

DIPLOMSKA NALOGA :  
FAKULTETA ZA MATEMATIKO IN FIZIKO

UNIVERZA V LJUBLJANI  
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – Praktična matematika (VSŠ)

Marjana Hlebanja

**VARNOSTNE NASTAVITVE PRI IZDELAVI E-TRGOVINE S  
PLATFORMO IBM WEBSPHERE COMMERCE**

Diplomska naloga

Ljubljana, 2010

DIPLOMSKA NALOGA :  
FAKULTETA ZA MATEMATIKO IN FIZIKO

DIPLOMSKA NALOGA :  
FAKULTETA ZA MATEMATIKO IN FIZIKO  
**ZAHVALA**

Zahvaljujem se mentorju mag. Matiju Lokarju za nasvete in skrbno pregledovanje diplomske naloge. Zahvaljujem se tudi somentorju Gregorju Humarju iz podjetja MZR d.o.o., ki je pomagal s svojimi nasveti in me usmerjal. Zahvaljujem se tudi Ivu Ščavničarju, ki si je vzel čas in mi razložil marsikatero nerazumljivo stvar. Prav tako se zahvaljujem vsem zaposlenim v podjetju MZR d.o.o., ki so na kakršen koli način pripomogli k izdelavi diplomske naloge.

Posebna zahvala gre vsem domačim in prijateljem za podporo in spodbudo v času študija in ob izdelavi diplomske naloge.

DIPLOMSKA NALOGA :  
FAKULTETA ZA MATEMATIKO IN FIZIKO  
**PROGRAM DELA**

V diplomski nalogi predstavite ustrezne avtentikacijske in avtorizacijske postopke pri postavitvi e-trgovine s platformo IBM WEBSPPHERE COMMERCE.

mentor

mag. Matija Lokar

somentor

Gregor Humar

## POVZETEK

V diplomski nalogi je opisana platforma IBM WebSphere Commerce, ki je namenjena izdelovanju e-trgovin in varnosti pri izdelavi le-teh.

V prvem poglavju je na kratko predstavljen način zagotavljanja ustrezne zaščite pred nepooblaščen uporabo sistema, ki se izvaja ob vstopu in delu v e-trgovini. V drugem poglavju je na kratko predstavljena e-trgovina in načini poslovanja. Tretje poglavje predstavlja platformo IBM WebSphere Commerce in njene verzije, opisano je, kako je sestavljena e-trgovina (organizacijske strukture) in s katerimi orodji se srečamo pri delu s to platformo. Četrto poglavje predstavlja avtentikacijski postopek. Opisana je politika za uporabniški račun, zakaj je pomembna, kako jo definiramo in kako spreminjamo. V petem poglavju pa je predstavljena avtorizacija in politika dostopa, s čimer uporabnika nadzorujemo. Opisano je, kako je sestavljena politika dostopa, kako definiramo novo politiko in posamezne komponente. Opisan je tudi postopek nadzora dostopa.

## ABSTRACT

This thesis deals with the IBM WebSphere Commerce platform, which is intended for designing online stores, and security in their designing.

Chapter one offers a brief presentation of the method of providing appropriate protection from unauthorized use of the system, employed on entering and working in an online store. Chapter two is a short presentation of an online store and ways of operation. Chapter three presents the IBM WebSphere Commerce platform and its versions, described is the composition of an online store (organizational structures) and the tools encountered when working with this platform. Chapter four discusses the characteristics of authentication process; described is the account policy, its importance, how it is defined and how it is changed. Chapter five gives a presentation of authorization and access control policy, by which the user is controlled. A description is given how the access control policy is composed, how a new policy and individual components are defined. Also the process of access control is described.

**Math. Subj. Class. (2010):** 68N01, 68N19

**Computing Review Class. System (1998):** D.3.2, D.4.6, K.4.4, K.6.5

**Ključne besede:** IBM WebSphere Commerce, e-trgovina, organizacija, varnost, avtentikacija, avtorizacija, politika za uporabniški račun, politika gesla, politika začasnega omejevanja dostopa, politika dostopa, skupina uporabnikov, vloge, skupina akcij, skupina virov, relacija

**Keywords:** IBM WebSphere Commerce, e-commerce, organization, securing, authentication, authorization, account policy, password policy, account lockout policy, access control policy, users group, role, action group, resource group, relation

DIPLOMSKA NALOGA :  
FAKULTETA ZA MATEMATIKO IN FIZIKO

# KAZALO

|          |                                                    |           |
|----------|----------------------------------------------------|-----------|
| <b>1</b> | <b>UVOD.....</b>                                   | <b>6</b>  |
| <b>2</b> | <b>E-TRGOVINA IN NAČINI POSLOVANJA.....</b>        | <b>7</b>  |
| 2.1      | KAJ JE E-TRGOVINA?.....                            | 7         |
| 2.2      | POSLOVANJE BUSINESS TO BUSINESS (B2B) .....        | 7         |
| 2.3      | POSLOVANJE BUSINESS TO CONSUMER (B2C) .....        | 8         |
| <b>3</b> | <b>IBM WEBSPHERE COMMERCE .....</b>                | <b>9</b>  |
| 3.1      | VERZIJE WEBSPHERE COMMERCE.....                    | 9         |
| 3.2      | KAJ OMOGOČA WSC.....                               | 10        |
| 3.3      | ORGANIZACIJE IN ORGANIZACIJSKE STRUKTURE .....     | 11        |
| 3.3.1    | <i>Osnovna organizacijska struktura .....</i>      | <i>11</i> |
| 3.3.2    | <i>Organizacijska struktura za model B2B.....</i>  | <i>12</i> |
| 3.3.3    | <i>Organizacijska struktura za model B2C.....</i>  | <i>13</i> |
| 3.4      | ORODJA ZA DELO Z WSC.....                          | 14        |
| 3.4.1    | <i>Administration Console .....</i>                | <i>15</i> |
| 3.4.2    | <i>WSC Accelerator .....</i>                       | <i>18</i> |
| 3.4.3    | <i>Organization Administration Console.....</i>    | <i>20</i> |
| <b>4</b> | <b>AVTENTIKACIJA .....</b>                         | <b>22</b> |
| 4.1      | POLITIKA ZA UPORABNIŠKI RAČUN.....                 | 22        |
| 4.1.1    | <i>Politika gesla.....</i>                         | <i>22</i> |
| 4.1.2    | <i>Politika začasnega omejevanja dostopa .....</i> | <i>22</i> |
| 4.2      | PRIVZETI POLITIKI ZA UPORABNIŠKI RAČUN .....       | 23        |
| 4.3      | PRILAGAJANJE POLITIKE ZA UPORABNIŠKI RAČUN .....   | 23        |
| <b>5</b> | <b>AVTORIZACIJA .....</b>                          | <b>27</b> |
| 5.1      | POLITIKA DOSTOPA.....                              | 27        |
| 5.1.1    | <i>Skupine uporabnikov .....</i>                   | <i>28</i> |
| 5.1.2    | <i>Akcije .....</i>                                | <i>30</i> |
| 5.1.3    | <i>Viri .....</i>                                  | <i>30</i> |
| 5.1.4    | <i>Relacije .....</i>                              | <i>32</i> |
| 5.2      | KAKO JE DEFINIRANA POLITIKA DOSTOPA.....           | 34        |
| 5.2.1    | <i>Organization Administration Console.....</i>    | <i>35</i> |
| 5.2.2    | <i>Definiranje skupin.....</i>                     | <i>38</i> |
| 5.2.3    | <i>Format XML .....</i>                            | <i>44</i> |
| 5.3      | SKUPINE POLITIK DOSTOPA .....                      | 48        |
| 5.3.1    | <i>Privzete skupine politik.....</i>               | <i>50</i> |
| 5.4      | KATEGORIJE POLITIK .....                           | 52        |
| 5.4.1    | <i>Prilagajanje politik.....</i>                   | <i>55</i> |
| 5.5      | DVA TIPA POLITIK.....                              | 56        |
| 5.6      | POSTOPKI ZA NADZOR DOSTOPA .....                   | 57        |
| 5.6.1    | <i>Standardna politika .....</i>                   | <i>60</i> |
| 5.6.2    | <i>Vzorčna politika .....</i>                      | <i>63</i> |
| <b>6</b> | <b>ZAKLJUČEK .....</b>                             | <b>65</b> |
| <b>7</b> | <b>LITERATURA .....</b>                            | <b>66</b> |

DIPLOMSKA NALOGA :  
FAKULTETA ZA MATEMATIKO IN FIZIKO  
**1 UVOD**

V današnjem svetu se čedalje več poslovanja seli na internet. Ta proces prinaša tudi določene nevarnosti, predvsem na področju nepooblaščenega dostopa do podatkov. Zato moramo takrat, ko postavljamo sisteme za e-poslovanje, poskrbeti tudi za ustrezno varnost.

Ena izmed platform, namenjena izdelovanju spletne trgovine, je IBM WebSphere Commerce. Ob namestitvi tega sistema na računalnik dobimo že vrsto privzetih pravil in nastavitev, ki skrbijo za varnost uporabnika.

Za varnost poskrbimo s pomočjo avtentikacije in avtorizacije. Uporabnik, ki želi uporabiti e-trgovino, se mora najprej prijaviti v sistem. To stori z vpisom uporabniškega imena in gesla. Ob tem se izvede avtentikacijski postopek. Ta preveri, ali sta kombinaciji uporabniškega imena in gesla pravilni. Če je kombinacija pravilna, strežnik uporabniku pošlje določeno tekstovno informacijo, tako imenovani sejni spletni piškotek. Ta piškotek se shrani na uporabnikov računalnik. V spletnem piškotku je zapisan niz informacij, ki vsebujejo informacije o uporabniku. Piškotek je »uporaben« toliko časa, dokler je uporabnik aktiven na spletni strani. Ko le ta postane neaktiven oz. se odjavi iz sistema, sejni spletni piškotek ni več veljaven. Ta piškotek omogoča, da strežnik ves čas aktivnosti na spletni strani prepozna uporabnika. Ob ponovnem vpisu se uporabniku dodeli nov sejni spletni piškotek.

Ko se uporabnik uspešno prijavi v sistem, lahko opravlja določene akcije. Te akcije so v spletni trgovini na primer listanje po katalogu, dodajanje izdelkov v košarico, pošiljanje naročil ... Katere akcije uporabnik lahko izvaja, je določeno s politiko dostopa. Ob uporabnikovih aktivnostih se ves čas izvaja avtorizacija, torej proces, ki nadzira, ali uporabnik izvaja njemu dovoljene akcije. S pomočjo revizijske sledi (angl. *audit trail*) sledimo akcijam, ki jih uporabnik izvaja.

Da pa je nadzor nad uporabnikom čim boljši, si pomagamo s tako imenovanimi politikami. To so skupine pravil, ki uporabniku omogočajo izvedbe določenih postopkov. Da te politike smiselno postavimo, moramo poskrbeti za smiselno organizacijsko strukturo in določiti vloge in skupine uporabnikov, skupine akcij in virov.

V diplomski nalogi kot orodje, s katerim skrbimo za ustrezno avtorizacijo in avtentikacijo, opisujemo platformo IBM WebSphere Commerce Enterprise. Opisano je, kako se izvaja nadzor nad izvedbo določenih akcij.

## 2 E-TRGOVINA IN NAČINI POSLOVANJA

### 2.1 Kaj je e-trgovina?

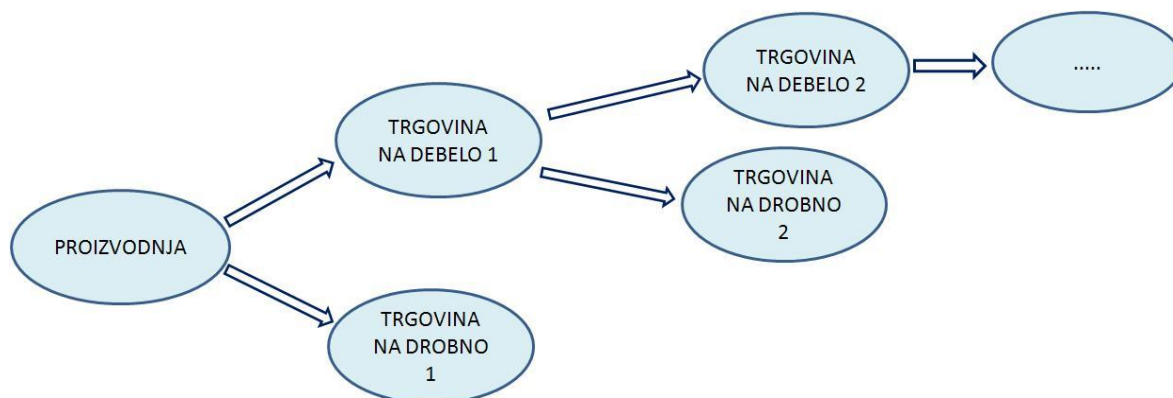
E-trgovina je trgovina, v kateri prodajalci preko spleta ponujajo svoje izdelke in storitve, potrošnikom pa je omogočen nakup le-teh. Elektronsko poslovanje poteka preko interneta ali drugih računalniških omrežij in je namenjeno poslovanju med podjetji (B2B – razdelek 2.2) in prodaji končnim kupcem (B2C – razdelek 2.3). Večina e-poslovanja B2C poteka preko svetovnega spleta (World Wide Web). Potrošnikom omogoča, da na hiter in dokaj enostaven način pridejo do željenih izdelkov. Takšen način poslovanja je »javen« in je namenjen končnim potrošnikom. Pri B2B poslovanju pa imamo pogosto vzpostavljena zaprta računalniška omrežja, do katerih imajo možnost dostopa samo tista podjetja, ki imajo sklenjeno pogodbo s ponudnikom.

Začetki e-trgovine segajo v leto 1979. Prvi tovrsten sistem je postavil Michael Aldrich. Sistem je postavil tako, da je 26-palčni barvni televizor povezal z računalnikom in preko telefonske linije demonstriral kupovanje v taki spletni trgovini. Aldrichov sistem so uporabljala avtomobilska podjetja, kot so Peugeot - Talbot, Ford, Nissan in General Motors ter druge industrije. E-trgovine so se v 80-ih pojavljale predvsem v Veliki Britaniji in nekaterih državah Srednje Evrope. Prvo B2B e-poslovanje se je pojavilo leta 1981 (Thomson Holidays), B2C pa tri leta kasneje, in sicer ga je uporabilo podjetje Gateshead SIS/Tesco.

Že dve leti potem, ko je Tim Berns-Lee predstavil sistem, ki ga danes poznamo kot *World Wide Web* oziroma svetovni splet, je Charles Stack ustvaril spletno knjigarno *Book Stacks Unlimited*. Leta 1992 pa je Jeff Bezos odprl spletno trgovino *Amazon.com*. Uporaba interneta je močno naraščala, kar je tudi sprožilo večjo uporabo spletne trgovine. Od leta 2000 dalje je vedno več podjetji začelo ponujati svoje izdelke in storitve preko spleta.

### 2.2 Poslovanje Business to business (B2B)

Poslovanje *Business to business* je poslovanje med podjetji. Gre za način poslovanja med proizvajalci (angl. *manufacturer*), trgovci na debelo (angl. *wholesaler*) in trgovci na drobno (angl. *retailer*). Proizvajalci izdelke prodajo trgovcem, ki te izdelke prodajo naprej drugim trgovcem ali pa končnim kupcem.



Slika 1: B2B

Slika 1 prikazuje shemo B2B poslovanja. Celotno poslovanje se začne, ko proizvodnja prodaja izdelke dobaviteljem (trgovina na debelo 1) ali trgovinam na drobno (trgovina na drobno 1). Dobavitelji so nekakšni posredniki, ki izdelke prodajo naprej trgovinam na debelo ali trgovinam na

drobno. Trgovine na drobno izdelke nudijo končnim kupcem, medtem ko trgovine na debelo izdelke »preprodajajo«.

B2B e-trgovanje v večini primerov poteka preko računalniških omrežij, do katerih dostopajo samo tisti kupci (trgovine na debelo in drobno), ki imajo sklenjeno pogodbo s prodajalci. Posamezna e-trgovina je običajno sestavljena iz več trgovin (razdelek 3.3.2).

## 2.3 Poslovanje Business to consumer (B2C)

Poslovanje *Business to consumer* je poslovanje med trgovinami na drobno (angl. *retailer*) in končnimi kupci.



Slika 2: B2C

Slika 2 prikazuje enostavno B2C poslovanje. Kot je že omenjeno v tem razdelku, poslovanje poteka med trgovinami in potrošniki – končnimi uporabniki izdelkov.

E-trgovanje tipa B2C poteka preko spleta in je javnega značaja. Vsak, ki želi kupiti določene izdelke, se prijavi v izbrano spletno trgovino, kjer ima dostop do izdelkov, ki jih ponuja trgovina. Prav tako kot pri B2B poslovanju, tudi v tem primeru e-trgovina pogosto zajema več trgovin (posamezne kategorije izdelkov ...) (razdelek 3.3.3).

### 3 IBM WEBSPHERE COMMERCE

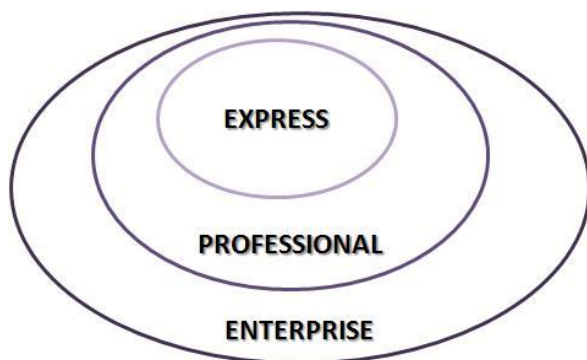
IBM WebSphere Commerce (v nadaljevanju WSC) je platforma, namenjena temu, da z njo izdelamo e-trgovino. Pod pojmom platforma mislimo na to, da imamo že ustvarjeno neko predlogo oziroma vzorec, ki nam pomaga pri izdelovanju sistema e-trgovine ter na voljo določena orodja za to izdelavo in kasnejše upravljanje in spreminjanje sistema. Za našo diplomsko nalogo je še posebej pomembno, da z namestitvijo celotnega sistema WSC za novo e-trgovino že velja vrsta politik uporabniškega računa (razdelek 4.1), politik dostopa (razdelek 5.1), vzpostavljena je določena organizacijska struktura in njej primerne organizacije (razdelek 3.3) ... To nam omogoča, da sistema ne postavljamo od začetka, saj imamo določene stvari že pripravljene. Tekom izdelave e-trgovine imamo seveda možnost te nastavitve spreminjati, prilagajati, brisati ...

WSC temelji na programiranju s programskim jezikom Java ter podpira odprte standarde, kot so na primer XML in standardi v povezavi z Web servisi. Poleg pisanja svojih programov za delo s to platformo uporabljamo orodja (razdelek 3.4), ki jih dobimo ob namestitvi. Pri delu, ki ga bomo opisovali v diplomski nalogi, programiranja ne bomo potrebovali. Več ali manj bomo uporabljali le orodja, ki so na voljo z namestitvijo WSC.

#### 3.1 Verzije WebSphere Commerce

Prva verzija WSC-ja se je pojavila leta 1996 pod imenom Net.Commerce. Pod tem imenom so se pojavile verzije V1.0, V2.0, V3.1 in V3.2. Leta 2001 se je Net.Commerce preimenoval v WebSphere Commerce Suite. Pod tem imenom sta bili izdani verziji V4.1 in V5.1. Leta 2002 pa se pojavi prva verzija platforme pod novim (sedanjim) imenom WebSphere Commerce, in sicer V5.4. Trenutno (december 2009) je najnovejša verzija V6.0.0.8 in slednjo tudi opisujemo v tej diplomski nalogi.

Poleg posameznih verzij, preko katerih se je razvijala in nadgrajevala platforma WSC, so pri IBM na tržišče dali tri oblike platforme WSC: Express, Professional in Enterprise. Vsaka oblika je nadgradnja prejšnje. Kot prikazuje Slika 3, je Express osnovna izdaja. Ostali dve pa sta nadgraditvi in dopolnitev prejšnje. Največ možnosti pri izdelavi e-trgovine torej nudi WSC Enterprise.



Slika 3: Izdaje WSC-ja

**WSC Express** je namenjen izdelavi enostavne e-trgovine za prodajo med podjetji (B2B) in prodajo končnim kupcem (B2C). Deluje na operacijskem sistemu Windows in Linux. Uporabljajo ga predvsem srednje velika podjetja, saj je cenovno ugoden. Je enostaven in hitro namestljiv. Prav tako je enostaven za uporabo in vzdrževanje celotne e-trgovine. Ob namestitvi ima pripravljene osnove za izdelavo e-trgovine in omogoča nadaljnjo nadgradnjo le-te.

Prav tako kot WSC Express je tudi **WSC Professional** namenjen izdelavi e-trgovine za načina poslovanja B2B in B2C. Poleg teh dveh načinov poslovanja podpira tudi nekoliko bolj zapleteno, večkanalno prodajo<sup>1</sup>. Uporabljajo ga tako srednje velika, kot tudi večja podjetja. Deluje na operacijskih sistemih Windows, Linux, AIX in Sun Solaris. Ob namestitvi te izdaje WSC-ja dobimo že pripravljene osnove za izdelavo e-trgovine, ki pa jih lahko nadgradimo. Omogoča nam neomejeno širjenje kataloga izdelkov. Prav tako nam omogoča spremljanje povpraševanja in prodaje na trgu (izdelava analiz).

**WSC Enterprise** deluje na operacijskih sistemih Windows, Linux, AIX ter Sun Solaris. Namenjen je vodenju tako enostavnih (B2B in B2C) kot tudi zapletenih modelov poslovanja (kot je razširjena večkanalna prodaja<sup>2</sup>). WSC Enterprise omogoča izdelovanje zapletenih poslovanj med podjetji, pri katerem se ustvari veriga povpraševanja (angl. *demand chain*). Takšna veriga zajema proizvajalca, ki določeno blago izdeluje, prodajalca, ki to blago prodaja naprej, ter končnega kupca. Prav tako v tej verigi poteka neposredna prodaja strankam in poslovnim partnerjem. Ta verzija pa podpira tudi izdelavo poslovnega modela med kupci (podjetja) in dobavitelji (tako imenovana dobavna veriga (angl. *supply chain*)). Poslovanje večinoma poteka preko zaprtih računalniških omrežji, torej z vzpostavitvijo zasebnega trga. To pomeni, da so v tej verigi tista podjetja, ki imajo sklenjene pogodbe z dobavitelji.

Vse te načine poslovanja, ki jih ustvarjamo s pomočjo WSC Enterprise, sestavljajo organizacije, ki skupaj tvorijo smiselno organizacijsko strukturo (razdelek 3.3). Vsako organizacijsko strukturo pa lahko nadgrajujemo in dopolnjujemo. Kot je opisano v razdelku 3.3.2, ta izdaja WSC-ja omogoča tudi združevanje več trgovin v eno e-trgovino.

## 3.2 Kaj omogoča WSC

S pomočjo WSC-ja ustvarimo e-trgovino za različne načine poslovanja. Trgovina lahko služi neposredni prodaji kupcem (B2B), trgovanju med podjetji (B2C) ali pa podpira oba načina poslovanja hkrati. Podjetjem, ki se ukvarjajo z e-trgovanjem, omogoča hitrejšo širjenje informacij o posebnih in novih ponudbah, boljše povezovanje z dobavitelji, poslovnimi partnerji in kupci ter z združevanjem poslovnih procesov zmanjšuje stroške poslovanja. S pomočjo WSC podjetje v e-trgovini lahko prodaja in predstavi vse svoje produkte, saj je katalog izdelkov in storitev prostorsko neomejen. Prav tako je vsak prodajni izdelek ali storitev lahko prikazan s sliko, opremljen s kratkim opisom, ceno, dobavljivostjo ... WSC e-trgovina strankam omogoča tudi, da pridobijo določene informacije o posameznih izdelkih, dobavi, naročanju ... Odgovore na vprašanja jim posreduje prodajni predstavnik, ki ima hkrati vpogled v zgodovino nakupov in katalog.

Platforma omogoča promocije izdelkov, kot so razni popusti, ugodnosti. Zaradi sledljivosti dogajanja WSC e-trgovina kupce lahko razvršča v ciljne skupine glede na povpraševanje. Tako podjetje lažje promovira določene izdelke.

Samo naročanje izdelkov je enostavno. Pri B2C načinu poslovanja kupci izbrane izdelke razvrščajo v nakupovalne košarice, pri B2B načinu poslovanja pa imajo posamezniki odprte naročilnice. Ko se kupec odloči, da bo izbrane izdelke, ki jih je uvrstil v košarico, naročil, preprosto klikne na gumb »Naroči«. Nato izpolni naročniški obrazec (ime, priimek, naslov, način plačila ...). Podobno je naročanje pri odprtih naročilnicah.

---

<sup>1</sup> Večkanalna prodaja predstavlja verigo poslovanj in zajema distributerje, dobavitelje, preprodajalce ... Vsi ti imajo nadzor nad posamezno trgovino. Skupek teh trgovin pa predstavlja celotno e-trgovino, pri kateri so končni kupci tako posamezniki kot tudi trgovine na debelo in drobno.

<sup>2</sup> Razširjena večkanalna prodaja je precej podobna večkanalni prodaji. Le da imamo v tem primeru poleg zastopnikov, dobaviteljev in preprodajalcev zajete tudi »končne prodajalce«. To pomeni, da kot prodajalci nastopajo trgovine na debelo in drobno.

Da poslovanje poteka čim bolj tekoče in nemoteno, poleg kupcev v celotnem sistemu sodelujejo trgovci in razni administratorji. Glede na dejavnosti uporabnikov so se izoblikovale vloge uporabnikov. Tem so s pomočjo politik dostopa dodeljene posamezne naloge in možnost dostopov do različnih informacij (razdelek 5.1).

#### **Primeri vlog in njihovih tipičnih zadolžitev:**

- *Glavni administrator* je tisti, ki skrbi za celotno delovanje e-trgovine ter ureja programsko in strojno opremo.
- *Prodajni predstavnik* je tisti, ki ima neposreden stik s kupci. Odgovarja na vprašanja kupcev, ima vpogled v celotno zgodovino nakupov, rešuje reklamacije ...
- *Vodja maloprodaje* skrbi za ohranjanje starih kupcev in pridobivanje novih, napoveduje trende prodaje, sodeluje pri določanju zalog.
- *Vodja veleprodaje* deluje na nivoju B2B načina poslovanja, pridobiva nove prodajalce.
- *Vodja dostave* skrbi za razpošiljanje izdelkov, ki so jih naročili kupci.
- *Vodja oglaševanja* skrbi za oglaševanje. Sestavlja vsebino oglasov.

Glede na potrebe pri e-poslovanju lahko ustvarimo tudi nove vloge. Prav tako obstoječim vlogam dodamo ali odvzamemo naloge in z njimi povezane pravice do dostopa do določenih podatkov.

### **3.3 Organizacije in organizacijske strukture**

Organizacije so hierarhično urejene enote, v katere so uporabniki razporejeni glede na pravice, ki jih imajo v sistemu. Posamezna organizacija predstavlja določen del pri e-poslovanju. Vzpostavitev organizacij, uvrščenih v ustrezno organizacijsko strukturo, pripomore k lažjemu nadzoru poslovanja in lažjemu nadzoru dostopa uporabnikov.

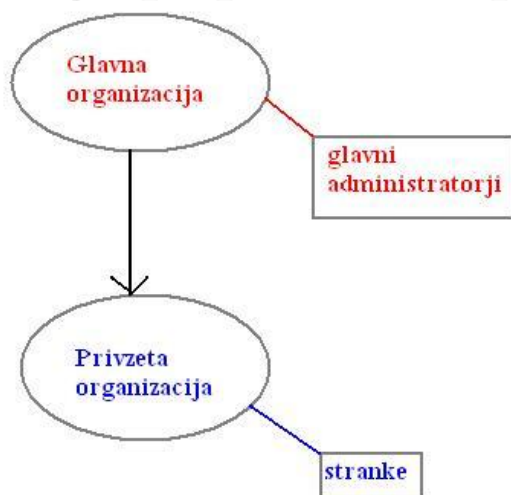
Določene organizacije so lahko razdeljene na organizacijske enote. Vsaka organizacija ali organizacijska enota vsebuje uporabnike, ki so v organizacije razporejeni glede na pravice oz. vloge, ki jih imajo v sistemu. Prav tako imajo organizacije v lasti trgovine, vire in skupine politik (razdelek 5.3).

Organizacije so razvrščene v organizacijske strukture, ki se med seboj razlikujejo glede na način poslovanja (B2C ali B2B). Običajno so organizacije povezane v drevesno strukturo, torej so med seboj v hierarhiji. Odnose med organizacijami v e-trgovini predstavimo s shemo.

Nadzor nad organizacijsko shemo, torej nad organizacijami in organizacijskimi strukturami, ima samo glavni administrator. Organizacije in organizacijske enote lahko na novo ustvarja, spreminja ter briše s pomočjo vmesnika Organization Administration Console (razdelek 3.4.3).

#### **3.3.1 Osnovna organizacijska struktura**

Osnovna organizacijska struktura je sestavljena iz glavne (angl. *root organization*) in privzete organizacije (angl. *default organization*). Struktura je neodvisna od načina poslovanja, torej jo uporabljamo tako pri poslovanju tipa B2C kot tudi B2B. Običajno ni uporabljena kot samostojna struktura, ampak kot del večje strukture.



**Slika 4:** Osnovna organizacijska struktura

Glavna organizacija je najvišja v hierarhiji in nima nadrejene organizacije. Pripadajo ji vsi uporabniki, ki imajo vlogo glavnega administratorja (angl. *site administrator*) in skrbijo za delovanje celotnega sistema.

Privzeta organizacija je podrejena glavni organizaciji (Slika 4). Vsebuje stranke, ki so tako registrirani uporabniki (angl. *customers*) kot tudi v sistemu neregistrirani uporabniki (angl. *guest customers*). Privzeta organizacija ima tako ime, ker so v njej zajeti vsi tisti uporabniki, ki ne sodijo v drugo organizacijo. Prav tako pa ta organizacija ne vsebuje nobene podorganizacije oziroma ni razdeljena na organizacijske enote.

### 3.3.2 Organizacijska struktura za model B2B

B2B je poslovanje med dvema trgovinama. Torej je tukaj nakup opravljen za nadaljnjo prodajo. Kupci pri B2B načinu poslovanja so tiste trgovine, ki bodo blago prodale končnim kupcem, ali pa tiste trgovine, ki bodo blago prodajale naprej drugim trgovinam.

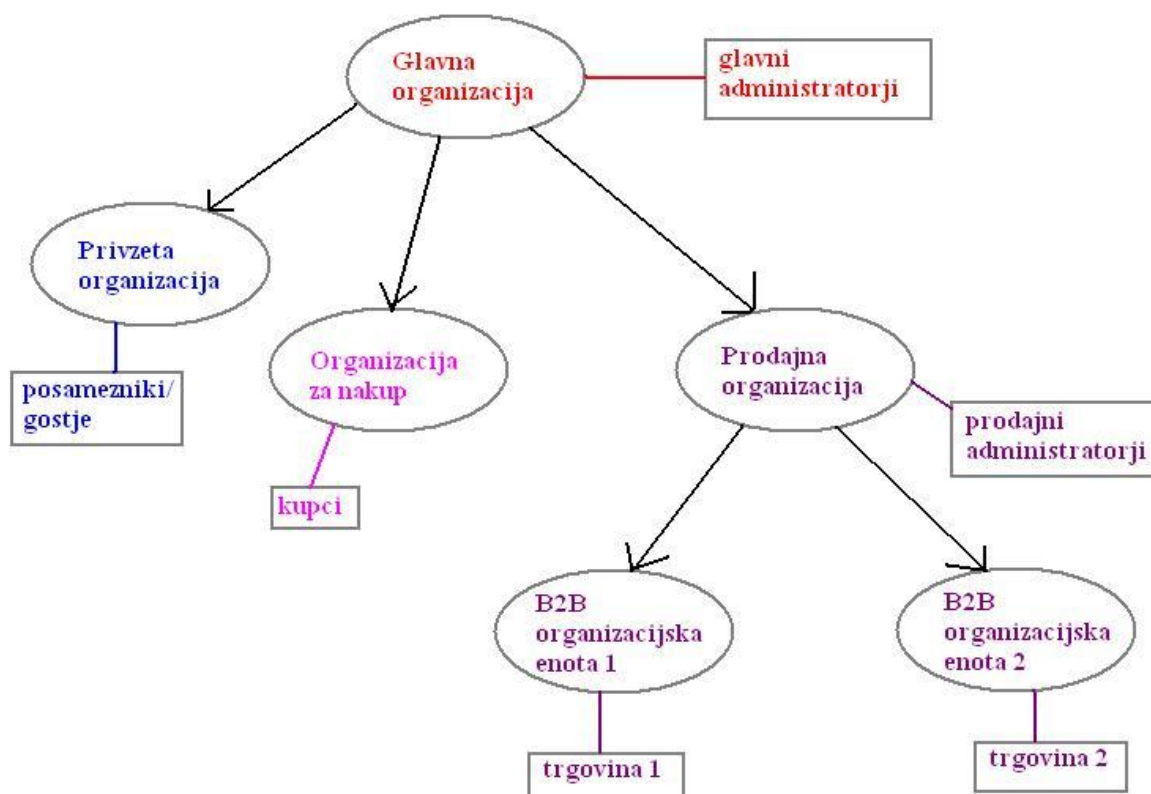
Organizacijska struktura za način poslovanja B2B vsebuje štiri različne organizacije. To so glavna, privzeta, prodajna organizacija (angl. *seller organization*) ter organizacija za nakup (angl. *buyer organization*) (Slika 5). Uporabniki so kupci (trgovine za končno ali nadaljnjo prodajo) in prodajalci. Glavna organizacija je najvišje v hierarhiji in vsebuje uporabnike z vlogo glavnega administratorja. Ti upravljajo celoten sistem. Privzeta organizacija je podrejena glavni organizaciji in vsebuje vse tiste uporabnike, ki niso del poslovanja B2B (posamezniki). Ti uporabniki so neregistrirani ali pa registrirani uporabniki, ki pa niso del organizacije za nakup. Ni nujno, da posamezniki obstajajo v sistemu, če pa se pojavijo, pripadajo privzeti organizaciji. Uporabniki se lahko pojavijo v poslovanju B2B, če je dostopno preko spleta. V tem primeru nastopajo kot neregistrirani uporabniki (gostje). Če pa v tej e-trgovini lahko kupujejo tudi posamezniki, so le-ti registrirani uporabniki, vendar pripadajo privzeti organizaciji. Organizacija za nakup je podrejena neposredno glavni organizaciji. Vsebuje kupce, ki so, kot je že omenjeno, v tem primeru trgovine.

Tudi prodajna organizacija je podrejena neposredno glavni organizaciji. Njen sestavni del so vse organizacijske enote in trgovine. Uporabniki z vlogo prodajnega administratorja sodijo k prodajni organizaciji. Upravljajo in nadzirajo celotno prodajo.

Prodajna organizacija je razdeljena na organizacijske enote B2B. Posamezna organizacijska enota ima v lasti eno trgovino, s katero upravljajo prodajni administratorji. Posamezne trgovine kupcem niso vidne, vendar so ustvarjene samo zaradi lažjega nadzora. Kupci (v tem primeru trgovine) nakupujejo v teh trgovinah.

V tem načinu poslovanja torej uporabnik pripada eni od štirih organizacij:

- če je administrator, spada v glavno organizacijo,
- če je kupec, je del organizacije za nakup,
- prodajalci so del prodajne organizacije,
- vsi preostali uporabniki (neregistrirani in registrirani uporabniki) sistema pa spadajo v privzeto organizacijo.



**Slika 5:** Organizacijska struktura za poslovni model B2B

Slika 5 prikazuje primer organizacijske strukture za model B2B. V tem primeru je prodajna organizacija razdeljena na dve organizacijski enoti, ki imata v lasti (upravljata) trgovini 1 in 2. Od teh dveh trgovin kupujejo izdelke kupci, torej trgovine na drobno, ki so del organizacije za nakup. V sklopu organizacije za nakup se torej zbirajo podatki o tistih trgovinah (kupcih), ki imajo sklenjene ustrezne pogodbe za nakup za nadaljnjo prodajo.

Denimo, da ima neko farmacevtsko podjetje dve farmacevtski trgovini, eno v Kopru in drugo v Mariboru. To sta v našem primeru trgovina 1 in trgovina 2. Kupci v tem sistemu so lekarne. Če želi neka lekarna kupovati pri tem farmacevtskem podjetju, se mora najprej registrirati v sklopu organizacije za nakup. Ko ta lekarna želi naročiti izdelke, jih ima na voljo iz obeh trgovin. Kupci torej ne kupujejo v posamezni trgovini, ampak neposredno pri prodajni organizaciji. Delitev na posamezne trgovine obstaja le zaradi organizacije poslovanja, za kupca pa je sistem enovit.

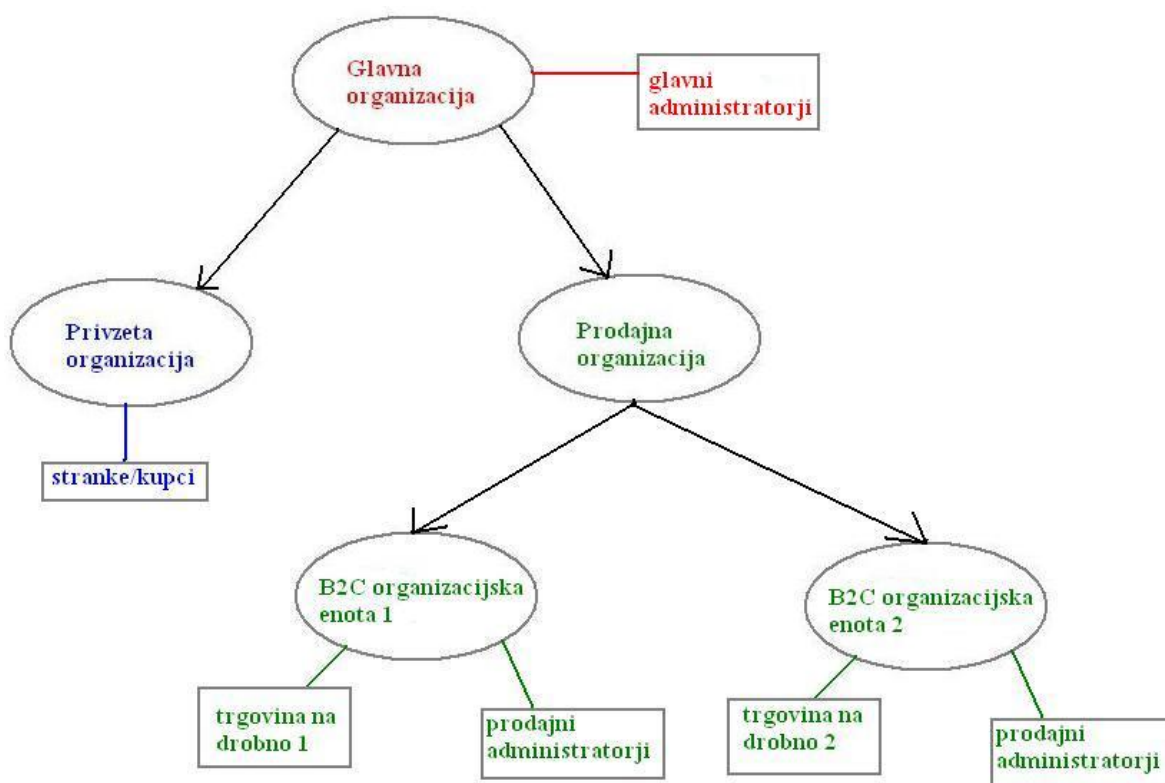
### 3.3.3 Organizacijska struktura za model B2C

Kot je že opisano v razdelku 2.3, model B2C predstavlja poslovanje med prodajalci oz. trgovci in kupci, ki so tu končni uporabniki (ne kupujejo za nadaljnjo prodajo). Slika 6 predstavlja organizacijsko strukturo modela B2C. Na eni strani so kupci, na drugi pa prodajalci. Glede na to so

uporabljene tri organizacije, med katere so uporabniki razdeljeni glede na vloge. Najvišja je glavna organizacija, ki vsebuje glavne administratorje. Le-ta vsebuje dve podorganizaciji, in sicer privzeto in prodajno organizacijo (angl. *seller organization*). Privzeti organizaciji pripadajo stranke oz. kupci, ki nakupujejo v spletnih trgovinah.

Prodajna organizacija ima v lasti vse trgovine (angl. *retailer*) in administratorje, ki na kakršenkoli način skrbijo za posamezno trgovino. Administratorji so razdeljeni na več vlog, kot je vloga prodajnega administratorja, ki skrbi za prodajo, upravljalca s produkti (angl. *product manager*) ... Prodajna organizacija je razdeljena na posamezne organizacijske enote B2C.

Organizacijska enota prodajne organizacije ima v lasti eno trgovino in administratorje, ki upravljajo s to trgovino. Ker ima posamezna organizacijska enota v lasti le eno trgovino, s tem lažje nadzorujemo poslovanje.



**Slika 6:** Organizacijska struktura za poslovni model B2C

Slika 6 prikazuje B2C poslovanje in zajema dve trgovini in kupce. Prodajna organizacija prodaja dva sklopa izdelkov in je razdeljena na dve organizacijski enoti, ki vsaka upravlja eno trgovino. Kot primer vzemimo spletno knjigarno. Spletna knjigarna združuje dve trgovini, in sicer trgovina 1 ponuja leposlovje, trgovina 2 pa strokovno literaturo. Kupci kupujejo neposredno v prodajni organizaciji in ne v vsaki trgovini posebej. Posamezne trgovine kupcem niso vidne. S stališča kupca so vse združene v eno trgovino. Takšna delitev na organizacijske enote je namenjena lažjemu vzdrževanju celotnega sistema in je za končne kupce nepomembna. S takšno delitvijo omogočimo, da administratorji lažje urejajo posamezne sklope e-trgovine.

### 3.4 Orodja za delo z WSC

Celoten potek poslovanja spletne trgovine upravljamo in nadzorujemo s pomočjo vmesnikov za delo s platformo IBM WSC. To so Administration Console, WSC Accelerator in Organization Administration Console. S pomočjo Administration Console upravljamo z nastavitvami celotnega

sistema, predvsem z nastavitvami s področja varnosti, arhiva trgovine in oblik sporočil. WSC Accelerator nam omogoča upravljanje s posameznimi trgovinami in produkti, medtem ko z uporabo vmesnika Organization Administration Console upravljamo z uporabniki (jim določamo vloge, uporabniška imena in podobno). V Administration Console prilagajamo pravila, ki jim morajo ustrezati uporabniški računi. Z vmesnikom Organization Administration Console pa uporabnikom dodeljujemo vloge in za konkretnega uporabnika določamo ali pa prilagajamo politike za pravice dostopa tega uporabnika do same trgovine. S pomočjo Administration Console imamo tudi nadzor nad spletno trgovino, potekom sporočanja (način uporabe e-pošte, način izmenjevanja datotek ...) in posodabljanjem komponent. Vmesnik WSC Accelerator pa je namenjen delu s posamezno trgovino. Omogoča nadzor nad trgovino (na primer poimenovanje, določanje logotipa ...) in nad katalogi proizvodov v njej (postavljanje cene, stopnje davka ...).

Vsi podatki o uporabnikih, trgovinah, politikah, katalogih proizvodov ... se beležijo v relacijski podatkovni bazi sistema WSC. Baza vsebuje preko 700 tabel in se namesti samodejno ob namestitvi celotnega IBM WSC. Tabele so po sklopih razporejene v podatkovne modele in so med seboj povezane. Ko s pomočjo WSC vmesnikov izvedemo določeno spremembo (npr. definiramo novo politiko, ustvarimo uporabnika, uporabnik spremeni geslo ...), se to zabeleži v ustrezni tabeli. Prav tako lahko spremembe oz. nove podatke vpisujemo neposredno (z ustreznimi SQL stavki, kot so INSERT, UPDATE) v določene tabele. Za pregledovanje podatkov v tabelah, vpisovanje in brisanje novih podatkov uporabljamo sistem za upravljanje s podatkovno relacijsko bazo IBM DB2.

Z vlogo je določeno, kaj uporabnik nadzira ali s čim upravlja. Meniji v vmesnikih se prilagajajo glede na uporabnikovo vlogo. S tem uporabnik vidi le tiste ukaze, katere lahko izvaja. S celotnim sistemom in podatki upravljajo samo tisti uporabniki, ki imajo vlogo glavnega administratorja (angl. *Site Administrator*).

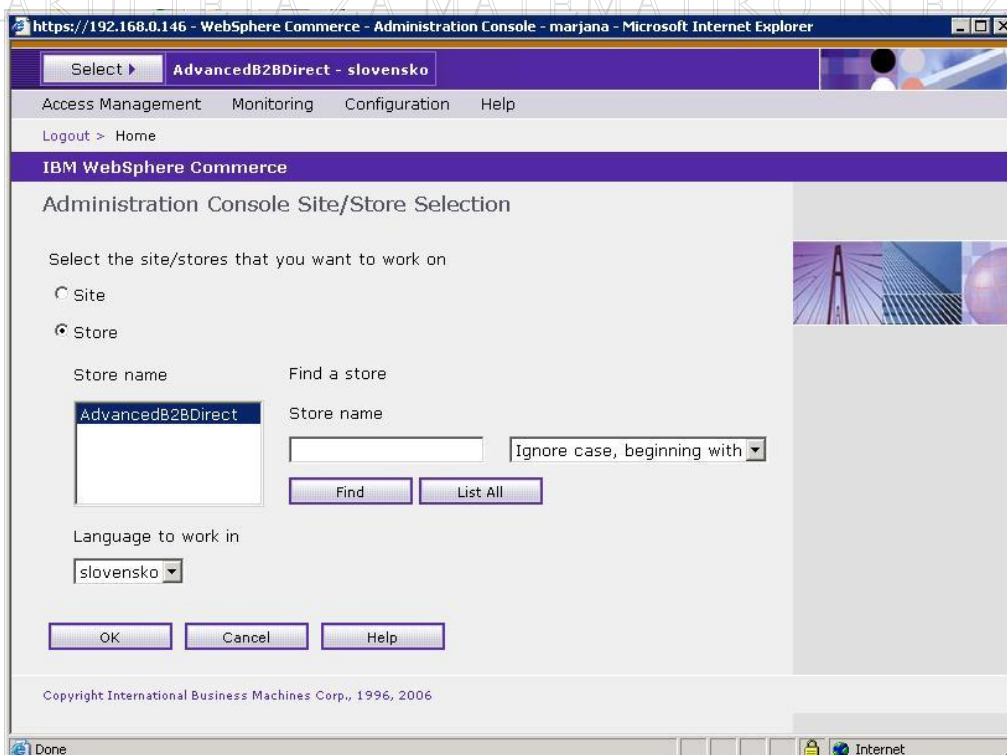
### 3.4.1 Administration Console

Kot je že omenjeno v razdelku 3.4, s pomočjo vmesnika Administration Console upravljamo s celotnim sistemom, trgovinami, varnostjo ter oblikami sporočil.

Dostop do vmesnika Administration Console ima samo uporabnik z vlogo glavnega administratorja. Vsem ostalim uporabnikom je dostop onemogočen.

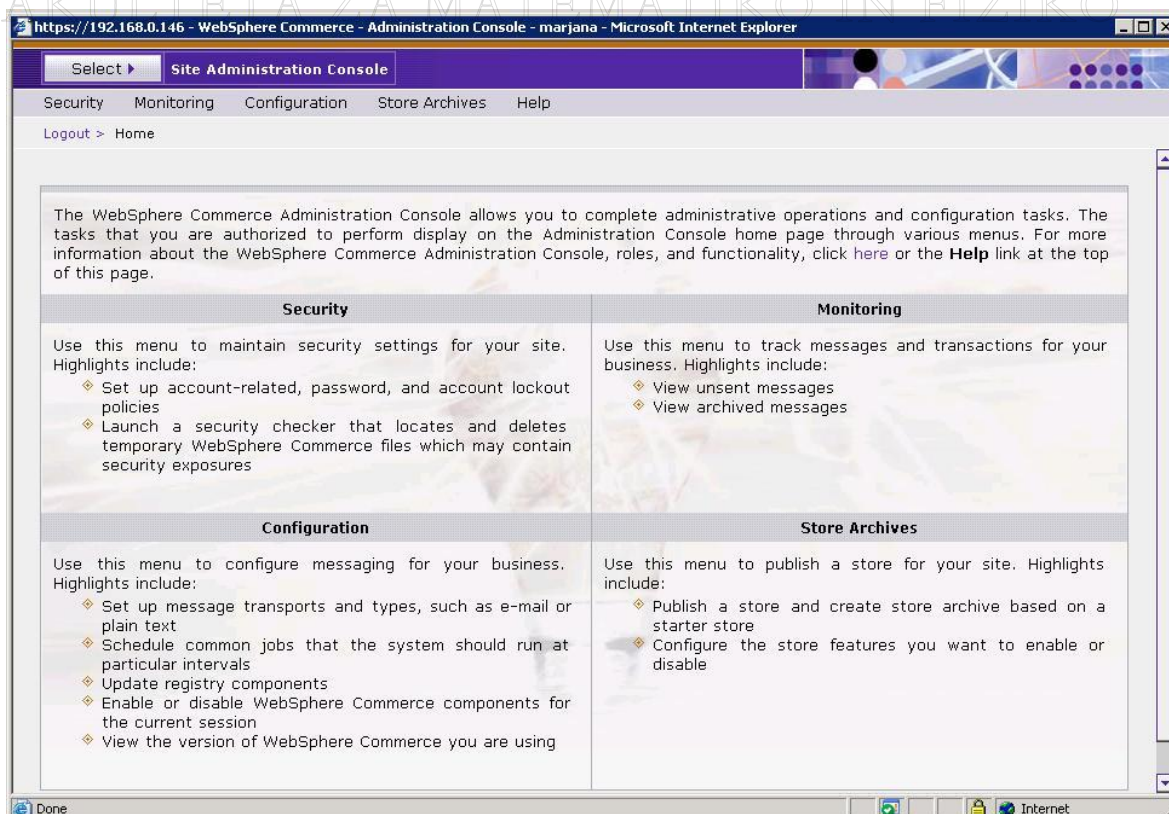
Ob vstopu v vmesnik izberemo, ali bomo upravljali s spletno stranjo (ang. *site*) ali le s posamezno trgovino (Slika 7). Ne glede na to, kaj izberemo, moramo izbrati jezik, v katerem delamo. Nekaj jezikov obstaja privzeto v sistemu, lahko pa ustvarimo še druge. Celoten meni vmesnika in opisi so prevedeni v vse že obstoječe jezike. Na sliki Slika 7 smo izbrali slovenski jezik. Ta v sistemu privzeto še ne obstaja, vendar smo ga definirali kasneje. Vmesnik na sliki Slika 8 je »prikazan v slovenskem jeziku«. Ker pa meni dejansko še ni preveden, je prikazan v angleščini (privzeti jezik). Če bi si izbrali na primer italijanščino, ki je privzeto že v sistemu, bi bil meni napisan v italijanščini.

Če izberemo trgovino (angl. *store*), moramo izbrati tudi ime trgovine.



**Slika 7:** Možnost izbire pri vmesniku Administration Console

Kadar izberemo upravljanje s celotno stranjo (*site*), imamo možnost izbire menijev *Security*, *Monitoring*, *Configuration* in *Store Archives* (Slika 8). Meni *Security* omogoča spreminjanje in prilagajanje politik za uporabniški račun (razdelek 4.1). Meni *Monitoring* omogoča nadzor nad poslanimi in neposlanimi sporočili na spletno stran e-trgovine (npr. nove datoteke, ki vsebujejo novo ponudbo) in uporabnikom (sporočanje preko e-pošte npr. ob pravilnem prvem vpisu v e-trgovino ...). S pomočjo menija *Configuration* pa določimo oblike sporočanja. Tako lahko določimo, v kakšnih oblikah (e-pošta, izpis na strani ...). bodo uporabniki dobivali razna obvestila. Prav tako s pomočjo tega menija spremljamo uspešnost posodabljanja posameznih komponent v sistemu. Ko v sistemu na novo definiramo politiko, skupine akcij ..., je posodabljanje pomembno zato, da sledimo »novostim« in da vidimo, ali so se spremembe zabeležile. V meniju *Store Archives* se hranijo podatki – spremembe in novosti (nove objave izdelkov ...), ki so se izvajale v trgovini.

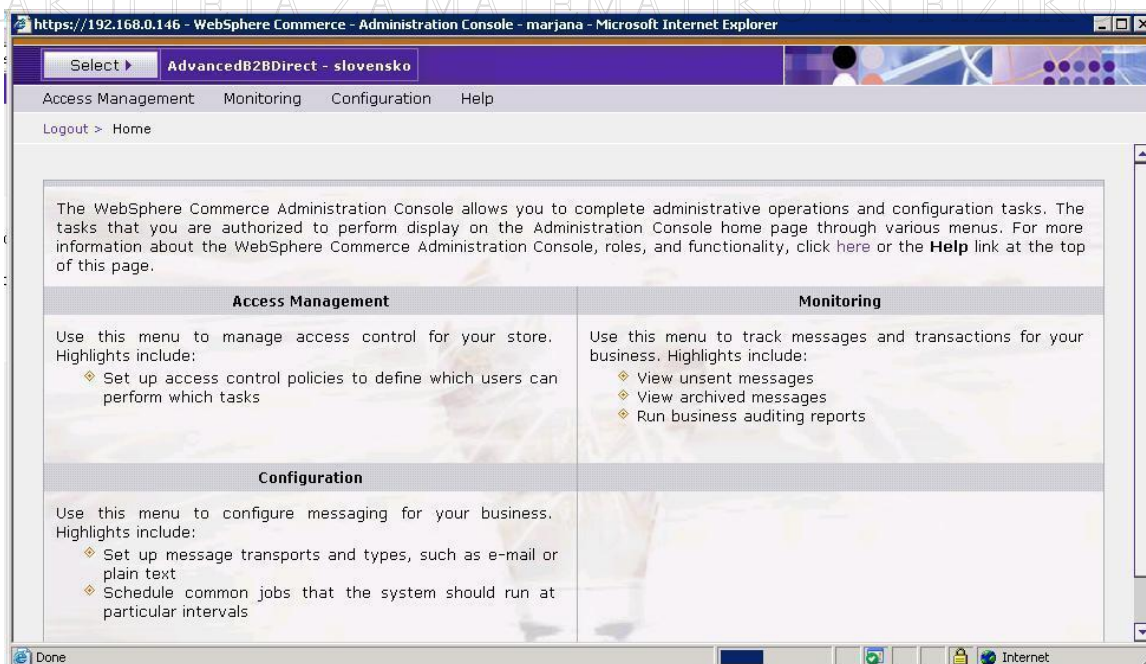


**Slika 8:** Meni vmesnika Administration Console – izbira site

Če na začetku izberemo upravljanje trgovine, dobimo možnost izbire treh menijev - *Access Management*, *Monitoring* in *Configuration* (Slika 9). Z ukazi prvega menija pregledujemo, dodajamo, brišemo in spreminjamo politike dostopa (razdelek 5.1). Bolj natančno s politikami dostopa, akcijami, uporabniki in viri upravljamo s pomočjo vmesnika Organization Administration Console (razdelek 3.4.3).

Meni *Monitoring* ima enake možnosti, kot pri izbiri *site*, le da pri trgovini poleg sporočil lahko pregledujemo vse transakcije (nakup, prodaja ...), ki so jih izvajali posamezni uporabniki v posamezni trgovini.

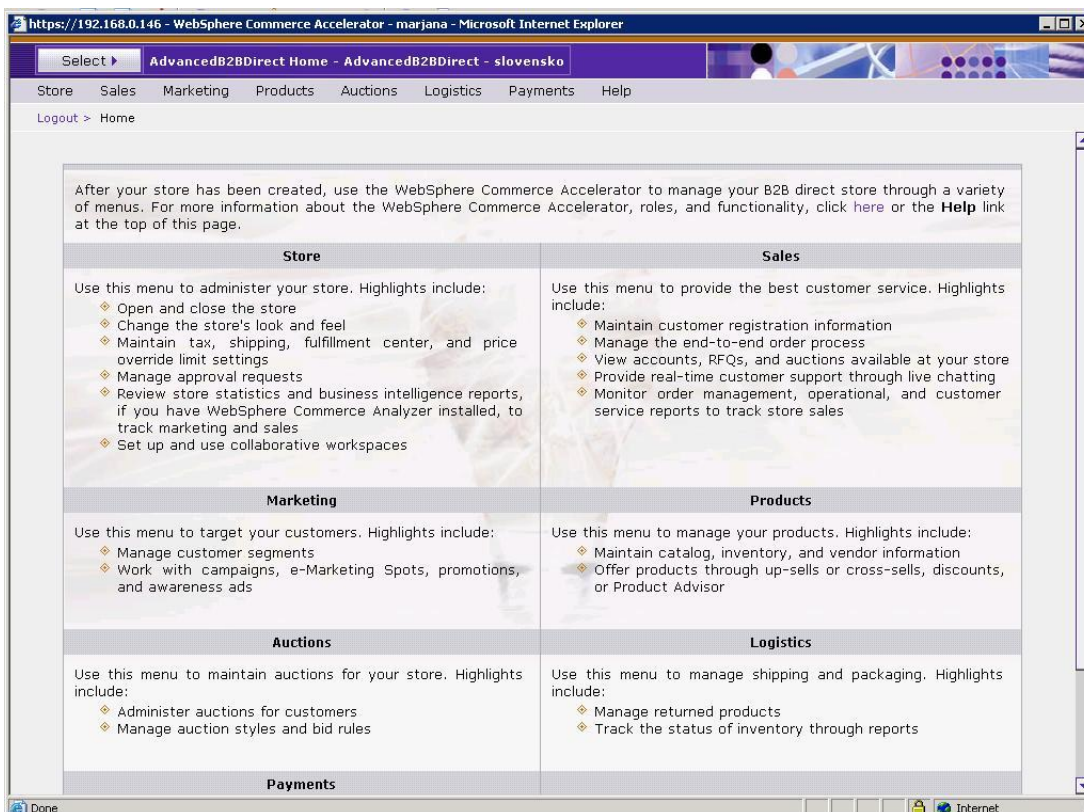
Pri izbiri menija *Configuration* določamo način sporočanja sistema uporabnikom (preko e-pošte, kot besedilo na strani) ter pregledujemo, ali so se posodobile vse komponente, kot so nove politike dostopa, akcije, viri ... Torej imamo s tem nadzor nad novimi definicijami. Kadar novo politiko definiramo v formatu XML (razdelek 5.2.3), šele tu dosežemo, da se posodobitve dejansko izvedejo.



Slika 9: Meni vmesnika Administration Console – izbira store

### 3.4.2 WSC Accelerator

S pomočjo vmesnika WSC Accelerator upravljamo s posameznimi trgovinami znotraj sistema Commerce, s katalogi produktov, prodajo, marketinškimi elementi (akcije, posebne ponudbe, dražbe, oglasi ...), načini plačila, logistiko, skladiščenjem ...



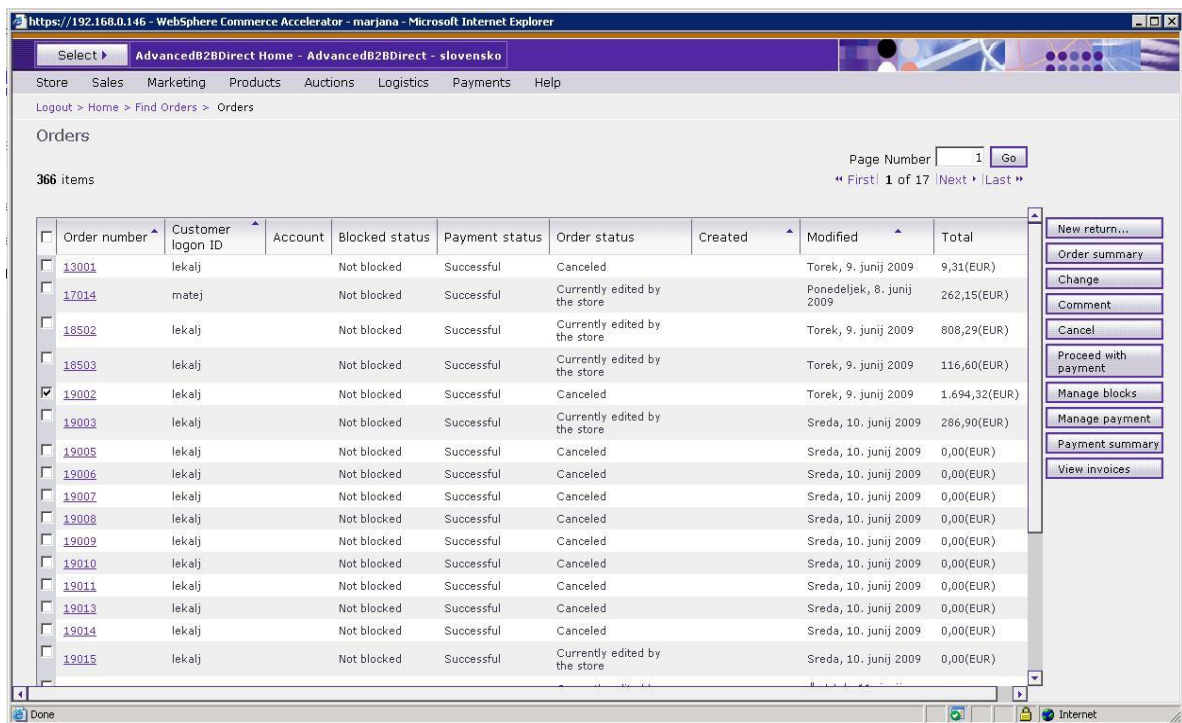
Slika 10: Meni vmesnika WSC Accelerator

Kot smo že omenili, je dostop do posameznih menijev, omenjenih v nadaljevanju, omejen glede na vlogo uporabnika. Glavni administrator ima dostop do vseh menijev, medtem ko imajo uporabniki z drugimi vlogami omejen dostop. Meni, do katerega ima posamezen uporabnik dostop, je prikazan, vsi ostali meniji pa so uporabniku prekriti.

S pomočjo menija *Store* trgovino zapiramo in odpiramo (torej določamo, ali je trgovina dostopna), spreminjamo naslov trgovine, definiramo davčne stopnje ... Meniji *Sales*, *Logistics* in *Marketing* nam omogočajo nadzor nad prodajo, naročili, promocijami, nadzor nad vrnjenim blagom ...

V trgovini izvajamo tudi dražbe. Te pregledujemo in iščemo s pomočjo izbire menija *Auction*.

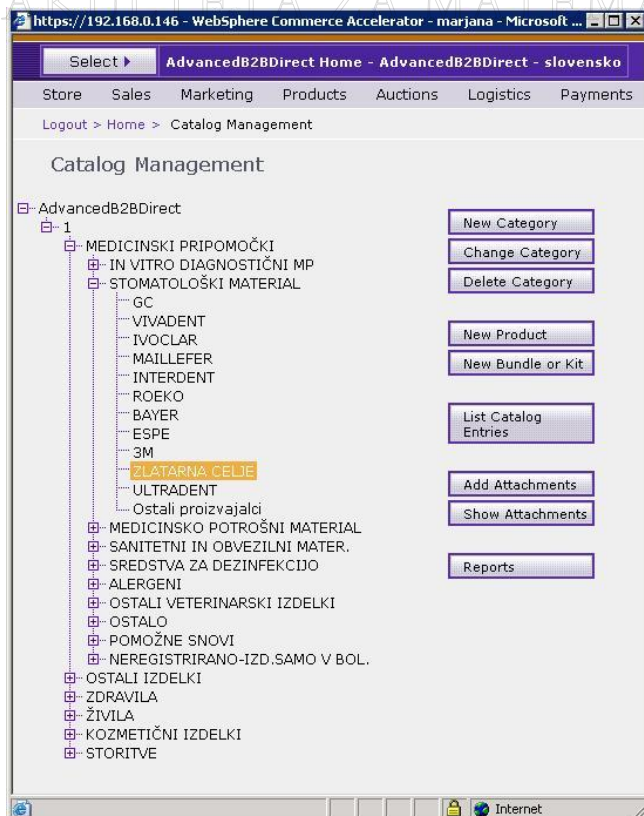
Meni *Products* nam omogoča nadzor nad produkti, katalogi, celotno zalogo v trgovini in podobno. S pomočjo menija *Payments* spremljamo plačila.



| Order number | Customer logon ID | Account | Blocked status | Payment status | Order status                  | Created                   | Modified | Total         |
|--------------|-------------------|---------|----------------|----------------|-------------------------------|---------------------------|----------|---------------|
| 13001        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Torek, 9. junij 2009      |          | 9,31(EUR)     |
| 17014        | matej             |         | Not blocked    | Successful     | Currently edited by the store | Ponedeljek, 8. junij 2009 |          | 262,15(EUR)   |
| 18502        | lekaj             |         | Not blocked    | Successful     | Currently edited by the store | Torek, 9. junij 2009      |          | 808,29(EUR)   |
| 18503        | lekaj             |         | Not blocked    | Successful     | Currently edited by the store | Torek, 9. junij 2009      |          | 116,60(EUR)   |
| 19002        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Torek, 9. junij 2009      |          | 1.694,32(EUR) |
| 19003        | lekaj             |         | Not blocked    | Successful     | Currently edited by the store | Sreda, 10. junij 2009     |          | 286,90(EUR)   |
| 19005        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19006        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19007        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19008        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19009        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19010        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19011        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19013        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19014        | lekaj             |         | Not blocked    | Successful     | Canceled                      | Sreda, 10. junij 2009     |          | 0,00(EUR)     |
| 19015        | lekaj             |         | Not blocked    | Successful     | Currently edited by the store | Sreda, 10. junij 2009     |          | 0,00(EUR)     |

Slika 11: Seznam naročilnic

Slika 11 prikazuje seznam vseh naročilnic. Do tega seznama dostopamo z uporabo menija *Sales* in podmenija *Find Orders*. Vsaka naročilnica ima svojo številko, uporabniško ime naročnika, informacijo o tem, ali je bila naročilnica zabeležena, plačana, poslana, kdaj je bila ustvarjena ter celoten znesek naročenega blaga. Pri vsaki naročilnici lahko pogledamo seznam naročenih produktov, kraj in dan dostave. Če smo v vlogi administratorja, naročilnice poljubno brišemo s seznama.



Slika 12: Katalog izdelkov

Slika 12 prikazuje katalog izdelkov. Do njega dostopamo z uporabo menija *Products* in podmenija *Catalog Management*. Izdelki so razvrščeni po skupinah in znotraj teh po proizvajalcih proizvodov. Če želimo pogledati seznam proizvodov enakega proizvajalca znotraj posamezne skupine, potem izberemo skupino in uporabimo gumb *List Catalog Entries*. Vsak proizvod lahko opišemo s kratkim in dolgim opisom in mu dodamo fotografijo. Le-ta v Acceleratorju ni vidna, prikazana pa je na spletni strani trgovine.

### 3.4.3 Organization Administration Console

Vmesnik *Organization Administration Console* (krajše OAC) nam omogoča nadzor nad organizacijami in uporabniki. Ima tri glavne menije: *Access Management*, *Approvals* in *Help*. S pomočjo menija *Access Management* ustvarjamo uporabnike in organizacije, uporabnikom določamo vloge, definiramo nove politike, akcije, vire ... Vse to omogoča nadzor nad izvajanjem ukazov, ki so dovoljeni posamezniku.

Meni *Approvals* administratorjem omogoča potrjevanje novih uporabnikov. Kadar se nov uporabnik (kupec kot posameznik ali trgovina) pojavi v določeni organizaciji, ga mora administrator te organizacije potrditi, lahko pa ga tudi zavrne.

V vmesnik OAC lahko vstopa vsak, vendar je to, kaj dela, določeno z njegovo vlogo. Če se uporabnik prijavi kot glavni administrator, ima vse pravice. Če pa je njegova vloga na primer prodajni administrator (angl. *Seller Administrator*), so njegove pravice omejene. Uporabnik s tako vlogo ne more določati in spreminjati politik, vlog, akcij, virov, lahko pa ustvari novega uporabnika ali organizacijo. Tudi tu možnosti, do katerih uporabnik (zaradi neustrezne vloge) ne more dostopati, niso prikazane. Vsak registriran uporabnik pa ima možnost dostopa do izbire menija *Help*.



**Slika 13:** Pogled glavnega administratorja na meni vmesnika Organization Administration Console

## 4 AVTENTIKACIJA

Avtentikacija je proces prepoznavanja uporabnika, ki se je prijavil v sistem ali na spletno stran. Sistem WSC zahteva, da mora uporabnik ob prijavi vpisati uporabniško ime in geslo. Kakšen mora biti uporabniški račun, kako mora biti sestavljeno geslo uporabnika in koliko časa je veljavno, je določeno s politiko za uporabniški račun.

### 4.1 Politika za uporabniški račun

Vsak uporabnik ima svoje uporabniško ime in geslo. Ob prijavi uporabnika se mora kombinacija uporabniškega imena in gesla ujemati. Gesla in uporabniška imena se hranijo v WSC v relacijski podatkovni bazi. Gesla so v bazi kriptirana, kar pomeni, da so zapisana kodirano. Geslo v nekriptirani obliki ni vidno nikomur.

S pomočjo različnih pravil določimo, kakšno mora biti uporabniško ime in kakšno geslo. Skupek pravil imenujemo politika za uporabniški račun (angl. *account policy*). Politika za uporabniški račun zajema politiko gesla (angl. *password policy*) in politiko začasnega omejevanja (angl. *account lockout policy*). Politika je torej spisek pravil, ki jim mora določena stvar zadoščati. Tako je politika gesla spisek pravil, ki jim mora zadoščati geslo.

Sistem WebSphere Commerce ima že vnaprej pripravljene določene politike za račune (razdelek 4.2). Običajno nam ustrezajo že ta. Lahko pa jih prilagodimo. V ta namen uporabimo vmesnik Administration Console (razdelek 4.3). Politike za uporabniški račun vedno prilagajamo kategorijam uporabnikov, na primer kupcem in administratorjem in ne vsakemu posamezniku. Če želimo, da določena politika velja le za posameznika, ustvarimo ustrezno kategorijo in vanj dodelimo tega posameznika. Politiko pa potem predpišemo za to novo ustvarjeno kategorijo.

#### 4.1.1 Politika gesla

Za vstop v sistem mora uporabnik vpisati uporabniško ime in geslo. Zagotoviti je potrebno, da je geslo tako, da ga nepooblaščen ne more hitro uginiti. V ta namen je določenih nekaj pravil, ki se jih mora uporabnik držati pri izbiri gesla. Ta pravila imenujemo politika gesla.

Nekaj pravil za gesla:

- Določeno je največje število enakih zaporednih znakov, ki jih geslo vsebuje.
- Določeno je največje število enakih znakov, ki se pojavljajo v geslu.
- Opredeljena je najmanjša dolžina (število znakov) gesla.
- ...

Vsako geslo ima življenjsko dobo, ki se določi glede na to, kakšno vlogo ima uporabnik (ali je administrator ali kupec). Ko geslu poteče življenjska doba, uporabnik s tem geslom ob prvi naslednji prijavi dobi zahtevek, da mora geslo spremeniti. Kakšna je življenjska doba gesla, določa ustrezno pravilo v sklopu politike gesla.

Privzeto je nastavljeno tudi pravilo, da mora biti vsako novo geslo različno od že prej uporabljenih. Podrobnosti glede pravil, ki jih uporabljamo pri politiki gesel in njihovega nastavljanja, si bomo ogledali v razdelku 4.3.

#### 4.1.2 Politika začasnega omejevanja dostopa

Politika začasnega omejevanja dostopa dodatno preprečuje zlorabe pri prijavi uporabnika. Ob vpisu na spletno stran ali v kakšen drug sistem mora uporabnik vnesti uporabniško ime in geslo. Kombinacija teh dveh se mora ujemati. Če vnos ni pravilen, uporabnik vpis ponovi. Število

napačnih zaporednih vnosov je omejeno. Če je prekoračeno, se uporabnik nekaj časa ne more prijaviti. Koliko sme biti zaporednih napačnih vnosov, je določeno s pravilom. Prav tako pravilo določa čas, ki mora preteči po prekoračenem številu poskusov prijave, da uporabnik lahko znova poskusi s prijavo.

## 4.2 Privzeti politiki za uporabniški račun

WebSphere Commerce vsebuje dve privzeti politiki uporabniških računov. Namenjeni sta dvema kategorijama uporabnikov, kupcem in administratorjem. Razlike med pravili, ki skupaj sestavljajo politiki za uporabniški račun, poimenovani politika za kupce oziroma politika za administratorje ponazarja Tabela 1.

**Tabela 1:** Pravila za račun

| Pravilo                                                                            | Privzeta vrednost<br>(kupci) | Privzeta vrednost<br>(administratorji) |
|------------------------------------------------------------------------------------|------------------------------|----------------------------------------|
| Število poskusov, preden se račun onemogoči*                                       | 6 poskusov                   | 3 poskusi                              |
| Koliko časa mora preteči po neuspešnem poskusu vnosa uporabniškega imena in gesla? | 10 sekund                    | 20 sekund                              |
| Ali se uporabniško ime in geslo lahko ujemata?                                     | ne                           | ne                                     |
| Največje dovoljeno število zaporednih znakov istega tipa**                         | 3                            | 3                                      |
| Največje dovoljeno število enakih znakov v geslu***                                | 4                            | 4                                      |
| Življenjska doba gesla                                                             | 180 dni                      | 90 dni                                 |
| Najmanjše število črk v geslu                                                      | 1                            | 1                                      |
| Najmanjše število števk v geslu                                                    | 1                            | 1                                      |
| Najmanjša dolžina gesla                                                            | 6 znakov                     | 8 znakov                               |
| Ali lahko ponovno uporabimo katerokoli prejšnje geslo?                             | ne                           | ne                                     |

\* Ob večkratnem napačnem vnosu uporabniškega imena ali gesla se račun onemogoči. Ponovno uporabo lahko omogoči samo glavni administrator.

\*\* Geslo »geslo1« ni v skladu s tem pravilom, ker je zaporedno število malih črk 5 in ne samo 3. »Geslo1« pa je pravilno, saj vsebuje dve zaporedni veliki črki, tri male črke in eno številko, kar pa je v skladu s tem pravilom.

\*\*\* Geslo »amamamiala« ni ustrezno, ker se črka »a« ponovi več kot štirikrat, geslo »mamamiala« pa je, vsaj kar se tiče tega pravila, pravilno.

## 4.3 Prilagajanje politike za uporabniški račun

Če nam vnaprej definirani politiki za uporabniške račune, ki sta opisani v razdelku 4.2, ne ustrezata, ju spremenimo. To storimo preko vmesnika Administration Console (razdelek 3.4.1). Prav tako lahko definiramo novo politiko, ki zajema novo kategorijo uporabnikov.

Pravila pri politiki gesla nastavimo na takšne vrednosti, ki zahtevajo od uporabnika geslo ustrezne kompleksnosti. Izbira gesla pa je na koncu še vedno stvar posameznika.



**Slika 14:** Kako so pravila razdeljena glede na kategorije uporabnikov

Z izbiro menija *Security* in podmenija *Account policy* odpremo seznam politik za račune (Slika 14). Politike lahko izbrisemo ali spremenimo. Če želimo na primer spremeniti politiko za kupce (na sliki Slika 14 je ta kategorija poimenovana s privzetim imenom *Shoppers*), kategorijo označimo in kliknemo na gumb *Change*. Prikaže se politika za kupce (Slika 15). Kot smo omenili že prej, se politika za račun deli na politiko gesla in politiko začasnega omejevanja dostopa. Na sliki vidimo, kateri dve politiki sestavljata politiko za uporabniški račun kupcev. V tem primeru politiko za kupce sestavlja politika gesla za kupce in politika začasnega omejevanja prav tako za kupce. Namesto teh dveh politik lahko izberemo tudi druge pripravljene politike. Če torej želimo, da bi imeli kupci enako politiko gesla kot administratorji, v spustnem seznamu pri *Password policy* izberemo administratorje in potrdimo.



**Slika 15:** Politika za kupce

Če nam nobena od obstoječih politik, med katerimi lahko izbiramo, ne ustreza, definiramo novo politiko. Kot primer definirajmo novo politiko gesla, ki bo namenjeno predvsem tistim uporabnikom, ki so študentje.

Izberemo meni *Security* in podmeni *Password policy* ter gumb *New*. Prikažejo se polja, v katera vnesemo željene vrednosti (Slika 16).

https://192.168.0.146 - WebSphere Commerce - Administration Console - marjana - Microsoft Internet Explorer

Select Site Administration Console

Security Monitoring Configuration Store Archives Help

Logout > Home > Password Policy > Change Password Policy

OK Cancel

### Password Policy

Define the criteria for a password policy.

Name (required)  
student

Can the userId and password match? (required)  
Yes

Maximum consecutive character types (required)  
2

Maximum instances of any character (required)  
4

Maximum lifetime of the password (days) (required)  
120

Minimum number of alphabetic characters (required)  
0

Minimum number of numeric characters (required)  
0

Minimum length of the password (required)  
6

Can the password be reused? (required)  
No

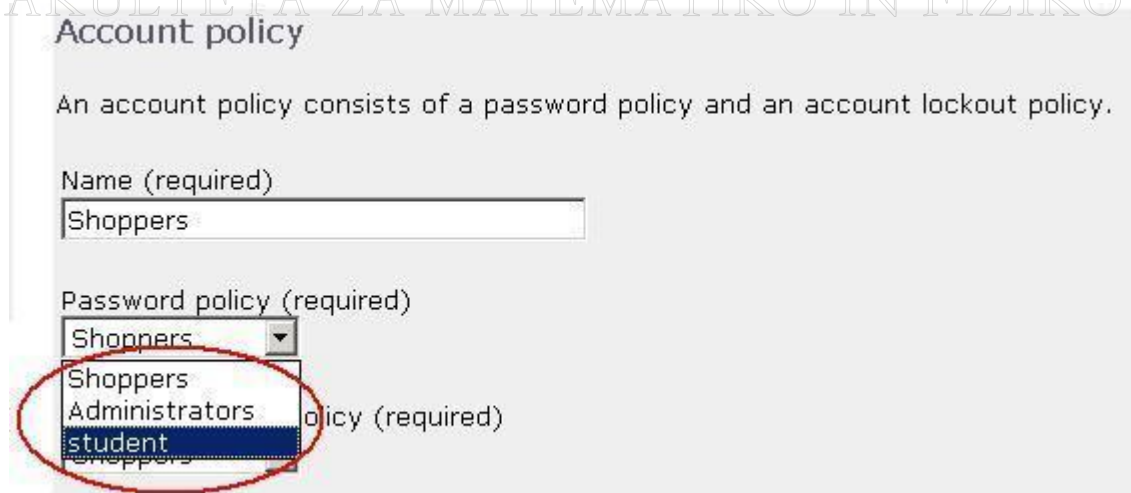
Done Internet

**Slika 16:** Nova politika gesla

Slika 16 prikazuje novo politiko gesla, namenjeno študentom. Določimo ime politike, ki naj bo *student*. Nato izpolnimo zahtevana polja in novo politiko gesla potrdimo s klikom na gumb *OK*.

Opišimo pravila s sliko Slika 16, ki sestavljajo to politiko. Uporabniško ime in geslo sta lahko enaka, vendar se geslo ob zamenjavi, ki je obvezna na 120 dni, ne sme ponoviti. Novo geslo ne sme biti enako kateremukoli izmed prejšnjih gesel. Geslo mora imeti najmanj šest znakov. Ker sistem loči znake glede na tip (velike in male črke, številke ...), smo v tem primeru določili, da sta samo dva zaporedna znaka lahko enakega tipa. Enak znak v geslu se lahko pojavi največ štirikrat. Geslo lahko vsebuje samo črke ali samo številke, kombinacija obeh ni potrebna.

To novo definirano politiko gesla, ki je prikazana na sliki Slika 16, lahko uporabimo pri sestavi nove politike za uporabniški račun. Slika 17 prikazuje, katere možnosti imamo, ko za kupce določamo politiko za uporabniški račun. V tem primeru lahko za kupce izberemo politiko gesla, ki je prilagojena kupcem, administratorjem ali študentom.



**Slika 17:** Možnost izbire pri politiki gesla

Vsako politiko gesla ali politiko za omejevanje dostopa lahko tudi spreminjamo. To storimo na podoben način, kot smo definirali novo politko. Razlika je le v tem, da najprej izberemo politiko gesla ali politiko za omejevanja dostopa, ki jo želimo spremeniti. Če izberemo politiko gesla, se nam odpre seznam pravil, kot je viden na sliki Slika 16. Nato spremenimo željene vrednosti in potrdimo s klikom na gumb *OK*.

Kot je že omenjeno v razdelku 3.4.1, s politikami za uporabniške račune upravlja samo uporabnik z vlogo glavnega administratorja.

## 5 AVTORIZACIJA

Avtorizacija je proces nadzora dostopa do določenih virov (razdelek 5.1.3), ki so pod nadzorom sistema. Običajno gre za to, da uporabnik želi dostopati do določenega vira, sistem pa preveri, ali to lahko stori.

Ko se uporabnik prijavi, ga sistem s pomočjo avtentikacije (razdelek 4) prepozna. Če avtentificirani uporabnik želi izvajati ukaze, ki zahtevajo dostop do določenih virov, proces za nadzor dostopa preveri, ali ima uporabnik pravico za dostop do teh virov. Ta proces je proces avtorizacije.

Za avtorizacijo posameznega uporabnika je potrebno imeti definirano politiko dostopa za skupino uporabnikov, v kateri je ta uporabnik.

### 5.1 Politika dostopa

Pri avtentikaciji smo ustrezen postopek preverjanja poimenovali politika. Ta je bila sestavljena iz več pravil. Za avtorizacijo uporabnika pa so vsi posamezni varnostni postopki sestavljeni le iz enega pravila. Glede na to, da je angleški izraz v obeh primerih *policy*, bomo tudi pri avtorizaciji uporabili izraz »politika«.

Politika dostopa (ang. *access control policy*) določa, katera skupina uporabnikov opravlja nek niz ukrepov (registriranje uporabnikov, posodabljanje katalogov produktov, vodenje spletne trgovine ...) na spletni strani.

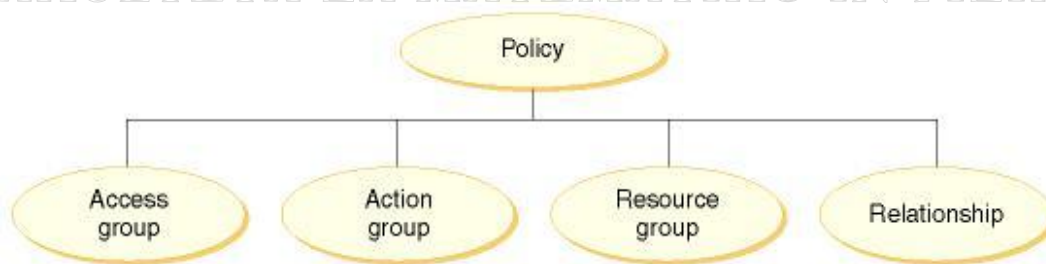
Politike uporabnikom dovoljujejo izvedbo akcij nad določenimi viri. Ko uporabnik želi izvesti akcijo nad virom, se preveri, ali mu je le-to dovoljeno. Če obstaja vsaj ena politika, ki to dovoljuje, potem lahko uporabnik izvede željeno akcijo nad virom. Če ustrezne politike ni, potem uporabnik akcije ne more izvesti.

Vsaka politika za nadzor dostopa se nanaša na štiri področja:

- Skupina uporabnikov (angl. *access group*): Določimo skupino uporabnikov, ki jim je politika namenjena (razdelek 5.1.1).
- Skupina akcij (angl. *action group*): Določimo akcije, ki jih uporabniki izvajajo nad viri (razdelek 5.1.2).
- Skupina virov (angl. *resource group*): Določimo vire, nad katerimi določeni uporabniki izvajajo akcije (razdelek 5.1.3).
- Relacije (angl. *relationship*): Z relacijami je določeno razmerje med uporabniki in viri. Z relacijami še dodatno definiramo, v kakšnem razmerju morata biti uporabnik in vir, da uporabnik lahko izvede akcijo nad virom (razdelek 5.1.4).

Pri definiranju politike zapis relacij ni obvezen, medtem ko so skupina uporabnikov, akcij in virov sestavni del vsake politike.

Celoten nadzor nad politikam, uporabniki, akcijami, viri in relacijami ima samo uporabnik z vlogo glavnega administratorja.



**Slika 18:** Področja, ki sestavljajo politiko  
(vir: <http://publib.boulder.ibm.com/infocenter/wchelp/v6r0m0/index.jsp>)

### **Primeri politik:**

Oglejmo si dva primera politik. Da bo bolj nazorno, bomo z barvami označili, za kateri sestavni del politike gre. Navedli bomo le imeni politik in njune sestavne dele. Kako pa so te politike dejansko videti, si bomo ogledali v nadaljevanju.

1. Politika, ki dovoljuje vsem uporabnikom, da lahko pregledujejo tista naročila, ki so jih ustvarili sami.

Ime politike: **AllUsersDisplayOrderDatabeanResourceGroup**

Skupina uporabnikov: **vsi uporabniki** (*AllUsers*)

Skupina akcij: **prikazovanje podatkov** (*DisplayDatabeanActionGroup*)

Skupina virov: **podatki o naročilih** (*OrderDatabeanResourceGroup*)

Relacija: ustvarjalec/avtor (*Creator*)

2. Politika, ki dovoljuje vsem registriranim uporabnikom, da lahko pripravljajo/sestavljajo naročila.

Ime politike:

**RegisteredCustomerForOrgExecuteOrderPrepareComandsOnOrderDataResourceGroup**

Skupina uporabnikov: **registrirani uporabniki v organizaciji** (*RegisteredCustomerForOrg*)

Skupina akcij: **priprava naročil** (*OrderPrepareComands*)

Skupina virov: **podatki o naročilih** (*OrderDataResourceGroup*)

Relacija: ni določena

Opomba: Besedi *Execute* (izvršiti) in *On* (nad) sta zapisani v imenu politike samo zaradi lažjega razumevanje same politike.

Nekatere skupine uporabnikov, akcij in virov ter nekatere politike dostopa privzeto že obstajajo v sistemu, lahko pa jih na novo definiramo tudi sami. Kako ustvarimo politiko in kje dobimo ustrezne skupine, si bomo ogledali v razdelku 5.2.

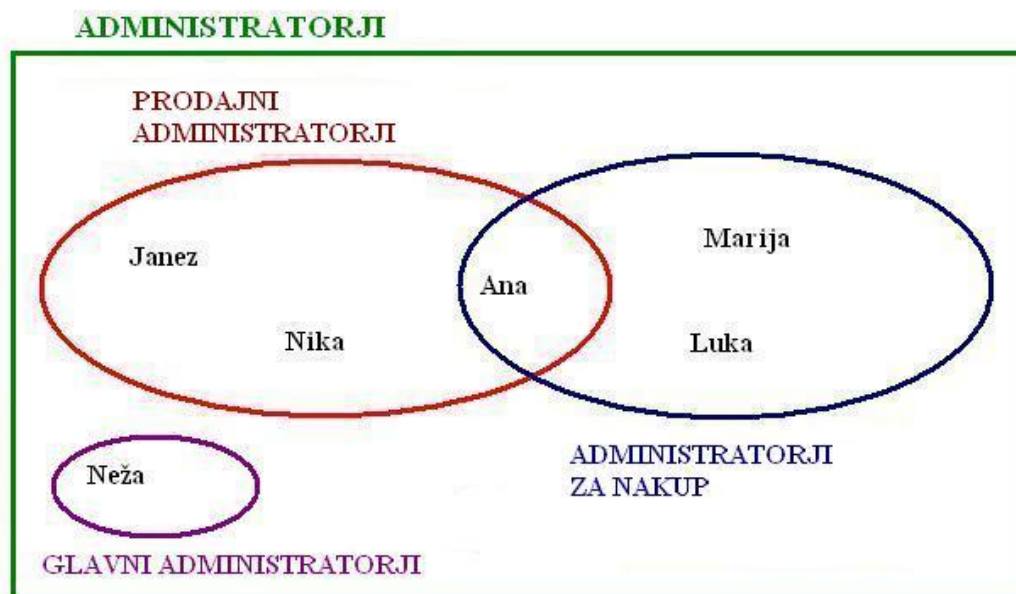
### **5.1.1 Skupine uporabnikov**

Uporabniki so razdeljeni v uporabniške skupine. To omogoča lažji nadzor dostopa kot v primeru, ko bi vsakemu uporabniku posebej dodeljevali pravice. Vsaka skupina uporabnikov izvaja nad viri le določene akcije.

Ob namestitvi platforme WSC dobimo že vrsto skupin uporabnikov (npr. *AllUsers*, *RegisteredCustomerForOrg*, *SiteAdministrators* ...). Za vse te skupine so določeni pogoji, ki jih morajo uporabniki izpolnjevati, da pripadajo določenim skupinam. Običajno je tako pravilo kar to, da uporabnik z določeno vlogo spada v to skupino. Posamezne skupine uporabnikov so sestavljene iz ene ali več vlog (npr. skupina *SiteAdministrators* vsebuje vse uporabnike z vlogo glavnega administratorja) ali pa vsebujejo uporabnike, ki pripadajo določeni organizaciji (npr. skupina *RegisteredCustomerForOrg* vsebuje vse registrirane uporabnike v organizaciji). Že obstoječim

skupinam uporabnikov imen ne moremo spremeniti. Ustvarimo lahko svoje skupine uporabnikov ali pa samo spremenimo (dodamo ali izbrišemo) vloge, ki sestavljajo že obstoječo skupino.

Ko ustvarimo novega uporabnika, mu določimo funkcijo, ki jo bo imel v sistemu. To storimo tako, da mu dodelimo eno ali več vlog. Glede na dodeljene vloge uporabnik potem pripada določenim skupinam uporabnikov. Posamezno skupino uporabnikov lahko sestavlja ena ali več vlog (npr. skupini glavni administratorji in administratorji na sliki Slika 19). V splošnem ima uporabnik vlogo neregistriranega, registriranega uporabnika ali pa vlogo administratorja. Slednjih je več vrst (prodajni, administrator za nakup ...). Uporabniku lahko vlogo dodelimo ali odvzamemo tudi kasneje.



**Slika 19:** Skupine uporabnikov

Slika 19 prikazuje štiri skupine uporabnikov – prodajni in glavni administratorji, administratorji za nakup in skupina administratorjev. Prve tri skupine ustrezajo vlogam (vsebujejo torej točno tiste uporabnike, ki imajo to vlogo), zadnja (skupina administratorjev) pa je sestavljena iz uporabnikov z različnimi vlogami (in seveda je zato ta skupina sestavljena iz ustreznih drugih skupin).

V skupini prodajnih administratorjev so uporabniki, ki imajo vlogo prodajnega administratorja, v skupini glavnih administratorjev so uporabniki z vlogo glavnega administratorja ter v skupini administratorjev za nakup so uporabniki z vlogo administratorja za nakup. Skupina administratorjev vsebuje vse uporabnike, ki imajo vsaj eno izmed naštetih vlog (glavni, prodajni ...). Ana ima vlogi prodajnega administratorja in administratorja za nakup, zato pripada obema skupinama uporabnikov. Poleg tega pa Ana (kot tudi Janez, Luka, Neža ...) pripada še skupini administratorjev. Iz slike Slika 19 je razvidno, da ima en uporabnik lahko več vlog. Takrat zagotovo pripada več skupinam uporabnikov (tak uporabnik je Ana). Prav tako več skupinam uporabnikov lahko pripada tudi uporabnik z eno vlogo (Janez in Nika sta tako v skupini prodajnih administratorjev in v skupini administratorjev, Neža v skupini glavnih administratorjev in administratorjev ...).

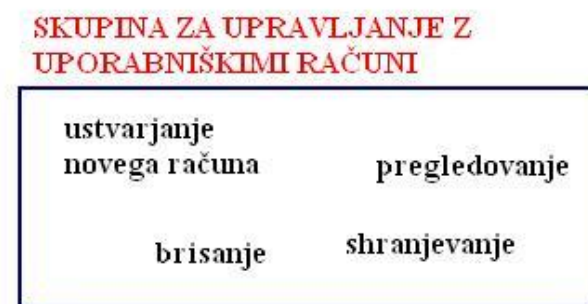
Večina skupin uporabnikov je implicitnega tipa. To pomeni, da takrat, ko ustvarimo skupino, izberemo pravilo, po katerem bodo uporabniki razvrščeni v to skupino. Skupina lahko vsebuje uporabnike glede na status – gosti, registrirani uporabniki, administratorji ali glavni administratorji. Lahko pa kot pogoj določimo željene vloge in organizacije.

Pri eksplicitnem tipu skupine pa sami določimo, kateri uporabniki bodo del skupine. Kako kreiramo novo skupino uporabnikov in kako izbiramo ključne, si bomo ogledali v razdelku 5.2.2.

### 5.1.2 Akcije

Akcije so operacije, ki jih uporabniki izvajajo nad viri. Primeri akcij so pregledovanje izdelkov, izpolnjevanje naročilnic, naročanje, vpisovanje novih uporabnikov ... Razvrščene so v skupine glede na to, nad čim se akcija izvaja. Vsaka skupina akcij vsebuje eno ali več akcij. Nekatere akcije in skupine akcij so ob namestitvi WSC-ja že definirane, vendar jih lahko spreminjamo, brišemo in definiramo nove. Skupine akcij definiramo s pomočjo vmesnika Organization Administration Console (razdelka 3.4.3 in 5.2.1) ali v formatu XML (razdelek 5.2.3).

Primer skupine akcij je skupina, ki vsebuje akcije za upravljanje z uporabniškimi računi, kot prikazuje Slika 20. Ta skupina vsebuje vse akcije, ki jih lahko uporabnik izvrši in s tem vpliva na spremembe posameznega uporabniškega računa.



Slika 20: Skupina akcij

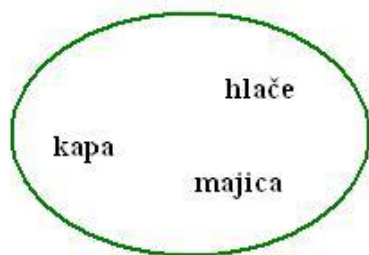
### 5.1.3 Viri

Predstavljeni izdelki, povezave na druge spletne strani, uporabniki, naročilnice ... vse to predstavlja vire (angl. *resource*). Prav tako so viri ukazi, ki jih izvajamo. Do virov lahko uporabniki dostopajo samo v primeru, če obstaja politika, ki to dovoljuje.

Viri so razvrščeni po kategorijah in skupinah. Kategorije virov predstavljajo posamezne vire z enakimi lastnostmi. Če je kategorija virov naročilnica, potem posamezna naročilnica (naročilnica št. 1, naročilnica št. 2 ...) predstavlja vir. V katero kategorijo sodi posamezen vir, določimo s pomočjo zapisa v formatu XML (razdelek 5.2.3). Posamezen vir lahko pripada več kategorijam.

Glede na lastnosti so viri na več načinov razvrščeni v posamezne skupine. Tako lahko skupina virov nastane z združevanjem kategorij virov. S tem, ko sami določamo, kateri viri se bodo nahajali v skupini, ustvarimo eksplicitni tip skupine virov. Slika 21 predstavlja skupino izdelkov, ki jo sestavljajo tri kategorije – kapa, hlače in majica. Posamezna kategorija zajema več izdelkov. To na primer pomeni, da kategorija kap vsebuje kape modre, zelene, rumene ... barve. Skupine, ki nastanejo na osnovi kategorij, so eksplicitnega tipa.

**SKUPINA IZDELKOV**



**Slika 21:** Skupina virov – izdelki

Prav tako vire razvrščamo v skupine glede na status, ki ga imajo v sistemu. Za primer vzemimo skupino virov, ki čakajo na potrditev (Slika 22). Kupec izpolni naročilnico, ki jo mora administrator kupcev potrditi. V skupino virov za potrjevanje sodijo novi izdelki, ki jih mora administrator potrditi, preden gredo v prodajo. S tem smo določili pogoj, kateri viri sodijo v skupino za potrjevanje. Viri se avtomatično uvrstijo v to skupino (če imajo ustrezen status), torej je skupina implicitnega tipa.

**SKUPINA VIROV ZA  
POTRJEVANJE**



**Slika 22:** Skupina virov - potrjevanje

Eden izmed načinov razvrščanja virov v skupine je glede na to, katera skupina uporabnikov lahko izvede določen ukaz. V tem primeru so v skupini virov ukazi, ki jih lahko posamezen uporabnik z določeno vlogo izvrši. Kot viri so navedeni ukazi, ki pa nam ne povedo, nad čim uporabnik ta ukaz izvede (Slika 23). Takšna skupina je prav tako eksplicitnega tipa, saj sami določamo, kateri viri bodo del skupine in kateri ne.



Slika 23: Skupini virov glede na vloge

Slika 23 prikazuje dve skupini virov, in sicer skupino virov za vlogo prodajnega administratorja in skupino virov za registriranega uporabnika. V tem primeru se vir »pregledovanje« nahaja v obeh skupinah. Politika, ki vsebuje skupino virov glede na vloge, je na nivoju vlog (razdelek 5.4). Kot je razvidno iz slike Slika 23, so viri (registriranje, potrjevanje in pregledovanje) sami ukazi, ki jih izvedejo uporabniki z vlogo prodajnega administratorja oziroma registrirani uporabniki, ni pa določeno, nad čim izvajajo te ukaze.

Tako implicitne kot eksplicitne skupine virov definiramo s pomočjo vmesnika Organization Administration Console, kot je to opisano v razdelku 5.2.2.

#### 5.1.4 Relacije

Vsaka politika je določena s skupino uporabnikov, skupino akcij ter s skupino virov. Relacija je zadnji del politike, ki pa ni obvezen. Določa razmerje med uporabnikom ali lastnikom vira (uporabnik ali organizacija) in samim virom. S pomočjo relacije še dodatno povemo, kakšno razmerje mora imeti uporabnik do vira, da ima dovoljeno izvajanje akcij.

Kot primer vzemimo politiko, ki vsem registriranim uporabnikom dovoljuje pregledovanje naročil. Ker ne želimo, da registrirani uporabniki pregledujejo prav vsa naročila, politiko omejimo z relacijo. Kot relacijo navedemo, da vsak registriran uporabnik pregleduje samo tisto naročilo, ki ga je sam ustvaril, je torej avtor naročila. S tem smo določili razmerje med uporabnikom in virom. Ker je razmerje med uporabnikom in virom neposredno, je to enostavna relacija.

Na sliki Slika 24 je prikazana enostavna relacija, ki opisuje razmerje med registriranim uporabnikom in naročilom.



Slika 24: Enostavna relacija

Kot primer enostavne relacije vzemimo politiko, ki dovoljuje registriranemu uporabniku pregledovati samo tista naročila, ki jih je sam ustvaril. Če relacije ne bi določili, potem bi registriran uporabnik lahko pregledoval tudi naročila, ki so jih ustvarili tudi drugi in ne samo svojih.

Primer politike, ki vsebuje enostavno relacijo:

*Politika, ki dovoljuje registriranemu uporabniku pregledovati naročila samo, če je njihov avtor.*

Ime politike: RegisteredCustomerExecuteOrderReadComandsOnOrderDataResourceGroup

Skupina uporabnikov: registrirani uporabniki (RegisteredCustomer)

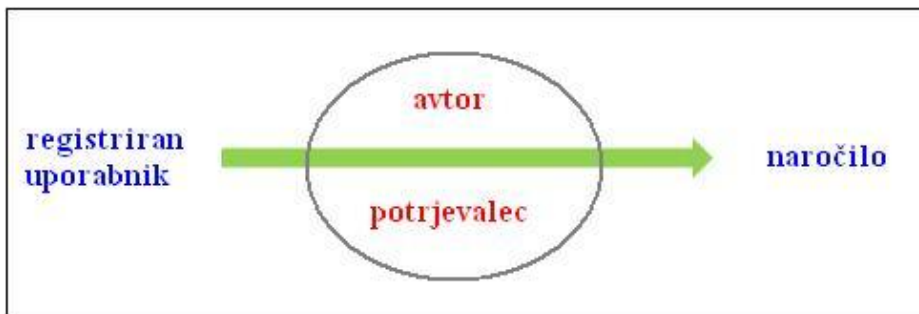
Skupina akcij: pregledovanje (OrderReadComands)

Skupina virov: podatki o naročilih (OrderDataResourceGroup)

Relacija: ustvarjalec/avtor (creator)

Opomba: Besedi *Execute* (izvršiti) in *On* (nad) sta zapisani v imenu politike samo zaradi lažjega razumevanje same politike.

Prav tako kot akcije in viri so tudi relacije združene v različne skupine. Če ima politika več relacij, torej če je določenih več razmerji med uporabnikom in virom, potem te relacije avtomatično predstavljajo skupino. Vzemimo prejšnji primer politike, ki je registriranemu uporabniku dovoljevala pregledovanje naročila le, če je bil njegov avtor. Sedaj dovolimo tudi, da vsak registriran uporabnik pregleduje tista naročila, ki jih je potrdil, če je torej potrjevalec naročil.



**Slika 25:** Skupina relacij

Skupina relacij vsebuje relaciji avtor in potrjevalec (Slika 25). Politika sedaj pravi, da vsak registriran uporabnik lahko pregleduje tista naročila, ki jih je sam ustvaril ali potrdil. V tem primeru ima registriran uporabnik več pravic kot pri politiki, ki vsebuje enostavno relacijo. Politika sedaj dovoljuje registriranemu uporabniku, da lahko pregleduje tista naročila, ki jih je sam ustvaril, in tudi tista naročila, ki jih je potrdil (ni nujno, da je hkrati tudi njihov avtor).

Primer politike, ki vsebuje več relacij – skupino relacij:

*Politika, ki dovoljuje registriranemu uporabniku pregledovati naročila samo, če je njihov avtor ali potrjevalec.*

Ime politike: RegisteredCustomerExecuteOrderReadComandsOnOrderDataResourceGroup

Skupina uporabnikov: registrirani uporabniki (RegisteredCustomer)

Skupina akcij: pregledovanje (OrderReadComands)

Skupina virov: podatki o naročilih (OrderDataResourceGroup)

Relacija: ustvarjalec/avtor ali potrjevalec (creator, approver)

Opomba: Besedi *Execute* (izvršiti) in *On* (nad) sta zapisani v imenu politike samo zaradi lažjega razumevanje same politike.

Do bolj kompleksnih relacij pride, ko želimo predpisati pogoj, da uporabnik pripada tisti organizaciji, ki ima v lasti vir, nad katerim želi izvesti akcijo. Take relacije ne predstavljajo direktne povezave med virom in uporabnikom.



**Slika 26:** Primer kompleksne relacije

Slika 26 prikazuje primer kompleksne relacije. Imamo registriranega uporabnika, organizacijo za nakup, naročilo kot vir ter akcijo pregledovati. Če želi registriran uporabnik pregledovati naročilo, mora pripadati organizaciji za nakup, ki ima v lasti to naročilo. Sama politika ne vsebuje dodatne relacije, vendar je le-ta določena s skupino uporabnikov. Skupina uporabnikov vsebuje vse registrirane uporabnike, ki pripadajo organizaciji za nakup. Ti uporabniki pa lahko izvajajo akcijo pregledovati nad tistimi naročili, ki so v lasti iste organizacije kot uporabnik sam ali njene podorganizacije. Če ne bi bilo z relacijo določeno, kateri organizaciji morata pripadati uporabnik in vir, bi politika dovoljevala vsem registriranim uporabnikom pregledovati naročila neodvisno od organizacije.

Primer politike, ki vsebuje kompleksno relacijo:

*Politika, ki dovoljuje registriranemu uporabniku pregledovati naročila samo, če se nahaja v organizaciji za nakup.*

Ime politike:

**RegisteredCustomerForBuyerOrgExecuteOrderReadComandsOnOrderDataResourceGroup**

Skupina uporabnikov: **registrirani uporabniki v organizaciji za nakup**

(RegisteredCustomerForBuyerOrg)

Skupina akcij: **pregledovanje** (OrderReadComands)

Skupina virov: **podatki o naročilih** (OrderDataResourceGroup)

Relacija: Relacijo določimo, ko definiramo skupino uporabnikov. Ko ustvarimo skupino registriranih uporabnikov, določimo, da v skupino sodijo samo tisti registrirani uporabniki, ki pripadajo organizaciji za nakup (razdelek 5.2.2).

Opomba: Besedi *Execute* (izvršiti) in *On* (nad) sta zapisani v imenu politike samo zaradi lažjega razumevanje same politike.

## 5.2 Kako je definirana politika dostopa

Kot smo povedali, politiko dostopa določajo skupine uporabnikov, skupine akcij ter skupine virov. Lahko je določena tudi relacija, ki predstavlja še dodaten pogoj. Posamezna politika nadzora dovoljuje uporabniku z določeno vlogo izvedbo akcij nad viri.

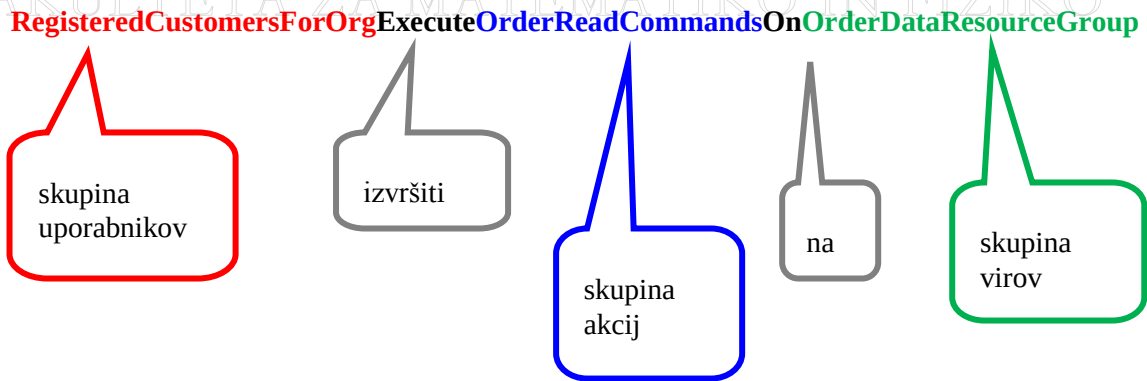
Novo politiko zapišemo s pomočjo vmesnika Organization Administration Console ali kar neposredno v obliki XML.

Vsaka politika ima svoje ime. Praviloma je ime politike sestavljeno tako, da takoj prepoznamo, kateri skupini uporabnikov je namenjena ter na katere akcije se nanaša. Vse politike, ki jih dobimo ob namestitvi sistema WSC, so poimenovane na ta način.

Primer zapisa politike:

Spodaj zapisano ime politike predstavlja politiko, ki dovoljuje vsem registriranim uporabnikom, da lahko berejo naročila. To razberemo iz imena. Politika spada med politike na nivoju virov (razdelek 5.4), ker vsebuje skupine akcij in skupine virov.

Ime politike je sestavljeno iz skupine uporabnikov (rdeča barva), skupine akcij (modra barva) ter skupine virov (zelena barva). V tem primeru sta besedi *execute* in *on* (črna barva) v imenu uporabljeni samo zato, da je prikazano ime politike dovolj razumljivo.

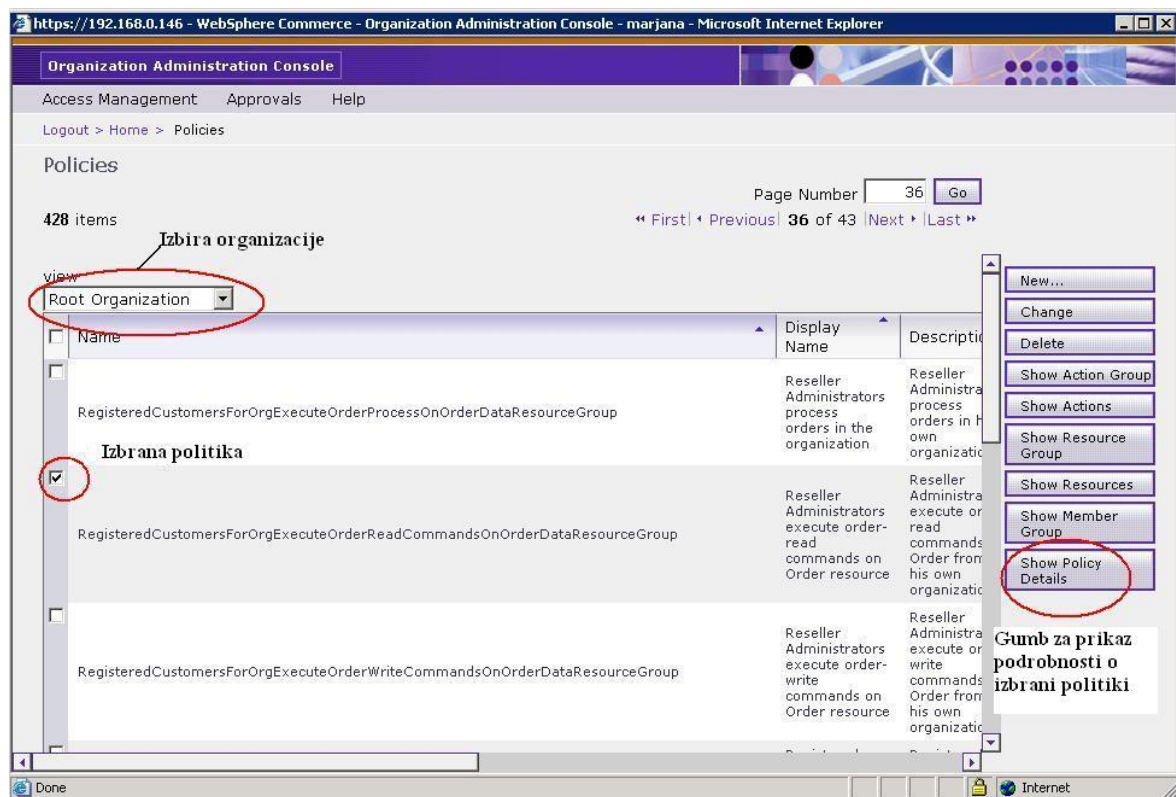


Ko definiramo novo politiko, je priporočljivo, da jo tudi mi poimenujemo na tak način. Le-to omogoča lažji pregled politik.

### 5.2.1 Organization Administration Console

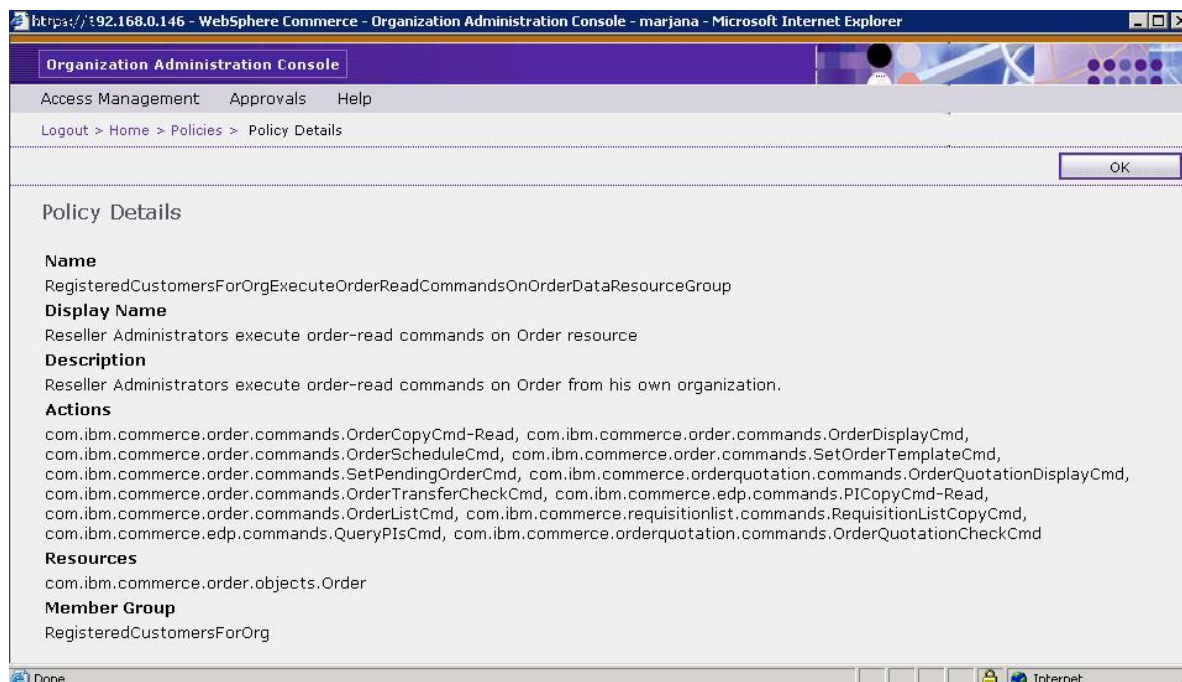
Vmesnik Organization Administration Console (v nadaljevanju OAC) je namenjen spreminjanju in definiranju politik, virov, akcij, uporabnikov ... (razdelek 3.4.3).

Če želimo pregledovati privzete in nove politike, moramo imeti vlogo glavnega administratorja. Ko se prijavimo v vmesnik OAC, v meniju izberemo zavihek *Access Management* in nato *Policies*. Nato izberemo organizacijo, katere politike želimo pregledati. Odpre se seznam politik, ki pripadajo izbrani organizaciji (Slika 27). Med pregledovanjem politik lahko s pomočjo izbirnika, ki je nad seznamom politik, izberemo drugo organizacijo. S tem dobimo seznam politik, ki so v lasti te na novo izbrane organizacije.



Slika 27: Politike, prikazane v vmesniku OAC

Posamezna vrstica tabele na sliki Slika 27 vsebuje ime politike, opis, skupino uporabnikov, skupino akcij, skupino virov ter relacijo. Če želimo pogledati podrobnosti določene politike, le-to označimo ter kliknemo na gumb *Show Policy Details*.



**Slika 28:** Prikaz podrobnosti politike

Slika 28 prikazuje podrobnosti politike, ki dovoljuje vsem registriranim uporabnikom v organizaciji pregledovati naročilnice. Politika je predstavljena z imenom, opisnim imenom in krajšim opisom. Izpisane so vse akcije iz skupine akcij in viri iz skupine virov, ki so del te politike. Izpisana je tudi skupina uporabnikov.

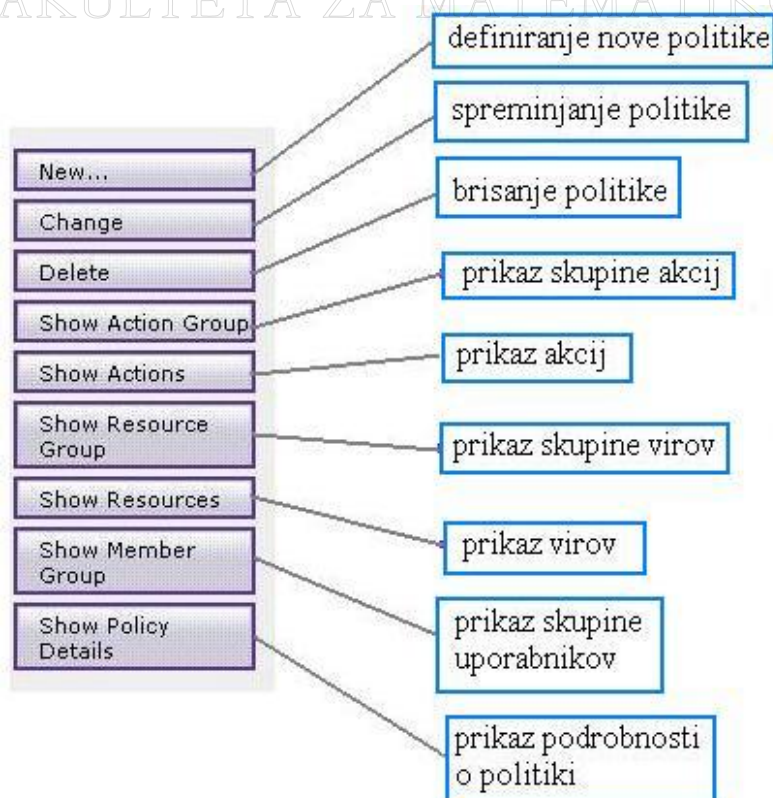
Del te politike je skupina virov, ki vsebuje en sam vir – naročilnico. Naročilnica je predstavljena kot kategorija virov, ki je definirana v javanskem razredu *Order*. Ta je vsebovan v paketu *com.ibm.commerce.order.objects*.

Skupina akcij je neposredno povezana s skupino virov. Že ko definiramo kategorijo virov, navedemo, katere akcije se bodo lahko izvajale nad to kategorijo (razdelek 5.2.3). V našem primeru (Slika 28) skupina akcij vsebuje akcije, ki omogočajo akcijo pregledovati in se izvajajo nad virom naročilnica. Posamezna akcija znotraj skupine predstavlja nek niz ukazov, ki se izvršijo in na koncu uporabniku omogočijo izvedbo željene akcije. Akcija je, prav tako kot vir, definirana v javanskem razredu. V našem primeru skupina akcij vsebuje akcijo *com.ibm.commerce.order.commands.OrderListCmd*, ki prikaže seznam naročilnic, akcijo *com.ibm.commerce.order.commands.OrderDisplayCmd*, ki prikaže naročilnico ...

Paket javanskih razredov *com.ibm.commerce.order.commands* vsebuje ukaze, ki upravljajo z naročilnicami. Ta politika vsebuje akcije tudi iz drugih paketov (npr. *com.ibm.commerce.order.commands.orderquotation*, *com.ibm.commerce.edp.commands* ...).

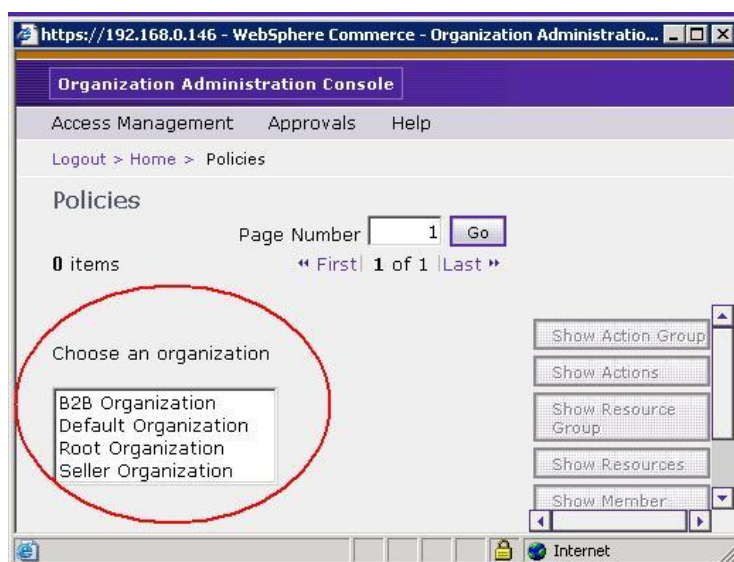
Prav tako imamo možnost pri posamezni politiki pogledati skupino akcij in akcije, skupino virov in vire ter skupino uporabnikov. Politiko lahko tudi brišemo ali spreminjamo.

Vsa ta opravila izvajamo preko gumbov, ki so prikazani na sliki Slika 29. Ti so na voljo šele, ko izberemo oz. označimo željeno politiko.



**Slika 29:** Izbirni gumbi

Gumb, ki je vedno na voljo, je *New*. Če želimo definirati novo politiko, kliknemo nanj. S tem bomo ustvarili politiko za trenutno izbrano organizacijo. Zato moramo najprej izbrati eno izmed organizacij, ki so trenutno v sistemu (Slika 30).



**Slika 30:** Organizacije, ki so trenutno v sistemu

Po kliku na gumb *New* se prikažejo polja, kot je prikazano na sliki Slika 31. Pri definiranju nove politike moramo uporabiti že obstoječe skupine uporabnikov, virov in akcij. Te skupine privzeto obstajajo v sistemu ali pa smo jih že prej kreirali sami. Kako to storimo, je opisano v razdelku 5.2.2.

Slika 31: Definiranje nove politike

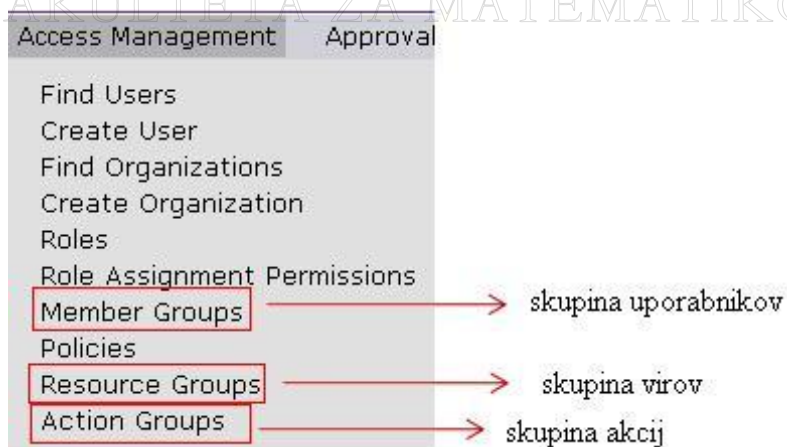
Slika 31 prikazuje novo politiko, ki vsem administratorjem dovoljuje upravljanje z naslovi uporabnikov. Najprej poiščemo željeno skupino uporabnikov. Nato izberemo skupino virov. Glede na izbrano skupino virov imamo možnost izbire skupine akcij, ki jih bodo lahko izvajali izbrani uporabniki. Glede na izbrano skupino uporabnikov in skupino virov lahko določimo relacijo. V primeru na sliki Slika 31 je ne določimo. Na koncu določimo še tip politike. Če želimo, da je ta politika vzorčna politika, le-to označimo. Privzeto gre za standardno politiko (razdelek 5.5).

Nove politike s pomočjo vmesnika OAC ne moremo uvrstiti v skupino politik. To moramo storiti z uporabo zapisa v jeziku XML (razdelek 5.2.3).

## 5.2.2 Definiranje skupin

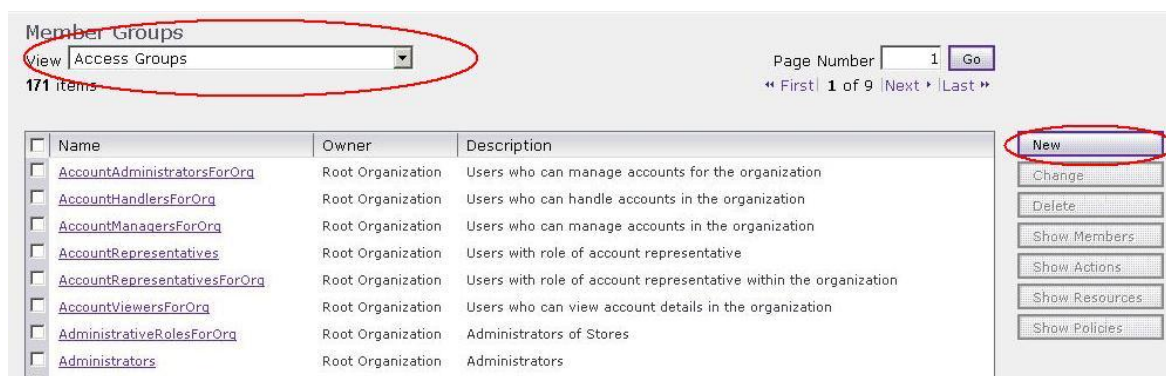
Če pri definiranju nove politike ugotovimo, da potrebujemo novo skupino uporabnikov, virov ali akcij, ustvarjanje nove politike prekinemo in najprej definiramo manjkajoče skupine. To storimo s pomočjo vmesnika OAC.

**Novo skupino uporabnikov** definiramo tako, da v vmesniku OAC izberemo meni *Access Management* in podmeni *Member Groups*, kot kaže Slika 32.



**Slika 32:** Možne izbire podmenijev v vmesniku OAC

Nato izberemo *Access Group* in kliknemo na gumb *New* (Slika 33).



**Slika 33:** Kako definiramo novo skupino uporabnikov

Prikažejo se polja, kot jih prikazuje Slika 34. V polja vpišemo ime skupine ter kratek opis. Nato izberemo, kateri organizaciji bo pripadala ta skupina – *Owner*, in s klikom na gumb *Select* potrdimo izbrano organizacijo ali organizacijsko enoto. Če želimo imeti v tej skupini samo izbrane uporabnike (neodvisno od vloge), izberemo *Add members explicitly* in kliknemo na gumb *Next*.

ber Groups > New Access Group

Next Finish Cancel

**Details**

Member group type  
Access Group

Name (required)  
novaSkupinaUporabnikov

Description  
to je nova skupina uporabnikov

Owner (required)  
Find

☒ Add members explicitly

**Select the organization**

Page Number 1 Go  
« First 1 of 2 Next » Last »

4 items

|                                     | Name              | Parent              | Business Category | Organization Type | Select |
|-------------------------------------|-------------------|---------------------|-------------------|-------------------|--------|
| <input type="checkbox"/>            | B2B Organization  | Seller Organization |                   | Organization Unit |        |
| <input type="checkbox"/>            | B2C Organization  | Seller Organization |                   | Organization Unit |        |
| <input checked="" type="checkbox"/> | Root Organization | None                |                   | Organization      |        |

**Slika 34:** Definiranje nove skupine uporabnikov

Če smo izbrali eksplicitno skupino uporabnikov, se odpre pogovorno okno, kot prikazuje Slika 35, in seznam uporabnikov, ki so trenutno registrirani v sistemu. Dodamo tiste uporabnike, za katere želimo, da bodo pripadali tej novi skupini. To storimo tako, da izberemo uporabnika iz seznama in kliknemo na gumb *Add* ob oknu *Selected members to include*. Če pa želimo, da uporabnik ne bo pripadal skupini, ga izberemo in ob oknu *Selected members to exclude* kliknemo na gumb *Add*. To je smiselno takrat, ko skupina implicitno vsebuje uporabnike z določeno vlogo (npr. prodajni administratorji). Pri tem pa nočemo, da bo v skupini tudi npr. Ana (ki ima tudi vlogo prodajnega administratorja). Z uporabo tega ukaza Ano izbrišemo iz skupine prodajnih administratorjev (vendar ima še vedno vlogo prodajnega administratorja). Uporabnike lahko brišemo iz seznama s klikom na gumb *Remove*.

ber Groups > New Access Group

Previous Next Finish Cancel

**Select Members**

Available members  
gregor  
wcsadmin  
gregor  
ivo  
matej

Search for members  
Match case, beginning with  
Find

Selected members to include  
marjana  
Add  
Remove

Selected members to exclude  
gregor  
Add  
Remove

**Slika 35:** Eksplicitno dodajanje uporabnikov v skupino

Ko smo izbrali vse uporabnike, kliknemo na gumb *Finish*. Če želimo skupini dodati uporabnike še implicitno, kliknemo na gumb *Next*. Odpre se nam pogovorno okno, kot prikazuje Slika 36. Enako pogovorno okno bi se nam prikazalo, če na začetku ne bi izbrali *Add members explicitly* (Slika 34). Če želimo, da uporabniki z določeno vlogo pripadajo točno določeni organizaciji, izberemo *Based on organizations and roles*. Iz seznama izberemo organizacijo in vlogo. Kot prikazuje Slika 36, smo izbrali glavno organizacijo (*Root Organization*) in vlogo prodajalca (*Seller*). Če ne želimo točno določene organizacije, potem izberemo *For organization*<sup>3</sup> ter vlogo s seznama. V našem primeru smo izbrali prodajnega administratorja (*Seller Administrator*). Ko dodamo vse vloge, potrdimo na novo ustvarjeno skupino uporabnikov s klikom na gumb *Finish*.

**Slika 36:** Definiranje implicitne skupine uporabnikov glede na vloge in organizacije

Pri definiranju nove skupine uporabnikov pa imamo tudi bolj enostavno možnost, kako določiti pogoj, kateri uporabniki bodo pripadali tej skupini. V tem primeru ne izberemo kriterija *Based on organizations and roles*, kot smo to storili na sliki Slika 36. Uporabnike lahko dodelimo skupini glede na status, ki ga ima v sistemu. Izberemo torej *Based on registration status* in iz seznama izberemo željeni status, kot kaže Slika 37. Skupino potrdimo s klikom na gumb *Finish*.

<sup>3</sup> Če je politika sestavljena iz skupine uporabnikov z eno ali več vlog in *For organization* (organizacija ni eksplicitno določena), je vzorčna politika (razdelek 5.5).

Slika 37: Definiranje implicitne skupine uporabnikov glede na status

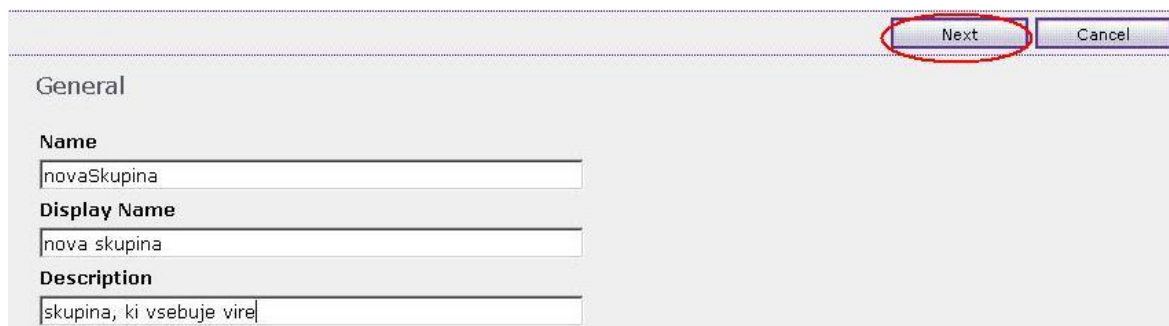
V tem meniju lahko spreminjamo in brišemo tudi obstoječe skupine uporabnikov. To storimo z izbiro skupine uporabnikov in klikom na ustrezen gumb – za spreminjanje na gumb *Change* ter za brisanje na gumb *Delete*.

S pomočjo vmesnika OAC lahko definiramo tudi **ново skupino akcij**. To storimo tako, da v meniju *Access Management* izberemo podmeni *Action Groups* (Slika 32). Odpre se seznam že obstoječih skupin akcij. Na desni strani kliknemo na gumb *New*. Prikažejo se vnosna polja, kamor vpišemo ime nove skupine akcije, opisno ime, opis in iz seznama akcij izberemo tiste akcije, ki bodo pripadale novi skupini (Slika 38). Ko izpolnimo vsa vnosna polja in izberemo akcije, kliknemo na gumb *OK* in s tem potrdimo novo skupino.

Slika 38: Definiranje nove skupine akcij

Seznam akcij lahko spreminjamo (dodajamo ali brišemo akcije iz skupine). S pomočjo vmesnika OAC pa ne moremo definirati nove akcije, saj so akcije predstavljene kot javanski razredi.

Poleg novih skupin uporabnikov in akcij lahko v vmesniku OAC definiramo tudi **nove skupine virov**. To storimo z izbiro menija *Access Management* in podmenija *Resource Groups*. Odpre se seznam vseh že obstoječih skupin virov. Na desni strani kliknemo na gumb *New*. Prikažejo se vnosna polja, kamor vpišemo ime nove skupine virov, opisno ime ter opis in kliknemo na gumb *Next* (Slika 39).



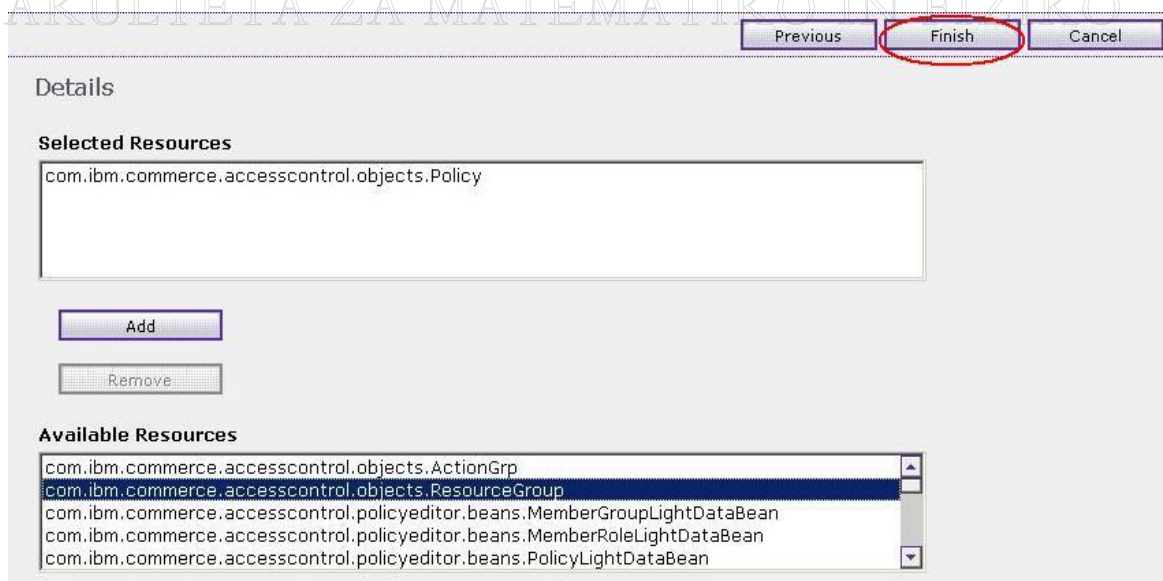
**Slika 39:** Definiranje nove skupine virov

V naslednjem koraku izberemo, ali bo skupina virov eksplicitna ali implicitna in kliknemo na gumb *Next* (Slika 40).



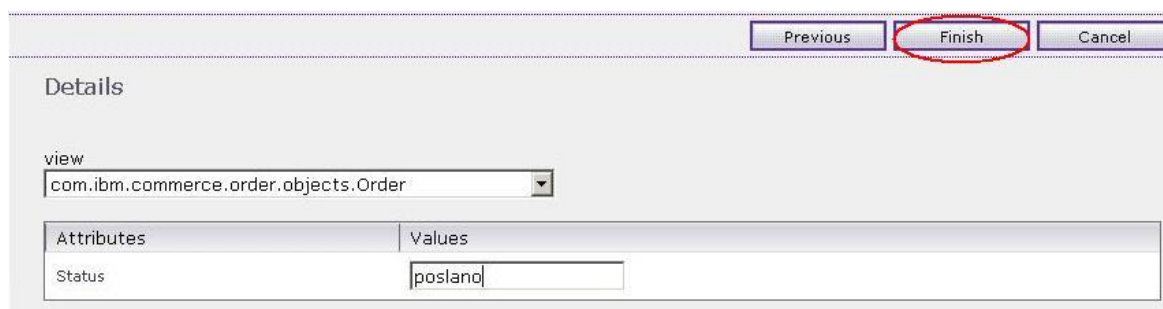
**Slika 40:** Tipa skupine virov

Če izberemo eksplicitni tip skupine virov, to pomeni, da sami določimo, kateri viri bodo pripadali tej skupini. Iz seznama izberemo željene vire, kot je prikazano na sliki Slika 41. V tem primeru imamo možnost izbrati tudi vire, ki v politiki dostopa na nivoju vlog (razdelek 5.4) nastopajo kot ukazi. Skupina bo vsebovala samo tiste vire, ki smo jih izbrali sami. Ko izberemo vse željene vire, kliknemo na gumb *Finish* in s tem zaključimo s kreiranjem nove skupine virov.



Slika 41: Dodajanje virov v skupino

Če pa izberemo implicitni tip skupine virov, imamo na voljo samo kategorije virov in ne tudi vire kot ukaze. Ko izberemo neko kategorijo virov iz seznama, moramo določiti lastnost tega vira (objekta). Kot primer izberimo naročilnice, kot je prikazano na sliki Slika 42. Edina lastnost, ki jo ima ta objekt, je status. Pri tem določimo, kakšen status mora imeti naročilnica, da pripada v to skupino virov. Tako bo implicitna skupina virov avtomatično vsebovala vse naročilnice, ki so bile poslano (ki imajo status poslano). Ko izberemo željeno kategorijo virov in zapišemo pogoj, s klikom na gumb *Finish* zaključimo s kreiranjem nove skupine virov.



Slika 42: Izbrana kategorija virov in zapisan pogoj

Vse že obstoječe skupine virov lahko spreminjamo tako, da dodajamo ali brišemo vire iz skupine, spremenimo ime skupine ... Prav tako posamezno skupino virov lahko izbrišemo. Z uporabo vmesnika OAC pa ne moremo ustvarjati novih virov, saj so ti predstavljeni kot javanski razredi.

Pri spreminjanju, dodajanju, brisanju politik ali spreminjanju skupin akcij in virov moramo biti pozorni na to, da lahko kakršnakoli sprememba vpliva tudi na druge politike (razdelek 5.4.1).

### 5.2.3 Format XML

Politiko lahko definiramo v formatu XML tako, da ustvarimo dokument, napisan v jeziku XML. Ta dokument prenesemo v bazo podatkov z ukazom *acpload*, ki kliče tri orodja. Najprej *transformer* (*com.ibm.wca.XMLTransformer*) datoteko z novo politiko preoblikuje v novo datoteko. Nato *resolver* (*com.ibm.wca.ResGen*) to novo datoteko dopolni s podatki o ključih v bazi podatkov, ki ustrezajo vnešenim podatkom. Takrat *resolver* določi ključ za nove vpise v bazo podatkov, ob spremembi obstoječe politike pa poišče ključ že obstoječih podatkov. Pri tem nastane nova XML

datoteka. Na koncu se s pomočjo orodja massloader (*com.ibm.wca.MassLoader*) izvede zapisovanje podatkov v bazo. Ko je politika zapisana v bazi, je vidna tudi v Organization Administration Console. Prav tako v formatu XML definiramo novo vlogo, skupino uporabnikov, skupino akcij in virov.

Pri definiranju nove politike moramo biti pozorni na to, da vpišemo vse potrebne podatke.

#### **Vzorec, kako definiramo novo politiko v formatu XML:**

```
<Policy Name = "imePolitike"
  OwnerId = "lastnikPolitike"
  UserGroup = "skupinaUporabnikov"
  UserGroupOwner = "lastnikUporabnikov"
  ActionGroupName = "skupinaAkcij"
  ResourceGroupName = "skupinaVirov"
  PolicyType = "tipPolitike"
  RelationName = "relacija"
  RelationGroupName = "skupinaRelacij"
  RelationGroupOwner = "lastnikSkupineRelacij">
</Policy>
```

#### **Kaj vse lahko vsebuje politika, zapisana v formatu XML:**

- Name je ime politike, pri čemer upoštevamo, iz česa je ime sestavljeno (razdelek 5.2).
- OwnerId je lastnik politike – organizacija, kateri politika pripada (razdelek 3.1).
- UserGroup je skupina uporabnikov, kateri je politika namenjena. Izbrana skupina uporabnikov mora že obstajati v sistemu (razdelek 5.1.1).
- UserGroupOwner je lastnik skupine uporabnikov – organizacija, kateri izbrana skupina uporabnikov pripada. Ta ključ navedemo samo v primeru, če skupina uporabnikov pripada drugi organizaciji kot ta nova politika.
- ActionGroupName je ime skupine akcij (razdelek 5.1.2).
- Resource GroupName je ime skupine virov (razdelek 5.1.3).
- PolicyType je tip politike (razdelek 5.5).
- RelationName je ime relacije. Ključ zapišemo samo v primeru, če med uporabnikom in virom obstaja kakšen dodaten pogoj (razdelek 5.1.4).
- RelationGroupName je ime skupine relacij. Če je relacija, ki smo jo določili, uvrščena v skupino relacij, ključ zapišemo, sicer ne.
- RelationGroupOwner je lastnik skupine relacij – organizacija ali organizacijska enota. Lastnika navedemo samo v primeru, če izbrana relacija pripada drugi organizaciji kot na novo definirana politika.

Za primer definirajmo novo politiko, ki dovoljuje vsem administratorjem upravljati z naslovi vseh uporabnikov v sistemu. Politika bo enaka, kot smo jo že definirali v OAC v razdelku 5.2.1. Zapisali pa jo bomo v formatu XML. Med prej navedenimi bomo uporabili samo tiste ključne, ki so potrebni.

#### **Primer nove politike:**

```
<Policy
```

```

        Name =
        "AdministratorsExecuteAddressManageOnUserDataResourceGroup"
        OwnerId = "RootOrganization"
        UserGroup = "Administrators"
        ActionGroupName = "AddressManage"
        ResourceGroupName = "UserDataResourceGroup"
        PolicyType = "groupableStandard">
</Policy>

```

To novo politiko uvrstimo še v eno izmed že obstoječih skupin politik. To storimo v formatu XML tako, da najprej napišemo ime skupine politik ter lastnika in nato še ime politike, ki jo vstavljamo v skupino. V našem primeru smo zgoraj definirano politiko dali v skupino politik *Management and Administration Policy Group*, ki je v lasti glavne organizacije.

#### **Primer vstavljanja nove politike v skupino politik:**

```

<!--skupina politik-->
<PolicyGroup Name = "ManagementAndAdministrationPolicyGroup"
            OwnerID = "RootOrganization">

    <!--politika, ki smo jo dodali skupini politik-->
    <PolicyGroupPolicy
        Name =
        "AdministratorsExecuteAddressManageOnUserDataResourceGroup"
        PolicyOwnerId = "RootOrganization" />
</PolicyGroup>

```

Pri definiranju nove politike smo uporabili že obstoječi skupini akcij in virov. V nadaljevanju pa si bomo ogledali, kako so v formatu XML definirane skupine akcij in virov. Prav tako si bomo ogledali, kako določimo ime akcije in vira.

#### **Primer skupine akcij:**

```

<!--skupina akcij-->
<ActionGroup
    Name = "AddressManage"
    OwnerID = "RootOrganization">

    <!--akcije, ki se nahajajo v tej skupini-->
    <ActionGroupAction
        Name =
        "com.ibm.commerce.usermanagement.commands.AddressAddCmd"/>
    <ActionGroupAction
        Name =
        "com.ibm.commerce.usermanagement.commands.AddressCheckCmd"/>
    <ActionGroupAction
        Name =
        "com.ibm.commerce.usermanagement.commands.AddressDeleteCmd"/>
    <ActionGroupAction
        Name =
        "com.ibm.commerce.usermanagement.commands.AddressUpdateCmd"/>
</ActionGroup>

```

Skupino akcij *AddressManage* (upravljanje z naslovi) smo zapisali v formatu XML. Vsaka skupina akcij ima svoje ime (*Name*) in lastnika (*OwnerID*; organizacija<sup>4</sup>). Prav tako smo zapisali tudi imena

---

<sup>4</sup> V večini primerih je lastnik skupine akcij kar glavna organizacija.

akcij, ki pripadajo tej skupini. Kot je že omenjeno v razdelku 5.2.1, je posamezna akcija javanski razred. Pri poimenovanju uporabimo ustrezne imenske prostore, ki ustrezajo strukturi, v katero so uvrščeni naši razredi.

#### **Primer poimenovanja akcije:**

```
<!--akcija-->
<Action
    Name =
        "com.ibm.commerce.usermanagement.commands.AddressDeleteCmd"
    CommandName =
        "com.ibm.commerce.usermanagement.commands.AddressDeleteCmd">
</Action>
```

Akcija, ki je zapisana v formatu XML, je del skupine akcij *AddressManage* in uporabniku omogoča brisanje naslova. Ko definiramo novo akcijo, ji določimo ime (*Name*) in ime razreda (*CommandName*), ki predstavlja to akcijo. Ni nujno, da sta imeni akcije in razreda enaki.

#### **Primer skupine virov:**

```
<!--skupina virov-->
<ResourceGroup
    Name = "UserDataResourceGroup"
    OwnerID = "RootOrganization">

    <!--vir, ki se nahaja v tej skupini-->
    <ResourceGroupResource
        Name = "com.ibm.commerce.user.objects.User"/>
</ResourceGroup>
```

V na novo definirani politiki smo kot skupino virov uporabili *UserDataResourceGroup* (podatki uporabnikov). Določili smo lastnika (*OwnerID*) skupine. Ta skupina virov vsebuje samo en vir oziroma kategorijo virov (razdelek 5.1.3), ki predstavlja podatke uporabnikov.

#### **Primer poimenovanja kategorije virov:**

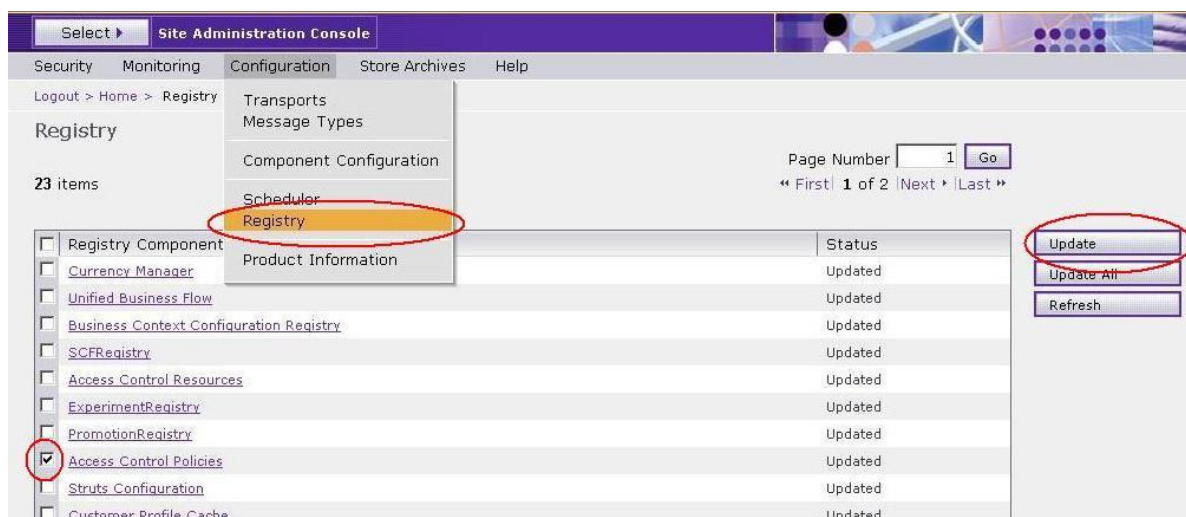
```
<!--kategorija virov-->
<ResourceCategory
    Name = "com.ibm.commerce.user.objects.User"
    ResourceBeanClass = "com.ibm.commerce.user.objects.User">

    <!--akcije, ki se lahko izvajajo nad to kategorijo virov-->
    <ResourceAction
        Name =
            "com.ibm.commerce.usermanagement.commands.AddressAddCmd"/>
    <ResourceAction
        Name =
            "com.ibm.commerce.usermanagement.commands.AddressCheckCmd"/>
    <ResourceAction
        Name =
            "com.ibm.commerce.usermanagement.commands.AddressDeleteCmd"/>
    <ResourceAction
        Name =
            "com.ibm.commerce.usermanagement.commands.AddressUpdateCmd"/>
    <ResourceAction
        Name =
            "com.ibm.commerce.usermanagement.commands.UserRegistrationAdminU
            pdateCmd"/>
```

```
<ResourceAction
    Name =
    "com.ibm.commerce.usermanagement.commands.UserRegistrationUpdate
    Cmd"/>
</ResourceCategory>
```

Kategorijo virov definiramo s pomočjo formata XML. Določimo ime kategorije (*Name*) in javanski razred (*ResourceBeanClass*), ki predstavlja to kategorijo. Enako kot pri definiranju akcij, tudi pri kategoriji virov ni nujno, da sta ime kategorije in ime razreda enaka. Ker nad virom ne moremo izvajati poljubnih akcij, smo določili, katere konkretne akcije se lahko izvedejo nad tem virom.

Če smo poleg nove politike definirali tudi nove skupine akcij, akcije, skupine virov ali vire, le-te shranimo v eni ali več datotekah. Če smo pri definiranju nove politike morali definirati tudi novo skupino akcij, mora biti le-ta definirana pred politiko. Če se torej skupina akcij in politika nahajata v isti datoteki, mora biti najprej zapisana skupina akcij. Če pa smo skupino akcij shranili v drugo datoteko, moramo najprej to prenesti v bazo. To datoteko prenesemo v bazo podatkov s pomočjo ukaza *acpload*. Na koncu moramo poskrbeti, da so spremembe pri politiki dostopa vidne tudi v vmesnikih (OAC, Accelerator in Administration Console; razdelek 3.4). To storimo s pomočjo vmesnika Accelerator (razdelek 3.4.2), kjer izberemo meni *Configuration* in nato podmeni *Registry*. Iz seznama izberemo *Access Control Policy* in kliknemo na gumb *Update* (Slika 43).



Slika 43: Posodabljanje politike dostopa

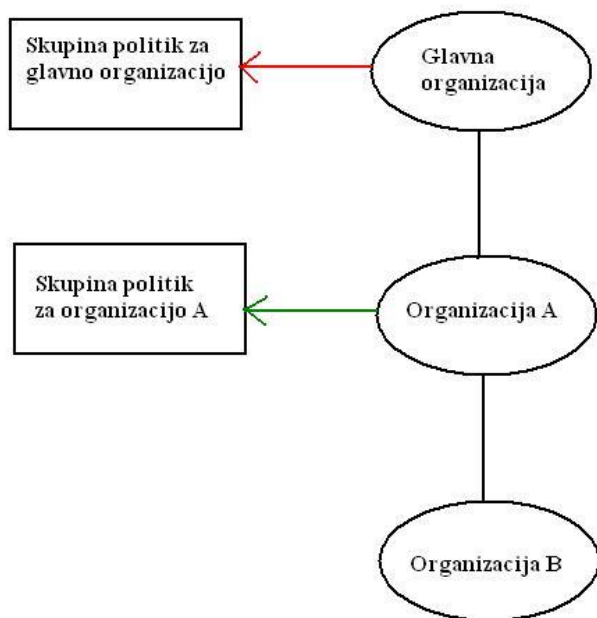
### 5.3 Skupine politik dostopa

Politike, ki pripadajo posamezni organizaciji, združujemo v skupine politik. Vsaka politika mora biti uvrščena v eno skupino (lahko tudi v več skupin). Posamezna skupina vsebuje eno ali več politik. Namen združevanja politik v skupine je to, da lažje vidimo, katere politike pripadajo posamezni organizaciji. Ko je potrebno ugotoviti, ali ima določen uporabnik pravico uporabljati nek vir, se pregledajo tiste skupine politik, ki veljajo za organizacijo, v lasti katere je vir.

Pri postavitvi sistema izberemo določeno organizacijsko strukturo (razdelek 3.3). S tem avtomatsko dobimo nekatere organizacije in njim privzete skupine politik, ki so že določene (razdelek 5.3.1). Ko organizacijo kreiramo na novo, ji moramo določiti tudi skupine politik, ki bodo veljale za to novo organizacijo. Povezave med skupinami politik in organizacijami oz. organizacijskimi enotami določimo s pomočjo relacijske baze podatkov ali z uporabo vmesnika OAC. Za posamezno organizacijo povemo eno ali več skupin politik, ki bodo veljale zanjo. Prav tako posamezna skupina politik lahko velja za več organizacij. Kadar pa ustvarimo neko organizacijo in ji ne

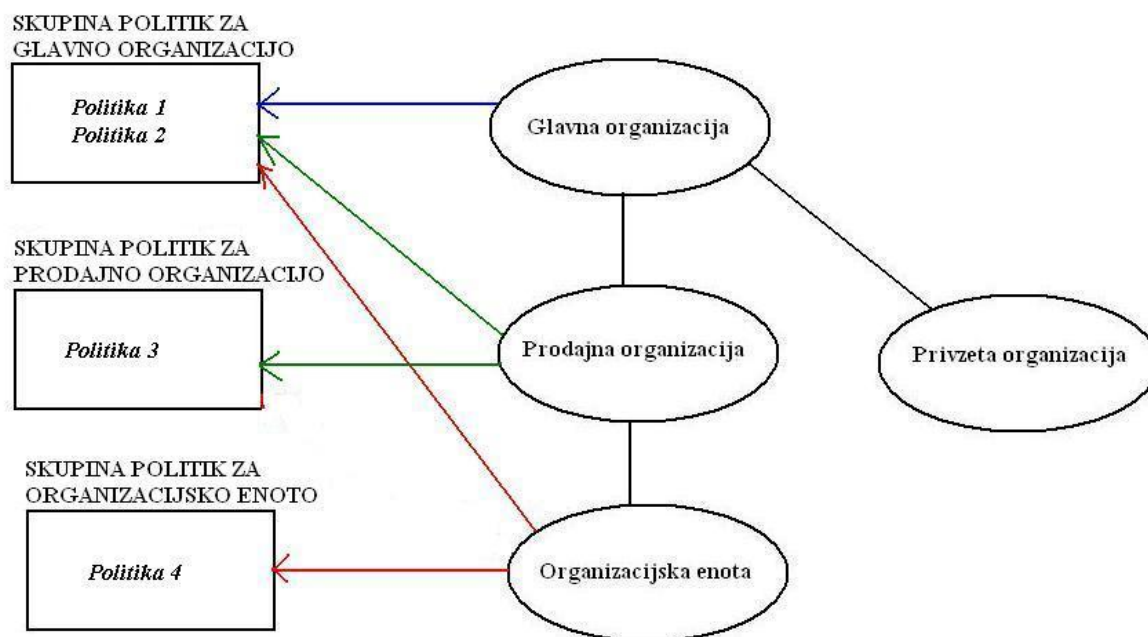
določimo skupine politik, ta organizacija »podeduje« skupino politik od njej nadrejene organizacije (Slika 44).

Slika 44 prikazuje primer organizacije in njim pripadajoče skupine politik. Glavni organizaciji pripada skupina politik za glavno organizacijo, organizaciji A pa pripada skupina politik za organizacijo A, medtem ko organizacija B nima »svoje« skupine politik. Torej za organizacijo B posredno velja tista skupina politik, ki pripada nadrejeni organizaciji, v tem primeru organizaciji A.



**Slika 44:** Organizacije in njim pripadajoče skupine politik

S primerom na sliki Slika 45 bomo pokazali, kako določimo, katere skupine politik veljajo za posamezno organizacijo. Za organizacijsko enoto velja skupina politik za to organizacijsko enoto. Določili smo tudi, da organizacijski enoti pripada še skupina politik za glavno organizacijo, ne pa tudi skupina politik za prodajno organizacijo. Prodajni organizaciji pripadata skupina politik za prodajno organizacijo in skupina politik za glavno organizacijo. Skupina politik za glavno organizacijo velja seveda tudi v glavni organizaciji. V tem primeru privzeta organizacija nima nobene »svoje« skupine politik. Prav tako ji nismo določili nobene druge skupine politik. Torej privzeta organizacija »podeduje« skupino politik nadrejene organizacije – glavne organizacije. Zanj torej veljajo tiste politike, ki jih vsebuje glavna organizacija.



**Slika 45:** Skupine politik za posamezno organizacijo

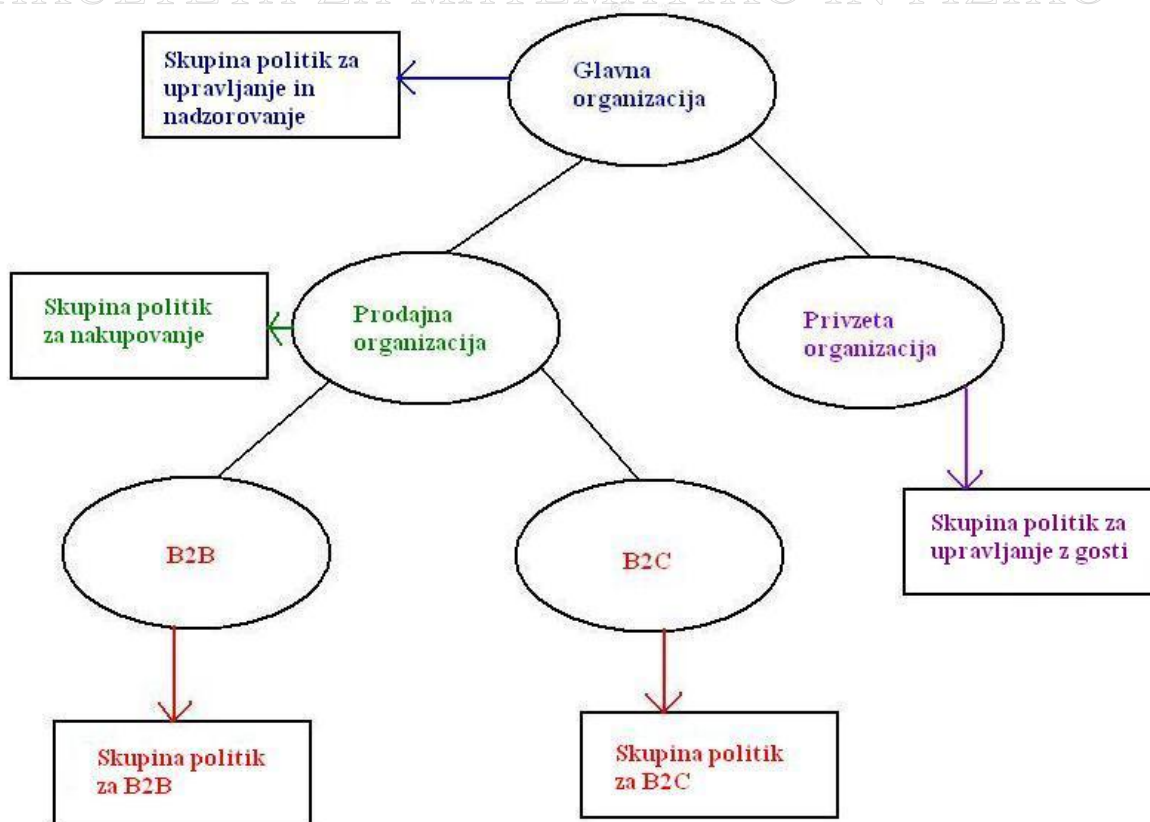
Če torej za vse organizacije naštejemo politike, ki zanje veljajo, dobimo:

- Organizacijska enota: politika1, politika 2 in politika 4
- Prodajna organizacija: politika1, politika 2 in politika 3
- Glavna organizacija: politika 1 in politika 2
- Privzeta organizacija: politika 1 in politika 2

Ne pozabimo, da velja, da nekaj lahko delamo, če obstaja vsaj kakšna politika, ki ustrezno opravilo dovoljuje.

### 5.3.1 Privzete skupine politik

Ko WSC Server namestimo na računalnik, dobimo vrsto privzetih politik in skupin politik dostopa. Kot smo že omenili v razdelku 5.3, si ob namestitvi izberemo ustrezno organizacijsko strukturo. V tem razdelku si bomo ogledali, katere skupine politik že obstajajo v sistemu.



Slika 46: Organizacije in skupine politik

Slika 46 prikazuje organizacijsko strukturo za oba načina poslovanja hkrati – B2B in B2C. Vsaki organizaciji pripada privzeta skupina politik.

#### Privzete skupine politik:

- Skupina politik za upravljanje in nadzorovanje (angl. *Management and administration policy group*)

Skupina vsebuje politike, ki dovoljujejo upravljanje z uporabniki in nadziranje celotnega sistema. V tej skupini je na primer politika, ki dovoljuje uporabniku z vlogo glavnega administratorja prijaviti novega uporabnika v sistem.

- Skupina politik za upravljanje z gosti (angl. *Guest shopper management policy group*)

Skupina vsebuje politike, ki poskrbijo za nadzor nad gosti. V primeru B2B poslovanja so gosti posamezniki (registrirani ali neregistrirani uporabniki). Pri poslovanju B2C pa so posamezniki kupci.

- Skupina politik za nakupovanje (angl. *Common shopping policy group*)

Ta skupina shranjuje politike, ki nadzorujejo nakupovanje oz. prodajo pri B2B ali B2C poslovanju. Primer je politika, ki dovoljuje uporabnikom z določeno vlogo pregledovati podatke o izdelkih.

- Skupina politik za B2B (angl. *B2B policy group*)

Skupina zajema politike, ki nadzorujejo potek B2B poslovanja.

- Skupina politik za B2C (angl. *B2C policy group*)

Skupina vsebuje politike, ki nadzorujejo potek B2C poslovanja.

## 5.4 Kategorije politik

Kot vemo (razdelek 5.1), je vsaka politika sestavljena iz skupine uporabnikov, skupine akcij in skupine virov. Glede na to, kako je politika definirana, ločimo dve kategoriji:

- politika na nivoju vlog (angl. *role – based policy*)
- politika na nivoju virov (angl. *resource – level policy*)

**Politika na nivoju vlog** je sestavljena iz skupine uporabnikov z enako vlogo in skupine virov, ki vsebuje vire za to vlogo (razdelek 5.1.3). Kot akcija je vedno uporabljena akcija izvršiti (angl. *execute*). Takšna politika v skupini virov vsebuje ukaze, ki jih izvaja določena skupina uporabnikov, ki vsebuje uporabnike z enako vlogo. S to kategorijo politik poudarimo, kdo – katera skupina uporabnikov – lahko izvaja določene ukaze, ki so združeni v skupini virov.

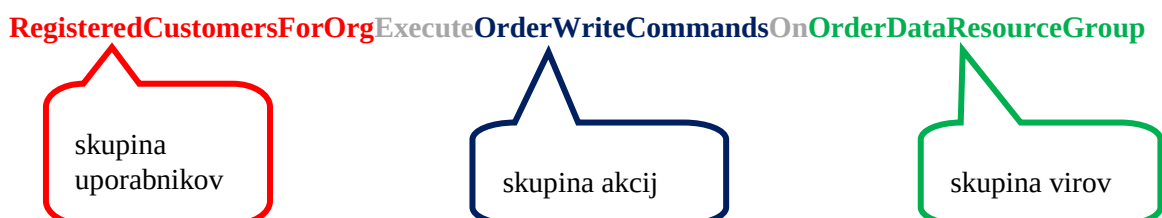
Primer poimenovanja politike na nivoju vlog:



Zgornji primer poimenovanja politike predstavlja politiko na nivoju vlog, ki vsem uporabnikom z vlogo administratorja za nakup (angl. *Buyer Administrator*) dovoljuje izvesti ukaze, ki so v skupini virov (*BuyersAdministratorsCommands*). Že iz imena je razvidno, da skupina virov vsebuje tiste ukaze, ki jih uporabniki z določeno vlogo lahko izvajajo. Takšna skupina virov je eksplicitnega tipa in sami, s pomočjo vmesnika OAC, dodajamo ali brišemo posamezne vire, ki predstavljajo ukaze (razdelek 5.2.1). V politiki skupina akcij vsebuje le eno akcijo – izvršiti.

**Politika na nivoju virov** je sestavljena iz dela, ki določi skupino uporabnikov, dela, ki opredeli skupine akcij, in dela, ki določi skupine virov. Skupina uporabnikov je v tej kategoriji politik sestavljena iz ene ali več vlog. Politika točno določa, kdo – uporabnik, ki pripada določeni skupini uporabnikov – izvede točno določene akcije nad viri.

Primer poimenovanja politike na nivoju virov:

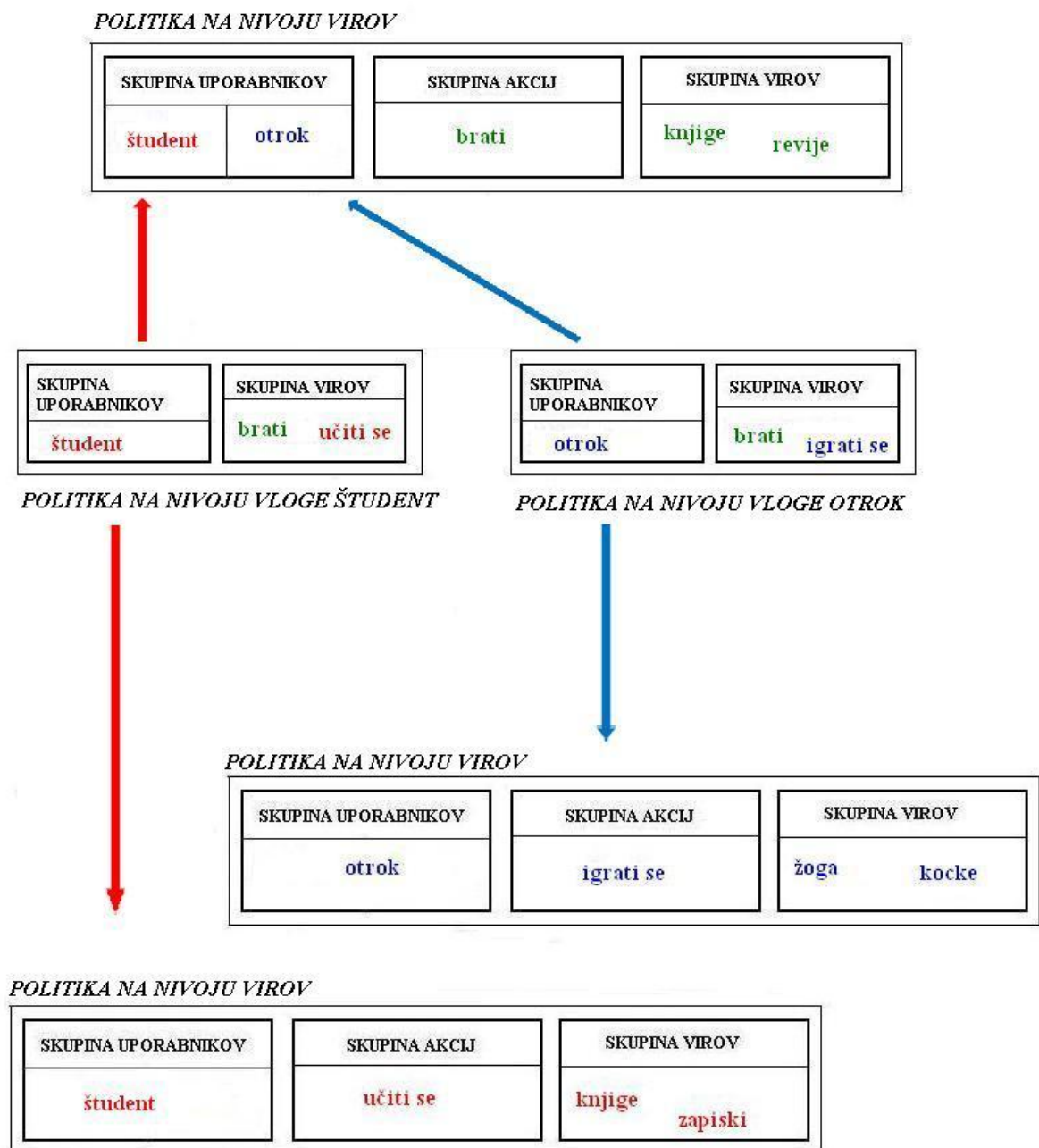


Zgornji primer prikazuje poimenovanje politike na nivoju virov (razdelek 5.2). Politika dovoljuje vsem registriranim uporabnikom znotraj organizacije (*RegisteredCustomersForOrg*) izpolniti (*OrderWriteCommands*) naročilnice (*OrderDataResourceGroup*). Iz imena je razvidno, da je

politika sestavljena iz skupine uporabnikov, skupine akcij in skupine virov, pri čemer so akcije na primer pisati, brisati, posodobiti ... in viri naročilnice, izdelki, uporabniki ...

V tem primeru je smiselno, da lahko dodajamo ali brišemo akcije iz skupine akcij in vire iz skupine virov. To storimo s pomočjo vmesnika OAC (razdelek 5.2.1) ali pa z uporabo poizvedovalnega jezika SQL tako, da neposredno brišemo (ukaz DELETE) ali dodajamo (ukaz INSERT) akcije in vire v tabelah. Pri tej kategoriji politik je skupina politik implicitnega ali eksplicitnega tipa. Če je skupina implicitnega tipa, dodamo nek pogoj, po katerem so viri razvrščeni v skupine (npr. vsi izdelki, na katere je popust). Če pa je skupina eksplicitna, moramo biti pozorni, katere vire bomo dodali v skupino. Skupina namreč ne vsebuje virov kot ukazov.

Kakšna je razlika med navedenima kategorijama politik, si razložimo s pomočjo enostavnega primera. Imamo skupino uporabnikov, ki jo sestavljajo uporabniki z eno vlogo – otrok. Politika na nivoju vlog je sestavljena iz akcije izvesti in skupine virov, ki vsebuje igrati se in brati. Ta kategorija politik dovoljuje otroku, da se igra, ne zanima pa nas, s čim se igra. Prav tako otrok lahko kaj prebere. Politika na nivoju virov ima v skupini akcij igrati se in v skupini virov žoga in kocke. To pomeni, če se otrok želi igrati, se lahko igra samo z žogo in kockami, ne pa tudi z medvedki.



**Slika 47:** Politike, razdeljene v kategorije

Slika 47 prikazuje pet politik dostopa. Dve politiki sta na nivoju vlog študent in otrok. Vsaka izmed teh dveh politik vsebuje vire kot akcije, ki jih izvaja posamezna vloga. Torej politika na nivoju vlog študentu dovoljuje brati in učiti se, otroku pa igrati se in brati. Kot vidimo, imata skupno akcijo brati. Politika na nivoju virov jima dovoli brati samo knjige ter revije in ne tudi časopisov. Prav tako smo omejili študentu izvedbo akcije učiti se. Politika na nivoju virov pravi, da se študent lahko uči samo iz knjig in zapiskov in ne tudi iz revij. Otrok se sploh ne sme učiti. Kot smo omenili, se otrok lahko igra, študent pa ne. Otrok se ne sme igrati s knjigo (lahko jo samo bere), medvedki ..., lahko pa se igra z žogo in kockami.

### 5.4.1 Prilagajanje politik

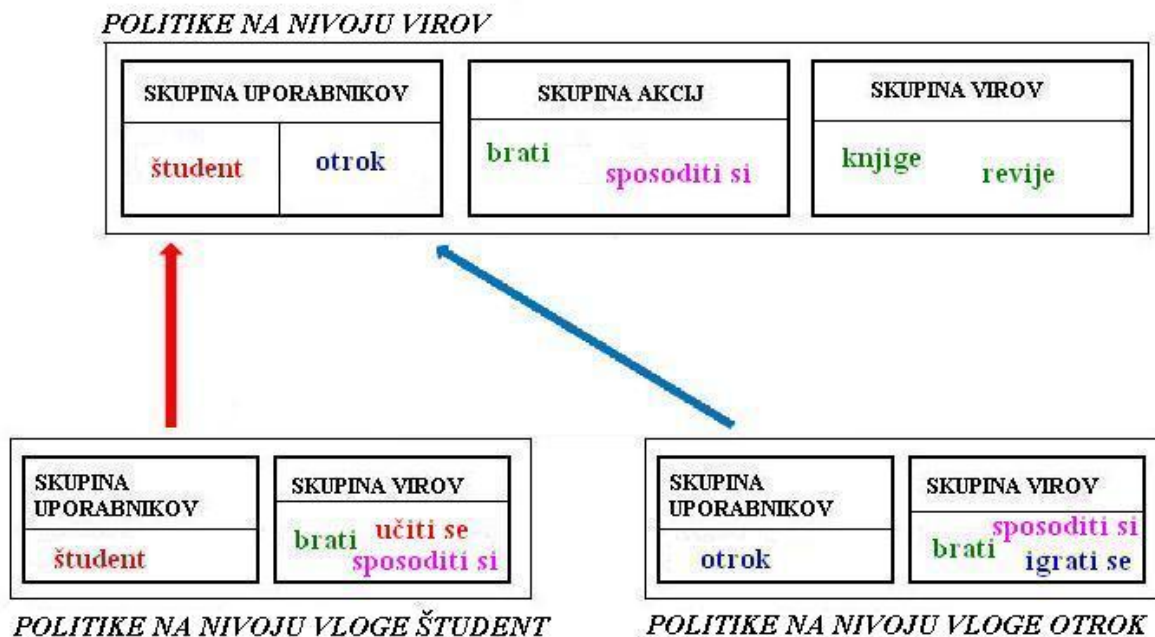
WSC vsebuje vrsto privzetih politik, ki so ob namestitvi sistema že aktivne. Lahko se zgodi, da privzeta politika ni taka, ki bi ustrezala našim potrebam. V tem primeru jo nadomestimo z novo, bolj natančno politiko. Ko je nova politika vnešena v bazo, je potrebno staro izbrisati. Če tega ne storimo, se lahko zgodi, da dopustimo izvajanje napačnih ukazov. Spomnimo se namreč, da nadzor dostopa deluje po principu »če obstaja katerakoli politika, ki dovoljuje izvedbo ukaza, se ukaz lahko izvede«. Ob pregledovanju nadzora dostopa bo torej uporabnik izvedel ukaz, če bo vsaj ena politika to dovoljevala. V primeru, ko stara politika še obstaja, bo uporabnik morda lahko izvedel ukaz, ki ga nova politika ne dovoljuje. Šele, ko bo stara politika izbrisana, uporabnik ne bo mogel izvesti željene akcije.

Po drugi strani pa je možno, da med obstoječimi politikami ni takšne, ki bi uporabniku dovoljevala izvesti določene ukaze. V tem primeru je potrebno politiko definirati na novo. Če pa želimo, da določena skupina uporabnikov izvede akcijo, ki v sistemu še ni zapisana, je dovolj, da jo na novo definiramo in uvrstimo v primerno skupino akcij. Enako storimo, če želimo skupini uporabnikov dovoliti izvedbo akcij nad novim virom. S tem, ko nov vir ali akcijo uvrstimo v skupino, se spremenijo politike na nivoju virov in politike na nivoju vlog. Pri takšnih spremembah moramo biti pozorni na to, da skupino, v katero smo uvrstili novo akcijo ali vir, lahko uporablja tudi druga politika.

Novo politiko, skupino akcij ali skupino virov definiramo s pomočjo orodja OAC, dodamo neposredno v bazo s pomočjo orodij za delo z bazo ali pa napišemo datoteko, ki vsebuje opis politike v jeziku XML.

Za primer vzemimo sliko Slika 47, ki vsebuje politike na nivoju virov in na nivoju vlog. Vlogi sta študent in otrok. Ena politika vsebuje uporabnike z vlogo študent ali otrok in jim dovoljuje izvajanje akcije brati nad knjigami in revijami. Sedaj dovolimo, da si študentje in otroci knjige in revije tudi sposodijo. Zato v skupino akcij, ki je del politike na nivoju virov, dodamo akcijo sposoditi si. S tem smo omogočili študentom in otrokom izvajanje nove akcije. Ker pa za vsako vlogo obstaja politika na nivoju vloge, se na novo dodana akcija zapiše tudi v tisti dve politiki. Torej se nova akcija sposoditi si nahaja v skupini virov, ki je del politike na nivoju vloge študent, in v skupini virov, ki je del politike na nivoju vloge otrok (Slika 48).

Pri tem opazimo, da je politika na nivoju virov samo dopolnitev politike na nivoju vlog. Vseeno pa moramo imeti obe kategoriji politik. Pri pregledovanju nadzora dostopa vedno najprej pogledamo, ali uporabnik lahko izvede željeno akcijo. In če najdemo tako politiko, poiščemo še politiko na nivoju virov. V nasprotnem primeru se mu prepreči izvedbo akcije že na začetku. Več o postopkih za nadzor dostopa si bomo ogledali v razdelku 5.6.



**Slika 48:** Spremenjene politike

Lahko pa se zgodi, da ne želimo, da bi nekateri uporabniki izvajali določene akcije. V tem primeru željeno akcijo odstranimo s pomočjo vmesnika OAC ali z uporabo poizvedovalnega jezika SQL. Prav tako lahko na enak način kot akcije dodajamo in odstranjujemo virov. Kot je že omenjeno v tem razdelku, pa je potrebno paziti na to, da ko posežemo v neko skupino akcij ali virov, nastanejo spremembe v vseh politikah, ki zajemajo spremenjeno skupino. Zato je običajno bolje, da takrat, ko moramo narediti določeno spremembo in želimo, da ni »globalna«, ustvarimo novo skupino in zanjo ustvarimo ustrezno politiko.

## 5.5 Dva tipa politik

Kot smo že opisali v razdelku 5.3, se politike združujejo v skupine politik. Za posamezno organizacijo veljajo določene skupine politik in posledično politike znotraj teh skupin. Glede na to, v kateri skupini politik je posamezna politika in za katero organizacijo velja ta skupina, ločimo dva tipa politik.

- Standardne politike (angl. *Groupable standard policies*)
- Vzorčne politike (angl. *Groupable template policies*)

**Standardne politike** so tiste politike, ki nam povejo, kateri uporabniki (z eno ali več vlogami) lahko izvajajo določene akcije iz skupine akcij nad viri iz skupine virov. Vsaka standardna politika pripada skupini politik, ki velja za določene organizacije. Primer takšne politike je politika, ki administratorju za nakup dovoljuje potrjevati naročila. Ta politika pripada skupini politik in velja za tiste uporabnike, ki pripadajo organizaciji, za katere velja ta skupina politik. V tem primeru je določena samo vloga uporabnika in ne tudi, v kateri organizaciji se mora nahajati.

Standardne politike so tudi tiste, ki dovoljujejo uporabnikom iz točno določene organizacije izvesti akcije nad viri. Primer takšne politike je politika, ki administratorju za nakup iz organizacije za nakup dovoljuje potrjevati naročila. Torej, če ima uporabnik vlogo administratorja za nakup in hkrati pripada organizaciji za nakup, potem lahko potrdi naročilo, ki je v lasti organizacije za nakup ali njene podorganizacije, sicer ne.

Nekoliko drugačne so **vzorčne politike**. Ta tip politike je dinamičen in se navezuje na uporabnika z eno ali več vlogami in organizacijo, ki ji ta uporabnik pripada. Ta tip politike ne določa konkretne organizacije, vendar samo navede, da uporabnik pripada organizaciji. Vzorčna politika se uporablja v »več organizacijah«. Kot primer vzemimo politiko, ki administratorju za nakup v organizaciji dovoljuje potrditi naročilo. Če se administrator za nakup nahaja v organizaciji za nakup, lahko potrdi tiste naročilnice, ki so v lasti organizacije za nakup ali njenih podorganizacij. Ista politika velja za administratorja za nakup, ki se nahaja npr. v glavni organizaciji ali organizacijski enoti ... Torej ni važno, v kateri organizaciji se nahaja uporabnik, lahko potrdi naročilnice, ki so v lasti iste organizacije ali njenih podorganizacij.

Kot primer si oglejmo organizacijsko strukturo, ki jo prikazuje Slika 49. Za posamezno prodajno organizacijo 1 in 2 imamo lahko dve standardni politiki. Ena politika dovoljuje prodajnemu administratorju v prodajni organizaciji 1 ustvariti nove ponudbe za pohištvo, druga politika pa dovoljuje prodajnemu administratorju v prodajni organizaciji 2 ustvariti nove ponudbe za obleke. Ti dve politiki se navezujeta na dve skupini uporabnikov – ena skupina vsebuje prodajne administratorje v prodajni organizaciji 1, druga pa prodajne administratorje v prodajni organizaciji 2. Sedaj želimo ti dve standardni politiki združiti v eno vzorčno politiko. Vzorčna politika dovoljuje prodajnemu administratorju iz organizacije ustvariti nove ponudbe za pohištvo in obleke. Ta politika pa se navezuje na eno skupino uporabnikov – prodajni administratorji v organizaciji. Če se torej prodajni administrator nahaja v prodajni organizaciji 1, lahko ustvari nove ponudbe za tisti vir (pohištvo), ki se prav tako nahaja v prodajni organizaciji 1.

V razdelku 5.6 si bomo ogledali, kako poteka postopek za nadzor dostopa. V razdelku 5.6.1 si bomo ogledali nadzor dostopa, če imamo opraviti s standardno politiko, v razdelku 5.6.2 pa za primer vzorčne politike.

## 5.6 Postopki za nadzor dostopa

Vsak uporabnik z vlogo pripada določeni organizaciji in vsak vir je v lasti neke organizacije. Kot smo pojasnili v razdelku 5.3, za vsako organizacijo velja, da ima določeno skupino politik dostopa. *Policy Manager* pregleda, kateri organizaciji pripada vir, nad katerim želi uporabnik izvesti akcijo. Glede na to, katere skupine politik veljajo za to organizacijo, poišče ustrezno politiko, ki bo dovoljevala izvesti akcijo. Pri iskanju ustrezne politike se upošteva tudi, kateri skupini uporabnikov pripada ta uporabnik. Če vsaj ena politika dovoljuje izvesti akcijo nad virom, potem uporabnik le-to lahko izvede.

Celoten nadzor dostopa poteka v dveh nivojih:

1. Nivo vlog (angl. *role - based access control*)
2. Nivo virov (angl. *resource - level access control*)

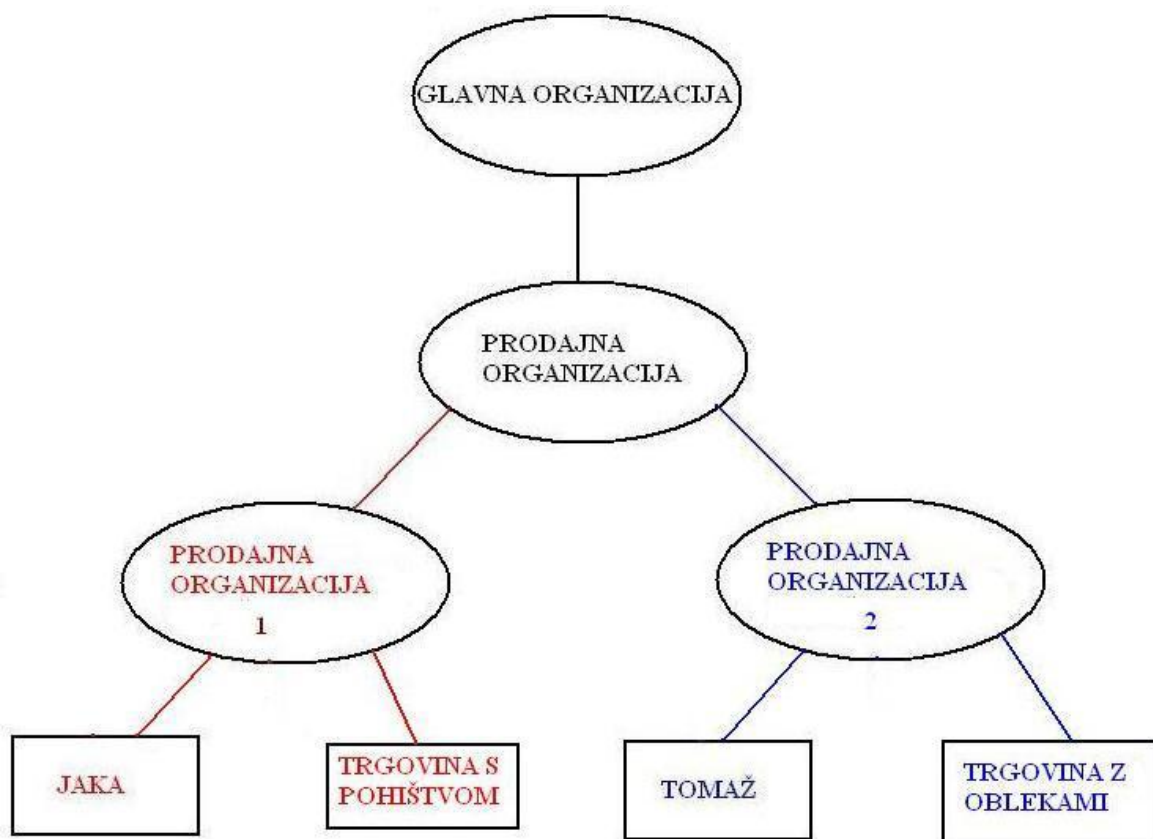
Na vsakem nivoju pregledovanja poiščemo politiko, ki dovoljuje uporabniku izvedbo željene akcije nad virom. Če jo že na prvem nivoju (nivoju vlog) ne najdemo, je dostop takoj zavrnjen.

Najprej se izvede pregled na **nivoju vlog**. Tu se preveri, ali uporabnik z določeno vlogo sploh lahko izvede željeno akcijo. Ker je za ustrezno dovoljenje dovolj, da obstaja vsaj ena politika, ki izvedbo dovoljuje, preiščemo vse ustrezne politike. Poišče se politika na nivoju vlog (razdelek 5.4), torej je v teh politikah vir ukaz, ki ga želi uporabnik izvesti. Posamezni ukazi, ki so vezani na vloge uporabnikov, so lahko specifični za posamezno trgovino. To pomeni, da določene ukaze izvedejo uporabniki samo v določeni trgovini. V tem primeru se politika na nivoju vlog nahaja v tistih skupinah politik, ki veljajo za organizacijo, ki predstavlja posamezno trgovino. Ali so ukazi specifični, vidimo pri nadzoru dostopa na nivoju vlog. Če so ukazi kot viri v lasti organizacije, ki predstavlja trgovino, je ukaz specifičen za določeno trgovino. Torej bomo politiko na nivoju vlog iskali v skupini politik, ki pripada organizaciji, ki predstavlja trgovino. Če pa ukazi niso specifični,

veljajo za vse trgovine. V tem primeru pa se ustrezna politika na nivoju vlog išče kar v skupini politik, ki velja za glavno organizacijo.

Če obstaja politika, ki uporabniku dovoli izvesti akcijo, poskusimo poiskati še ustrezno politiko na nivoju virov.

Na **nivoju virov** poiščemo politiko, ki dovoljuje uporabniku izvesti akcijo nad točno določenim virom. Naprej pogledamo, v lasti katere organizacije je vir, nad katerim želi uporabnik izvesti akcijo. Nato ustrezno politiko iščemo v tistih skupinah politik, ki pripadajo tej organizaciji. Pozorni moramo biti tudi na to, katero vlogo ima uporabnik. Če obstaja vsaj ena politika, ki uporabniku dovoljuje izvesti akcijo nad željenim virom, le-to lahko izvede.



**Slika 49:** Organizacijska struktura ter organizacije, trgovine in uporabniki, ki jo sestavljajo

Slika 49 prikazuje organizacijsko strukturo. Prodajna organizacija je razdeljena na dve podorganizaciji. Prodajna organizacija 1 ima v lasti trgovino s pohištvom, prodajna organizacija 2 pa trgovino z oblekami. Jaka in Tomaž sta prodajna administratorja. Jaka ima nadzor nad trgovino s pohištvom, Tomaž pa nad trgovino z oblekami. Rada bi ustvarila nove ponudbe za pohištvo oz. obleke.

Imamo tri standardne politike:

Politika 1: Dovoljuje prodajnemu administratorju ustvariti nove ponudbe. Politika velja za Prodajno organizacijo, Prodajno organizacijo 1 in Prodajno organizacijo 2. Politika je na nivoju vlog.

Politika 2: Dovoljuje prodajnemu administratorju v Prodajni organizaciji 1 ustvariti nove ponudbe za pohištvo. Pripada Prodajni organizaciji 1, ki predstavlja trgovino s pohištvom. Politika je na nivoju virov, saj točno opredeli, da uporabnik lahko izvede akcijo nad ponudbami za pohištvo.

**Politika 3:** Dovoljuje prodajnemu administratorju v Prodajni organizaciji 2 ustvariti nove ponudbe za obleke. Pripada Prodajni organizaciji 2, ki predstavlja trgovino z oblekami. Politika je, prav tako kot politika 2, na nivoju virov.

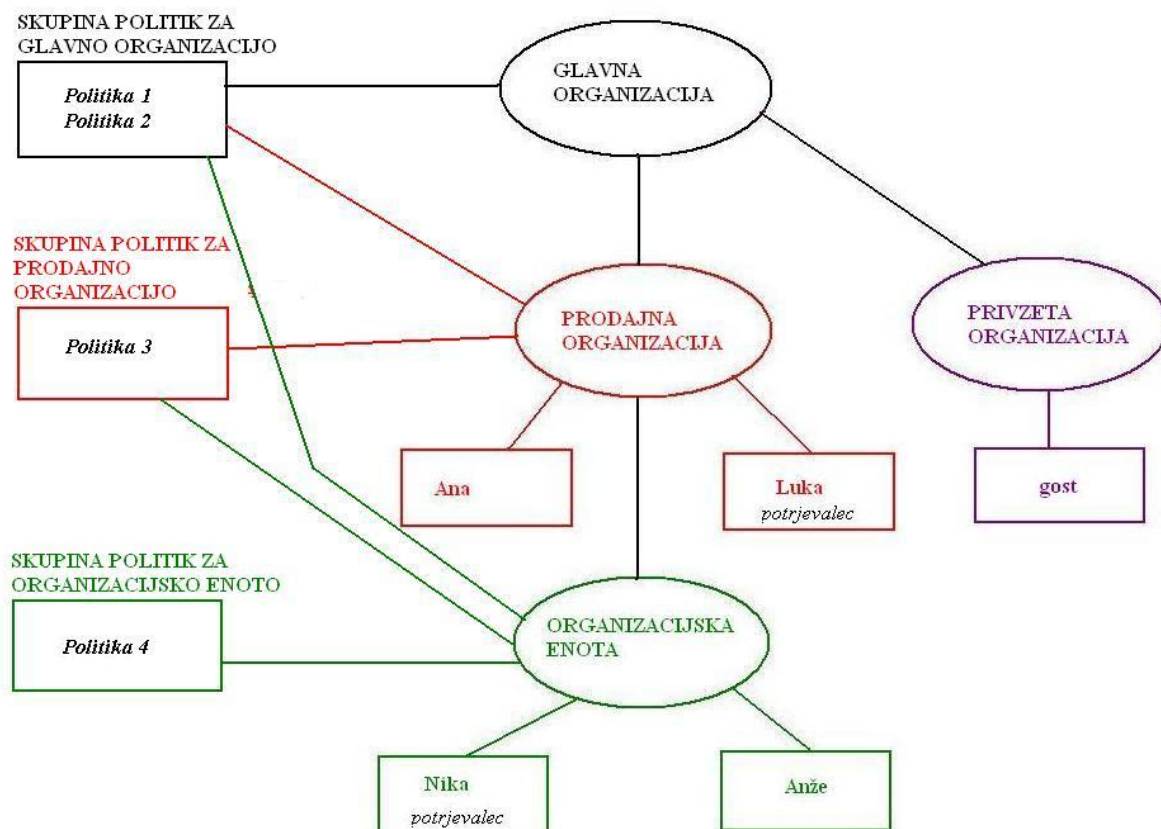
Poglejmo, ali Jaka lahko doda novo ponudbo za pohištvo. Najprej se na nivoju vlog pregleda, ali Jaka sploh lahko ustvari novo ponudbo. Ker ima vlogo prodajnega administratorja in obstaja politika 1, ki dovoljuje ustvariti nove ponudbe, akcijo lahko izvede. Sedaj poiščemo še ustrezno politiko na nivoju virov (torej ali lahko Jaka ustvari ponudbo prav za pohištvo). Vir pohištvo je v lasti Prodajne organizacije 1, za katero velja politika 2, ki dovoljuje prodajnemu administratorju ustvariti novo ponudbo za pohištvo, vendar samo v primeru, če tudi uporabnik pripada Prodajni organizaciji 1. Jaka je prodajni administrator in pripada tej organizaciji, torej lahko izvede željeno akcijo nad virom.

Denimo, da bi sedaj Jaka želel ustvariti ponudbo za obleke. Kot smo opisali že v prejšnjem odstavku, Jaka lahko ustvari novo ponudbo. Preveriti moramo še na nivoju virov (torej ali lahko Jaka ustvari ponudbo za obleke). Vir obleke se nahaja v Prodajni organizaciji 2, za katero velja politika 3, ki dovoljuje prodajnemu administratorju v Prodajni organizaciji 2 ustvariti novo ponudbo za obleke. Ker pa Jaka pripada Prodajni organizaciji 1, zanj politika 3 ni ustrezna. Torej Jaka ne more ustvariti nove ponudbe za obleke. Izvedbo akcije nad željenim virom (oblekami) mu je preprečilo pregledovanje na nivoju virov.

Postopek pregledovanja je enak, če vzamemo primer, da Tomaž želi ustvariti novo ponudbo za obleke. Pri pregledovanju na nivoju vlog mu politika 1 dovoli izvesti akcijo ustvarjanje novih ponudb. Na nivoju virov pa mu politika 3 dovoljuje izvesti akcijo nad virom obleke, saj ima Tomaž vlogo prodajnega administratorja v Prodajni organizaciji 2, kateri pripadajo tudi obleke. Če pa bi Tomaž želel ustvariti ponudbo za pohištvo, le-te akcije ne more izvesti, saj ni ustrezne politike na nivoju virov, ki bi mu to dovoljevala.

Pri pregledovanju nadzora dostopa vedno najprej pogledamo, v kateri organizaciji se nahaja vir ter katere skupine politik veljajo za to organizacijo. Nato se pogleda, kakšno vlogo ima uporabnik in kateri organizaciji pripada. Glede na vse te izbrane »podatke«, poiščemo politiko, ki bo uporabniku dovolila izvesti akcijo nad željenim virom.

### 5.6.1 Standardna politika



**Slika 50:** Shema prikazuje povezavo med organizacijami in skupinami politik, ki vsebujejo standardne politike

Slika 50 prikazuje uporabnike in skupine politik, ki veljajo za posamezno organizacijo. Vse politike so razvrščene v skupine in so standardne (razdelek 5.5). Sami smo določili, katere skupine politik veljajo za posamezno organizacijo, kot je to opisano v razdelku 5.3. Ko se preverja, ali uporabnik lahko izvede željeno akcijo nad virom, se upošteva, katera organizacija ima v lasti ta vir, katere skupine politik veljajo za to organizacijo ter katero vlogo ima uporabnik. V nadaljevanju bomo za primer kot akcijo vzeli akcijo posodabljanje. Uporabljeni viri bodo ponudbe, uporabniki, politike in organizacije pa bodo take, kot so prikazane na sliki Slika 50.

Uporabniki pripadajo posameznim organizacijam in imajo vlogo registriranega uporabnika. Uporabnik, ki ni registriran, v naši shemi pripada privzeti organizaciji. Luka in Nika nista samo registrirana uporabnika, ampak imata tudi vlogo potrjevalca<sup>5</sup> (angl. *approver*).

V shemi na sliki Slika 50 smo uporabili štiri organizacije, ki so med seboj v hierarhiji. Najvišje v hierarhiji je glavna organizacija. Tik pod njo sta prodajna in privzeta organizacija, najnižje pa je organizacijska enota.

Predpostavimo, da imamo v celotni shemi le štiri politike, ki so razvrščene po skupinah, kot kaže Slika 50. Za vsako organizacijo veljajo izbrane skupine politik. V tem primeru ima vsaka organizacija, razen privzete, svojo specifično skupino politik. Prav tako pa zanjo veljajo tudi

<sup>5</sup> Potrjevalec je tisti, ki je pooblaščen za potrjevanje ali zavračanje določenih dokumentov (npr. ponudb, naročilnic ...)

skupine politik iz nadrejenih organizacij. Ker privzeta organizacija nima »svoje« skupine politik, le-to »podeduje« od nadrejene glavne organizacije (Slika 50).

Kaj opisuje posamezna politika:

Politika 1: Registriran uporabnik lahko izvaja ukaz posodabljanje. Politika je na nivoju vlog, torej ni točno definirano, nad katerim virom lahko uporabnik z vlogo registriranega uporabnika izvede ukaz.

Politika 2: Registriran uporabnik lahko posodablja ponudbe, ki jih je sam ustvaril. Politika je na nivoju virov. Točno je določeno, nad katerimi viri lahko uporabniki izvajajo akcijo posodabljanje. Določena je tudi relacija med uporabnikom in virom. Registriran uporabnik lahko posodobi samo tiste ponudbe, katerih avtor je.

Politika 3: Registriran uporabnik z vlogo potrjevalca v prodajni organizaciji lahko posodobi ponudbe, ki so v lasti prodajne organizacije. Politika je na nivoju virov, ker je točno določeno, nad katerimi viri uporabnik lahko izvaja akcijo.

Politika 4: Registriran uporabnik z vlogo potrjevalca v organizacijski enoti lahko posodobi ponudbe, ki so v lasti organizacijske enote. Tudi ta politika je na nivoju virov.

Vse politike so standardne. Politiki 3 in 4 še dodatno vsebujeta razmerje med uporabnikom in organizacijo.

S pomočjo zgoraj navedenih politik, uporabnikov, organizacij bomo na konkretnih primerih razložili, kdo lahko posodobi naročilnice in kako poteka pregledovanje.

**Ali Anže lahko posodobi ponudbe, ki jih je sam ustvaril?**

Anže pripada organizacijski enoti in ima vlogo registriranega uporabnika. Za organizacijsko enoto veljajo vse skupine politik. Najprej se izvede preverjanje na nivoju vlog, torej moramo poiskati politiko na nivoju vlog. Kot smo povedali v razdelku 5.6, se tu preveri, ali ima uporabnik pravico izvesti določeno akcijo. V našem primeru najprej želimo preveriti, ali Anže sploh lahko izvede akcijo posodabljanje. Da bo to možno, mora obstajati vsaj ena politika na nivoju vlog, ki dovoljuje izvedbo te akcije. V našem primeru nimamo posebnih trgovin v sistemu in tudi politike na nivoju vlog niso specifično določene, torej iščemo politiko na nivoju vlog v skupini politik za glavno organizacijo. Politika 1 Anžetu, kot registriranemu uporabniku, dovoljuje izvedbo željene akcije. S tem je končan prvi nivo pregledovanja – nivo vlog. Ker smo našli politiko, ki dovoljuje izvedbo akcije, preverimo še ustrezna dovoljenja na nivoju virov.

Tudi na nivoju virov iščemo ustrezno politiko. Ta mora biti takšna, da Anžetu dovoljuje posodobitev ponudb, katerih avtor je on sam. Te naročilnice so v lasti organizacijske enote, za katero veljajo vse skupine politik. Ustrezno politiko iščemo med vsemi štirimi politikami. Vrstni red iskanja ni točno določen. Politika 4 ni ustrezna, saj Anže nima vloge potrjevalca, torej pogledamo politiko 3. Tudi ta iz istega razloga ne dovoljuje izvedbo željene akcije nad virom. Nato pogledamo še politiki iz skupine politik za glavno organizacijo. Politika 1 ni ustrezna, ker je na nivoju vlog, mi pa iščemo politiko na nivoju virov. Politika 2 pa dovoljuje vsem registriranim uporabnikom posodobiti ponudbe, ki so jih sami ustvarili. Kot smo že omenili, je Anže registriran uporabnik, torej lahko posodobi »svoje« ponudbe.

Ker smo na obeh nivojih našli politiko, ki dovoljuje izvedbo nameravanega postopka, Anže lahko posodobi svoje ponudbe.

Enak postopek bi uporabili za preverjanje tega, ali lahko Ana posodobi svoje ponudbe. Ana je tako kot Anže samo registriran uporabnik. Ker so Anine ponudbe v lasti prodajne organizacije, pri preverjanju ne moremo uporabiti le politike 4. A s to politiko si v Anžetovem primeru tako ali tako nismo mogli pomagati. Torej tudi Ana lahko posodobi svoje ponudbe. Ker pa registrirani

uporabniki posodablajo samo ponudbe, ki so jih sami ustvarili, vidimo, da tako Anže kot Ana posodabljata le svoje ponudbe, torej tiste, katerih avtorja sta.

**Ali Luka lahko posodobi ponudbe, ki jih je ustvaril Anže?**

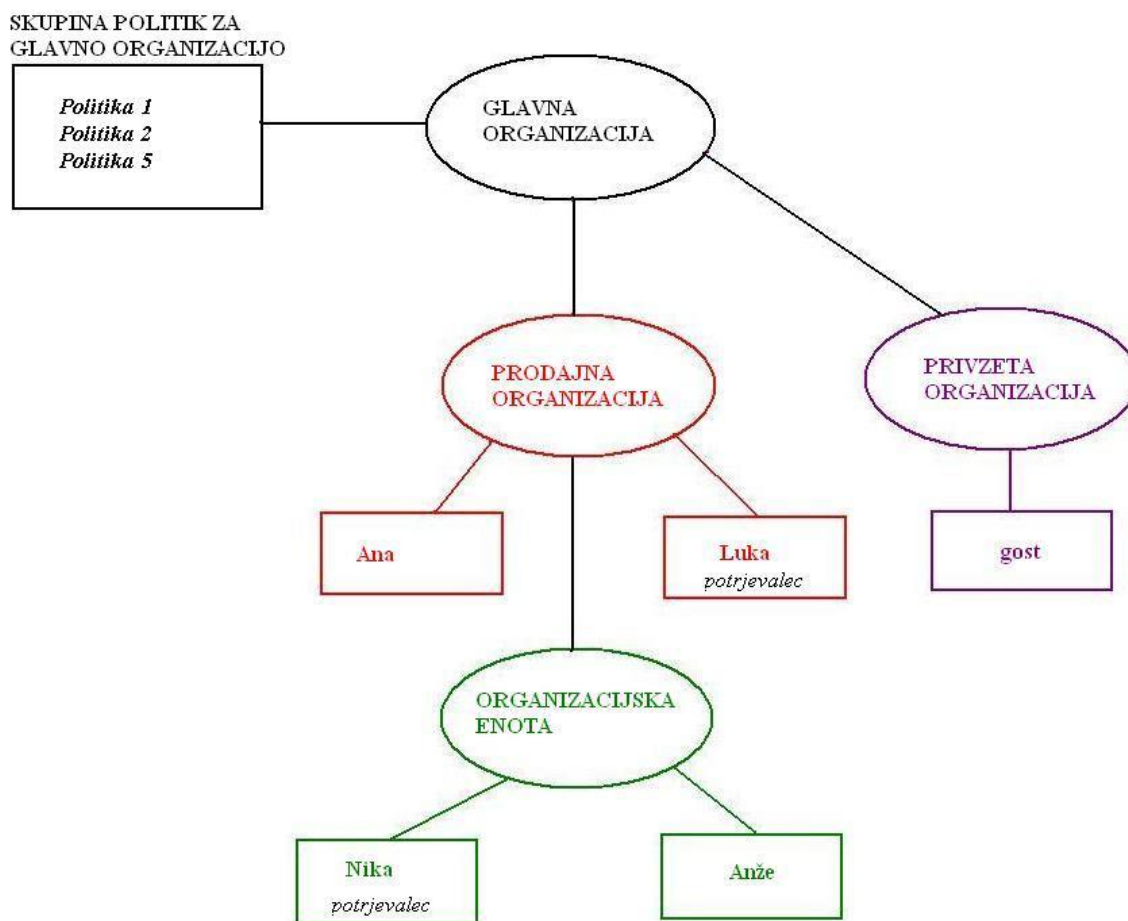
Luka pripada isti organizaciji kot Ana in je tudi registriran uporabnik. Enak premislek kot pri Ani pove, da na nivoju vlog ugotovimo, da Luka lahko izvede akcijo posodabljanje. Ker pa bi rad posodobil ponudbo, ki jo je ustvaril Anže, moramo poiskati vsaj eno politiko, ki dovoljuje izvedbo akcije nad točno določenim virom. Anžetove ponudbe so v lasti organizacijske enote, za katero veljajo vse politike, torej moramo izmed vseh najti ustrezno politiko na nivoju virov. Najprej pregledamo politiko 4. Ta dovoljuje uporabniku z vlogo potrjevalca v organizacijski enoti posodobiti ponudbe, ki so v lasti organizacijske enote. Anžetove ponudbe so res v lasti organizacijske enote, vendar Luka nima vloge potrjevalca v tej organizacijski enoti. Ker politika 4 ni ustrezna, pogledamo politiko 3. Le ta dovoljuje potrjevalcu v prodajni organizaciji posodobiti tiste ponudbe, ki so v lasti prodajne organizacije. Luka ima vlogo potrjevalca v prodajni organizaciji. Anžetove ponudbe so v lasti tiste organizacije, kateri pripada Anže sam – organizacijske enote, ki pa je podorganizacija prodajne organizacije, torej so tudi v lasti prodajne organizacije. Torej Luka lahko posodobi ponudbe, ki jih je ustvaril Anže.

Povejmo še, da Luka lahko posodobi vse ponudbe, ki so v lasti prodajne organizacije in organizacijske enote ter ponudbe, ki jih je ustvaril sam. Prav tako ima tudi Nika vlogo potrjevalca. Ker pa pripada organizacijski enoti, lahko posodobi samo tiste ponudbe, ki so v lasti organizacijske enote in tiste, ki jih je ustvarila sama. Ne more pa posodobiti tistih ponudb, ki so v lasti le prodajne organizacije in ne organizacijske enote.

**Ali gost lahko posodobi ponudbe, ki jih je sam ustvaril?**

Gost pripada privzeti organizaciji, za katero velja skupina politik za glavno organizacijo. Gost ni registriran uporabnik, vendar bi rad posodobil svoje ponudbe. Najprej se izvede pregledovanje na nivoju vlog. Obstajati mora vsaj ena politika, ki dovoljuje neregistriranemu uporabniku izvesti akcijo posodabljanja. Edini politiki, ki bi mu to omogočili, sta politiki 1 in 2, vendar nobena ni ustrezna. Gostu že nivo vlog prepreči izvedbo akcije posodabljanje, zato se pregledovanje konča že na prvem nivoju pregledovanja.

### 5.6.2 Vzorčna politika



**Slika 51:** Shema prikazuje povezavo med organizacijo in skupino politik, ki vsebuje dve standardni in eno vzorčno politiko

Slika 51 prikazuje organizacije, uporabnike in skupine politik. V tem razdelku bodo uporabljene standardne in vzorčne politike. Kot je opisano v razdelku 5.5, se ena vzorčna politika uporablja za več organizacij, medtem ko je standardna politika namenjena posamezni organizaciji ali pa se ne navezuje na posebno organizacijo.

Tako kot v razdelku 5.6.1 je tudi v tem primeru akcija »posodabljanje« in vir »ponudba«. Uporabniki so bodisi registrirani uporabniki, gosti oziroma imajo vlogo potrjevalca. V organizacijski strukturi so uporabljene štiri organizacije in ena skupina politik, ki je v lasti glavne organizacije. Ker ostale organizacije nimajo specifičnih skupin politik, podedujejo skupino politik za glavno organizacijo.

#### Kaj opisuje posamezna politika:

Politika 1: Registriran uporabnik lahko izvaja ukaz posodabljanje. Politika je na nivoju vlog, torej ni točno definirano, nad katerim virom lahko uporabnik z vlogo registriranega uporabnika izvede ukaz. Politika je standardna.

Politika 2: Registriran uporabnik lahko posodablja ponudbe, ki jih je sam ustvaril. Politika je na nivoju virov. Točno je določeno, nad katerimi viri lahko uporabniki izvajajo akcijo posodabljanje. Določena je tudi relacija med uporabnikom in virom. Politika je standardna.

**Politika 5:** Politika je podobna kombinaciji politik 3 in 4 (razdelek 5.6.1) in je na nivoju virov. Politika pravi, da uporabnik z vlogo potrjevalca v katerikoli organizaciji lahko posodobi vse naročilnice, ki so v lasti organizacije, kateri pripada uporabnik. Je vzorčna politika. To pomeni, da se uporablja v »več organizacijah«. Razlika med standardnima politikama 3 in 4 iz razdelka 5.6.1 in to politiko je v tem, da se politiki 3 in 4 uporabljata za uporabnike iz točno določene organizacije (politika 3 za prodajno organizacijo in politika 4 za organizacijsko enoto), politika 5 pa je namenjena tisti organizaciji, v kateri je trenutni uporabnik.

S pomočjo konkretnih primerov si oglejmo, kako uporabljamo te politike.

#### **Ali Anže lahko posodobi ponudbe, ki jih je sam ustvaril?**

Anže je registriran uporabnik in pripada organizacijski enoti. Ponudbe, ki jih želi posodobiti, prav tako pripadajo organizacijski enoti. Najprej se izvede pregledovanje na nivoju vlog. Torej moramo poiskati politiko, ki Anžetu dovoljuje izvesti akcijo posodabljanje. Ker organizacijska enota nima točno določenih skupin, zanjo velja prva skupina politik, ki velja za nadrejeno organizacijo – skupina politik za glavno organizacijo (razdelek 5.3). Pri pregledovanju politik znotraj posamezne skupine vrstni red ni pomemben. Politika, ki dovoljuje izvedbo akcije, je politika 1.

Ker se je pregledovanje na nivoju vlog uspešno izvedlo, preverimo še nivo virov in poiščemo politiko, ki Anžetu dovoljuje posodobiti njegove ponudbe. Anžetove ponudbe so v lasti organizacijske enote, za katero velja v tem primeru samo skupina politik za glavno organizacijo. Politika 1 ni ustrezna, ker je na nivoju vlog, mi pa iščemo na nivoju virov. Politika 2 dovoljuje registriranemu uporabniku, da posodobi svoje ponudbe. Ugotovili smo torej, da Anže, ki ima vlogo registriranega uporabnika, lahko posodobi ponudbe, ki jih je sam ustvaril. Vidimo pa tudi, da ostalih ponudb ne more posodobiti, ker ni nobene politike, ki bi mu to dovoljevala.

Omenimo še to, da enak postopek avtorizacije velja za vse ostale registrirane uporabnike. Tako kot Anže tudi Ana lahko posodobi samo tiste ponudbe, ki jih je ustvarila sama.

#### **Ali Luka lahko posodobi ponudbe, ki jih je ustvaril Anže?**

Luka je registriran uporabnik in ima vlogo potrjevalca v prodajni organizaciji. »Anžetove ponudbe«, ki bi jih Luka rad posodobil, tako kot Anže pripadajo organizacijski enoti. Najprej se izvede preverjanje na nivoju vlog. Poiskati moramo politiko, ki Luki dovoljuje izvesti akcijo posodabljanje. Taka je politika 1, ki dovoljuje vsem registriranim uporabnikom, da izvedejo akcijo posodabljanje. Torej se je pregledovanje na nivoju vlog uspešno izvedlo.

Pri preverjanju nivoja virov poiščemo politiko, ki dovoljuje Luki posodobiti Anžetove ponudbe. Politika 5 dovoljuje uporabniku z vlogo potrjevalca, da posodobi tiste ponudbe, ki so v lasti organizacije, kateri pripada uporabnik. Ker viri, ki jih želi Luka posodobiti, pripadajo podorganizaciji prodajne organizacije, lahko izvede željeno akcijo nad virom.

#### **Ali gost lahko posodobi ponudbe, ki jih je sam ustvaril?**

Gost ni registriran uporabnik in pripada privzeti organizaciji. Rad bi posodobil tiste ponudbe, ki jih je ustvaril sam. Najprej se izvede pregledovanje na nivoju vlog. Torej mora obstajati politika, ki gostu dovoljuje izvesti akcijo posodabljanje. Ker nobena izmed treh politik ni ustrezna, gost ne more posodobiti željenih ponudb. Ker že pri prvem nivoju pregledovanja ne najdemo ustrezne politike, se pregledovanje na nivoju virov sploh ne izvede.

## 6 ZAKLJUČEK

V diplomski nalogi smo spoznali, kako poskrbeti za varnost pri izdelavi e-trgovine s pomočjo platforme WebSphere Commerce. Kot smo omenili v diplomski nalogi, že pri namestitvi WSC-ja dobimo vrsto privzetih politik in kar okoli 700 tabel, ki se med seboj povezujejo.

Kaj hitro se lahko zgodi, da naletimo na problem, kako smiselno dopolniti organizacijsko strukturo. Glede na potrebe moramo smiselno ustvariti in uvrstiti v strukturo nove organizacije ali organizacijske enote. Že prej pa moramo vedeti, čemu bo namenjena ta nova organizacija ali organizacijska enota. Upoštevati moramo, katera skupina uporabnikov bo pripadala tej novi organizaciji in katere vire bo imela v lasti. Glede na vse to določimo skupino politik, ki bo vsebovala primerne politike.

Lahko pa se nam zgodi, da ne najdemo nobene primerne politike, ki bi ustrezala neki novi skupini uporabnikov. Takrat moramo ustvariti novo politiko. Ali bomo uporabili že obstoječe akcije in vire ali bomo morali tudi te narediti na novo, je odvisno od tega, kaj želimo. Če bi radi novi skupini uporabnikov dovolili izvajati že obstoječe akcije nad viri, potem bo dovolj, da sestavimo samo novo politiko, ki bo le-to dovoljevala. V primeru, če želimo novo akcijo ali vir, moramo le-to ustvariti in uvrstiti v ustrezno skupino. Pri definiranju nove politike moramo biti pozorni na to, da ne vplivamo na avtorizacijo drugih uporabnikov. V razdelku 5.4 in 5.4.1 je opisano, kako spremembe v skupini akcij ali virov vplivajo na spremembe celotne politike.

Za prepoznavanje uporabnika v e-trgovini je pomembna avtentikacija. Kakšen mora biti uporabniški račun, geslo in koliko časa je veljavno, je opisano s politiko za uporabniški račun. Prav tako kot politiko dostopa, lahko spreminjamo tudi politiko za uporabniški račun. Nekaj pravil za uporabniški račun dobimo z namestitvijo platforme WSC. Če želimo nove ali že ostoječe, imamo možnost spreminjati s pomočjo orodja Administration Console, kot je to opisano v razdelku 4.3.

Kljub temu da je platforma WSC dobro zasnovana, naletimo na kar nekaj pomanjkljivosti. Z vsako nadaljnjo verzijo se platforma izboljšuje in nudi vedno več možnosti tako tistim, ki izdelujejo in vzdržujejo e-trgovine, kot tudi strankam, ki te trgovine uporabljajo.

## 7 LITERATURA

1. WebSphere Commerce Version 6 Information Center, pridobljeno iz <http://publib.boulder.ibm.com/infocenter/wchelp/v6r0m0/index.jsp> (zadnji dostop: 18. 2. 2010)
2. WebSphere Commerce V6.0 delivers a complete end-to-end e-commerce solution, pridobljeno iz <http://www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=ca&infotype=an&appname=iSource&supplier=897&letternum=ENUS206-115> (zadnji dostop: 18. 2. 2010)
3. WebSphere Commerce – Express, pridobljeno iz <http://www-01.ibm.com/software/genservers/commerce/express/> (zadnji dostop: 18. 2. 2010)
4. WebSphere Commerce Professional, pridobljeno iz <http://www-01.ibm.com/software/genservers/commerce/wcpe/> (zadnji dostop: 18. 2. 2010)
5. WebSphere Commerce Enterprise, pridobljeno iz <http://www-01.ibm.com/software/genservers/commerce/wcbe/> (zadnji dostop: 18. 2. 2010)
6. Wikipedia, Online Shopping, pridobljeno iz <http://en.wikipedia.org/wiki/E-Shop> (zadnji dostop: 18. 2. 2010)
7. Wikipedia, Elektronik Commerce, pridobljeno iz <http://en.wikipedia.org/wiki/E-commerce> (zadnji dostop: 18. 2. 2010)
8. Wikipedia, Business-to-business, pridobljeno iz <http://en.wikipedia.org/wiki/Business-to-business> (zadnji dostop: 18. 2. 2010)
9. Wikipedia, Business-to-consumer, pridobljeno iz <http://en.wikipedia.org/wiki/Business-to-consumer> (zadnji dostop: 18. 2. 2010)
10. Wikipedia, Authorization, pridobljeno iz <http://en.wikipedia.org/wiki/Authorization> (zadnji dostop: 18. 2. 2010)
11. Wikipedia, HTTP cookie, pridobljeno iz [http://en.wikipedia.org/wiki/Session\\_cookie](http://en.wikipedia.org/wiki/Session_cookie) (zadnji dostop: 18. 2. 2010)