

UNIVERZA V LJUBLJANI  
FAKULTETA ZA RAČUNALNIŠTVO IN INFORMATIKO

Uroš Ipavec

## Izdelava varnostnih kopij podatkov v okolju SharePoint

DIPLOMSKO DELO NA VISOKOŠOLSKEM STROKOVNEM ŠTUDIJU

Mentor: doc. dr. Janez Demšar

Ljubljana, 2009



Št. naloge: 00430/2009

Datum: 05.04.2009

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

Kandidat: **UROŠ IPAVEC**

Naslov: **IZDELAVA VARNOSTNIH KOPIJ PODATKOV V OKOLJU  
SHAREPOINT  
DATA BACKUP TECHNIQUES FOR SHAREPOINT ENVIRONMENT**

Vrsta naloge: Diplomsko delo visokošolskega strokovnega študija

Tematika naloge:

SharePoint je okolje, ki podjetjem omogoča učinkovitejše delo s podatki. V diplomskem delu najprej okvirno predstavite okolje in njegove različice, nato pa preučite različne načine izdelave varnostnih kopij, vključno s programskim vmesnikom, s katerim lahko sami razvijamo aplikacije za shranjevanje varnostnih kopij. V delo vključite tudi njihovo primerjavo in podajte nekaj ugotovitev o prednostih in slabostih posameznih načinov.

Mentor:

  
doc. dr. Janez Demšar



Dekan:

  
prof. dr. Franc Solina

# Kazalo

<b>1</b>	<b>Povzetek .....</b>	<b>1</b>
<b>2</b>	<b>Abstract .....</b>	<b>2</b>
<b>3</b>	<b>Uvod.....</b>	<b>3</b>
3.1	<i>Zgodovina .....</i>	3
3.2	<i>Verzije.....</i>	4
3.3	<i>Windows SharePoint Services 3.0.....</i>	5
3.4	<i>Microsoft Office SharePoint Server 2007.....</i>	7
<b>4</b>	<b>Arhitektura MOSS-a 2007.....</b>	<b>9</b>
4.1	<i>Storitve operacijskega sistema.....</i>	11
4.2	<i>Storitve podatkovne baze .....</i>	12
4.2.1	Konfiguracijska podatkovna baza .....	12
4.2.2	Vsebinske podatkovne baze .....	12
4.2.3	Podatkovna baza Shared Services Provider .....	12
4.2.4	Podatkovna baza iskalnika .....	12
4.2.5	Indeks iskalnika .....	13
4.2.6	Zunanje podatkovne baze.....	13
<b>5</b>	<b>Varnostno shranjevanje podatkov v MOSS 2007.....</b>	<b>13</b>
5.1	<i>Rešitve za izdelovanje varnostnih kopij podatkov in obnovitev podatkov.....</i>	13
5.1.1	Obnova vsebine in obnova podatkov po katastrofi .....	14
5.2	<i>Izdelava varnostnih kopij in obnova podatkov iz varnostnih kopij.....</i>	16
5.2.1	Označevanje verzij.....	16
5.2.2	Koš.....	17
5.2.3	Prestrezanje dogodka brisanja strani z Microsoftovim IT Site Delete Capture feature 1.0.....	18
5.2.4	Izdelovanje varnostne kopije z uporabo priloženih orodij .....	19
5.2.5	Obnova podatkov iz varnostne kopije.....	21
5.2.6	Prednosti in slabosti priloženih orodij.....	21
5.3	<i>Izdelava varnostnih kopij z orodji strežnika SQL .....</i>	21
5.3.1	Arhitektura podatkovne baze strežnika SQL .....	21
5.3.1.1	Fizična in logična arhitektura .....	22
5.3.1.2	Transakcijski dnevniki.....	22
5.3.1.3	Arhitektura diska .....	23
5.3.2	Podatkovne baze WSS 3.0 .....	23
5.3.3	Podatkovne baze MOSS-a 2007.....	23
5.3.4	Konfiguracija strežnika SQL za izdelavo varnostne kopije podatkov .....	23
5.3.4.1	Strategije izdelovanja varnostnih kopij podatkov.....	24
5.3.5	Obnovitev podatkov v SQL strežniku.....	25
5.3.6	Posnetki strežnika SQL.....	25
5.3.6.1	Proces izdelave posnetka.....	25
5.3.7	Pošiljanje dnevnikov SQL .....	26
5.3.7.1	Proces "Failover" .....	26
5.4	<i>MOSS API za izdelavo varnostnih kopij podatkov.....</i>	27
5.4.1	Objektni model za izdelavo varnostnih kopij in obnovo podatkov .....	27
5.4.1.1	Uporabniške pravice .....	29
5.4.1.2	Shranjevanje informacij o napakah .....	29
5.5	<i>Migriranje podatkov na drugo SharePoint farmo .....</i>	30
5.5.1	Katere podatke lahko migriramo? .....	30
5.5.2	Vmesnik API za izvoz podatkov.....	30

5.6	<i>VSS (Volume Shadow Copy)</i> .....	30
5.6.1	Model VSS .....	31
5.6.2	Servis Volume Shadow Copy .....	32
5.6.3	Shadow kopije in zbirke shadow kopij .....	32
5.6.4	Privzeto stanje shadow kopije .....	33
5.6.5	Zamrznitev in odmrznitev shadow kopije .....	33
5.6.6	Dobavitelji .....	33
5.6.7	Sistemske dobavitelji .....	34
5.6.8	Programske dobavitelji .....	34
5.6.9	Strojne dobavitelji .....	35
5.6.10	Zahtevniki .....	35
5.6.11	Stanje zahtevnika .....	35
5.6.12	Medprocesna komunikacija zahtevnika .....	36
5.6.13	Življenjski cikel zahtevnika med izdelavo varnostne kopije .....	36
5.6.14	Življenjski cikel zahtevnika med obnovo podatkov iz varnostne kopije .....	37
5.6.15	Zapisovalniki .....	37
5.6.16	Stanje zapisovalnika .....	37
5.6.17	Rokovanje zapisovalnikovih dogodkov .....	38
5.6.18	Rokovanje dogodkov za identifikacijo .....	38
5.6.19	Dogodki o izdelavi varnostne kopije in obnovi podatkov .....	38
5.7	<i>MOSS VSS</i> .....	39
5.7.1	Zapisovalnik .....	41
5.7.2	Zahtevnik .....	42
5.7.3	Kako napisati in uporabiti zahtevnik .....	42
5.7.4	Varnostne pravice za poganjanje VSS-ja .....	42
5.8	<i>Obnova podatkov po katastrofi</i> .....	43
5.8.1	Komponente MOSS-a .....	43
5.8.1.1	Binarne datoteke .....	43
5.8.1.2	Konfiguracije MOSS-a 2007 .....	43
5.8.1.3	Dodatki po meri .....	45
5.8.1.4	Vsebina .....	46
<b>6</b>	<b>Implementacija prototipa za izdelavo varnostne kopije in obnovo podatkov na osnovi objektnega modela (WSS 3.0 API)</b> .....	<b>47</b>
6.1	<i>Implementacija Izdelave varnostne kopije komponente</i> .....	51
6.2	<i>Implementacija obnove komponente iz varnostne kopije</i> .....	52
<b>7</b>	<b>Ugotovitve</b> .....	<b>53</b>
<b>Dodatek A</b>	.....	<b>55</b>
7.1	<i>Kazalo slik</i> .....	55
7.2	<i>Kazalo tabel</i> .....	55
<b>8</b>	<b>Priloge</b> .....	<b>55</b>
<b>9</b>	<b>Seznam virov</b> .....	<b>56</b>

# 1 Povzetek

SharePoint je platforma, ki podjetjem omogoča učinkovitejše delo s podatki. Ti so jedro SharePoint-a, saj vsa funkcionalnost SharePoint-a temelji na rokovanju s podatki. SharePoint okolje je lahko zelo obsežno in ima lahko na tisoče uporabnikov, ki uporabljajo in ustvarjajo velike količine podatkov, pomembnih za učinkovito in nemoteno poslovanje podjetja. Zaradi pomembnosti podatkov in zahteve po stalni dostopnosti podatkov, je nujno in smiselno poskrbeti za varnostne kopije podatkov.

Diplomsko delo obravnava različne tehnologije in pristope za izdelavo varnostnih kopij podatkov v okolju SharePoint. S predstavitvijo arhitekture okolja in obravnavo pristopov nudi razvijalcu oziroma programerju temeljne informacije o možnostih, ki jih ima na voljo za lasten razvoj in implementacijo aplikacij za izdelavo varnostnih kopij podatkov.

Z namenom temeljitejšega razumevanja okolja in tehnologij SharePoint, se v uvodnih poglavjih najprej posvečamo predstavitvi SharePoint-a. Na kratko obravnavamo razloge za razvoj SharePoint tehnologije, tržni uspeh, zgodovino od začetnih verzij do današnjih verzij z različnimi licenčinami in funkcionalnostjo. V nadaljevanju podrobneje opisujemo WSS 3.0 in MOSS 2007. Za tem se posvečamo arhitekturi okolja in njegovemu bistvu – shranjevanju podatkov. Predstavljamo kako in kje so podatki v SharePoint okolju shranjeni in kakšna orodja in pristopi so nam na voljo za izdelavo varnostnih kopij podatkov. Poleg obstoječih pristopov obravnavamo tudi programska vmesnika, ki jih nudi okolje SharePoint in preko katerih lahko sami razvijemo aplikacijo za izdelavo varnostnih kopij podatkov.

Diplomsko delo zaključujemo z ugotavljanjem o tem, kateri izmed pristopov je primernejši za varovanje podatkov pred izgubo.

Ključne besede: SharePoint, MOSS, izdelava varnostne kopije, obnova podatkov, obnova podatkov po katastrofi.

## 2 Abstract

SharePoint is a platform which makes the work with data for the companies more efficient. Data is the core of SharePoint. In fact, the whole SharePoint functionality is about managing data. SharePoint environment can be really large and can host thousands of users using and creating big amounts of data that are crucial for an efficient and undisturbed business process. For importance of the data and the demand of having the data always available, it is crucial and sensible to have backup procedures in place.

This degree presents different technologies and approaches to backup the SharePoint environment. With the presentation of architecture, different approaches and programming interfaces, it gives to the developer the base information about the possibilities that are available for developing a backup application.

With the intention of better understanding of the SharePoint technologies and environment, we first introduce SharePoint. We shortly describe the base reasons of SharePoint existence, economic success, history from the first versions to the latest versions with different licensing models and functionality. In chapters following that, we present WSS 3.0 and MOSS 2007 in more detail, followed by focus on architecture and its essence – storing the data. We present how and where the data is stored and what tools and approaches are available for developing backup applications. We also present two APIs that SharePoint support and which we can use to build our own backup application.

We are ending the degree with reasoning about which approach is best for protecting the data against loss.

Keywords: SharePoint, MOSS, backup, restore, disaster recovery

## 3 Uvod

Bill Gates je na najvišjem srečanju direktorjev leta 2006 (CEO Summit 2006) iskanje in upravljanje informacij opisal kot dvojni problem. Prvi je nasičenost z informacijami, kar pomeni, da se obseg podatkov na delovnem mestu veča z neverjetno hitrostjo. To ima na zaposlene, ki morajo ob poplavi informacij ostati osredotočeni še na svoje delo, velik, negativen vpliv. Druga težava pa je pomanjkanje pravih informacij. Zaposleni sicer so obkroženi z veliko informacijami, vendar pa zelo težko najdejo in uporabijo koristne informacije [3].

Rešitev omenjenih problemov naj bi predstavljala linja produktov SharePoint. Da podjetja prepoznajo SharePoint kot pravo rešitev za omenjene probleme potrjujejo podatki o prodaji, ter projekcije prihodnje prodaje SharePoint-a s strani priznanih tržnih analitskih hiš [6].

Šestindvajsetega julija 2007 so na Microsoftovem sestanku finančne analize za leto 2007 sporočili, da so produkti Office SharePoint Server ustvarili več kot 800 milijonov dolarjev prihodka v fiskalnem letu 2007, predvsem zaradi povpraševanja po funkcionalnosti namenjeni velikim podjetjem, ki je implementirana v MOSS 2007. Omenjen prihodek predstavlja več kot 35 odstotno rast glede na fiskalno leto 2006 [7].

Poročilo iz finančne analize iz leta 2008 uspeh linije produktov Sharepoint še potrjuje, saj je bilo prodanih 4,86 milijona licenc za Sharepoint, Exchange Server in Office skupaj, samo strankam, ki so dotlej uporabljale IBM Lotus Notes [8]. Po nekaterih podatkih je v letu 2008 Microsoft prodal 100 milijonov licenc za SharePoint. Po Gartnerjevih študijah pa naj bi do leta 2010 SharePoint uporabljalo 80 odstotkov podjetij [4].

SharePoint je najbolj vroč produkt v zgodovini Microsofta in prvi, ki je v najkrajšem času prinesel podjetju skoraj milijardo dolarjev. Leta 2009 sestanka finančne analize še ni bilo vendar pa, direktor podjetja Steve Ballmer napoveduje segmentu, v katerega spada tudi SharePoint linija produktov, dodaten uspeh [8].

### 3.1 Zgodovina

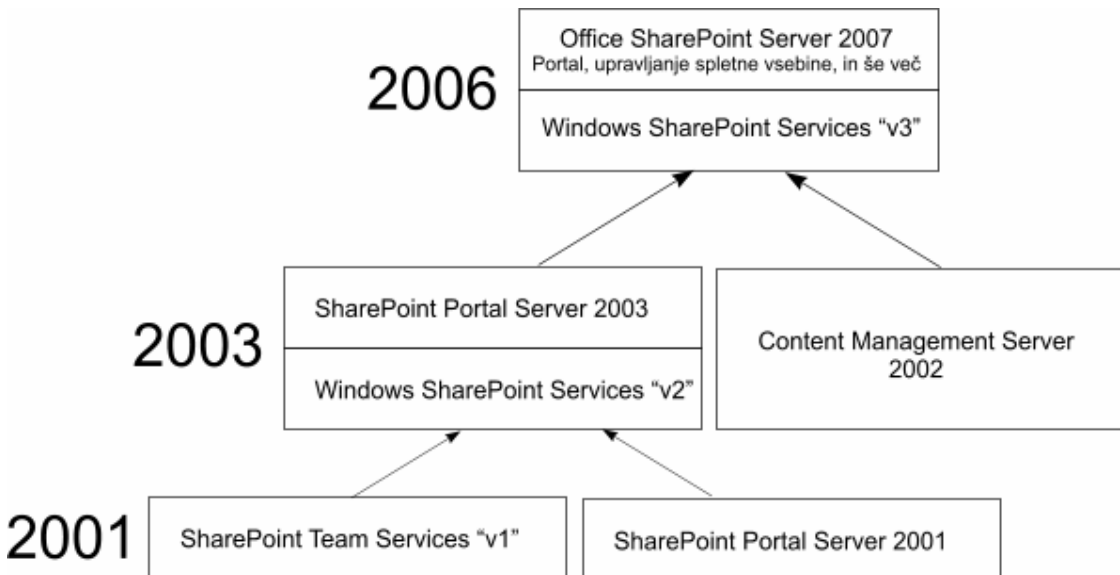
Prva verzija linije produktov SharePoint sega v leto 2001, ko je Microsoft izdal produkta SharePoint Team Services in SharePoint Portal Server 2001. Sledila je različica linije produktov pod imenom SharePoint 2003, s produktoma SharePoint Portal 2003 in Windows SharePoint Services 2.0, ki sta v večji meri izpolnila nekaj od najpogosteje navedenih potreb uporabnikov[1]:

- Potrebo po boljšem upravljanju z dokumenti kot jo nudi datotečni sistem.
- Izboljšano sodelovanje med uporabniki in krajšo učno krivuljo.
- Boljši intranet.
- Centraliziran način iskanja informacij.
- Ustvarjanje portala.

Eden od razlogov za uspeh SharePoint-a 2003 je bila relativno ugodna cena. Podjetja so se namreč odločala za nakup SharePoint-a 2003, kljub temu, da so potrebovala le del od številnih funkcionalnosti, ki jih je ta produkt nudil. Z uporabo SharePoint-a 2003 pa so

zahteve postajale vedno večje in podjetja so potrebovala tudi funkcionalnosti, ki jih SharePoint 2003 ni vseboval. Nekatera podjetja (3rd-parties) so v tem prepoznala priložnost in začela izdelovati funkcionalnost, ki je dopolnjevala SharePoint 2003 glede na potrebe uporabnikov. Z namestitvijo takšnih dodatnih funkcionalnosti je okolje SharePoint postajalo čedalje kompleksnejše in podpora, vzdrževanje in odpravljanje napak vedno težje. Tako različica linije produktov SharePoint 2007, katera vsebuje Windows SharePoint Services 3.0 in Microsoft Office SharePoint Server 2007, gradi na uspehih prejšnje različice in dodaja nove funkcionalnosti po katerih so uporabniki povpraševali, ter mnoge druge, dodatne funkcionalnosti, ki produktu dodatno povečujejo uporabnost.

Razvoj okolja SharePoint skozi različne verzije predstavlja spodnja slika.



Slika 1: Konvergenca tehnologij [13]

### 3.2 Verzije

Linijo SharePoint sestavlja več produktov, ki so medsebojno povezani vendar pa med njimi obstajajo razlike v funkcionalnosti in licenčnini:

- Windows SharePoint Services 3.0
- Microsoft Office SharePoint Server 2007 (standardni CAL<sup>1</sup>)
- Microsoft Office SharePoint Server 2007 (CAL za velika podjetja)
- Microsoft Office SharePoint Server for Search 2007 (standardna verzija)
- Microsoft Office SharePoint Server for Search 2007 (verzija za velika podjetja)

Windows SharePoint Services 3.0 je brezplačen produkt, ki si ga uporabniki lahko namestijo iz Microsoftove spletne strani ali iz operacijskega sistema Windows Server 2003 brez dodatnih licenčnin. Ponuja jedro za upravljanje dokumentov (core document management), zmožnosti sodelovanja (collaboration) in zmožnosti iskanja (search capabilities).

Microsoft Office SharePoint Server (MOSS) 2007 vsebuje dva tipa licenc za dostop za posameznega klienta (CAL): standardno licenco CAL in licenco CAL za velika podjetja. Obe

<sup>1</sup> CAL – client access licenses, licenca za dostop za posameznega klienta

verziji CAL-a nadgradita jedro WSS funkcionalnosti z iskalnikom za velika podjetja in z možnostjo iskanja ljudi (people search capability). MOSS 2007 je namenjen velikim, distribuiranim organizacijam ali podjetjem s potrebo po shranjevanju več kot 500000 dokumentov.

Dodatek CAL-a za velika podjetja k standardnemu CAL-u omogoča dodajanje poslovnega kataloga podatkov (Business Data Catalog).

Verzija Microsoft Office SharePoint Server for Search 2007 (standardna verzija) je namenjena organizacijam in podjetjem, ki potrebujejo iskalnik vendar pa ne potrebujejo sistema za upravljanje dokumentov in zmožnosti sodelovanja, kot ga nudi polna verzija MOSS 2007.

Verzija Microsoft Office SharePoint Server for Search 2007 (verzija za velika podjetja) daje na voljo dodatne ponudnike iskalnikov (search providers) in nudi večjo skalabilnost.

Spodnja tabela prikazuje večje sklope funkcionalnosti, ki jih nudijo različne verzije SharePoint-a.

Zmožnosti	Windows SharePoint services 3.0	Office SharePoint Server 2007 Standard CAL	Office SharePoint Server 2007 Enterprise CAL	Office SharePoint Server For Internet Sites
Sodelovanje	X	X	X	X
Portali		X	X	X
Iskalnik za velika podjetja (enterprise search)		X	X	X
upravljanje vsebine za velika podjetja (enterprise content management)		X	X	X
Poslovni procesi in forme			X	X
Poslovna inteligenca			X	X
Licenciran za internet/extranet	X	X	X	X

Tabela 1: Prikaz zmožnosti različnih verzij SharePoint-a 2007

### 3.3 Windows SharePoint Services 3.0

Microsoft Windows SharePoint Services 3.0 (v nadaljevanju WSS 3.0) je tehnologija, ki organizacijam in podjetjem vseh velikosti nudi podporo pri povečanju učinkovitosti poslovnih procesov in izboljšanju produktivnosti ekip, ki v poslovnih procesih sodelujejo. Z orodji za sodelovanje SharePoint nudi dostop do informacij, ki jih ljudje potrebujejo[12].

WSS 3.0 temelji na Microsoft Windows Server 2003 in nudi platformo za gradnjo poslovnih spletnih aplikacij, za katere omogoča visoko stopnjo skalabilnosti in fleksibilnosti pri izpolnjevanju zahtev v rastočem okolju. Robustne administrativne kontrole za upravljanje podatkov in spletne infrastrukture, nudijo IT oddelku stroškovno učinkovit način implementacije in upravljanja visoko performančnega okolja za sodelovanje. S spletno zasnovanim uporabniškim vmesnikom in tesno integracijo vsakdanjih orodij, vključno s sistemom Microsoft Office, je WSS 3.0 orodje, ki je enostavno za uporabo in ga je možno namestiti v zelo kratkem času.

WSS 3.0 je v pomoč ekipam pri ohranjanju stikov in produktivnosti s tem, da omogoča dostop do ljudi, dokumentov in informacij, ki so potrebne pri sprejemanju odločitev. WSS 3.0 na enostaven način omogoča skupno rabo dokumentov, vodenje opravil, učinkovito uporabo elektronske pošte in deljenje idej in informacij z ostalimi uporabniki na sledeče načine:

- Omogoča delovno okolje v katerem ekipe lahko koordinirajo urnike, organizirajo dokumente in sodelujejo v diskusijah znotraj organizacije ali podjetja ali izven njega.
- Enostavno ustvarjanje in rokovanje z dokumenti in pomoč za zagotovitev njihove integritete s pomočjo funkcij kot je »checkout« pred urejanjem dokumenta, možnost pregledovanja prejšnjih verzij, obnovo na prejšnje verzije in možnost nastavljanja pravic dostopa do dokumentov.
- Posameznikom in ekipam omogoča boljši nadzor nad opravili (objave, alarme, ankete in javne table (discussion boards)) s pomočjo komunikacijskih zmožnosti, ki uporabnike obveščajo kdaj je potrebno kakšno opravilo iz njihove strani ali kdaj je bila kakšna informacija ali dokument spremenjen.
- Ponuja forume, gradnjo baz znanja, ali zbiranje informacij v obliki, ki je enostavna za urejanje in nove predloge za implementacijo blogov in wikijev, brez zahteve po posebnem tehničnem znanju.
- Ohranitev produktivnosti med mobilnostjo z izboljšano podporo »offline« sinhronizacije s pomočjo Microsoft Outlook-a 2007, preko katerega lahko uporabniki upravljajo s knjižnicami dokumentov, sezname, koledarji, kontakti, opravili in javnimi tablami tudi takrat, ko nimajo mrežne povezave. Vse spremembe se sinhronizirajo ob ponovni priključitvi v omrežje.

Kot komponenta, ki je del strežnika Windows Server 2003, je WSS 3.0 za IT oddelke enostavna za implementacijo skalabilne infrastrukture in zahteva minimalne administrativne posege. WSS 3.0 povečuje varnost podatkov in informacij v organizaciji ali podjetju. Zmanjšuje odvisnost poslovnih enot od IT oddelka za opravila kot so skrb za upravljanje strani (site provisioning), implementacija, varnostno shranjevanje podatkov. Z WSS 3.0 je mogoče prirediti ali razširiti SharePoint okolje in ustvarjati nova, učinkovitejša, na spletnih tehnologijah temelječa orodja in specifične servise za organizacijo ali podjetje, oddelke in poslovne procese.

WSS 3.0 nudi naslednje zmožnosti:

- Funkcionalnost za upravljanje z dokumenti (Document Management functionality), do 500000 dokumentov.
- Vsebine, ki se v SharePoint-u samodejno ustvari na podlagi poslani elektronske pošte (Email-enabled content capabilities).
- Osnovne možnosti iskanja (Basic search capabilities).
- Možnosti obveščanja.
- RSS novice (RSS feed).
- Wiki strani (wikis).

- Blogi.
- Podpora mobilnim napravam.
- Direktna integracija s klienti Office 2003/2007.
- Možnost uporabe, kot nadomestilo Exchange-ovega javnega imenika.

### 3.4 Microsoft Office SharePoint Server 2007

Microsoft Office SharePoint Server 2007 (v nadaljevanju MOSS 2007) je strežniški programski paket, ki je del Microsoft Office sistema, bolj znanega pod imenom Microsoft Office[11, 14]. Microsoft Office je komplet vzajemno povezanih namiznih aplikacij, strežnikov in servisov, ki vsebuje funkcionalnost s katero stremi k učinkovitejšemu sodelovanju in k skupni rabi podatkov. MOSS 2007 razširja ali gradi na WSS 3.0 okolju in nudi rešitve, ki so še posebej uporabne za večja podjetja. Šest področji, ki jih pokriva MOSS 2007 lahko vidimo na spodnji sliki.



Slika 2: Glavna področja funkcionalnosti MOSS-a 2007

Zmožnosti MOSS-a 2007 so:

- **Sodelovanje** - Omogoča ekipam učinkovito skupno delo, sodelovanje in objavljanje dokumentov, vzdrževanje seznamov opravil, implementacijo delovnih tokov (workflow) in deljenje informacij z ostalimi uporabniki s pomočjo wikijev in blogov.
- **Portali** - Ustvarjanje osebnega portala MySite za deljenje informacij z ostalimi uporabniki, posebej uporabniške izkušnje in vsebine spletnega mesta glede na uporabnikov profil.
- **Iskalnik za velika podjetja** - Hitro in enostavno iskanje ljudi, znanja in vsebin v poslovnih aplikacijah.
- **Upravljanje vsebine za velika podjetja Enterprise Content Management** - Ustvarjanje in upravljanje dokumentov, zapisov in spletne vsebine.

- **Poslovni proces in obrazci (Business process and forms)** - Ustvarjanje delovnih tokov in elektronskih obrazcev za avtomatizacijo poslovnih procesov.
- **Poslovna inteligenca** - Omogoča enostaven dostop do kritičnih poslovnih informacij, analizo, pregled in objavo poročil kot podporo kvalitetnejšemu odločanju.

Kot primer strežniške komponente za aplikacije, ki deluje v okolju MOSS 2007, naj navedemo Excel, kateri v povezavi s servisi<sup>1</sup> SharePoint nudi platformo za sodelovanje. SharePoint sodeluje z MOSS-om 2007, na katerem gostuje stran SharePoint. Ta se izvaja na spletnem strežniku Internet Information Server (IIS) in ogrodju ASP.NET 2.0. Excel strežnik nudi storitve Excel, katere omogočajo ustvarjanje, urejanje in vzdrževanje Excel-ovih delovnih zvezkov (worksheets) v spletnem brskalniku. SharePoint<sup>2</sup> omogoča tudi skupno delo z wordovimi dokumenti preko funkcionalnosti skupne rabe, gostovanje predstavitev powerpoint v knjižnici predstavitev (slide library), iz katere se lahko uporabljajo predloge za predstavitve. V primeru spremembe katere od predlog je uporabnik o tem avtomatsko obveščen. Do vsakega dokumenta, ki gostuje na SharePoint-u je mogoče dostopati iz programa, ki je bil uporabljen za ustvaritev dokumenta, iz brskalnika ali iz Microsoft Outlook-a.

Zmožnosti MOSS-a 2007:

- Neomejena velikost skladišča za dokumente (Unlimited document repository capabilities).
- Osebnostne strani MySite (MySite personal sites).
- Dodatni vgrajeni spletni gradniki (web part), kot so npr. gradniki za socialna omrežja.
- Možnosti iskanja informacij po vsebinskih virih vključno z datotekami v skupni rabi, spletnimi stranmi, podatkovnimi bazami Lotus Notes in ostalimi viri vsebine iz drugih podjetij<sup>3</sup>.
- Iskanje ljudi.
- Podpora delovnim tokovom.
- Podpora za ASP .NET preverjanjem identitete (ASP .NET authentication) v obliki vtiča in avtentikacijo z obrazci.
- Podpora Single Sign-On.
- Imenik spletnih mest (site directory).
- Občinstvo (strani s ciljno vsebino) (Audiences (targeted site content))
- Iskalnik za velika podjetja.
- Pomembnost iskanih podatkov (Search relevance).
- Orodje za upravljanje indeksiranja (Indexing controls).
- Nastavitev varnostnih mehanizmov na iskane pojme (Security-trimmed search results).
- Predloge strani (Site templates).
- Politika zadrževanja in revizije (Retention and auditing policies).
- Glavne strani in načrti strani (Master pages and page layouts).
- Urejevalnik vsebine spletnih strani (Web content editor).
- Navigacijske kontrole.

Enterprise verzija nudi naslednje dodatne zmožnosti:

- Servise Excel.

<sup>1</sup> Besedna zveza servisi SharePoint se tu nanaša na servise, ki jih nudi WSS 3.0

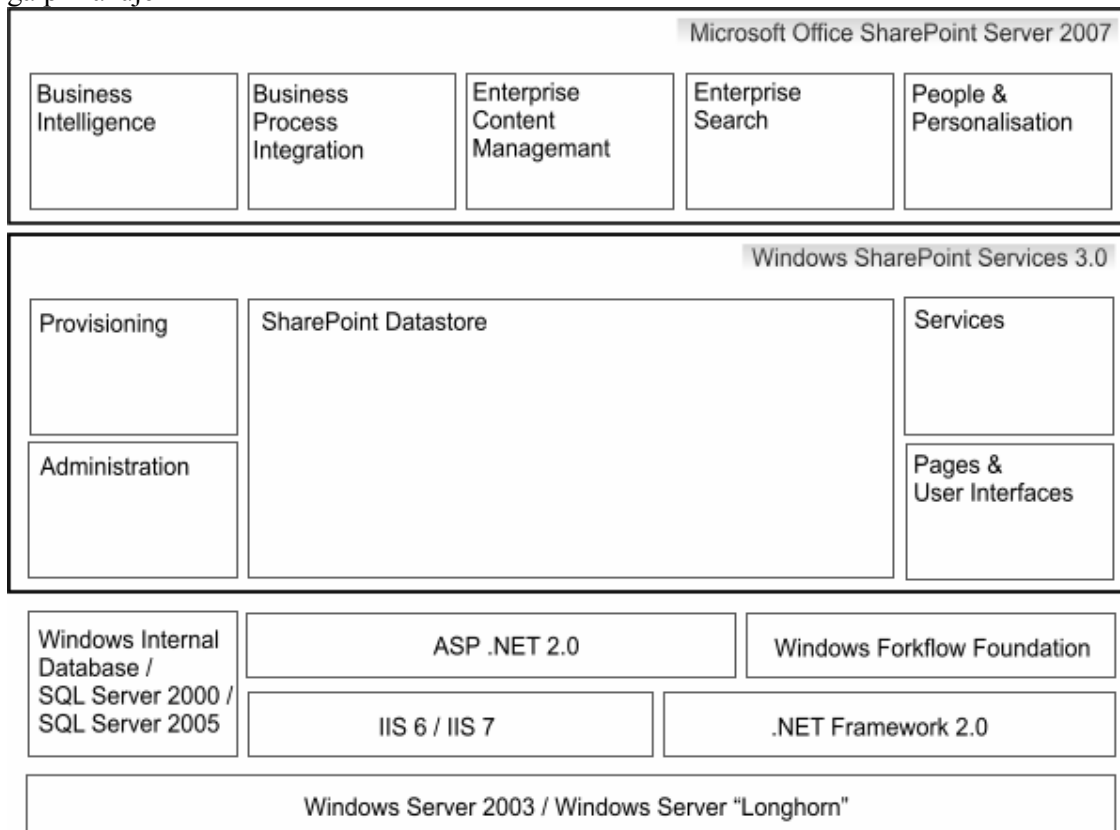
<sup>2</sup> Mišljeno kot celotno okolje, platforma, vključno z WSS 3.0 in MOSS 2007

<sup>3</sup> Vsebine, ki jo ustvarijo druga, zunanja podjetja in se nato uvozi v SharePoint okolje

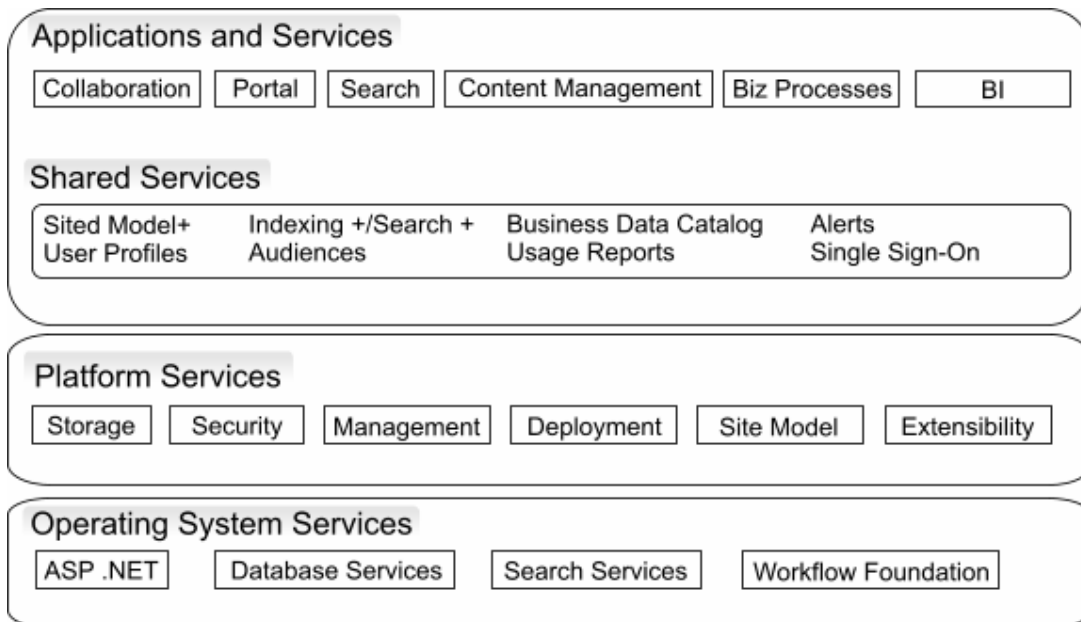
- Poslovno inteligenco.
- Podporo poslovnim procesom in poslovnim obrazcem.
- Iskanje poslovnih podatkov.

## 4 Arhitektura MOSS-a 2007

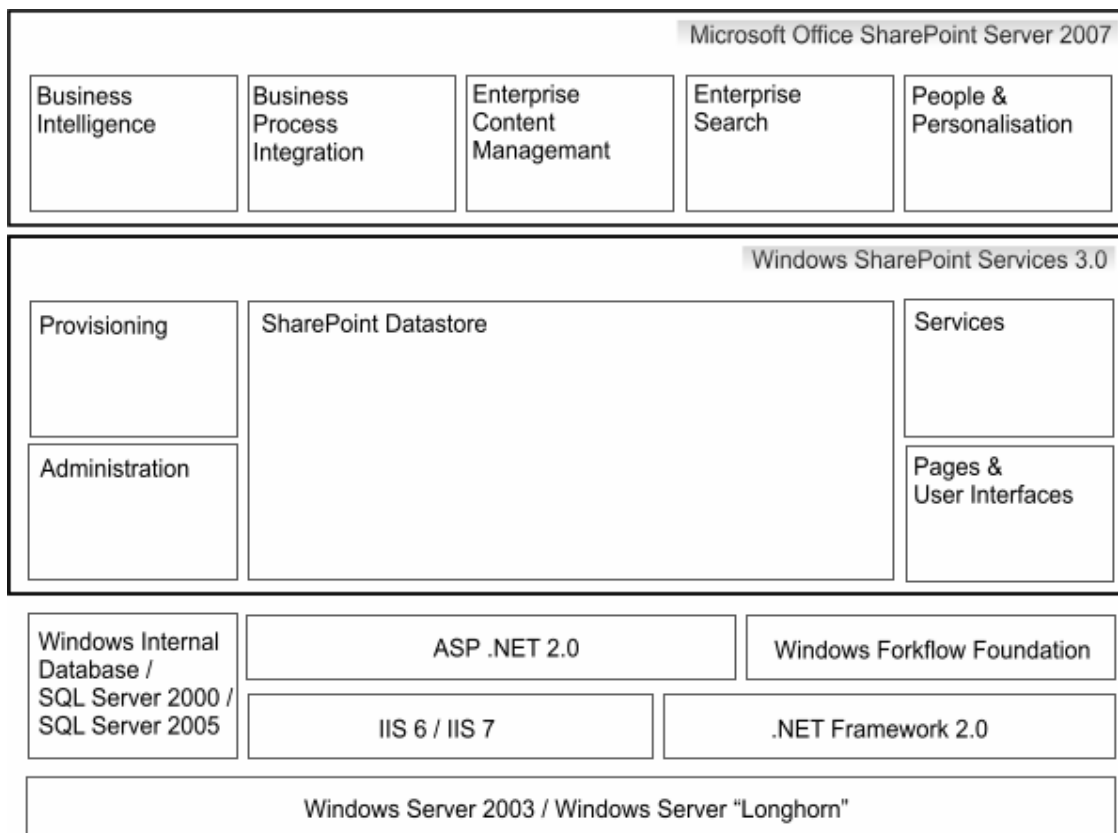
MOSS 2007 je okolje, ki je tesno povezano z več Microsoftovimi tehnologijami. Kot je razvidno iz Slika 3: Visokonivojska arhitektura Microsoft Office SharePoint Server 2007 je povezanost MOSS-a 2007 z ostalimi tehnologijami večplastna. Pogled s stališča razvijalca, ki ga prikazuje



Slika 4: Pogled na sodelujoče servise iz stališča razvijalca, nazorneje prikazuje povezave oz. meje med posameznimi komponentami.

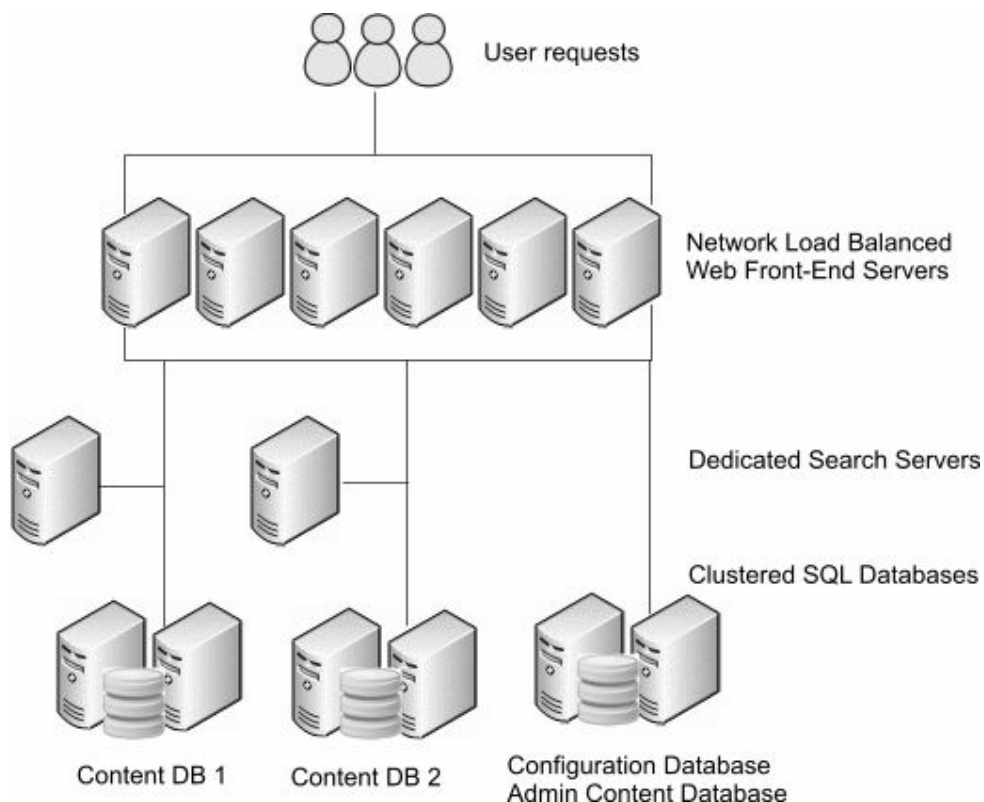


Slika 3: Visokonivojska arhitektura Microsoft Office SharePoint Server 2007



Slika 4: Pogled na sodelujoče servise iz stališča razvijalca [5]

Slika 5: Fizična arhitektura MOSS-a 2007 prikazuje fizični pogled na SharePoint okolje. Okolje sestavljajo strežniki Web Front-End, ki so konfigurirani v načinu »load balance«. To je način, ki omogoča porazdelitev obremenitve spletnih strežnikov in posledično izboljšanje odzivnosti posameznega strežnika. Na drugem nivoju sta prikazana dva strežnika, ki sta namenjena zmožnosti iskanja. Tretji nivo prikazuje gručo strežnikov SQL z različnimi podatkovnimi bazami. Strežnik namenjen iskanju, na levi strani, deluje v okviru vsebine vsebinske podatkovne baze številka ena, tisti na desni pa v okviru vsebinske podatkovne baze številka dva. Na desni strani je predstavljena konfiguracijska podatkovna baza (Configuration Database (configdb)) in administrativna podatkovna baza.



Slika 5: Fizična arhitektura MOSS-a 2007

#### 4.1 Storitve operacijskega sistema

MOSS 2007 je zgrajen na tehnologijah in storitvah Windows Server 2003 Service Pack 1 (SP1) in Microsoft SQL Server 2005.

Servisi, ki tvorijo jedro in razvojno platformo operacijskega sistema vključujejo:

- Microsoft .NET 2.0 Framework
- ASP.NET 2.0 glavne strani, vsebinske strani in spletni gradniki
- Modeli vtičnikov s ponudnik servisov za personalizacijo, članarino, navigacijo in izboljšano varnost (Pluggable service-provider models for personalization, membership, navigation, and enhanced security)
- Storitve za dostop do podatkovne baze
- Internet Information Services (IIS)
- Windows Workflow Foundation
- Indeksiranje na namiznem računalniku z operacijskim sistemom Windows in servisi za iskanje (Windows desktop indexing and search services)

SQL Server je relacijska podatkovna baza, ki se uporablja za shranjevanje vsebine, podatkov in konfiguracije v okolju MOSS 2007. Ob privzetem načinu namestitve MOSS-a 2007 se instalira Server 2005 Express, priporočljiva izbira pa je SQL Server 2005. Podprta je tudi verzija SQL Server 2000.

## **4.2 Storitve podatkovne baze**

### **4.2.1 Konfiguracijska podatkovna baza**

WSS 3.0 kreira konfiguracijsko podatkovno bazo med instalacijo. Vsaka farma ima lahko samo eno konfiguracijsko podatkovno bazo. Konfiguracijska podatkovna baza shranjuje sledeče nastavitve:

- Strani (Sites).
- Podatkovne baze - ne vključuje podatkovnih baz povezanih s storitvami Excel-a ali zunanjih podatkovnih baz. Slednje se obravnavajo kot zunanji podatki, ki niso del okolja MOSS 2007.
- Strežnike.
- Spletne aplikacije.

### **4.2.2 Vsebinske podatkovne baze**

Vsaka spletna aplikacija ima vsebinsko podatkovno bazo. WSS 3.0 omogoča širjenje strani na več podatkovnih baz. To je priporočljivo storiti v primeru, da baza zraste čez 100 GB.

Podatkovna baza služi kot zbirka podatkov za zbirko strani in vsebino znotraj zbirke strani vključno z:

- Detajli o WSS straneh.
- Detajli o strukturi.
- Vsebino uporabnikov.
- Datotekami.
- Informacijami o varnosti.

### **4.2.3 Podatkovna baza Shared Services Provider**

Vsak ponudnik skupnih servisov (Shared Services Provider ali SSP) ima natanko eno podatkovno bazo SSP. Podatkovna baza SSP služi kot skladišče za:

- Uporabniške profile.
- Podatke uporabnikov (Audience data).
- Podatke poslovnih aplikacij (Business application data).
- Funkcije servisov Excel (Excel Services functions).
- Podatke o uporabi strani (Site usage data).
- Informacije o stanju sej servisov InfoPath Forms (InfoPath Forms Services session state information).

### **4.2.4 Podatkovna baza iskalnika**

MOSS 2007 uporablja ločeno podatkovno bazo za shranjevanje podatkov, ki jih zbere iskalnik. Podatkovna baza iskalnika (Search Database) je ločena od SSP podatkovne baze z namenom lažjega upravljanja s takšnimi podatkovnimi bazami. Takšen pristop omogoča

administratorju farme ustvarjanje varnostnih kopij z večjo stopnjo granularnosti. Natanko ena podatkovna baza iskalnika je lahko ustvarjena za vsak SSP. Podatkovna baza iskalnika vsebuje:

- Podatke po katerih iskalnik išče (Search data)
- Dnevnik zgodovine (History log)
- Dnevnik iskanj (Search log)
- Računske tabele za statistiko brskanja (Calculation tables for crawl statistics)
- Tabele povezav in statistične tabele (Links tables and statistical tables)

#### 4.2.5 Indeks iskalnika

Indeks iskalnika se shranjuje na datotečnem sistemu (*file system*). Primerki (instance) podatkov takšnega tipa se shranijo v konfiguracijsko podatkovno bazo in iskalnik ponuja vmesnik za shranjevanje takšnih podatkov.

#### 4.2.6 Zunanje podatkovne baze

Aplikacije zunanjih podjetij (3rd-party applications) lahko shranjujejo specifične podatke v svoje podatkovne baze. Takšne podatkovne baze je mogoče registrirati v konfiguracijski podatkovni bazi in jih tako vključiti v MOSS 2007 infrastrukturo. Nad podatkovnimi bazami vključenimi v to infrastrukturo pa je mogoče izvajati operacije varnostnega shranjevanja podatkov in obnove podatkov.

## 5 Varnostno shranjevanje podatkov v MOSS 2007

Shranjevanje podatkov z vidika ustvarjanja varnostnih kopij obstoječih podatkov je v današnjih poslovnih okoljih nujen, preventiven poseg, ki varuje in zmanjšuje prekinitev poslovnih procesov v podjetju, v primeru programske napake strežnika, nekonsistentnosti podatkovne baze ali kakršnekoli oblike izgube podatkov. Varnostne kopije podatkov so nujne za obnovo posameznih podatkovnih baz ali ponovno vzpostavitev celotnega sistema po katastrofi.

Za ilustracijo pomembnosti varovanja podatkov naj omenimo za koliko uporabnikov je MOSS 2007 okolje načrtovano [2]:

- Samostojni strežnik z SQL Express: običajno do 500 uporabnikov
- Samostojni strežnik z SQL Server: običajno do 5000 uporabnikov
- Majhna farma: običajno do 50000 uporabnikov
- Srednja farma: običajno do 100000 uporabnikov
- Velika farma: običajno do 500000 uporabnikov

Okolja z nekaj terabajti podatkov niso redkost.

### 5.1 Rešitve za izdelovanje varnostnih kopij podatkov in obnovitev podatkov

V tem poglavju si bomo najprej ogledali načine izdelovanja varnostne kopije podatkov (backup) glede na osnovna namena shranjevanja podatkov. Podatke lahko shranjujemo z namenom obnove (restore) določenega dela vsebine ali z namenom ponovne vzpostavitve

celotnega sistema. V nadaljevanju bomo podrobneje obravnavali vsakega od načinov varnostnega shranjevanja podatkov z njegovimi pozitivnimi in negativnimi lastnostmi.

### **5.1.1 Obnova vsebine in obnova podatkov po katastrofi**

Namen izdelovanja varnostnih kopij podatkov glede na obnovo vsebine (content recovery) izhaja iz potrebe po pripravljenosti na okvare zaradi nadgradnje programske opreme ali nenamerne izbrise podatkov iz strani uporabnikov. Nenamerni izbrisi so pogost pojav, vpliv na celotno okolje pa je navadno zelo majhen.

Operacije za obnovo podatkov po katastrofi (Disaster recovery - Catastrophic restore operation) se izvršujejo za zaščito podatkov pred tako imenovanimi katastrofalnimi dogodki, ki imajo za posledico zamenjavo strojne opreme ali ponovno namestitev programske opreme.

Obnovo vsebine in ostalih podatkov v MOSS-u 2007 lahko obnovimo:

- Iz koša.
- S pomočjo sistema verzij vsebine.
- Z izdelavo ali obnovo varnostne kopije zbirke strani (V Tabela 2: Pregled orodij za obnovo podatkov imenovan SC B/R - Site Collection Backup and Restore)
- S pomočjo uporabe mehanizma dogodka o brisanju spletne aplikacije. Objektne model SharePoint-a omogoča programerjem gradnjo po meri narejenih aplikacij za varnostno shranjevanje podatkov, ki temeljijo na omenjenem mehanizmu.
- Omogoča varnostno shranjevanje in obnovo podatkov z orodji, ki so del MOSS 2007 okolja. Z ogrodjem, ki ga je mogoče razširiti preko objektnega modela za izdelavo varnostne kopije podatkov in obnovo podatkov iz varnostne kopije (V spodnji tabeli označena kot SharePoint B/R).
- Zapisovalnik SharePoint Volume Shadow Copy Services (VSS). VSS omogoča centralizirano ogrodje za vse strežniške aplikacije.
- Izdelava varnostne kopije podatkov in obnova z orodji SQL.
- Pošiljanje dnevnikov SQL.

<b>Rešitev/Objekt</b>	<b>SQL</b>	<b>Pošiljanje dnevnikov</b>	<b>WSS API</b>	<b>VSS zapisovalnik</b>	<b>Koš</b>
<b>Farma</b>			X	X	X
<b>Konfiguracijska podatkovna baza</b>	Da, če obnovimo podatke na enaki sistemski konfiguraciji		Da, če obnovimo podatke na enaki sistemski konfiguraciji	Da, če obnovimo podatke na enaki sistemski konfiguraciji	Da, če obnovimo podatke na enaki sistemski konfiguraciji
<b>Spletna aplikacija</b>			X		
<b>Vsebinska podatkovna baza</b>	X	X	X	X	
<b>Zunanja podatkovna baza</b>	X	X	X	X	
<b>Zbirka strani (site collection)</b>					
<b>Spletna stran</b>					
<b>Seznam/knjižnica dokumentov</b>					X
<b>Imenik knjižnice dokumentov</b>					X
<b>Datoteka knjižnice dokumentov</b>					X
<b>Predmet iz seznama (List item)</b>					X
<b>Verzija</b>					X

Rešitev/Objekt	Označevanje verzij	Zbirka strani	Dogodek brisanja spletne aplikacije	Migracija vsebine
Farma				
Konfiguracijska podatkovna baza				
Spletna aplikacija				
Vsebinska podatkovna baza				
Zunanja podatkovna baza				
Zbirka strani (site collection)		X		
Spletna stran			X	X
Seznam/knjižnica dokumentov				X
Imenik knjižnice dokumentov				X
Datoteka knjižnice dokumentov	X			X
Predmet iz seznama (List item)	X			X
Verzija	X			X

Tabela 2: Pregled orodij za obnovo podatkov

## 5.2 Izdelava varnostnih kopij in obnova podatkov iz varnostnih kopij

### 5.2.1 Označevanje verzij

Označevanje verzij rešuje težavo izgube podatkov v primeru prepisovanja dokumentov. Omogoča hranjenje več kopij istega dokumenta. V primeru nenamerne spremembe, kot je brisanje ali nekonsistenca dokumenta, lahko uporabnik dokument obnovi. Označevanje verzij je mogoče vključiti na nivoju knjižnice (library level) ali na nivoju seznamov (list level). Z verzijo lahko označujemo predmete (items) in datoteke.

Poleg tega, da uporabnik lahko sam upravlja z verzijami in tako razbremeni administratorja, je mogoče s premišljeno uporabo sistema za označevanje verzij uporabniku tudi sporočiti v kateri fazi se določen dokument nahaja. Lahko je na primer osnutek ali pa končna verzija. Sporoča nam lahko katere nedavne spremembe so bile storjene in ali so se meta podatki dokumenta spremenili, ter zakaj so se spremenili.

Pri delu z označevanjem verzij imamo na voljo tri opcije:

- Brez označevanja verzij: Prejšnje verzije dokumenta in zgodovina dokumenta (npr. komentarji) povezana z vsako verzijo dokumenta ni na voljo. To je privzeta opcija.
- Ustvarjanje večjih verzij: Znano tudi kot enostavno označevanje verzij. Vsaka iteracija postane polna kopija (full copy) dokumenta, kjer je vsaka verzija označena z zaporedno številko (1, 2, 3, itd.). Vsi uporabniki s pravicami dostopa do knjižnice dokumentov lahko pregledujejo obnovljene verzije. Navadno se ta opcija uporabi, če ni potrebe med verzijami osnutkov in končne verzije. Za boljšo kontrolo nad diskovnim prostorom, ki ga verzije zavzamejo, je mogoče določiti kolikšno število prejšnjih verzij naj se ohrani, glede na trenutno verzijo.
- Ustvarjanje večjih in manjših verzij: Verzije, ki se končajo s številko 0 predstavljajo večje verzije, tiste, ki imajo večji obseg sprememb. Verzije, ki se končajo s številkami različnimi od 0 so verzije z manjšim obsegom sprememb. Objavijo se lahko le večje verzije. Dodatne pravice dostopa do manjših verzij je mogoče nastaviti. V večini primerov imajo uporabniki s pravicami za urejanje večjih verzij tudi pravico za urejanje manjših verzij. Uporabniki s pravicami omejenimi na branje lahko večje verzije le pregledujejo, ne morejo pa jih spreminjati. Možno je nastaviti koliko verzij, glede na trenutno verzijo, naj se hrani. Obstaja tudi opcija za nastavitve ohranitve števila manjših verzij glede na večjo verzijo.

Označevanje verzij za standardne sezname je omejeno na večje verzije.

### 5.2.2 Koš

Koš je zelo praktična funkcionalnost, ki lahko administratorju zelo olajša delo. Pretekle verzije MOSS-a, ki te funkcionalnosti niso vključevale, so za obnovo posameznega dokumenta zahtevale poseg administratorja in obnovo celotne vsebinske baze podatkov. MOSS 2007 vsebuje dvonivojski koš, ki takšne scenarije preprečuje.

Prvonivojski koš (ali koš na nivoju uporabnika) je postavljen na nivo končnega uporabnika. Omogoča funkcijo "odbrisanja" s katerim lahko uporabnik s primernimi pravicami obnovi nenamerno izbrisane datoteke, dokumente, sezname predmetov, sezname in knjižnice dokumentov iz strani (site).

Drugonivojski koš (ali koš zbirke strani) je postavljen na nivoju administratorja seznama spletnih mest (site collection). Drugonivojski koš je sestavljen iz objektov, ki so v prvonivojskem košu vseh spletnih mest, v seznamu spletnih mest in objektov v drugonivojskem košu. Ko je predmet izbrisan iz prvonivojskega koša, se premakne v drugonivojski koš, iz tam pa ga lahko obnovi le administrator seznama spletnih mest.

Nastavitve koša se lahko nastavijo na nivo spletne aplikacije (web application level) iz centralne administrativne strani.

Zmožnosti koša:

- Koš hrani izbrisane dokumente in elemente seznamov (dokumente, verzije dokumentov, knjižnice dokumentov, knjižnice slik, obvestila, koledarje, povezave, opravila, mape, strani, diskusije tima).
- Ko je predmet iz seznama izbrisan se izbriše tudi vsakršna priponka vezana na ta predmet. Takšen predmet je možno obnoviti iz koša.

- Predmetov ni mogoče odpirati ali pregledovati medtem ko so v košu. Preden se lahko dokument odpre ali se ga ogleda, ga je potrebno obnoviti.
- Ob privzetih nastavitvah se predmeti v obeh koših samodejno izbrišejo po tridesetih dneh. Uporabnik lahko ta čas nastavi po svojih potrebah. Mehanizem samodejnega brisanja predmetov drugonivojskega koša pa se sproži, ko vsota velikosti dokumentov, ki ga zasedajo na disku, preseže določljivo nastavljeno vrednost. Zbrišejo se najprej najstarejši predmeti in sicer v takšni količini, da skupna velikost preostalih dokumentov ostane znotraj okvira nastavljene vrednosti. Predmeti se premaknejo iz prvostopenjskega koša v drugostopenjski koš, ko se vsebina prvostopenjskega koša izprazni. Časovni limit za samodejno brisanje predmeta se nanaša na prvotno brisanje predmeta (s strani uporabnika) in ne na čas, ki ga je predmet prebil v katerem izmed košev.
- Izklop koša spletne aplikacije ima za posledico brisanje celotne vsebine, ki jo koš v tistem trenutku vsebuje.
- Koša lahko vsebujeta več kopij dokumenta z enakim imenom in izvorom. Takšne dokumente je nemogoče obnoviti čez obstoječi dokument.
- Koš je nemogoče uporabiti za obnovo prejšnjih verzij ali nenamernih prepisov dokumentov – v ta namen je potrebno uporabiti označevanje verzij.
- Koš ne upravlja brisanja strani in brisanja seznama strani.

Dejstva prvonivojskega koša:

- Predmeti, ki se nahajajo v prvonivojskem košu zasedajo diskovni prostor v okviru strani (site quota)
- Uporabniki morajo imeti “prispeva” (contribute), “načrtuj” (design) ali “polne pravice” (full control) na strani, če želijo izvajati operaciji brisanja in obnove.
- Po privzetih nastavitvah, so predmeti urejeni v padajočem vrstnem redu, glede na datum izbrisa.

Dejstva o drugonivojskem košu:

- Definirati je mogoče količino prostora, ki jo MOSS 2007 rezervira za drugonivojski koš. Količina je izražena v odstotkih glede na kvoto strani (site quota).
- Predmeti, ki so shranjeni v drugonivojskem košu ne zasedajo diskovne kvote, ki je dodeljena strani. Velikost, ki je definirana za drugonivojski koš poveča skupno velikost strani in vsebinske podatkovne baze, ki jo gostuje. Če diskovna kvota ni določena potem tudi meje pri velikosti drugostopenjskega koša ni.
- Drugonivojski koš je mogoče izklopiti.
- Samo administratorji seznamov strani (site collection) lahko obnavljajo iz drugonivojskega koša.
- Po privzetih nastavitvah se predmeti v košu sortirajo po padajočem vrstnem redu glede na datum izbrisa. Poleg datuma lahko kot parameter za sortiranje izberemo tudi katerega izmed drugih stolpcev: Ime, Originalna lokacija, avtor, izbrisano (datum in ura), velikost.

### **5.2.3 Prestrežanje dogodka brisanja strani z Microsoftovim IT Site Delete Capture feature 1.0**

Ko se stran izbriše, se sproži dogodek izbrisa spletne strani. Microsoft IT (MSIT) je razvil Microsoft IT Site Delete Capture feature 1.0 za zaznavo in reagiranje ob dogodku izbrisa

spletne strani. Ko je takšen dogodek zaznan, Site Delete Capture arhivira stran na omrežno mesto (file share) preden se ta dokončno izbriše iz konfiguracijske podatkovne baze in vsebinske podatkovne baze. Site Delete capture je mogoče nastaviti tako, da se ob uspešnem ali neuspešnem arhiviranju in brisanju pošlje elektronska pošta.

To orodje je brezplačno in je na voljo na Microsoftovih spletnih straneh<sup>1</sup>. Orodje ni del MOSS 2007 in ni zagotovila, da bo v prihodnosti nadgrajeno, saj ga Microsoft uradno ne podpira. Orodje lahko instalira le administrator strani (site administrator) ali administrator farme.

## 5.2.4 Izdelovanje varnostne kopije z uporabo priloženih orodij

SharePoint nudi varnostno shranjevanje podatkov s pomočjo sledečih priloženih orodij:

- Centralne administracije, kjer operacijo izvedemo preko grafičnega vmesnika v spletnem brskalniku
- Iz ukazne vrstice s pomočjo programa stsadm

Kot primer ustvarjanja varnostne kopije navajamo uporabo programa stsadm pri ustvarjanju varnostne kopije celotne farme, web aplikacije ali katere koli druge logične komponente:

```
stsadm -o backup -directory <UNC path or local drive> -backupmethod <Full or Differential>
```

Kot je razvidno iz primera, je programu potrebno navesti sledeče parametre:

- Operacijo izdelava varnostne kopije (backup) ali obnovo podatkov iz varnostne kopije (restore)
- Imenik na datotečnem sistemu ali imenik v skupni rabi na katerem koli oddaljenem računalniku
- Način varnostnega kopiranja (backupmethod)
- Logično ime komponente za katero želimo, da se varnostna kopija ustvari

WSS 3.0 in MOSS 2007 podpirata diferencialen (differential backup) in poln način izdelave varnostne kopije podatkov (full backup). Preden lahko naredimo diferencialno varnostno kopijo moramo poskrbeti, da obstaja polna varnostna kopija podatkov:

- Polna varnostna kopija podatkov: Ustvari se celotna kopija podatkov izbranih logičnih komponent
- Diferencialna varnostna kopija: Kopirajo se le podatki, ki so se spremenili od zadnje polne varnostne kopije

Pomembno pri definiranju ciljnega imenika je, da uporabnik zagotovi ustrezne uporabniške pravice za agenta SQL, kateri na izbran imenik zapisuje varnostno kopijo podatkov.

Z orodjem stsadm je možno izdelati tudi varnostno kopijo za posamezno zbirko strani ali pa celotno farmo:

```
stsadm -o backup -url <URL of the site collection> -filename <Name of the backup file>
```

Izdelava varnostne kopije v centralni administraciji poteka preko spletnega uporabniškega vmesnika. Funkcionalnost, ki jo nudi centralna administracija, se v večji meri prekriva s funkcionalnostjo orodja stsadm, saj obe temeljita na rešitvi objektnega modela za izdelavo

<sup>1</sup> CodePlex governance, <http://go.microsoft.com/fwlink/?LinkID=92682&clcid=0x409>

varnostnih kopij, ki je del MOSS okolja. Naslednji dve sliki prikazujeta dva koraka pri izdelavi varnostne kopije. Slika 6: Izbor komponent za izdelavo varnostne kopije v priloženem orodju centralne administracije prikazuje logične komponente, ki jih MOSS 2007 okolje vsebuje in jih lahko vključimo v izdelavo varnostne kopije.

Central Administration > Operations > Perform a Backup

## Perform a Backup - Step 1 of 2: Select Component to Backup

Select the items you want to backup now. To start a backup, click **Continue to Backup Options**. To see a list of previous backups, click **View History**.

Select	Component	Type
<input type="checkbox"/>	Farm	Farm
	SharePoint_Config	Configuration Database
<input type="checkbox"/>	Windows SharePoint Services Web Application	Windows SharePoint Services Web Application
<input type="checkbox"/>	Juventus - 26098	Web Application
<input type="checkbox"/>	WSS_Content_30b2c9ad1b004d978519b0adf1f9f0dd	Content Database
<input type="checkbox"/>	Milan - 4298	Web Application
<input type="checkbox"/>	WSS_Content_7e35eff91fe04f98b532e36f01887300	Content Database
<input type="checkbox"/>	SharePoint MySites - 101	Web Application
<input type="checkbox"/>	WSS_Content	Content Database
	WSS_Administration	Central Administration
	Web Application	Web Application
<input type="checkbox"/>	SharePoint_AdminContent_4707d700-bdfa-4299-8305-08828cfd06e3	Content Database
<input type="checkbox"/>	MySSP1	Shared Services Provider
	SharePoint - 100	Web Application
<input type="checkbox"/>	WSS_Content_webapp_100	Content Database

**Slika 6: Izbor komponent za izdelavo varnostne kopije v priloženem orodju centralne administracije**

Slika 7: Določitev vrste varnostne kopije in lokacije v priloženem orodju centralne administracije prikazuje drugi korak v postopku izdelovanja varnostne kopije in sicer izbor načina izdelave varnostne kopije, ki je lahko poln ali diferencialen, in določitev lokacije kamor se varnostna kopija shrani.

Central Administration > Operations > Perform a Backup > Start Backup - Step 2 of 2: Select Backup Options

## Start Backup - Step 2 of 2: Select Backup Options

Use this page to configure a backup job.

<p><b>Backup Content</b></p> <p>Specify content to include in the backup.</p>	<p>Backup the following component:</p> <p>Farm\Windows SharePoint Services Web Application\Juventus - 26098</p>
<p><b>Type of Backup</b></p> <p>Specify which type of backup to start:</p> <ul style="list-style-type: none"> <li>Full - backs up the selected content with all history.</li> <li>Differential - backs up all changes to the selected content since the last full backup.</li> </ul>	<p>Type of backup:</p> <p><input checked="" type="radio"/> Full</p> <p><input type="radio"/> Differential</p>
<p><b>Backup File Location</b></p> <p>Specify where to store the backup files. Each backup job is stored in a separate subdirectory at the location you specify, and each object is backed up to an individual file in that subdirectory. Learn about backup locations.</p>	<p>Backup location:</p> <p><input type="text"/></p> <p>Example: \\backup\SharePoint</p> <p>Estimated Disk Space Required: 14.69 MB.</p>

**Slika 7: Določitev vrste varnostne kopije in lokacije v priloženem orodju centralne administracije**

## 5.2.5 Obnova podatkov iz varnostne kopije

Postopek obnove podatkov s pomočjo grafičnega vmesnika v centralnem administratorju ali s pomočjo stsadm programa je povsem analogen postopku za kreiranje varnostne kopije. Razlika je le v tem, da se pri obnovi podatkov konfiguracijska podatkovna baza ne obnovi. Razlog za to tiči v tem, da konfiguracijska baza vsebuje specifične podatke o topologiji MOSS farme (imena strežnikov, informacije o strojni opremi), ki bi lahko povzročili težave v primeru obnove te podatkovne baze na drugi farmi.

## 5.2.6 Prednosti in slabosti priloženih orodij

Prednosti	Slabosti
Edini orodji s katerimi je mogoče narediti varnostno kopijo iskalnega indeksa (search index) in ga tudi obnoviti	Operaciji kreiranja varnostne kopije in obnove podatkov sta lahko procesorsko zelo intenzivni
Možno je ustvariti varnostne kopije in obnovo Internet Information Service (IIS) konfiguracij narejenih s SharePoint produkti in tehnologijami.	Operaciji kreiranja varnostne kopije in obnove podatkov zahtevata veliko časa in lahko povzročita nedostopnost okolja oz. slabo odzivnost.
Po obnovi podatkov ponovno vzpostavi povezavo vsebinskih podatkovnih baz s spletnimi aplikacijami	

Tabela 3: Prednosti in slabosti priloženih orodij

## 5.3 Izdelava varnostnih kopij z orodji strežnika SQL

Poglavje opisuje ustvarjanje varnostne kopije in obnovo podatkov s pomočjo strežnika SQL Server 2005 v okolju SharePoint. Najprej si bomo ogledali arhitekturo ter kako WSS 3.0 in MOSS 2007 shranjujeta podatke v strežniku SQL, nato pa predstavili rešitve.

### 5.3.1 Arhitektura podatkovne baze strežnika SQL

Preden lahko učinkovito upravljamo s podatkovnimi bazami je potrebno razumeti kako so fizično in logično organizirane. V nadaljevanju si bomo zato ogledali pogoste diskovne arhitekture, ki izpolnjujejo performančne zahteve in zahteve po dostopnosti pri podatkovnih bazah.

### 5.3.1.1 Fizična in logična arhitektura

Podatkovna baza strežnika SQL Server 2005 uporablja tri tipe fizičnih datotek, ki so opisane v spodnji tabeli.

Tip datoteke	Opis
Primarna podatkovna datoteka (.mdf)	Vsak strežnik SQL Server 2005 ima eno primarno podatkovno datoteko. To je privzeta datoteka v kateri strežnik hrani podatke.
Sekundarna podatkovna datoteka (.ndf)	Podatkovna baza lahko vključuje več sekundarnih podatkovnih datotek, ki ravno tako kot primarna datoteka, hranijo podatke. Primarna podatkovna datoteka hrani podatke o sekundarnih podatkovnih datotekah za vsako podatkovno bazo posebej.
Dnevniška datoteka (.ldf)	Vsaka podatkovna baza vključuje eno ali več dnevniških datotek, ki vsebujejo dnevnik o transakcijah (transaction logs). To so zapisi vsake transakcije v podatkovni bazi. Transakcijski zapisi se lahko uporabijo za obnovo podatkovne baze v primeru okvare podatkovne baze.

**Tabela 4: Fizična in logična arhitektura podatkovne baze na strežniku SQL**

Vsaka podatkovna datoteka je sestavljena iz sekvenčno oštevilčenih strani podatkovne baze. V strežniku SQL Server 2005 je velikost vsake strani 8KB. Strani podatkovne baze so najmanjša fizična enota za hranjenje podatkov. Strežnik SQL bere in piše strani podatkovne baze na disk. Strani lahko vsebujejo podatke, indekse ali druge informacije. Strežnik SQL Server 2005 vključuje funkcijo, ki omogoča detekcijo nekonsistence podatkov na nivoju strani. Ta funkcija se ob privzetih nastavitvah vključi ob kreiranju nove podatkovne baze in v primeru nekonsistence podatkov strani vrne napako s kodo 824 vključno z detajli o strani na katero se nanaša. Strežnik SQL Server 2005 Enterprise Edition omogoča tudi obnovitev posamezne strani, ne da bi pri tem ustavil delovanje podatkovne baze.

### 5.3.1.2 Transakcijski dnevnik

Transakcijski zapis je osnovni zapis, ki ga lahko uporabimo za preprečitev izgube podatkov v primeru okvare strojne opreme ali v primeru okvare stroja podatkovne baze (database engine). V primeru okvare, moramo obnoviti podatkovno bazo tako, da je njeno stanje takšno, kot je bilo ob zadnji varnostni kopiji te baze. Za preprečitev izgube podatkov pa je potrebno nato aplicirati na obnovljeno podatkovno bazo vsako transakcijo, ki se je izvedla med časom, ko je bila ustvarjena zadnja varnostna kopija in časom okvare.

Zaradi pomembnosti transakcijskih dnevnikov je priporočljivo, da se ti dnevnik nahajajo na disku, ki je fizično ločen od datotek s podatki. Uporabnik mora poskrbeti, da je za transakcijske dnevnik namenjeno dovolj prostora za zapis vsake transakcije, ki se je zgodila

od časa kreiranja zadnje varnostne kopije. Zaradi omenjenih priporočil in zahtev je priporočljiva tudi izdelava varnostne kopije transakcijskih dnevnikov.

### 5.3.1.3 Arhitektura diska

V večini namestitev MOSS-a se datoteke podatkovne baze shranjujejo na RAID (Redundant Array od Independent Drives). RAID se uporablja za izboljšanje vhodno izhodne hitrosti diska in/ali redundanco podatkov za primer okvare posameznega diska.

### 5.3.2 Podatkovne baze WSS 3.0

Instalacija farme z WSS 3.0 vsebuje:

- konfiguracijsko bazo,
- eno ali več vsebinskih baz,
- vsebinsko bazo za centralno administracijo,
- bazo iskalnika

Za obnovitev konfiguracijske podatkovne baze ali za obnovitev vsebinske baze za centralno administracijo ne moremo uporabiti orodij, ki jih nudi WSS 3.0. V teh primerih lahko uporabimo orodja za izdelavo varnostnih kopij, ki jih nudi strežnik SQL. Moramo pa se zavedati, da je obnovitev konfiguracijske podatkovne baze na strežniku z drugačnim imenom, kot ga ima strežnik, na katerem je bila konfiguracijska baza ustvarjena, odsvetovana, saj v takšnem primeru, WSS 3.0 ali MOSS 2007 ne bo deloval pravilno. Prav tako odsvetujemo obnovitev konfiguracijske podatkovne baze v okolje z drugačno topologijo od originalne.

### 5.3.3 Podatkovne baze MOSS-a 2007

Instalacija Office SharePoint Server 2007 farme vsebuje:

- konfiguracijsko podatkovno bazo,
- eno ali več vsebinskih podatkovnih baz,
- vsebinsko podatkovno bazo za centralno administracijo,
- podatkovno bazo iskalnika
- eno ali več podatkovnih baz ponudnika skupnih servisov (Shared Service Provider-ja - SSP),
- eno ali več vsebinskih podatkovnih baz ponudnika skupnih servisov,
- eno ali več podatkovnih baz iskalnika za ponudnika skupnih servisov (opozorilo: indeks iskalnika se ob uporabi orodij SQL za izdelavo varnostne kopije podatkov ne shrani, saj so datoteke, ki indeks tvorijo, na datotečnem sistemu in ne v okviru podatkovne baze)

Orodja za izdelavo varnostne kopije podatkov v MOSS 2007 ni mogoče uporabiti za obnovo konfiguracijske podatkovne baze ali za obnovitev vsebinske podatkovne baze centralne administracije. Ti dve podatkovni bazi je mogoče obnoviti s pomočjo orodij strežnika SQL vendar pa veljajo enake omejitve kot pri obnovitvi podatkovnih baz v okolju WSS 3.0.

### 5.3.4 Konfiguracija strežnika SQL za izdelavo varnostne kopije podatkov

S pomočjo orodij strežnika SQL Server 2005 je mogoče izdelovati varnostne kopije podatkovnih baz na štiri načine:

Tipi varnostne kopije	Opis
Polna varnostna kopija	Izdela polno kopijo strukture in vsebine podatkovne baze
Diferencialna varnostna kopija	Izdela kopijo podatkov, ki so se spremenili od zadnje polne kopije
Delna varnostna kopija (Partial backup)	Izdela kopijo specifičnih datotek ali datotečnih skupin
Varnostna kopija transakcijskih dnevnikov (Transaction log backup)	Izdela kopijo transakcijskih dnevnikov

**Tabela 5: Tipi varnostne kopije**

V praksi se običajno uporablja kombinacija vseh omenjenih tipov.

### 5.3.4.1 Strategije izdelovanja varnostnih kopij podatkov

Izdelava polne varnostne kopije je lahko časovno potratna in skoraj gotovo vpliva na performance podatkovne baze. Zato se v večini primerov proces izdelave polne varnostne kopije izvaja v času, ko je uporaba podatkovnih baz nizka. To je običajno ponoči oz. ob takšnih urah, ko zahteve po podatkih iz podatkovnih baz s strani uporabnikov ni ali pa so te minimalne. V namen pohitritve procesa izdelave varnostne kopije se zato običajno izdeluje varnostne kopije tako, da izdelamo polno varnostno kopijo enkrat tedensko, diferencialno kopiranje pa izvajamo v preostalih šestih dneh v tednu. Po potrebi lahko v obstoječi urnik izdelave varnostnih kopij vključimo tudi varnostne kopije s transakcijskimi dnevniki, saj le te ne vplivajo na dostopni čas podatkovnih baz in posledično nimajo bistvenih performančnih vplivov za uporabnike podatkovne baze.

Primer strategije izdelave varnostne kopije podatkov:

Način izdelave varnostne kopije	Urnik
Polna kopija	Tedensko, nedelja ob 1:00
Diferencialna kopija	Dnevno, ob 1:00
Kopija transakcijskih dnevnikov	Vsakah 10 minut

**Tabela 6: Načini izdelave varnostne kopije**

Pomembno je, da se proces izdelave varnostne kopije podatkov izvaja v urah, ko na strežnikih ni ostalih performančno zahtevnih aktivnosti, kot je na primer indeksiranje.

Glede na zgornji primer, bi v primeru okvare lahko administrator podatkovne baze obnovil podatke, ki so nastali v času med zadnjo varnostno kopijo transakcijskih dnevnikov in časom okvare, s pomočjo tekočega transakcijskega dnevnika (live transaction log). Kopije transakcijskih dnevnikov bi bilo potrebno hraniti do štiriindvajset ur (do naslednje izdelave polne ali diferencialne varnostne kopije). Najnovejšo diferencialno varnostno kopijo pa bi morali hraniti do 7 dni (do naslednje polne varnostne kopije). Različni primeri seveda zahtevajo različne urnike in strategije. V primeru, da je velikost diferencialne kopije podatkov približno enaka velikosti polne kopije podatkov bi bilo smotno izvajati polno kopiranje pogosteje.

Za izdelavo varnostnih kopij lahko uporabimo SQL Server Management Studio.

### 5.3.5 Obnovitev podatkov v SQL strežniku

V primeru okvare je potrebno obnoviti podatke v naslednjem vrstnem redu:

- Če je le mogoče je potrebno izdelati varnostno kopijo tekočega transakcijskega dnevnika.
- Obnoviti zadnje polne varnostne kopije.
- Obnoviti zadnje diferencialne varnostne kopije.
- Obnoviti vse transakcijske dnevnike od zadnje polne kopije ali od zadnje diferencialne kopije.

V nekaterih primerih je mogoče obnoviti obstoječo podatkovno bazo. V primeru odpovedi diska pa je potrebno ustvariti novo podatkovno bazo iz obstoječih varnostnih kopij.

WSS 3.0 in MOSS 2007 se s podatkovno bazo povežeta samodejno, ko je ta zopet priključena (online).

### 5.3.6 Posnetki strežnika SQL

SQL Server 2005 omogoča izdelavo posnetka podatkovne baze (SQL Server snapshot). Posnetek je varnostna kopija podatkovne baze z dostopom za branje, izdelana v točno določenem času. S preusmeritvijo spletne aplikacije na takšno kopijo podatkovne baze, lahko uporabniki dostopajo do podatkovne baze ne da bi jo bilo potrebno obnoviti. Tehnologija posnetka se zanaša na dostop do primarne podatkovne baze. Posnetki torej ne morejo nadomestiti polne varnostne kopije podatkov, lahko pa nudijo uporabnikom visoko dostopnost in označevanje verzij vsebine podatkovnih baz.

#### 5.3.6.1 Proces izdelave posnetka

Ko ustvarimo posnetek podatkovne baze SQL, rezerviramo prostor za shranjevanje obstoječih podatkov. Datoteka, ki hrani posnetek bo na videz zasedla enako število bajtov kot originalna datoteka v kateri je shranjena baza podatkov, vendar pa takšna datoteka na datotečnem sistemu ne zavzema skoraj nič prostora. Shranjevanje podatkov se zgodi le takrat, ko se obstoječi podatki spremenijo. Preden se podatki spremenijo strežnik SQL samodejno prebere obstoječe podatke in jih shrani v za njih rezerviran prostor v posnetku.

Večja prednost posnetkov podatkovne baze je v hitrosti, učinkovitosti in zmanjšanju potrebne količine prostega diskovnega prostora. Ob uporabi posnetkov je potrebno upoštevati sledeče:

- Izdelava posnetkov podatkovne baze je prostorsko učinkovita.
- Izdelava prevelikega števila posnetkov podatkovne baze ni prostorsko ali performančno učinkovita.
- Uporaba posnetkov podatkovne baze je povezana z dodatnimi vhodno izhodnimi operacijami, ko se podatki prenašajo v posnetek.
- Obnova podatkov iz posnetka je lahko hitrejša od obnove podatkov polne varnostne kopije, vendar pa moramo upoštevati, da so posnetki namenjeni hitremu reševanju vsebine in niso nadomestilo za običajno varnostno shranjevanje podatkov.

Posnetek podatkovne baze je možno izdelati z orodjem SQL Server Management Studio in sicer s preprostim stavkom SQL:

```
CREATE DATABASE WSS_ContentSnapshot
ON
(
    NAME = 'WSS_Content',
    FILENAME = 'C:\SnapShots\WSS_ContentSnapshot.mdf'
)
AS SNAPSHOT OF WSS_Content
```

Seveda pa je možno izdelati posnetke tudi z namenskimi orodji kot so razni programi za izdelavo varnostnih kopij s podporo izdelave posnetkov.

### 5.3.7 Pošiljanje dnevnikov SQL

Pošiljanje dnevnikov (log shipping) v strežniku SQL je učinkovita metoda redundance, ki omogoča visoko stopnjo dosegljivosti za produkte in tehnologije SharePoint. Z uporabo pošiljanja dnevnikov se za primarno podatkovno bazo ustvari sekundarna podatkovna baza, ki v primeru okvare, lahko nadomesti primarno podatkovno bazo. Pošiljanje dnevnikov se nanaša na proces pošiljanja transakcijskih dnevnikov sekundarni podatkovni bazi, kjer se po vrstnem redu aplicirajo na podatkovno bazo in s tem vzdržujejo enosmerno sinhronizacijo s primarno podatkovno bazo. Pošiljanje dnevnikov je ročna tehnika preprečevanja izgube podatkov, ki zahteva delo s strani administratorja podatkovne baze, da ročno aktivira novo podatkovno bazo. Ko se sekundarna podatkovna baza aktivira jo je potrebno povezati s spletnimi aplikacijami v okolju SharePoint.

#### 5.3.7.1 Proces "Failover"

Proces "Failover" poteka ročno. Ko strežnika SQL konfiguriramo za pošiljanje dnevnikov je potrebno ročno obnoviti podatkovno bazo na sekundarnem strežniku. Primarni strežnik izdeluje varnostne kopije transakcijskih dnevnikov za podatkovno bazo. Ti dnevniki se nato pošljejo na lokacijo, ki je v skupni rabi obeh strežnikov SQL, od tam pa se aplicirajo na sekundarni strežnik. V primeru odpovedi primarne podatkovne baze je potreben ročni poseg:

1. Ugotoviti je potrebno ali je mogoče izdelati zadnjo varnostno kopijo transakcijskih dnevnikov. V primeru, da je to nemogoče, lahko nadaljujemo s točko 3.
2. Izdelamo varnostno kopijo transakcijskih dnevnikov na primarnem strežniku in jih pošljemo na sekundarni strežnik.
3. Apliciramo vse transakcijske dnevnike, ki še niso bili aplicirani, na sekundarni strežnik.
4. Zagotovimo, da so računi za prijavo na sekundarnem strežniku pravilno konfigurirani.
5. Zadnja varnostna kopija, ki jo apliciramo na sekundarni strežnik mora biti obnovljena z ukazom recovery. To naredimo tako, da izvedemo sledeči stavek SQL:

```
RESTORE LOG <Database Name>
FROM DISK = <Location of the Backup File>
WITH RECOVERY
```

Ko je proces obnove končan in je podatkovna baza na voljo, moramo podatkovno bazo povezati s SharePoint okoljem, saj bo v nasprotnem primeru za uporabnike nedosegljiva.

Pošiljanje dnevnikov je mogoče konfigurirati s pomočjo Microsoft SQL Server Management Studia in je relativno enostaven proces.

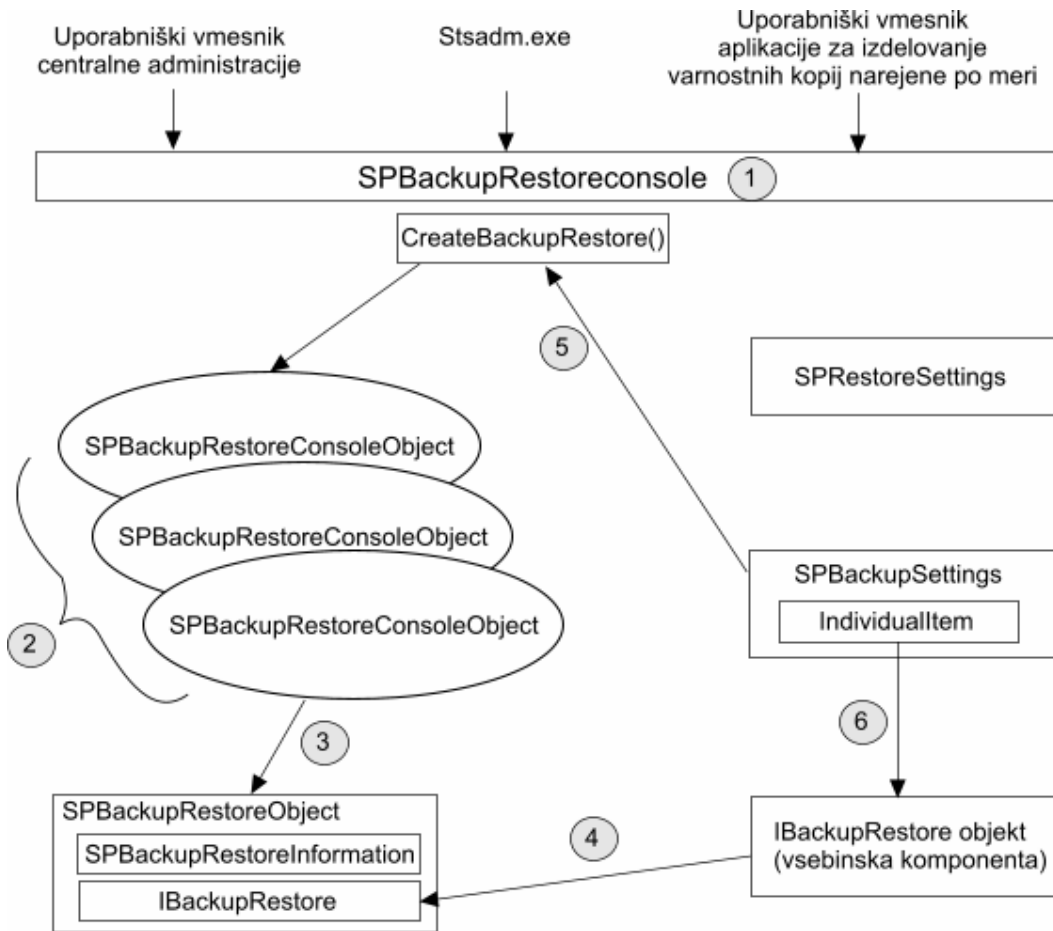
## **5.4 MOSS API za izdelavo varnostnih kopij podatkov**

Kot smo že omenili v poglavju 0, vsebuje okolje MOSS 2007 priložena orodja (native tools) za izdelavo varnostnih kopij podatkov. Orodje v centralni administraciji temelji na objektnem modelu za izdelavo varnostnih kopij podatkov, ki je dosegljiv preko vmesnika API. Vmesnik omogoča integracijo zmožnosti, ki jih omenjeni model ponuja, v aplikacije narejene po meri uporabnika. S pomočjo omenjenega modela pa je mogoče tudi razširiti funkcionalnost priloženega orodja stsadm.

### **5.4.1 Objektni model za izdelavo varnostnih kopij in obnovo podatkov**

Temelj objektnega modela, kot ga prikazuje slika 8, je SPBackupRestoreConsole razred, ki omogoča upravljanje sej za izdelavo varnostnih kopij in obnovo podatkov, poganjanje sej in shranjevanje zgodovine o sejah v obliki xml datotek. Objekt tega razreda je z arhitekturnega vidika tik pod površjem uporabniškega vmesnika aplikacije za izdelavo varnostnih kopij podatkov. Večina njegovih članskih funkcij (member functions) je statičnih, lastnosti pa v večji meri omogočajo le povezave z uporabniškim vmesnikom. Tako centralna administracija kot stsadm.exe uporabljata te povezave [9].

V SharePoint okolju je vedno samo en primerek (instance) objekta takšnega razreda. Ustvarjen je prvič, ko se izvrši klic ene izmed njegovih članskih funkcij. Objekt ostane v spominu dokler se spletni strežnik IIS ne resetira. Kljub temu, da se to ne dogaja pogosto, pa je zaskrbljenost odveč, saj je vpliv omenjenega objekta na delovanja spletnega strežnika oz. na celoten sistem minimalen.



Slika 8: Primarni objekti v hierarhiji izdelovanja varnostne kopije in obnove podatkov

Vsaka operacija izdelave kopiranja varnostne kopije ali obnove podatkov je predstavljena z objektom razreda SPBackupRestoreConsoleObject, katerega primerek izdelava metoda CreateBackupRestore, ki je del objekta SPBackupRestoreConsole. Lastnosti teh majhnih in nepotravnih objektov vsebujejo informacije o operaciji (izdelava varnostne kopije ali obnova), lokaciji datotek na datotečnem sistemu, ki jih ustvari operacija izdelovanja varnostne kopije podatkov, tip izdelave varnostne kopije ali tip obnovitve podatkov, stopnjo v kateri se v določenem trenutku operacija nahaja in drevo komponent, ki se shranjujejo ali obnavljajo. Ti objekti imajo tudi identifikacijo (Id), ki je tipa Guid in služi kot referenca objekta, ki jo lahko pošljemo metodam objekta SPBackupRestoreConsole. Metoda Run na primer, prejme identifikacijsko številko operacije (to je SPBackupRestoreConsoleObject objekt), katero naj konzola kot naslednjo požene. Vsak objekt razreda SPBackupRestoreConsoleObject ima lastnost imenovano Settings, katera vsebuje objekt. Ta objekt vsebuje vzorec nastavitvev, ki jih lahko ponovno uporabimo. Objekt identificira tudi vsebino komponente, ki jo operacija izdelave varnostne kopije shrani ali obnovi.

Tako kot SPBackupRestoreConsoleObject predstavlja operacije, tako so komponente vsebine (content components) predstavljene z objekti SPBackupRestoreObject. Ti objekti se lahko gnezdijo s pomočjo lastnosti Children. Vsak objekt predstavlja drevo ene ali več komponent vsebine. Spletna aplikacija bi lahko bila npr. predstavljena z objektom SPBackupRestoreObject, ki ima vsako od podatkovnih baz vezanih na to spletno aplikacijo predstavljeno kot objekt otroka razreda SPBackupRestoreObject. Drevo komponent, ki so

predmet določene operacije izdelave varnostne kopije ali obnove komponente, so notranje povezane z objektom `SPBackupRestoreConsoleObject`, ki predstavlja operacijo. S posredovanjem identifikacijske številke objekta `SPBackupRestoreConsoleObject` metodi `GetRoot` lahko pridobimo referenco korenске komponente objekta `SPBackupRestoreObject`.

Objekt `SPBackupRestoreObject` je vsebnik (container) dveh kritičnih tipov objektov:

- V lastnosti `Information` hrani objekt `SPBackupInformation` ali `SPRestoreInformation`. Ti tipi objektov hranijo informacije o tem, kako se izdelava varnostna kopija podatkov za posamezne komponente in katere metode se lahko interno kličejo s strani objektov `SPBackupRestoreConsoleObject` in `SPBackupRestoreObject`. Omenjena razreda vsebujeta metode in lastnosti, za katere se implementacija ne bo spremenila ne glede na to nad kakšnim tipom vsebinske komponente operiramo. Torej sta zapečateni (sealed) in izpeljevanje novih razredov iz njihovih staršev `SPBackupRestoreInformation` ni dovoljeno.
- Objekt `SPBackupRestoreObject` hrani v svoji lastnosti `IbackupRestore` drugi objekt, ki implementira `IBackupRestore` vmesnik (lahko deduje tudi iz `SPPersistedObject`). Implementacija slednjega vmesnika spremeni objekt v nekaj, za kar je mogoče izdelati varnostno kopijo ali obnoviti. Tako kot objekt `SPBackupRestoreInformation` tudi objekt `IbackupRestore` vsebuje člane, ki posredujejo informacije in metode potrebne za izdelavo varnostnih kopij in obnovo podatkov. Članske funkcije `IBackupRestore` pa morajo imeti različne implementacije glede na vsebinsko komponento, ki jo predstavljajo. Najpomembnejše pa je, da implementacija vsebuje upravljalce dogodkov (event handlers) za dogodke operacij kot sta dogodka `OnBackup` in `OnRestore`.

`SPBackupRestoreObject` je tudi razred s pomočjo katerega je poenostavljena interakcija med objekti operacije (`SPBackupRestoreConsoleObject`) in objekti komponente informacije (`SPBackupRestoreInformation` in `IBackupRestore`)

Večja razreda sta še `SPBackupSettings` in `SPRestoreSettings`. Objekt kateregakoli od omenjenih razredov je posredovan `CreateBackupRestore` metodi v trenutku, ko se ustvari operacija. Vsak od teh objektov hrani nastavitve, ki se uporabijo med operacijami. Z lastnostjo `IndividualItem` pa identificirajo komponento, ki je predmet operacije izdelave varnostne kopije podatkov ali obnove podatkov.

#### 5.4.1.1 Uporabniške pravice

Programska koda, ki ustvarja varnostno kopijo mora imeti uporabniške pravice administratorja SharePoint farme. Programska koda, ki obnavlja podatke, pa mora imeti uporabniške pravice uporabnika, ki je administrator SharePoint farme in hkrati administrator na vseh spletnih serverjih v farmi (front-end servers). Uporabnik mora imeti tudi pravice za branje in pisanje na lokaciji, kjer programska koda shranjuje (in bere) podatke.

#### 5.4.1.2 Shranjevanje informacij o napakah

V primeru, da se operacija shranjevanja varnostne kopije podatkov ali operacija obnove podatkov konča z napako se informacije o napaki zapišejo v `spbackup.log` ali `sprestore.log` na mesto, ki je bilo določeno kot ciljno mesto za shranjevanje varnostnih kopij podatkov oz. mesto, od koder je uporabnik poskusil obnoviti podatke.

## 5.5 Migriranje podatkov na drugo SharePoint farmo

WSS 3.0 in MOSS 2007 omogočata prenos podatkov iz ene strežniške farme na drugo na prijaznejši način, kot je to bilo doslej (v prejšnjih verzijah) možno s pomočjo orodja za migracijo (smigrate).

### 5.5.1 Katere podatke lahko migriramo?

S pomočjo orodja stsadm je možno migrirati podatke iz ene strežniške farme na drugo, vendar z eno omejitvijo. Orodje stsadm omogoča migracijo le na nivoju mest strani, medtem ko je s pomočjo objektnega modela možno migrirati predmete od nivoja SPWeb do nivoja SPListItem.

Za izvoz strani iz okolja SharePoint uporabimo ukaz stsadm:

```
Stsadm -o export -url <URL> -filename <FileName>.cmp
```

Za uvoz strani v okolje SharePoint uporabimo ukaz stsadm:

```
Stsadm -o import -url <URL> -filename <FileName>.cmp
```

### 5.5.2 Vmesnik API za izvoz podatkov

Migriranje podatkov je mogoče tudi z vmesnikom API. Objektni model Microsoft.SharePoint.Deployment v WSS 3.0 nudi množico orodij za migriranje vsebine med WSS stranmi. WSS 3.0 ustvari migracijski paket z vsebino, ki lahko vsebuje eno ali več datotek XML in hkrati nudi vmesnik za izvoz in uvoz migracijskih paketov. Pomembno je, da ta model omogoča tudi izvoz in uvoz obstoječih odvisnosti kot so varnostne zmožnosti, vloge uporabnikov, označevanje verzij podatkov, delovne tokove in ostale metapodatke. Poleg tega je Microsoft.SharePoint.Deployment načrtovan tako, da omogoča delovanje od nivoja spletne strani do posameznega predmeta v seznamu ali knjižnici. Omogoča tudi določitev nivoja metapodatkov, ki naj se vključijo v migrirano vsebino ter polno migracijo ali le inkrementalno.

Objektni model Microsoft.SharePoint.Deployment uporablja dva ključna objekta: Microsoft.SharePoint.Deployment.Import in Microsoft.SharePoint.Deployment.SPExport. Lastnosti operacije za izvoz in uvoz podatkov določimo z objektom Microsoft.SharePoint.Deployment.SPImportSettings oz. z Microsoft.SharePoint.Deployment.SPExportSettings. Operacijo uvoza ali izvoza pa sprožimo s klicem metode Run, ki je del SPImport ali SPExport objekta.

## 5.6 VSS (Volume Shadow Copy)

Vsaka operacija izdelovanja varnostne kopije podatkov, ki poskuša kopirati polno in stabilno sliko sistema mora upoštevati naslednje dejavnike[10]:

- Nedostopnost datotek med operacijo izdelovanja varnostne kopije podatkov. Aplikacije, ki tečejo na sistemu velikokrat potrebujejo, da so datoteke s katerimi

operirajo, odprte v ekskluzivnem načinu, kar programom za izdelovanje varnostnih kopij onemogoča delovanje oz. shranjevanje takšnih datotek.

- Nekonsistentno stanje datotek. Tudi če aplikacije nimajo odprtih datotek v ekskluzivnem načinu, je možno, zaradi končnega časa, ki je potreben za odpiranje, shranjevanje in zapiranje datoteke, da se datoteke, ki se shranijo kot varnostne kopije razlikujejo od originala in torej odražajo drugačno stanje.
- Potreba po minimiziranju prekinitev med servisi. Za zagotovitev dostopnosti in integritete datotek, za katere želimo ustvariti varnostno kopijo so možne zahteve po prekinitvi ali začasni ustavitvi programov, ki tečejo na sistemu. Takšno početje bi zahtevalo zelo veliko časa, kar je nedopustno. Nedavno, so nekateri ponudniki opreme za shranjevanje podatkov poskusili rešiti to težavo z mehanizmom, ki prepreči spremembe na nosilcu podatkov (volume) s pomočjo copy-on-write ali split mirror mehanizma, vendar pa imajo tudi te rešitve svoje težave:
  - Nekompatibilne implementacije zajema podatkov iz nosilca podatkov glede na proizvajalca. Ker imajo različni proizvajalci različne implementacije morajo prodajalci podpirati različne rešitve, kar je nezaželeno.
  - Pomanjkanje koordinacije aplikacije.
  - Omejena podpora za naprave, ki ne podpirajo RAID-a.
  - Potreba po rokovanju s spremenjenimi podatki med zajemom podatkov iz podatkovnega nosilca. Kljub temu, da ponudniki, strojne opreme ponujajo mehanizme za zamrznitev (freeze) podatkov na disku ne znajo vedno komunicirati z aplikacijami, ki tečejo na sistemu. To predstavlja možnost izgube podatkov.
  - Konsistenten zajem podatkov iz večjega števila nosilcev podatkov. Naprava za shranjevanje podatkov izvede zajem podatkov iz nosilcev podatkov, običajno pa nima mehanizma za časovno koordinacijo zamrznitve podatkov. To je še posebej pogosto, ko naprave prihajajo od različnih ponudnikov in predstavlja tveganje za nekonsistentnost podatkov.

### 5.6.1 Model VSS

VSS je načrtovan kot odgovor na težave omenjene v poglavju 5.6 in vsebuje sledeče rešitve:

- VSS model sestavlja mehanizem shadow copy, ki omogoča zajem stanja nosilca podatkov v trenutku. Ta kopija nosilca podatkov obstaja vzporedno s tekočim nosilcem podatkov (live volume) in vsebuje kopije vseh datotek na disku, ki so shranjene in so na voljo kot da so na ločeni napravi.
- Konsistentno stanje datotek preko koordinacije s strani aplikacij. VSS omogoča na modelu COM temelječ, dogodkovno krmiljen medprocesni komunikacijski mehanizem, katerega lahko uporabljajo sodelujoči procesi z namenom, določitev stanja sistema pri operacijah za izdelavo varnostnih kopij podatkov, obnove podatkov in shadow-copy operacije. Ti dogodki definirajo korake po katerih vse aplikacije, ki spreminjajo stanje na disku (zapisovalniki oz. writers) postavijo vse svoje datoteke v konsistentno stanje, pred začetkom kreiranja shadow kopije.
- Minimiziranje nedostopnosti aplikacij (application downtime). Shadow kopija VSS obstaja paralelno s tekočo kopijo nosilca podatkov za katerega želimo izdelati varnostno kopijo, kar omogoča, da aplikacije nemoteno delujejo in so za uporabnika dosegljive, razen za nekaj trenutkov, ki so potrebni, da se shadow kopija pripravi. Čas, ki je potreben za ustvarjanje shadow kopije znaša približno eno minuto in je postavljen med dogodka zamrznitve in odmrznitve (thaw).

Čeprav čas potreben za pripravo shadow kopije ni neopazen je v primerjavi s časom potrebnim za ustvarjanje varnostne kopije celotnega nosilca podatkov, ki lahko traja nekaj ur, relativno majhen.

- Poenoten vmesnik do VSS funkcionalnosti – VSS abstrahira mehanizme shadow kopije preko skupnega vmesnika in hkrati omogoča izdelovalcu strojne opreme dodajanje in upravljanje zmožnosti. Katerikoli aplikacija za izdelavo varnostnih kopij podatkov (zahtevnik oz. requester) in katerikoli zapisovalnik bi morala delovati na kakršnekoli diskovnem polju, ki podpira vmesnik VSS.
- Večkratna izdelava varnostne kopije nosilca podatkov -VSS podpira zbirke shadow kopij (shadow copy sets) različnih tipov nosilcev podatkov različnih proizvajalcev. Vse shadow kopije, v zbirki shadow kopij, se kreirajo z enako časovno oznako (timestamp) in predstavljajo enako stanje diska skozi vse nosilce podatkov.
- Podpora domorodni shadow kopiji (Native shadow copy support). Podpora shadow kopiji je na voljo preko VSS-ja kot del operacijskega sistema že vse od Windows XP.

### 5.6.2 Servis Volume Shadow Copy

Servis Volume Shadow Copy (VSS) nudi sistemsko infrastrukturo za poganjanje aplikacij VSS na sistemih z MS Windows.

Servis VSS skrbi za sledeče:

- Koordinira aktivnosti za dobavitelje (providers), zapisovalnike in zahtevnike v procesu kreiranja in uporabe shadow kopij.
- Zalaga privzetega sistemskega dobavitelja (default system provider).
- Implementira nizkonivojsko gonilniško funkcionalnost, ki omogoča delovanje vsakega dobavitelja

Servis VSS poženemo na zahtevo in zato ga moramo pognati preden aplikacije zahtevajo izdelavo varnostne kopije z VSS-jem.

### 5.6.3 Shadow kopije in zbirke shadow kopij

Shadow kopija nosilca podatkov duplicira vse podatke iz nosilca v točno določenem trenutku. VSS identificira vsako shadow kopijo s pomočjo GUID-a.

Zbirka shadow kopij predstavlja kopije različnih nosilcev podatkov, ki so bili ustvarjeni v istem trenutku.

Način implementacije shadow kopij je prepuščena izdelovalcem strojne ali programske opreme. V trenutku, ko je shadow kopija ustvarjena, sta na sistemu dva posnetka podatkov. Do originala lahko dostopamo na konvencionalen način, medtem ko za dostop do kopije podatkov uporabimo vmesnik VSS API.

Takšen pristop omogoča, da se na sistemu v istem trenutku izvaja več aktivnosti:

- Navadne aplikacije lahko na sistemu nadaljujejo z uporabo originalnega nosilca podatkov (lahko spreminjajo podatke).
- Aplikacije, ki uporabljajo zahtevnik VSS API za dostop do shadow kopije pa lahko izdelujejo varnostno kopijo podatkov.

Shadow kopije ne potrebujejo enake implementacije za vsako datoteko, imenik ali zbirko podatkov. Različne implementacije shadow copy mehanizma (ponudniki) lahko uporabijo

različne pristope za kreiranje shadow kopije, vendar pa morajo shadow kopije izgledati enako vsem aplikacijam, ki uporabljajo vmesnik VSS API.

#### 5.6.4 Privzeto stanje shadow kopije

Kljub temu, da datotečni sistem izprazni vse vhodno/izhodne predpomnilnike preden se ustvari shadow kopija, to še vedno ne zagotavlja pravilnega rokovanja z nekompletnimi vhodno/izhodnimi podatki.

V primeru, da ne bi imeli aplikacij, ki uporabljajo VSS, bi dejali, da so podatki v shadow kopiji v crash-consistent stanju. Shadow kopija v crash-consistent stanju vsebuje sliko diska, ki je enaka tisti, ki bi obstajala ob nasilni zaustavitvi sistema. Vse datoteke, ki so bile ob času zaustavitve sistema na disku in so bile odprte za pisanje, bi po zaustavitvi sistema še vedno obstajale vendar pa bi bila njihova konsistentnost in completeness vprašljiva.

Crash-consistent stanje sicer ne odpravlja vseh težav potrebnih za stabilno varnostno kopijo podatkov vendar pa je vseeno boljši od načina, ki ga uporabljajo konvencionalne aplikacije za izdelovanje varnostnih kopij podatkov:

- Nosilec podatkov, ki je vsebovan v shadow kopiji (čeprav je mogoče v crash-consistent stanju), še vedno vsebuje vse datoteke. Varnostna kopija ustvarjena s konvencionalnimi orodji za ustvarjanje varnostnih kopij podatkov ne bi vsebovala datotek, ki bi bile v času izdelave varnostne kopije podatkov odprte.
- Shadow kopija nosilca podatkov je izdelana v trenutku, brez prehoda skozi drevesno strukturo datotečnega sistema, ki običajno traja veliko več časa.

Aplikacije, ki ni ne znajo sodelovati z VSS-jem (urejevalniki besedil, itn.) in bi imele v času izdelave varnostne kopije podatkov odprte datoteke, bi povzročile, da bi te datoteke bile v crash-consistent stanju. Aplikacije s podporo VSS (zapisovalniki) pa lahko koordinirajo svoje akcije tako, da ostanejo datoteke konsistentne tudi po opravljenem procesu izdelovanja varnostne kopije.

#### 5.6.5 Zamrznitev in odmrznitev shadow kopije

VSS shadow copy operacija se zgodi med dogodkoma zamrznitve in odmrznitve, v trenutku, ko zapisovalniki postavijo datoteke v konsistentno stanje.

Zamrznitev in odmrznitev ponujata mehanizme s pomočjo katerih programerji zapisovalnikov poskrbijo za konsistentnost datotek in ponovno pisanje.

#### 5.6.6 Dobavitelji

Dobavitelji upravljajo s tekočimi nosilci podatkov in ustvarjajo shadow kopije teh nosilcev podatkov na zahtevo.

V odgovor na zahtevo zahtevnika, dobavitelj generira dogodke COM, ki aplikacijam signalizirajo, da se pripravlja shadow kopija. Nato dobavitelj kreira in vzdržuje kopijo dokler je potrebna. Dokler shadow kopija obstaja, dobavitelj ustvari okolje kjer so dve neodvisni kopiji vsakega nosilca podatkov za katerega je bila narejena shadow kopija:

- Ena je povezana z diskom v uporabi na katerem se stanje nenehno spreminja
- Druga je fiksna in pripravljena na izdelavo varnostne kopije

Medtem ko je privzeti dobavitelj na voljo z operacijskim sistemom Windows lahko ostali prodajalci ponudijo svoje implementacije, ki so optimizirane za strojno in programsko opremo, ki jo ponujajo. Iz vidika končnega uporabnika ali programerja aplikacije za izdelavo varnostne kopije imajo vsi dobavitelji enak vmesnik zato morajo izpolnjevati naslednje zahteve:

- Prestrezati morajo vhodno-izhodne zahteve med datotečnim sistemom in sistemom za shranjevanje podatkov, ki leži pod njim (gledano iz perspektive logike teh dveh komponent).
- Zajeti in izluščiti morajo stanje nosilca podatkov v času shadow kopije in vzdrževati morajo takšen pogled na podatke na disku, kot je bil v času nastanka shadow kopije – brez sprememb na datotečnem sistemu.
- Shadow kopija, ustvarjena v določenem trenutku, mora biti na voljo aplikacijam, ki znajo sodelovati z VSS-jem, preko navideznega nosilca podatkov.

Omenjene zahteve so lahko implementirane na sledeče načine:

- s sistemskimi dobavitelji,
- s programskimi dobavitelji,
- s strojnimi dobavitelji

### 5.6.7 Sistemski dobavitelj

Sistemski dobavitelj je na voljo kot del operacijskega sistema Windows in je primerek programskega dobavitelja, vendar pa se slednje lahko v prihodnosti spremeni. Za ohranjanje pogleda na nosilca podatkov v shadow kopiji sistem uporablja dobavitelja z copy-on-write tehniko. Kopije sektorjev na disku, ki so bile spremenjene od začetka izdelave shadow kopije so shranjene na področju rezerviranem za shadow kopijo. Tako lahko sistem izpostavi tekoči nosilec podatkov na katerega lahko pišemo in iz katerega lahko beremo. Zahteva za sistemskega dobavitelja je, da se področje za shadow kopijo nahaja na nosilcu podatkov NTFS. Pogoji, ki ga moramo izpolnjevati je, da je vsaj en nosilec podatkov, ki je vpet v sistem, tipa NTFS. Nosilec podatkov za katerega želimo izdelati shadow kopijo pa je lahko tudi različen od NTFS.

### 5.6.8 Programski dobavitelji

Programski dobavitelji prestrezajo in procesirajo vhodno-izhodne zahtevke na programskem nivoju med datotečnim sistemom in programsko opremo za upravljanje nosilcev podatkov. Ti dobavitelji so implementirani kot uporabniške knjižnice DLL in vsaj enim gonilnikom, ki deluje na nivoju jedra. Običajno je to filtrirni gonilnik datotečnega sistema, ni pa to nujno. Delo za kreiranje shadow kopij opravi programska oprema.

Dobavitelj mora zagotoviti pogled na nosilca podatkov z dostopom do zbirke datotek, s katerimi lahko natančno poustvari stanje na nosilcu podatkov kakršno je bilo pred izdelavo shadow kopije. Takšen primer je copy-on-write tehnika, kot jo uporablja sistemski dobavitelj. Prodajalci različnih rešitev pa niso zavezani k uporabi točno določene tehnike saj jim VSS omogoča, da implementirajo svojo rešitev. VSS podpira večino funkcionalnosti, ki jo nudijo programski dobavitelji kot je definiranje točke v času, sinhronizacijo in splakovanje, skupni vmesnik za aplikacije za izdelavo varnostnih kopij podatkov in upravljanje shadow kopij.

Programski dobavitelj se aplicira širšemu delu platform za shranjevanje podatkov kot strojni dobavitelj in mora delovati tako z enostavnimi diski kot z logičnimi nosilci podatkov.

### 5.6.9 Strojni dobavitelji

Strojni dobavitelji prestrezajo vhodno-izhodne zahteve datotečnega sistema na strojnem nivoju tako, da sodelujejo s strojnim adapterjem ali krmilnikom. Delo za kreiranje shadow kopije opravi adpter na gostujočem računalniku (host adapter), namenski sistem za shranjevanje podatkov (storage appliance) ali krmilnik RAID, ki deluje izven operacijskega sistema. Ti dobavitelji so implementirani kot uporabniške knjižnice DLL, ki komunicirajo s strojno opremo, katera izpostavlja podatke shadow kopije. Strojni dobavitelji shadow kopij lahko tako kličejo ali ustvarjajo ostale komponente na nivoju jedra. Strojni dobavitelji izpostavljajo VSS-ju shadow kopije celotnih diskov ali logičnih enot (LUN-ov) . Zahtevniki še vedno delujejo s shadow kopijami nosilcev podatkov, vendar pa preslikave iz nosilcev podatkov na diske interno izvaja VSS. Shadow kopije, ki jih kreirajo strojni dobavitelji in imajo nosilce podatkov na dinamičnih diskih imajo posebno zahtevo oz. omejitev: Ni jih mogoče uvoziti na isti sistem. Potrebno jih je kreirati kot prenosne in jih nato uvoziti na drugem sistemu.

Strojni dobavitelj uporablja funkcionalnost VSS kot je definiranje točke v času, sinhronizacijo, skupni vmesnik za aplikacije za izdelavo varnostnih kopij podatkov in upravljanje shadow kopij. VSS pa ne določa mehanizma po katerem strojni dobavitelj izdeluje in ohranja shadow kopije.

### 5.6.10 Zahtevniki

Zahtevnik je vsaka aplikacija, ki uporablja vmesnik VSS API oz. vmesnik IVssBackupComponents za zahtevo servisov VSS pri ustvarjanju in upravljanju shadow kopij in zbirk shadow kopij enega ali več nosilcev podatkov.

Najbolj tipičen primer zahtevnika je aplikacija za izdelavo varnostnih kopij podatkov in obnovo podatkov, ki zna komunicirati z VSS-jem in upravlja podatke iz shadow kopije za svojo operacijo izdelave varnostne kopije.

Poleg tega, da zahtevniki začnejo proces izdelave varnostne kopije, komunicirajo z zapisovalniki z namenom zbiranja informacij iz sistema in za pošiljanje signalov zapisnikom, da pripravijo podatke za izdelavo varnostne kopije.

### 5.6.11 Stanje zahtevnika

Zahtevnik ohranja informacije o svojem stanju v metapodatkovnemu XML objektu imenovanem dokument varnostnih kopij komponent (backup components document). Zahtevnik metapodatkov je potreben ampak ne zadosten, da bi zahtevnik lahko ustvaril varnostno kopijo podatkov in obnovo. Razlogi za to so:

- Med operacijo izdelovanja varnostne kopije, je v operacijo vpletena samo podmnožica od vseh komponent. Komponente, ki jih ni mogoče vključiti v varnostno kopijo (brez komponent, ki so njihovi otroci in jih je mogoče vključiti v varnostno kopijo) in komponente, ki jih je mogoče vključiti v izdelavo varnostne kopije in so bile vključene eksplicitno, imajo svoje podatke shranjene v dokumentu varnostnih kopij komponent.

- Informacije vseh komponent (tudi tistih dodanih v dokument varnostnih kopij komponent) niso popolne (datoteke in poti niso vključene)
- Med operacijo obnove podatkov, je lahko komponenta, ki je implicitno vključena v izdelavo varnostne kopije, na voljo za vključitev v obnovo podatkov in je tako eksplicitno vključena v obnovo podatkov. To zahteva osvežitev zahtevnikovega dokumenta varnostnih kopij komponent z informacijami iz shranjenih kopij zapisnikovega metapodatkovnega dokumenta.

Vmesnik VSS API omogoča zahtevniku, da izvaja povpraševanja nad zapisovalniki v teku (med izdelovanjem varnostne kopije) in pridobitev metapodatkov ali pregledovanje shranjenih metapodatkov med obnovo podatkov. Zapisovalnik lahko spreminja informacije komponent v dokumentu varnostnih kopij komponent med izvajanjem procesa izdelave varnostne kopije ali obnove podatkov. Z uporabo informacij o tem katere komponente so bile vključene v izdelavo varnostne kopije in obnovo podatkov in uporabo informacij o pravilih za izbor komponent, lahko zahtevnik določi katere datoteke mora posameznik zapisovalnik shraniti ali obnoviti in kje se le te nahajajo. Metapodatki o zahtevniku in zapisovalniku se morajo shraniti v varnostno kopijo podatkov, da to kopijo sploh lahko obnovimo. Operacije za obnovo podatkov pa potrebujejo star dokument varnostnih kopij komponent in zapisnikov metapodatke dokumentov, da lahko pridobijo popolna navodila za obnovo datotek.

### 5.6.12 Medprocesna komunikacija zahtevnika

Zahtevnik obdrži kontrolo nad operacijo izdelave varnostne kopije in obnove podatkov preko VSS-ja z generiranjem COM dogodkov preko različnih klicev v vmesniku zahtevnika. Ti klici lahko naredijo sledeče:

- Ustvarijo zahteve po dobaviteljih. `IvssBackupComponents::DoSnapshotSet` signalizira dobavitelju naj ustvari shadow kopijo izbranega nosilca podatkov.
- Sproži zapisovalnike, da vrnejo informacije. `IvssBackupComponents::GatherWriterMetadata` omogoči zahtevniku, da pridobi zapisovalnikov metadata dokument (writer metadata document).
- Zahteva od zapisovalnikov, da pripravijo ali upravljajo z različnimi fazami shadow kopij operacij. `IvssBackupComponents::PrepareForBackup` signalizira zapisovalnikom naj pripravijo vhode-izhode za zamrznitev.

Zahtevnik sprejme informacije s strani zapisovalnikov preko tekočega ali shranjenega zapisovalnikovega metapodatkovnega dokumenta in preko uporabe vmesnika `IvssComponent`, katerega zapisovalnik lahko tudi obnovi.

### 5.6.13 Življenjski cikel zahtevnika med izdelavo varnostne kopije

Naslednje točke opisujejo potek življenjskega cikla zahtevnika med izdelavo varnostne kopije:

1. Ustvarjanje primerka in inicializacija vmesnika VSS API.
2. Kontaktiranje zapisovalnikov z namenom pridobitve informacij.
3. Izbira podatkov, ki naj se vključijo v varnostno kopijo.
4. Ponudnik zahteva shadow kopijo.
5. Izdelava varnostne kopije.
6. Sprostitev vmesnika in shadow kopije.

### 5.6.14 Življenjski cikel zahtevnika med obnovo podatkov iz varnostne kopije

Življenjski cikel za obnovo podatkov ne potrebuje shadow kopije vendar vseeno potrebuje sodelovanje z zapisovalnikom:

1. Ustvarjanje primerka vmesnika VSS API.
2. Inicializacija zahtevnika z nalaganjem dokumenta varnostnih kopij komponent za operacijo obnove podatkov.
3. Pridobitev shranjenih zapisovalnikovih metapodatkov in dokumentov varnostnih kopij komponent.
4. Kontaktiranje zapisovalnikov za začetek sodelovanja.
5. Preverjanje zapisovalnikov po spremembah v dokumentu varnostnih kopij komponent.
6. Obnova podatkov.

### 5.6.15 Zapisovalniki

Zapisovalniki so aplikacije ali servisi, ki shranjujejo informacije na disk in sodelujejo z dobavitelji in zahtevniki preko vmesnika VSS. Med izdelavo varnostnih kopij zapisniki zagotovijo, da njihovi podatki mirujejo in so stabilni ter primerni za shadow kopijo. Zapisovalniki sodelujejo z obnovo podatkov z odklepanjem datotek, ko je to mogoče in z javljanjem alternativnih poti, ko je to mogoče. Če zapisovalnikov med izdelovanjem VSS varnostne operacije ni, potem lahko shadow kopijo še vedno ustvarimo. V tem primeru bodo vsi podatki na nosilcu podatkov, za katerega je bila shadow kopija izdelana, v crash-consistent stanju.

### 5.6.16 Stanje zapisovalnika

Zapisovalniki hranijo svoje stanje v metadata objektu XML imenovanem zapisovalnikov dokument z metapodatki.

Ti metapodatki so edina podatkovna struktura, ki hrani zbirko datotek (poti, specifikacije o datotekah, rekurzijsko zastavico) o podatkih, ki naj bi se vključili v varnostno kopijo ali pa bi bili uporabljeni pri obnovi podatkov.

Zapisovalnikov dokument z metapodatki organizira zapisovalnikove zbirke datotek v skupine ali komponente. Relacija ene od komponent med izdelavo varnostne kopije in obnovo podatkov z drugimi komponentami, ki jih upravlja zapisovalnik je opisana v zapisovalnikovem dokumentu z metapodatki. Opis vsebuje informacije o tem ali je komponento mogoče vključiti v izdelavo varnostne kopije, v obnovo in logične poti do komponente. Dokument prav tako hrani dodatne informacije, ki so pomembne pri obnovi podatkov.

Za izvedbo varnostne kopije ali obnove podatkov, potrebuje zahtevnik metapodatke zapisovalnika skupaj s svojimi podatki, iz dokumenta za izdelavo varnostne kopije komponent. Za razliko od dokumenta za izdelavo varnostne kopije komponent je zapisovalnikov dokument za metapodatke mišljen kot struktura, namenjena samo za branje. Enkrat, ko jo zapisovalnik ustvari, se ne spreminja več.

### 5.6.17 Rokovanje zapisovalnikovih dogodkov

Zapisovalnikove operacije VSS se sprožijo preko prejetja dogodkov COM. Ko dogodkov ni, zapisovalnik ne opravlja operacij izdelovanja varnostne kopije podatkov ali obnove podatkov, temveč opravlja svoje normalno delo, kot je odgovarjanje na povpraševanje s strani podatkovne baze, upravljanje uporabniških podatkov ali pa nudi druge storitve.

### 5.6.18 Rokovanje dogodkov za identifikacijo

Z izjemo dogodka za identifikacijo (Identify events) je vrsta in zaporedje dogodkov, ki jih zapisovalnik prejme, odvisna od unikatnega tipa operacij VSS, ki so trenutno v teku.

Dogodek za identifikacijo zahteva od zapisovalnikov systemske informacije o konfiguraciji in informacije o datotekah, ki jih upravlja preko zapisovalnikovega dokumenta za metapodatke. Dogodek za identifikacijo se generira v podporo skoraj vsake operacije VSS, vključno s sistemskimi poizvedbami, shadow kopijami in operacijami za izdelavo varnostnih kopij in operacijami za obnovo podatkov. Tako mora vsaka implementacija upravljalca dogodka `CvssWriter::OnIdentify` za identifikacijo iz zapisovalnika biti sposobna upravljati identifikacijski dogodek, kadarkoli se ta sproži - tudi med procesiranjem druge operacije VSS, kot je denimo izdelava varnostne kopije ali obnova podatkov. Dogodek za identifikacijo ni del življenjskega cikla operacij VSS, kljub temu, da se lahko generira in včasih celo zahteva kot predpogoj za začetek takšne operacije.

Posebej pomembno je, da se informacije o stanju VSS operacije ne spreminjajo v `CvssWriter::OnIdentify`, saj bi prejetje dogodka o napaki ponastavilo informacijo.

### 5.6.19 Dogodki o izdelavi varnostne kopije in obnovi podatkov

Glede na to v kateri operaciji zapisovalnik sodeluje, bo poleg dogodkov o identifikaciji prejel dodatnih dva do sedem dogodkov. Rokovanje s temi dogodki s strani zapisovalnika tvori življenjski cikel izdelave varnostne kopije ali obnove podatkov iz varnostne kopije.

V tipični operaciji varnostne kopije podatkov bi zapisovalnik rokoval s sledečimi dogodki:

- priprava na izdelavo varnostne kopije (`PrepareForBackup`),
- priprava za ustvarjanje posnetka (`PrepareForSnapshot`),
- zamrznitev,
- odmrznitev,
- operacije po ustvarjanju posnetka (`PostSnapshot`),
- zaključek izdelave varnostne kopije (`BackupComplete`),
- ugasnitev izdelave varnostne kopije (`BackupShutdown`)

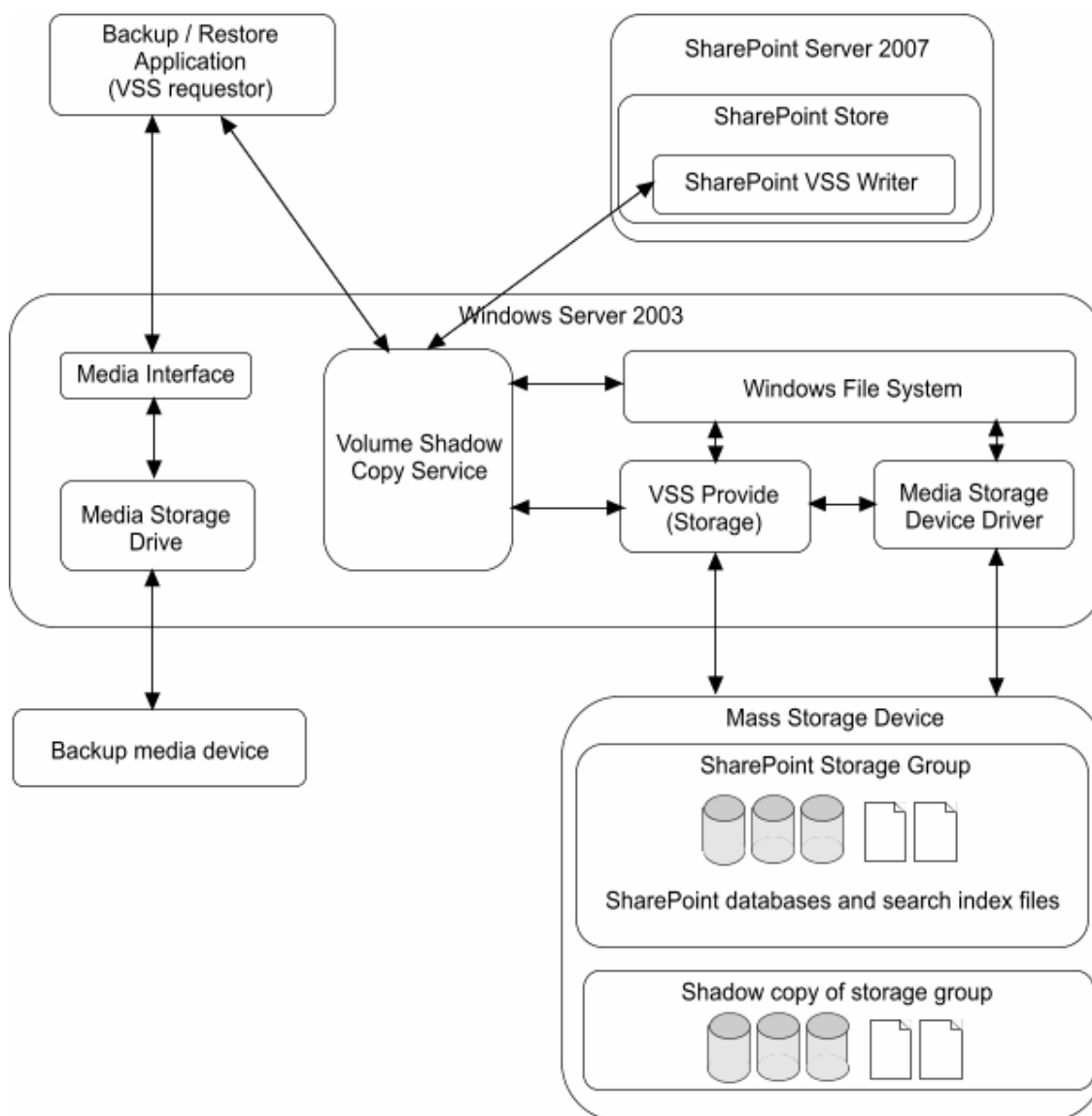
V tipični operaciji za obnovitev podatkov bi zapisovalec rokoval s sledečimi dogodki:

- operacije pred obnovo podatkov (`PreRestore`),
- operacije po obnovi podatkov (`PostRestore`)

## 5.7 MOSS VSS

VSS z vmesnikom API zelo poenostavi izdelavo varnostnih kopij podatkov Microsoftovih strežniških rešitev. MOSS 2007 vsebuje zapisovalnik VSS, ki je integriran z ogrodjem za izdelavo varnostnih kopij (VSS backup framework) in s tem omogoča aplikacijam za izdelavo varnostnih kopij nemoteno in enostavnejše delo. Na ta način je mogoče izdelati varnostno kopijo celotne farme, vključno z indeksom iskalnika.

Spodnja slika prikazuje glavne komponente sistema: Microsoft Windows Server 2003 (in Volume Shadow Copy Service), MOSS 2007 (in Microsoft Office SharePoint Server 2007 zapisovalnik za Windows Server 2003 Volume Shadow Copy Service), in po meri narejeno aplikacijo za izdelavo varnostnih kopij vključno z zahtevnikom in ponudnikom.



Slika 9: VSS MOSS 2007 arhitektura

VSS komunicira z datotečnim sistemom Windows Server 2003 in z gonilnikom naprave za shranjevanje podatkov preko ponudnika, ki je narejen po meri. Strojni ponudnik mora

ugotoviti kje se shadow kopija ustvari. VSS abstrahira strojno shadow kopijo tako, da aplikacija za izdelavo varnostne kopije podatkov lahko dostopa do shadow kopije na univerzalen način, ne da bi vedela za detajle o strojni implementaciji.

SharePoint Store je komponenta MOSS-a 2007 in dostopa do MOSS 2007 skupine podatkov preko datotečnega sistema Windows Server 2003. Na datotečnem sistemu ima vsaka skupina podatkov MOSS 2007 konfiguracijo, vsebino, ponudnika skupnih servisov (SSP) in podatkovno bazo iskalnika, v konfiguracijski podatkovni bazi registrirane podatkovne baze zunanjega izvora (3rd-party database) in indeksne datoteke iskalnika (search index files).

MOSS 2007 podpira VSS s pomočjo zapisovalnika SharePoint, ki je vgrajen v SharePoint Store. Zapisovalnik SharePoint koordinira potek izdelave varnostne kopije podatkov tako, da zamrzne in odklopi skupino podatkov preden jo kopira. Ko s procesom zaključijo odmrzne in ponovno priklopi.

Aplikacija za izdelovanje varnostne kopije med obnovo podatkov (zahtevnik) izda zahtevo zapisovalniku SharePoint za koordinacijo s SharePoint store-om. Koordinacija obsega izklop skupine podatkov, zamenjavo datotek podatkovne baze in priklop skupine podatkov.

Zahtevnik komunicira z VSS-jem, da pridobi informacije o MOSS-u 2007, izvede ukaze za izdelavo shadow kopije in dostopa do podatkov za namene izdelave varnostne kopije. Ob obnovi podatkov zahtevnik komunicira z VSS-jem tudi zato, da pripravi sistem na obnovenitveno operacijo in ponovno shrani podatke na napravi za shranjevanje podatkov (mass storage device). Aplikacija za izdelavo varnostne kopije pa je odgovorna za komunikacijo z Windows Server 2003, za branje in pisanje podatkov na medije, kjer je medij lahko arhiv na traku, podatkovno omrežje (storage area network - SAN) ali kakšen drug medij.

Informacije, ki so potrebne za uspešen zaključek izdelave varnostne kopije podatkov ali obnovo podatkov, med MOSS 2007, VSS in aplikacijo za izdelavo varnostnih kopij podatkov se prenesejo kot zapisovalnikovi metapodatki.

Visoko nivojska interakcija med omenjenimi komponentami poteka na sledeči način:

1. Aplikacija za izdelavo varnostne kopije podatkov požene planirano opravilo (scheduled job).
2. VSS zahtevnik v aplikaciji za izdelavo varnostne kopije pošlje ukaz za izdelavo shadow kopije izbrane skupine podatkov VSS-ju.
3. VSS sporoči zapisovalniku SharePoint naj se pripravi za izdelavo posnetka. MOSS 2007 preprečuje administrativne posege nad skupino podatkov, preveri odvisnosti med nosilci podatkov in preneha z operacijami zapisovanja v podatkovno bazo in transakcijske dnevnike, medtem ko še vedno omogoča dostop za branje.
4. VSS komunicira s primernim podatkovnim ponudnikom (storage provider) z namenom, da se ustvari shadow kopija nosilca podatkov, ki vsebuje skupine podatkov MOSS-a 2007.
5. VSS MOSS-u 2007 sporoči, da lahko nadaljuje z običajnim delom.
6. VSS zahtevnik preveri integriteto varnostne kopije preden sporoči, da je operacija uspela, MOSS 2007 pa si zabeleži čas zadnje izdelave varnostne kopije.

### 5.7.1 Zapisovalnik

VSS predstavlja infrastrukturo z vgrajeno funkcionalnostjo za shadow kopijo. VSS v okolju SharePoint ima sledeče zmožnosti:

- **En sam VSS referenčni zapisovalnik (VSS reference writer).** Pred tem so aplikacije za izdelavo varnostnih kopij uporabljale celo vrsto vmesnikov API za katere je bilo potrebno napisati veliko dodatne kode.
- **Polna varnostna kopija in obnova v primeru katastrofe.** Zapisovalnik omogoča aplikaciji za izdelavo varnostne kopije (zahtevniku) enostaven dostop do vmesnika VSS API z namenom ustvarjanja varnostne kopije ali obnove podatkov za celotno SharePoint farmo.
- **Granularnost podatkovne baze.** Zapisovalnik omogoča zahtevniku izbor vseh podatkovnih baz, segment podatkovnih baz (večkratni izbor - multiple select) ali eno podatkovno bazo (enojni izbor - single select) tako za izdelavo varnostne kopije kot za njeno obnovo. Vse podatkovne baze razen konfiguracijske podatkovne baze in vsebinske podatkovne baze za centralno administracijo je preko zapisovalnika mogoče izbrati za izdelavo varnostne kopije. Varnostna kopija slednjih dveh podatkovnih baz je možna z izdelavo varnostne kopije celotne farme.
- **SharePoint-ov seznam zalog (SharePoint inventory list).** Pred izdelavo varnostne kopije SharePoint zapisovalnik generira seznam podatkovnih baz izbranih za izdelavo varnostne kopije. Seznam se vrne zahtevniku, tako da se operacija izdelave varnostne kopije lahko prične na mestu, kjer se podatkovna baza fizično nahaja.
- **Podpora konfiguraciji spletne farme.** Zapisovalnik razume in omogoča podporo sinhronizaciji izdelave varnostne kopije in obnove podatkov na spletni farmi. Zapisovalnik posreduje zahtevniku seznam strežnikov, podatkovnih baz in datotek povezanih s farmo. Zahtevnikova naloga je, da vzpostavi ločene povezave do vsakega strežnika, kjer nato pokliče VSS zapisovalnik za kreiranje varnostne kopije ali obnovo podatkov.
- **Izdelovanje varnostne kopije podatkov brez prekinitev (Backup content without interruption).** Aplikacija lahko spreminja datoteko medtem, ko se nad njo izvaja operacija kreiranja varnostne kopije, kar lahko privede do napak ali nekonsistentnosti. VSS omogoča izdelavo hitrega posnetka, medtem ko aplikaciji dovoli neprekinjeno izvajanje operacij nad datoteko.
- **Podpora izdelave varnostne kopije za zunanje podatkovne baze (Custom Third-Party Databases).** Zapisovalnik omogoča izdelavo varnostnih kopij za podatkovne baze, ki so vključene v okolje SharePoint s strani zunanjih rešitev pod pogojem, da so le te registrirane v konfiguracijski podatkovni bazi.
- **Izdelava varnostne kopije indeksnih datotek iskalnika.** Indeksne datoteke iskalnika se shranjujejo na datotečnem sistemu in zato za izdelavo varnostne kopije teh datotek potreben dodaten zapisovalnik, ki je del MOSS-a 2007.
- **Polna povrnitev SharePoint aplikacije.** Zapisovalnik lahko rokuje z vsemi komponentami v aplikaciji SharePoint, vključno s podatkovnimi bazami. Sodeluje pa tudi z zapisovalnikom za ustvarjanje varnostnih kopij indeksnih datotek iskalnika. V času obnove podatkov, lahko zapisovalnik povrne celotno aplikacijo SharePoint z obnovo podatkov iz prejšnje varnostne kopije farme.
- **Sinhronizacija podatkovnih baz po opravljeni obnovi podatkov.** Da bi zagotovili sinhronizacijo vseh podatkovnih baz (Post-restore synchronization of databases), ko se obnova podatkov zaključi, je vsaka od podatkovnih baz samodejno ločena (detached)

in ponovno priključena (attached) k farmi. Administratorju tako ni potrebno opraviti nikakršnega dela za sinhronizacijo podatkovnih baz.

### 5.7.2 Zahtevnik

VSS koordinira komunikacijo med zahtevniki (aplikacije za izdelavo varnostnih kopij podatkov), zapisovalniki (Windows aplikacije kot so MOSS 2007 ali SQL Server 2005) in ponudniki (sistemski, ponudniki programske opreme ali komponent strojne opreme, ki kreirajo shadow kopije).

Da bi aplikacije, ki temeljijo na VSS, bile združljive oz. da bi izpolnjevale zahteve za ustvarjanje varnostnih kopij v okolju MOSS 2007, morajo izpolnjevati sledeče zahteve:

- Varnostne kopije SharePoint-ovih podatkovnih baz in indeksnih datotek morajo biti ustvarjene izključno z zapisovalnikom SharePoint.
- Aplikacija za izdelavo varnostne kopije mora preveriti integriteto shadow kopije.
- Obnova podatkov na originalno lokacijo mora biti izvedena izključno z zapisovalnikom SharePoint.

### 5.7.3 Kako napisati in uporabiti zahtevnik

Postopek za izdelavo zahtevnika je povsem enak postopku izgradnje zahtevnika za druge aplikacije sistema Windows, kot je strežnik MS SQL ali strežnik MS Exchange.

Navodila za uporabo zahtevnika pa so sledeča:

1. Ko se MOSS 2007 namesti moramo ročno pognati servis Windows SharePoint Services VSS Writer (zapisovalnik).
2. Zapisovalnik registriramo v registru operacijskega sistema Windows s pomočjo ukaza `stsadm -o registerwsswriter`, ki ga poženemo v ukazni vrstici konzole.
3. Uporabimo aplikacijo z implementiranim zahtevnikom za izdelavo varnostnih kopij podatkov.

### 5.7.4 Varnostne pravice za poganjanje VSS-ja

Varnostne pravice za račune pod katerimi tečejo zapisovalniki morajo izpolnjevati sledeče zahteve:

- Račun mora imeti pravico za klic VSS-ja. Ob privzetih možnostih mora biti zapisovalnik član skupine Administratorjev ali skupine Backup Operators. Možno pa je nastaviti določene ključe v registru s katerimi omogočimo dostop do VSS-ja tudi z drugimi računi.
- Račun mora imeti pravico za klic »backup database« in »restore database« ukazov v strežniku s podatkovno bazo.
- Račun mora imeti pravico odpreti VDI, kateri zahteva, da je klient član skupine sysadmin na strežniku SQL.
- Račun mora biti sposoben poganjati poizvedbe SQL v katalogu `sys.master_files` in »master« podatkovni bazi v strežniku SQL.

## **5.8 Obnova podatkov po katastrofi**

Po katastrofi je običajno cilj, da pridobimo čim več podatkov in nastavitev in jih obnovimo čim hitreje. Izdelavo varnostne kopije in obnovo pa lahko opravljamo tudi z namenom skalabilnosti obstoječe farme ali pa za selitev podatkov na novo farmo. Pogledali si bomo katere komponente je potrebno za takšna primera shranjevati in s katerimi orodji lahko to počnemo.

### **5.8.1 Komponente MOSS-a**

Strežnik MOSS vključuje sledeče komponente:

- Vsebino.
- Dodatke po meri.
- Konfiguracije MOSS-a 2007.
- Binarne datoteke.
- Konfiguracije IIS.
- Binarne datoteke (del operacijskega sistema)

Strategija izdelave varnostnih kopij podatkov in obnovo podatkov v primeru katastrofe mora zajemati vsako izmed naštetih komponent. Izbrana strategija je pogosto odvisna od tega ali je okolje SharePoint prilagojeno oz. spremenjeno po meri uporabnika.

Naslednja poglavja opisujejo strategije za ustvarjanje varnostnih kopij vsake od naštetih komponent.

#### **5.8.1.1 Binarne datoteke**

Za ustvarjanje varnostnih kopij datotek operacijskega sistema in programskih datotek MOSS-a 2007 je priporočljiva uporaba orodja za ustvarjanje varnostnih kopij datotečnega sistema. Takšno orodje je lahko NTBackup, ki je priložen k Windows Server 2003. Priporočljivo je tudi hranjenje namestitvenih medijev operacijskega sistema, strežnika SQL, strežnika MOSS 2007 in nadgradenj omenjenih produktov na lokaciji, kjer se farma nahaja in na fizično oddaljeni lokaciji. V primeru potrebe obnovitve podatkov po katastrofi je priporočljivo, da se ponovno namesti operacijski sistem, strežnik SQL in strežnik MOSS 2007.

#### **5.8.1.2 Konfiguracije MOSS-a 2007**

Okolje MOSS 2007 vsebuje konfiguracijo IIS-ja in konfiguracije shranjene v konfiguracijski podatkovni bazi in vsebinski bazi centralne administracije.

##### **5.8.1.2.1 Konfiguracija IIS-ja**

Konfiguracija IIS-ja se nastavi v centralni administraciji ali upravljavcu IIS (IIS Manager) na vsakem spletnem strežniku farme SharePoint ter na sistemih, ki poganjajo servise SQL Server Reporting.

IIS konfiguracije se shranijo v metabazo IIS. Metabaza je navadna tekstovna datoteka XML, ki je prisotna na vsakem spletnem serverju v okolju SharePoint. Metabaza postane lahko

nekonistentna ali se prepíše in jo je zato potrebno vključiti v strategijo izdelave varnostne kopije podatkov. Konfiguracija IIS vsebuje sledeče:

- Nastavitve bazena aplikacij vključno s servisnimi računi (Application pool settings, including service accounts)
- Nastavitve kompresije HTTP-ja (HTTP compression settings).
- Nastavitve poteka časa (Time-out settings).
- Filtri ISAPI po meri (Custom Internet Server Application Programming Interface (ISAPI) filters).
- Članstvo računalnika v domeni (Computer domain membership).
- Nastavitve IPsec-a (Internet Protocol security (IPsec) settings).
- Nastavitve za porazdelitev omrežne obremenitve (NLB Network Load Balancing settings).
- Certifikati SSL (Secure Sockets Layer (SSL) certificates).
- Nastavitve namenskih IP naslovov (Dedicated IP address settings).

Priporočljivo je, da se nastavitve metabaze zabeležijo in ne samo shranijo v obliki varnostne kopije.

#### **5.8.1.2.2 Konfiguracije shranjene v konfiguracijski podatkovni bazi in vsebinski bazi centralne administracije**

Konfiguracije v strežniku MOSS se nastavijo v centralni administraciji in shranijo v konfiguracijsko in vsebinsko podatkovno bazo centralne administracije. Kljub temu, da je ti dve podatkovni bazi možno vključiti v varnostno kopijo, obnova omenjenih podatkovnih baz s pomočjo priloženih orodij za izdelavo varnostnih kopij in obnovo podatkov ni podprta iz razloga, da ti dve bazi nista sinhronizirani s podatki v ostalih podatkovnih bazah MOSS 2007. V primeru, da podatkovne baze niso sinhronizirane lahko v sistemu prihaja do napak. Obnova teh dveh baz je mogoča na sledeče načine:

- Uporabiti je možno varnostno kopijo na nivoju farme, izdelano s System Center Data Protection Manager. V takšnem primeru lahko obnovimo celotno farmo, vključno s konfiguracijskima podatkovnima bazama.
- Obnoviti je mogoče varnostno kopijo konfiguracijskih baz, če je le ta bila narejena pri popolnoma ustavljenih servisih farme.

V primeru, da katera od konfiguracijskih podatkovnih baz postane nesinhronizirana je potrebno ponovno ustvariti obe podatkovni bazi z uporabo SharePoint Products and Technologies Configuration Wizard ali orodja psconfig iz ukazne vrstice.

Za zaščito konfiguracijske in vsebinske podatkovne baze centralne administracije je priporočljivo:

- Dokumentirati vse konfiguracijske nastavitve in rešitve narejene po meri.
- Vzpostaviti redundantni sistem kot so gruče ali zrcaljenje za računalnik, kjer je nameščen strežnik SQL z omenjenimi podatkovnimi bazami.

Konfiguracijske nastavitve v MOSS-u vključujejo sledeče:

- Nastavitve bazena za aplikacije, skupaj s servisnimi računi (z vsemi računi za poganjanje spletnih aplikacij, vključno z računom za indeksiranje in iskanje).
- Nastavitve za Alternate Access Mappings (AAM).
- Nastavitve iskalnika na nivoju farme.
- Nastavitve povezav zunanjega servisa.

- Nastavitve upravljanja delovnih tokov.
- Nastavitve elektronske pošte.
- Nastavitve A/V.
- Nastavitve procesiranja analize uporabe (Usage analysis processing settings).
- Nastavitve diagnostičnega dnevnika.
- Nastavitve namestitve vsebine (Content deployment settings).
- Nastavitve opravila časomera (Timer job settings).
- Nastavitve pregledovalnika HTML (HTML viewer settings).
- Nastavitve koša in druge nastavitve spletnih aplikacij.
- Privzete predloge za kvote.
- Imena podatkovnih baz in njihove lokacije.
- Imena spletnih aplikacij in podatkovnih baz.
- Pravila indeksiranja.
- Aktivirane zmožnosti.
- Blokiranje vrste datotek.

### 5.8.1.3 Dodatki po meri

Dodatki po meri (Customizations) lahko vključujejo:

- Glavne strani (master pages), predloge in CSS stile (cascading style sheets). Ti objekti so shranjeni v vsebinski bazi spletne aplikacije.
- Spletni deli, postavitve strani (page layout) ali definicije seznamov (page layouts or list definitions), stolpce po meri (custom columns), nove tipe vsebine (new content types), polja po meri (custom fields), akcije po meri (custom actions), kodirane elemente delovnih tokov, ali aktivnosti delovnih tokov
- Third party rešitve in z njimi povezane binarne datoteke, ključe v registru, kot je npr. Ifilters
- Spremembe standardnih xml datotek
- Definicije strani narejenih po meri (custom site defintions)

Priporočljivo je, da se vsi dodatki po meri zapakirajo kot rešitve. Rešitev je vsebovalnik za enega ali več dodatkov po meri. Rešitve lahko vsebujejo zmožnosti, spletne dele (Web parts), spremembe varnostne politike in ostale datoteke, ki omogočajo avtomatizirano namestitev na datotečni sistem. Na spletnih strežnikih (front-end web servers), se datoteke dodatkov po meri hranijo v Program Files\Common Files\Microsoft Shared\Web server extensions\12. Nekateri dodatki lahko tudi spreminjajo web.config datoteko. Za sisteme, ki niso centralizirani ali sisteme pri katerih dodatki po meri ne morejo biti zapakirani kot rešitve je izdelovanje varnostnih kopij le teh, kompleksnejše opravilo. Spodnja tabela prikazuje lokacije, kjer se navadno datoteke dodatkov po meri nahajajo na spletnih strežnikih. Priporočljivo je, da se te datoteke dodajo v varnostno kopijo in prav tako morebitne ostale datoteke, ki niso shranjene na teh lokacijah vendar so del dodatkov po meri.

Lokacija	Opis
Program Files\Common Files\Microsoft Shared\Web server extensions\12	Običajno nadgrajene datoteke, po meri narejeni zbiru (assemblies), po meri narejene predloge (custom templates), po meri narejene definicije strani.
Inetpub	Lokacija IIS navideznih imenikov (IIS virtual directories).
C:\WINNT\assembly	Predpomnilnik globalnega zbira (Global assembly cache). To je zaščitena lokacija na operacijskem sistemu, kjer se koda zbiru .NET ogrođa namesti in tako omogoči poln dostop do sistema.

Tabela 7: Lokacija datotek za vključitev v varnostno kopijo

### 5.8.1.4 Vsebina

Vsebina v okolju MOSS se hrani v podatkovnih bazah SQL. Z okoljem MOSS pa so povezane tudi sledeče podatkovne baze:

- Konfiguracijska podatkovna baza (naj se ne vključi v varnostno kopijo)
- Vsebinske podatkovne baze
- SSP podatkovna baza
- Podatkovna baza iskalnika

Priporočljivo je, da se vsebinske podatkovne baze, vključno s podatkovno bazo SSP, vključi v varnostno kopijo podatkov. Kot smo že omenili v poglavju 5.8.1.2.2 pa ni priporočljivo vključevanje konfiguracijske in vsebinske podatkovne baze centralne administracije, saj se podatke le teh lahko obnovi v okoljih z natančno enako konfiguracijo, kot je bila na originalnem okolju. Podatkovna baza iskalnika je poseben primer in jo vključimo v varnostno kopijo le z Office SharePoint Server orodji ali System Center Data Protection Manager-jem. Ta orodja znajo sinhronizirati podatkovno bazo iskalnika z indeksno datoteko iskalnika in obe lahko tudi skupaj obnovimo. Izdelava varnostne kopije podatkovne baze iskalnika s pomočjo orodij SQL Server se odsvetuje, saj ta ne omogočajo sinhronizacije baze z indeksno datoteko iskalnika. V primeru, da bi takšno podatkovno bazo obnovili bi MOSS ponovno začel s polnim indeksiranjem vsebine z namenom ustvarjanja novega indeksa.

## 6 Implementacija prototipa za izdelavo varnostne kopije in obnovo podatkov na osnovi objektnega modela (WSS 3.0 API)

V tem poglavju si bomo ogledali prototip aplikacije za izdelavo varnostne kopije in obnovo podatkov v kateri smo uporabili objektni model z uporabo MOSS-ovega vmesnika API.

Aplikacija je sestavljena iz preprostega menija s sledečim izborom operacij:

- **Prikaži drevo (Showtree)**  
Prikaže drevo komponent, ki so na voljo za vključitev v varnostno kopijo.
- **Varnostna kopija (Backup)**  
Izdelava varnostne kopije z navedbo komponente, ki jo želimo vključiti v varnostno kopijo.
- **Obnova podatkov (Restore)**  
Obnova komponente iz varnostne kopije z navedbo komponente, ki je del varnostne kopije in iz katere želimo obnoviti podatke.
- **Pokaži zgodovino operacij (ShowHistoryList)**  
Prikaz vseh ali posamičnih operacij izdelave varnostne kopije in obnove podatkov.
- **Izbriši zgodovino operacij (RemoveAllHistory)**  
Izbris vse zgodovine o operacijah izdelave varnostne kopije in obnove podatkov.
- **Izpiši podatkovne baze (ListDBs)**  
Izpis podatkovnih baz na farmi.
- **Izpiši strežnike (ShowServers)**  
Izpis strežnikov skupaj z njihovo vlogo.
- **Preveri ali je MOSS nameščen samo na enem strežniku (IsStandalone)**  
Preveri ali je strežnik na katerem poganjamo aplikacijo vključen v farmo ali pa gre le za tako imenovano »standalone« verzijo oz. za samostojni strežnik.

Opisane opcije iz menija so vidne tudi na sliki Slika 10: Prikaz menija z opcijami, ki jih prototip implementira. Ostale slike prototipa, oštevičene od 11 do 15, prikazujejo uporabo različnih opcij implementiranih na podlagi vmesnika WSS 3.0 API.

```

C:\downloads\uros>mossbackup.exe
1 Prikazi drevo (Showtree)
2 Varnostna kopija (Backup)
3 Obnova podatkov (Restore)
4 Pokazi zgodovino operacij (ShowHistoryList)
5 Izbriši zgodovino operacij (RemoveAllHistory)
6 Izpisi podatkovne baze (ListDBs)
7 Izpisi streznike (ShowServers)
8 Preveri ali je MOSS nameščen samo na enem strezniku (IsStandalone)
Izberi:
  
```

Slika 10: Prikaz menija z opcijami, ki jih prototip implementira.

```

C:\downloads\uros>mosbackup.exe
1 Prikazi drevo <Showtree>
2 Varnostna kopija <Backup>
3 Obnova podatkov <Restore>
4 Pokazi zgodovino operacij <ShowHistoryList>
5 Izbrisi zgodovino operacij <RemoveAllHistory>
6 Izpisi podatkovne baze <ListDBs>
7 Izpisi streznike <ShowServers>
8 Preveri ali je MOSS namestjen samo na enem strezniku <IsStandalone>
Izberi:
1
Farm
  [SharePoint_Config]
  Windows SharePoint Services Web Application
    Juventus - 26098
      WSS_Content_30b2c9ad1b004d978519b0adf1f9f0dd
    Milan - 4298
      WSS_Content_7e35eff91fe04f98b532e36f01887300
  SharePoint MySites - 101
    WSS_Content
  [WSS_Administration]
  Web Application
    [SharePoint_AdminContent_4707d700-bdfa-4299-8305-08828cfd06e3]
  MySSP1
    [SharePoint - 100]
      [WSS_Content_webapp_100]
      [MySharedServices1_DB]
      [UserProfileApplication]
      [SessionStateSharedApplication]
      [Shared Search Index]
      [SharedServices1_Search_DB]
    Global Search Settings
    SSO
    Windows SharePoint Services Help Search
      [Search instance]
      [WSS_Search_URAN]

Komponente v oglatih oklepajih ni mogoce izbrati za izdelavo varnostne
C:\downloads\uros>_

```

Slika 11: Prikaz logičnih komponent v okolju MOSS 2007, ki so na voljo za vključitev v varnostno kopijo.

```

C:\downloads\uros>moosbackup.exe
1 Prikazi drevo (Showtree)
2 Varnostna kopija (Backup)
3 Obnova podatkov (Restore)
4 Pokazi zgodovino operacij (ShowHistoryList)
5 Izbrisi zgodovino operacij (RemoveAllHistory)
6 Izpisi podatkovne baze (ListDBs)
7 Izpisi streznike (ShowServers)
8 Preveri ali je MOSS namestjen samo na enem strezniku (IsStandalone)
Izberi:
4
Lokacija spbrtoc.xml (default: \\uran\spbkp): \\uran\spbkp\mojtool
Ime filtra (e.g. backup ! restore ! all, default: all):
1.
ID = 8a05bc92-6ba6-4e4d-8763-744a66d40822
TopComponent = Farm\Windows SharePoint Services Web Application\Milan
isbackup = True
isFailure = False
BackupMethod = Full
directory = \\uran\spbkp\mojtool\spbpr0003\
directoryName = spbr0003
2.
ID = e6eefa87-2b9b-4743-af07-40b8a28cbf68
TopComponent = Farm\Windows SharePoint Services Web Application\Juvent
isbackup = True
isFailure = False
BackupMethod = Full
directory = \\uran\spbkp\mojtool\spbpr0002\
directoryName = spbr0002
C:\downloads\uros>_

```

Slika 12: Pregled zgodovine izdelanih varnostnih kopij in opravil obnove podatkov iz varnostnih kopij

```

C:\downloads\uros>moosbackup.exe
1 Prikazi drevo (Showtree)
2 Varnostna kopija (Backup)
3 Obnova podatkov (Restore)
4 Pokazi zgodovino operacij (ShowHistoryList)
5 Izbrisi zgodovino operacij (RemoveAllHistory)
6 Izpisi podatkovne baze (ListDBs)
7 Izpisi streznike (ShowServers)
8 Preveri ali je MOSS namestjen samo na enem strezniku (IsStandalone)
Izberi:
6
Strezniki v farmi:
  IUDSUPPORT-05
  URAN
  venera

Primerek servisa s podatkovno bazo: venera

Podatkovne baze:
  MySharedServices1_DB
  SharePoint_Config
  SSO
  SharedServices1_Search_DB
  SharePoint_AdminContent_4707d700-bdfa-4299-8305-08828cfd06e3
  WSS_Content
  WSS_Content_30b2c9ad1b004d978519b0adf1f9f0dd
  WSS_Content_7e35eff91fe04f98b532e36f01887300
  WSS_Content_wehapp_100
  WSS_Search_URAN
C:\downloads\uros>_

```

Slika 13: Izpis streznikov in podatkovnih baz v okolju MOSS 2007

```

C:\> Command Prompt
C:\downloads\uros> mossbackup.exe
1 Prikazi drevo (Showtree)
2 Uarnostna kopija (Backup)
3 Obnova podatkov (Restore)
4 Pokazi zgodovino operacij (ShowHistoryList)
5 Izbriši zgodovino operacij (RemoveAllHistory)
6 Izpisi podatkovne baze (ListDBs)
7 Izpisi streznike (ShowServers)
8 Preveri ali je MOSS nameščen samo na enem strezniku (IsStandalone)
Izberi:
7
Ime streznika = IUJSUPPORT-05
Farma v kateri se streznik nahaja = SPFarm Name=SharePoint_Config
Uloga streznika v farmi = WebFrontEnd

Ime streznika = URAN
Farma v kateri se streznik nahaja = SPFarm Name=SharePoint_Config
Uloga streznika v farmi = Application

Ime streznika = venera
Farma v kateri se streznik nahaja = SPFarm Name=SharePoint_Config
Uloga streznika v farmi = Invalid

C:\downloads\uros>_

```

Slika 14: Izpis strežnikov v okolju MOSS 2007 skupaj s pripadajočimi vlogami

```

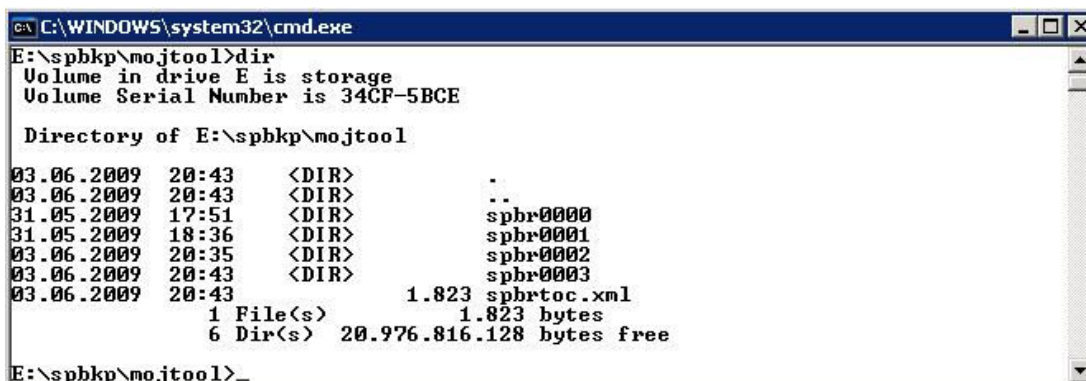
C:\> Command Prompt
C:\downloads\uros> mossbackup.exe
1 Prikazi drevo (Showtree)
2 Uarnostna kopija (Backup)
3 Obnova podatkov (Restore)
4 Pokazi zgodovino operacij (ShowHistoryList)
5 Izbriši zgodovino operacij (RemoveAllHistory)
6 Izpisi podatkovne baze (ListDBs)
7 Izpisi streznike (ShowServers)
8 Preveri ali je MOSS nameščen samo na enem strezniku (IsStandalone)
Izberi:
8
IsStandalone = False

C:\downloads\uros>_

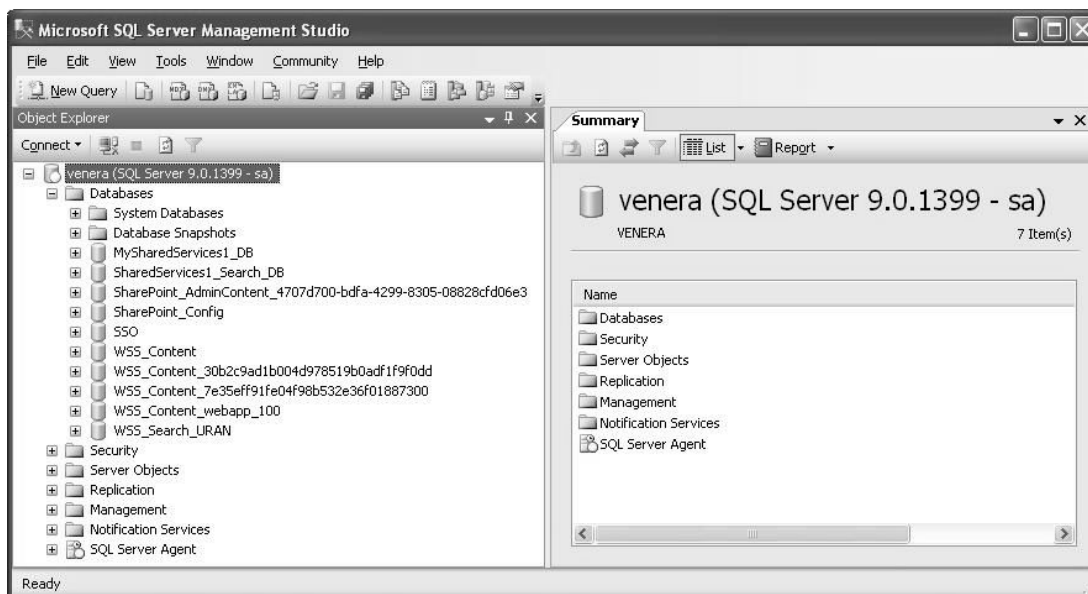
```

Slika 15: Preverjanje ali okolje MOSS deluje na enem samem strežniku (standalone) ali je sestavljeno iz več strežnikov

Za vsako varnostno kopijo se ustvari podimenik z začetnimi črkami spbr in zaporedno štirimestno številko, ki vsebuje varnostno kopijo. V imeniku je tudi datoteka spbrtoc.xml, z zgodovino vseh operacij izdelave varnostne kopije oz. obnove podatkov iz varnostne kopije (Slika 16: Prikaz vsebine imenika, kjer se shranjujejo varnostne kopije..).



Slika 16: Prikaz vsebine imenika, kjer se shranjujejo varnostne kopije.



Slika 17: Prikaz podatkovnih baz v SQL Server management studio

## 6.1 Implementacija izdelave varnostne kopije komponente

Najprej ustvarimo BackupSettings objekt, ki določa lastnosti operacij kot sta tip varnostne kopije, ki je lahko polna ali diferencialna in lokacija kamor naj se varnostna kopija shrani.

```
SPBackupSettings spBSettings =
SPBackupRestoreSettings.GetBackupSettings(backupPath, type);
```

Določimo komponento, ki jo želimo vključiti v izdelavo varnostne kopije. Omejitev je, da lahko izdelamo varnostno kopijo le za eno komponento naenkrat. V primeru, da je vrednost NULL se izdelava varnostna kopija celotne farme.

```
spBSettings.IndividualItem = item;
```

Določimo stopnjo količine podatkov, ki naj se med operacijo izpisujejo v dnevnik oz. na zaslon ter kako pogosto naj se podatki izpisujejo. V našem primeru se bodo podatki izpisovali vsakič, ko se bo delež opravljenega dela celotne operacije povečal za 5 odstotkov.

```
spBSettings.IsVerbose = true;
spBSettings.UpdateProgress = 5;
```

guidBackup je objekt tipa Guid in hrani unikatno identifikacijo operacije, saj je lahko v sistemu več operacij, ki čakajo na izvedbo.

```
Guid guidBackup = SPBackupRestoreConsole.CreateBackupRestore(spBSettings);
```

List predstavlja objekt, ki hrani vse komponente, ki jih funkcija FindItems za določeno operacijo in podano ime komponente najde v okolju SharPoint. IndividualItem je lahko le nekaj začetnih črk komponente. V takšnem primeru bi lahko list vseboval tudi druge komponente, ki se v prvih črkah ujemajo s tisto, ki je navedena kot IndividualItem. Če je zadetkov več moramo biti pri imenu komponente natančnejši, dokler list ne vsebuje samo ene komponente. Le tako lahko sprožimo operacijo za izdelavo varnostne kopije.

```
SPBackupRestoreObjectCollection list =
SPBackupRestoreConsole.FindItems(guidBackup, spBSettings.IndividualItem);
```

S pomočjo SetActive funkcije aktiviramo operacijo, s funkcijo Run pa jo nato poženemo in počakamo, da se operacija zaključi. Ob zaključku pa odstranimo tudi referenco na zaključeno operacijo.

```
if (SPBackupRestoreConsole.SetActive(guidBackup))
{
    if (!SPBackupRestoreConsole.Run(guidBackup, node))
        throw new Exception("Izdelava varnostne kopije neuspešna!");
}
SPBackupRestoreConsole.Remove(guidBackup);
```

## 6.2 Implementacija obnove komponente iz varnostne kopije

Podobni objekti kot nastopajo v izdelavi varnostne kopije podatkov nastopajo tudi pri obnovi podatkov. Razlika je predvsem v tipu, ki je pri obnovi podatkov lahko »overwrite« ali »new«. S prvim tipom obnove podatkov obnovimo obstoječe podatke v okolju SharePoint, drugi način pa uporabimo za obnovitev podatkov na nov sistem ali v novo podatkovno bazo.

```
SPRestoreSettings settings =
SPBackupRestoreSettings.GetRestoreSettings(backupPath, type);
settings.IndividualItem = item;
settings.IsVerbose = true;
settings.UpdateProgress = 10;
Guid restore = SPBackupRestoreConsole.CreateBackupRestore(settings);
```

## 7 Ugotovitve

S ciljem, da bi programerju predstavili tehnologije, ki so na voljo za implementacijo lastne aplikacije za izdelavo varnostnih kopij podatkov in mu kar najbolj olajšali izbor najprimernejše tehnologije, smo obravnavali različna orodja in programske vmesnike.

Glede na namen, lahko izdelavo varnostne kopije podatkov opredelimo kot:

- Varnostno kopijo za obnovo vsebine
- Varnostno kopijo za obnovo celotnega sistema po katastrofi

Okolje SharePoint je za izdelavo varnostnih kopij podatkov ter obnovo podatkov zelo kompleksno. Kompleksnost je posledica uporabe različnih tehnologij, ki tvorijo okolje SharePoint, in stopnja granularnosti podatkov, ki jo imamo na voljo za izdelavo varnostne kopije in obnovo podatkov. Potreba po granularnosti se izkaže predvsem ob obnovi podatkov. V primerih, ko želimo obnoviti kakšen majhen del podatkov, kot je na primer en sam dokument, je nesmiselno obnavljati celotno podatkovno bazo. To namreč vzame veliko časa in sistemskih virov. Rešitev prvega problema je opisana v poglavju o obnovi podatkov po katastrofi (5.8.). Rešitev problema granularnosti pa ni tako trivialna, saj se mora upravitelj varnostnih kopij običajno odločiti med več možnostmi, od katerih pa nobena ni idealna.

Objektni model in priložena orodja, opisana v poglavju 5.2.4 ponujata granularnost na nivoju različnih komponent, od Farme, skupine spletnih aplikacij, posamezne spletne aplikacije, administrativne aplikacije, pa do najnižjega nivoja, ki je v tem primeru podatkovna baza. Problem granularnosti se rešuje z enonivojskim in dvonivojskim košem, vendar, ko dokumenta v koših ni več, tudi to ne zadošča. Varnostno kopijo z večjo mero granularnosti bi lahko izdelali tudi z uvozno/izvoznim vmesnikom API, vendar ta način ni najboljša izbira, saj s tem ne izdelamo varnostne kopije vseh potrebnih podatkov ampak samo kopije določenih, granularnih predmetov kot so datoteke, sezname predmetov in podobno. Zaradi naštetih razlogov ta način tudi ni namenjen izdelavi varnostne kopije temveč selitvi določene vsebine iz ene farme na drugo.

Dobra lastnost objektnega modela je ta, da lahko sinhronizira določene podatkovne baze tako, da je okolje SharePoint med izdelavo varnostne kopije za uporabnika še vedno dosegljivo, pa čeprav nekoliko počasnejše. Omejitev pri tem načinu predstavlja tudi velikost posameznih podatkovnih baz za katere Microsoft priporoča, da naj ne presegajo sto giga bajtov, in dejstvo, da objektni model ne omogoča izdelave varnostne kopije v obliki toka podatkov (data stream). Objektni model shranjuje podatke na imenik, ki je v omrežju v skupni rabi. To seveda zahteva veliko diskovnega prostora, saj farme lahko zasedajo tudi po nekaj tera bajtov. Način shranjevanja podatkov z orodji strežnika SQL omogoča shranjevanje v obliki toka podatkov vendar pa je cena izdelovanja takšnih varnostnih kopij odklop podatkovne baze, saj lahko v nasprotnem primeru postane podatkovna baza nekonsistentna. Poleg tega je s orodji SQL nemogoče vključiti v varnostno kopijo podatkovno bazo iskalnika z indeksnimi datotekami, saj SQL le teh ne zna sinhronizirati.

Izdelovanje varnostne kopije s pomočjo vmesnika WSS VSS API je iz performančnega vidika zelo zanimiva rešitev. Izdelovanje varnostne kopije namreč nima večjega vpliva na obremenitev okolja SharePoint. Zaradi majhne obremenitve se izdelovanje varnostne kopije lahko izvaja tudi v nekaj minutnih intervalih. Slabost tega pristopa je granularnost, saj lahko

izdelujemo varnostne kopije na nivoju celotne podatkovne baze oziroma na delu podatkovne baze, ne moremo pa izdelovati varnostne kopije na nivoju komponent.

Na tržišču obstaja veliko programske opreme za izdelovanje varnostnih kopij podatkov okolja SharePoint, ki jo tržijo svetovno znana in manj znana podjetja. Eno izmed bolj znanih podjetij iz tega področja je AvePoint, ki se z izdelavo varnostnih kopij SharePoint-a ukvarja že od leta 2001. AvePoint rešuje problem granularnosti tako, da iz obstoječe varnostne kopije, ki je izdelana na podlagi objektnega modela oziroma s priloženimi orodji, poišče posamezne datoteke in jih na zahtevo uporabnika obnovi. Takšna rešitev je seveda zelo priročna vendar pa ni izdelana na podlagi dostopne Microsoftove dokumentacije. V primeru, da bi se v prihodnjih verzijah ali s kakšnim paketom popravkov (service pack) shema podatkovne baze v MOSS-u spremenila, bi bilo potrebno to rešitev najverjetneje adaptirati.

Diplomsko delo zaključujemo z ugotovitvijo, da razvijalec nima na voljo univerzalne rešitve, ki bi jo lahko implementiral v svojo aplikacijo za izdelavo varnostnih kopij in s katero bi lahko zadostil vsem zahtevam ali potrebam uporabnika. Pri vsaki od rešitev gre za kompromise, med enostavnostjo implementacije, uporabe, zmožnosti in performančnih zahtev. Vsekakor pa je smotrno izbrati med programskim objektnim modelom za izdelavo varnostne kopije in programskim vmesnikom MOSS VSS. Slednjega namreč uporablja Microsoftovo orodje za izdelovanje varnostnih kopij podatkov, imenovano Data Protection Manager, prvega pa centralna administracija v okolju MOSS in program stsadm, ki sta priloženi orodji. Zaradi teh dejstev lahko v prihodnjih verzijah SharePointa upravičeno pričakujemo še večje Microsoftovo osredotočenje na ta dva programska vmesnika in izboljšavo dokumentacije na tem področju.

## Dodatek A

### 7.1 Kazalo slik

Slika 1: Konvergenca tehnologij [13] .....	4
Slika 2: Glavna področja funkcionalnosti MOSS-a 2007 .....	7
Slika 3: Visokonivojska arhitektura Microsoft Office SharePoint Server 2007 .....	10
Slika 4: Pogled na sodelujoče servise iz stališča razvijalca [5] .....	10
Slika 5: Fizična arhitektura MOSS-a 2007 .....	11
Slika 6: Izbor komponent za izdelavo varnostne kopije v priloženem orodju centralne administracije .....	20
Slika 7: Določitev vrste varnostne kopije in lokacije v priloženem orodju centralne administracije .....	20
Slika 8: Primarni objekti v hierarhiji izdelovanja varnostne kopije in obnove podatkov .....	28
Slika 9: VSS MOSS 2007 arhitektura .....	39
Slika 10: Prikaz menija z opcijami, ki jih prototip implementira .....	47
Slika 11: Prikaz logičnih komponent v okolju MOSS 2007, ki so na voljo za vključitev v varnostno kopijo .....	48
Slika 12: Pregled zgodovine izdelanih varnostnih kopij in opravil obnove podatkov iz varnostnih kopij .....	49
Slika 13: Izpis strežnikov in podatkovnih baz v okolju MOSS 2007 .....	49
Slika 14: Izpis strežnikov v okolju MOSS 2007 skupaj s pripadajočimi vlogami .....	50
Slika 15: Preverjanje ali okolje MOSS deluje na enem samem strežniku (standalone) ali je sestavljeno iz več strežnikov .....	50
Slika 16: Prikaz vsebine imenika, kjer se shranjujejo varnostne kopije .....	51
Slika 17: Prikaz podatkovnih baz v SQL Server management studio .....	51

### 7.2 Kazalo tabel

Tabela 1: Prikaz zmožnosti različnih verzij SharePoint-a 2007 .....	5
Tabela 2: Pregled orodij za obnovo podatkov .....	16
Tabela 3: Prednosti in slabosti priloženih orodij .....	21
Tabela 4: Fizična in logična arhitektura podatkovne baze na strežniku SQL .....	22
Tabela 5: Tipi varnostne kopije .....	24
Tabela 6: Načini izdelave varnostne kopije .....	24
Tabela 7: Lokacija datotek za vključitev v varnostno kopijo .....	46

## 8 Priloge

CD s sledečo vsebino:

- elektronsko verzijo diplomskega dela
- z izvorno kodo primera uporabe objektnega modela za izdelovanje in obnovo podatkov

## 9 Seznam virov

- [1] M. Noel, C. Spence, "Microsoft SharePoint 2007 Unleashed"
- [2] W. Leon, W. Tynes, S. "Cathey, SharePoint Server Bible 2007"
- [3] B. Gates, "Microsoft CEO Summit 2006", Dostopno na:  
<http://www.microsoft.com/presspass/exec/billg/speeches/2006/05-17CEOSummit.mspix>
- [4] Devx, SharePoint Proving a Goldmine for Microsoft Partners, Dostopno na:  
[http://www.devx.com/MS\\_Partner/Article/39761](http://www.devx.com/MS_Partner/Article/39761)
- [5] Microsoft, 2007 Office System Document: 2007 Office System Logical Architecture Diagram, Dostopno na:  
<http://www.microsoft.com/downloads/details.aspx?FamilyID=14c6b1c1-ad26-4ed0-87b8-b691ebdd9662&displaylang=en#filelist>
- [6] Microsoft, Microsoft's fastest growing product ever, SharePoint Server 2007 - Available from Genesis Communications, Dostopno na: <http://www.24-7pressrelease.com/press-release/microsofts-fastest-growing-product-ever-sharepoint-server-2007-available-from-genesis-communications-52532.php>
- [7] Microsoft, Financial Analyst Meeting 2008, Dostopno na:  
<http://www.microsoft.com/msft/speech/FY08/TurnerFAM2008.mspix>
- [8] Microsoft, Microsoft Sales of Microsoft Office SharePoint Server Break \$800 Million, Dostopno na:  
<http://www.microsoft.com/Presspass/press/2007/jul07/07-26SPPT800MPR.mspix>
- [9] Microsoft, MSDN, Programming with the Backup/Restore Object Model, API, Dostopno na: <http://msdn.microsoft.com/en-us/library/cc805878.aspx>
- [10] Microsoft, MSDN, Volume Shadow Copy Service, Dostopno na:  
[http://msdn.microsoft.com/en-us/library/bb968832\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/bb968832(VS.85).aspx)
- [11] Microsoft, What is Microsoft Office SharePoint Server?, Dostopno na:  
<http://www.microsoft.com/sharepoint/prodinfo/what.mspix>
- [12] Microsoft, Windows SharePoint Services 3.0, Dostopno na:  
<http://technet.microsoft.com/en-us/windowsserver/sharepoint/bb684453.aspx>
- [13] SharePoint Joel, Dostopno na: <http://www.sharepointjoel.com/default.aspx>
- [14] Wikipedia, Microsoft Office 2007, Dostopno na:  
[http://en.wikipedia.org/wiki/Microsoft\\_Office\\_2007](http://en.wikipedia.org/wiki/Microsoft_Office_2007)