Provozní bezpečnost databáze

Tato kapitola popisuje způsoby zajištění provozní bezpečnosti databázového systému – preventivní ochranu proti haváriím a řešení již vzniklých havárií. Tyto činnosti patří do kompetence správce databáze.

Dále jsou v této kapitole popsány metody zabezpečení databáze proti neoprávněnému průniku, zakotvení vrcholu hierarchie certifikačních autorit a rozdělení pravomocí mezi bezpečnostní funkcionáře.

Obsahem této kapitoly *není* správa uživatelů, uživatelských práv a skupin uživatelů. O těchto otázkách pojednává zvláštní kapitola.

Některé činnosti správce, týkající se jednouživatelského provozu databáze, jsou detailněji popsány v kapitole *Údržba a zabezpečení databáze* v *Příručce uživatele*.

Postavení správce databáze

Z pohledu WinBase602 **je správcem ta osoba, která se přihlásila pod uživatelským jménem, které patří do skupiny DB_ADMIN. To může být kdokoli, kdo zná heslo příslušející k takovému jménu, a proto hesla správců je třeba pečlivě tajit.**

Používá-li databázový systém více osob, je nanejvýš moudré určit jednu z nich do funkce správce. Jinak se může stát, že se teprve po zničení nebo vyzrazení dat ukáže, že za jejich zabezpečení vlastně nikdo nezodpovídal.

Okruh činnosti správce

Do kompetence správce patří tyto činnosti:

- instalace serveru, zajištění síťové dostupnosti serveru, přidávání dalších licencí (popsáno ve zvláštní kapitole)
- volba způsobu zabezpečení provozu databáze a výkon činností, které jsou pro zabezpečení nezbytné (mimo ty kompetence, které patří *bezpečnostní autoritě*);
- volba provozních parametrů databáze (např. volba vhodného kompromisu mezi rychlostí práce a možností restaurace při poškození databáze);
- rozhodování o právech jednotlivých uživatelů pracovat s určitými daty, s určitými pohledy, tabulkami, programy atd. (část této pravomoci je rozdělena i mezi správce aplikace a uživatele);
- provádění rekonstrukce databáze poškozené např. technickou poruchou.

Počínaje verzí 5.0 se ve **WinBase602** okruh kompetencí správce zúžil ve prospěch buď specializovaných funkcionářů (bezpečnostní autorita, správce aplikace), anebo uživatelů (správa hesel, obnovování zrušených záznamů).

Periodické činnosti správce

Většina akcí databázového správce směřuje ke zlepšení provozních vlastností systému a není nutno je provádět. Jsou však akce, na něž by správce neměl zapomínat:

- pořizovat záložní kopie obsahu databáze, případně nastavit automatické zálohování;
- vede-li se journal, sledovat jeho velikost a při překročení jisté hranice vytvořit záložní kopii a případně journal smazat;
- pokud server často končí práci nenormálně - např. vypnutím počítače bez ukončení programů - občas zkontrolovat strukturu databáze a případně vyhledat ztracené bloky diskové paměti.

Principy zabezpečení systému

Jaké havárie hrozí?

Při provozu databáze je nutné brát v úvahu možnost výskytu těchto událostí:

- výpadek napájení nebo technická havárie počítače uprostřed provádění složité aktualizace;
- poškození části diskové paměti počítače;
- havarijní chování oprávněného uživatele.

Každá z těchto situací má jinou povahu a způsobuje jiný druh škod:

Výpadek počítače

Výpadek napájení nebo technická havárie počítače jsou situace, které nabývají na nebezpečnosti, pokud k nim dojde uprostřed aktualizace sestávající se z více kroků. Je-li aktualizace provedena pouze zčásti, databáze se může dostat do nekonzistentního stavu. Na některých discích může v důsledku výpadku během operace zápisu dojít i k neopravitelnému poškození sektoru. Pak tato havárie přechází na případ uvedený pod dalším bodem.

Poškození média

Údaje, které byly zaznamenány na disk mohou být vlivem chyby povrchu média nečitelné. V takovém případě je velmi významný fakt, zda se nečitelnost odhalí již při zápisu, nebo až při čtení. V prvním případě je náprava podstatně jednodušší.

Chyba uživatele

Systém přístupových práv zabrání tomu, aby neoprávněný uživatel manipuloval s daty. Nezabrání však oprávněnému uživateli “v náhlém pominutí smyslů” zničit důležitá data.

Dále popíšeme, jak se lze proti jednotlivým druhům katastrof bránit.

Ochrana přesměrováním zápisu

Při zápisu údajů na disk může být zjištěno, že příslušný diskový sektor je poškozený a nelze do něj zapisovat. V takovém případě WinBase602 **automaticky přidělí nové místo na disku a přesměruje všechny odkazy z původního sektoru na nový sektor.**

Tato ochrana je velmi jednoduchá, funguje zcela automaticky a **nevyžaduje žádnou aktivitu ze strany správce**. Může selhat ve dvou případech:

- pokud počet poškozených sektorů na disku dosáhne mnoha stovek;
- pokud k chybě při zápisu dojde mnohokrát za sebou v určitých důležitých oblastech **WinBase602** (což je značně nepravděpodobné).

Ochrana záložní kopií

Nejjednodušší ochrana obsahu databáze spočívá v pořizování záložních kopií kompletního databázového souboru, tedy veškerého obsahu databáze. Později, vyžadují-li to okolnosti, lze OBNOVIT DATABÁZI Z KOPIE**, tedy uvést databázi do toho stavu, v němž byla v okamžiku vytvoření kopie.**

Tato ochrana má sama o sobě omezenou účinnost (záložní kopie časem ztrácí aktuálnost), ale získává na důležitosti v kombinaci s JOURNALEM (popis dále).

Správce databáze by měl posoudit, do jaké míry postačuje možnost obnovit po zhroucení databáze její dřívější stav. V některých oblastech nasazení není problém zopakovat aktualizace, které byly provedeny od vytvoření záložní kopie, v jiných to nepřipadá v úvahu a pořizování záložních kopií je nutno doplnit vedením journalu změn (popis dále).

Záloha databáze se provádí zkopírováním (doporučujeme s komprimací) databázového souboru WB5.FIL na vhodné archivní medium (ZIP nebo JAZ disk, páska apod.). Při obnovování databáze nahradíme poškozený databázový soubor dříve pořízenou kopií.

Automatické zálohování

Záložní kopie lze vytvářet buď ručně, nebo lze předepsat periodické zálohování do určeného adresáře. Automatické periodické zálohování nastavíte na konfiguračním panelu **WinBase602**, když na stránce **Databáze a servery** vyberete databázi a stisknete tlačítko **Zálohování**. (detaily viz kapitola *Údržba a zabezpečení databáze* v základním uživatelském manuálu).

Předpokladem k zálohování databázového souboru jsou přístupová práva k adresáři, v němž je umístěn. Tato práva může mít správce databáze nebo správce výpočetního systému.

Ochrana parciálním zálohováním

Každý uživatel si může pořizovat záložní kopie jednotlivých objektů z databáze, dat ze svých tabulek nebo celých aplikací pomocí akcí dostupných na řídicím panelu. K povedení exportu postačí právo číst objekt, objekt nesmí být v zašifrovaném stavu.

Ochrana parciálním zálohováním je velmi jednoduchá a výhodná. Doporučujeme ji využívat zejména tehdy, pokud se nevyplatí zálohovat celý obsah databáze.

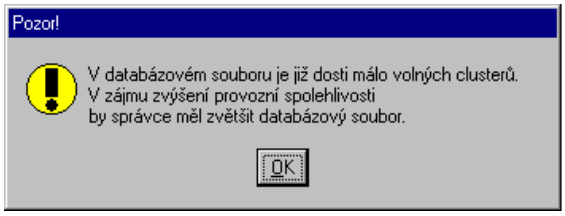
Nejčastěji se používá export celé aplikace. Během vývoje aplikace ji zálohuje její autor, při provozu pak její správce. K exportu aplikace je třeba mít práva čtení ke všem jejím objektům, případně i k datům. Dobré aplikace zpravidla obsahují příkazy na export a import vlastních dat, takže stačí mít jednu kopii aplikace a periodicky exportovat data podle manuálu k aplikaci.

Ochrana preventivním zvětšováním databázového souboru

WinBase602 má veškerá data uložena v databázovém souboru (jménem WB5.FIL) uloženým na disku. Soubor má po svém vzniku určitou velikost, data zabírají jen malou část. Postupem času objem dat roste a volného místa v souboru ubývá.

Dojde-li při provozu **WinBase602** k situaci, že je třeba do datového souboru zapsat další údaje a přitom tam již není volné místo, databázový soubor se dynamicky zvětší. Zde však číhá nebezpečí: dojde-li v této situaci k nekorektnímu ukončení serveru (například při výpadku napájení počítače), ta část databázového souboru, která přibyla, se ztratí a tím se poruší konzistence dat.

Této teoretické situaci lze předejít. **WinBase602** při spuštění kontroluje volné místo v databázovém souboru, a klesne-li pod jistou hranici, vydá následující varování:



Správce by v této chvíli měl provést doporučované zvětšení databázového souboru. Pokud tak neučiní, bude se tato hláška ukazovat při každém dalším spuštění.

Úpravu velikosti databázového souboru může provést i aplikační program pomocí funkce **`GetSet_fil_size`**.

Ochrana transakcemi a jištěním transakcí

Transakční způsob provozu databáze a jištění transakcí je velmi účinnou metodou ochrany proti vzniku nekonzistencí způsobených nedokončením série navzájem souvisejících aktualizací.

Server provádí veškeré zápisy do databáze v tzv. TRANSAKCÍCH, které, dle specifikace klienta, zahrnují jednu nebo více aktualizací. V pracovním režimu s jištěním transakcí server zaručuje, že za každých okolností se transakce provede buď celá, nebo se neprovede vůbec. To platí i tehdy, pokud během provádění transakce v kterémkoli okamžiku vypadne napájení počítače.

Sdružování operací do transakcí definuje programátor aplikace. Pokud tak nečiní, tvoří každá jednotlivá operace samostatnou transakci.

Jištění transakcí

Při jištění transakcí se používá mechanismus, který zajistí konzistenci databáze i v případě, že by k výpadku došlo během uzavírání transakce. Na rozdíl od *použití* transakcí (které má pod kontrolou autor aplikace) je *jištění transakcí* zapínáno a vypínáno správcem jako jeden z provozních parametrů **WinBase602**. Nic nebrání tomu, aby se jištění zapínalo a vypínalo podle okamžitých okolností. Například během importu velkého množství dat, což je časově náročná operace, je možno jištění transakcí vypnout.

Zápis změn na disk

Většina operačních systému má zabudovanou funkci, která odkládá zápis změn v souborech na disk a tím dosahuje zrychlení práce aplikací. Důsledkem toho však je nedefinovaný stav souborů na disku během práce. Pokud má ve **WinBase602** fungovat jištění transakcí, pak je nezbytné zapisovat při ukončení transakce všechny změny na disk.

Nastavování transakčních parametrů je popsáno níže v této kapitole.

Rychlost

Zatímco použití transakcí snižuje počet zápisů na disk v aktualizacích a zrychluje činnost databáze, jištění transakcí vyžaduje přibližně dvojnásobek diskových operací při každé transakci oproti stavu bez jištění. Na rychlost čtení z databáze nebo vyhledávání nemají transakce žádný vliv.

Zápis změn na disk na konci každé transakce může výrazně zpomalit aplikace, které provádějí velké množství aktualizací databáze *nesdružených* do transakcí. Pro orientaci uvádíme změřený čas provedení 1000 zápisů z aplikace ve vnitřním jazyce na nepříliš výkonném počítači, v závislosti na tom, zda je zapnuto jištění transakcí a zápis změn na disk (v sekundách). Konkrétní hodnoty závisejí na použitém počítači, uvádíme je pro vyjádření závislosti času na způsobu práce.

	bez jištění, bez zápisu	jištění, bez zápisu	bez jištění, zápis	jištění, zápis
Všechny aktualizace v 1 transakci	1	<2	<2	<2
Každá aktualizace v nové transakci	2	5	41	68

Ochrana vedením journalu změn

Tato ochrana je nejsilnějším kalibrem proti haváriím všeho druhu. Vyžaduje ovšem kvalifikované použití. Je určena spíše pro období, kdy je databáze v rutinním provozu, a nikoli pro dobu vývoje, kdy ještě dochází k častým hlubokým reorganizacím dat.

WinBase602 může pracovat tak, že si vede *journal* [1] všech aktualizací. To znamená, že po každé aktualizaci obsahu databáze se nová hodnota zapsaná do databáze zaznamenává navíc do určitého zvláštního souboru (journalu), který eviduje všechny změny.

Existence journalu má vliv na spolehlivost databáze **pouze v kombinaci s pořizováním záložních kopií**. Kopie dovoluje obnovit obsah databáze v tom stavu, v němž byl při vytvoření kopie. Na základě obsahu journalu lze pak zopakovat všechny aktualizace, které byly provedeny od pořízení kopie až do zadaného okamžiku (např. do okamžiku poškození databáze).

Journal tedy umožňuje plnou restauraci obsahu databáze po téměř každé havárii. Dokáže chránit i před selháním uživatele, a to i v případě, že se na tuto skutečnost přijde až s určitým zpožděním. Pokud některý uživatel provedl destruktivní akci, pak lze nejprve obnovit databázi z kopie a pak na ni "přehrát" z journalu všechny aktualizace s výjimkou té, která neměla být provedena.

Soubor JOURNAL.FIL

Journal je veden v souboru **JOURNAL.FIL**. Tento soubor při aktualizacích v databázi neustále roste - přidávají se do něj informace o nových a nových změnách. Po vytvoření nové záložní kopie můžete journal smazat.

K tomu, abyste stav databáze obnovený ze záložní kopie mohli pomocí journalu aktualizovat, musíte v něm mít všechny záznamy od doby, kdy byla záložní kopie vytvořena.

Pokud po vytvoření nové záložní kopie journal nesmažete, pak lze databází obnovit i ze záložních kopií staršího data. Tím se zvětšuje míra zabezpečení. Pomocí příkazu **Vztah journalu a databáze** v menu ***Nástroje / Server*** lze zjistit datum nejstaršího záznamu v journalu. Máte-li záložní kopie označeny datem, zjistíte, zda se záložní kopie dá ještě použít.

Journal a počet diskových operací

Vedení journalu zvyšuje množství diskových operací potřebných k aktualizacím. Toto zvýšení však zpravidla nedosahuje dvojnásobku (při použití mnoha indexů k aktualizovaným tabulkám je podstatně menší než dvojnásobek).

Na rozdíl od jištění transakci dokáže journal čelit podstatně širší třídě katastrof, ale vyžaduje složitější restauraci (restaurace není automatická).

---

[1] Čti *žurnál*, a je-li libo, pak i piš žurnál.

Doporučujeme sledovat velikost souboru obsahujícího journal. Pokud budete vkládat do databáze obrázky nebo editovat rozsáhlé texty uložené v databázi, poroste journal velmi rychle. To by mohlo po čase vést ke kritickému nedostatku místa na disku.

Vyčerpání veškerého diskového prostoru uprostřed databázové operace může poškodit databázi. Proto průběžně sledujte, kolik místa na disku zbývá.

Pozor:

Nedoporučujeme zapínat a vypínat vedení journalu podle okamžitých okolností. Přerušovaně vedený journal nemůže účinně chránit. Výjimkou, kdy má smysl v zájmu rychlosti dočasně vypnout vedení journalu, je restrukturalizace tabulky naplněné velkým množstvím dat nebo rozsáhlý import dat.

Zapnutí vedení journalu je popsáno níže v této kapitole.

Konfigurování provozní bezpečnosti WinBase602

Na tomto místě popíšeme nastavování parametrů ovlivňující bezpečnost serveru, které správce databáze provádí z prostředí klienta připojeného na server.

Příkaz **Provozní parametry** v menu ***Nástroje / Server*** otevírá okno, v němž lze nastavit tyto parametry:

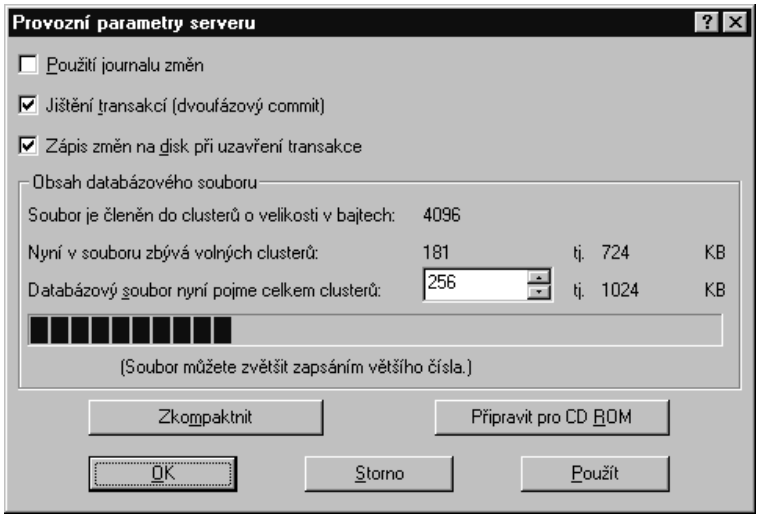
Použití journalu
zda se aktualizace dat mají zapisovat do journalu.

Jištění transakcí
zda má databáze pracovat v režimu s jištěním transakcí.

Zápis změn na disk při uzavření transakce
zda se má vynutit uložení změn na disk bez ohledu na systémové cache.

Nastavené parametry se zaznamenají do databáze a zůstanou v platnosti až do další změny.

Nastavení provozních parametrů a velikosti databázového souboru



Zvětšení databázového souboru lze manuálně provést v rámci nadepsaném **Obsah databázového souboru**.

První údaj udává, na jak velké clustery (alokační jednotky diskové paměti) je rozdělen databázový soubor. Zvětšování velikosti může probíhat pouze v násobcích těchto clusterů. Druhý řádek říká, kolik volných clusterů zbývá dosud v databázovém souboru. Třetí řádek ukazuje, kolik clusterů má databázový soubor celkem. Poměr celkového počtu clusterů k počtu volných clusterů je graficky znázorněn ve spodní části. Součin počtu clusterů a velikosti clusteru v bajtech se rovná velikosti databázového souboru v bajtech.

Zvětšení velikosti databázového souboru se provede zapsáním čísla do editačního pole s dosavadní velikostí. Číslo udávající nový počet clusterů musí samozřejmě být větší než číslo stávající. Tlačítkem **Použít** popř. **OK** se navržená změna uplatní.

K provedení všech těchto změn je nutné zamknutí serveru. Pokud server nebyl dosud zamknut, bude zamknut při provedení příkazu. Server nelze zamknout (tudíž parametry nelze nastavit), jsou-li na server připojení jiní uživatelé.

Z programu se velikost databázového souboru zjišťuje a nastavuje funkcí **`(cd_)GetSet_fil_size`**.

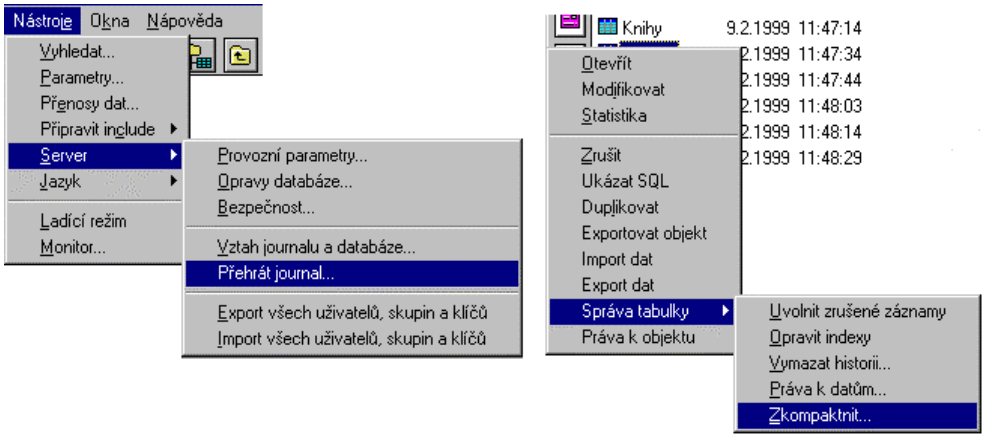
Záchrana poškozené databáze

Dojde-li k poškození databáze, má správce k dispozici sadu nástrojů, jak zachránit data a uvést databázový server opět do chodu. Podle povahy a závažnosti poškození přicházejí v úvahu tyto akce:

Problém	*Řešení*
Poškozené indexy	Přebudovat indexy dotčených tabulek
Chyby ve vnitřní integritě databázového souboru	Spuštění oprav integrity
Zničení databáze	Obnovení databáze ze záložní kopie a aktualizace pomocí journalu
Omylem vymazána důležitá data	Obnovení databáze ze záložní kopie a aktualizace pomocí journalu, s vyloučením akcí určitého uživatele v určitém období
Nelze spustit server nad databází	Provést podepření databáze
Nespecifické chyby	Přenést obsah do nové databáze

Nástroje pro tyto záchranné operace se nacházejí na Konfiguračním panelu **WinBase602** a v menu ***Nástroje / Server*** klienta **WinBase602**. Obnovu indexů tabulky lze vyvolat pomocí popup menu otevřeného na tabulce nebo tlačítkem v pravé části řídicího panelu.

Nástroje správce databáze



Přebudování indexů

Nedokončení aktualizační operace v režimu bez jištění transakcí může mít za následek poškození indexů tabulky. Chyby v indexech se projevují nesprávným vybíráním záznamů podle zadaných kritérií nebo chybným tříděním. Pokud se zjistí, že se chyby omezují **pouze** na indexy, pak je možné nechat je znovu vytvořit.

Je to podstatně rychlejší a bezpečnější akce, než obnovování obsahu databáze ze záložní kopie a její aktualizování z journalu.

Indexy se přebudovávají pro každou tabulku zvlášť. Slouží k tomu příkaz **Opravit indexy**. Tento příkaz lze nalézt na řídicím panelu v popup menu pro tabulku nebo pod tlačítkem **Správa tabulky**.

Opravy poškozené databáze

Při provozu databáze může dojít z různých příčin k jejímu poškození. Kupříkladu ke ztrátě malého množství (nevyužité) diskové paměti dochází pokaždé, když je server nekorektně ukončen (např. resetováním počítače za běhu).

Proto je **WinBase602** vybavena nástroji, které dokážou nalézt a odstranit některé druhy chyb ve struktuře databáze. Opravování databáze lze vyvolat z řídicího panelu příkazem **Opravy databáze** v menu ***Nástroje / Server*** (z programu pomocí funkce `(cd_)Database_integrity`) .

K provedení této akce je nutné zamknutí serveru. Pokud server nebyl dosud zamknut, bude zamknut při provedení tohoto příkazu. Server nelze zamknout (tudíž databázi nelze opravovat), jsou-li na server připojení jiní uživatelé.

Příkaz **Opravy databáze** otevře dialogové okno, v němž pomocí označovacích čtverců zvolíte, které druhy chyb vás zajímají. Poté stisknete tlačítko **Zjistit počet chyb** nebo **Opravit chyby**.

Tlačítkem **Zjistit počet chyb** zahájíte kontrolu obsahu databáze. Poté, co kontrola skončí, se vedle zatržených položek objeví počty *zjištěných* chyb příslušných druhů. Při opravě chyb se na tomtéž místě objeví počty chyb *opravených*.

Oprava databáze

Tlačítkem **Opravit chyby** zahájíte provádění oprav z databázi. Přitom se provádějí tyto akce:

- Je-li zatržen čtverec **Ztracené bloky** nebo **Ztracené kusy diskové paměti**, vracejí se tyto objekty do správy volné diskové paměti.
- Je-li zatržen čtverec **Dvojí využití diskové paměti**, pak pokaždé, když dva databázové objekty sdílejí stejný kus diskové paměti, každý z nich obdrží vlastní kopii. Je nutno ovšem počítat s tím, že pouze jeden z těchto objektů bude mít v této diskové paměti správná data.
- Je-li zatržen čtverec **Zničené definice tabulek**, pak se z databáze odstraní ty tabulky, s nimiž nelze dělat vůbec nic. Tato akce se netýká tabulek, které pouze obsahují poškozená data.
- Je-li zatržen čtverec **Odkazy na neexistující bloky**, pak se z tabulek a indexů odstraní odkazy vedoucí "do prázdna". Po této akci by měl být odblokován export poškozených tabulek a práce s nepoškozenými částmi informace.

Hledání chyb v rozsáhlé databázi i jejich opravování může být časově náročné.

Obnova databáze pomocí záložní kopie a journalu změn

Vhodné využití záložní kopie databáze a journalu dovoluje obnovit databázi ve stavu bezprostředně před její poškozením.

Databáze v toku času...

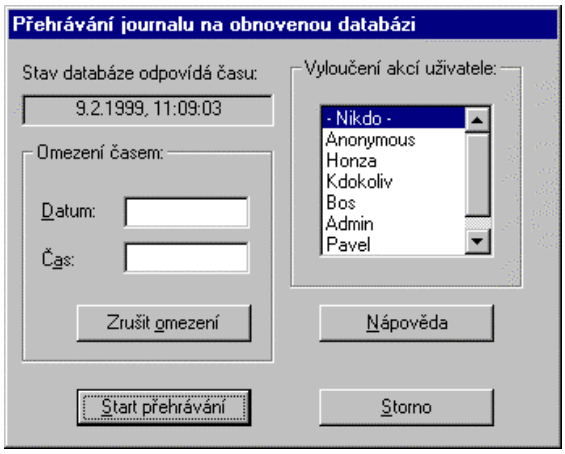
Pro pochopení spolupráce záložních kopii a journalu je dobré si představit, jak se databáze vyvíjí v čase. Každému časovému okamžiku odpovídá určitý stav databáze. Při vytvoření záložní kopie uložíte stav databáze odpovídající určitému okamžiku. Poté se databáze může měnit a změny se zaznamenávají do journalu. Nahrazením poškozené databáze její záložní kopií se stav databáze vrátí do minulosti, do toho okamžiku, kdy byla kopie pořízena. Chcete-li poté databázi aktualizovat, musíte na ní přehrát ty záznamy z journalu, které vznikly mezi vytvořením záložní kopie a jejím načtením. Tím zopakujete všechny změny, kterými databáze v tomto časovém intervalu prošla. Přehráváním journalu se čas databáze bude postupně posouvat kupředu.

Jak použít journal?

Pomocí příkazu **Vztah journalu a databáze** z menu ***Nástroje / Server*** zjistíte datum a čas prvního záznamu v journalu. Pokud jste journal vedli od toho okamžiku bez přerušení, pak záložní kopie pořízené po tomto okamžiku se dají použít k obnově aktuálního stavu databáze, zatímco starší záložní kopie nikoli.

Příkaz **Přehrát journal** z menu ***Nástroje / Server*** otevře dialogové okno, které dovoluje řídit přehrávání journalu na databázi.

Parametry přehrávání



Pokud toto dialogové okno otevřete během normální práce s databází, uvidíte v něm čas provedení poslední aktualizace. Pokusíte-li se pak zahájit přehrávání, **WinBase602** sdělí, že v journalu není žádný platný záznam, tedy záznam o změně, která by se odehrála po čase odpovídajícím aktuálnímu stavu databáze. Pokud jste však předtím načetli záložní kopii, můžete journal přehrávat.

Omezení přehrávání časem

Během aktualizace databáze se neustále opakuje tento proces:

1. z journalu se vybere nejstarší aktualizace, která je novější než stav databáze;
2. tato aktualizace se provede;
3. stav databáze se tím posune kupředu na okamžik, který je zapsán ve vybrané aktualizaci.

Před zahájením přehrávání můžete zadat omezení, do jakého času má tento proces pokračovat. Databázi lze aktualizovat po krocích: můžete postupně zvyšovat časový limit a přehrávat určitý interval aktualizací. Není ale možné některý časový úsek přeskočit.

V části **Omezení časem** můžete vyplnit datum a čas, před nimiž má být přehrávání přerušeno. Tlačítkem **Zrušit omezení** odstraníte zadané omezení.

Vyloučení uživatele

Z aktualizací lze vyloučit akce, které byly provedeny určitým uživatelem. Jméno tohoto uživatele můžete zvolit v pravé části dialogového okna.

Aktualizace s vyloučením některého uživatele může ovšem vést k chybám, pokud akce jiných uživatelů navazují na vyloučené akce, například pokud jiní uživatelé chtějí zapisovat do záznamů, které vyloučený uživatel vytvořil. Proto doporučujeme používat vyloučení pouze v krajních případech: např. k "odzrušení" zrušené tabulky apod.

Akce některého uživatele můžete z přehrávání vyloučit tak, že jeho jméno označíte v seznamu v prvé části okna.

Přehrávání journalu

V dialogovém okně řídícím přehrávání journalu je uveden čas, kterému odpovídá aktuální stav databáze. Pokud přehrajete určitou část záznamů, tento časový údaj se posune kupředu.

Stiskem tlačítka **Start přehrávání** zahájíte přehrávání záznamů z journalu. Během něj se budou přeskakovat záznamy o změnách provedených vyloučeným uživatelem a přehrávání skončí buď dosažením nastaveného časového limitu nebo vyčerpáním obsahu journalu.

Principy a záludnosti aktualizace

Přehrávání journalu WinBase602 **je schopno opakovat pouze ty aktualizace, které byly zaznamenány do journalu. Pokud se journal nevedl po celou dobu od pořízení kopie, může to vést k chybám.**

Jestliže na akce nezaznamenané do journalu navazují jiné, zaznamenávané akce, nemusí být jejich úspěšné zopakování možné. Pokud se například nezaznamená vložení jednoho záznamu do tabulky a zaznamená se vložení dalších, dojde ke ztrátě synchronizace v číslech záznamů a obnova se nezdaří.

Otázka časového intervalu

Pokud hodláte načíst záložní kopii databáze a přehrát na ní obsah journalu, musíte tyto akce provést bezprostředně po sobě. Pokud byste totiž po načtení záložní kopie provedli sebejednodušší aktualizaci, posunul by se tím čas posledního zásahu do databáze a z journalu by se nevybraly k přehrání žádné záznamy.

Práva

Pokud se v přehrávané části journalu vytvářejí nové objekty, pak práva tvůrce k těmto objektům bude mít správce databáze. Proto může být potřebné po přehrání journalu přidělit určitá práva uživatelům **WinBase602**.

Co journal nesleduje

Vede-li se journal aktualizací, zaznamenávají se do něj všechny aktualizace obsahu databáze s **těmito výjimkami**:

- přebudování indexů;
- uvolnění zrušených záznamů;
- zapomenutí (části) historie;
- opravování obsahu databáze;
- změna provozních parametrů databáze.

Journal tedy nezajistí zopakování výše uvedených operací během aktualizace kopie databáze.

Jak postupovat v praxi ?

V případě poškození databáze postupujte takto:

1. Pořiďte si kopii aktuálního stavu databázového souboru WB5.FIL, neboť vzhledem k výše uvedeným omezením nelze zcela vyloučit neúspěch operace;
2. obnovte databázi tak, že databázový soubor WB5.FIL přepíšete obsahem poslední záložní kopie;
3. spusťte klienta a přehrajte na databázi záznamy z journalu.

Pokud jste po vytvoření záložní kopie nesmazali journal, pak budete mít možnost obnovit databázi z posledních dvou kopií, a tak dále. Jistíte se tedy i proti případu, že by některá záložní kopie byla nečitelná.

Podepření vážně poškozené databáze

I z databáze, které se dostala do takového stavu, že na ní nelze spustit server (a tedy ani žádného klienta), je často možné získat uložená data.

Chybový stav vhodný pro podepření databáze se projevuje hlášeními jako *Poškozen databázový soubor* případně i *Chybná verze serveru* nebo se ztratí přidělená práva a není možné se nijak přihlásit. K této situaci může dojít například tehdy, pokud nějaký program přepíše část obsahu databázového souboru.

I v této situaci mohou však některé části dat v databázi být nepoškozené. Podepření databáze se pokusí uvést databázi do takového stavu, aby se šlo k serveru přihlásit, nepoškozená data exportovat a poté je přenést do nově vytvořené databáze.

POZOR:

Nepoužívejte podepírání databáze v situaci, kdy se server spustit sice dá, ale některá její část je poškozená nebo některá data scházejí. V tomto případě podepření nepomůže. Podepření nelze provést na šifrovaný databázový soubor.

Podepření poškozené databáze pod Windows

Podepření lokální databáze lze provést z Konfiguračního panelu **WinBase602**. Na stránce **Databáze a servery** označte poškozenou databázi a stiskněte tlačítko **Podepřít databázi**. Po dvojím vážném varování se záchranná akce provede.

Podepření poškozené databáze pod Novell Netware

Pro podepření poškozené databáze se na konzoli přepněte do adresáře, který obsahuje programy **WinBase602**. Pak zadejte konzolový příkaz:

```
LOAD BERLE &adr
```

kde *adr* je cesta k adresáři obsahujícímu databázový soubor.

Podepření poškozené databáze pod Unixem

Pro podepření poškozené databáze se přepněte do adresáře, který obsahuje programy **WinBase602**. Pak zadejte příkaz:

```
berle &adr
```

kde *adr* je cesta k adresáři obsahujícímu databázový soubor.

Restaurování databáze

Po úspěšném podepření databáze spusťte provozní nebo vývojové prostředí **WinBase602** s parametrem `/B` (upravte příkazovou řádku zástupce). Tento parametr zabrání případné kompilaci programu ve vnitřním jazyce při otevírání aplikace a tím i zápisu na disk.

Dále pak pracujte s **WinBase602** obvyklým způsobem a proveďte export definic objektů a dat z tabulek do souborů. Data doporučujeme exportovat ve vnitřním formátu **WinBase602**. Je jistější exportovat jednotlivé komponenty každé aplikace než aplikaci jako celek, protože jedna poškozená komponenta zabrání exportu dalších komponent aplikace.

POZOR ! Nepokoušejte se do podepřené databáze cokoli zapisovat!

Po exportu všech objektů a dat, která se dají zachránit, vytvořte databázi znova.

Jsou-li programy **WinBase602** nepoškozeny, nemusíte ji instalovat z distribučních disket, ale stačí vytvořit databázi pomocí akce **Vytvořit databázi** z řídicího panelu nebo z Konfiguračního panelu.

Po novém vytvoření je databáze prázdná a můžete do ní importovat data zachráněná z poškozené databáze.

Odstranění nespecifických chyb přenosem dat do nové databáze

Vyskytne-li se v databázi chyba, na jejíž řešení se nehodí žádný z popsaných postupů, lze se jí zbavit poměrně jednoduchým postupem:

1. Exportujte z databáze všechny aplikace, včetně dat a práv uživatelů, skupin i rolí. Každou aplikaci exportujte do zvláštního adresáře, aby se stejně pojmenované objekty v různých aplikacích navzájem nepřepsaly.
2. Exportujte z databáze všechny uživatele pomocí příkazu **Export všech uživatelů, skupin a klíčů** z menu ***Nástroje / Server***.
3. Založte novou databázi a připojte se k ní.
4. Importujte do databáze všechny uživatele pomocí příkazu **Import všech uživatelů, skupin a klíčů** z menu ***Nástroje / Server***.
5. Importujte do databáze všechny vyexportované aplikace.

Pokud chyba brání exportu některé aplikace, pokuste se z ní exportovat alespoň jednotlivé nepoškozené objekty. Nedaří-li se exportovat data z některé tabulky, pokuste se exportovat alespoň část záznamů vybranou vhodně položeným dotazem.

Bezpečnostní parametry

V této sekci shrneme informace o způsobech zajištění **WinBase602** proti nepovolaným osobám (tedy nikoli proti technickým haváriím) a popíšeme rozdělení kompetencí různých osob spoluodpovědných za bezpečnost.

Ochrana obsahu databázového souboru

Všechny zde popisované mechanismy ochrany obsahu databáze proti přístupu neoprávněných osob se týkají přístupu k datům uloženým pod správou databázového serveru prostřednictvím některého klienta.

Mimo to je však třeba databázový soubor chránit i před přímou manipulací obcházející server. Přestože vnitřní struktura souboru je složitá a není zveřejněná, vyhledáváním klíčových frázi v tomto souboru by bylo možno zjistit některé informace uložené v databázi. Přepsáním tohoto souboru lze snadno zničit obsah databáze.

Základní ochrana databázového souboru by měla spočívat v jeho umístění do adresáře chráněného proti čtení nebo přepisu. Přístup k databázovému souboru musí mít pouze server. Klient ke své práci *nepotřebuje* žádná přístupová práva k databázovému souboru, svazek nebo adresář obsahující tento soubor nemusí být vůbec v síti viditelný.

Pokud server pracuje jako *NT service*, pak má systémová práva pro přístup k souborům.

Šifrování databázového souboru

Pokud ochrana databázového souboru přístupovými právy není realizovatelná nebo dostatečná, lze ji doplnit nebo částečně nahradit šifrováním obsahu tohoto souboru. Ve **WinBase602** jsou implementovány tři způsoby šifrování:

1. Jednoduché a rychlé šifrování založené na pevném heslu.
2. Jednoduché a rychlé šifrování založené na heslu zvoleném uživatelem.
3. Velmi účinné, ale pomalejší šifrování založené na heslu zvoleném uživatelem.

První způsob šifrování může být prolomen odborníkem při vynaložení mírného úsilí, druhý způsob lze prolomit při použití značného úsilí. Třetí způsob je založen na kvalitním šifrovacím algoritmu a šance na jeho prolomení teoreticky existuje při vynaložení extrémních nákladů. Použití třetího způsobu zpomalí činnost serveru.

Při použití druhého nebo třetího způsobu je nutno při spouštění serveru zadat šifrovací heslo.

Ochrana databázového souboru heslem je vhodná pro síťové servery, ale již méně pro lokální servery spouštěné přímo klientem. Pokud klient spouští server, pak na odpověď od serveru čeká pouze omezenou dobu, a po jejím uplynutí oznámí, že server neodpovídá. K této situaci může dojít také tehdy, je-li databázový soubor serveru chráněn heslem a obsluha toto heslo ve stanovené době nezadá.

Přehled dalších bezpečnostních parametrů

Ve **WinBase602** lze nastavit parametry, které ovlivní míru její odolnosti proti proniknutí nepovolaných osob na server.

Parametry ovlivňující přihlašování na server

Minimální délka uživatelského hesla - předepisuje minimální počet znaků hesla, které si smí zvolit uživatel. Větší hodnota snižuje riziko proniknutí do systému vyzkoušením všech možných krátkých slov ze slovníku.

Expirační doba hesla - udává počet dnů, po jejichž uplynutí bude uživatel donucen si změnit heslo. S dobou platnosti hesla se zvyšuje riziko jeho vyzrazení, proto omezení doby platnosti chrání uživatele před zneužitím jejich hesel.

Jméno síťového serveru, z něhož se přebírá přihlášení - je-li uvedeno jméno síťového souborového serveru, pak uživatel, který je na tento server přihlášen a má ve **WinBase602** stejné jméno, bude přihlášen do **WinBase602** bez udávání hesla. Tento mechanismus urychluje spouštění **WinBase602** a jejích aplikací, ale snižuje bezpečnost systému. Pokud se uvede místo jména síťového serveru slovo NULL, využije se pro přihlášení do **WinBase602** jméno, pod kterým je uživatel přihlášen na svůj počítač. Tím se ovšem podstatně sníží bezpečnost.

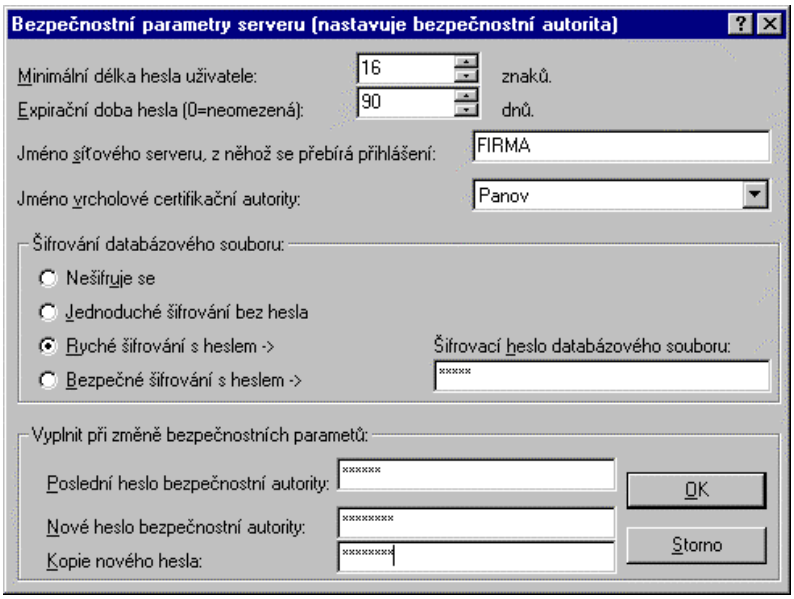
Volba vrcholové certifikační autority

Z hlediska bezpečného ověřování identity uživatelů je klíčová volba osoby, která tvoří vrchol hierarchie certifikačních autorit.

Nastavování bezpečnostních parametrů

Bezpečnostní parametry se nastavují v dialogovém okně, které se otevírá příkazem **Bezpečnost** ze submenu ***Server*** v menu ***Nástroje***.

Bezpečnostní parametry



Bezpečnostní autorita

Osobu oprávněnou ke změnám bezpečnostních parametrů serveru nazýváme *bezpečnostní autorita*. Bezpečnostní autorita nemusí mít na serveru, jehož bezpečnost řídí, žádná práva, a může se přihlašovat jako anonymní uživatel.

Bezpečnostní autoritou může být správce databáze, ale v oblastech citlivých na bezpečnost je vhodné oddělit tyto dvě funkce. Není-li správce bezpečnostní autoritou, pak zejména:

- ztrácí kontrolu nad hierarchií certifikačních autorit, protože nemůže volit vrcholovou CA;
- ztrácí kontrolu nad možností přihlašování se do **WinBase602** na základě přihlášení na zvolený souborový server a tím se odstraňuje jeho šance vydávat se za jiného uživatele po vhodném překonfigurování sítě a manipulaci se souborovými servery.

Bezpečnostní autorita zadá při zastavení bezpečnostních parametrů heslo, které bude nutno uvést při příštím nastavování bezpečnostních parametrů. Doporučuje se při každém nastavení použít jiné heslo.

Bezpečnostní autorita je tedy definována jako osoba, která zná heslo zadané při posledním nastavování bezpečnostních parametrů. Před prvním nastavením parametrů je toto heslo prázdné.

Rozdělení pravomocí ve vztahu k bezpečnosti

Pravomoci ovlivňovat bezpečnost databáze jsou úmyslně rozděleny mezi řadu osob tak, aby se minimalizovaly případné škody vzniklé při selhání jedné osoby.

Bezpečnostní autorita nastavuje parametry, které ovlivňují celkovou odolnost proti proniknutí zvenčí, tedy minimální délku a expirační dobu hesel, možnosti zrychleného přihlašování, šifrování obsahu databázového souboru. Dále nastavuje vrcholovou certifikační autoritu.

Správce souborového serveru, na němž je umístěn databázový soubor, zajišťuje, že s databázovým souborem smí pracovat pouze databázový server. Znemožňuje přístup k databázovému souboru z počítačů v síti a znemožňuje fyzický přístup k počítači, na němž běží server.

Správce databáze definuje skupiny uživatelů a zařazuje do nich uživatele, může obsazovat uživatele a skupiny do rolí, může přidělovat a odebírat veškerá uživatelská práva. Sám disponuje veškerými právy. Nastavuje také provozní parametry serveru, které ovlivní jeho schopnost zotavení z technických havárií. Řeší havarijní situace.

Správce aplikace obsazuje uživatele a jejich skupiny do rolí definovaných v aplikaci a obvykle také může přidělovat práva ke všem objektům aplikace.

Certifikační autorita ověřuje identitu uživatelů databáze a případně ověřuje i níže postavené certifikační autority. Tím dává uživatelům možnost podepisovat dokumenty.

Uživatel si sám volí heslo a kdykoli jej může měnit. Sám si generuje dvojici klíčů a zodpovídá za bezpečné uložení svého soukromého klíče. Pokud nevyzradí své heslo a nevydá svůj soukromý klíč, nikdo se nemůže přihlásit pod jeho jménem nebo podepisovat dokumenty jeho jménem.

Nejdůslednější je rozdělení pravomocí mezi hierarchií certifikačních autorit a ostatními bezpečnostními funkcionáři. Certifikační autority nemají žádný vliv na uživatelská práva a samy nemusejí žádná mít. Naopak nikdo nemůže zasáhnout do kompetenci certifikačních autorit, dokonce ani bezpečnostní autorita. V případě, že by bezpečnostní autorita zvolila nesprávnou vrcholovou certifikační autoritu, při hloubkovém prověřování kteréhokoli podpisu uživatele ověřeného touto autoritou (nebo jí podřízenou autoritou) by tato skutečnost vyšla najevo.

Činnosti vyhrazené pro správce

Níže uvedené činnosti smí provádět pouze správce databáze (tj. člen skupiny DB_ADMIN):

- odpojování jiných uživatelů od serveru;
- rušení zámků na serveru;

- nastavování provozních parametrů serveru (zvětšování databázového souboru, jištění transakcí, vedení journalu, ukládání na disk);
- přehrávání journalu;
- omezení délky historie ve sledovacích atributech tabulky;
- zařazování uživatelů do skupin a vyřazování z nich.