Süsteemi register (System registry)

Windows'i süsteemi register on süsteemne hierarhiline andmebaas, kus säilitatakse kõiki operatsioonisüsteemi seadeid. Sellise andmebaasi pidamine võimaldab hoida kõigi programmide seadeid n.ö. „ühes kohas“ selle asemel, et kasutada iga programmi kohta eraldi seadistusfaili (näiteks vanemate programmide poolt kasutatud .ini failid).

Samuti võimaldab registri kasutamine kasutada Group Policy'd mis annab administraatorile võimaluse kontrollida nii lokaalse kui ka võrgus oleva arvuti ja erinevate installeeritud programmide seadeid. Lihtsam on ka seadetest varukoopia tegemine, seda siis kas kogu registri sisu eksportimise abil või registrifailide otsese kopeerimise teel. Kuna register loetakse korraga mällu on seal seadete väärtuste lugemine palju kiirem kui näiteks tekstifailist.

Samas toob register kaasa ka uusi probleeme. Näiteks on HKEY_LOCAL_MACHINE võti koos oma alamvõtmetega süsteemi jaoks nii oluline, et väiksemgi viga selle struktuuris võib muuta kogu operatsioonisüsteemi töökõlbmatuks. Tõsi küll sellise olukorra vältimiseks on loodud turvamehhanisme. Halb on ka see, et registrit ei saa dokumenteerida ja kommenteerida nagu tekstipõhiseid seadetefaile. Samuti on vigasaanud registri taastamine küllaltki raske ülesanne, sest tihti puudub sellises olukorras otsene juurdepääs andmetele.

Andmed on registris organiseeritud puu kujulisse struktuuri. Register koosneb:

- Võtmetest (key)
- Andmekirjetest (data entry)

Igal võtmel võib (kuid ei pruugi) olla temaga seotud andmekirjeid ning alamvõtmeid. Kokkukuuluvaid võtmeid ja andmekirjeid, millede jaoks on süsteemis olemas eraldi failid, kuhu neid salvestatakse, nimetatakse sülemiteks (hive).

Windows XP registris on järgmised sülemid:

Sülem:	**Sülemiga seotud failid:**
HKEY_LOCAL_MACHINE\SAM	Sam, Sam.log, Sam.sav
HKEY_LOCAL_MACHINE\Security	Security, Security.log, Security.sav
HKEY_LOCAL_MACHINE\Software	Software, Software.log, Software.sav
HKEY_LOCAL_MACHINE\System	System, System.alt, System.log, System.sav
HKEY_CURRENT_CONFIG	System, System.alt, System.log, System.sav, Ntuser.dat, Ntuser.dat.log
HKEY_USERS\DEFAULT	Default, Default.log, Default.sav

http://support.microsoft.com/kb/256986

Sülemitega seotud failid asuvad kataloogides:

- %SystemRoot%\System32\Config\
- %UserProfile%\
- %UserProfile%\Local Settings\Application Data\Microsoft\Windows\

Windows XP registri sisu on võimalik vaadata ja muuta operatsioonisüsteemiga kaasatuleva vahendi „Registry Editor“ (regedit32.exe) abil. Käivitades Registry Editor'i näeme lokaalses masinas viit registrivõtit:

Registrivõti	Kirjeldus
HKEY_CURRENT_USER	Sisaldab parajasti aktiivse kasutaja n.ö. „isiklikud“ seadeid. Näiteks on siin kirjas kõik Control Panel'i seaded. Tegelikult on tegemist HKEY_USERS võtme alamvõtmega.
HKEY_USERS	Sisaldab kõiki operatsioonisüsteemi sisseloginud kasutajaprofiilide seadeid.
HKEY_LOCAL_MACHINE	Sisaldab konkreetse arvuti seadeid. Kehtib kõigile kasutajatele,
HKEY_CLASSES_ROOT	On HKEY_LOCAL_MACHINE\Software alamvõti. Sisaldab informatsiooni, mille abil „windows exploreriga“ avatud fail avaneb või käivitatakse sobiva programmiga. Põhimõtteliselt seob faililaiendi programmiga, millega vaikimisi sellise laiendiga faile avatakse. Alates Windows 2000'st on see informatsioon nii HKEY_LOCAL_MACHINE kui ka HKEY_CURRENT_USER võtmete all. HKEY_LOCAL_MACHINE\Software\Classes Võti sisaldab informatsiooni, mis käib kõigi kohaliku masina kasutajate kohta samas kui HKEY_CURRENT_USER\Software\Classes võti sisaldab informatsiooni, mis kehtib aktiivse kasutaja kohta ja on tühistab kõigi kasutajat kohta käiva sama seade (kui selline seade on olemas). HKEY_CLASSES_ROOT võti esitab parajasti aktiivse kasutaja ja kõigi kasutajate kohta käiva vastava informatsiooni kombinatsiooni.
HKEY_CURRENT_CONFIG	Sisaldab informatsiooni arvuti riistvara ja sellega seotud seadete kohta.

http://support.microsoft.com/kb/256986

Windows Vista puhul on registriga seotud kaks olulist uuendust:

- Registry virtualization – registri virtualiseerimine võimaldab vältida mälus hoitava süsteemiregistri liiga suureks muutumist. Vaikimisi (ja kasutajale nähtamatult) suunatakse kasutaja õigustes tehtavad süsteemsete registrivõtmete alla suunatud muudatused ümber kasutaja registrivõtmete alla, kuid mälus hoitakse neid süsteemsete võtmete all. Kui kasutaja välja logib eemaldatakse mälust ka tema registrivõtmed (mis loomulikult salvestatakse, et need kasutaja sisselogides uuesti laadida).
- Transactional Registry – sarnaselt transaktionaalse failisüsteemiga on süsteemituuma tasemel võimalik registrimuudatusi tagasi võtta. See võimaldab veasituatsioonide korral vältida registrisse pooliku või süsteemi käitumist vigaseks muutva info kirjutamist.

Muudatuste tegemine registrisse

Register on ülioluline osa Windows operatsioonisüsteemist, seega tuleb igasuguste muudatustega olla ettevaatlik. Enne muudatuste tegemist on mõistlik teha registrist tagavarakoopia. Registrist tagavarakoopia tegemine

1) Käivita regedit32.exe
2) Vali menüüst Fail>Export...
3) Avanenud aknas märgi ära valik „Export range – all“, pane tagavarakoopiale sobiv nimi ning määra ära loodava faili asukoht.
4) Vajuta „Save“

Registrivõtme või andmekirje lisamine

1) Käivita regedit32.exe
2) Vali aknas vasakul olevast puustruktuurist võti, millele soovid lisada alamvõtit või andmekirjet.
3) Vali menüüst Edit > New ja vastavalt soovile kas „Key“ (võtme lisamiseks) või sobiv kirje andmetüüp (andmekirje lisamiseks). Vastavalt valikule luuakse uus võti või andmekirje, millele tuleb anda sobiv nimi. Andmekirje loomise puhul tuleb peale nime sisestamist sisestada ka kirje väärtus. Seda saab teha tehes kirjel topeltkliki.

Registrivõtme või andmekirje leidmine

1) Käivita regedit32.exe
2) Vali menüüst edit > find
3) Avanenud aknas märgi ära, kas otsida võtmete, andmekirjete või andmekirjete väärtuste

seast. Lisage otsitav fraas ning vajutage „Find“. Peale esimese sobiva vaste leidmist saab liikuda järgmise sobiva vaste juurde vajutades F3.

Registrivõtme või andmekirje muutmine

1) Käivita regedit32.exe
2) Vali sobiv registrivõti või andmekirje
3) Vali menüüst edit>rename (võtme või kirje nime muutmiseks) või edit>modify (kirje väärtuse muutmiseks)

Registrivõtme või andmekirje kustutamine

1) Käivita regedit32.exe
2) Vali sobiv registrivõti või andmekirje
3) Vali menüüst edit>delete

Registrivõtmete eksportimine ja importimine

1) Käivita regedit32.exe
2) Vali registrivõti mida soovid eksportida (koos võtmega eksporditakse kõik selle võtme alamvõtmed ning nende juurde kuuluvad andmekirjed oma väärtustega)
3) Vali menüüst Fail>Export
4) Avanenud aknas kontrolli, et oleks valitud valik „Export range – selected branch“ (tekstiväljal on kirjas ka valitud võti). Anna failile nimi ning vajuta „Save“

1) Käivita regedit32.exe
2) Vali menüüst Fail>Import
3) Avanenud aknast otsi vajalik registrivõtmeid ja andmekirjeid sisaldav fail ning vajuta „open“

Süsteemi registrist tagavarakoopia tegemine ja sellest taastamine

Windows XP:

Eraldi töövahendit Registrist varukoopia tegemiseks Windows XP-ga kaasa ei tulu, kuid vajadusel on võimalik käsitsi luua System Restore Point, mis sisaldab ka registrit.

1) Käivitame töövahendi rstui.exe (c:\windows\system32\restore\rstui.exe). Kui system restore teenus on välja lülitatud tuleb see enne sisse lülitada – selle kohta kuvatakse vajadusel ka teade.
2) Avanenud aknas valige "Create a restore point" ja vajutage Next.
3) Andke loodavale Restore Point'ile nimi ja vajutage "Create"

Restore point loodi kataloogi "C:\System Volume Information". Seda, millised failid ja registrivõtmed Restore Point'ist välja jäetakse, saab kontrollida järgnevate registrivõtmete alt:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\FilesNotToBackup
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\BackupRestore\KeysNotToRestore

Registri taastamine:

1. Käivitame töövahendi rstui.exe (c:\windows\system32\restore\rstui.exe). Kui system restore teenus on välja lülitatud tuleb see enne sisse lülitada – selle kohta kuvatakse vajadusel ka teade.
2. Avanenud aknas valige „Restore my computer to an earlier time" ja vajutage Next
3. valige sobiv restore point ja vajutage Next
4. Ilmub hoiatav ekraan, mis teatab, et süsteemi seaded taastatakse valitud ajahetke seisuga ja arvutile tehakse restart. Valige Next.

Windows Vista:

1. Start menüüs kirjutage Start Search ribale „systempropertiesprotection".
2. Avanenud „System Properties" dialoogiaknas valige „System Protection" sakk ja vajutage „Create"
3. Andke Restore Point'ile nimi ja vajutage „Create"
4. Restore Point'i eduka loomise kohta kuvatakse teade.

Registri taasatamine:

1. Start menüüs kirjutage Start Search ribale „systempropertiesprotection“.
2. Avanenud „System Properties“ dialoogiaknas valige „System Protection“ sakk ja vajutage „System Restore“
3. Avanenud „System Restore“ dialoogiaknas valige „Choose a differest restore point“ ja vajutage Next
4. Valige teile sobiv Restore Point ja vajutage Next
5. Kinnitage oma valikuid vajutades Finish

Registration Entries (.reg) failid

Faililaiend .reg on Windows XP puhul vaikimisi määratud tähistama Registration Entries tüüpi faile. Tegemist on tekstifailidega, mis sisaldavad kokkulepitud formaadis registrivõtmeid ja andmekirjeid. Süntaks on järgmine:

RegistryEditorVersion
Blank line
[RegistryPath1]
"DataItemName1"="DataType1:DataValue1"
„DataItemName2"="DataType2:DataValue2"
Blank line
[RegistryPath2]
"DataItemName3"="DataType3:DataValue3"

RegistryEditorVersion - „Windows Registry Editor Version 5.00" kui tegemist on Windows 2000 või XP registrivõtmetega või „REGEDIT4“ kui tegemist on Windows 95 või 98 registrivõtmetega.
[RegistryPath] – Registrivõtme nimi koos tema ülemvõtmete nimedega.
DataItemName – andmekirje nimi
DataValue – Andmekirje andmetüübile vastavas formaadis väärtus
DataType – Andmekirje andmete tüüp.

Võimalikud .reg faili andmetüübid on:

Nimi	Andmetüüp	Kirjeldus
Binaarväärtus	REG_BINARY	Binaarsed toorandmed. Suuremat osa riistvarakomponentide teabest talletatakse binaarandmetena ja kuvatakse registriredaktoris kuueteistkümnendvormingus.
Väärtus DWORD	REG_DWORD	Andmed, mida tähistab nelja (4) baidi pikkune arv (32-bitine täisarv). Paljud seadmedraiverite ja teenuste parameetrid on seda tüüpi ning need kuvatakse registriredaktoris binaar-, kuueteistkümnend- või kümnendvormingus. Seotud väärtused on DWORD_LITTLE_ENDIAN (tähtsusetuim bait asub madalaimas aadressis) ja REG_DWORD_BIG_ENDIAN (tähtsusetuim bait asub kõrgeimas aadressis).
Laiendatav stringiväärtus	REG_EXPAND_SZ	Muutujapikkune andmestring. See andmetüüp hõlmab muutujaid, mis lahendatakse siis, kui mõni programm või teenus neid andmeid kasutab.
Mitmest stringist koosnev väärtus	REG_MULTI_SZ	Mitmene string. Seda tüüpi on tavaliselt väärtused, mis sisaldavad loetavas vormis loendeid või mitut väärtust. Kirjed on eraldatud tühikute, komade või muude märkidega.
Stringi väärtus	REG_SZ	Kindla pikkusega tekstistring
Binaarväärtus	REG_RESOURCE_LIST	Pesastatud massiivide jada, mis on ette nähtud sellise ressursiloendi talletamiseks, mida kasutab riistvara seadmedraiver või füüsiline seade, mida see juhib. Süsteem tuvastab need andmed ja kirjutab puusse \ResourceMap ning need kuvatakse registriredaktoris kuueteistkümnendvormingus binaarväärtusena.
Binaarväärtus	REG_RESOURCE_REQUIREMENTS_LIST	Pesastatud massiivide jada, mis on mõeldud seadmedraiveri võimalike riistvararessursside loendi salvestamiseks, mida see draiver või mõni selle kontrollitavatest füüsilistest seadmetest saab kasutada. Süsteem kirjutab selle loendi alamhulga puusse \ResourceMap. Süsteem tuvastab need andmed ning need kuvatakse registriredaktoris kuueteistkümnendvormingus binaarväärtusena.
Binaarväärtus	REG_FULL_RESOURCE_DESCRIPTOR	Pesastatud massiivide jada, mis on mõeldud ressursiloendi salvestamiseks, mida kasutab füüsiline riistvaraseade. Süsteem tuvastab need andmed ja kirjutab puusse \HardwareDescription ning need kuvatakse registriredaktoris kuueteistkümnendvormingus binaarväärtusena.
Mitte ühtegi	REG_NONE	Kindla tüübita andmed. Need andmed kirjutab registrisse süsteem (või teevad seda rakendused) ning need kuvatakse registriredaktoris kuueteistkümnendvormingus binaarväärtusena.
Link	REG_LINK	Unicode-string, mis on sümboolse lingi nimi.
Väärtus QWORD	REG_QWORD	Andmed, mida tähistab 64-bitine täisarv. Need andmed kuvatakse registriredaktoris binaarväärtusena ning neid kasutati esmakordselt opsüsteemis Windows 2000.

Ülaltoodud viisil kirja pandud .reg fail lisab käivitamisel vastavad võtmed ja andmekirjed registrisse. Samas on võimalik .reg fail kirjutada ka viisil, et käivitamisel vastavad võtmed ja andmekirjed hoopis kustutatakse.

Registrivõtme kustutamiseks tuleb vastava registrivõtme nime ette kirjutada miinusmärk.

Näiteks: [HKEY_LOCAL_MACHINE\Software\Test]

Andmekirje kustutamiseks tuleb kohe andmekirje nimele järgneva võrdusmärgi taha kirjutada miinusmärk. Näiteks: "TestValue"=-

Registrivõtmete juurdepääsuõigused

Sarnaselt NTFS failisüsteemile on Windows XP registrivõtmetel juurdepääsuõiguste süsteem, mis reguleerib kasutajale õigusi registrivõtmete suhtes (võtme juures olevaid andmekirjeid loetakse registrivõtmega kokkukuuluvaks, neile eraldi õigusi ei määrata). Kuna register on sarnaselt failisüsteemile ülesehitatud puukujuliselt, siis toimub õiguste määramine ja pärimine täpselt samal viisil kui failisüsteemi juures.

Harjutus

1. Lisage võtmele [HKEY_LOCAL_MACHINE\Software] alamvõti „test“
2. Lisage loodud võtmele andmekirje nimega „kirje1“ väärtusega 1 (andmetüüp DWORD)
3. Eksportige loodud võti faili „key1.reg“
4. Leidke parajasti aktiivsele Windows XP kasutajale kehtivad Windows Movie Maker seaded (vastav võti, selle alamvõtmed ja nende juurde kuuluvad andmekirjed). Eksportige need faili „moviemaker.reg“
5. Kopeerige fail „key1.reg“ faili „key2.reg“. Muutke faili „key2.reg“ faili sisu nii, et käivitades kustutatakse võti „test“ ja andmekirje „kirje1“. Veenduge, et faili käivitamisel vastavad andmed tõesti kustutati.