih oblakov ter implementirali hibridno platformo s pomočjo komponente vCloud Connector.

Ključne besede: Računalništvo v oblaku, privatni oblak, hibridni oblak, IaaS, virtualizacija, VMware vCloud

Abstract

Cloud computing changes the IT sphere and brings numerous advantages and opportunities to organizations, which can contribute to improve business efficiency. The thesis addresses the cloud computing topic and focuses on the fields of private and hybrid clouds, where we want to establish an environment with the use of current and established technologies. The goal of the environment is to enable and provide self-provisioning of the infrastructure - IaaS services. In the introductory part we addressed the basic concepts of virtualization which is a key cloud computing technology. We also introduced the basic concepts of cloud computing, where we identified the essential characteristics of the cloud computing model. In the following part we provided a detailed overview of VMware vCloud solution, in which we described the individual components and analyzed key functionalities and building blocks of the solution. In addition, we described the establishment of the private cloud architecture, with the inclusion of best practice analysis. We provided architecture design and we implemented it using the vCloud solution. Finally, we have shown the concepts and benefits of hybrid clouds, while implementing the hybrid cloud platform.

Keywords: Cloud Computing, private cloud, hybrid cloud, IaaS, virtualization, VMware vCloud

Poglavje 1

Uvod

Računalništvo v oblaku (ang. Cloud Computing) se kot nova paradigma vse več uveljavlja v svetu informacijske tehnologije (IT) in spreminja model tradicionalnega računalništva podobno je bila vzpostavitev električnega omrežja in centralizacije elektrarn. Z vidika končnega porabnika električne energije ni pomembno kako se le-ta generira ter kako pride do vtičnice v domovih. Če slednji koncept razširimo na področje računalništva dobimo model, ki izpostavlja računalniške vire in funkcionalnosti, ki so na voljo končnim uporabnikom in pri tem abstrahira podrobnosti kje in kako se izvajajo.

Izpostavljeni viri in funkcionalnosti so definirani kot storitve glede na nivo abstrakcije in so dostopni preko omrežne povezave. Glavna značilnost in prednost tega modela je, da sledi konceptu storitvenega računalništva (ang. Utility computing), kjer je zaračunavanje izvedeno na osnovi dejanske porabe virov s strani uporabnika. Model sam po sebi nima velikega pomena brez ustreznih tehnologij, ki ga omogočajo in mu dajejo pomen. Tehnologije kot so virtualizacija strojne opreme, avtomatizacija podatkovnih centrov, gruče, spletne tehnologije (Web 2.0, Spletne storitve, Storitveno-orientirane arhitekture), omogočajo ter so prispevale k uveljavitvi modela računalništva v oblaku.

Po mnenjih številnih IT podjetji in ponudnikov storitev kot so Amazon, Google, Microsoft, Cisco, IBM in drugi, je računalništvo v oblaku nasle-

dnji logični korak, saj ponuja mehanizme kako povečati nadzor IT virov in obenem tudi zmanjšati celotne stroške lastništva (ang. Total Cost of Ownership - TCO). Računalništvo v oblaku končnim uporabnikom/najemnikom računalniških virov in storitev prinaša številne prednosti v primerjavi s tradicionalnim modelom. Podjetja lahko potrebne računalniške vire najamejo na zahtevo pri enem izmed ponudnikov. S tem se izognejo nakupu nove strojne opreme in posredno zmanjšajo stroške vzdrževanja strojne opreme, kar lahko pomeni doseganje bolj konkurenčnih cen na trgu. Razvijalcem aplikacij nudi bolj fleksibilen in hitrejši način razvoja, saj se lahko razvijalci osredotočijo na implementacijo funkcionalnosti, ki prinašajo dodano vrednost ne pa na pripravo in konfiguracijo izvajalnega okolja.

Kljub veliki priljubljenosti modela računalništva v oblaku se številne poslovne in druge organizacije ne odločajo za prehod v oblak. Glavni razlog za to je seveda varnost, zasebnost in nadzor podatkov v okolju javnih oblakov. Določene poslovne organizacije, posebej tiste ki se ukvarjajo z občutljivimi podatki, morajo namreč zagotoviti skladnost z določenimi predpisi za varnost in nadzor podatkov. Slednje je seveda v okolju, kjer je infrastruktura deljena med zelo veliko število uporabnikov, težko doseči. Zelo pomembno vprašanje, ki se pojavi, je kako izkoristiti prednosti, ki jih prinaša računalništvo v oblaku in obenem obdržati skladnost z določenimi predpisi. Odgovor je, s postavitvijo modela računalništva v oblaku znotraj podatkovnega centra v privatnem omrežju ene poslovne organizacije. Kot bomo spoznali v nadaljevanju, je takšna postavitev definirana kot privatni - zasebni oblak.

Cilj diplomske naloge je (1) opisati ključne komponente rešitve VMware vCloud ter analizirati njihove funkcionalnosti in gradnike, (2) vzpostaviti arhitekturo privatnega oblaka skozi analizo dobrih praks ter smernic iz kataloga vCAT (vCloud Architecture Toolkit) za načrtovanje in implementacijo arhitektur privatnih oblakov, ter (3) nadgraditi arhitekturo privatnega oblaka z vzpostavitvijo hibridne platforme.

Poglavje 2

Osnove virtualizacije

Živimo v času, kjer je učinkovitost podatkovnih centrov ključnega pomena za obstoj poslovanja poslovne organizacije. Virtualizacija se je izkazala kot tehnologija, ki prinaša mehanizme, ki lahko močno izboljšajo učinkovitost obratovanja podatkovnih centrov. Virtualizacija je danes postala v sodobnih podatkovnih centrih nekaj običajnega, saj ponuja številne koristi kot so prihranki energije, zmanjševanje fizičnih prostorov, hitrejše oskrbovanje (ang. Provisioning) strežnikov, boljša izolacija med aplikacijami, odpravi nezdružljivost programske in strojne opreme, zmanjšanje stroškov kapitala ter stroškov obratovanja, itd. Vsi omenjeni faktorji lahko pozitivno učinkujejo na obratovanje poslovne organizacije.

Osnovni koncept virtualizacije je v abstrakciji fizičnih komponent v logične objekte, kot so na primer strežniki, omrežne naprave, naprave za shrambo [1], itd. S tem skriva fizične lastnosti naprave. Delo z logičnimi objekti omogoča večjo fleksibilnost in lažje upravljanje. Virtualizacija strežnikov prinaša tudi večjo izkoriščenost fizične platforme, tako da se na enem fizičnem stroju izvaja več virtualnih strojev, kar pripelje do zmanjšanja števila potrebnih fizičnih strežnikov.

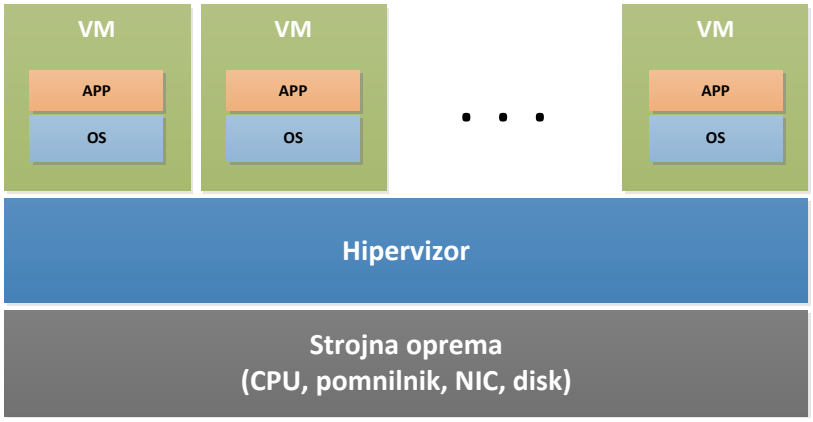
Virtualizacijo lahko obravnavamo z dveh aspektov [2]. Prvi aspekt se nanaša na kreiranju več virtualnih virov iz enega fizičnega vira. Kot primer lahko vzamemo postopek konsolidacije strežnikov skozi proces virtualizacije,

kar prinese boljša izkoriščenost fizičnega strežnika. Drugi aspekt se nanaša na kreiranje virtualnega (logičnega) vira iz več fizičnih virov. Virtualizacijo celotne infrastrukture podatkovnega centra lahko vzamemo kot primer takšnega pristopa virtualizacije. Večje število fizičnih strežnikov združimo in abstrahiramo kot en virtualni vir. Takšen pristop virtualizacije se izkaže kot zelo primerna oblika v kontekstu računalništva v oblaku. Virtualizacija infrastrukture v ekosistem oblaka prinaša večjo fleksibilnost.

Skoraj vse rešitve, ki omogočajo gradnjo in upravljanje oblakov, kot temelj oblaka uporabljajo virtualizirano infrastrukturo. Zelo pogosto se pojem virtualizacije poistoveti z računalništvom v oblaku, kar seveda ni pravilno. Virtualizacija je le ena izmed tehnologij, ki igra pomembo vlogo v modelu računalništva v oblaku. Pri tem je potrebno omeniti, da virtualizacija ni nujno potrebna za računalništvo v oblaku, saj je model računalništva v oblaku možno implementirati tudi na ne-virtualizirano infrastrukturo. Obstajajo ponudniki, ki so to praktično demonstrirali. Najbolj odmeven primer je Google. Kljub izvedljivosti implementacije modela na ne-virtualizirano infrastrukturo se tak pristop za večino ponudnikov in poslovnih organizacij izkaže kot stroškovno neučinkovit v primerjavi z implementacijo modela na virtualizirano infrastrukturo. Dejstvo je, da večina aplikacij, ki se danes izvaja v podatkovnih centrih ne bi pridobila na zmogljivosti, če bi se izvajale na fizičnem strežniku. Aplikacije ne morejo učinkovito izkoristiti današnje več-jedrne centralne procesne enote.

2.1 Osnovni tipi virtualizacije

Virtualizacija kot pojem ima širši pomen. Skozi čas se je uveljavilo več tipov virtualizacije glede na domeno fizične infrastrukture, ki se virtualizira [2]. V nadaljevanju poglavja si bomo ogledali osnovne tipe virtualizacije in njihove značilnosti.



Slika 2.1: Princip strežniške virtualizacije [1].

2.1.1 Strežniška virtualizacija

Strežniška virtualizacija, znana tudi kot strojna virtualizacija, je najbolj znana in najstarejša oblika virtualizacije. Osnovni princip te oblike virtualizacije je v izvajanju več virtualiziranih strojev na enem fizičnem stroju. S tem želimo izboljšati učinkovitost fizičnih strojev. Današnja arhitektura x86, je bila namreč zasnovana za izvajanje enega samega operacijskega sistema na enem samem fizičnem stroju, kar pripelje do slabe izkoriščenosti stroja. Princip strežniške virtualizacije je prikazan na sliki 2.1.

Da bi omogočili virtualizacijo fizičnega stroja potrebujemo dodatno komponento imenovano *hipervizor* (ang. Hypervisor), ki doda nivo abstrakcije nad fizično strojno opremo. Hipervizor, znan tudi kot upravljalec virtualnih strojev (ang. Virtual Machine Manager - VMM), je programska oprema, ki omogoča kreiranje virtualnih strojev tako, da naredi ločeno okolje operacijskega sistema. Več operacijskih sistemov se izvaja sočasno na istem fizičnem stroju. Okolje je logično izolirano od fizičnega stroja. Fizični stroj na katerem je nameščen hipervizor je poimenovan kot *gostitelj* (ang. Host).

V praksi obstajata dva tipa hipervizorjev [3]. Prvi tip hipervizorjev je nameščen in se izvaja neposredno na strojni opremi gostitelja ter ne potre-

buje prednameščenega operacijskega sistema. Znan je tudi kot *bare-metal* hipervizor. Primeri hipervizorjev tega tipa so VMware ESX/ESXi, Microsoft Hyper-V, KVM, Xen, itd. Za drug tip hipervizorjev je značilno, da je nameščen in se izvaja kot programska oprema znotraj operacijskega sistema nameščenega na fizičnem stroju. Primer takšnih hipervizorjev so VMware Workstation, VirtualBox, Windows Virtual PC, itd. Produkti prvega tipa hipervizorjev v primerjavi z drugim tipom neposredno komunicira s strojno opremo, kar izboljša zmogljivostne karakteristike. Zaradi tega se v strežniški virtualizaciji uporablja prvi tip.

Ključne prednosti, ki jih prinaša strežniška virtualizacija v primerjavi s tradicionalnim modelom gostovanja aplikacij so:

- Sočasno izvajanje več različnih operacijskih sistemov na enem fizičnem stroju.
- Napaka v enem virtualnem stroju nima vpliva na delovanje ostalih.
- Celotno stanje virtualnega stroja se lahko shrani v datoteki.
- Premikanje in kopiranje stanja virtualnega stroja postane trivialno, saj premikamo in kopiramo datoteko.
- Možnost spreminjanja konfiguracije virtualnega stroja med izvajanjem.

2.1.2 Virtualizacija shrambe

Princip virtualizacije shrambe zagotavlja logičen, abstrahiran pogled fizičnih naprav za shrambo podatkov. Na ta način je shramba uporabnikom predstavljena kot bazen shrambe brez navidezno fizičnih mej. Virtualizacija skrije dejstvo, da je shramba sestavljena iz več fizičnih enot za shranjevanje podatkov, in sicer na način, da prikaže posamezne naprave kot eno napravo.

Virtualizacija shrambe se nanaša tako na lokalno kot tudi na oddaljeno shrambo. V primeru lokalne shrambe je to logično particioniranje fizičnih diskovnih enot. Druga oblika virtualizacije lokalne shrambe so tudi redundantna

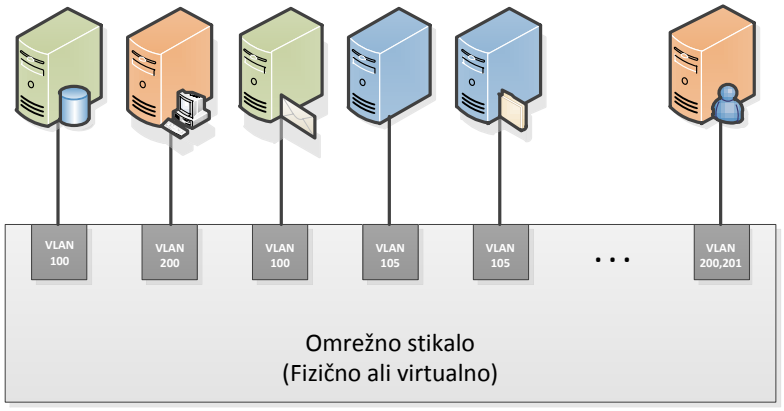
polja neodvisnih diskovnih enot (ang. Redundant Array of Independent Disks - RAID), saj RAID polje prikaže eno logično enoto ne glede na število fizičnih diskov enot.

Virtualizacija oddaljene shrambe se nanaša na SAN (Storage-Area Network) polja. V tem primeru shramba je odklopljena od strežnike in je dostopna preko omrežja. Za dostop do oddaljene shrambe se uporablja protokol iSCSI (ang. Internet Small Computer System Interface), FC (ang. Fibre Channel) ali FCoE (ang. Fibre Channel over Ethernet). Z izpostavljanjem virtualizirane shrambe na omrežju se omogoči bolj učinkovito delitev shrambe med strežniki ter poveča skalabilnost in fleksibilnost. Ker so strežniki povezani na SAN shrambo, se ne zavedajo prisotnosti fizičnih diskovnih enot. Zaradi tega je dodajanje novih diskovnih enot ali zamenjava ob okvari enostavna.

2.1.3 Virtualizacija omrežja

Virtualizacija omrežja zajema več različnih oblik. Najbolj znana in pomembna oblika v kontekstu računalništva v oblaku so virtualna lokalna omrežja (ang. Virtual Local Area Network - VLAN) [4]. Osnovni koncept uporabe VLAN-ov je v logičnem segmentiranju fizičnih LAN omrežij v več izoliranih *broadcast* domen. VLAN segmente je možno konfigurirati na omrežnem stikalu, ki takšno segmentacijo podpira. Vratom na stikalu lahko določimo kateremu VLAN segmentu pripada, kot je to prikazano na sliki 2.2. Vsakemu VLAN segmentu pripada 12-biten VLAN identifikator. Vrata na stikalu so lahko konfigurirana tudi v t.i. *trunk* načinu. V tem primeru so vrata konfigurirana tako, da prepuščajo promet iz več VLAN segmentov. Naprave znotraj enega VLAN segmenta lahko komunicirajo le z napravami v istem VLAN segmentu. S tem se doseže izolacija omrežij na drugem nivoju modela OSI (ang. Open Systems Interconnection).

VLAN segmentacija igra zelo pomembno vlogo tudi v ekosistemu oblaka, saj predstavlja mehanizem, ki zagotovi izolacijo med posameznimi uporabniki/najemniki oblaka, kar je ključnega značaja v deljenem okolju. Poleg



Slika 2.2: VLAN segmentacija omrežja.

tega prinaša tudi večjo skalabilnost in fleksibilnost omrežja.

Poleg virtualizacije omrežij je možno virtualizirati tudi same fizične naprave, ki skrbijo za omrežno povezavo, kot so na primer omrežna stikala, usmerjevalniki, itd. Kot bomo videli v nadaljevanju, imajo številne virtualizacijske platforme vgrajena virtualna stikala za povezavo virtualnih strojev, ki se izvajajo na enem gostitelju. Možna je tudi virtualizacija omrežnih storitev kot so na primer požarni zidovi, izenačevalniki obremenitev, VPN (ang. Virtual Private Network) storitve, itd.

Poglavje 3

Koncepti računalništva v oblaku

Kljub temu, da računalništvo v oblaku združujejo že znani in uveljavljeni koncepti in tehnologije, ne obstaja enotna definicija, ki bi definirala model računalništva v oblaku. Skoraj vsak strokovnjak na področju interpretira lastno definicijo tega modela. Nekatere so bolj splošne, druge pa bolj specifične za določeni postavitveni ter storitveni model. Definicije, ki so se najbolj izpostavile so naslednje:

- NIST (National Institute of Standards and Technology) [5] *"Model za omogočanje omrežnega dostopa do deljenih računalniških virov (omrežje, strežniki, shramba, aplikacije in storitve), ki so lahko rapidno oskrbovane in izdane z minimalnim trudom vodstva oziroma z interakcijo ponudnika storitve."*

- UC Barkley [6] *"Gre za aplikacije, strojno opremo in sistemsko programsko opremo znotraj podatkovnih centrov, ki so dostavljene kot storitev preko medmrežja."*

- Wikipedia [7] *"Računalništvo, pri katerem so dinamično razširljiva in pogosto virtualizirana računalniška sredstva na voljo kot storitev preko interneta."*

3.1 Bistvene značilnosti oblaka

Kljub velikemu številu definicij računalništva v oblaku lahko ugotovimo, da večina definicij naslavlja podobne karakteristike. Osnovne značilnosti računalništva v oblaku izhajajo iz definicije, ki jo je postavil NIST. Definicija velja kot najbolj splošna in velja za vse postavitvene in storitvene modele, ki jih bomo spoznali v nadaljevanju. Kot ključne značilnosti lahko izpostavimo naslednje [5]:

- **Samopostrežba (ang. On-demand self-service):** Končni uporabniki oblaka morajo imeti možnost oskrbovanja z računalniškimi viri kot so računanje, shramba, omrežna povezava, brez potrebe po človeškem posredovanju. Rešitve, ki implementirajo in omogočajo računalništvo v oblaku morajo zagotavljati mehanizme, ki omogočajo samopostrežbo končnim uporabnikom. Slednje je v večini primerov izvedeno v obliki samopostrežnega portala, preko katerega se uporabniki oskrbijo z zahtevanimi viri.

- **Omrežni dostop (ang. Broad network access):** Vse zmožnosti in storitve, ki se izvajajo v oblaku morajo biti na voljo preko omrežja in dostopne preko standardnih mehanizmov, ne glede na heterogenost platform (mobilne naprave, tablični računalniki, prenosni računalniki itd.) iz katerih se dostopa. Vendar ni nujno, da so storitve vedno dostopni preko interneta - slednje je odvisno od postavitvenega modela oblaka.

- **Agregacija virov in več-najemniški model (ang. Resource pooling and multi-tenancy):** Viri oblaka so agregirani v bazen virov in so v večini primerov deljeni med različne najemnike oblaka. Deljene virov omogoča bolj učinkovito izkoriščenost virov. Ker so viri deljeni, je potrebno zagotoviti izolacijo med posameznimi najemniki. Agregacija virov v bazen virov dodaja abstrakcijski nivo, kar omogoča dinamično razvrščanje in razporejanje virov za čim bolj učinkovito izkoriščenost infrastrukture.

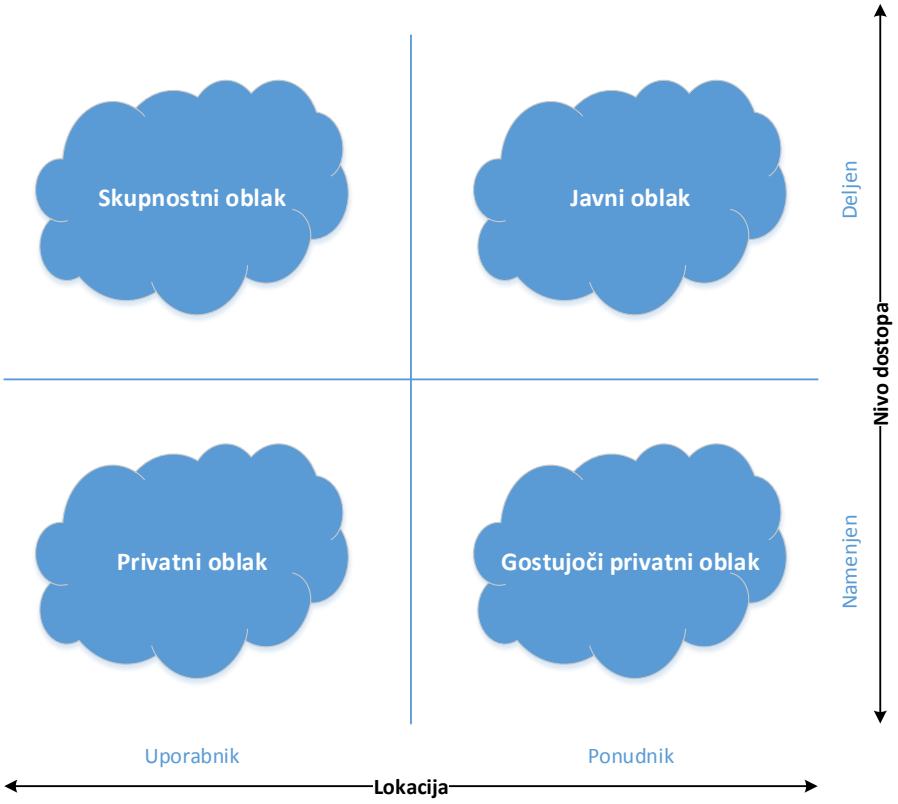
- **Elastičnost (ang. Elasticity):** Zmožnost dinamičnega dodajanja in odstranjevanja kapacitete virov sorazmerno potrebam. Ob povečanih kapacitetah se dodelijo dodatne kapacitete iz bazena virov ter ko se potrebe zmanjšajo se dodatne kapacitete vrnejo v bazen virov. Elastičnost kot ena izmed najbolj pomembnih značilnosti računalništva v oblaku prinaša bolj fleksibilno načrtovanje kapacitet, kar posredno lahko zmanjša stroške izvajanje storitve ter zagotovi izvajanje storitve ne glede na povpraševanja.

- **Merjenje storitev (ang. Measured service):** Rešitve, ki implementirajo model računalništva v oblaku morajo zagotoviti mehanizme za merjenje porabe in spremljanje izvajanja storitve v oblaku. Na osnovi tega se končnemu uporabniku zaračuna dejanska poraba storitve.

Poleg zgoraj obravnavanih značilnosti jih obstaja še veliko več, ki igrajo pomembno vlogo, kot so na primer avtomatizacija, programski vmesniki, upravljanje s podatki, itd.

3.2 Postavitveni modeli oblaka

Postavitveni model oblaka je model, ki opisuje okolje, kjer je infrastruktura oblaka postavljena, ter izvajalno okolje za storitve oblaka. Model računalništva v oblaku je bil v osnovi zasnovan kot javno dostopna storitev deljena med več uporabnikov. Izkazalo se je, da takšen pristop ne ustreza vsem organizacijam. Iz tega razloga se je skozi čas uveljavilo več različnih oblik postavitev računalniškega oblaka. Glede na fizično lokacijo postavitve oblaka in na delitev infrastrukture in vire oblaka poznamo javni oblak, privatni ali zasebni oblak, skupnostni oblak in hibridni oblak. Slika 3.1 bolj ilustrativno prikazuje vse postavitvene modele.



Slika 3.1: Postavitveni modeli oblaka.

3.2.1 Javni oblak

Najstarejšo in najbolj uporabljeno obliko postavitvenega modela računalništva v oblaku predstavlja javni oblak. Infrastruktura oblaka je deljena med veliko število uporabnikov/najemnikov virov in storitev oblaku. Infrastruktura oblaka je upravljana in v lasti zunanjega ponudnika, ki zagotavlja zahtevane vire in storitve končnim uporabnikom/najemnikom oblaka. Glavna lastnost javnih oblakov je zaračunavanja glede na porabo (ang. Pay-as-you-go), kar je tudi glavna prednost pred tradicionalnem gostovanju aplikacij.

Zagotavljanje storitev je izvedena na podlagi pogodb o zagotavljanju nivoju storitve (ang. Service-level agreement - SLA) med uporabnikom in ponudnikom storitve. SLA-ji nedvomno igrajo pomembno vlogo ne glede na

postavitveni model, vendar imajo v okviru javnih oblakov najbolj izraziti vpliv, saj predstavljajo osnovni mehanizem, ki končnemu uporabniku zagotavlja izvajanje storitve po določenih zahtevah.

Glavna pomanjkljivost javnih oblakov je pomanjkanje zaupanja med uporabnikom in ponudnikom javnih oblakov ter nadzor podatkov, kar se pojavi zaradi narave okolja v katerem se izvajajo storitve.

Primeri komercialnih javnih oblakov so Amazon AWS, IBM SmartCloud, Oracle Public Cloud, Windows Azure, itd.

3.2.2 Privatni oblak

Ta tip oblaka predstavlja zasebno postavitev modela računalništva v oblaku, ki je namenjen eni poslovni organizaciji. Infrastruktura oblaka je upravljana s strani organizacije ter postavljena v zasebnem podatkovnem centru. V večini primerov vzpostavitev privatnih oblakov predstavlja le prestrukturiranje obstoječe infrastrukture. Storitve, ki jih ponuja organizacija so lahko dostopne tako od zunaj kot tudi interno. V primerjavi z javnimi oblaki so infrastruktura in viri v tem primeru namenjeni izključno organizaciji. Slednje predstavlja glavno prednost pred javnimi oblaki in obenem tudi motivacijo za izbiro zasebne postavitve oblaka. Infrastruktura je namreč namenjena izključno eni organizaciji, pri čemer lahko organizacije implementirajo lastne politike o varnosti, nadzora in zasebnosti podatkov.

V primeru, da je infrastruktura oblaka upravljana in v lasti zunanjega ponudnika, gre za gostujoči privatni oblak. V primerjavi s klasično postavitvijo je slednja lahko cenejša izbira, vendar podatki niso na lokaciji odjemalca, temveč se nahajajo pri ponudniku.

Zasebna postavitev oblaka je v primerjavi z najemom virov v javnem oblaku lahko dražja izbira, saj mora organizacija sama poskrbeti za upravljanje in vzdrževanje celotne infrastrukture. Slednje je seveda odvisno tudi od velikosti in obsega poslovanja organizacije. V nadaljevanju se bomo osredotočili na ta postavitveni model. Trenutno najbolj uveljavljene rešitve pri-

vatnih oblakov so VMware vCloud, Microsoft Private Cloud, OpenStack, Eucalyptus, itd.

3.2.3 Skupnostni oblak

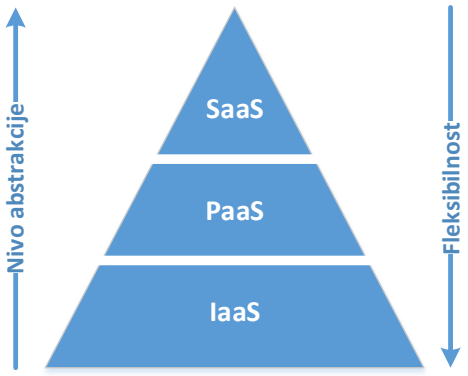
Postavitev oblaka je namenjena uporabi ene skupnosti, ki je sestavljena iz več organizacij. Organizacije v skupnosti si delijo določene skupne interese, kar prispeva do večjega zaupanja med posameznimi organizacijami v skupnosti. Slednje ja tudi glavna prednost pred javnim oblakom. Infrastruktura oblaka je lahko upravljana in v lasti ene ali več organizacij v skupnosti ali v lasti zunanjega ponudnika.

3.2.4 Hibridni oblak

Hibridni postavitveni model predstavlja rešitev, ki je sestavljena iz dveh ali več različnih oblakov (privatni, skupnostni ali javni), ki ohranjajo unikatne entitete. Najbolj razširjena oblika hibridnega oblaka sestoji iz enega privatnega in enega javnega oblaka. Postaja vse bolj priljubljena rešitev, ki odpira možnosti za zmanjševanje stroškov privatnega oblaka ter eliminira potrebni model zaupanja med uporabnikom in ponudnikom oblaka. Slednje je možno, ker so kritični podatki znotraj privatnega oblaka in nekritični podatki v javnem oblaku, kar organizaciji omogoča večjo fleksibilnost. Druga prednost hibridne rešitve je možnost razširitve oblaka (ang. Cloud-bursting) [6]. V določenih obdobjih, ko se povečajo potrebe po dodatnih kapacitetah, ki jih zasebni podatkovni center ne more zagotoviti za nemoteno izvajanje storitve, se del nekritičnih delovnih obremenitev prenese v javni oblak. S tem se odpravi potreba po nakupu dodatnih kapacitet. Glavna pomanjkljivost hibridnih oblakov je interoperabilnost in prenosljivost delovnih obremenitev med posameznimi oblaki. Zagotavljanje brezhibne prenosljivosti delovnih obremenitev je kompleksen proces, za kar potrebujemo rešitve, ki to problematiko naslavljajo in rešujejo.

3.3 Storitveni modeli oblaka

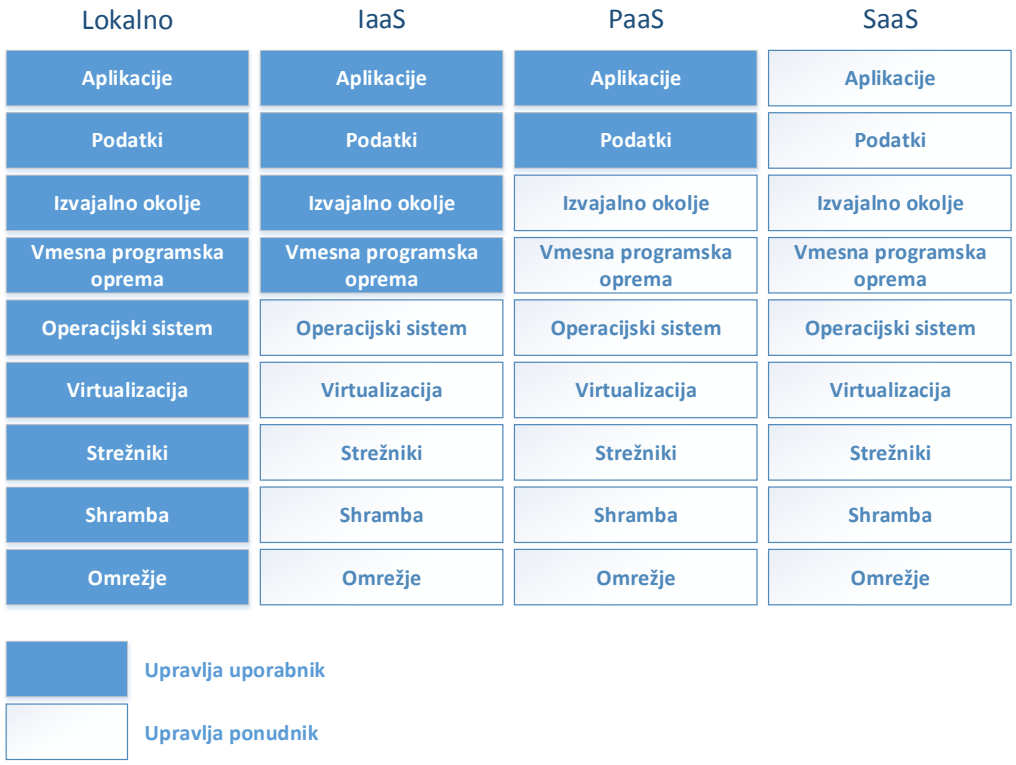
Ključni koncept računalništva v oblaku je izpostaviti in definirati posamezne zmožnosti in funkcionalnosti kot storitve, ki so merjene, spremljane in ustrezno zaračunane. Storitveni modeli računalništva v oblaku skušajo klasificirati določeno storitev - XaaS (ang. Anything as a service), kjer X predstavlja poljubno storitev (na primer programsko opremo, shrambo, infrastrukturo). Storitveni model oblaka predstavlja več-slojna abstrakcija osnovnih razredov storitev, ki jih zagotavlja model računalništva v oblaku. Definira tudi ustrezno povezavo med posameznimi nivoji abstrakcije. NIST [5] definira tri osnovne storitvene modele oblaka in sicer infrastrukturo kot storitev - IaaS (ang. Infrastructure as a Service), platformo kot storitev - PaaS (ang. Platform as a Service) ter programsko opremo kot storitev - SaaS (ang. Software as a Service).



Slika 3.2: Hierarhija storitvenih modelov.

Slika 3.2 ponazarja hierarhijo osnovnih storitvenih modelov. Kot lahko opazimo na slike se posamezni nivoji gradijo eden na drugemu. Slednji pristop omogoča ponudnikom, da se osredotočijo na ključne storitve, ki jih ponujajo, ne da bi skrbeli za spodnji nivo. Ob tem pa se ponovno uporabijo storitve iz spodnjih nivojev preko standardnih mehanizmov in protokolov.

Ločitev nivojev je izvedena glede na nivo abstrakcije, ki jo posamezni nivo ponuja. Slika 3.3 podaja ilustrativno primerjavo med posameznimi nivoji.



Slika 3.3: Storitveni modeli oblaka [8].

3.3.1 Infrastruktura kot storitev

Predstavlja osnovni storitveni model, na katerem temeljijo vsi ostali [6]. Končnim uporabnikom ponuja oskrbo z računalniškimi viri kot so računanje, shramba, omrežna povezava ter podobno. Pri tem abstrahira spodnje nivoje in podrobnosti fizične infrastrukture, kar uporabnikom odpravi potrebo po upravljanju in vzdrževanju fizične infrastrukture. V večini primerov so infrastrukturne storitve zagotovljene v obliki virtualnih strojev, virtualnih omrežij ter virtualne shrambe. Obstajajo sicer ponudniki, ki ponujajo fizične infrastrukturne storitve, vendar jih je veliko manj kot v virtualizirani obliki. Na

dodeljenih infrastrukturnih virih lahko uporabnik izvaja poljubno programsko opremo kot so podprti operacijski sistemi, razvojna okolja, aplikacije itd.

Infrastrukturni storitveni nivo ponuja največ fleksibilnosti v primerjavi z ostalimi. Večina rešitev, ki omogočajo postavitev privatnih oblakov zagotavlja le infrastrukturo kot storitev - IaaS. Za implementacijo ostalih nivojev je potreben dodaten razvoj in razširjava rešitve. Kot primer privatnih IaaS rešitev lahko naštejemo VMware vCloud, Microsoft Private Cloud, OpenStack itd. Kot javne oblake, ki ponujajo IaaS storitve lahko naštejemo Amazon EC2 (Amazon Elastic Compute Cloud), Microsoft Windows Azure, Google Compute Engine itd.

V nadaljevanju se bomo osredotočili na ta storitveni model, ki predstavlja temelj preostalih storitvenih modelov računalništva v oblaku.

3.3.2 Platforma kot storitev

Predstavlja abstrakcijski nivo, ki gradi na infrastrukturnem nivoju [6]. Zagotavlja izvajalno okolje za izvajanje aplikacij, ki jih ponudniki programske opreme (storitve SaaS) zagotavljajo končnim uporabnikom. Razvijalcem omogoča razvoj aplikacij v različnih podprtih programskih jezikih. Podpora je odvisna od ponudnika platformskih storitev. Ker abstrakcija skrije podrobnosti o spodaj ležeči infrastrukturi na kateri se izvajajo in razvijajo aplikacije se lahko razvijalci osredotočijo na implementacijo kritičnih funkcionalnosti, ne da bi se ukvarjali z upravljanjem operacijskega sistema, omrežja, shrambe ali z namestitvijo in konfiguracijo izvajalnega okolja in podobno. Poleg izvajalnega okolja številni ponudniki ponujajo tudi različna orodja ter dodatne programske module, ki jih je mogoče ponovno uporabiti z namenom poenostavljanja razvoja storitev.

Primer najbolj uveljavljenih javnih ponudnikov platformskih storitev so Amazon AWS, Microsoft Windows Azure, Google App Engine, RedHat OpenShift, IBM SmartCloud Application Services, Oracle Public Cloud. Na področju privatnih oblakov, kot smo že omenili, večina rešitev zagotavlja le

storitve IaaS. Nekatere rešitve ponujajo dodatne komponente, ki delno pokrijejo platformske storitve, vendar se ne morejo primerjati z javnimi.

3.3.3 Programska oprema kot storitev

Programska oprema kot storitev ali tudi programska storitev na zahtevo predstavlja najvišji nivo abstrakcije v hierarhiji storitvenih modelov računalništva v oblaku [6]. Storitev SaaS predstavlja programska oprema - aplikacija, ki se izvaja na infrastrukturi oblaka in omogoča ter zagotavlja bistvene značilnosti definirane v poglavju 3.1 in omogoča dostop končnim uporabnikom. Uporabniki teh storitev imajo omejen nadzor nad uporabo aplikacije in omejeno interakcijo z aplikacijo glede na njihovo vlogo. Storitve SaaS so v večini primerov dostopne preko spleta z uporabo spletnega brskalnika. Večina storitev SaaS izpostavlja tudi programske vmesnike za programski dostop do funkcionalnosti storitve.

V ta storitveni model lahko uvrstimo različne CRM (ang. Customer relationship management) aplikacije, ERP (ang. Enterprise resource planning) sisteme, HRM (ang. Human resource management) aplikacije, itd. Poleg teh lahko uvrstimo še nekatere splošno namenske aplikacije kot so Google Apps, Windows Live, itd.

3.3.4 Drugi storitveni modeli - XaaS

Na začetku poglavja smo opisali storitvene modele, ki jih definira NIST. Ti storitveni modeli so osnovni, vendar so se skozi čas uveljavili tudi nekateri drugi, ki lahko vsebujejo in ponovno uporabljajo osnovne storitvene modele. Ključni pomen izraza XaaS je v izpostavitvi ter zagotavljanju informacijskih ter komunikacijskih tehnologij in funkcionalnosti kot storitev, ki bodo merjene ter ustrezno zaračunane po dejanski porabi. Drugi storitveni modeli, ki so se uveljavili poleg osnovnih so naslednji:

- **Komunikacija kot storitev (ang. Communication as a Service**

- CaaS): Zagotavlja komunikacijske rešitve kot so VoIP (Voice over IP), video konference, IM (Instant Messaging) in podobno. Na voljo so na zahtevo uporabnika in se zaračunavajo po porabi. Vsa strojna in programska oprema za zagotavljanje teh storitev je v lasti ponudnika.

- **Spremljanje kot storitev (ang. Monitoring as a Service - MaaS):** Predstavljajo orodja, ki omogočajo spremljanje aplikacij ne glede na njihovo lokacijo in centralizirani pogled vseh spremljanih aplikacij. Orodja se ponujajo kot storitev zagotovljena s strani ponudnika teh orodij.

- **Poslovni proces kot storitev (ang. Business Process as a Service - BPaaS):** Predstavlja še višji nivo abstrakcije kot SaaS. Koncept BPaaS predstavlja izvajanje in zagotavljanje poslovnih procesov skozi mehanizme računalniškega oblaka.

- **Shramba kot storitev (ang. Storage as a Service - STaaS):** Predstavlja zagotavljanje kapacitete podatkovne shrambe, ki jo najemniki zahtevajo. Podatki so shranjeni na infrastrukturi ponudnika. Storitev se tipično zaračunava glede na porabljeno kapaciteto, v določenih primerih pa se storitev zaračuna glede na prenos podatkov.

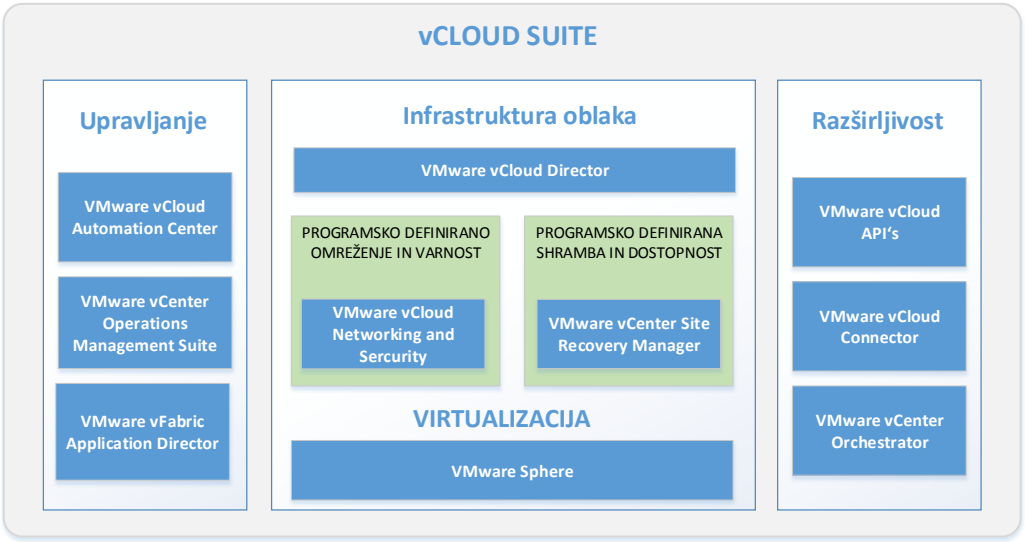
- **Namizje kot storitev (ang. Desktop as a Service - DaaS):** Predstavlja zagotavljanje virtualiziranih računalniških namizij (virtualni stroji z nameščenim operacijskim sistemom) s strani ponudnika. Ponudniki DaaS storitev imajo vzpostavljen VDI (Virtual Desktop Infrastructure) infrastrukturo v njihovih podatkovnih centrih.

Poglavje 4

Komponente rešitve VMware vCloud

V poglavju 3 smo obravnavali osnovne koncepte računalništva v oblaku, kjer smo opisali posamezne tipe oblakov ter storitvene modele, ki jih definira NIST. Poleg tega smo pregledali tudi bistvene značilnosti računalništva v oblaku, ki jih mora omogočati in zagotavljati določena rešitev, ki implementira model računalništva v oblaku. Trenutno na področju računalništva v oblaku obstaja veliko rešitev, ki omogočajo postavitev privatnih oblakov in zagotavljajo storitve IaaS. Kot ena izmed daleč najbolj razširjenih in uveljavljenih rešitev za postavitev in upravljanje privatnih oblakov je VMware vCloud, na katero se bomo osredotočili v nadaljevanju. Poleg možnosti zasebne postavitve, omogoča vCloud tudi javno postavitev. Določeni javni ponudniki IaaS temeljijo na rešitvi vCloud, vendar njihovo velikost ne moremo primerjati s ponudnikom javnih oblakov kot so Amazon ali Google, ki imajo implementirane lastne rešitve. Poleg zasebnih in javnih postavitev rešitev vCloud ponuja tudi možnost hibridne postavitve oblaka, ki jo bomo ravno tako naslovili v diplomski nalogi.

VMware vCloud je celovita rešitev za implementacijo modela računalništva v oblaku in je sestavljena iz več komponent. V nadaljevanju poglavja bomo obravnavali posamezne komponente rešitve, analizirali njihovo vlogo v sami



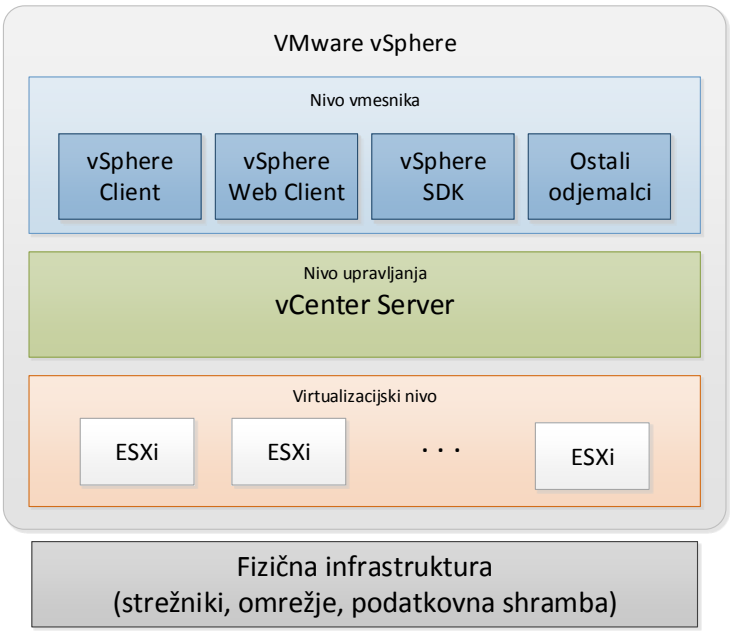
Slika 4.1: Nabor komponent rešitve VMware vCloud [24].

rešitvi ter njihov prispevek k implementaciji modela računalništva v oblaku in zagotavljanje bistvenih značilnosti oblaka.

Komponente rešitve, prikazane na sliki 4.1, lahko razdelimo v dve skupini. V prvo skupino spadajo osnovne komponente, ki so ključne pri vzpostavitvi privatnega oblaka. V drugo skupino pa spadajo komponente, ki omogočajo dodatne funkcionalnosti. Potreba po dodatnih funkcionalnosti je seveda odvisna od namena postavitve oblaka, tipa oblaka ter tipa storitev, ki bi jih ponudnik zagotavljal. Pri izbiri komponent je ključnega pomena tudi velikost okolja h kateremu cilja poslovna organizacija ali ponudnik, ki vzpostavlja privatni oblak. Izbira komponent vpliva tudi na stroškovno učinkovitost oblaka, saj obstaja več licenčnih modelov. Osnovne komponente so uvrščene v standardni licenčni model. Z vidika poslovne organizacije, ki vzpostavlja privatni oblak, je najbolj smiselno, da sprva zagotovijo osnovne komponente, nato pa ostale komponente dodajajo po potrebi, saj sprememba licenčnega modela v obratni smeri ni možna. V nadaljevanju se bomo osredotočili na osnovne komponente, ki zagotavljajo ključne funkcionalnosti oblaka.

4.1 Ključne komponente privatnega oblaka

Poglavje podaja bolj podroben tehnični opis ter analizo funkcionalnosti, ki jih zagotavljajo osnovne komponente rešitve vCloud. Poglavje predstavlja izhodišče pri vzpostavitvi arhitekture privatnega oblaka, ki sledi v poglavju 5.



Slika 4.2: Virtualizacijska platforma vSphere [9].

4.1.1 vSphere

Kot smo že omenili, je infrastruktura oblaka, kjer se izvajajo delovne obremenitve oblaka, lahko tako fizična kot tudi virtualizirana, pri čemer večina rešitev temelji na virtualizirani infrastrukturi. Le-to v primeru rešitve vCloud zagotavlja virtualizacijska platforma vSphere [9]. Virtualizacijska platforma abstrahira fizično infrastrukturo in zagotavlja virtualizacijo računalniških virov, ki jih ponujajo fizični strežniki. To je virtualizacija računskih virov (CPU, pomnilnik), omrežja ter shrambe. Platformo vSphere lahko razdelimo na tri nivoje in sicer virtualizacijski nivo, nivo upravljanja in nivo vmesnika.

Hierarhija posameznih nivojev platforme je prikazana na sliki 4.2.

Slika 4.3: Virtualizacijski nivo platforme [9].

4.1.1.1 Virtualizacijski nivo

Virtualizacijski nivo platforme skrbi za abstrakcijo fizične infrastrukture in zagotavlja potrebne virtualizirane računalniške vire za izvajanje delovnih obremenitev v oblaku. Jedro nivoja je hipervizor ESXi, ki je nameščen neposredno na fizičnih strežnikih. Kot smo že omenili v poglavju 2, spada hipervizor ESXi v prvo skupino hipervizorjev, kar pomeni, da ima neposredni dostop do strojne opreme. Poleg zagotavljanja samih virov, virtualizacijski nivo zagotavlja tudi določene funkcionalnosti - storitve, in sicer s pomočjo ustreznih tehnologij. Storitve, ki jih zagotavlja virtualizacijski nivo platforme lahko razdelimo v dve skupini. V prvo skupino spadajo infrastrukturne storitve, v drugo pa aplikacijske storitve. Aplikacijske storitve ponujajo funkcionalnosti, ki zagotavljajo razpoložljivost okolja, varnost virtualiziranega okolja ter skalabilnost infrastrukture. Bolj ilustrativen pregled virtualizacijskega nivoja podaja slika 4.3.

Glede na segment infrastrukture, za katerega zagotavljajo določene funkcionalnosti obstajajo naslednje infrastrukturne storitve:

- **Računske storitve (ang. Compute Services):** Funkcionalnosti, ki zagotavljajo abstrakcijo virov fizičnih strežnikov. Skrbijo tudi za agregacijo teh virov.

- **Omrežne storitve (ang. Network Services):** Storitve v tej skupini zagotavljajo funkcionalnosti in tehnologije, ki podpirajo upravljanje omrežja in zagotavljajo omrežno povezljivost v virtualiziranem okolju.

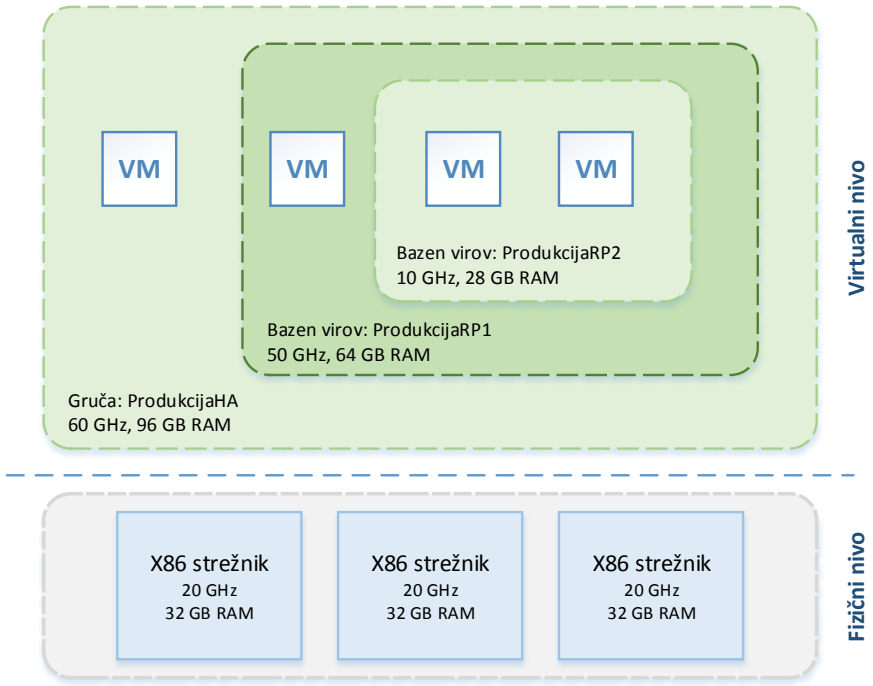
- **Storitve shrambe (ang. Storage Services):** Ponujajo funkcionalnosti in tehnologije, ki omogočajo upravljanje in nadzor shrambe v virtualiziranem okolju.

Aplikacijske storitve zagotavljajo visoko nivojske funkcionalnosti, ki dopolnjujejo infrastrukturni nivo. Lahko jih razdelimo na:

- **Razpoložljivost (ang. Availability):** Izboljšanje razpoložljivosti okolja v oblaku igra ključno vlogo. Nabor storitev v tej skupini ponujajo funkcionalnosti in tehnologije, ki zagotavljajo izvajanje delovnih obremenitev v visoko razpoložljivem načinu.

- **Varnost (ang. Security):** Z vidika varnosti virtualiziranega okolja so na voljo mehanizmi, ki zagotavljajo varnost hipervizorja pred omrežnimi napadi ter varnost posameznih virtualnih strojev.

- **Skalabilnost (ang. Scalability):** Funkcionalnosti za zagotavljanje skalabilnosti infrastrukture in delovnih obremenitev, ki se izvajajo v oblaku. Za skalabilnost računskih virov virtualnih strojev je zagotovljena funkcionalnost za dodajanje CPU virov med izvajanjem virtualnega stroja ter funkcionalnost za dodajanje pomnilnika med izvajanjem virtualnega stroja.



Slika 4.4: Agregacija virtualizacijskih virov.

Virtualizacijske vire, ki jih zagotavlja virtualizacijski nivo platforme za izvajanje delovnih obremenitev v oblaku lahko razdelimo v tri osnovne segmente virov. V prvi segment spadajo računski viri (ang. Compute Resources), kot so CPU in pomnilnik, ki se jih dodeli virtualnim strojem. V drugi segment spadajo omrežni viri (ang. Network Resources), ki se dodelijo virtualnim strojem za omogočanje omrežne povezave tako med seboj kot tudi z zunanjim omrežjem. Tretji segment virtualizacijskih virov vsebuje shrambo (ang. Storage Resources), kjer so shranjeni posamezni virtualni stroji ter podatke, ki jih obdelujejo. Z omenjeno segmentacijo lahko vire razdelimo v skupine neglede na konkretno rešitev, ki zagotavlja ustrezne fizične ali virtualizirane vire. Vendar vsaka rešitev uporablja lastne gradnike, ki zagotovijo potrebne vire.

Računski viri infrastrukture

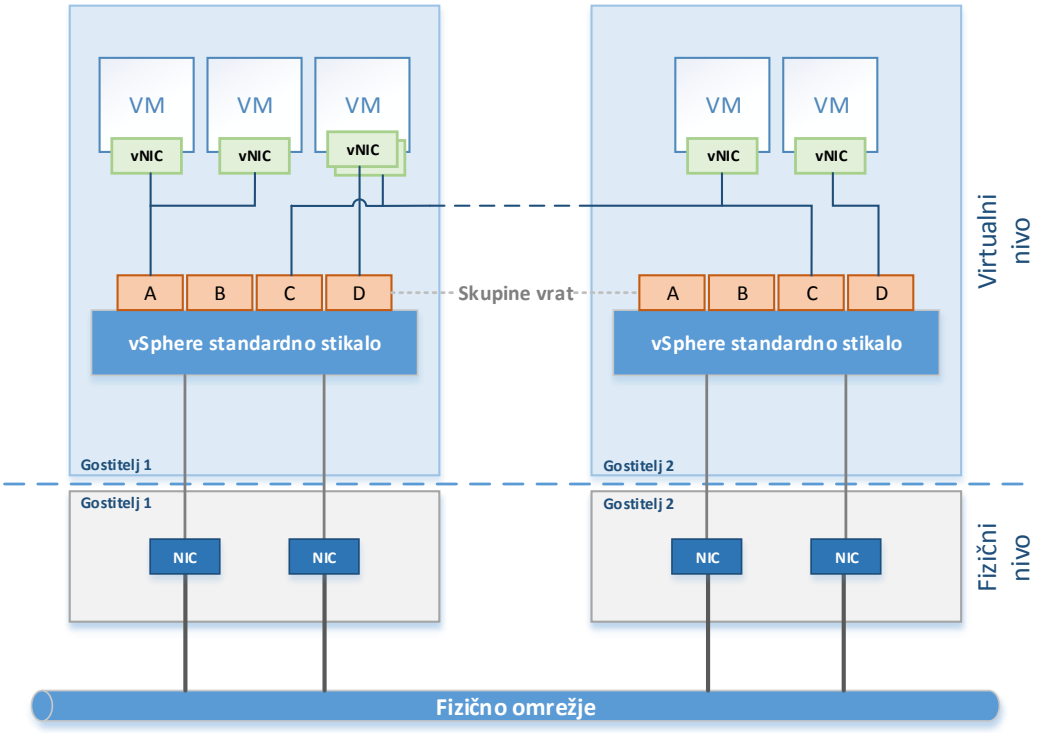
Gradniki virtualizacijske platforme, ki zagotavljajo računske vire za izvajanje delovnih obremenitev na infrastrukturi oblaka so gostitelji virtualizacije, gruče (ang. Clusters) in bazeni virov (ang. Resource Pools). Najbolj osnovni gradnik so gostitelji, ki abstrahirajo in agregirajo vire fizičnega strežnika. Če ima strežnik dva procesorja s frekvenco 3 GHz in vsak procesor po deset jeder, se prikažejo kot en vir s 60 GHz. Na višjem nivoju so gruče virtualizacijske platforme. Omogočajo agregacijo virov, ki jih ponujajo posamezni gostitelji znotraj gruče. Bazeni virov omogočajo segmentacijo virov znotraj gruče, z namenom bolj učinkovite izrabe virov. Slika 4.4 prikazuje primer ene gruče iz treh gostiteljev. Znotraj gruče lahko razberemo da sta v gruči ugnezdena še dva bazena virov. Posameznemu bazenu virov je mogoče nastaviti kapaciteto dodeljenih virov, ki se lahko porabijo, rezervacije virov ter omejitve. Slednji mehanizmi igrajo ključno vlogo pri upravljanju z viri v oblaku, saj kot bomo videli komponenta vCloud Director neposredno uporablja te mehanizme za dodeljevanje in omejevanje porabe virov delovnim obremenitvam oblaka. V poglavju 3.1, kjer smo obravnavali bistvene značilnosti enega oblaka, smo spoznali, da je ena izmed teh značilnosti agregacija virov, kar pomeni, da so gruče in bazeni virov tisti gradniki, ki omogočajo to značilnost. Ker gruče dodajo še en nivo abstrakcije virov, skalabilnost infrastrukture postane enostavno izvedljiva. Če se pojavijo potrebe po dodatnih kapacitetah, se v gručo lahko dodajo novi gostitelji, kar dinamično poveča celotno kapaciteto, ki je na voljo delovnim obremenitvam.

Omrežni viri infrastrukture

Omrežni viri zagotavljajo omrežno povezljivost tako virtualnim strojem kot tudi nekaterim storitvam virtualizacijske platforme. Omrežna povezljivost je zagotovljena s strani virtualiziranega omrežnega stikala. Virtualizirano stikalo je lahko realizirano na dva načina. Prvi tip stakala je standardni - lokalni (ang. vNetwork Standard Switch), drugi tip pa je porazdeljeni (ang. vNetwork Distributed Switch). Povezava virtualnih strojev na virtualizi-

rano stikalo je izvedena preko enega ali več virtualnih omrežnih vmesnikov (ang. Virtual Network Interface Card - vNIC). Na strani virtualnega stikala, virtualni stroji so povezani v standardne ter porazdeljene skupine vrat v odvisnosti od tipa virtualiziranega stikala na katerega se povezujejo. Ne glede na tip, skupino vrat predstavljajo logična omrežja v katerih se virtualni stroji znotraj gostitelja povezujejo med seboj. Dostop do zunanjega - fizičnega omrežja poteka preko fizičnih omrežnih vmesnikov gostitelja. Za vsako skupino vrat se lahko posebej nastavijo parametri, ne glede na ostale skupine vrat. S pomočjo skupine vrat lahko dosežemo izolacijo omrežja. Tako virtualni stroji v eni skupini ne vidijo virtualnih strojev v drugi. Za vsako skupino vrat namreč lahko nastavimo VLAN identifikator, ki pripada temu omrežju. Pri tem morajo biti VLAN identifikatorji nastavljeni tudi na fizičnih stikalih, ki povezujejo gostitelje med seboj. Kot smo opisali v poglavju 2, VLAN segmentacija fizičnih omrežij zagotavlja izolacijo na drugem nivoju OSI modela. S tem se zagotovi izolacija omrežij v več-najemniškem modelu, saj si eno fizično omrežje deli več uporabnikov/najemnikov oblaka.

Slika 4.5 prikazuje arhitekturo omrežja virtualizacijske platforme, ki je realizirana s pomočjo standardnega virtualiziranega stikala. Implementacija standardnega stikala se izvaja in velja v okviru enega gostitelja. Skupine vrat na standardnem stikalu veljajo le za virtualne stroje, ki se izvajajo na tem gostitelju. Če želimo nek virtualni stroj prenesti na drugega gostitelja, moramo zagotoviti, da imamo na drugem gostitelju identično skupino vrat, v smislu poimenovanja ter vseh nastavitev. V večjem okolju je slednje zelo težko doseči, kajti če imamo veliko število gostiteljev, moramo za vsakega gostitelja posebej kreirati in nastavljati vse potrebne skupine vrat. Alternativa zgornjemu pristopu je uporaba porazdeljenega stikala. Arhitektura omrežja virtualizacijske platforme realiziranega z uporabo porazdeljenega stikala je prikazana na sliki 4.6. V primerjavi s standardnim stikalom, katera konfiguracija velja lokalno v okviru enega gostitelja, je pri porazdeljenem stikalu konfiguracija stikala porazdeljena med vse gostitelje, ki uporabljajo to stikalo. Skupine vrat so porazdeljene med gostitelji, kar pomeni, da jih je potrebno

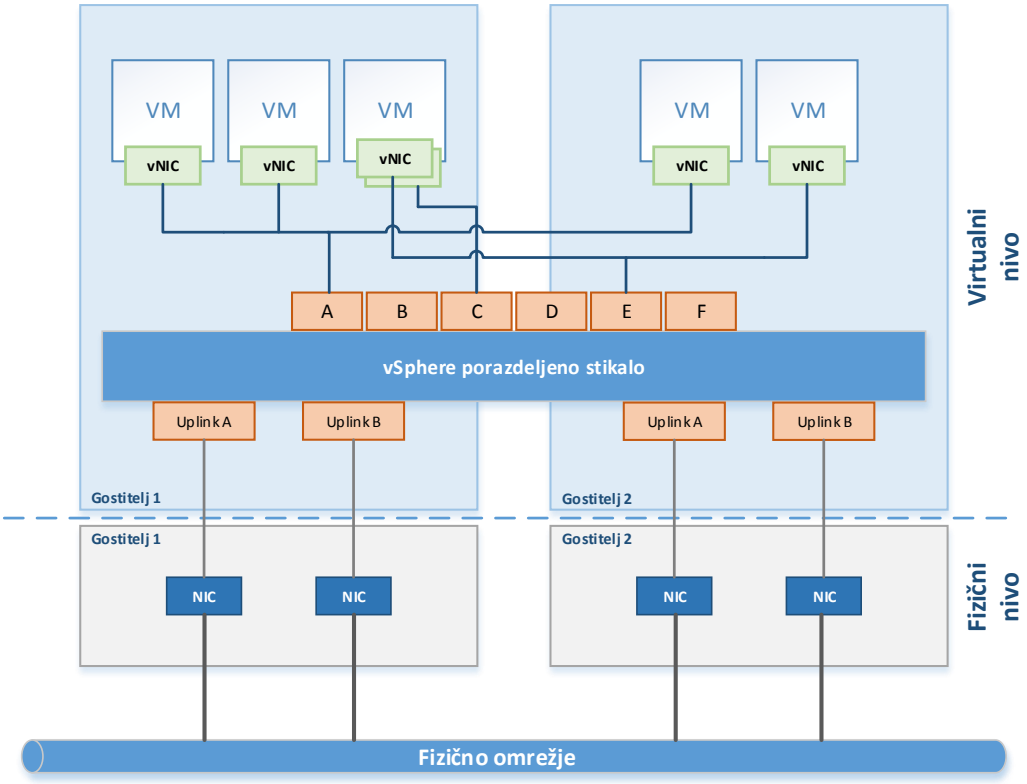


Slika 4.5: Standardno stikalo platforme vSphere [9].

kreirati le enkrat. Ker so porazdeljene, so vse nastavitve konsistentne med vsemi gostitelji. Upravljanje stikala je centralizirano, kar zmanjša tveganje za napačne konfiguracije.

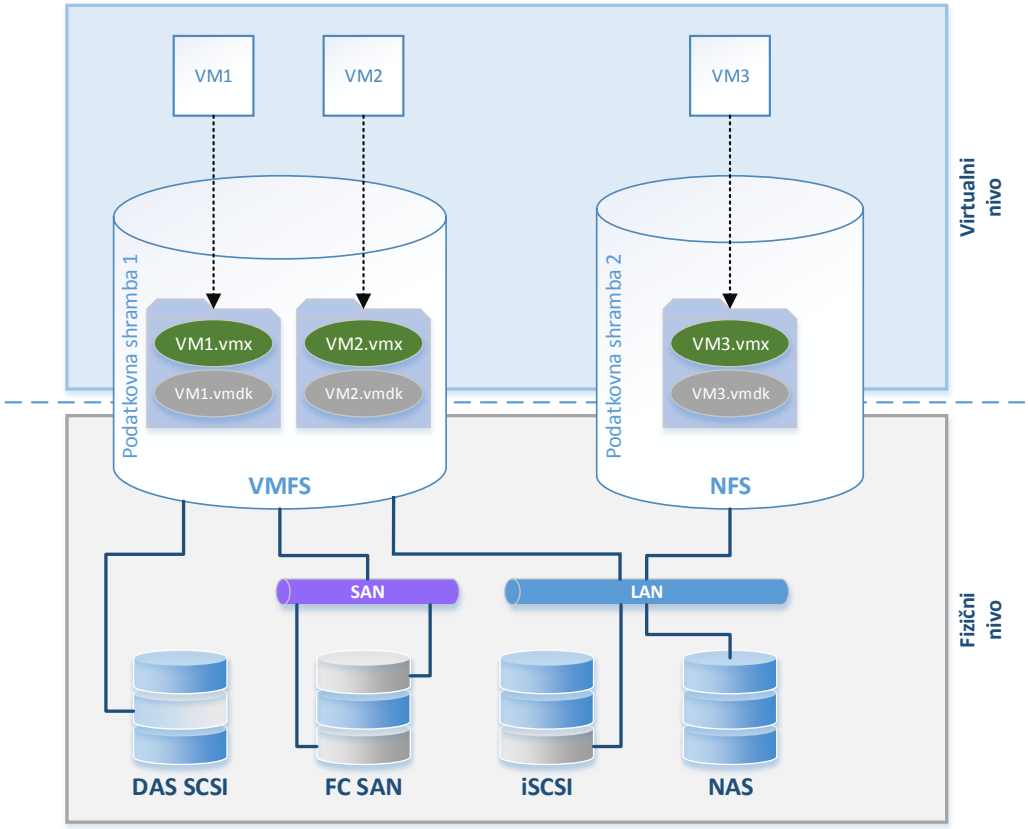
Viri shrambe infrastrukture

Shramba za potrebe virtualnih strojev na virtualizacijski platformi je realizirana v obliki podatkovnih shramb (ang. Datastores), ki abstrahirajo fizično shrambo. Sama shramba je znotraj podatkovnih shramb podprta s strani fizične shrambe v logičnih enotah (ang. Logical Unit Number - LUN). Logične enote lahko segajo na enega fizičnega diska ali na neko polje diskovnih enot, ki je sestavljeno iz več fizičnih diskov. Podatkovna shramba lahko vsebuje eno ali več logičnih enot. Datotečni sistem, ki se uporablja na logičnih enotah je VMFS - Virtual Machine File System. Shrambo virtualni stroji do-



Slika 4.6: Porazdeljeno stikalo platforme vSphere [9].

bijo v obliki enega ali več virtualnih diskov. Kot smo predstavili v poglavju 2, so virtualni diski shranjeni v obliki datotek, kar omogoča enostaven prenos virtualnega stroja. Fizično shrambo, ki zagotavlja kapaciteto za shrambe, lahko razdelimo na lokalno in oddaljeno. Lokalno shrambo predstavljajo fizični diski ali polje diskovnih enot, ki jih ima strežnik neposredno-direktno priklopljene (ang. Direct Attached Storage - DAS). Lokalna shramba se v večini primerov uporablja izključno za potrebe hipervizorja, kajti kapacitete lokalnih diskov v strežnikih, ki so namenjeni izvajanju delovnih obremenitev, so bistveno manjše. Vendar, kot bomo predstavili pri vzpostavitvi arhitekture, obstajajo načini, ki zagotavljajo večjo zanesljivost shrambe namenjene hipervizorju. Druga oblika shrambe, ki zagotavlja kapaciteto podatkovnih shramb je oddaljena shramba. Slednja je v večini primerov realizirana kot



Slika 4.7: Arhitektura shrambe virtualizacijske platforme [9].

SAN sistem, ki zagotavlja potrebne kapacitete. Podprte oblike oddaljene shrambe so NAS (ang. Network Attached Storage), iSCSI ter FC SAN. Vsi tipi shrambe so prikazani na sliki 4.7, kjer je prikazana arhitektura virtualizirane shrambe, ki jo zagotavlja virtualizacijska platforma. Kot lahko opazimo na sliki, se v primeru NAS shrambe uporablja omrežni datotečni sistem (ang. Network File System - NFS). V ostalih primerih se uporablja datotečni sistem VMFS. Povezava med gostiteljem in oddaljeno shrambo je izvedena v obliki SAN omrežja preko optične povezave ali preko ustreznega LAN omrežja. Dostop do NAS in iSCSI shrambe poteka preko LAN omrežja, dostop do FC SAN shrambe pa poteka preko SAN omrežja. Ker je oddaljena shramba dostopna preko omrežja, se lahko deli med več gostiteljev, kar pa predstavlja

predpogoj za izvajanje določenih funkcionalnosti, ki jih virtualizacijski nivo ponuja.

Porazdeljene storitve virtualizacijske platforme

Na začetku obravnave virtualizacijskega nivoja, smo nivo razdelili na infrastrukturne ter aplikacijske storitve, ki zagotavljajo določene funkcionalnosti. Del teh funkcionalnosti se nanaša in izvaja v okviru enega gostitelja. Še bolj pomembne funkcionalnosti predstavljajo tiste, ki se izvajajo med dvema ali več gostitelji. Storitve, ki zagotavljajo takšne funkcionalnosti lahko obravnavamo kot porazdeljene. Koncepti vseh teh rešitev veljajo splošno, ne glede na rešitve, saj večina rešitev delno ali popolnoma implementirajo podobne funkcionalnosti.

- **vSphere vMotion:** Ena izmed najbolj pomembnih funkcionalnosti in tudi predpogoj nekaterih ostalih. Zagotavlja migracijo-prenos delovnih obremenitev oblaka med izvajanjem. Migracija virtualnega stroja poteka med gostiteljem na katerem se izvaja ter ciljnim gostiteljem. Migracija delovnih obremenitev v okolju oblaka igra ključno vlogo, saj lahko tako dosežemo večjo razpoložljivost storitev v primeru napovedanih vzdrževalnih akcij na infrastrukturi. Namesto izklopa vseh virtualnih strojev, ki se izvajajo na gostitelju katerega vzdržujemo, jih lahko migriramo na drugega gostitelja in s tem zagotovimo dosegljivost storitev kljub vzdrževalnim akcijam.

- **vSphere Storage vMotion:** Temelji na podobnem konceptu kot vMotion. Razlika je ta, da se v tem primeru migrirajo diski ter konfiguracijske datoteke virtualnih strojev. Migracija poteka med podatkovno shrambo na katerem je shranjen virtualni stroj ter neko drugo ciljno podatkovno shrambo. Na ta način lahko dosežemo večjo razpoložljivost storitev v primeru napovedanih vzdrževalnih akcij na nivoju shrambe.

- **vSphere Distributed Resource Scheduler (DRS):** Zagotavlja upravljanje z virtualizacijskimi viri ter omogoča dinamično porazdeljevanje

delovnih obremenitev. Deluje na nivoju ene gruče. Druga značilnost je ta da skrbi tudi za čim bolj izenačeno obremenitev gostiteljev znotraj gruče. Dinamična prerazporeditev se izvaja na podlagi aktivnega spremljanja kapacitet na nivoju gruče ter posameznih gostiteljev. V primeru prevelike obremenitve enega izmed gostiteljev, se del virtualnih strojev migrira na manj obremenjene gostitelje znotraj gruče. Kot mehanizem za migracijo se uporablja vMotion. To pomeni da morajo gostitelji biti pripravljeni na uporabo funkcionalnosti vMotion.

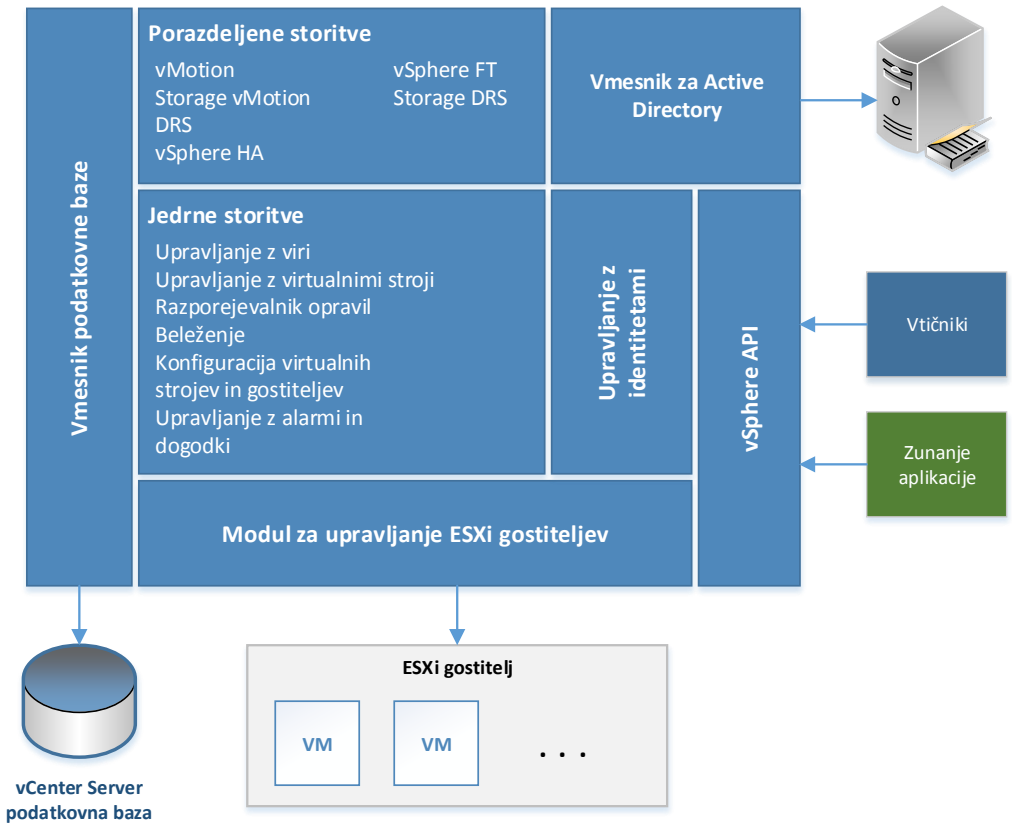
- **vSphere Distributed Power Management (DPM):** Upravljanje porabe energije se v praksi izkaže kot zelo pomemben aspekt v okolju oblaka, saj ne želimo niti neobremenjeno niti preveč obremenjeno infrastrukturo. V primeru neizkoriščenega gostitelja se virtualni stroji, ki se izvajajo na tem gostitelju, prenesejo na ostale gostitelje v gruči, sam pa se izklopi. Če so potrebne dodatne kapacitete, se gostitelj ponovno vklopi, pri čemer se virtualni stroji prenesejo nazaj na gostitelja. Na ta način se lahko doseže bolj učinkovita poraba energije.

- **vSphere Storage DRS:** Uporablja podoben koncept kot DRS. V tem primeru namesto slike pomnilnika virtualnega stroja, dinamično prerazporejajo virtualne diski med podatkovnimi shrambami. Prerazporejanje se izvaja na nivoju gruč podatkovnih shramb (ang. Datastore Cluster). S tem se zagotovi čim bolj enakomerna zasedenost podatkovnih shramb, tako z vidika kapacitet kot tudi z vidika zmogljivosti.

- **vSphere High Availability (HA):** Ekosistem oblaka je zasnovan holistično v smislu izvajanja delovnih obremenitev, saj mora zagotavljati izvajanje tako nekritičnih kot tudi kritičnih delovnih obremenitev. Kritične delovne obremenitve morajo imeti čim manjši ali celo ničelni čas izpada. S pomočjo vMotion lahko dosežemo dosegljivost delovnih obremenitev ob napovedanih dogodkih, vendar v primeru nenapovedanega izpada gostiteljev, vse delovne obremenitve, ki so se izvajale na tem gostitelju postanejo nedosegljive. Rešitev problema v primeru

vSphere zagotavlja funkcionalnost HA, ki omogoča izvajanje virtualnih strojev v visoko razpoložljivem načinu. Slednje pomeni, da v primeru izpada gostitelja zagotovi ponovni zagon virtualnih strojev na enem izmed delujočih gostiteljev v gruči. Poleg spremljanja gostiteljev, lahko HA spremlja tudi izvajanje operacijskega sistema znotraj virtualnega stroja. Če pride do napake v OS virtualnega stroja, se stroj ponovno zažene. Če aplikacije, ki se izvajajo na virtualnem stroju implementirajo funkcionalnosti za pošiljanje signalov za preverjanje stanja (ang. Heartbeat), jih je možno spremljati in ob morebitni napaki v aplikaciji se OS ponovno zažene. Implementacija pošiljanja signalov za preverjanje stanja je možna z uporabno vSphere Guest SDK (ang. Software Development Kit). Pogoj uporabe funkcionalnosti je deljena shramba med gostitelji znotraj gruče. Virtualni stroji, ki jih želimo zaščiti s pomočjo vSphere HA morajo biti shranjeni na deljeni podatkovni shrambi.

- **vSphere Fault Tolerance (FT):** Določene kritične delovne obremenitve zahtevajo izvajanje brez prekinitve delovanja (ang. Zero downtime). vSphere HA zagotavlja izvajanje delovnih obremenitev v visoko razpoložljivem načinu, vendar ne zagotavlja ničelnega časa izpada. Virtualne stroje namreč ponovno zažene, kar pa traja določen čas. Za tiste virtualne stroje, ki zahtevajo delovanje brez prekinitve je na voljo funkcionalnost FT. Virtualni stroj označen kot FT se izvaja podvojeno - primarni virtualni stroj na enem ter sekundarni virtualni stroj na drugem gostitelju. Vse vhodne in izhodne operacije virtualnega stroja, se izvajajo na primarnem, nato pa se preko omrežja sinhronizirajo na sekundarnem. V primeru izpada primarnega virtualnega stroja sekundarni virtualni stroj postane primarni. Podobno kot pri HA je pogoj deljena shramba.



Slika 4.8: Visokonivojska arhitektura komponente vCenter Server [9].

4.1.1.2 Nivo upravljanja

Vse funkcionalnosti in zmožnosti, ki jih ponuja virtualizacijski nivo platforme, brez ustreznih mehanizmov za upravljanje in nadzor izgubijo pravi pomen. Nivo upravljanja virtualizacijske platforme predstavlja komponenta vCenter Server. vCenter Sever kot osrednja komponenta virtualizacijske platforme omogoča centralizirano upravljanje in konfiguracijo celotne virtualizirane infrastrukture oblaka. Funkcionalnosti, ki smo jih obravnavali v okviru virtualizacijskega nivoja se lahko konfigurirajo in upravljajo izključno preko komponente vCenter Server. Kot osrednja komponenta zagotavlja še nekatere dodatne funkcionalnosti kot so oskrba in upravljanje virtualnih strojev, konfiguracija gostiteljev virtualizacije in virtualnih strojev, beleženje in izva-

janje statistik, upravljanje dogodkov in alarmov itd.

Slika 4.8 ponazarja arhitekturo komponente vCenter Server, kjer so prikazani vsi moduli, ki skrbijo za upravljanje določenih funkcionalnosti ter moduli za integracijo z zunanjimi komponentami.

4.1.1.3 Nivo vmesnika

Najvišji nivo virtualizacijske platforme je nivo vmesnika. Kot lahko vidimo na sliki 4.2, je nivo sestavljen iz več podkomponent. Cilj nivoja je omogočiti dostop in upravljanje virtualizacijske platforme tako iz zunanjih kot tudi preostalih VMware vCloud komponent. Za dostop in upravljanje se ponuja odjemalec v obliki namizne aplikacije (vSphere Client) ter odjemalec v obliki spletne konzole (vSphere Web Client) za dostop iz spletnega brskalnika. Ti odjemalci ponujajo osnovni način za dostop do virtualnih strojev, ki se izvajajo na platformi.

Kljub orodjem, ki jih ponuja, je še bolj pomemben aspekt možnost programskega dostopa do funkcionalnosti platforme. Za ta namen izpostavlja vmesnik vSphere API, preko katerega je možen programski dostop do virtualizacijske platforme [10]. Vmesnik je izpostavljen kot SOAP (ang. Simple Object Access Protocol) spletna storitev, ki je v skladu z Web Services Interoperability Organization (WS-I) Basic Profile 1.0. Spletna storitev se izvaja na komponenti vCenter Server. Zaradi tega lahko uporabimo katerikoli programski ali skriptni jezik, ki ponuja mehanizme za generiranje proxy vmesnikov iz podanih WSDL (ang. Web Service Definition Language) datotek. Za lažji dostop ponuja tudi določene SDK-je, kot so SDK za Perl, SDK za .NET in Web Services SDK za dostop iz Jave.

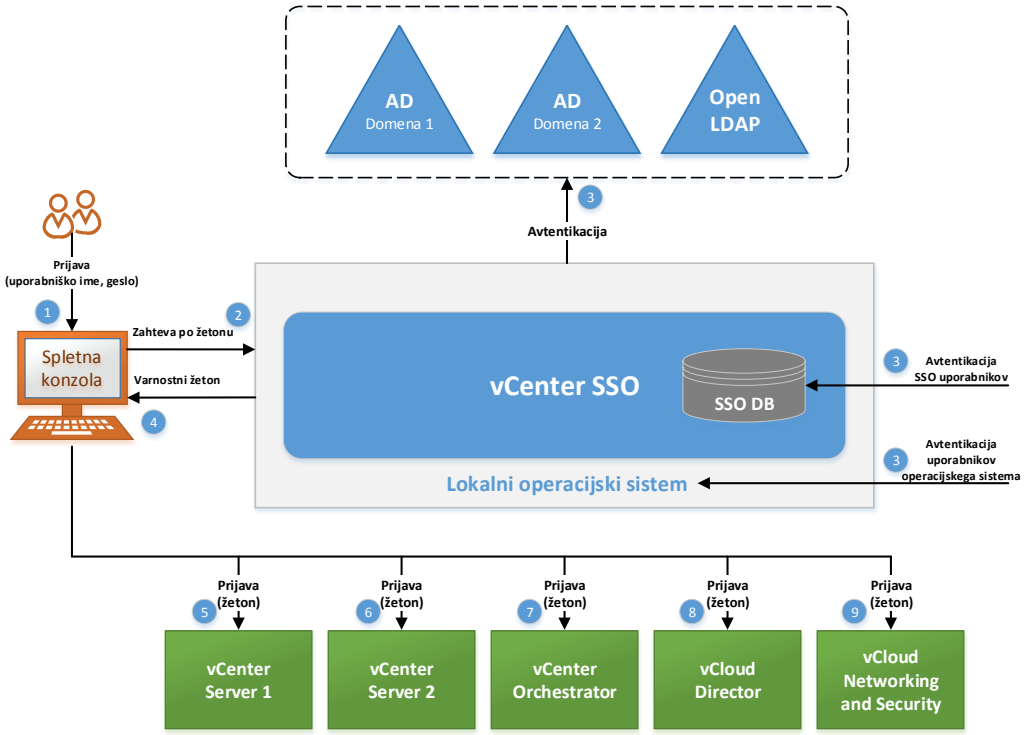
Dostop iz ukazne vrstice je možen s pomočjo orodja vSphere PowerCLI ter vSphere CLI. S tem pristopom lahko dosežemo avtomatizacijo virtualizacijske platforme s pomočjo skript.

4.1.2 vCenter Single Sign-On (SSO)

Upravljanje z identitetami (ang. Identity management) [11] postaja vse bolj pomembna tema, še posebej v ekosistemu oblaka, kjer je potrebno zagotoviti čim bolj varne mehanizme za dostop in upravljanje oblaka in kljub temu ohraniti enostavnost uporabe. Večina komponent različnih rešitev, ki omogočajo postavitev privatnih oblakov, omogoča integracijo z različnimi LDAP (ang. Lightweight Directory Access Protocol) sistemi za avtentikacijo uporabnikov. To so tipično administratorji ali končni uporabniki oblaka. Skoraj vsaka komponenta za upravljanje oblaka ponuja lastno konzolo za dostop do funkcionalnosti komponente. Ker se vsaka komponenta posebej integrira z zunanjimi sistemi za upravljanje z identitetami pomeni, da se morajo uporabniki teh komponent avtenticirati za vsako posamezno komponento. Slednji pristop je lahko razlog za številne težave. Večina akcij, ki jih izvajajo administratorji oblaka na infrastrukturi namreč zahteva sočasno delo z več komponentami. To pomeni da se morajo administratorji večkrat prijavljati v posamezne konzole. Potreba po specifikaciji uporabniških imen in gesel za vsako posamično komponento vpeljuje dodatna varnostna tveganja. Rešitev problema je uporaba enotne prijave (ang. Single Sign-On - SSO), vendar kot bomo v nadaljevanju izpostavili, se lahko pojavijo novi problemi.

Novo dodana komponenta vCenter SSO [12], zagotavlja enotno prijavo čez komponente rešitve vCloud. Komponenta ima vlogo avtentikacijskega posrednika (ang. Authentication Broker), saj omogoča integracijo z zunanjimi LDAP sistemi. Uporabnik enkrat posreduje uporabniške poverilnice preko spletne konzole na komponenti na katero se prijavlja, nato pa se po uspešni avtentikaciji s strani enega izmed podprtih mehanizmov dodeli varnostni žeton, preko katerega se uporabniku zagotovi prijava za preostale komponente.

Kot lahko vidimo na sliki 4.9, v prvem koraku uporabnik specificira uporabniške poverilnice do ciljne spletne konzole. Konzola posreduje specificirane poverilnice z zahtevkom po varnostnem žetonu do komponente SSO.



Slika 4.9: Visokonivojska arhitektura komponente vCenter SSO [12].

V tretjem koraku se uporabnik avtenticira na enega izmed podprtih mehanizmov in sicer Microsoft Active Directory, OpenLDAP ter lokalni SSO uporabnik. Po uspešni avtentikaciji se uporabniku dodeli SAML (ang. Security Assertion Markup Language) 2.0 varnostni žeton, ki se uporabi tudi za prijavo na ostale komponente.

4.1.3 vCloud Networking and Security (vCNS)

V poglavju 4.1.1.1, kjer smo obravnavali in analizirali gradnike, ki zagotavljajo potrebne virtualizacijske vire na nivoju omrežja, smo izpostavili, da je omrežna povezljivost virtualnim strojem zagotovljena s povezavo na standardno ali porazdeljeno virtualizirano stikalo. Poleg izolacije logičnih omrežij (skupine vrat) z uporabo VLAN-ov stikala ne ponujajo nobenih dodatnih varnostnih mehanizmov. Te vrzeli zapolni komponenta vCNS [13].

Ta predstavlja paket podkomponent za zagotavljanje dodatnih varnostnih mehanizmov in ponuja dodatne omrežne storitve kot so požarni zid (ang. Firewall), NAT (ang. Network Address Translation), VPN, DHCP (ang. Dynamic Host Configuration Protocol) itd. Komponenta je sestavljena iz naslednjih podkomponent:

- **App:** Predstavlja požarni zid na nivoju vNIC-ov, ki omogoča omrežno izolacijo znotraj istega VLAN omrežja. Komponenta spremlja in analizira ves vhodni in izhodni promet, ki poteka na ESXi gostitelju in omogoča nadzor nad omrežnimi komunikacijami.

- **Edge:** Zagotavlja varnostne mehanizme in ponuja omrežne storitve na nivoju logičnih omrežij (skupine vrat). Nabor storitev, ki jih ponuja so DHCP, NAT, L2 požarni zid, izenačevanje obremenitve, VPN itd.

- **Data Security:** Omogoča definicijo politik varovanja podatkov na nivoju posameznega hipervizorja ali celotnega podatkovnega centra. Omogoča varovanje podatkov dokumentov/datotek v virtualnih strojih. Omogoča izdajanje poročil, ki identificirajo datoteke z občutljivimi podatke, kot so kreditne kartice ipd.

- **Endpoint:** Komponenta ponuja antivirusno zaščito ter zaščito pred škodljivo programsko opremo. Skrbi za kontinuirano zaščito že postavljenih virtualnih strojev na gostitelju in zaščito na novo pognanih virtualnih strojev. Endpoint deluje kot modul znotraj hipervizorja. Slednje pomeni, da ni potrebno nameščati dodatnih agentov na vsak virtualni stroj, ki ga želimo zaščititi.

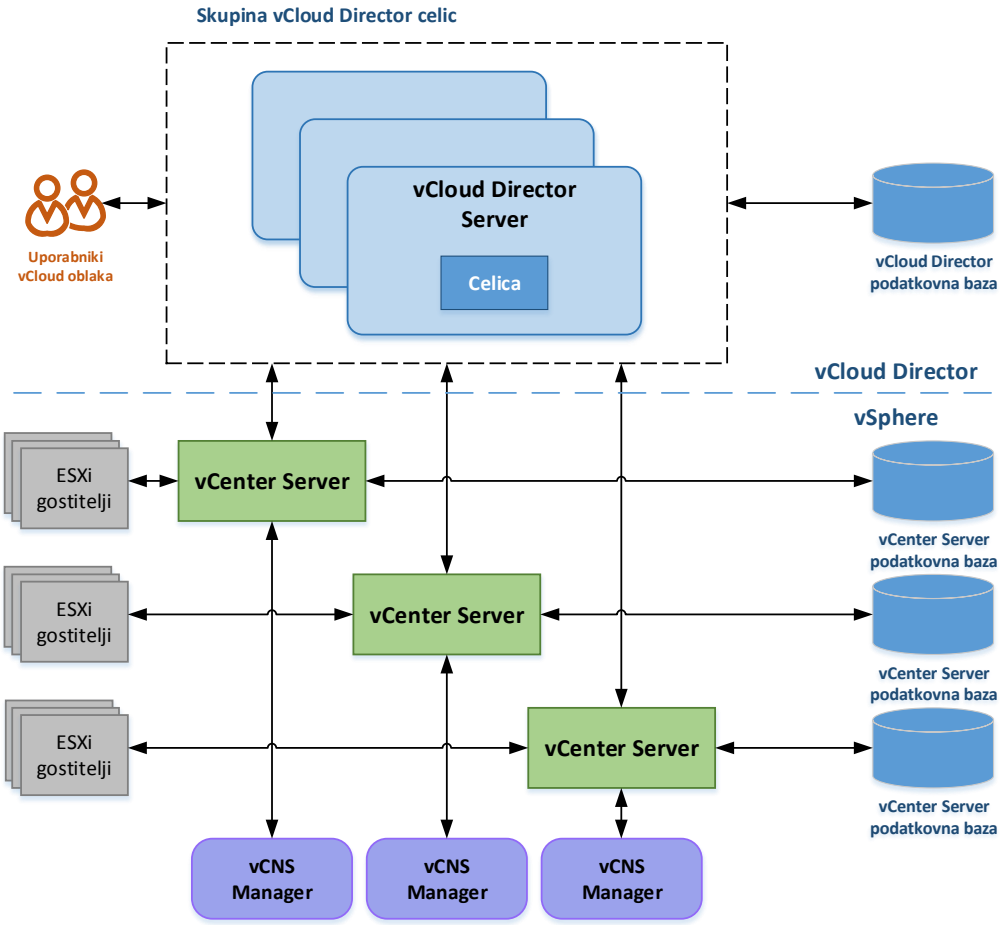
- **vCNS Manager:** Komponenta v paketu vCNS, ki zagotavlja centraliziran pogled in upravljanje nad posameznimi postavitvami ostalih komponent v paketu. Za dostop in konfiguracijo posameznih komponent ponuja spletno konzolo ter izpostavlja REST vmesnik za programski dostop. vCNS Manager se je možno neposredno integrirati s komponento vCenter Server. Integracija med vCenter in vCNS Manager je

vedno ena proti ena, za vsak vCenter strežnik je potreben en vCNS Manager.

4.1.4 vCloud Director

Komponenta vCloud Director [14] predstavlja najbolj pomembno komponento v rešitvi vCloud, saj implementira model računalništva v oblaku. Ne glede na to ali se gre za zasebno ali javno postavitev rešitve vCloud, igra komponenta vCloud Director centralno vlogo in končnim uporabnikom predstavlja vstopno točko v oblak. Kot smo predstavili v poglavju 3.1 je samopostrežba ena izmed bistvenih značilnosti računalništva v oblaku. V primeru rešitve vCloud, je samopostrežba zagotovljena s strani komponente vCloud Director, v obliki samopostrežnega portala. Poleg samopostrežbe smo izpostavili, da je med bistvenimi značilnostmi tudi več-najemniški model. Kot bomo videli v nadaljevanju, vCloud Director s pomočjo vgrajenih gradnikov zagotavlja izoliran več-najemniški model. Druga ključna lastnost komponente je ta, da dodaja nivo abstrakcije nad virtualizacijskimi viri, ki jih zagotavlja virtualizacijska platforma vSphere. Abstrahirane virtualizacijske vire izpostavi kot logične infrastrukturne storitve s pomočjo vgrajenih gradnikov. Kot osrednja komponenta rešitve se integrira z vsemi ostalimi komponentami rešitve. Slika 4.10 prikazuje visokonivojsko arhitekturo komponente ter integracijo z ostalimi komponentami.

Kot lahko vidimo s slike, arhitektura je zasnovana skalabilno. Najbolj enostavna oblika postavitve je v primeru, ko imamo eno vCloud Director celico znotraj skupine. Takšna oblika postavitve ni najbolj primerna za resno produkcijsko okolje, saj ne zagotavlja nobene aktivne redundance. Bolj priporočljiva je postavitev gruče vCloud Director celic, ki je dostopna preko izenačevalnika obremenitve. Bolj podrobno bomo arhitekturo postavitve analizirali pri vzpostavitvi arhitekture privatnega oblaka. Kot je razvidno iz slike, je podatkovna baza komponente skupna za vse celice. Ker je maksimalno število ESXi gostiteljev, ki jih upravlja vCenter omejeno, se lahko vCloud Director integrira z več vCenter strežniki. V takšnem primeru se lahko agre-



Slika 4.10: Visokonivojska arhitektura komponente vCloud Director [14].

girajo virtualizacijski viri, ki jih upravlja posamezen vCenter strežnik. Poleg tega se vCloud Director integrira tudi z komponento vCNS, z namenom upravljanja in nadzora omrežne varnosti ter storitev vCloud oblaka. Povezava do omenjenih komponent je dinamično nastavljiva, kar pomeni možnost dodajanja povezave do novih strežnikov ali spreminjanje obstoječih strežnikov.

4.1.4.1 Ključni gradniki komponente vCloud Director

V tem delu bomo naslovili posamezne gradnike komponente vCloud Director, ki implementirajo ključne funkcionalnosti oblaka in zagotovijo infrastruk-

turne - IaaS storitve končnim uporabnikom/najemnikom oblaka iz obstoječih virtualizacijskih virov.

Organizacije

Organizacije predstavljajo logične enote, ki so izolirane med seboj. Organizacija je tisti gradnik v vCloud Director, ki zagotovi izoliran več-najemniški model. Organizacijo lahko obravnavamo kot enega najemnika virov v oblaku. V primeru, da gre za zasebno postavitev vCloud oblaka, lahko organizacijo obravnavamo kot eno poslovno enoto v okviru poslovne organizacije, ki zagotavlja privatni oblak. Vsaki organizaciji pripada določeno število uporabnikov, ki veljajo v okviru te organizacije. Vsaka organizacija ima določeno kapaciteto virov, ki jih lahko izkorišča za izvajanje delovnih obremenitev. Kreiranje organizacij in alokacijo virov organizacije izvaja sistemski administrator oblaka. Upravljanje in nadzor uporabnikov izvaja organizacijski administrator. Za vsakega uporabnika organizacije je možno določiti ustrezen nivo dostopa glede na vlogo, ki jo ima v poslovni organizaciji ali poslovni enoti poslovne organizacije.

Virtualne namenske aplikacije - vApp

Delovne obremenitve oblaka v okviru rešitve vCloud predstavljajo vApp enote. Vsaka vApp enota predstavlja logični - virtualni vsebnik enega ali več virtualnih strojev ter vsebuje parametre, ki definirajo operacijske podrobnosti. vApp enote se lahko predstavijo kot OVF (Open Virtualization Format) datoteka [15, 16]. Vsaka vApp enota v vCloud Director ima lahko enega ali več omrežij za povezavo virtualnih strojev med seboj. Koncept uporabe vApp enot pomeni, da lahko celotno več-slojno aplikacijo zapakiramo kot enoto, ki vsebuje različne komponente, od izenačevalnika obremenitve, aplikacijskih strežnikov, spletnih strežnikov do podatkovne baze. Tako zapakirana več-slojna aplikacija ima bistveno večjo prenosljivost.

Katalogi

Vsaki organizaciji pripada en ali več katalogov. Slednji predstavljajo centra-

liziran repozitorij vApp predlog in ISO slik. vApp predloga predstavlja že pripravljena vApp enota, ki jo želimo ponovno uporabiti kot končni gradnik ali celotno aplikacijo. Katalogi so v okviru ene organizacije bodisi javni bodisi zasebni. Če je katalog, ki je pripravljen s strani ene organizacije označen kot javni, potem je ta dostopen tudi ostalim organizacijam oblaka.

Ponudnik virtualnih podatkovnih centrov

Ponudnik virtualnih podatkovnih centrov (ang. Provider vDC - virtual Data Center) - PVPC, predstavlja logično reprezentacijo agregiranih računskih ter virov shrambe, ki jih zagotavlja virtualizacijska platforma. PVPC doda sloj abstrakcije k virtualizacijski platformi na nivoju gruče ali bazena virov. PVPC lahko vsebuje enega ali več gruč ali bazenov virov. Predstavlja osnovni mehanizem za alokacijo virov organizacij. Značilno je to, da je en PVPC deljen med večje število organizacij vCloud oblaka. Ker je PVPC le logična reprezentacija spodnjega nivoja - gruča gostiteljev na virtualizacijski platformi, vse delovne obremenitve, ki imajo alocirane vire v tej PVPC, podedujejo lastnosti gruče. To pomeni, da če gruča zagotavlja visoko razpoložljivost potem se virtualni stroji izvajajo v visoko razpoložljivem načinu.

Zunanja omrežja

Zunanje omrežje (ang. External network) je gradnik komponente vCloud Director, ki omogoča omrežno povezavo med organizacijami ter dostop do interneta. V osnovi je logično omrežje, ki temelji na vSphere skupini vrat. Podprta skupina vrat je lahko bodisi na standardnem ali na porazdeljenem stikalu. Pri tem mora biti omrežje ustrezno izolirano od vseh ostalih omrežij, ki si delijo isto fizično omrežje. Značilno je to, da so zunanja omrežja deljena med več organizacij, kar pomeni, da je promet znotraj teh omrežij dostopen vsem organizacijam, ki si omrežje delijo.

Organizacijski virtualni podatkovni centri

Da bi se organizacija funkcionalno omogočila je potrebna alokacija virov, saj se šele takrat lahko izvajajo potrebne delovne obremenitve. Gradniki, ki

omogoča alokacijo virov organizacije so organizacijski virtualni podatkovni centri (ang. Organization vDC) - OVPC. Viri, ki jih OVPC zagotavlja organizaciji, so alocirani v enem izmed PVPC-jev. Značilno je to, da ima organizacija lahko več podatkovnih centrov, ki so alocirani na različni PVPC-ji. Na nivoju virtualizacijske platforme predstavlja OVPC bazen virov znotraj gruče gostiteljev. Kot smo predstavili v poglavju 4.1.1.1, kjer smo obravnavali računske vire, bazeni virov ponujajo mehanizmi za določanje alokacije, omejitve ter rezervacije virov. vCloud Director uporablja te mehanizme za ustrezno alokacijo virov organizacije. OVPC podpira tri alokacijske modele in sicer:

- **Alokacija bazena virov (ang. Allocation pool):** organizaciji se alocira del virov, ki so na voljo. Delež alociranih virov se lahko tudi rezervira.
- **Zaračunavanje po porabi (ang. Pay-as-you-go):** Alokacija virov se izvede na nivoju posameznega virtualnega stroja. Celoten delež alociranih virov je odvisen od števila virtualnih strojev ter od njihovih velikosti. Predstavlja najbolj pogosto uporabljen alokacijski model, še posebej pri javnih oblakih.
- **Rezervacija bazena virov (ang. Reservation pool):** Podoben model kot alokacija bazena virov. Razlika je ta, da ne moremo vplivati na delež rezerviranih virov. Vsi alocirani viri se vedno tudi zagotovijo – rezervirajo.

Bazeni omrežij in organizacijska omrežja

Poleg računskih virov in virov shrambe vCloud Director na nivoju omrežja ponuja gradnike, ki zagotovijo omrežno povezavo virtualnih strojev v okviru ene organizacije. Bazen omrežij predstavlja skupino logičnih omrežij, ki so na voljo organizacijam. Bazen omrežij je lahko deljen med več organizacij, vendar morajo biti logična omrežja, ki jih vsebuje, ustrezno ločena. Ločevanje je nujno, kajti iz bazena se zagotavljajo organizacijska omrežja, ki so namenjena

izključno eni organizaciji. vCloud Director z uporabo bazenov omrežij vpeljuje elastičnost na nivoju omrežja, saj se v primeru kreiranja novega omrežja v organizaciji iz bazena dodeli logično omrežje, ter obratno, ko omrežje ni več potrebno se ustrezno logično omrežje vrne v bazen. Glede na način izolacije logičnega omrežja, lahko bazen omrežij temelji na:

- **VLAN-backed:** Predstavlja obseg VLAN identifikatorjev. Vsako logično omrežje ima določen svoj VLAN identifikator. Število omrežij je odvisno od števila identifikatorjev. Vsi VLAN identifikatorji morajo biti konfigurirani tudi na fizičnem stikalu, ki povezuje ESXi gostitelje med seboj.

- **Network isolation-backed:** Potrebujemo le en VLAN. Izolacija med omrežji se zagotovi z uporabo MAC-in-MAC enkapsulacije. Uporabljen VLAN, znotraj katerega se izvaja enkapsulacija, mora biti edinstven.

- **vSphere port group-backed:** Izberemo že ustvarjene skupine vrat na virtualizacijski platformi na stikalu. Predpogoj uspešne konfiguracije je, da so vse skupine vrat na svojem podomrežju – ločeni vsaj na drugem (L2) nivoju omrežja.

Organizacijska omrežja, ki jih zagotavlja bazen omrežij lahko razdelimo na:

- **Zunanje organizacijsko omrežje z direktno povezavo (ang. External organization network – direct connection):** Organizacijsko omrežje, ki ima neposredno povezavo do zunanjega omrežja. Ker se virtualni stroji povezujejo neposredno v zunanjem omrežju, dodatno logično omrežje iz bazena omrežij ni potrebno.

- **Zunanje organizacijsko omrežje povezano preko NAT (ang. External organization network – NAT routed connection):** Organizacijsko omrežje, povezano preko NAT usmerjene povezave. Med zunanjem in logičnem omrežju, ki se dodeli organizaciji je postavljen

vCNS Edge. Kot smo že izpostavili, vCNS Edge zagotavlja požarni zid ter druge omrežne storitve.

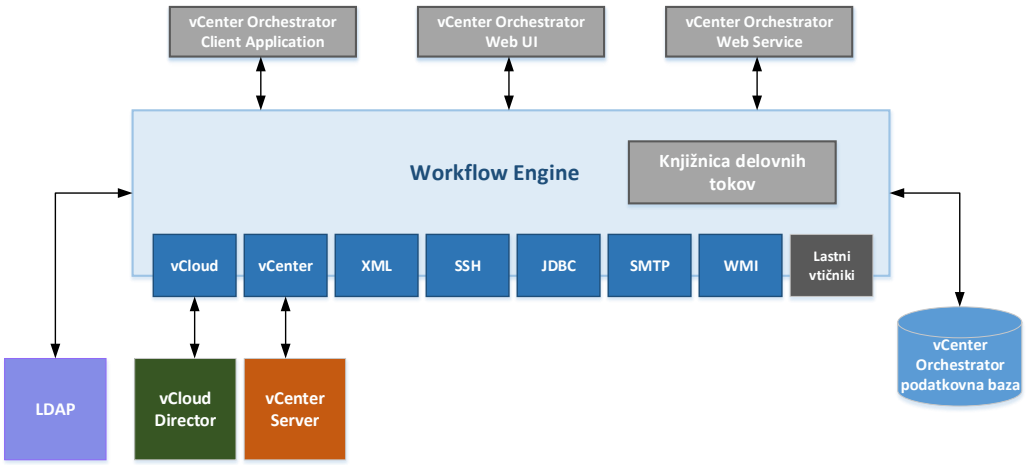
- **Interno organizacijsko omrežje (ang. Internal organization network):** Izolirano, privatno omrežje, ki si ga delijo virtualni stroji znotraj ene organizacije.

4.1.5 vCenter Orchestrator

Določeni procesi in postopki znotraj podatkovnih centrov so ponovljivi, kar pomeni, da jih je možno avtomatizirati. Avtomatizacija teh procesov in postopkov, ki bi jih bilo sicer potrebno izvesti ročno, lahko zmanjša tveganje človeških napak. Avtomatizacija se izkaže kot drugi najbolj pomembni faktor po upravljanju podatkovnega centra, še posebej v večjih okoljih, kot je primer današnjih virtualiziranih podatkovnih centrov, ki predstavljajo osnovo ekosistema oblaka. Virtualizacija infrastrukture namreč omogoča bolj učinkovito izkoriščenost infrastrukture, vendar hkrati vpeljuje bolj kompleksno okolje, saj je oskrba z novimi virtualnimi strežniki enostavnejša in se zaradi tega poveča velikost okolja. Od tod se pojavi vse večji pomen avtomatizacije oblaka.

Poleg tega avtomatizacija predstavlja tudi temelj orkestracije. Orkestracija je postopek združevanja različnih procesov, v smiselni delovni tok (ang. Workflow). Večina teh procesov, ki jih s pomočjo orkestracije združimo, so ravno avtomatizirani procesi. Najbolj pomembno lastnost, ki jo orkestracija prinaša v okolju oblaka, je orkestracija storitev. S pomočjo orkestracije posameznih avtomatiziranih procesov lahko orkestriramo postavitev celotne več-slojne aplikacije, ki je lahko sestavljena iz podatkovnega nivoja, aplikacijskega nivoja ter spletnega nivoja. Postavitev posameznega nivoja je lahko avtomatiziran proces ali celo gnezdeni delovni tok.

Velika večina rešitev na področju računalništva v oblaku ponuja vgrajene mehanizme za avtomatizacijo in orkestracijo procesov. Rešitev vCloud



Slika 4.11: Arhitektura komponente vCenter Orchestrator [17].

omogoča orkestracijo s pomočjo komponente vCenter Orchestrator [17]. Arhitektura komponente je prikazana na sliki 4.11.

Poleg avtomatizacije in orkestracije, komponenta omogoča tudi integracijo, tako z ostalimi komponentami oblaka vCloud, kot tudi z zunanji sistemi. Integracija z zunanjimi sistemi je dosežena preko vgrajenih ter lastno razvitih vtičnikov. Vtičniki omogočajo razširljivost oblaka, kar igra ključno vlogo, saj predstavlja način kako razširiti zmožnosti oblaka ter implementirati dodatne funkcionalnosti, ki jih vgrajene komponente ne omogočajo.

4.1.6 vCenter Operations Manager

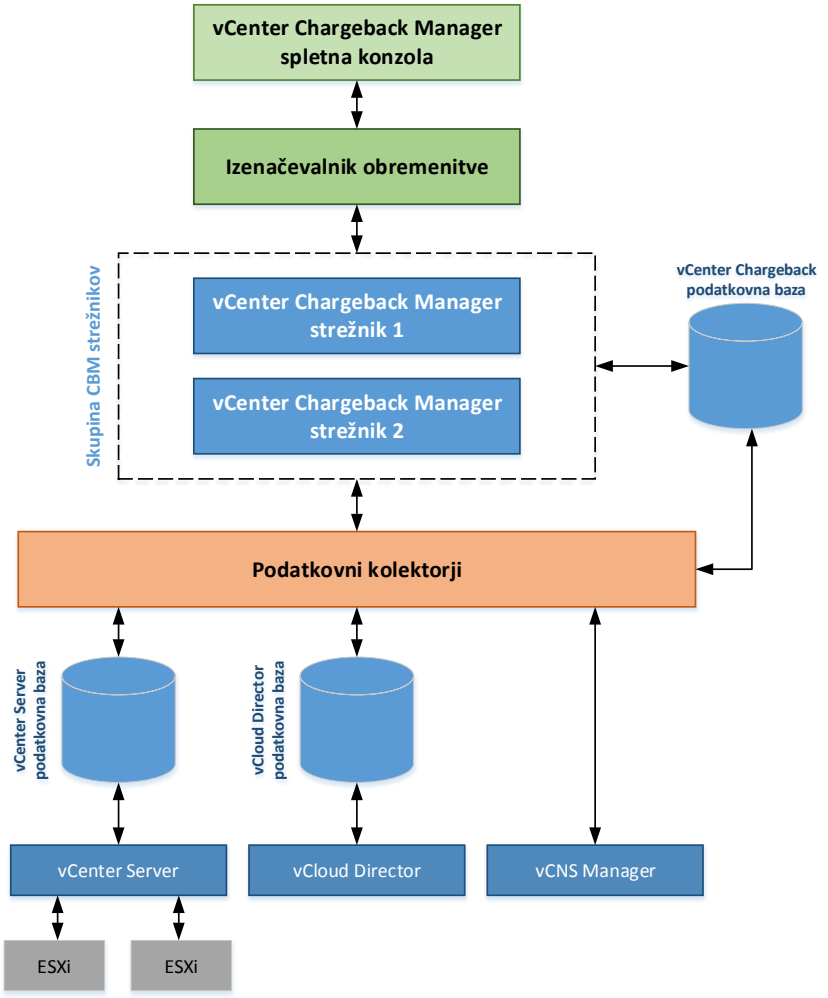
Spremljanje stanja virtualizirane infrastrukture oblaka se v praksi izkaže za enako pomembno kot samo upravljanje. Spremljanje infrastrukture v primeru rešitve vCloud omogoča komponenta vCenter Operations Manager [18]. Slednja zbira podatke o vsakem objektu virtualizirane in fizične infrastrukture. To vključuje podatke o posameznih virtualnih strojih, podatkovnih shrambah, fizičnih diskih, logičnih diskovnih enotah itd. Podatki so zbrani glede na številne metrike, ki se kombinirajo za izračun ocene stanja. Zbrani podatki se analizirajo, nato pa se na podlagi rezultatov analize določajo

pragovi pravilnega obnašanja. Operations Manager omogoča pregled stanja celotnega oblaka in ponuja zelo hiter način za identifikacijo tistih virov v postavljeni infrastrukturi, ki odstopajo od povprečja. To je mogoče doseči z načinom ocenjevanja podatkovnega centra, ki v drevesni strukturi povezuje slabše ocenjene vire, pri čemer uporabnik brez težav ugotovi vzrok poslabšanega delovanja. Komponenta omogoča napovedovanje obnašanja posameznih objektov v prihodnosti. V primeru zmanjšanja zmogljivosti oziroma kapacitet objektov, omogoča tudi opozarjanje. Kot dodatno možnost za integracijo z zunanjimi komponentami, vCenter Operations Manager ponuja podporo za SNMP (ang. Simple Network Management Protocol) ter SMTP (ang. Simple Mail Transfer Protocol) protokol za obveščanje o dogodkih.

4.1.7 vCenter Chargeback Manager

Merjenje storitve v oblaku je kot smo videli v poglavju 3.1 ena izmed bistvenih značilnosti oblaka. Ključni koncept računalništva v oblaku je zaračunavanje glede na dejansko porabo virov. Rešitev vCloud zagotavlja merjenje porabe virov, alociranih za izvajanje delovnih obremenitev v oblaku, s pomočjo komponente vCenter Chargeback Manager [19]. Tudi v primeru, ko gre za privatni oblak namenjen eni poslovni organizaciji, se merjenje porabe virov izkaže kot pomembno. S pomočjo merjenja porabljenih virov po posameznih delovnih obremenitvah in objektih na nivoju komponente vCloud Director [20], se lahko doseže bolj učinkovita izraba virov in sredstev v poslovni organizaciji. Slika 4.12 prikazuje arhitekturo komponente vCenter Chargeback.

Ključni lastnosti komponente sta možnost merjenja porabe virov ter izdelava poročil o porabi in stroških porabe. Poročila o stroških porabe so izdelana na osnovi definiranih stroškovnih modelov, ki zajemajo posamezne objekte v hierarhiji. Hierarhija vsebuje vCloud objekte, ki segajo od ponudnika virtualnih podatkovnih centrov do posameznih virtualnih strojev znotraj vApp-ov. Na nivoju omrežja komponenta omogoča merjenje porabe virov, kot so uporabljeni javni IP naslovi, požarni zid, VPN ipd. Podpira vse tri tipe alokacijskih modelov iz komponente vCloud Director. V odvisnosti



Slika 4.12: Arhitektura komponente vCenter Chargeback [19].

od tipa alokacijskega modela na katerem temelji OVPC, vCenter Chargeback uporabi ustrezen model za zaračunavanje porabljenih virov.

4.2 Dodatne komponente privatnega oblaka

V prvem delu poglavja smo obravnavali ključne komponente rešitve vCloud oblaka. Ker je koncept rešitve zasnovam tako, da lahko omogoča še druge oblike postavitve kot je javna ter hibridna, ponuja še dodatne komponente, ki

prinašajo nekatere dodatnih funkcionalnosti. Potreba po teh dodatnih komponente je seveda odvisna od potrebe poslovne organizacije ali ponudnika storitev v oblaku, ki vzpostavlja model računalništva v oblaku. vCloud ponuja naslednje dodatne komponente:

- **vCloud Connector:** Komponenta [21], ki omogoča vzpostavitev homogene hibridne platforme med dvema vCloud oblakoma. Najbolj pogosta oblika je povezava med zasebno ter javno postavitvijo.
- **vFabric Application Director:** Predstavlja komponento [22], ki omogoča upravljanje aplikacij, ki se izvajajo v oblaku. Komponenta delno implementira PaaS nivo. Ključna lastnost je možnost kreiranja načrta postavitve aplikacij (ang. Blueprints), s katerim bi se poenostavil postopek postavljanja novih aplikacij. Načrti v večini primerov predstavljajo več-slojne arhitekture (npr. tri-nivojska arhitektura). Posamezni gradniki arhitekture so vApp predloge na nivoju komponente vCloud Director.
- **vCloud Automation Center:** Komponenta, ki dodaja dodatni nivo abstrakcije nad celotno rešitev in poskuša zagotoviti postavitev javnih in privatnih oblakov na osnovi različnih virtualizacijskih platform skozi enoten spletni portal. Poleg tega ponuja tudi možnost povezave z nekaterimi javnimi ponudniki, kot sta Amazon in Azure.

Poglavje 5

Vzpostavitev arhitekture privatnega oblaka

V poglavju 4 smo obravnavali rešitev vCloud, kot eno izmed rešitev, ki omogoča implementacijo modela računalništva v oblaku in ponuja IaaS storitve. Za posamezne komponente rešitve smo povzeli njihove vloge v sklopu rešitve ter analizirali funkcionalnosti in gradnike, ki jih zagotavljajo in omogočajo. Temeljno znanje teh gradnikov in funkcionalnosti predstavlja izhodišče pri vzpostavitvi arhitekture tako privatnega kot tudi javnega oblaka, saj lahko s pomočjo teh funkcionalnosti in gradnikov implementiramo arhitekturo oblaka ter končnim uporabnikom/najemnikom ponudimo IaaS storitev.

5.1 Definiranje storitev in opredelitev kapacitete okolja

Sama vzpostavitev arhitekture privatnega oblaka in postavitev posameznih komponent na splošno, ne glede na izbrano rešitev, zajema več faz sestavljenih iz več korakov. Začetna faza vzpostavitve arhitekture predstavlja opredelitev kapacitete infrastrukture (računskih virov, viri shrambe in omrežnih virov) ter definicijo storitev [24], ki jih bo postavitev oblaka zagotavljala. Na opredelitev velikosti okolja neposredno vpliva klasifikacija in število delovnih

obremenitev, ki se bodo izvajale v ciljnem okolju privatnega oblaka. Klasifikacija delovnih obremenitev je zaželena, saj so tipi delovnih obremenitev odvisni od narave poslovanja poslovne organizacije, ki vzpostavlja privatni oblak. Delovne obremenitve lahko v splošnem razdelimo na tri tipe [24]:

- **Prehodne (ang. Transient):** Za ta tip delovnih obremenitev je značilno, da obstajajo zgolj za določen čas in se ne uporabljajo pogosto. Po navadi so namenjene točno določenemu opravilu.
- **Dinamične - elastične (ang. Elastic):** Delovne obremenitve tega tipa so nepredvidljive vsaj v določeni meri. Imajo zelo dinamično spremembo povpraševanja ter porabe virov. V določenem obdobju povpraševanje lahko močno naraste, v drugem pa močno pade.
- **Statične (ang. Steady State):** V to skupino spadajo delovne obremenitve, ki imajo predvidljivo povpraševanje ter porabo virov skozi čas.

Ustrezna klasifikacija delovnih obremenitev pred samo postavitvijo igra pomembno vlogo pri razporejanju kapacitete ter izbiri deleža različnih alokacijskih modelov. Kot smo obravnavali v poglavju 4, rešitev vCloud ponuja tri tipe alokacijskih modelov in sicer alokacijski model, ki temelji na alokaciji bazena virov; rezervacijski model ter model, ki temelji na principu zaračunavanja po porabi. Za vsak tip delovnih obremenitev je mogoče uporabiti ustrezen alokacijski model [24]. V primeru prvega tipa delovnih obremenitev je najbolj učinkovita izbira alokacijskega modela, ki temelji na principu zaračunavanja po porabi, saj predstavlja najbolj fleksibilno izbiro. Alokacija virov se namreč izvaja na nivoju posameznega virtualnega stroja. Za drugi tip delovnih obremenitev je smiselna uporaba modela, ki temelji na principu alokacije bazena virov. V primeru delovnih obremenitev statičnega tipa je najbolj optimalna uporaba rezervacijskega modela, saj imajo v povprečju delovne obremenitve tega tipa konstantno povpraševanje in porabo virov. S pomočjo klasifikacije delovnih obremenitev se lahko doseže

učinkovitejša razporeditev in poraba kapacitet virov oblaka. Poleg osnovnih tipov, lahko delovne obremenitve razdelimo tudi glede na zahtevo virov in sicer kot: računsko zahtevne, omrežno zahtevne ter delovne obremenitve, ki zahtevajo visoko zmogljivo shrambo predvsem z vidika latence dostopa. Glede na stopnjo zastopanja posameznih delovnih obremenitev je potrebno temu ustrezno prilagoditi infrastrukturo. V praksi se izkaže, da je zastopanost različnih delovnih obremenitev v okolju heterogena, kar pomeni še večji izziv pri postavitvi oblaka.

Poleg opredelitve kapacitete okolja je potrebno analizirati tudi strategijo postavitve. Slednje izhaja iz dejstva, da je možno posamezne delovne obremenitve razdeliti tudi s stališča zahtevane varnosti in zaupnosti ter integritete podatkov s katerimi delajo. Postavitev je namreč lahko popolnoma zasebna ali hibridna. V primeru popolnoma zasebne postavitve se vse delovne obremenitve izvajajo v privatnem oblaku. V primeru hibridne postavitve pa se določen delež delovnih obremenitev izvaja v javnem oblaku. Določene aplikacije, ki ne zahtevajo strogih varnostnih principov, je možno izvajati tako v zasebnem podatkovnem centru, kot tudi v javnem oblaku. Kot bomo videli v poglavju 6, se v določenih primerih hibridna postavitev lahko izkaže kot izhodna strategija za doseganje stroškovne učinkovitosti privatnega oblaka.

Kot drugi pomemben aspekt, ki ga je potrebno nasloviti v prvi fazi vzpostavitve arhitekture privatnega oblaka, je definicija storitev [24], ki jih bo privatni oblak zagotavljal. Za vsako posamezno storitev je potrebno definirati cilje storitve, način merjenja, poročanja ter zaračunavanja storitve. Definirati je potrebno uporabniške vloge, ki imajo omogočeno interakcijo s to storitvijo ter druge parametre kot so razpoložljivost, zahtevani tip shrambe, parametri zmogljivosti ipd. Definirane storitve združimo v storitveni/aplikacijski katalog. V najbolj osnovni obliki ena IaaS storitev predstavlja enega ali več virtualnih strojev na katerih je lahko že nameščena ter konfigurirana določena programska oprema in je v takšni obliki na voljo končnim uporabnikom preko samopostrežnega portala. Tako pripravljeni virtualni stroji so osnova za storitve višjih nivojev (PaaS in SaaS aplikacije). Instance virtualnih strojev

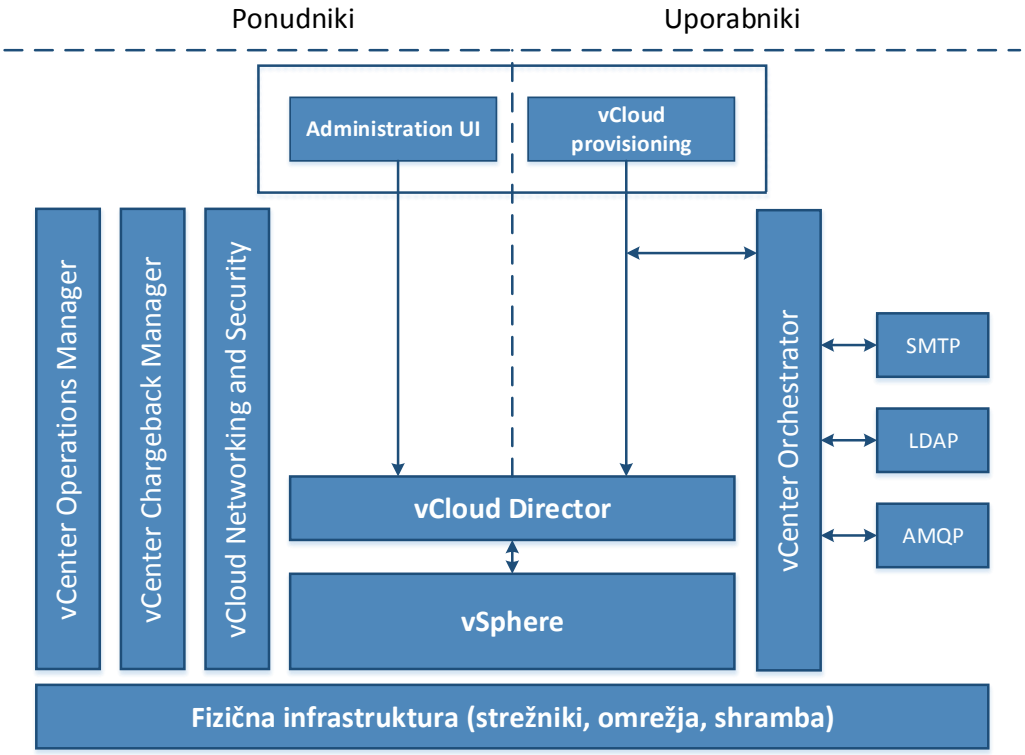
je smiselno razdeliti v določene velikostne skupine s stališča kapacitete pomnilnika, števila virtualnih procesorjev in kapacitete shrambe, ki je na voljo virtualnemu stroju.

Definiramo lahko na primer majhno instanco, ki bo imela 1 vCPU, 2GB pomnilnika ter 40GB diska. V drugi skupini lahko definiramo srednjo instanco z 2 vCPU-ja, 4GB pomnilnika, 70GB diskovnega prostora in v zadnji skupini veliko instanca, ki bo imela 4 vCPU-ji, 8GB pomnilnika ter 100GB diska. Na tak način lahko dosežemo boljšo razpredelitev kapacitet infrastrukture in obenem učinkovitejšo rabo virov. Izbira velikosti instanc je odvisna od narave poslovanja poslovne organizacije ter od tipov delovnih obremenitev, ki se bodo izvajale v privatnem oblaku.

V okviru izdelave diplomskega dela je izvedena testna postavitev rešitve vCloud z osnovnimi komponentami, ki smo jih opisali in analizirali v poglavju 5. Zasebna postavitev bo primarno zagotavljala IaaS storitve končnim uporabnikom v obliki pripravljenih instanc virtualnih strojev, na katerih bo nameščen in konfiguriran operacijski sistem. Instance virtualnih strojev bodo na voljo v treh velikostnih razredih in sicer: majhna, srednja in velika instanca. Velikosti instanc so enake kot v zgoraj omenjenem primeru. Končnim uporabnikom bodo na voljo operacijski sistemi Windows Server 2008 R2, Windows Server 2012 in CentOS Linux 6.3.

5.2 Konceptualna arhitektura rešitve vCloud

Pri vzpostavitvi arhitekture privatnega oblaka z uporabo rešitve vCloud lahko uporabimo katalog dokumentov vCAT [25], ki podaja smernice in dobre prakse pri namestitvi in konfiguraciji posameznih komponent rešitve vCloud. V nadaljevanju se poglavje osredotoča na načrt arhitekture privatnega oblaka ter okvirno podaja opis namestitve posameznih komponent, s pomočjo katerih lahko implementiramo zasnovano arhitekturo in končnim uporabnikom ponudimo na začetku definirane storitve.



Slika 5.1: Konceptualna arhitektura rešitve vCloud [26].

V poglavju 4 smo obravnavali posamezne komponente rešitve, kjer smo se osredotočili na ključne komponente. Slika 5.1 prikazuje konceptualno arhitekturo ključnih komponent rešitve [26]. Kot lahko opazimo na sliki, horizontalno postavljene komponente v arhitekturi zagotavljajo temeljne funkcionalnosti in predstavljajo osnovni način zagotavljanja virov oblaka. Kot smo že videli v poglavju 4, vertikalno postavljene komponente v konceptualni arhitekturi na sliki zagotavljajo spremljanje, nadzor, varnost ter razširljivost in avtomatizacijo okolja. Poleg tega lahko opazimo, da vCloud Director ponuja ločen dostop sistemskim administratorjem oblaka, saj se na ta način omogoči konfiguracija in upravljanje oblaka preko sistemskega portala.

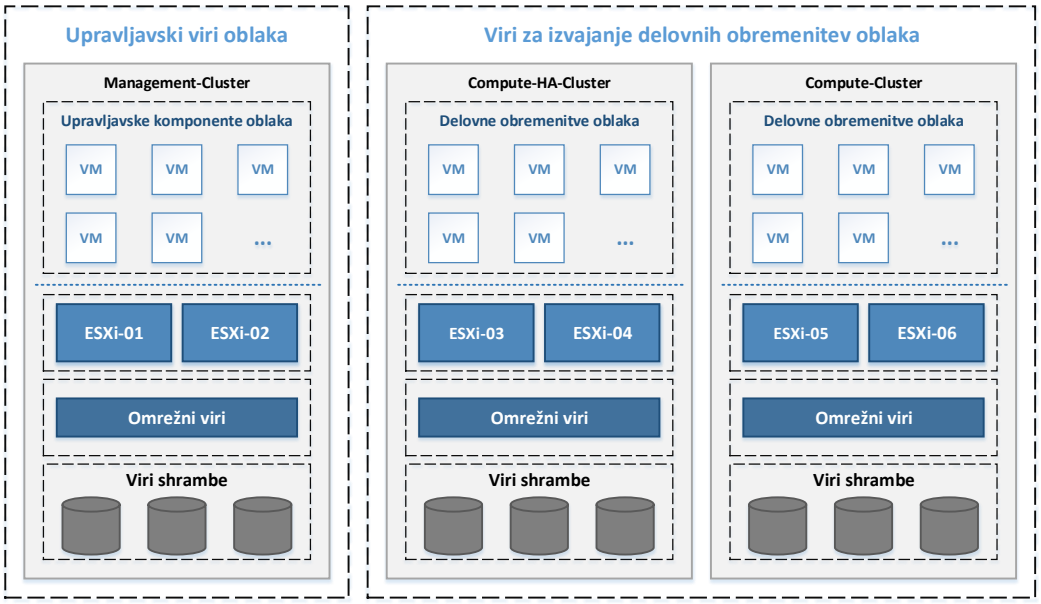
V okviru testne postavitve rešitve vCloud, v prvi fazi je izvedena postavitev osnovnih komponent, z namenom implementacije zasnovane arhi-

tekture privatnega oblaka in ponujanja osnovnih IaaS storitev preko vgrajenega samopostrežnega portala, ki ga ponuja komponenta vCloud Director. V drugi fazi je arhitektura zasebne postavitve dopolnjena z vpeljavo komponente vCloud Connector, ki omogoča vzpostavitev hibridne platforme med zasebno postavitvijo oblaka vCloud ter enem ali več ponudnikov javnih oblakov, temelječih na rešitvi vCloud. Zasnova in implementacija arhitekture privatnega oblaka je opisana v nadaljevanju tega poglavja. Implementacija hibridne platforme je opisana v poglavju 6.

5.3 Načrt arhitekture privatnega oblaka

Preden se lotimo implementacije arhitekture moramo izdelati načrt same arhitekture, ki bo služil kot izhodišče pri implementaciji. Ključna točka načrtovanja arhitekture, ne glede na izbrano rešitev, je določitev namestitvene strategije posameznih komponent rešitve, ki skrbijo za upravljanje, spremljanje in nadzor oblaka. Prvi način je klasična postavitev posameznih komponent neposredno na fizične strežnike. Druga možnost je postavitev posameznih komponent na virtualizirane strežnike (virtualnih strojih), ki se bodo izvajali na virtualizacijski platformi podobno kot same delovne obremenitve oblaka. Kot smo izpostavili v poglavju 2, predstavlja drugi način v primerjavi z uporabo fizičnih strežnikov za upravljavske komponente oblaka bolj učinkovito izbiro. Slednji predstavlja tudi dobro prakso, ki velja v splošnem pri namestitvah ne glede na izbrane rešitve in tehnologije s katerimi implementiramo arhitekturo privatnega oblaka. Dodatna motivacija za uporabo virtualiziranih strežnikov za upravljavske komponente oblaka je dejstvo, da je lažje zagotoviti izvajanje virtualnih strojev v visoko razpoložljivem načinu v primerjavi s fizičnimi strežniki.

Ker se v tem primeru komponente za upravljanje oblaka izvajajo v virtualiziranem okolju podobno kot same delovne obremenitve, je priporočljivo ločevanje (ang. Segregation) virov na nivoju infrastrukture [26]. Kljub popolnoma ustrezni implementaciji arhitekture brez ločevanja virov je to zaželeno



Slika 5.2: Logična arhitektura privatnega oblaka.

in predstavlja dobro prakso pri načrtovanju arhitektur privatnih oblakov, kar velja ne glede na izbrano rešitev za implementacijo arhitekture. S pomočjo ustreznega ločevanja virov na vire, ki so namenjeni izvajanju komponent za upravljanje oblaka in vire namenjene za izvajanje delovnih obremenitev oblaka, se lahko doseže večja varnost, skalabilnost ter večja odpornost (ang. Resilience) okolja proti napakam. Ločevanje je zaželeno za vse tipe infrastrukturnih virov (računski viri, omrežni viri in viri shrambe). Poleg tega, lahko s pomočjo ločevanja virov dosežemo jasno ločevanje nalog in vlog. Lahko imamo namreč ločene sistemske administratorje, ki skrbijo za upravljavske komponente in sistemske administratorje, ki skrbijo za vire namenjene izvajanju delovnih obremenitev.

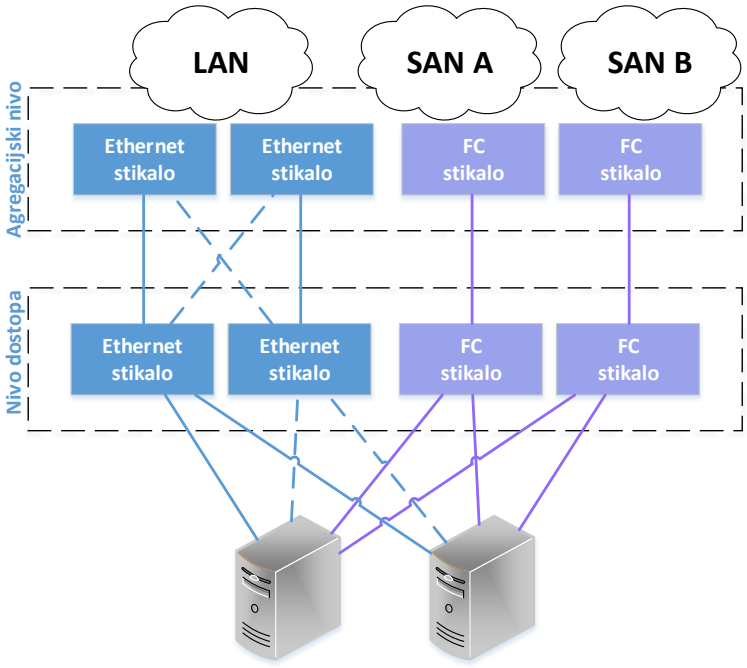
Slika 5.2 prikazuje ločevanje infrastrukture v primeru testne postavitve privatnega oblaka. Infrastruktura je sestavljena iz šestih gostiteljev virtualizacije, omrežnih virov ter virov shrambe. Kot lahko opazimo na sliki so viri infrastrukture ločeni v dve skupini. Prva skupina vsebuje vire za izvajanje upravljavskih komponent oblaka, druga skupina pa vsebuje vire za izvajanje

delovnih obremenitev oblaka. Ločevanje računskih virov infrastrukture lahko dosežemo s pomočjo gruče, ki smo jo analizirali v poglavju 4. V prvi skupini virov (upravljavski viri oblaka) imamo gručo (Management-Cluster) dveh gostiteljev. Če bolj pozorno pogledamo logično arhitekturo oblaka na sliki 5.2, je druga skupina virov (viri za izvajanje delovnih obremenitev oblaka) segmentirana v dveh gručah. Prva gruča gostiteljev (Compute-HA-Cluster) vsebuje dva gostitelja virtualizacije, ki bodo implementaciji omogočala izvajanje delovnih obremenitev v visoko razpoložljivem načinu. Druga gruča (Compute-Cluster) vsebuje dva gostitelja, vendar ne ponuja izvajanja delovnih obremenitev v visoko razpoložljivem načinu. S tem lahko klasificiramo fizične strežnike glede njihovih zmogljivosti in konfiguracije (kot na primer: strežniki, ki imajo redundantne omrežne adapterje in strežniki, ki nimajo redundantne omrežne adapterji). S tem lahko dosežemo različne nivoje zagotavljanja storitev na osnovi ponujenih SLA-jev za definirane storitve. Klasifikacija nenazadnje izboljša učinkovitost razporeditve porabe virov, saj vse delovne obremenitve ne potrebujejo izvajanja v visoko razpoložljivem načinu ali redundantne omrežne povezave.

Poleg ločevanja računskih virov, ki jih zagotavljajo fizični strežniki, je zaželeno ločevanje omrežij, ki se uporabljajo s strani upravljavskih komponent oblaka ter delovnih obremenitev. Z ustreznim ločevanjem omrežnih virov lahko dosežemo tako boljšo zmogljivost kot tudi večjo varnost omrežja. Prav tako s tem zagotovimo tudi večjo odpornost omrežne infrastrukture proti napakam. Promet, ki ga generirajo delovne obremenitve, namreč nima vpliva na promet in zmogljivost omrežja namenjenega upravljavskim komponentam oblaka. V primeru, ko ne moremo zagotoviti fizično ločenih omrežij, upravljavskih komponent in delovnih obremenitev je treba zagotoviti ločevanje omrežij s pomočjo VLAN-ov. Na ta način lahko zagotovimo vsaj ustrezno varnost in izolacijo med posameznimi omrežji. Poleg fizičnega ločevanja omrežnih virov na nivoju virtualizacijske platforme, je priporočljiva uporaba ločenih virtualiziranih stikal. Uporaba ločenih virtualiziranih stikal v primerjavi s fizičnim ločevanjem omrežij predstavlja bistveno manjši konfiguracijski

zalogaj, prinese pa lahko veliko. S tem preprečimo vpliv prometa enega tipa na drugega, kot na primer napačna konfiguracija stikala namenjenega upravljavskim komponentam ne povzroči moteno delovanje stikala namenjenega delovnim obremenitvam. Kljub temu, da lahko v takem primeru začasno izgubimo nekatere upravljavske funkcije, je dostop do virtualnih strojev, ki so na drugem stikalu, nemoten. Gostitelji virtualizacije imajo znotraj upravljavske gruče dostop le do upravljavskega stikala in obratno gostitelji, namenjeni vCloud Director virom, za izvajanje delovnih obremenitev imajo dostop le do stikala namenjenega delovnim obremenitvam.

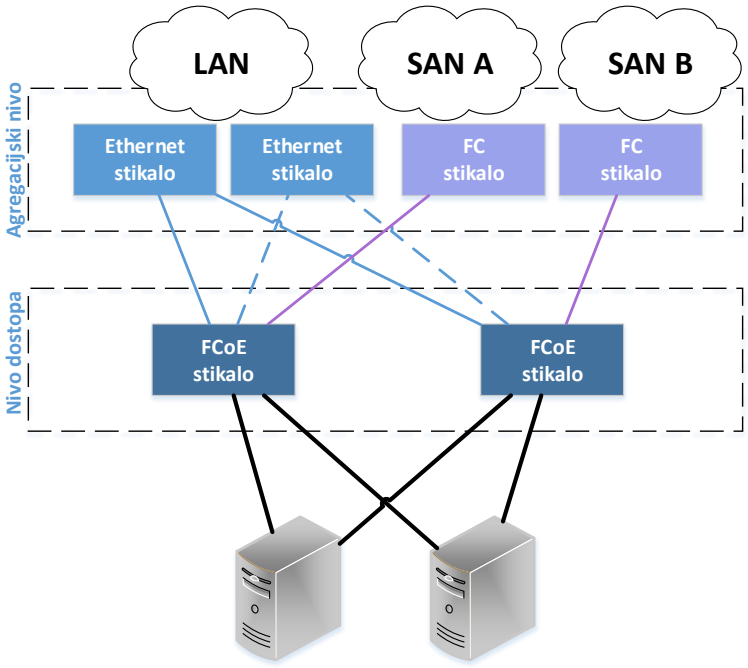
Podobno kot pri računskih in omrežnih virih infrastrukture je tudi pri virov shrambe priporočljivo zagotoviti ločene podatkovne shrambe, kjer so shranjeni virtualni stroji, na katerih so nameščene komponente za upravljanje oblaka ter virtualni stroji za izvajanje delovnih obremenitev oblaka. Kljub temu, da se v praksi uporablja en sistem za shrambo, je možno za posameznemu gostitelju virtualizacije določiti do katere logične enote (ki zagotavljajo shrambo podatkovnim shrambam na nivoju virtualizacijske platforme) ima dostop. Povezava do sistema, ki zagotavlja shrambo, je odvisna od uporabljenega tipa oddaljene shrambe. V primeru uporabe FC oddaljene shrambe povezava poteka po ločenem fizičnem omrežju (FC SAN) preko optične povezave. Alternativa FC oddaljeni shrambi je shramba, ki za komunikacijo uporablja protokol TCP/IP in sicer iSCSI (IP SAN) ter NAS. V tem primeru je lahko povezava do shrambe realizirana preko LAN omrežja. Dobra praksa je, da se za shrambo uporabi ločeno LAN omrežje, ki bo namenjeno le shrambi. Če ni mogoča uporaba ločenega omrežja za shrambo, je zaželeno uporabiti ločeno VLAN omrežje zaradi boljše varnosti in vzdržljivosti. Če se uporablja isto omrežje tako za upravljavski promet kot tudi za shrambo je potrebno zagotoviti mehanizme, ki preprečijo preobremenjenost omrežja s strani enega tipa prometa. Primeri takšnih mehanizmov so NIOC (ang. Network I/O Control), QoS (ang. Quality of Service) ipd. Druga možnost za dostop do oddaljene shrambe, poleg FC ter IP SAN, je uporaba FCoE. V primer uporabe FCoE se FC okviri enkapsulirajo v Ethernet okvirje. Iz



Slika 5.3: Povezava strežnikov v ne-združenem omrežju.

tega izhaja dejstvo, da se lahko isti prenosni medij uporabi tako za navaden LAN promet kot tudi za SAN promet v t.i. združenem omrežju (ang. Converged network). S tem se zmanjša število fizičnih povezav med strežniki in stikali. Za FCoE potrebujemo posebna stikala ter posebne omrežne adapterje na strežnikih (ang. Converged Network Adapter - CNA), ki omogočajo povezavo preko združenega omrežja.

Slika 5.3 prikazuje primer povezave dveh strežnikov z LAN ter SAN omrežjem preko navadnih LAN omrežij. Kot lahko vidimo so stikala podvojena za zagotavljanje redundantne povezave tako iz strežnikov, kot tudi do agregacijskega nivoja, kar je tudi dobra praksa. Na sliki 5.4 lahko vidimo, da povezava med strežniki po vmesnih stikalih poteka preko iste fizične povezave. V tem primeru se število stikal na vmesnem nivoju ter število povezav iz strežnikov do stikal prepolovi.



Slika 5.4: Povezava strežnikov v združenem omrežju.

5.3.1 Arhitektura upravljavskega dela oblaka

Upravljavski del oblaka, kot daleč najbolj pomemben segment arhitekture privatnega oblaka, je potrebno sistematično načrtovati. Načrt podaja smernice pri sami implementaciji arhitekture in prispeva k doseganju na začetku zastavljenih ciljev. Kot smo obravnavali v prejšnjem podpoglavju, je dobra praksa ločiti vire za upravljavski del oblaka. Poleg ločevanja virov v posebne gruče, je mogoče ločiti nivo upravljanja posameznih skupin virov. Komponenta vCenter Server, kot smo videli v poglavju 4, zagotavlja centralizirano upravljanje in konfiguracijo gostiteljev virtualizacije ter ostalih virov. Po drugi strani se komponenta vCloud Director za zagotovitev logičnih virov oblaka integrira neposredno s komponento vCenter Server. Če uporabimo ločen vCenter strežnik za upravljavski del ter ločen vCenter strežnik za skupino virov namenjeno izvajanju delovnih obremenitev, dosežemo šibko sklopljenost med upravljavskim nivojem virtualizacijske platforme za upravlja-

vske komponente oblaka ter upravljavskim nivojem virtualizacijske platforme za delovne obremenitve [26]. vCloud Director se v tem primeru integrira z vCenter strežnikom, ki upravlja virtualizacijske vire namenjene izvajanju delovnih obremenitev. Ločevanje nivoja upravljanja izboljša upravljivost okolja ter poveča skalabilnost arhitekture. Če se v prihodnosti izkaže, da postane velikost okolja neobvladljiva s strani enega vCenter strežnika, je mogoča enostavna nadgradnja okolja z dodajanjem novega vCenter strežnika. vCenter strežnik je mogoče namestiti v povezani skupini in s tem omogočiti upravljanje posameznih vCenter strežnikov preko enotne upravljavske konzole (ang. Single-pane-of-glass).

Upravljavski del v osnovni obliki vsebuje ključne komponente prikazane v konceptualni arhitekturi rešitve s sliko 5.1. Poleg teh osnovnih komponent, ki so del same rešitve, za vzpostavitev potrebujemo tudi nekatere zunanje komponente za določene infrastrukturne storitve kot so LDAP/Active Directory, DNS, DHCP, NTP, strežniki za beleženje (Syslog), itd. Določene komponente rešitve zahtevajo, da so nameščeni operacijski sistemi, na katerih so nameščene komponente, del domene. V ta namen potrebujemo vzpostavljeno domeno organizacije, s priporočljivim domenskim nadzornikom (ang. Domain controller) Active Directory (AD). Poleg zagotavljanja domene, AD ponuja imeniške storitve in omogoča upravljanje z identitetami v privatnem oblaku. Določene komponente rešitve vCloud zahtevajo medsebojno komunikacijo z uporabo polnih domenskih imen (ang. Fully Qualified Domain Name - FQDN) računalnikov, za kar potrebujemo dostop do DNS strežnika, ki omogoča razrešitev domenskih imen in IP naslovov. Zunanje komponente so lahko na novo nameščene na virtualne stroje, ki se izvajajo v upravljavski gruči ali pa so že obstoječe iz okvira poslovne organizacije. V okviru testne postavitve privatnega oblaka so zunanje komponente nameščene na virtualne stroje znotraj upravljavske gruče.

Za shranjevanja stanja komponente zahtevajo namensko podatkovno bazo na enem izmed podprtih instanc podatkovnih baz. Pri tem je mogoče uporabiti ločen strežnik podatkovne baze za vsako posamezno komponento ali

uporabiti skupni strežnik, ki je ustrezno dimenzioniran. Slednje ponuja učinkovitejšo izrab virov, zahteva manjše število licenc operacijskih sistemov ter poenostavi upravljanje in vzdrževanje podatkovnih baz. Strežnik podatkovne baze je lahko nameščen na virtualnem stroju znotraj upravljavske gruče. Možna je tudi uporaba že obstoječega strežnika s podatkovno bazo ali gruče strežnikov podatkovnih baz.

Zaradi pomembnosti komponent za upravljanje oblaka je priporočljivo ter tudi spada pod dobro prakso [26, 27], zagotoviti zanesljivost in razpoložljivost okolja v katerem se komponente izvajajo. Osnovni mehanizem s katerim je to mogoče je izvajanje virtualnih strojev na katerih so nameščene upravljavske komponente, v visoko razpoložljivem (HA) načinu. V primeru rešitve vCloud lahko to dosežemo tako, da na upravljavski gruči uporabimo funkcionalnost vSphere HA. Če želimo uporabiti visoke razpoložljivosti je minimalno število gostiteljev v gruči dva. Če okoliščine dopuščajo, je priporočljivo, da upravljavska gruča vsebuje vsaj tri gostitelje [26]. S tem dosežemo redundanco N+1;

vSphere HA zagotavlja visoko razpoložljivost le v primeru odpovedi gostiteljev ter v primeru odpovedi operacijskega sistema znotraj virtualnih strojev. V praksi pa se odpovedi in napake pojavljajo tudi znotraj aplikacij. Poleg tega ne zagotavlja ničelnega časa izpada - vedno imamo določen čas nedosegljivosti. Kljub temu, da vSphere HA zagotavlja ponovni zagon virtualnih strojev v primeru izpada enega izmed gostiteljev v gruči, za določene komponente to ni dovolj (na primer v primeru izpada komponente AD avtentikacija in avtorizacija uporabnikov ni mogoča, v primeru izpada komponente vCenter Server, ni več mogoče upravljanje delovnih obremenitev), kar lahko pomeni morebitno kršitev SLA dogovorov.

Če želimo zagotoviti visoko razpoložljivost na nivoju samih komponent in zagotoviti ničelni čas izpada potrebujemo dodatne mehanizme. V primeru AD in domenskega nadzornika je mogoče postaviti dodatne sekundarne AD strežnike. S tem zagotovimo dosegljivost domene kljub izpadu primarnega domenskega nadzornika. Splošne dobre prakse pri virtualizaciji komponente

AD so na voljo v [28].

Za povečevanje razpoložljivosti podatkovne baze lahko uporabimo Microsoft Failover Clustering [29] in v gručo namestimo dva ali več SQL strežnikov, ki vsebujejo podatkovne baze posameznih upravljavskih komponent rešitve vCloud. Ob morebitni napaki na primarnem SQL strežniku se izvajanje podatkovnih operacij samodejno preklopi na enega izmed sekundarnih strežnikov. S tem zagotovimo dostop do podatkovnih baz tudi v primeru, ko odpove primarni SQL strežnik. Vsi strežniki v SQL gruči si delijo dostop do shrambe. Slednje lahko predstavlja enotno točko odpovedi (ang. Single point of failure), kajti v primeru, da shramba, ki hrani podatke, ni replicirana lahko morebitne odpovedi delovanja pomenijo trajno izgubo podatkov. Poleg replikacije deljene shrambe je enotna točka odpovedi lahko tudi sama povezava do oddaljene shrambe.

Razpoložljivost komponente vCenter Server je možno izboljšati z uporabo komponente vCenter Server Heartbeat [30], ki omogoča aktivno/pasivno redundanco komponente. Komponenta vCenter Server Heartbeat je na voljo izven rešitve vCloud. Poleg primarnega vCenter strežnika se postavi dodaten vCenter strežnik, ki je v pasivnem stanju. V primeru odpovedi primarnega se aktivira sekundarni. S tem dosežemo neprekinjeno dosegljivost komponente.

Kot smo videli v poglavju 4, kjer smo obravnavali komponento vCloud Director, je arhitektura komponente zasnovana skalabilno, kar pomeni, da lahko postavimo več vCloud Director instanc (celic) v skupini in jih izpostavimo preko izenačevalnika obremenitve v aktivni/aktivni redundanci. S tem lahko dosežemo večjo dosegljivost komponente ter večjo odzivnost kajti prihajajoče zahteve se razporejajo po posameznih strežnikih v skupini. V primeru odpovedi enega izmed strežnikov je dostop do oblaka še vedno mogoč preko ostalih celic.

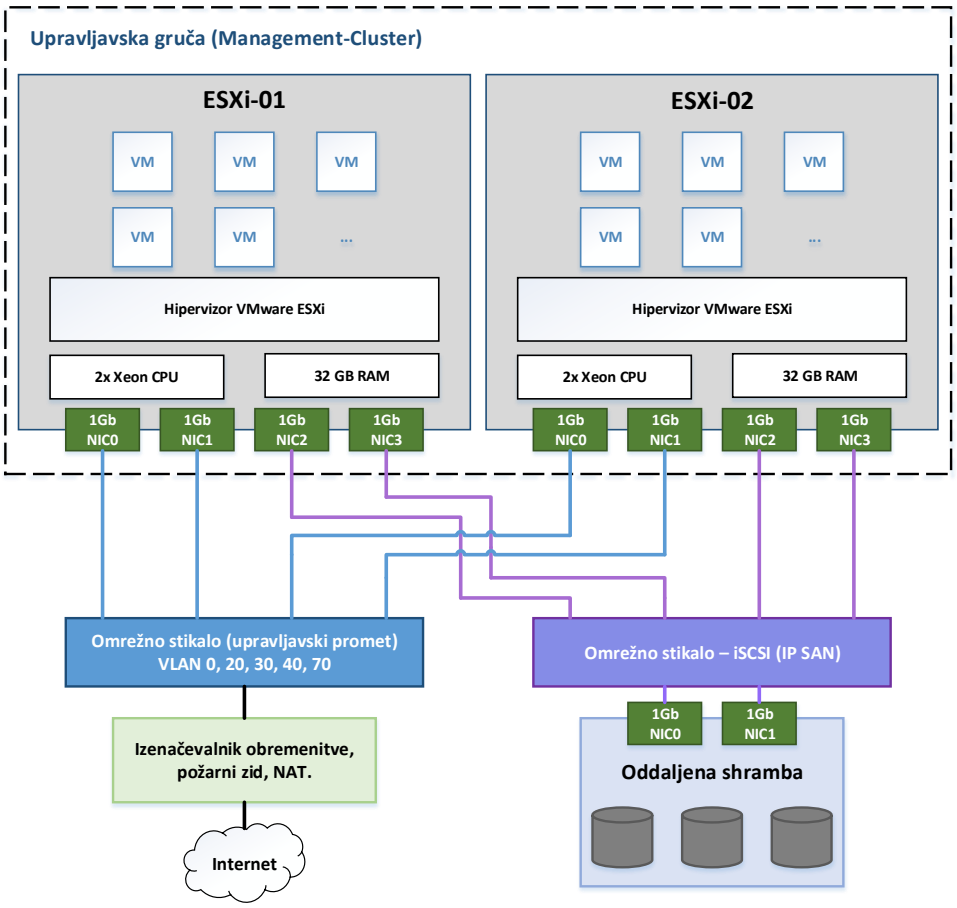
5.3.1.1 Fizična konfiguracija arhitekture

Slika 5.5 prikazuje fizično konfiguracijo omrežnih povezav gostiteljev znotraj upravljavske gruče v okviru testne postavitve privatnega oblaka z rešitvijo

vCloud. Slika prikazuje tako fizično konfiguracijo LAN omrežja kot tudi fizično konfiguracijo omrežja za dostop do oddaljene shrambe (IP SAN). Kot smo že omenili, je dobra praksa v primeru uporabe iSCSI oddaljene shrambe fizično ločevanje omrežja za shrambo od ostalih omrežij. Temu smo tudi sledili pri testni postavitvi, imamo namreč ločeno fizično stikalo za upravljavski promet ter ločeno stikalo za shrambo. Slednje ima še večji pomen v primeru, ko imamo hitrost povezave 1Gb ali manj. Zaželeno je, da stikalo podpira t.i. Jumbo Ethernet okvirje, z nastavitvijo velikosti MTU na 9000. S tem želimo preprečiti fragmentacijo okvirjev in posredno povečati zmogljivost omrežja. Paketi, ki se prenašajo vsebujejo SCSI ukaze, ki lahko presegajo privzete MTU velikosti 1500.

Fizično stikalo LAN omrežja je primarno namenjeno upravljavskemu prometu na katerega so povezane upravljavske komponente oblaka. Poleg tega se fizično omrežje uporablja tudi za nekatere druge tipe prometa kot so vMotion, vSphere FT, komunikacija med vozlišči v SQL gruči ter komunikacija med primarnim in sekundarnim vCenter strežnikom. Kljub temu, da uporabljamo deljeno fizično omrežje za različne namene, je vsak posamezen tip prometa na svojem izoliranem VLAN omrežju.

Na strani strežnikov znotraj upravljavske gruče imamo na vsakem strežniku štiri omrežne adapterje. Dva adapterja sta povezana v LAN omrežje in dva v IP SAN omrežje. Uporaba podvojenih adapterjev prinaša redundantno povezavo ter večjo prepustnost povezave (če je ustrezno konfigurirana). S tem želimo preprečiti enotne točke odpovedi na nivoju omrežnih povezav, vendar slednje velja zgolj na nivoju fizičnega stikala, kajti kot lahko vidimo s slike, imamo le eno fizično stikalo. Tako v primeru odpovedi stikala izgubimo omrežno povezavo do vseh gostiteljev in posledično tudi do vseh virtualnih strojev na tem fizičnem omrežju. Podobno velja za omrežnega stikala namenjeni shrambi. Enotno točko odpovedi na nivoju fizičnih stikal odpravimo z uporabo redundantnih stikal, vendar to prinese dodatne stroške. Na stopnjo redundance vplivajo različni faktorji. V razvojnem ali testnem okolju si lahko privoščimo manjšo stopnjo redundance, v primeru produkcijskega ali

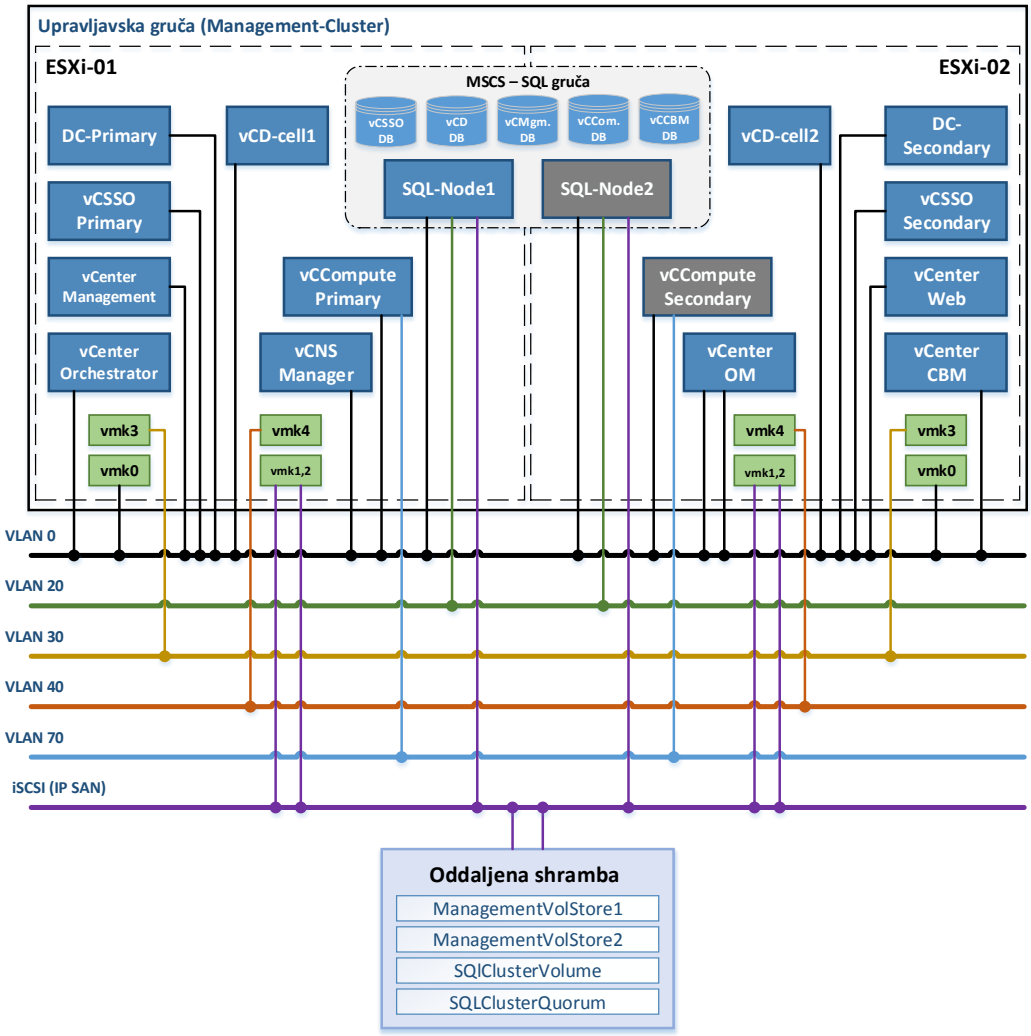


Slika 5.5: Fizična konfiguracija omrežnih povezav.

poslovno kritičnega okolja pa uporabljamo višjo stopnjo redundance.

5.3.1.2 Logična konfiguracija arhitekture

Logična konfiguracija prikazuje arhitekturo z vidika virtualnih strojev znotraj upravljavske gruče, na katerih so nameščene posamezne upravljavske komponente. Slika 5.2 prikazuje vse komponente, ki se izvajajo znotraj upravljavske gruče, v primeru testne postavitve privatnega oblaka. Poleg tega prikazuje vsa logična omrežja preko katerih se komponente povezujejo. Prikazana logična omrežja na sliki predstavljajo skupine vrat na porazdeljenem stikalu virtualizacijske platforme, ki so bodisi izolirana v svojem VLAN-u bo-



Slika 5.6: Logična konfiguracija arhitekture.

disi na ločenem fizičnem omrežju, kot je omrežje iSCSI (IP SAN). Povezava samih gostiteljev do ustreznih omrežij je za določene tipe prometa je izvedena preko virtualnih omrežnih adapterjev (vmk 0 do 4). Pri tem vmk0 povezuje gostitelje na upravljavskem omrežju. Za povezavo do oddaljene shrambe se uporabljata vmk 1 in 2, ki sta na sliki združena zaradi boljši preglednosti. Za vMotion se uporablja vmk 3 in za vSphere FT vmk 4. Posamezni tipi omrežnih prometov so ločeni med seboj, kar je na splošno dobra praksa ne glede na izbrano rešitev.

Določene komponente prikazane na sliki se izvajajo redundantno. Komponenta vCloud Director vsebuje dve celici, ki jih je treba izpostaviti preko izenačevalnika obremenitev, saj se ne izvajata v gruči s samodejnim preklopom v primeru odpovedi celice. Podobno velja tudi za komponento vCenter SSO. Razpoložljivost upravljavskega nivoja se za delovne obremenitve zagotovi s komponent vCenterCompute, ki se izvaja v redundanci z uporabo vCenter Server Heartbeat. Komponenta vCenter Compute (vCCompute Primary ter vCCompute Secondary na sliki) ima poleg dostopa do upravljavskega omrežja dostop tudi do izoliranega omrežja z VLAN ID-jem 70. Slednje se uporablja za interni promet med primarnim ter sekundarnim vozliščem komponente. Razpoložljivost podatkovnih baz je dosežena z izvajanjem dveh SQL strežnikov v gruči. Podobni koncept velja tudi v primeru SQL gruče. Vozlišča v gruči imajo (v tem primeru dve) dostop do ločenega logičnega omrežja za interno komunikacijo. V primeru SQL gruče potrebujemo še dostop do oddaljene shrambe, kajti podatki podatkovnih baz morajo biti shranjeni na lokaciji, ki je vidna iz vsem SQL strežnikom v gruči.

Ker se znotraj upravljavske gruče, kjer imamo več strežnikov, nekatere komponente izvajajo redundantno (podvojeno), je potrebno preprečiti izvajanje primarnega in sekundarnega vozlišča komponente na istem gostitelju, saj je v tem primeru gostitelj enotna točka odpovedi in redundantno izvajanje komponente nima dodane vrednosti. Mehanizmi s katerimi lahko to zagotovimo so odvisni od izbrane rešitve. V primeru rešitve vCloud bomo to naslovili pri implementaciji arhitekture.

Slika 5.2 prikazuje tudi logični vidik shrambe. Za shranjevanje upravljavskih komponent ter podatkov imamo na voljo logične enote ManagementVolStore 1 in 2. Za namene SQL gruče imamo za shranjevanje podatkov logično diskovno enoto SQLClusterVolume ter za interne potrebe logično diskovno enoto SQLClusterQuorum. Ker je število vozlišč v gruči sodo število, potrebujemo dodatno logično diskovno enoto za ugotavljanje sklepčnosti (ang. Quorum Witness).

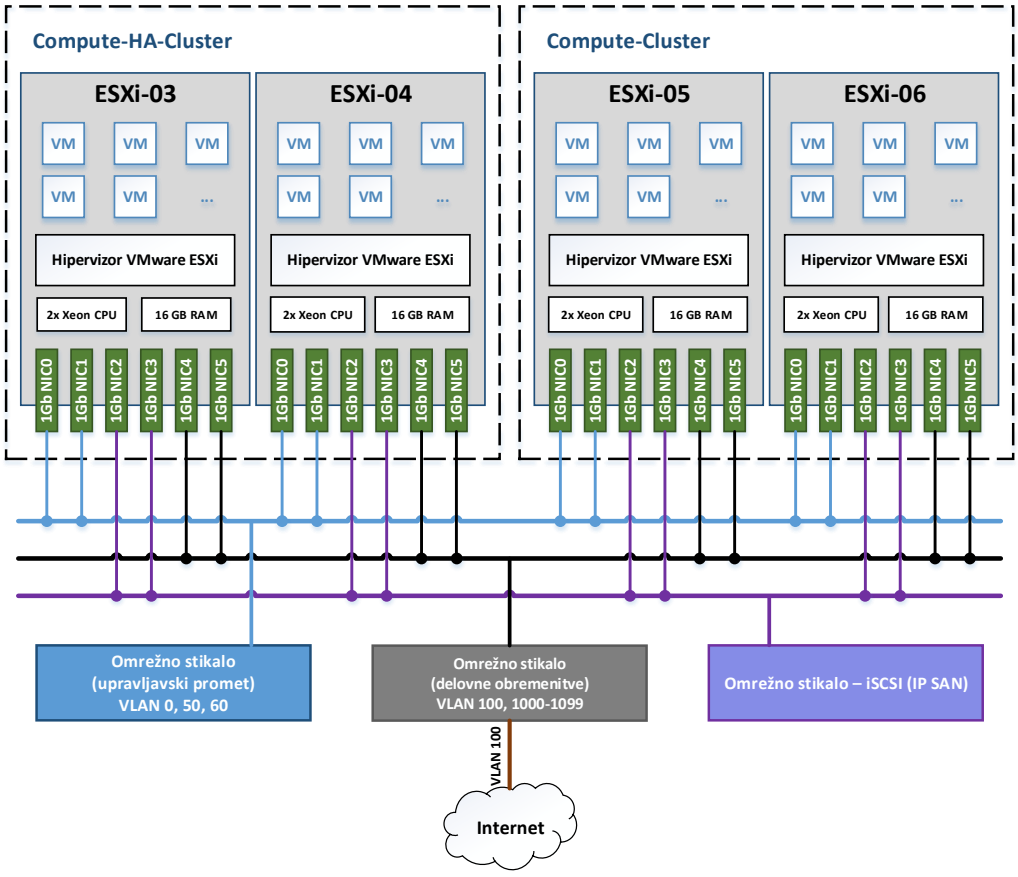
5.3.2 Arhitektura skupine virov za izvajanje delovnih obremenitev

Arhitektura skupine virov, v primerjavi z upravljavskim delom, ne vsebuje nobenih dodatnih upravljavskih komponent, saj so viri izključno namenjeni izvajanju delovnih obremenitev. Idealna oblika postavitve je uporaba ločenega vCenter strežnika za upravljanje skupine virov. S tem se poveča skalabilnost arhitekture (vCenter ima določene maksimalne priporočene velikosti infrastrukture [26]). Komponenta vCenter strežnik je namenjena upravljanju skupine virov in je integracijska točka za komponente vCloud Director. Vse zahteve za oskrbo virov se indicirajo s strani komponente vCloud Director in se posredujejo naprej do ustreznega vCenter strežnika (saj imamo lahko več vCenter strežnikov s katerimi dela vCloud Director).

Pri testni postavitvi smo sledili dobrim praksam pri načrtovanju arhitekture za skupino virov. Uporabili smo ločen vCenter strežnik (vCenter Compute), ki je prikazan na sliki 5.6.

5.3.2.1 Fizična konfiguracija arhitekture

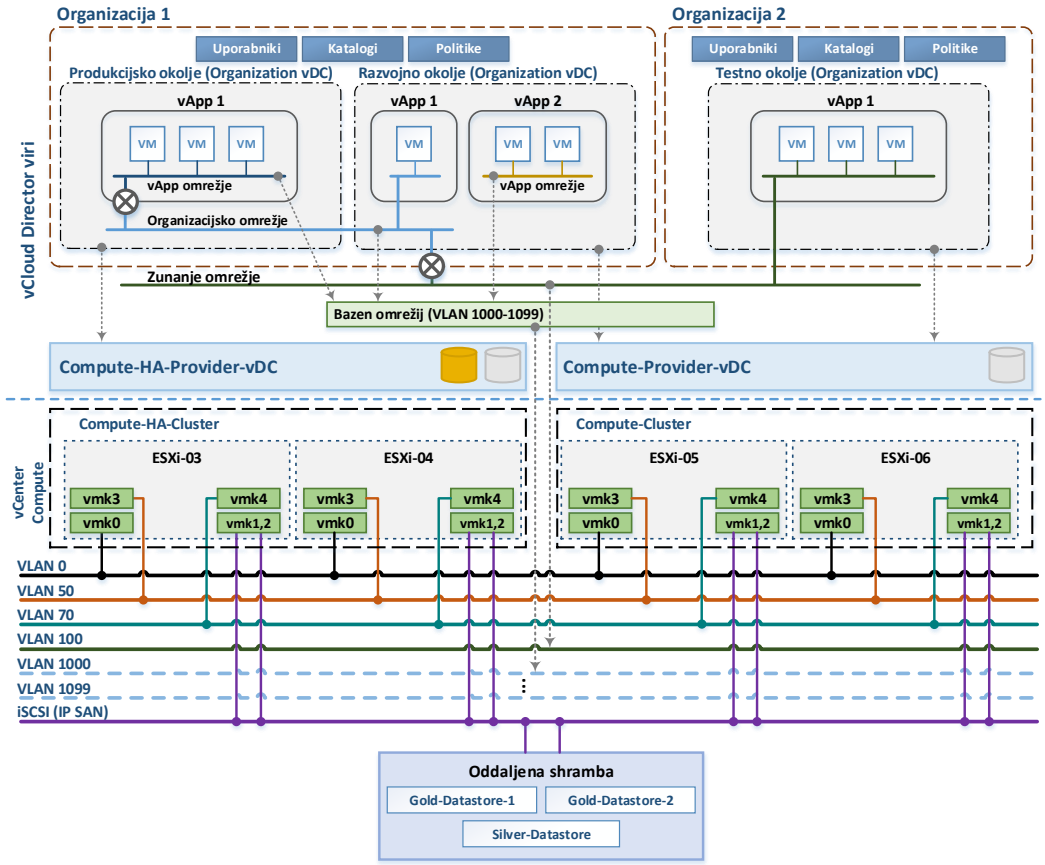
Slika 5.7 prikazuje fizično konfiguracija gostiteljev znotraj posamezne gruče ter fizičnih omrežnih povezav. Kot lahko opazimo na sliki imamo poleg upravljavskega omrežja ter omrežja za shrambo dodatno ločeno fizično omrežje. Namenjeno je izključno delovnim obremenitvam, ki se izvajajo na gostitelju. Na fizičnem stikalu za delovnih obremenitev so konfigurirana tudi ustrezna VLAN omrežja. V primerjavi s fizično konfiguracijo upravljavskih gostiteljev imajo tukaj gostitelji dva dodatna omrežna adapterja NIC4 in NIC5. Povezana sta izključno na fizično stikalo za delovne obremenitve. Preko fizičnega stikala je na voljo tudi dostop do javnega omrežja z uporabo ustreznega VLAN omrežja. To je namenjeno dostopu delovnih obremenitev do javnega omrežja. Ostala konfiguracija je podobna kot, pri upravljavskem delu.



Slika 5.7: Fizična konfiguracija arhitekture.

5.3.2.2 Logična konfiguracija arhitekture

Logično konfiguracijo arhitekture skupine virov lahko razdelimo na dva dela. Prvi del predstavljajo virtualizacijski viri s katerimi upravlja vCenter, drugi del arhitekture pa predstavlja le logična reprezentacija (vCloud Director viri) spodnje nivojskih virov (vSphere viri). Z logično reprezentacijo spodnje nivojskih virov upravlja vCloud Director. Logična konfiguracija arhitekture testne postavitve privatnega oblaka je prikazana na sliki 5.8. Spodnji del arhitekture je kot lahko opazimo podoben logični arhitekturi upravljavskega dela. Razlika je ta, da imamo dve gruči z dvema gostiteljema. Prva zagotavlja visoko razpoložljivost z uporabo vSphere HA, druga pa ne. Razpored virtualnih omrežnih adapterjev je podoben kot v primeru upravljavskega



Slika 5.8: Logična konfiguracija arhitekture.

dela. Razlika je ta, da se za vMotion in vSphere FT uporabljajo različna VLAN omrežja kot pri upravljavskem delu. Povezava gostiteljev do oddaljene shrambe je izvedena podobno kot pri upravljavskem delu, vendar gostitelji virtualizacije znotraj skupine virov nimajo dostopa do logične diskovne enote namenjene upravljavskem delu. Za shranjevanje virtualnih strojev na katerih se izvajajo delovne obremenitve imajo gostitelji dostop do ločenih logičnih diskovnih enot. Logične diskovne enote so lahko na istem fizičnem diskovnem polju z logičnimi diskovnimi enotami za upravljavske komponente, vendar je dobra praksa uporaba ločenih fizičnih diskovnih polj.

Drugi, zgornji del logične konfiguracije arhitekture na sliki predstavljajo

vCloud Director viri. Osnovni gradnik na nivoju komponente vCloud Director je ponudnik virtualnih podatkovnih centrov - PVPC, ki smo ga analizirali v sklopu komponente vCloud Director v poglavju 4. V našem primeru postavitve privatnega oblaka imamo dva PVPC-ja. Prvi PVPC (Compute-HA-Provider-vDC na sliki) je logična reprezentacija gruče (Compute-HA-Cluster) na spodnjem nivoju. Drugi PVPC pa je logična reprezentacija gruče Compute-Cluster na spodnjem nivoju. Prvi PVPC - Compute-HA-Provider-vDC vsebuje klasificirano shrambo Gold-storage, ki vsebuje podatkovne shrambe podprte s strani logične diskovne enote Gold-Datastore 1 in 2. Poleg tega vsebuje tudi klasificirano shrambo Silver-storage, ki vsebuje podatkovno shrambo, katera temelji na logični diskovni enoti Silver-Datastore. Drugi PVPC vsebuje le shrambo Silver-storage. PVPC lahko temelji na eni gruči ali na bazenu virov znotraj ene gruče. Druga opcija omogoča, da imamo več PVPC-jev na eni gruči. V praksi je boljše, da PVPC temelji na nivoju gruče, saj slednje poenostavi upravljanje virov [26]. Druga možnost se izkaže za uporabno, ko imamo omejeno velikost infrastrukture.

Zagotavljanje omrežnih povezljivosti na različnih omrežnih nivojih je v okviru komponente vCloud Director izvedeno preko bazenov omrežij ter zunanjih omrežij. Razvidno iz slike imamo en bazen omrežij, ki temelji na VLAN logičnemu segmentiranju omrežij. V konkretnem primeru se uporabljajo omrežja z VLAN identifikatorji od 1000 do 1099. Logična omrežja v bazenu predstavljajo skupine vrat na nivoju virtualizacijske platforme. Kreiranje in odstranjevanje logičnih omrežij je dinamično in se izvede na zahtevo. Povezava med posameznimi organizacijami poteka preko zunanjih omrežij. Zunanja omrežja lahko omogočajo tudi dostop do interneta. S tem se omogoči vzpostavitev VPN povezave do organizacije v oblaku. V konkretnem primeru postavitve imamo eno zunanje omrežje, ki je logična reprezentacija skupine vrat na nivoju virtualizacijske platforme z ustreznim VLAN identifikatorjem. Uporablja se logično omrežje z VLAN identifikatorjem 100.

Na najvišjem nivoju, tudi nivoju končnih uporabnikov/najemnikov oblaka, imamo dve organizacije. Prva organizacija ima dva organizacijska virtualna

podatkovna centra - OVPC. Prvi OVPC (Produkcijsko okolje) je alociran na prvem (Compute-HA-Provider-vDC) PVPC-ju ter vsebuje eno vApp enoto. Drugi OVPC (Razvojno okolje) je alociran na drugem PVPC, ki ne zagotavlja izvajanja v visoko razpoložljivem načinu. Druga organizacija vsebuje en OVPC, alociran na drugem PVPC. Prva organizacija ima organizacijsko omrežje, ki povezuje vApp enote iz obeh OVPC. Organizacijsko omrežje je alocirano iz bazena omrežij. Pri kreiranju se dodeli ustrezen prost VLAN (v obsegu od 1000 do 1099). Kreira se skupina vrat na nivoju virtualizacijske platforme. V primeru vApp omrežij je koncept podoben, le da velja znotraj ene vApp enote. Za omrežno varnost v okviru organizacije skrbi komponenta vCNS. Za vsako logično omrežje se namreč lahko postavi vCNS Edge napravo (virtualni stroj), ki zagotavlja programsko definirane omrežne storitve in varnost. Komponento smo podrobneje analizirali v okviru poglavja 4.

5.4 Implementacija zasnovane arhitekture privatnega oblaka

Implementacije arhitekture se lahko lotimo po ustrezno izdelanem načrtu arhitekture, kjer so jasno definirani cilji in smernice. Implementacija v osnovi predstavlja konfiguracijo fizične infrastrukture, namestitev posamezne komponente glede na ustrezno izdelan načrt, konfiguracijo nameščenih komponent ter realizacijo na začetku definiranih storitev. Konfiguracija fizične infrastrukture v grobem zajema pripravo strežnikov, konfiguracijo fizičnih stikal, konfiguracijo oddaljene shrambe ter vzpostavitev omrežnih povezav.

Namestitev in konfiguracija komponent rešitve vCloud je izvedena v skladu z načrtom. V prvi fazi je izvedena implementacija upravljavskega dela, kjer se izbrane komponente namestijo in ustrezno konfigurirajo glede na zastavljeno konfiguracijo v načrtu. Druga faza je implementacija drugega dela arhitekture za izvajanje delovnih obremenitev. Implementacija obsega namestitev in konfiguracijo virtualizacijske platforme ter konfiguracijo komponente vCloud Director.

5.4.1 Implementacija upravljavskega dela arhitekture

Izhodišče implementacije upravljavskega dela arhitekture je namestitev in konfiguracija virtualizacijske platforme. Slednje je predpogoj za izvajanje virtualnih strojev na katerih so nameščene komponente za upravljanje oblaka.

Namestitev virtualizacijske platforme zahteva namestitev hipervizorja neposredno na fizične strežnike ter konfiguracijo hipervizorja (določanje IP naslovov, virtualni omrežni adapterji za upravljavsko omrežje). Namestitev je možna tako na lokalni shrambi kot tudi na oddaljeni, če fizični strežnik podpira Boot from SAN. V primeru namestitve na lokalno shrambo je zaželena namestitev na diskovno polje RAID 1 ali podobno konfiguracijo, ki zagotavlja določeno stopnjo redundantnosti podatkov. Po namestitvi je konfiguracija izvedena delno preko neposrednega dostopa do konzole strežnika ter delno preko namizne aplikacije vSphere Client. Po začetni konfiguraciji gostitelja je potrebna konfiguracija dostopa do oddaljene shrambe za namene shranjevanja virtualnih strojev. Konfiguracija zajema kreiranje ustreznih virtualnih omrežnih adapterjev (vmk-ji na sliki 5.6) ter konfiguracijo programskega iSCSI krmilnika. Po uspešni povezavi na oddaljeno shrambo je potrebno narediti podatkovne shrambe iz dosegljivih logičnih diskovnih enot, ki so vnaprej konfigurirane na oddaljeni shrambi.

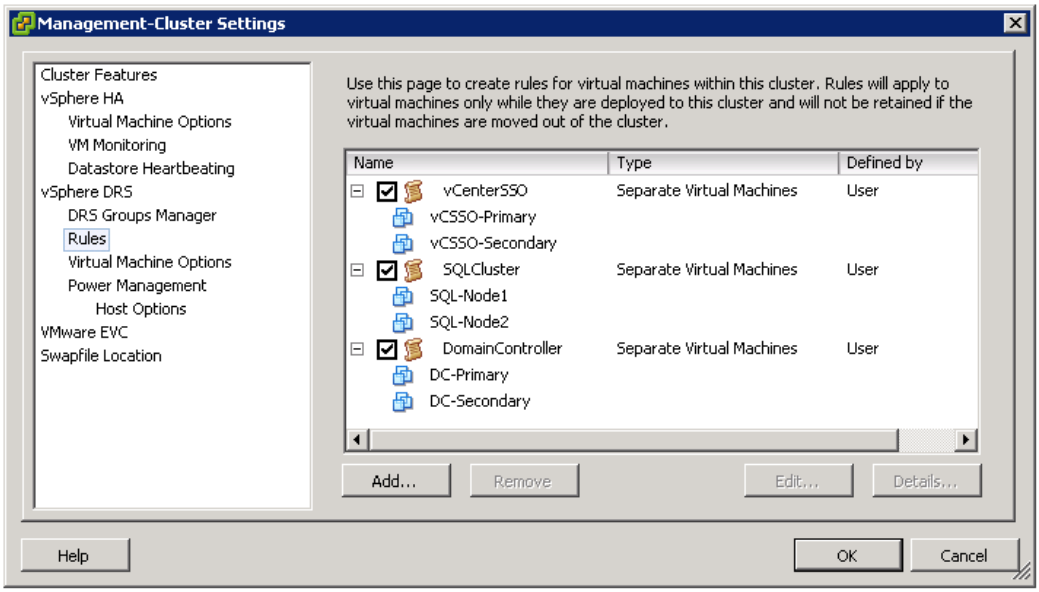
Za namestitev komponente vCenter potrebujemo dodatne infrastrukturne komponente in sicer domenskega nadzornika z vzpostavljeno domeno ter strežnik podatkovne baze. Poleg teh je predpogoj tudi ustrezna namestitev komponente vCenter SSO. V primeru, da se uporabi že obstoječi domenski nadzornik in strežnik podatkovne baze s podprto instanco, se ustrezno lete konfigurirajo za potrebe ostalih komponent. V nasprotnem primeru, ko vzpostavljamo popolnoma novo okolje, je potrebno pripraviti virtualne stroje za domenskega nadzornika ter podatkovne baze za ostale komponente. Slednje velja, če se odločimo za virtualizirano postavitev. Za bolj učinkovito in hitrejšo pripravo virtualnih strojev je možno uporabiti orodje VMware Studio [31], ki nam omogoča pripravo OVF predlog. Na predlogi je nameščen

in ustrezno posodobljen operacijski sistem. Po namestitvi primarnega ter sekundarnega nadzornika konfiguriramo potrebne uporabnike ter skupine. Dobra praksa je, da glede na določen segment arhitekture pripravimo različne varnostne skupine, kot na primer vCenter administratorji, vCloud administratorji, itd. Po namestitvi domenskega nadzornika se lahko lotimo priprave virtualnih strojev za primarni ter sekundarni SQL strežnik. Konfiguracija SQL gruče zahteva konfiguracijo dostopa do oddaljene deljene shrambe ter konfiguracijo omrežja med vozlišči v gruči. Po namestitvi SQL Server instanc na obe vozlišči lahko pripravimo podatkovne baze za posamezne komponente, ki jih potrebujejo. Potrebne podatkovne baze so prikazane na sliki 5.6.

Komponento vCenter SSO lahko namestimo na ločen ali isti virtualni strežnik, kot tudi na vCenter Server. Bolj priporočljiva oblika je postavitev na ločenem virtualnem strežniku, saj se s tem zagotovi največja fleksibilnost. Po ustrezno nameščeni komponenti vCenter SSO sledi namestitev komponente vCenter Server ter komponente vCenter Server Web Client.

Konfiguracija komponente vCenter Server je po namestitvi možna preko spletnega odjemalca ali preko aplikacije vSphere Client. Začetna konfiguracija zahteva dodajanje gostiteljev, ki so namenjeni upravljavskemu delu (v konkretnem primeru testne postavitve privatnega oblaka sta dodana gostitelja ESXi-01 ter ESXi-02). Kot smo načrtovali v zasnovani arhitekturi sta oba gostitelja dodana v upravljavsko gručo (Management-Cluster). Gruča je konfigurirana kot HA ter DRS gruča. Ker so nekatere komponente postavljene redundantno, je potrebno zagotoviti mehanizem, ki bo preprečil izvajanje primarne ter sekundarne komponente na istem fizičnem gostitelju znotraj gruče. Slednje lahko dosežemo z definiranjem anti-afinitetnih pravil na nivoju gruče.

Konfigurirana anti-afinitetna pravila v primeru testne postavitve privatnega oblaka prikazuje slika 5.9. Po konfiguraciji upravljavske gruče je potrebna omrežna konfiguracija za omogočanje ostalih porazdeljenih storitev (vMotion, vSphere FT). Kljub izvedljivosti konfiguracije na standardnem stikalu je bolj smiselno uporabiti porazdeljeno stikalo. Končna konfigura-



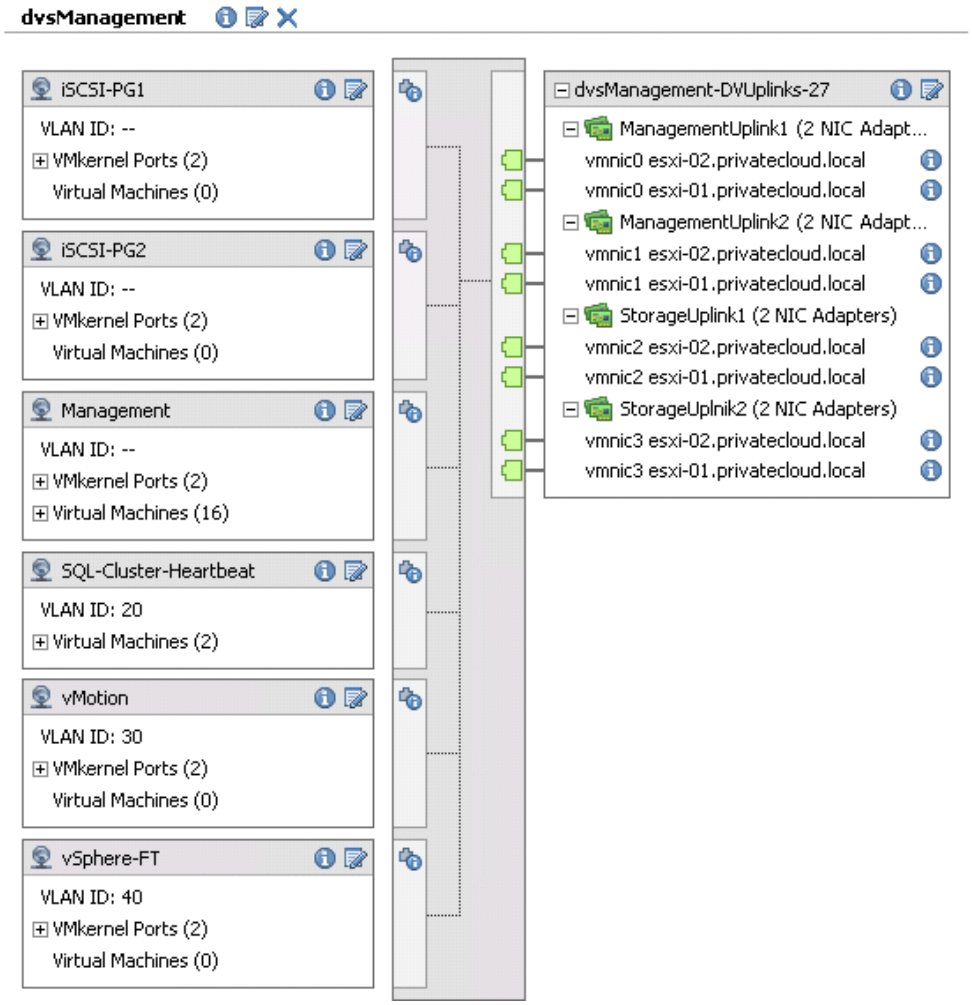
Slika 5.9: DRS anti-afinitetna pravila.

cija omrežnega stikala v primeru testne postavitve je prikazana na sliki 5.10. Kot je razvidno iz slike, konfiguracija porazdeljenega stikala ustreza logični konfiguraciji na sliki 5.6.

Po ustrezni konfiguraciji vCenter strežnika namenjenega upravljanju virtualizacijske platforme upravljavskega dela, sledi namestitev vCenter strežnika za upravljanje virtualizacijske platforme in izvajanje delovnih obremenitev. Konfiguracija pa je izvedena v okviru druge faze implementacije. Namestitev je izvedena na redundantni par primarnega ter sekundarnega vCenter strežnika, ter je ustrezno definirano anti-afinitetno pravilo na gruči. Pri namestitvi je izbrani tip namestitve v povezanem načinu z vCenter strežnika namenjenega upravljavskemu delu.

Namestitev komponente vCNS je možna s postavitvijo OVF predloge na kateri je komponenta že nameščena, potrebna je le še njena konfiguracija. Konfiguracija zajema nastavitve povezave z vCenter strežnikom, ki je namenjen komponenti vCloud Director.

Za namestitev in konfiguracijo preostalih komponent zgolj sledimo ustrezni dokumentaciji. Konfiguracija preostalih komponent, specifičnih za arhi-



Slika 5.10: Konfiguracija porazdeljenega stikala.

tekturo, ni potrebna.

5.4.2 Implementacija arhitekture skupine virov

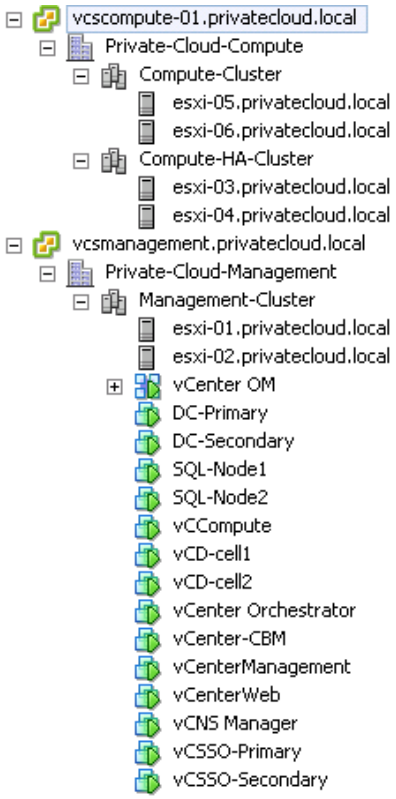
Izhodišče druge faze, to je implementacija arhitekture skupine virov, predstavlja namestitev in konfiguracija ESXi hipervizorja na fizičnih strežnikih. Ker skupina virov v večini primerov vsebuje bistveno več gostiteljev kot upravljavski del, klasična namestitev in konfiguracija postane neobvladljiva. Poleg tega je v velikem okolju težko zagotoviti ustrezno skladnost z določenimi

nastavitvami konfiguracije. Rešitev problema v primeru rešitve vCloud je uporaba Auto Deploy strežnika [32], ki omogoča avtomatizirano postavitev in konfiguracijo gostiteljev na fizičnih strežnikih.

Po namestitvi ter začetni konfiguraciji gostiteljev je potrebna konfiguracija že nameščenega vCenter strežnika, namenjenega komponenti vCloud Director. Konfiguracija je izvedena v skladu z zasnovano arhitekturo. V okviru konfiguracije virtualizacijske platforme je izvedeno kreiranje gruč Compute-Cluster ter Compute-HA-Cluster skladno z načrtom arhitekture. Druga gruča je konfigurirana kot HA gruča. DRS je omogočen v obeh primerih. Konfiguracija omrežja zahteva pripravo dveh porazdeljenih stikal. Prvo stikalo vsebuje fizične omrežne adapterje za upravljavski promet ter iSCSI promet. Drugo stikalo vsebuje adapterja povezana na fizičnem omrežju za delovne obremenitve. Poleg priprave porazdeljenih stikal, je potrebno na nivoju shrambe definirati še klasifikacije podatkovnih shramb na podlagi definiranih zmožnosti shrambe. Pri tem smo definirali klasifikacijo shrambe in sicer Gold-storage ter Silver-storage.

Slika 5.11 prikazuje celotno virtualizacijsko platformo: vCenter strežnik namenjen upravljanju ter vCenter strežnik namenjen komponenti vCloud Director. Kot je razvidno iz slike, virtualizacijski nivo okolja ustreza zasnovani arhitekturi.

Po ustrezno pripravljenem virtualizacijskem nivoju sledi začetna konfiguracija komponente vCloud Director. Prva faza konfiguracije komponente vCloud Director zajema ustrezno nastavitev sistemskih parametrov, integracijo z LDAP strežnikom (v našem primeru je to postavljen Active Directory), konfiguracijo poštnih strežnikov itd. Druga faza konfiguracije komponente vCloud Director pa zajema pripravo sistema za sprejem delovnih obremenitev. Šele s tem se komponenta funkcijsko omogoči. Začetek priprave sistema predstavlja dodajanje osnovnih gradnikov, in sicer PVPC-jev, skladno z načrtom. V konkretnem primeru je to PVPC Compute-HA-Provider-vDC, ki se navezuje na gručo Compute-HA-Cluster. Pri tem smo izbrali tudi ustre-



Slika 5.11: Pregled konfiguriranih virov na nivoju virtualizacijske platforme.

zno klasificirano shrambo za vsak posamezni PVPC. Na nivoju omrežja je potrebno konfigurirati bazen omrežij ter zunanjih omrežij. Konfiguracija zunanjih omrežij zahteva izbiro skupine vrat, ki ima ustrezno internetno povezavo. Kot smo predstavili v poglavju 4 imamo pri dodajanju bazena omrežij v okviru obravnave komponente vCloud Director na izbiro tri tipe. Bazenu omrežij, ki temelji na že pripravljeni skupini vrat, se izogibamo, saj ne ponuja elastičnosti (vse skupine vrat so vnaprej pripravljene). Bazen omrežij, ki temelji na MAC-in-MAC enkapsulaciji se uporablja le takrat, ko nimamo dovolj velikega števila VLAN-ov, saj je počasnejši kot bazen omrežij na osnovi VLAN-ov.

Končna faza konfiguracije komponente vCloud Director predstavlja kreiranje ene sistemske organizacije. Cilj sistemske organizacije je priprava glavnega kataloga, ki je na voljo vsem ostalim organizacijam. Katalog vsebuje

pripravljene vApp predloge, ki vsebujejo virtualne stroje, na katerih je lahko že nameščena in konfigurirana določena programska oprema.

5.4.3 Realizacija definiranih storitev oblaka

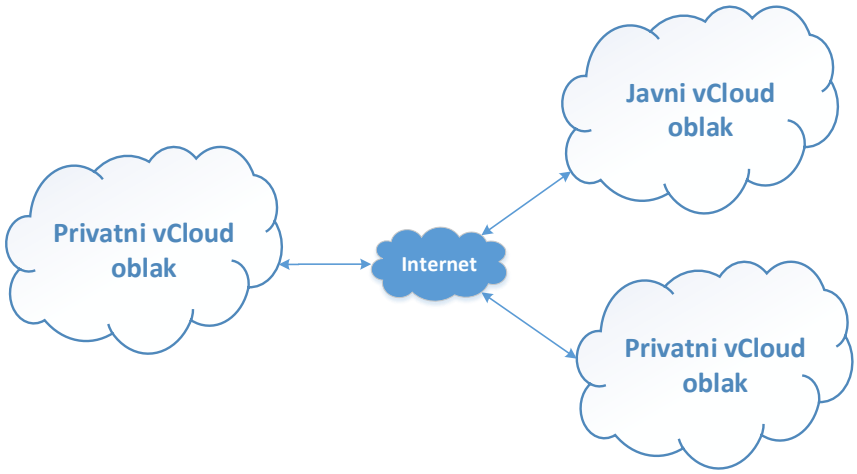
Realizacijo definiranih storitev v osnovi obliki predstavlja priprava ustreznih predlog vApp. V našem primeru so to predloge vApp, ki vsebujejo virtualne stroje z že nameščenim operacijskim sistemom. Predloge vApp ustvarimo z dodajanjem ustrezne enote vApp iz sistemske organizacije v ciljnem katalogu. Iz tako pripravljenih predlog se lahko uporabniki ostalih organizacij samo-oskrbijo s potrebnimi virtualnimi stroji. Na teh virtualnih strojev je že nameščen potreben operacijski sistem, ki ga ni potrebno vedno znova nameščati in konfigurirati. Velikokrat pa vendarle želimo realizirati kompleksnejše višje nivojske storitve, kot na primer avtomatizirano postavitev aplikacijskih strežnikov, spletnih strežnikov, podatkovnih baz, itd. Poleg tega lahko realiziramo tudi kombinacijo storitev, kot na primer storitve, ki vsebujejo gručo aplikacijskih strežnikov, podatkovne baze, ter izenačevalnik obremenitve. Realizacijo bolj kompleksnih storitev realiziramo s pomočjo orkestracijskih orodij, kjer posamezne procese orkestriramo v celoto. Po postavitvi posameznih virtualnih strojev znotraj vApp enote je namreč potrebna dodatna konfiguracija, ki izvede kontekstualizacijo storitev glede na specificirane parametre s strani uporabnika. V primeru rešitve vCloud je to komponenta vCenter Orchestrator.

Poglavje 6

Vzpostavitev hibridne platforme

V poglavju 6 smo obravnavali vzpostavitev arhitekture privatnega oblaka. Vzpostavljena arhitektura privatnega oblaka v okviru ene poslovne organizacije zagotavlja IaaS storitev končnim uporabnikom/najemnikom tega oblaka. Izključno zasebna postavitev oblaka se lahko v določenih primerih izkaže kot stroškovno neučinkovita. Izhodno strategijo v takšnih primerih predstavlja hibridna postavitev oblaka.

Hibridni oblaki prinašajo unikatno prednost uporabe storitev v oblaku, saj združujejo prednosti iz okolja privatnega oblaka in javnega oblaka. Okolje privatnega oblaka ponuja zagotovilo in nadzor nad delovanjem vzdrževanih sistemov, kot tudi enostavnejšo implementacijo strožjih zahtev uporabe storitev v oblaku, kar še posebej velja poudariti ob občutljivih podatkih in storitvah. Kljub prednosti relativno nizkih stroškov implementacije in vzdrževanja privatnega oblaka le-ta še vedno predstavlja nezaželene stroške vzdrževanja neizkoriščenih virov privatnega oblaka. Ti viri so na voljo v izkoristek ob predvidenih in nepredvidenih obremenitvah. Te obremenitve lahko predstavljajo vzdrževalna dela ali povečane potrebe po infrastrukturnih kapacitetah obremenjenih storitev. Da bi se izognili večjemu deležu neizrabljenih infrastrukturnih kapacitet privatnega oblaka, vedno več organizacij po svetu im-



Slika 6.1: Koncept hibridnega oblaka z uporabo VMware vCloud.

plementira hibridne platforme. Te omogočajo prenos delovnih obremenitev med privatnim oblakom in javnim oblakom. To se praviloma izvaja predvsem z razlogom stroškovne optimizacije, saj so stroški uporabe storitev javnega oblaka, kjer se infrastrukturni viri običajno plačajo po porabi, neprimerno nižji lastnini večjih delov neizkoriščene infrastrukture v zasebnem oblaku.

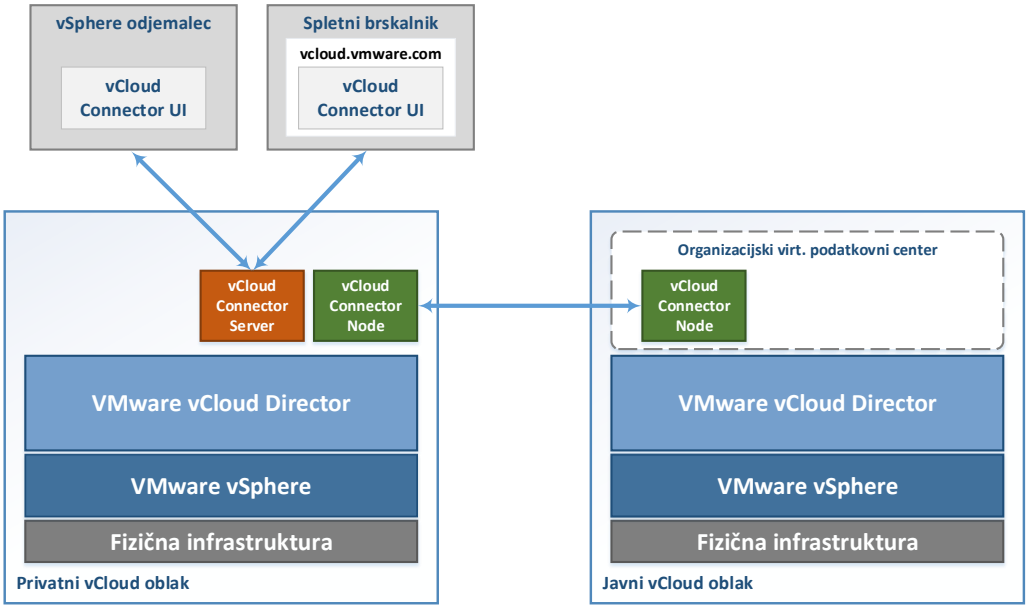
6.1 Implementacija hibridne platforme z uporabo rešitve vCloud

Poglavje podaja opis realizacije hibridne platforme v primeru privatnega oblaka implementiranega z uporabo rešitve VMware vCloud. Koncept hibridnega oblaka z uporabo rešitve vCloud omogoča dinamičen prenos delovnih obremenitev med zasebnim ter javnim oblakom in obratno, kot to ponazarja slika 6.1.

Privatni oblak predstavlja zasebno postavitev nabora komponent iz rešitve vCloud, ki smo ga obravnavali pri vzpostavitvi arhitekture privatnega oblaka v poglavju 5. Javni oblak vCloud predstavlja vCloud Director organizacijo, ki ima vire dodeljene v obliki virtualnih podatkovnih centrov s strani ponudnika

javnega oblaka. Poleg povezave privatnega in javnega oblaka je mogoča povezava tudi med dvema privatnima vCloud oblakoma. Prvi scenarij je v praksi bolj razširjen kot drugi in je zaradi tega tudi bolj zanimiv za obravnavo. Cilj hibridne platforme je omogočiti potencialno razbremenitev kapacitet v zasebnem oblaku ob določenih tako napovedanih kot tudi nenapovedanih obdobjih, kadar so zahtevane kapacitete večje, kot bi jih lahko zasebni podatkovni center zagotovil za nemoteno izvajanje računalniških storitev. Prerazporeditev lahko realiziramo s pomočjo migracije delovnih obremenitev k enemu izmed ponudnikov javnih vCloud oblakov. Migracija delovnih obremenitev je mogoča v obeh smeri. Storitev, ki se izvaja v zasebnem vCloud oblaku lahko migriramo v javni vCloud oblak [33]. Prav tako lahko storitev, ki se izvaja v javnem vCloud oblaku migriramo nazaj v zasebno postavitev oblaka.

Vzpostavitev povezave med privatnim in javnim oblakom ter realizacija hibridne platforme je možna na več načinov. Kot bomo videli v nadaljevanju je eden izmed načinov realizacije uporaba komponente vCloud Connector [21]. Ta zagotavlja in skrbi za prenos delovnih obremenitev med zasebno postavitvijo rešitve vCloud ter javno in obratno [26]. Kljub temu, da je realizacija hibridne platforme z uporabo komponente vCloud Connector enostavna, se izkaže, da je trenutna različica komponente precej omejena, saj ne omogoča razširljivost, kar pa je ključnega pomena. Poleg razširljivosti komponenta ne zagotavlja določenih bolj naprednih funkcionalnosti, kot je na primer dinamična postavitev novih delovnih obremenitev glede na trenutno stanje v privatnem in javnem oblaku, samodejna optimizacija obremenitev med zasebno postavitvijo oblaka ter javno postavitvijo oblaka. Ker ne ponuja programskih vmesnikov, ni načina programske uporabe osnovne funkcionalnosti, ki jih zagotavlja. Alternativa podane rešitve je razvoj lastne rešitve, ki implementira hibridno platformo z uporabo orodij in ustreznih programskih vmesnikov, s programskim dostopom do rešitve vCloud. Takšna orodja so VMware vCenter Orchestrator, vCloud API, vSphere API itd.



Slika 6.2: Visokonivojska arhitektura hibridnega oblaka.

6.1.1 Arhitektura hibridne platforme

Kot smo omenili je ena izmed rešitev implementacije hibridne platforme komponenta vCloud Connector. Osnovna funkcionalnost komponente je prenos delovnih obremenitev med zasebno postavitvijo vCloud oblaka ter javno in obratno. Delovne obremenitve oblaka v okviru vCloud predstavljajo vApp enote. V primeru, da je vApp sestavljen iz več virtualnih strojev, se pri migraciji z uporabo komponente vCloud Connector prenesejo vsi virtualni stroji v okviru ene operacije.

Slika 6.2 prikazuje visokonivojsko arhitekturo hibridne platforme ter ključne komponente, ki sestavljajo hibridno platformo. Na sliki smo izpustili ostale komponente zaradi boljše preglednosti. Kot lahko vidimo, je hibridna platforma sestavljena iz privatne postavitve rešitve vCloud ter javne in ustrezno povezavo med njima z uporabo komponente vCloud Connector. Implementacija hibridne platforme z uporabo komponente vCloud Connector zahteva ustrezno pripravo okolja, namestitev komponente ter konfiguracijo.

Kot je razvidno z visoko nivojske arhitekture, je vCloud Connector sestavljen iz več podkomponent in sicer:

- **vCloud Connector Server:** Že pripravljen virtualni stroj, ki se ga namesti z uporabo OVF predloge. Skrbi za upravljanje posameznih vCloud Connector vozlišč, ki so postavljeni v posamezne oblake med katerimi želimo vzpostaviti povezavo. Za hibridno platformo je potreben le en vCloud Connector Server.

- **vCloud Connector Node:** Prav tako v obliki že pripravljenega virtualnega stroja, ki se ga namesti z uporabo OVF predloge. Število vCloud Connector vozlišč je odvisno od števila oblakov, ki jih želimo povezati. Za vsako postavitev oblaka potrebujemo po eno vozlišče. Eno vozlišče je postavljeno v zasebnem oblaku nad katerim imamo popoln nadzor. Drugo vozlišče je postavljeno s strani ponudnika javnega vCloud oblaka. Poleg tega vozlišča skrbijo tudi za fizični prenos delovnih obremenitev med posameznimi oblaki. Vsako vCloud Connector vozlišče ima dostop do lokalne vCloud postavitve, preko vCloud programskega vmesnika (vCloud API). vCloud Connector Node podpira več-najemniški model, kar pomeni, da je možno uporabiti eno vozlišče za več organizacij (najemnikov) znotraj vCloud Director. Za vsako posamezno organizacijo se ustrezno konfigurira dostop z organizacijskim administrativnim računom.

- **vCloud Connector UI:** Zagotavlja uporabniški vmesnik za konfiguracijo in upravljanje hibridne platforme. Izvaja se kot modul znotraj podkomponente vCloud Connector Server. Uporabniški vmesnik je lahko izpostavljen na dva načina in sicer kot vtičnik za namizne aplikacije vSphere Client ter kot modul znotraj spletne strani vcloud.vmware.com za dostop preko spletnega brskalnika. Za dostop do vcloud.vmware.com je naprej potrebno registrirati uporabniški račun.

Drugi del hibridne platforme predstavlja javna postavitev vCloud oblaka.

Razlika v primerjavi z zasebno postavitvijo je ta, da imamo pri tem nadzor le nad organizacijo, ki je pripravljena s strani ponudnika. Pri izbiri ponudnika javnega vCloud oblaka za implementacijo hibridne platforme je pomembno zagotoviti, da je javna postavitev vCloud oblaka iste različice kot je lokalna. Za ustrezno povezavo z javnim oblaka je potrebno zagotoviti povezavo do vCloud Connector vozlišča, ki ima dostop do programskega vmesnika javnega vCloud oblaka. Zaradi tega potrebujemo javno dostopni URL do vCloud Connector vozlišča, preko katerega se bomo povezali z lokalno postavitvijo komponente vCloud Connector Server.

6.1.1.1 Namestitev in konfiguracija komponente vCloud Connector

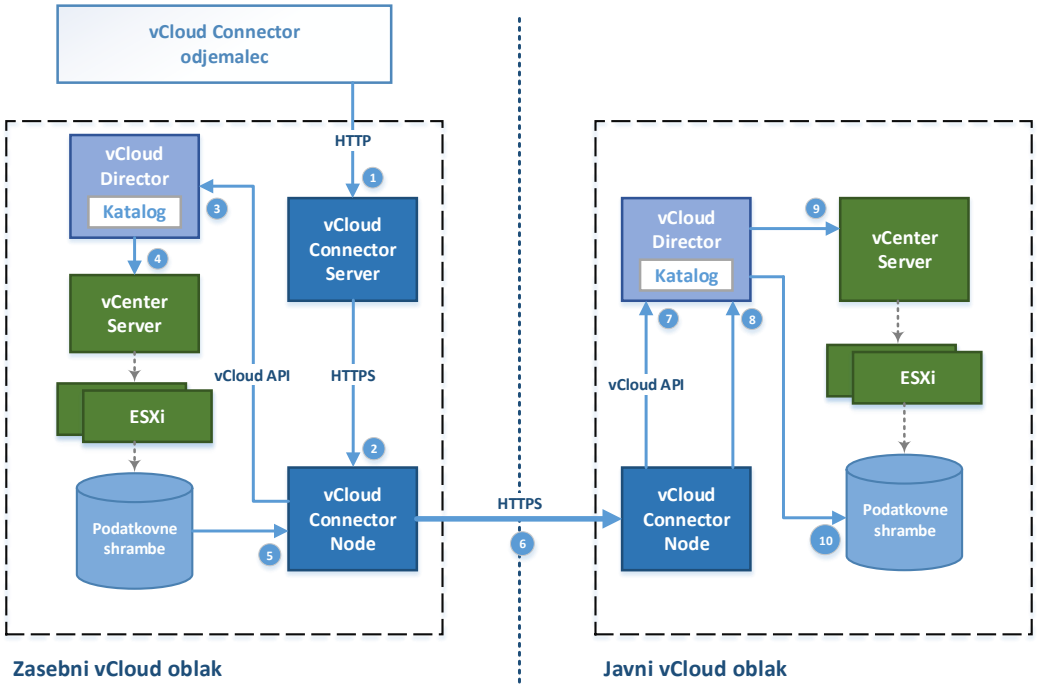
V primeru implementacije hibridne platforme z uporabo komponente vCloud Connector je potrebno komponento namestiti z uporabo OVF predloge. Kot smo že poprej omenili je vCloud Connector sestavljen iz treh podkomponent in sicer vCloud Connector Server ter vCloud Connector Node ter vCloud Connector UI. vCloud Connector Server je mogoče namestiti znotraj ene organizacije v vCloud Director ali pa neposredno na nivo komponente vCenter Server. Bolj priporočljiva je postavitev komponente znotraj sistemske organizacije v vCloud Director, kajti vCloud Director ponuja fleksibilnejše okolje, s stališča omrežne povezljivosti to pomeni omrežne storitve kot so Firewall, NAT itd. V obeh primerih moramo zagotoviti ustrezno omrežno povezljivost komponente. Če strežniški del komponente postavimo znotraj NAT omrežja je potrebno ustrezno nastaviti tudi NAT preslikavo IP naslovov. Slednje je nujno kadar želimo do uporabniškega vmesnika hibridne platforme dostopati iz zunanjih omrežij, ki so izven domene požarnega zidu. V nasprotnem primeru bo uporabniški vmesnik dostopen le iz brskalnikov ter vSphere odjemalcev, ki so znotraj domene požarnega zidu. Na podoben način kot strežniški del komponente vCloud Connector je potrebno namestiti še vCloud Connector vozlišče, ki bo skrbelo za prenos delovnih obremenitev med privatnim in javnim oblakom.

Namestitev hibridne platforme z uporabo komponente vCloud Connector po namestitvi komponente zahteva še konfiguracijo. Strežniški del komponente je potrebno povezati bodisi z vSphere odjemalcem ali spletno stranjo vcloud.vmware.com za dostop preko spletnega brskalnika. Možno je uporabiti oba pristopa hkrati. V produkcijskem okolju je potrebno uvoziti podpisan certifikat za zagotavljanje varne komunikacije med odjemalcem in vCloud Connector strežnikom. Privzeto komunikacija ni posebej zaščitena, ker je uporaba digitalno podpisanega certifikata obvezna. Konfiguracija vCloud Connector vozlišča zajema povezavo vozlišča bodisi z določeno organizacijo v vCloud Director ali vSphere platformo. V prvem primeru se povežejo viri organizacije, v drugem pa virtualizacijski viri, ki jih zagotavlja platforma vSphere. Če je vozlišče postavljeno znotraj NAT omrežja in za požarnem zidom je potrebno ustrezno konfigurirati NAT preslikave ter dodati pravila na ustrezna vrata za omrežno komunikacijo preko požarnega zidu.

Po konfiguraciji vCloud Connector vozlišča se je potrebno registrirati znotraj vCloud Connector Server. Na ta način vCloud Connector pridobi nadzor nad tem vozliščem, ki izpostavlja vire določeni organizaciji zasebnega oblaka. Komunikacija med vCloud Connector strežnikom ter posameznimi vCloud Connector vozlišči je privzeto zaščitena. Kljub temu je priporočljiva uporaba digitalno podpisanih certifikatov.

6.2 Migracija delovnih obremenitev z uporabo komponente vCloud Connector

Ključna funkcionalnost komponente vCloud Connector, ki zagotavlja hibridno platformo je možnost migracije delovnih obremenitev med zasebnim in javnim oblakom. Uporaba funkcionalnosti je možna le preko uporabniškega vmesnika. Slednje je tudi glavna pomanjkljivost. Postopek migracije zajema številne korake. Posamezne korake bolj podrobno ponazarja Slika 5. Na sliki so prikazani vsi koraki, ki so potrebni pri migraciji delovnih obremenitev. Ti se izvajajo znotraj ene organizacije v zasebnem oblaku vCloud. Kot je raz-



Slika 6.3: Migracija delovnih obremenitev v hibridnem oblaku.

vidno iz slike, prenos delovnih obremenitev vedno poteka med posameznimi vCloud Connector vozlišči.

Dejanski prenos OVF predlog se izvaja v korakih 5, 6, 8 in 10. Po ustreznem API klicu se iz podatkovne shrambe, kjer je OVF predloga shranjena, le-ta prenese v medpomnilnik komponente vCloud Connector Node. V koraku 6 pa se OVF predloga prenese do ciljnega vozlišča, od katerega se naprej uvozi v medpomnilnik komponente vCloud Director. V koraku 9 se predloga doda v organizacijski katalog ter se shrani v eno izmed podatkovnih shramb, ki je organizaciji na voljo. Iz kataloga je kasneje možno postaviti preneseni vApp.

Poglavje 7

Zaključek

V diplomski nalogi smo obravnavali področje računalništva v oblaku in se pri tem osredotočili na privatne in hibridne oblake ter zagotavljanje infrastrukturnih - IaaS storitev. Cilji diplomske naloge so bili podati temeljni opis ključnih komponent rešitve vCloud za postavitev in upravljanje privatnih, hibridnih ter javnih oblakov, vzpostaviti arhitekturo privatnega oblaka in pri tem analizirati dobre prakse in smernice pri vzpostavitvi samega privatnega oblaka, ter s pomočjo hibridne platforme nadgraditi arhitekturo privatnega oblaka.

V prvem delu diplomske naloge smo naslovili osnovne koncepte virtualizacije, kot tehnologije, ki je prispevala k uveljavitvi računalništva v oblaku in ob pravilnem načrtovanju prinaša unikatne priložnosti za doseganje učinkovitejšega obratovanja sodobnih podatkovnih centrov. Obravnavali smo osnovne koncepte računalništva v oblaku, kjer smo spoznali posamezne postavitvene ter storitvene modele oblaka. Izpostavili smo bistvene značilnosti računalništva v oblaku, ki jih mora ta nova paradigma zagotavljati.

V drugem delu diplomske naloge smo se osredotočili na VMware vCloud steber kot ene izmed rešitev, ki omogoča implementacijo modela računalništva v oblaku. Pri tem smo podrobno opisali posamezne komponente rešitve. Osredotočili smo se na ključne komponente, pri čemer smo analizirali funkcionalnosti in gradnike s katerimi lahko zagotovimo v prvem delu izpostavljene

značilnosti računalniškega oblaka. Iz analize komponent smo ugotovili, da rešitev vCloud tudi v primeru, ko uporabljamo le osnovne komponente, zagotavlja bistvene značilnosti računalniškega oblaka.

V nadaljevanju smo v okviru vzpostavitve arhitekture privatnega oblaka izdelali arhitekturni načrt, kjer smo upoštevali tako splošne dobre prakse, ki veljajo ne glede na izbrano rešitev, kot tudi dobre prakse in smernice specifične za rešitev vCloud. Pri tem smo uporabili nabor dokumentov iz kataloga vCAT. Načrtovanja arhitekture smo se lotili tako, da smo načrt razdelili na dva dela. V prvem delu smo obravnavali upravljavski del, v drugem pa skupine virov namenjene izključno izvajanju delovnih obremenitev oblaka. Ugotovili smo tudi, da slednje prispeva k bolj učinkoviti implementaciji arhitekture ter kasnejšega vzdrževanja. V načrtu zasnovano arhitekturo smo tudi implementirali, pri čemer smo namestili ter ustrezno po načrtu konfigurirali ključne komponente rešitve. Ugotovili smo, da vzpostavitev ene arhitekture računalniškega oblaka predstavlja kompleksen proces, ki zahteva veliko truda ter vnaprejšnjo planiranje za učinkovito doseganje na začetku zastavljenih ciljev.

Arhitekturo privatnega oblaka smo dopolnili tako, da smo vzpostavili hibridno platformo. V okviru tega smo implementirali hibridno platformo z uporabo komponente vCloud Connector, s čimer smo omogočili povezavo storitev privatnega in javnega značaja. Skozi analizo komponente smo ugotovili, da ponuja le najbolj osnovne funkcionalnosti. Za produkcijsko postavitev, kjer želimo samodejno optimizacijo virov med privatnim ter javnim oblakov ali dinamično postavitev novih delovnih obremenitev, se uporaba te tehnologije izkaže kot neprimerna. Kot možno rešitev smo izpostavili razvoja lastne rešitve skozi uporabo orodja vCenter Orchestrator ter ustreznih programskih vmesnikov, vendar slednje zahteva precej dodatnega truda.

Splošni sklep oz. ugotovitve kažejo na to, da računalništvo v oblaku s seboj prinaša številne poslovne in tehnološke prednosti in je kot tako vredno obravnave. Po drugi strani ponuja rešitev VMware vCloud ustrezne mehanizme za gradnjo privatnih in hibridnih oblakov. Ti mehanizmi so nam

omogočili doseganje zastavljenih ciljev, kljub temu da smo uporabili le nabor osnovnih komponent. Čeprav je rešitev vCloud ena izmed najbolj uveljavljenih rešitev za realizacijo [34, 35] računalniškega oblaka, to še ne pomeni da je rešitev vCloud brezhibna, saj ima tudi določene pomanjkljivosti tako na področju privatnih kot tudi hibridnih oblakov.

Kot glavno pomanjkljivost lahko izpostavimo zaprtost rešitve z vidika podpore virtualizacijske platforme. Komponenta vCloud Director se lahko namreč integrira izključno z virtualizacijsko platformo vSphere. Dejstvo je, da zaradi različnih licenčnih modelov, podpore operacijskih sistemov ipd., številne organizacije uporabljajo več kot eno virtualizacijsko platformo. Slednje lahko pripelje organizacije do potreb po vzpostavljanju več vzporednih rešitev za upravljanje računalniškega oblaka. Pomanjkljivost zaprtosti komponente vCloud Director se lahko odpravi z uporabo nove komponente vCloud Automation Center. Vendar je komponenta na voljo zgolj v celotnem licenčnem paketu (tj. vCloud Suite, ki vsebuje vse komponente), kar lahko predstavlja precej dražjo opcijo v primeru, da ne bi potrebovali ostalih komponent paketa.

Na področju hibridnih oblakov, se poleg zgoraj izpostavljenih pomanjkljivosti komponente vCloud Connector, tudi tukaj pojavlja problem zaprtosti. Hibridna platforma, ki temelji na komponenti vCloud Connector je izključno homogena. To pomeni, da je povezava privatnega oblaka z javnim možna le v primeru, ko javna postavitev oblaka temelji na rešitvi vCloud. Iz tega razloga končnim uporabnikom ne moremo zagotoviti portabilnosti storitev med heterogenimi platformami, saj smo omejeni zgolj na vSphere podprte namestitve.

Poleg pomanjkljivosti na področju privatnih in hibridnih oblakov lahko izpostavimo tudi nekatere splošne odprte probleme, ki lahko v določenih primerih igrajo ključno vlogo (na primer pri izbiri ustrezne tehnologije v podjetjih in organizacijah). Eden izmed odprtih problemov je samodejna elastičnost, saj rešitev ne ponuja vgrajenih mehanizmov, ki bi omogočale samodejno dodajanje ali odstranjevanje instanc virtualnih strojev glede na

uporabniško definirana pravila ali glede na ustrezne napovedne modele. Na področju zagotavljanja kakovosti izvajanja storitev, vCloud ne ponuja enostavnih mehanizmov za upravljanje, uveljavljanje in spremljanje SLA-jev. Pomanjkljivost je tudi upravljanje z licencami operacijskih sistemov, kajti za te namene ne ponuja vgrajenih funkcionalnosti in je potrebna integracija z zunanjimi rešitvami. Iz tega razloga so na področjih, kjer smo identificirali odprte probleme in pomanjkljivosti, prisotne še številne priložnosti za izboljšave, tako na znanstvenem področju kot tudi v industriji.

Literatura

[1] M. Portnoy, *"Virtualization Essentials"*, 2012, pogl. 1.

[2] V. Josyula, M. Orr, G. Page, *"Cloud Computing: Automating the Virtualized Data Center"*, 2012, pogl. 1.

[3] D. Kusnetzky, *"Virtualization: A Manager's Guide"*, 2011, str. 18.

[4] B. Hartpence, *"Packet Guide to Routing and Switching"*, 2011, pogl. 4.

[5] P. Mell, T. Grance, *"The NIST Definition of Cloud Computing"*, September 2011.

[6] R. Buyya, J. Broberg, A. Goscinski, *"Cloud Computing: Principles and Paradigms"*, 2011, pogl. 1.

[7] (2013) Cloud computing. Dostopno na: `http://en.wikipedia.org/wiki/Cloud_computing`

[8] (2011) Rise of the Cloud Ecosystems. Dostopno na: `http://blogs.msdn.com/b/dachou/archive/2011/03/16/rise-of-the-cloud-ecosystems.aspx`

[9] (2013) VMware vSphere 5.1 Documentation. Dostopno na: `http://pubs.vmware.com/vsphere-51/index.jsp`

[10] vSphere API/SDK Documentation. Dostopno na: `http://pubs.vmware.com/vsphere-51/index.jsp?topic=%2Fcom.vmware.wssdk.dsg.doc%2Fsdk_sg_preface.html`

[11] E. Bertino, K. Takahashi, *"Identity Management: Concepts, Technologies, and Systems"*, 2011, pogl. 2.

[12] (2012) vCenter Single Sign-On. Dostopno na:
http://blogs.vmware.com/vsphere/2012/09/vcenter-single-sign-on-part-1-what-is-vcenter-single-sign-on.html

[13] (2012) VMware vCloud Networking and Security. Dostopno na:
http://www.vmware.com/files/pdf/products/vcns/VMware-VCloud-Networking-Security-datasheet.pdf

[14] (2012) vCloud Director Installation and Upgrade Guide. Dostopno na:
http://pubs.vmware.com/vcd-51/topic/com.vmware.ICbase/PDF/vcd_51_install.pdf

[15] Virtual Appliances. Dostopno na:
http://www.vmware.com/technical-resources/virtualization-topics/virtual-appliances/ovf.html

[16] (2012) Open Virtualization Format Specification. Dostopno na:
http://dmtf.org/sites/default/files/standards/documents/DSP0243_2.0.0.pdf

[17] (2013) Installing and Configuring VMware vCenter Orchestrator. Dostopno na:
http://pubs.vmware.com/vsphere-51/topic/com.vmware.ICbase/PDF/vcenter-orchestrator-51-install-config-guide.pdf

[18] (2012) VMware vCenter Operations Manager Getting Started Guide. Dostopno na:
http://www.vmware.com/pdf/vcops-56-getting-started-guide.pdf

[19] (2012) vCenter Chargeback Manager User's Guide. Dostopno na:
http://www.vmware.com/pdf/cbm_users_guide_2_5_0.pdf

[20] (2012) Technical Note: Using VMware vCenter Chargeback Manager with VMware vCloud Director. Dostopno na:
http://www.vmware.com/files/pdf/techpaper/VMware-Technote-Using-vCenter-Chargeback-vCloud-Director.pdf

[21] (2012) Using vCloud Connector. Dostopno na:
http://pubs.vmware.com/hybridcloud-20/topic/com.vmware.ICbase/PDF/vCloudConnector_20_UsingvCC.pdf

[22] (2012) Using VMware vFabric Application Director. Dostopno na:
http://pubs.vmware.com/appdirector-5/topic/com.vmware.ICbase/PDF/using-vfabric-appdirector50.pdf

[23] (2012) VMware vCloud Automation Center. Dostopno na:
http://www.vmware.com/files/pdf/vcloud/vmware-vcloud-automation-center-datasheet.pdf

[24] VMware, "Service Definitions", *vCloud Architecture Toolkit*, 2013.

[25] VMware, "Introduction", *vCloud Architecture Toolkit*, 2013.

[26] VMware, "Architecting VMware vCloud", *vCloud Architecture Toolkit*, 2013.

[27] (2012) Designing Private and Hybrid Clouds: Architectural Best Practices. Dostopno na:
https://www.rightscale.com/info_center/white-papers/rightscale-white-paper-designing-private-hybrid-clouds.pdf

[28] (2008) Virtualizing a Windows Active Directoy Domain Infrastructure. Dostopno na:
http://www.vmware.com/files/pdf/Virtualizing_Windows_Active_Directory.pdf

[29] (2012) Failover Clustering Overview. Dostopno na:
http://technet.microsoft.com/en-us/library/hh831579.aspx

[30] (2012) VMware vCenter Server Heartbeat. Dostopno na:
http://www.vmware.com/files/pdf/products/vCenter/
VMware-vCenter-Server-Heartbeat-Datasheet.pdf

[31] (2012) User's Guide to Deploying vApps and Virtual Appliances. Dostopno na:
http://www.vmware.com/support/developer/studio/studio26/va_
user.pdf

[32] Installing ESXi Using vSphere Auto Deploy. Dostopno na:
http://pubs.vmware.com/vsphere-50/index.jsp

[33] vCloud Services Provider. Dostopno na:
http://vcloud.vmware.com/vcloud-ecosystem#view=full

[34] Forrester Evaluates Private Cloud Vendors – Platform Tops Media Scoring. Dostopno na:
http://platformcomputing.blogspot.com/2011/05/
forrester-scores-private-cloud-vendors.html

[35] (2012) T. J. Bittman, G. J. Weiss, M. A. Margevicius, P. Dawson "Magic Quadrant for x86 Server Virtualization Infrastructure", Gartner. Dostopno na:
http://www.gartner.com/technology/reprints.do?id=
1-1B2IRYF&ct=120626&st=sg