Skrbniška orodja v modulu Administracija

V tem prispevku

Zadnja sprememba 27/03/2026 11:14 am CET

Model Saop Proizvodnja avtentikacije

Model deluje na osnovi sistema dostopov do podatkov na dveh nivojih sočasno:

- zagotavlja dostop do opravil na nivoju Saop Proizvodnja Poslovnega Informacijskega Sistema
- sočasno skrbi za omejen dostop do podatkov na nivoju SQL strežnika

Načini in mehanizmi zagotavljanja varnosti dostopa do podatkov in opravil znotraj poslovnih funkcij

Za dostop do poslovnih opravil skrbi sistem pravic Saop Proizvodnja. Deluje tudi pri drugih modelih avtentikacije.

Dostop do podatkov Saop Proizvodnja PIS je omejen samo na uporabnike, ki jih kreira skrbniški modul.

Uporabnike, pravice uporabnikov, nadzor nad prijavami v program Saop Proizvodnja izvajamo preko modula Administracija (v nadaljevanju modul ADM), ki je sestavni del Saop Proizvodnja.

- Uporabniška imena, ki jih kreira modul ADM imajo vsa predpono MIT_. Primer imena MIT_UPORABNIK. Zato na SQL strežniku ne sme biti ročno narejenih uporabniških imen in login-ov po tem vzorcu. Vsakemu uporabniškemu imenu modul Administracija dodeli geslo, ki se razlikuje od gesla, ki ga uporabnik vpiše ob prijavi v aplikacije Saop Proizvodnja.

- Geslo uporabnika za vstop v Saop Proizvodnja ni enako geslu uporabnika za dostop do podatkov na strežniku.

- Gesla tega istega uporabnika za dostop do podatkov z nekim drugim orodjem razen z aplikacijami, ki so del Saop Proizvodnja, ni mogoče ugotoviti. Za pretvorbo gesla skrbi poseben algoritem.

- Če skrbnik sistema uporabnikom ne zagotovi dostopa do podatkov Saop Proizvodnja na kak drug način, so podatki zavarovani in nedostopni.

Opozorila

- Uporabnika MIT_SA se ne sme brisati iz baze ali z SQL strežnika. V tem primeru bo onemogočeno normalno izvajanje nadgradenj in primerno

administriranje sistema pravic Saop Proizvodnja.

- Uporabniškim imenom na SQL strežniku ne smemo ročno spreminjati gesel. Geslo uporabnika za vstop v Saop Proizvodnja se lahko spremeni izključno skozi temu namenjen program za spreminjanje gesel, ki je dostopen v vseh aplikacijah Saop Proizvodnja. Ročna zamenjava gesla neposredno na SQL strežniku ni dovoljena. Tak uporabnik ne bo več mogel prijaviti v nobeno aplikacijo Saop Proizvodnja s svojim geslom.

Uporabniška imena, gesla in skupine

Podatki so pred nepooblaščeno uporabo varovani na več različnih načinov:
- vstop v programe imajo posamezniki s svojim uporabniškim imenom
- vsako uporabniško ime ima svoje geslo
- za posamezno uporabniško ime določamo dostopne pravice do objektov
- za vsak varovani objekt (pravico) določamo dovoljenja za delo (Read, Write, Delete, ...)

Za lažji nadzor in zmanjšano potrebo po administriranju skrbi sistem združevanja v skupine:
- pravice do objektov združimo v skupino
- uporabnike pripnemo v izbrano skupino

V sistemu je določen poseben privzeti sistemski administrator MIT_SA. Zanj veljajo naslednja pravila:
- je privzeti uporabnik Saop Proizvodnja. Obnaša se podobno kot SA, torej privzeti administrator na SQL strežniku.
- Uporabnika MIT_SA sistem Saop Proizvodnja samodejno doda na za to predvidena mesta v tabele za konfiguracijo sistema pravic.
- Ima neomejen dostop do vseh virov znotraj sistema Saop Proizvodnja.
- Je edini login - uporabnik, ki ga je potrebno določiti že pred namestitvijo programske opreme Saop Proizvodnja tudi na nivoju SQL strežnika.
- Ta login-uporabnik naj ima obvezno gesla, ki ni poznano ostalim uporabnikom.
- Je edini uporabnik, ki ima geslo za vstop v Saop Proizvodnja enako tistemu, ki velja tudi za vstop v SQL strežnik.
- Geslo mu lahko zamenjamo znotraj Saop Proizvodnja-a ali pa neposredno na SQL strežniku.
- MIT_SA ni mogoče brisati iz tabele uporabnikov. To velja za sistemska orodja, ki so del Saop Proizvodnje.

V sistem avtentikacije in dovoljenj za izvajanje opravil nad podatki sta vgrajeni dve posebni pravici ADMIN in ADMINSQL. ADMIN je pravica, ki omogoča uporabniku, ki mu je dodeljena, neomejeno izvajanje vseh opravil znotraj Saop Proizvodnje. Lahko spreminja vse podatke in izvaja prav vsa opravila brez omejitev. Ne more pa dodajati novih uporabnikov in ne more menjati gesla drugim uporabnikom brez omejitev. ADMINSQL

uporabniku s predhodno dodeljeno pravico ADMIN omogoči še dodatne možnosti:
- lahko dodaja nove uporabnike v sistem,
- lahko spreminja gesla drugim uporabnikom.

Kljub temu pa uporabnik s pravico ADMINSQL nima neposrednega dostopa do podatkov na SQL strežniku in še vedno mu ni moč določiti gesla neposredno na SQL strežniku. Uporabnik s pravico ADMINSQL je podaljšana roka nosilca vseh inistrativnih privilegijev s privzetim administratorskim loginom MIT_SA.

Prva namestitev - priprava pred namestitvijo

Da bi prva namestitev potekala s čim manj zapleti, se je nanjo potrebno pripraviti. Priprave lahko uredi skrbnik sistema pri naročniku (sistemski administrator). Nameščen mora biti SQL strežnik, ki mora zadoščati pogojem, ki so navedeni v prilogi k pogodbi. Priloga vsebuje minimalne in priporočene tehnične zahteve za računalnik in namestitev SQL strežnika. Priloga se imenuje "Priporočena strojna in sistemska oprema".

Delovne postaje morajo imeti nameščene primerne odjemalce za SQL server native client.

Namestitvena procedura za navedene odjemalce je dostopna na spletni strani proizvajalca SQL strežnika. Na strani poiščite datoteko sqlncli.msi, ki jo shranite nekam na mrežni disk, ki je dostopen vsem osebnim računalnikom. S tega mesta se potem z dvojnim klikom požene namestitev odjemalca na vsakem osebnem računalniku posebej.

Novejši odjemalci ne delujejo na Windows XP!

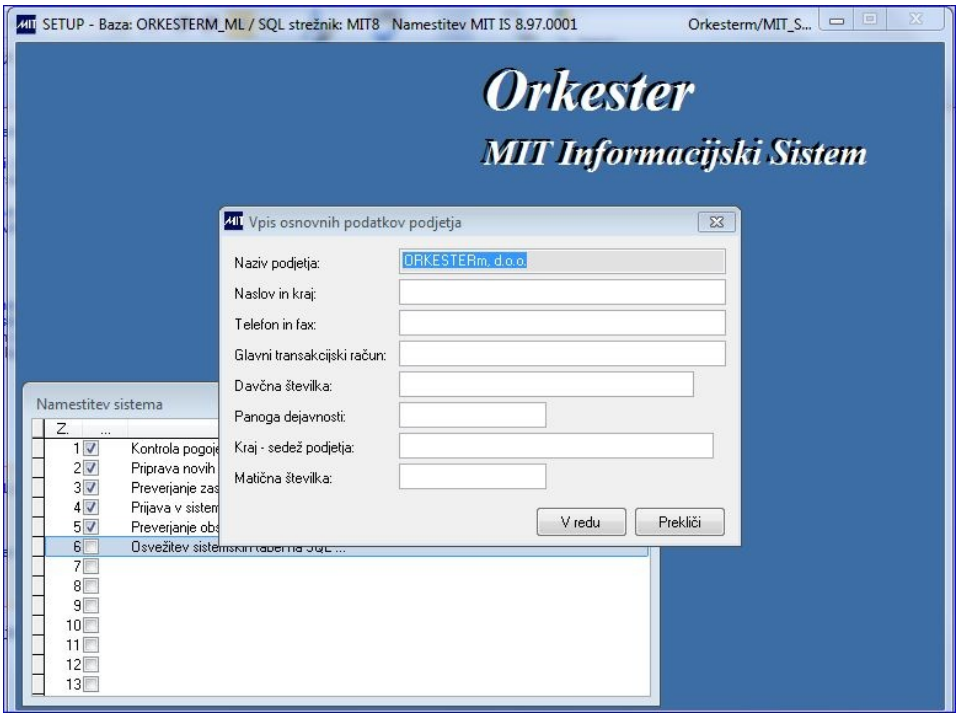
Druge zahteve in priporočila:

- Collate na strežniku naj bo Slovenian_CI_AS. Če ni isti collate na strežniku kot na bazah, potem nekatere procedure javljajo napake.
- Saop Proizvodnja naj bo SQL na svoji instanci,
- Na SQL strežniku naj bo pripravljena Baza, kjer se bodo shranjevali podatki za Saop Proizvodnja.
- Na SQL strežniku naj bo pripravljen LOGIN z imenom MIT_SA (ime je obvezno!). LOGIN mora biti član strežniške vloge "System Administrators".

Prepovedani znaki v imenu BAZE na SQL strežniku so: '_' in '%'. Ti znaki lahko povzročijo, da program ne najde ustrezne baze in ni možna prijava na SQL strežnik.

Ob prvi namestitvi mora izvajalec določiti osnovne podatke podjetja. Ti

obvezni podatki so: Naziv podjetja, Naslov in kraj sedeža podjetja, Telefon in fax, Glavni transakcijski račun, Davčna številka, Panoga dejavnosti, Matična številka.



Program Saop Proizvodnja lokalno

Potrebne nastavitve katere omogočajo, da je program Saop Proizvodnja nameščen na lokalnem disku računalnika in je le dostop do SQL strežnika kjer je nameščena osnovna namestitev in baza podatkov.

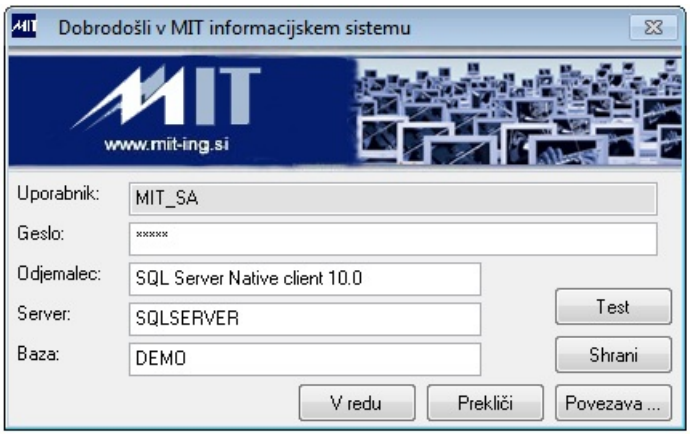
Povezava programa in baze na SQL Strežniku

V primeru, da se na posameznem računalniku dogaja, da po mirovanju program ne vzpostavi ponovno povezave z bazo je potrebno preveriti:
- nastavitev mrežne kartice ali je nastavljena na varčevanje z energijo in zaspi. Potrebno izklopiti varčevanje.
- mrežni kabel,
- mrežna kartica.

Nadgradnja na višjo verzijo Saop Proizvodnja

V sklopu sistema Saop Proizvodnja je zagotovljena nadzorovana in naročniku prijazna nadgradnja informacijskega sistema Saop Proizvodnja. Sistem nadgradenj zagotavlja uveljavljanje informacijske podpore zakonskim spremembam, v zvezi s poslovanjem podjetja v okviru ERP sistema. Prav tako se s sistemom nadgradnje uveljavijo dopolnitve programske podpore na podlagi zahtev in naročil naročnikov.

Dodatni podatki na prijavnem oknu:
- Odjemalec - naziv odjemalca. Na računalniku mora biti naložen primeren odjemalec za SQL server.
- Server - ime SQL strežnika v uporabniku in aplikaciji dostopnem delu omrežja.
- Baza - ime BAZE na strežniku, do katere dostopa uporabnik.



Vsi trije podatki so vidni ob proženju gumba Povezava. Podatkov sam uporabnik ob prijavi ne more spreminjati. Spreminja jih lahko samo skrbnik sistema s primernim geslom. Podatki so skupni za vse odjemalce, kjer se poganjajo aplikacije PIS. Aplikacija prebere parametre iz sistemskih nastavitev PIS. Nastavijo se samo enkrat na enem samem odjemalcu ob prvi namestitvi sistema PIS.

Zamenjava gesla

Geslo za vstop se prvič vpiše, ko se kreira uporabniško ime in pravice do dostopanja v programe Saop Proizvodnja. To naredi koordinator ali pa skrbnik sistema. Po prvem vstopu v program si lahko uporabnik sam poljubno spreminja svoje geslo. Oblika gesla in kdaj se geslo spreminja je stvar dogovora oziroma predpisa podjetja. V primeru, da bi radi spremenili geslo, pa niste seznanjeni z vašim predpisom o kreiranju gesel, se obvezno posvetujte z vašim skbnikom (koordinatorjem) informacijskega sistema. V skladu sistemskih nastavitev, se določa:
- ali je geslo obvezno
- dolžino gesla
- časovno veljavnost gesla

Forma za spremembo gesla ima naslednja vnosna polja:
- Uporabnik : sistem predlaga ime uporabnika, ki je trenutno prijavljen v program. Lahko vpišete tudi drugo ime, kateremu želite spremeniti geslo
- Staro geslo : vpišite do sedaj veljavno geslo
- Novo geslo : vpišite novo geslo, po predpisu vašega podjetja
- Potrdi geslo : še enkrat vpišite vaše novo geslo, za kontrolo, da se morda niste prvič zmotili pri vnosu

Po vnosu vseh potrebnih podatkov za spremembo gesla pritisnite gumb V redu. Če ste se morda zmotili pri vnosu starega ali novega gesla, vas bo program na to opozoril. Pravilno vnesite gesla in ponovno pritisnite gumb V redu. Če gesla ne želite spremeniti, potem pritisnite gumb Prekliči.

Pri zamenjavi gesla veljajo naslednje omejitve:

- Običajni uporabnik lahko zamenja geslo samo sam sebi.
- Privzeti MIT_SA sistemski administrator lahko zamenja geslo vsakemu uporabniku.
- Privzetemu sistemskemu administratorju MIT_SA ni potrebno vedeti prejšnjega gesla, če menja geslo običajnemu uporabniku.
- Uporabniki Administratorji z dodeljeno pravico ADMIN in dodatno dodeljeno pravico ADMINSQL imajo enaka pooblasitla kot privzeti sistemski administrator MIT_SA.

Geslo je omogočeno zamenjati v okviru:
- programa Administracija / Uporabniki in skupine (ikona in podmeni med dodatnimi meniji)
- vsi programi v meniju Opcije / Okolje - Sprememba gesla.

Uporabnik za spremembo gesla potrebuje pravico VSI.GESLO.

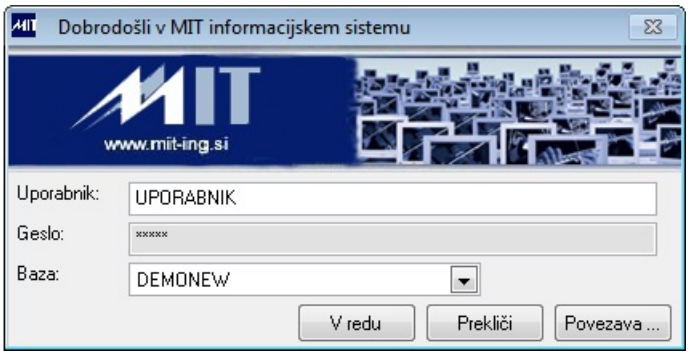
Prijava v program

Po zagonu kateregakoli programa IS se najprej prikaže vnosna maska za prijavo uporabnika. Program iz Windows okolja samodejno prebere:
- ime uporabnika, ki je trenutno prijavljen v računalnik in
- ime računalnika, na katerem se program poganja.

Uporabniško ime, ki je predlagano za vstop v sistem, je možno ob vstopu spremeniti, kar pomeni, da ni nujno enako imenu uporabnika, prijavljenega v mrežo ali imenu uporabnika poslovnega informacijskega sistema. Imena uporabnikov ne smejo biti daljša od osmih znakov (do predvidene spremembe).
Uporabniško ime ne sme imeti presledkov ali šumnikov. V primeru, da se uporabniško ime razlikuje z imenom iz Windows okolja si lahko v modulu Administracija - uporabniki - vnesemo domeno in windows uporabniško ime. Program bo prepoznal uporabniško ime Saop Proizvodnja glede na vneseno windows uporabniško ime. V primeru, da je polje Windows uporabnik prazno bo program ponudil Windows uporabniško ime, ki ga je potrebno spremeniti, če se razlikuje z Saop Proizvodnja uporabniškim imenom.

Za uporabniškim imenom je potrebno vnesti še geslo uporabnika. Geslo se preverja na nivoju Seyfor in ne na nivoju operacijskega sistema. Geslo

je obvezen podatek, če je sistem gesel in uporabnikov aktiviran. Sistem gesel uporabnikov je aktiviran s prvim vnosom uporabnika in gesla v tabelo uporabnikov skozi program Vadmin.exe, ki je namenjen skrbnikom sistema Saop Proizvodnja.



V programe lahko vstopamo preko (bližnjice) programa Saop Proizvodnja. V primeru, da imamo sistem več povezanih baz lahko na bližnjici določimo katera obstoječa baza se nam predlaga kot prva baza sicer se ponudi osnovna baza kot prva baza za izbor. Če je samo ena baza ali želimo bazo izbirati, naj bo pot cilja brez podatka o imenu baze.

Slika: Primer nastavitve bližnjice pri povezanih bazah

Uporabniki in gesla

Administracija uporabniških imen in gesel je možna v paketu Vadmin.exe. Program je namenjen skrbnikom informacijskih sistemov. V meniju Pravice se postavite na podmeni Gesla uporabnikov. Odpre se vam značilno okno za pregled. S tipko za dodajanje pozicij se vam ponudi vnosna maska:

Uporabnik : ime uporabnika, pod katerim se prijavlja v informacijski sistem

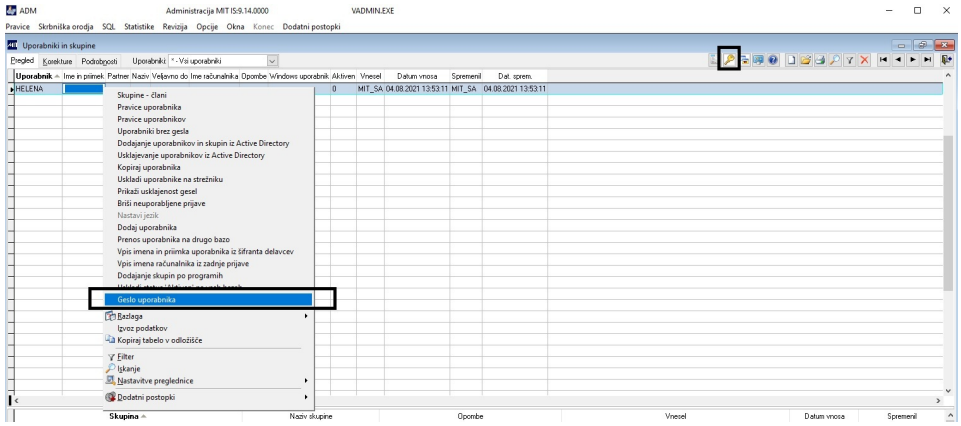
Geslo : geslo uporabnika, ki je kodirano in se pri vnosu na ekranu ne vidi. V pregledu so vidne številke, ki jih ni mogoče enostavno prevesti v znake, ki sestavljajo geslo, saj za njihovo kreiranje skrbi algoritem za naključno generiranje.

Ime in Priimek : vpišemo ime in priimek uporabnika ali drugo razpoznavno ime

Geslo je omogočeno zamenjati v okviru:
- programa Administracija / Uporabniki in skupine (ikona in podmeni med dodatnimi meniji)
- vsi programi v meniju Opcije / Okolje - Sprememba gesla

Uporabnik za spremembo gesla potrebuje pravico VSI.GESLO.

Če želimo uporabnika blokirati za uporabo (odhod iz podjetja...) je dodano polje Aktivno. V primeru, da je uporabnik označen, da je neaktiven=9, prijava v programe ni omogočena. Svetujemo pa še odvzem vseh pravic za takega uporabnika.



Povezovanje pravic z Uporabniki in Skupinami

V meniju Pravice se postavite na podmeni Pravice uporabnikov. Odpre se vam značilno okno za pregled. S tipko za dodajanje pozicij se vam ponudi vnosna maska, ki zahteva vnos imena-oznake pravice in uporabnika:

Pravica: oznaka-naziv pravice. V polje je možno vnesti oznako ene izmed pravic, ki so na voljo. Ena od pravic je tudi ADMIN. Namenjena je skrbnikom sistema. Omogoča vsa opravila v sistemu, brez omejitev.

Če oznak pravic ne poznate, je na voljo sistem pomoči, ki pokaže seznam oznak in kratkih opisov pravic. Podrobnejše informacije za posamezno pravico so na voljo v poglavjih navodil posameznih delov informacijskega sistema, na katerega se nanaša.

Uporabnik: uporabniško ime ali ime skupine

Maska: označimo dovoljena opravila ARWCDPGT (na podlagi MASKE pravice).

Postopek uvedbe sistema pravic

Sistem pravic v celotnem IS začne delovati takoj po namestitvi. Edini uporabnik, ki se lahko v sistem prijavi po namestitvi, je privzeti administrator MIT_SA. Zato je nujno potrebno, da pred pričetkom uporabe pripravimo vsaj spisek uporabnikov, ki jim želimo omogočiti vstop v sistem.

Takoj po namestitvi se prijavimo v administracijski modul ADM (Vadmin.exe) in vnesemo vsa želena uporabniška imena.

Prvi način:
- priprava seznama skupina, pravica, maska pravice
- priprava seznama skupina, uporabnik
- vnos seznama v sistem

Drugi način:
- kreiramo skupino ZACASNO, skupini dodelimo pravico ADMIN
- vse uporabnike dodelimo v skupino ZACASNO
- pripravimo sezname skupina, pravica
- vnesemo pripravljen seznam v sistem
- pripravimo seznam skupina, uporabniki
- vnesemo seznam v sistem
- uporabnike odstranimo iz skupine ZACASNO
- odstranimo skupino ZACASNO

Opredelitev pravic

Opredelitev pojma pravica:
- pravica je povezovalni element do objekta, ki ga pravica ščiti
- vsaka pravica ima svojo masko, ki opredeljujejo dovoljenja ali akcije, kaj lahko s posameznim objektom počnemo

Način označevanja pravic:
- oznake (imena pravic) so sestavljene iz dveh delov
- prvi del vsebuje oznako paketa, ki mu pravica pripada
- drugi del vsebuje kratko oznako pravice

Primer: VSI.ARTIKLI. Oznaka pravice pomeni: VSI - da gre za skupne datoteke (šifrante), ARTIKLI - da gre za tabelo artiklov.

Za lažjo orientacijo so določeni tudi opisi in nazivi pravic, da je uporabniku lažje poiskati primerno pravico.
Nabor možnih pravic se prikaže administratorju pri povezovanju:
- med uporabnikom in pravico
- med skupino in pravico

Priprava in umestitev baz na SQL strežnik

V primeru potrebe po arhivski ali testni bazi je potrebno upoštevati povezanost vseh baz, ki vsebujejo Saop Proizvodnja avtentikacijo uporabnika. Da bo zadeva lažje razumljiva, se Testna in Arhivska baza v nadaljevanju teksta imenuje z eni samim imenom Dodatna baza.

Imamo naslednje možnosti:
- Dodatno bazo postavimo znotraj istega SQL strežnika, kot je postavljena produkcijska baza
- Dodatno ali arhivsko bazo postavimo v novo instanco SQL strežnika (na dodatni instanci je lahko v takem primeru ena sama Saop Proizvodnja baza)

Za postavitev dodatne vzporedne baze je potrebno upoštevati način delovanja Saop Proizvodnja avtentikacije uporabnikov. V vseh vzporednih bazah morajo biti vsi Saop Proizvodnja uporabniki usklajeni z imeni uporabnikov v vzporednih bazah in z ustreznimi Login-i na SQL strežniku. Upoštevati je potrebno, da nobena od vzporednih Saop Proizvodnja baz ne sme biti postavljena v stanje ReadOnly (samo za branje).

Priprava vzporedne Dodatne baze

Na SQL strežniku obstaja produkcijska baza. Nekje v eni od starejših zaščitnih kopij imamo podatke, ki bi jih radi pregledovali, nikakor pa ne spreminjali.

Postopek priprave:

1. Na SQL strežniku postavimo novo bazo s primernim imenom (prepoznavna naj bo namembnost). Ime baze naj bo po možnosti brez presledkov, šumnikov in posebnih matematičnih znakov.

2. Izvedemo Restore podatkov v pripravljeno bazo.

3. V mapo poimenovano enako kot je imenovana dodatna baza, postavimo sistem s primernimi verzijami programov in spremljajočimi dodatki (izpisi ...).

4. V novi dodatni bazi pobrišemo vse User-je, ki se jim imen pričenjajo z "MIT_", pobrišemo aplikacijsko Vlogo MIT_APP, pobrišemo User-ja MIT_LOGIN.

5. Spraznimo tabele VSI_LOGIN (tu obvezno pustimo en sam prazen zapis), VSI_BAZAGRP,VSI_BAZAMAT ...

6 Če nobenega od korakov nismo izpustili, vstopimo v sistem dodatne baze s programom Vadmin.exe. Vanj se prijavimo z uporabniškim imenom MIT_SA in s pripadajočim geslom.

7 Na novo dodamo v sistem uporabnike in na novo jim dodelimo primerne pravice, ki bodo omogočale samo pregledovanje in morebitno izpisovanje, ne pa tudi spreminjanje podatkov.

8 V nobenem primeru pa ne smemo take dodatne baze označiti kor ReadOnly!

Primeri morebitnih težav:

Pri vnosu novega uporabnika v eno od Saop Proizvodnja baz skozi administracijski modul Vadmin.exe program javi napako. Pogost vzrok je dejstvo, da je ena od vzporednih Dodatnih baz "ReadOnly". Pri spremembi gesla obstoječega uporabnika v produkcijski bazi program javi nelogično napako. Najpogostejši razlog je, da je ena od vzporednih Dodatnih baz postavljena v stanje ReadOnly. Razlog gre iskati v dejstvu, da program za spremembo gesla mora uskladiti dodatno kriptirana gesla tudi v dodatnih vzporednih bazah, kjer se nahaja uporabnik z enakim imenom in je le-ta vezan na Login na SQL strežniku. Nobena Dodatna vzporedna baza ne sme biti v stanju ReadOnly!

Menjamo geslo uporabnika v produkcijski bazi. Geslo celo brez težav zamenjamo. Naslednji trenutek nas kliče uporabnik, ki se nikakor ne more prijaviti v eno od vzporednih dodatnih baz. Ugotovimo, da je vzporedna dodatna baza postavljena v stanje ReadOnly. Vzrok za nezmožnost prijave uporabnika v dodatno vzporedno bazo je neusklajenost gesla v tej bazi z geslom Login-a na SQL strežniku. Rešitev je, da nikdar ne uporabimo enakih uporabniških imen v vseh vzporednih Saop Proizvodnja bazah na istem strežniku, če to ni smiselno. Gesla uporabnikom vedno menjajmo izključno na produkcijski bazi.