



WINDOWS სისტემების ადმინისტრირება



შესავალი

წინამდებარე სახელმძღვანელო შედგენილია პროფესიული სტუდენტებისათვის, საგანმანათლებლო პროგრამის „სისტემების ადმინისტრატორი“ სწავლებისათვის და მოიცავს ამ პროგრამით გათვალისწინებულ Windows Server სისტემაზე დაფუძნებულ ძირითად მოდულებს.

სახელმძღვანელოს მიზანია დაეხმაროს სტუდენტს დაეუფლოს სისტემების ადმინისტრირების პრინციპებს და შეძლოს მისი ეფექტური გამოყენება პროფესიულ საქმიანობაში. სახელმძღვანელოში მოცემული საკითხები საინტერესო და აქტუალური იქნება სისტემების ადმინისტრატორებისათვის, სახელმძღვანელოში მოცემული ინსტრუმენტების გამოყენება შესაძლებელია, როგორც სწავლების, ასევე დასაქმებისა და ყოველდღიური საქმიანობის პირობებში.

სახელმძღვანელოში აღწერილია მიმდინარე პერიოდში აქტუალური და ფართოდ გამოყენებადი პროგრამულ-აპარატურული უზრუნველყოფის ელემენტები და სერვისები.

სახელმძღვანელო დაყოფილია 6 ნაწილად (თავი). ყოველი თავი შეესაბამება კონკრეტული მოდულის დასახელებას, შესაბამისი ქვეთავები კი ეხმაურება მოდულის ჩარჩოთი განსაზღვრულ სწავლის შედეგებს. თითოეულ ნაწილში თემატურ ტექსტურ-ილუსტრირებულ მასალასთან ერთად წარმოდგენილია სავარჯიშოები, სახელმძღვანელოს ყოველი თავის ბოლოს შეფასების მიდგომებიდან გამომდინარე დართული აქვს შემაჯამებელი სამუშაო, პრაქტიკული დავალება-სავარჯიშო ან/და ტესტის ნიმუში.

რეცენზენტები:

ეკატერინე ჩიკაშუა

ასოც. პროფესორი, საგანმანათლებლო პროგრამის შემმუშავებელი ჯგუფის წევრი

ვლადიმერ ადამია

ასოც პროფესორი, სტუ-ს კომპიუტერული ქსელის ადმინისტრატორი

სარჩევი

1. სერვერული ინფრასტრუქტურის გამართვა.....	6
სერვერული სისტემის ზოგადი მიმოხილვა	6
1.1. სერვერული აპარატურის კომპლექტაცია	12
1.2. Windows სერვერული ოპერაციული სისტემების ინსტალაცია.....	21
1.3. სერვერული ინფრასტრუქტურის მომსახურება/განვითარება	35
1.3.1. ინფორმაციის მრავალდონური შენახვის მეთოდები.....	38
1.3.2. მონაცემთა საცავები.....	42
1.3.3. მონაცემთა დამუშავების ცენტრი	45
1.3.4. კლასტერული არქიტექტურა.....	46
პრაქტიკული სავარჯიშო.....	49
ცოდნის შეფასება	49
2. დირექტორიების სერვისების გამართვა.....	54
2.1. ცენტრალური დირექტორიების სერვისების (Directory Service) ადმინისტრირება	61
2.2. დომენური სახელების სერვერის (DNS) ადმინისტრირება	65
2.3. ქსელური მისამართების მართვის სისტემის (DHCP) ადმინისტრირება	68
პრაქტიკული სავარჯიშო.....	73
ცოდნის შეფასება	73
3. კლიენტებისა და სერვერების ვირტუალიზაცია	85
3.1. ვირტუალური პროგრამული უზრუნველყოფის (Hypervisor) კონფიგურაცია.....	85
3.2. VMware Workstation-ის ინსტალაცია	107
3.3. ვირტუალური მანქანის შექმნა	108
3.4. ვირტუალური მანქანის პარამეტრების კონფიგურაცია	122
3.5. ვირტუალიზაციის Hypervisor-ების მართვა და მონიტორინგი	128
3.5.1. ქსელის მართვის ორგანიზაცია ვირტუალურ მანქანებს შორის.....	128
3.6. უსაფრთხოების უზრუნველყოფა ვირტუალურ გარემოში.....	140
პრაქტიკული სავარჯიშო.....	153
ცოდნის შეფასება	153
4. ვებ, ფაილური და მონაცემთა ბაზის სერვერების გამართვა	155
4.1. ვებ-სერვერული ინფრასტრუქტურის აწყობა და მართვა.....	155
4.1.1. ვებ-ინფრასტრუქტურის აგებულება	155

4.1.1.1.	ვებ-სერვერის აქტივაცია და მართვა Internet Information Server-ის გარემოში	160
4.1.1.2.	ვებ-აპლიკაციების მართვა MS SharePoint-ის გარემოში	164
4.1.1.3.	სისტემის დაყენება და გამართვა	166
4.1.1.4.	SharePoint-სერვისების ნიმუშები	169
4.1.2.	მონაცემთა მართვისა და ძებნის სერვისები	171
4.1.3.	მომხმარებელთა მართვა	174
4.2.	ფაილური, ბეჭდვის და სკანირების სერვისის მართვა	176
4.2.1	ფაილური სერვისის ძირითადი ფუნქციები	176
4.2.2	ფაილური სერვისის სარგებლიანობის და საიმედოობის უზრუნველყოფა	182
4.3.	მონაცემთა ბაზების სერვერული გარემოს მომზადება	186
4.3.1.	შესავალი რელაციური მონაცემთა ბაზების მართვის სისტემებში	186
4.3.2.	SQL Server-ის ინტერფეისი	189
4.3.3.	მონაცემთა ბაზების მაღალსარგებლიანობის უზრუნველყოფა	192
4.3.4.	მონაცემთა ბაზების სარეზერვო კოპირება	195
	პრაქტიკული სავარჯიშო.....	199
	ცოდნის შეფასება	200
5.	საფოსტო და საკომუნიკაციო სერვერების გამართვა	202
5.1.	საფოსტო სერვერის მართვა	202
5.1.1.	საფოსტო და საკომუნიკაციო სერვისების ზოგადი მიმოხილვა	202
5.2.	შიდა კომუნიკაციის პროგრამული უზრუნველყოფის სერვერების მართვა	204
5.2.1.	საფოსტო სერვისის მართვა Microsoft Exchange Server-ის გარემოში	204
5.2.1.1.	Exchange Server-ის სტრუქტურა.....	204
5.2.1.2.	წესების მართვა MS Exchange Server-ის გარემოში	210
5.2.1.3.	სპამის მოგერიების მეთოდები ელექტრონული ფოსტის სერვისებში	214
5.2.2.	მცხირე შეტყობინებათა სერვისის მართვა MS Lync-ის გარემოში.....	216
5.2.2.1.	5.3.1 Lync 2010-ის არქიტექტურა.....	216
5.3.	სპეციფიკური კლიენტ სერვისების მართვა	220
5.3.1.	Lync 2010-ის დანერგვა	220
5.3.1.1.	Lync 2010-ის მართვის პანელი.....	224
5.3.1.2.	ჯგუფური შეხვედრების ორგანიზება (კონფერენსინგი)	225
5.3.1.3.	MS System Center-ის ზოგადი მიმოხილვა.....	229

5.3.1.4.	Configuration Manager-ის დაყენება და გამართვა.....	231
5.3.1.5.	მოთხოვნების ფორმირება WQL-ენის საშუალებით.....	234
5.3.2.	რეპორტი 239	
	პრაქტიკული სავარჯიშო.....	241
	ცოდნის შეფასება	241
6.	კონტროლისა და მონიტორინგის სისტემები.....	244
6.1.	დაშორებული წვდომის სერვისების (Remote Access) ადმინისტრირება	244
6.2.	ინტერნეტის კონტროლის და უსაფრთხოების სისტემების (Proxy, Firewall) ინსტალაცია 252	
6.3.	სარეზერვო ასლების ადმინისტრირება	273
6.3.1	Acronis True Image Home პროგრამის მიმოხილვა	278
6.3.1.1	Acronis True Image -ის ინსტალაცია და აქტივაცია	286
6.3.1.2	მონაცემთა სარეზერვო ასლის შექმნა.....	291
6.3.1.3	ელექტრონული ფოსტის სარეზერვო კოპირება.....	298
6.3.1.4	ოპერაციული სისტემის სარეზერვო ასლის შექმნა Flash ან CD/DVD ჩამტვირთავი მედია საშუალებით	330
6.4	არსებული სისტემების მონიტორინგი.....	363
	პრაქტიკული სავარჯიშო.....	372
	ცოდნის შეფასება	372
	დასკვნა.....	375
	გამოყენებული ლიტერატურა.....	376

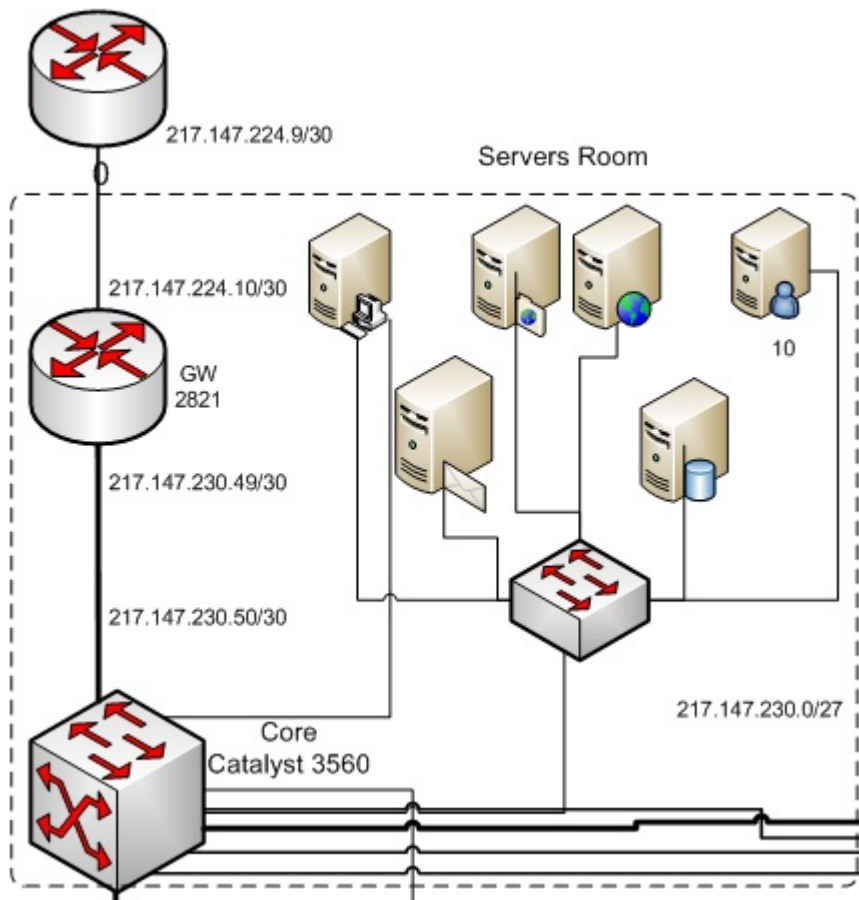
1. სერვერული ინფრასტრუქტურის გამართვა

სერვერული ინფრასტრუქტურის გამართვა გულისხმობს შესაბამისი ძირითადი აპარატურული და სისტემური პროგრამული უზრუნველყოფის ინსტალაციას. მოცემულ თავში განვიხილავთ სერვერული სისტემებისთვის დამახასიათებელ თავისებურებებს, აპარატურული კომპლექტაციის წესებს და სისტემური პროგრამული უზრუნველყოფის ინსტალაცია-გამართვის მექანიზმებს.

მოცემული თავის გაცნობის შემდგომ, სტუდენტი შეძლებს სერვერული ინფრასტრუქტურის მოწყობას, მისი აპარატურული და პროგრამული უზრუნველყოფის გამართვის გზით.

სერვერული სისტემის ზოგადი მიმოხილვა

კორპორაციული სერვერული სისტემა ორ ძირითად ქვესისტემად შეიძლება დაყვით: საკუთრივ სერვერული და გარემოსთან ურთიერთობის ანუ ქსელური ქვესისტემები (სურ. 1).



სურ. 1 სერვერული და ქსელური ქვესისტემების ფრაგმენტი

სერვერული სისტემის ქსელური ქვესისტემა მოიცავს მაგისტრალურ და სხვა ტიპის ქსელურ აპარატურას (რუთერები, მე-3 დონის კომუტატორები, კონვერტირების მოწყობილობები და სხვა), რომლებიც ინტერნეტთან მიერთებას და კორპორაციული ქსელის სხვადასხვა სეგმენტების ურთიერთკავშირს უზრუნველყოფენ. სერვერული სისტემა ქსელის მომხმარებელთათვის განკუთვნილი მრავალფეროვანი სერვისების (ფაილ-სერვისი, მონაცემთა ბაზები, ელექტრონული ფოსტა, ვები და სხვა) განთავსებისა და მართვის ამოცანას ემსახურება.

სტანდარტული სერვერული სისტემა თითოეული სერვისისთვის, როგორც წესი, ცალკე ფიზიკური მანქანის ან მანქანების (სერვერების) გამოყოფას ითვალისწინებს. შეზღუდული რესურსების არსებობისას შეიძლება რამდენიმე სერვისი ერთსა და იმავე სერვერზე იყოს განთავსებული. არსებობს საკმაოდ მოქნილი მეთოდები მონაცემთა საიმედო შენახვისა და ინფორმაციასთან უწყვეტი წვდომის უზრუნველსაყოფად, თუმცა მოცემული მიდგომა მაინც საკმაოდ „ხისტია“ და გააჩნია რიგი ნაკლოვანებებისა, რომელთაგან უპირველესად რესურსების უყარათო ხარჯვა უნდა მივიჩნიოთ. სერვერული სისტემის პირველადი არქიტექტურა მეტნაკლებად ითვალისწინებს ყოველი სერვერის წინაშე მდგარ სარესურსო მოთხოვნებს, თუმცა ორგანიზაციის ინფორმაციული მოთხოვნების გაზრდის კვალდაკვალ სერვერული სისტემების მათზე მორგება საკმაოდ შრომატევადი საქმეა და მნიშვნელოვან ფინანსურ და შრომით დანახარჯებათანაა დაკავშირებული.

ბოლო წლებში განვითარებული რამდენიმე ტექნოლოგიის (ვირტუალიზაცია, კლასტერული არქიტექტურა, ინფორმაციის მრავალდონური შენახვა) წყალობით აღნიშნულ ამოცანათა მეტი ეფექტურობით გადაჭრა გახდა შესაძლებელი. ქვემოთ თითოეული მათგანის მოკლე აღწერაა მოცემული.

ვირტუალიზაცია

ვირტუალიზაციის თეორიული და პრაქტიკული ასპექტები ჯერ კიდევ გასული საუკუნის 70-იან წლებში იქნა დამუშავებული ფირმა **IBM**-ის სუპერმანქანებისთვის. სისტემის ყოველ მომხმარებელს მთლიანი სერვერიდან გამოეყოფოდა რესურსების საკუთარი ნაკრები და უქმნიდა გამოყოფილ გამოთვლით სისტემასთან მუშაობის ილუზიას.

2000-იან წლებში იდეა ხელახლა გახდა აქტუალური, განსაკუთრებით სერვერულ სისტემებში, თუმცა ზოგადად ტერმინი „ვირტუალიზაცია“ ბევრად ფართო შინაარს ატარებს. ვირტუალურად შეიძლება ვაქციოთ გამოთვლითი სისტემის პრაქტიკულად ყველა კომპონენტი, როგორც აპარატული, ასევე პროგრამული (მაგალითად, ოპტიკური დისკამპრავები, ქსელური ინტერფეისები, ოპერატიული მეხსიერება, ოპერაციული სისტემები და ასე შემდეგ).

სერვერის ვირტუალიზაცია ერთ ფიზიკულ სერვერზე რამდენიმე ვირტუალური სერვერის გაშვებას გულისხმობს. ვირტუალური მანქანები ან სერვერები წარმოადგენენ პროგრამებს, რომლებიც ეშვებიან ფიზიკური, ე.წ. "მასპინძელი" ოპერაციული სისტემის ფარგლებში (ჰოსტ-სერვერი). თავის მხრივ, ყოველი ვირტუალური მანქანა წარმოადგენს დამოუკიდებელ ოპერაციულ სისტემას, საკუთარი პროგრამებით და სერვისებით.

ვირტუალიზაციის შედეგად მიღებული ეკონომიკური ეფექტი უდავოა. დიდი სერვერული სისტემა (მონაცემთა დამუშავების ცენტრი) ვრცელ ფართობზე განთავსებული და ელექტრო ენერჯის დიდ რაოდენობას მოიხმარს, განსაკუთრებით მაშინ, როცა ცენტრს გაციების სპეციალური სისტემები და დამატებითი ინფრასტრუქტურა ემსახურება. ვირტუალიზაციის გამოყენება რამდენიმე ფიზიკური სერვერის ერთ მძლავრ სერვერზე „შეფუთვის“ საშუალებას იძლევა, რითაც იზოგება ადგილი და მცირდება ელექტროენერჯის ხარჯი. ამასთან მცირდება აპარატურაზე საერთო დანახარჯებიც ნაკლები რაოდენობის სერვერთა არსებობის გამო.

შეგვიძლია ჩამოვთვალოთ ვირტუალური სისტემების სხვა უპირატესობებიც ფიზიკურ სისტემებთან შედარებით, განსაკუთრებით კომპიუტერული ქსელების სერვერული ინფრასტრუქტურის აგებისა და მართვის თვალსაზრისით:

- ერთ გამოთვლით სისტემაში ერთზე მეტი ოპერაციული სისტემის პარალელური მუშაობა;
- კრიტიკული რესურსების (პროცესორის დრო, ოპერატიული და გარე მეხსიერება) ოპტიმალური განაწილება ვირტუალურ მანქანებს შორის;
- ოპერაციული სისტემების სწრაფი გადატანა ფიზიკურ ჰოსტებს შორის. ოპერაციული სისტემების ინსტალაციისა და კონფიგურირების დროითი დანახარჯების შემცირება წინასწარ მომზადებული ვირტუალური სისტემების (იმიჯების) ხარჯზე.

გვერდს ვერ ავუვლით ძირითად ნაკლოვანებებსაც, რაც ვირტუალურ სისტემებს ახასიათებთ:

- სერვერულ რესურსებზე მაღალი მოთხოვნები - ვირტუალური მანქანა ფაქტობრივად დამოუკიდებელ ოპერაციულ სისტემას წარმოადგენს და გამოთვლითი რესურსებიც პრაქტიკულად ფიზიკური მანქანის მასშტაბებით სჭირდება, ანუ ბევრად მეტი, ვიდრე ამას სტანდარტული პროგრამები მოითხოვენ;

- დამოკიდებულება ერთ ფიზიკურ სერვერზე, რომლის მწყობრიდან გამოსვლაც მასზე არსებული ყველა ვირტუალური მანქანის მწყობრიდან გამოსვლის ტოლფასია.

ბოლო პრობლემის აღმოფხვრა ვირტუალიზაციისა და კლასტერული არქიტექტურის ურთიერთშერწყმით ხდება შესაძლებელი, რაც მოცემული ნაშრომის ერთერთ ძირითად საგანს წარმოადგენს.

ვირტუალიზაციის პროცესი საკმაოდ კომპლექსურია და რამდენიმე ამოცანის გადაჭრას ითხოვს:

იზოლირება ვირტუალიზაციის მნიშვნელოვანი კომპონენტია და ვირტუალური სისტემების სრულ ურთიერთდამოუკიდებლობაში მდგომარეობს. ერთი ვირტუალური მანქანის მწყობრიდან გამოსვლას მეორის მუშაობაზე არავითარი გავლენის მოხდენა არ შეუძლია. კერძოდ, ფიზიკურ სერვერზე განთავსებულ ვირტუალურ მანქანებს შორის მონაცემთა არანაირი ერთიანი სივრცე არ არსებობს. მათ შორის ინფორმაციის ნებისმიერი ტრანსფერი ჩვეულებრივი ქსელური ინტერფეისების გავლით ხორციელდება.

ინკაპსულაცია ნიშნავს მთლიანი ვირტუალური სისტემის ერთ (ან მეტ) ჩვეულებრივ კომპიუტერულ ფაილში ინტეგრირებას. ამგვარი სისტემები მეტად მოქნილია ფიზიკურ სისტემებს შორის გადატანის, კოპირებისა თუ არქივირების ოპერაციების შესრულებისას.

გამოთვლითი მანქანების ვირტუალიზაციისას განიხილავენ 2 მთავარ კომპონენტს: მასპინძელ (**Host**) და სტუმარ (**Guest**) სისტემებს, ამასთან მასპინძელი ერთია და როგორც წესი, ფიზიკურ გამოთვლით სისტემას წარმოადგენს, ხოლო სტუმარ-სისტემები მასზე განთავსებული 1 ან მეტი ვირტუალური მანქანებია.

ცხადია, ამგვარი მარტივი სტრუქტურა გამოსადეგია მხოლოდ დესკტოპ-სისტემებისთვის, სადაც მომხმარებელს რამდენიმე ოპერაციული სისტემის

ერთდროული გამოყენება სჭირდება. იგი ასაგებად საკმაოდ ადვილია, თუმცა რამდენიმე ამოცანის გადაჭრას მაინც საჭიროებს. ეს ზოგადი ამოცანები ნებისმიერი ვირტუალური ინფრასტრუქტურის ფარგლებში წარმოიშობა და მათი განხილვა აუცილებელია:

- **სტუმარ-სისტემათა შაბლონების აგება** - წარმოადგენს პროცედურას, რომელსაც ვირტუალური სისტემის ასაგებად საჭირო დროითი დანახარჯების მნიშვნელოვნად შემცირება ძალუძს. ყოველი სტუმარ-ოპერაციული სისტემისთვის (**Windows, LINUX, Mac OS X** და სხვა) იქმნება საბაზისო კონფიგურაცია, რომელიც შემდეგ ყოველი კონკრეტული მოთხოვნის მიხედვით ფართოვდება;

- **ვირტუალური სისტემების კოპირება ან კლონირება** – კოპირების ოპერაცია ვირტუალური სისტემის ჩვეულებრივი ასლის აგებას გულისხმობს და ნაკლებად ეფექტურია, რადგან მასპინძელ-სისტემის გარე მეხსიერების სწრაფ გავსებას იწვევს. ბევრად უფრო მოქნილი კლონირების მექანიზმი მომხმარებელს არჩევანს უტოვებს: სრული კლონირებისას ვირტუალური მანქანის სრული და დამოუკიდებელი ასლი იქმნება, ხოლო ბმული (ლინკირებული) კლონირება საწყის ვირტუალურ მანქანას ეყრდნობა (მის მოდიფიკაციას წარმოადგენს) და მეხსიერების მინიმალურ ხარჯვას სჯერდება;

- **სკრინშოტების შექმნა** – სკრინშოტი ვირტუალური სისტემის მიმდინარე მდგომარეობას ეწოდება და საჭიროების მიხედვით სისტემის მოცემული მდგომარეობის აღდგენას განაპირობებს;

- **ფიზიკური მანქანების ვირტუალიზაცია** – გულისხმობს არსებული ფიზიკური სისტემების ვირტუალურ ინფრასტრუქტურაში მიგრაციას ვირტუალური მანქანების სახით.

- **რესურსების განაწილება მასპინძელ და სტუმარ სისტემებს შორის** – გულისხმობს მასპინძელ-სისტემის რესურსების (პროცესორული სიმძლავრეები, ოპერატიული და გარე მეხსიერება, დისკამპრავები, ქსელური ინტერფეისები) სტუმარ-სისტემებზე გადანაწილებას. ეხება პირველ რიგში ქსელურ რესურსებს (სისტემის უნიკალური ქსელური **MAC**-მისამართი, **IP**-მისამართი).

ზემოთ აღწერილი ამოცანების პრაქტიკული რეალიზაციის პროცესი სადღეისოდ საკმაოდ შორს არის წასული. ვირტუალიზაციის პროგრამული პროდუქტები (ფირმა

VMWare-ის ESX Server, vSphere და Workstation; ფირმა Citrix-ის XenApp, ფირმა Microsoft-ის Hyper-V, Virtual Server, Virtual PC, ფირმა Oracle-ის VirtualBox) მოიცავენ ინსტრუმენტების ფართო ნაკრებს სხვადასხვა (მათ შორის კორპორაციული) მასშტაბის კომპიუტერული ქსელების სერვერულ სისტემათა ვირტუალიზაციისთვის. საყურადღებოა, რომ ამ ინსტრუმენტების ნაწილი არსებული ფიზიკური ინფრასტრუქტურის უმტკივნელოდ "გავირტუალებს" საქმეს ემსახურება, რაც ორგანიზაციებს საშუალებას აძლევს თავიანთი სერვერული ინფრასტრუქტურის მოდერნიზაცია და ვირტუალურ რელსებზე გადაყვანა ძირითადი საწარმოო პროცესის შეწყვეტის გარეშე შეასრულონ.

საილუსტრაციოდ განვიხილოთ ვირტუალიზაციის ერთერთი სრული პროგრამული პაკეტი (ფირმა **VMWare**) და მისი მთავარი კომპონენტები:

- **ჰაიპერვაიზორი VMware ESX (ESXi) Server** - ჰოსტ-სისტემის მმართველი პროგრამა (იხილეთ ქვემოთ);

- **VMWare Converter** - ფიზიკური გამოთვლითი სისტემების ვირტუალიზაციის ან ვირტუალური მანქანების სხვადასხვა ფორმატებში კონვერტირების ინსტრუმენტი;

- **VMotion** – ვირტუალური მანქანების მიგრაცია სერვერებს შორის მათი გამორთვის გარეშე;

- **Virtual SMP** - სტუმარ-სისტემის 4-ზე მეტ პროცესორთან მუშაობის უზრუნველყოფა.

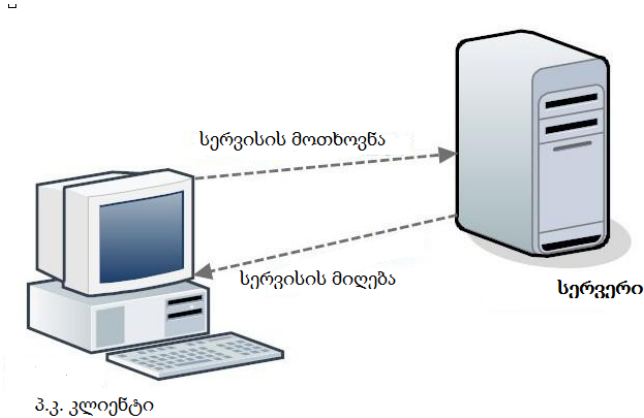
ბოლო წლებში ვირტუალიზაცია სერვერულ აპარატურასაც შეეხო. **x86-**არქიტექტურაზე მომუშავე პროცესორების ახალი თაობა (**Intel, AMD**) ვირტუალიზაციის აპარატურული მხარდაჭერითაა აღჭურვილი, რაც ერთიორად ამაღლებს ვირტუალური ოპერაციული სისტემების მუშაობის ეფექტურობას. სწორედ ამგვარი პროცესორებით აღჭურვილ სერვერულ სისტემებშია ყველაზე ეფექტური "აბსოლუტური ვირტუალიზაციის" განხორციელება, რომელიც ჰოსტ-მანქანად არა სტანდარტული ოპერაციული სისტემების, არამედ ე.წ. ჰაიპერვაიზორების გამოყენებას გულისხმობს. ჰაიპერვაიზორი სპეციალურად ვირტუალური მანქანების მომსახურებისთვის შექმნილი მინი ოპერაციული სისტემაა. ვირტუალურ "მასპინძლად" სტანდარტული ოპერაციული სისტემების ჰაიპერვაიზორებით ჩანაცვლება მნიშვნელოვნად ზოგავს სერვერის რესურსებს. მიმდინარე ეტაპზე ყველაზე

გავრცელებული ჰაიპერვაიზორებია **VMware ESX Server, Microsoft Hyper-V** და უფასო პროგრამა **Xen**.

1.1. სერვერული აპარატურის კომპლექტაცია

სერვერი - აპარატურული თვალსაზრისით შეგვიძლია განვიხილოთ როგორც სპეციალიზირებული კომპიუტერი ან მოწყობილობა, რომელიც განკუთვნილია, მასში ჩაწერილი სერვერული ოპერაციული სისტემის სერვისების სამართავად.

სერვერ კომპიუტერებს უნდა ჰქონდეს შესაძლებლობა მიიღოს მოთხოვნები კლიენტი კომპიუტერებისგან და უპასუხოს მათ. მიზანი შესაძლებელია იყოს მონაცემთა ან აპარატურული და პროგრამული რესურსების გაცვლა კლიენტებს შორის. ამგვარი არქიტექტურა იწოდება როგორც კლიენტი-სერვერი მოდელი. ტიპურ კომპიუტერულ სერვერებს მიეკუთვნება: მონაცემთა ბაზის სერვერები, ფაილური სერვერი, საფოსტო სერვერი, ვებ სერვერი, სათამაშო სერვერი, ბეჭდვის სერვერი, გამოყენებითი პროგრამული უზრუნველყოფის სერვერები.



სურ.1.1 1 კლიენტი-სერვერი მოდელი

შენიშვნა: მიუხედავად ტიპისა და აპარატურული შესაძლებლობებისა, სერვერული სერვისების განხორციელების შესაძლებლობა აქვთ მხოლოდ იმ კომპიუტერულ სისტემებს, რომლებშიც ჩაწერილია ესა თუ ის სერვერული ოპერაციული სისტემა

სერვერული მოწყობილობებისადმი მოთხოვნები განსხვავდება სერვერის მიზნებისა და მისი პროგრამული უზრუნველყოფის შესაბამისად.

ვინაიდან სერვერებთან წვდომა ძირითადად ხორციელდება ქსელით, სერვერი შესაძლებელია მუშაობდეს მონიტორის, ინფორმაციის შემტანი მოწყობილობების, ხმოვანი აპარატურული საშუალებებისა და უნივერსალური ინტერფეისების გარეშე. მათი კონფიგურირება და მართვა ხდება დაშორებული მანძილიდან.

განსხვავება პერსონალურ კომპიუტერებსა და სერვერებს შორის

პერსონალურ კომპიუტერებსა და სერვერებს შორის, აპარატურული უზრუნველყოფის თვალსაზრისით განსხვავებების აღწერისას შეიძლება გამოვყოთ



სურ.1.1 2 სერვერული კომპონენტები

მსგავსებებიც და განსხვავებებიც.

უმეტეს შემთხვევაში სერვერული და სამაგიდო პერსონალური კომპიუტერების აპარატურული უზრუნველყოფის დეტალები შეიძლება რეალურად არ განსხვავდებოდეს ერთმანეთისგან, ორივე იყენებს ისეთ ძირითად კომპონენტებს როგორცაა: მეხსიერება, პროცესორი, კვება. თუმცა სერვერის ფუნქციონალური დანიშნულებიდან გამომდინარე ცალკეული კომპონენტები სერვერში, უთუოდ მეტი წარმადობით უნდა გამოირჩეოდეს ვინემ ანალოგური დანიშნულების დეტალები, პერსონალური გამოყენების სისტემებში.

სერვერის ფორმ-ფაქტორები

ტერმინი ფორმ-ფაქტორი აღწერს იმ ფიზიკურ ასპექტებსა და სტანდარტებს, რომელსაც იყენებს განსხვავებული აპარატურული სისტემის კომპონენტი და კომპიუტერი მთლიანად. პერსონალურ კომპიუტერებში გავრცელებული ფორმ-ფაქტორია ATX. მაგალითისთვის.: სტანდარტული ATX კორპუსი ფიზიკურად

შეითავსებს ნებისმიერ სტანდარტულ ATX ფორმ-ფაქტორის დედაპლათას და კვების ბლოკს, მიუხედავად იმისა თუ რომელი მწარმოებლის მიერ არის შექმნილი ესა თუ ის კომპონენტი.

ფორმ-ფაქტორი აქტუალურია სერვერის აპარატურულ ელემენტებთან მიმართებაშიც. არსებობს რამოდენიმე განსხვავებული ფორმ-ფაქტორი გამოყენებული ქსელურ სერვერებში, თუმცა ძირითადად გავრცელებულია: Tower, Rack და Blade სერვერები.

Tower სერვერი

Tower სერვერები ძალიან გავს პერსონალურ კომპიუტერებს (ATX ფორმ-ფაქტორის სამაგიდო სისტემებს). თითოეული Tower სერვერი წარმოადგენს ავტონომიურ სისტემას, რომელიც განთავსებულია ვერტიკალურ კორპუსში

Tower სერვერები ძირითადად გამოიყენება შედარებით მცირე მონაცემთა გაცვლის ცენტრებში. შედარებით დიდი მონაცემთა გაცვლის ცენტრებში, როგორც წესი თავს იკავებენ Tower სერვერების გამოყენებისგან, მათი განთავსებისთვის საჭირო დიდი ფიზიკური გარემოსა და შედარებით მაღალი ხმაურის გამო.

სხვა ნაკლოვანებად ასევე შეიძლება ჩაითვალოს კაბელების განთავსების მოუწყვრიგებლობა. Rack და Blade სერვერების კარადასა და შასებზე გათვალისწინებულია კაბელების ორგანიზებული განლაგების სქემა - Tower სერვერებისგან განსხვავებით.



სურ.1.13 Tower სერვერი

Rack სერვერი

როგორც დასახელებიდან ჩანს, Rack სერვერები(იხ. სურ.1.1.4) წარმოადგენს სერვერს, რომელიც მონტაჟდება შესაბამის კარადაში(Rack)(იხ.სურ.1.4.5). კარადას აქვს სერვერის თავსებადი ზომის სიგანე და სერვერები ჩამაგრებულია ჭანჭიკების საშუალებით. კარადაში როგორც წესი განთავსებულია ერთმანეთზე დაწყობილი რამოდენიმე სერვერი.



სურ.1.1 4 Rack სერვერი

რადგან კარადის თაროები განკუთვნილია სტანდარტული ზომის კომპონენტებისთვის, ქსელური მოწყობილობების მწარმოებლები, სერვერების გარდა გვთავაზობენ კარადაში განთავსებისთვის თავსებად სხვა ქსელურ კომპონენტებს, როგორცაა აპარატურული ფაერვოლები, კომპუტატორები და სხვ.



სურ.1.1 5 საკომუნიკაციო კარადა სერვერებისთვის

კარადაში ჩასამონტაჟებელი კომპონენტები ფორმ-ფაქტორის მიხედვით განსხვავდება ზომებით, რომელიც იზომება Rack ერთეულით. სტანდარტული Rack სერვერი აღინიშნება როგორც 1U სერვერი, რაც იმას ნიშნავს, რომ ის იკავებს 1 თაროს

შესაბამის სივრცეს კარადაში. სერვერები სიმაღლით 2U იყენებს 2 თაროს შესაბამის სივრცეს კარადაში. ზოგიერთი მწარმოებელი გვთავაზობს 4U და 1/2U სერვერებს. უფრო დიდი ფორმ-ფაქტორები გამოიყენება, როცა სერვერებზე მოთხოვნილია განსაკუთრებით დიდი მოცულობის ინფორმაციის შენახვა

Blade სერვერი

როგორც Rack სერვერების შემთხვევაში, Blade სერვერებიც ხასიათდება სტანდარტული ზომებით, რათა ჩამონტაჟებულ იქნას სპეციალურ „კარადაში“, რომელსაც Blade სერვერების შემთხვევაში ჩარჩოს(შასი) უწოდებენ.

Blade სერვერები, როგორც წესი წარმოადგენს მწარმოებლის ფორმ-ფაქტორს(სტანდარტს). ასე მაგალითად, თქვენ ვერ შეძლებთ ერთი ფორმის Blade სერვერის ჩადგმას სხვა ფორმის კორპუსში.



სურ.1.1 6 Blade სერვერი

მიზეზი თუ რატომ არის Blade სერვერები დაპატენტებული, მდგომარეობს იმაში, რომ Rack სერვერებისგან განსხვავებით, რომლებიც თავის მხრივ სრულიად ავტონომიურია, Blade სერვერებს არ აქვთ ზოგიერთი კომპონენტი, რომელიც აუცილებელია მათი ფუნქციონირებისთვის. მაგ.: Blade სერვერებს არ აქვთ კვების ბლოკი.

Blade სერვერის ჩარჩო(შასი) განკუთვნილია, სხვადასხვა მოდულური კომპონენტების მიღებისთვის, მათ შორის თავად Blade სერვერების. მაგ.: ჩარჩო(შასი) შეიძლება შეიცავდეს კვების ბლოკს, გამაგრილებელ ბლოკს და Blade სერვერს.

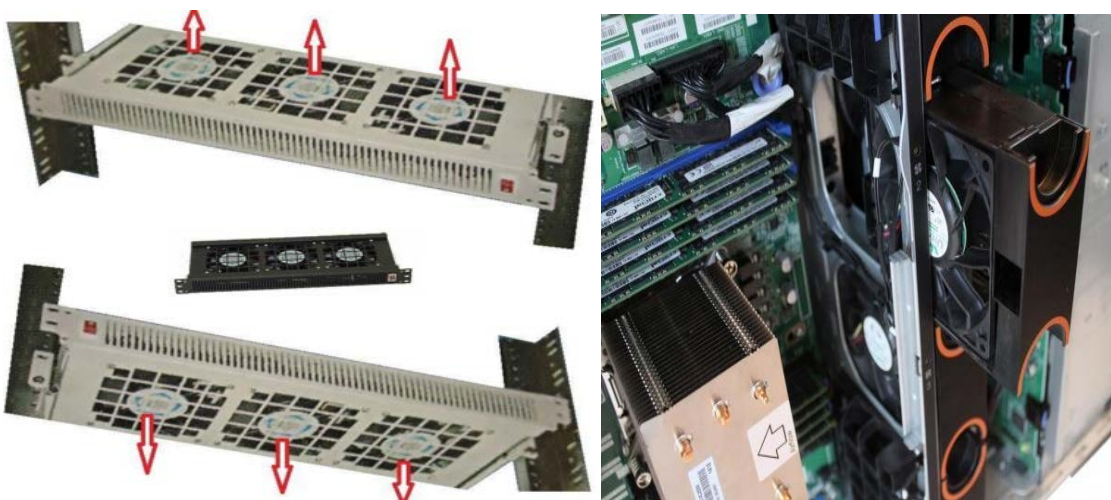
კითხვები თვითშემოწმებისთვის:

• დაახასიათეთ კლიენტი-სერვერი არქიტექტურა და ჩამოაყალიბეთ მოცემულ არქიტექტურაში კლიენტი კომპიუტერისა და სერვერის როლი.

- რა არის ფორმ-ფაქტორი?
- რა და რა სახის ფორმ-ფაქტორია გავრცელებული სერვერულ სისტემებში?
- დაახასიათეთ Tower სერვერები
- დაახასიათეთ Rack სერვერები
- დაახასიათეთ Blade სერვერები

გაგრილება სერვერულ სისტემებში

სათანადო ფუნქციონირების მხარდასაჭერად კომპიუტერები გრილ ტემპერატურულ გარემოში უნდა ფუნქციონირებდეს. ხშირად ყველაზე უჩვეულო შეცდომების მიზეზი, სწორედ სისტემის გადახურებაა. სერვერები ცალკეული კომპონენტების გასაგრილებლად იყენებს რადიატორებს და ვენტილატორებს, სერვერის საერთო ტემპერატურის შესანარჩუნებლად ასევე მნიშვნელოვან როლს თამაშობს კორპუსის დიზაინი. Blade სერვერები წარმოადგენს გამონაკლისს, სადაც შასი-ჩარჩოა პასუხისმგებელი ცალკეული ბლეიდ-სერვერების გაგრილებაზე.



სურ.1.17 გაგრილება სერვერულ სისტემებში

როგორც წესი, სერვერებს აქვს მინიმუმ წყვილი კორპუსის ვენტილატორი, ვენტილატორების ზომა და რაოდენობა, მნიშვნელოვნად განსხვავდება კორპუსის კონსტრუქციის შესაბამისად.

სერვერები ასევე აღჭურვილია ტემპერატურული სენსორებით. სენსორები შესაძლებელია ინტეგრირებული იყოს როგორც დედაპლატაზე ან ცალკეულ კომპონენტებზე, ასევე კორპუსში. როდესაც ტემპერატურა კორპუსის შიგნით დაიწყებს ზრდას, თავის მხრივ გაიზრდება ვენტილატორის ტრიალის სიჩქარე. უსაფრთხოების მექანიზმების მხარდაჭერა აქვს ასევე BIOS¹ სისტემასაც, რომელიც დაზიანებებისგან თავის აცილების მიზნით თიშავს სერვერს, როცა ტემპერატურა აღწევს ძალიან მაღალ ნიშნულს.

ფილტრაცია

ხშირად ვენტილატორი არ არის საკმარისი სერვერის გაგრილების უზრუნველსაყოფად. სპეციფიკური განლაგების მიხედვით ვენტილატორებმა თავის მხრივ შეიძლება შეისრუტოს ჭუჭყი, მტვერი და სხვ. ამგვარი შემთხვევების თავიდან ასაცილებლად სერვერებში გამოიყენება საჰაერო ფილტრები.

ფიზიკური უსაფრთხოება

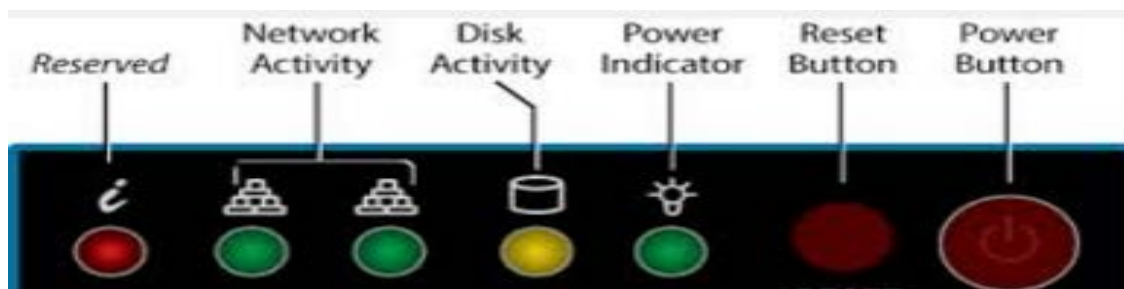
სერვერების ფიზიკური დაცვა არ არის პრიორიტეტული სერვერების დიზაინზე საუბრისას. სერვერების მწარმოებლები ვარაუდობენ, რომ როგორც წესი სერვერები უნდა იყოს განთავსებული ფიზიკურად საიმედოდ დაცულ ცენტრებში, ამიტომაც შესაძლებელია არ იყოს აუცილებელი სერვერის კორპუსის ფიზიკური დაცვა. მიუხედავად ამისა მეტი ფიზიკური დაცვისათვის სერვერები სპეციალური კორპუსით და გასაღებით არის აღჭურვილი.

¹ BIOS- შეტანა-გამოტანის ბაზისური სისტემა, პირველადი პროგრამული უზრუნველყოფა, რომელიც მწარმოებლის მიერ იწერება დედაპლატაზე არსებულ ინტეგრირებულ მიკროსქემაში

ინდიკატორები

სერვერებს თითქმის ყოველთვის აქვს სხვადასხვა ფორმის მდგომარეობის ინდიკატორები, რომლებიც შუქ-დიოდურ ნათურებს წარმოადგენს. ინდიკატორები არ წარმოადგენს გამონაკლისს სერვერებისთვის, ის როგორც წესი ყველა პერსონალურ კომპიუტერში გვხვდება. მაგ.: ყველა კომპიუტერს აქვს კვების და მყარი დისკის მდგომარეობის ინდიკატორები. სერვერებში გვხვდება სხვა დამატებითი ინდიკატორებიც, რომელსაც ვერ შევხვდებით პერსონალურ კომპიუტერებში.

მწარმოებლები იყენებენ ინდივიდუალურ ინდიკატორების კრებულს, მაგრამ არსებობს ყველასთვის მიღებული, გლობალური ინდიკატორის ნათებები, რომლებიც გვამცნობს სერვერის მდგომარეობას.



სურ.1.1 8 ინდიკატორები

შუქ-დიოდური ინდიკატორების დამატებას წარმოადგენს სერვერებში ინტეგრირებული თერმომეტრები, რომელიც ვიზუალურად გვაჩვენებს სერვერის კორპუსის შიდა ტემპერატურას.

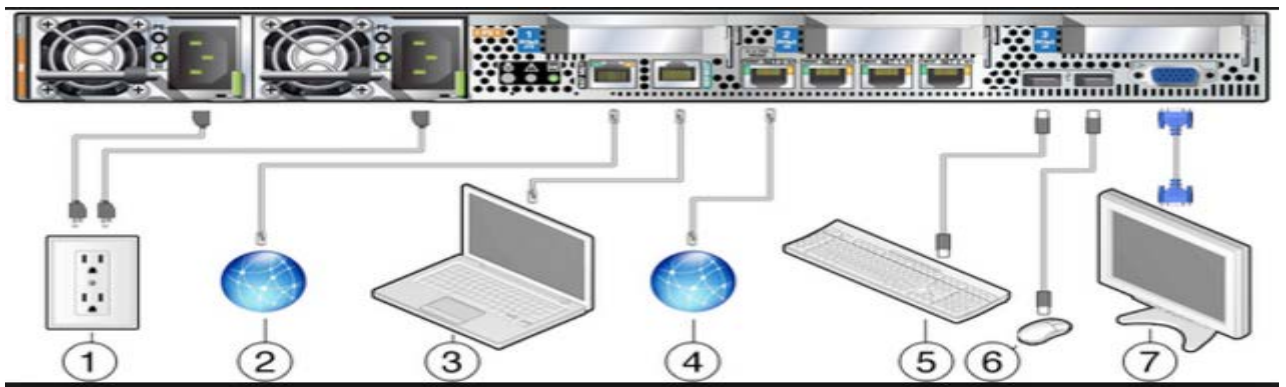
პორტები

სერვერებთან წვდომა ჩვეულებრივ დაშორებული მანძილიდან ხორციელდება. სერვერებზე გვხვდება ხშირად გამოყენებული პორტებიდან - კლავიატურის, მაუსის და ვიდეო გამოსასვლელი პორტები, მაგრამ როგორც წესი ეს პორტები გამოიყენება საწყისი

გამართვისას და იმ შემთხვევებში, როცა აუცილებელია ადგილზე ჩატარდეს დიაგნოსტიკის ამოცანები.

ბლიდ სერვერების შემთხვევაში, მათ არ აქვს ინდივიდუალურად კლავიატურის, მაუსის და ვიდეო გამოსასვლელი პორტები. მოცემული პორტები გათვალისწინებულია ბლიდ სერვერის შასებზე(ჩარჩოებზე).

სერვერებზე ასევე გვხვდება უნივერსალური USB პორტები, შესაბამისი ინტერფეისის მოწყობილობების დასაკავშირებლად.



სურ.1.19

ბუდეები ინფორმაციის დამგროვებლებისთვის

სერვერებზე დამგროვებლებისთვის განკუთვნილი ბუდეების რაოდენობა დამოკიდებულია სერვერის ფორმ-ფაქტორზე. 1U სერვერებზე შეიძლება გვხვდებოდეს 1 ან 2 ბუდე, მაშინ როდესაც ზოგიერთ 4U სერვერში გვხვდება ათეულობით ბუდე დამგროვებლებისთვის.

სერვერები მცირე ფორმ-ფაქტორებით, იყენებს ლოკალურ მყარ დისკებს უშუალოდ ოპერაციული სისტემისთვის და დაშორებულ საცავთან (მაგ. SAN) წვდომისათვის.



სურ.1.1 10 სერვერი 4 ბუდით

1.2. Windows სერვერული ოპერაციული სისტემების ინსტალაცია

სერვერებში ფართოდ გავრცელებულია Windows და Linux ოპერაციული სისტემების სერვერული ვერსიები.

სურათზე მოცემულია Windows ოპერაციული სისტემის თანამედროვე სერვერული ვერსიები

Name	Release date	Release version number	Editions
Windows Server 2016	2016	NT 10.0	<ul style="list-style-type: none"> N/A
Windows Server 2012 R2	2013	NT 6.3	<ul style="list-style-type: none"> Windows Server 2012 R2 Foundation Windows Server 2012 R2 Essentials Windows Server 2012 R2 Standard Windows Server 2012 R2 Datacenter
Windows Server 2012	2012	NT 6.2	<ul style="list-style-type: none"> Windows Server 2012 Foundation Windows Server 2012 Essentials Windows Server 2012 Standard Windows Server 2012 Datacenter Windows MultiPoint Server 2012
Windows Server 2008 R2	2010	NT 6.1	<ul style="list-style-type: none"> Windows Server 2008 R2 Foundation Windows Server 2008 R2 Standard Windows Server 2008 R2 Enterprise Windows Server 2008 R2 Datacenter Windows Server 2008 R2 for Itanium-based Systems Windows Web Server 2008 R2 Windows Storage Server 2008 R2 Windows HPC Server 2008 R2 Windows Small Business Server 2011 Windows MultiPoint Server 2011 Windows Home Server 2011 Windows MultiPoint Server 2010
Windows Server 2008	2008	NT 6.0	<ul style="list-style-type: none"> Windows Server 2008 Standard Windows Server 2008 Enterprise Windows Server 2008 Datacenter Windows Server 2008 for Itanium-based Systems Windows Server Foundation 2008 Windows Essential Business Server 2008 Windows HPC Server 2008 Windows Small Business Server 2008 Windows Storage Server 2008 Windows Web Server 2008

სურ.1.2. 1

ოპერაციული სისტემა Microsoft windows Server 2012 წარმოჩენილია სიახლეები წინა ვერსიებთან შედარებით:

- ახალი სამომხმარებლო ინტერფეისი Modern UI
- გაუმჯობესებული ბრძანებათა ველის ინტერფეისი PowerShell
- გაუმჯობესებული ამოცანათა დისპეჩერი
- Server Core გახდა ინსტალაციის რეკომენდირებული ვარიანტი, ხოლო გადართვა კლასიკური სამუშაო მაგიდის რეჟიმსა და Server Core რეჟიმებს შორის შესაძლებელია სერვერის გადაყენების გარეშე
- განახლებული **IPAM** (IP Address Management) IPv4 და IPv6 მისამართების სივრცის მართვისა და აუდიტისათვის
- ცვლილებები Active Directory -ს სერვისში

- ახალი ვერსია Hyper-V 3.0. ახალი ფაილური სისტემა ReFS (Resilient File System).
- ახალი ვერსია IIS 8.0 (Internet Information Services).

Windows Server 2012-ს აქვს შემდეგი აპარატურული უზრუნველყოფის მხარდაჭერა:

სპეციფიკაცია	Windows Server 2012	Windows Server 2012 R2
ფიზიკური პროცესორები (CPU)	64	64
ლოგიკური პროცესორები (როცა Hyper-V გამორთულია)	640	256
ლოგიკური პროცესორები (როცა Hyper-V აქტიურია)	320	64
ოპერატიული მეხსიერება	4 TB	2 TB

Windows Server 2012-ის მინიმალური სისტემური მოთხოვნები

პროცესორი	1,4 GHz x64
ოპერატიული მეხსიერება	512 MB
ადგილი მყარ დისკზე	32 GB (უფრო მეტი 16 GB და მეტი ოპერატიულის შემთხვევაში)

ჩატვირთვის პრიორიტეტის განსაზღვრა

ოპერაციული სისტემის ინსტალაციის წინ აუცილებელია შევცვალოთ კომპიუტერის ჩატვირთვის პრიორიტეტი ისე, რომ პირველ ჩამტვირთავ მოწყობილობად დავაყენოთ ოპტიკური დისკწამკითხავი ან ფლემ მებსიერება, იმის მიხედვით საიდანაც ვახდენთ ინსტალაციას.

თუ კომპიუტერის მყარ დისკზე ადრე არ ყოფილა ინსტალირებული ოპერაციული სისტემა, ერთადერთი ჩამტვირთავი ჩანაწერი იქნება ჩადებულ საინსტალაციო დისკზე ან მიერთებულ ფლემ მებსიერებაზე, ამ შემთხვევაში არავითარი ჩატვირთვის პრიორიტეტის განსაზღვრა არ გვიჭირდება და ოპერაციული სისტემის ინსტალაცია დაიწყება ყოველგვარი დამატებითი მოქმედებების გარეშე. თუ მყარ დისკზე უკვე არსებობს ძველი ოპერაციული სისტემა, რომლის შეცვლაც გვინდა ახლით, მაშინ ჩამტვირთავი მოწყობილობის არჩევა იქნება აუცილებელი.

მაშ ასე გვაქვს ის კომპიუტერი რომელიც აკმაყოფილებს **Windows Server 2012**-ის მინიმალურ სისტემურ მოთხოვნებს და საინსტალაციო დისკი. ეს არის ყველაფერი რაც გვჭირდება **Windows**-ის დასაყენებლად კომპიუტერზე.

Windows ოპერაციული სისტემის ინსტალაცია ხანგრძლივი პროცესია. კომპიუტერის პარამეტრებიდან გამომდინარე ის შეიძლება გაგრძელდეს 10 წუთიდან 40 წუთამდე, აქედან გამომდინარე დაახლოებით ერთი საათი უნდა გამოვყოთ მხოლოდ ინსტალაციისთვის.

1. ჩადეთ **Windows Server 2012**-ის საინსტალაციო დისკი კომპიუტერის ოპტიკურ დისკწამკითხავში ან მიაერთეთ ფლემ მებსიერება, რომელზეც წინასწარ არის ჩაწერილი ოპერაციული სისტემა (**Bootable Flash**).

2. ჩართეთ კომპიუტერი (ან გადატვირთეთ თუ უკვე ჩართულია). რამდენიმე წამში კომპიუტერი ჩაიტვირთება ოპტიკური დისკწამკითხავიდან ან ფლემიდან, რის შემდეგაც გაეშვება **Windows Server 2012**-ის ინსტალაციის ოსტატი (სურ. 1.2.1):



სურ.1.2. 2

Windows-ის ინსტალაციის ოსტატი პირველ ფანჯარაში გვთავაზობს ოპერაციული სისტემის ინტერფეისის ენის არჩევანს, კლავიატურის განლაგებას და დროისა და ფულადი ფორმატის წარმოდგენის რეგიონალურ ფორმატს.

1. ინტერფეისის ენის (**Language to install**), დროისა და ფულადი ფორმატის (**Time and currency format**), კლავიატურის განლაგებისა ან ინფორმაციის შეტანის მეთოდის (**Keyboard or input method**) ჩამოშლად ველებში აირჩიეთ სასურველი პარამეტრები ან დატოვეთ უცვლელად. შეგახსენებთ რომ მათი შეცვლა შესაძლებელია ინსტალაციის დასრულების შემდეგაც მართვის პანელის (**Control Panel**) **Region** და **Language** უტილიტების საშუალებით.

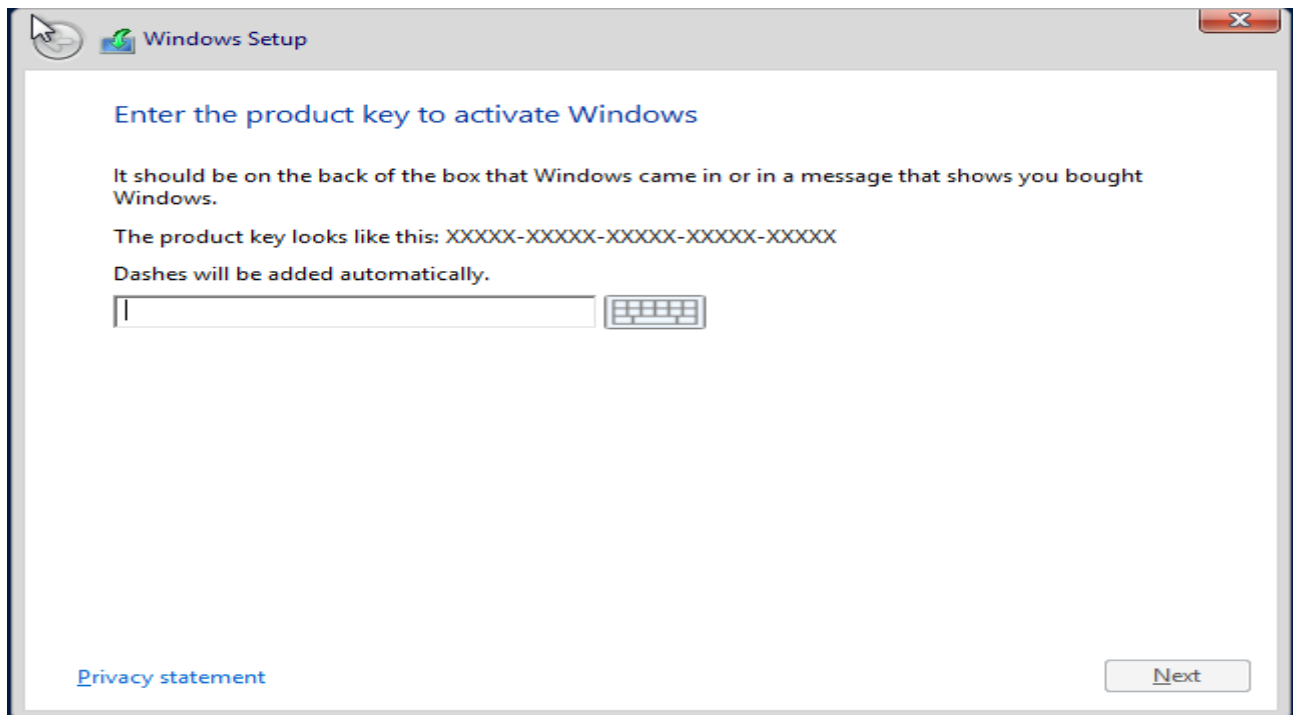
2. დააჭირეთ **Next** ღილაკს. ეკრანზე გამოვა ინსტალაციის ოსტატის მომდევნო ფანჯარა (სურ. 1.2.3), რომელიც შეიცავს მხოლოდ ერთ ღილაკს (**Install now**) და **Repair your computer** ბმულს, რომელიც გამოიყენება დაზიანებული ოპერაციული სისტემის ან სისტემის კომპონენტების აღდგენის დროს.

3. მოცემულ ფანჯარაში დააწექით **Install now** ღილაკს.



სურ.1.2. 3

გამოსულ ფანჯარაში (სურ. 1.2.4) აუცილებელია მივუთითოთ **Windows**-ის ლიცენზიის გასაღები (**License Code**). გასაღები როგორც წესი მითითებულია საინსტალაციო დისკის ყუთზე ან დაკრულია კომპიუტერის სისტემური ბლოკის უკანა მხარეს/წოუთბუქის ქვედა მხარეს (ეს იმ შემთხვევაში, როდესაც ვიყიდეთ კომპიუტერი უკვე ინსტალირებული ლიცენზირებული ოპერაციული სისტემით).



სურ.1.2. 4

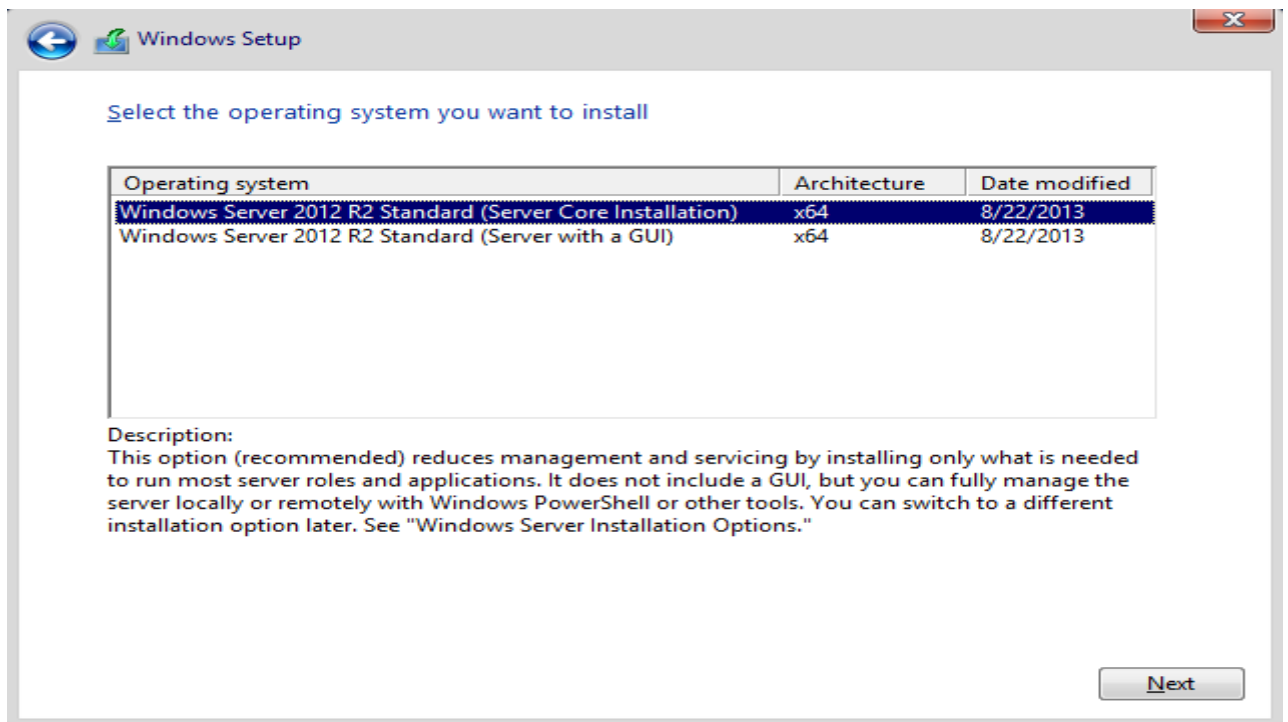
შესაძლებელია მოხდეს ისე, რომ ინსტალაციის დროს არ იქნას მოთხოვნილი ლიცენზიის კოდი. ეს იმ შემთხვევაში ხდება, როცა შეძენილი გვაქვს კომპიუტერი, რომელზეც წინასწარ არის დაყენებული **Windows Server 2012** და რომელიც უკვე „მიბმულია“ კომპიუტერში ჩაყენებულ კონკრეტულ მოწყობილობასთან, და არ შეიძლება ამ სისტემის დაინსტალირება სხვა კომპიუტერებზე.

1. ლიცენზიის კოდისთვის გამოყოფილ ველში შეიყვანეთ 25 ციფრიანი კოდი. ტირების ხელით მითითება არ არის საჭირო ის ავტომატურად მიეთითება ყოველი 5 ციფრის შეყვანის შემდეგ. ყურადღება მიაქციეთ იმას, რომ კლავიატურის განლაგება იდგეს ინგლისურ ენაზე რადგან ლიცენზიის კოდი მოცემულია ლათინური შრიფტით. მოცემულ ეტაპზე ენებს შორის გადართვა ხდება **Alt+Shift** კლავიშთა კომბინაციით.

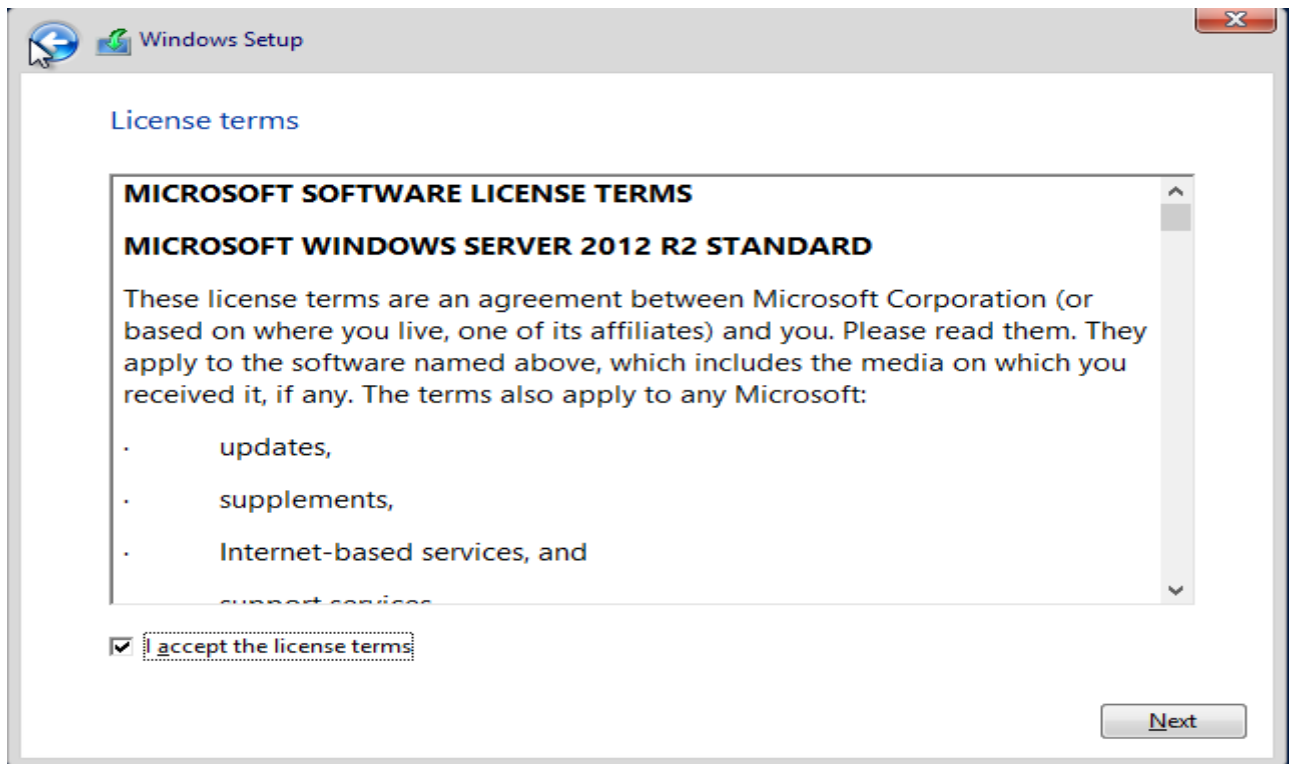
2. დააჭირეთ **Next** ღილაკს. გამოჩნდება ფანჯარა (სურ. 1.2.5) სადაც უნდა ავირჩიოთ ოპერაციული სისტემის ტიპი (ჩვენს შემთხვევაში განხილულია Server with GUI

3. დააჭირეთ **Next** ღილაკს. ეკრანზე გამოჩნდება სალიცენზიო შეთანხმების ტექსტი.

სალიცენზიო შეთანხმების ტექსტში შედის **Windows**-ის გამოყენების პირობები. ეს არის შეთანხმება ჩვენსა და პროგრამული უზრუნველყოფის მწარმოებელს შორის, რომელზეც აუცილებელია თანხმობა რათა გავაგრძელოთ ოპერაციული სისტემის ინსტალაცია. ინსტალაციის გაგრძელებისთვის საჭიროა დავაყენოთ ალამი **I accept the license terms** (ვეთანხმები ლიცენზიის პირობებს) პუნქტზე (სურ. 1.2.6): ამით ვადასტურებთ რომ გავეცანით და ბოლომდე წავიკითხეთ სალიცენზიო შეთანხმების პირობები და ყველაფერზე ვართ თანახმა. დააჭირეთ **Next** ღილაკს. გამოჩნდება ფანჯარა, სადაც უნდა ავირჩიოთ ინსტალაციის ვარიანტი.



სურ.1.2. 5

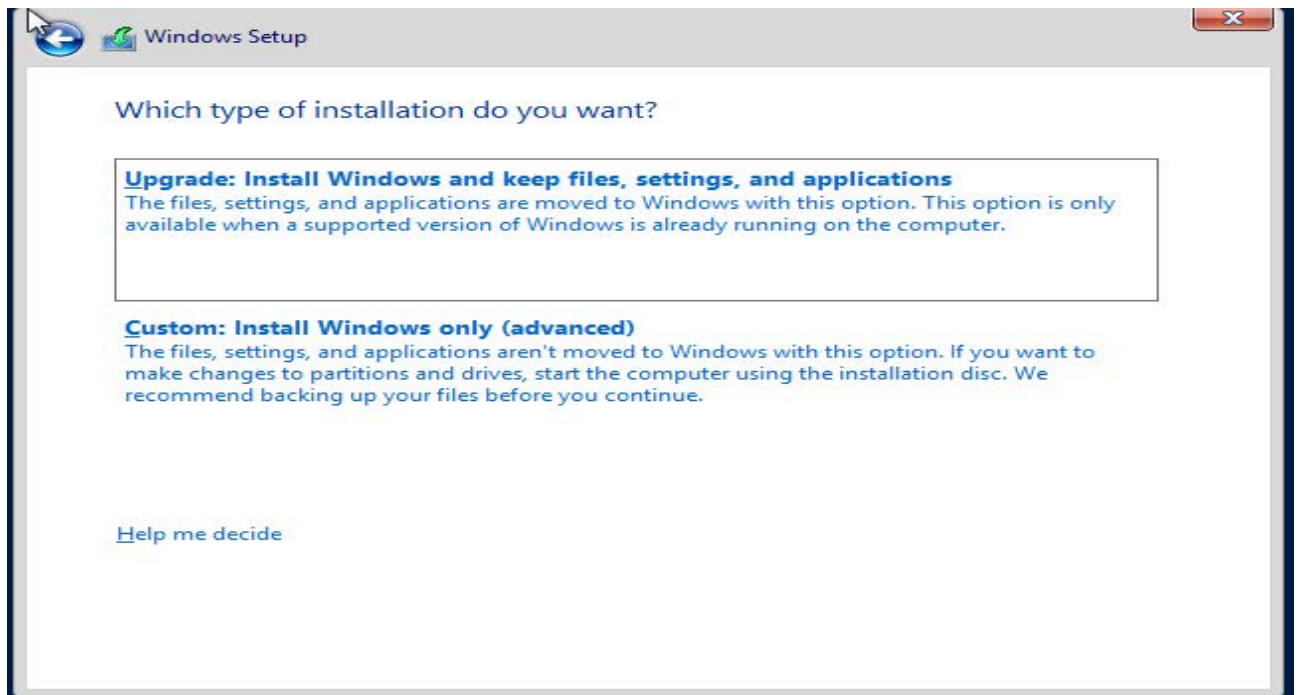


სურ.1.2. 6

Windows Server2012-ის ინსტალაცია შეიძლება შესრულდეს ორი საშუალებით (სურ. 1.2.7):

❖ განახლება (**Upgrade**). ეს ვარიანტი გამოიყენება მაშინ, როდესაც ვახდენთ ადრე ინსტალირებული **Windows** ოპერაციული სისტემის განახლებას ახალი ვერსიით. მაგალითად, თუ კომპიუტერზე იყო დაინსტალირებული **სხვა** ოპერაციული სისტემა, და იყო მუშა მდგომარეობაში, ჩვენ შეგვიძლია შევასრულოთ ინსტალაცია განახლების რეჟიმში. ამ შემთხვევაში კომპიუტერზე შეინახება დაინსტალირებული პროგრამები, დრაივერები, მომხმარებლის სააღრიცხვო ჩანაწერის და მომხმარებლის პარამეტრები. რეკომენდებულია თუ გააკეთებთ საჭირო ფაილების სარეზერვო ასლს.

❖ შერჩევითი (**Custom**). ინსტალაციის მოცემულ ვარიანტში იგულისხმება ძველი ვერსიის **Windows**-ის, ინსტალირებული პროგრამების, დრაივერებისა და მომხმარებლის პარამეტრების მთლიანად წაშლა იმ დანაყოფიდან, რომელზეც ვაპირებთ ახალი სისტემის ინსტალაციას.



სურ.1.2. 7

Custom (Advanced) დილაკზე დაჭერით გამოვა შემდეგი ფანჯარა (სურ. 1.2.8):

გვაქვს ორი ვარიანტი:

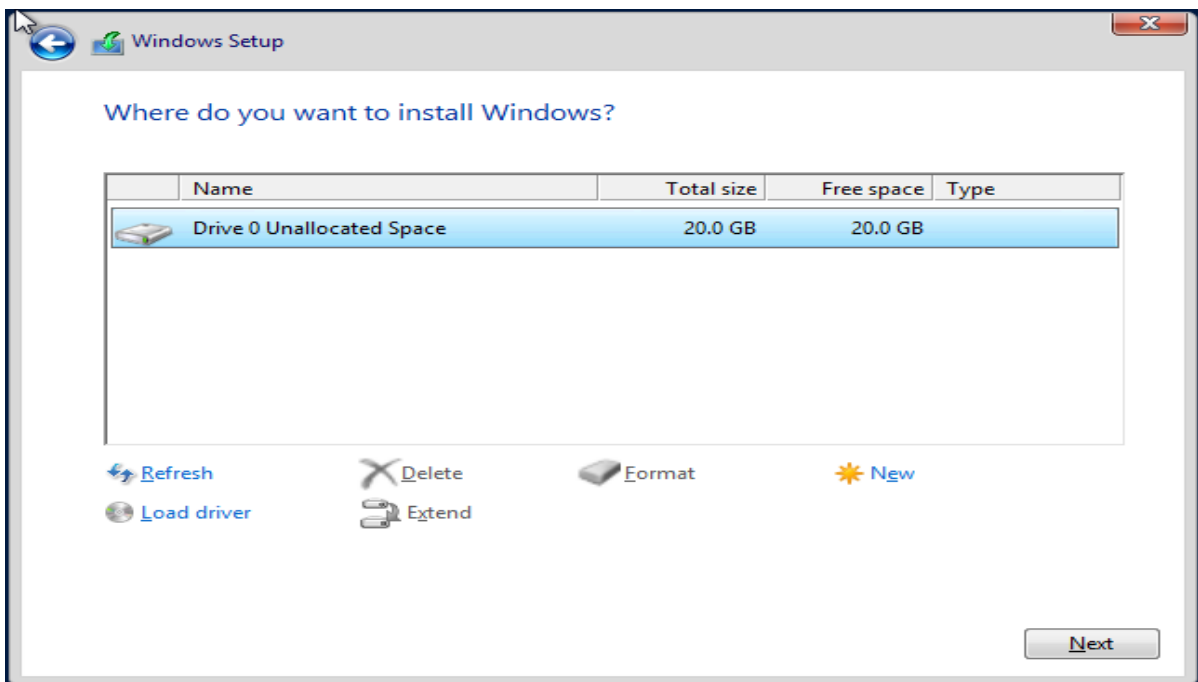
1. დაინსტალება შეიძლება მყარი დისკის ლოგიკურ დისკებად დაყოფის გარეშე მთლიან ვინჩესტერზე, შემდეგ კი, სპეციალური პროგრამების მეშვეობით, შესაძლებელია მისი დაყოფა სასურველი ზომის ლოგიკურ დისკებად;

2. წინასწარ განვსაზღვროთ, რა ზომის დანაყოფი (განყოფილება) გვჭირდება სისტემისათვის, გამოვყოთ ამ ზომის ლოგიკური დისკი და შემდეგ სწორედ მასზე დავაინსტალოთ სისტემა. ბუნებრივია, ეს დისკი იქნება პირველადი ლოგიკური დისკი.

თავიდანვე გაითვალისწინეთ: თუ ერთ კომპიუტერზე ორი ოპერაციული სისტემის ჩაწერას აპირებთ, უმჯობესია, პირველი სისტემისათვის წინასწარ გამოვყოთ ლოგიკური დისკი და დარჩენილი ნაწილი დაუფორმატებელი დაუტოვოთ მეორე სისტემას.

როგორც აღვნიშნეთ, ამ დროს წინასწარ უნდა განისაზღვროს სისტემური დისკის ზომა. მყარ დისკზე ზომების დანაწილება - ყველაზე საპასუხისმგებლო ეტაპია ოპერაციული სისტემის ინსტალაციისას. მყარი დისკზე ზომების დანაწილების მოქმედებების შესრულების მიმდევრობა დამოკიდებულია ბევრ ფაქტორზე (იმ

დავალეებზე რისი შესრულებაც მოუწევს ოპერაციულ სისტემას, დისკის ზომაზე, მყარი დისკების რაოდენობაზე კომპიუტერში, ასევე გვანტერებს ახალია თუ არა მყარი დისკი, თუ უკვე შეიცავს რაიმე ინფორმაციას). ჩვენ განვიხილავთ შემთხვევას როცა სისტემა ინსტალირდება ახალ მყარ დისკზე ან მთლიანად ვშლით ფაილებს იმ დანაყოფზე, რომელზეც ვაყენებთ ოპერაციულ სისტემას. ამ შემთხვევაში უბრალოდ ვირჩევთ იმ დანაყოფს რომელზეც ხდება **Windows**-ის ინსტალაცია. მიაქციეთ ყურადღება თითოეული დანაყოფის მთლიან ზომას (**Total size**). ჩვენ უნდა ავირჩიოთ ის დანაყოფი, რომლის ზომაც საკმარისი იქნება როგორც ოპერაციული სისტემისთვის, ასევე სხვა დასაინსტალირებელი პროგრამებისთვის. ზოგადად სასურველია ხელმისაწვდომი იყოს 50-100 გიგაბაიტი მოცულობა იმ დანაყოფზე სადაც ხდება სისტემის ინსტალაცია.



სურ.1.2. 8

სურ. 1.2.8 მონიშნულია დაუყოფელი, მთლიანი მყარი დისკი. აქ უნდა განსაზღვროთ სისტემური დისკის ზომა.

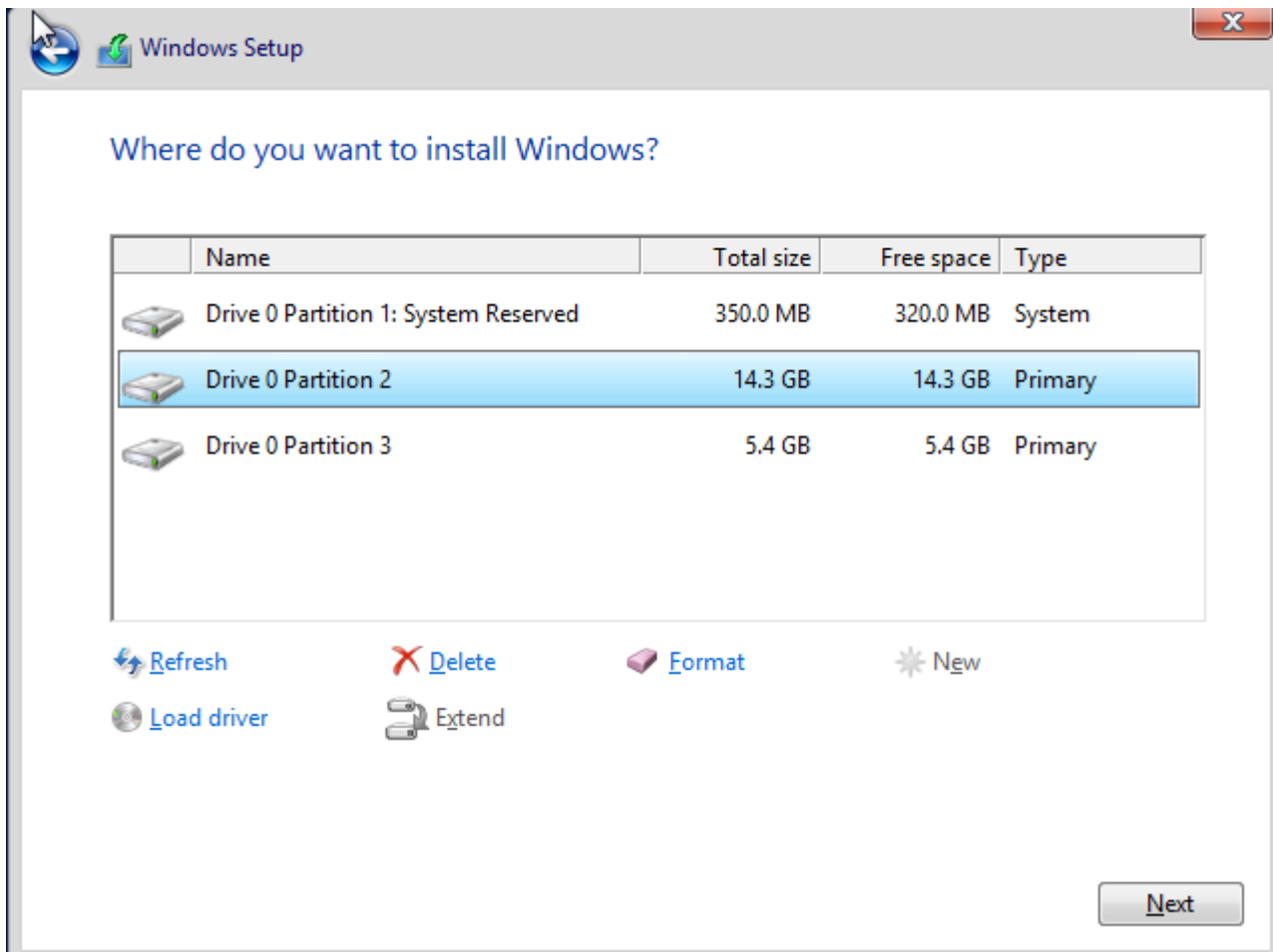
ფანჯარაში შემოთავაზებულია მოქმედების გაგრძელების შემდეგი საშუალებები (სურ. 1.2.8):

- მონიშნული ელემენტის **ოპერაციული სისტემის** ინსტალაციისათვის გამოყენების მიზნით დააჭირეთ **Next**-ს;

- ახალი დანაყოფის შესაქმნელად დააჭირეთ **New**-ს;

შევქმნათ ახალი დანაყოფი

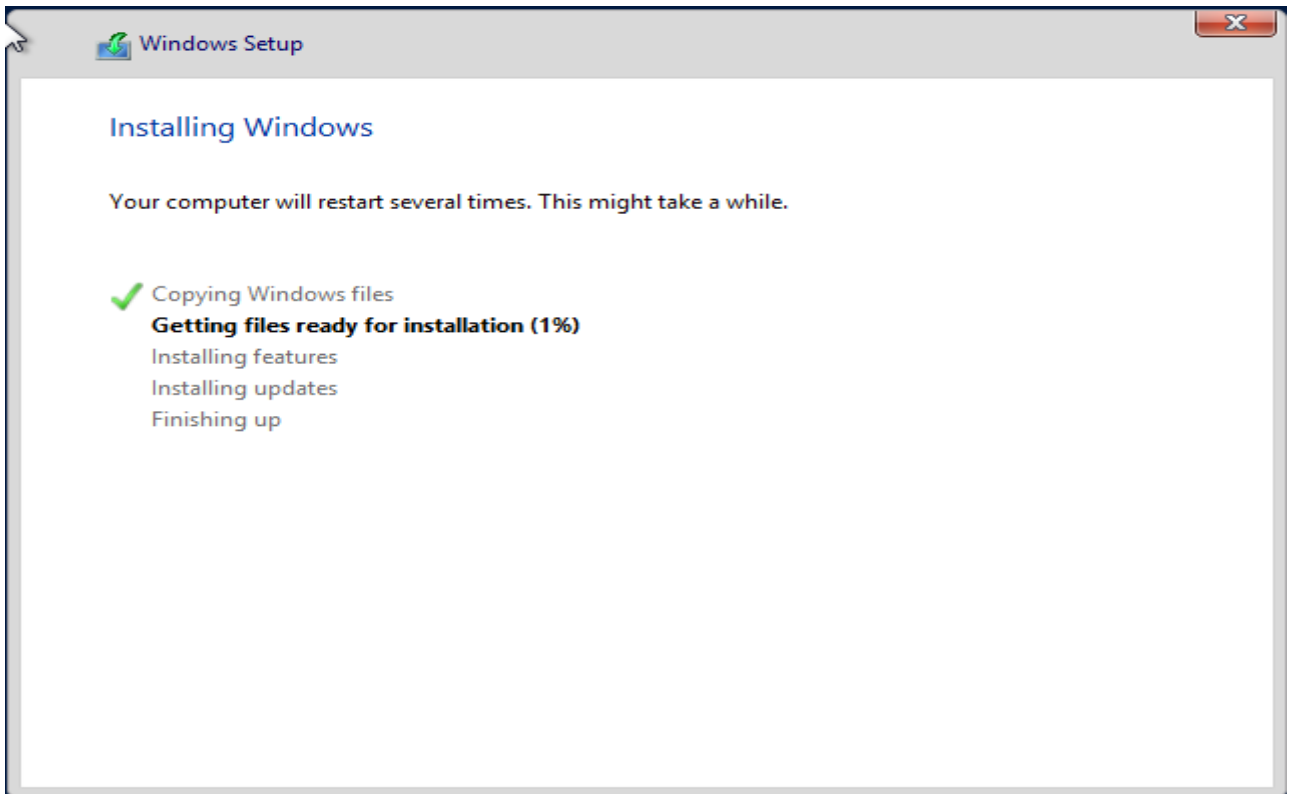
ჩვენს მიერ განხილულ ფანჯარაში (სურ. 1.2.8) ჩანს 20 გიგაბაიტი, ეს ამ შემთხვევაში, მყარი დისკის სრული მოცულობაა. თუ გვინდა, რომ ახალი დანაყოფის ზომა იყოს იგივე, დატოვებთ უცვლელად შესავსები ველი, დააჭირეთ **Apply**-ს და დაბრუნდებით წინა ფანჯარაში. განსხვავება იქნება ის, რომ ერთი მთლიანი დისკი ორად გაიყო. მივიღეთ ერთი 350 მეგაბაიტისანი დანაყოფილება ჩამტვირთავი ფაილების შესანახად და დანარჩენი (59.7 გბ) ოპერაციული სისტემისა და პროგრამების საინსტალაციოდ. ჩვენს შემთხვევაში რადგან მყარი დისკის ზომა გვაქვს 20 გიგაბაიტი, მის გაყოფას აზრი არ აქვს. უფრო მეტი ზომის მყარი დისკის არსებობის შემთხვევაში შეგვეძლო დაგვეყოფა 4 ნაწილად. მაგალითად, მყარი დისკის ზომაა 500 გიგაბაიტი, ერთ დანაყოფს გავაკეთებდით 350 მეგაბაიტისან ჩამტვირთავი ფაილებისთვის, მეორეს 100 გიგაბაიტისან (შემდგომში **C:** დისკი) - ოპერაციული სისტემისა სხვა პროგრამული უზრუნველყოფის საინსტალაციოდ, მესამეს 200 გიგაბაიტისან (შემდგომში **D:** დისკი) - მეოთხესაც 200 გიგაბაიტისან (შემდგომში **E:** დისკი)



სურ.1.2. 9

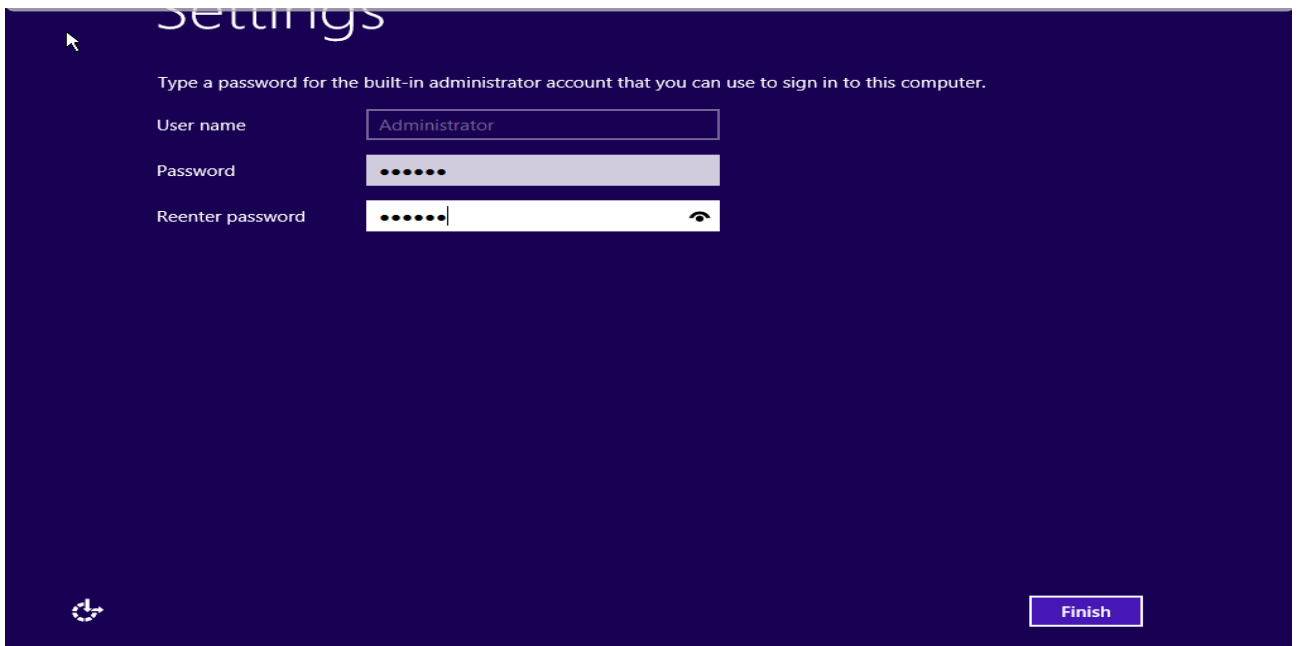
ჩვენს შემთხვევაში, სისტემის დაინსტალებისთვის გამოვყავით 14,3 გიგაბაიტი განყოფილება (სურ. 1.2.9) და ასევე შევექმენით დამატებითი განყოფი ზომით 5,4 გიგაბაიტი.

დაბლითა მხარეს ჩანს ღილაკები **Delete** (დანაყოფის წასაშლელად) და **Format** (დასაფორმატებლად). ავირჩიოთ 14,3 გიგაბაიტიანი ლოგიკური დისკი, რადგან სხვა დანაყოფზე მისი სხვა დანიშნულებიდან გამომდინარე ვერ მოვახდენთ სისტემის დაყენებას და დავაჭიროთ **Next** ღილაკს. დაიწყება მყარ დისკზე **Windows**-ის საინსტალაციო ფაილების ასლის გადმოტანის ინსტალაციის პროცესი (სურ. 1.2.10):



სურ.1.2. 10

მოცემული ეტაპი არის ყველაზე ხანგრძლივი და არ საჭიროებს მომხმარებლისგან რაიმე დამატებით მოქმედებებს. ინსტალაციის პროცესში კომპიუტერი შეიძლება რამდენიმეჯერ ავტომატურად გადაიტვირთოს. ჩვენ უბრალოდ უნდა დაველოდოთ ოპერაციული სისტემის ინსტალაციის დამამთავრებელ ეტაპს.

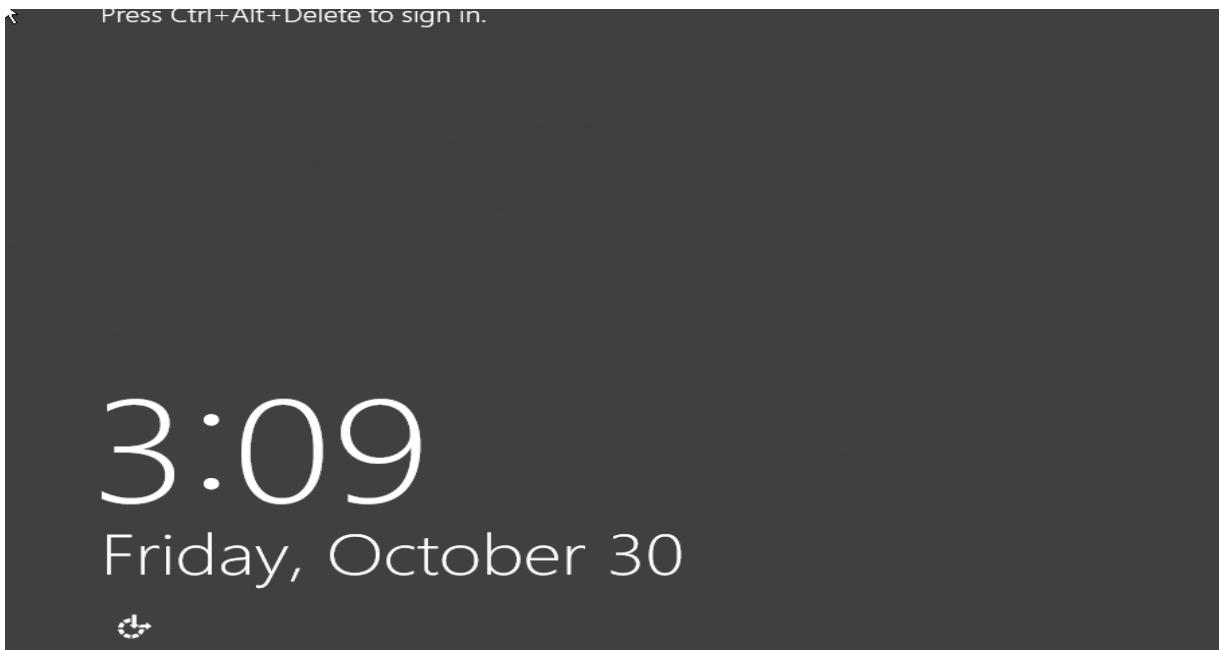


სურ.1.2. 11

სურ 1.2.11-ზე გამოსახულია მომხმარებლის ანგარიშის შექმნის პროცესი, რომელიც აუცილებლად დაცული უნდა იყოს პაროლით.

შენიშვნა: პაროლის შერჩევასა და ისარგებლეთ პაროლის შერჩევის უსაფრთხოების პარამეტრებით

მოცემულ ფანჯარაში უბრალოდ დააწეეთ Finish ღილაკს. რამდენიმე წამის ან წუთის განმავლობაში შესრულდება სისტემის დამამთავრებელი პარამეტრები, რის შემდეგაც ეკრანზე გამოჩნდება სისტემაში ინიცირების ფანჯარა (სურ. 1.2.12):



სურ.1.2. 12

1.3. სერვერული ინფრასტრუქტურის მომსახურება/განვითარება

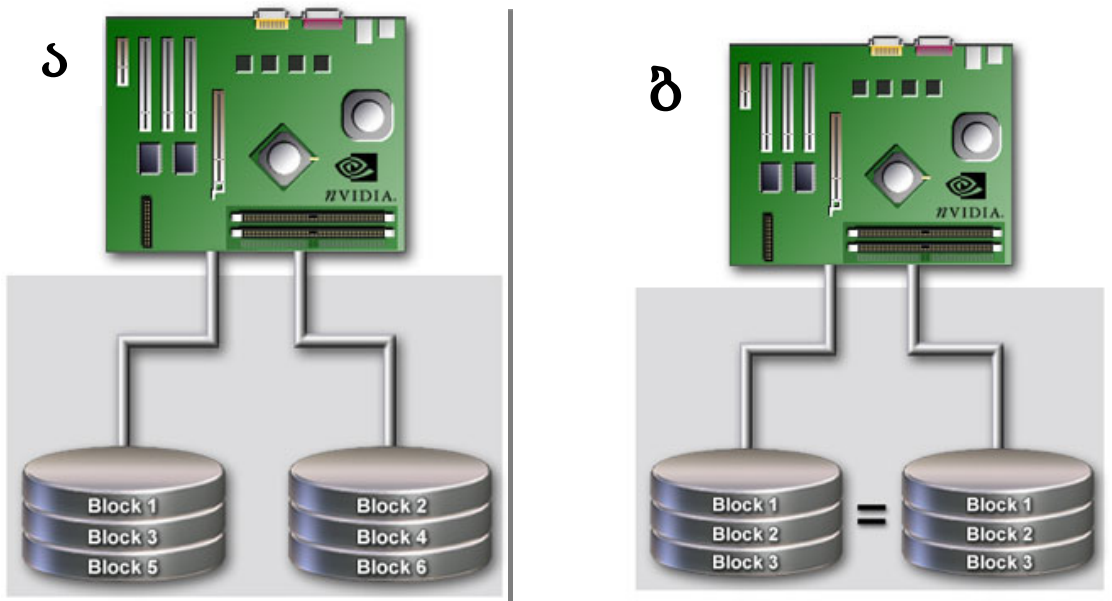
გარე მეხსიერების ის მოწყობილობები, რომლებიც დღევანდელ გამოთვლით სისტემებში გამოიყენება (ხისტი, ნახევარგამტარული, ოპტიკური), თავისთავად წარმოადგენენ ინფორმაციის საიმედო მატარებლებს ფუნქციონირების მრავალწლიანი გარანტიით, თუმცა ცხადია, მათი პირდაპირი გამოყენება განსაკუთრებით სერვერულ

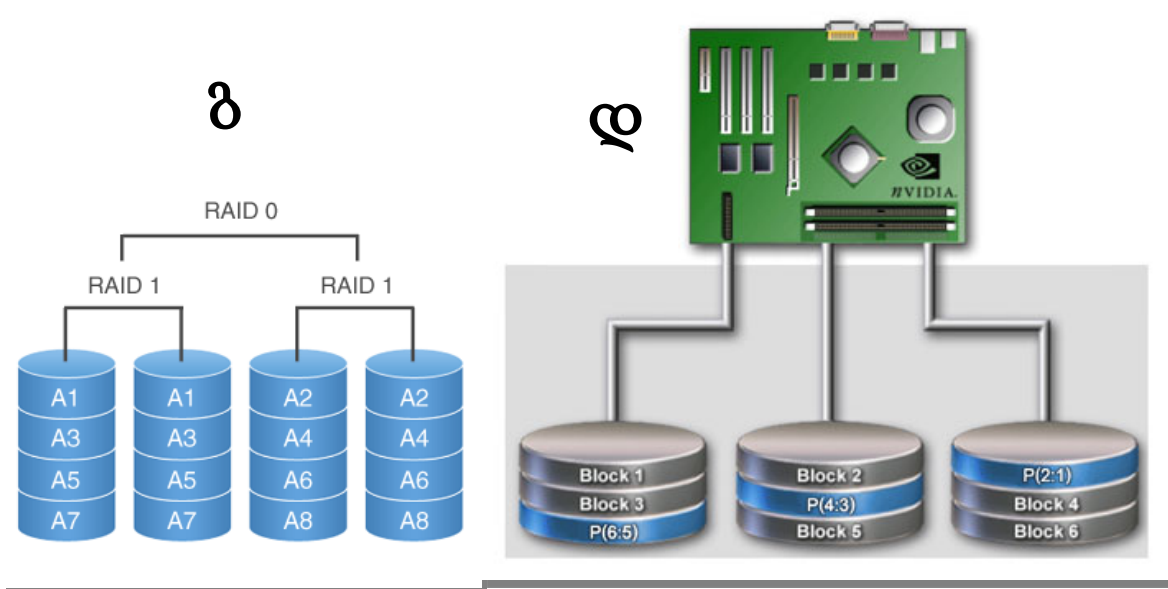
სისტემებში მიუღებელია. კრიტიკული ინფორმაციის (საბანკო და სადაზღვევო მონაცემთა ბაზები, სახელმწიფო და კორპორაციული ინფორმაცია) ერთ ეგზემპლარად შენახვა ინფორმაციის დაკარგვის თუნდაც მინიმალური რისკით გაუმართლებელია. სარეზერვო კოპირების და არქივაციის (იხ. ქვემოთ) ინსტრუმენტები შეიძლება ინფორმაციის კარგვისგან თავდაცვის ერთერთ მოხერხებულ მეთოდად მივიჩნიოთ, მათი გამოყენება მაინც არასაკმარისია ინფორმაციის საიმედო შენახვის პრაქტიკულად გარანტირებული უზრუნველყოფისთვის.

კომპიუტერული აპარატურის მწარმოებლები გვთავაზობენ სხვადასხვა საშუალებს ინფორმაციული სიჭარბის (**Redundancy**) მისაღწევად, რომელთაგან ყველაზე პოპულარულია გარე მეხსიერებაში განლაგებული ინფორმაციის დუბლირების მექანიზმები ეგრეთ წოდებული **RAID**-ტექნოლოგიის გამოყენებით, რომელსაც მოკლედ შევხებით.

RAID გაიშიფრება როგორც Redundant Array of Independent Disks და დისკური მეხსიერებაში განთავსებულ ინფორმაციასთან მიმართვის დაჩქარების ან მისი შენახვის საიმედოობის ამაღლების სხვადასხვა ალგორითმებს შეიცავს. სადღეისოდ არსებობს რამდენიმე **RAID**-არქიტექტურა (**RAID0...RAID6**) ან არქიტექტურათა კომბინაცია (მაგ. **RAID1+0**). ქართულ აიტი-სლენგზე ნახსენები ტერმინები შემდეგნაირად გამოითქმის: მე-10 მასივი - RAID10, მე-5 მასივი - RAID5 და ასე შემდეგ.

ყველაზე გავრცელებულთა ფუნქციონალობის სქემატური ასახვა იხილეთ სურ.1.3.1-ზე.





სურ.1.3. 1 RAID-მასივების ტიპები: ა) RAID0 - სტრაიპი; ბ) RAID1 - სარკე; გ) RAID1+0 კომბინირებული სტრაიპი და სარკე; დ) RAID5 - დისკური მასივი პარიტეტული ბლოკებით

შევხვით მოკლედ ერთერთი, **RAID5**-არქიტექტურის მოქმედების პრინციპს, რომელიც 3-დან 32 ხისტ დისკთან მუშაობის საშუალებას იძლევა. არქიტექტურა ეფუძნება მარტივ ოპერატორს „გამომრიცხავი ან“ (**XOR**), რომელიც ბიტების მიმდევრობათა სიმრავლისგან ე.წ. „პარიტეტული ბლოკების“ მიღებისა და მათგან შემდგომ ბიტების რომელიმე საწყისი მიმდევრობის აღდგენის საშუალებას იძლევა. ამასთან, სტანდარტული არითმეტიკული ოპერაციებისგან განსხვავებით, აღნიშნული ოპერაცია არ იწვევს თანრიგების გადავსებას, რაც მისი გამოყენების ეკონომიურობას და მოხერხებულობას განაპირობებს. პარიტეტული ბლოკების ფორმირებისა და საწყისი ინფორმაციის აღდგენის ნიმუში იხილეთ ნახ. 3-ზე.

	Drive 1	Drive 2	Drive 3	Drive 4
Stripe 1	0100	0101	0010	0011
Stripe 2	0010	0000	0110	0100
Stripe 3	0011	0001	1010	1000
Stripe 4	0110	0001	1101	1010

სურ.1.3. 2 - პარიტეტული ბლოკები (აღნიშნულია ყვითელი ფერით)

პარიტეტული ბლოკის ფორმირების მაგალითი (პირველი სტრაიპისთვის)

$$(0100) \text{ XOR } (0101) \text{ XOR } (0010) = (0011)$$

საწყისი ინფორმაციის აღდგენის მაგალითი (დაკარგულად ითვლება პირველი სტრაიპის პირველი ბლოკი)

$$(0101) \text{ XOR } (0010) \text{ XOR } (0011) = (0100)$$

RAID5-ის მთავარ ღირსებას თანაფარდობის „ინფორმაციის საიმედო შენახვა - სასარგებლო მეხსიერება“ მაღალი კოეფიციენტი წარმოადგენს. მაგალითად, 10-დისკიანი მასივისთვის სასარგებლო მეხსიერება მთლიანი მეხსიერების 90%-ს შეადგენს (ზოგიერთი წინაპირობის შესრულების შემთხვევაში), რაც დისკების „სარკული“ ასახვის 50%-თან შედარებით მაღალი მაჩვენებელია. თანამედროვე მონაცემთა საცავებში უპირატესობა სწორედ **RAID5**-ს ან მის მოდიფიცირებულ ვარიანტს, **RAID6**-ს ენიჭება.

1.3.1. ინფორმაციის მრავალდონური შენახვის მეთოდები

თანამედროვე კორპორაციულ ქსელებში გამოყენებული ინფორმაციის მოცულობა განუხრელად იზრდება. ინფორმაციის შენახვის ტექნოლოგიების მზარდი პროგრესის მიუხედავად, ახალი მეთოდების შემოღების აუცილებლობა დროის მცირე მონაკვეთებში ხდება საჭირო. სადღეისოდ კორპორაციული ინფორმაციის შენახვის ყველაზე პოპულარულ ტექნოლოგიას შენახვის მრავალდონიანი არქიტექტურა (**Multi Tier Storage**) წარმოადგენს, რომელშიც გარკვეული წესების საფუძველზე თავმოყრილია სხვადასხვა მწარმოებლობისა და ღირებულების მოწყობილობები ინფორმაციის შენახვისთვის და მათი მმართველი ინტერფეისები. სადღეისოდ აღნიშნულ მოწყობილობათა შემდეგი კლასები შეიძლება გამოვყოთ:

SSD (Solid State Drive) - მყარსხულიანი დისკური ტექნოლოგია, რომელიც ნახევარგამტარულ ტექნოლოგიას ეფუძნება და საყოველთაოდ ცნობილი ფლემ-მეხსიერების სინონიმს წარმოადგენს. გამოირჩევა უაღრესად მაღალი მწარმოებლობით და ასევე მაღალი ფასით;

SAS/FC (Serial Attached SCSI/Fibre Channel) - ხისტი დისკებზე აგებული ტექნოლოგია, რომელშიც ინფორმაცია კავშირის მაღალსიჩქარიანი არხით (მაგალითად, ოპტიკურბოჭკოვანი არხი) გადაიცემა, ხოლო ინფორმაციის შენახვის ღირებულება საკმაოდ დაბალია;

SATA - ხისტი დისკებზე აგებული ტექნოლოგია, რომელშიც კომბინაცია "მწარმოებლობა/ღირებულება" ყველაზე ოპტიმალურია;

LTO - ლენტური ტექნოლოგია. ყველაზე იაფი და დაბალმწარმოებლური სისტემა ინფორმაციასთან მიმდევრობითი მიმართვით;

Blu Ray - ინფორმაციის შენახვის ოპტიკური ტექნოლოგია დაბალი ღირებულებით და დამაკმაყოფილებელი მწარმოებლურობით.



სურ.1.3.1.1 მონაცემთა მრავალდონიანი საცავის კომპონენტები: SATA და SAS-ინტერფეისები, მყარსხეულიანი დისკი (SSD), მაღალტევადი ოპტიკური დისკი Blu Ray, ლენტური მეხსიერების კარადა

კორპორაციულ ინფორმაციის სხვადასხვა ტიპის საცავებში განაწილებისას მთავარ ამოცანას მოთხოვნის მიხედვით მისი კლასიფიცირება წარმოადგენს. საჭიროა შესრულდეს ინფორმაციის სასიცოცხლო ციკლის ანალიზი, რომლის დროსაც ირკვევა, რომ დროის კონკრეტულ მომენტში კონკრეტული ინფორმაცია ხშირად ან ნაკლები სიხშირით იცვლება, ხოლო რაღაც მომენტიდან იგი პრაქტიკულად აღარ არის საჭირო.

ანალიზის პროცესში გასათვალისწინებელია დაგროვილი ინფორმაციის მოცულობაც. სწორედ ეს პარამეტრი განაპირობებს მრავალდონიან ინფორმაციულ საცავებში მონაცემთა მიგრაციის საჭიროებას და სიხშირეს, რისთვისაც სპეციალური პროგრამული უზრუნველყოფა არსებობს. იგი ავტომატურ რეჟიმში ასრულებს ინფორმაციის გადატანას მრავალდონიანი არქიტექტურის ფარგლებში, ინფორმაციის სტატუსის გათვალისწინებით.

თანამედროვე კორპორაციულ ქსელებში ინფორმაციის შენახვის და მართვის ყველაზე ოპტიმალურ სტრუქტურად სამდონიანი არქიტექტურა (**3-Tier Architecture**) ითვლება, რომელშიც ყოველ დონეს საკუთარი აგებულება და ამოცანები გააჩნია (სურ.1.3.1.2).



სურ.1.3.1.2 ინფორმაციის შენახვის სამდონიანი არქიტექტურის ზოგადი სქემა

პირველ, ე.წ. მწარმოებლურობის დონეზე (**Performance Tier, Tier 1**) პირველადი, ყველაზე ხშირად გამოსაყენებელი ინფორმაცია ინახება. მოცემული დონის ფიზიკური შემადგენლობა წარმოადგენს სწრაფქმედი **SAS/FC**-დისკების მასივს ინფორმაციის საიმედო შენახვის **RAID**-ინტერფეისებით. ამავე დონეზე მოიაზრება **SSD**-დისკების გარკვეული რაოდენობაც განსაკუთრებით აქტუალური ინფორმაციული მასივების შესანახად, თუმცა ჯერჯერობით ამგვარი დისკების ხვედრითი წილი კორპორაციულ ინფორმაციულ საცავებში ჯერ კიდევ დაბალია, რასაც მათი სიძვირე განაპირობებს.

მეორე დონე (**Capacity Tier, Tier 2**), რომელსაც "მოცულობითი დონე" ეწოდება, კორპორაციის ძირითადი, შედარებით ნაკლებაქტუალური ინფორმაციული მასივების შენახვას ემსახურება და როგორც წესი, **SATA/RAID**-ტექნოლოგიით ორგანიზებული გარე მეხსიერების მასივების ერთობლიობას წარმოადგენს.

მესამე, არქივაციის დონე (**Archive Tier, Tier 3**) გრძელვადიანი არქივების შესანახადაა განკუთვნილი და ლენტური და ოპტიკური შემნახველი მოწყობილობების საფუძველზეა აგებული. ამასთან, როგორც წესი, პრიორიტეტი ლენტური მეხსიერების აპარატურას ენიჭება, როგორც მეხსიერების დიდი მოცულობის, ასევე მეხსიერების მოწყობილობათა (მეხსიერების კასეტები) დიდი, ავტონომიური სისტემების აგების შესაძლებლობათა გამო. არქივაციის დონეზე ინფორმაციის ცვლილება ან წაშლა მეტწილად მხოლოდ წინაწარ განსაზღვრულ, გრძელვადიან პერსპექტივაში ხდება.

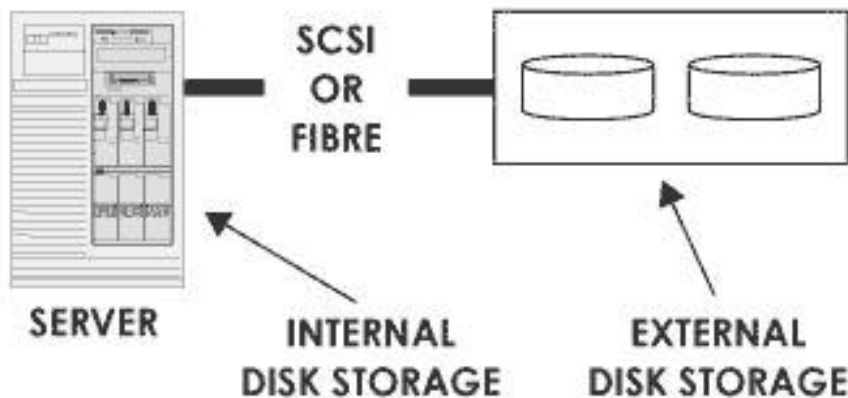
აღწერილ დონეებს შორის ინფორმაციის ავტომატური მიგრაცია, როგორც აღვნიშნეთ, მონაცემთა მართვის წინასწარ განსაზღვრული წესებით სრულდება, შესაბამისი პროგრამული უზრუნველყოფის გამოყენებით.

1.3.2. მონაცემთა საცავები

წინა ქვეთავში განხილული მონაცემთა შენახვის ფიზიკური ინფრასტრუქტურის დანიშნულებაა ინფორმაციის საიმედო და ოპტიმალური შენახვის უზრუნველყოფა და დროული მიწოდება მომხმარებლებისთვის. მეორე მოთხოვნა პირველზე არანაკლებ მნიშვნელოვანია, რადგან ინფორმაციის დაგვიანებით მიღება ხშირ შემთხვევაში მისი არმიღების ტოლფასია. სადღეისოდ არსებობს ინფორმაციის შენახვის ისეთი სისტემები, რომლებიც მომხმარებლებს მონაცემებთან მაქსიმალურად ეფექტური მიმართვის და მათი საიმედო შენახვის საშუალებებს სთავაზობენ.

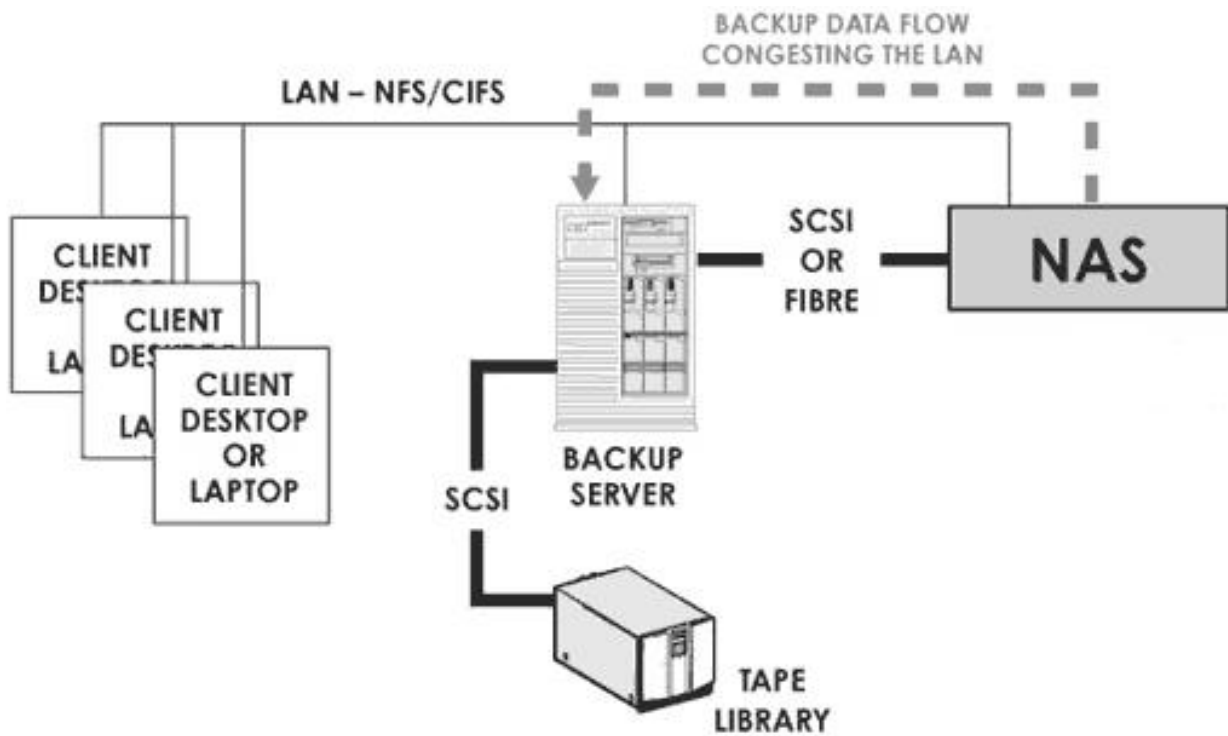
განვიხილოთ რამდენიმე ყველაზე გავრცელებული სისტემა, კერძოდ, **DAS, NAS** და **SAN**-სისტემები.

DAS (Direct Attached Storage) - მოწყობილება შიდა მეხსიერებით, პირდაპირ უერთდება ძირითად კომპიუტერს და ძირითადად ლოკალური სარეზერვო კოპირების ამოცანებს ემსახურება. მარტივად რომ ვთქვათ, **DAS** არის ჩვეულებრივი ხისტი დისკი, რომელიც ჰოსტთან დასაკავშირებლად ფართოდ გავრცელებულ **SCSI**-ტექნოლოგიას (**Small Computer System Interface**) იყენებს.



სურ.1.3.2.1 DAS-სისტემის სქემა

DAS-სისტემა ვერ უზრუნველყოფს მონაცემთა სარეზერვო კოპირებას რამდენიმე ჰოსტიდან, მითუმეტეს მონაცემთა განაწილებას. ამგვარი მოწყობილობის დაყენება სარეზერვო კოპირების იაფფასიანი ვარიანტია, თუმცა გამოუსადეგარი მეტნაკლებად დიდი ორგანიზაციის კომპიუტერულ ქსელში.



სურ.1.3.2. 2 NAS-სისტემის სქემა

NAS (Network Attached Storage) - "მონაცემთა ქსელური საცავი". წარმოადგენს კომპიუტერული ქსელის სრულფუნქციონირებელ წევრს შესაბამისი საიდენტიფიკაციო მონაცემებით (**MAC** და **IP-მისამართები**). **NAS**-სერვერის ძირითად ფიზიკურ კომპონენტს, როგორც წესი, 1 ან მეტი მეხსიერების ხისტი დისკი წარმოადგენს, თუმცა ხანდახან მის კონფიგურაციაში ოპტიკული ან ლენტური მოწყობილობებიცაა გათვალისწინებული. **NAS-მოწყობილობა (NAS Appliance)** მარტივად ირთვება ქსელში და წარმოადგენს ფაილ-სერვერს საკუთარი მცირე ოპერაციული სისტემითა და მართვის ვებ-ბაზირებული ინტერფეისით. **NAS-სერვერები** გარეგნულად **DAS-მოწყობილობებს** ჰგავს, მაგრამ პრინციპული განსხვავება მისგან ფაილებთან ქსელური წვდომის ეფექტური საშუალებებით.

SAN (Storage Area Network) - "მონაცემთა საცავების ქსელი" მაღალი საიმედოობისა და სისწრაფის გამო სადღეისოდ მონაცემთა საიმედო შენახვის ყველაზე გავცელებულ ტექნოლოგიას წარმოადგენს და მასობრივად იწერება კორპორაციულ ქსელებში.

ტექნოლოგია ეფუძნება გამოყენებულია ძალიან სწრაფ ოპტიკურ-ბოჭკოვანი კავშირის **Fibre Channel**-ტექნოლოგიას, რომელიც ინფორმაციის გადაცემის სიჩქარეა 1-2 გბ/წმ სიჩქარეს უზრუნველყოფს. ამასთან, მონაცემთა საცავის ქსელი ფიზიკურად

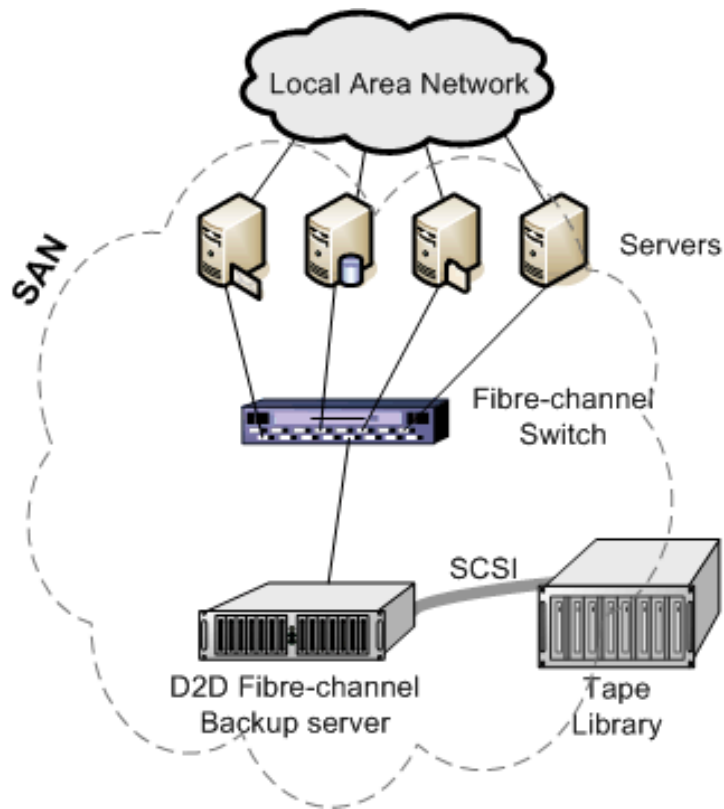
გამოცალკევებულია ძირითადი კორპორაციული ქსელიდან, რაც ძლიერ ზრდის სარეზერვო ასლების შექმნისა და არქივაციის პროცედურების ეფექტურობას და ინფორმაციის შენახვის საიმედოობას. ამასთან, მნიშვნელოვანია ძირითადი ქსელური არხების განტვირთვის ფაქტორიც, რადგან სწორედ აღნიშნული პროცედურები (სარეზერვო კოპირება, არქივაცია) მოითხოვენ ყველაზე დიდი ოდენობით ქსელურ რესურსებს და ინფორმაციული არხების მაღალ გამტარუნარიანობას.

სადღისოდ სერვერული სისტემების ბაზარზე **SAN**-საცავების საკმაოდ ბევრი ვარიანტი არსებობს, რაც დამკვეთი კომპანიების ერთმანეთისგან რადიკალური მოთხოვნების დაკმაყოფილებას უზრუნველყოფს.

მაგალითად, **Fibre Channel** ტექნოლოგიის გამოყენება შეიძლება 100 კილომეტრის რადიუსში (შედარებისთვის: ჩვეულებრივი **SCSI**-ინტერფეისების მოქმედების რადიუსი მხოლოდ 25 მეტრს შეადგენს).

SAN-ქსელის ცენტრალურ კომპონენტს ოპტიკური არხის ადაპტერი (**Fibre Channel host bus adapter – FC HBA**), რომელიც სერვერებსა და მონაცემთა საცავებს შორის კავშირს უზრუნველყოფს. კერძოდ, იგულისხმება შემდეგი ფუნქციონალობა:

- ინტერფეისი სერვერებსა და მონაცემთა საცავებს შორის ნებისმიერი ქსელური ტოპოლოგიის ფარგლებში
- მონაცემთა საცავების ცენტრალიზებული მართვა (კონფიგურება, მონიტორინგი და ქსელის კომპონენტების ანალიზი).
- დისკურ მასივებთან წვდომის უფლებების მართვა.



სურ.1.3.2. 3 SAN-სისტემის სქემა

1.3.3. მონაცემთა დამუშავების ცენტრი

მონაცემთა საცავების ყველაზე მასშტაბურ მოდიფიკაციას **მონაცემთა დამუშავების ცენტრი (Data Center)** წარმოადგენს, რომელიც დიდი მოცულობის და მრავალფეროვანი ინფორმაციის (ტექსტური, მონაცემთა ბაზები, მულტიმედია) ეფექტურ და საიმედო შენახვას უზრუნველყოფს. მონაცემთა დამუშავების ცენტრი შედარებით ნაკლებადაა გავრცელებული მისი მაღალი ღირებულების გამო. საკუთარი მონაცემთა ცენტრები გააჩნიათ მეტწილად დიდ კორპორაციებს და ინტერნეტ-სერვის-პროვაიდერებს, რომლებიც მომხმარებლებს კარგად განვითარებულ ჰოსტინგის სერვისს სთავაზობენ.

სარეზერვო კოპირება და არქივაცია

კორპორაციული ქსელის სერვერული სისტემა წარმოდგენელია კარგად გამართული სარეზერვო კოპირებისა და არქივაციის სისტემის გარეშე. ინფორმაციის

სარეზერვო საცავები გვამღებენ გარანტიას, რომ კორპორაციული ინფორმაცია არ დაიკარგება უკიდურეს შემთხვევაშიც კი, ხანძრის ან სტიქიური უბედურების შედეგად.

სარეზერვო კოპირების მრავალფეროვანი სისტემები არსებობს, რომელთაგან თითოეულს საკუთარი გამოყენების სფერო გააჩნია კომპიუტერული ქსელის მასშტაბებისა და შესასრულებელ ამოცანათა მოცულობის მიხედვით.

1.3.4. კლასტერული არქიტექტურა

კლასტერული არქიტექტურა სერვერულ სისტემებში (განსაკუთრებით მონაცემთა ბაზის სერვერებზე) ერთერთ ყველაზე აპრობირებულ ტექნოლოგიას წარმოადგენს.

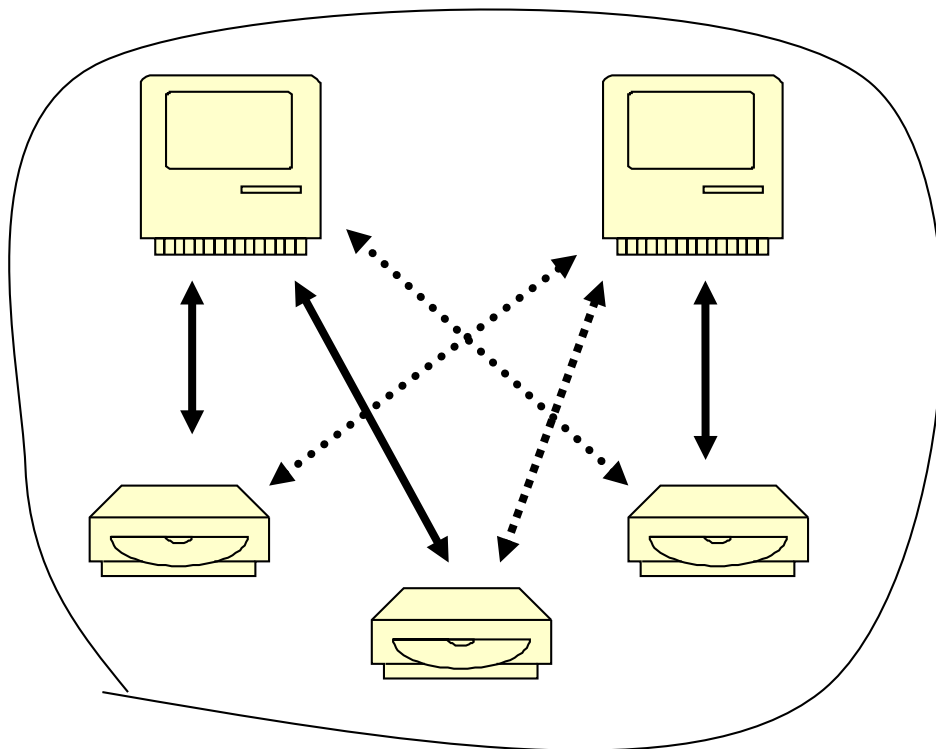
კლასტერი - ეს არის კომპიუტერების ჯგუფი რომელიც შედგება ორი ან მეტი კომპიუტერებისგან, რომლებიც მუშაობენ ერთად იმისთვის, რომ უზრუნველყონ პროგრამების საერთო ნაკრების ან სერვისების მუშაობა რომლებსაც მომხმარებელი აღიქვამს როგორც ერთ მთლიანს. კომპიუტერები ფიზიკურად ერთიანდებიან აპარატურული საშუალებებით ქსელის სახით ან საერთო შესანახი მოწყობილობებით. კლასტერების პროგრამული უზრუნველყოფა უზრუნველყოფს საერთო ინტერფეისს, ამასთან ერთად მართავს რესურსებს და კლასტერის შიგნით მყოფი კომპიუტერების დატვირთვას.

კლასტერი შემდეგი ძირითადი ელემენტებისგან შედგება

- **კვანძი** (როგორც წესი, ფიზიკური ან ვირტუალური სერვერი)
- **რესურსთა ჯგუფი**
 - **ქვორუმ-რესურსი** (ხისტი დისკი კლასტერის კონფიგურაციის მონაცემთა ბაზით)
 - **რესურსები** (ფიზიკური დისკი ლოკალური ან გარე მეხსიერების მასივიდან, IP-მისამართი, კომპიუტერის ქსელური სახელი (ვირტუალური სერვერი), სისტემური სერვისი, განაწილებული ფოლდერი, განაწილებული პროგრამა, ვირტუალური მანქანა

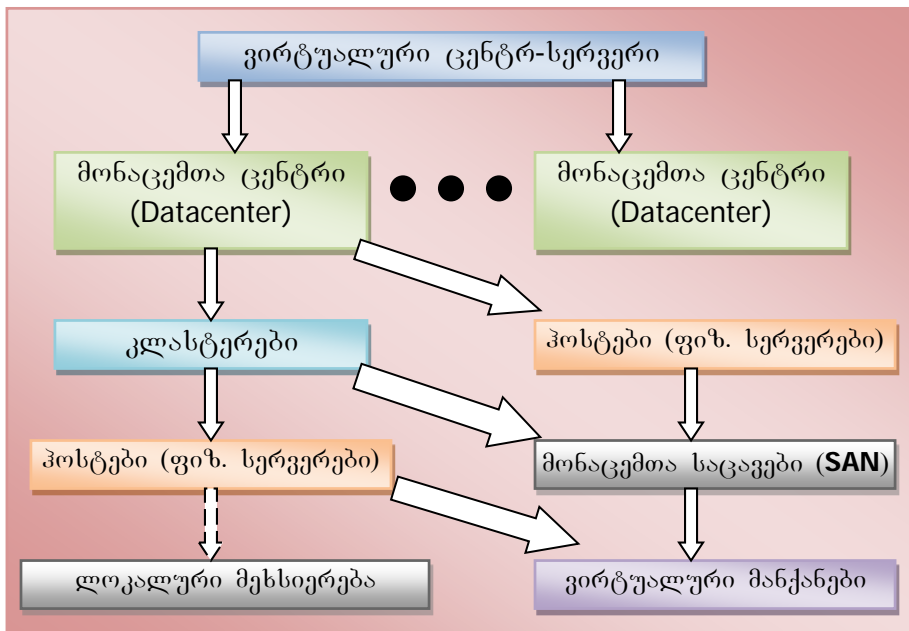
კლასტერის ელემენტებს შორის დამოკიდებულებებს შემდეგი სახე აქვს: **რესურსი** -> **რესურსი** (მაგ. განაწილებული ფოლდერი -> ხისტი დისკი). მოქმედებს იერარქიულობის პრინციპი

კლასტერის მუშაობის პრინციპი: კლასტერის რომელიმე კვანძის მწყობრიდან გამოსვლისას მასზე განთავსებული რესურსები ავტომატურად გადამისამართდება აქტიურ კვანძზე (**Failover**). სისტემა აგრძელებს მუშაობას (სურ.1.3.4.1).



სურ.1.3.4.1 კლასტერის მუშაობის პრინციპი

ზემოთ აღწერილი ტექნოლოგიების კომბინირებული გამოყენება რთული სერვერული სისტემების დაპროექტებისა და აგების საშუალებას იძლევა. სერვერული სისტემის ზოგადი სტრუქტურა სურ.1.3.4.2-ზეა მოცემული.



სურ.1.3.4. 2 ვირტუალური სერვერული სისტემის არქიტექტურა

როგორც ნახაზი უჩვენებს, ინტეგრირებული სერვერული არქიტექტურა შეიძლება გასცდეს კიდევ კორპორაციული ქსელის ფარგლებს და მონაცემთა ცენტრის სახით რამდენიმე ქსელის ინფორმაციული სივრცე მოიცვას, თუმცა უნდა აღინიშნოს, რომ პრაქტიკაში ამგვარი შემთხვევები შედარებით ნაკლებია.

პრაქტიკული სავარჯიშო

ვირტუალურ მანქანაზე Windows Server 2012-ის დაყენება

დააინსტალირეთ ოპერაციული სისტემა შემდეგი პარამეტრებით

- ოპერაციული სისტემის ენა - ინგლისური;
- თარიღის, ფულადი და წერის რეჟიმები - ინგლისური;
- ოპერაციული სისტემა **Windows server 2012** Server with GUI 64ბიტანი;
- შექმენით მყარი დისკის ორი დანაყოფი ზომებით: **I დანაყოფი - 100GB, II – 20GB;**

III – 20GB;

- დააფორმატეთ სამივე ლოგიკური დისკი;
- სისტემა დააყენეთ **I** დანაყოფზე;
- მომხმარებლის ანგარიში - დაიცავით პაროლით

ცოდნის შეფასება

I - პრაქტიკული დავალება

სტუდენტებს მიეცემათ პრაქტიკული დავალება

- შეასრულონ სერვერული ინფრასტრუქტურის შემადგენელი აპარატურული კომპონენტების დაკავშირება
- მოახდინონ სერვერული ოპერაციული სისტემის ინსტალაციის მომზადება
- დააინსტალირონ სერვერული ოპერაციული სისტემა

შემფასებელი აკვირდება შესაფასებელ პირის მუშაობას პროფესიული სტანდარტით (პროგრამით / მოდულით) განსაზღვრული ამოცანების შესრულების პროცესში. დაკვირვება ხორციელდება კომპიუტერებით აღჭურვილ ლაბორატორიაში, სადაც შესაფასებელი პირი პრაქტიკულ საქმიანობას ეწევა. შემფასებელმა წინასწარ უნდა დაგეგმოს დაკვირვების პროცესი, იმის დასადგენად, თუ რამდენად სწორად იყენებს შესაფასებელი პირი ცოდნას, უნარებსა და ყველა რესურსს შედეგის მისაღწევად.

შეფასება განხორციელდება პროცესზე დაკვირვებით, წინასწარ განსაზღვრული შეფასების ინდიკატორების საფუძველზე.

დავალების ნიმუში და შეფასების რუბრიკა

პროცესზე დაკვირვება

- ✚ დააკავშიროს სერვერული ინფრასტრუქტურის აპარატურული კომპონენტები
- ✚ მოახდინოს სერვერული ოპერაციული სისტემის ინსტალაცია

სწავლის შედეგი	N	დასახელება	შეფასება	
			კი	არა
სერვერული ინფრასტრუქტურის გამართვა	1.	დავალების შესაბამისად დააკავშირა კომპონენტები		
	2.	დავალების შესაბამისად შექმნა სისტემური და ლოგიკური დისკები		
	3.	დავალების შესაბამისად დააინსტალირა სერვერული ოპერაციული სისტემა		

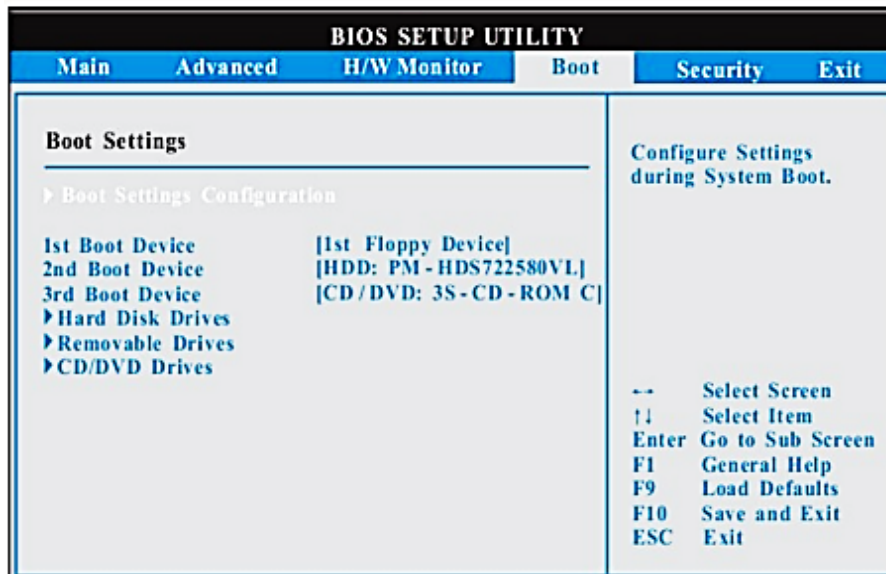
სწავლის შედეგი ჩაითვლება მიღწეულად თუ სტუდენტმა შეძლო შედეგის ყველა პუნქტის შესრულება

II - ტესტირება კითხვები მრავალი არჩევითი პასუხით

ასეთი ტიპის დავალება ორი ნაწილისგან შედგება. პირობის, რომელიც ჩამოყალიბებულია შეკითხვის ან არასრული მტკიცებულების სახით (ძირითადი მოცემულობა) და პასუხების ვარიანტებისგან. სავარაუდო პასუხი ძირითადად 4 ან 5-ია, რომელთაგან სტუდენტმა სწორი ვარიანტი უნდა აირჩიოს. საბოლოოდ ხდება პასუხების ტესტის გასაღებთან შედარება და სწორი პასუხების მიხედვით ქულების დათვლა. სწორ პასუხს ეწოდება საკვანძო, არასწორს - დისტრაქტორი (დამაბნეველი პასუხი). დისტრაქტორად ირჩევენ იმ ტიპურ შეცდომებს, რომელთაც ხშირად უშვებენ სტუდენტები.

ტესტის ნიმუში

მოცემული სურათის მიხედვით, მართებულია მსჯელობა...



Choose one answer.

- a. Floppy დისკვანაკვითხველის არ არსებობის შემთხვევაში ჩატვირთვა მოხდება CD/DVD დისკიდან
- b. კომპიუტერი მზადაა ქსელური ჩატვირთვისთვის
- c. სურათის მიხედვით BIOS-ში არ არის გააქტიურებული ქსელური ჩატვირთვის სერვისი
- d. ჩატვირთვის მიმართვის საწყისი ობიექტია მყარი დისკი

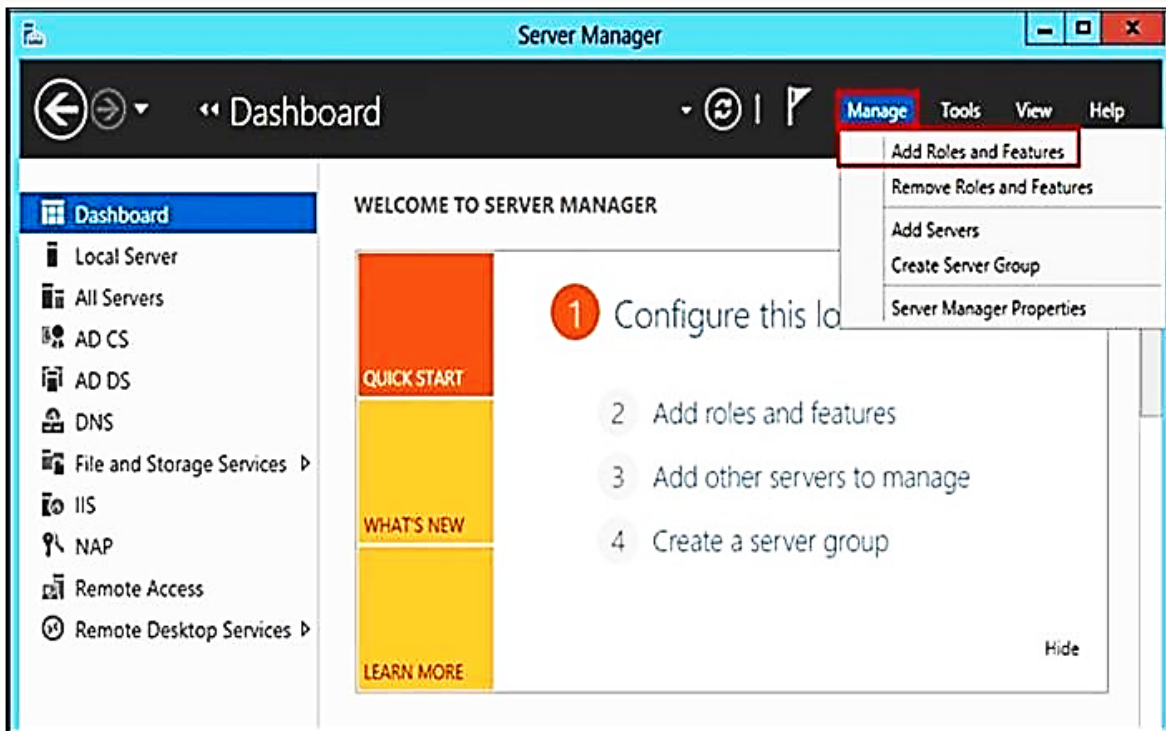
მოცემული სურათის მიხედვით, მცდარია მსჯელობა:



Choose one answer.

- a. სურათზე ასახულის მიხედვით დასაკავშირებელი სერვერის მისამართია 10.0.0.100
- b. სურათზე ასახულის მიხედვით დასაკავშირებელი სერვერის მისამართია 10.0.0.1
- c. სურათზე ასახულია ქსელური სერვისებით ჩატვირთვის პროცესი
- d. ქსელური სერვისებიდან ჩატვირთვის დასაწყებად უნდა დავაჭიროთ F12 ღილაკს

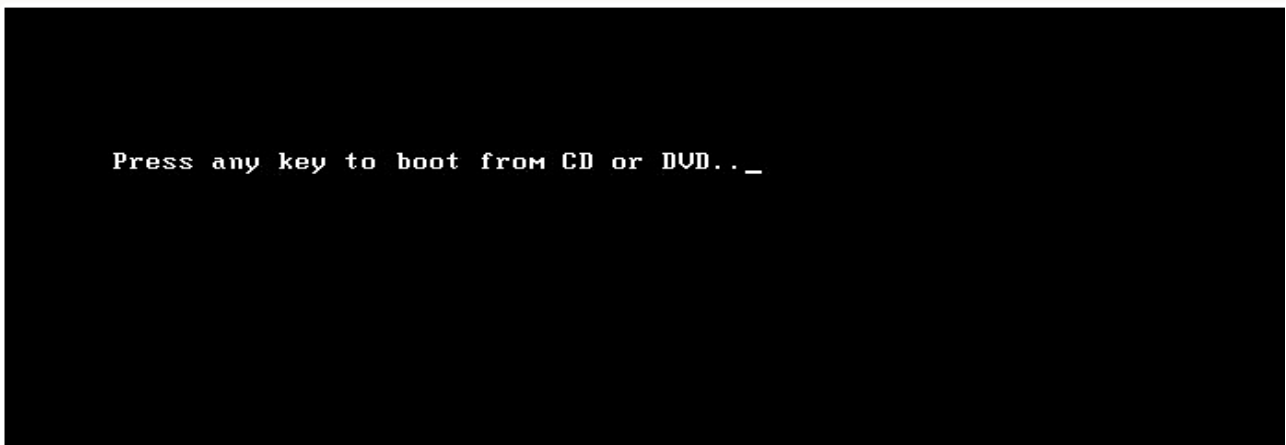
ქვემოთ მოცემული სურათის მიხედვით რომელი მსჯელობა არ არის სწორი?



Choose one answer.

- a. მოცემულ სერვერზე დამატებულია Internet Information Services სერვისი(Role)
- b. მოცემულ სერვერს უკვე ინსტალირებული სერვისების მეშვეობით შეუძლია დომენში გაწევრიანებულ კლიენტ-კომპიუტერებს დაურთოს ლოგიკური მისამართები
- c. მოცემულ სერვერს უკვე ინსტალირებული სერვისების მეშვეობით შეუძლია დომენში გაწევრიანებულ კლიენტ-კომპიუტერებს მიანიჭოს FTP სერვერზე წვდომა
- d. მოცემულ სერვერზე დამატებულია DNS სერვისი(Role)

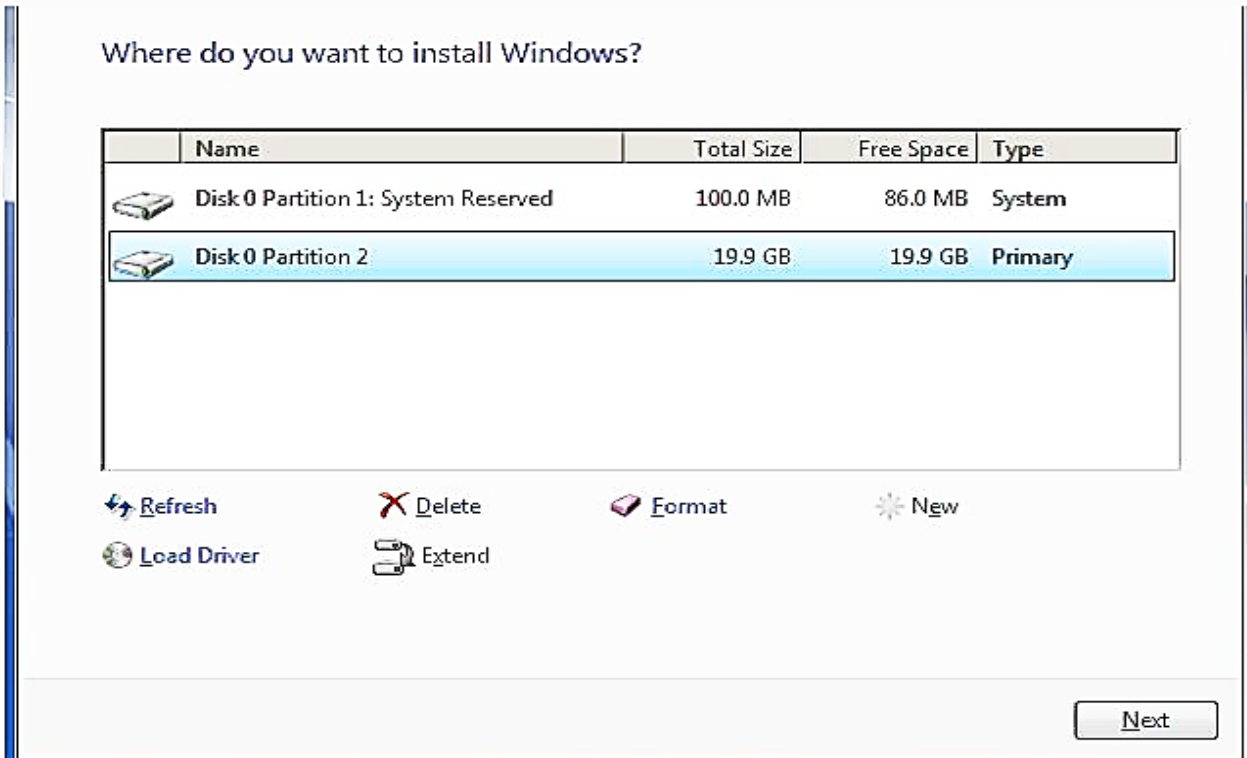
სურათზე მოცემული ჩანაწერის შესაბამისად მართებულია მსჯელობა:



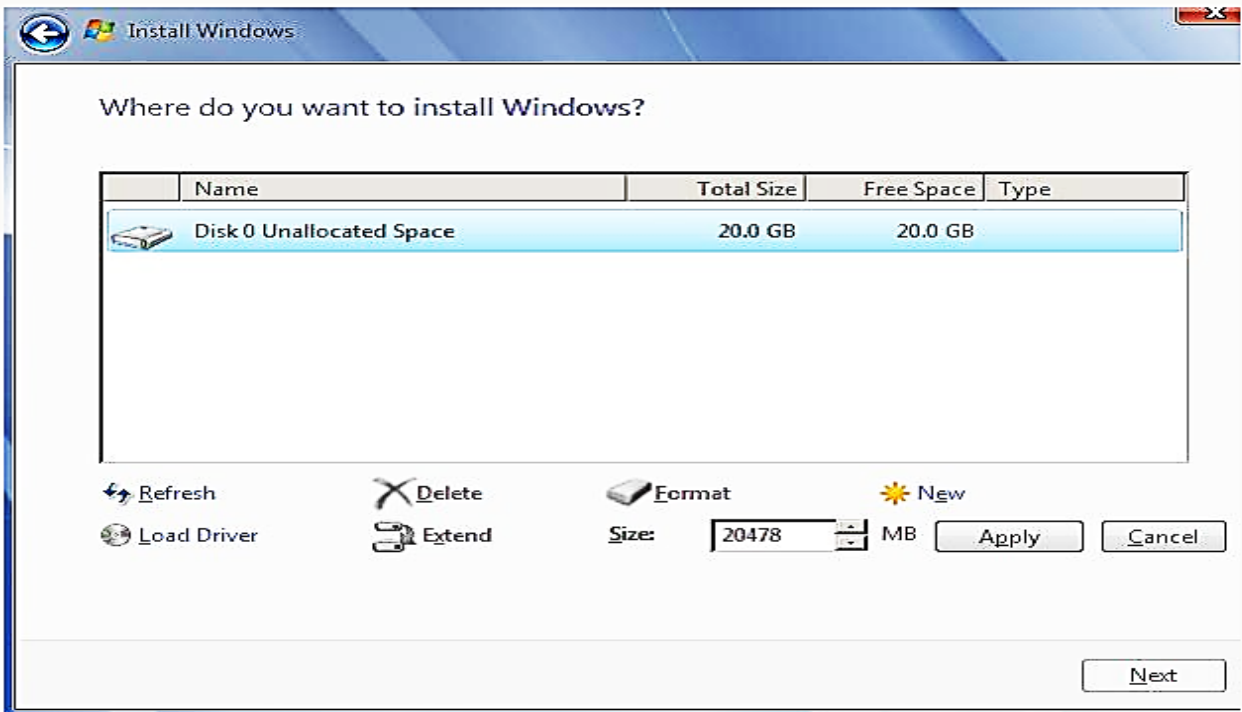
Choose one answer.

- a. მოცემული შეტყობინების იგნორირების შემთხვევაში ოპერაციული სისტემა ჩაიტვირთება CD-DVD დისკვამპითხველიდან
- b. რომელიმე ღილაკზე დაჭერის შემთხვევაში ოპერაციული სისტემა ჩაიტვირთება CD-DVD დისკვამპითხველიდან
- c. პირველ ჩამტვირთავ მოწყობილობად არჩეულია Floppy დისკვამპითხველი
- d. პირველ ჩამტვირთავ მოწყობილობად არჩეულია მყარი დისკი

მოცემული სურათის მიხედვით, როცა საჭიროა მყარი დისკის 2 ლოგიკურ დისკად გაყოფა, ვირჩევთ ბრძანებას -



სურათის მიხედვით რომელი მსჯელობაა სწორი?

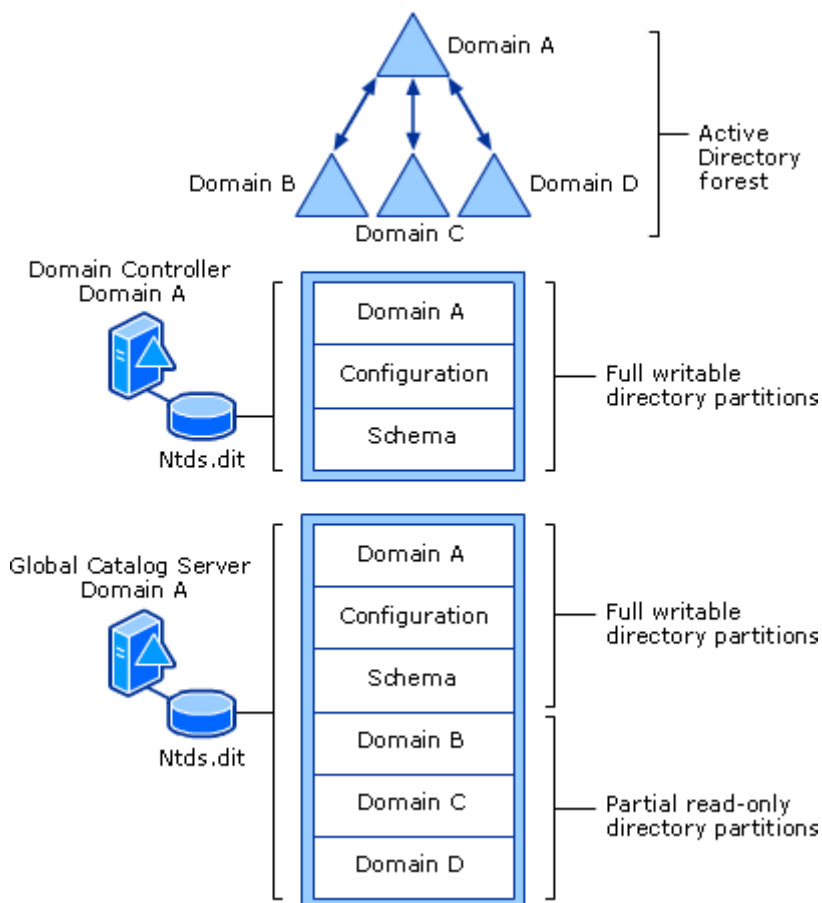


Choose one answer.

- a. მყარ დისკზე შექმნილია ერთი ლოგიკური დისკი და მისი ზომაა 20 გბაიტი
- b. დისკის დასაყოფად აუცილებელია Delete ბრძანების არჩევა
- c. ოპერაციული სისტემა ჩაწერილია 20 გბაიტი მოცულობის ლოგიკურ დისკზე
- d. ამ ეტაპზე მყარი დისკი არ არის დაყოფილი ლოგიკურ დისკებად

2. დირექტორიების სერვისების გამართვა

კატალოგების სამსახურების ძირითადი დანიშნულებაა ქსელური უსართხოების მართვა. ქსელური უსაფრთხოების საფუძველია მომხმარებელთა, მომხმარებელთა ჯგუფებისა და კომპიუტერების საადრიცხო ჩანაწერების მონაცემთა ბაზა (**accounts**), რომელთა საშუალებითაც ხორციელდება დაშვებების მართვა ქსელურ რესურსებზე (სურ.2.1).



სურ.2.1 კატალოგური სერვისის ზოგადი სქემა

კატალოგური სქემის აგება აუცილებელია შედარებით დიდი ზომის ლოკალურ ქსელებში, სადაც ვერ გამოიყენება მოდელი „სამუშაო ჯგუფი“, რომელიც ყველა სხვა მოდელზე პრიმიტიულია.

„სამუშაო ჯგუფი“ დანერგვა მცირე ქსელებშია მიღებული (3–10 კომპიუტერი). იგი ეფუძნება არქიტექტურას, რომელშიც ქსელის ყოველ კომპიუტერს (ოპერაციული სისტემებით **Windows NT/2000/XP/2003/Vista/2008/7/8/ 8.1/10**) გააჩნია საადრიცხო ჩანაწერთა საკუთარი, ლოკალური მონაცემთა ბაზა და მისი დახმარებით

ხორციელდება დაშვებების მართვა მოცემული, კონკრეტული კომპიუტერის რესურსებზე. საადრიცხვო ჩანაწერების ლოგიკური მონაცემთა ბაზა (**SAM - Security Account Manager**) ინახება ოპერაციული სისტემის რეესტრში და იგი სრულებით იზოლირებულია სხვა კომპიუტერების ანალოგიური ბაზებისგან.

მოდელი „სამუშაო ჯგუფი“ შედარებით მარტივი აგებულებით გამოირჩევა და ადმინისტრირების მინიმალურ ხარჯებს მოითხოვს, მაგრამ იმ ქსელებში, სადაც მრავალი კომპიუტერი გამოიყენება, ქსელური რესურსების მართვის პროცესი რთულდება. მომხმარებლებს უწევთ ყოველ კომპიუტერზე საკუთარი საადრიცხვო ჩანაწერების ხელით შექმნა ერთი და იგივე პაროლებით, რაც ინფორმაციის შენახვისა და მასთან მიმართვის სიცხადეს მეტად ამცირებს.

შედარებით დიდი ქსელების სამართავად დამუშავებულია **დომენური მოდელი**, რომელიც მოიცავს კატალოგურ სერვისს და ამ სერვისის ერთიან მონაცემთა ბაზას. დომენური მოდელის სამოქმედო სივრცე შეიძლება იყოს მთლიანი კორპორაციული ქსელის ან სულაც ქსელთა სიმრავლე

დომენური მოდელი იყენებს სპეციალიზებულ სერვერებს, რომელთაც **დომენის კონტროლერები** ეწოდებათ.

დომენური მოდელის ძირითადი ტერმინოლოგია მოცემულია ქვემოთ:

ერთიანი კატალოგი წარმოადგენს ინფორმაციის ნაკრებს ცალკეულ მომხმარებელთა და მათი ჯგუფების, ქსელში შემავალი კომპიუტერების, ქსელური პრინტერების, საერთო ფაილური რესურსებისა და სხვა ელემენტების შესახებ – ყველა ამ ელემენტს ობიექტი ეწოდება. ობიექტებს გააჩნიათ თვისებები (**ატრიბუტები**). მაგალითად, მომხმარებლის კატალოგში შენახულ ატრიბუტები შეიძლება იყოს სახელი, ტელეფონის ნომერი, მისამართი, სახელი სისტემაში შესასვლელად, პაროლი, ჯგუფები, რომლებშიც მოხმარებელი შედის და სხვა.

Windows-ბაზირებულ ოპერაციულ სისტემებში დომენური სისტემის სამართავად გამოიყენება სისტემა **Active Directory (AD)**, რომელიც არა მარტო საბაზო (მომხმარებელი, მომხმარებელთა ჯგუფი, კომპიუტერი), არამედ კომპლექსური ობიექტების, ეგრეთ წოდებული „ორგანიზაციული ქვედანაყოფების“ შექმნისა და

მართვის საშუალებას, აგრეთვე კატალოგური სისტემის ფიზიკური და ლოგიკური დეკომპოზიციის საშუალებას იძლევა (ე.წ. „საიტების“ სახით).

კორპორაციული ქსელის კატალოგური სერვისის **Active Directory** უზრუნველყოფს შემდეგ ფუნქციონალობას:

- **ერთიანი რეგისტრაცია ქსელში.** მომხმარებლები შეიძლება დარეგისტრირდნენ ქსელში ერთი სახელითა და პაროლით და ამასთან მიიღონ დაშვება ყველა ქსელურ რესურსებთან და სამსახურთან (ქსელური ინფრასტრუქტურების სამსახური, ფაილების სამსახური და შეჯგუფების სამსახური, დანართების და მონაცემთა ბაზის სერვერები და ა.შ.)
- **ინფორმაციის უსაფრთხოება.** აუთენტიფიკაციის საშუალებები და რესურსებთან დაშვების მართვა.
- **ცენტრალიზებული დაცვა.** ქსელის ადმინისტრატორებს შეუძლიათ ერთიანად მართონ ყველა კორპორაციული რესურსი.
- **ადმინისტრირება ჯგუფური პოლიტიკის გამოყენებით.** კომპიუტერის დატვირთვისას ან მომხმარებლის რეგისტრაციისას სისტემაში ხორციელდება ჯგუფური პოლიტიკის მოთხოვნები, მათი კონფიგურაცია ინახება ჯგუფური პოლიტიკის ობიექტებში (**GPO – Group Policy Objects**) და გამოიყენება კომპიუტერების მომხმარებლების საადრიცხვო ჩანაწერებში.
- **ინტეგრაცია DNS-თან.** კატალოგების სამსახურის ფუნქციონირება მთლიანად დამოკიდებულია დომენურ სახელთა სერვისის (**DNS**) სერვისების მუშაობაზე. თავის მხრივ სერვერების **DNS**-ებს შეუძლია შეინახონ ზონების ინფორმაცია **Active Directory**-ის მონაცემთა ბაზაში.
- **კატალოგის გაფართოებადობა.** ადმინისტრატორებს შეუძლიათ დაუმატონ კატალოგების სქენაში ახალი ობიექტების კლასები ან დაუმატონ ახალი ატრიბუტები არსებულ კლასებს.
- **მასშტაბირება.** **Active Directory**-ის სამსახურმა შეიძლება მოიცვას როგორც ერთი დომენი, ასევე მრავალი დომენი. დომენების **ხეობა** გაერთიანება ქმნის **ტყეს**.
- **ინფორმაციის რეპლიკაცია.** მოცემული სერვისის წყალობით დომენური ინფორმაცია რამდენიმე დომენის კონტროლერზე ინახება სინქრონულად. რამდენიმე კონტროლერის არსებობა დომენებში უზრუნველყოფს მტყუნებათა

მიმართ მდგრადობას და ქსელური დატვირთვის განაწილების შესაძლებლობას იძლევა.

კატალოგური სერვისის მონაცემთა ბაზა

დომენის კონტროლერებზე კატალოგური ინფორმაცია ინახება სპეციალური ფორმატის მონაცემთა ბაზის სახით. სერვისის განვითარების საწყის ეტაპზე კატალოგების სამსახურებისათვის შემუშავებულ იქნა სტანდარტი **X.500**, რომელიც ხის სტრუქტურის მქონე, იერარქიული, მასშტაბირებადი ცნობარების შესაქმნელად იყო გათვალისწინებული, ობიექტთა კლასებისა და მათი ატრიბუტების ნაკრების გაფართოების შესაძლებლობით.

X.500 სტანდარტის პრაქტიკული რეალიზაცია არაეფექტური გამოდგა არასაკმარისი მწარმოებლობის გამო, ამიტომ აღნიშნული სტანდარტის ბაზაზე შემუშავებული იქნა კატალოგის მონაცემთა ბაზის გამარტივებული ვერსია, **LDAP (Lightweight Directory Access Protocol)**, რომელშიც შენაჩუნდა **X.500**-ის ყველა ეფექტური ფუნქცია და ამასთან სტანდარტის პრაქტიკული რეალიზების საშუალება მისცა მომხმარებელს.

სადღეისოდ **LDAP** წარმოადგენს ქსელური კატალოგების მონაცემებთან დაშვების სტანდარტულ მეთოდს და მრავალი პროდუქტის საფუძველს წარმოადგენს (აუტენტიფიკაციის სისტემები, ელექტრონული ფოსტის პროგრამები, ელექტრონული კომერციის სისტემები და სხვა). **LDAP**-სერვისები დამუშავებულია პრაქტიკულად ყველა გავრცელებული ოპერაციული სისტემისთვის და ბუნებრივია მისი დიდი როლი ღრუბლოვანი ტექნოლოგიებშიც, რადგან ეს უკანასკნელი კატალოგურ სერვისს ინტენსიურად საჭიროებს.

დღეისათვის ბაზარზე **LDAP**-ის 60-ზე მეტი კომერციული სერვერია წარმოდგენილია. მათი 90% წარმოადგენს **LDAP**-კატალოგების ავტონომიურ სერვერებს, ხოლო დანარჩენები სხვა დანართების კომპონენტების სახით არიან წარმოდგენილნი. ჩვენს ნაშრომში გამოყენებულია ერთერთი მათგანი - **Active Directory**

კატალოგური სერვისის დომენური სტრუქტურა

მოცემულ ქვეთავში შევხებით კატალოგური სერვისის სტრუქტურულ ერთეულებს (დომენი, ხე, ტყე, ორგანიზაციული ერთეული, გლობალური კატალოგი), აგრეთვე განვიხილოთ კატალოგის ობიექტთა სახელდების წესები.

დომენი კატალოგური სერვისის ძირითად ერთეულს წარმოადგენს. იგი აყალიბებს ადმინისტრაციული პასუხისმგებლობის სფეროს. დომენის მონაცემთა ბაზა შეიცავს მომხმარებლის სააღრიცხვო ჩანაწერებს, ჯგუფებსა და კომპიუტერებს. კატალოგური სერვისის ფუნქციების დიდი ნაწილი სწორედ დომენურ დონეზე მუშაობს, კერძოდ: მომხმარებლის აუტენტიფიკაცია, რესურსებთან დაშვების მართვა, სამსახურების მართვა, რეპლიკაციების მართვა, უსაფრთხოების პოლიტიკა.

დომენების სახელები **Active Directory**-ში ფორმირდება იმავე სქემით, როგორც დომენურ სახელთა სერვისის (DNS) სახელები და ეს არ არის შემთხვევითი ფაქტი. DNS-ის სამსახური წარმოადგენს კომპონენტ დომენების ძეგნის პროცესის საინიციალიზაციო მოვლენას დომენის კონტროლერებზე.

დომენის კონტროლერები — სპეციალური სერვერებია, რომლებიც ინახავენ **Active Directory**-ის მონაცემთა ბაზის დომენური ნაწილის შესაბამის მონაცემებს. მათი ძირითადი ფუნქციებია:

- **Active Directory**-ის მონაცემთა ბაზის შენახვა (კატალოგურ ინფორმაციასთან წვდომა, მართვა და მოდიფიკაცია);
- **Active Directory**-ში ცვლილებათა სინქრონიზაცია. კერძოდ, კატალოგში ცვლილების შეტანა შეიძლება დომენის ნებისმიერი კონტროლერიდან; ნებისმიერი ცვლილება სინქრონულად დაფიქსირდება დომენის სხვა კონტროლერებზეც;
- **მომხმარებლის აუტენტიფიკაცია** - ნებისმიერი დომენის კონტროლერი ანხორციელებს კლიენტ-სისტემაზე დარეგისტრირებული მომხმარებლის უფლებამოსილების შემოწმებას;

ბე წარმოადგენს დომენების კრებულს, რომლებიც გამოიყენებენ ერთიან დამაკავშირებელ სივრცეს. ამ შემთხვევაში „შვილობილი“ დომენი მემკვიდრეობით იღებს „მშობელი“ დომენის სახელს.

შვილობილი დომენი ავტომატურად აყენებს **ორმხრივ, ტრანზიტულ, ნდობით დამოკიდებულებებს** მშობელ დომენთან, რაც ნიშნავს, რომ ერთი დომენის რესურსები შეიძლება გამოყენებულ იქნას სხვა დომენების მომხმარებელთა მიერაც.

ტყე მეტნაკლებად მსხვილი სტრუქტურაა **Active Directory**-ში. ტყე აერთიანებს დომენურ ხეებს სხვადასხვა სახელთა სივრცეებით და ამით უზრუნველყოფს ობიექტთა ერთიან სქემის არსებობას (სქემა – განსაზღვრული ტიპების ან კლასების კრებულია). ტყეში ყველა დომენს შორის ორმხრივი, ტრანზიტული ნდობითი დამოკიდებულებაა დამყარებული, რაც ნებისმიერი დომენის მომხმარებლებს ყველა დანარჩენ დომენებზე დაშვებით უზრუნველყოფს შესაბამისი დაშვების უფლების არსებობის შემთხვევაში. სტანდარტულად, ტყეში შექმნილი პირველი დომენი ფესვურ დომენად ითვლება. სწორედ მასში ინახება ე.წ. **AD**-სქემა.

ორგანიზაციული ერთეული (Organizational Units, OU) მოთავსებულია **Active Directory**-ის ერთერთი დომენის ფარგლებში და უფლებათა დელეგირების ამოცანას ემსახურება. ორგანიზაციული ერთეული დომენის გარეთ არ არსებობს. მისი გამოყენება განსაკუთრებით მოხერხებულია დიდი ორგანიზაციის ერთიანი დომენის აგებისას, როდესაც დომენის ადმინისტრატორს ფიზიკურად აღარ შეუძლია მთლიანი დომენის ყველა საადრიცხო ჩანაწერის მომსახურება. ამ დროს დომენის ადმინისტრატორი ასრულებს დელეგირებას, ანუ საკუთარი უფლებების გადაცემას სხვა მომხმარებლებზე, რომელთაც შემდგომ დომენში საკუთარი „წილი“ ეძლევათ მასში ცვლილებების შეტანის უფლებით. ორგანიზაციული ერთეული მთლიანად დომენს დაქვემდებარებული სტრუქტურაა, მას არ შეუძლია კატალოგური ინფორმაციის მიღება სხვა დომენიდან.

გლობალური კატალოგი წარმოადგენს დომენური სივრცის ყველა ობიექტის ერთიან ბაზას. სტანდარტულად, დომენების კონტროლერები შეიცავენ ინფორმაციას მხოლოდ საკუთარი ობიექტების შესახებ, მაშინ, როდესაც გლობალური კატალოგის სერვერი წარმოადგენს დომენის კონტროლერს, რომელშიც განთავსებულია ინფორმაცია დომენთა ტყის ყოველი ობიექტის შესახებ. ამასთან, უნდა აღინიშნოს, რომ გლობალურ

კატალოგში ობიექტთა ატრიბუტების მხოლოდ ნაწილი ხვდება ყველაზე მნიშვნელოვანი ატრიბუტების სახით.

კატალოგურ სერვისში მნიშვნელოვანია **ობიექტების სახელების განმასხვავებელი მექანიზმი (Distinguished Name, DN)**, რომელიც კატალოგის ნებისმიერი ობიექტის დომენთა ტყის მასშტაბით ცალსახად იდენტიფიცირების საშუალებას იძლევა. **DN** წარმოადგენს ქვესახელების ერთობლიობას, რომელთა კომბინაცია გვაძლევს სწორედ ობიექტის უნიკალურ იდენტიფიკატორს.

მაგალითისთვის ავიღოთ მომხმარებელი **testuser** დომენიდან **sangu.ge**, რომელიც განთავსებული დომენის მომხმარებელთა სტანდარტულ კონტეინერში „**Users**“. მომხმარებლის უნიკალური სახელი შემდეგი ფორმით იქნება წარმოდგენილი:

DC=ge, DC=sangu, OU=Professors, CN=Users, CN=testuser

სადაც

- **DC (Domain Component)** — პირველი და მეორე დონის დომენური სახელები (საპატრიარქოს უნივერსიტეტის დომენი).
- **OU (Organizational Unit)** — ორგანიზაციული ერთეული (უნივერსიტეტის პროფესორები)
- **CN (Common Name)** — მომხმარებელთა სტანდარტული ჯგუფი (**Users**) და მასში შემავალი მომხმარებლის სახელი (**testuser**).

Active Directory-ის სახელთა განაწილების ეფექტური სქემის დაპროექტება ძალიან საპასუხისმგებლო საქმეა კორპორაციული ქსელის უსაფრთხოების თვალსაზრისითა და იმ ფაქტორის გათვალისწინებით, რომ უკვე ჩამოყალიბებული სახელთა სტრუქტურის შეცვლა ძნელ, ხანდახან კი შეუძლებელ ამოცანას წარმოადგენს. ამიტომ სახელთა სივრცის დაპროექტებისას შემდეგი ფაქტორები უნდა იქნეს გათვალისწინებული:

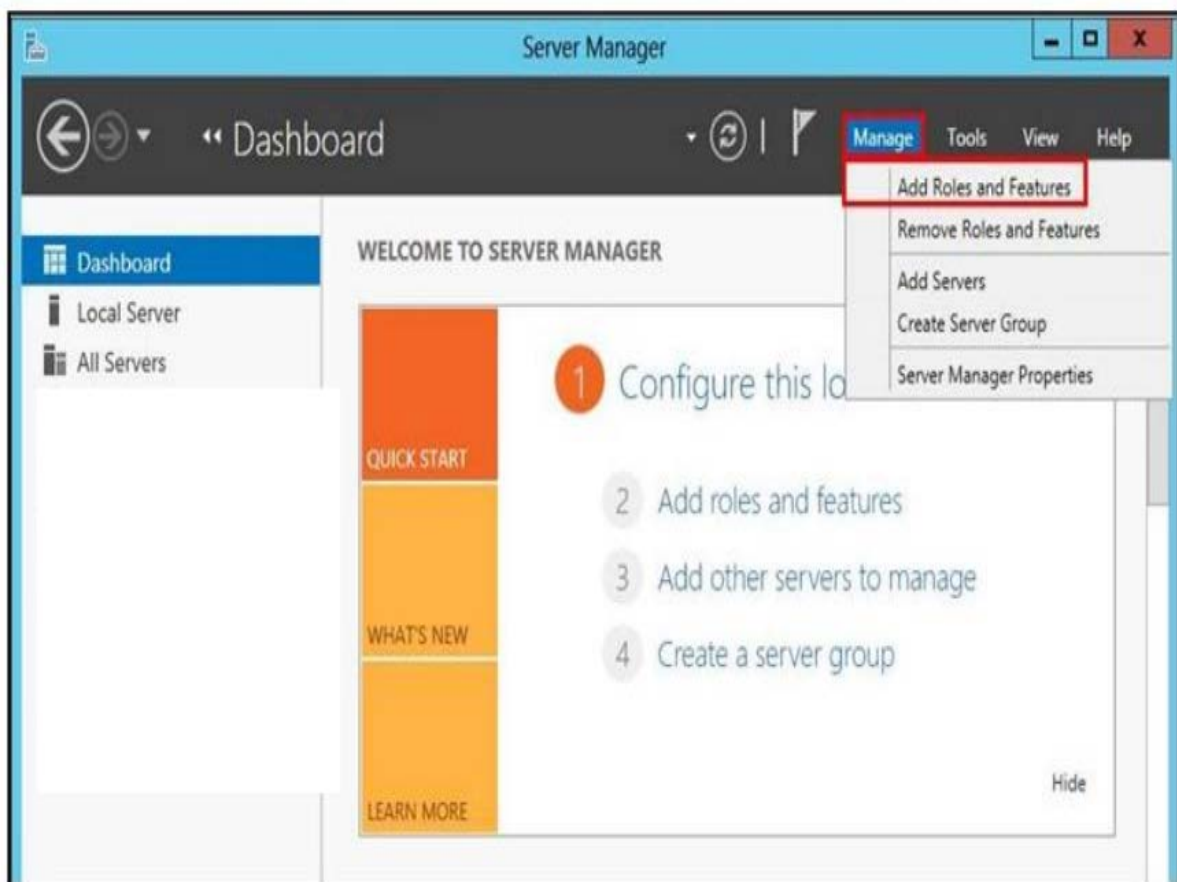
- ზედა დონის დომენების სახელების გულდასმით შერჩევა.
- კომპანიაში კომუნიკაციების ხარისხი (კავშირი ცალკეულ ქვედანაყოფებთან და ფილიალებთან).
- კომპანიის ორგანიზაციული სტრუქტურა.

- კომპიუტერების მომხმარებელთა რაოდენობის ზრდის ტემპების პერსპექტივა.

2.1. ცენტრალური დირექტორიების სერვისების (Directory Service) ადმინისტრირება

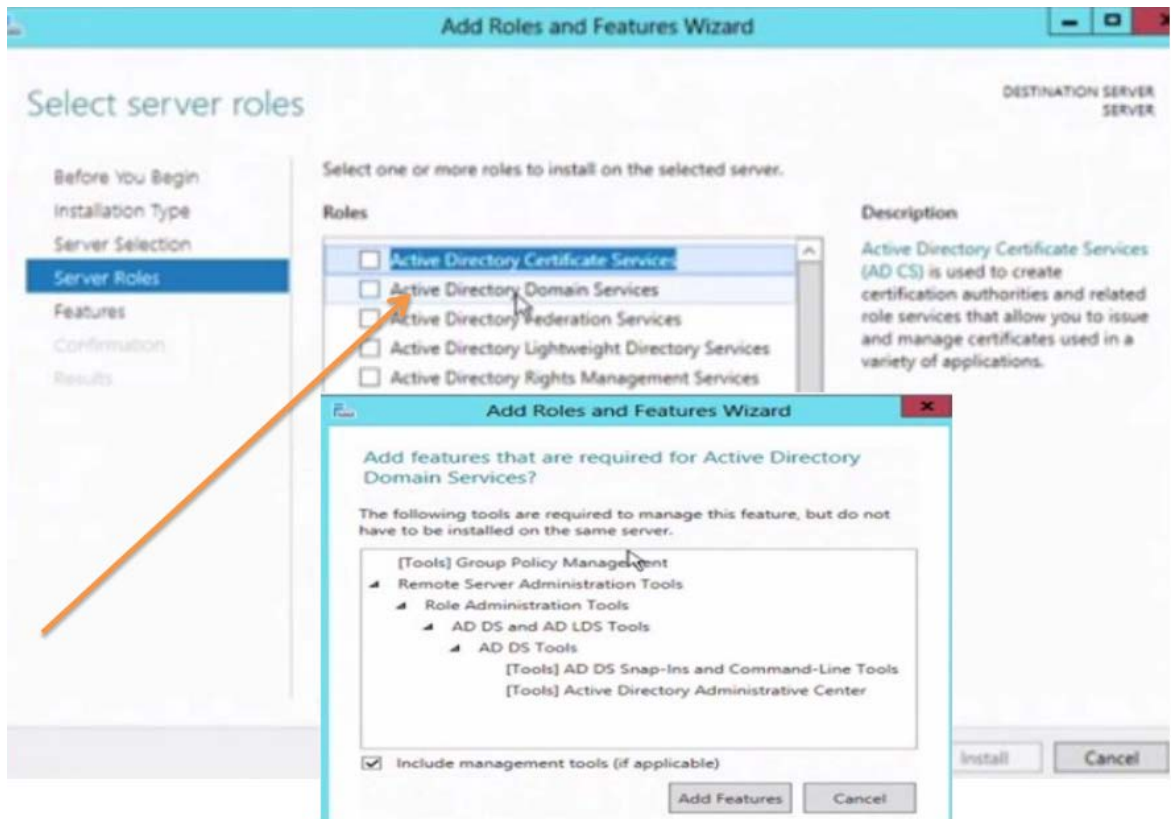
ნაბიჯი 1- Add Roles and Features მენიუს გააქტიურება

- On the **Start** screen, type **Server Manager**, and open it from the results displayed.
- On the **Server Manager** window, click **Manage** on the Title bar, and then click **Add Roles and Features**.

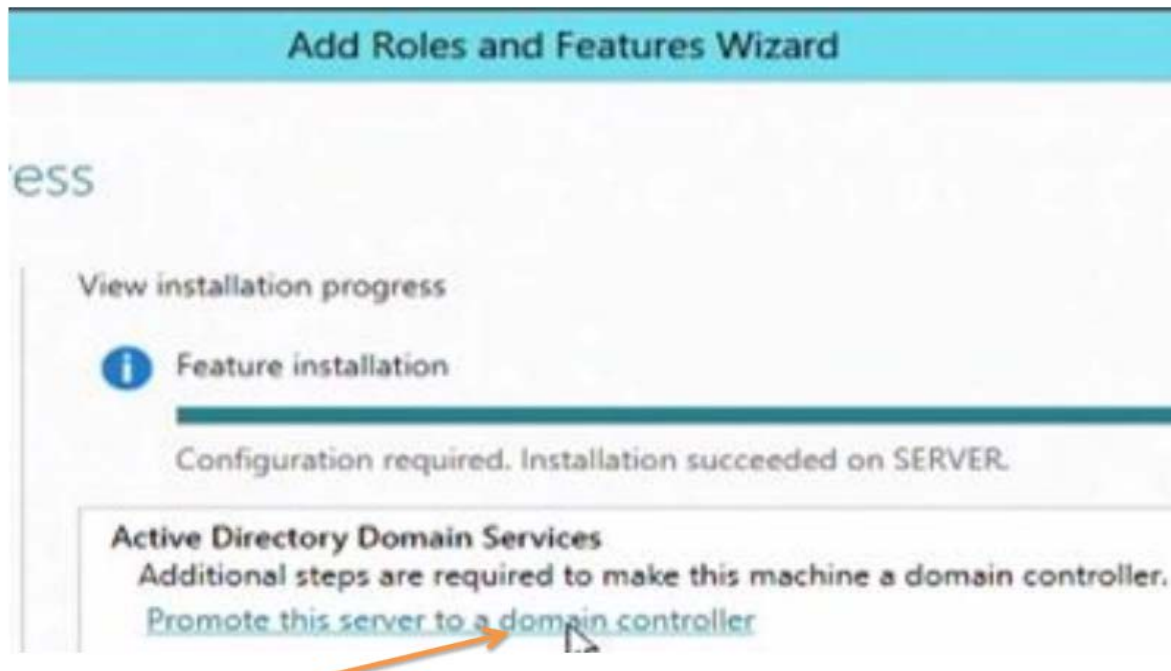


სურ.2.1. 1

ნაბოჯო 2- AD DS სერვისის არჩევა და Domain Controller-თან დაკავშირება

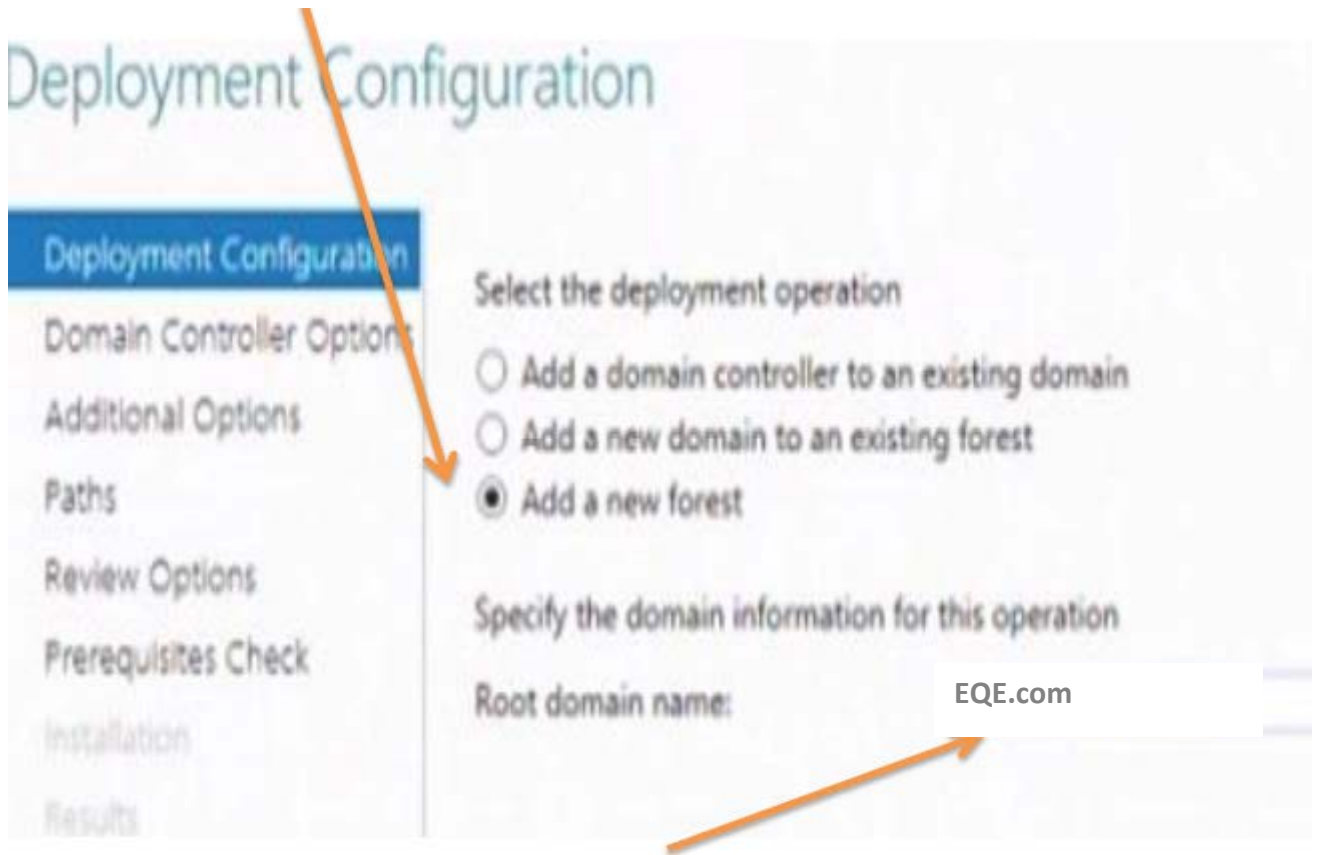


სურ.2.1. 2



სურ.2.1. 3

ნაბიჯი 3- დომენის გაწევრიანება არსებულ დომენში (ან forest) ან ახალ forest-ში დამატება

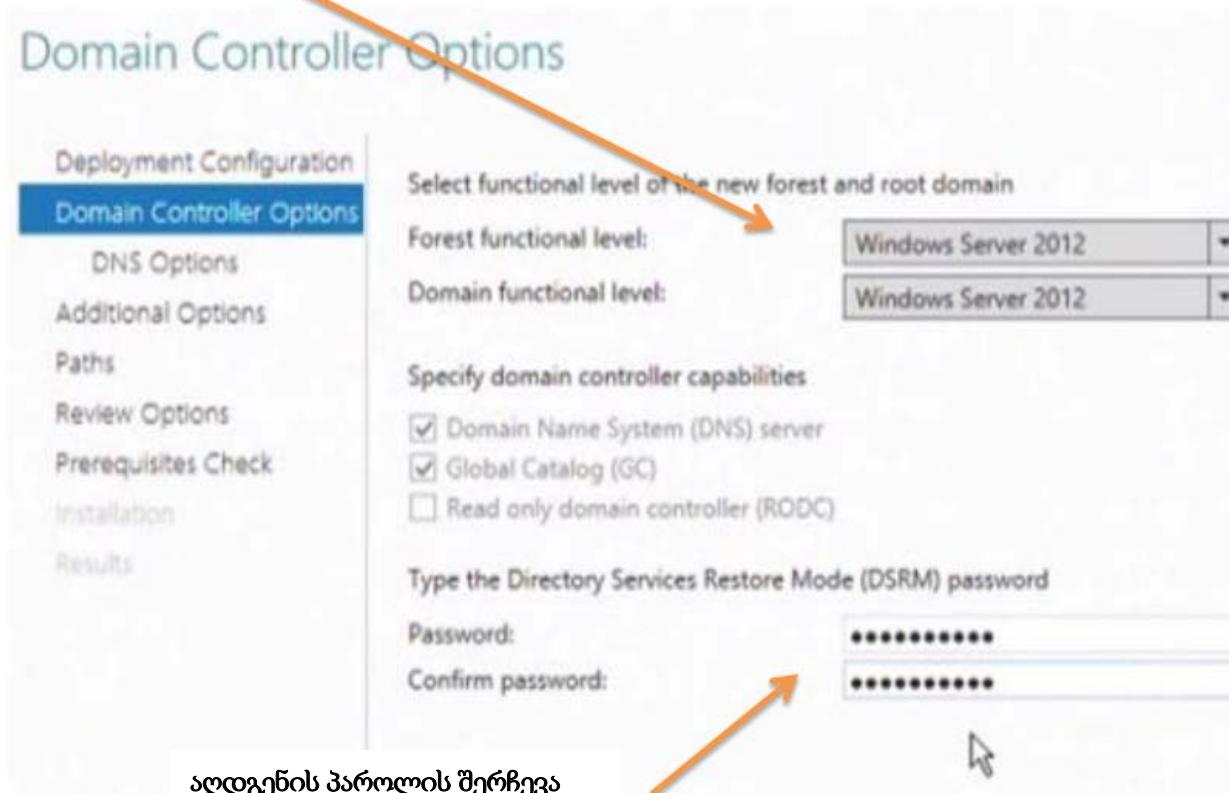


Root დომენ სახელის შერჩევა

5

სურ.2.1. 4

ნაბიჯი 4 - ახალი Forest-ისა და Root Domain-ის ფუნქციონალური დონის განსაზღვრა

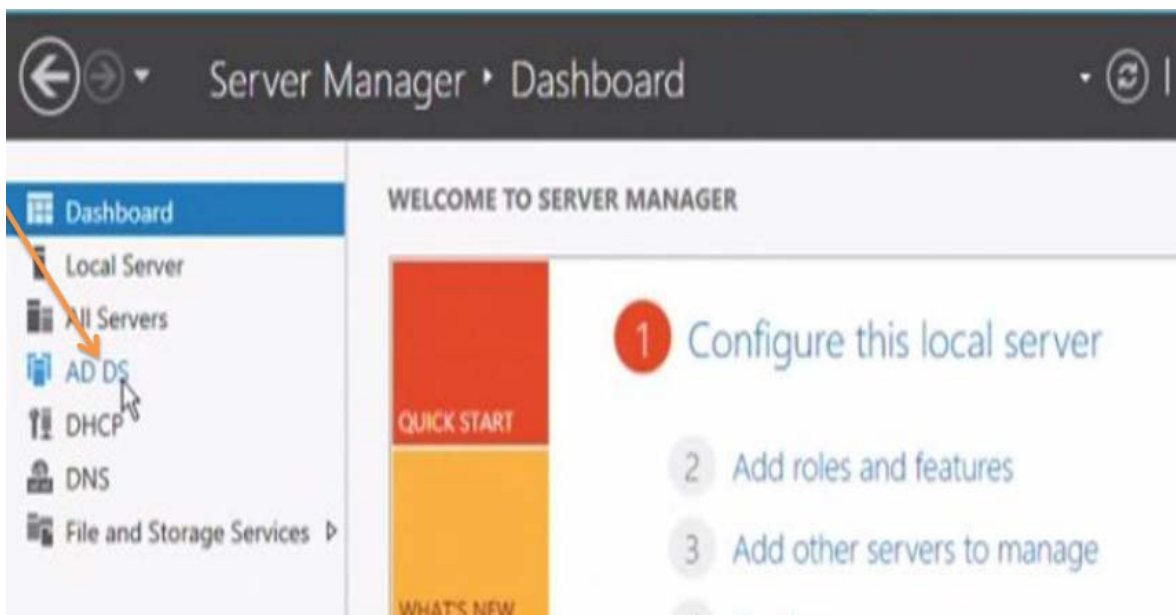


ადღენის პაროლის შერჩევა

სურ.2.1. 5

ინსტალაციის შემდგომი ფანჯარა

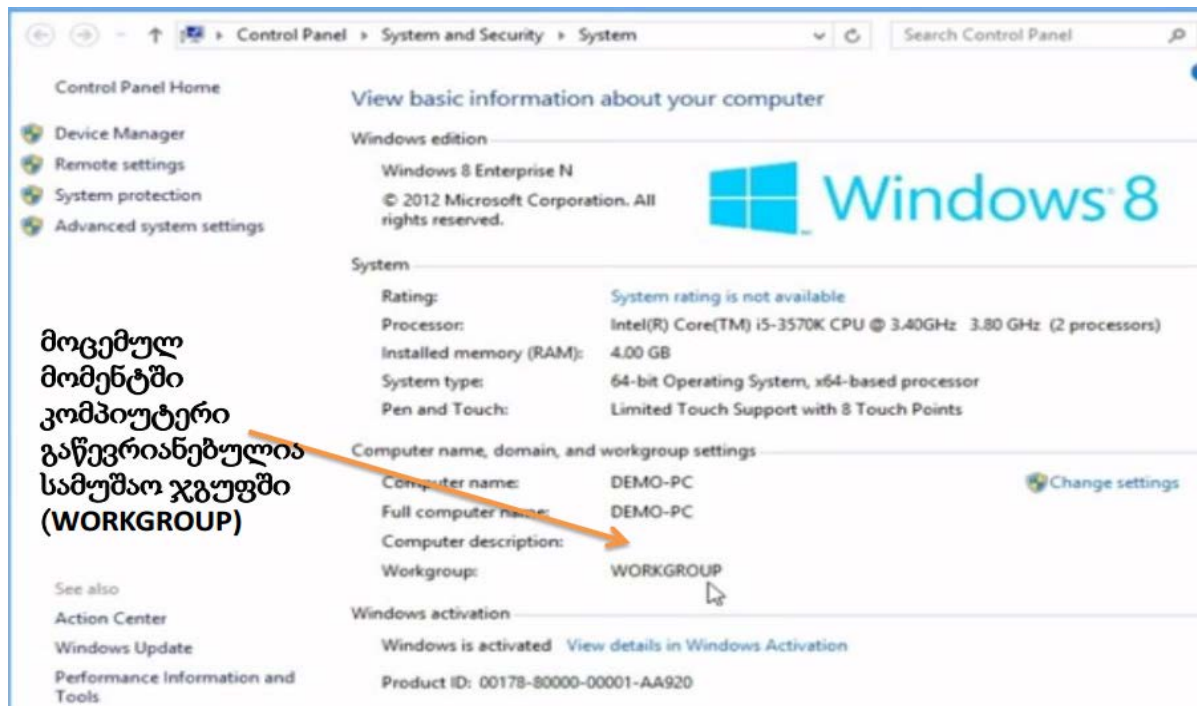
]



სურ.2.1. 6

2.2. დომენური სახელების სერვერის (DNS) ადმინისტრირება

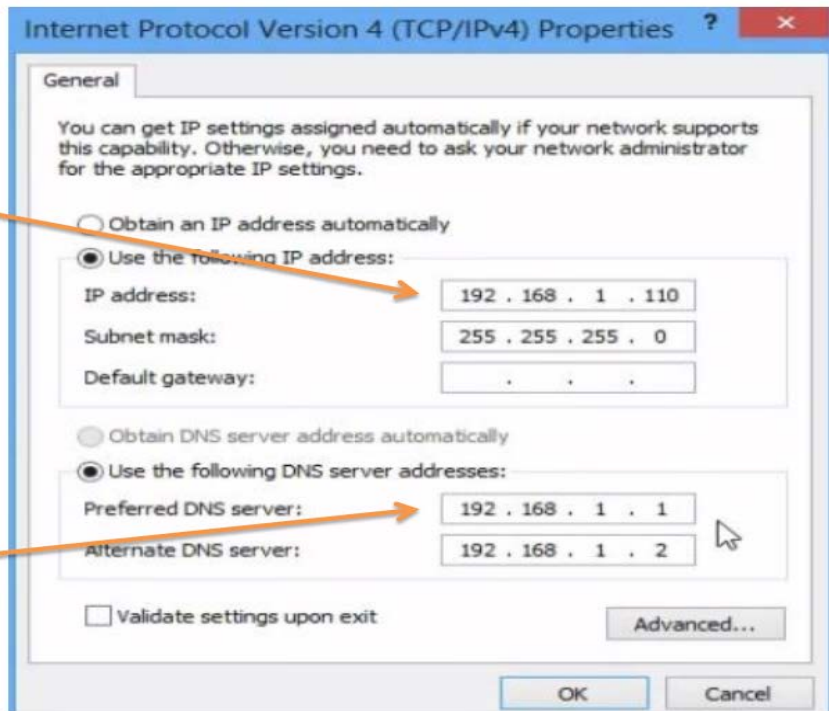
ნაბიჯი 5 - კლიენტი კომპიუტერის გაწევრიანება დომენში



სურ.2.1. 7

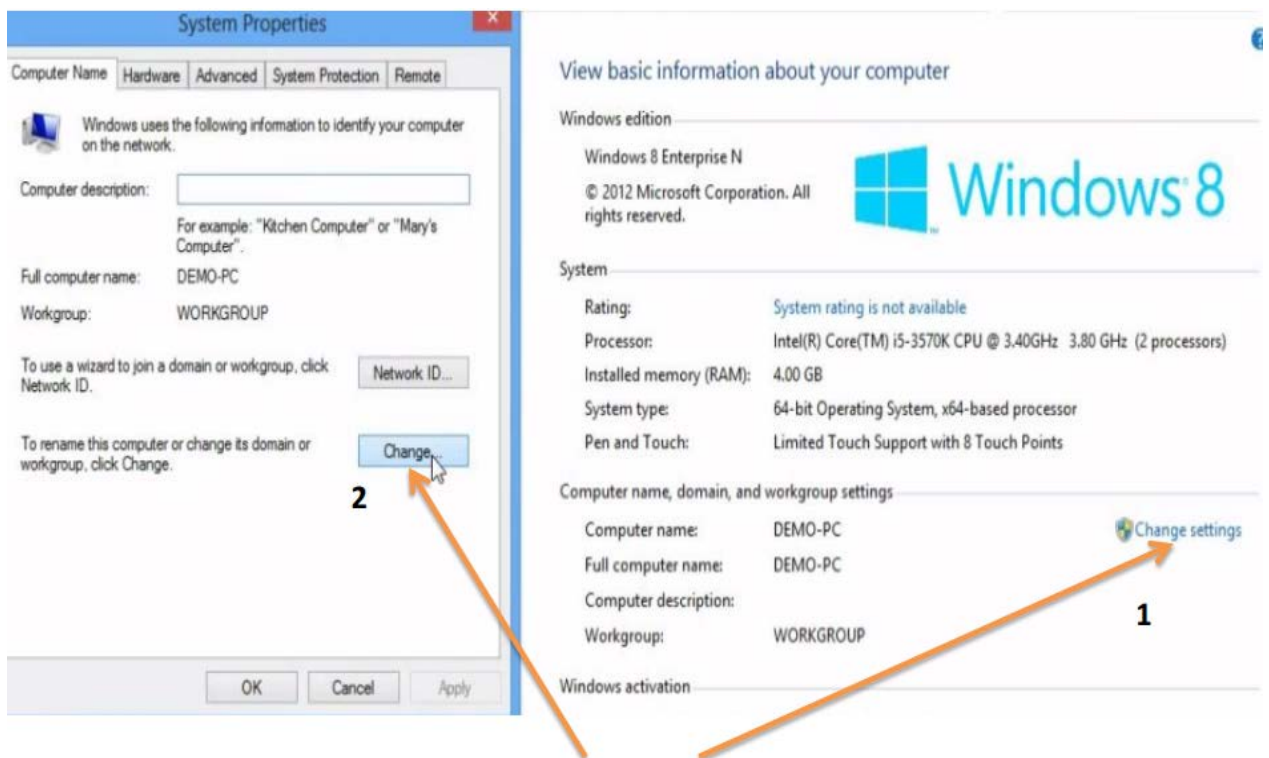
მოცემულ კომპიუტერი იმავე ქსელში უნდა იყოს იდენტიფიცირებული, რომელი ქსელის მისამართიც აქვს გასაწევრიანებელი დომენის შესაბამის სერვერ-ს

DNS სერვერის მისამართი მითითებული მისამართი უნდა შეესაბამებოდეს დომენური სერვერის IP მისამართს

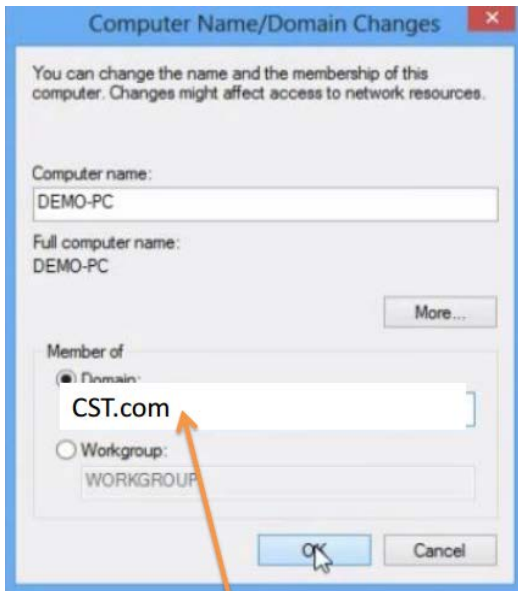


სურ.2.1. 8

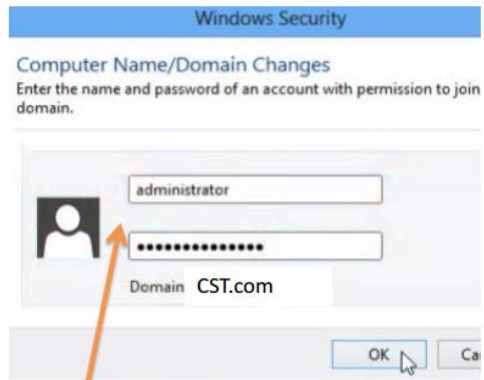
შესაბამის მენიუებში ვორჩევთ სათანადო ბრძანებებს (იხილეთ სურათი)



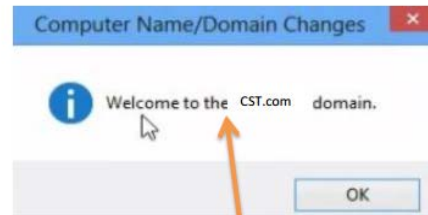
სურ.2.1. 9



დომენური სახელის ველში
მივუთითოთ
გასაწევრიანებელი
დომენის სახელი



მივუთითოთ
ადმინისტრატორის
უფლებების მქონე
ანგარიშის სახელი და
პაროლი



წარმატებით
გაწევრიანების
მაგალითი

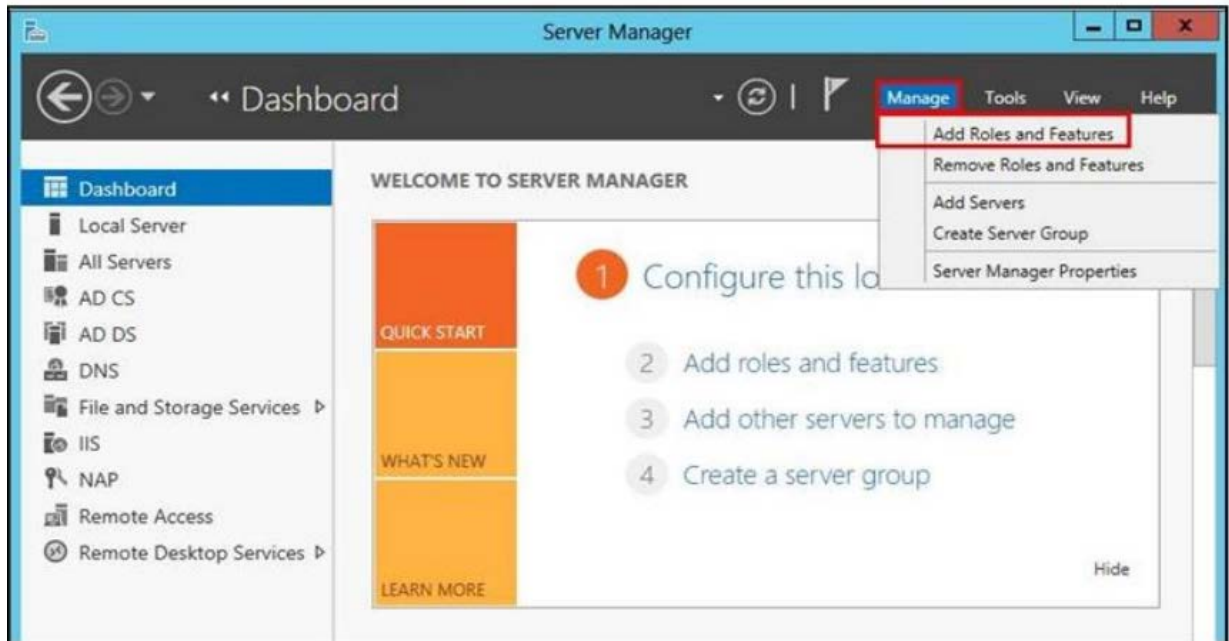
სურ.2.1. 10

2.3. ქსელური მისამართების მართვის სისტემის (DHCP)

ადმინისტრირება

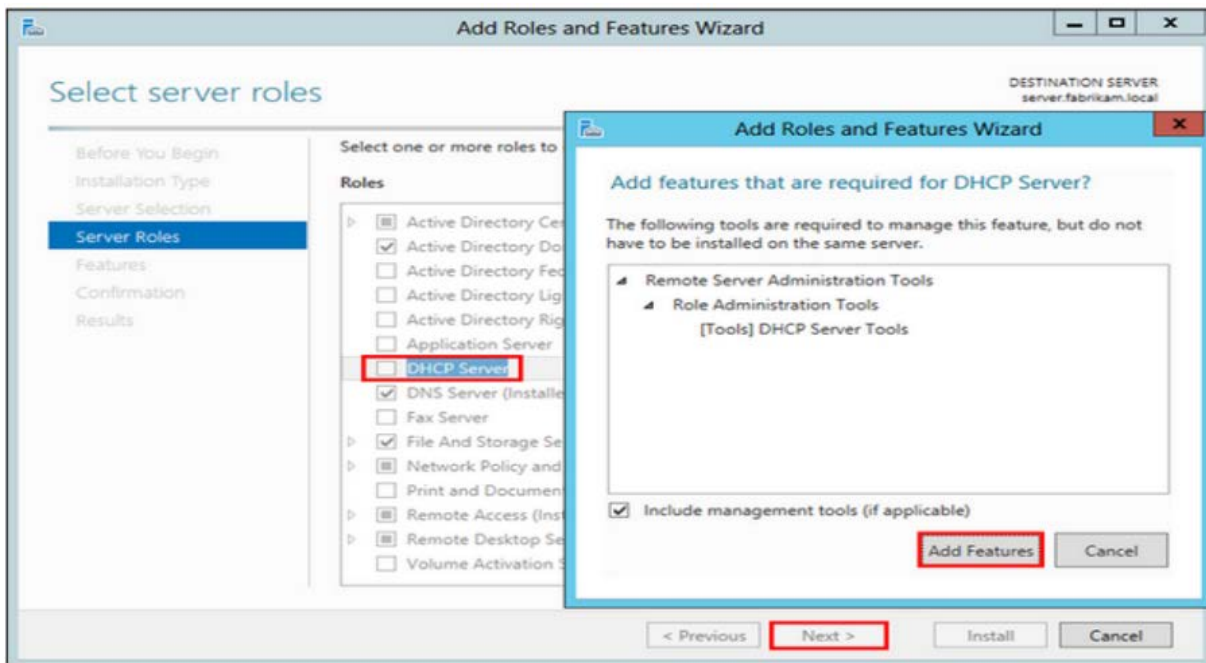
ნაბიჯი 1- Add Roles and Features მენიუს გააქტიურება

- On the **Start** screen, type **Server Manager**, and open it from the results displayed.
- On the **Server Manager** window, click **Manage** on the Title bar, and then click **Add Roles and Features**.



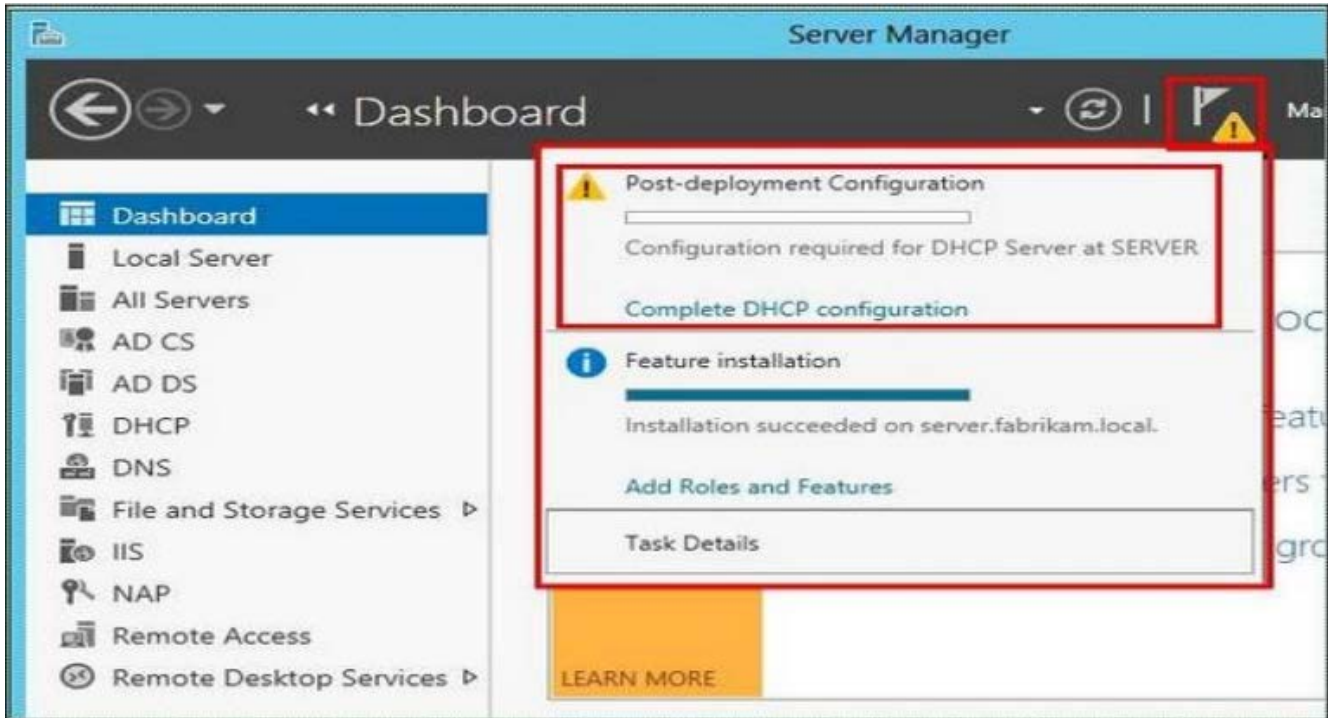
სურ.2.3. 1

ნაბიჯი 2- DHCP სერვისის არჩევა



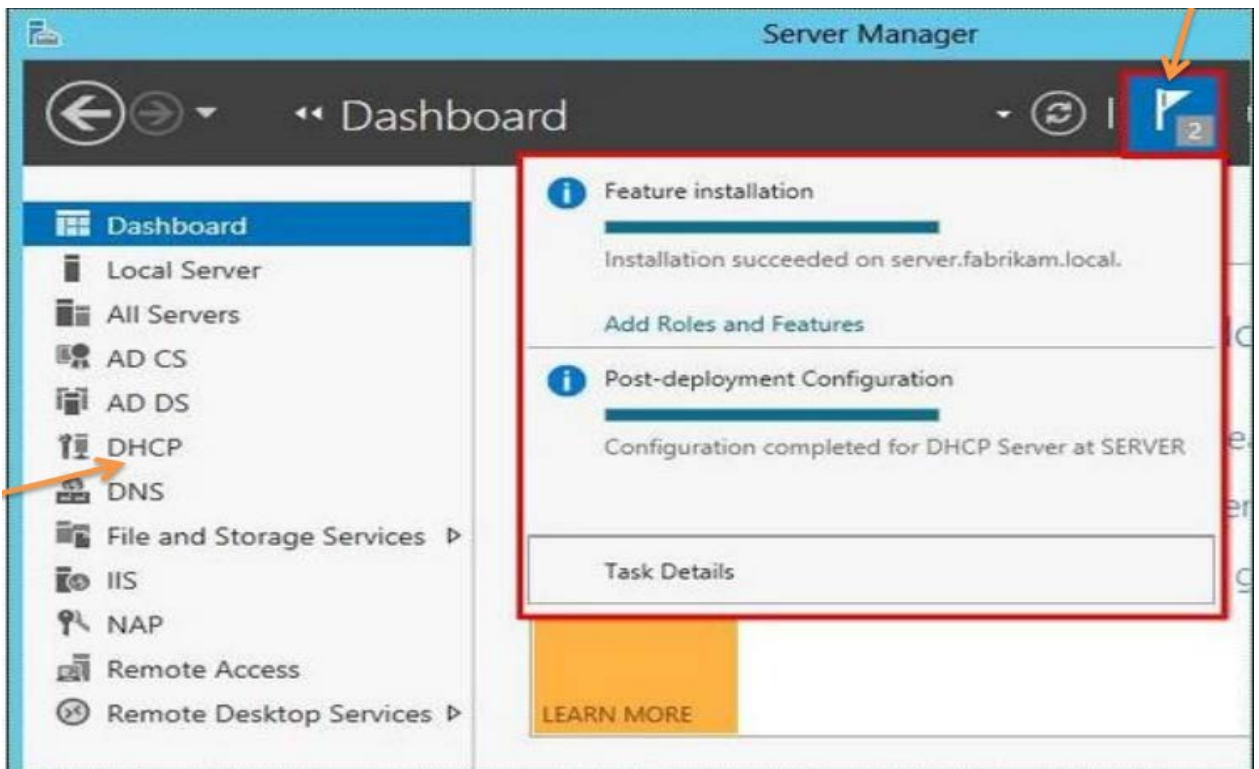
სურ.2.3. 2

ნაბიჯი 3- DHCP სერვისის ინსტალაციის დასრულება



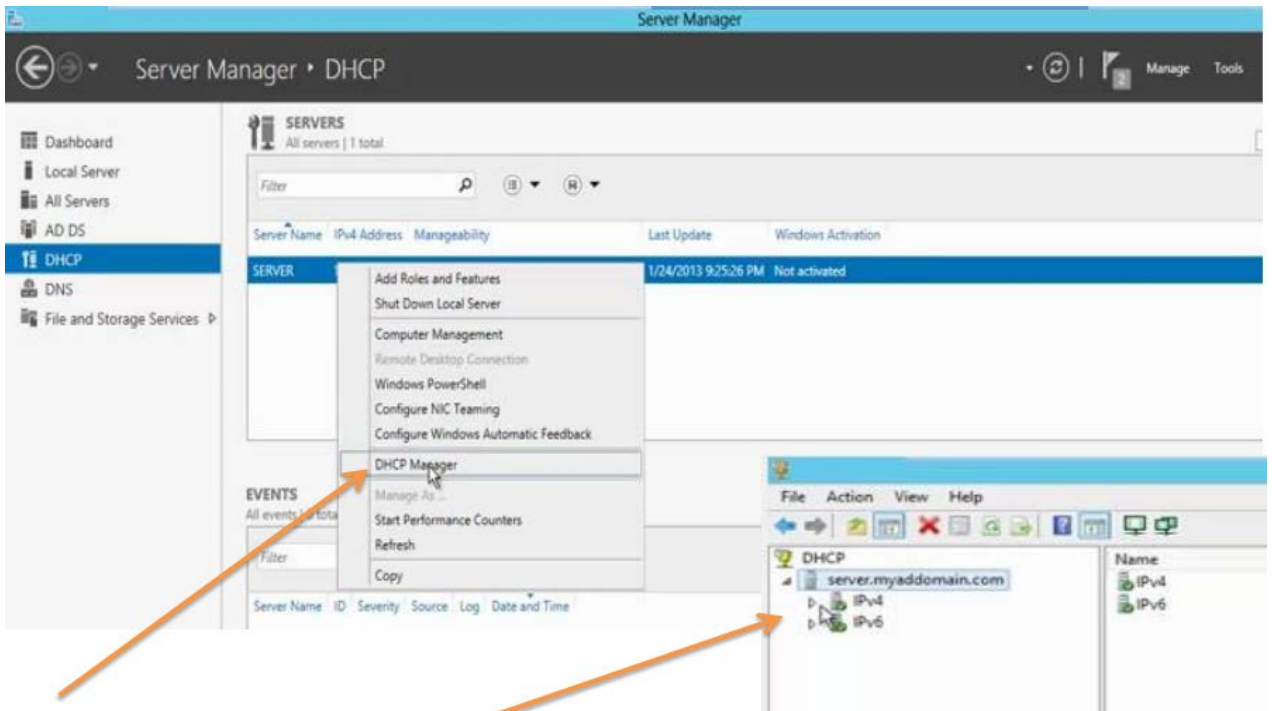
სურ.2.3. 3

ინსტალაციის ფინალური ფანჯარა



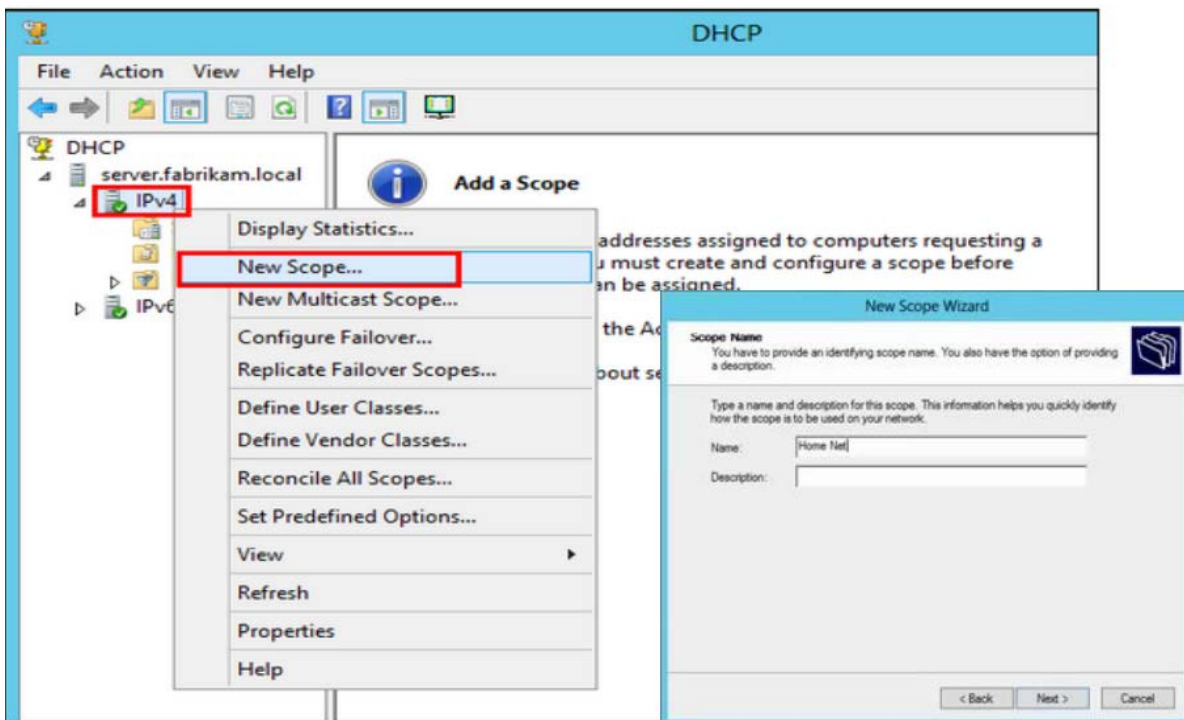
სურ.2.3. 4

ნაბიჯი 3 - DHCP კონფიგურირება - DHCP Manager-ის გააქტიურება



სურ.2.3. 5

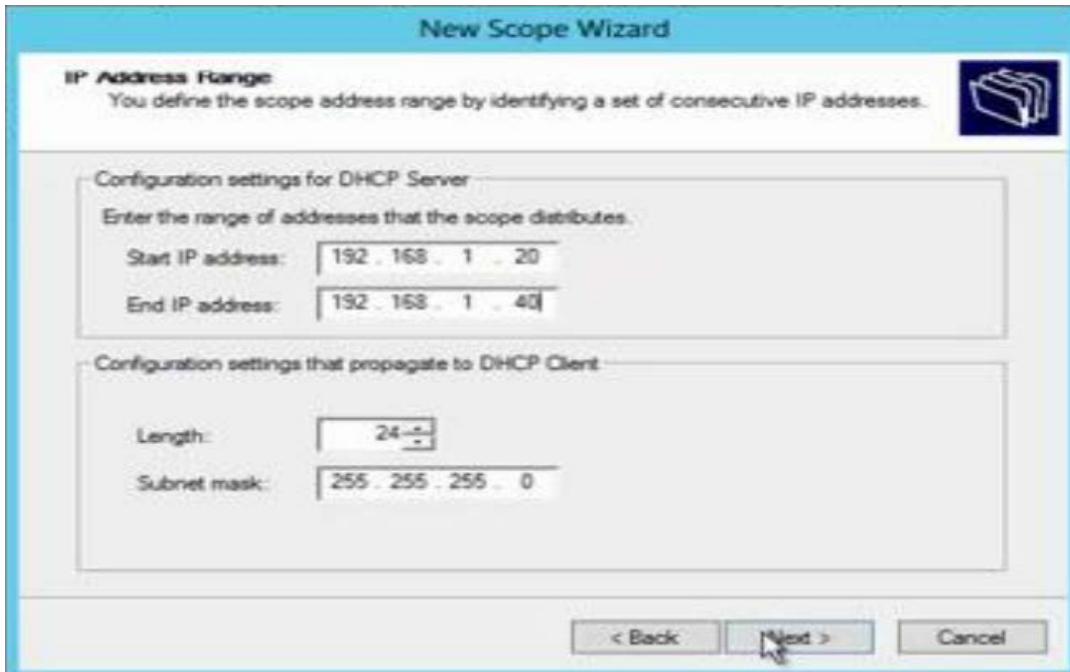
DHCP კონფიგურირება



სურ.2.3. 6

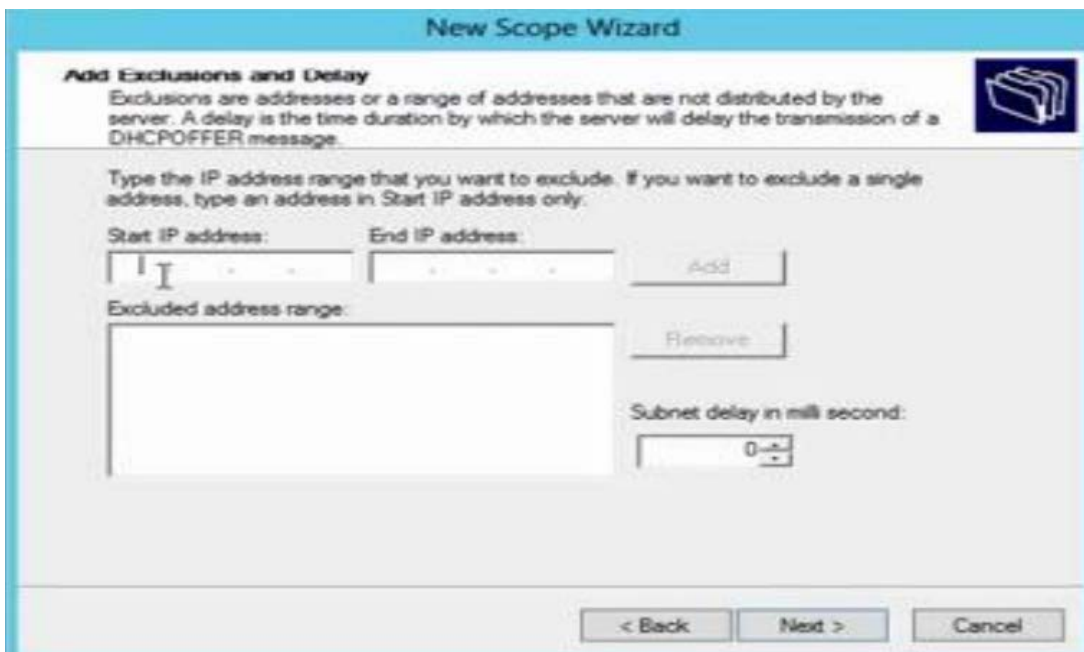
IP მისამართების დიაპაზონის (range) განსაზღვრა

მითითებული მისამართები უნდა იყოს საკუთრივ სერვერის შესაბამისი ქსელის მისამართები



სურ.2.3. 7

დარეზერვებული მისამართების დიაპაზონის განსაზღვრა (არ არის აუცილებელი შესავსები ველი)

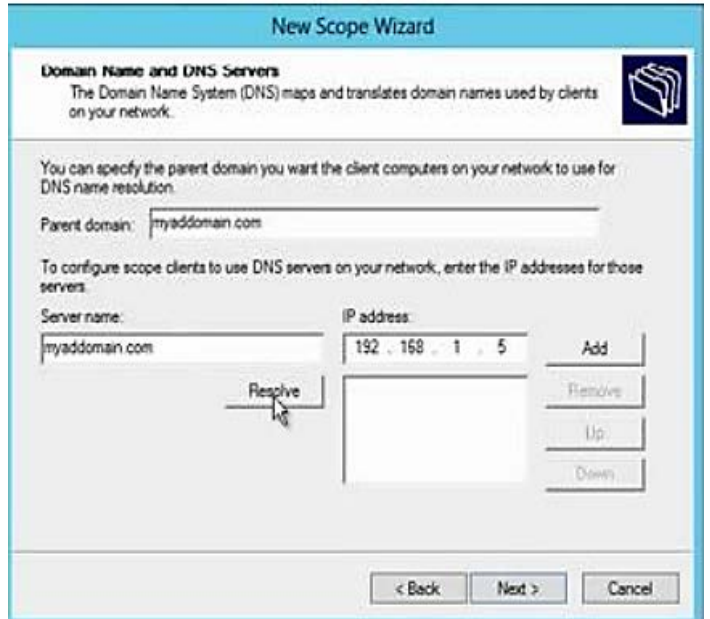


სურ.2.3. 8

Gateway და DNS მისამართის შერჩევა

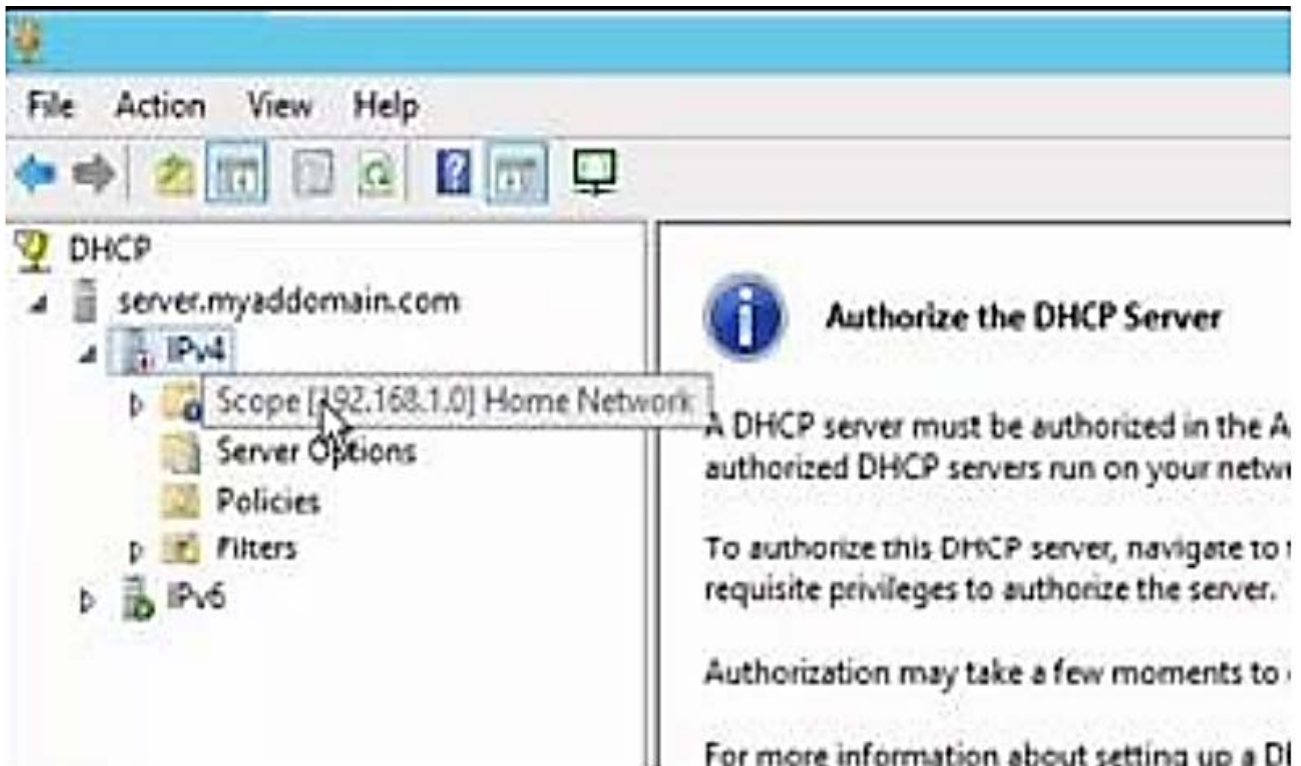


სურ.2.3. 10



სურ.2.3. 9

ძირითადი კონფიგურირების ელემენტებით მიღებული DHCP scope ჩანაწერი



სურ.2.3. 11

კითხვები თვითშემოწმებისთვის:

- დაახასიათეთ ცენტრალური დირექტორიების სერვისები
- რა არის დომენი?
- აღწერეთ DHCP
- აღწერეთ ლოგიკური ქსელური მისამართები

პრაქტიკული სავარჯიშო

- მოახდინეთ AD DS ადმინისტრირება
 - შექმენით ახალი ფორესტი
 - შექმენით Root დომენი
- გააქტიურეთ DHCP სერვისი
 - შექმენით C კლასის ლოგიკური მისამართების სივრცე
 - დაარეზერვეთ პირველი 10 მისამართი
 - განსაზღვრეთ მისანიჭებელი Gateway და DNS მისამართები

ცოდნის შეფასება

I - პრაქტიკული დავალება

სტუდენტებს მიეცემათ პრაქტიკული დავალება

- შეასრულონ სატესტო სერვერზე დირექტორიების სერვისების ინსტალაცია
- შეასრულონ დირექტორიების სერვისების კონფიგურაცია
- დაარეგისტრონ პერსონალური კომპიუტერები და მომხმარებლები დირექტორიების სერვისების ბაზაში
- დააკონფიგურირონ დომენური სახელების სერვერი
- გამართონ DHCP სერვისი

შემფასებელი აკვირდება შესაფასებელ პირის მუშაობას პროფესიული სტანდარტით (პროგრამით / მოდულით) განსაზღვრული ამოცანების შესრულების პროცესში. დაკვირვება ხორციელდება კომპიუტერებით აღჭურვილ ლაბორატორიაში, სადაც შესაფასებელი პირი პრაქტიკულ საქმიანობას ეწევა. შემფასებელმა წინასწარ უნდა დაგეგმოს დაკვირვების

პროცესი, იმის დასადგენად, თუ რამდენად სწორად იყენებს შესაფასებელი პირი ცოდნას, უნარებსა და ყველა რესურსს შედეგის მისაღწევად.

შეფასება განხორციელდება პროცესზე დაკვირვებით, წინასწარ განსაზღვრული შეფასების ინდიკატორების საფუძველზე.

დავალების ნიმუში და შეფასების რუბრიკა

პროცესზე დაკვირვება

- ✚ შეასრულოს დირექტორიების სერვისების (AD DS, DNS, FTP, DHCP) აქტივაცია/ინსტალაცია
- ✚ მოახდინოს დირექტორიების სერვისების კონფიგურაცია/გამართვა

სწავლის შედეგი	N	დასახელება	შეფასება	
			კი	არა
ვების, ფაილური და მონაცემთა ბაზის სერვერების გამართვა	4.	დავალების შესაბამისად დააინსტალირა დირექტორიების სერვისები		
	5.	დავალების შესაბამისად დააკონფიგურირა დირექტორიების სერვისები		
	6.	დავალების შესაბამისად დაარეგისტრირა პერსონალურ კომპიუტერები და მომხმარებლები დირექტორიების სერვისების ბაზაში		
	7.	დავალების შესაბამისად დააინსტალირა დომენური სახელების სერვერი		
	8.	დავალების შესაბამისად დააკონფიგურირა დომენური სახელების სერვერი		
	9.	დავალების შესაბამისად დაარეგისტრირა პერსონალურ კომპიუტერები და მომხმარებლები დომენური სახელების სერვერების ბაზაში		
	10.	დავალების შესაბამისად გამართა DHCP სერვისი		

სწავლის შედეგი ჩაითვლება მიღწეულად თუ სტუდენტმა შეძლო შედეგის მინიმუმ 5

პუნქტის შესრულება

II - ტესტირება კითხვები მრავალი არჩევითი პასუხით

ასეთი ტიპის დავალება ორი ნაწილისგან შედგება. პირობის, რომელიც ჩამოყალიბებულია შეკითხვის ან არასრული მტკიცებულების სახით (ძირითადი მოცემულობა) და პასუხების ვარიანტებისგან. სავარაუდო პასუხი ძირითადად 4 ან 5-ია, რომელთაგან სტუდენტმა სწორი ვარიანტი უნდა აირჩიოს. საბოლოოდ ხდება პასუხების ტესტის გასაღებთან შედარება და სწორი პასუხების მიხედვით ქულების დათვლა. სწორ პასუხს ეწოდება საკვანძო, არასწორს - დისტრაქტორი (დამაბნეველი პასუხი). დისტრაქტორად ირჩევენ იმ ტიპურ შეცდომებს, რომელთაც ხშირად უშვებენ სტუდენტები.

ტესტის ნიმუში

1

აღნიშვნები: 1 **შეუსაბამეთ ერთმანეთს:**

სერვისი, რომელიც ჰოსტის ქსელურ მისამართს შეუსაბამებს დომენურ სახელს

წესების ერთობლიობა, რომლითაც რეგულირდება(იმართება) დომენში გაწვევრიანებული ობიექტები

სერვისი, რომელიც იძლევა დომენების შექმნის საშუალებას

სერვისი, რომელიც იძლევა ოპერაციული სისტემის ქსელურად ჩატვირთვის საშუალებას

სერვისი, რომელიც საშუალებას იძლევა ჰოსტებმა დინამიურად მიიღონ ლოგიკური ქსელური მისამართები

აირჩიე...
აირჩიე...
DHCP
FRS
Hyper-V
WDS
AD DS
GPO
DNS

1

აღნიშვნები: **GPO-სთან მიმართებაში რომელი მსჯელობაა მცდარი?**

1

- Choose one answer.
- a. GPO ქმნის წესების ერთობლიობას, რომელიც შეიძლება გავრცელდეს ცალკეულ მომხმარებლებზე(User) ან მათს ჯგუფებზე(Group)
 - b. GPO ქმნის წესების ერთობლიობას, რომელიც შეიძლება გავრცელდეს Organization Unit-ში გაწვევრიანებულ ყველა ობიექტზე
 - c. GPO წარმოადგენს DHCP სერვისის(Role) ერთ-ერთ მახასიათებელს (Features)
 - d. GPO წარმოადგენს AD DS სერვისის(Role) მახასიათებელს (Features)

Image File

Enter the location of the Windows image file that contains the images to add.

File location:

Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.

[More information about images and image types](#)

Choose one answer.

- a. შერჩეული ფაილი უზრუნველყოფს ქსელური ჩატვირთვისას ოპერაციული სისტემის ინსტალაციას
- b. შერჩეული ფაილი უზრუნველყოფს ქსელურ ჩატვირთვისას
- c. მოცემულ ეტაპზე განისაზღვრება საინსტალაციო პაკეტის განთავსების(შენახვის ადგილი) მდებარეობა
- d. მოცემულ ეტაპზე განისაზღვრება ჩამტვირთავი ფაილის განთავსების(შენახვის ადგილი) მდებარეობა

Add Image Wizard

Image File

Enter the location of the Windows image file that contains the images to add.

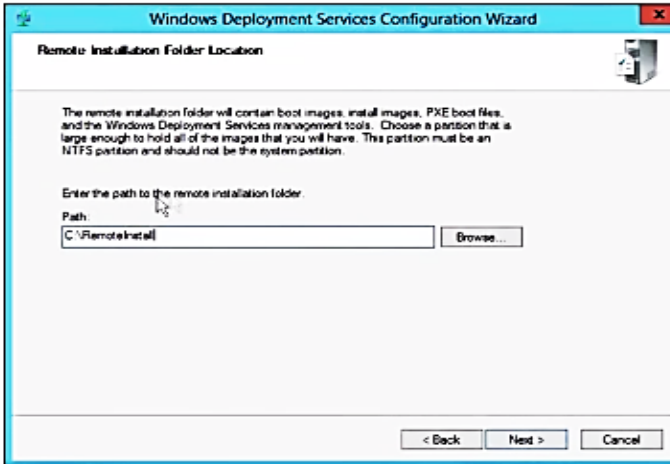
File location:

Note: The default boot and install images (Boot.wim and Install.wim) are located on the installation DVD in the \Sources folder.

[More information about images and image types](#)

- Choose one answer.
- a. შერჩეული ფაილი უზრუნველყოფს ქსელური მიმართვისას ოპერაციული სისტემის ჩატვირთვისას
 - b. შერჩეული ფაილი უზრუნველყოფს საინსტალაციო ფაილის შექმნას
 - c. მოცემულ ეტაპზე განისაზღვრება ჩამტვირთავი პაკეტის განთავსების(შენახვის ადგილი) მდებარეობა
 - d. მოცემულ ეტაპზე განისაზღვრება ჩამტვირთავი ფაილის სარეზერვო ასლის შექმნის ადგილი

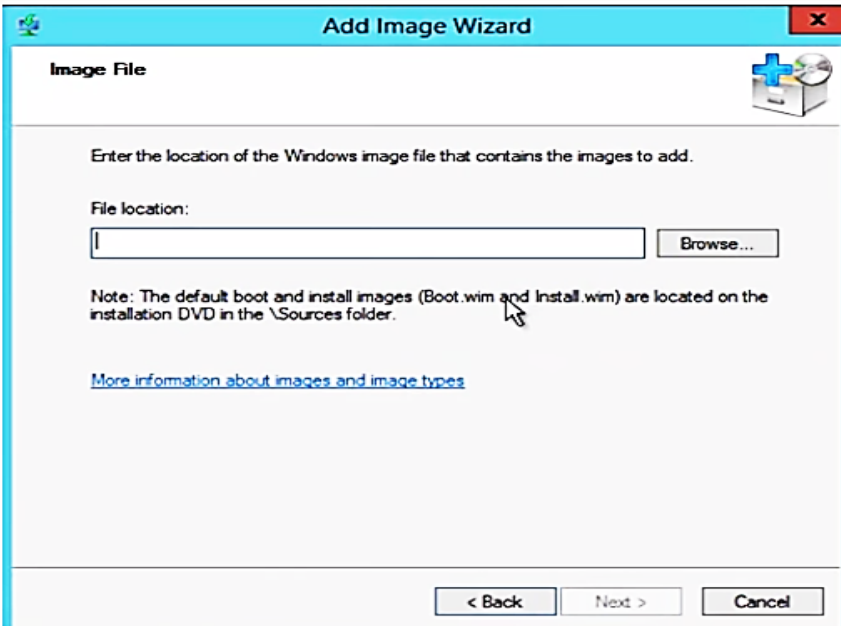
მოცემული სურათის მიხედვით, რომელი მსჯელობაა მცდარი?



Choose one answer.

- a. მითითებულ დირექტორიაში იქნება ჩაწერილი ოპერაციული სისტემის ჩამტვირთავი და საინსტალაციო პაკეტები
- b. რეკომენდირებულია მოცემული დირექტორიის შეცვლა
- c. მოცემული დირექტორია შერჩეულია მომხმარებლის მიერ
- d. მოცემული დირექტორია Default შემოთავაზებულია კონფიგურაციის რეჟიმში

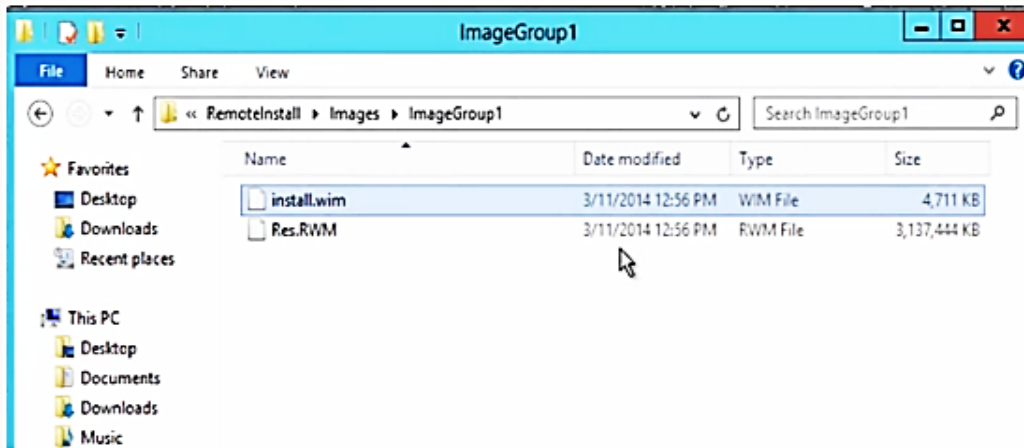
მოცემული სურათის მიხედვით, რომელი მსჯელობაა მცდარი?



Choose one answer.

- a. მოცემულ ეტაპზე ხდება ჩამტვირთავი(Boot) ფაილის დამატება საინსტალაციო დისკის შესაბამისი დირექტორიიდან
- b. მოცემულ ეტაპზე ხდება ჩამტვირთავი(Boot) ფაილის შერჩევა და დამატება
- c. მოცემულ ეტაპზე ხდება ჩამტვირთვის(Boot) და ინსტალაციის(Install) მეთოდების განსაზღვრა
- d. მოცემულ ფანჯარაში უნდა მიეთითოს ჩამტვირთავი(Boot) ფაილის მდებარეობა

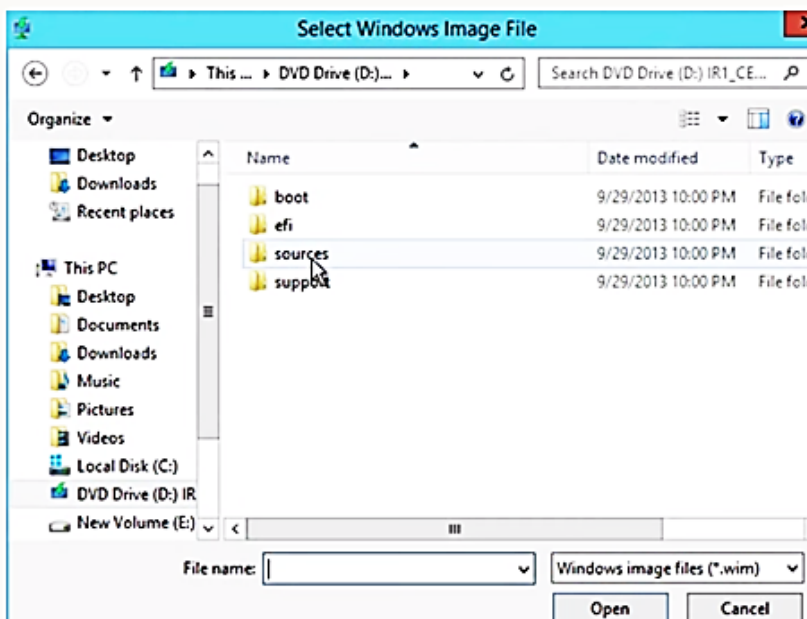
მოცემული სურათის მიხედვით, სწორია მსჯელობა:



Choose one answer.

- a. სურათზე ნაჩვენებია იმ დირექტორიის მისამართი საიდანაც ხდება საინსტალაციო ფაილის დამატება
- b. სურათზე ასახულია WDS კონფიგურაციაში ინსტალაციის ფაილის დამატების პროცესი
- c. სურათზე ნაჩვენებია იმ დირექტორიის მისამართი სადაც მოხდა საინსტალაციო ფაილის დამატება
- d. სურათზე ასახულია WDS კონფიგურაციაში Windows ოპერაციული სისტემის საინსტალაციო ფაილის დამატების პროცესი

სურათზე მოცემული საქაღალდე, წარმოადგენს:



Choose one answer.

- a. საინსტალაციო პაკეტში იმ დირექტორიას, სადაც განთავსებულია ჩატვირთვისა და ინსტალაციის ფაილები
- b. სერვერის მენუსიერებაში იმ დირექტორიას, სადაც ინახება ჩატვირთვისა და ინსტალაციის ფაილები
- c. გარე ინფორმაციის მატარებელზე იმ დირექტორიას, სადაც ინახება ჩატვირთვისა და ინსტალაციის ფაილები
- d. საინსტალაციო პაკეტში იმ დირექტორიას, სადაც WDS სერვისის კონფიგურირებისას იქმნება ჩატვირთვისა და ინსტალაციის ფაილები

1

რომელი მსჯელობაა სწორი?

აღნიშვნები:

1

Choose one answer.

- a. WDS სერვისი (Role) იძლევა საშუალებას დომენში გაწევრიანებულ მომხმარებლებს დაუწესდეთ შეზღუდვები
- b. WDS სერვისის (Role) თვისებების რეალიზებისთვის აუცილებელია წინმსწრებად AD DS, DHCP და DNS სერვისების(Role) ინსტალაცია-გამართვა
- c. WDS სერვისი (Role) იძლევა ფაილების გაზიარების საშუალებას ერთობლივი გამოყენების მიზნით
- d. WDS სერვისის (Role) თვისებების რეალიზება არ არის დამოკიდებული სხვა სერვისების თვისებებზე

1

რომელი მსჯელობაა სწორი?

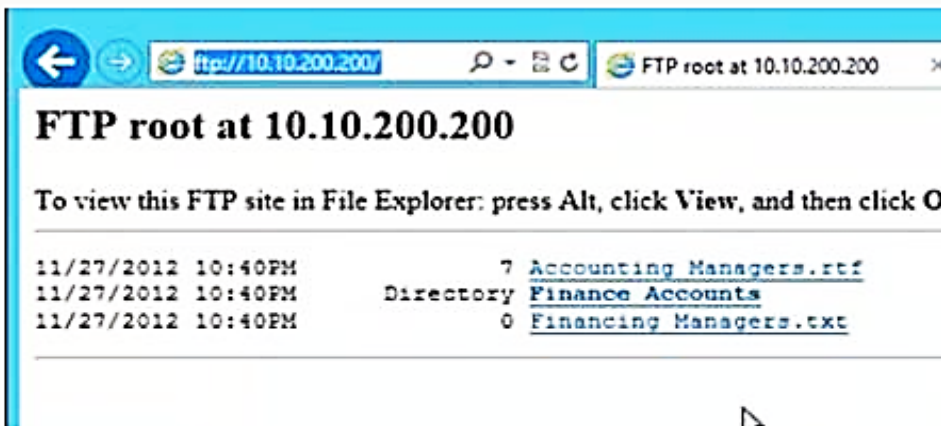
აღნიშვნები:

1

Choose one answer.

- a. IIS Manager ბრძანების მითითებით გამოსულ ფანჯარაში, გვექნება შესაძლებლობა მოვახდინოთ DHCP კონფიგურირება
- b. FRSM გვამლევს საშუალებას გავაზიაროთ ფაილები FTP საიტის მეშვეობით
- c. WDS სერვისის მუშაობის წინაპირობაა AD DS, DNS და DHCP სერვისების ინსტალაცია-გამართვა
- d. AD DS სერვისის ინსტალაცია დამოკიდებულია DHCP Scope მისამართების სივრცის პარამეტრების შერჩევაზე

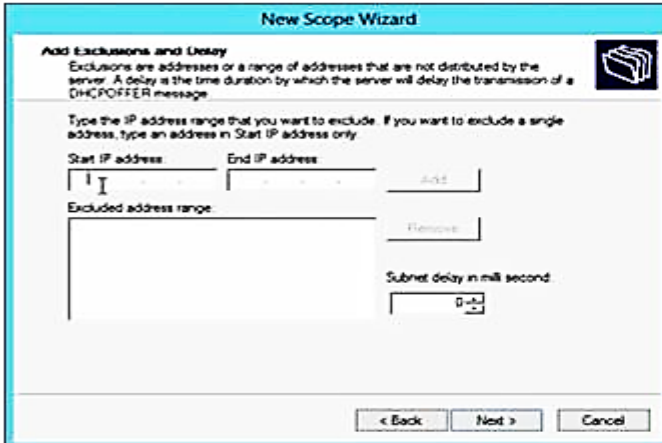
მოცემულ სურათზე ასახულია -



Choose one answer.

- a. დომენში გაწევრიანებული კლიენტი ჰოსტის კავშირი FTP საიტთან
- b. FTP საიტზე წარმოსაჩენი ინფორმაციისთვის ნებართვის მინიჭების პროცესი
- c. FTP საიტის კლიენტის ოპერაციულ სისტემასთან დაკავშირება
- d. FTP საიტის ფორმირების პროცესი

მოცემულ ფანჯარაში აისახება:



Choose one answer.

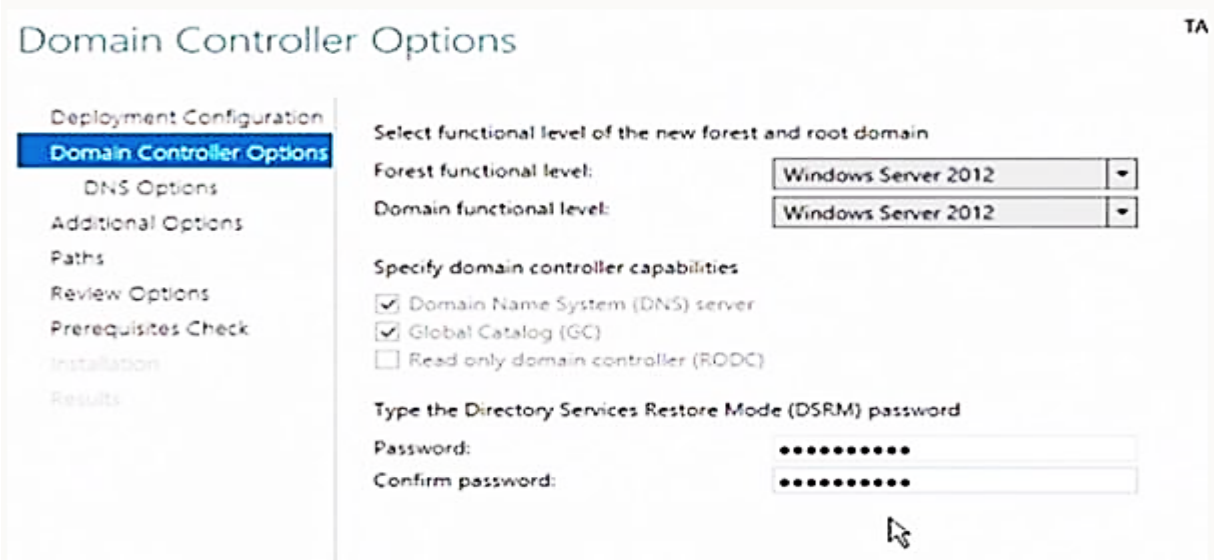
- a. არც ერთი პასუხი არ არის სწორი
- b. ქსელში ჩართული სერვერების დარეზერვებული IP მისამართების დიაპაზონი
- c. ჰოსტების IP მისამართების დიაპაზონი
- d. ჰოსტების MAC მისამართების დიაპაზონი

მოცემული სურათის მიხედვით -



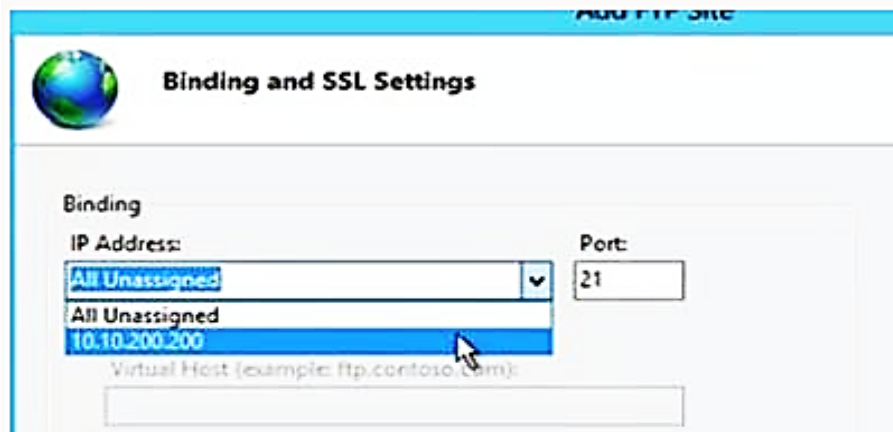
Choose one answer.

- a. მითითებულია იმ მოწყობილობის მისამართი, რომელიც შესაბამის ჰოსტს დაკავშირებს სხვა ქსელის ჰოსტებთან
- b. მითითებულია დასარეზერვებული IP მისამართი
- c. მითითებულია საკუთრივ სერვერის IP მისამართი
- d. მითითებულია DNS სერვერის მისამართი



- Choose at least one answer.
- a. სურათზე ნაჩვენებების მიხედვით მოცემული სერვერი შემდეგს მხოლოდ windows Server 2012-ის ფუნქციონალური დონეების აღქმას
 - b. სისტემის ადგენის პაროლის მითითება არ არის აუცილებელი შესავსები ველი
 - c. სისტემის ადგენის პაროლის მითითება აუცილებელი შესავსები ველია
 - d. სურათზე ნაჩვენებების მიხედვით მოცემული სერვერი შემდეგს სხვა windows Server-ის ნებისმიერი მოდელის ფუნქციონალური დონეების აღქმას

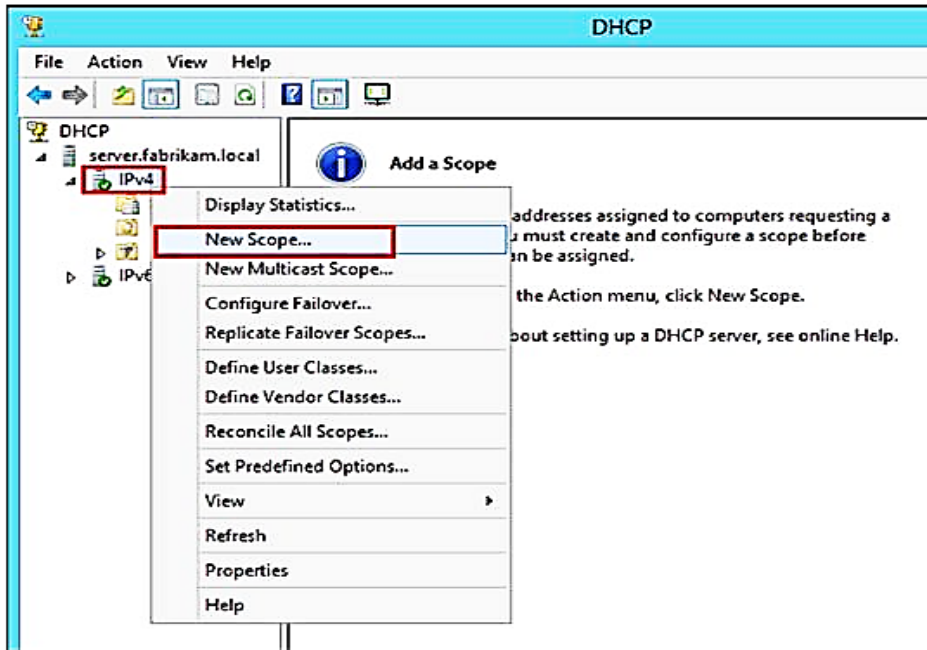
რომელი მსჯელობა არ არის სწორი?



- Choose one answer.
- a. პორტის ნომრის შეცვლის შემთხვევაში, საიტზე წვდომისთვის აუცილებელი იქნება პორტის ნომრის მითითება
 - b. საიტზე წვდომა შესაძლებელი იქნება არჩეული IP მისამართის მითითებით
 - c. პორტის ნომრის არ შეცვლის შემთხვევაში, საიტზე წვდომისთვის აუცილებელი იქნება პორტის ნომრის მითითება
 - d. ჩამონათვალში მითითებულია სერვერის IP მისამართი

რომელი მსჯელობა მცდარი?

- On the Start screen, type DHCP, and click to open DHCP console.
- On the DHCP console, expand the Server name, and then right-click IPv4. Click New Scope...



addresses assigned to computers requesting a must create and configure a scope before can be assigned.

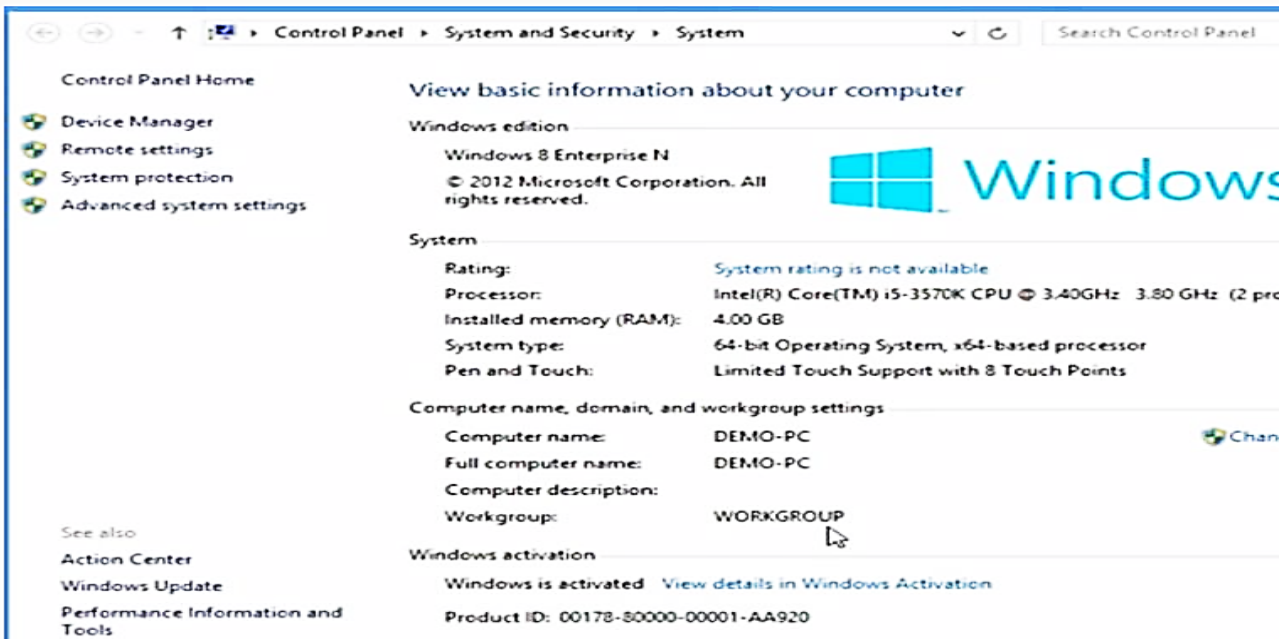
the Action menu, click New Scope.

about setting up a DHCP server, see online Help.

Choose one answer.

- a. მოცემული სურათის მიხედვით იქმნება IP და MAC მისამართების სივრცე, რომელიც დაურთდება ქვედომენებში გაწევრიანებულ ჰოსტებს
- b. მოცემული სურათის მიხედვით იქმნება IP მისამართების სივრცე, რომელიც დაურთდება დომენში გაწევრიანებულ ჰოსტებს
- c. მისანიჭებელი მისამართების სივრცე წარმოადგენილი იქნება IPv4 ფორმატში
- d. მისანიჭებელი მისამართების სივრცე შესაბამისობაში უნდა იყოს დომენური სერვერის მისამართთან

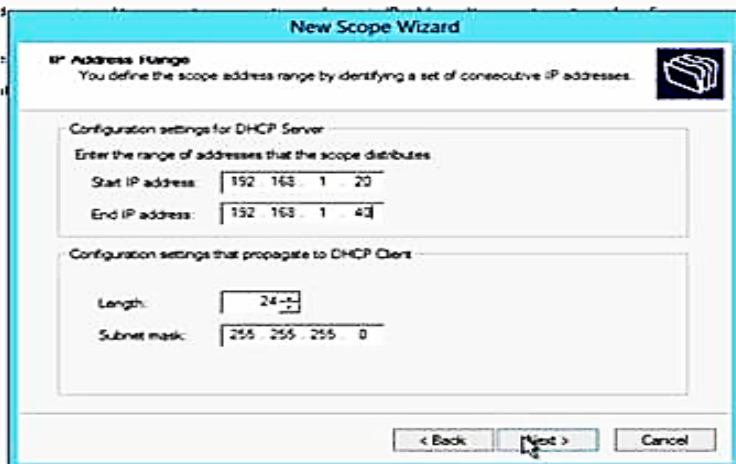
რომელი მსჯელობა მცდარი?



Choose one answer.

- a. მოცემულ ჰოსტის ოპერატიული მეხსიერების ზომაა 4 გბ
- b. მოცემული ჰოსტი გაწევრიანებულია დომენში
- c. მოცემულ ჰოსტზე ჩაწერილია 64 ბიტის ოპერატიული სისტემა
- d. მოცემულ ჰოსტზე ჩაწერილია კლიენტის ოპერატიული სისტემა

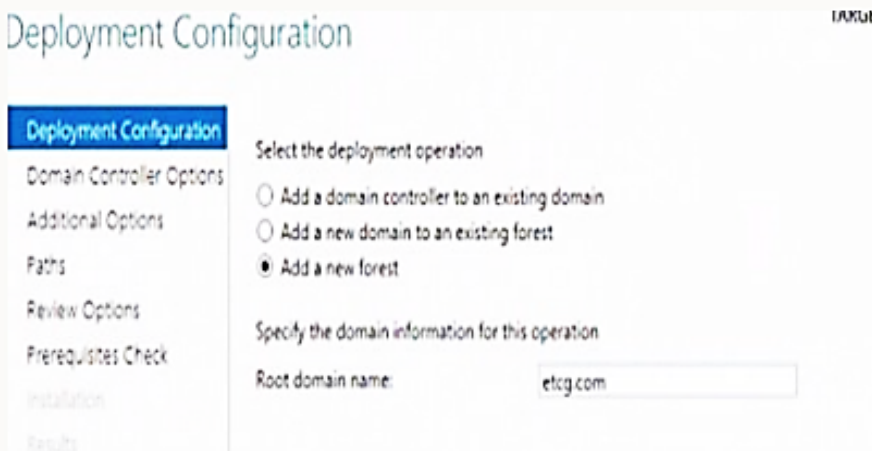
რომელი მსჯელობაა სწორი?



Choose one answer.

- a. სურათზე ასახულია დარეზერვებულ მისამართთა დიაპაზონი
- b. სურათზე ასახული ქვექსელის ნიღაბი(Subnet Mask) არ გახლავთ Default ნიღაბი(Mask) მოცემული ქსელისთვის
- c. სურათზე ასახულია 192.168.1.20 ქსელის მისამართები
- d. სურათზე ასახულია 192.168.1.0 ქსელის მისამართები

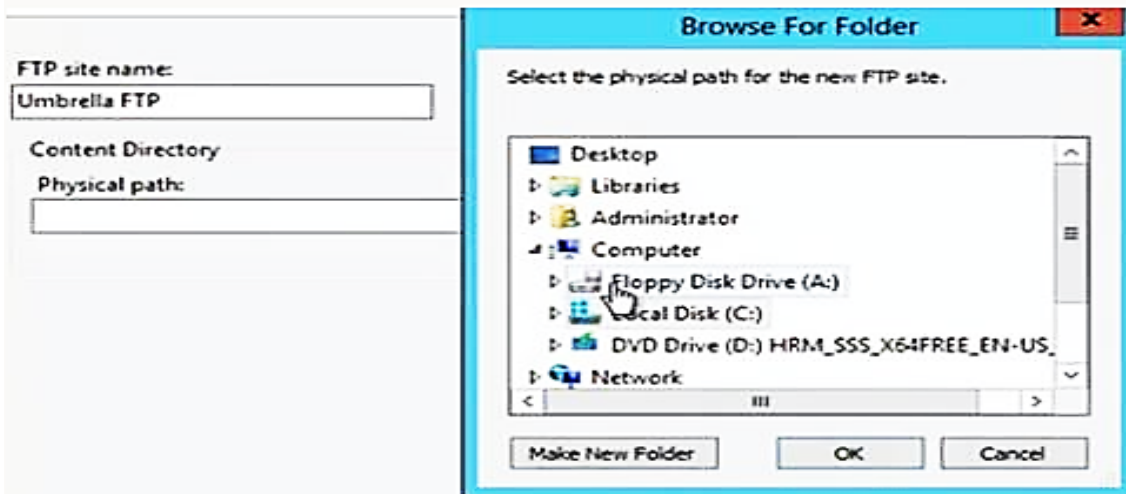
რომელი მსჯელობაა სწორი?



Choose one answer.

- a. იქმნება ახალი Forest-ი ახალ დომენში
- b. იქმნება ახალი დომენი რომელიც იქნება უკვე არსებული დომენის ქვედომენი
- c. იქმნება ახალი დომენი რომელიც გაწევრიანდება უკვე არსებულ forest-ში
- d. იქმნება ახალი დომენი ახალ forest-ში

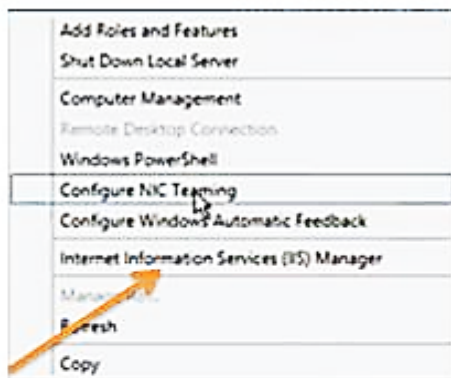
სურათზე ნაჩვენებია:



Choose one answer.

- a. FTP საიტის კლიენტის ოპერაციულ სისტემასთან დაკავშირება
- b. FTP საიტისთვის IP მისამართის მინიჭება
- c. FTP საიტზე წარმოსაჩენი ინფორმაციის მითითების(არჩევის) პროცესი
- d. FTP საიტზე წვდომის უფლებების მქონე მომხმარებლების(User) განსაზღვრა

ქვემოთ მოცემული სურათის მიხედვით რომელი მსჯელობაა სწორი?



Choose one answer.

- a. IIS Manager ბრძანების მითითებით გამოსულ ფანჯარაში, გვექნება შესაძლებლობა შევქმნათ FTP საიტი
- b. სურათზე ასახულია DHCP სერვერის გამართვის დიალოგური ფანჯარა
- c. სურათზე ასახულია DNS სერვერის გამართვის დიალოგური ფანჯარა
- d. IIS Manager ბრძანების მითითებით გამოსულ ფანჯარაში, გვექნება შესაძლებლობა შევქმნათ IP მისამართების სივრცე (Scope)

3. კლიენტებისა და სერვერების ვირტუალიზაცია

3.1. ვირტუალური პროგრამული უზრუნველყოფის (Hypervisor)

კონფიგურაცია

ინფორმაციულმა ტექნოლოგიებმა თანამედროვე საზოგადოებრივ ცხოვრებაში მრავალი საჭირო და საინტერესო რამ შემოიტანა. სხვადასხვა ტექნოლოგიისა და სერვისის პროგრამულ-აპარატურული საშუალება იძლევა შესაძლებლობას უზრუნველყოს ინფორმაციასთან მუშაობის მოხერხებულობა და სისწრაფე. სულ უფრო რთული ხდება ამ აუარებელი ტექნოლოგიებიდან ჩვენთვის სასარგებლოს გამოყოფა და მათგან მაქსიმალური სარგებელის მიღება. მოცემულ თემაში საუბარი გვექნება ერთ-ერთ პერსპექტიულ და ნამდვილად ეფექტურ ტექნოლოგიაზე, რომელიც შემოიჭრა კომპიუტერულ სამყაროში - ეს არის ვირტუალიზაციის ტექნოლოგიები.

ვირტუალიზაციას საფუძვლად უდევს ერთი კომპიუტერის მიერ რამდენიმე კომპიუტერის სამუშაოს შესრულება, რესურსების სხვადასხვა არეებზე გადანაწილების გზით. ვირტუალური სერვერებისა და ვირტუალური სამაგიდო კომპიუტერების საშუალებით შესაძლებელია, რომ განვათავსოთ ერთ კომპიუტერზე რამდენიმე კომპიუტერი სხვადასხვა ოპერაციული სისტემით და დანართით, ერთიან სივრცეში. ვირტუალური ინფრასტრუქტურა უზრუნველყოფს რესურსებზე წვდომის მაღალ დონეს, სამაგიდო კომპიუტერების მართვის უფრო მარტივ სისტემას, გაზრდილ უსაფრთხოებას და კრიტიკული მომენტების შემთხვევაში, აღდგენის გაუმჯობესებულ სისტემას.

ვირტუალიზაციის გამოყენების სფერო

ოპერაციული სისტემების ვირტუალიზაციის გამოყენებამ ბოლო რამდენიმე წლის განმავლობაში წინ წაიწია როგორც ტექნოლოგიურ, ასევე მარკეტინგული მნიშვნელობით. ერთი მხრივ - ვირტუალიზაციის პროდუქტებით სარგებლობა უფრო გაიოლდა, ისინი უფრო საიმედო და ფუნქციურები გახდნენ, სხვა მხრივ კი - მოიძებნა ვირტუალური მანქანის გამოყენების უამრავი ახალი საინტერესო საშუალება. აღსანიშნავია ვირტუალიზაციის პროდუქტების გამოყენების შემდეგი ვარიანტები:

1. **სერვერების კონსოლიდაცია.** მოცემულ მომენტში დანართები, რომლებიც მუშაობენ კომპანიის IT-ინფრასტრუქტურის სერვერებზე, ქმნიან მცირეოდენ

დატვირთვას სერვერების აპარატულ რესურსებზე (საშუალოდ 5-15 პროცენტს). ვირტუალიზაცია ახდენს ამ ფიზიკური სერვერების მიგრირებას ვირტუალურზე და მათ ათავსებს ერთ ფიზიკურ სერვერზე, შედეგად იზრდება დატვირთვა 60-80 პროცენტამდე, ეს კი ამალღებს აპარატურის გამოყენების კოეფიციენტს, რაც აპარატურაზე, მომსახურებასა და ელექტროენერგიაზე არსებითად ეკონომიის გაწევის საშუალებას იძლევა.

2. დანართების შემუშავება და ტესტირება. ვირტუალიზაციის მრავალი ნაწარმი რამდენიმე სხვადასხვა ოპერაციული სისტემების ერთდროული გაშვების შესაძლებლობას გვაძლევს, ამით კი შესაძლებელია, რომ პროგრამული უზრუნველყოფის შემუშავებლებმა და ტესტირებმა მოახდინონ დანართების ტესტირება სხვადასხვა პლატფორმაზე და კონფიგურაციაში. ასევე მოსახერხებელი საშუალებები სისტემის მიმდინარე მდგომარეობის მაუსის ერთი დაჭერით „აღბეჭდვისათვის“ და ასევე იოლად ამ მდგომარეობის აღსადგენად, ქმნიან სატესტო გარემოს სხვადასხვა კონფიგურაციისათვის, რაც მნიშვნელოვნად ზრდის დამუშავების სიჩქარესა და ხარისხს.

3. ბიზნესში გამოყენება. ვირტუალური მანქანების გამოყენების ეს ვარიანტი წარმოადგენს ყველაზე უფრო ფართო და შემოქმედებით სფეროს. მას მიეკუთვნება ყველაფერი, რაც კი გამოდგება ბიზნესში IT-რესურსებთან ყოველდღიური ურთიერთობისას. მაგალითად, ვირტუალური მანქანების საფუძველზე შესაძლებელია მარტივად შეიქმნას სამუშაო სადგურების და სერვერების სარეზერვო ასლები (უბრალოდ საქაღალდეების ასლის შექმნა), სისტემების აწყობა, რომლებიც უზრუნველყოფენ დაზიანების შემთხვევაში აღდგენის მინიმალურ დროს, და სხვა. გამოყენების ვარიანტების მოცემულ ჯგუფს მიეკუთვნება ყველა ის ბიზნეს გადაწყვეტა, რომლებიც გამოიყენებენ ვირტუალური მანქანების ძირითად უპირატესობებს.

4. ვირტუალური სამუშაო სადგურების გამოყენება. ვირტუალური მანქანების შემოღების პირობებში უაზრობაა ისეთი სამუშაო სადგურის შექმნა, რომელიც მიზნულია აპარატურასთან. ახლა ვირტუალური მანქანის ერთჯერადად შექმნისას, თავისი სამუშაო ან საშინაო გარემოთი, შესაძლებელია მისი გამოყენება ნებისმიერ სხვა კომპიუტერზე. ასევე შესაძლებელია ვირტუალური მანქანების მზა შაბლონების გამოყენება (**Virtual Appliances**), რომელთა მეშვეობითაც გადაიჭრება გარკვეული ამოცანები (მაგალითად, დანართის სერვერი). ვირტუალური სამუშაო სადგურების გამოყენების ასეთი კონცეფცია

ხორციელდება ჰოსტ-სერვერებზე მათზე მომხმარებლის გადასატანი სამაგიდო კომპიუტერების გასაშვებად. მომავალში მომხმარებელს შეუძლია ეს სამუშაო მაგიდები თან წაიღოს, ისე რომ არ მოახდინოს სინქრონიზაცია ნოუთბუქიდან. გამოყენების ეს ვარიანტი ასევე გვაძლევს დაცული სამომხმარებლო სადგურების შექმნის საშუალებას, რომელთა გამოყენება შეიძლება, მაგალითად შემკვეთისათვის პროგრამის შესაძლებლობების სადემონსტრაციოდ. შესაძლოა განისაზღვროს ვირტუალური მანქანის გამოყენების დრო და მისი გასვლის შემდეგ ვირტუალური მანქანა გამოირთვება. გამოყენების ამ ვარიანტში ჩადებულია დიდი შესაძლებლობები.

ვირტუალური მანქანების უპირატესობები:

- ეკონომია აპარატურულ უზრუნველყოფაზე, სერვერების კონსოლიდაციისას;
- პოტენციურად საშიში გარემოს იზოლირების შესაძლებლობა;
- ძველი ოპერაციული სისტემების მხარდაჭერის შესაძლებლობა,

თავსებადობის უზრუნველყოფის მიზნით;

- საჭირო აპარატურული კონფიგურაციის შექმნის შესაძლებლობა;
- ვირტუალურ მანქანებს შეუძლიათ შექმნან ისეთი მოწყობილობები, რომელიც

ჩვენ არ გვაქვს კომპიუტერზე;

▪ ერთ საკვანძო კომპიუტერზე შესაძლებელია ერთდროულად რამდენიმე ვირტუალური მანქანის გაშვება, რომლებიც გაერთიანებულნი იქნებიან ვირტუალურ ქსელში;

▪ ვირტუალური მანქანები წარმოგვიდგენენ დიდ შესაძლებლობებს ოპერაციულ სისტემებთან მუშაობის შესწავლისას;

- ვირტუალური მანქანები აუმჯობესებენ მობილურობას;

▪ ვირტუალური მანქანები შეიძლება იქნენ ორგანიზებული „პაკეტურ დანართებში“;

- ვირტუალური მანქანები არიან უფრო მართვადები.

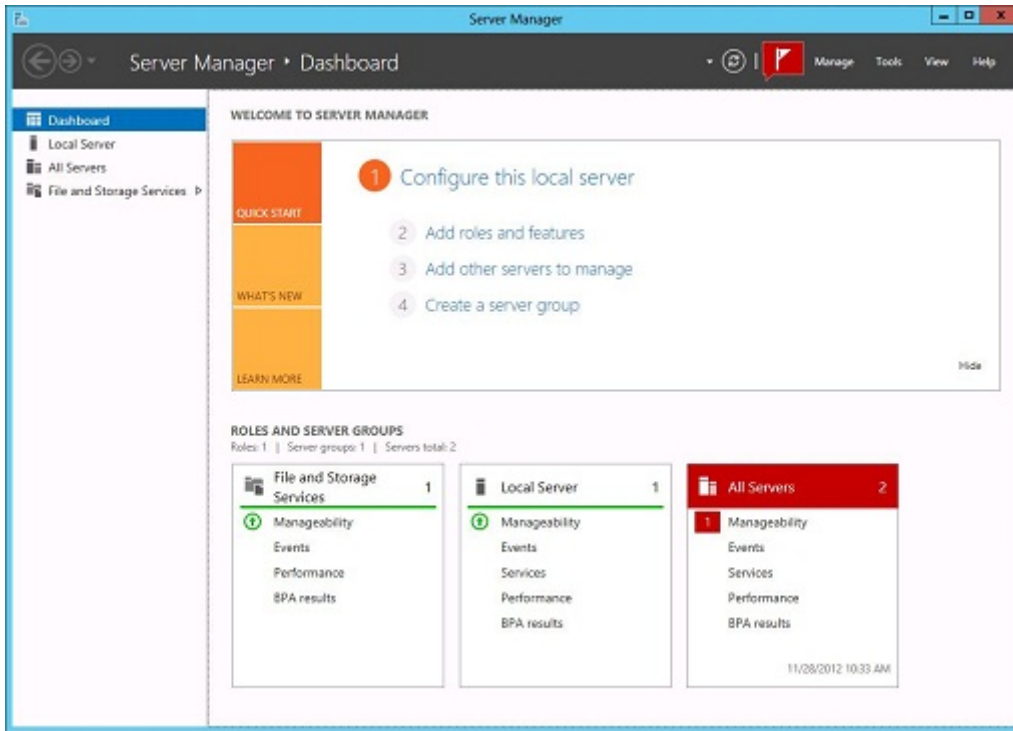
ვირტუალური მანქანების ნაკლოვანებები:

რა თქმა უნდა მხოლოდ ზემოთ ჩამოთვლილით არ შემოიფარგლება ვირტუალური მანქანების შესაძლებლობები, მათ აქვთ კიდევ ბევრი სასარგებლო ფუნქცია. თუმცა როგორც ნებისმიერ ახალ ან პერსპექტიულ გადაწყვეტას, ვირტუალურ მანქანებსაც აქვთ ხარვეზები:

- შეუძლებელია ყველა მოწყობილობის ემულაცია;
- ვირტუალიზაცია საჭიროებს დამატებით აპარატურულ რესურსებს;
- ვირტუალიზაციის ზოგიერთი პლატფორმა მოითხოვს კონკრეტულ აპარატურულ უზრუნველყოფას;
- ძვირი ღირს ვირტუალიზაციის კარგი პლატფორმები.

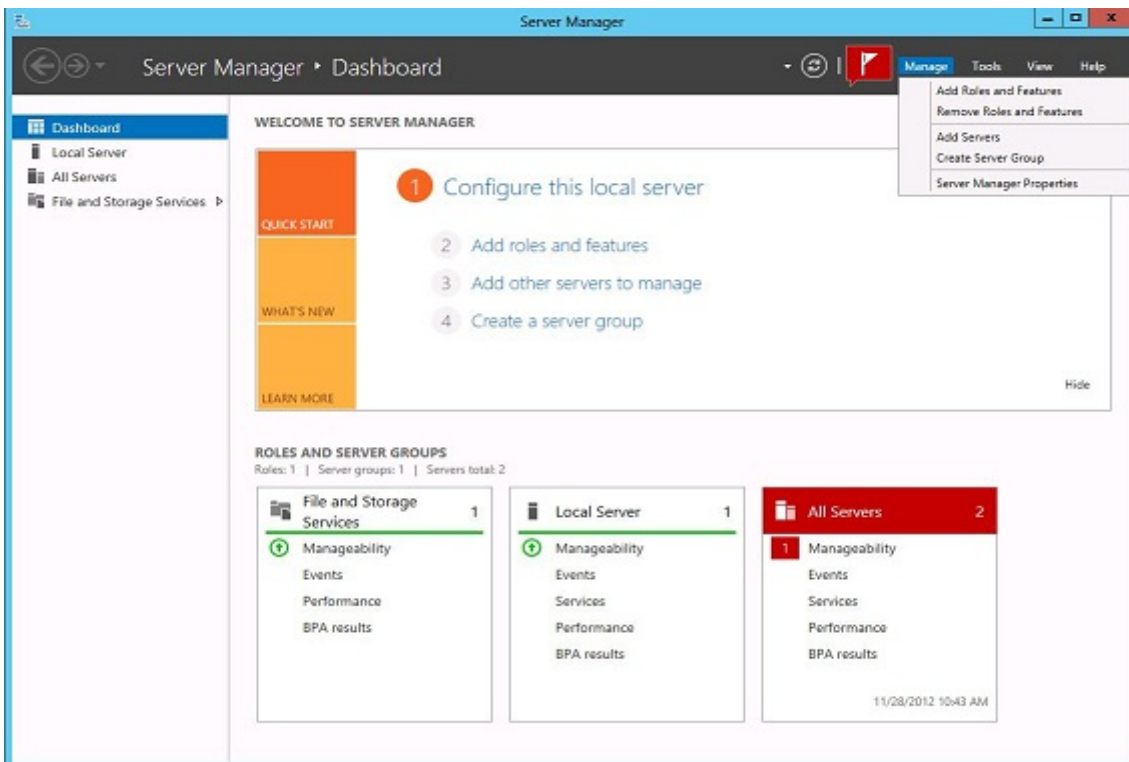
Windows Server 2012 Hyper-V-ს ინსტალაცია და კონფიგურაცია

სერვერის სამუშაო მაგიდაზე გახსენით **Server Manager** ფანჯარა.



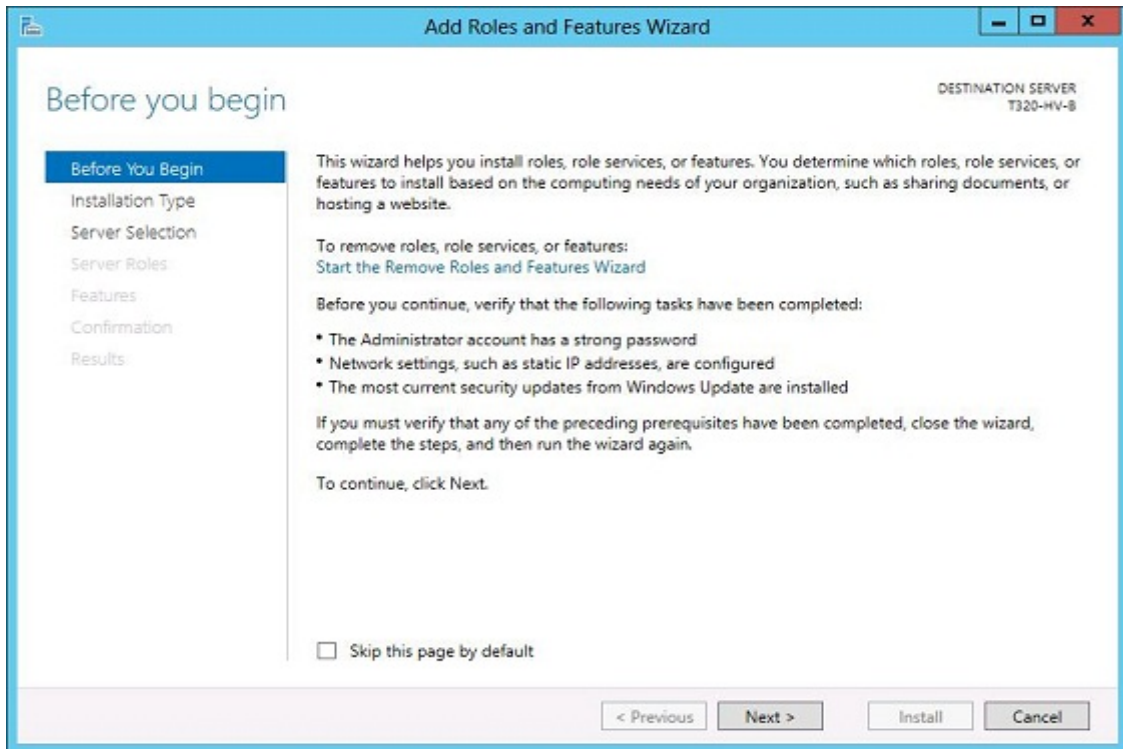
სურ.3.1. 1

გამოსული ფანჯრის მენიუს ზოლში დააჭირეთ **Manage** ლილავს და აირჩიეთ **Add Roles and Features** (როლებისა და კომპონენტების დამატება) ბრძანება.



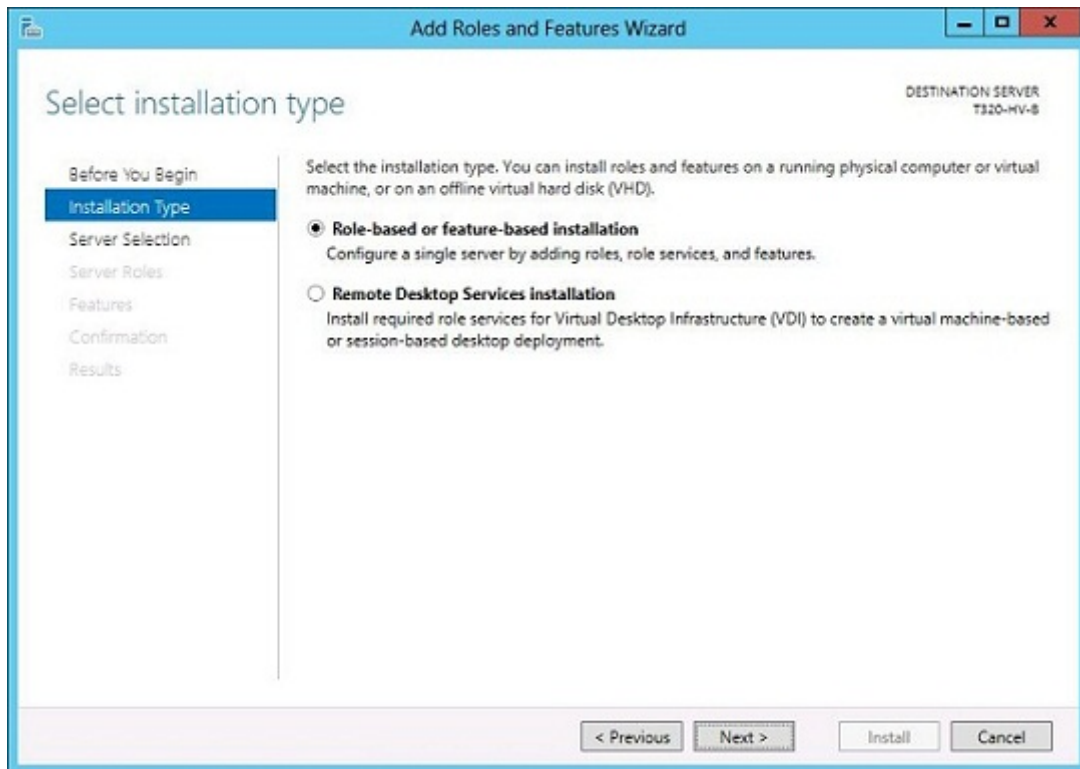
სურ.3.1. 2

Add Roles and Features Wizard ფანჯარაში, **Before You Begin** გვერდზე, დააჭირეთ **Next** ლილავს.



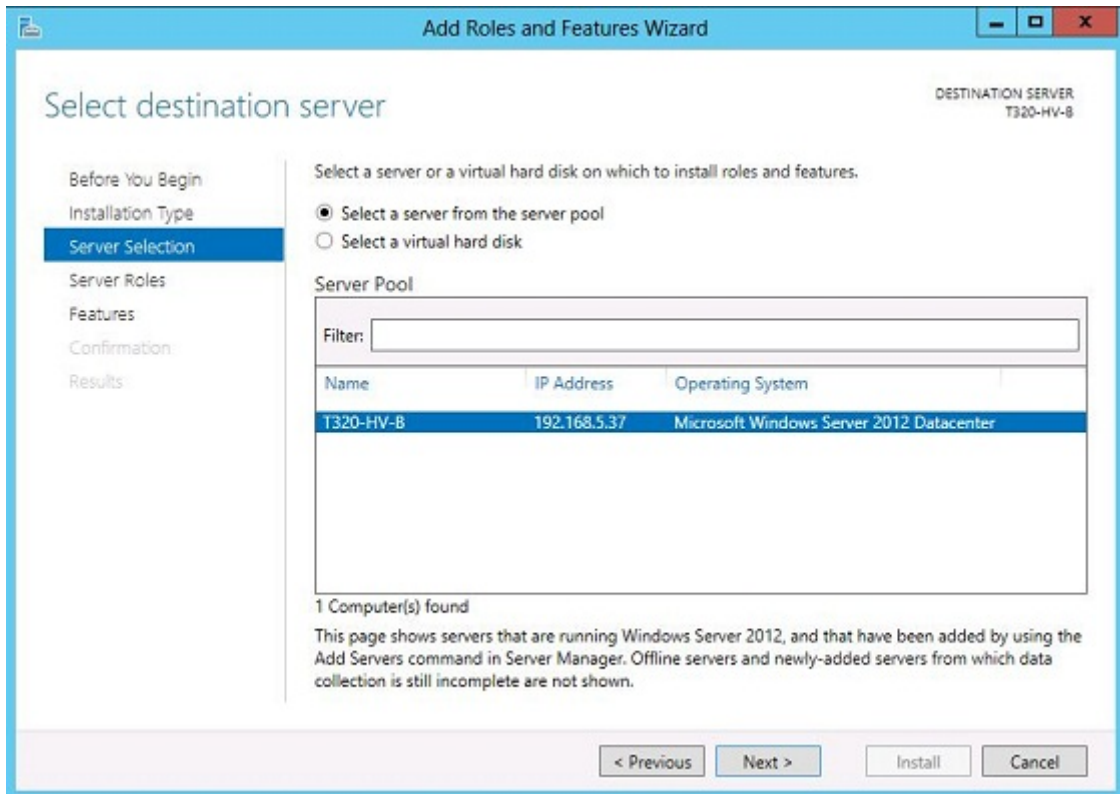
სურ.3.1. 3

Installation Type გვერდზე, აირჩიეთ **Role-based or feature-based installation** და **Next**.



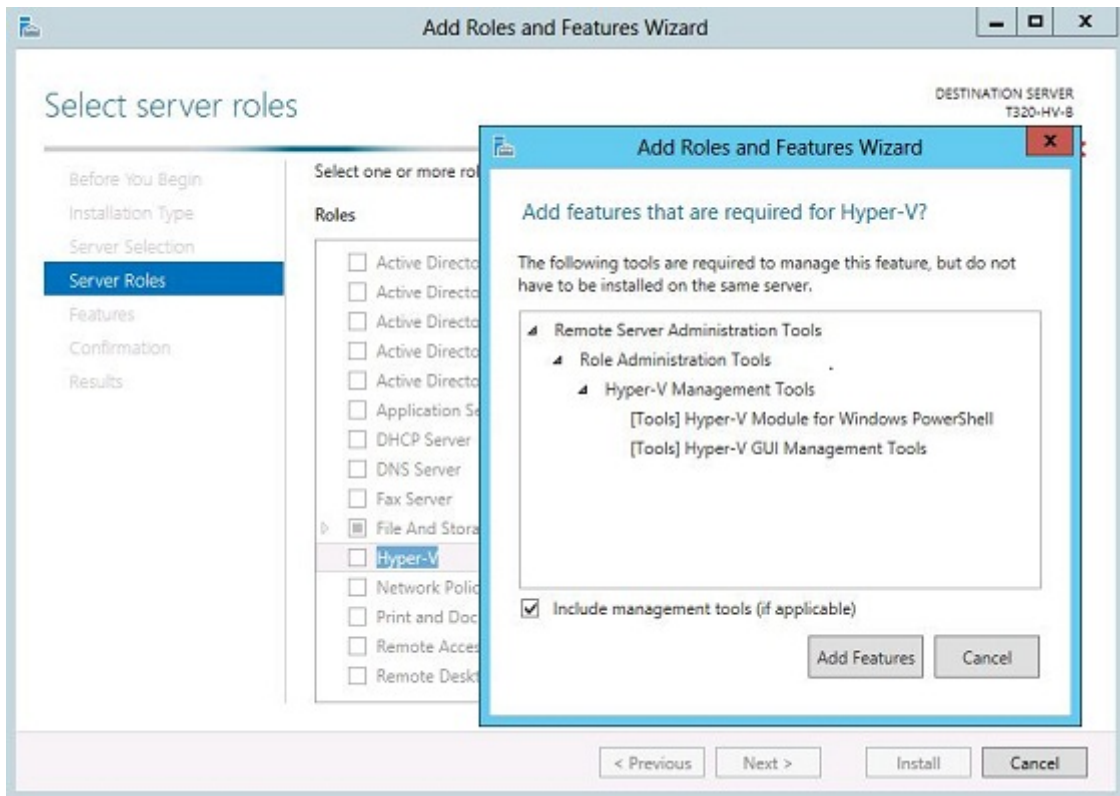
სურ.3.1. 4

Select Destination Server გვერდზე, აირჩიეთ სერვერი და დააჭირეთ **Next**-ს.



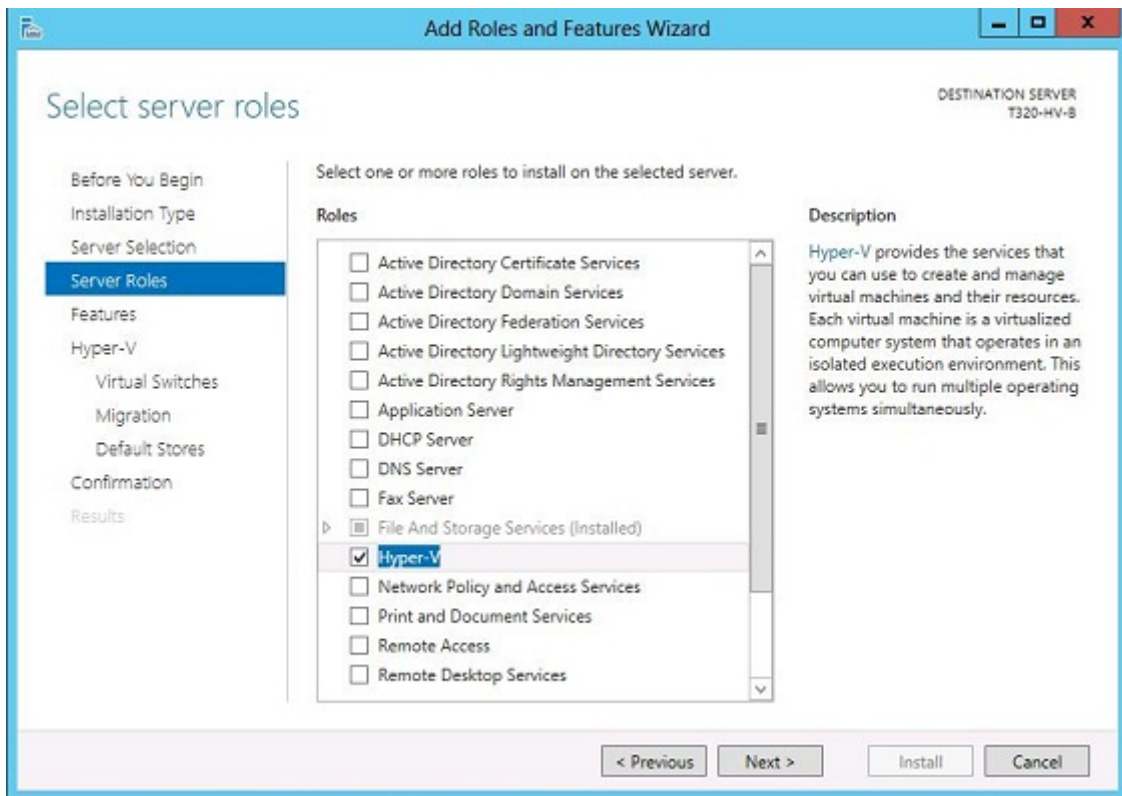
სურ.3.1. 5

Select Server Roles გვერდზე, აირჩიეთ **Hyper-V**, და დააჭირეთ **Add Features** შემოთავაზებულ დიალოგურ ფანჯარაში.



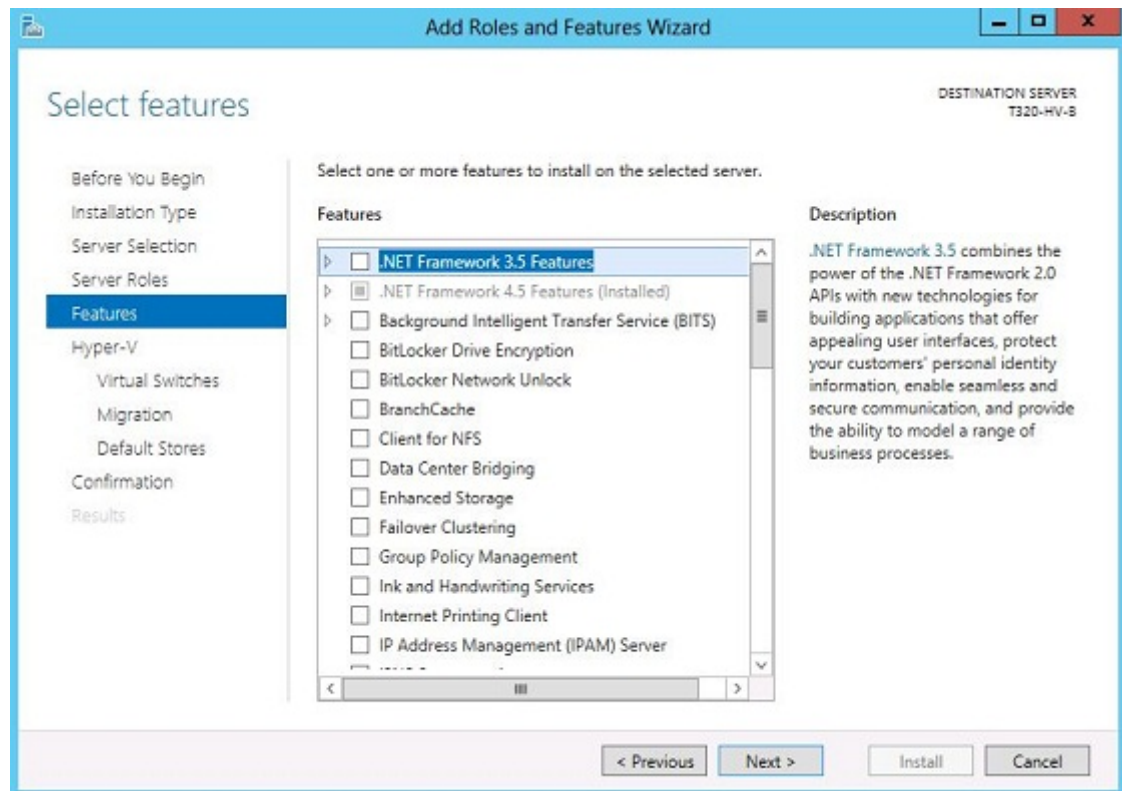
სურ.3.1. 6

Select Server Roles - როლების არჩევის გვერდზე, დააჭირეთ **Next** ლილავს.



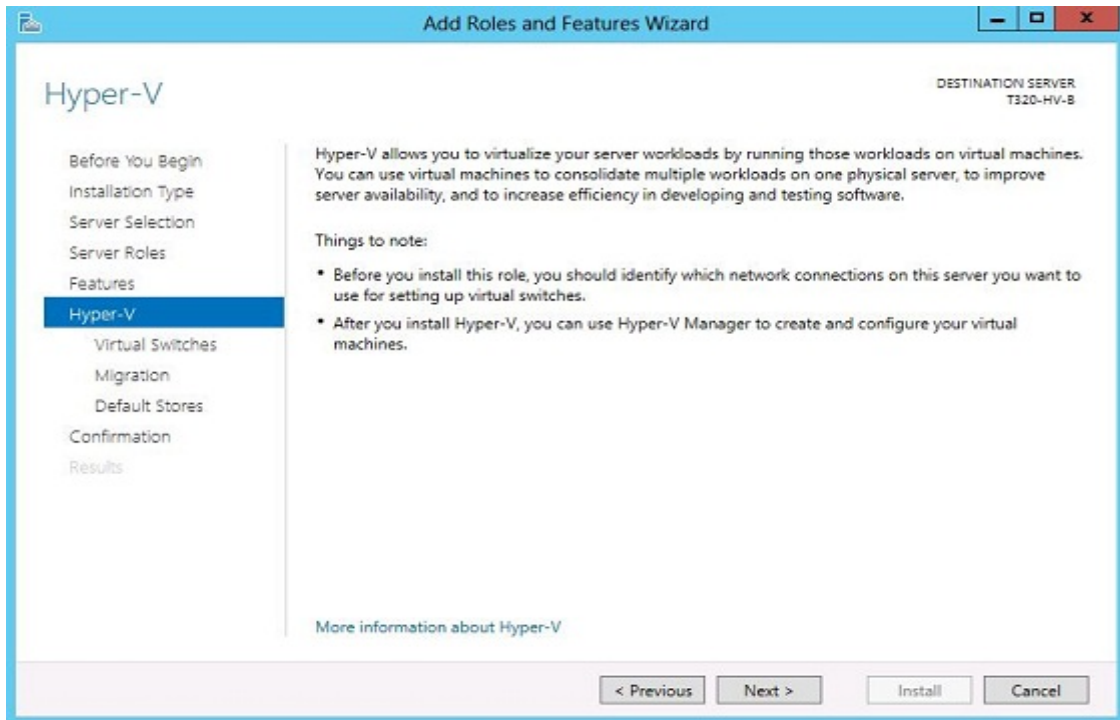
სურ.3.1. 7

Select Features - კომპონენტების არჩევის გვერდზე დააჭიროთ **Next**-ს.



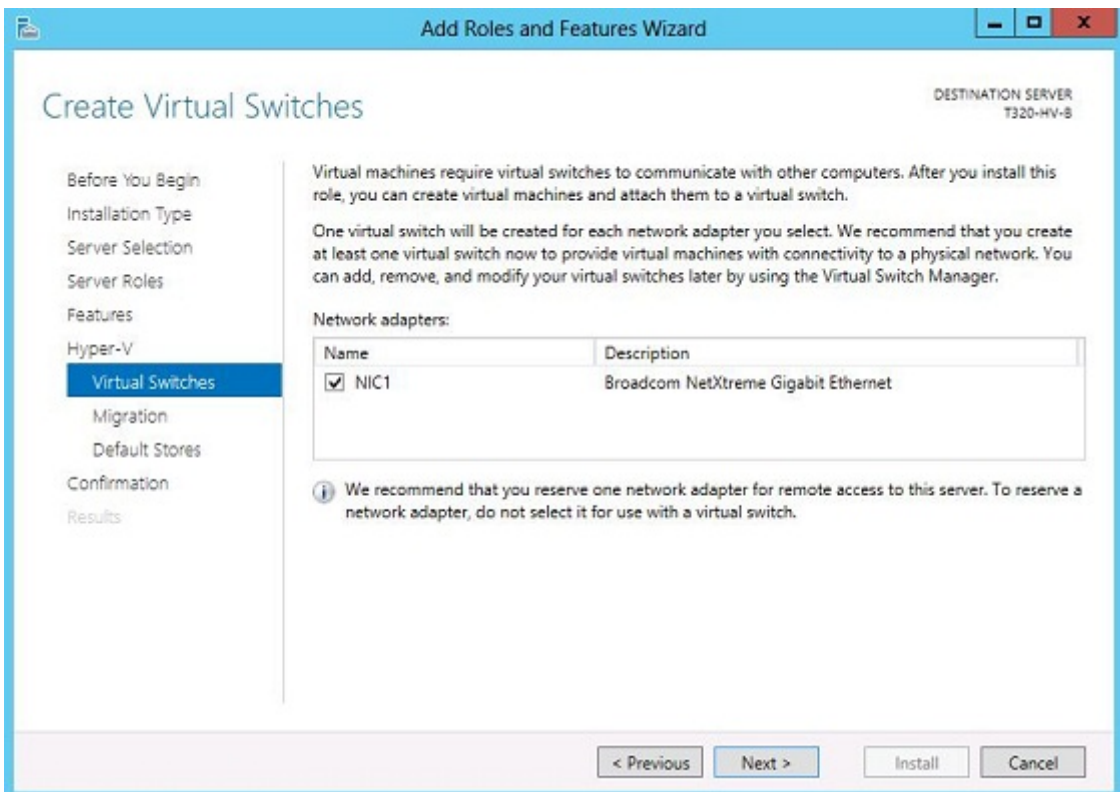
სურ.3.1. 8

Hyper-V გვერდზე, დააჭიროთ **Next** ღილაკს.



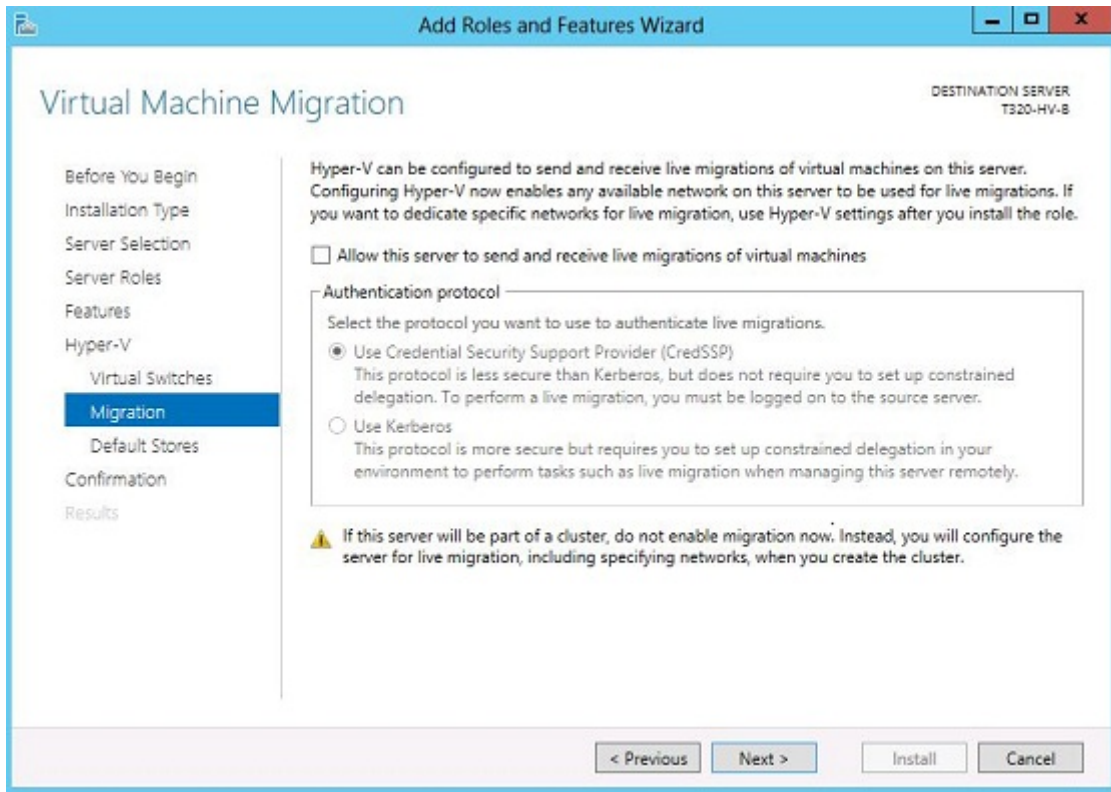
სურ.3.1. 9

Create Virtual Switches - ვირტუალური კომპუტატორების შექმნის გვერდზე, აირჩიეთ ქსელის ადაპტერი და შემდეგ **Next**.



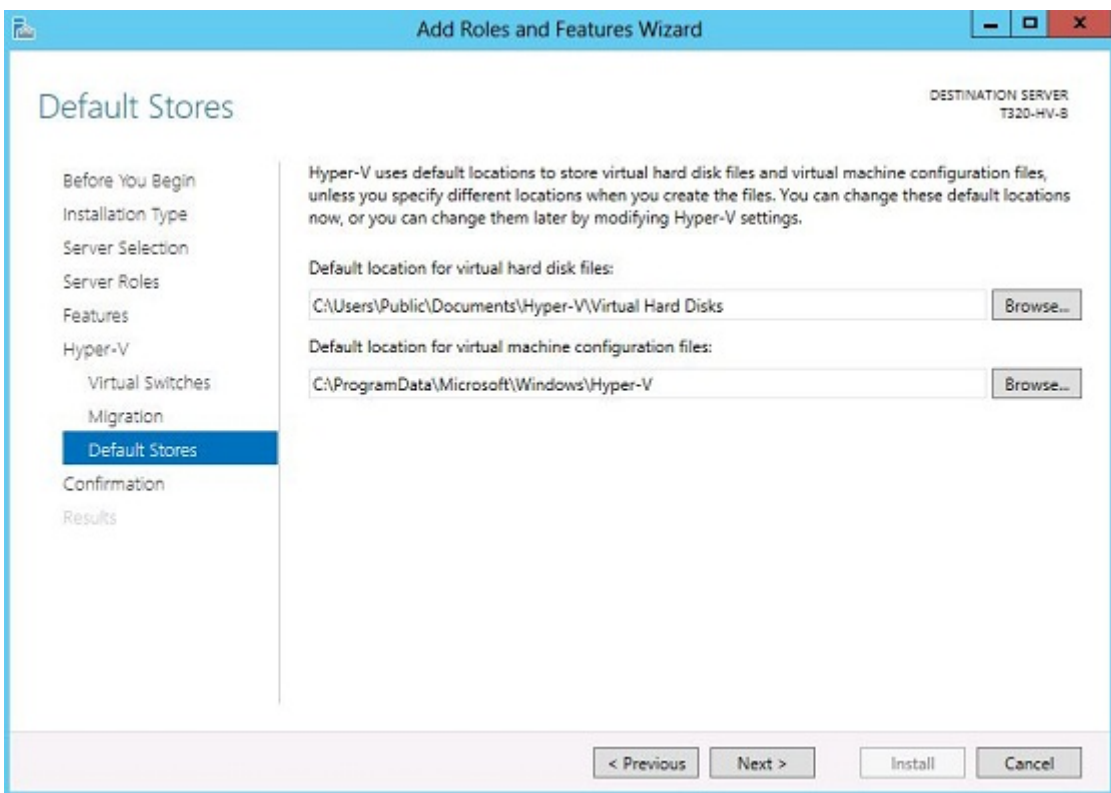
სურ.3.1. 10

Virtual Machine Migration - ვირტუალური მანქანის გადაადგილების გვერდზე დააჭირეთ **Next**-ს.



სურ.3.1. 11

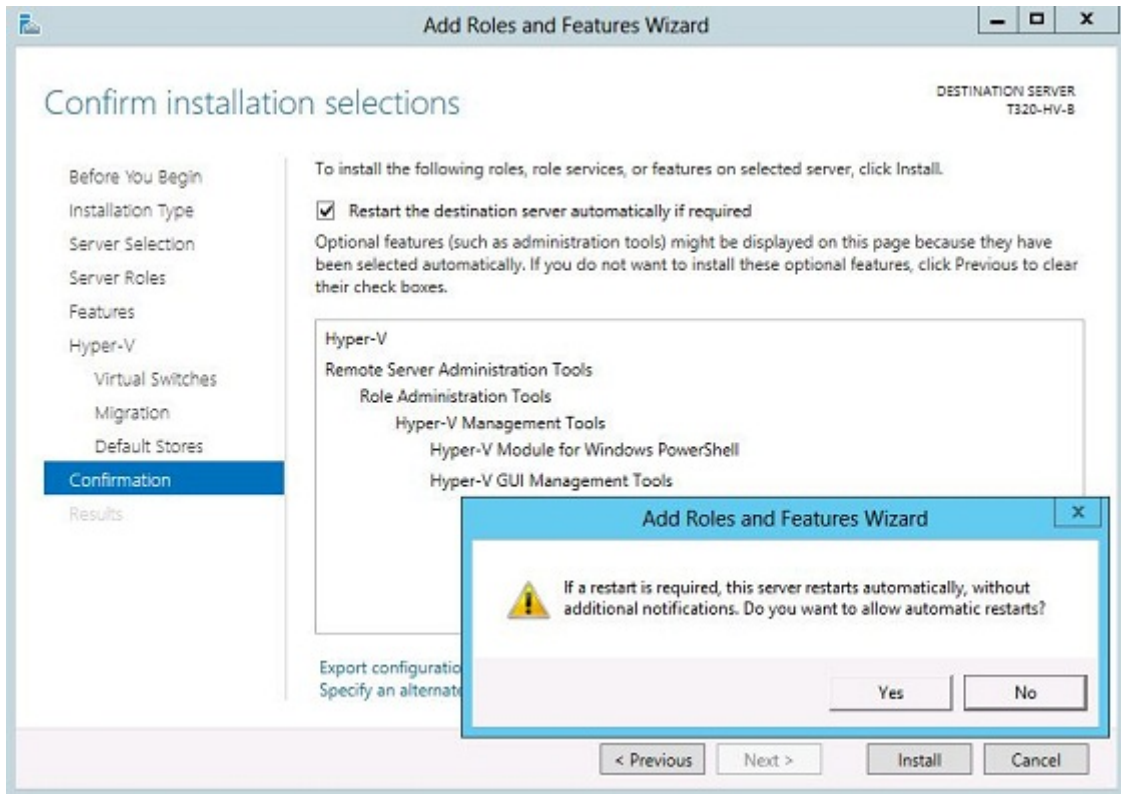
Default Stores - ნაგულისხმევი შენახვის გვერდზე დააჭირეთ **Next** ლილავს.



სურ.3.1. 12

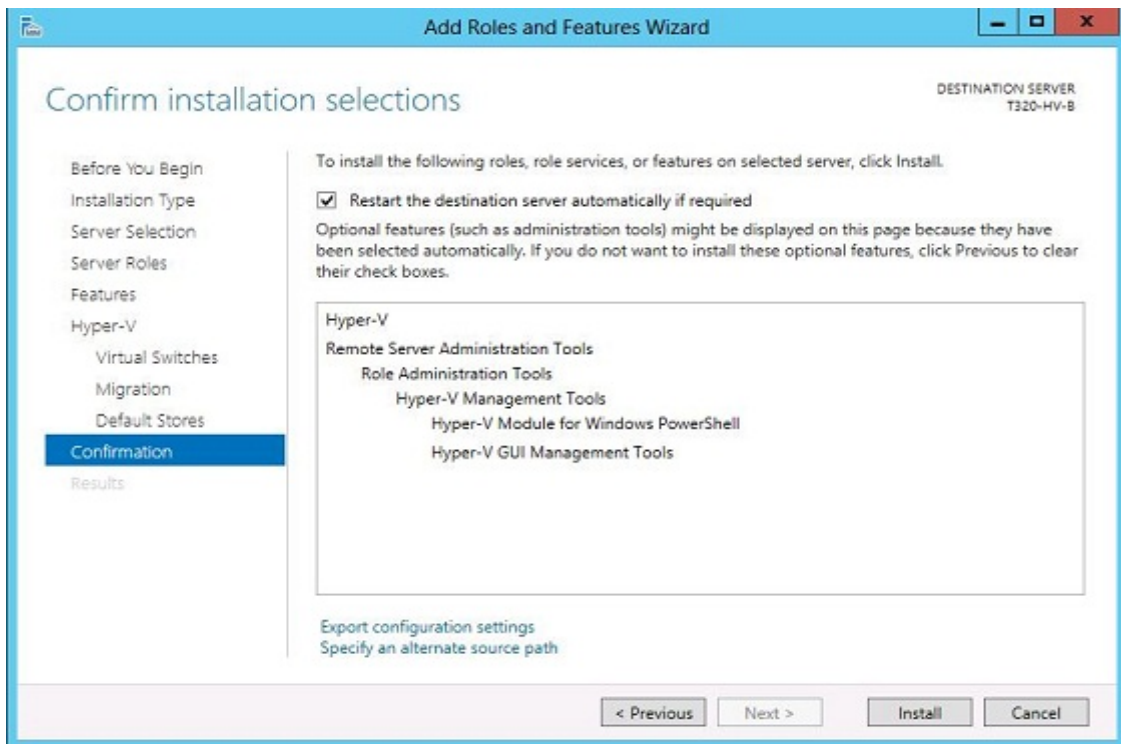
დადასტურების გვერდზე - **Confirmation page**, აირჩიეთ **Restart the destination server automatically if required** - აუცილებლობის შემთხვევაში დანიშნულების სერვერის

ავტომატური გადატვირთვა, და შემდეგ გამოსულ დიალოგურ ფანჯარაში დააჭირეთ **Yes** ღილაკს.



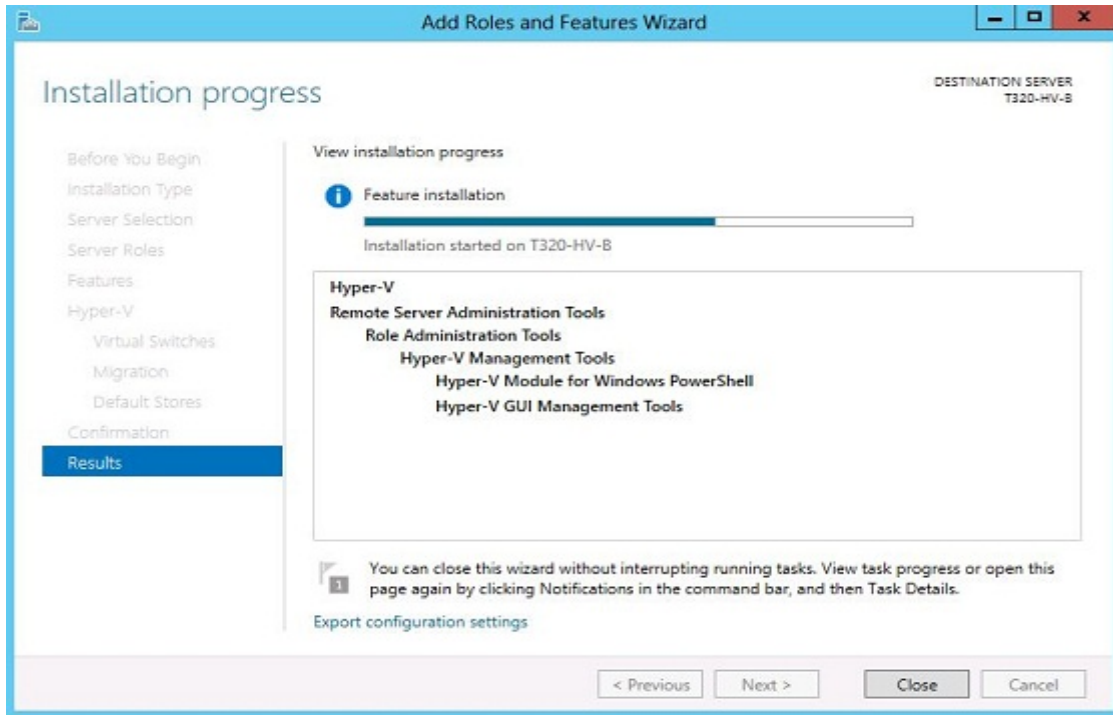
სურ.3.1. 13

დადასტურების გვერდზე - **Confirmation page**, დააჭირეთ **Install** ბრძანება.



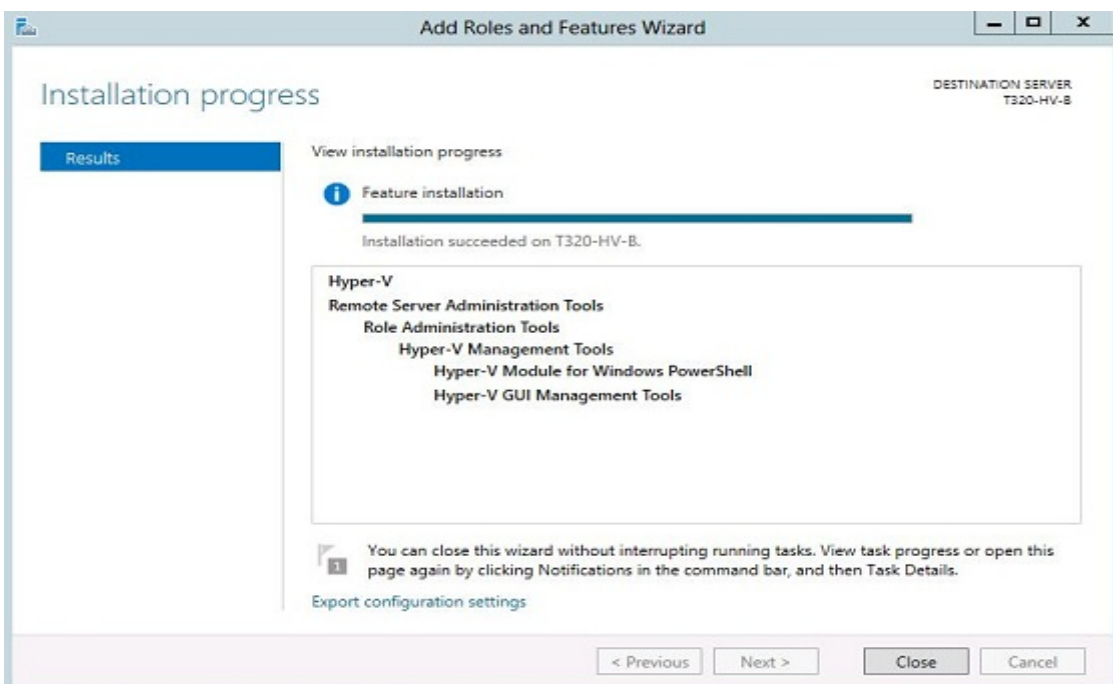
სურ.3.1. 14

Installation Progress - ინსტალაციის მიმდინარეობის გვერდზე, თქვენ შეგიძლიათ თვალი ადევნოთ **Hyper-V** როლის ინსტალაციას, სანამ სისტემა ავტომატურად არ გადაიტვირთება.



სურ.3.1. 15

სერვერის გადატვირთვისა და **Server Manager**-ის გახსნის შემდეგ, შეამოწმეთ ინსტალაციის მიმდინარეობის გვერდი რათა დარწმუნდეთ **Hyper-V** როლის ინსტალაცია დასრულდა წარმატებით, შემდეგ დააჭირეთ **Close** ღილაკს.



სურ.3.1. 16

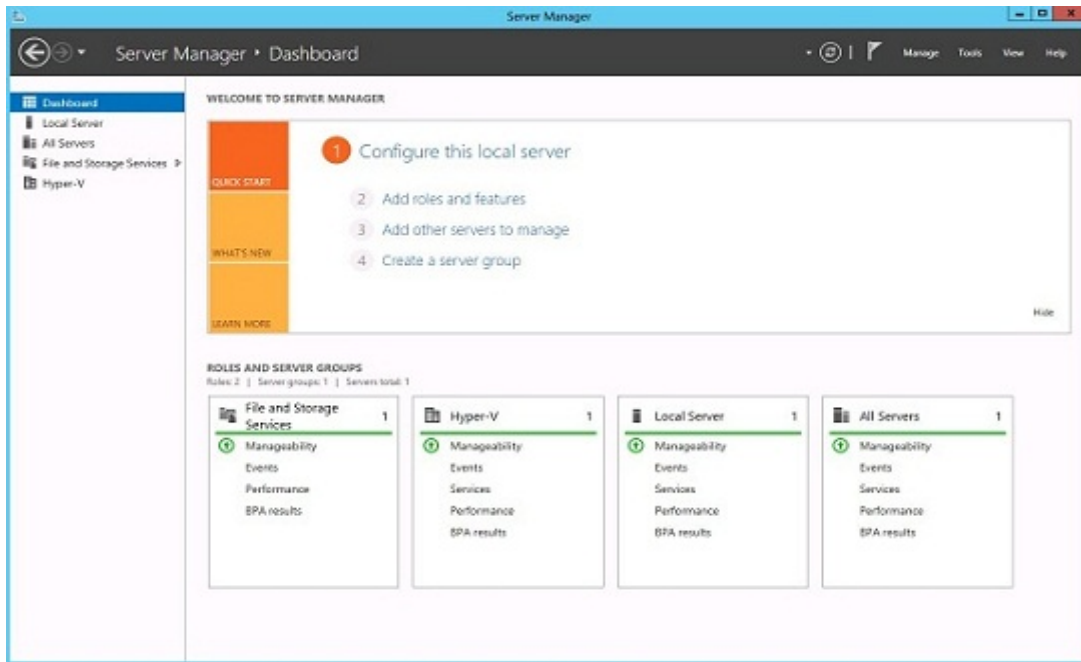
Hyper-V ჰოსტის პარამეტრების კონფიგურაცია

სერვერზე **Hyper-V** როლის ინსტალაციის შემდეგ, თქვენ შეგიძლიათ შეასრულოთ **Hyper-V** ჰოსტის პარამეტრების კონფიგურაცია. ქვემოთ მოცემულია ბაზისურ პარამეტრები, რომლის მომართვაც უნდა მოხდეს.

- ვირტუალური მყარი დისკისა და ვირტუალური მანქანის კონფიგურაციის ფაილების შენახვის ადგილის კონფიგურაცია;
- ფიზიკური გრაფიკული პროცესორების (GPUs) კონფიგურაცია, **RemoteFX**-თან გამოსაყენებლად (თუ დაინსტალირებულია დაშორებული სამუშაო მაგიდის ვირტუალიზაციის ჰოსტის როლი - **Remote Desktop Virtualization Host**);
- **NUMA (Non-uniform memory access** - მუხსიერებასთან არათანაბარი წვდომა) **spanning**-ის კონფიგურაცია, როცა სერვერს აქვს **NUMA** კვანძები ვირტუალური მანქანის წარმადობის გასაზრდელად;
- **Live Migration**-ცოცხალი გადაადგილებისა და აუთენტიფიკაციის პროტოკოლის კონფიგურაცია, რათა გამოყენებულ იქნას რამოდენიმე ერთდროული ცოცხალი გადაადგილებების დაშვება (ნაგულისხმევად 2) და სერვერის ქსელები ცოცხალი გადაადგილებების ღონისძიებების (Event) მხარდასაჭერად;
- საცავის გადაადგილების - **Storage Migration** და ერთდროულად რამოდენიმე საცავის გადაადგილების დაშვების (ნაგულისხმევად არის 2) კონფიგურაცია;
- **Replication** - გამეორების კონფიგურაცია სერვერის ასლის-**Replica** ფუნქციონალის მხარდაჭერისა და აუთენტიფიკაციის პროტოკოლის გამოყენებისთვის, ასევე გამეორებისთვის - **Replication** ავტორიზებული სერვერების მხარდასაჭერად.

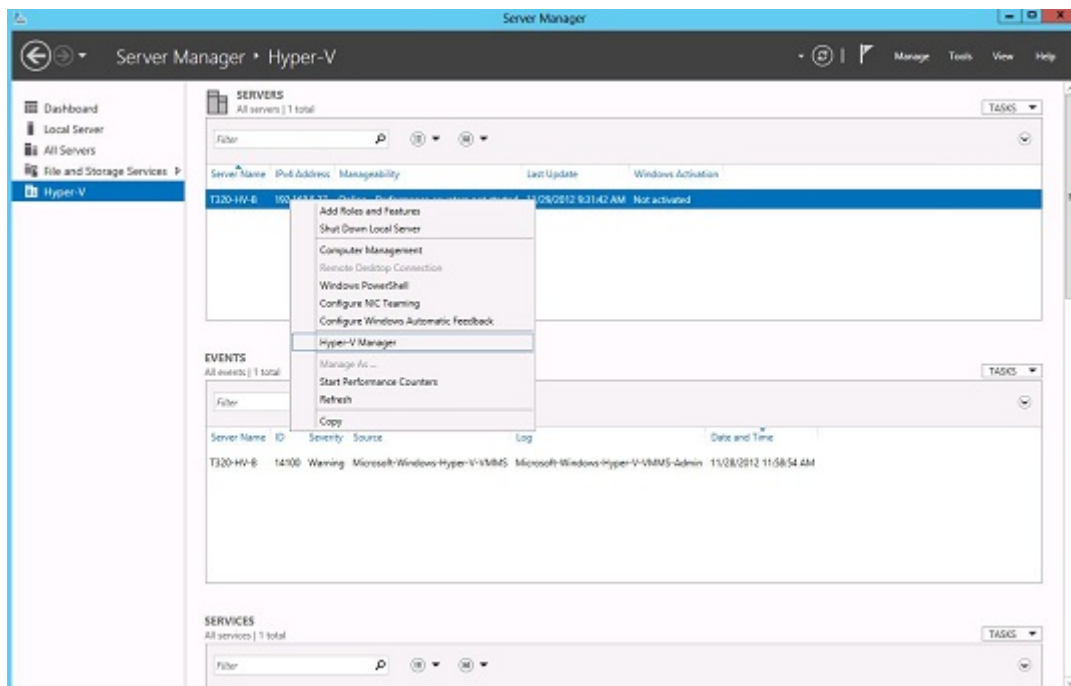
სერვერზე Hyper-V ჰოსტის პარამეტრების კონფიგურაცია

სერვერის სამუშაო მაგიდაზე გახსენით **Server Manager** - სერვერის მმართველი ფანჯარა.



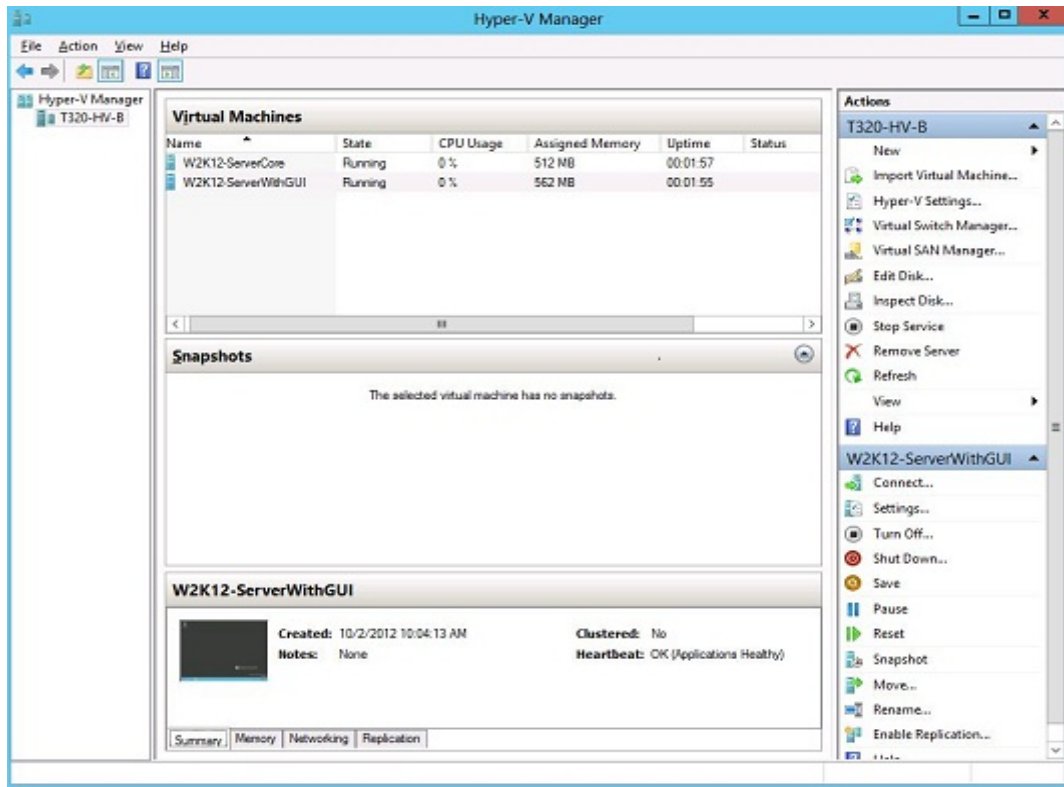
სურ.3.1. 17

გამოსული ფანჯრის ნავიგაციის პანელზე დააჭირეთ **Hyper-V**, შემდეგ მასის მარჯვენა ღილაკით მონიშნეთ სერვერი და გამოსული ჩამონათვალიდან აირჩიეთ **Hyper-V Manager**.



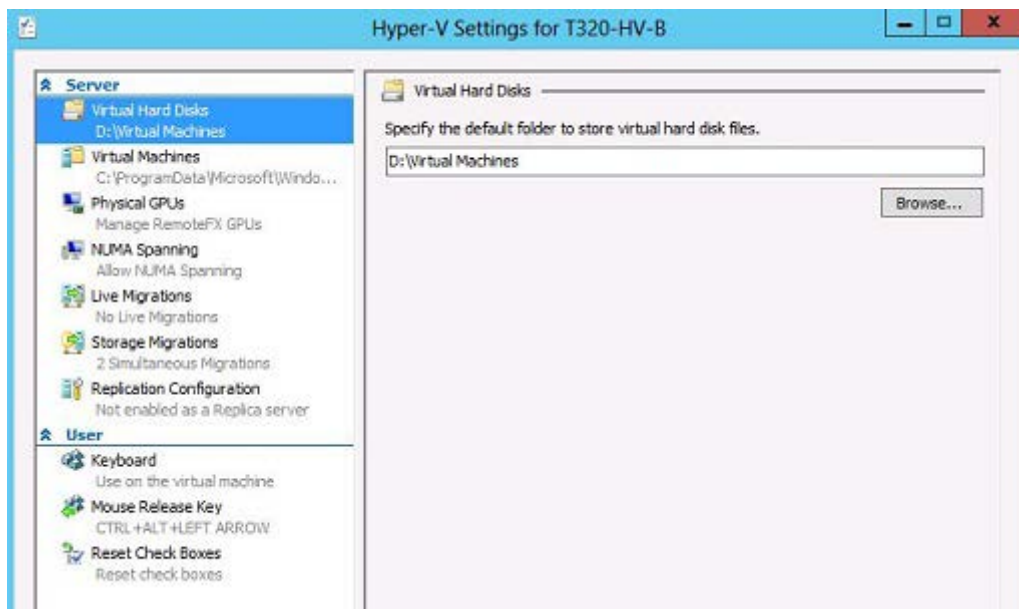
სურ.3.1. 18

Hyper-V Manager-ის **Actions** pane-მოქმედებათა პანელში აირჩიეთ **Hyper-V Settings**-პარამეტრები.



სურ.3.1. 19

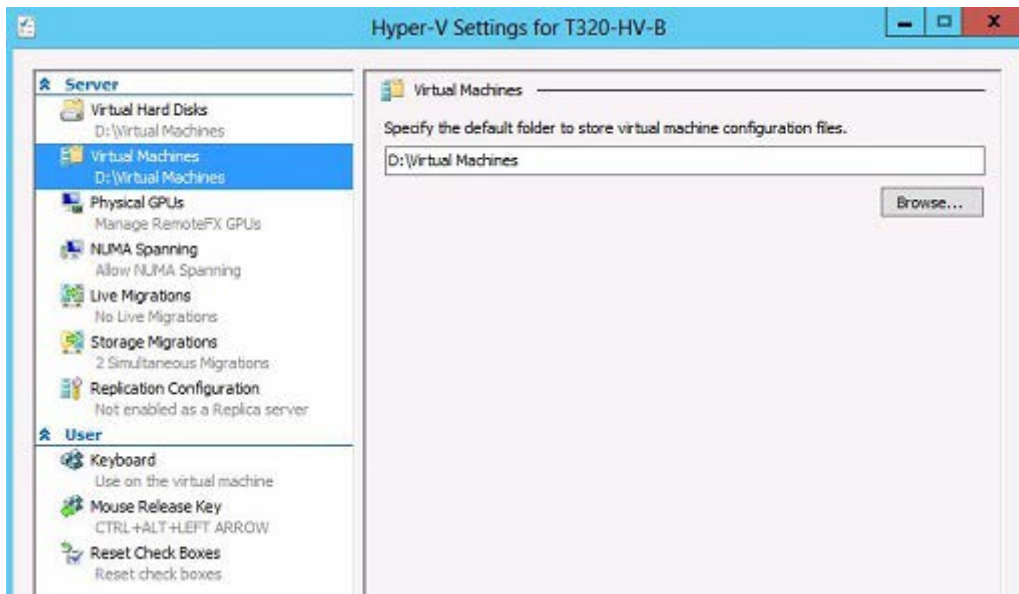
Hyper-V პარამეტრების გვერდზე აირჩიეთ **Virtual Hard Disks** - ვირტუალური მყარი დისკები პუნქტი, ვირტუალური მყარი დისკის ფაილების შენახვისთვის საჭირო ნაგულისხმევი მოწყობილობისა და საქალაქის მისათითებლად. დააჭირეთ **Apply** ღილაკს.



სურ.3.1. 20

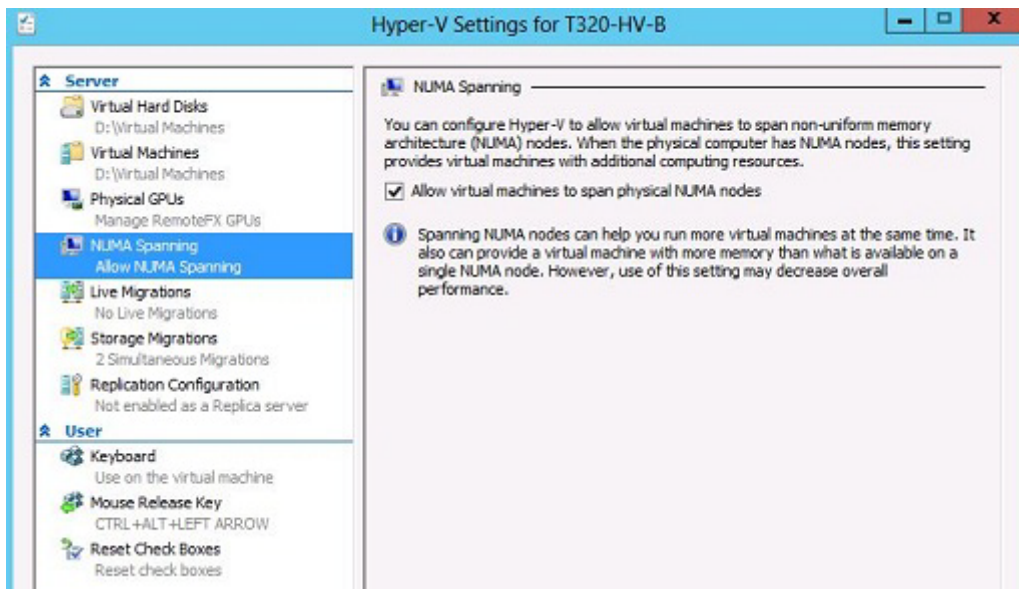
Hyper-V პარამეტრების გვერდზე აირჩიეთ ვირტუალური მანქანები - **Virtual Machines** პუნქტი, ვირტუალური მანქანის კონფიგურაციის ფაილების შესანახი

ნაგულისხმევი საქაღალდის მისათითებლად. მითითების შემდეგ დააჭირეთ **Apply** ღილაკს.



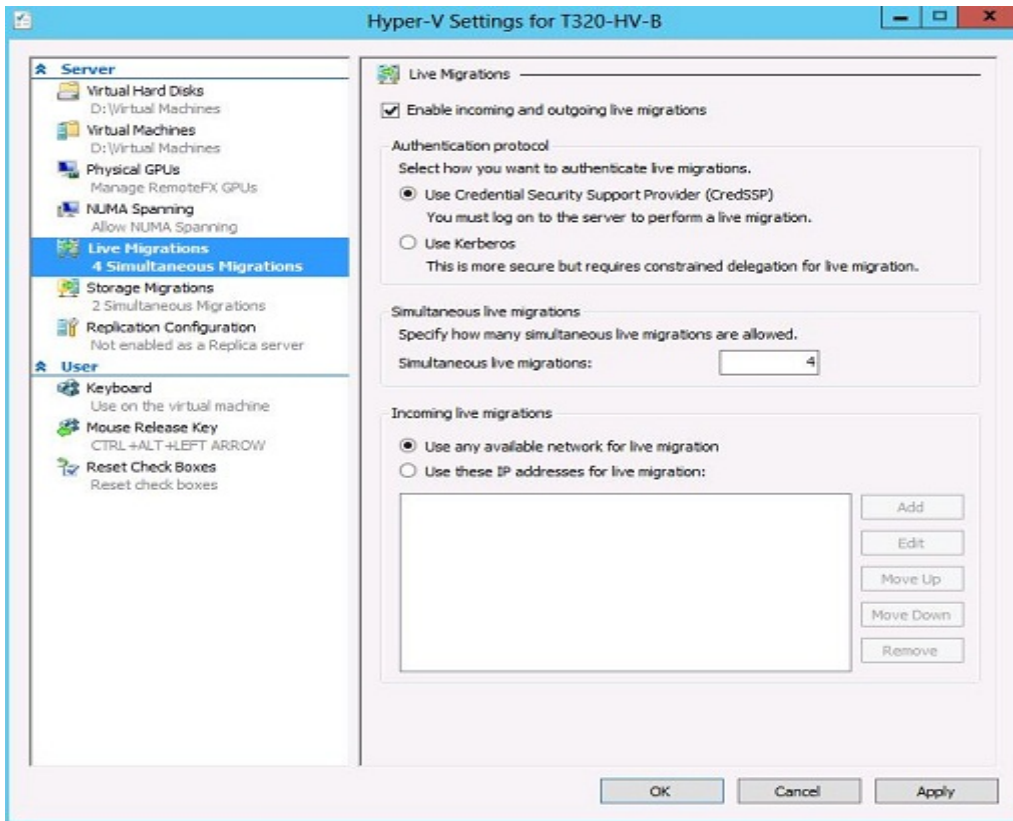
სურ.3.1. 21

Hyper-V პარამეტრების გვერდზე აირჩიეთ **NUMA Spanning** პუნქტი, მისი პარამეტრების ჩასართავად. ჩართვის შემდეგ დააჭირეთ **Apply** ღილაკს.



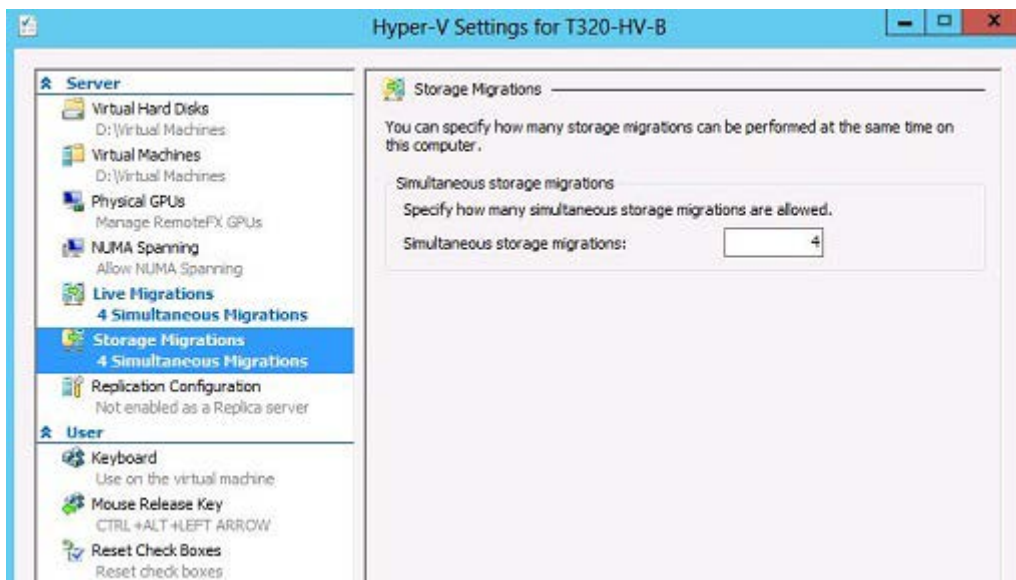
სურ.3.1. 22

Hyper-V Settings გვერდზე, აირჩიეთ **Live Migrations** - ცოცხალი გადაადგილება, ერთდროულად დაშვებული ცოცხალი გადაადგილებების რაოდენობის დასაყენებლად და დააჭირეთ **Apply** ღილაკს. **შენიშვნა:** მოცემული პარამეტრი მოითხოვს რომ სერვერი იყოს აქტიური დირექტორიის დომეინის წევრი.



სურ.3.1. 23

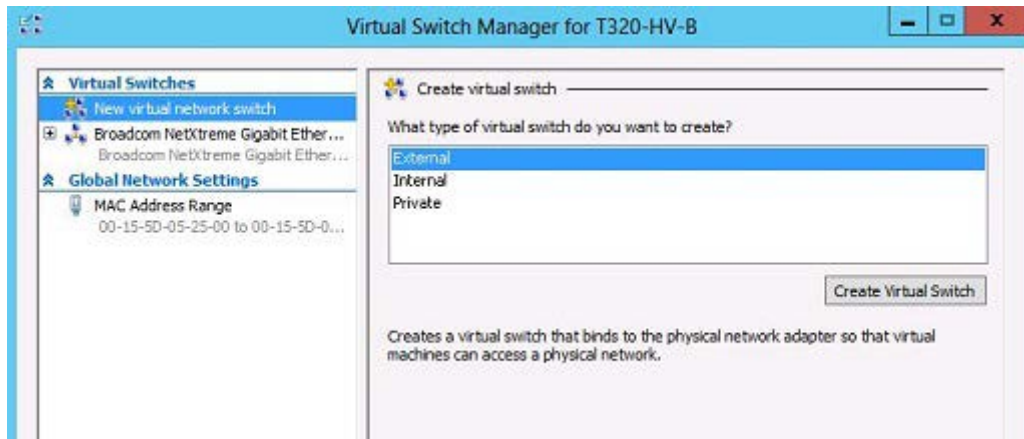
Hyper-V პარამეტრების გვერდზე, აირჩიეთ **Storage Migrations** - საცავის გადაადგილებები, ერთდროულად დაშვებული საცავის გადაადგილებების რაოდენობის დასაყენებლად და დააჭირეთ **Apply** ღილაკს.



სურ.3.1. 24

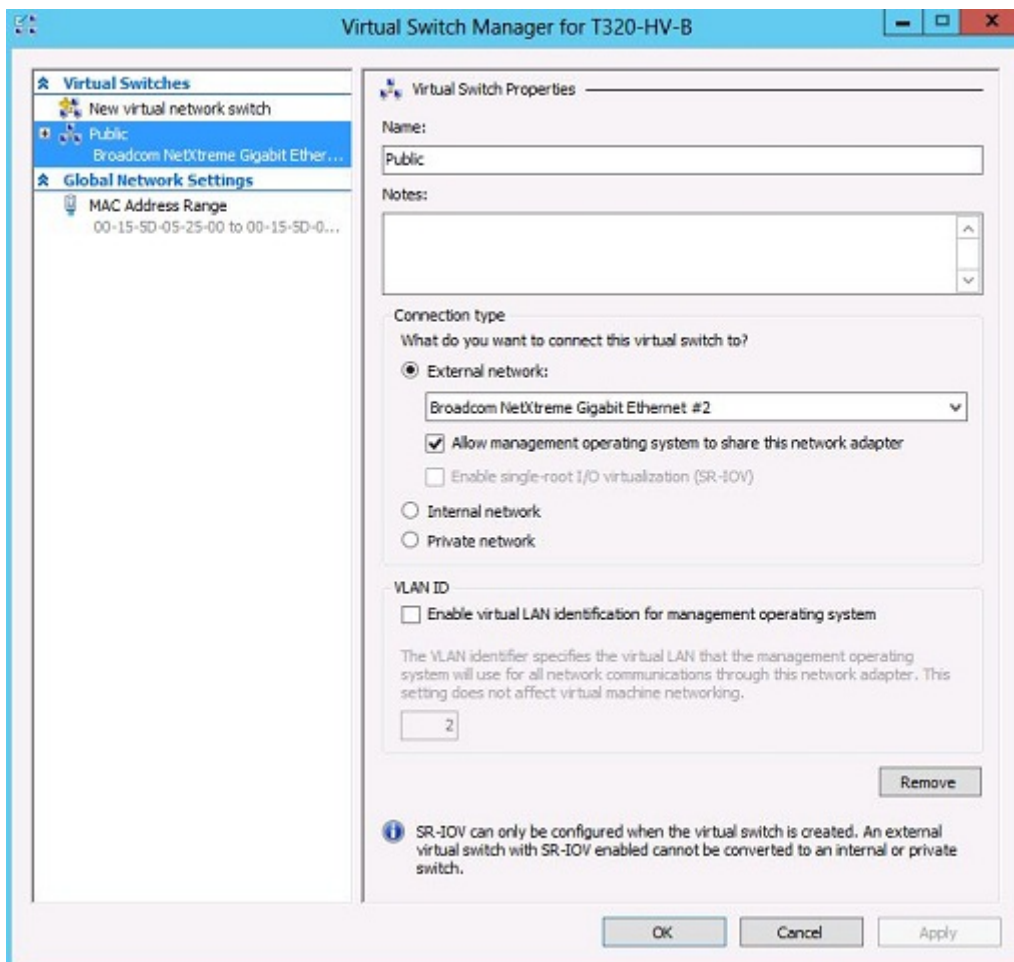
თქვენ შეგიძლიათ გამოიყენოთ **Virtual Switch Manager** - ვირტუალური კომპუტატორის მმართველი, **Hyper-V**-ში ვირტუალური კომპუტატორების შესაქმნელად და სამართავად:

Hyper-V Manager-ის მოქმედებათა პანელში დააჭირეთ **Virtual Switch Manager**-ს.



სურ.3.1. 25

შექმენით ახალი გარე ვირტუალური კომპუტატორი, დაარქვით სახელი - **Public**, და დაუშვით მშობელი დანაყოფი, რომ ჰქონდეს წვდომა ქსელის ადაპტერთან, რომელიც ესაზღვრება ვირტუალურ კომპუტატორს. შემდეგ დააჭირეთ **Apply** ღილაკს.



სურ.3.1. 26

ვირტუალური მანქანების შერჩევა

დღესდღეისობით, ვირტუალიზაციის სამაგიდო პლატფორმების არჩევისას, მომხმარებელს რეალურად აქვს ორი არჩევანი – **VMware Workstation** და **Oracle Virtualbox**. დანარჩენი ანალოგიური სამაგიდო პლატფორმები ან უკვე მოხსნილნი არიან წარმოებიდან ან ფუნქციონალურობით ვეღარ უწევენ კონკურენციას ზემოთ აღნიშნულ პროდუქტებს.

Vmware Workstation-ისა და Oracle Virtualbox-ის საუკეთესო თვისებები:

- ორივეს აქვს მარტივი გრაფიკული ინტერფეისი;
- ქსელური ურთიერთქმედების მოსახერხებელი რედაქტორი საკვანძო კომპიუტერზე;

- კადრების (**Snapshots**) სწრაფად შექმნის ტექნოლოგია;
- დიდი რაოდენობის სტუმარი ოპერაციული სისტემების მხარდაჭერა;
- **64** ბიტიანი ოპერაციული სისტემების მხარდაჭერა;
- **Intel VT** და **AMD-V**-ს მხარდაჭერა;
- **USB 3.0** მოწყობილობა ვირტუალურ მანქანებში;
- ვირტუალური მანქანიდან ხმოვანი სიგნალის გამოტანა ჰოსტ კომპიუტერის მოწყობილობაზე;

- გაცვლის ბუფერი სტუმარ და ჰოსტ კომპიუტერს შორის;
- **3D** – გამოსახულების მხარდაჭერა თამაშებისა და სხვა დანართებისათვის;
- ვირტუალური მოდულების (**Virtual Appliances**) იმპორტის მხარდაჭერა;
- გაუმჯობესებული დრაივერები სტუმარ ოპერაციულ სისტემაში: **Vmware Tools** და **Virtualbox Guest Additions** (ორივე პაკეტის განახლება ხდება ავტომატურად);

- ორივე პლატფორმა მხარს უჭერს **Memory Overcommit** ტექნიკას (ე.წ. **Memory Balloning** – თავისუფალი ფიზიკური მეხსიერების გადანაწილება სტუმარ ოპერაციულ სისტემებს შორის ვირტუალურ მანქანაში);

- ორივე პლატფორმა მხარს უჭერს მრავალპროცესორულ ვირტუალურ მანქანებს (მინიმუმ **8 CPU**);

- ორივე პლატფორმას აქვს ვირტუალური მანქანის კონსოლთან წვდომის მხარდაჭერა **RDP** – სერვერის დახმარებით.

VirtualBox-ის უპირატესობა VMvare Workstation-თან შედარებით:

- **VirtualBox**-ი აბსოლუტურად უფასოა, რაც შეეხება **VMware Workstation**-ს, ღირს **220\$**;

- **VMware Workstation** მუშაობს მხოლოდ **Windows** და **Linux** ოჯახის ჰოსტ ოპერაციულ სისტემებზე, **VirtualBox**-ი კი მხარს უჭერს **Windows, Linux, Mac OS X** და **Solaris** ჰოსტ ოპერაციულ სისტემებს;

- **Teleportation** ტექნოლოგია საშუალებას იძლევა გადავაადგილოთ გაშვებული ვირტუალური მანქანა სხვა ჰოსტ **VirtualBox**-ზე, მისი გათიშვის აუცილებლობის გარეშე. მოცემული ფუნქცია არ არის **VMware Workstation**-ში;

- **VirtualBox**-ს აქვს არა მარტო **.VDI** ფორმატთან მუშაობის შესაძლებლობა, არამედ **.VMDK** და **.VHD** ფორმატებთანაც. **VMware Workstation**-ს აქვს შესაძლებლობა გაუშვას ვირტუალური მანქანები მხოლოდ **VMDK** ვირტუალური დისკის იმიჯიდან (თუმცა მას აქვს უფასო პროდუქტი **VMware Converter**, რომელიც გამოიყენება ვირტუალური მანქანების იმპორტისათვის სხვა ფორმატებიდან);

- **VirtualBox**-ს აქვს შესაძლებლობა შეზღუდოს **CPU**-ს და შეტანა-გამოტანის რესურსების მოხმარება, **VMware Workstation**-ში ეს არ გვაქვს (ეს ფუნქცია აქვს მხოლოდ **VMware VpShare**);

- **VirtualBox**-ს აქვს ვიდეო მეხსიერების რეგულირების შესაძლებლობა.

VMware Workstation-ის უპირატესობა VirtualBox-თან შედარებით:

- **VMware Workstation**-ს აქვს **3D**-გამოსახულების მხარდაჭერის მეტი შესაძლებლობა, როგორცაა: **Windows Aero user interface, OpenGL 2.1** და **Shader Model 3.0**. თვითონ **3D**-აქსელერაცია მუშაობს უფრო სტაბილურად, ვიდრე **VirtualBox**-ში;

- **VMware Workstation**-ს აქვს უნივერსალური ბეჭდვის დრაივერი **ThinPrint** (რომელსაც არ სჭირდება დრაივერების დაყენება სტუმარ ოპერაციულ სისტემაში);

- კადრების (**Snapshots**) შექმნა დროის მითითებული ინტერვალის შემდეგ (**AutoProtect**), რაც უზრუნველყოფს ვირტუალური მანქანების დაცვას ავტოშენახვის შესაძლებლობის ანალოგიურად (მაგალითად, როგორც **Ms Word**-ში);

- **VMware Workstation**-ს აქვს მეტი ფუნქციები ვირტუალური ქსელური ურთიერთქმედების უტილიტებთან - კომუტატორი, **DHCP, NAT** და სხვა (თუმცა **VirtualBox** ასევე აქვს **NAT, Bridge Networking** - **VMware Workstation**-ში ეს უფრო ადვილია);

- **VMware Workstation**-ს აქვს კლონებთან დაკავშირებული ფუნქცია (**Linked Clones**), ვირტუალური მანქანისთვის;

- ვირტუალური მანქანების აქტიურობის ჩაწერა ვიდეოფორმატში, ასევე მომხმარებლის მოქმედების მიმდევრობის რეჟიმში (**Guest Record/Replay**);

- **Workstation**-ს აქვს განვითარების და ტესტირების სფეროში ინტეგრაციის შესაძლებლობები (მაგალითად, **Eclipse**), ასევე სპეციალური ფუნქცია დეველოპერებისათვის (სამაგიეროდ **VirtualBox** აქვს **API**);

- ვირტუალური მანქანების დაცვა **256** ბიტის შიფრაციით;

- **VMware Workstation**-ს აქვს რამდენიმე სასარგებლო წვრილმანი –მაგალითად: ვირტუალური მანქანის დაპაუზება და ბევრი სხვა.

- ჩაშენებული **Phoenix Bios 4.0 Release 6 with Vesa Bios**;

ზოგადად, თუ არ ვიცით კონკრეტულად რაში გვჭირდება კერძოდ **VMware Workstation**-ი, მაშინ ავირჩიოთ უფასო **VirtualBox**-ი. თუ ვართ დეველოპერები ან ტესტირების ინჟინრები, მაშინ რეკომენდებულია **VMware Workstation**-ის გამოყენება, რომელსაც აქვს უამრავი საჭირო წვრილმანი, რასაც ყოველდღიურად ვიყენებთ, და რომელიც არ გვაქვს **VirtualBox**-ში. აღსანიშნავია ის ფაქტი, რომ **VMware Workstation**-ს ასევე გააჩნია უსაფრთხოების დაცვის უამრავი საშუალება (კადრების შექმნის ტექნოლოგია - **Snapshot**, ვირტუალური მანქანის ასლის შექმნის ფუნქცია - **Clone**, ვირტუალური მანქანის კონფიგურაციის შეცვლისაგან თავდაცვის მექანიზმები - პაროლით დაცვა ან შიფრაცია.

როგორც ჩანს უპირატესობა **VMware Workstation** პროგრამული უზრუნველყოფის მხარეზეა. მას ინტეგრირებული აქვს ისეთი ფუნქციები (სისტემის გაფართოებული შესაძლებლობები, უსაფრთხოების დაცვის მექანიზმები), რომლებიც აუცილებელად



დაგვირდება ოპერაციული სისტემების შესწავლისას. ამ ეტაპზე გამოსულია **VMware Workstation 10.0** ვერსია და სწორედ მას განვიხილავთ მოცემულ თემაში.

3.2. VMware Workstation-ის ინსტალაცია

➤ პირველ რიგში გადმოწერეთ საინსტალაციო პაკეტი მითითებული მისამართიდან: <http://youshare.ge/?d=522F1C7E5>, გადმოწერის შემდეგ ამოაარქივეთ და გაუშვით ინსტალატორი;

➤ მიყევით დაყენების ინსტრუქციას და დააწექით **Next** ღილაკს;

➤ შემდეგ აირჩიეთ **Custom** მენიუ. მიუთითეთ ადგილი, სადაც უნდა დაინსტალირდეს პროგრამა ან დატოვეთ უცვლელად. შეგვიძლია ჩავრთოთ დამატებითი პარამეტრები, რომლებსაც შემდგომში განვიხილავთ დაწვრილებით. ვაჭერთ **Next** ღილაკს;

➤ **HTTPS** პორტი დატოვეთ უცვლელად და **Next**;

➤ **Check for product updates on startup** - ის მონიშვნის შემთხვევაში პროგრამას ექნება ავტომატური განახლების მხარდაჭერა. როდესაც გაუშვებთ **VMware Workstation**-ს, ის ავტომატურად შეამოწმებს ოფიციალურ საიტზე ახალი ვერსიის არსებობას, თუ ასეთი იქნება სისტემა შეგვეკითხება გვსურს თუ არა განახლების გადმოწერა. სურვილის შემთხვევაში შეგიძლიათ გადმოწეროთ და დააინსტალიროთ. ჩართეთ ან გამორთეთ განახლების მხარდაჭერა და **Next**;

➤ მომდევნო ფანჯარაში სისტემა გვთავაზობს გაეგზავნოს თუ არა კონფიდენციალური სისტემური მონაცემები და გამოყენების სტატისტიკა კომპანია **VMware**-ს. თანხმობის შემთხვევაში დავტოვოთ უცვლელად, წინააღმდეგ შემთხვევაში ამორთეთ მონიშვნა და **Next**;

➤ შემდეგ ეტაპზე ვირჩევთ თუ სად გვინდა რომ შეიქმნას **VMware workstation**-ის გამშვები იარლიყი :

• **Desktop** - სამუშაო მაგიდაზე;

• **Start Menu Programs folder**- სასტარტო მენიუში;

მონიშნეთ სასურველი ადგილმდებარეობა და **Next**;

➤ ინსტალაციის დასაწყებად დააჭირეთ **Continue** ღილაკს. დაყენების პროცესი გაგრძელდება დაახლოებით **3-4** წუთი;

➤ ინსტალაციის შემდეგ გახსენით სამუშაო მაგიდაზე მიღებული გამშვები, დაეთანხმეთ სალიცენზიო შეთანხმებას, რის შემდეგაც შეიყვანეთ სერიული ნომერი, რომელსაც მოძებნით საინსტალაციო პაკეტში;

➤ ბოლოს დააწეეთ **finish** ღილაკზე, რაც იმის მანიშნებელია, რომ ინსტალაცია დასრულდა. მისი კორექტული მუშაობისათვის აუცილებელია გადავტვირთოთ კომპიუტერი. მომავალში ჩვენ გამოვიყენებთ ისეთ ტერმინებს როგორცაა ფიზიკური კომპიუტერი ანუ რეალური მანქანა და ვირტუალური კომპიუტერი, რომელსაც პროგრამის საშუალებით „ავაწყობთ“ ამ რეალურ მანქანაზე.

3.3. ვირტუალური მანქანის შექმნა

შევქმნათ ვირტუალური მანქანა და გავერკვეთ მის პარამეტრებში.

მენიუში **file** ავირჩიოთ **New virtual machine** ან სამუშაო არეში დავაწვეთ **Create a New Virtual Machine** სახელწოდების ღილაკს (სურ. 1.1):



სურ.3.3. 1

გაეშვება დაყენების ოსტატი რომლის დახმარებითაც ჩვენ შეგვიძლია შევქმნათ ახალი ვირტუალური მანქანა. ავირჩიოთ პუნქტი **custom**. განსხვავება **typical**-სა და **custom** პუნქტებს შორის არის მხოლოდ ის რომ **custom**-ის დახმარებით შეგვიძლია მოვმართოთ და ავირჩიოთ დაწვრილებითი პარამეტრები, ხოლო **typical** გვაძლევს ვირტუალური

მანქანის რეკომენდებულ პარამეტრებს, რომელიც სისტემაში ავტომატურადაა ჩადებული. ვაწვებით **Next** ღილაკს.

გამოსულ ფანჯარაში მოცემულია პროგრამის ახალ და წინა ვერსიებს შორის არსებული სხვაობები: ნაჩვენებია თუ რა მაქსიმალური სისტემური რესურსების ათვისების საშუალება და რომელი მოწყობილობის მხარდაჭერის შესაძლებლობა გააჩნია თითოეულ მათგანს.

საინტერესოა მხარდაჭერისა და თავსებადობის შედარებითი დახასიათება, რაც მოცემულია ცხრილ 1-ში.

Hardware compatibility	Compatible products	Limitations	Compatible with ESX server
Workstation 10.0	<ul style="list-style-type: none"> • Fusion 6.0 • Workstation 10.0 	<ul style="list-style-type: none"> • 64 GB memory limit • 16 processor limit • 10 network adapter limit • 8 TB disk size limit 	ESX server on
Workstation 9.0	<ul style="list-style-type: none"> • ESXi 5.1 • Fusion 5.0 • Fusion 6.0 • Workstation 9.0 • Workstation 10.0 	<ul style="list-style-type: none"> • 64 GB memory limit • 8 processor limit • 10 network adapter limit • 2 TB disk size limit • No SATA devices 	ESX server on
Workstation 8.0	<ul style="list-style-type: none"> • ESXi 5.0 • ESXi 5.1 • Fusion 4.0 • Fusion 5.0 • Fusion 6.0 • Workstation 8.0 	<ul style="list-style-type: none"> • 64 GB memory limit • 8 processor limit • 10 network adapter limit • 2 TB disk size limit • No SATA devices 	ESX server on

	<ul style="list-style-type: none"> • Workstation 9.0 • Workstation 10.0 		
<p>Workstation 6.5 – 7.x</p>	<ul style="list-style-type: none"> • ACE 2.5 - 2.7 • ESXi 4.x • ESXi 5.0, 5.1 • Fusion 2.x • Fusion 3.x • Fusion 4.0 • Fusion 5.0 • Fusion 6.0 • Server 2.x • Workstation 6.5 • Workstation 7.x • Workstation 8.0 • Workstation 9.0 • Workstation 10.0 	<ul style="list-style-type: none"> • 32 GB memory limit • 8 processor limit • 10 network adapter limit • 2 TB disk size limit • No SATA devices • No HD Audio 	<p>ESX server on</p>

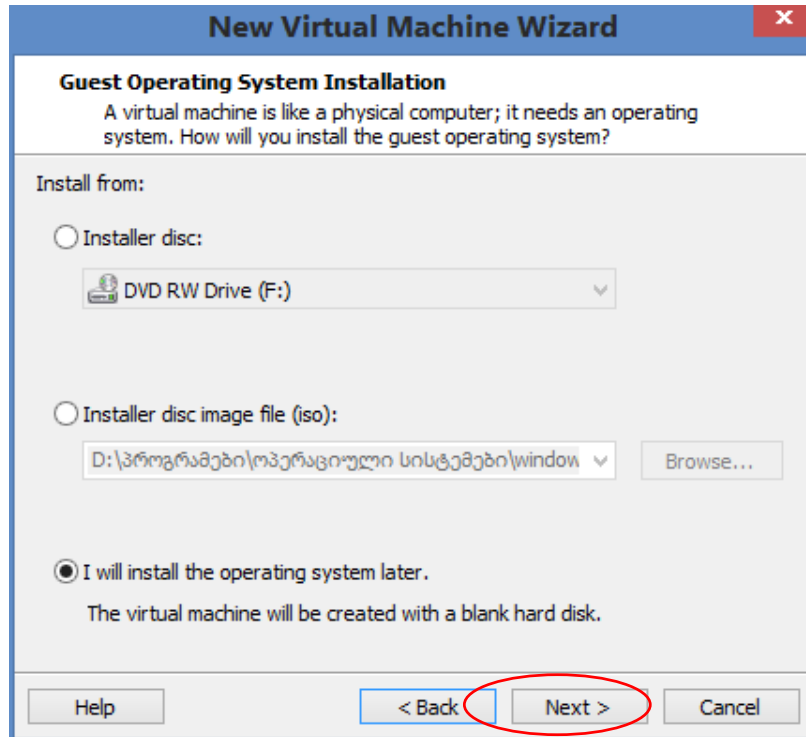
<p style="text-align: center;">Workstation 6.0</p>	<ul style="list-style-type: none"> • ACE 2.0 • ACE 2.5 - 2.7 • ESXi 4.x • ESXi 5.0 • ESXi 5.1 • Fusion 1.1 • Fusion 2.x • Fusion 3.x • Fusion 4.0, 5.0 • Fusion 6.0 • Server 2.x • Workstation 6.0 • Workstation 6.5 • Workstation 7.x • Workstation 8.0 • Workstation 9.0 • Workstation 10.0 	<ul style="list-style-type: none"> • 8 GB memory limit • 2 processor limit • 10 network adapter limit • 950 GB disk size limit • No SATA devices • No HD Audio • No CPU hot plug • No device hot plug • No memory hot plug • No LSI logic SAS SCSI controller • No printer support 	<p style="text-align: center;">ESX server on</p>
----------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------

Workstation 5.x	<ul style="list-style-type: none"> • ACE 2.0 • ACE 2.5 – 2.7 • ESXi 4.x • ESXi 5.0, 5.1 • Fusion 1.1 • Fusion 2.x • Fusion 3.x • Fusion 4.0, 5.0 • Fusion 6.0 • Server 1.x • Server 2.x • Workstation 	<ul style="list-style-type: none"> • 3.5 GB memory limit • 2 processor limit • 4 network adapter limit • 950 GB disk size limit • No SATA devices • No HD Audio • No USB 2.0 • No multiple monitor display 	ESX Server must on
	5.x	<ul style="list-style-type: none"> • No battery status • No CPU hot plug • No device hot plug • No memory hot plug • No LSI Logic SAS 	
	6.0	<ul style="list-style-type: none"> • No VMCI support • No printer support 	
	6.5	<ul style="list-style-type: none"> • No VMCI support • No printer support 	
	7.x	<ul style="list-style-type: none"> • No VMCI support • No printer support 	
	8.0	<ul style="list-style-type: none"> • No VMCI support • No printer support 	
	9.0	<ul style="list-style-type: none"> • No VMCI support • No printer support 	
	10.0	<ul style="list-style-type: none"> • No VMCI support • No printer support 	
		<ul style="list-style-type: none"> • No VMCI support • No printer support 	
		<ul style="list-style-type: none"> • No VMCI support • No printer support 	
		<ul style="list-style-type: none"> • No VMCI support • No printer support 	
		<ul style="list-style-type: none"> • No VMCI support • No printer support 	

ცხრ.1 *Vmware Workstation-ის ვერსიების შედარების ცხრილი*

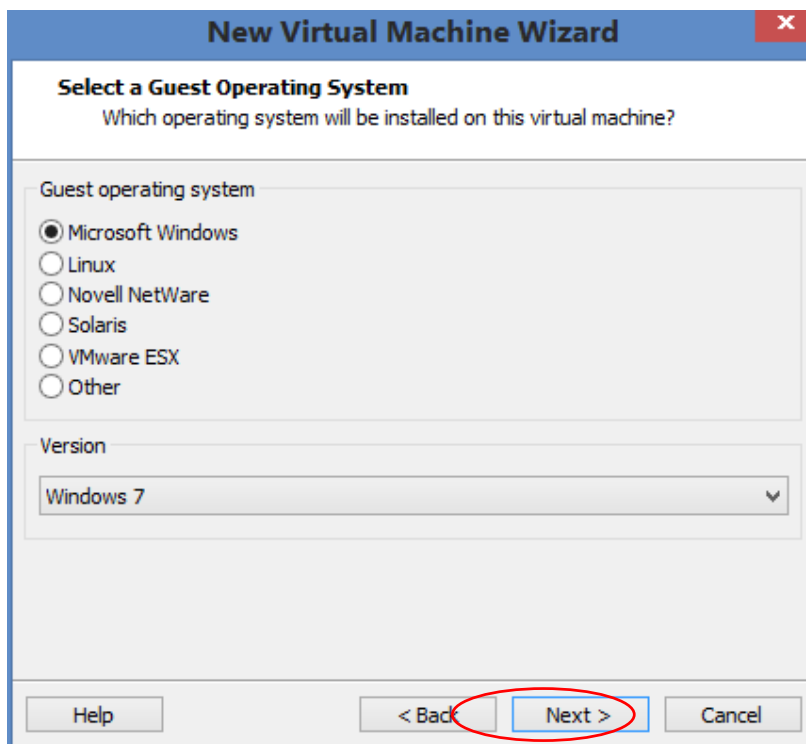
ღეგაპი - აირჩიეთ ადგილი საიდანაც უნდა მოხდეს ოპერაციული სისტემის ინსტალაცია. გაითვალისწინეთ, რომ თუ შექმნის მომენტშივე მიუთითებთ საინსტალაციო პაკეტს, ამ შემთხვევაში ოპერაციული სისტემის დაყენების დროს კოდი

და სალიცენზიო შეთანხმებები მოთხოვნილი იქნება ვირტუალური მანქანის ჩართვისთანავე, ასევე ვერ შეძლებთ დისკის დაყოფას და დაფორმატებას.



სურ.3.3. 2

II ეტაპი - მიუთითეთ ოპერაციული სისტემა, რომლის დაყენებასაც აპირებთ:



სურ.3.3. 3

ოპერაციული სისტემების სია საკმაოდ მრავალრიცხოვანია. ქვემოთ ჩამოთვლილია ის ოპერაციული სისტემები რომელთა დაყენებაც შეგვიძლია **Vmware workstation**-ის 10.0 ვერსიით.

	ვერსია		ვერსია
Microsoft Windows	<ul style="list-style-type: none"> • Windows 7/8 • Windows 7/8 x64 • Windows Vista • Windows Vista x64 Edition • Windows XP Home Edition • Windows XP Professional • Windows XP Professional 	LINUX	<ul style="list-style-type: none"> • Asianux Server 3/4 • Asianux Server 3/4 64-bit • CentOS • CentOS 64 –bit • Debian 5/6/7 • Debian 5/6/7 64 –bit • Fedora • Fedora 64 –bit • Mandrake Linux • Mandriva Linux • Mandriva Linux 64 –bit • Novell Linux Desktop 9 • OpenSUSE • OpenSUSE 64 –bit • Oracle Enterprise Linux • Oracle Enterprise Linux 64 –
	X64		bit
	<ul style="list-style-type: none"> • Windows 2000 Professional • Windows NT • Windows Server 2012 • Hyper-V (Unsupported) • Windows Server 2008 R2 X64 • Windows Server 2008 • Windows Server 2008 X64 • Windows Server 2003 		<ul style="list-style-type: none"> • Red Hat Enterprise Linux • Red Hat Enterprise Linux 4/5/6 • Red Hat Enterprise Linux 4/5/6 64 –bit • Red Hat Enterprise Linux 3 • Red Hat Enterprise Linux 3 • Red Hat Enterprise Linux 2
	Standart		4/5/6
	<ul style="list-style-type: none"> • Windows Server 2003 		64 –bit
	Standart x64		
	<ul style="list-style-type: none"> • Windows Server 2003 		
	Enterprise		
	<ul style="list-style-type: none"> • Windows Server 2003 		
	Enterprise x64		
	<ul style="list-style-type: none"> • Windows Server 2003 		
	Business		

	<ul style="list-style-type: none"> • Windows Server 2003 Web Edition • Windows 2000 Server • Windows 2000 Advanced Server • Windows Me • Windows 3.1/95/98 		<ul style="list-style-type: none"> • Sun Java Desktop System • SUSE Linux Enterprise 11 • SUSE Linux Enterprise 11 64-bit • SUSE Linux Enterprise 10 • SUSE Linux Enterprise 10 64-bit • SUSE Linux Enterprise 7/8/9 • SUSE Linux Enterprise 11 64-bit • SUSE Linux Enterprise 7/8/9 64-bit • SUSE Linux • SUSE Linux 64-bit • Turbolinux • Turbolinux 64-bit • Ubuntu • Ubuntu 64-bit • Other Linux 3.x kernel • Other Linux 3.x kernel 64-bit • Other Linux 2.6.x kernel • Other Linux 2.6.x kernel 64-bit • Other Linux 2.4.x kernel • Other Linux 2.4.x kernel 64-bit • Other Linux 2.2.x kernel
Novell NetWar	<ul style="list-style-type: none"> • NetWare 6 • NetWare 5 		
Sun Solaris	<ul style="list-style-type: none"> • Solaris 11 64-bit • Solaris 10 • Solaris 10 64-bit • Solaris 9 (Unsupported) • Solaris 8 (Unsupported) 		
VMware ESX	<ul style="list-style-type: none"> • VMware ESXI 5 • VMware ESX/ESXI 4 		

Other	<ul style="list-style-type: none"> • eComStation 2 • eComStation • FreeBSD • FreeBSD 64 –bit • MS-DOS • Other • Other 64 - bit 		
-------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--	--

ცხრ. 2

თუ ვერ იპოვეთ სასურველი ოპერაციული სისტემა ჩამონათვალში გული არ გაიტეხოთ! სავარაუდოთ ის გაეშვება პუნქტ **other**-ის ბოლო ორი პუნქტიდან ერთ-ერთის არჩევით, ან ყურადღებით გაეცანით ინსტრუქციას ოპერაციული სისტემის შესახებ განყოფილებაში სისტემური მოთხოვნები.

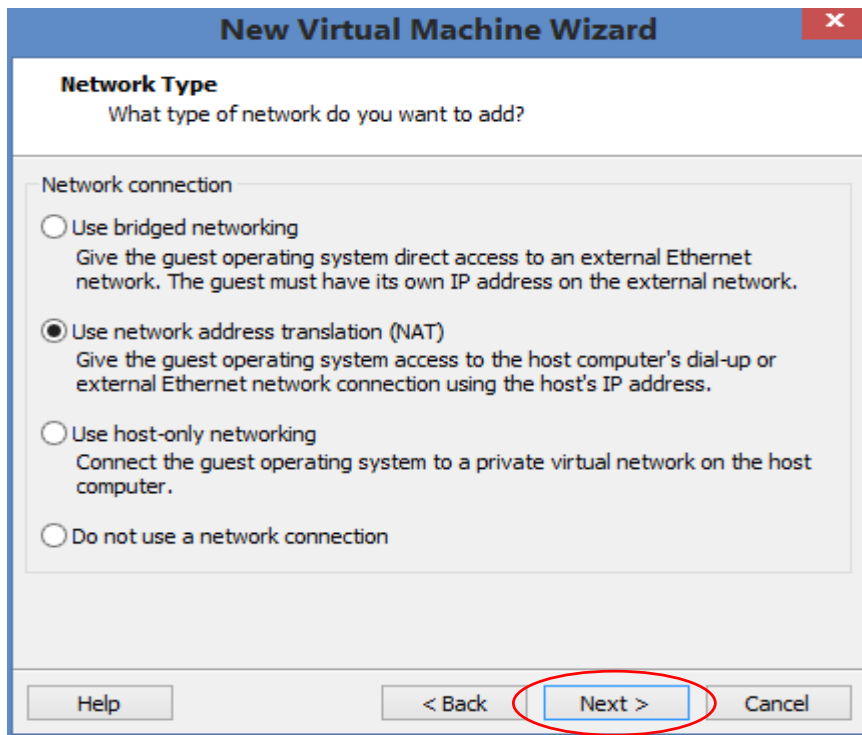
ჩამონათვალიდან აირჩიეთ ის ოპერაციული სისტემა, რომლის დაყენებასაც აპირებთ სასურველი კონფიგურაციის ვირტუალური მანქანის აწყობის შემდეგ და დააჭირეთ **Next** ღილაკს.

III ეტაპი - ვარქმევთ სახელს ჩვენს მომავალ ვირტუალურ კომპიუტერს. ასევე მიუთითეთ ვირტუალური მანქანის განთავსების ადგილი ან დატოვეთ უცვლელად. დააჭირეთ **Next** ღილაკს;

IV ეტაპზე - ვუთითებთ პროცესორების და ბირთვების რაოდენობას. **Next;**

V ეტაპი - მიუთითეთ ოპერაციული მეხსიერების მაქსიმალური ზომა ვირტუალური მანქანისათვის. **Next;**

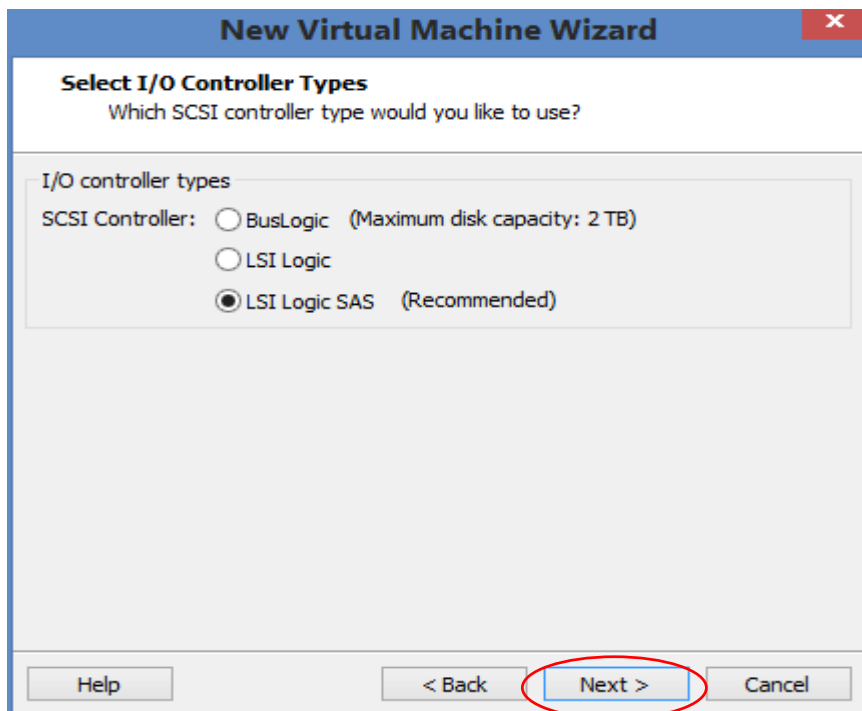
VI ეტაპი - ქსელის ადაპტერის პარამეტრებში (სურ. 1.4) ჯერ მოვნიშნოთ ბრძანება **Use network address translation (NAT)**, ხოლო შემდგომში აგიხსნით თუ როგორ მოვმართოთ ვირტუალური ქსელი და ადაპტერის მახასიათებლები.



სურ.3.3. 4

VII ეტაპი - შეტანა/გამოტანის კონტოლერის ტიპი - ვირტუალური მანქანისთვის SCSI კონტროლერის არჩევა.

SCSI კონტროლერისათვის შესაძლებელია ავირჩიოთ ერთერთი შემდეგი კონფიგურაციიდან (სურ. 1.5):



სურ.3.3. 5

Bus Logic და **LSI Logic** ადაპტერებს აქვთ პარალელური ინტერფეისი, ხოლო **LSI Logic SAS** ადაპტერს მიმდევრობითი ინტერფეისი.

ადაპტერი **LSI Logic** აქვს მაღალი წარმადობა და უკეთესად მუშაობს **SCSI** მოწყობილობებთან ერთად. ადაპტერი **LSI Logic**-ს აქვს **Esx Server 2.0** და უფრო ძველი ვერსიების მხარდაჭერა.

PVSCSI ადაპტერები - მაღალიწარმადობის სისტემაა, რომელიც უზრუნველყოფს მეტ გამტარუნარიანობას პროცესორის ნაკლები დატვირთვით.

შენიშვნა:

SCSI კონტროლერის არჩევა გავლენას არ ახდენს ვირტუალურ დისკზე, რომელიც შეიძლება იყოს როგორც **IDE** ასევე **SCSI** დისკი. ზოგიერთი სტუმარი ოპერაციული სისტემა როგორცაა **windows XP** , არ შეიცავს **LSI Logic** და **LSI Logic SCSI** ადაპტერების დრაივერებს ამიტომ თქვენ თვითონ უნდა ჩატვირთოთ დრაივერები **LSI Logic** -ის საიტიდან. ამჯერად დავტოვოთ შემოთავაზებული **LSI Logic SAS**.

VIII ეტაპი - მოცემულ ეტაპზე უნდა შევქმნათ ვირტუალური მყარი დისკი (სურ.1.6). ვირტუალური მყარი დისკი წარმოადგენს ფაილს ან ფაილების ნაკრებს სადაც ინახება გარკვეული ინფორმაცია.

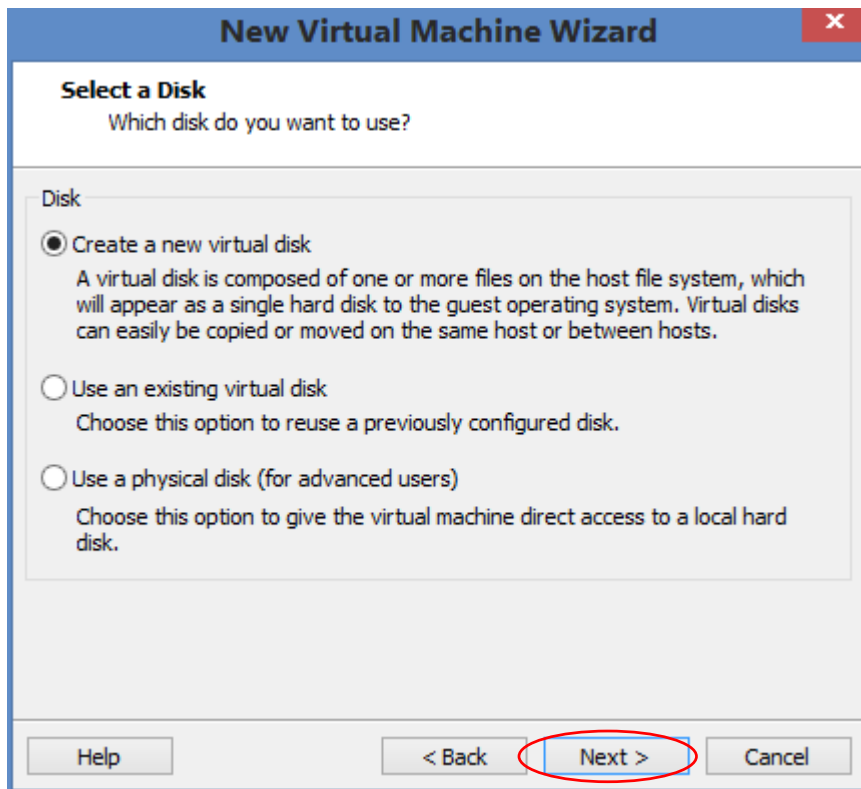
მოცემული გვაქვს სამი ვარიანტი:

Create a new virtual disk – ახალი ვირტუალური დისკის შექმნა;

Use existing virtual disk – არსებული ვირტუალური დისკის გამოყენება;

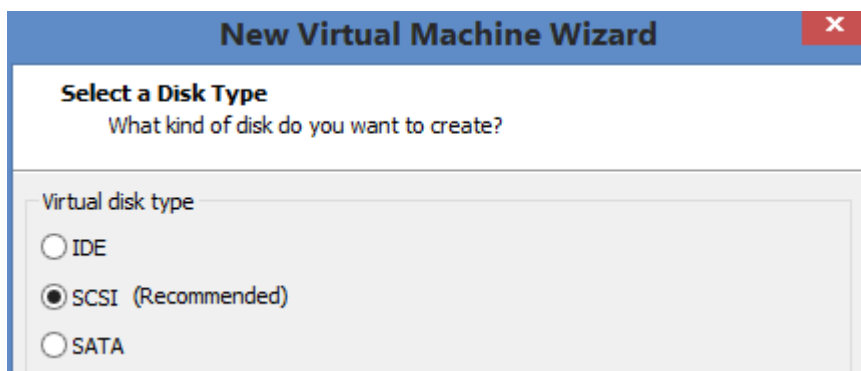
Use a physical disk (for advanced users) - ფიზიკური მყარი დისკის გამოყენება (გამოცდილი მომხმარებლისთვის);

Vmware workstation- ში შესაძლებელია მუშაობა ფიზიკურ მყარ დისკზე „guest”(სტუმარი) ოპერაციულ სისტემაში. ვირჩევთ პუნქტს **Create a new virtual disk** და ვაწვებით **Next**.



სურ.3.3. 6

IX ეტაპი - შექმნის ოსტატი მოგვთხოვს ინტერფეისი არჩევას - **IDE, SCSI** თუ **SATA**, ჩვენი ვირტუალური მყარი დისკისათვის (სურ.3.3.6). რადგანაც **IDE** უფრო ძველი ინტერფეისია **HDD**-სი რეკომენდებულია ავირჩიოთ **SCSI** ინტერფეისი. გაითვალისწინეთ, რომ ზოგიერთ ძველ ოპერაციულ სისტემას არა აქვს **SCSI** და **SATA** დრაივერების მხარდაჭერა, ამიტომ მათთვის რეკომენდებულია **IDE**.



სურ.3.3. 7

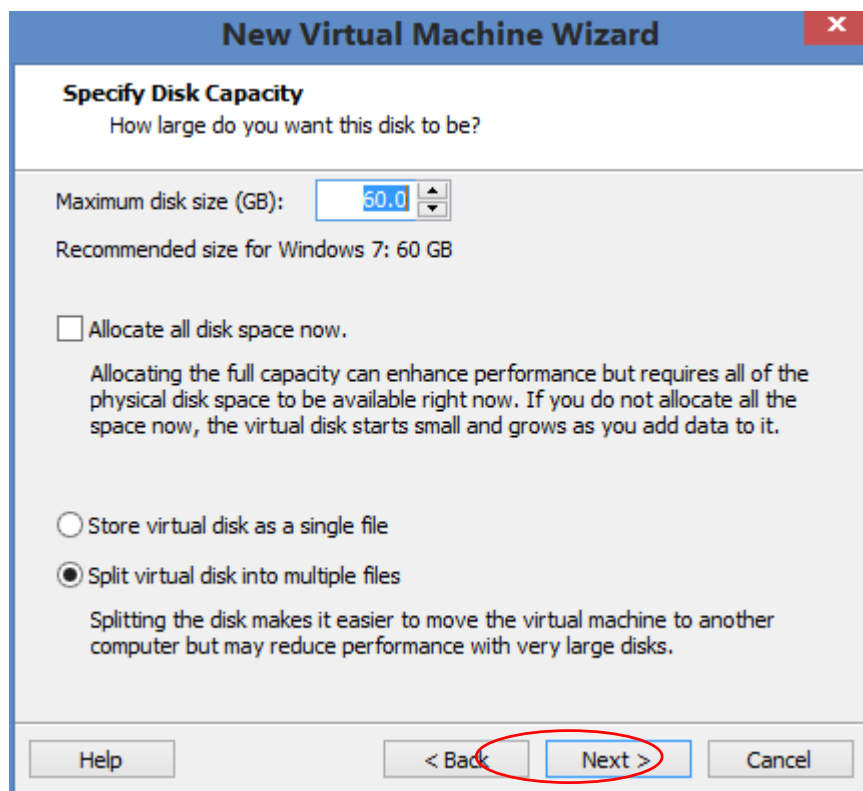
X ეტაპი - გამოვეყთ ჩვენი მომავალი მყარი დისკის ზომა, სტრიქონში **Maximum disk size(GB)** საჭიროა შევიყვანოთ ზომა გიგაბაიტებში. ავტომატურად **windows 7**-სთვის შემოთავაზებულია **60 GB** (სურ. 3.3..7).

Allocate all disk space now - გავანაწილოთ დისკის სივრცე. ეს პუნქტი დაკავშირებულია იმასთან რომ ახალი მყარი დისკის შექმნისას (ვირტუალური დისკის ფაილი) მისი რეალური ზომა სივრცის გამოყოფის გარეშე დაიკავებს **1MG 8GB**-ზე „**Maximum disk size NTFS**“-ზე, რათა არ დაკავდეს დისკის თავისუფალი სივრცე საჭიროების გარეშე. და ვირტუალური მყარი დისკის ინფორმაციით შევსებისას ის როგორც რეზინა გაიჭიმება და დაიკავებს სივრცეს ფიზიკურ **HDD**-ზე **Maximum disk size**-მდე.

აქვე მოცემულია ვირტუალური მყარი დისკის შენახვის ორი ვარიანტი:

Store virtual disk as a single file - შეინახოს ვირტუალური დისკი როგორც ერთიანი ფაილი;

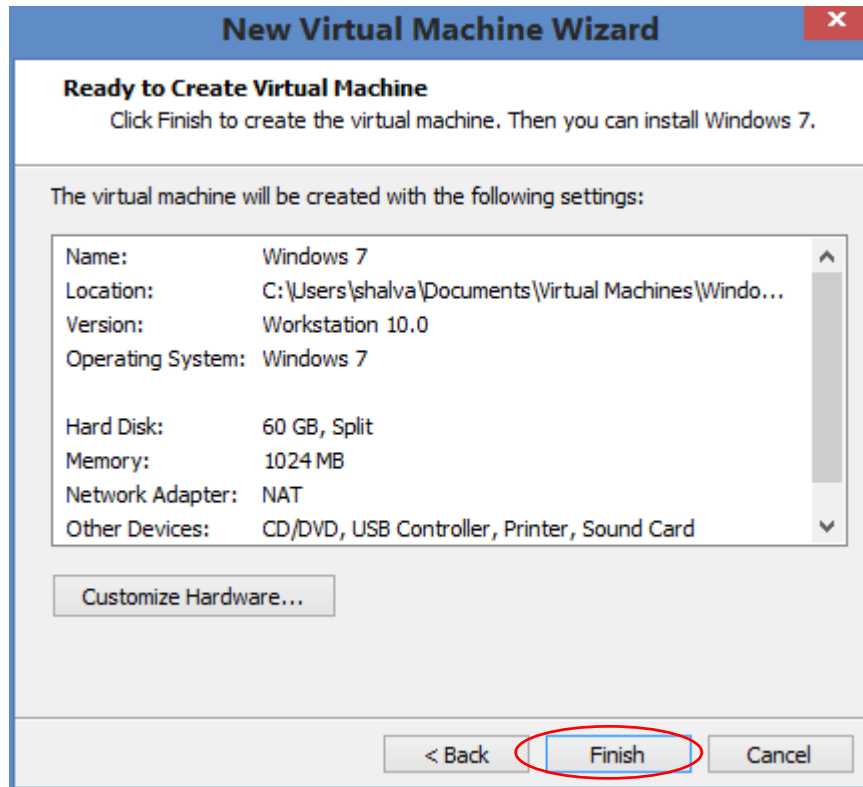
Split virtual disk into multiple files - დაიყოს ვირტუალური მყარი დისკი ნაწილებად, ეს აქტუალურია იმ შემთხვევაში, როცა ფაილურ სისტემას აქვს შეზღუდვა ფაილის ზომაში ან როცა გვინდა ვირტუალური მანქანის სხვა კომპიუტერზე გადატანა.



სურ.3.3. 8

XI ეტაპი - ვირტუალური დისკი ინახება სტანდარტულ საქალაქდემო ვირტუალური მანქანის დანარჩენ სისტემურ ფაილებთან ერთად, თუმცა შესაძლებელია მივუთითოთ სხვა ადგილი. დავაჭიროთ **Next** ღილაკს;

XII ეტაპი - ბოლო ეტაპზე გამოდის ანგარიში და ჩვენ ვამოწმებთ სწორად გავაკეთეთ თუ არა ყველაფერი, ასევე სწორად მივუთითეთ თუ არა სტუმარი ოპერაციული სისტემის განთავსების ადგილი. თუ გამოგვჩა რაიმე დავაჭიროთ მოცემულ ფორმაში ღილაკზე **Customize Hardware** (სურ. 3.3.9):



სურ.3.3. 9

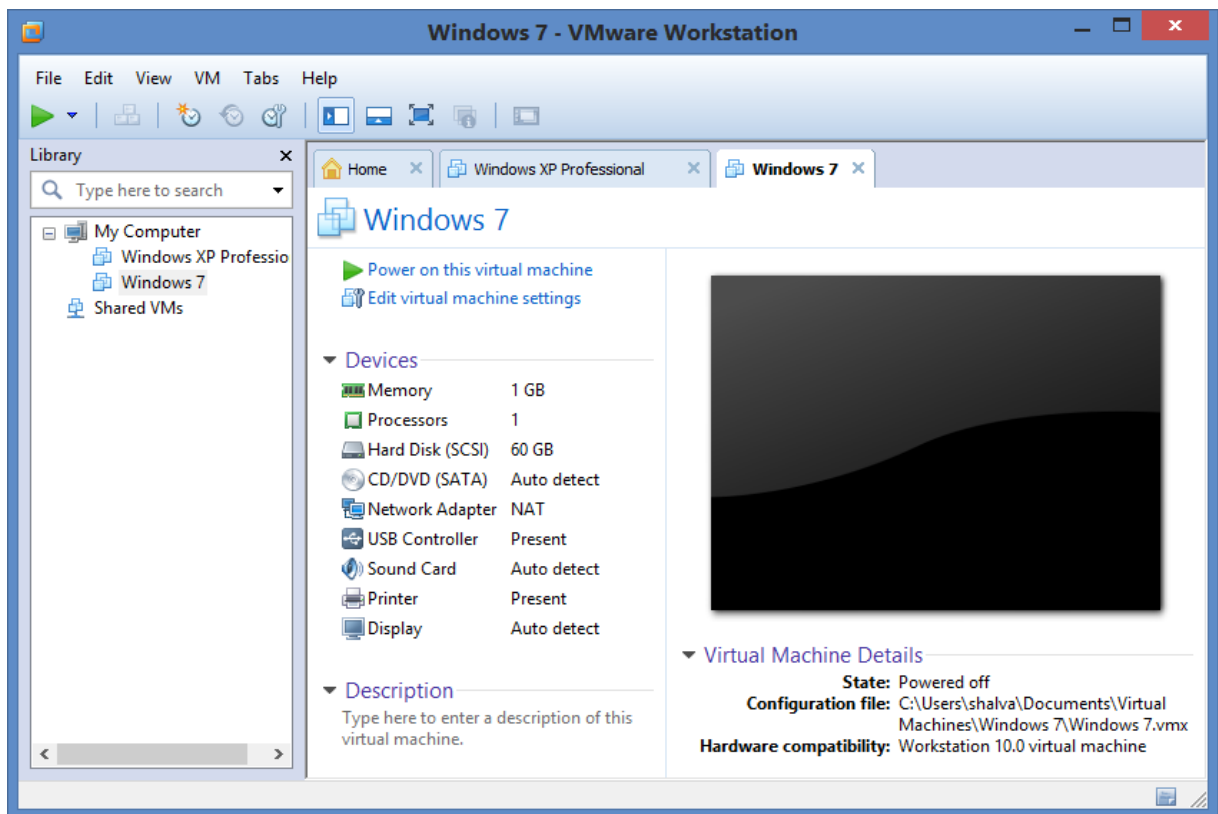
თუ ყველაფერი სწორადაა მომართული დავაჭიროთ **Finish** ღილაკს. ამით ვირტუალური მანქანის შექმნის პროცესი დასრულებულია.

ნებისმიერ დროს შეგვიძლია ვირტუალური მანქანის კონფიგურაციის შეცვლა, მაგალითად ფიზიკურ კომპიუტერზე დავამატეთ ოპერატიული მეხსიერება, მყარი დისკი და ა.შ. მოწყობილობები, ამიტომ სავსებით ლოგიკურია მოგვინდეს სტუმარი ოპერაციული სისტემისთვის რესურსების დამატება (ოპერატიული მეხსიერების გაზრდა, მყარი დისკის ზომის მომატება).

შენიშვნა: ისეთი სისტემური რესურსების ცვლილებისას, როგორცაა ოპერატიული მეხსიერების გაზრდა/შემცირება, პროცესორის ბირთვების ან ნაკადების მომატება/დაკლება და ნებისმიერი სხვა მოწყობილობის დამატება, აუცილებელია სტუმარი ოპერაციული სისტემა იყოს გათიშულ მდგომარეობაში.

3.4. ვირტუალური მანქანის პარამეტრების კონფიგურაცია

გამოვიძახოთ ვირტუალური პერსონალური კომპიუტერის მახასიათებლების დიალოგური ფანჯარა მთავარი მენიუდან **Edit virtul machine settings** ღილაკზე დაჭერით (სურ. 3.4.1). გამოვა დეტალური პარამეტრების ფანჯარა ორი ჩანართით **Hardware** და **Options**. ჩანართ **Hardware**-დან ხდება ვირტუალური მანქანის ნაწილების მომართვა, ხოლო ჩანართ **Options** -დან დამატებითი ოპციების. განვიხილოთ უფრო დაწვრილებით მოცემული მახასიათებლები.



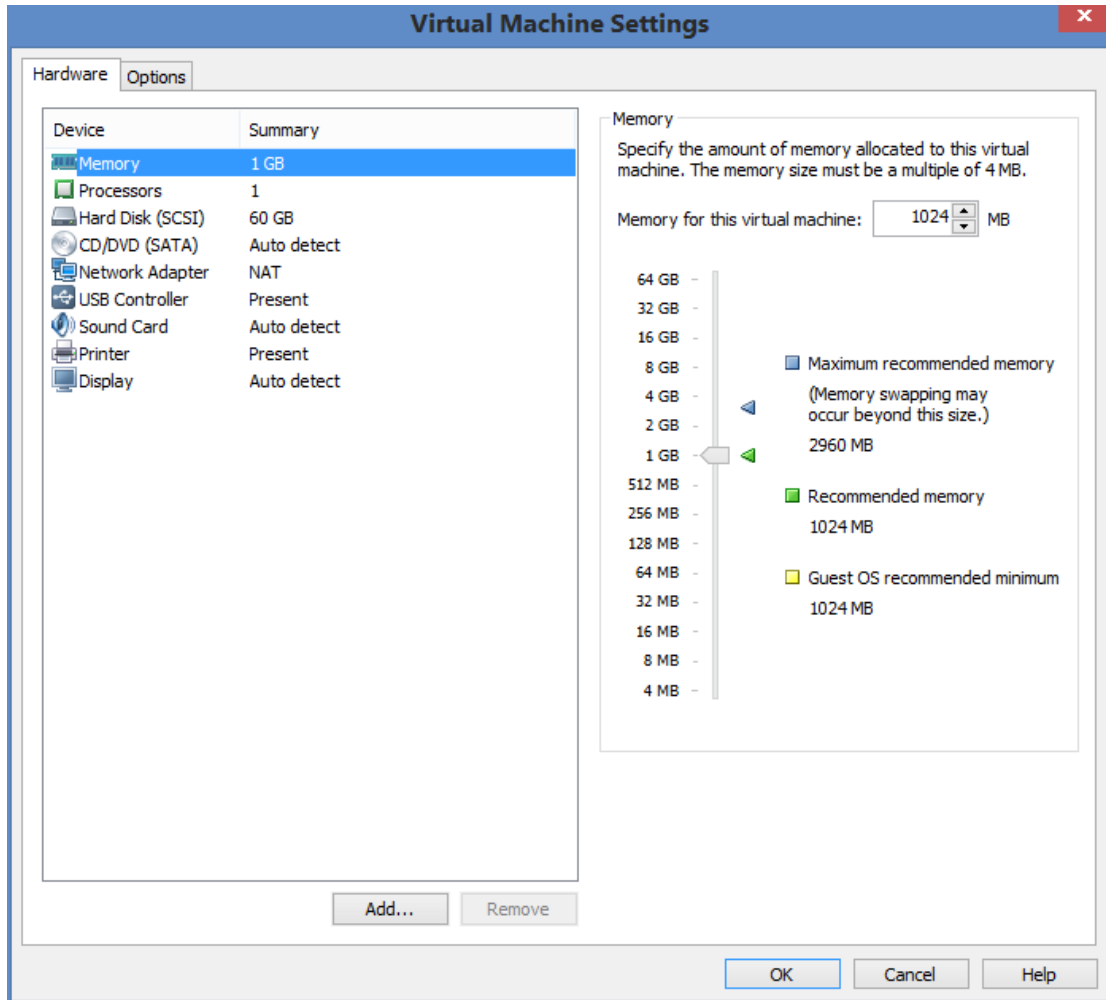
სურ.3.4. 1

❖ **Memory** - ოპერატიული მეხსიერება. ნებისმიერ მომენტში შესაძლებელია შევცვალოთ მანქანის გამოყოფილი ოპერატიული მეხსიერების ზომა (სურ. 3.4.2), ცვლილების მომენტში სტუმარი ოპერაციული სისტემა უნდა იყოს გამორთული.

მეხსიერების მოსამატებლად ან დასაკლებად გადაადგილეთ მცოცავი სასურველი მიმართულებით ან ხელით ჩაწერეთ სასურველი ციფრი, ფანჯრის ზედა მარჯვენა გამოყოფილ არეში.

შენიშვნა: გამოყოფილი ოპერატიული მეხსიერება არის ზღვარი, რომლის იქითაც ვირტუალური ოპერაციული სისტემა ვერ შეძლებს მის გამოყენებას. იმ შემთხვევაში თუ ვირტუალური ოპერაციული სისტემა გამოიყენებს გამოყოფილზე ნაკლებს, მაშინ

დარჩენილი მებსიერების გამოყენება შეეძლება სხვა ვირტუალურ ოპერაციულ სისტემებსაც. ამ პროცესს **Memory Overcommit** ან **Memory Balloning** ტექნიკას უწოდებენ.



სურ.3.4. 2

❖ **Processors** - პროცესორები. შეგვიძლია მოვმართოთ ვირტუალური მანქანის პროცესორის პარამეტრები (სურ. 3.4.3), ამასთან ერთად განვსაზღვროთ პროცესორების რაოდენობა, ბირთვების რაოდენობა პროცესორში და ვირტუალიზაციის შესრულების სასურველი რეჟიმი.

Number of processors – პროცესორების რაოდენობა;

Number of cores per processor - ბირთვების რაოდენობა თითოეულ პროცესორში.

ავირჩიოთ პროცესორებისა და ბირთვების სასურველი რაოდენობა. **Vmware workstation**-ის მახასიათებლების შედარების ცხრილიდან, რომელიც ზემოთ მოვიყვანეთ, ჩანს რომ სამუშაო სადგურს შეუძლია მხარი დაუჭიროს სტუმარი ოპერაციული სისტემის, ვირტუალური სიმეტრიული მრავალპროცესორული დამუშევების 16-მდე ვარიაციას, რომლებიც მუშაობენ მრავალპროცესორულ ჰოსტებზე. თქვენ შეგიძლიათ

განსაზღვრეთ ვირტუალურ მანქანისათვის პროცესორებისა და ბირთვების რაოდენობა ნებისმიერ ჰოსტზე, რომელსაც ორი ლოგიკური პროცესორი და პროცესორის ორი ბირთვი მაინც აქვს.

Preferred mode - აირჩიეთ სასურველი რეჟიმი ვირტუალიზაციისთვის:

Automatic – შესრულების ავტომატური რეჟიმი სტუმარი ოპერაციული სისტემის საფუძველზე;

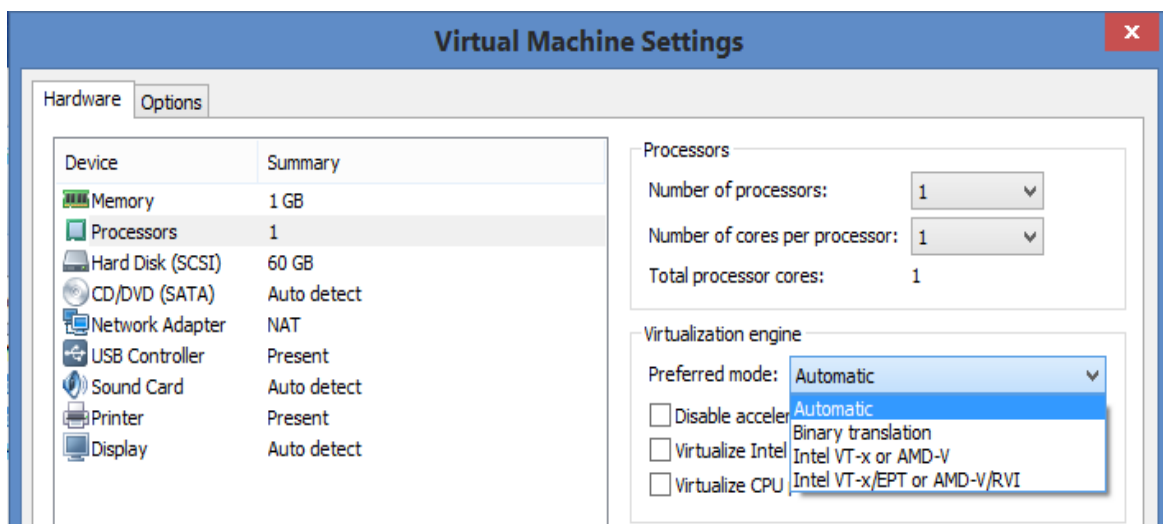
Binary translation – ჰოსტი იყენებს, უშუალოდ სტუმარი ოპერაციული სისტემის შემსრულებელი კოდის კომბინაციას და ბინარულ გადაყვანას.

Intel VT or AMD-V –

Intel VT – x/EPT or AMD –V/RVI -

ბოლო ორი ვარიანტი სრულდება პროცესორებზე აპარატურული ვირტუალიზაციით. თუმცა ყველა პროცესორი არ უჭერს მხარს ამ ტექნოლოგიას. იმისათვის რომ დავრწმუნდეთ უჭერს თუ არა მხარს ჩვენი პროცესორი მოცემულ ფუნქციას იხილეთ ჩამონათვალი **Intel** პროცესორებისა, რომლებიც მხარს უჭერენ **Intel VT** ან აპარატურულ ვირტუალიზაციას <http://www.vsphere5.ru/doku.php?id=technical-info:intel-vt-support>.

და ვირტუალიზაციის მზარდაჭერა **AMD** პროცესორების მიერ <http://www.vsphere5.ru/doku.php?id=amd-v-support>

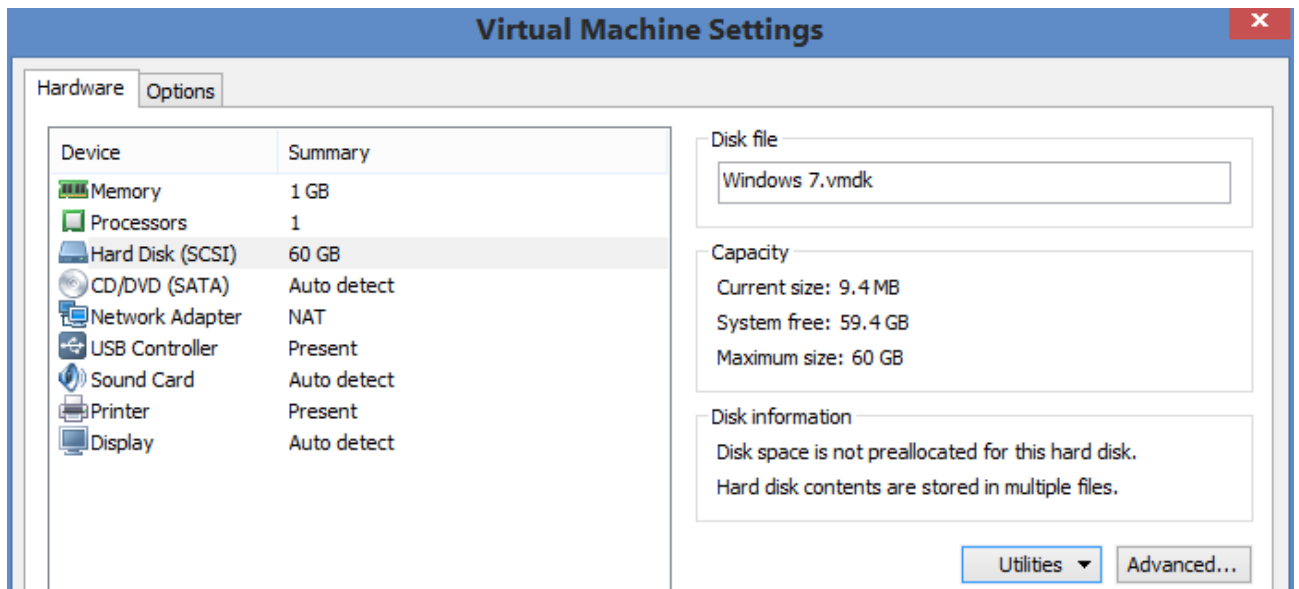


სურ.3.4. 3

Disable acceleration for binary translation - გამოვრთოთ აჩქარება ბინარული ტრანსლაციისათვის. ზოგჯერ ჩნდება პრობლემები ვირტუალურ გარემოში, მაგალითად სტუმარი ოპერაციული სისტემა შეიძლება დაეკიდოს ვირტუალური მანქანის შიგნით

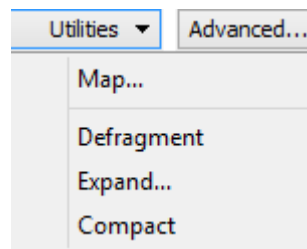
პროგრამული უზრუნველყოფის ინსტალაციის ან გაშვების დროს. ეს პრობლემა ჩვეულებრივ ჩნდება პროგრამის შესრულების დასაწყისში. ბევრ შემთხვევაში შესაძლებელია პრობლემის აღმოფხვრა თუკი დროებით გამოვრთავთ ვირტუალური მანქანის ბინარული ტრანსლაციის აჩქარებას. მას შემდეგ რაც პროგრამა გაივლის იმ წერტილს სადაც ჩნდება პრობლემა, გავაუქმოთ ამ პარამეტრის მოქმედება.

❖ **Hard disk** - მყარი დისკი (სურ. 3.4.4). **Capacity** ჯგუფში მოცემულია თუ რა ადგილია დაკავებული თუ თავისუფალი ვირტუალურ მყარ დისკზე. ჯგუფში **Disk information** - ასახულია ინფორმაცია დისკის შესახებ. არის კიდევ ორი ღილაკი: **Utilities** და **Advanced**.



სურ.3.4. 4

Utilities ღილაკზე დაჭერისას ჩამოიშლება მენიუ რამდენიმე ასარჩევი ვარიანტით (სურ.3.4.5):



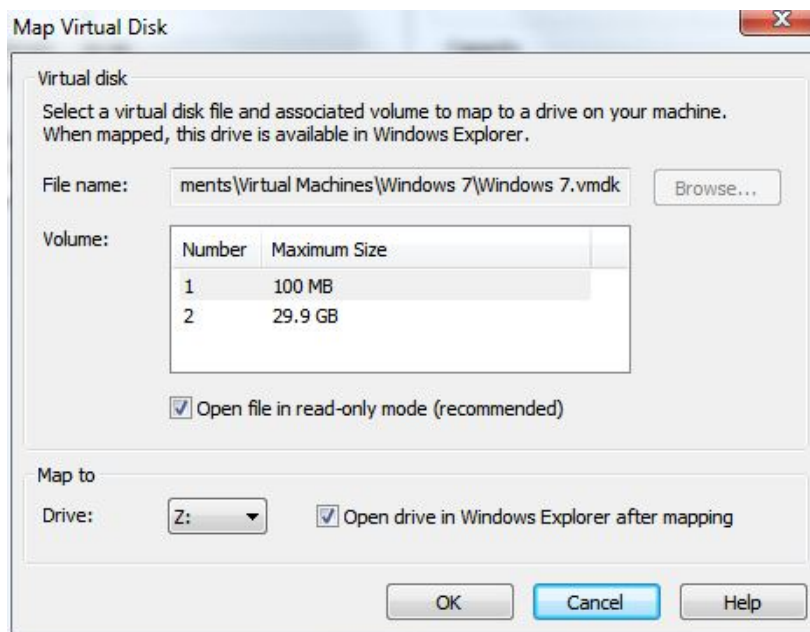
სურ.3.4. 5

Map - ეს არის ფუნქცია, რომლის საშუალებითაც შეგვიძლია ვირტუალური მყარი დისკის დაკავშირება ფიზიკურ მყარ დისკთან. დაწვრილებითი ინფორმაცია **Map**-ის შესახებ იხილეთ მისამართზე: <http://blog.pskovsoft.com/?p=465> ;

იმ შემთხვევაში თუ ვირტუალურ მყარ დისკზე ინახება ფაილები, რომლებიც გვინდა რომ გადავიტანოთ ჰოსტ ოპერაციულ სისტემაში (ფიზიკურ მყარ დისკზე), ჩვენ შეგვიძლია ამის გაკეთება აღნიშნული უტილიტით (სურ. 3.4.6).

Open file in read-only mode - ფაილის გახსნა მხოლოდ კითხვის რეჟიმში;

Drive - საშუალებას იძლევა დავაკავშიროთ ფიზიკური მყარი დისკი ვირტუალური დისკის შესაბამის დანაყოფთან.



სურ.3.4. 6

ჩამოშლილი მენიუს დანარჩენი სამი უტილიტა საშუალებას გვაძლევს შევასრულოთ შემდეგი ოპერაციები.

Defragment - მონაცემთა დეფრაგმენტაცია;

Expand - დისკის გაფართოება იმ შემთხვევაში, როცა საკმარისი ადგილი არ არის ვირტუალურ დისკზე.

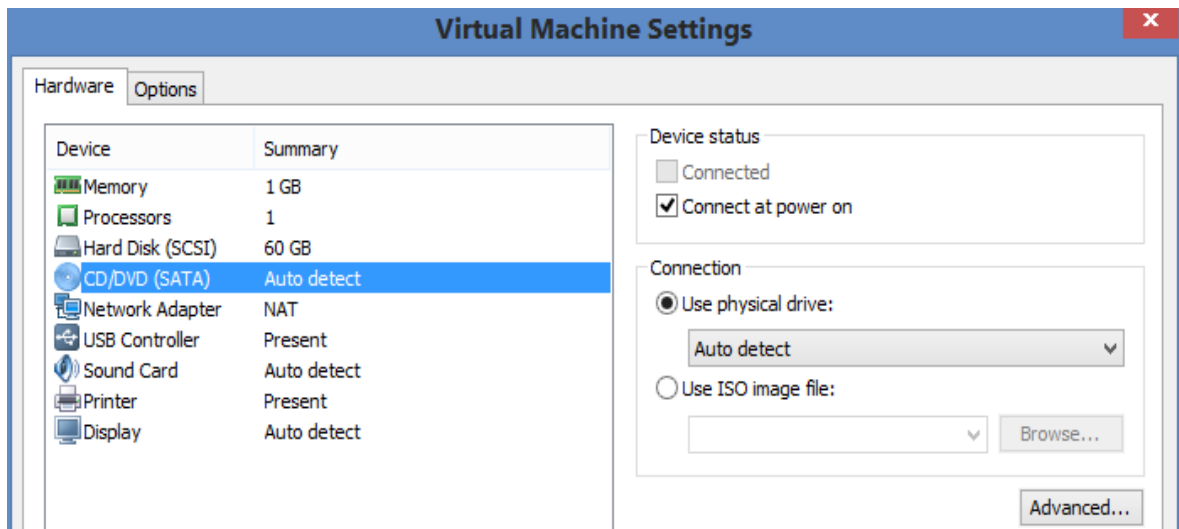
Compact - ვირტუალური დისკის შემჭიდროება ადგილის გამონთავისუფლების მიზნით.

❖ **CD\DVD (SATA):**

CD/DVD წამყვანი მუშაობს ორ რეჟიმში:

Use physical drive – გამოიყენოს ფიზიკური დისკწამყვანი;

Use ISO image file - გამოიყენოს ISO ფაილი.



სურ.3.4. 7

Device status

ზოგიერთი მოწყობილობისათვის დამახასიათებელია პარამეტრი, რომელიც საშუალებას იძლევა „ცხელი მეთოდით“ მივაერთოთ მოწყობილობა ვირტუალურ გარემოს:

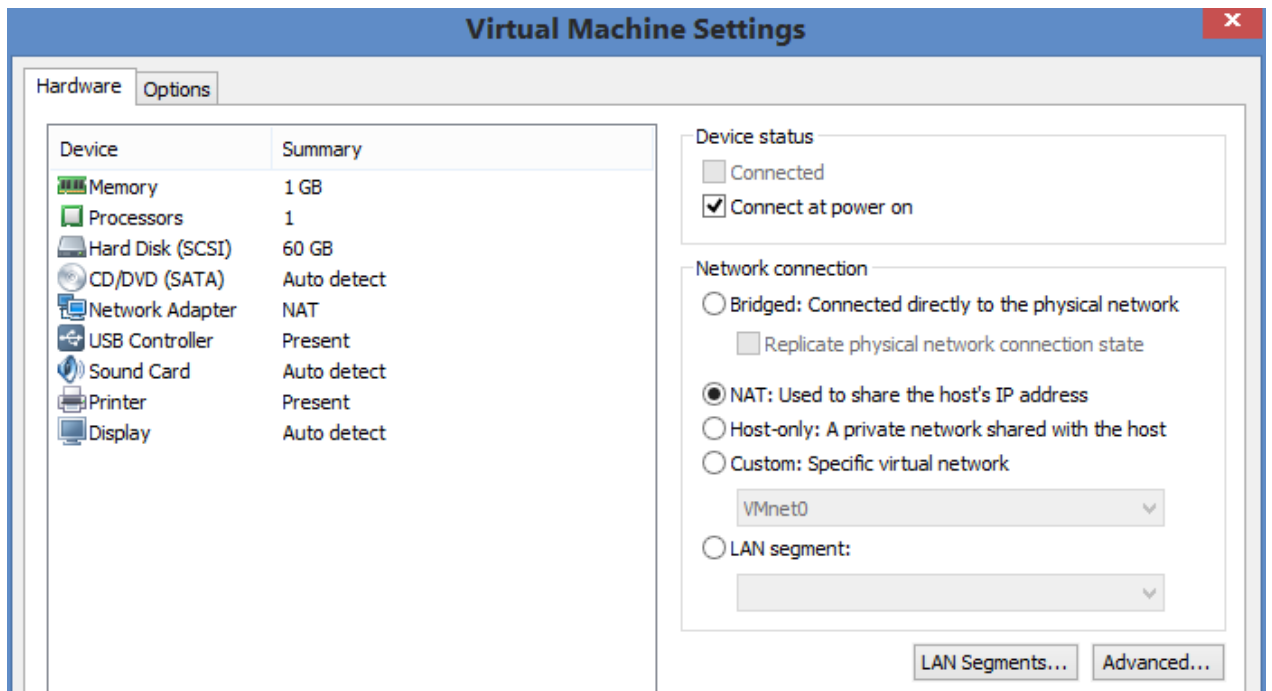
Connected – ჩართულ ვირტუალურ მანქანაზე;

Connected at power on - ვირტუალური მანქანის ჩართვისას (ავტომატურად).

ისევე როგორც HDD, დისკწამყვანი შეიძლება იყოს შეერთებული IDE ან SCSI კონტროლერზე, შესაბამისად შესაძლებელია შეიცვალოს მაგალითად IDE მოწყობილობის და კონტროლერის ნომერი.

Use ISO image file: ეს პარამეტრი გვაძლევს საშუალებას მოვძებნოთ ოპერაციული სისტემის ISO ფაილი და იქიდან მოვახდინოთ სტუმარი ოპერაციული სისტემის ინსტალაცია. ასევე შეგვიძლია მისი გამოყენება ისეთი პროგრამების გასაშვებად, რომელსაც გააჩნია ჩამტვირთავი (Boot) ფაილი, მაგალითად: Acronis, Hiren's Boot CD და ა.შ. აღსანიშნავია ის ფაქტი, რომ ISO ფაილიდან ოპერაციული სისტემის დაყენება გაცილებით სწრაფად ხდება ვიდრე CD/DVD დისკებიდან.

❖ **Network Adapter** - ქსელის ადაპტერი):



სურ.3.4. 8

3.5. ვირტუალიზაციის Hypervisor-ების მართვა და მონიტორინგი

3.5.1. ქსელის მართვის ორგანიზაცია ვირტუალურ მანქანებს შორის

ვირტუალური მანქანა **Vmware** პლატფორმაზე, მომხმარებელს აძლევს საშუალებას შექმნან ვირტუალური სისტემის განსხვავებული კომბინაცია, რომლებიც მუშაობენ ქსელური ურთიერთქმედების განსხვავებული პრინციპებით. **Vmware**-ში არის შემდეგი ძირითადი ქსელური კომპონენტი:

- ვირტუალური კომუტატორი (**Virtual Switches**);
- ვირტუალური ქსელური ინტერფეისი (**Virtual Ethernet Adapters**);
- ვირტუალური ხიდი (**Virtual Bridge**);
- ჩაშენებული **DHCP**-სერვერი;
- ქსელური მისამართების ტრანსლირების მოწყობილობა (**NAT**).

VMware Workstation-სა და **VMware Server**-ში ქსელური ურთიერთქმედების ფუნდამენტური ელემენტი არის ვირტუალური კომუტატორი, რომელიც უზრუნველყოფს ვირტუალური მანქანის ქსელურ ურთიერთქმედებას ფიზიკური მოწყობილობის მსგავსად: ვირტუალურ კომუტატორზე არის პორტები, რომელზეც

შეიძლება იყვნენ დაკავშირებული ვირტუალური მანქანის ვირტუალური ქსელური ინტერფეისები, ასევე ვირტუალური ინფრასტრუქტურის სხვა კომპონენტები ჰოსტის ფარგლებში. ზოგიერთი ვირტუალური კომპიუტერი, დაკავშირებული ერთ ვირტუალურ კომპუტატორზე ეკუთვნის ერთ ქვექსელს. ვირტუალური ხიდი არის მექანიზმი, რომლის მეშვეობითაც ხდება დაკავშირება კომპიუტერის ფიზიკურ ქსელურ ადაპტერსა და ვირტუალურ ქსელურ ინტერფეისს შორის. **VMware**-ის ჩამოთვლილი **DHCP**-სერვერი საშუალებას აძლევს ვირტუალურ კომპიუტერებს ავტომატურად მიიღონ **IP** მისამართები, თავის ქვექსელში. რაც შეეხება ვირტუალურ **NAT**-მოწყობილობას, ის უზრუნველყოფს ქსელის მისამართების ტრანსლაციას, ვირტუალური კომპიუტერის ურთიერთობით გარე ქსელთან.

ვირტუალურ მანქანაში არსებობს ქსელური ურთიერთქმედების სამი სახე:

VMware Workstation პროდუქტი მომხმარებელს აძლევს შესაძლებლობას მიაწოდოს ვირტუალური კომპიუტერის თითოეულ ქსელურ ადაპტერს ქსელური ურთიერთქმედების სამი ტიპიდან ერთ-ერთი:

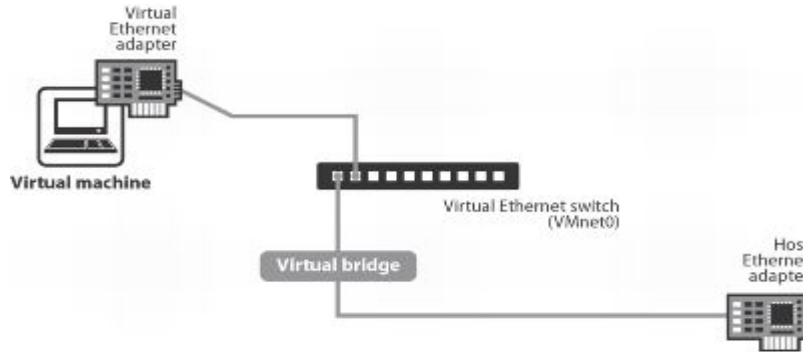
- **Bridged**
- **Host-only**
- **NAT**

ქსელური ურთიერთქმედების თითოეული ეს ტიპი შეიძლება გავრცელდეს ვირტუალური კომპიუტერის გამოყენების განსხვავებულ ვარიანტებში. აუცილებელია საფუძვლიანად ავირჩიოთ ქსელური ურთიერთქმედების ტიპი უფრო ეფექტური გამოყენებისთვის ქსელური ინფრასტრუქტურის სხვა კომპონენტებთან ერთად.

Bridged Networking

ქსელური ურთიერთქმედების ეს ტიპი საშუალებას იძლევა დავაკავშიროთ ვირტუალური კომპიუტერის ქსელური ადაპტერი კომპიუტერის ფიზიკურ ქსელურ ინტერფეისთან, რაც იძლევა შესაძლებლობას გაიყოს ქსელური ადაპტერის რესურსები ჰოსტ და ვირტუალურ სისტემას შორის. ვირტუალური მანქანა ქსელური ურთიერთქმედების ასეთი ტიპით იქნება კავშირში გარე ქსელთან როგორც დამოუკიდებელი კომპიუტერი. ასეთ მანქანას შეგვიძლია მივანიჭოთ საკუთარი **IP** მისამართი სახლის ან ორგანიზაციის ქსელში, ან ის მისამართს მიიღებს გარე **DHCP**-

სერვერიდან. შექმნის პროცესში მყოფი ვირტუალური კომპიუტერისთვის, ქსელის ეს ტიპი ავტომატურადაა მინიჭებული, რადგან ეს ყველაზე მარტივი საშუალებაა ქსელის ორგანიზებისთვის ვირტუალურ მანქანებს, ჰოსტსა და გარე ქსელს შორის. ქვემოთ წარმოდგენილია **Bridged Networking** მოდელი (სურ.3.5.1.1):

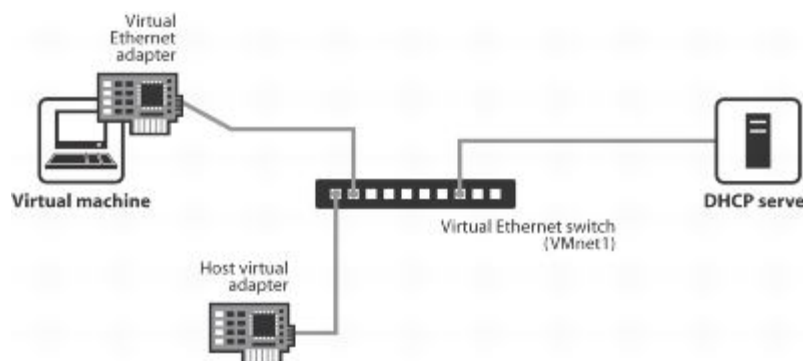


სურ.3.5.1.1 *Bridged Networking*

სტუმარი სისტემის ვირტუალური ქსელური ადაპტერი უკავშირდება ვირტუალურ კომპიუტორს **VMnet0**, რომელზეც ასევე მიერთებულია ვირტუალური ხიდი, რომელიც პირდაპირ ურთიერთქმედებაშია ფიზიკურ ქსელურ ადაპტერთან.

Host-Only Networking

ქსელური ურთიერთქმედების ასეთი ტიპი ოპტიმალურია პროგრამული უზრუნველყოფის სრული ტესტირების დროს, როცა გვჭიდება ვირტუალური ქსელის ორგანიზება ჰოსტ კომპიუტერის ფარგლებში, რაც შეეხება ვირტუალურ მანქანას, მას არ სჭირდება გარე ქსელიდან გამოსვლა. ვირტუალურ ქვექსელში მოქმედებს DHCP-სერვერი, რომელიც დაკავშირებულია ვირტუალურ კომპიუტორთან **VMnet1** და ვირტუალურ კომპიუტერებს მინიჭებული აქვთ IP-მისამართები მოცემული დიაპაზონიდან (ავტომატურად განსაზღვრულია **192.168.179.128 – 192.168.179.254** დიაპაზონი). ქვემოთ მოცემულია **Host-Only Networking** ტიპი (სურ. 3.5.1. 2):

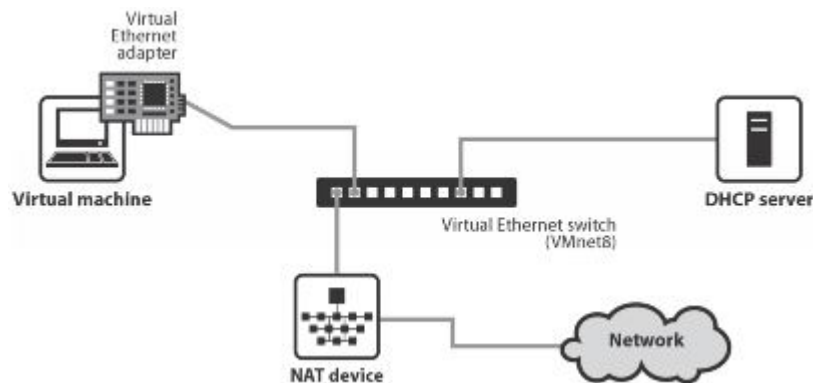


სურ.3.5.1.2 *Host-Only Networking*

სტუმარი სისტემის ვირტუალური ქსელური ადაპტერი უერთდება კომპუტატორ VMnet-ს და ურთიერთქმედებს 192.168.179.0/24 ქვესელში. ჰოსტ სისტემაში ასევე იქმნება ვირტუალური ქსელური ინტერფეისი დაკავშირებული VMnet1-თან, რომელიც თავის მხრივ ურთიერთქმედებაშია ვირტუალურ მანქანასთან.

NAT Networking

ქსელური ურთიერთქმედების ეს ტიპი ძალიან ახლოსაა Host-Only-სთან, ერთი გამონაკლისით: ვირტუალურ კომპუტატორთან VMnet8 დაკავშირებულია IP-მისამართების ტრანსლირების მოწყობილობა (NAT). ამ კომპუტატორთან ასევე მიერთებულია DHCP-სერვერი, რომელიც ვირტუალურ მანქანებს ურიგებს მისამართებს მოცემული დიაპაზონიდან (192.168.89.128 – 192.168.89.254). NAT-მოწყობილობა საშუალებას იძლევა განახორციელოს IP-მისამართების ტრანსლაცია, რაც უზრუნველყოფს ვირტუალური კომპიუტერების კავშირის ინიცირებას გარე ქსელთან. ქვემოთ მოცემულია NAT Networking ტიპი (სურ. 3.5.1.3):



სურ.3.5.1. 3 NAT Networking

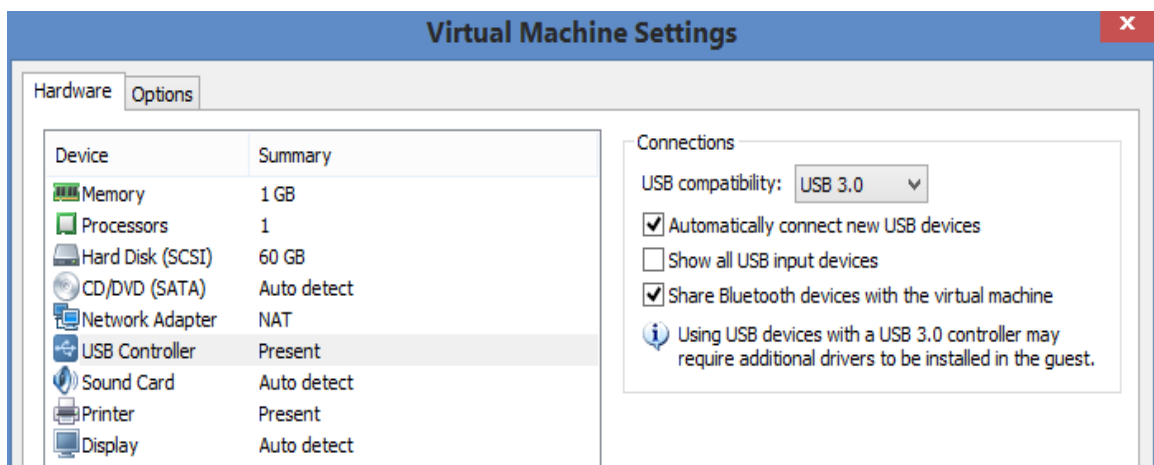
ჰოსტ ოპერაციულ სისტემაში ისევე როგორც Host-Only Networking-ში იქმნება ვირტუალური ქსელური ინტერფეისი VMnet 8-კომპუტატორისთვის, რომელიც იძლევა ვირტუალურ მანქანებთან კავშირის საშუალებას.

ქსელური ურთიერთქმედების ასეთი მოდელი ოპტიმალურია უსაფრთხოების თვალსაზრისით (რადგან შეუძლებელია გარე შეერთების ინიცირება ვირტუალურ მანქანასთან), მაგრამ მნიშვნელოვნად მცირდება ქსელის სიჩქარე (დაახლოებით 20-30 პროცენტით). NAT-კავშირი შესაძლებელია გამოყენებულ იქნას, მაგალითად, ვირტუალური მანქანის უსაფრთხო მუშაობისთვის ინტერნეტში.

თითოეულ ვირტუალურ კომპიუტერს შეიძლება ჰქონდეს რამდენიმე ვირტუალური ქსელური ადაპტერი, დაკავშირებულნი განსხვავებულ ვირტუალურ კომპიუტორთან, რომლებზეც რეალიზდება ქსელური ურთიერთქმედების განსხვავებული ტიპები. **VMware Workstation 10** პლატფორმაზე შესაძლებელია ერთდროულად 10 ქსელური ადაპტერის მუშაობის უზრუნველყოფა.

❖ **USB Controller** (სურ. 3.5.1.4) – „**Connection**“ ჯგუფს ექვემდებარება სამი ძირითადი ფუნქცია:

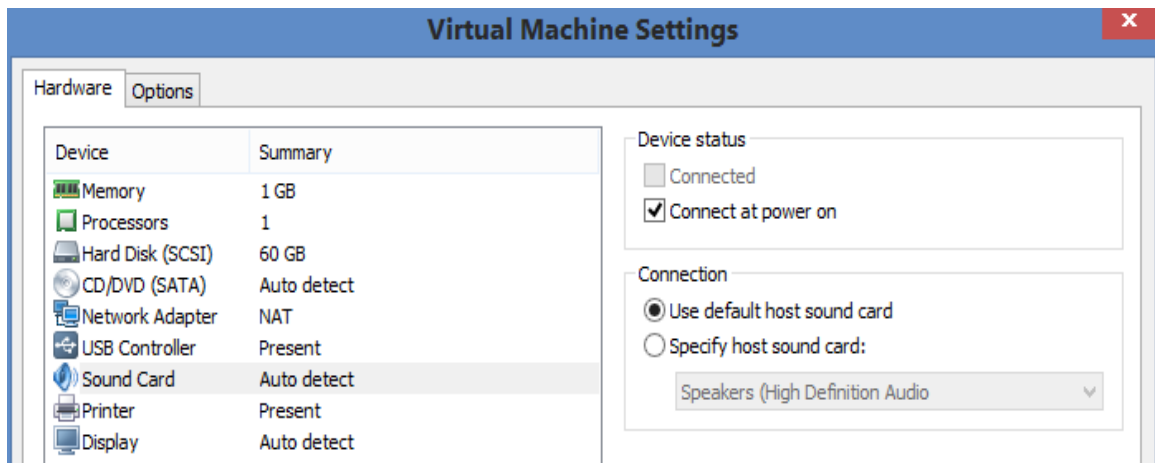
- **Automatically connect new USB devices** - ვირტუალური მანქანის გაშვების შემდეგ ავტომატურად მოხდება ახალი USB მოწყობილობის მოძებნა და ჩართვა;
- **Show all USB input devices** - მისი ჩართვის შემდეგ გამოჩნდება ყველა მიერთებული USB მოწყობილობა;
- **Share Bluetooth devices with the virtual machine** - ეს ფუნქცია უზრუნველყოფს **Bluetooth** მოწყობილობის საერთო წვდომის ჩართვას ვირტუალურ მანქანებს შორის.



სურ.3.5.1. 4

❖ **Sound Card** - ხმის ადაპტერი. აქაც გვაქვს სამი პუნქტი:

- **Connect at power on** - მოხდეს ხმის ადაპტერის ავტომატური დაკავშირება, ვირტუალური მანქანის ჩართვისთანავე;
- **Use default host sound card** - გამოყენებულ იქნას ფიზიკური მანქანის ხმის ადაპტერი, რომელიც ავტომატურადაა მომართული;
- **Specify host sound card** - სპეციფიკური ხმის ადაპტერი. ეს პარამეტრი საშუალებას იძლევა ფიზიკურ კომპიუტერზე დაიყოს ხმის არხები სხვადასხვა ხმის ადაპტერებად.



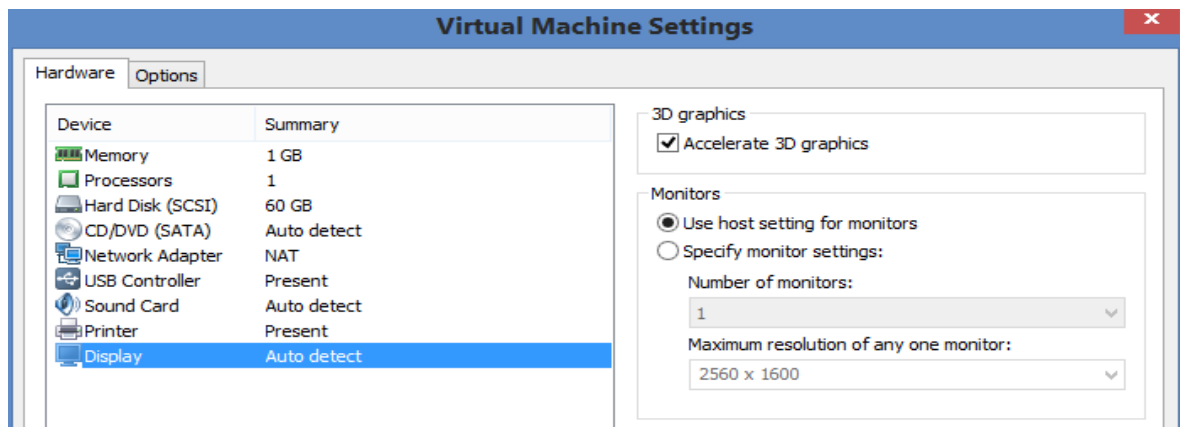
სურ.3.5.1. 5

❖ **Printer** - პრინტერი. იმისათვის რომ დავაყენოთ და ვამუშაოთ ჩვენთვის სასურველი პრინტერი ვირტუალურ მანქანაზე, გვჭირდება დამხმარე უტილიტა **Vmware Tools**, რომელიც ჩაშენებულია **Vmware Workstation**-ში. ინსტალაციის დროს ის აყენებს როგორც პრინტერის ისე სხვა მოწყობილობების დრაივერებს. პრინტერი ვირტუალურ მანქანაში იყენებს **port 1**-ს.

❖ **Display** - მონიტორი პარამეტრი **Accelerate 3D graphics** ჩართავს/გამორთავს **3D** ფუნქციის მხარდაჭერას.

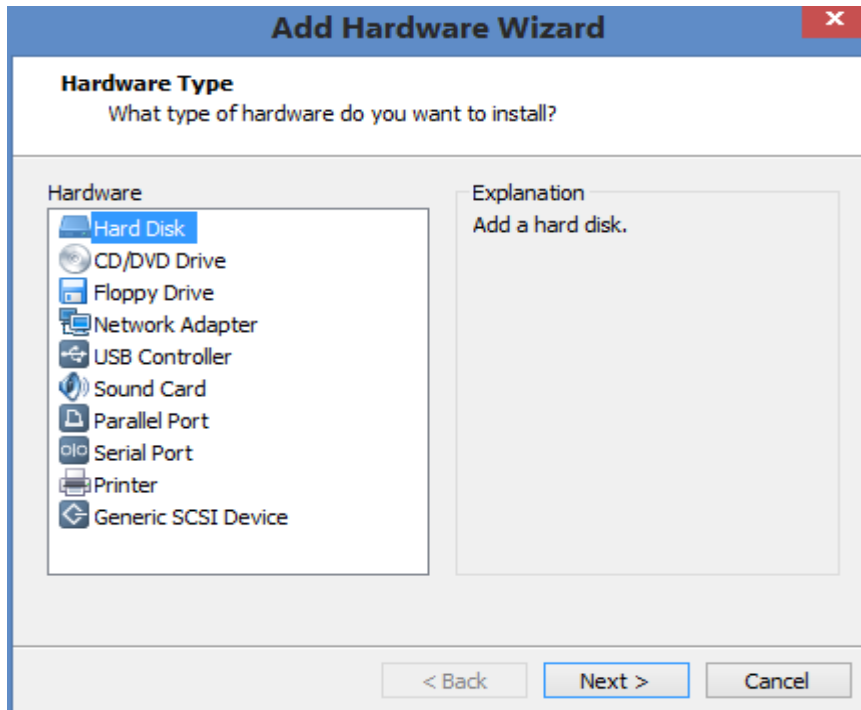
➤ **Use host settings for monitors** - გამოყენებული იქნას ფიზიკური კომპიუტერის პარამეტრები ვირტუალური მონიტორისთვის.

➤ **Specify monitor settings** - მონიტორის სპეციფიური პარამეტრები, საშუალებას გვაძლევს მოვმართოთ მონიტორის პარამეტრები, როგორცაა მონიტორის რაოდენობა და თითოეული მონიტორის გარჩევადობა.



სურ.3.5.1. 6

ვირტუალური კომპიუტერის აპარატურული ნაწილის მომართვა დასრულდა. დაგვრჩა მხოლოდ სასურველი მოწყობილობის დამატება სტუმარ ოპერაციულ სისტემაში. ამისათვის ვაწვებით **Add** ღილაკს. შესაძლებელია დავამატოთ ახალი მყარი დისკი, CD/DVD დისკვაჩი, ქსელის ადაპტერი, პორტები და ა.შ.



სურ.3.5.1. 7

შენიშვნა: ზოგიერთ მოწყობილობაზე დაწესებულია ლიმიტი, ანუ ერთზე მეტის გამოყენების საშუალება არ გვაქვს. ასეთი მოწყობილობებია:

- **USB** კონტროლერი;
- ხმის ადაპტერი;
- პრინტერი.

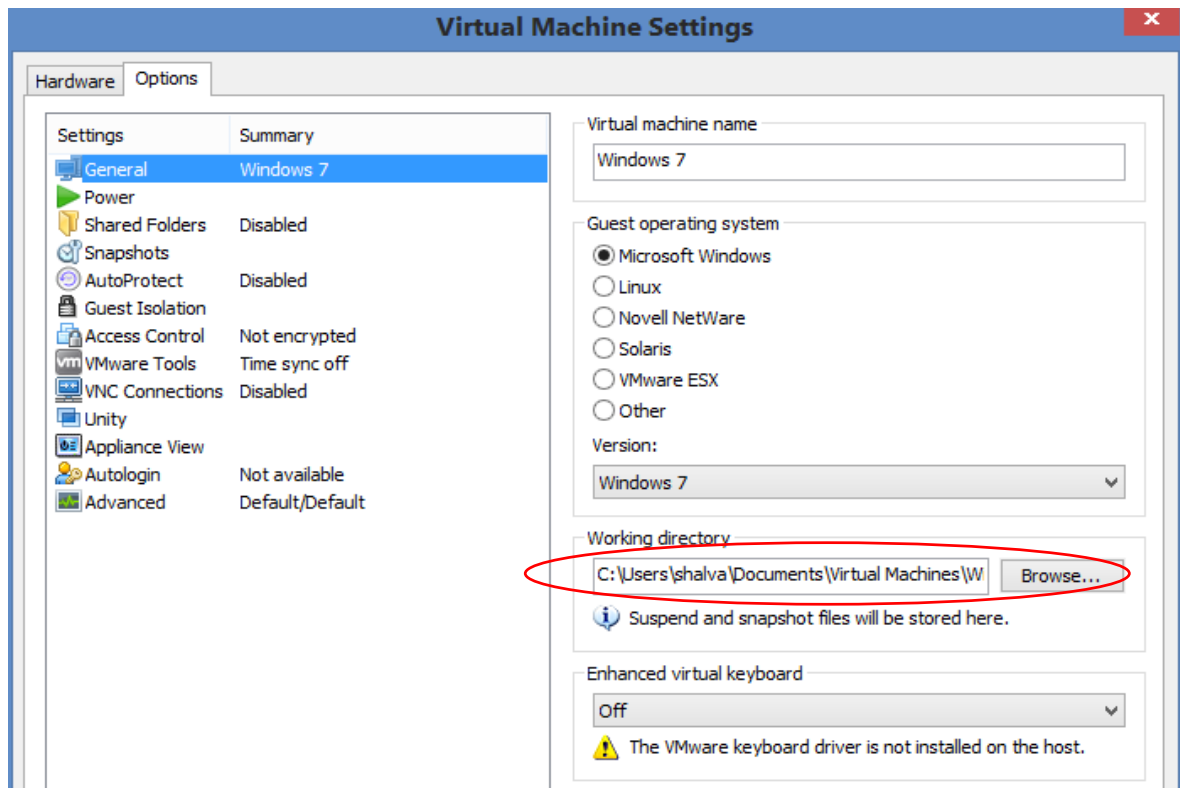
ახლა გადავიდეთ **Options** ჩანართში და განვიხილოთ იქ არსებული პარამეტრები.

1) **General** - მთავარი მენიუ, საიდანაც შეგვიძლია მოვმართოთ:

- **Virtual machine name** - ვირტუალური მანქანის სახელი;
- **Guest operating system** – სურვილისამებრ შეგვიძლია შევცვალოთ სტუმარი ოპერაციული სისტემა;

- **Version** – შევცვალოთ ოპერაციული სისტემის ვერსია;

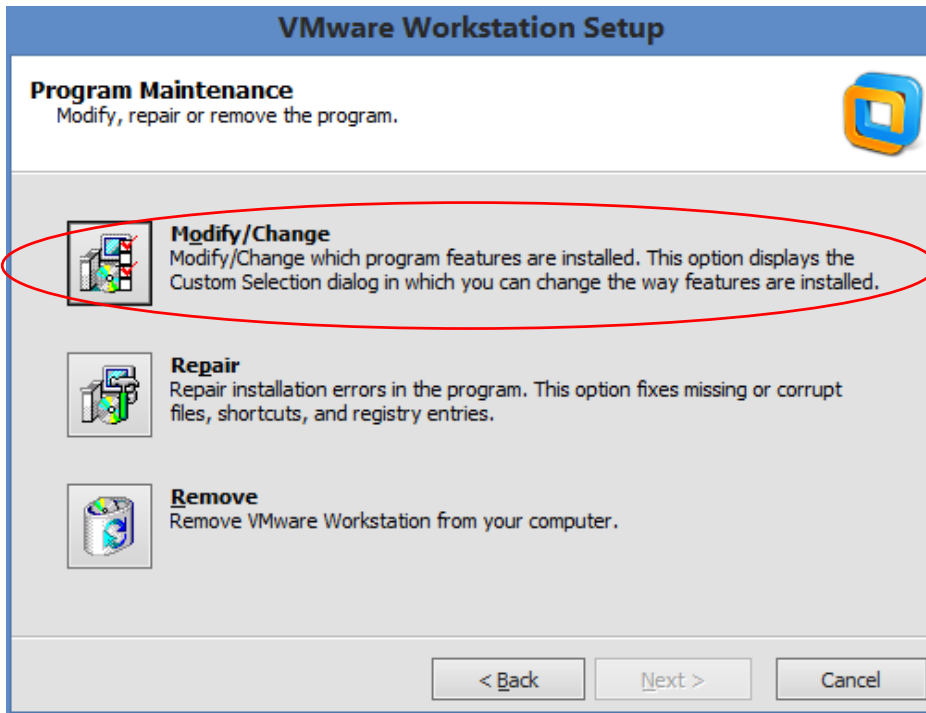
- **Working directory** – მივუთითოთ სამუშაო კატალოგის განთავსების სხვა ადგილი. ამ კატალოგში შეინახება შეჩერებული (**Suspend Mode**) მანქანის და მდგომარეობის აღსადგენი (**Snapshots**) ფაილები;



სურ.3.5.1. 8

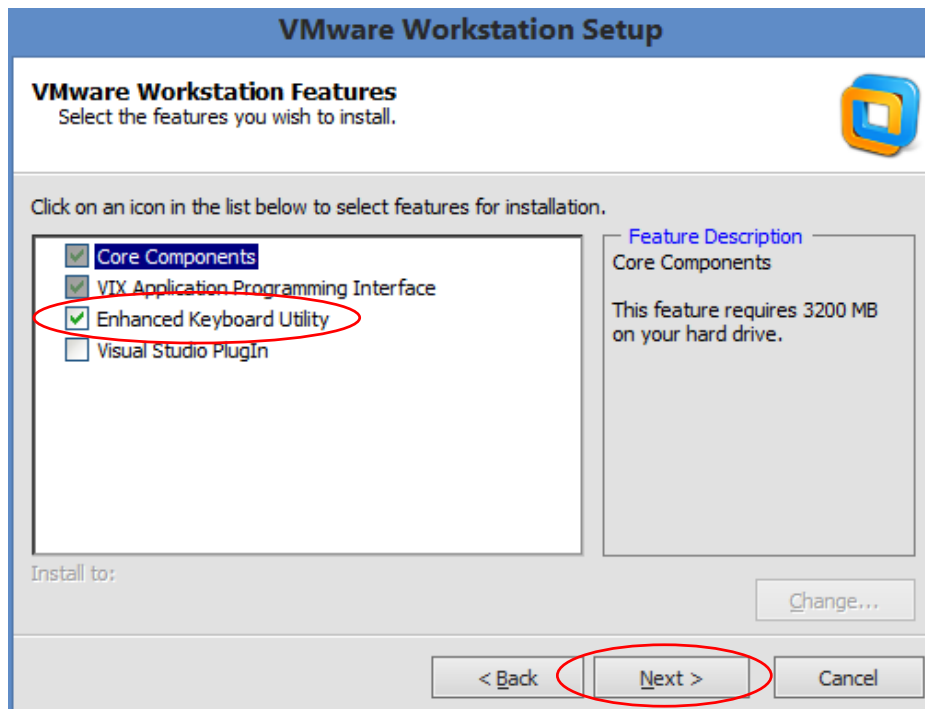
Enhanced virtual keyboard - ვირტუალური მანქანის კლავიატურის გაფართოებული ფუნქციები. ეს ფუნქცია საშუალებას იძლევა ჩავრთოთ ან გამოვრთოთ ვირტუალური კლავიატურის მხარდაჭერა. საერთოდ, ვირტუალური კლავიატურის გაფართოებული ფუნქციები უზრუნველყოფს საუკეთესო მართვას თანამედროვე კლავიატურის და კლავიატურის, რომელთაც აქვთ დამატებითი ღილაკები. ეს ფუნქცია ხელმისაწვდომია მხოლოდ **Windows**-ის ჰოსტ სისტემაზე.

Vmware-ის ვირტუალური გარემო გვთავაზობს ოპერაციული სისტემა **Windows**-ის უსაფრთხოების თანამედროვე სისტემას, **API** ფუნქციის გენერაციის (ღილაკზე დაჭერა) და ნებისმიერი საზიანო პროგრამის (რომლებიც შეიძლება განთავსდნენ ჰოსტ კომპიუტერზე) მოხსნის გვერდის ავლით. გაფართოებული ვირტუალური კლავიატურის გამოყენებისას, მხოლოდ სტუმარი ოპერაციული სისტემა მოქმედებს **Ctrl+Alt+Delete** კომბინაციაზე დაჭერისას.



სურ.3.5.1. 9

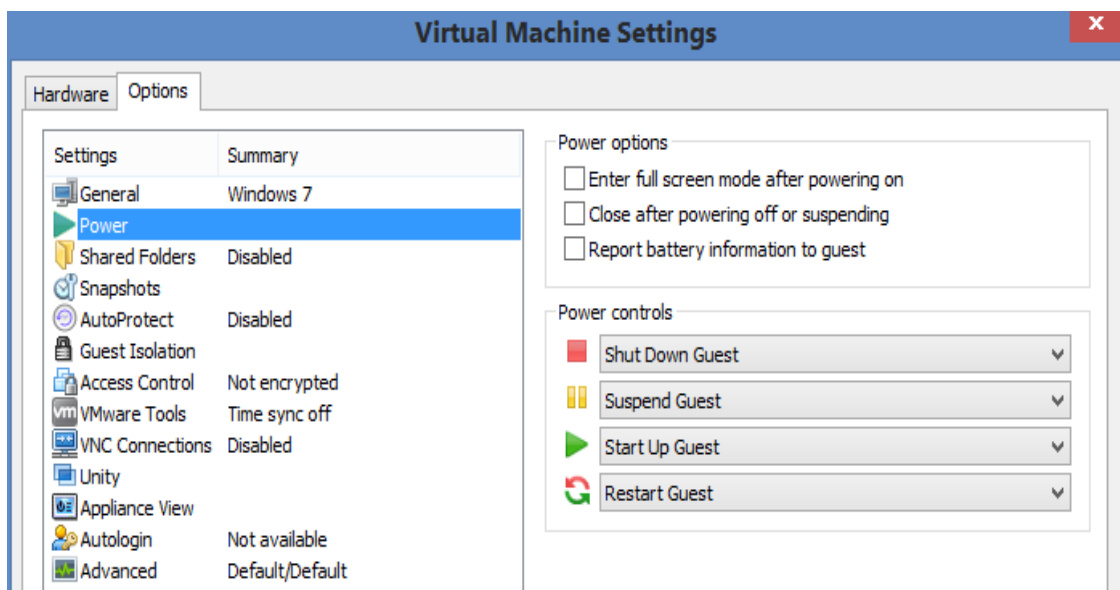
თუ არ გაქვთ დაინსტალირებული ვირტუალური კლავიატურის დრაივერი, რაზეც მეტყველებს ფანჯრის ბოლოს გამოსული შეტყობინება, და გადაწყვიტეთ ამ ფუნქციის გამოყენება, ხელახლა გაუშვით **VMware**-ის ინსტალატორი **Modify/change** რეჟიმში (სურ.3.5.1.10). შემდეგ მონიშნეთ პუნქტი „**Enhanced Keyboard Utility**” :



სურ.3.5.1. 10

2) **Power** - კვება (სურ. 3.5.1.11). **Power option** ჯგუფი მოიცავს შემდეგ ბრძანებებს:

- **Enter full screen mode after powering on** - ვირტუალური მანქანის ჩართვის შემდეგ ავტომატურად მოხდეს სრულეკრანიან რეჟიმში გადასვლა;
- **Close after powering of or suspending** - კვებიდან გამორთვის ან დაპაუზების შემდეგ დაიხუროს **Vmware Workstation** პროგრამის ფანჯარა.
- **Report battery information to guest** - ეს ბრძანება გამოიტანს შეტყობინებას სტუმარი ოპერაციული სისტემის კვების მდგომარეობის შესახებ. (ეს პარამეტრი აქტუალურია იმ შემთხვევაში, როცა სტუმარი ოპერაციული სისტემა მუშაობს სრულ-ეკრანიან რეჟიმში, ფიზიკური კომპიუტერის შემთხვევაში კი ეს ფუნქცია გამოიყენება ნოუთბუქებში და სხვა მოწყობილობებში, რომლებიც მუშაობენ ელექტროქსელის გარეშე.



სურ.3.5.1. 11

ჯგუფი Power controls:

აქ კვება იყოფა ორ განყოფილებად: ერთი - უბრალოდ კვების მართვა და მეორე - სტუმარი ოპერაციული სისტემის მართვა.

Power Off - ვირტუალური კომპიუტერის გამორთვა;

Suspend - დაპაუზება (ვირტუალური კომპიუტერის მუშაობის დაპაუზება);

Power On - კვების ჩართვა (ვირტუალური კომპიუტერის გაშვება);

Reset - გადატვირთვა (ვირტუალური კომპიუტერის გადატვირთვა);

Shut Down Guest - სტუმარი ოპერაციული სისტემის გამორთვა (ოპერაციული სისტემის გათიშვა და სიგნალის გაგზავნა ვირტუალური მანქანის გათიშვაზე);

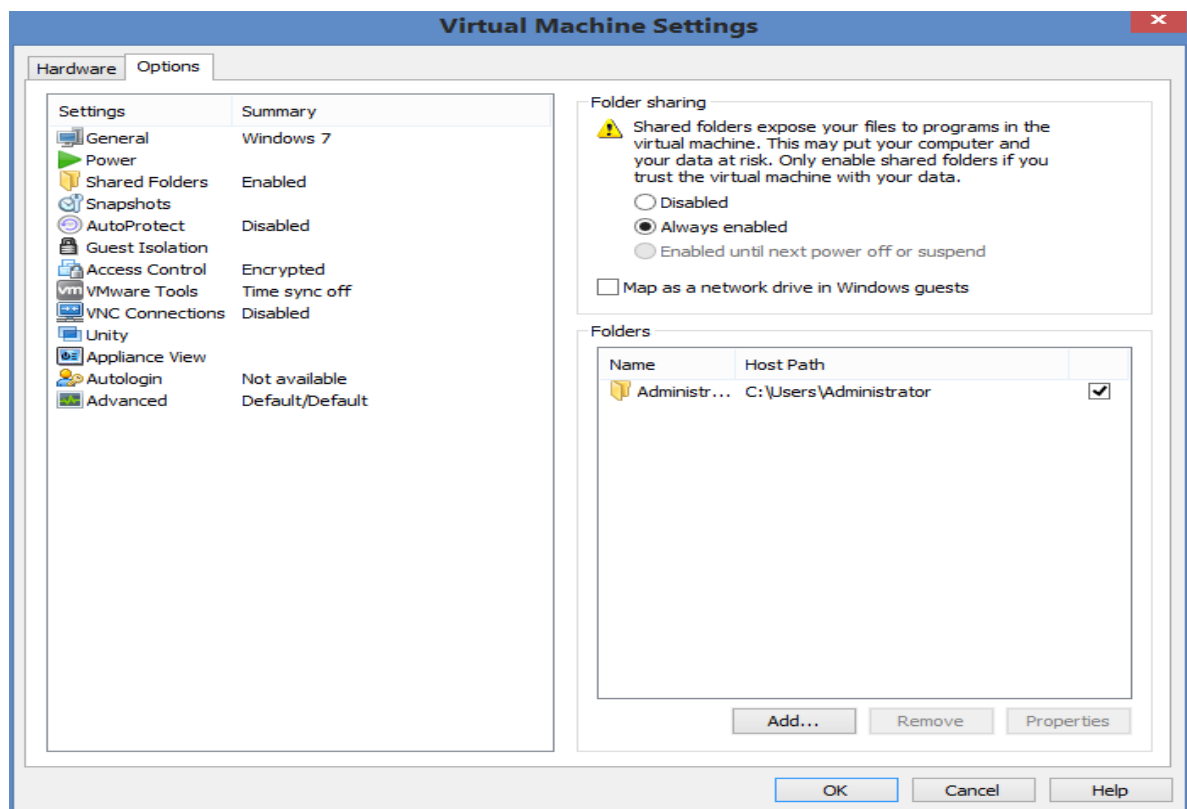
Suspend Guest - სტუმარი ოპერაციული სისტემის მუშაობის დაპაუზება;

Start Up Guest - სტუმარი ოპერაციული სისტემის გაშვება;

Restart Guest - სტუმარი ოპერაციული სისტემის გადატვირთვა;

კვების უფრო კორექტული მართვისთვის მისასაღმებელია **Power Off**-ის შეცვლა **Shut Down Guest**-ით, ოპერაციული სისტემის კორექტული გამორთვისთვის, თუ უცებ შემთხვევით დაჭერილ იქნა ვირტუალური კომპიუტერის გამორთვის ღილაკზე.

3) **Shared Folders** - საქალაქდებთან საერთო წვდომა. მოცემული ფუნქცია საშუალებას იძლევა შესრულდეს საქალაქდის გადამისამართება ქსელური პროტოკოლის გამოყენების გარეშე. იმისათვის, რომ გამოვიყენოთ ეს ფუნქცია, აუცილებელია შესრულდეს **Vmware Tools** -ის წინასწარ დაყენება სტუმარ ოპერაციულ სისტემაზე.



სურ.3.5.1. 12

ჯგუფი **Folder sharing** (სურ.):

- **Disable** - მიუწვდომელია;
- **Always enabled** - ყოველთვის ხელმისაწვდომია;
- **Enabled until next power off or suspend** – გაიხსნას წვდომა შემდგომ გათიშვამდე ან დაპაუზებამდე.

Map as a network drive in Windows guest - ჩაერთოს როგორც ქსელური დისკი **Windows** სტუმარ ოპერაციულ სისტემაში.

ჯგუფი საქაღალდეები (**Folders**). სათანადოდ ამ ჯგუფისა იქნება განთავსებული ფიზიკური კომპიუტერის საქაღალდის მონიტორების წერტილი ვირტუალური მანქანის შიგნით. მოდით დავამატოთ კატალოგი სტუმარი ოპერაციული სისტემის შიგნით.

ენიშნავთ პუნქტს „**Always enabled**“ და „**Map as a network drive in Windows guest**“ და შემდეგ ვაწვებით ღილაკზე **Add**. გაეშვება საქაღალდის საერთო წვდომის ოსტატი ვაწვებით **Next** ღილაკს, მომდევნო ფანჯარაში ვუთითებთ გასაზიარებელი საქაღალდის სრულ მისამართს და სახელს, რომლითაც გამოჩნდება საქაღალდე სტუმარ ოპერაციულ სისტემაში.

მომდევნო ეტაპზე უნდა განისაზღვროს საქაღალდესთან წვდომის უფლებები:

- **Enable this share** – წვდომის დაშვება/აკრძალვა;
- **Read-only** - მხოლოდ დათვალიერების რეჟიმი.

ასე გამოიყურება უკვე გაზიარებული საქაღალდე სტუმარი ოპერაციული სისტემის შიგნით (სურ. 3.5.1.13):



სურ.3.5.1. 13

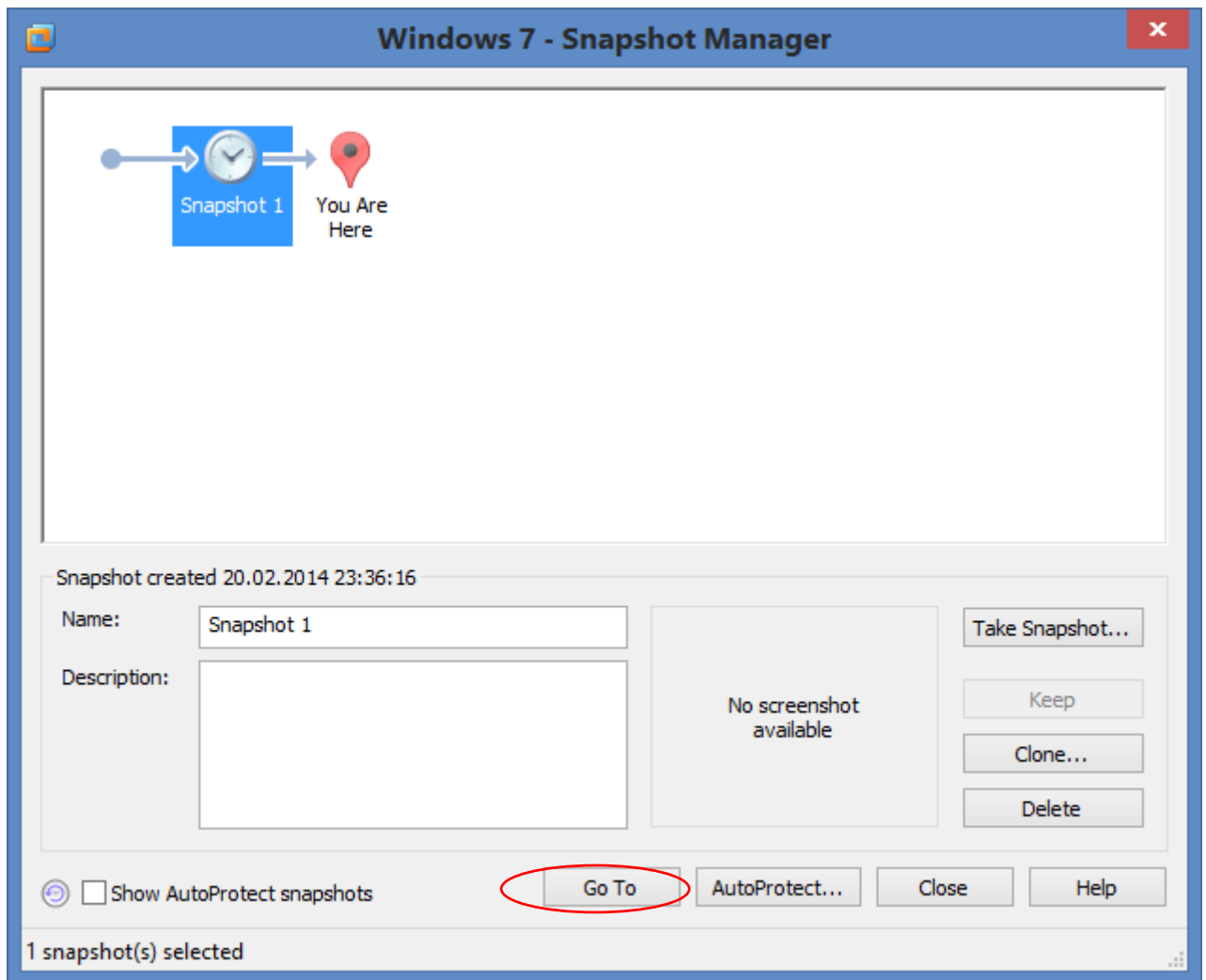
3.6. უსაფრთხოების უზრუნველყოფა ვირტუალურ გარემოში

Snapshots - კადრები (აღდგენის წერტილები):

ეს ფუნქცია შექმნილია იმისთვის რომ შემდგომში შესრულდეს იმ მდგომარეობის აღდგენა, როცა შეიქმნა ეს კადრი. ე.ი არსებობს ვირტუალური მანქანის სარეზერვო ასლი. მოცემული ფუნქცია აქტუალურია, თუ მაგალითად ჩვენ გვინდა დავაყენოთ რომელიმე პროგრამა ფიზიკურ კომპიუტერზე და ფუნქციონირების შესამოწმებლად ვიყენებთ სტუმარ ოპერაციულ სისტემას. კადრის აღდგენის შემდეგ სტუმარი ოპერაციული სისტემა უბრუნდება ძველ მდგომარეობას. აღსანიშნავია რომ რეესტრი და თავისუფალი ადგილი მყარ დისკზე იქნება ისევე, როგორც იყო კადრის შექმნის დროს. კადრის ფუნქციის შესრულება ასევე მოსახერხებელია იმ შემთხვევაშიც თუ გვინდა შესრულდეს სარეზერვო ასლის შექმნა ვირტუალური მანქანის კვებიდან გათიშვის შემდეგ, და შემდეგ სენსზე თუ ყველაფერი ისე არ წავიდა როგორც ვგეგმავდით, დავუბრუნდეთ წინა მდგომარეობას. მოცემული ფუნქცია არის უსაფრთხოების დაცვის ძალიან კარგი საშუალება.

შემდგომში, კადრის მდგომარეობის დაბრუნების საშუალებას გვაძლევს მხოლოდ ორი მოქმედება:

- 1) დავყოთ კადრები თარიღის და დასახელების მიხედვით;
- 2) დავაჭიროთ ღილაკზე „Go To“



სურ.3.5.1. 14

არ უნდა დაგვავიწყდეს შევასრულოთ კადრების შექმნა ავტომატურ ან ხელით რეჟიმში, რადგან ისინი ეკონომიას უკეთებენ თქვენს დროს და „ნერვებს“. გვაქვს ოთხი რეჟიმი (სურ.3.5.1.14):

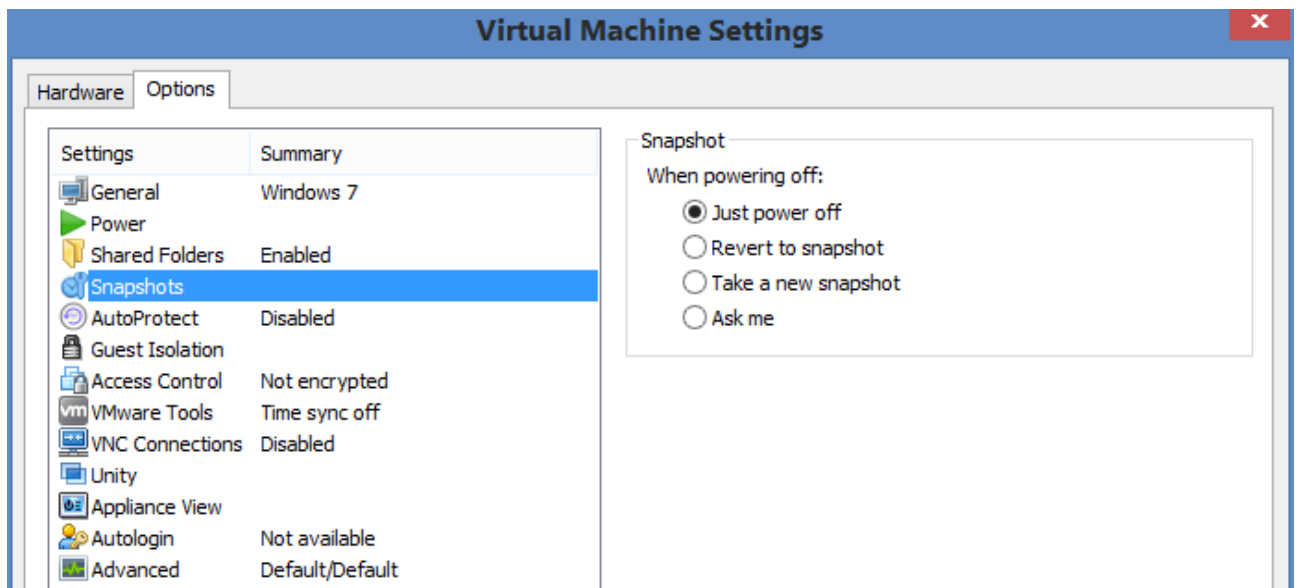
Just power off – გამოირთოს ვირტუალური კომპიუტერი კადრებში რაიმე ცვლილების გარეშე;

Revert to snapshot – შესრულდეს კადრის აღდგენა. ვირტუალური მანქანის მიმდინარე მდგომარეობა დაბრუნდეს კადრის შექმნის დროზე. როცა აბრუნებთ კადრს, თქვენ აბრუნებთ მეხსიერების მდგომარეობას, პარამეტრებს და ვირტუალური მანქანის დისკებს, იმ მდგომარეობაში როცა შეიქმნა კადრი;

Take a new snapshot – კადრი ავტომატურად შეიქმნება გათიშვის მომენტში. შეიქმნება ვირტუალური მანქანის ახალი კადრი მას შემდეგ რაც გამოირთვება კვება. კადრი ჩნდება

კადრების მართვის პანელში (**Snapshot manager**). კადრის დასახელება დაემთხვევა იმ თარიღს და დროს, როცა მოხდა ვირტუალური მანქანის გათიშვა.

Ask me - გათიშვისას შეგვეკითხოს, თუ რომელი მოქმედების შესრულება გვინდა.



სურ.3.5.1. 15

4) **AutoProtect** - ავტოდაცვის პარამეტრების მომართვა (სურ.3.5.1.15):

ავტომატური დაცვის ფუნქცია ინახავს ვირტუალური მანქანის მდგომარეობას, ქმნის რა კადრებს დროის განსაზღვრულ მონაკვეთში. ასევე შეგვიძლია სურვილისამებრ მივუთითოთ კადრის შექმნის ნებისმიერი დრო.

გვაქვს ავტომატური დაცვის შემდეგი პარამეტრები:

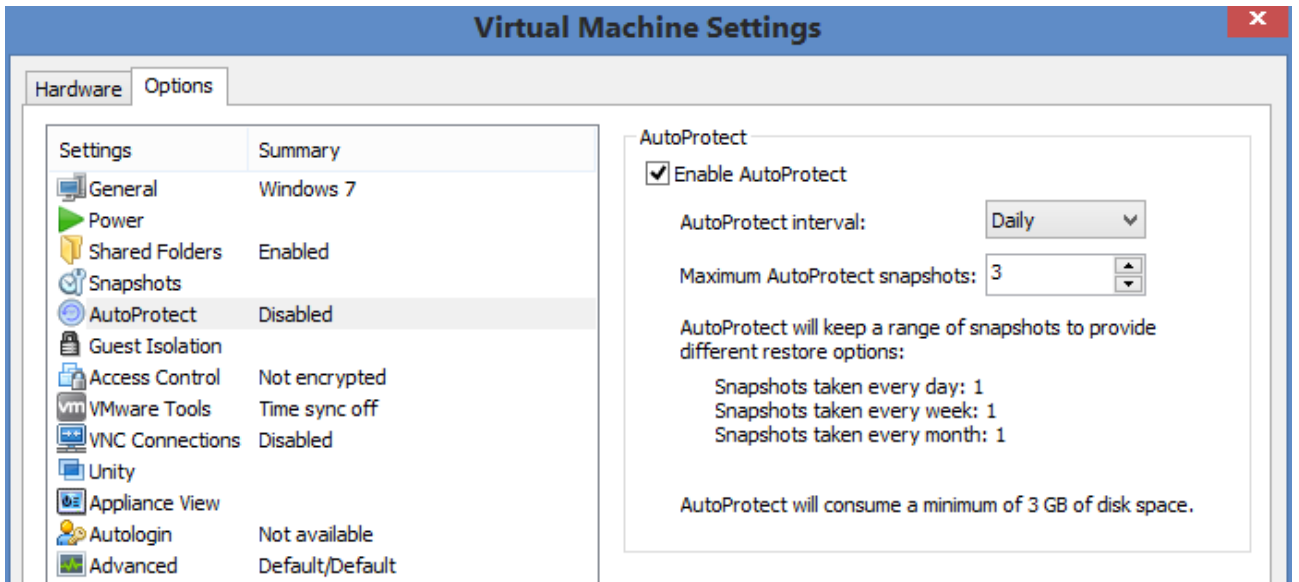
Enable AutoProtect – ფუნქციის ავტომატური ჩართვა;

AutoProtect interval - კადრის შექმნის ინტერვალი;

- **Half-Hourly** - ყოველ ნახევარ საათში;
- **Hourly** – ყოველ საათში;
- **Daily** - ყოველდღე.

Maximum AutoProtect Snapshots - კარდთა შექმნის მაქსიმალური რაოდენობა.

შენიშვნა: გაითვალისწინეთ, რომ კადრთა რაოდენობის გაზრდით იზრდება მყარი დისკის მოცულობაზე მოთხოვნაც, ამიტომ არაა რეკომენდებული ბევრი აღდგენის წერტილის (**Snapshot**) შექმნა.



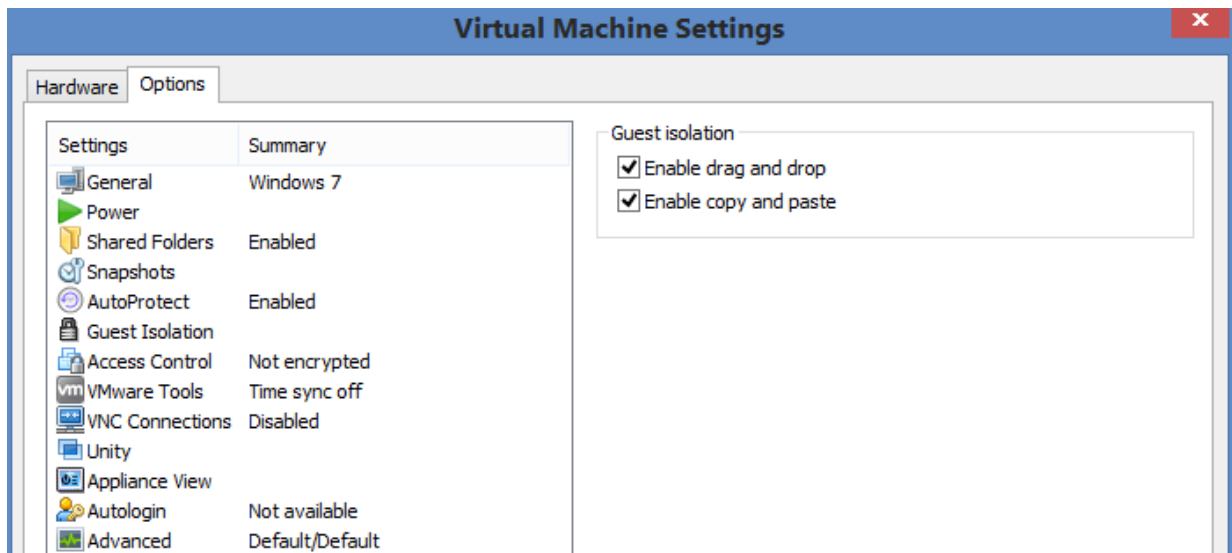
სურ.3.5.1. 16

5) **Guest Isolation** - სტუმარი ოპერაციული სისტემის იზოლირება (სურ.3.5.1.16):

- **Enable drag and drop** - სტუმარ ოპერაციულ სისტემაში ფაილების გადატანის ფუნქციის ჩართვა/გამორთვა. შეგვიძლია ჩვენთვის სასურველი ფაილის ან საქაღალდის გადატანა მაუსის საშუალებით (დააჭირეთ სასურველ დოკუმენტს მაუსის მარცხენა ღილაკით და ხელის აულებლად გადაადგილეთ) ჰოსტ ოპერაციული სისტემიდან სტუმარ ოპერაციულ სისტემაში ან პირიქით;

- **Enable copy and paste** - ოპერატიულ მეხსიერებაში ტექსტის კოპირება/ჩასმის ფუნქციის ჩართვა/გამორთვა; ამ შემთხვევაში რაიმე საქაღალდის ან ფაილის დაკოპირებისას შეიქმნება საერთო გაცვლის ბუფერი ფიზიკურ და ვირტუალურ ოპერაციულ სისტემას შორის, რაც საშუალებას მოგვცემს ჩავდგათ ფაილი/საქაღალდე სასურველ ოპერაციულ სისტემაში.

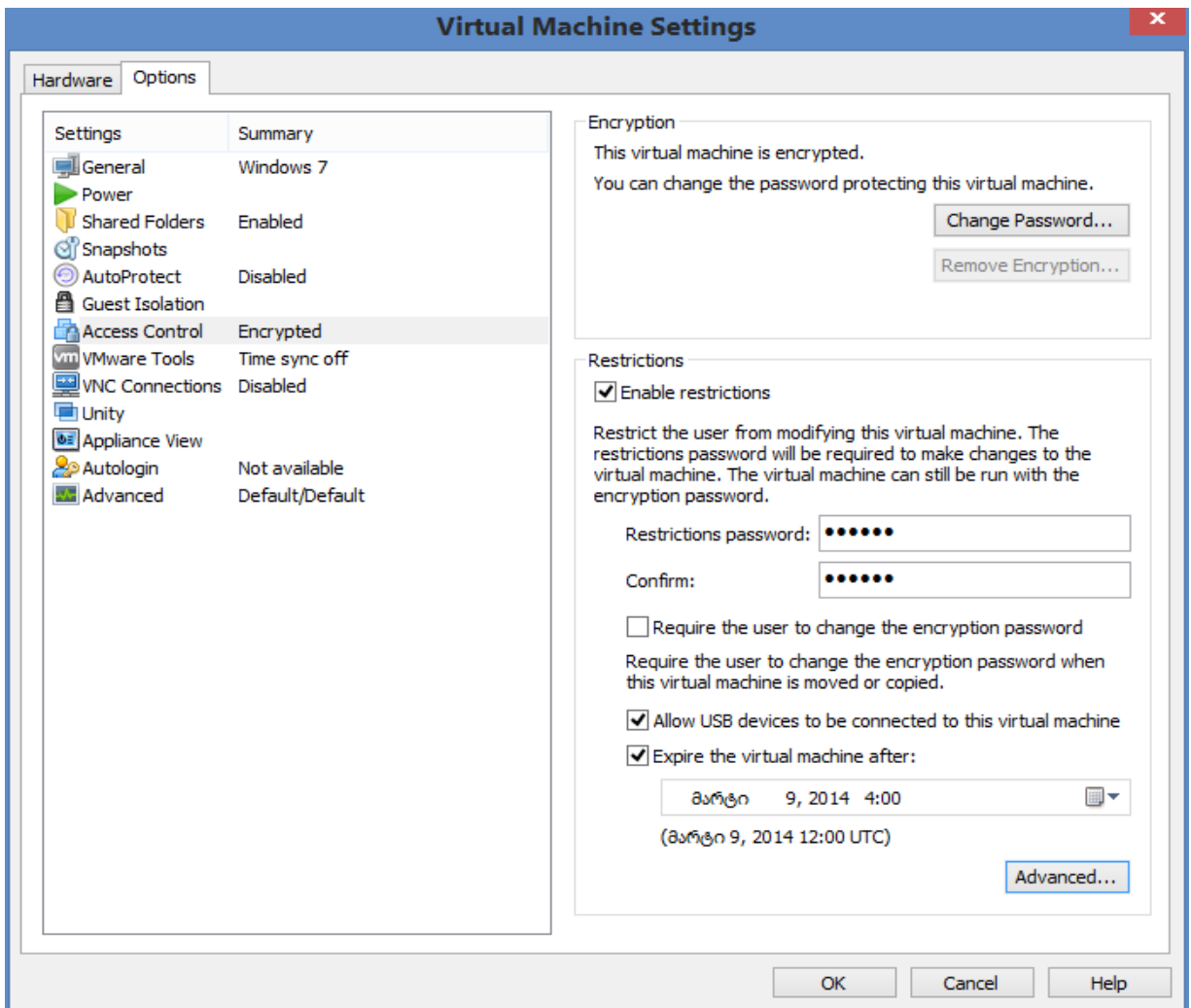
Guest Isolation ფუნქციის გამოყენება შესაძლებელია მხოლოდ **VMware Tools** - უტილიტების დაყენების შემდეგ.



სურ.3.5.1. 17

6) **Encryption** - შიფრაცია:

ვირტუალური მანქანისთვის შეგვიძლია შიფრირების ფუნქციის გამოყენება. ამისათვის საჭიროა დავაჭიროთ **Encrypt** ღილაკს და შევიყვანოთ პაროლი.



სურ.3.5.1. 18

ვირტუალური მანქანის დაშიფრულ რეჟიმში გაშვების შემდეგ, აუცილებელია პაროლის შეტანა, იმისთვის რომ გავხსნათ ვირტუალური მანქანა ან მოვხსნათ შიფრაცია მასზე. სამუშაო სადგურზე ჩანს დაშიფრული ვირტუალური მანქანა საკეტის ნიშნით სანამ არ შევიყვანთ პაროლს. ვირტუალური მანქანის შიფრაცია გამოიყენება იმ შემთხვევაშიც, თუ გვინდა დავიცვათ სტუმარი ოპერაციული სისტემის მონაცემები. დაუშიფრველ ვირტუალურ მანქანაზე შესაძლებელია გაიხსნას მიმაგრებული ვირტუალური მყარი დისკი და იქიდან მოხდეს მონაცემების მიტაცება.

დაშიფრის შემდეგ აქტიურდება განყოფილება აკრძალვა (**Restrictions**). ამ ფუნქციის საშუალებით შეგვიძლია ავუკრძალოთ მომხმარებელს ვირტუალური მანქანის პარამეტრების შეცვლა. აკრძალვის პაროლი საჭირო იქნება ვირტუალურ კომპიუტერში რაიმე ცვლილების შესრულების დროს. ვირტუალური მანქანის მუშაობაზე გაშვება ჯერ კიდევ დაშიფრვის პაროლით ხდება.

Restrictions ჯგუფში წარმოდგენილია ოთხი პუნქტი (სურ.3.5.1.18):

- **Enable restrictions** – აკრძალვის ჩართვა/გამორთვა;
- **Require the user to change the encryption password** – მოეთხოვოს მომხმარებელს

შეცვალოს დაშიფრვის პაროლი;

- **Allow USB devices to be connected to this virtual machine** - დაშვებული იქნას, რომ USB მოწყობილობები იყვნენ დაკავშირებული ვირტუალურ კომპიუტერთან.

- **Expire the virtual machine after** - ამ პარამეტრის ჩართვის შემდეგ ჩვენ შეგვეძლება დროის ლიმიტის დაწესება ვირტუალური მანქანისთვის, რომლის ამოწურვის შემდეგ ის აღარ იმუშავებს. **Advanced Restrictions** ფანჯარაში შესაძლებელია იმ ტექსტის შეყვანა, რომელიც გვამცნობს თუ რამდენი დღე დარჩა ვირტუალური მანქანის ლიმიტის ამოწურვამდე.

7) **Vmware Tools** – Vmware უტილიტები. ამ ფუნქციაზე ზემოთ უკვე გვქონდა საუბარი. რაც შეეხება Vmware Tools-ის განახლებას, გვაქვს სამი რეჟიმი:

- **Update manually (do nothing)** - განახლება მოთხოვნის მიხედვით;
- **Update automatically** - ავტომატური განახლება;
- **Use application default (currently update automatically)** - გამოყენებულ იქნას

პროგრამის გლობალური პარამეტრები (საწყისად აყენია ხელით განახლება).

იმისათვის რომ შევცვალოთ გლობალური პარამეტრები, უნდა გამოვიძახოთ **Edit > Preferences > Updates** ბრძანება, რომელსაც შემდგომში განვიხილავთ.

8) **VNC connections** - შეერთება VNC viewer პროგრამის საშუალებით:

VNC viewer (Virtual Network Computing) - ეს არის პროგრამა, რომელიც გამოიყენება ოპერაციული სისტემის დაშორებული მართვისთვის. ამ ლაბორატორიულში არ გვექნება საუბარი თუ საიდან უნდა გადმოწეროთ და დააყენოთ ეს პროგრამა დაშორებულ კომპიუტერზე და კლიენტზე. გვაქვს სამი ბრძანება:

- **Enable VNC Connections** - დავუშვათ ან აკრძალოთ VNC კავშირი;
- **Port** - დაკავშირების პორტი, ავტომატურად შემოთავაზებულია **5900**;
- **Password** - კავშირის პაროლი.

9) **Unity** - თავსებადობა:

განყოფილება „Unity window borders“ მოიცავს შემდეგ ბრძანებებს:

- **Show borders** – ფანჯრის საზღვრების დამალვა/გამოჩენა;
- **Show badges** – დამატებითი ღილაკების დამალვა/გამოჩენა;
- **Use a custom color in window borders** – მომხმარებლის ფერების გამოყენება ფანჯრის საზღვრებზე; **Choose color** ღილაკზე დაჭერით შეგვიძლია ავირჩიოთ საზღვრების სასურველი ფერი.

10) **Appliance View** - ვირტუალურ კომპიუტერში შეგვიძლია მივუთითოთ ინფორმაცია ვერსიის და ავტორის შესახებ, ასევე გავხსნათ **HTTP**-წვდომის პორტი. ამ განყოფილებაში მოცემული გვაქვს სამი შესავსები ველი:

- **Version** – ვერსია;
- **Author** – ავტორი;
- **Access port inside virtual machine** - ვირტუალურ კომპიუტერში წვდომის პორტი.

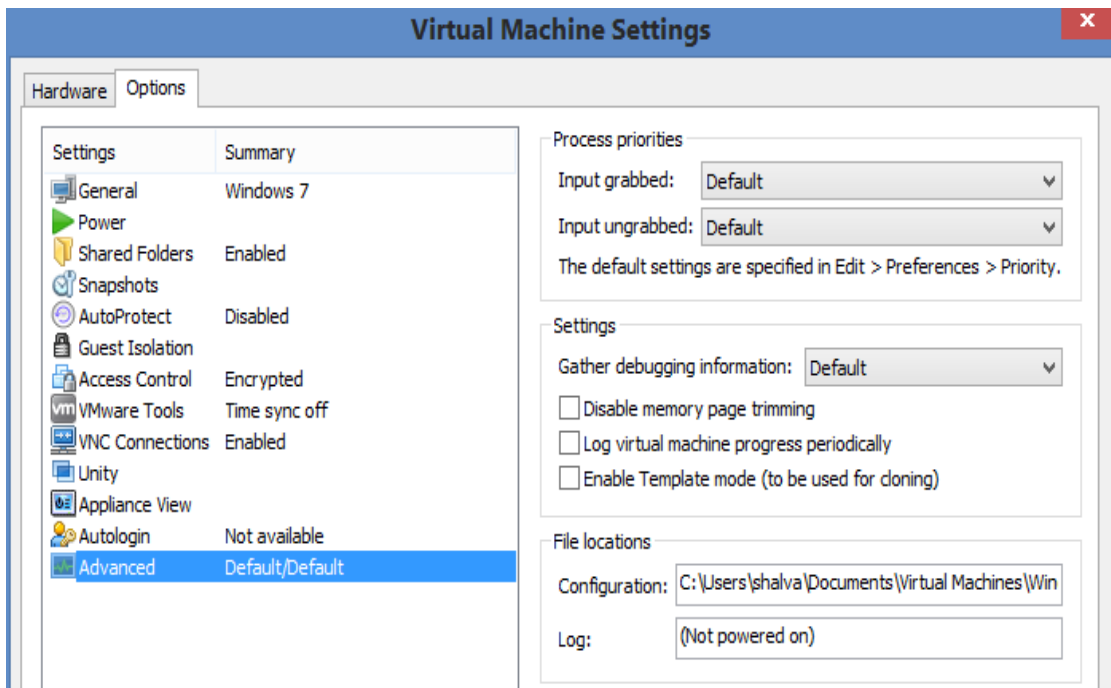
11) **Autologon** - ავტომატური შესვლა სტუმარ ოპერაციულ სისტემაში.

ჩვენ შეგვიძლია მოვმართოთ ფუნქცია ვირტუალურ კომპიუტერში ავტომატურად შესასვლელად. ეს ფუნქცია მუშაობს მხოლოდ **Windows 2000**-ზე ან უფრო ძველ სტუმარ ოპერაციულ სისტემებში. ავტომატური შესვლისთვის აუცილებელია დაცული იყოს შემდეგი პირობები:

- ვირტუალური კომპიუტერი უნდა იყოს ჩართული;
- ლოკალურ კომპიუტერზე უნდა გვქონდეს მოქმედი საადრიცხო ჩანაწერი;
- სტუმარ ოპერაციულ სისტემაში უნდა იყოს დაყენებული **Vmware Tools** უტილიტის ბოლო ვერსია.

13) **Advanced** - დამატებითი პარამეტრები.

ამ ფუნქციით შეგვიძლია განვსაზღვროთ პროცესების პრიორიტეტი. საწყისად მოქმედებს გლობალური პარამეტრები, სურვილისამებრ შეგვიძლია შევცვალოთ ისინი ყოველი ვირტუალური მანქანისთვის (სურ. 3.5.1.19).



სურ.3.5.1. 19

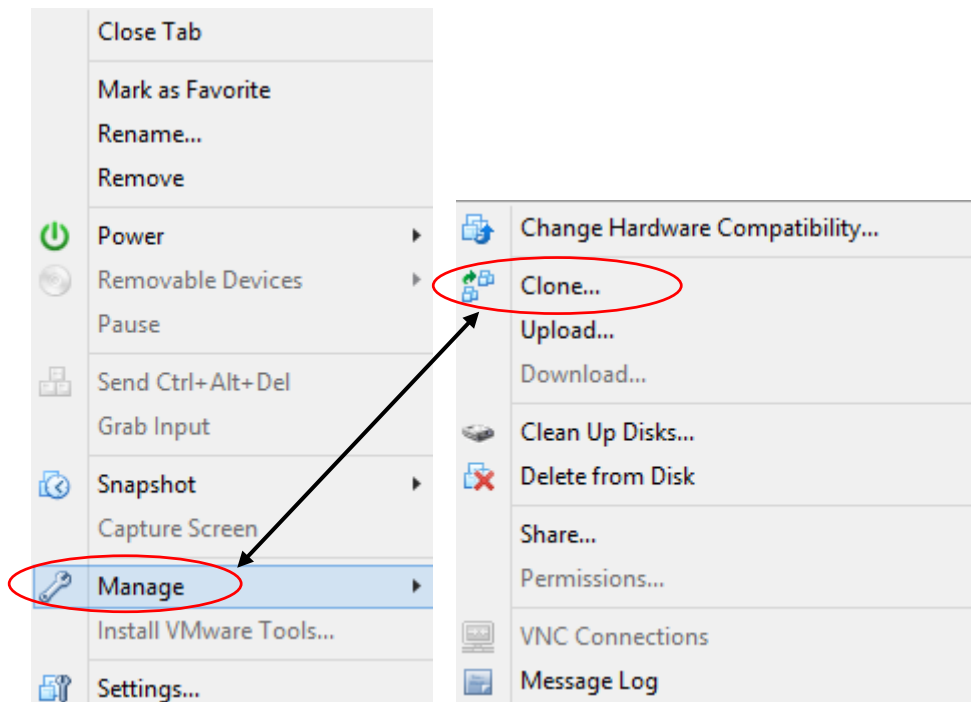
ვირტუალური მანქანის სარეზერვო ასლის შექმნა (Clone)

გარდა ზემოთ აღწერილი ფუნქციებისა, ვირტუალურ მანქანას აქვს ერთი მეტად მნიშვნელოვანი ფუნქცია - მუშაობა კლონებთან (**Clone**). მისი საშუალებით მარტივად და დროის მცირე მონაკვეთში შეგვიძლია ვირტუალური მანქანის სარეზერვო ასლის შექმნა. სარეზერვო ასლში ვირტუალური მანქანის პარამეტრებთან ერთად შევა ოპერაციული სისტემა და მასზე ინსტალირებული ყველა პროგრამა თუ უტილიტა.

ვირტუალური მანქანის, ვირტუალური ოპერაციული სისტემის ან მასში არსებული რაიმე პროგრამული უზრუნველყოფის დაზიანების შემთხვევაში წამებში შეგვიძლია კლონირებული ვირტუალური მანქანის ჩართვა და არ მოგვიწევს სისტემის გამართვა თავიდან, რომელსაც დღეები და შესაძლოა თვეც კი დასჭირდეს. ამ ფუნქციის გამოსაყენებლად უბრალოდ გვჭირდება მეტი მოცულობა მყარ დისკზე.

ვირტუალური მანქანის ასლის შესაქმნელად მივყვით ბრძანებათა თანმიმდევრობას:

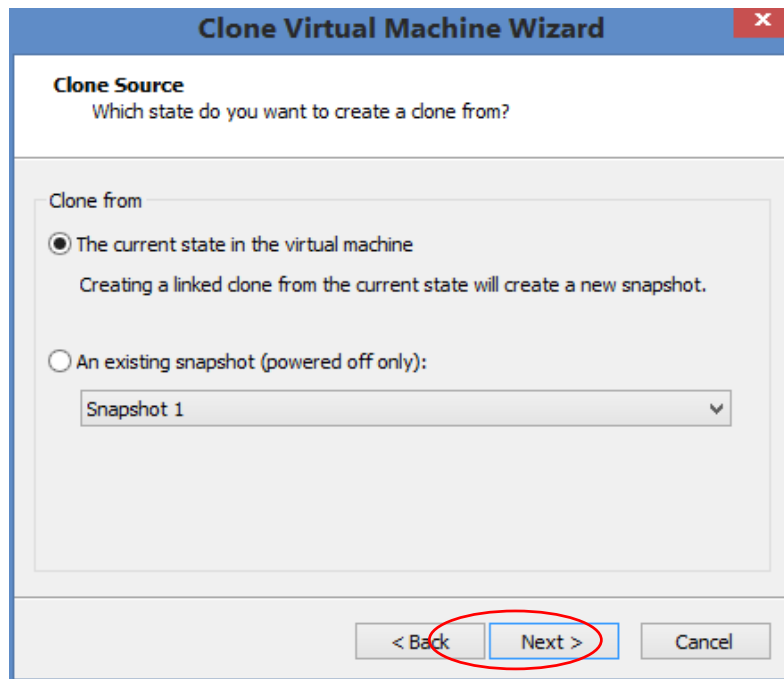
ღეგაპი - VMware Workstation პროგრამის მთავარი მენიუს **Library** განყოფილებაში, დავაჭიროთ მაუსის მარჯვენა ღილაკით იმ ოპერაციულ სისტემაზე, რომლის ასლის შექმნაც გვინდა. გამოსულ კონტექსტურ მენიუში ჩამოვშალოთ **Manage** პუნქტი და ავირჩიოთ ბრძანება **Clone** (სურ. 3.5.1.20):



სურ.3.5.1. 20

II ეტაპი - გამოსულ ფანჯარაში ვაწვებით **Next** ღილაკს;

III ეტაპი - ამ ეტაპზე უნდა დავაკონკრეტოთ ვირტუალური მანქანის, რომელი მდგომარეობის მიხედვით გვინდა ასლის შექმნა, შემოთავაზებული გვაქვს ორი ვარიანტი: ა) **The current state in the virtual machine** - ვირტუალური მანქანის მიმდინარე მდგომარეობის მიხედვით; ბ) **An existing snapshot (powered off only)** - არსებული აღდგენის წერტილის (**Snapshot**) მიხედვით. რადგან ჩვენ გვინდა მიმდინარე მდგომარეობის სარეზერვო ასლი (**Clone**), ვირჩევთ პირველ ვარიანტს და ვაწვებით **Next** ღილაკს (სურ. 3.5.1.21):



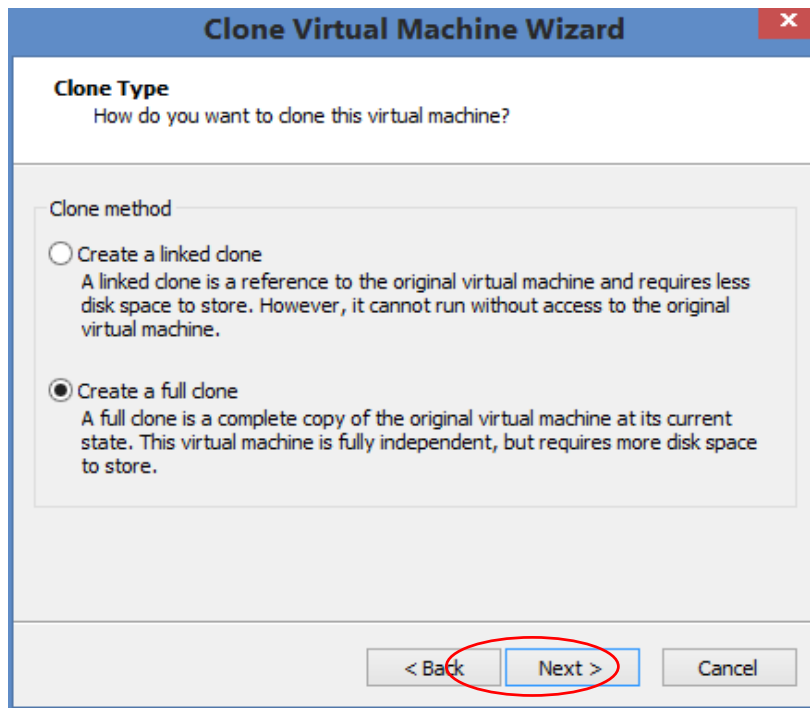
სურ.3.5.1. 21

სურ.

IV ეტაპი - ასლის შექმნის მეთოდი (**Clone method**). ამ შემთხვევაშიც გვაქვს ორი ვარიანტი:

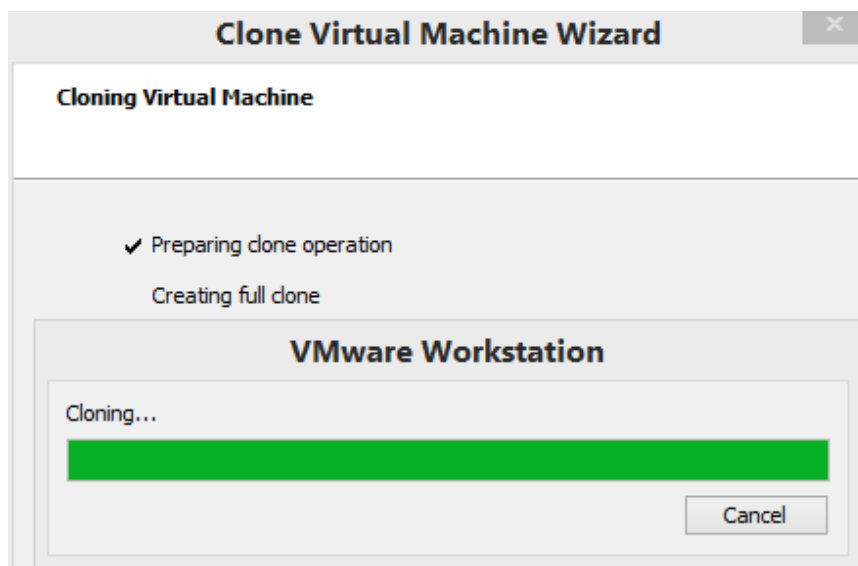
ა) **Create a linked clone** (დაკავშირებული კლონის შექმნა) - დაკავშირებული კლონი არის ვირტუალური მანქანის ასლი, რომელიც ანაწილებს მშობელი ვირტუალური მანქანების ვირტუალურ დისკებს ეტაპობრივად, რაც იძლევა მყარ დისკზე მეხსიერების ეკონომიას და საშუალებას აძლევს ვირტუალურ მანქანებს გამოიყენონ პროგრამული უზრუნველყოფის იგივე აპარატურა. დაკავშირებული კლონი შექმნილია მშობელი ვირტუალური მანქანის აღდგენის წერტილიდან (**Snapshot**). ყველა ფაილი, რომელიც ხელმისაწვდომია მშობელ ვირტუალურ მანქანაზე, კადრის (**Snapshot**) შექმნის მომენტში ისევ რჩებიან ხელმისაწვდომნი დაკავშირებული კლონისთვის (**Linked Clone**). ვირტუალურ დისკზე მიმდინარე ცვლილებები არ ახდენს გავლენას დაკავშირებულ კლონზე და პირიქით, დაკავშირებული კლონის დისკზე ცვლილება გავლენას არ ახდენს მშობელზე.

ბ) **Create a full clone** - სრული კლონი არის ორიგინალი ვირტუალური მანქანის მიმდინარე მდგომარეობის ზუსტი ასლი. ეს ვირტუალური მანქანა არის მთლიანად დამოუკიდებელი, მაგრამ მოითხოვს მეტ სივრცეს მყარ დისკზე.



სურ.3.5.1. 22

უცვლად - ვარქმევთ სახელს კლონირებულ ვირტუალურ მანქანას და ვუთითებთ მისი განთავსების ადგილს ან ვტოვებთ ორივე პარამეტრს უცვლელად. ვაწვევით **Next** ღილაკს. დაიწყება ასლის შექმნის პროცესი. მისი დასრულების დრო დამოკიდებულია ვირტუალურ მანქანაში არსებული ფაილების ზომაზე.



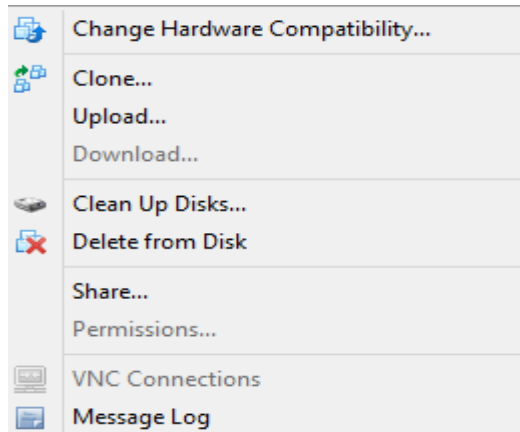
სურ.3.5.1. 23

პროცესის დასრულების შემდეგ ვაჭერთ **Close** ღილაკს. ამით ვირტუალური მანქანის ასლის შექმნა დამთავრებულია.

ვირტუალური მანქანის წაშლა

იქმნება სიტუაცია, როდესაც უბრალოდ აღარ გვჭირდება შექმნილი ვირტუალური მანქანა ან დაზიანებულია ან კიდევ დიდ ადგილს იკავებს მყარ დისკზე და გვინდა მისი წაშლა ადგილის გამოთავისუფლების მიზნით.

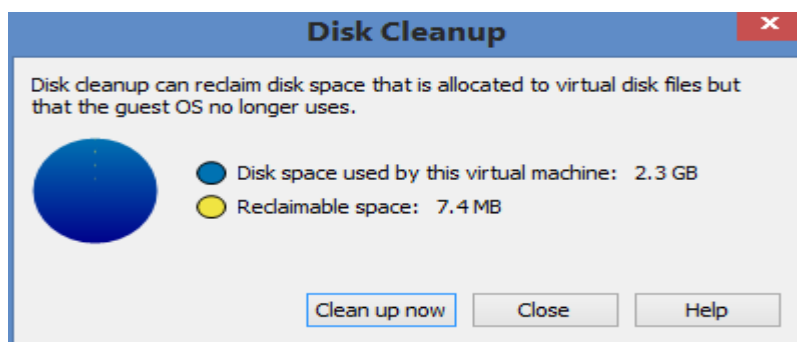
ამისათვის წასაშლელ ვირტუალურ მანქანაზე გამოვიძახოთ კონტექსტური მენიუ და ჩამოვშალოთ **Manage** პუნქტი.



სურ.3.5.1. 24

გამოვა **Manage** პუნქტის ქვემენიუ (სურ. 3.5.1.24), საიდანაც ჩვენ გვჭირდება მხოლოდ ორი ბრძანება:

- **Clean Up Disks...** - მოცემული **Disk Cleanup** ბრძანება მყარი დისკიდან დააბრუნებს იმ სივრცეს, რომელიც გამოყოფილი იყო ვირტუალური დისკის ფაილებისთვის, და რომელსაც სტუმარი ოპერაციული სისტემა აღარ გამოიყენებს. დააჭირეთ **Clean up now** ღილაკს (სურ. 1.42) ადგილის გამოსათავისუფლებლად;



სურ.3.5.1. 25

Delete from Disk - მოცემული ბრძანებით მთლიანად წაიშლება ვირტუალური მანქანა მყარი დისკიდან. გამოთავისუფლდება მყარი დისკის ის მოცულობა, რომელიც თავის დროზე გამოყავით ვირტუალური ოპერაციული სისტემის დასაყენებლად.

პრაქტიკული სავარჯიშო

1. შეასრულეთ Hyper-V-ს ინსტალაცია და კონფიგურაცია, ვირტუალური ქსელების კონფიგურაცია, ვირტუალური მანქანების დამატება, მონიტორინგი და ოპტიმიზაცია;
2. განახორციელეთ ESX სერვერის ინსტალაცია და კონფიგურაცია, vCenter სერვერის ინსტალაცია და კონფიგურაცია, ვირტუალური ქსელების გამართვა, ვირტუალური საცავის გამართვა, ESXi ფაიერვოლის გამართვა, ESXi რეჟიმისა და იზოლაციის გამართვა, ESXi და Active Directory-ის ინტეგრაცია, VMware კომპონენტების დაყენება;
3. შეასრულეთ VMware Workstation-ის ინსტალაცია, ვირტუალური მანქანის შექმნა, ვირტუალური მანქანის პარამეტრების კონფიგურაცია, ქსელის მართვის ორგანიზაცია ვირტუალურ მანქანებს შორის, უსაფრთხოების უზრუნველყოფა ვირტუალურ გარემოში (Snapshot, Encryption), ვირტუალური მანქანის სარეზერვო ასლის შექმნა (Clone).

ცოდნის შეფასება

სტუდენტებს მიეცემათ პრაქტიკული დავალება

- შეასრულონ Hyper-V-ს ინსტალაცია და კონფიგურაცია, ვირტუალური ქსელების კონფიგურაცია, ვირტუალური მანქანების დამატება, მონიტორინგი და ოპტიმიზაცია;
- განახორციელონ ESX სერვერის ინსტალაცია და კონფიგურაცია, vCenter სერვერის ინსტალაცია და კონფიგურაცია, ვირტუალური ქსელების გამართვა, ვირტუალური საცავის გამართვა, ESXi ფაიერვოლის გამართვა, ESXi რეჟიმისა და იზოლაციის გამართვა, ESXi და Active Directory-ის ინტეგრაცია, VMware კომპონენტების დაყენება;
- შეასრულონ VMware Workstation-ის ინსტალაცია, ვირტუალური მანქანის შექმნა, ვირტუალური მანქანის პარამეტრების კონფიგურაცია, ქსელის მართვის ორგანიზაცია ვირტუალურ მანქანებს შორის, უსაფრთხოების უზრუნველყოფა ვირტუალურ გარემოში (Snapshot, Encryption), ვირტუალური მანქანის სარეზერვო ასლის შექმნა (Clone).

შემფასებელი აკვირდება შესაფასებელ პირის მუშაობას პროფესიული სტანდარტით (პროგრამით / მოდულით) განსაზღვრული ამოცანების შესრულების პროცესში. დაკვირვება ხორციელდება კომპიუტერებით აღჭურვილ ლაბორატორიაში, სადაც შესაფასებელი პირი პრაქტიკულ საქმიანობას ეწევა. შემფასებელმა წინასწარ უნდა

დაგეგმოს დაკვირვების პროცესი, იმის დასადგენად, თუ რამდენად სწორად იყენებს შესაფასებელი პირი ცოდნას, უნარებსა და ყველა რესურსს შედეგის მისაღწევად.

შეფასება განხორციელდება პროცესზე დაკვირვებით, წინასწარ განსაზღვრული შეფასების ინდიკატორების საფუძველზე.

დავალების ნიმუში და შეფასების რუბრიკა

პროცესზე დაკვირვება

- ✚ შეასრულოს სხვადასხვა საკომუნიკაციო და ინფრასტრუქტურის მართვის პროგრამების ინსტალაცია
- ✚ გამოიყენოს დაყენებული პრაქტიკული ამოცანებისთვის (ელ.ფოსტის სთორების და მეილბოქსების შექმნა, ტექსტური, ვიდეო- და აუდიო კომუნიკაციის მართვა, IT-ინფრასტრუქტურის მართვა)

სწავლის შედეგი	N	დასახელება	შეფასება	
			კი	არა
კლიენტებისა და სერვერების ვირტუალიზაცია	1.	შეასრულა Hyper-V-ს ინსტალაცია და კონფიგურაცია		
	2.	შეასრულა ვირტუალური ქსელების კონფიგურაცია		
	3.	შეასრულა ვირტუალური მანქანების დამატება, მონიტორინგი და ოპტიმიზაცია;		
	4.	შეასრულა ESX-ის ინსტალაცია და კონფიგურაცია		
	5.	შეასრულა vCenter სერვერის ინსტალირებას და კონფიგურირებას		
	6.	შეასრულა ESX-ის ქსელისა და მეხსიერების ინსტალირებას და კონფიგურირებას vCenter სერვერის გამოყენებით		
	7.	შეასრულა ვირტუალური საცავის გამართვა და მისი მართვა		
	8.	შეასრულა VMware კომპონენტების დაყენება		
	9.	შეასრულა VMware Workstation-ის ინსტალაცია, ვირტუალური მანქანის შექმნა,		
	10.	შეასრულა უსაფრთხოების უზრუნველყოფა ვირტუალურ გარემოში		

სწავლის შედეგი ჩაითვლება მიღწეულად თუ სტუდენტმა შეძლო შედეგის მინიმუმ 8

პუნქტის შესრულება

4. ვებ, ფაილური და მონაცემთა ბაზის სერვერების გამართვა

4.1. ვებ-სერვერული ინფრასტრუქტურის აწყობა და მართვა

4.1.1. ვებ-ინფრასტრუქტურის აგებულება

თანამედროვე ელექტრონულ ინფორმაციულ პროცესებში ვებ-ტექნოლოგიის როლი განუხრელად იზრდება. მე-20 საუკუნის 40-იან წლებში რამდენიმე მეცნიერის (ვანევარ ბუში, ტედ ნელსონი, დაგლას ენგელბარტი) მიერ ჰიპერტექსტური ინფორმაციული მოდელის შექმნამ, ხოლო 1990 წელს CERN-ში ტიმ ბერნერს-ლის მიერ World Wide Web (WWW)-ტექნოლოგიის დამუშავებამ უდიდესი ციფრული ინფორმაციული სივრცის - მსოფლიო აბლაზუდის შექმნას ჩაუყარა საფუძველი. დღეს როგორც გლობალური, ასევე ლოკალური (კორპორაციული) ინფორმაციული სისტემების დიდი ნაწილი ვებ-ტექნოლოგიის საფუძველზე იქმნება, ხოლო ძველი, **დესკტოპ-აპლიკაციების** ახალი ვერსიებიც, როგორც წესი, იმავე მიმართულებით ვითარდებიან.

მე-20 საუკუნის 90-იანი წლების მსოფლიო აბლაზუდა ინფორმაციული კონტენტის მხოლოდ გამოყენებას (ვებ-გვერდის წაკითხვა, ფაილების და პროგრამების ჩამოტვირთვა და ა.შ.) ითვალისწინებდა, თუმცა საუკუნეთა გასაყარზე შექმნილი ახალი კონცეფციის (WEB 2.0) მიხედვით, ვებ-მომხმარებელი იმავდროულად **ვებ-კონტენტის რედაქტორსაც** წარმოადგენს, ანუ ვებ-გვერდის გარეგნული სახის შეცვლაში მონაწილეობს. WEB 2.0 **რედაქტირებადი აბლაზუდაა**, ანუ ინფორმაციული სივრცე, რომლის ხარისხიც უმჯობესდება მომხმარებელთა რაოდენობის ზრდასთან ერთად. WEB 2.0-ის სახეებია **მულტიმედია-პორტალები** (youtube, myvideo.ge...), **სოციალური ქსელები** (Facebook, ok.ru...), **ბლოგოსფერო** (blogger.com, wordpress.com...), ვიკი-პორტალები (wikipedia...) და სხვა მრავალი. ვებ-ტექნოლოგიებზე მომუშავე მრავალრციხოვან სპეციალისტთა ჯგუფები (პირველ რიგში W3C - ვების განვითარების კონსორციუმი) მიღწეულს არ სჯერდებიან და მსოფლიო აბლაზუდის ახალი შესაძლებლობებით აღჭურვისთვის იღწვიან. კერძოდ, ე.წ. **სემანტიკური ვების** კონცეფციით, რომელიც ჯერ უფრო თეორიულ დონეზეა დამუშავებული, ვებ-სივრცემ მომხმარებელს სემანტიკური სერვისები უნდა შესთავაზოს, ანუ უბრალოდ თუ ვიტყვით, მის პერსონალურ ასისტენტად უნდა იქცეს. მაგალითად, სემანტიკური ვები მიიღებს მოთხოვნას მომხმარებლისგან: „*სად შევიძინო*

ყველაზე იაფად ავტომანქანა Toyota, ჩემგან 50 კილომეტრის რადიუსში, 2002-დან 2008 წლამდე გამოშვების, თეთრი ან ბორდოსფერი, 7-10 ლიტრი ბენზინის ხარჯით 100 კილომეტრზე, ტყავის სალონით, კონდიციონერით, მარცხენა საჭიანი?“ და გასცემს მას საუკეთესო პასუხს.

მსოფლიო აბლაბუდის ჩონჩხი, მისი არქიტექტურა უცვლელია შექმნის დღიდან და შემდეგი კომპონენტებისგან შედგება:

- **ჰიპერტექსტური მონიშვნების ენა HTML** (Hypertext Markup Language) - ვებ-კონტენტის შენახვის ფორმატი;
- **პროტოკოლი http** (Hyper Text Transport Protocol) - აბლაბუდაში ინფორმაციის ტრანსპორტირების საშუალება;
- **ვებ-სერვერი** (Apache, IIS, lighttpd, nginx...) - ვებ-კონტენტის (HTML-ფაილები, ფოლდერები, ვებ-აპლიკაციები) საცავი;
- **ვებ-ბრაუზერი** (Firefox, Internet Explorer/ Microsoft Edge, Opera, Chrome, Safari...) - ვებ-კონტენტთან მიმართვის და ინფორმაციის მიღების საშუალება;
- **ინტერნეტ-პროგრამირების ენები** (JavaScript, PHP, ASP.NET...) - მსოფლიო აბლაბუდისთვის პროგრამული პროდუქტების შექმნის ინსტრუმენტები.

შევეხოთ თითოეულს უფრო დეტალურად. HTML-ენა ვებ-სივრცეში ინფორმაციის წარმოდგენის სტანდარტული ფორმატს წარმოადგენს, რომელიც 1990 წლიდან მუდმივ მოდერნიზაციას და სტანდარტიზაციას განიცდის. ენის ბოლო ვერსია, HTML5 სხვა ფუნქციებთან ერთად მულტიმედიური ინფორმაციის (ვიდეო, აუდიო, რუქები და სხვა) გამოტანის საშუალებებსაც შეიცავს. HTML-დოკუმენტი წარმოადგენს მონიშვნის სპეციალური საშუალებების (ტეგები) იერარქიულად დალაგებულ ნაკრებს, რომლის წაკითხვისა და ფორმატირებულად ასახვისთვის სპეციალური პროგრამა, ვებ-ბრაუზერი გამოიყენება. აღსანიშნავია, რომ თანამედროვე ვებ-დოკუმენტებში **კონტენტი** (შინაარსი) და **ფორმატირება** (გარეგნული სახე) ურთიერთგამიჯნულია. კონტენტი უშუალოდ HTML-დოკუმენტში ინახება, ხოლო ფორმატირების ელემენტები, როგორც წესი, ე.წ. ჩადგმულ CSS (Cascade Style Sheet)-ფაილებშია აღწერილი. ქვემოთ მოცემულია HTML და მასთან დაკავშირებული CSS-ფაილების ფრაგმენტები:

CSS-ფაილი **test.css**

```
body {background-color: Yellow;}
```

```
h1 {
```

```
text-align: center;
```

```
color: blue;}
```

HTML-ფაილი ჩადგმული CSS-ით

```
<!DOCTYPE html>
```

```
<html> <head>
```

```
<title>Main HTML-Document</title>
```

```
<link rel="stylesheet" type="text/css" href="B:\Web\test.css">
```

```
</head>
```

```
<body>
```

```
<h1>ქართული ფილმების არქივი</h1>
```

```
<table border="5">
```

```
<tr> <th>ფილმის დასახელება</th>
```

```
<th>რეჟისორი</th> </tr>
```

```
<tr> <td style="color:red">დარიკო</td>
```

```
<td>სიკო დოლოძე</td> </tr>
```

```
<tr> <td>ცისფერი მთები</td>
```

```
<td>ელდარ შენგელაია</td></tr>
```

```
</table> </body> </html>
```

ვებ-კონტენტის, ანუ **ვებ-გვერდების** შესაქმნელად მრავალი პროგრამა არსებობს. სწავლების პროცესში უბრალო ტექსტურ რედაქტორებს მიმართავენ (მაგ. Notepad++), ხოლო რეალური ვებ-საიტების შესაქმნელად იყენებენ ისეთ პროფესიონალურ პროდუქტებს, როგორცაა Adobe Dreamweaver, Microsoft Expression Web, CoffeeCup HTML Editor და სხვა მრავალი.

ვებ-ბრაუზერსა და ვებ-სერვერს შორის კავშირის საშუალებას **http-პროტოკოლი** წარმოადგენს, რომელიც საამისოდ ბრძანებათა საკუთარ ნაკრებს შეიცავს, ხოლო ვებ-რესურსის ადგილსამყოფელის დასადგენად **უნიფიცირებულ რესურსთა ლოკატორს** (URL) იყენებს. URL-მისამართის რამდენიმე ელემენტის კომპინაციისგან შედგება. ესენია: **პროტოკოლი, ჰოსტის DNS-სახელი ან IP-მისამართი, პორტის ნომერი, ვებ-ფოლდერი.** მოვიყვანოთ ამგვარად მიღებული URL-ის ნიმუში:

<http://lockss.cms.hu-berlin.de:8081/BatchAuConfig>

ვებ-სერვერი მსოფლიო აბლაბუდის მონაცემთა განთავსების და მართვის ამოცანას ემსახურება. იგი წარმოადგენს სერვერული ოპერაციული სისტემის გაფართოებას ან დამოუკიდებელ პროგრამულ უზრუნველყოფას და შექმნილია პრაქტიკულად ყველა გავრცელებული ოპერაციული სისტემისთვის. ყველაზე გავრცელებული ვებ-სერვერებიდან შეიძლება დავასახელოთ Apache, IIS (Internet Information Services), Nginx, Google Web Server...

ვებ-ბრაუზერი ვებ-სერვერიდან გამოძახებული კონტენტის ფორმატირებული ასახვის (გამოტანის) საშუალებაა და შექმნილია ყველა პოპულარული ოპერაციული სისტემისთვის (Windows, MAC OS X, LINUX...). ბრაუზერებს გააჩნიათ ინფორმაციის ქეშირების საშუალება მონაცემებთან მიმართვის დასაჩქარებლად. ისტორიულად პირველი ვებ-ბრაუზერებიდან ფართოდ გავრცელდა Lynx (რომელიც ტექსტურ, ანუ კონსოლის რეჟიმში მუშაობდა), Mosaic და Netscape Navigator. სადღეისოდ ყველაზე გავრცელებული ვებ-ბრაუზერებია Google Chrome, Mozilla Firefox (და მისი კლონი Debian LINUX-ისთვის Icweweasel), MS Edge, Internet Explorer, Opera, Safari...

დაპროგრამების ინსტრუმენტების გამოყენებით ვებ-ინფრასტრუქტურის დინამიური მართვა ხორციელდება. ვებ-პროგრამირების ენები ორი ძირითად ჯგუფად იყოფა:

• **სერვერული ვებ-პროგრამები (Server-side Scripting Languages)** - სრულდება ვებ-სერვერის მხარეს და მიზნად ისახავს დინამიური HTML-კონტენტის გენერაციას. მომხმარებელი გზავნის მოთხოვნას ბრაუზერიდან ვებ-სერვერისკენ, რომელიც სერვერის მხარეს მუშავდება (მაგალითად, ამოკრეფს ინფორმაციას მონაცემთა ბაზებიდან) და საბოლოო სახით (გენერირებული HTML-დოკუმენტი) უბრუნდება მომხმარებელს. სერვერული ვებ-პროგრამების კოდი ბრაუზერში უხილავია. სერვერული ვებ-პროგრამირების ენებიდან შეიძლება დავასახელოთ: **Perl, PHP, ASP.NET, JAVA-Servlet, XML, Python, Ruby;**

• **კლიენტის ვებ-პროგრამები (Client-side Scripting)** - სრულდება ვებ-ბრაუზერში და მიზნად ისახავს HTML-კოდზე მოქმედებების შესრულებას (ფორმის ან შინაარსის შეცვლა) ან მომხმარებლის მიერ განხორციელებულ ქმედებათა (მაგ. ღილაკზე მაუსის დაწკაპუნება) დამუშავებას. ისინი ინტეგრირებულია ვებ-ბრაუზერებში ანუ წაკითხვადია კლიენტის მხარეს (Browser source code), რაც მათი გამოყენების უსაფრთხოებას ამცირებს. კლიენტის ვებ-პროგრამირების ცნობილი ენებია: **JavaScript, VBScript, JAVA-Applet...**

ზემოთ აღწერილი კომპონენტების საფუძველზე აიგება ორგანიზაციის ვებ-ინფრასტრუქტურა (ვებ-აპლიკაციების ფრეიმვორკი). ცნობილია ოპერაციული სისტემების, მონაცემთა ბაზების მართვის სისტემების, ვებ-სერვერების და ვებ-დაპროგრამების სისტემების რამდენიმე კომბინაცია, რომლებიც ფართოდაა ბაზარზე გავრცელებული. მოვიყვანოთ მაგალითები:

- Windows, Internet Information Server, MS SQL Server, ASP.NET
- LINUX, Apache Server, MySQL, PHP (LAMP-სერვერი)
 - Windows, Apache, MySQL, PHP (WAMP-სერვერი)
- IBM WebSphere – AIX, Java, XML, Web-Services
- და მრავალი სხვა...

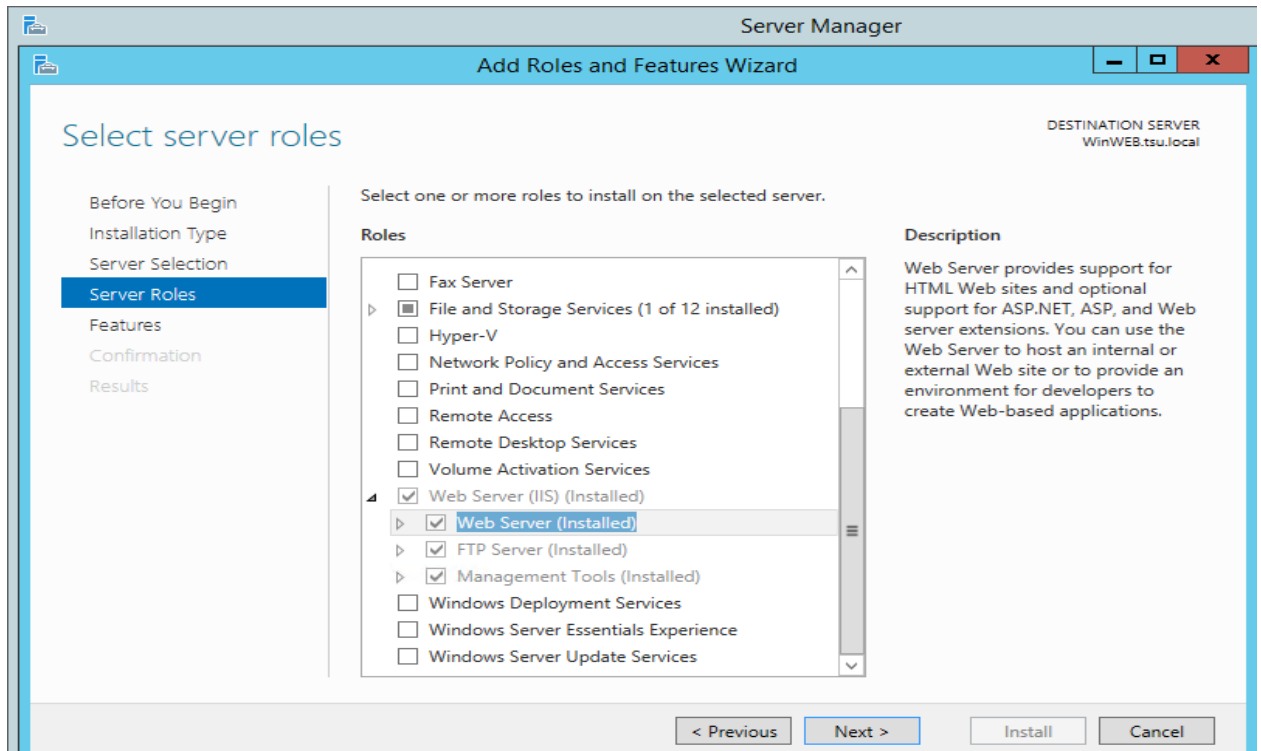
თანამედროვე ვებ-სივრცეში ფართოდ გავრცელდა **კონტენტის მართვის სისტემები (CMS – Content Management Systems)**, რომლებიც წარმოადგენენ მეტწილად უფასო, „ღია კოდზე“ (OpenSource) მომუშავე ვებ-აპლიკაციებს, წინასწარ მომზადებული ფუნქციების ნაკრებით, რაც ვებ-დეველოპმენტისთვის დასახარჯ დროს ხშირ შემთხვევაში მნიშვნელოვნად ამცირებს. CMS-სისტემები შექმნილია მრავალი სხვადასხვა ტიპის

საპრობლემოს სფეროსთვის. სტანდარტული ვებ-კონტენტის მართვის სისტემებს წარმოადგენენ Joomla, Drupal, Wordpress და სხვები. **სასწავლო პროცესის მართვის LMS-სისტემებიდან** (Learning Management Systems) შეიძლება დავასახელოთ Moodle და ILIAS, **ბიბლიოთეკების მართვის** (LMS – Library Management Systems) ყველაზე ცნობილი სისტემებია Evergreen და Koha. მრავალი პროგრამა ემსახურება **ელექტრონული კომერციის** (E-commerce) სფეროსაც (ონლაინ-მაღაზიები, ონლაინ-აუქციონები). მაგალითად პროგრამა PrestaShop შეიძლება მოვიყვანოთ. ერთერთ ქვეთავში ჩვენ შევხებით სრულფუნქციური, მზა ვებ-პორტალის უმოკლეს დროში მიღების პროცედურას სისტემა MS SharePoint-ის მაგალითზე.

ყურადღების გარეშე ვერ დავტოვებთ **ვებ-ჰოსტინგის მართვის სისტემებსაც**, რომელთა დანერგვა პირველ რიგში აუცილებელია **ვებ-ჰოსტინგ-პროვაიდერებისთვის**, აგრეთვე ისეთი ორგანიზაციებისთვის, რომელთა ვებ-ინფრასტრუქტურა ათობით და ასობით ვებ-გვერდისგან შედგება. ვებ-ინფრასტრუქტურის მართვის ავტომატიზაციის ისეთი პროგრამები, როგორცაა Cpanel, ISPConfig და სხვები მნიშვნელოვნად ამცირებენ სისტემის ადმინისტრატორის დროით დანახარჯებს ვებ-ინფრასტრუქტურის მართვის პროცესში.

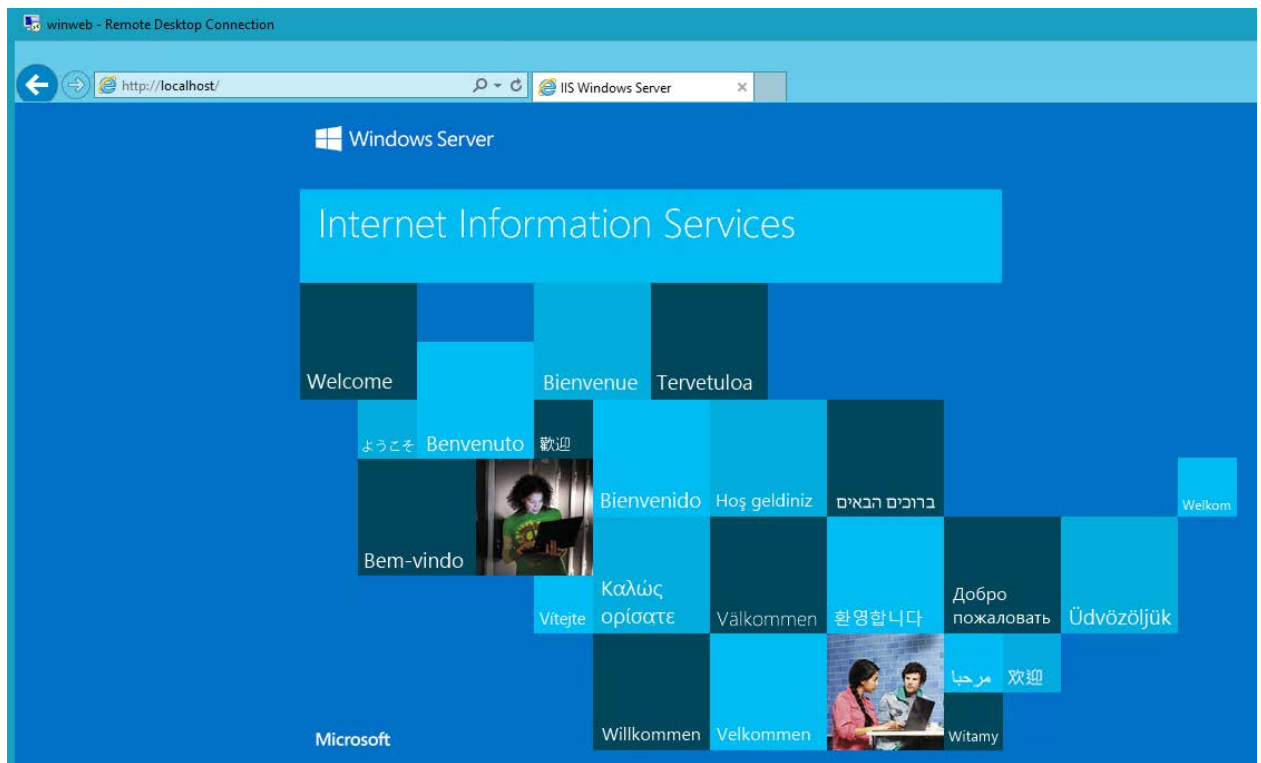
4.1.1.1. ვებ-სერვერის აქტივაცია და მართვა Internet Information Server-ის გარემოში

პროგრამა Internet Information Server წარმოადგენს ოპერაციული სისტემა Windows Server-ის ერთერთ **როლს**, ვებ-გვერდების შექმნის, შენახვის და მართვის ინსტრუმენტებით. მისი აქტივაცია Server Manager-პროგრამის Add Roles and Features-ფუნქციითაა შესაძლებელი (სურათი).



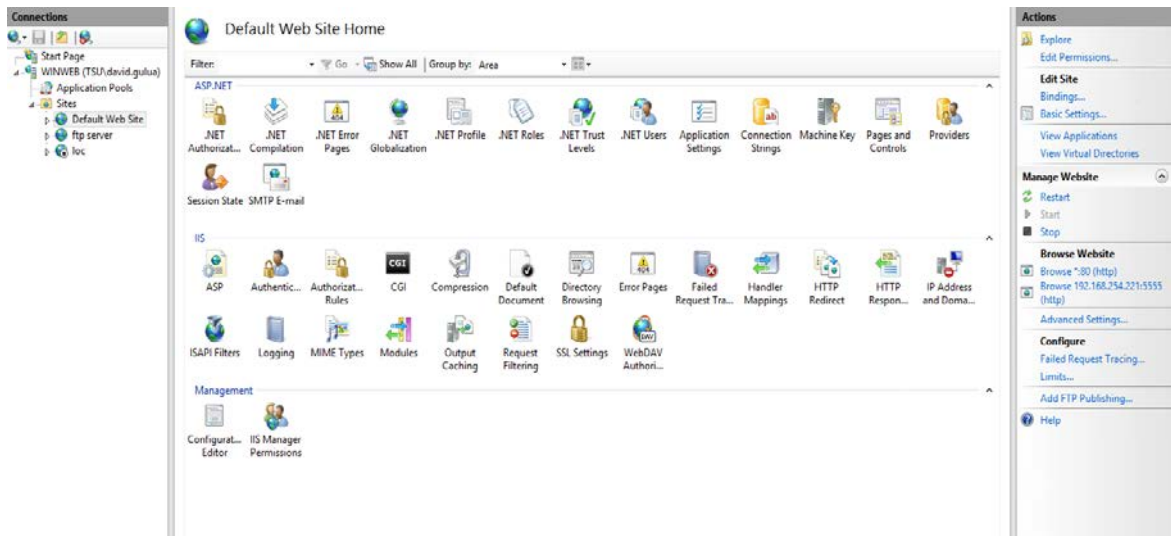
სურ.4.1.1.1 IIS-ის აქტივაცია Windows 2012 Server-ის გარემოში

აქტივაციის წარმატებული შესრულების ნიშანია ვებ-ბრაუზერში ვებ-სერვერის გვერდის გამოტანა, რომელიც გავრცელებულ ენებზე ესაღმება მომხმარებელს (სურათი).



სურ.4.1.1.2 IIS-სერვერის საწყისი გვერდი ვებ-ბრაუზერში

უშუალოდ ვებ-სერვერზე პროგრამა Internet Information Services (IIS) Manager-ის გაშვებით ვებ-ადმინისტრატორს შეუძლია შეუდგეს ვებ-საიტების და ვებ-აპლიკაციების სერვერზე ატვირთვის და მართვას.

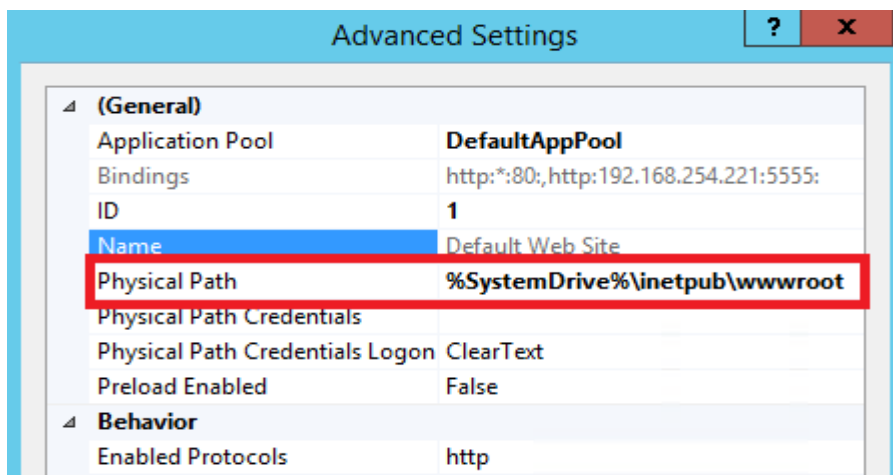


სურ.4.1.1.3 IIS-ის მართვის ინტერფეისი

წარმოდგენილი ინტერფეისის ყველა ფუნქციის განხილვა მოცემული წიგნის ფარგალს სცილდება. გამოიყენეთ რამდენიმე ძირითადი მომენტი:

ვებ-გვერდების ნაგულისხმევ (Default) საცავს სერვერის ფაილურ სისტემაში ფოლდერი %System Drive%\inetpub\wwwroot წარმოადგენს. ვებ-გვერდების და ვებ-აპლიკაციების ლოკაციის შესაცვლელად გამოიყენება ბრძანება:

ვებ-გვერდზე მათხის მარჯვენა ღილაკი -> Manage Website -> Advanced Settings -> პარამეტრი Physical Path (სურათი).



სურ.4.1.1.4 ვებ-გვერდის ადგილმდებარეობის შეცვლა IIS-ში

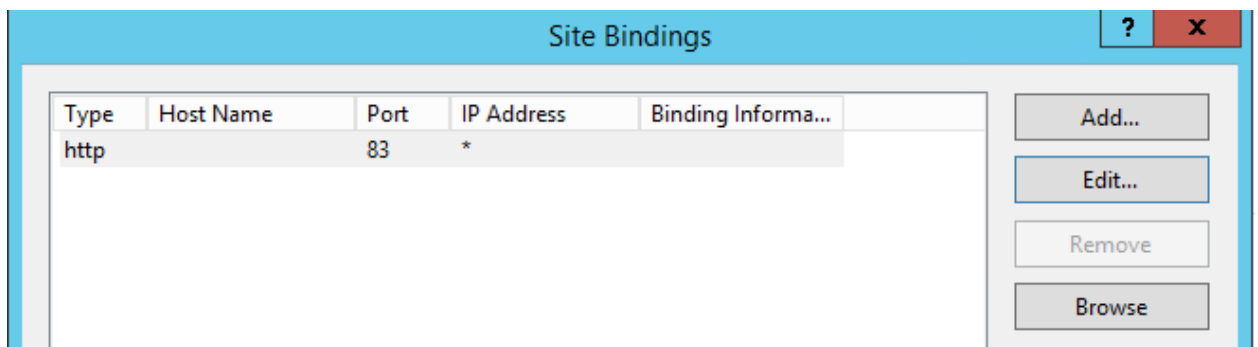
ვებ-რესურსთან მიმართვის აუცილებელ წინაპირობას ვებ-სერვერზე თავისუფალი პორტის არსებობა წარმოადგენს. http-პროტოკოლი სტანდარტულად მე-80 პორტს იყენებს, ანუ URL-ში პორტის ნომრის არარსებობა მე-80 პორტის გამოყენებაზე მიუთითებს. ორ ვებ-აპლიკაციას საერთო პორტის გამოყენება არ შეუძლია. კონფლიქტის აღმოსაფხვრელად ორი გზა არსებობს:

- ერთერთი ვებ-აპლიკაციის გადამისამართება **ალტერნატიულ** (მაგ. 81-ე, 82-ე და ა.შ.) პორტზე;
- ვებ-აპლიკაციისთვის **ვირტუალური ჰოსტის** სახელის (Host Name) განსაზღვრა და იმავე (მე-80) პორტის პარალელური გამოყენება.

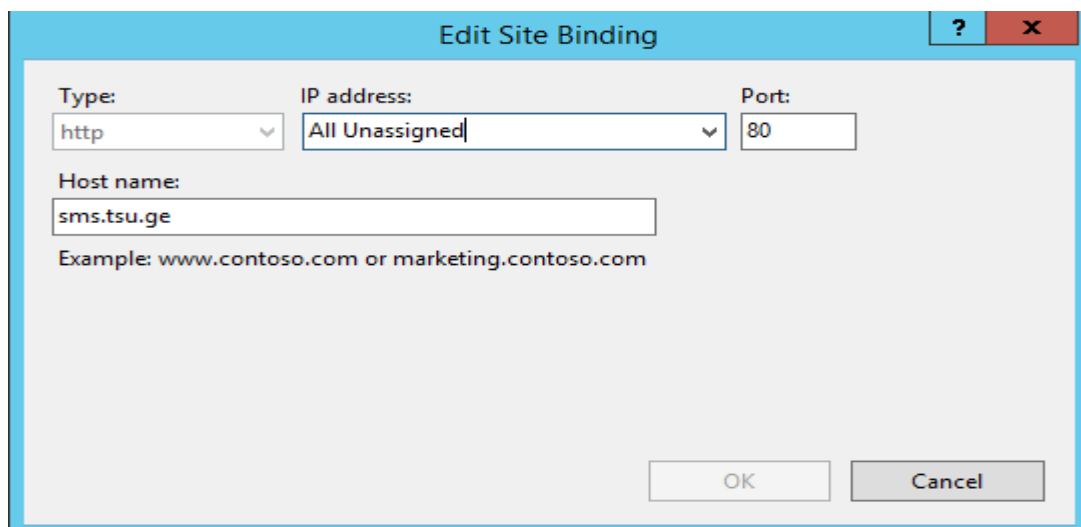
ორივე შემთხვევაში გამოიყენება ბრძანება:

ვებ-გვერდზე მათის მარჯვენა ღილაკი -> Edit Bindings

ბრძანების ინტერფეისის ნიმუშები მოცემულია სურათებზე.



სურ.4.1.1. 5 ვებ-აპლიკაციისთვის ალტერნატიული პორტის არჩევა



სურ.4.1.1. 6 ვირტუალური ჰოსტის სახელის განსაზღვრა

4.1.1.2. ვებ-აპლიკაციების მართვა MS SharePoint-ის გარემოში

ფირმა **Microsoft**-ის ტექნოლოგია **SharePoint** წარმოადგენს კორპორაციული ქსელების ინფორმაციულ მოთხოვნებზე მორგებულ, ვებ-ბაზირებულ პროგრამულ უზრუნველყოფას, რომელიც მომხმარებლებს თანამშრომლობის და ჯგუფური სერვისების გამოყენების მოქნილ შესაძლებლობებს სთავაზობს. კერძოდ, პროგრამის მეშვეობით შესაძლებელი ხდება ვებ-ბაზირებული სერვისების სწრაფი შექმნა ჯგუფური მუშაობისთვის, რაც კორპორაციულ ქსელებში მიმდინარე პროცესების მზარდ ავტომატიზაციას უწყობს ხელს. ანალოგიური ფუნქციონალის მქონე პროგრამული პროდუქტებიდან გამოირჩევიან WebSphere (IBM), Lotus Notes/Lotus Domino (LOTUS), MediaWiki (Wikimedia Foundation) და სხვები.

SharePoint-ტექნოლოგიის ძირითადი შესაძლებლობები მოცემულია სურათზე.



სურ.4.1.2 1 Microsoft SharePoint-ის ძირითადი კომპონენტები

სისტემა უზრუნველყოფს კორპორაციული ვებ-საიტების შექმნას და გაწყობას (Sites), კორპორაციულ ქსელში ინტერესთა ჯგუფების შექმნასა და მართვას (Communities), ინფორმაციის შენახვას (Content) და ძიებას (Search), გარე (მაგალითად, საოფისე) აპლიკაციების ინტეგრირებას ერთიან გარემოში (Insights) და წინასწარ დამუშავებული

ფუნქციონალური ბლოკების გამოყენებას ბიზნეს-გადაწყვეტილებათა შესაქმნელად (Composities). თითოეული ამ სერვისისთვის დეტალურად განისაზღვრება წვდომათა მართვის სიები, რის შედეგსაც კორპორაციული ქსელი ერთიანი ინფორმაციული პორტალი წარმოადგენს, სადაც კომფორტულად მუშაობის საშუალებები გააჩნიათ ორგანიზაციული იერარქიის სხვადასხვა დონეზე მდგომ მომხმარებლებს.

სამაგალითოდ ავიღოთ თანამედროვე საინფორმაციო (ახალი ამბების) ვებ-პორტალი, რომლის ფარგლებშიც მუშაობენ სრულიად განსხვავებული ამოცანების მქონე მომხმარებლები: IT-სპეციალისტები, ჟურნალისტები, რედაქტორები და მენეჯერები. მათი ნაწილი პორტალის შიგთავსს (კონტენტს) ანახლებს რეალური დროის რეჟიმში, მეორე ნაწილი - კონტენტის გარეგნული სახის დახვეწაზე ზრუნავს, სხვები ამატებენ და შლიან სისტემის ახალ მომხმარებლებს და ასე შემდეგ. საჭიროა პორტალის უწყვეტი მუშაობის უზრუნველყოფა და ამოცანათა სინქრონიზაცია პასუხისმგებლობის ზონების განაწილებასთან ერთად, რათა, ერთი მხრივ პროგრამისტებს და ვებდიზაინერებს რეალურ კონტენტთან წვდომა შეეზღუდოთ, ხოლო მეორე მხრივ, კონტენტის რედაქტორებს აკრძალოთ ცვლილებების შეტანა პორტალის დიზაინსა და პროგრამულ კოდებში. თვით ერთი ტიპის მომხმარებელთა საქმიანობაც (მაგალითად, რედაქტორები და მიმომხილველები) მკაცრად გამიჯვნას მოითხოვს. ერთი სიტყვით, წვდომათა მართვა **SharePoint**-ის უმნიშვნელოვანესი ფუნქციონალია.

შეზღუდვების დაწესებისა და უფლებათა გაცემის პროცესს სისტემაში მართავს სუპერუფლებების მქონე ერთი ან რამდენიმე ადმინისტრატორი. ყველა დანარჩენი მომხმარებელი სისტემაში მეტნაკლებად შეზღუდულია. მომხმარებელთა დაჯგუფების ერთი ნიმუში მოცემულია ცხრილში.

ცხრილი 1	
ჯგუფები	აღწერა
ადმინისტრატორები	სრული წვდომა ყველა ფუნქციონალურ კვანძზე.
დიზაინერები	პორტალის დიზაინს მოდიფიცირება, გვერდების და შვილობილი კვანძების შექმნა
ავტორები	ვებგვერდის კონტენტით შევსება

მონაწილეები	
დამთვალეებლები	ვებგვერდის დათვალეება

SharePoint-ის კიდევ ერთ უდავო ღირსებას მისი შედარებით ადვილად გამოყენება წარმოადგენს. კლიენტის მხარეს სამუშაოდ ნებისმიერი გავრცელებული ინტერნეტ-ბრაუზერიც საკმარია (**Internet Explorer, Mozilla Firefox, Google Chrome, Opera**), ხოლო სერვერზე სერვისთა სირთულის მიხედვით შეიძლება გამოყენებულ იქნას სხვადასხვა პროგრამები:

- **Windows SharePoint Foundation Service** - მოკრძალებული კორპორაციული პორტალებისთვის;
- **Microsoft Office SharePoint Designer** - მაღალი დონის დიზაინზე ორიენტირებული კორპორაციული პორტალებისთვის;
- **Microsoft Office SharePoint Server (MOSS)** - მძლავრი კორპორაციული პორტალებისთვის.

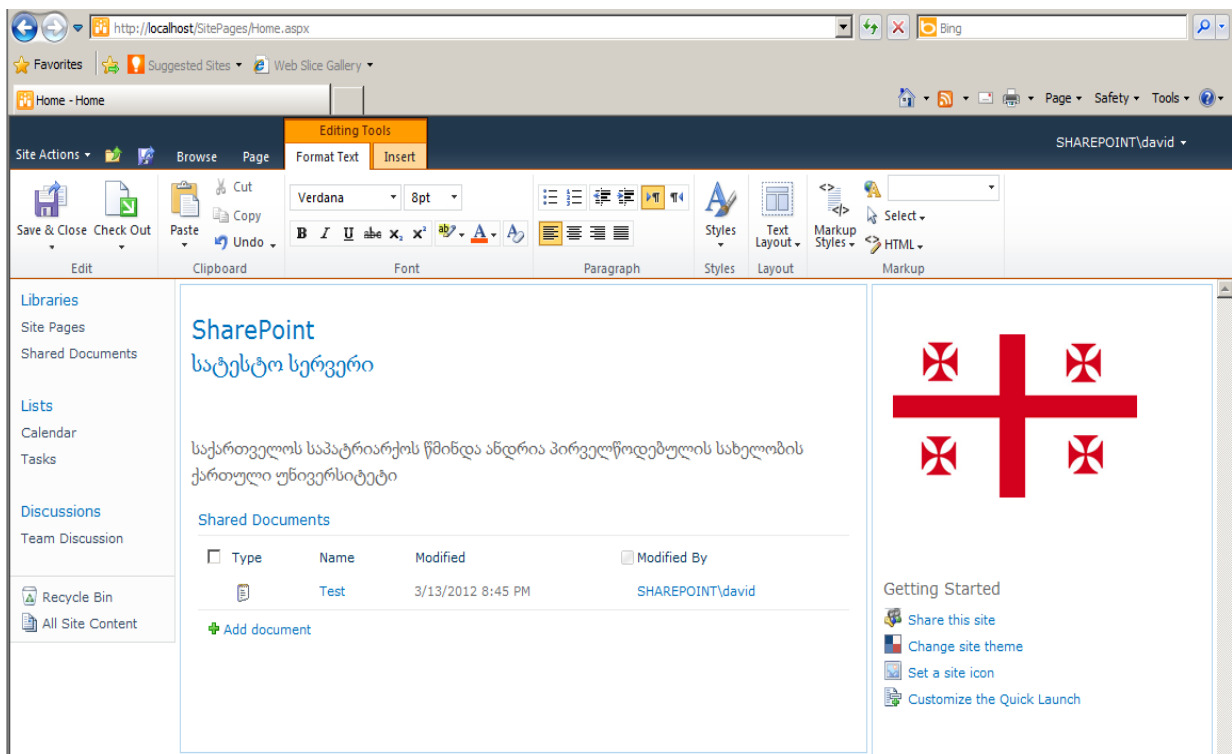
4.1.1.3. სისტემის დაყენება და გამართვა



სურ.4.1.1.3. 1 *SharePoint-ის კონფიგურაცია ვებ-სერვერზე Internet Information Server*

SharePoint-ის საინსტალაციო პაკეტის მეშვეობით სერვისისთვის გამოყოფილ მანქანებზე პროგრამის სერვერული პაკეტი ყენდება. ინსტალაციის პროცესში არჩევანის გაკეთება შეიძლება: სერვისი ან გამოყოფილ სერვერზე იმუშავეს, ან სერვერთა ფერმის (სერვერ-ფარმი) წევრი გახდება, რაც სერვისის მუშაობის საიმედოობას მეტად გაზრდის. სისტემის ინსტალაცია ავტომატურად აისახება IIS-ვებ-სერვერზეც (სურათი).

ინსტალაციის დასრულების შემდეგ სერვისის საწყისი ინტერფეისის გამოძახება შეიძლება ლოკალური ან კლიენტ-კომპიუტერის ბრაუზერიდან რესურსის URL-ის მითითებით (სურათი)



სურ.4.1.1.3. 2 *SharePoint*-ის საწყისი ვებგვერდი

მომხმარებლის განკარგულებაშია რამდენიმე საბაზო ობიექტი:

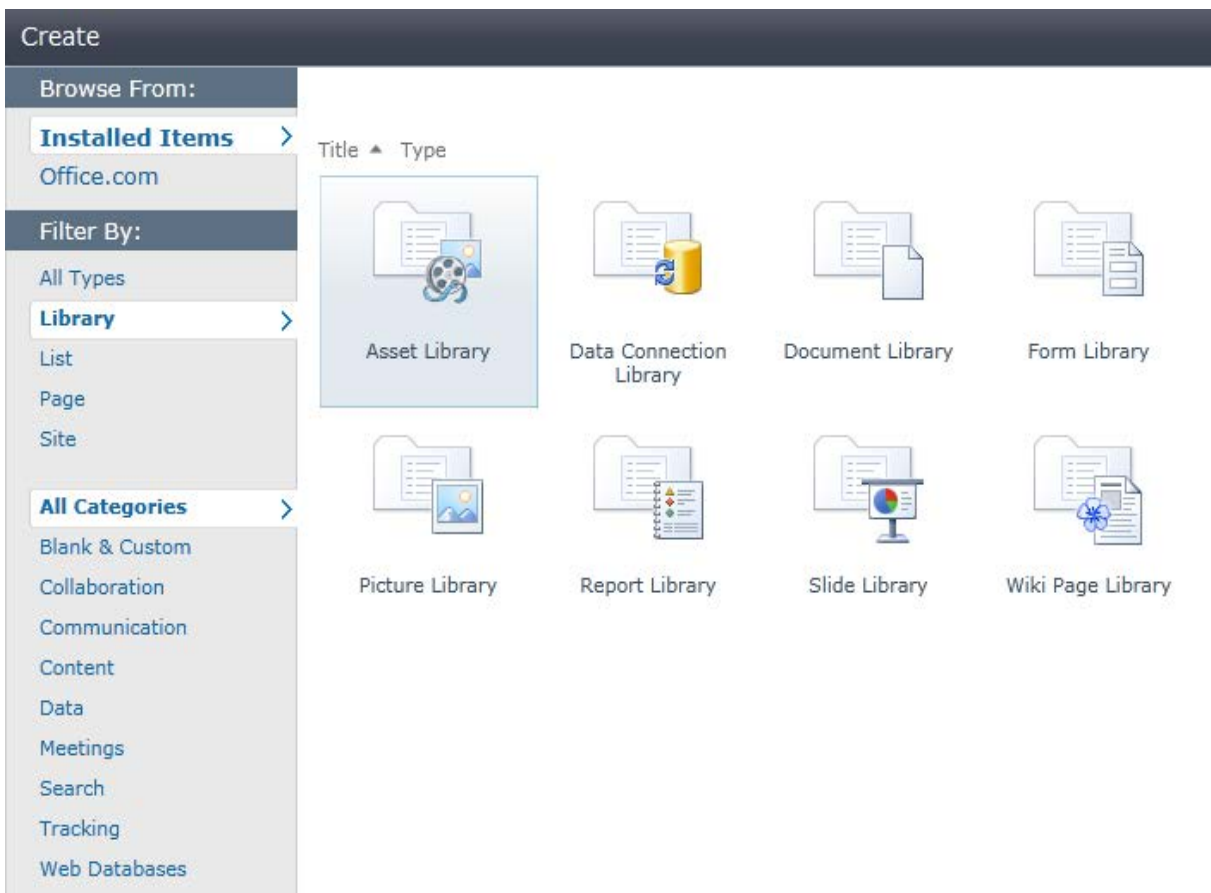
- **ბიბლიოთეკები (Libraries)** - ყველა ტიპის დოკუმენტების საცავი (ბიბლიოთეკები დოკუმენტების, გრაფიკული ინფორმაციის, ანგარიშების, სლაიდებისა და სხვა ტიპის ინფორმაციის შესანახად და გამოსატანად);

- **სიები (Lists)** - კონტეინერული ტიპის ელემენტი ინფორმაციის სხვადასხვა ტიპის წყაროებიდან ინფორმაციის მოპოვებისა და კონსოლიდირებული ასახვისთვის; სიების ნიმუშებად შეიძლება დავასახელოთ კალენდარი, კონტაქტების ბაზა, ამოცანები, სადიკუსიო პლატფორმა და სხვა.

- ვებგვერდი (Page) – ახალი გვერდი არსებული ვებსაიტის ფარგლებში;
- ვებსაიტი (Site) - ახალი ვებსაიტი რომელიმე ამოცანის შესასრულებლად.

ვებსაიტების კატეგორიებია საძიებო საიტი, გუნდური მუშაობის საიტი, ბლოგი, საკონტაქტო ინფორმაციის მართვის საიტი და სხვა მრავალი.

ქვემოთ მოცემული ინტერფეისი ასახავს **SharePoint**-ის ახალი კომპონენტის შექმნის ინტერფეისს, რომლის მარცხენა ზედა კუთხეში ჩვენს მიერ ჩამოთვლილი ობიექტის ტიპებს შორის კეთდება არჩევანი, ხოლო იქვე ქვემოთ მომხმარებელს კატეგორიული არჩევანის გაკეთება შეუძლია იმის მიხედვით, თუ რომელი ფუნქციონალი სჭირდება (კოლაბორაცია, კომუნიკაცია, კონტენტის მართვა, მონაცემთა ბაზები, ინფორმაციის ძიება თუ სხვა რომელიმე).

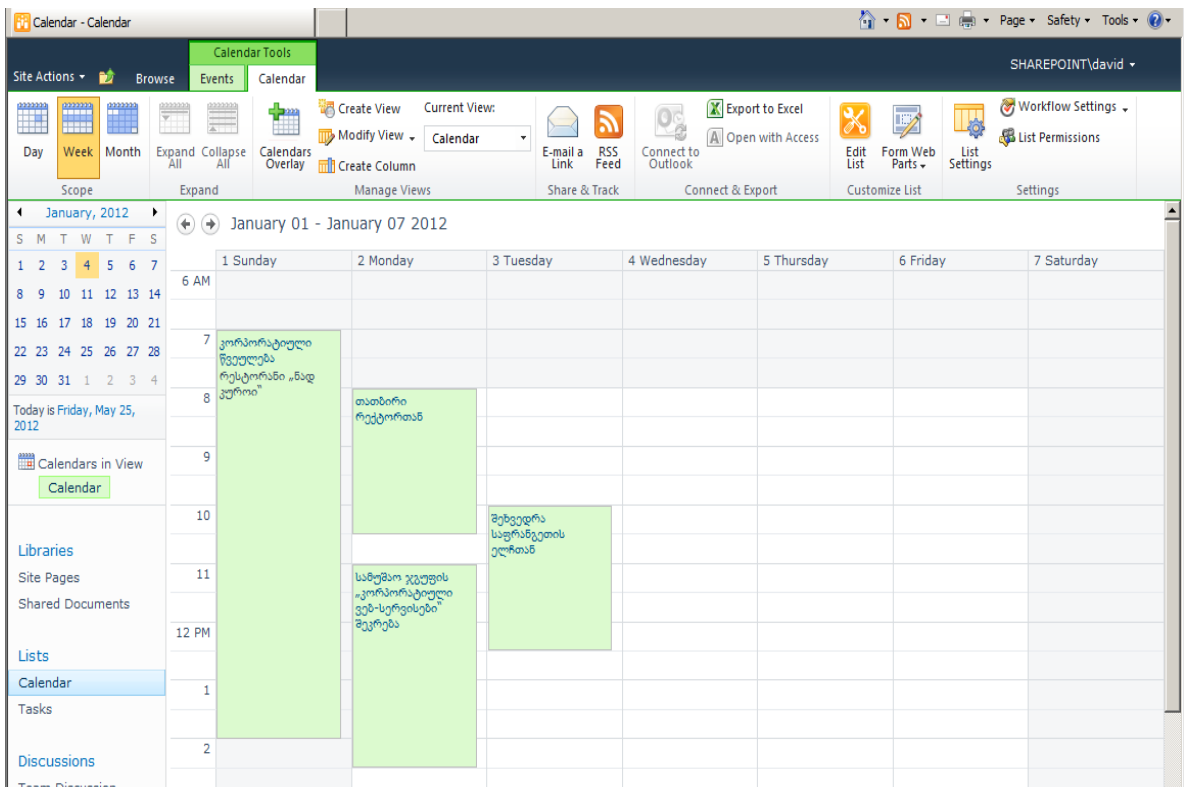


სურ.4.1.1.3.3 **SharePoint**-ის ახალი ობიექტის შექმნის ინტერფეისი

4.1.1.4. SharePoint-სერვისების ნიმუშები

SharePoint-ის საწყისი ინტერფეისის ფარგლებშივე შეიძლება სხვადასხვა სასარგებლო ფუნქციების გამოძახება და კორპორაციულ ინფორმაციულ სივრცეში გამოყენება. ქვემოთ შევხვებით ზოგიერთ მათგანს.

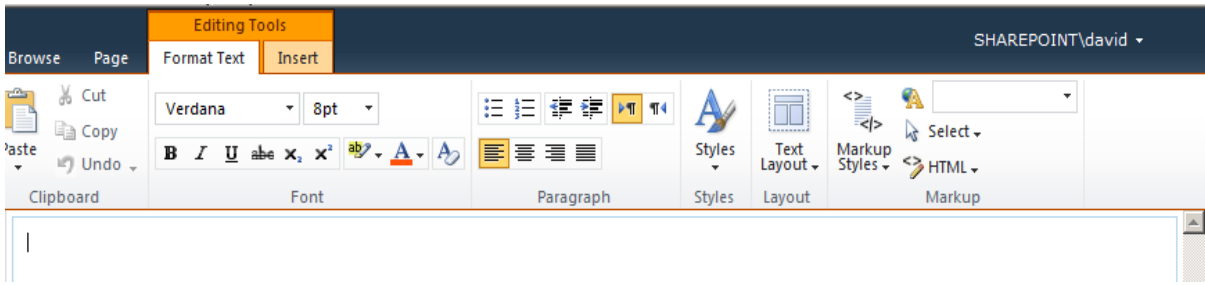
კალენდარი. კალენდრის სერვისი ორგანიზაციის საქმიანობის ვებ-სივრცეში დაგეგმვის საშუალებას იძლევა. ვებ-კალენდარი თავის ფუნქციონალობით თუმც შესამჩნევად ჩამოუვარდება სტანდარტულ კლიენტ-პროგრამებს (მაგალითად **MS Outlook**-ის კალენდარს), მაგრამ მისი ფუნქციათა ნაკრები მაინც საკმაოდ მდიდარია და კორპორაციული ღონისძიებათა დასაგეგმად ინსტრუმენტების ფართო ნაკრები გააჩნია. კალენდრის ნიმუში **SharePoint**-სერვერიდან იხილეთ სურათზე.



სურ.4.1.1.4.1 **SharePoint**-ის ის კალენდრის სერვისი

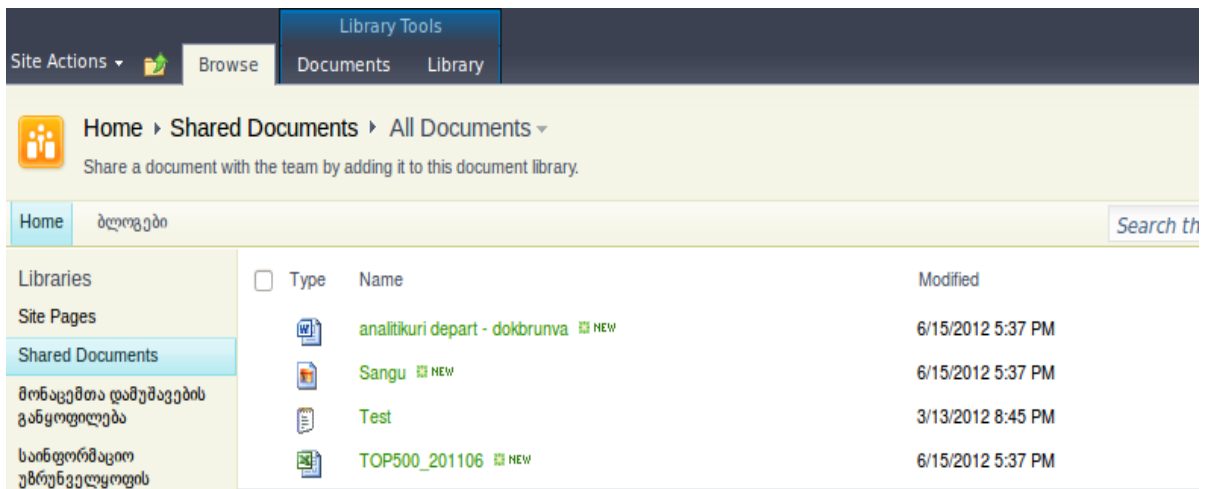
ამოცანები. ამოცანათა მოდული ასევე სასარგებლო ინსტრუმენტია. მისი დახმარებით კორპორაციის ან მისი ქვედანაყოფების საქმიანობის ეფექტურად დაგეგმვა შეიძლება.

საოფისე პროგრამები. SharePoint საკუთარ საოფისე საშუალებებს ფლობს, მაგალითად, საკმაოდ მძლავრი ტექსტური ონლაინ-რედაქტორის სახით (სურათი)



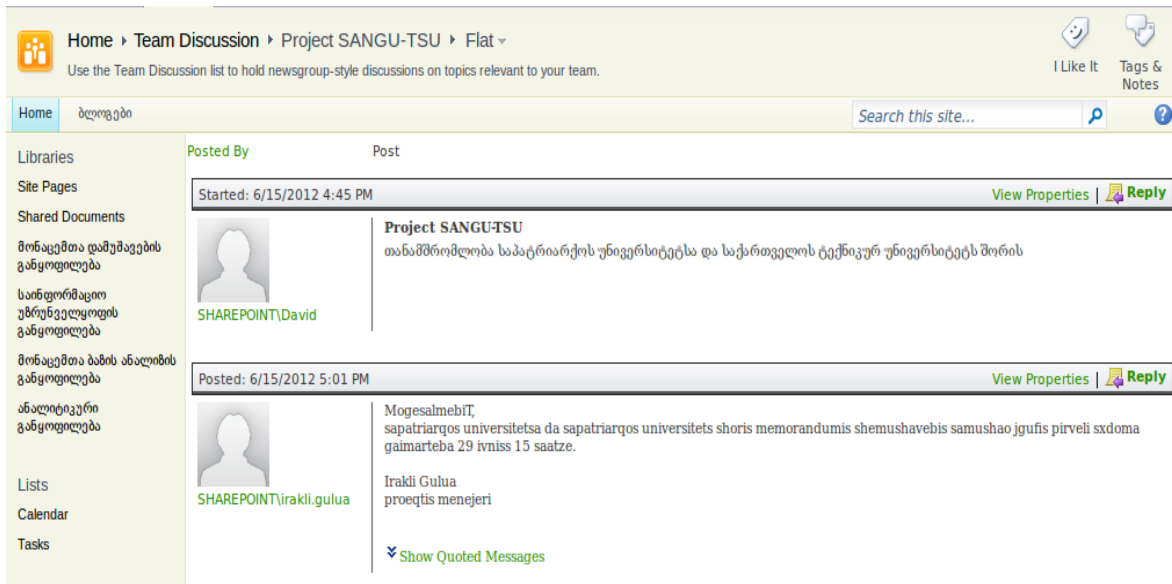
სურ.4.1.1.4 2 SharePoint-ის ონლაინ-რედაქტორი

ონლაინ რედაქტორით შედგენილი ან იმპორტირებული დოკუმენტების განაწილების ფუნქცია (**Sharing**) რამდენიმე მომხმარებელს ერთ ფაილზე პარალელურად მუშაობის საშუალება ეძლევა, რითაც სამუშაოს ეფექტურობა მატულობს (სურათი)



სურ.4.1.1.4 3 განაწილებული დოკუმენტების საცავი SharePoint-ში

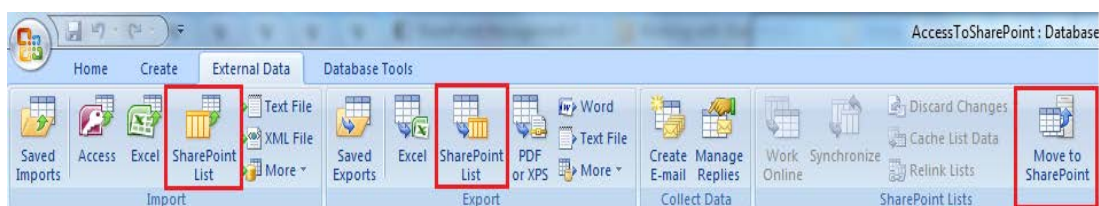
სადისკუსიო დაფა წარმოადგენს კორპორაციული პროექტების ირგვლივ ონლაინ-დისკუსიების გამართვის ინსტრუმენტს



სურ.4.1.1.4 სადისკუსიო დაფა SharePoint-ში

4.1.2. მონაცემთა მართვისა და ძებნის სერვისები

მონაცემთა ბაზებთან სინქრონული მუშაობა ნებისმიერი ვებ-ბაზირებული კორპორაციული პორტალის პირველხარისხოვანი ამოცანაა. SharePoint-ს ამ მხრივაც კარგად განვითარებული ინსტრუმენტების ნაკრები გააჩნია. ფირმა Microsoft-ის საოფისე პროგრამებისა თუ მონაცემთა ბაზების მართვის სისტემების ინტერფეისებში SharePoint-სერვერთან მონაცემთა მიმოცვლის ინსტრუმენტები უკვე ჩაშენებულია და მათი მეშვეობით შესაძლებელია არამარტო მონაცემთა ატვირთვა სერვერზე, არამედ სერვერზევე მათი დამუშავებაც. მაგალითად, ქვემოთ მოცემულია MS ACCESS-სა და SharePoint-სერვერს შორის მონაცემთა ექპორტ/იმპორტის ინტერფეისი.



სურ.4.1.2.2 მონაცემთა მიგრაცია MS ACCESS-სა და SharePoint-სერვერს შორის

ატვირთული მონაცემები დაუყოვნებლივ ხელმისაწვდომია ვებ-გვერდებსა და სერვისების სხვა ელემენტებზე, მაგალითად, SharePoint-ის სიის სახით (სურ.4.1.2.3).

ID	Rank	Site	Manufacturer	Computer	Country	Year	Cores	RMax
1	1	RIKEN Advanced Institute for Computational Science (AICS)	Fujitsu	K computer, SPARC64 VIIIfx 2.0GHz, Tofu interconnect	Japan	2,011	548,352	8,162,000
2	2	National Supercomputing Center in Tianjin	NUDT	NUDT TH MPP, X5670 2.93Ghz 6C, NVIDIA GPU, FT-1000 8C	China	2,010	186,368	2,566,000
3	3	DOE/SC/Oak Ridge National Laboratory	Cray Inc.	Cray XT5-HE Opteron 6-core 2.6 GHz	United States	2,009	224,162	1,759,000
4	4	National Supercomputing Centre in Shenzhen (NSCS)	Dawning	Dawning TC3600 Blade, Intel X5650, NVidia Tesla C2050 GPU	China	2,010	120,640	1,271,000
5	5	GSIC Center, Tokyo Institute of Technoloav	NEC/HP	HP ProLiant SL390s G7 Xeon 6C X5670.	Japan	2,010	73,278	1,192,000

სურ.4.1.2.3 მონაცემთა ბაზის ჩანაწერთა გამოტანა SharePoint-ის სიის ფარგლებში

ამასთან, **ექსპორტის** ფუნქციისგან (Export -> SharePoint List) განსხვავებით SharePoint-ზე **გადატანის** ფუნქცია (Move to SharePoint) ქმნის არა მონაცემთა ბაზის ასლს, არამედ თავად მონაცემთა ბაზას აქცევს ვებ-ბაზირებული სერვისის ნაწილად. სხვა სიტყვებით, ნებისმიერი ცვლილება მონაცემთა ბაზაში დაუყოვნებლივ აისახება ვებ-გვერდზე და პირიქით: ვებ-ინტერფისიდანაც შესაძლებელი ხდება მონაცემთა ბაზის მოდიფიცირება.

შესაძლებელია მონაცემთა გამოტანის კორექტირება მომხმარებლის მოთხოვნათა შესაბამისად. საამისოდ, ისევე როგორც მონაცემთა ბაზებში, იქმნება ე. წ. **სქემები (View)**, რომლებიც ველებისა და ჩანაწერების მხოლოდ წინასწარ განსაზღვრულ ქვესიმრავლებს მოიცავენ (სურათი)

Site Actions ▾ Browse **List Tools** **Items** List

New Item ▾ New Folder View Item Edit Item Delete Item Version History Item Permissions Attach File Workflows Approve/Reject I Like It Tags & Notes

New Manage Actions Workflows Tags and Notes

Libraries	Rank	Manufacturer
Site Pages	Rank	1
Shared Documents	Manufacturer	Fujitsu
მონაცემთა დაშუქების განყოფილება	Computer	K computer, SPARC64 VIIIfx 2.0GHz, Tofu interconnect
საინფორმაციო უზრუნველყოფის განყოფილება	Country	Japan
მონაცემთა ბაზის ანალიზის განყოფილება	Year	2,011
ანალიტიკური განყოფილება	Continent	Asia
Lists	Rank	3
Calendar	Manufacturer	Cray Inc.
Tasks	Computer	Cray XT5-HE Opteron 6-core 2.6 GHz
Discussions	Country	United States
Team Discussion	Year	2,009
	Continent	Americas
	Rank	5
	Manufacturer	NEC/HP
	Computer	HP ProLiant SL390s G7 Xeon 6C X5670, Nvidia GPU, Linux/Windows
	Country	Japan
	Year	2,010
	Continent	Asia

სურ.4.1.2.4 მონაცემთა ბაზიდან ინფორმაციის გამოტანა სქემების სახით

მონაცემთა ძებნის ჩადგმული ფუნქცია სასურველი ინფორმაციის სრულტექსტურ რეჟიმში (Full-text search) მოძიებისა და გამოტანის საშუალებას იძლევა (სურ.4.1.2.5).

Home ▸ Site Search Results

Home ბლოგები

This List: TOP500

Result Type 1-10 of 30 results

Any Result Type

Webpage

Site

Any Site

sharepoint/Lists

Author

Any Author

Sharepoint\David

Modified Date

Any Modified Date

Past 24 Hours

Cray Inc.
Cray XE6 12-core 2.1 GHz ... Cray XE ...
 Authors: Sharepoint\David Date: 6/15/2012
<http://sharepoint/Lists/TOP500/DispForm.aspx?ID=180>

Cray Inc.
Cray XT6 12-Core 2.0/2.1/2.2 GHz ... Cray XT ...
 Authors: Sharepoint\David Date: 6/15/2012
<http://sharepoint/Lists/TOP500/DispForm.aspx?ID=237>

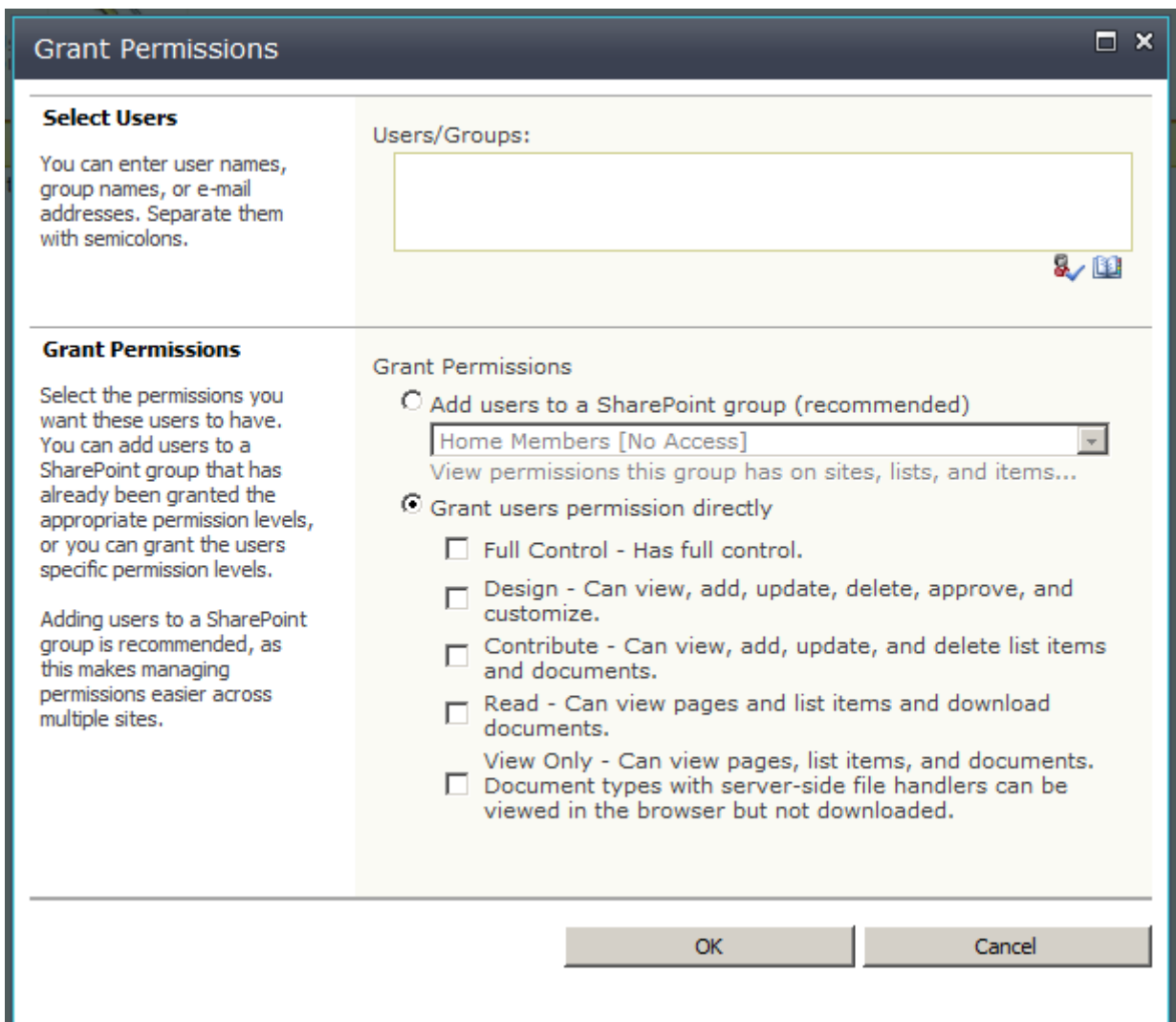
Government
Cray Inc. ... Cray XE6 12-core 2.2 GHz ... Cray XE ...
 Authors: Sharepoint\David Date: 6/15/2012
<http://sharepoint/Lists/TOP500/DispForm.aspx?ID=23>

Sandia National Laboratories
Cray Inc. ... United States ... AMD x86_64 ... Cray XT ... Cray XT3/XT4 ... Linux ... None ... MPP ...
 Research ... Proprietary ... North America ... Americas
 Authors: Sharepoint\David Date: 6/15/2012
<http://sharepoint/Lists/TOP500/DispForm.aspx?ID=36>

სურ.4.1.2.5 ინფორმაციის ძებნა სერვერზე სრულტექსტურ რეჟიმში

4.1.3. მომხმარებელთა მართვა

SharePoint-ში შესაძლებელია მომხმარებელთა მართვა როგორც ლოკალური, ასევე დომენური მომხმარებლებისა და მათი ჯგუფების დონეზე. სტანდარტულად, ინსტალაციის დასრულებისას სისტემა ერთი მომხმარებლისა და 4 ჯგუფის საადრიცხვო ჩანაწერებს შეიცავს მიმართვის სხვადასხვა უფლებებით. ამასთან საყურადღებოა, რომ SharePoint-ის ჯგუფები საკუთრივ სერვისის ფარგლებში იქმნება, ხოლო მომხმარებლები ოპერაციული სისტემის ლოკალურ (SAM-ბაზა) ან დომენის (AD) მომხმარებლებს წარმოადგენენ. ქვემოთ სურათზე მოცემულია ძირითად უფლებათა არჩევის ინტერფეისი.



სურ.4.1.3.1 ძირითად უფლებათა ტიპების არჩევის ინტერფეისი

სტანდარტული უფლებები ჩამოთვლილია ქვემოთ:

- **სრული წვდომა (Full Control)** - ყველა ოპერაციის შესრულების უფლება
- **სერვისის კომპონენტების შეცვლის უფლება (Design)** - სერვისზე ელემენტების ჩამატება, წაშლა, შეცვლა და სხვა;
- **შევსება/რედაქტირების უფლება (Contribute)** - სერვისის შეგთავსის (კონტენტი) შევსება, წაშლა, რედაქტირება;
- **წაკითხვის უფლება (Read)** - კონტენტის წაკითხვა და დოკუმენტების ჩამოტვირთვა;
- **ნახვის უფლება (View Only)** - მხოლოდ წაკითხვა, ჩამოტვირთვის გარეშე.

მოცემული წვდომის ძირითადი უფლებების კომბინირებით შეიძლება **წვდომის დონეთა** ჩამოყალიბება ყოველი მომხმარებლის ან მომხმარებელთა ჯგუფისთვის (სურათი)

Libraries	Name	Type	Permission Levels
Site Pages	Home Members	SharePoint Group	Contribute
Shared Documents	Home Owners	SharePoint Group	Full Control
მონაცემთა დაზუსტების განყოფილება	Home Visitors	SharePoint Group	Read
საინფორმაციო უზრუნველყოფის განყოფილება	SHAREPOINT\David (SHAREPOINT\david)	User	Limited Access
მონაცემთა ბაზის ანალიზის განყოფილება	Viewers	SharePoint Group	View Only
ანალიტიკური განყოფილება	ანალიტიკური განყოფილება	SharePoint Group	View Only
	მონაცემთა ბაზის ანალიზის განყოფილება	SharePoint Group	View Only
Lists	მონაცემთა დაზუსტების განყოფილება	SharePoint Group	Read, View Only
Calendar	საინფორმაციო უზრუნველყოფის განყოფილება	SharePoint Group	Contribute, Read, View Only
Tasks			

სურ.4.1.3. 2 მომხმარებელთა და ჯგუფების მართვა SharePoint-ში

როგორც მოცემული სურათიდან ჩანს, წვდომის დონე ერთი ან მეტი წვდომის უფლების სიმრავლისგან შედგება, რაც სერვისთან მიმართვის მაქსიმალურ მოქნილობას უწყობს ხელს.

შეიძლება დავასკვნათ, რომ სისტემა SharePoint მძლავრი ფუნქციონალის მქონე კორპორაციული ვებ-პორტალების უმოკლეს ვადებში დანერგვის ეფექტური საშუალებაა.

4.2. ფაილური, ბექდვის და სკანირების სერვისის მართვა

4.2.1 ფაილური სერვისის ძირითადი ფუნქციები

ფაილური სერვისი ორგანიზაციის ინფორმაციული ინფრასტრუქტურის საბაზო კომპონენტს წარმოადგენს. მის დანიშნულებას ფაილური რესურსების (ფოლდერები, ტექსტური და მულტიმედია ფაილები) საიმედოდ შენახვა, მართვა და მოხმარებლებისთვის მიწოდება წარმოადგენს. სადღეისოდ, Windows-სისტემებში ფაილური სერვისი შემდეგ ძირითად ამოცანებს განაგებს:

- ხელმისაწვდომი მესსიერების კვოტების დადგენა მომხმარებლებისთვის;
- ფაილების ინდექსირება (Index Service) ძეხნის ოპერაციათა დასაჩქარებლად;
- საერთო ქსელური დისკების მართვა;
- მომხმარებელთა პროფილების მართვა;
- საერთო ფაილური რესურსების გამოყენების მონიტორინგი და ფილტრაცია.

ორგანიზაციის ფაილურ სერვისს ფაილ-სერვერი ემსახურება. ოპერაციული სისტემა Windows Server-ის ფაილური სერვისის გასააქტიურებლად (ფაილ-სერვერის შესაქმნელად) აუცილებელია შესაბამისი სერვერული როლის გააქტიურება, რომელსაც File and Storage Services ეწოდება და რამდენიმე ქვეროლს მოიცავს (მათგანს ზოგიერთს ქვემოთ შევხებით).

ფაილ-სერვერის უპირველეს მახასიათებელს, ბუნებრივია, გარე მესსიერების დიდი მოცულობა წარმოადგენს. ოპერაციული სისტემა Windows Server შეიცავს როგორც ლოკალური და ქსელური, ასევე მონაცემთა საცავების ლოგიკური ტომების (Data Storage Volumes) ინტეგრირების საშუალებებს, ისე, რომ სისტემური აპლეტის Disk Management ფანჯარაში ხშირად უამრავი დისკის დაფიქსირებაა შესაძლებელი (სურათი).

Disk 0 Basic 136.70 GB Online	100 MB Healthy (System, Active, Prime	(C:) 136.60 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)	
Disk 1 Dynamic 1955.77 GB Online	Users (X:) 1955.00 GB NTFS Healthy	HO_Disk (Z:) 792 MB NTFS Healthy	
Disk 2 Dynamic 46.56 GB Online	(L:) 46.00 GB RAW Healthy	HO_Disk (Z:) 407 MB NTFS Healthy	166 MB Unallocated
Disk 3 Dynamic 139.69 GB Online	Reporting_Disk (P:) 139.00 GB NTFS Healthy	711 MB Unallocated	
Disk 4 Dynamic 93.13 GB Online	Applications (K:) 93.00 GB NTFS Healthy	129 MB Unallocated	
Disk 5 Dynamic 232.83 GB Online	HO_Disk (Z:) 186.00 GB NTFS Healthy	HO_Disk (Z:) 46.83 GB NTFS Healthy	
Disk 6 Basic 465.66 GB Online	New Volume (D:) 465.66 GB NTFS Healthy (Primary Partition)		
Unallocated Primary partition Simple volume Mirrored volume			

სურ.4.2.1.1

ლოგიკური დისკები Windows Disk Management-ში

თითოეულ ლოგიკურ დისკზე ფაილური სერვისის რესურსების მომხმარებლებზე განაწილება კვოტირების ფუნქციის თანხლებით სრულდება, რომელიც ოპერაციული სისტემა Windows-ის როგორც სერვერულ, ასევე დესკტოპ-ვერსიებშია წარმოდგენილი და დისკზე მაუსის მარჯვენა ღილაკის დაწკაპუნებით, *Properties-ბრძანების არჩევითა და გადამრთველ Quota-ზე გადასვლით შეიძლება იქნეს გამოძახებული (სურათი).*

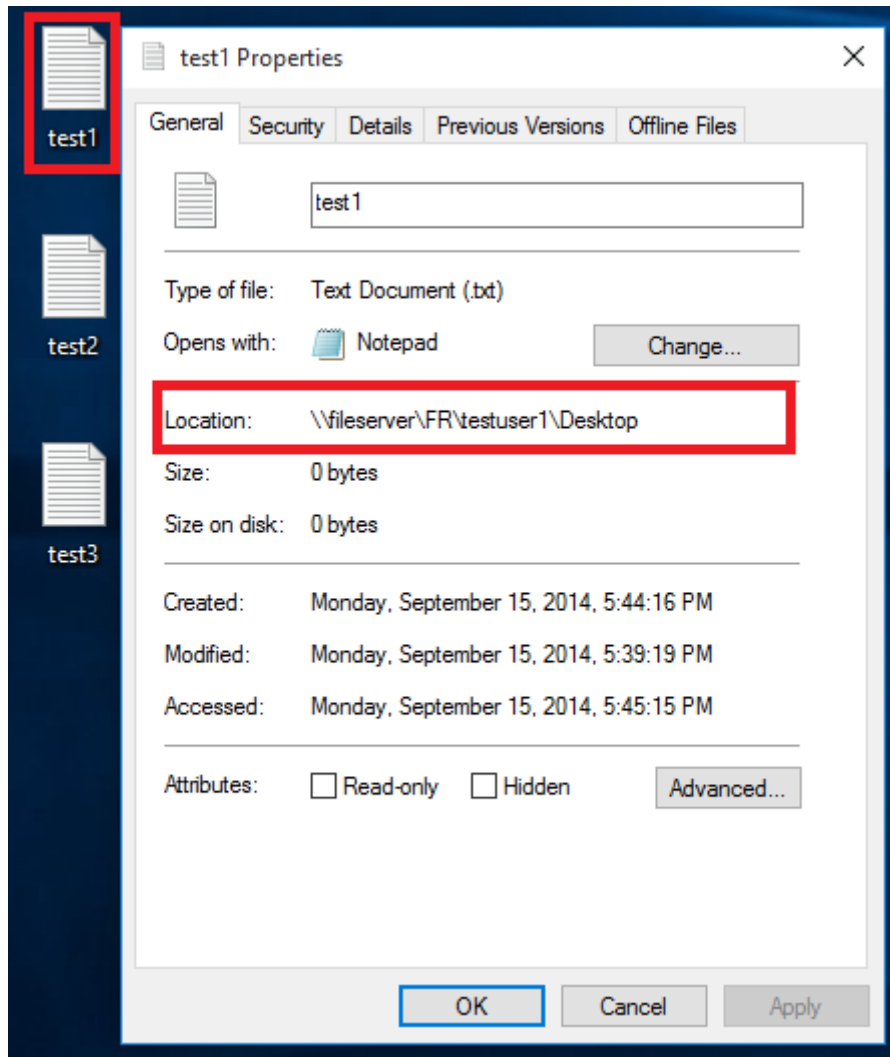
სურათზე ჩანს, რომ ყოველი მომხმარებლისთვის 2 GB ფაილური რესურსია გამოყოფილი, თუმცა ორგანიზაციის ზოგიერთი დეპარტამენტი (მაგ. ბუღალტერია, რეპორტინგი), მუშაობის სპეციფიკიდან გამომდინარე, შეიძლება ცალკე დისკურ რესურსებს და დამატებით გარე მეხსიერებასაც ფლობდეს.

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
OK	Ana Balesiashvili	a.balesiashvili@procreditbank.ge	59.03 MB	2 GB	2 GB	2
OK	Ana Beridze	a.beridze@procreditbank.ge	169.78 MB	2 GB	2 GB	8
OK	Aleksandre Danielidze	a.danielidze@procreditbank.ge	606.88 MB	2 GB	2 GB	29
OK	Ana Gochashvili	a.gochashvili@procreditbank.ge	228.33 MB	2 GB	2 GB	11
OK	Ana Gordeladze	a.gordeladze@procreditbank.ge	248.77 MB	2 GB	2 GB	12
OK	Anna Karkishvili	a.karkishvili@procreditbank.ge	177.07 MB	2 GB	2 GB	8
Above Limit	Alexandre Krivosheev	a.krivosheev@procreditbank.ge	3.2 GB	2 GB	2 GB	160
OK	Archil Machaidze	a.machaidze@procreditbank.ge	59.9 MB	2 GB	2 GB	2
Above Limit	Artur Manukian	a.manukian@procreditbank.ge	3.54 GB	2 GB	2 GB	177
OK	Ana Mghebrishvili	a.mghebrishvili@procreditbank.ge	111.68 MB	2 GB	2 GB	5
OK	Amiran Shavshishvili	a.shavshishvili@procreditbank.ge	200.06 MB	2 GB	2 GB	9
Above Limit	Ana Sirbiladze	a.sirbiladze@procreditbank.ge	2.14 GB	2 GB	2 GB	107
Above Limit	Aleksandre Tabatadze	a.tabatadze@procreditbank.ge	2.72 GB	2 GB	2 GB	136
OK	Ana Usenashvili	a.usenashvili@procreditbank.ge	153.55 MB	2 GB	2 GB	7
OK	Ana Abashidze	ana.abashidze@procreditbank.ge	125.12 MB	2 GB	2 GB	6

სურ.4.2.1.2 საერთო დისკის კვოტირების ინტერფეისი

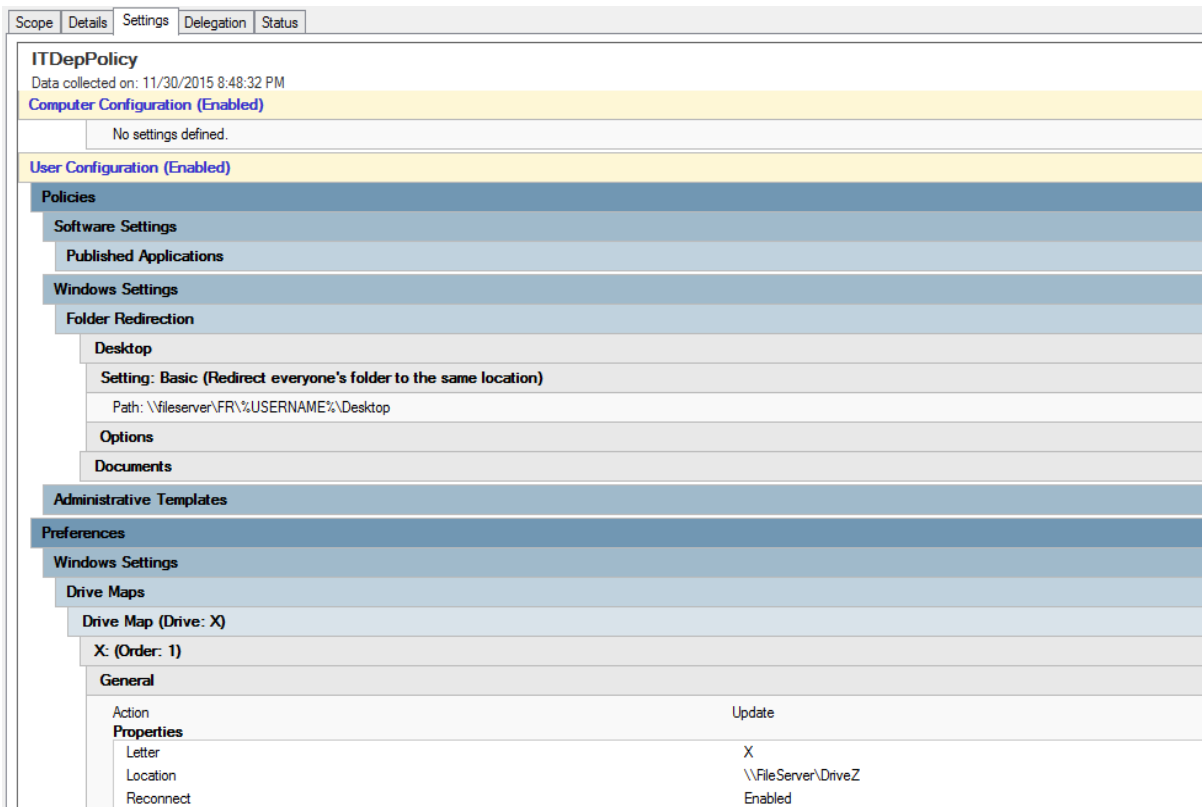
საერთო ქსელური დისკების მართვის ამოცანა გულისხმობს არსებული საშუალებების გათვალისწინებით მომხმარებლების ან მათი ჯგუფებისთვის გარკვეული ოდენობის მეხსიერების გამოყოფას ე.წ. **ქსელური დისკის** სახით.

მომხმარებელთა პროფილების მართვის ამოცანას მათ პერსონალურ კომპიუტერებზე დისკური მეხსიერების იმ უბნების საიმედო შენახვა წარმოადგენს, რომლებშიც ისინი ყველაზე მნიშვნელოვან ინფორმაციას განათავსებენ. იგულისხმება ოპერაციული სისტემის სამუშაო მაგიდა (დესკტოპი), დოკუმენტების, სურათების, აუდიო და ვიდეოფოლდერები და სხვა. **კატალოგების გადამისამართების** (Folder Redirection) ინსტრუმენტი მომხმარებელს უქმნის ილუზიას, რომ ყველა საჭირო ფაილი მის პერსონალურ კომპიუტერშია განთავსებული, მაშინ, როცა დესკტოპების, დოკუმენტების და სხვა პერსონალური ფოლდერების რეალურ ადგილსამყოფელს ფაილ-სერვერი წარმოადგენს (სურათი).



სურ.4.2.1.3 კატალოგების გადამისამართების (Folder Redirection) ასახვა Windows 10-ის დესკტოპზე

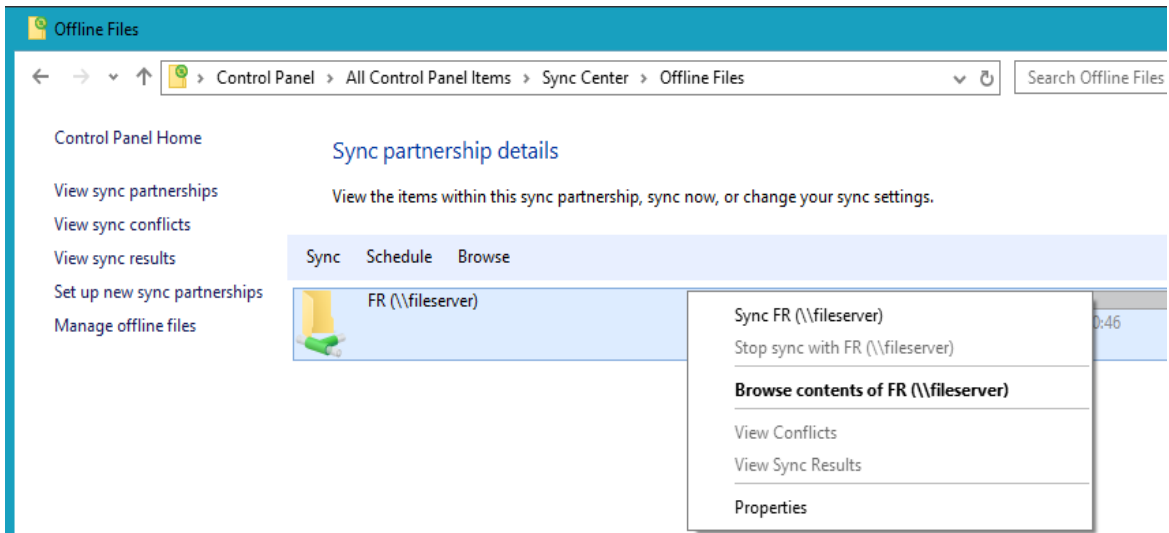
ზემოთ განხილულ ორივე შემთხვევაში ფაილური რესურსების მომხმარებელთა განკარგულებაში გადასაცემად აღარ არის საჭირო სპეციალური სკრიპტების წერა და ყოველ ლოკალურ ოპერაციული სისტემაში მათი ავტომატურად გაშვება. გამოიყენება ბევრად უფრო ადვილი ხერხი - დომენური ინფრასტრუქტურის (Active Directory) ჯგუფური პოლიტიკა (Group Policy), რომლის ფუნქციებიც ერთერთ წინა თავშია აღწერილი. ამჯერად წარმოვადგინოთ ჯგუფური პოლიტიკის ნიმუში კატალოგების გადამისამართებისთვის (სურათი).



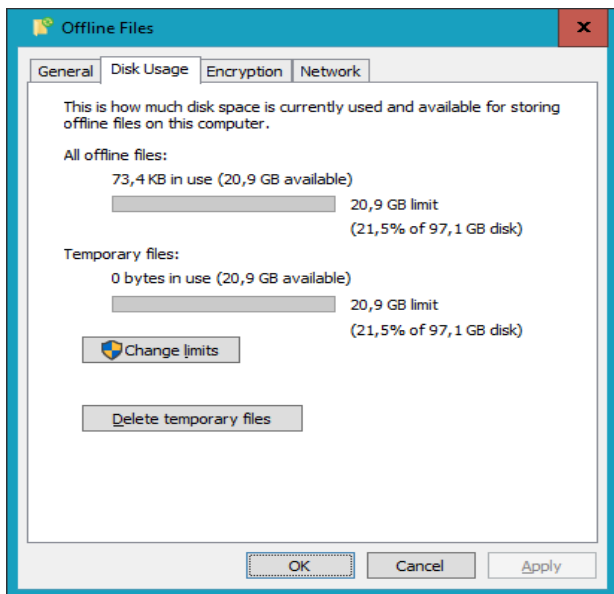
სურ.4.2.1.4 ჯგუფური პოლიტიკის (Group policy) ფრაგმენტი კატალოგების გადამისამართებისთვის

ფაილური სერვისის გამოყენება მომხმარებელს **ონლაინ** ან **ოფლაინ-რეჟიმებში** შეუძლია. ეს უკანასკნელი საშუალებას იძლევა მივმართოთ ქსელურ რესურსებს გათიშული ქსელის პირობებში, რისთვისაც კლიენტ-მანქანის კემ-მეხსიერებაში შენახული ინფორმაცია გამოიყენება. **ფაილური კეში** (Client Side Cash) ქსელური რესურსის (მაგ. ფოლდერი) იერარქიულ სტრუქტურას ინახავს და კლიენტ-კომპიუტერზე განთავსებულია ფოლდერში **%SystemRoot%\CSC**. ფაილ-სერვერთან კავშირის აღდგენის შემდეგ კეშირებული ინფორმაცია სერვერთან მონაცემების სინქრონიზაციას შეასრულებს.

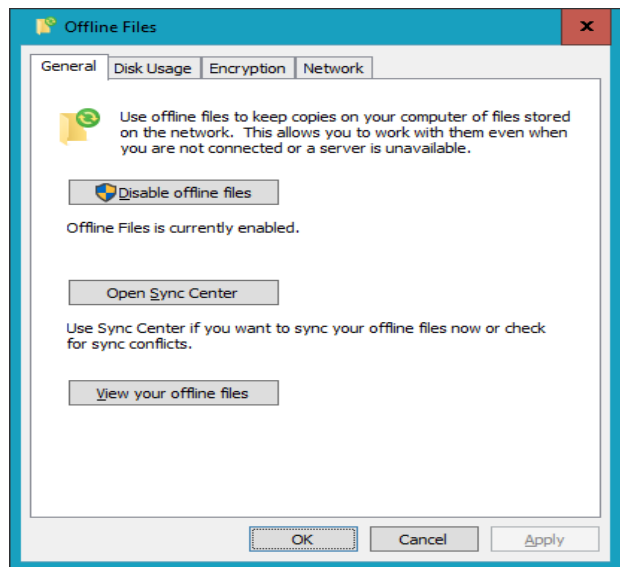
ოფლაინ-რეჟიმში მუშაობის საშუალებას Windows-ის უტილიტა Sync Center იძლევა, რომელსაც რამდენიმე ფუნქცია გააჩნია: **ოფლაინ-კეშის აქტივაცია**, **სინქრონიზაციის გრაფიკის შედგენა**, **ოფლაინ-მეხსიერების ქვოტირება** საერთო ლოკალური მეხსიერების ფარგლებში და **სხვა** (სურათები).



სურ.4.2.1.5 კლიენტსა და ფაილ-სერვერს შორის მონაცემთა სინქრონიზაციის ინტერფეისი



სურ.4.2.1.7 ოფლაინ-რეჟიმის მართვა



სურ.4.2.1.6 ოფლაინ-რეჟიმის ფაილური ქვოტის მართვა

უშუალოდ ფაილ-სერვერის მხარეს, ფაილური სერვისის სამართავად გამოიყენება პროგრამა File Server Resource Manager (სისტემური აპლეტი fsm.msc). მისი დახმარებით ფაილური სერვისის ოპტიმალურ მდგომარეობაში შენარჩუნება შეიძლება, ისე, რომ ერთი მხრივ, მომხმარებლებმა საჭირო ფაილური რესურსების ნაკლებობა არ იგრძნონ, ხოლო მეორე მხრივ, მეხსიერება ყაირათიანად გაიცეს და ყოველგვარი ზედმეტი კონტენტისგან თავისუფალი იყოს. საილუსტრაციო სურათზე მოცემულია ერთერთი ინტერფეისი სახელით File Screens, რომელიც ფაილ-სერვერის სხვადასხვა დისკებზე

სხვადასხვა ტიპის ფაილების დაშვება/შეზღუდვის პოლიტიკას განსაზღვრავს. სურათის მიხედვით, ფაილ-სერვერის Z: და P:-დისკებზე აკრძალულია შესრულებადი (.exe, .com) ფაილების განთავსება, ხოლო X:-დისკზე, ორიოდე გამონაკლისის გარდა (განყოფილება allow) შეუძლებელია აუდიო, ვიდეო და შესრულებადი ფაილების კოპირება.

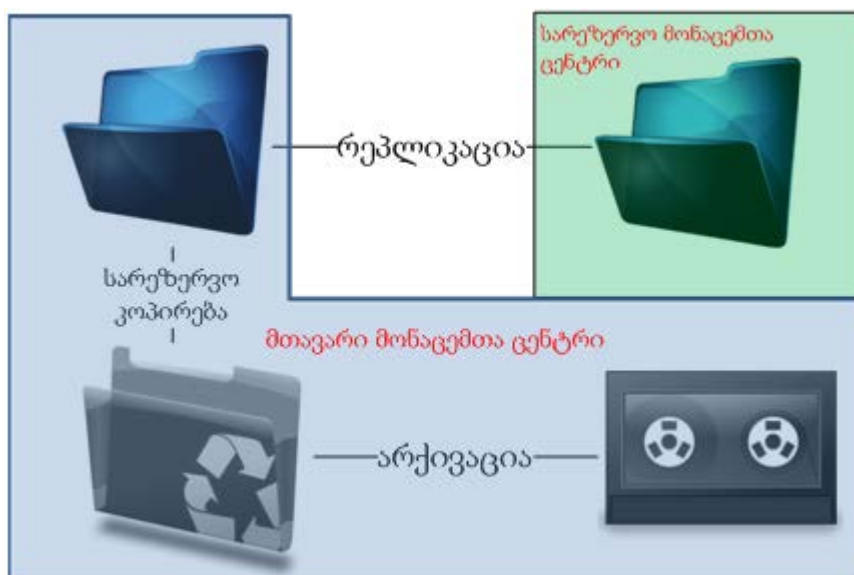
File Screen Path	Screening Type	File Groups	Source Template	Match ...
Source Template: (2 items)				
X:\FileServer\00 Head Office\Mar...	Exception	Allow: Audio and Video Files, Backup Files, ...		
X:\FileServer\Farewell	Exception	Allow: Audio and Video Files, Backup Files, ...		
Source Template: Block Executable Files (2 items)				
Z:\	Active	Block: Executable Files	Block Executable Files	No
P:\	Active	Block: Executable Files	Block Executable Files	No
Source Template: Block Large Video Files (1 item)				
X:\	Active	Block: Audio and Video Files, Executable File...	Block Large Video Files	No

სურ.4.2.1. 8 ფაილ-სერვერის დისკების მართვის ინტერფეისის ფრაგმენტი

4.2.2 ფაილური სერვისის სარგებლიანობის და საიმედოობის უზრუნველყოფა

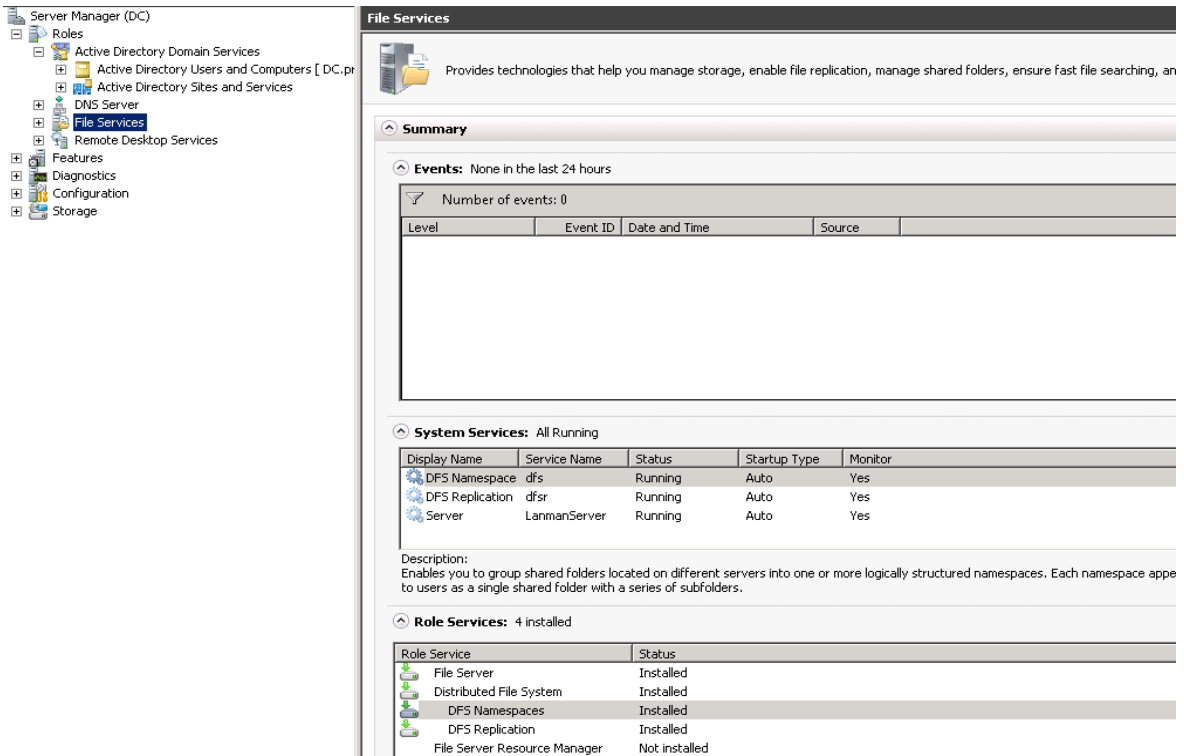
ზოგადად, ინფორმაციის სარგებლიანობასა და საიმედოებაში მასთვის წვდომის უწყვეტობის უზრუნველყოფას და სერვისის უმოქმედობის დროის მინიმიზაციას გულისხმობენ. ფაილური სერვისის სარგებლიანობის ასამაღლებლად შემდეგი მეთოდები გამოიყენება (ნახაზი):

- სარეზერვო კოპირება და არქივაცია
- განაწილებული ფაილური სისტემა (DFS) და ფაილთა ტომების რეპლიკაცია

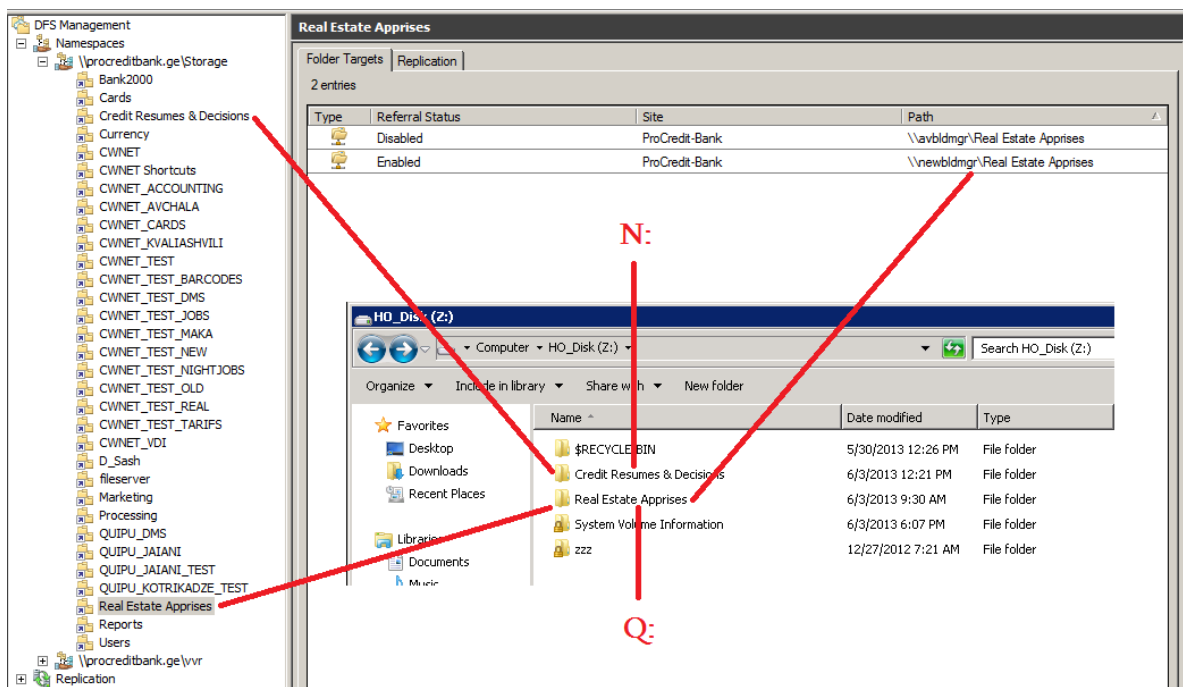


სურ.4.2.2. 1 რეპლიკაციის, სარეზერვო კოპირების და არქივაციის სანიმუშო სქემა

ფაილური და სხვა რესურსების სარეზერვო კოპირების და არქივაციის თემა ცალკე ქვეთავში განიხილება. **განაწილებული ფაილური სისტემის** ინსტრუმენტებით (Windows 2008 Distributed File System - DFS) სხვადასხვა ადგილებზე განთავსებული (მაგალითად, ორ დამოუკიდებელ ფაილ-სერვერზე) ფაილური რესურსებისგან დამოუკიდებელი **ვირტუალური ფაილური სივრცეა** შექმნილი (Namespace-მექანიზმის საშუალებით), რომელთანაც მომუშავე მომხმარებელს „არ აინტერესს“ ფოლდერების და ფაილების ფიზიკური მდებარეობა და აგრძელებს საკუთარ რესურსებთან მიმართებას მაშინაც, როცა რომელიმე სერვერი მწყობრიდან გამოდის (სურათები).



სურ.4.2.2.2 DFS-ფუნქციის აქტივაცია Windows Server-ში

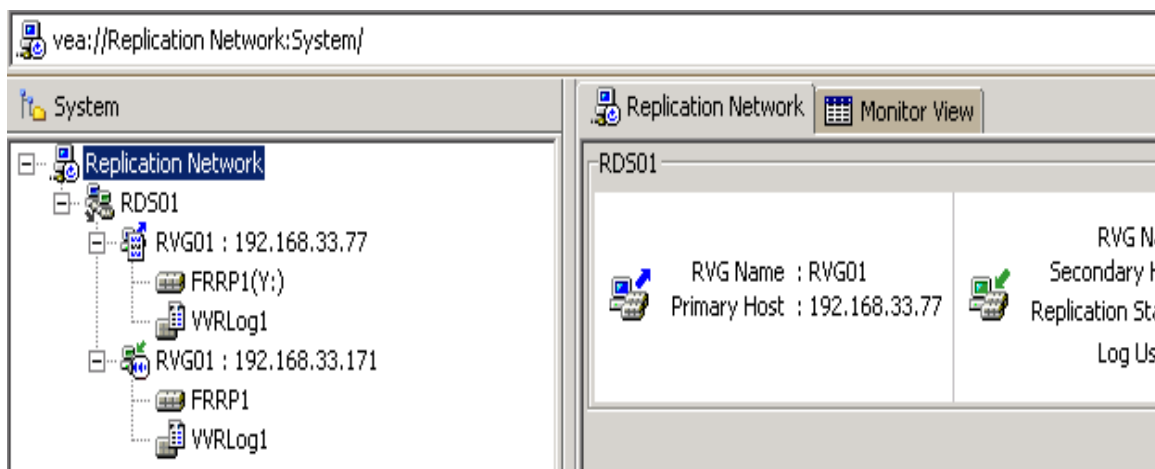


სურ.4.2.2.3 DFS-სერვისის მართვის ინტერფეისი

ფაილური რეპლიკაციის დამსახურებით კრიტიკული ინფორმაციული მასივები, კერძოდ მომხმარებელთა პროფილები და საერთო სარგებლობის დისკები, მუდმივად მინიმუმ ორი სინქრონული ასლის სახით ინახება (მაგალითად, ცენტრალურ და სარეზერვო მონაცემთა ცენტრებში). ერთერთი მხარის გათიშვისას ავტომატურად

ფაილთა მეორე რეპლიკა ირთვება, რაც ფაილურ რესურსებთან შეფერხებელ მიმართვას უზრუნველყოფს.

IT-ინფრასტრუქტურაში რეპლიკაციისთვის სპეციალური პროგრამული უზრუნველყოფა გამოიყენება (მაგალითად, Symantec Veritas Volume Replication), რომელიც DFS-ის რეპლიკაციის მოდულისგან განსხვავებით მუშაობს არა ფაილური სისტემის, არამედ უფრო საიმედო, მონაცემთა ტომების და ფიზიკური დისკების დონეზე. რეპლიკაციის საშუალებით მომხმარებელთა მონაცემების აქტუალური ასლები სინქრონულად მრავლდება, მაგალითად, ცენტრალურ და სარეზერვო მონაცემთა ცენტრებს შორის (სურ.4.2.2.4).



სურ.4.2.2.4 რეპლიკაციის ნიმუში: 192.168.33.77-დან 192.168.33.171-ისკენ

DFS და VVR-სისტემების ერთიანი მოქმედება ფაილური სერვისის სარგებლიანობას შესამჩნევად ამაღლებს.

4.3. მონაცემთა ბაზების სერვერული გარემოს მომზადება

4.3.1. შესავალი რელაციური მონაცემთა ბაზების მართვის სისტემებში

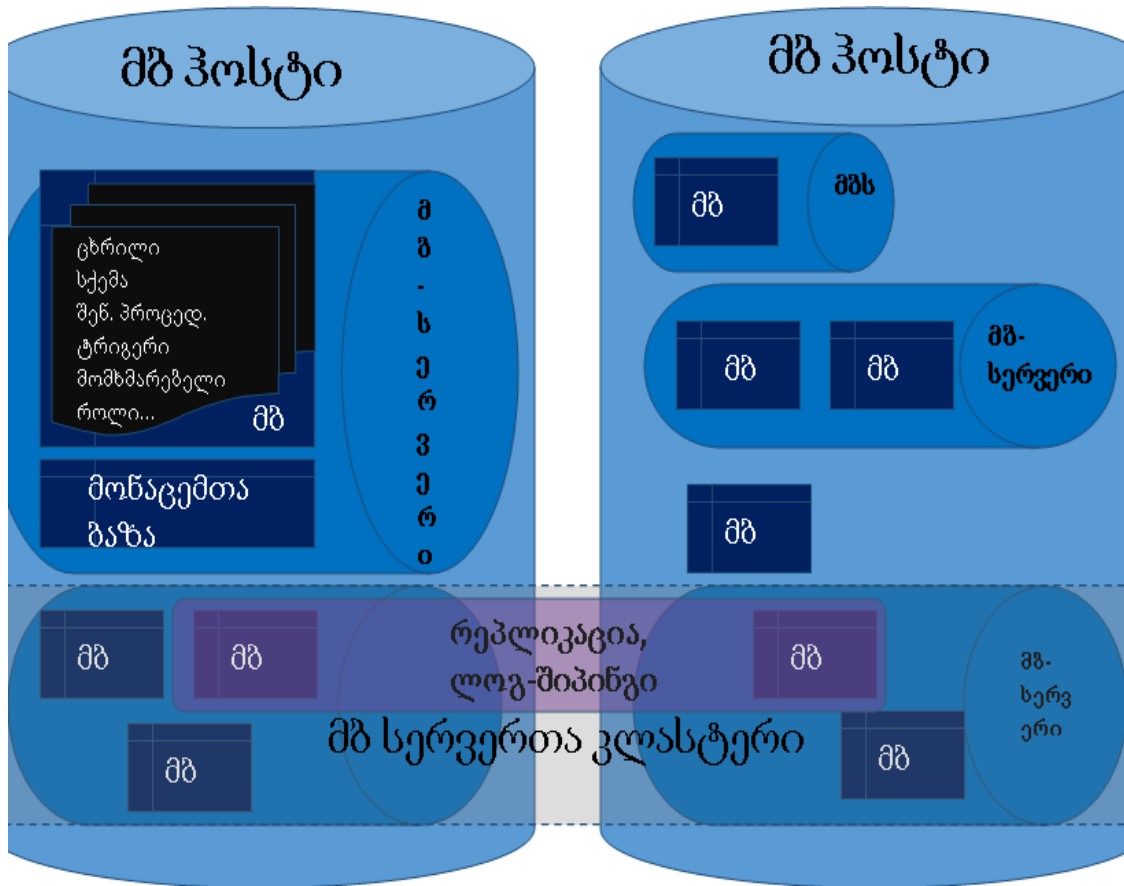
მონაცემთა ბაზების თეორია და მათი მართვის სისტემების შექმნა ინფორმაციული ტექნოლოგიების ერთერთ უმნიშვნელოვანეს სფეროს წარმოადგენს. უდავოა, რომ სადღეისოდ ცხოვრების პრაქტიულად ყველა სფეროში ინფორმაციული სისტემების დაპროექტებისა და აგებისას ყველაზე დიდი ყურადღება ამ სისტემების „უკანა მხარეს“ (Back-End), ანუ **მონაცემთა ბაზებს** ერგება. არასწორად შედგენილ მონაცემთა ბაზის მოდელს და მის პრაქტიკულ რეალიზაციას, აგრეთვე არასწორად შერჩეულ და გამართულ მონაცემთა ბაზების მართვის სისტემას ბიზნესის ან სხვა ტიპის საქმიანობისთვის აუნაზღაურებელი ზარალის მიყენება შეუძლია.

სანამ ინფორმაციული სისტემა მონაცემთა ბაზებთან სატესტო თუ საწარმოო რეჟიმში მუშაობას დაიწყებდეს, სისტემის ან/და მონაცემთა ბაზების ადმინისტრატორებს მართებთ საიმედო გარემოს შექმნა, რომელშიც ინფორმაციის დაზიანების ან დაკარგვის ალბათობა მინიმალური იქნება.

ჩვენს სახელმძღვანელოში ვეხებით მონაცემთა ბაზების ყველაზე პოპულარულ, გასული საუკუნის 70-იანი წლებში ამერიკელი მეცნიერის **ედგარ კოდის** მიერ დამუშავებულ **რელაციურ მოდელს**, კერძოდ კი ამ მოდელის საფუძველზე მოქმედი სისტემა MS SQL Server-ის ადმინისტრირების საკითხებს. ზოგადად, თუ მონაცემთა ბაზების მართვის სისტემების სარწმუნო რეიტინგ-ლისტებს გადავხედავთ, გამოჩნდება, რომ გავრცელების მიხედვით რელაციური მონაცემთა ბაზების მართვის სისტემებს პირველი სამი ადგილი უჭირავთ და საუკეთესო მბმს-ების პირველ ოცეულშიც ამ ტიპის 13 სისტემაა წარმოდგენილი (წყარო: საიტი db-engines.com). ლოკალური (დესკტოპ-) სისტემები MS Access, MS Foxpro, Borland Paradox, სერვერული სისტემები Oracle, Informix, SAP Adaptive Server Enterprise (Sybase SQL server), DB2, MS SQL Server, Ingres, MySQL, PostgresSQL, Borland Interbase/Firebird Database Server, Clarion და მრავალი სხვა რელაციური მბმს წარმატებით გამოიყენება პრაქტიკულად ყველა ტიპის საპრობლემო სფეროს ინფორმაციული სისტემების მოდელირებისა და იმპლემენტაციისთვის. ბოლო წლებში არარელაციურ, ე.წ. „არა SQL“-სისტემების (პირველ რიგში MongoDB უნდა

დავასახელოთ) მზარდი პოპულარობა ჯერჯერობით არასაკმარისია არსებული ტენდენციების შესაცვლელად, განსაკუთრებით საქართველოში.

სისტემის ან/და მონაცემთა ბაზების ადმინისტრატორისთვის მონაცემთა ბაზების ზოგადი ინფრასტრუქტურა სურათზე მოცემული სახით შეიძლება გამოვსახოთ.



სურ.4.3.1.1 მონაცემთა ბაზების ზოგადი ინფრასტრუქტურა

მონაცემთა ბაზების აპარატულ საცავს ფიზიკური ან ვირტუალური ჰოსტი წარმოადგენს, რომელიც შეიძლება ერთი ან მეტი მონაცემთა ბაზების სერვერ(ებ)ისგან (ეგზემპლარი, ინსტანსი) შედგებოდეს. მონაცემთა ბაზის სერვერი SQL Server წარმოადგენს დამოუკიდებელ პროგრამას (ოპერაციული სისტემის პროცესები sqlservr.exe, sqlWb.exe), რომელიც შემდეგი ძირითადი კომპონენტებისგან შედგება:

- მონაცემთა ბაზების მართვის ინსტრუმენტი (Database Engine)
- მეხსიერების მართვის ინსტრუმენტი (Storage engine)
- უსაფრთხოების ქვესისტემა (Security Subsystem)
- პროგრამული ინტერფეისი (Programming Interfaces)
- სერვისების ბროკერი (Service Broker)

- სერვერის აგენტი (SQL Server Agent)
- რეპლიკაციის მოდული (Replication)
- მაღალსარგებლიანობის უზრუნველყოფის ინსტრუმენტი (High Availability)
- რელაციურ ოპერაციათა მართვის ინსტრუმენტი (Relational engine)

მონაცემთა ბაზის სერვერი მართავს მონაცემთა ბაზებს, რომლებიც Windows Server-ის ფაილურ სისტემაში .mdf (მონაცემთა ბაზის ფაილი), .mdl (მონაცემთა ბაზის ინდექსური ფაილი) და .ldf (ტრანზაქციების ლოგ-ფაილი) გაფართოებათა მქონე ფაილების სახითაა წარმოდგენილი. როგორც წესი, ერთ მონაცემთა ბაზას თითო .mdf და .ldf-ფაილში ინახავენ, თუმცა მათი ოდენობა შეიძლება მეტიც იყოს. MS SQL Server 2012-სთვის მონაცემთა ბაზების სტანდარტულ ადგილსამყოფელს წარმოადგენს ფოლდერი:

%Program Files%\Microsoft SQL Server\MSSQL11.MSSQLSERVER\MSSQL\DATA

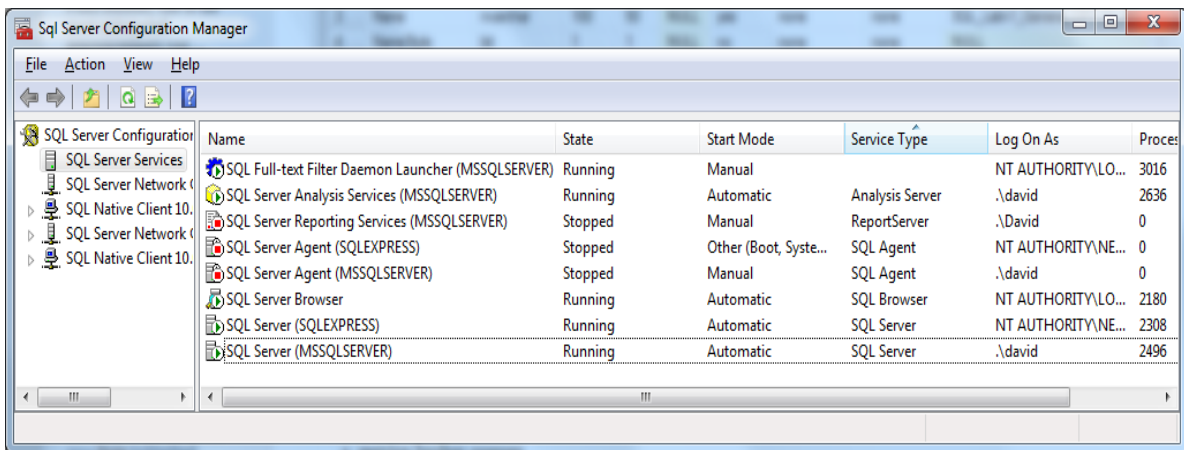
დასმული ამოცანის მიხედვით შეიძლება მისი გადატანა სხვა ადგილას (მაგალითად, არასისტემურ ლოგიკურ დისკზე). საილუსტრაციოდ მოვიყვანოთ შესაბამისი SQL-სკრიპტის ნიმუში:

```
-----
--
ALTER DATABASE TestDB SET single_user WITH ROLLBACK IMMEDIATE
GO
ALTER DATABASE TestDB SET OFFLINE
GO
ALTER DATABASE TestDB SET ONLINE
GO
ALTER DATABASE TestDB SET MULTI_USER
ALTER DATABASE TestDB MODIFY FILE
(NAME = SM_DATA, FILENAME = 'E:\Test_Databases\TestDB.mdf')
ALTER DATABASE TestDB MODIFY FILE
(NAME = SM_LOG, FILENAME = 'E:\Test_Databases\TestDB.LDF')
```

მონაცემთა ბაზა, თავის მხრივ, შეიცავს რელაციური მოდელის მიხედვით დაპროექტებულ ცხრილებს, სქემებს (Views), ტრიგერებს, შენახული პროცედურებს და ინფორმაციის დასამუშავებლად აუცილებელ სხვა ელემენტებს.

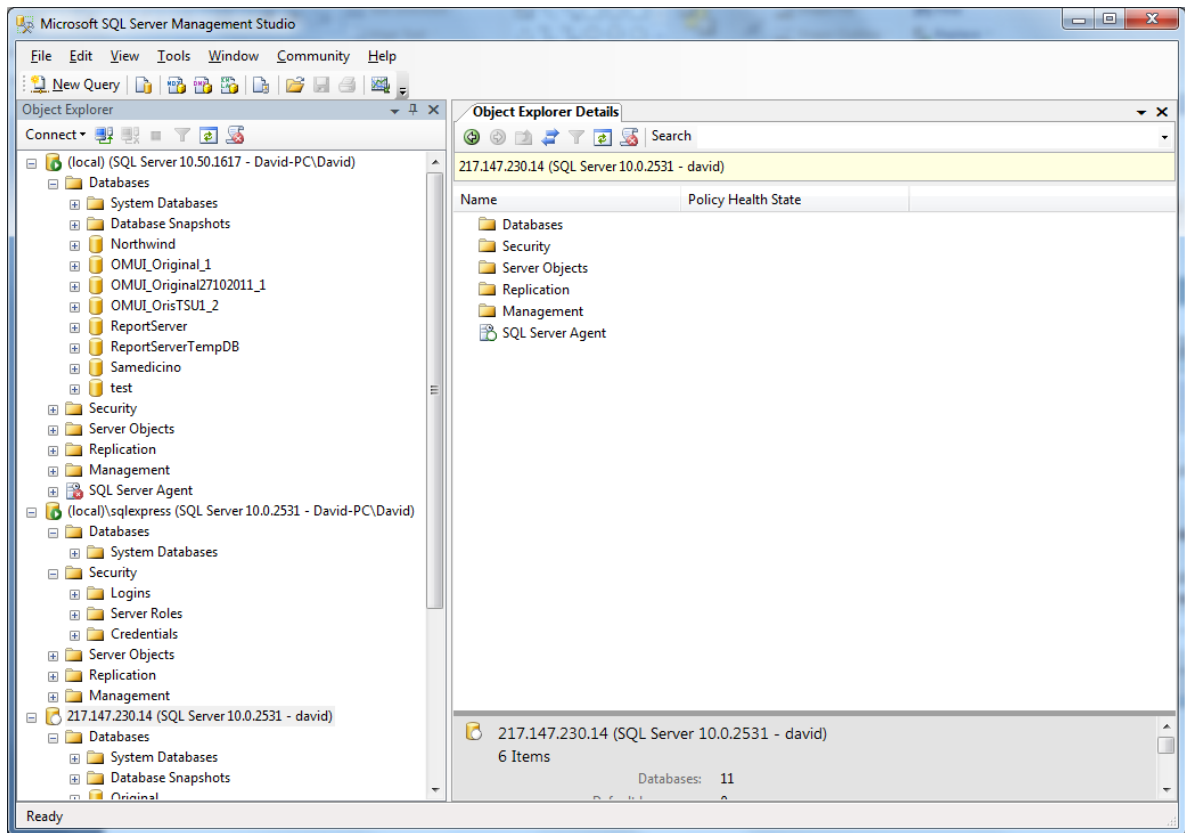
4.3.2. SQL Server-ის ინტერფეისი

სისტემის ინსტალაცია „მეგობრულ“ რეჟიმში მიმდინარეობს და მასზე დეტალურად არ შევჩერდებით. ინსტალაციის დასრულების შემდეგ მომხმარებლის განკარგულებაშია რამდენიმე აპლიკაცია, რომელთაგან ორს გამოვარჩევთ: SQL Server-ის ეგზემპლარების (ინსტანსების) მართვის უტილიტას SQL Server Configuration Manager და მონაცემთა ბაზებთან მიმართვის ინტერფეისს SQL Server Management Studio. პირველი პროგრამა წარმოგვიდგენს ფიზიკურ ან ვირტუალურ სერვერზე (ჰოსტზე) დაყენებული მონაცემთა ბაზის სერვერთა ეგზემპლარებს (ინსტანსებს) და მათზე გამწვებულ სერვისებს, როგორებიცაა: ანალიზის სერვისი (Analysis Services), რეპორტინგის სერვისი (Reporting Services), SQL Server Browser, SQL Server Agent და სხვა, აგრეთვე მათთან მიმართვის საშუალებებს.



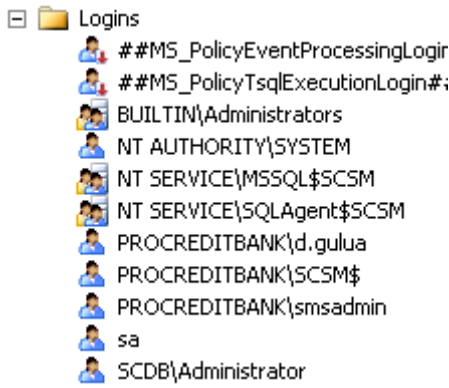
სურ.4.3.2. 1 SQL Server Configuration Manager - SQL-სერვერის ეგზემპლარების და სხვა სერვისების გამართვის უტილიტა

SQL Server Management Studio გრაფიკული ინტერფეისია, რომლის მეშვეობითაც მომხმარებელს მონაცემთა ბაზებთან კომფორტულად მუშაობის საშუალება ეძლევა (სურ.4.3.2.2).

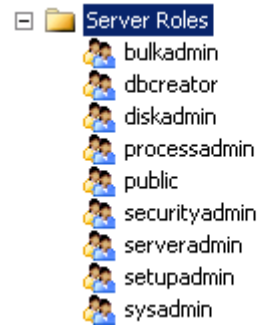


სურ.4.3.2.2 SQL Server Management Studio - ლოკალურ და დაშორებულ სერვერთა ეგზემპლარების მართვის გრაფიკული ინტერფეისი

როგორც სურათიდან ვხედავთ, SQL Server Management Studio მონაცემთა ბაზის სერვერის ზემოთ ჩამოთვლილ ფუნქციებთან მიმართვის საშუალებას გვაძლევს. განსაკუთრებით საყურადღებოა მომხმარებელთა მართვის ინტერფეისი, რომელიც MS SQL Server-ში ორდონიანია: პირველ რიგში აუცილებელი მომხმარებლის საადრიცხვო ჩანაწერის შექმნა მონაცემთა ბაზის სერვერის დონეზე (Database server logins), ხოლო შემდეგ ამ მომხმარებლისთვის კონკრეტულ მონაცემთა ბაზაში გარკვეული უფლებების მინიჭება (Database users). ორივე დონეზე მომხმარებლები ნაწილდებიან გარკვეული წვდომის უფლებათა მქონე ჯგუფებში, რომლებსაც SQL Server-ის ტერმინოლოგიით როლებს უწოდებენ. მონაცემთა ბაზის სერვერის (ეგზემპლარის) მომხმარებლების და როლების ნიმუშები მოცემულია ქვემოთ.

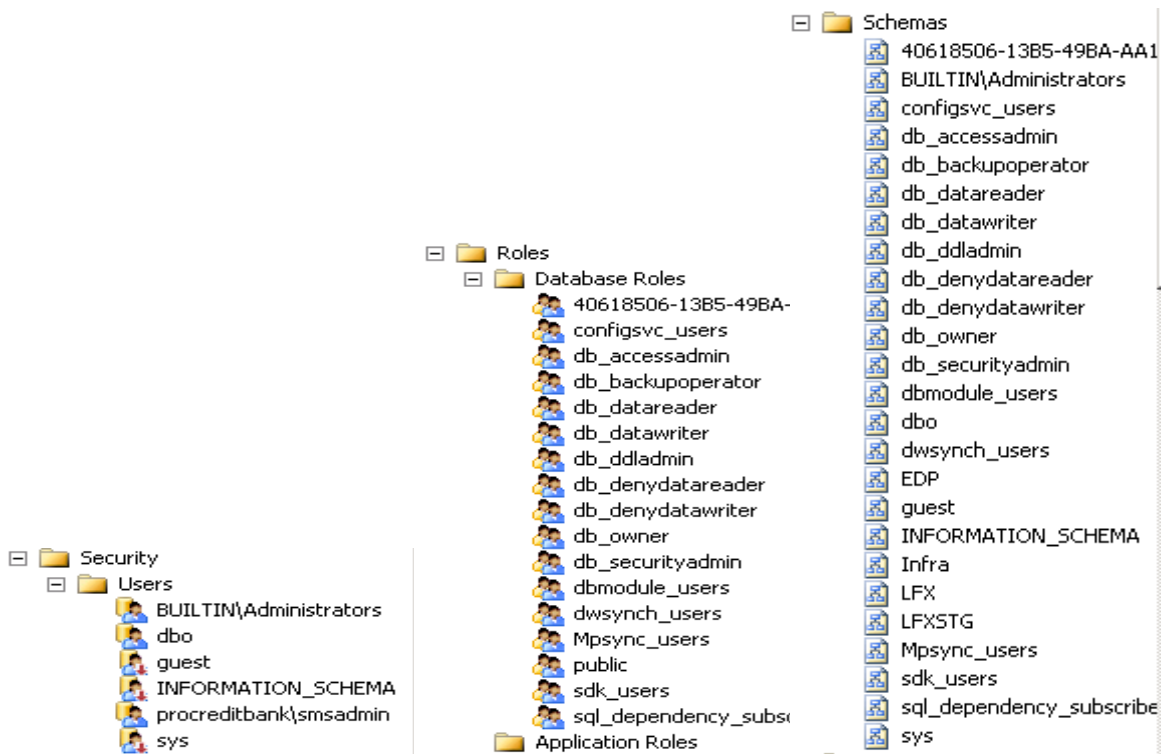


სურ.4.3.2. 3 მზ სერვერის მომხმარებლები



სურ.4.3.2. 4 მზ სერვერის როლები

მონაცემთა ბაზების დონეზე **ბაზის როლებთან** (Database Roles) ერთად ფართოდ გამოიყენება **აპლიკაციის როლების** (Application roles) მექანიზმიც, ხოლო უფლებათა გაწერის ობიექტებს წარმოადგენენ **მონაცემთა ბაზები, ცხრილები, სქემები, ცხრილის ველები და სხვა ობიექტები**. გარდა როლების და მომხმარებლებისა, მონაცემთა ბაზებში გარკვეულ ლოგიკით დაჯგუფებული ცხრილების და სხვა ელემენტების ერთობლიობათა განსაზღვრაც შეიძლება, რომელთაც **სქემები** (Schemes) ეწოდებათ. მონაცემთა ბაზის მომხმარებელთა, როლების და სქემების ნიმუშები იხილეთ ქვემოთ სურათებზე.



მონაცემთა ბაზის მომხმარებლები

მონაცემთა ბაზის როლები

მონაცემთა ბაზის სქემები

4.3.3. მონაცემთა ბაზების მაღალსარგებლიანობის უზრუნველყოფა

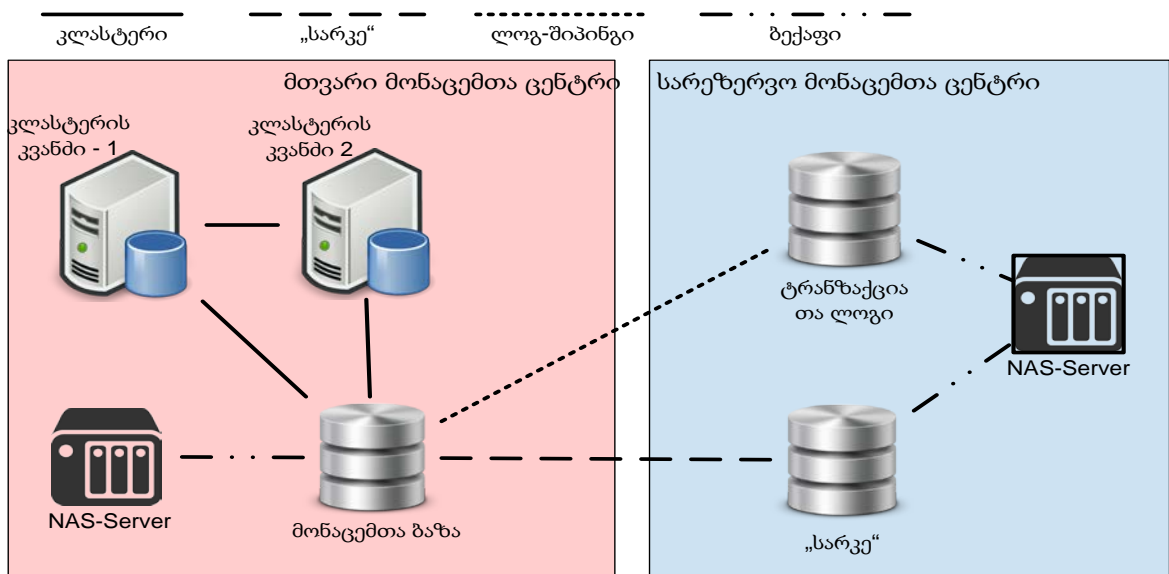
მონაცემთა ბაზებში ინფორმაციის შენახვის სარგებლიანობის მაღალი დონე გულისხმობს მონაცემთა გამრავლების (კოპირების) ისეთი მექანიზმის შემუშავებას, რომლებიც:

- მაქსიმალურად შეამცირებს ინფორმაციის დაკარგვის ალბათობას მინიმალური შესაძლო რესურსების გამოყენებით;
- უზრუნველყოფს დაკარგული ინფორმაციის სწრაფ აღდგენას მინიმალური ინფორმაციული დანაკარგებით.

მოცემული მიზნების მისაღწევად მონაცემთა ბაზების სერვერებსა და მონაცემთა ბაზებზე სრულდება შემდეგი პროცედურები:

- მონაცემთა ბაზების სერვერთა კლასტერის შექმნა;
- მონაცემთა ბაზების სარკული ასახვა (მირორინგი);
- მონაცემთა ბაზების რეპლიკაცია;
- ტრანზაქციათა ჟურნალის გატანა (ლოგ-შიპინგი);
- მონაცემთა ბაზების სარეზერვო კოპირება (ბექაფი).

ჩამოთვლილი თვისებებით აღჭურვილი მონაცემთა ბაზების მაღალსარგებლიანი ინფრასტრუქტურის ნიმუში მოცემულია ნახაზზე.



სურ.4.3.3. 1 მაღალსარგებლიანი მონაცემთა ბაზების ინფრასტრუქტურის მაგალითი

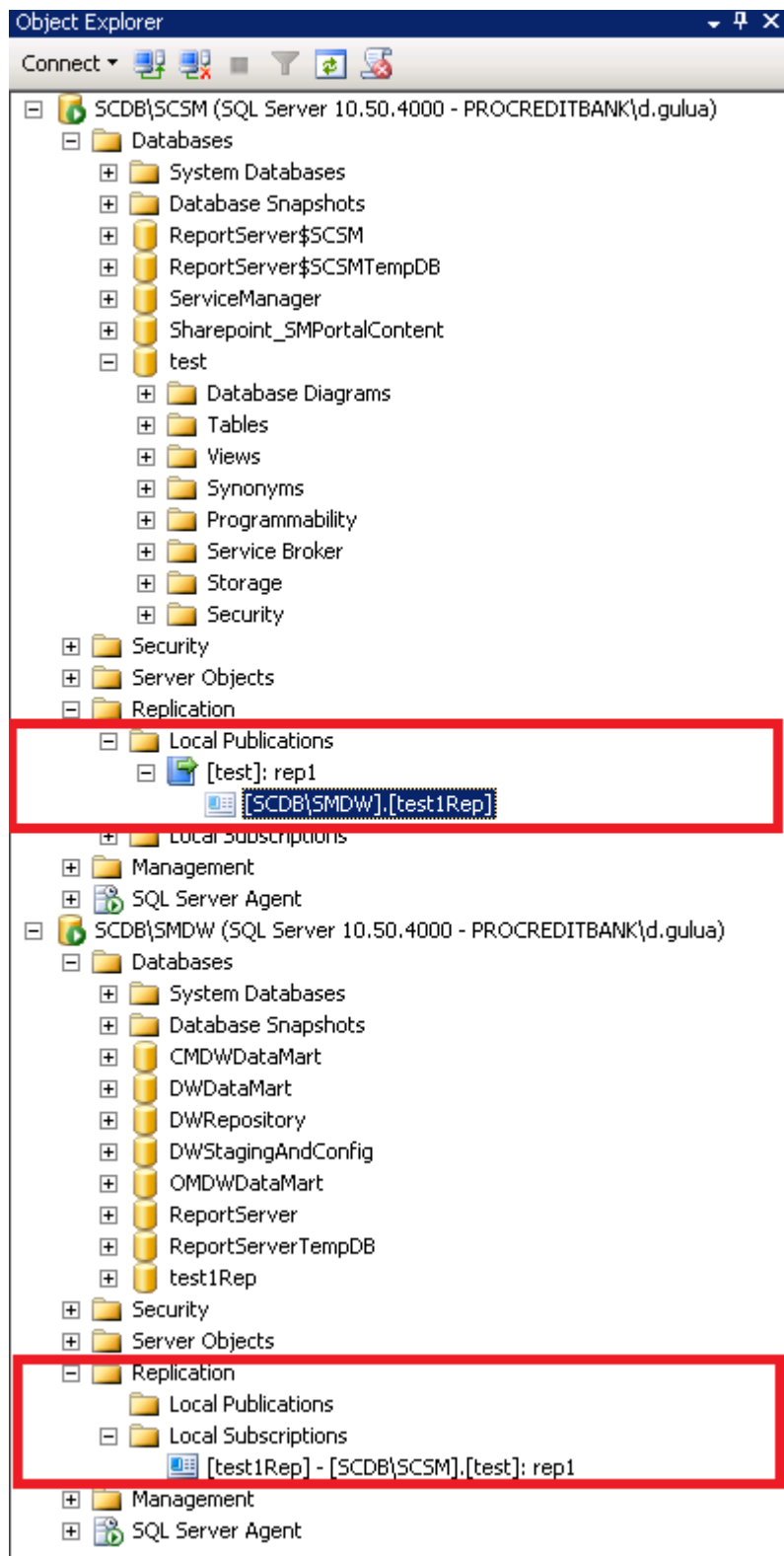
მონაცემთა ბაზის სერვერთა კლასტერი (Database Server Cluster) ბაზის სერვერების ორი ან მეტი ეგზემპლარისთვის (ინსტანსებისთვის) აიგება. ძირითადი SQL-სერვერის ავარიული გათიშვის შემთხვევაში მონაცემთა ბაზების მართვის ფუნქციებს ავტომატურად, Failover-ფუნქციის გამოყენებით, კლასტერის სხვა სერვერი გადაიბარებს. ამრიგად, კლასტერული არქიტექტურა ერთადერთია, რომელიც არა **მონაცემთა ბაზების**, არამედ **მონაცემთა ბაზის სერვერების** დონეზე მუშაობს.

რეპლიკაცია (Database Replication) შეიძლება განვავრცოთ მთლიან მონაცემთა ბაზაზე ან მის ნაწილზე (ცხრილები, სქემები და სხვა). მის დანიშნულებას მონაცემთა ბაზებს შორის ინფორმაციის საიმედო გაცვლის უზრუნველყოფა წარმოადგენს: **მონაცემთა გამცემი (Database Publication)** მუდამ უახლეს ინფორმაციას აწვდის **მონაცემთა მიმღებს (Database Subscription)**. იხილეთ სურათი მომდევნო გვერდზე.

ლოგ-შიპინგი (Log shipping) მონაცემთა სარეზერვო კოპირების ყველაზე იაფ და იოლად განხორციელებად საშუალებას წარმოადგენს. მისი საშუალებით სრულდება **მონაცემთა ბაზის ტრანზაქციათა ლოგის** (ანუ ბაზაში შესრულებული მოქმედებების სრული ჟურნალის) კოპირება სხვა სერვერზე, ხოლო ძირითადი ბაზის დაკარგვის შემთხვევაში არის შესაძლებლობა ლოგიდან ბაზის აღდგენისა. ლოგ-შიპინგის მიზნის ისაა, რომ საწყისი ბაზის აღდგენას ხშირად საკმაოდ დიდი დრო სჭირდება.

მირორი („სარკე“) (Database Mirror) მონაცემთა ბაზისთვის სხვა SQL Server-ის ეგზემპლარზე იდენტური მონაცემთა ბაზის შექმნას გულისხმობს. ნებისმიერი ცვლილება **საწყის ბაზაში (Primary Database)** ავტომატურად ფიქსირდება „**სარკე**“-**ბაზაშიც (Secondary Database)**. საწყისი მონაცემთა ბაზის მწყობრიდან გამოსვლის შემთხვევაში ადმინისტრატორი შეასრულებს გადართვას ბაზის სათადარიგო ეგზემპლარზე. გადართვა შეიძლება ავტომატურ რეჟიმშიც განხორციელდეს, მესამე, ე.წ. „**მოწმე**“-**სერვერის (Witness Server)** გამოყენებით. სარკული ასახვა 1:1-ტიპის სტრუქტურაა, მონაცემთა ბაზას მხოლოდ ერთი „სარკული“ ასლი შეიძლება გააჩნდეს.

და ბოლოს, მონაცემთა ბაზების **სარეზერვო ასლების (Backup)** შექმნა-ტრანსპორტირება გულისხმობს ბაზის ასლის შექმნას კონკრეტული დროის მდგომარეობით. სარეზერვო ასლების ფორმირების თემა დეტალურად მომდევნო ქვეთავში იქნება აღწერილი.



სურ.4.3.3. 2 რეპლიკაციის ნიმუში MS SQL Server-ში

4.3.4. მონაცემთა ბაზების სარეზერვო კოპირება

სარეზერვო კოპირებას დროის კონკრეტულ მომენტში მონაცემთა ბაზის მდგომარეობის დასაფიქსირებლად და შესანახად იყენებენ. სარეზერვო ასლის შექმნის შემდეგ (Database Backup), საჭიროების შემთხვევაში, შესაძლებელია მონაცემთა ბაზის აღდგენა (Restore) იმ მდგომარეობაში, რომელშიც იგი სარეზერვო ასლის შექმნისას იმყოფებოდა.

სარეზერვო ასლები ორ ძირითად ფორმატში ინახება: .bak-ფაილში სრული ან დიფერენციალური ასლები იქმნება, ხოლო .trn-ფაილები ტრანზაქციების ჟურნალს (ანუ ლოგებს) ინახავს. მარტივი სარეზერვო ასლის შესაქმნელად ადმინისტრატორმა SQL Server Management Console-ში უნდა გამოიძახოს ბრძანება:

მონაცემთა ბაზაზე მაუსის მარჯვენა ღილაკი -> Tasks -> Backup

ხოლო აღსადგენად:

მონაცემთა ბაზაზე მაუსის მარჯვენა ღილაკი -> Tasks -> Restore -> Database

ორივე შემთხვევაში გამოდის საკმაოდ მარტივი ინტერფეისი, რომელშიც სისტემის ან/და მონაცემთა ბაზის ადმინისტრატორი ადვილად გაერკვევა. განვიხილოთ შედარებით კომპლექსური ამოცანა, რომელიც ორგანიზაციის ინფორმაციული სისტემების მონაცემთა ბაზების, გეგმიურ, ავტომატიზებულ სარეზერვო კოპირებასა და სარეზერვო ასლების დაშორებულ საცავში (NAS-სერვერზე) გადატანას გულისხმობს.

სანიმუშოდ ავაგოთ ორგანიზაციის ორი (კადრების და ბუღალტერიის) მონაცემთა ბაზების სარეზერვო კოპირების გრაფიკი.

მბ სერვერი	მონაცემთა ბაზა	ბეჭაფის ტიპი	თარიღი და დრო
HR	HRMain	სრული	ყოველ კვირადღეს 1:00AM
	HRMain	დიფერენციალური	ყოველდღე გარდა კვირისა 1:00AM

	HRFiles	სრული	ყოველ კვირადღეს 12:30AM
	HRFiles	დიფერენციალური	ყოველდღე 12:30AM
	HRMain, HRFiles	NAS-ზე კოპირება	ყოველ კვირადღეს 2:30AM
Accounting	AccountingDB	სრული	ყოველ კვირადღეს 1:00AM
	AccountingDB	დიფერენციალური	ყოველდღე გარდა კვირისა 1:00AM
	AccountingDB	სრული	ყოველი თვის პირველ რიცხვში 2:00AM
	AccountingDB	NAS-ზე კოპირება	ყოველდღე 1:30AM

მოცემული გრაფიკის რეალიზაციას რამდენიმე პროგრამული მოდულის გამოყენება სჭირდება:

- SQL Server Management Studio
 - Management -> Maintenance Plans
 - SQL Server Agent;
- NAS-სერვერის (Network Area Storage) მართვის პროგრამა.

მონაცემთა ბაზების მოვლის მოდული (Management -> Maintenance Plans) არამარტო სარეზერვო კოპირების, არამედ მონაცემთა ბაზების ოპტიმალურ მდგომარეობაში შენახვის მრავალფეროვან ამოცანებს ემსახურება. ჩამოვთვალოთ რამდენიმე:

- სარეზერვო ასლების შექმნა და წაშლა;

- მონაცემთა ცხრილები რეინდექსაცია/ინდექსების რეორგანიზაცია მონაცემთა ბაზასთან მიმართვის დასაჩქარებლად;

- მონაცემთა ბაზების შეკუმშვა (Shrinking) გარე მეხსიერების ეკონომიისთვის;
- MS SQL Server-ის გარემოში T-SQL-სკრიპტების გაშვება;
- და სხვა მრავალი...

მონაცემთა ბაზის მოვლის გეგმა ყალიბდება **ქვეამოცანების** (Subplans) მიმდევრობის სახით. საჭიროების შემთხვევაში დგება განრიგი ანუ თითოეულ მოქმედებას (ბიჯს) განესაზღვრება შესრულების თარიღი და დრო. მაგალითად, მონაცემთა ბაზების, HRMain და HRFiles-ისთვის ზემოთ მოცემული სარეზერვო კოპირების გეგმის შესასრულებლად საჭირო ბიჯები შემდეგი სახით შეიძლება წარმოვადგინოთ:

- ყოველ კვირა დღეს, ღამის 12 საათსა და 30 წუთზე იქმნება **სრული** სარეზერვო ასლი მონაცემთა ბაზისთვის HRFiles. იმავე სახელის მქონე არსებული სარეზერვო ასლი იშლება;

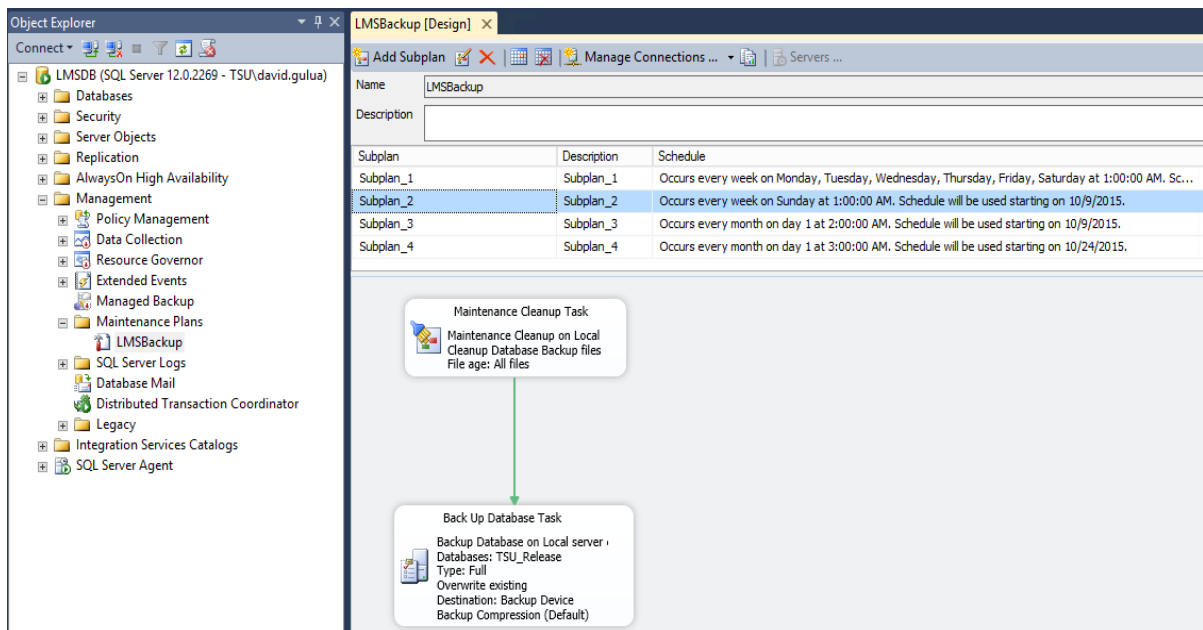
- ყოველდღე, გარდა კვირისა, ღამის 12 საათსა და 30 წუთზე მონაცემთა ბაზის არსებულ სარეზერვო ასლს ზემოდან „დააშენდება“ **დიფერენციალური** სარეზერვო ასლი (დიფერენციალური სარეზერვო ასლი მხოლოდ იმ ცვლილებებს ინახავს, რომლებიც მონაცემთა ბაზაში ბოლო სარეზერვო ასლის აღების შემდეგ იქნა განხორციელებული);

- ყოველ კვირა დღეს, ღამის 1 საათზე იქმნება სრული სარეზერვო ასლი მონაცემთა ბაზისთვის HRMain. იმავე სახელის მქონე არსებული სარეზერვო ასლი იშლება;

- ყოველდღე, გარდა კვირისა, ღამის 1 საათზე მონაცემთა ბაზის არსებულ სარეზერვო ასლს ზემოდან „დააშენდება“ **დიფერენციალური** სარეზერვო ასლი;

- ყოველ კვირადღეს, ღამის 2 საათსა და 30 წუთზე სრულდება HRFiles და HRMain-ბაზების სარეზერვო ასლების კოპირება მონაცემთა ქსელურ საცავში (NAS-სერვერი).

აღწერილი ამოცანის შესრულების ინტერფეისი მოცემულია სურ.4.3.4.1-ზე

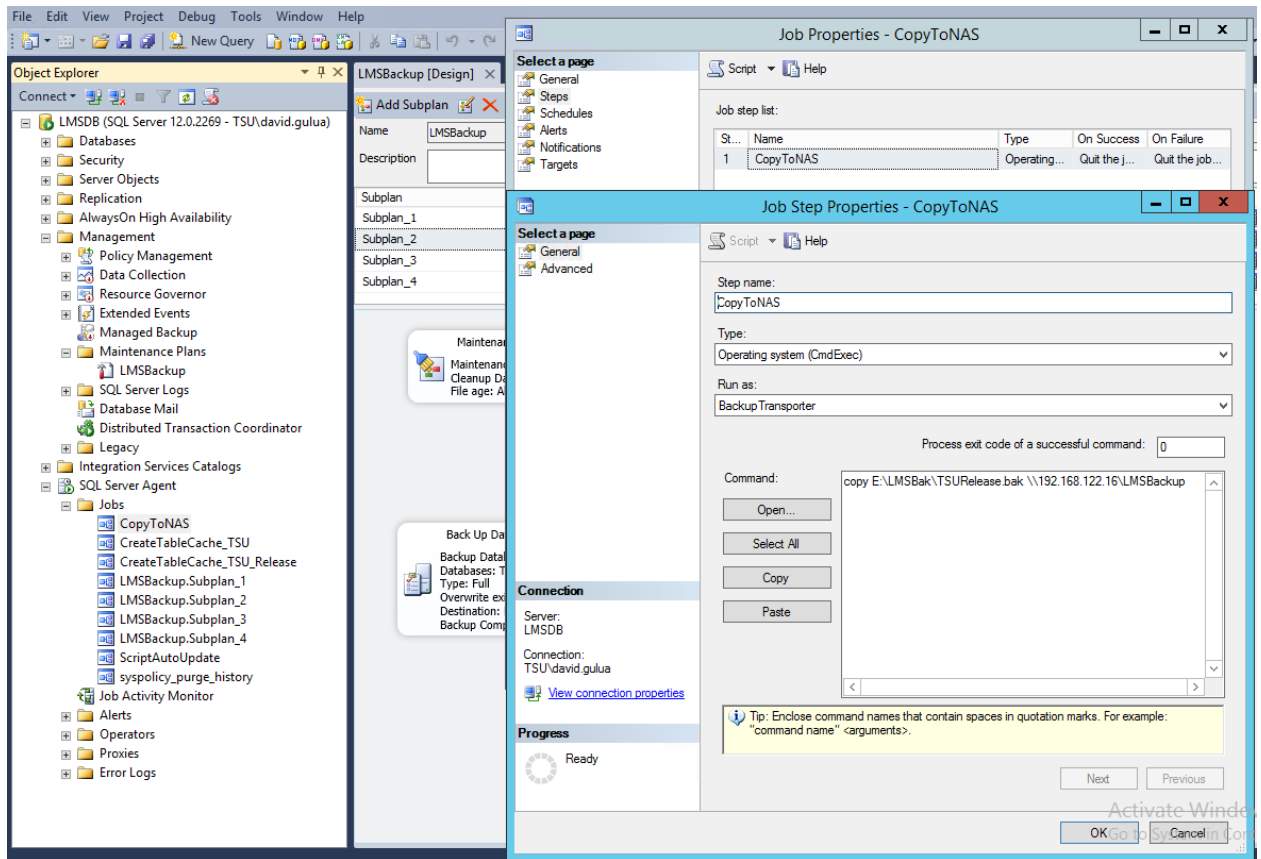


სურ.4.3.4. 1 SQL Server-ის მოვლის გეგმის (Maintenance Plan) ნიმუში მონაცემთა ბაზების სარეზერვო კოპირებისთვის

ყოველი ბიჯი თავის შესრულების გეგმით მიეწოდება Microsoft Windows-ის სერვისს SQL Server Agent (SQL Server Agent -> Jobs), რომელიც მათ შესრულებას უზრუნველყოფს. ინფორმაცია შესრულებული სამუშაოს შესახებ ინახება იმავე პროგრამული მოდულის SQL Server Log-განყოფილებაში (სურათი). სურათზე საყურადღებოა ის გარემოება, რომ SQL Server Agent-ის გარემოში შესაძლებელია არამარტო SQL-ის, არამედ ოპერაციული სისტემის ბრძანებათა ინტეგრირებაც, მაგალითად სარეზერვო ასლების ერთი ადგილიდან (SQL-ჰოსტი) მეორეზე (NAS-სერვერი) კოპირებისთვის. მოვიყვანოთ ორი CMD-ბრძანებისგან შემდგარი სკრიპტი კოპირების ამოცანისთვის, სადაც ბრძანებების გამყოფად „&&“-სიმბოლოების წყვილი გამოიყენება:

copy E:\Bak\HRMain.bak [\\192.168.122.16\Backup](http://192.168.122.16) &&

copy E:\Bak\HRFiles.bak [\\192.168.122.16\Backup](http://192.168.122.16)



სურ.4.3.4.2 SQL Server Agent-ის ჯობების ინტერფეისი

პრაქტიკული სავარჯიშო

1. შეასრულეთ პროგრამა MS SQL Server 2012-ის ინსტალაცია;
2. აამუშავეთ უტილიტა SQL Server Configuration Manager. დააფიქსირეთ ახლად შექმნილი მონაცემთა ბაზის სერვერის ეგზემპლარი (ინსტანსი) და შეამოქმეთ მისი მდგომარეობა;
3. შექმენით 2-3 ცხრილისგან ახალი მონაცემთა ბაზა, შეავსეთ იგი სატესტო მონაცემებით;
4. შეასრულეთ მონაცემთა ბაზის სარეზერვო კოპირება, წაშალეთ საწყისი ბაზა და აღადგინეთ იგი სარეზერვო ასლიდან.

ცოდნის შეფასება

სტუდენტებს მიეცემათ პრაქტიკული დავალება

- შეასრულონ სატესტო სერვერზე ვების და ფაილური სერვერების როლების აქტივაცია და დააყენონ მონაცემთა ბაზების მართვის სისტემა MS SQL Server და კორპორაციული რესურსების მართვის სისტემა SharePoint;
- შეასრულონ ვებ-სერვერზე ინფორმაციის ატვირთვა და ააწყო მარტივი კორპორაციული პორტალი (დოკუმენტების საცავით, კალენდრით და სადისკუსიო დაფით);
- წარმოადგინონ ფაილური რესურსების მართვის ინსტრუმენტები (კვოტირება, ქსელური დისკების მართვა, კატალოგების გადამისამართება);
- ააგონ მარტივი მონაცემთა ბაზა და შეასრულონ მასში სარეზერვო კოპირებისა და მონაცემთა ბაზის აღდგენის ამოცანები.

შემფასებელი აკვირდება შესაფასებელ პირის მუშაობას პროფესიული სტანდარტით (პროგრამით / მოდულით) განსაზღვრული ამოცანების შესრულების პროცესში. დაკვირვება ხორციელდება კომპიუტერებით აღჭურვილ ლაბორატორიაში, სადაც შესაფასებელი პირი პრაქტიკულ საქმიანობას ეწევა. შემფასებელმა წინასწარ უნდა დაგეგმოს დაკვირვების პროცესი, იმის დასადგენად, თუ რამდენად სწორად იყენებს შესაფასებელი პირი ცოდნას, უნარებსა და ყველა რესურსს შედეგის მისაღწევად.

შეფასება განხორციელდება პროცესზე დაკვირვებით, წინასწარ განსაზღვრული შეფასების ინდიკატორების საფუძველზე.

დავალების ნიმუში და შეფასების რუბრიკა

პროცესზე დაკვირვება

- ✚ შეასრულოს სხვადასხვა სერვერული პროგრამების (ვები, ფაილ-სერვისი, მონაცემთა ბაზები) აქტივაცია/ინსტალაცია
- ✚ გამოიყენოს დაყენებული სერვერული პროგრამები სატესტო ამოცანებისთვის (ვებ-პორტალის აწყობა, ფაილური რესურსების მართვა, მონაცემთა ბაზების სარეზერვო კოპირება)

სწავლის შედეგი	N	დასახელება	შეფასება	
			კი	არა
ვებს, ფაილური და მონაცემთა ბაზის სერვერების გამართვა	11.	შეასრულა ვებ-სერვერის აქტივაცია		
	12.	შეასრულა ფაილური სერვისის აქტივაცია		
	13.	დააყენა მზმს MS SQL Server		
	14.	დააყენა სისტემა MS Share Point		
	15.	ატვირთა HTML-ფაილი ვებ-სერვერზე და და გამოიტანა მისი შიგთავსი ბრაუზერებში		
	16.	შექმნა SharePoint-ში დოკუმენტების საცავი, ახალი კალენდარი და სადისკუსიო დაფა		
	17.	შექმნა SharePoint-ის ახალი მომხმარებლები და გაუწერა მათ უფლებები		
	18.	შეასრულა ფაილ-სერვერის დისკის კვოტირება, მათ შორის ცალკეული მომხმარებლებისთვის		
	19.	შექმნა ჯგუფური პოლიტიკები ქსელური დისკისა და ფოლდერების გადასამისამართებლად		
	20.	შექმნა ახალი მონაცემთა ბაზა MS SQL Server-ში, შეავსო იგი ცხრილებით და მონაცემებით. შეასრულა ბაზის სარეზერვო კოპირება და აღდგენა		

სწავლის შედეგი ჩაითვლება მიღწეულად თუ სტუდენტმა შეძლო შედეგის მინიმუმ 8 პუნქტის შესრულება

5. საფოსტო და საკომუნიკაციო სერვერების გამართვა

5.1. საფოსტო სერვერის მართვა

5.1.1. საფოსტო და საკომუნიკაციო სერვისების ზოგადი მიმოხილვა

სწრაფი და საიმედო კომუნიკაცია 21-ე საუკუნეში საქმის წარმოების ერთერთ უმთავრეს წინაპირობას წარმოადგენს. სადღეისოდ ინტერნეტის ფიზიკური მონაცემები (კარგად განვითარებული ქსელური და კაბელური ინფრასტრუქტურა, ინფორმაციის გადაცემის საიმედო პროტოკოლები) უკვე იძლევა დიდი მოცულობის ინფორმაციის მთელი პლანეტის ფარგლებში გადაცემის საშუალებას, თუმცა ეს პრობლემის მხოლოდ ერთი ნაწილია. არანაკლებ მნიშვნელოვანია ინფორმაციის გაცვლის პროცესის იმგვარად ორგანიზება, რომ კომპიუტერული სისტემების და ზოგადად ინტერნეტის მომხმარებლებმა მაქსიმალურად მრავალფეროვანი ინფორმაციის (ტექსტი, გამოსახულება, ხმა, ვიდეო) გაცვლა შესძლონ და ამასთან, მაღალი დონის უსაფრთხოებით და საიმედოობით.

ნებისმიერი თანამედროვე, მეტნაკლებად დიდი ორგანიზაციის გამართული მუშაობისთვის სტაბილური საკომუნიკაციო სისტემების არსებობა აუცილებელია. ითვლება, რომ კორპორაციულ ქსელში კომუნიკაციის შემდეგი სისტემები უნდა არსებობდეს:

- ელექტრონული ფოსტა;
- სატელეფონო სერვისი (ქალაქის და მობილური);
- მყისიერ შეტყობინებათა სერვისი;

პროგრამული უზრუნველყოფის ბაზარზე მრავალი საკომუნიკაციო პროგრამული უზრუნველყოფა არსებობს. გასული საუკუნის 90-იანი წლების პირველი ნახევრიდან, ანუ ინტერნეტის განვითარების კვალდაკვალ, შეტყობინებათა გადაცემის სერვისები გამოდის ვიწრო ინფორმაციული სეგმენტებიდან (სამეცნიერო კვლევითი ორგანიზაციები, სამხედრო საქმე) და ელექტრონული ფოსტის სახელით იმკვიდრებს თავს მომხმარებელთა ფართო წრეში. ელექტრონული ფოსტა ორგანიზაციის საკომუნიკაციო ინფრასტრუქტურის პირველადი, ყველაზე „ოფიციალური“ კომპონენტია.

გამართული სატელეფონო კავშირის არსებობა აუცილებელია როგორც ორგანიზაციის შიდა, ასევე გარე კომუნიკაციისთვის. ამასთან, თანამედროვე ორგანიზაციის სატელეფონო სერვისი დამატებით მოთხოვნებსაც უნდა პასუხობდეს. კლიენტთა მომსახურების განყოფილება (**ქოლ-ცენტრი**), თანამშრომელთა მხარდაჭერის განყოფილება (**ჰელდესკი**) ის სტრუქტურული ერთეულებია, სადაც თანამშრომელთა ვალდებულებას შემოსული ზარების მაქსიმალური რაოდენობით მიღება და მომსახურება წარმოადგენს, რისთვისაც ზარების ოპტიმალური გადანაწილებაა საჭირო. ამგვარი ამოცანების გადასაჭრელად ადრე ანალოგური სატელეფონო ინფრასტრუქტურა გამოიყენებოდა, რომელსაც სადღეისოდ ინტენსიურად ანაცვლებს VoIP-ტექნოლოგია (Voice over IP) IP-პროტოკოლის გამოყენებით და აქედან გამომდინარე, ორგანიზაციის კომპიუტერულ ინფრასტრუქტურასთან ინტეგრირების გაუმჯობესებული მეთოდებით. VoIP ზოგადი ცნებაა და არამარტო სატელეფონო კომუნიკაციის, არამედ დაკვირვების, სასიგნალო და სხვა სისტემებშიც გამოიყენება.

აპარატული და პროგრამული უზრუნველყოფის ბაზარზე სადღეისოდ რამდენიმე წამყვანი სატელეფონო სისტემაა წარმოდგენილი. მათი უმრავლესობა პროპრიეტარულია (ფასიანია) როგორც აპარატულად, ასევე პროგრამულად, თუმცა არსებობს ეფექტური სისტემები Open Source-კოდით, სადაც მომხმარებელს მხოლოდ აპარატული პლატფორმის ხარჯების გაღება უწევს. პირველი ჯგუფის პროდუქტებიდან ლიდერობს კომპანია Cisco, რომელიც ტელეფონიის სრულფასოვან ინფრასტრუქტურას აწარმოებს დაწყებული ქსელური მოწყობილობებით და სერვერებით და დასრულებული IP-ტელეფონებით. მეორე ჯგუფის სისტემებიდან საქართველოში ყველაზე მეტად Asterisk-სისტემებია გავრცელებული.

პარალელურად, უწყვეტად ვითარდება **მყისიერ შეტყობინებათა** (Instant Messaging) სერვისებიც. 1988 წელს დამუშავებული პროტოკოლი IRC (Internet Relay Chat) ამ მიმართულებით „პირველ მერცხალს“ წარმოადგენდა. მის ბაზაზე იმპლემენტირებული პროგრამები (პირველ რიგში miRC) ყველაზე პოპულარული მყისიერი კომუნიკაციის (Instant Messaging) საშუალებას წარმოადგენდა საქართველოში ინტერნეტის განვითარების გარიჟრაჟზე.

ჩვენს საუკუნეში მყისიერ შეტყობინებათა სერვისებმა უდავო პროგრესი განიცადეს. გამოვიდა მრავალი პოპულარული პროგრამა (ICQ, Windows Live Messenger, Yahoo!

Messenger, Skype, ooVoo, AIM, ICQ, MSN, Jitsi, XMPP). გარდა ამისა, მყისიერ შეტყობინებათა მოდულები პოპულარული პროგრამული პროდუქტების და ონლაინ-სისტემების (მაგ. სოციალური ქსელები) განუყრელ ნაწილად იქცა. სადღეისოდ მათ პრაქტიკულად ნებისმიერი ტიპის მონაცემებთან სწრაფად და საიმედოდ მუშაობა შეუძლიათ.

უნდა ითქვას, რომ მყისიერ შეტყობინებათა (Instant Messaging) სერვისის საზოგადოდ ცნობილი პროგრამული უზრუნველყოფა (Skype და სხვა) შიდა, კორპორაციული ქსელის ფარგლებში ნაკლებად გამოსადეგია. თუმცა შესაძლებელია მყისიერ შეტყობინებათა ცნობილი სერვისების მორგება კორპორაციულ ინფორმაციულ ინფრასტრუქტურაზე, მაგრამ სისტემის ადმინისტრატორებს უჭირთ აკონტროლონ Skype-ის, Google Talk-ის და სხვა ამგვარი სისტემების მომხმარებლები. **შიდა მყისიერ შეტყობინებათა სერვისები** (მაგ. MS Lync), მათი გლობალური კოლეგებისგან განსხვავებით, პირდაპირ ორგანიზაციის საკომუნიკაციო მოთხოვნებზეა მორგებული და გარე სამყაროსთან ყოველგვარი კავშირის გარეშე მუშაობენ. მიმდინარე ეტაპზე მსგავსი სისტემები მრავალი ოპერაციული სისტემისთვის არსებობს.

5.2. შიდა კომუნიკაციის პროგრამული უზრუნველყოფის სერვერების მართვა

5.2.1. საფოსტო სერვისის მართვა Microsoft Exchange Server-ის გარემოში

5.2.1.1. Exchange Server-ის სტრუქტურა

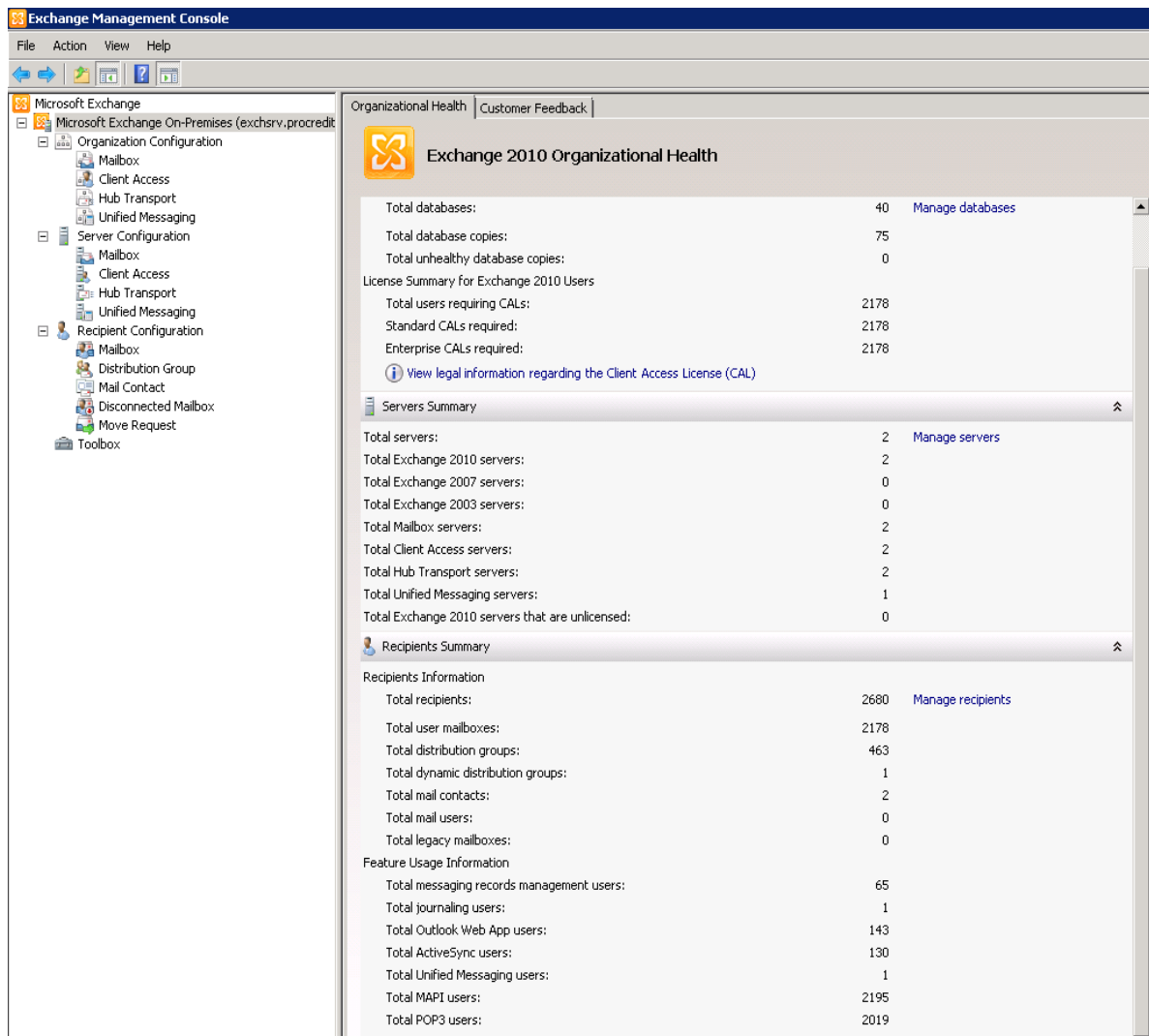
ელექტრონული ფოსტა შიდა და გარე კომუნიკაციის ძირითად ფორმას წარმოადგენს. მიუხედავად იმისა, რომ სადღეისოდ უამრავი კომპანია სხვადასხვა სერვისების და მათ შორის, ელექტრონული ფოსტის სამართავად მომხმარებლებს „ღრუბლოვან“ სივრცეებს სთავაზობს, დიდი ორგანიზაციებისთვის ელექტრონული ფოსტის შიდა ინფრასტრუქტურის განვითარება მაინც აუცილებელ ამოცანად რჩება.

პროგრამა MS Exchange Server კორპორაციულ ქსელში ელექტრონული ფოსტის მართვის მძლავრ საშუალებებს ფლობს. შევხებით პირველ რიგში აპარატულ-პროგრამულ მოთხოვნებს და ელექტრონული ფოსტის მონაცემთა შენახვის და მართვის საშუალებებს.

MS Exchange Server რესურსების მიმართ პრეტენზიული პროგრამაა. სისტემის წარმატებული ინსტალაციის და საწარმოო რეჟიმში გაშვების შემდეგ ადვილი შესამჩნევია, რომ სერვერის პროცესორისა და განსაკუთრებით ოპერატიული მეხსიერების მოზრდილ წილს პროცესი Store.exe (MS Exchange Server-ის მთავარი შერულებადი ფაილი) ფლობს, ამიტომ სისტემის ადმინისტრატორებს მსგავსი სისტემების მართვისას მწარმოებლურობის მაჩვენებლებზე მუდმივად ყურადღების გამახვილება უწევთ.

სისტემა MS Exchange Server აუთენტიფიკაციას, როგორც წესი, დომენურ სისტემაში ასრულებს, ანუ ელ.ფოსტის სერვერის მომხმარებლები იგივე დომენური მომხმარებლებს წარმოადგენენ.

სერვერზე ინფორმაცია იერარქიულად ინახება: ელ.ფოსტის ფაილურ საცავს მეილების მონაცემთა ბაზა ანუ **სთორი** (Store) ეწოდება, რომელიც თავის მხრივ, გარკვეული რაოდენობის, მომხმარებელთა ელექტრონული ფოსტის მისამართებთან დაკავშირებული **საფოსტო ყუთებისგან** (Mailboxes) შედგება. სწორედ სთორების შექმნისას ითვალისწინებენ დაწესებულების ორგანიზაციული სტრუქტურას: მაგალითად, ცალკე სთორებში შეიძლება იყოს თავმოყრილი უმაღლესი და საშუალო რგოლის მენეჯერების, აგრეთვე სხვადასხვა დეპარტამენტების რიგით თანამშრომელთა საფოსტო ყუთები. ამგვარი მიდგომა გარე მეხსიერების და სხვა რესურსების, აგრეთვე ელექტრონული ფოსტის გამოყენების განსხვავებული წესების დადგენის საშუალებას იძლევა. ქვემოთ, სურათზე ნაჩვენებია MS Exchange-ის მართვის პანელის (Exchange Management Console) საწყისი ფანჯარა ინფორმაციით Exchange-სერვერების, ელ.ფოსტის მონაცემთა ბაზების (სთორების) და საფოსტო ყუთების (მეილბოქსების) შესახებ.



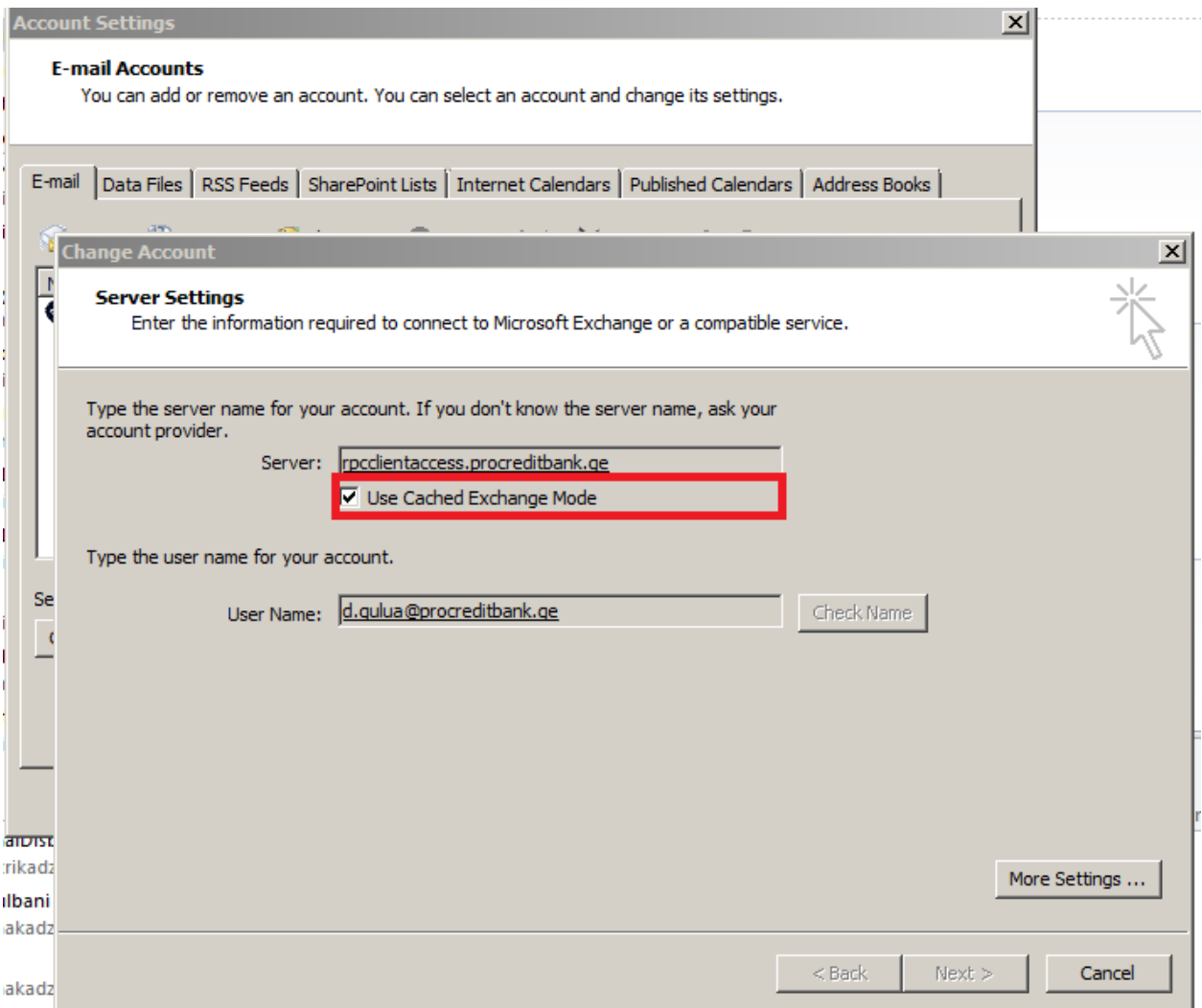
Exchange Management Console-ს მთავარი ფანჯარა

სურათის მიხედვით, Exchange-სერვისი 2 Exchange-სერვერზე მუშაობს, რაც მთლიანად სისტემის სარგებლიანობის ამაღლებას ემსახურება. სპეციალური, DAG-სერვისი (Database Availability Group) უზრუნველყოფს სთორების და მეილბოქსების რეპლიკაციას სერვერებს შორის, რომელთაგან ერთი მუდმივად აქტიურ, ხოლო მეორე - პასიურ მდგომარეობაში იმყოფება. მთავარი სერვერის გათიშვისას DAG-სერვისი მართვას ავტომატურად სათადარიგო სერვერს გადასცემს. ქსელური კავშირები Exchange-სერვერებს შორის დუბლირებულია, რაც ასევე ამაღლებს მთლიანი სისტემის სარგებლიანობას (სურათი).

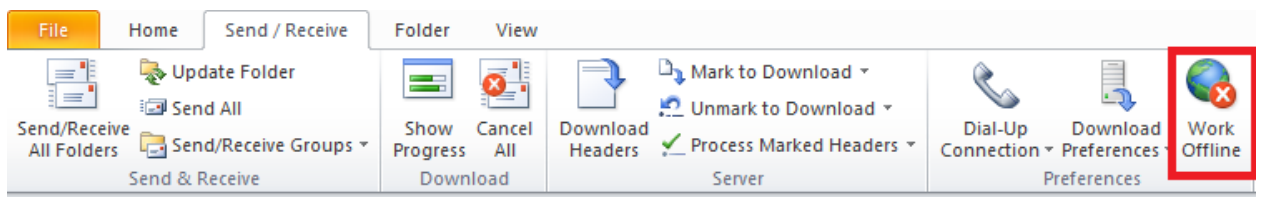
Dag		4 objects
Networks		
Name	Status	
33_DAG		
Replication Enabled		
Subnets		
192.168.33.0/24	Up	
Network Interfaces		
192.168.33.32	Up	
192.168.33.33	Up	
DAGNetwork01		
Replication Disabled		
Subnets		
192.168.252.0/24	Up	
Network Interfaces		
192.168.252.248	Up	
DAGNetwork02		
Replication Enabled		
Subnets		
192.168.253.0/24	Up	
Network Interfaces		
192.168.253.233	Up	
DAGNetwork03		
Replication Disabled		
Subnets		
192.168.16.0/24	Up	
Network Interfaces		
192.168.16.248	Up	

DAG-სერვისის მართვის ინტერფეისი

Exchange Server-ის მომხმარებელს სერვერთან პირდაპირ მიმართვის (online) და კეშის (Cached Exchanged Mode) რეჟიმებში მუშაობის საშუალებას აძლევს. მეორე რეჟიმი მოხერხებულია, როცა მოხმარებელს ელ.ფოსტის სერვერთან მუდმივი ან/და სწრაფი კავშირის საშუალება არ გააჩნია. ასეთ შემთხვევაში ელექტრონული წერილები, კონტაქტები, კალენდარი, ამოცანები და მომხმარებლის სხვა რესურსები ლოკალურ კეშში, კერძოდ .ost-ფაილებში იყრის თავს და სერვერთან პერიოდულ სინქრონიზაციას ასრულებს (ზოგადად, ლოკალური მეიბოქსები კომპიუტერზე .pst-ფორმატის ფაილებში ინახება). სურათზე ნაჩენებია ელ.ფოსტის კლიენტ-პროგრამაში (MS Outlook) კეშის რეჟიმის აქტივაციისა და ოფლაინ-რეჟიმზე გადართვის დიალოგები.



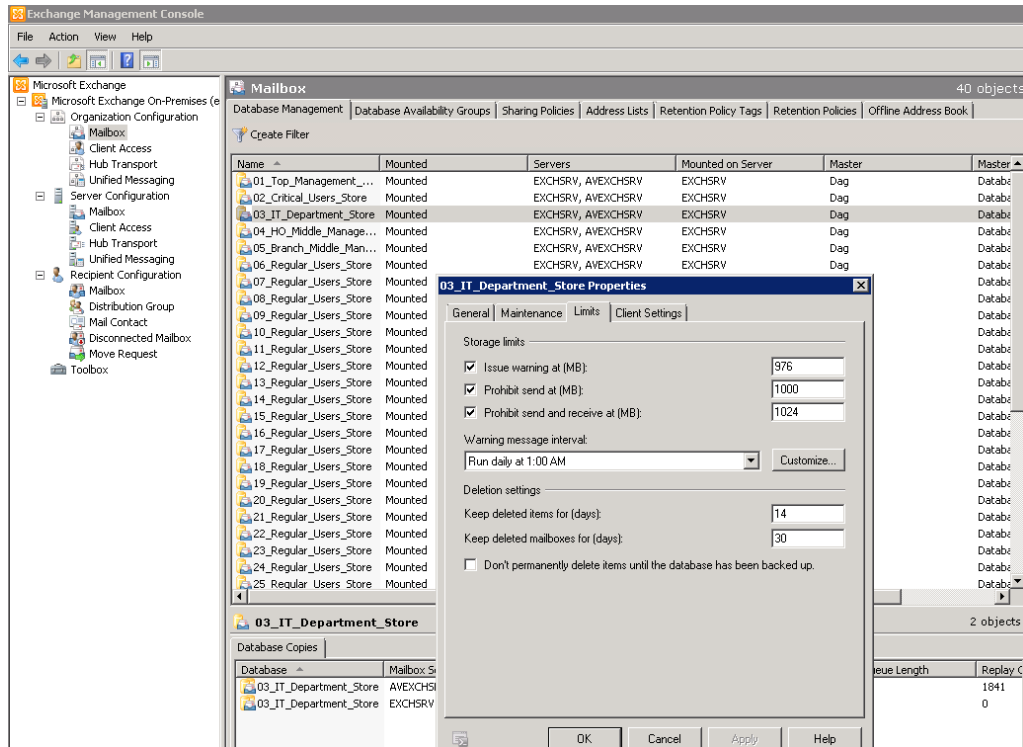
კემის რეჟიმის აქტივაცია MS Outlook-ში



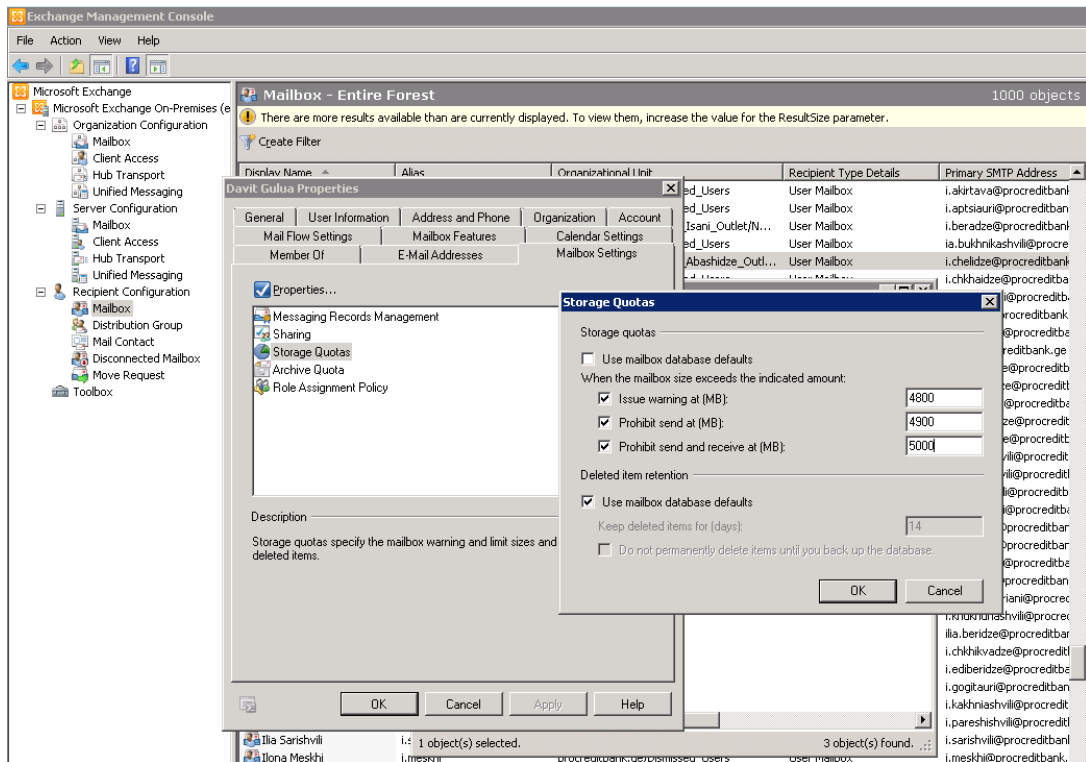
ოფლაინ-რეჟიმის აქტივაცია MS Outlook-ში

როგორც ფაილურ სერვერს, ელ.ფოსტის სერვერსაც მეხსიერების კვოტირების ფუნქცია გააჩნია, რომელიც ყოველი მომხმარებლისთვის ელექტრონული წერილებისთვის გარკვეული დისკური სივრცის გამოყოფას ითვალისწინებს (მაგ. 500 მბ-დან სტანდარტული მომხმარებლებისთვის 2,5 გბ-მდე ტოპ-მენეჯმენტისთვის). ცალკე ფუნქციას წარმოადგენს **ონლაინ არქივიც** (მაგალითად 5 გბ დამატებითი მეხსიერების მოცულობით), რომელშიც ელ.ფოსტის ძირითადი საცავიდან, გარკვეული წესების

მიხედვით, მეილების გადატანა ხორციელდება ძირითადი საცავის განტვირთვის მიზნით. მომდევნო ორ სურათზე ნაჩვენებია გარე მეხსიერების კვოტების განსაზღვრის დიალოგები მთლიანი მეილ-სთორის ანუ ყველა მეილბოქსისა და კონკრეტული მეილ-ბოქსისთვის.



მეხსიერების კვოტირება მეილ-სთორისთვის



მეხსიერების კვოტირება მეილ-ბოქსისთვის

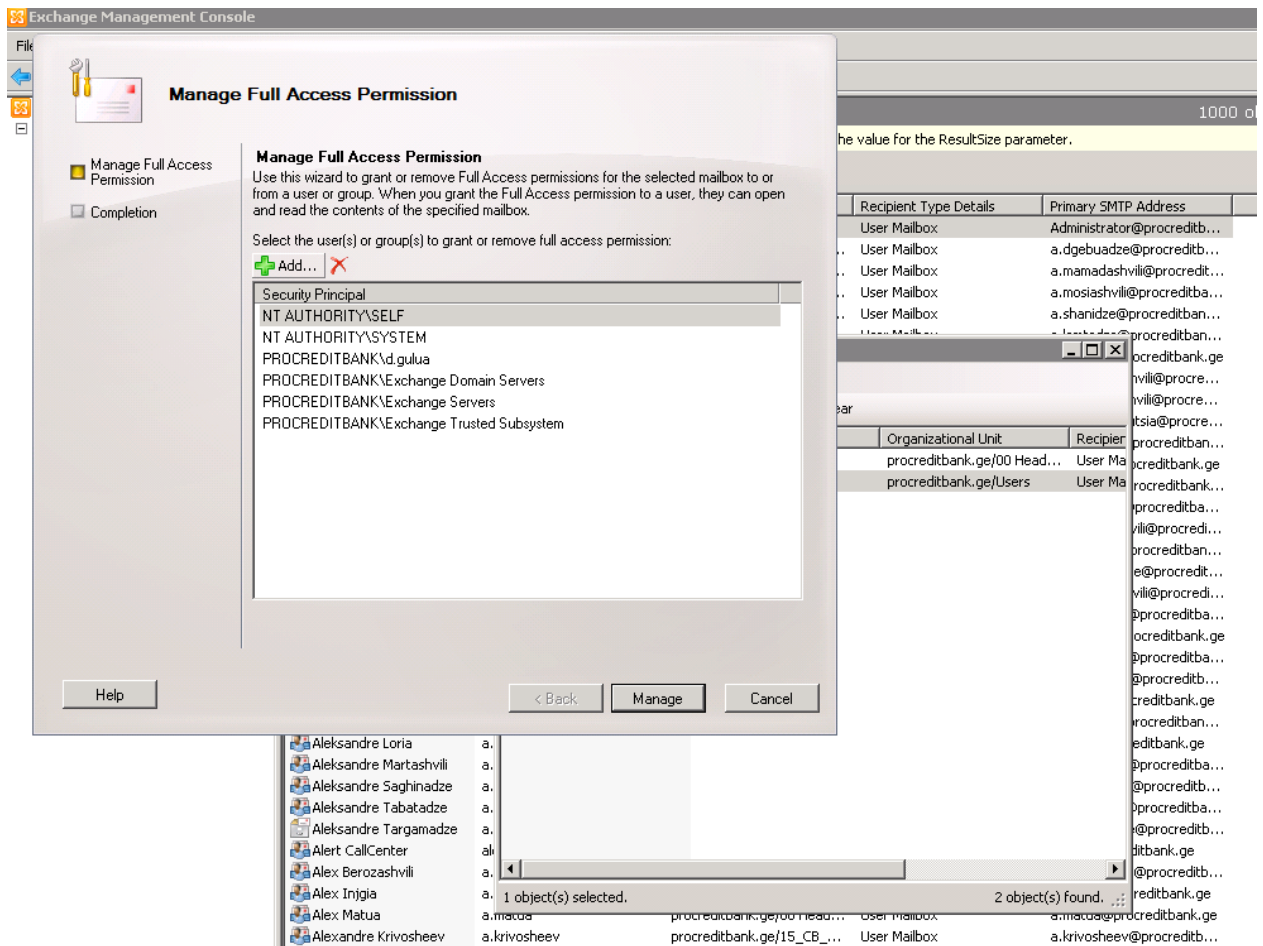
5.2.1.2. წესების მართვა MS Exchange Server-ის გარემოში

ელექტრონული ფოსტის სერვერზე ადმინისტრირების სხვადასხვა ამოცანების გადაწყვეტა შეიძლება. თავდაპირველად ორიოდ ყველაზე მარტივი ფუნქცია გავარჩიოთ:

თუ მომხმარებლის მეილ-ბოქსზე სრული წვდომის დამყარება (მ.შ. ჩვენს ელ.ფოსტის კლიენტის ფანჯარაში მისი ელექტრონული წერილების გამოტანა) გვჭირდება, საჭიროა გამოვიძახოთ ბრძანება:

მაუსის მარჯვენა ღილაკი მეილ-ბოქსზე -> Manage Full Access Permission

და Add-ღილაკით დავამატოთ ჩვენი (ან სხვა მომხმარებლის) დომენური საადრიცხვო ჩანაწერი.

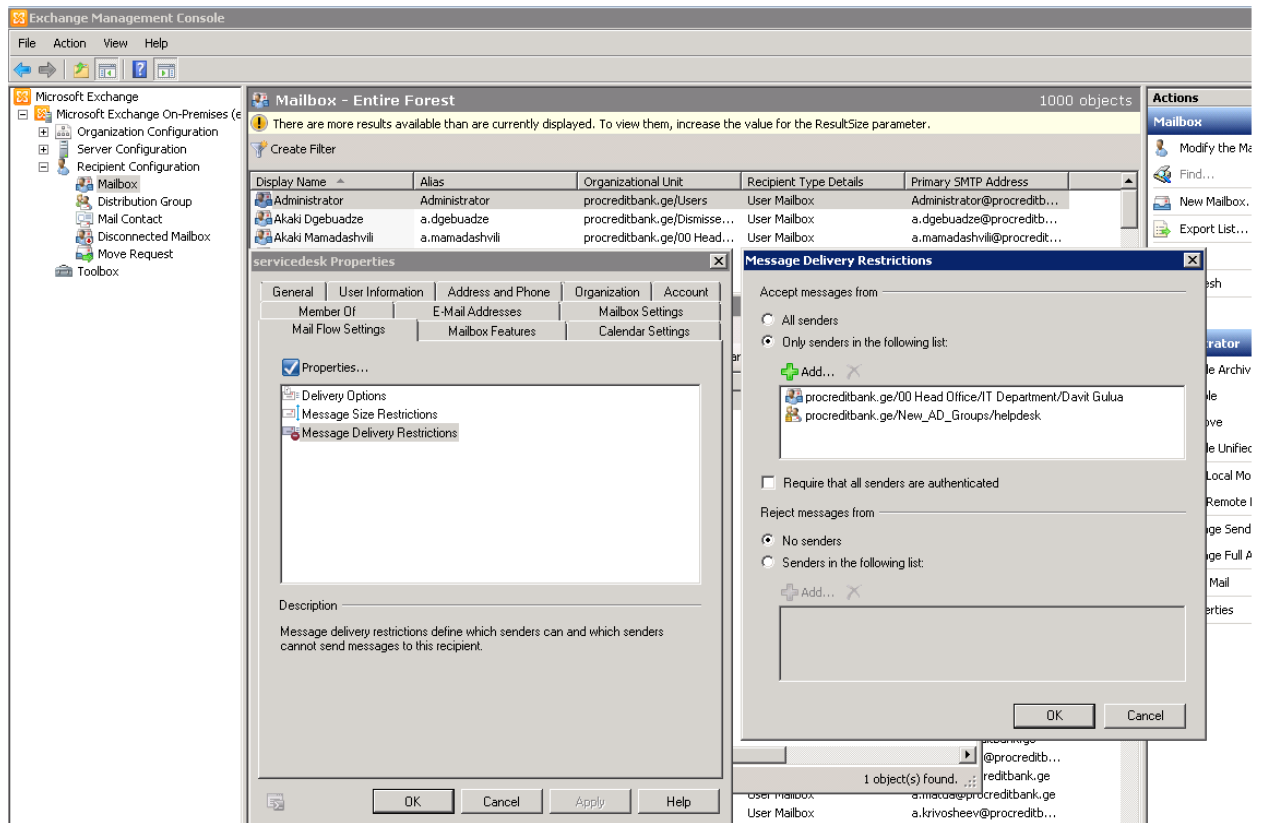


სრული უფლებების ჩართვა მეილ-ბოქსზე

თუ საჭიროა იმ მომხმარებელთა რაოდენობის შეზღუდვა, რომელთაც მოცემული მეილის მისამართზე მოწერა შეუძლიათ, საჭიროა შემდეგი ბრძანების შესრულება:

მაუსის მარჯვენა ღილაკი მეილ-ბოქსზე -> Properties -> Mail Flow Settings -> Message Delivery Restrictions

რის შემდეგაც გამოსულ ფანჯარაში All Senders ჩავანაცვლოთ ბრძანებით: Only Senders in the following list და ავირჩიოთ სასურველი დომენური მომხმარებლები.



მეილ-ბოქსზე გამოგზავნის უფლებათა შეზღუდვა

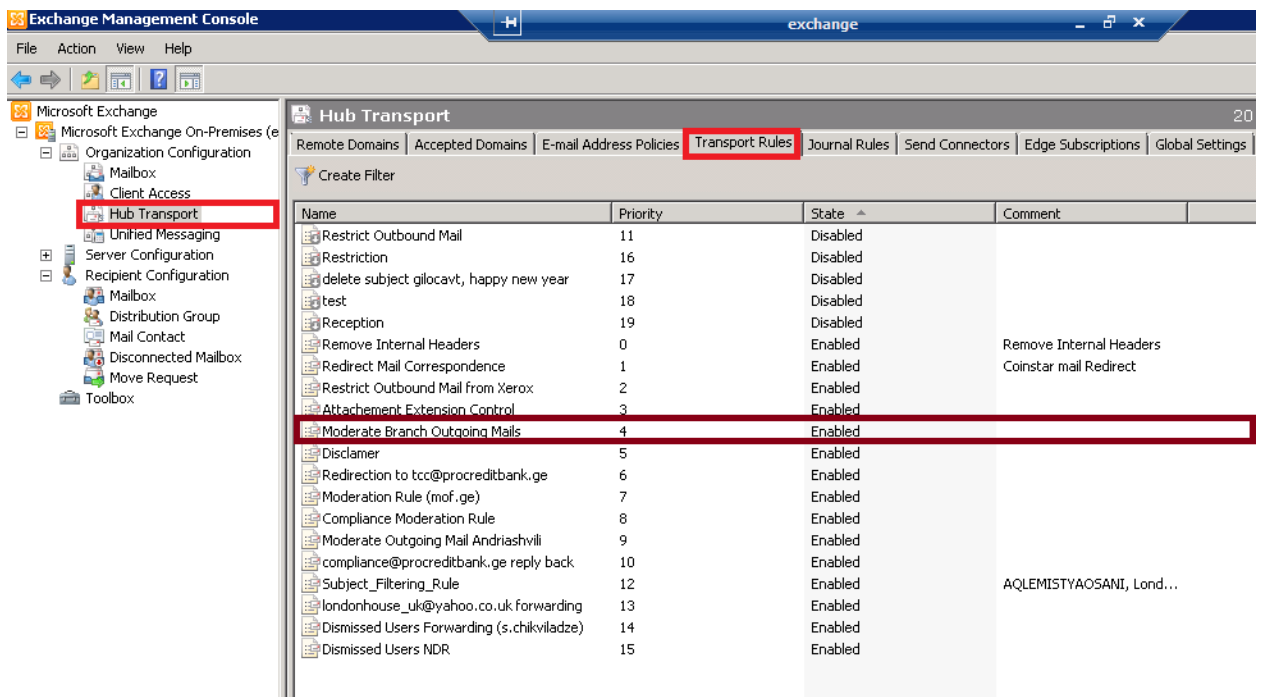
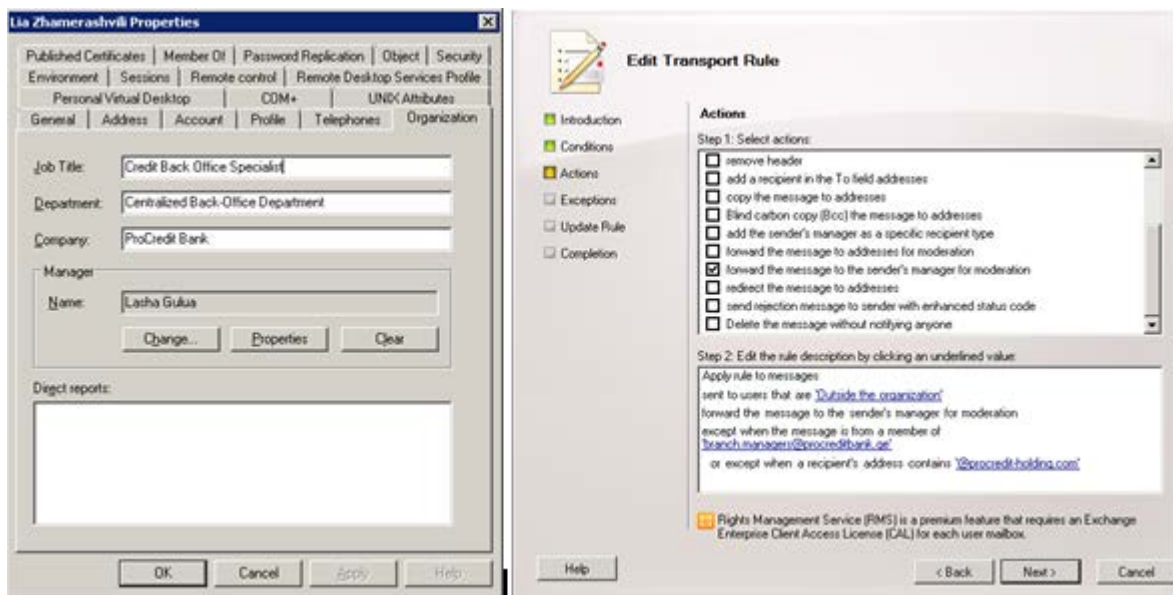
მართვის შედარებით რთული ოპერაციების განსახორციელებლად MS Exchange Server წესების განსაზღვრის საშუალებას იძლევა, რომელთა საშუალებითაც ელექტრონული ფოსტის სერვერზე მომხმარებლის პრაქტიკულად ყველა მოქმედების გაკონტროლება შეიძლება. განვიხილოთ მაგალითი, რომელიც ორგანიზაციის გარეთ გამავალი და ორგანიზაციაში შემომავალი ელექტრონული წერილების კონტროლს ეხება. ამგვარი წესის აუცილებლობა ნათელია: მონაცემთა გაჟონვას ან არაკვალიფიციურ მიმღეებს ორგანიზაციისთვის სერიოზული ფინანსური და საიმპიჯე ზარალის მიყენება შეუძლია. შიდა IT-ინფრასტრუქტურის ფარგლებს გარეთ გამავალი და შემომავალი ელექტრონულ წერილებს უფლებამოსილი პირები (როგორც წესი, თანამშრომლების უშუალო ხელმძღვანელები) აკონტროლებენ (ამ პროცესს მოდერაციასაც უწოდებენ).

მოდერაცია ავტომატური პროცესია, ანუ Exchange Server-ის ფარგლებიდან გამავალი ნებისმიერი მეილი დასტურის ან უარყოფისთვის თავდაპირველად მოდერატორს მისდის და გზას მხოლოდ დადებით პასუხის შემთხვევაში გააგრძელებს. მოდერატორის ვინაობა მომხმარებლის დომენური სააღრიცხვო ჩანაწერის მართვის დიალოგში (გადამრთველი Organization, ველი Manager) დგინდება. ქვემოთ, პირველ

სურათზე ნაჩვენებია Manager-ის განსაზღვრის დიალოგი დომენური მომხმარებლისთვის, ხოლო მეორეზე გააქტიურებულია MS Exchange-ის ე.წ. ტრანსპორტირების წესი (Transport Rule):

Forward the Message to the senders Manager for moderation

რომელიც მოდერაციის ოპერაციის შესრულებას უზრუნველყოფს. მესამე სურათზე გამოტანილია Exchange Server-ის წესების მართვის ინტერფეისი, რომელშიც ჩვენს მიერ განსაზღვრული წესია გამოყოფილი (*Exchange Management Console -> Moderate Branch Outgoing Mail*).



AD-მენეჯერის მიერ გარე ბეილის მოდერაციის დიალოგები

5.2.1.3. სპამის მოგერიების მეთოდები ელექტრონული ფოსტის სერვისებში

თანამედროვე ელექტრონული ფოსტის სერვისებში უსაფრთხოების ყველაზე დიდ პრობლემას სპამი, ანუ არასასურველი ელექტრონული წერილები წარმოადგენს, რომელთაც მავნე საქმიანობას ფართო დიაპაზონი გააჩნიათ, თავის მობეზრებიდან მავნე პროგრამული უზრუნველყოფის გავრცელებამდე. სპამთან ბრძოლის საკმაოდ კარგი საშუალებები აქვთ უშუალოდ ელექტრონული ფოსტის სერვერებსაც, მაგრამ სადღეისოდ ყველაზე ეფექტურად სპეციალიზებული აპარატული და პროგრამული უზრუნველყოფის, სპამ-ფაიერვოლის გამოყენება ითვლება, რომელსაც მრავალფეროვანი ფუნქციების შესრულება შეუძლია:

- სპამის მოგერიება;
- ვირუსებთან ბრძოლა;
- მეილების კონტენტის და ბმული ფაილების გაფილტვა;
- ელ.ფოსტის მისამართების რეპუტაციის მონაცემთა ბაზებთან მიმართვა;
- ლოგების შექმნა და ანალიზი;
- და მრავალი სხვა...

საილუსტრაციო სურათზე მოცემულია ერთერთი ცნობილი სპამ-ფაიერვოლის, Barracuda Spam&Virus Firewall-ს მიერ დამუშავებული შემომავალი და გამავალი ელექტრონული წერილების სტატისტიკა. ყურადღებას იქცევს შემომავალი ბლოკირებული მეილების ხუთჯერადი მეტობა ნებადართულ მეილებზე, რაც სპამთან წარმატებული ბრძოლის მანიშნებელია.

Email Statistics [inbound]				Email Statistics [outbound]			
	Total	Day	Hour		Total	Day	Hour
Blocked	17,611,279	3,132	37	Blocked: Policy	18,156	0	0
Blocked: Virus	9,421	0	0	Blocked: Spam	83,312	2	0
Rate Controlled	879,288	0	0	Blocked: Virus	30	0	0
Quarantined	0	0	0	Rate Controlled	93,707	0	0
Allowed: Tagged	144,747	7	1	Quarantined	0	0	0
Allowed	3,156,863	431	4	Encrypted	0	0	0
Total Received	21,801,598	3,570	42	Redirected	0	0	0
				Sent	4,425,465	1,357	14
				Total	4,620,670	1,359	14

Barracuda Spam&Virus firewall-ის ინტერფეისის ფრაგმენტი

მოკლედ შევხვით სპამ-ფაიერვოლის რამდენიმე ფუნქციას შესაბამისი პრაქტიკული მაგალითების თანხლებით.

დომენების და IP-მისამართების „თეთრი სიის“ ფორმირება, რომლებსაც ბლოკირების ყველა წესის გვერდის ავლა შეუძლიათ (სურათი).

IP Reputation	Rate Control	IP Filters	Sender Filters	Sender Authentication	Recipient Filters
Attachment Filters	Content Filtering	Reverse DNS	Regional Settings		

Allowed Email Addresses and Domains Save Changes Help

Email Address/Domain	Comment	Bulk Edit
		Add
Monetary.Operations@nbg.gov.ge	treasury	<input type="checkbox"/>
aldagibci.ge	Aldagi BCI Mail	<input type="checkbox"/>
bagrationi.ge	Bagrationi Shampanski	<input type="checkbox"/>
bn.com		<input type="checkbox"/>
bog.ge		<input type="checkbox"/>
borjomi.com	Georgian Borjomi Mail	<input type="checkbox"/>
coinstar.com	Travelex Mail	<input type="checkbox"/>
coinstar.ru	Travelex Mail	<input type="checkbox"/>
constantia.ge	Constantia	<input type="checkbox"/>
court.ge	COURTS OF GEORGIA	<input type="checkbox"/>
cpanel.host.ge	NGT	<input type="checkbox"/>
david@ngt.ge		<input type="checkbox"/>
demasi.ge	Demasi	<input type="checkbox"/>
deutscheschule.ge	Deutsche Schule	<input type="checkbox"/>
dlh.de	Something German	<input type="checkbox"/>
eTisSupport@commerzbank.com	Treasury	<input type="checkbox"/>
eliteelectronics.ge	Elit Electronics	<input type="checkbox"/>
energo-pro.ge	Energo Pro	<input type="checkbox"/>
fxpm@bloomberg.net	Treasury	<input type="checkbox"/>
galtandtaggart.de	Something German	<input type="checkbox"/>
galtandtaggart.ge	Something German	<input type="checkbox"/>
ge.pwc.com		<input type="checkbox"/>
geocell.com.ge	Geocell	<input type="checkbox"/>

Sender Email Addresses and Domains, TLDs to be whitelisted. **Warning:** Spammers can spoof whitelisted domains. Instead, whitelisting by IP address is recommended.

ნებადართული დომენების სია

IP Reputation	Rate Control	IP Filters	Sender Filters	Sender Authentication	Recipient Filters
Attachment Filters	Content Filtering	Reverse DNS	Regional Settings		

Allowed IP/Range Save Changes Help

IP/Network Address	Netmask	Comment	Bulk Edit
			Add
62 . 159 . 157 . 115	255 . 255 . 255 . 255	procredit-holding.com	<input type="checkbox"/>
193 . 58 . 244 . 104	255 . 255 . 255 . 255	procredit-holding.com	<input type="checkbox"/>
198 . 80 . 42 . 54	255 . 255 . 255 . 255	broadcast01b.visabroadcasts.com	<input type="checkbox"/>
198 . 80 . 42 . 55	255 . 255 . 255 . 255	broadcast01b.visaclientcommunications.com	<input type="checkbox"/>
198 . 80 . 42 . 63	255 . 255 . 255 . 255	broadcast01b.visabusinessnews.com	<input type="checkbox"/>
198 . 241 . 174 . 141	255 . 255 . 255 . 255	broadcast01p.visabroadcasts.com	<input type="checkbox"/>
198 . 241 . 174 . 142	255 . 255 . 255 . 255	broadcast01p.visaclientcommunications.com	<input type="checkbox"/>
198 . 241 . 174 . 147	255 . 255 . 255 . 255	broadcast01p.visabusinessnews.com	<input type="checkbox"/>
212 . 185 . 98 . 86	255 . 255 . 255 . 255	procredit-holding.com	<input type="checkbox"/>

Inbound and outbound messages from the listed IP addresses will bypass all spam scanning.
Examples:
 Single IP IP=204.33.21.56 Netmask=255.255.255.255
 subnet IP=204.33.21.0 Netmask=255.255.255.0

Blocked IP/Range Save Changes Help

IP/Network Address	Netmask	Comment	Block	Quarantine	Tag	Bulk Edit
			<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	Add

Add any IP addresses or networks to blocklist and the action to take with messages from these IPs.

ნებადართული IP-მისამართების სია

მეილს ბმული ფაილების ბლოკირება ფაილის ტიპის მიხედვით (სურათი).

*.jse		Block	Block	<input checked="" type="checkbox"/>	
*.lnk		Block	Block	<input checked="" type="checkbox"/>	
*.mdb		Block	Block	<input checked="" type="checkbox"/>	
*.mde		Block	Block	<input checked="" type="checkbox"/>	
*.msc		Block	Block	<input checked="" type="checkbox"/>	
*.msi		Block	Block	<input checked="" type="checkbox"/>	
*.msp		Block	Block	<input checked="" type="checkbox"/>	
*.mst		Block	Block	<input checked="" type="checkbox"/>	
*.pcd		Block	Block	<input checked="" type="checkbox"/>	
*.pif		Block	Block	<input checked="" type="checkbox"/>	
*.reg		Block	Block	<input checked="" type="checkbox"/>	
*.scr		Block	Block	<input checked="" type="checkbox"/>	
*.sct		Block	Block	<input checked="" type="checkbox"/>	
*.shs		Block	Block	<input checked="" type="checkbox"/>	
*.url		Block	Block	<input checked="" type="checkbox"/>	
*.vbe		Block	Block	<input checked="" type="checkbox"/>	
*.wsc		Block	Block	<input checked="" type="checkbox"/>	
*.wsf		Block	Block	<input checked="" type="checkbox"/>	
*.wsh		Block	Block	<input checked="" type="checkbox"/>	

Attachment File Type Filters

Description	Inbound	Outbound	Check Archives
Multimedia - Audio/Video Files	Off <input type="checkbox"/>	Off <input type="checkbox"/>	<input checked="" type="checkbox"/>
Documents - MS-Access	Off <input type="checkbox"/>	Off <input type="checkbox"/>	<input checked="" type="checkbox"/>
Documents - MS-Excel	Off <input type="checkbox"/>	Off <input type="checkbox"/>	<input checked="" type="checkbox"/>
Documents - MS-Word	Off <input type="checkbox"/>	Off <input type="checkbox"/>	<input checked="" type="checkbox"/>
Documents - Adobe PDF	Off <input type="checkbox"/>	Off <input type="checkbox"/>	<input checked="" type="checkbox"/>
Documents - MS-Powerpoint	Off <input type="checkbox"/>	Off <input type="checkbox"/>	<input checked="" type="checkbox"/>
Executables - Windows Executables	Block <input type="checkbox"/>	Block <input type="checkbox"/>	<input type="checkbox"/>
Executables - Windows Scripts	Block <input type="checkbox"/>	Block <input type="checkbox"/>	<input type="checkbox"/>

ბმული ფაილების ბლოკირება ფაილის ტიპის მიხედვით

Time	From	To	Subject	Size	Action	Reason	S...	Source IP	Delivery St...
2014-05-19 1...	d.gulua@pro...	Khrystenko@quipugmbh.com	RE: log	58...	Allowed	Message Size		exchsrv.pr...	Delivered
2014-05-19 1...	d.gulua@pro...	Khrystenko@quipugmbh.com	DLLs	58...	Blocked	Attachment (SignPadDLLs.rar [Exec...		exchsrv.pr...	
2014-05-19 1...	d.gulua@pro...	Khrystenko@quipugmbh.com	RE: log	58...	Blocked	Attachment (SignPadDLLs.rar [Exec...		exchsrv.pr...	

შეტყობინება აკრძალული ტიპის ფაილების ბლოკირების შესახებ

5.2.2. მყისიერ შეტყობინებათა სერვისის მართვა MS Lync-ის გარემოში

5.2.2.1. 5.3.1 Lync 2010-ის არქიტექტურა

მეტნაკლებად დიდი, განვითარებული IT-ინფრასტრუქტურის მქონე ორგანიზაციის ფარგლებში საკუთარ საკომუნიკაციო აპარატურასა და პროგრამებს იყენებენ. მოცემული თავი კომუნიკაციის სისტემა MS Lync-ის განხილვას მოიცავს. ამ

სისტემაზე არჩევანი, სხვათა შორის, მისი უნივერსალურობის გამო შევაჩერეთ. MS Lync მრავალი საკომუნიკაციო ფუნქციის კომბინირებულად გამოყენების საშუალებას აძლევს მომხმარებელს. განსაკუთრებით ისეთ შემთხვევებში, როცა ორგანიზაციის საკომუნიკაციო ინფრასტრუქტურის თავიდან აგებაა საჭირო, სისტემა Lync სეროზული დროითი და ფინანსური რესურსების დაზოგვის საშუალებას იძლევა მყისიერ შეტყობინებათა, ფაილთა გაცვლის, ჯგუფური შეხვედრების ორგანიზების, ტელეფონის, გარე სისტემებთან მოქნილი ინტეგრირების და სხვა ფუნქციების ერთ პლატფორმაზე გამართვის შესაძლებლობიდან გამომდინარე.

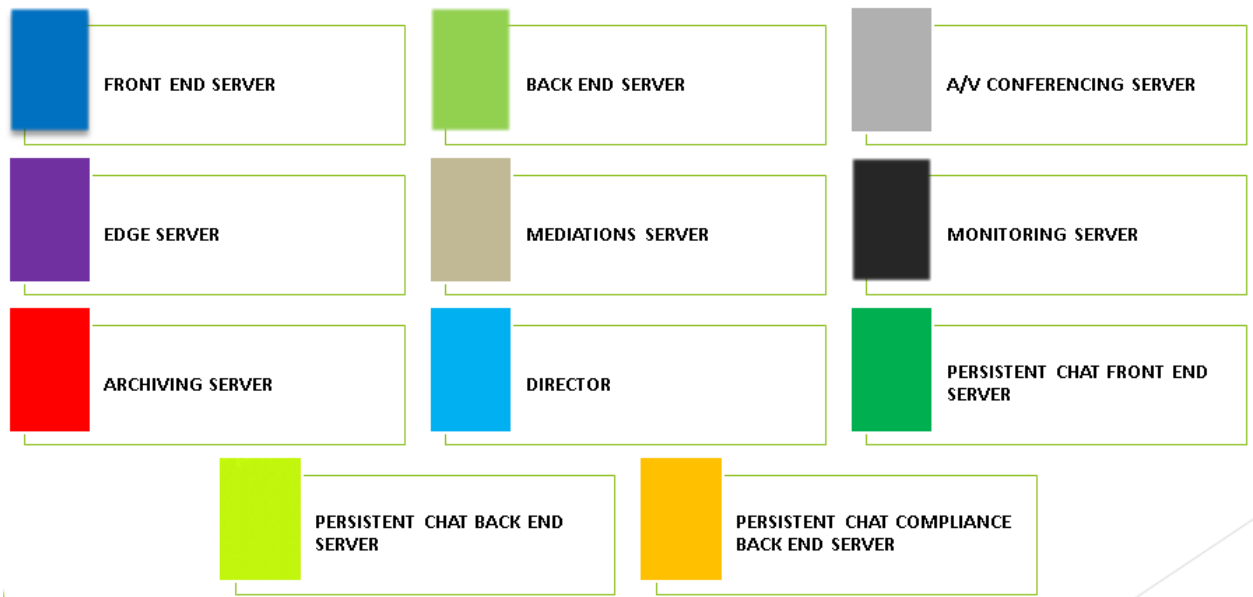
განხილული თემატიკა პროგრამული უზრუნველყოფის მოწინავე მწარმოებელთა შეუწელებელი ყურადღების საგანს წარმოადგებს. ამ მიმართულებით ახალი ტექნოლოგიების განვითარებას და დანერგვას ახლო მომავალში უნდა ველოდოთ. უკვე დღეს არსებობს Lync-კლიენტები სხვადასხვა ოპერაციული სისტემებისთვის (LINUX, MAC), აგრეთვე მრავალი მობილური პლატფორმისთვის (iPhone, Android) და ვებ-სივრცეში, რაც ამ სისტემის შემდგომი გაფართოების პერპექტივას უეჭველს ხდის.

MS Lync 2010 წარმატებით გამოიყენება, როგორც შიდა და გარე Instant Messaging-ის სისტემა. ბევრ ორგანიზაციაში მან სრულებით ჩაანაცვლა საყოველთაოდ ცნობილი სისტემა Skype. MS Lync-ის უდავო უპირატესობას წარმოადგენს გარე სისტემებისგან სრული დამოუკიდებლობა (კონკურენტისგან განსხვავებით), თუმცა მეორე მხრივ, სისტემა სხვა პარტნიორებთან (იგივე Skype-თან) ინფორმაციის გაცვლის მძლავრ საშუალებებს შეიცავს, რაც ბუნებრივია, თუ გავითვალისწინებთ იმას, რომ ორივე პროდუქტი სადღეისოდ ერთი და იგივე კომპანიის (Microsoft) მიერ არის წარმოდგენილი პროგრამული უზრუნველყოფის ბაზარზე და ეს კომპანია მაქსიმალურად ინტეგრირებული საკომუნიკაციო გარემოს შექმნით არის დაინტერესებული.

MS Lync-ის ისტორია 2003 წლიდან იწყება, როცა იგი MS Exchange 2003-ს დამოუკიდებელი პროგრამული პაკეტის სახით გამოეყო (Live Communications Server 2003) და პროგრამა Exchange Instant Messenger Service ჩაანაცვლა. გარკვეული ხნის განმავლობაში პროგრამა ცნობილი იყო Microsoft Office Communications Server-ის სახელით ანუ საოფისე პროგრამული პაკეტის ნაწილს წარმოადგენდა (Office Communications Server 2007 R2), ხოლო ახალი ფუნქციების დამატების და უნივერსალურობის ზრდის კვალობაზე სრულიად დამოუკიდებელ პროგრამული

პროდუქტის სახით გამოვიდა (Lync Server 2010). ამჟამად სისტემის უახლეს ვერსიას Lync Server 2013 წარმოადგენს.

Lync-ის სრული სერვერული არქიტექტურა მოცემულია სურათზე.



MS Lync - სერვერული მხარის სტრუქტურა

თითოეული სერვერის ამუშავება შესაძლებელია როგორც ერთიანი, ასევე ცალცალკე გამოთვლითი სისტემების გარემოში. ამასთან, პროგრამის შექმნა ორი განსხვავებული პაკეტის სახით შეიძლება: სტანდარტული (Standard Edition) და საწარმოო (Enterprise Edition).

სტანდარტულ ვერსიას არ გააჩნია სატელეფონო სერვისების ინტეგრაციისა და მაღალსარგებლიანობის (High Availability) უზრუნველყოფა. მხოლოდ საწარმოო ვერსია იძლევა ორგანიზაციის ფარგლებში და გარე სამყაროსთან ნებისმიერი კომუნიკაციის (ტელეფონი, კონფერენცია, მყისიერი შეტყობინებები) ერთიან სისტემაში თავმოყრის და მართვის საშუალებას.

Lync 2010 Server-ს ძირითადი ფუნქციებია შემდეგი:

- **Audio and Video Conferencing** – აუდიო- და ვიდეოკონფერენციები;
- **Dial-in Conferencing** (PSTN Conferencing) - ტელეფონის აპარატის დაშვება კონფერენციაში მონაწილეობის მისაღებად;
- **Web-conferencing** (Meetings) – კომუნიკაციის ვებ-სივრციდან განხორციელება;

- **Enterprise Voice** – ლინქის აწყობა კორპორატიული ტელეფონისთვის (Cisco, Asterisk და სხვა სისტემების კონკურენტი). Lync as PBX (Private Branch Exchange);

- **Exchange Unified Messaging** - კავშირი MS Exchange Unified Messaging სერვისთან;

- **Call Admission Control** – ახალი ფუნქცია ქსელის გამტარუნარიანობის გასათვალისწინებლად;

- **Monitoring** – მონიტორინგი;

- **Archiving** – არქივაცია;

- **Federation** - კავშირები გარე საკომუნიკაციო სისტემებთან;

- **High Availability** - მაღალსარგებლიანობის უზრუნველყოფა.

თითოეული ჩამოთვლილი ფუნქციის აქტივაცია შეიძლება შესაბამისი ლიცენზიის შეძენისა და აქტივაციის შემდეგ. ლიცენზირების მოდელი (იხევე, როგორც Microsoft-ის უმრავლესი პროდუქტებისთვის) საკმაოდ რთულია. სერვერული ნაწილის და კლიენტთა ლიცენზიები ცალცალკეა შესაძენი და ფასის თვალსაზრისით ოპტიმალური პაკეტის შეძენა საკმაოდ კვალიფიციური სპეციალისტის შრომას მოითხოვს.

ჩვენს წიგნში Lync-ის საბაზო ფუნქციაზე, მყისიერ შეტყობინებათა სერვისზე გვექნება საუბარი.

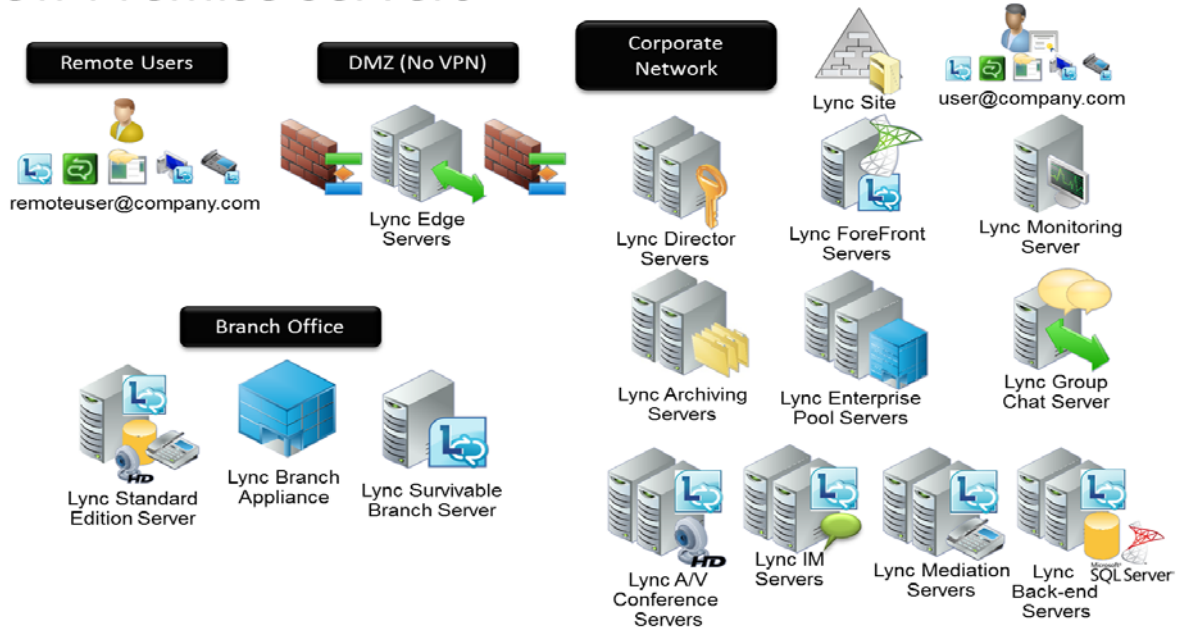
5.3. სპეციფიკური კლიენტ სერვისების მართვა

5.3.1. Lync 2010-ის დანერგვა

ვერსიების განახლების კვალდაკვალ MS Lync-ის დანერგვა კორპორაციულ ქსელში გამართივდა, თუმცა დღესაც საკმაოდ შრომატევადია. პირველი, რაც უნდა აღინიშნოს, არის ის, რომ სისტემის დანერგვის პროცესში ხორციელდება მთელი რიგი განახლებები ორგანიზაციის IT-ინფრასტრუქტურის საკვანძო ობიექტებში (Active Directory, Exchange Server და სხვა), ამიტომ ინსტალაციის პროცედურა დაკვირვებით უნდა განხორციელდეს.

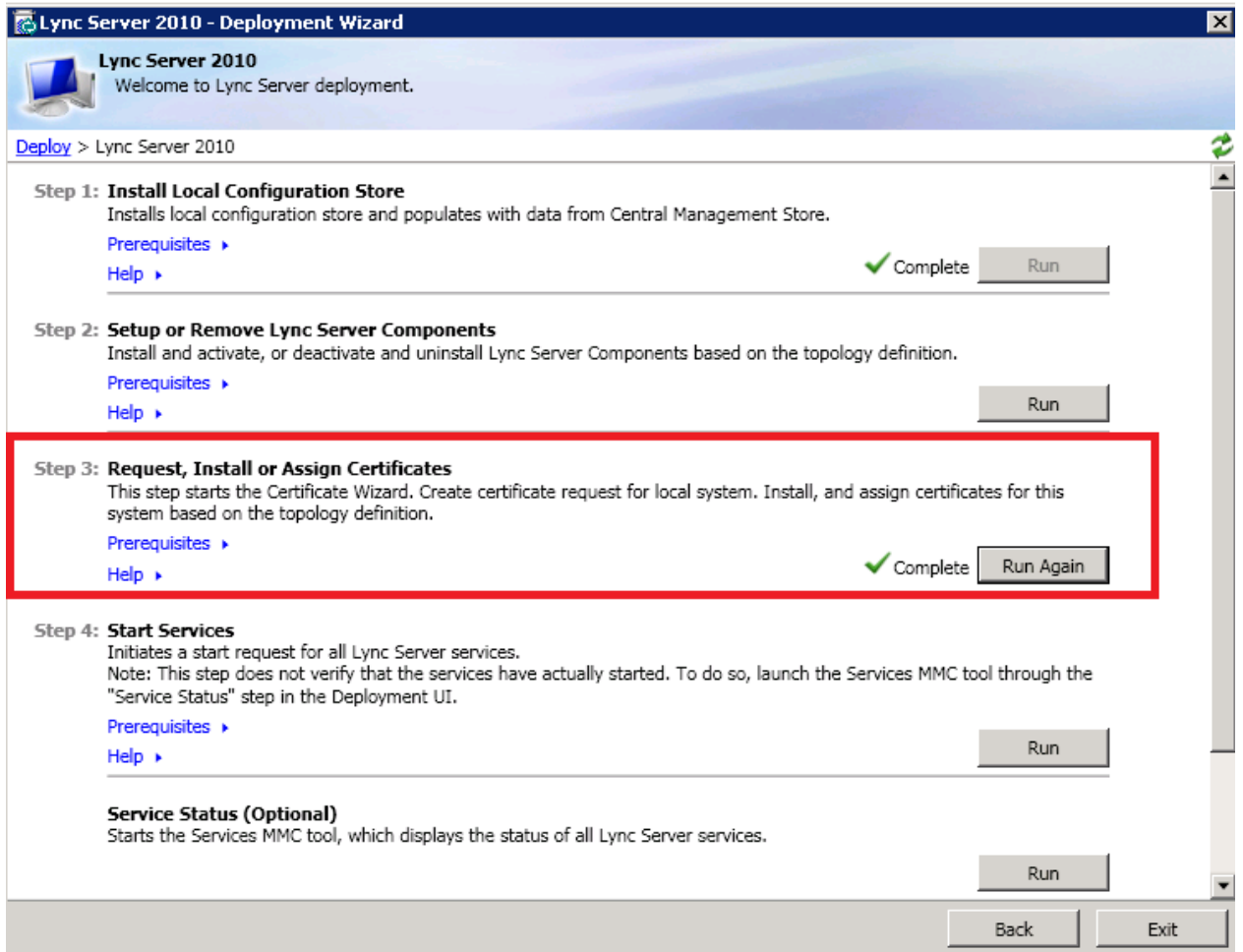
აპარატული და სისტემური რესურსების მიმართ პროგრამა ნაკლებად პრეტენზიულია. Quad Core - პროცესორი 2 გიგაჰერცი ტაქტური სიხშირით და 4-6 გბ ოპერატიული მეხსიერება სავსებით აკმაყოფილებს Lync 2010 Standard სისტემის საჭიროებებს და 700-800 მომხმარებელს ემსახურება. სისტემური მოთხოვნა: Windows Server 2008, ხოლო პროგრამული მოთხოვნები მოიცავს შემდეგ სისტემებს: Windows PowerShell, MS .NET Framework, IIS, Silverlight. აღწერილი მოთხოვნები ვრცელდება სისტემის სტანდარტულ ვერსიაზე, საწარმოო ვერსიის შემთხვევაში მეტი რესურსი იქნება საჭირო და სისტემის მასშტაბების მიხედვით, სხვადასხვა დანიშნულების სერვერებიც, როგორც წესი, სხვადასხვა ფიზიკურ (ზოგჯერ ვირტუალურ) მანქანებზე ყენდება (სურათი).

Microsoft Lync On-Premise Servers



Lync-სერვერების განაწილების სქემა

ინსტალაციის პროცედურა რამდენიმე ოპერაციისგან შედგება, რომლებიც ინსტალაციის საწყის ფანჯარაშია მოცემული (სურათი).



Lync-ის ინსტალაციის პროცედურები

სისტემის ინსტალაცია, როგორც აღვნიშნეთ, კორპორაციული ქსელის დომენურ სტრუქტურაში მნიშვნელოვან ცვლილებებს იწვევს:

ემატება ჰოსტების და სერვისების ჩანაწერები DNS ბაზაში (სურათი)

LYNC	Host (A)	192.168.33.247
sipexternal	Host (A)	192.168.33.247
sipinternal	Host (A)	192.168.33.247

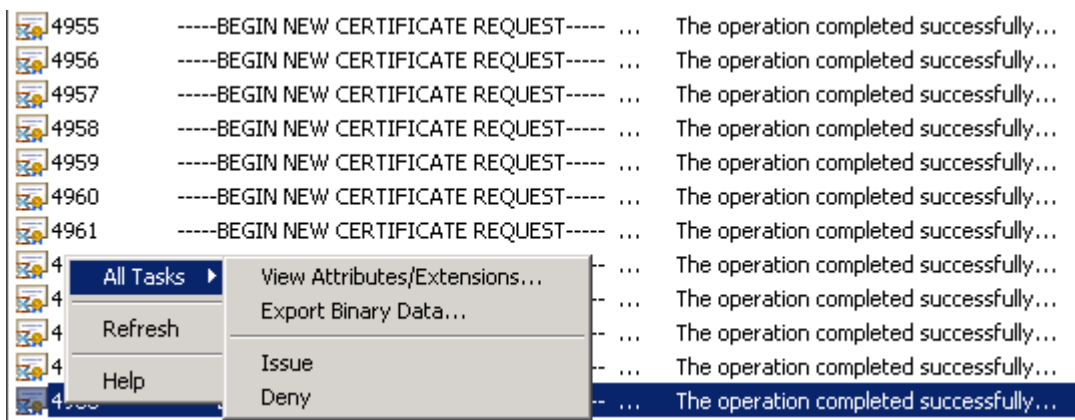
ცვლილებები DNS-ბაზაში

ემატება ახალი დომენური მომხმარებლები და ჯგუფები მიმართვის სხვადასხვა უფლებებით (სურათი)

Name	Type
CSViewOnlyAdministrator	Group
CSUserAdministrator	Group
CSServerAdministrator	Group
CSResponseGroupAdministrator	Group
CSLocationAdministrator	Group
CSHelpDesk	Group
csd.employees	Group
CSArchivingAdministrator	Group
CSAdministrator	Group
CSVoiceAdministrator	Group

ცვლილებები კორპორაციულ დომენში

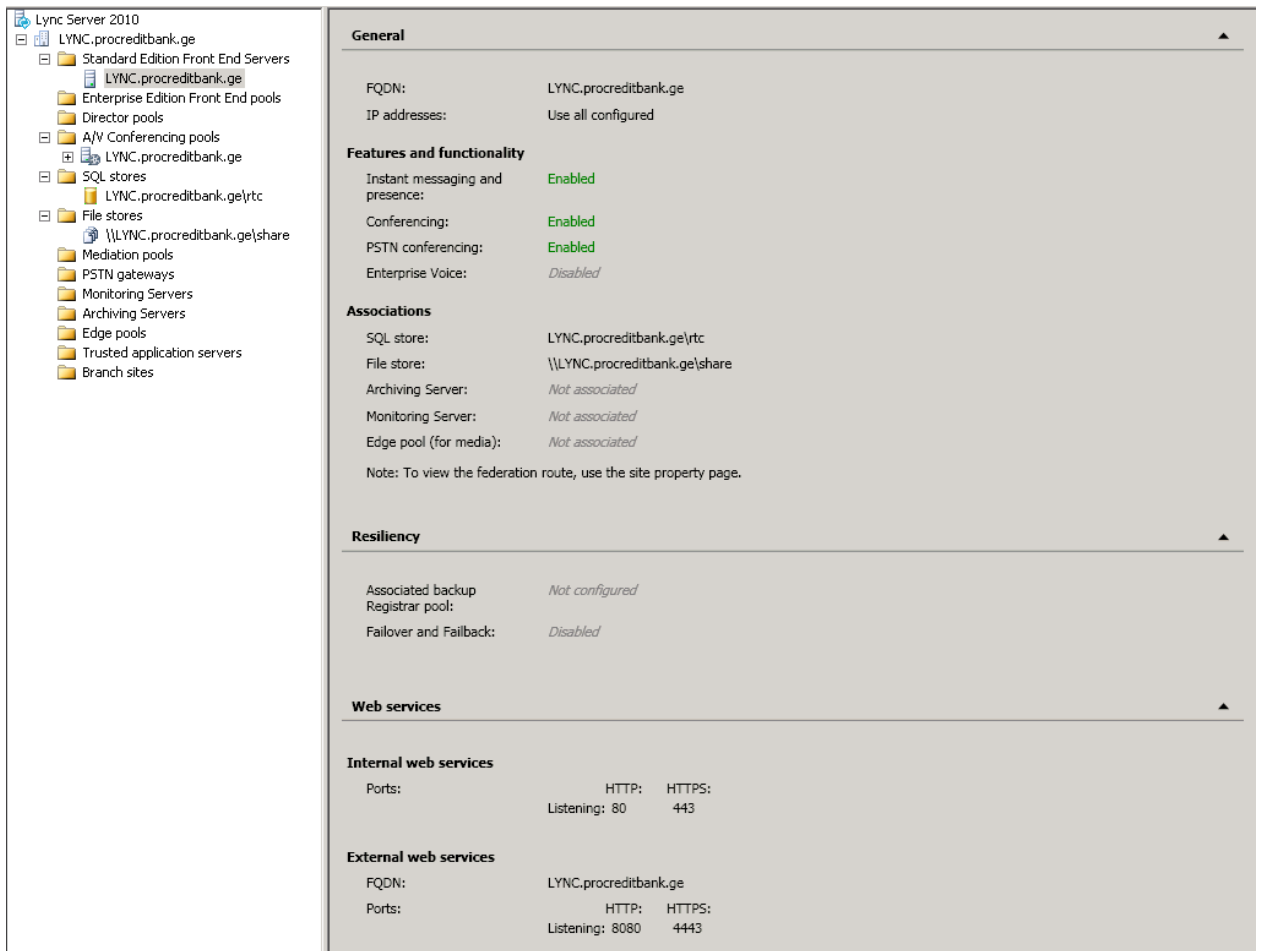
მოითხოვება და სისტემას უმტკიცდება უსაფრთხოების სერტიფიკატი. სერტიფიკატის მიღება შეიძლება სარწმუნო გამცემისგანაც (Trusted Certificate Authority) გარკვეული თანხის საფასურად (მაგალითად Symantec, VeriSign, Thawte, GlobalSign etc), თუმცა თუ Lync მხოლოდ შიდაკორპორაციულ კომუნიკაციას ახორციელებს, საკმარისია სერტიფიკატის მოთხოვნა სერტიფიკატების ადგილობრივი სერვერიდან (CA – Certificate Authority). იხილეთ სურათი, რომელიც Lync-ისთვის მოთხოვნილი სერტიფიკატის გაცემის ან უარყოფის დიალოგს წარმოადგენს სერტიფიკაციის ადგილობრივ სერვერზე.



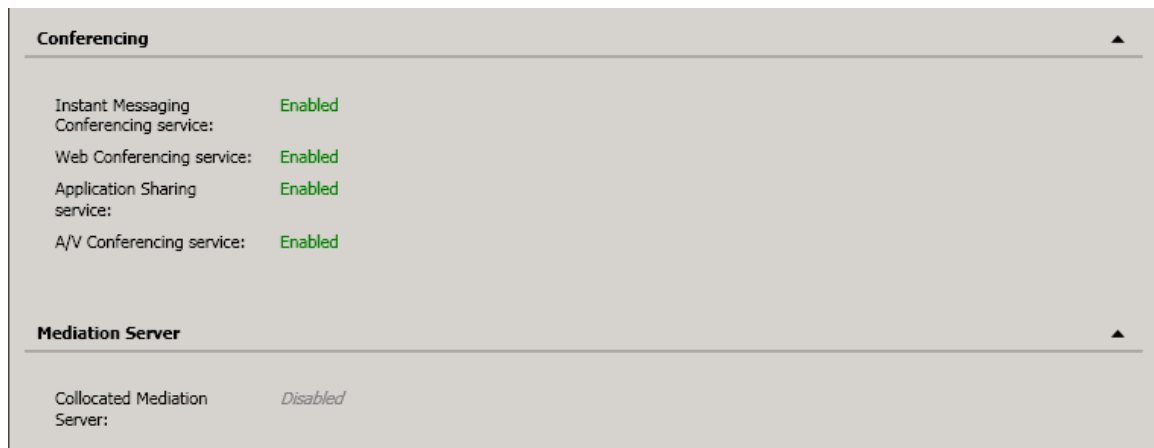
უსაფრთხოების სერტიფიკატის გაცემა

საკომუნიკაციო სისტემის **ტოპოლოგია** ინსტალაციის პროცესში ყალიბდება. იგი სისტემის თითოეული კომპონენტის შესახებ დეტალურ ინფორმაციას შეიცავს და შეიძლება ცალკე ფაილის სახით იქნეს შენახული, რაც სისტემის სხვადასხვა ფიზიკურ ინფრასტრუქტურებს შორის მიგრაციას აადვილებს.

ტოპოლოგიის მართვისთვის გამოიყენება მოდული Lync Server Topology Builder (სურათი)



Lync-ის ტოპოლოგია - სურათი 1

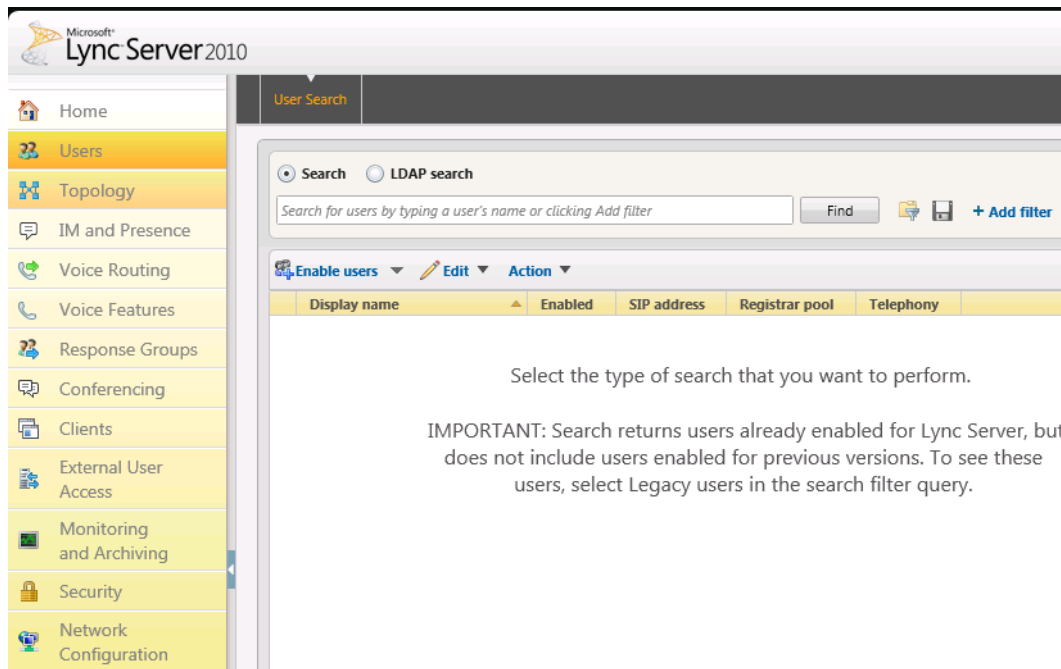


Lync-ის ტოპოლოგია - სურათი 2

5.3.1.1. Lync 2010-ის მართვის პანელი

ვებ-ბაზირებული მართვის პანელი მრავალფეროვან ფუნქციონალს სთავაზობს სისტემის ადმინისტრატორს. შესაძლებელია გრაფიკულ რეჟიმში მომხარებელთა მართვა (დამატება წაშლა, სერვერ-პულებში გადანაწილება და სხვა), აგრეთვე სერვერის

ტოპოლოგიაში ფუნქციების აქტივაცია/დეაქტივაცია და კასტომიზაცია. მართვის პანელის ფრაგმენტი მოცემულია სურათზე.



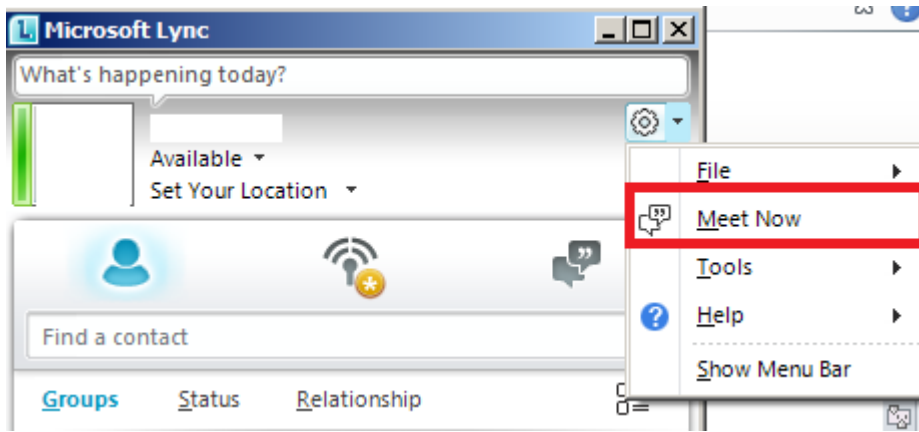
Lync-ის მართვის პანელის ფრაგმენტი

5.3.1.2. ჯგუფური შეხვედრების ორგანიზება (კონფერენსინგი)

განვიხილოთ MS Lync-ის ერთერთი პოპულარული, აუდიო- და ვიდეოკონფერენსინგის მოდული, რომელი ჯგუფური შეხვედრების ეფექტურად ორგანიზების საშუალებას იძლევა. სერვერის მხარეს შესაბამისი მოდულის აქტივაციის შემდეგ მომხმარებლებს შეუძლიათ კონფერენსინგის რეჟიმში მუშაობის დაწყება. როგორც წესი, ჯგუფურ შეხვედრას (Group Meeting) მოდერატორი ჰყავს, რომელიც შეხვედრას ორგანიზებას უკეთებს და წარმართავს. ზოგადად, მოდერატორი და შეხვედრის სხვა მონაწილეები ორ ძირითად ჯგუფში ერთიანდებიან:

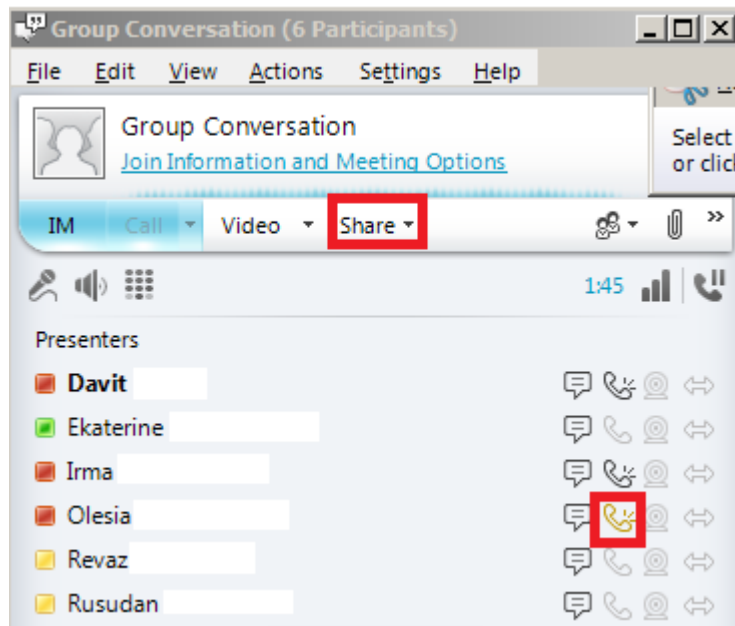
- Presenter - შეხვედრის დაწყება/დასრულების უფლებით;
- Attendee - შეხვედრაში მონაწილეობით.

ჯგუფური შეხვედრის ორგანიზებისთვის მოდერატორმა ლინქში უნდა გამოიყენოს ფუნქცია Meet Now:



ჯგუფური შეხვედრის დაწყება

შეხვედრის მოდერატორი ამ ფუნქციის გააქტიურების შემდეგ გადადის ჯგუფური საუბრის ფანჯარაში (ამ დროს ლინქის მთავარ ფანჯარაში მისი სტატუსიც შესაბამისად იცვლება წითელი ფერით და In a Conference Call სტატუსის ტექსტით). მაუსის საშუალებით შეხვედრის ინიციატორს სასურველი მომხმარებლები შეხვედრის ფანჯარაში გადაჰყავს:



ჯგუფური შეხვედრის მსვლელობა დესკტოპების გაზიარებით

შეხვედრის მონაწილეებს შეუძლიათ შეხვედრა დროებით დატოვონ და ისევ დაბრუნდნენ. მხოლოდ წითელი სტატუსების მქონე მონაწილეები არიან დროის მოცემულ მომენტში ხაზზე.

ვინც მოცემულ მომენტში ლაპარაკობს, ტელეფონის ყურმილი უყვითლდება (მოქცეულია წითელ ჩარჩოში).

შეხვედრის მონაწილეს შეუძლია საუბრის პარალელურად თავისი დესკტოპი შეხვედრის მონაწილეებს წარუდგინოს (Share-დილაკით) ისე, რომ ზედ მიმდინარე მოქმედებებს შეხვედრის მონაწილეებმა შეხედონ (მაგ. პრეზენტაციის წარდგენისას).

შეხვედრის მონაწილეები ჯგუფური შეხვედრის დაწყებამდე თავიანთი Lync-ის ექაუნტით უნდა დარეგისტრირდნენ პერსონალურ კომპიუტერზე ან ნოუთბუქზე, სადაც სპიკერი და მიკროფონი მუშაობს. პირველ რიგში ისინი მიიღებენ მოწვევას მოდერატორისგან (ეკრანის მარჯვენა ქვედა კუთხეში), რომელზეც დასტურის მიცემის შემდეგ გადავლენ ჯგუფური შეხვედრის ფანჯარაში.

ერთერთი მონაწილის საუბრის დროს სასურველია მონაწილეებმა გათიშონ თავიანთი მიკროფონები (იხილეთ სქრინშოტი მაღლა) და ჩართონ მხოლოდ მაშინ, როცა კითხვის დასმას დააპირებენ. ამით მთლიანად შეხვედრის ხარისხი გაუმჯობესდება, რაც განსაკუთრებით დაბალსიჩქარიანი კავშირის გარემოშია მნიშვნელოვანი.

სპეციფიკური კლიენტ სერვისების მართვა Configuration Manager-ის მაგალითზე

5.3.1 ორგანიზაციის სტანდარტული IT-ინფრასტრუქტურის მართვის პრობლემები

თანამედროვე ინფორმაციული ტექნოლოგიების განვითარება კომპიუტერული სისტემების წინაშე ახალ, სპეციფიკურ ამოცანებს აყენებს. ადამიანის საქმიანობის სხვადასხვა სფეროს ავტომატიზაციამ უდავო სარგებლის გარდა ახალი პრობლემებიც დიდი რაოდენობით წარმოშვა. გამოთვლითი ტექნიკის და ინტერნეტის განვითარებამ წარმოებისა და ბიზნესის „მადის“ მკვეთრი ზრდა გამოიწვია. დღეს ჩვენ ვცხოვროთ საზოგადოებაში, რომლის გლობალიზაციის დონე დიდი სისწრაფით იზრდება. საქონელი თუ მომსახურება მინიმალურ დროში შეიძლება იქნეს მიწოდებული დედამიწის ერთი ბოლოდან მეორემდე. გაზრდილი შემომავალი და გამავალი ინფორმაციული ნაკადების ფონზე ნებისმიერი ორგანიზაციისთვის (წარმოების თუ მომსახურების სფეროდან) მნიშვნელოვანია თავისი საქმიანობის არა უბრალოდ, არამედ სწორად ავტომატიზება. ეს არცთუ მარტივი საქმეა, რადგან ნებისმიერი მეტნაკლებად სოლიდური ორგანიზაცია (სახელმწიფო დაწესებულებები, ბანკები, სადაზღვევო კომპანიები და სხვა მრავალი) სადღეისოდ საკმაოდ კარგად განვითარებულ IT-ინფრასტრუქტურას ფლობს და მრავალფეროვან, მათ შორის ონლაინ-სერვისებს

სთავაზობს მომხმარებელს. ხშირად საჭიროა სულ მცირე ათეულ ათასობით კლიენტის მომსახურება, რაშიც ასობით და ათასობით თანამშრომელია ჩართული. ამგვარ პირობებში, ცხადია, ორგანიზაციის ინფორმაციული უზრუნველყოფის ანუ **IT-დეპარტამენტის** თანამშრომლებს (რომელთა რაოდენობა, როგორც წესი, შეზღუდულია) რეგულარურად საკმაოდ შრომატევადი საქმეების შესრულება უწევთ, რაც ამ საქმეების ავტომატიზების და სწორად ორგანიზების აუცილებლობას წარმოშობს.

მოცემული ქვეთავის მიზანს IT-ინფრასტრუქტურის მართვის ავტომატიზაციის თანამედროვე მეთოდების და შესაბამისი პროგრამული უზრუნველყოფის, კერძოდ, კომპანია Microsoft-ის პროგრამა Configuration Manager-ის არქიტექტურისა და ფუნქციონალის მიმოხილვა წარმოადგენს. ნახსენები პროგრამა მოქნილ და მძლავრ ინსტრუმენტს წარმოადგენს როგორც სისტემების ადმინისტრატორებისთვის, ასევე IT-მხარდაჭერის (IT Support) ჯგუფებისთვის, რომელთა საქმიანობაში რუტინული, დროში გაწელილი საქმეების ხვედრითი წილი ყოველთვის მაღალია. ნაჩვენები იქნება ის დროითი და ხარისხობრივი პროგრესი, რომელსაც IT-სპეციალისტი ამ ტიპის პროგრამული უზრუნველყოფის გამოყენებით მიაღწევს.

თანამედროვე ორგანიზაციის IT-ინფრასტრუქტურა აპარატული და პროგრამული უზრუნველყოფის რთულ სიმბიოზს წარმოადგენს. ძირითადი და დამხმარე ელექტრონული სერვისები, რომელსაც თანამშრომლები და კლიენტები იყენებენ, ხშირ შემთხვევაში ინსტალაციისა და გამართვისთვის საკმაოდ დიდ დროით და ადამიანურ რესურსებს მოითხოვენ. ყველაზე მარტივი მაგალითია ოპერაციული სისტემის დაყენება ან განახლება დიდი რაოდენობით კომპიუტერებზე, რასაც IT-მხარდაჭერის ჯგუფის საკმაოდ დიდი დროითი და ადამიანური რესურსი სჭირდება. იგივე შეიძლება ითქვას ნებისმიერი ტიპის პროგრამული უზრუნველყოფის (მათ შორის აპარატული **დრაივერების**) ინსტალაციის პროცესზეც: სპეციალისტები სათითაოდ ჩამოივლიან პერსონალურ კომპიუტერებს ინფორმაციის ოპტიკური მატარებლებით ან ფლემ-მეხსიერებით, რასაც საერთო ჯამში დიდი დრო მიაქვს.

მომდევნო პრობლემას არსებული აპარატული და პროგრამული უზრუნველყოფის **ინვენტარიზაცია** წარმოადგენს. ძველი მიდგომით პრაქტიკულად შეუძლებელია სრულყოფილი ინფორმაციის მიღება იმის შესახებ, თუ რომელი მომხმარებლის განკარგულებაში რომელი პროგრამული უზრუნველყოფა იმყოფება. არაფერს ვამბობთ

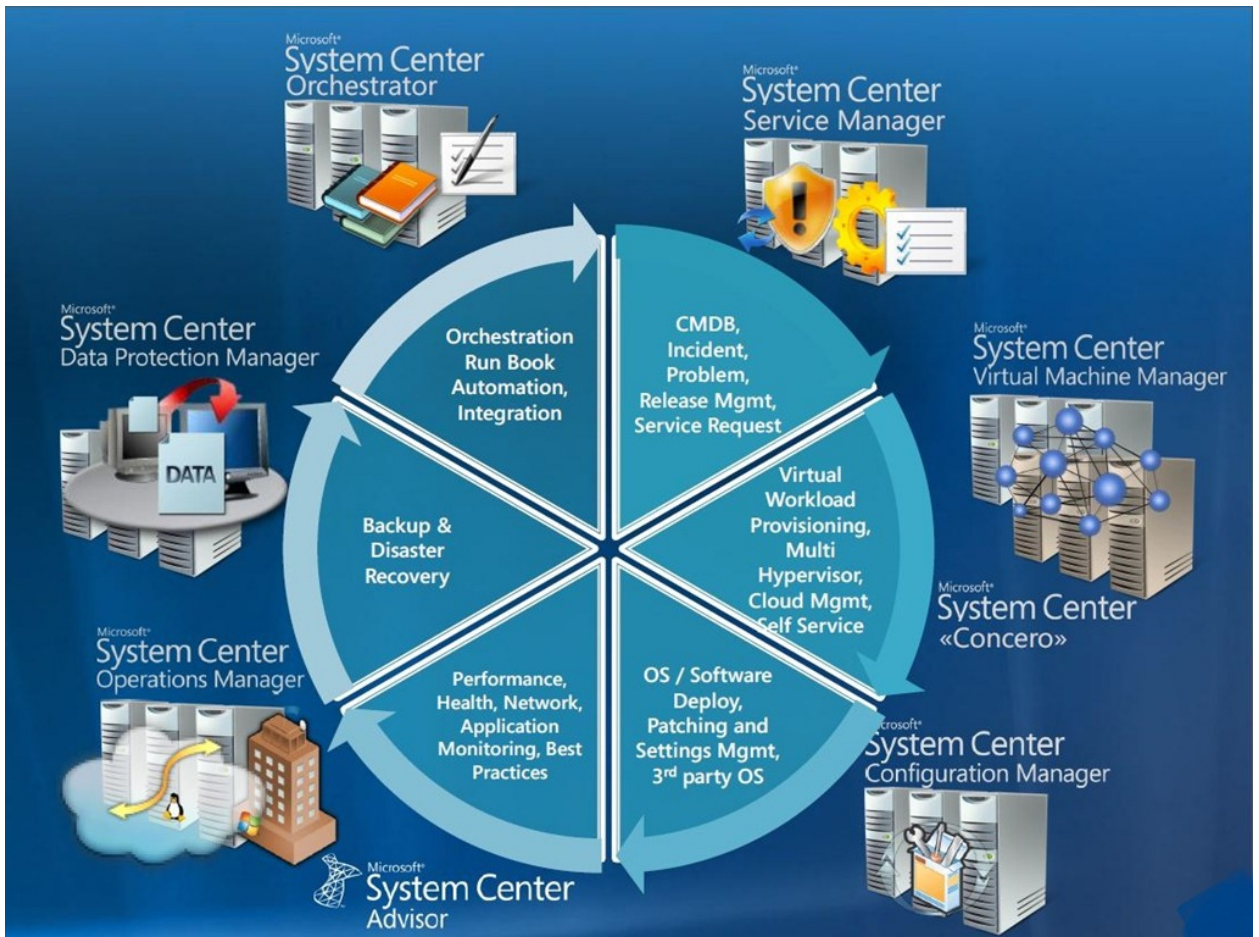
პროგრამების ვერსიების მართვაზე, რომელიც განსაკუთრებით მნიშვნელოვანია ორგანიზაციის საწარმოო და მმართველი აპლიკაციების დანერგვის პროცესში. არსებული გამოცდილება გვეუბნება, რომ პროგრამული უზრუნველყოფის მუდმივი განახლება-გაუმჯობესება, ახალი სერვისების დანერგვა ორგანიზაციაში უწყვეტი პროცესია, ამიტომ თანამშრომელთა კომპიუტერებზე მათი განახლება აუცილებლად მოწესრიგებული პროცესი უნდა იყოს. სხვაგვარად ორგანიზაციის ინფორმაციულ სივრცეში ქაოსური მდგომარეობა შეიქმნება.

მესამე პრობლემას **რეპორტინგის** არარსებობა წარმოადგენს. IT-ინფრასტრუქტურა დინამიურად ცვალებადი სივრცეა. IT-ხელმძღვანელს პერიოდულად სჭირდება დეტალური ინფორმაცია იმის შესახებ, თუ რა რესურსები იხარჯება ორგანიზაციის ინფორმაციულ სივრცეში, რათა სამომავლოდ ხარჯების დაგეგმვა გაუადვილდეს. გამართული, ერთიანი (და არა Excel-ის ფაილებში მიმოფანტული) რეპორტინგის სისტემა IT-ინფრასტრუქტურის ყოველი ელემენტის (აპარატურა, პროგრამული უზრუნველყოფა და მისი ვერსიები) ფუნქციონირების დეტალური აღწერით მართვის აუცილებელი და მძლავრი კომპონენტია.

ამ და სხვა პრობლემებს სადღეისოდ IT-ინფრასტრუქტურის მართვის ცენტრალიზებული, ავტომატიზებული სისტემებით აგვარებენ.

5.3.1.3. MS System Center-ის ზოგადი მიმოხილვა

პროგრამა **Configuration Manager** კომპანია **Microsoft**-ის პროდუქტია. თავის ადრეულ ვერსიებში (1994-2007 წწ.) იგი ცნობილი იყო სახელით **Systems Management Server (SMS)**, ხოლო 2007 წლიდან ინტეგრირებული პროგრამული პაკეტის **System Center**-ის შემადგენელ ნაწილს წარმოადგენს (სურათი).



System Center 2012 - საერთო სტრუქტურა

აღწეროთ მოკლედ System Center 2012-ის კომპონენტები:

- **Orchestrator** – პროცესების ავტომატიზაცია და ინტეგრაცია;
- **Service Manager** – მოთხოვნების (ინციდენტები, სერვისები), პრობლემების, ცვლილებების და პროგრამული რელიზების მომსახურება;
- **Virtual Machine Manager** – ვირტუალური ინფრასტრუქტურის მართვა;
- **Configuration Manager** – აპარატურის და პროგრამული უზრუნველყოფის გამართვის ავტომატიზაცია;
- **Operations Manager** – ოპერაციათა მართვა
- **Data Protection Manager** - მონაცემთა სარეზერვო ასლების მართვა.

თითოეული ჩამოთვლილი კომპონენტი დამოუკიდებელი პროგრამული უზრუნველყოფის სახით გამოდის, მაგრამ ერთიანი პროგრამის სახით იყიდება და იმავდროულად ცალკეული კომპონენტების ურთიერთინტეგრაციის კარგი საშუალებები გააჩნია. მოცემული ექვსი პროგრამა პრაქტიკულად უზრუნველყოფს თანამედროვე IT-

ინფრასტრუქტურის საკვანძო ელემენტების (ვირტუალური ინფრასტრუქტურა, სარეზერვო ასლები, შექმნა, პროცესების მართვა, რესურსების მართვა) მენეჯმენტისა და მონიტორინგის ცენტრების ერთ პუნქტში თავმოყრას, რაც სისტემის ადმინისტრატორებისთვის დროის და ძალების ეკონომიის კარგ საშუალებად უნდა მივიჩნიოთ. ამგვარი მიდგომით ასევე მარტივდება პროგრამული უზრუნველყოფის შესყიდვის და დანერგვის პროცედურებიც.

5.3.1.4. Configuration Manager-ის დაყენება და გამართვა

ჩვენს მიერ განხილული სისტემის მორგება ორგანიზაციის IT-მოდელზე საკმაოდ შრომატევადი ამოცანაა. **Configuration Manager**-ის დაყენებისას პასუხი უნდა გავცეთ შემდეგ მნიშვნელოვან კითხვას: რომელი სისტემის ფარგლებშია თავმოყრილი და იმართება IT-ინფრასტრუქტურის ობიექტები (კომპიუტერები, მომხმარებლები, წესები) და რა სახის წესებია მათი მართვისთვის განსაზღვრული. სტანდარტულად, **Configuration Manager**-ის პირველად მონაცემთა წყაროს **Windows**-ოპერაციული სისტემის ფარგლებში მომუშავე დომენური სერვისი **Active Directory (AD)** წარმოადგენს. გარდა დომენისა, სისტემა Configuration Manager-ის ინსტალაციის წინაპირობებს (პრერეკვიზიტებს) წარმოადგენენ შემდეგი პროგრამული სისტემები:

- WSUS – Windows სისტემების განახლებათა სერვისი;
- Internet Information Server - ვებ-სერვერი;
- MS SQL Server - მონაცემთა ბაზის სერვერი.

ინსტალაციის პროცედურა მოიცავს სისტემის პირველადი გამართვის ეტაპსაც. უნდა შევნიშნოთ, რომ Configuration Manager გამოთვლით რესურსებზე საკმაოდ მაღალ მოთხოვნებს აყენებს (როგორც კომპანია Microsoft-ის პროგრამული პროდუქტების უმრავლესობა). კერძოდ, პროგრამის სერვერული ინფრასტრუქტურა სხვადასხვა ტიპის სერვერებისგან შედგება, რომელთაგან თითოეული, სასურველია, ცალკე ფიზიკურ ან ვირტუალურ სერვერზე იყოს განთავსებული:

- Database Server - მონაცემთა ბაზის სერვერი, რომელზეც განთავსებულია Configuration Manager-ის მთელი მონაცემთა ბაზა;
- Site Server - მმართველი სერვერი, რომლის ხელმძღვანელობითაც შეიძლება სხვადასხვა ფუნქციების მქონე რამდენიმე სერვერი მუშაობდეს, მაგალითად:

o Management Point (MP) – IT-ინფრასტრუქტურის მართვის პუნქტი, რომელიც მისი კონკრეტული სეგმენტის (IP-სივრცე, გეოგრაფიული არე) მართვის ამოცანებს ემსახურება;

o Distribution Point (DP) - კლიენტისთვის განკუთვნილი პროგრამული პაკეტების საცავი (განაწილების პუნქტი), საიდანაც მათი ინსტალაცია უნდა შესრულდეს.

თუ მაგალითად, ორგანიზაციას გააჩნია ქვედანაყოფები თბილისში, ქუთაისსა და ბათუმში. ასეთ შემთხვევაში Configuration Manager-ის ოპტიმალური არქიტექტურა შეიძლება სურათზე მოცემული სახით წარმოვადგინოთ.

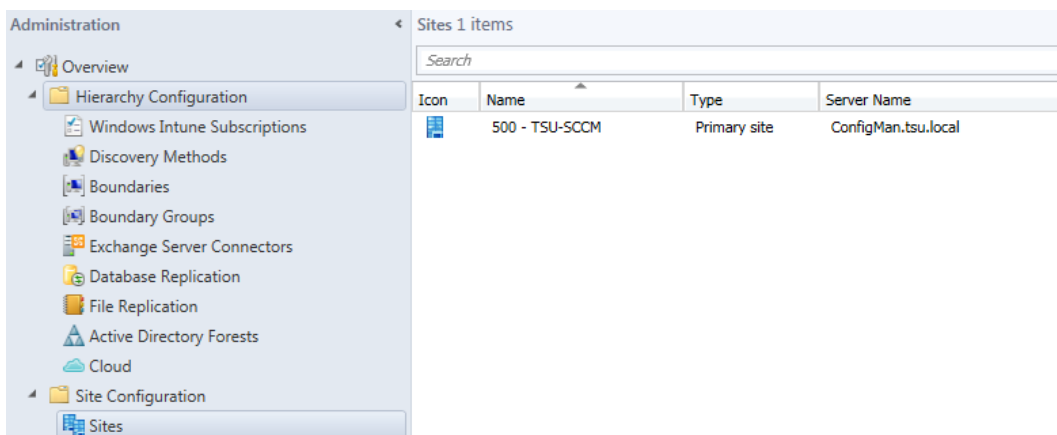
მონაცემთა ბაზის სერვერი (Database Server)

მმართველი სერვერი (Site Server)

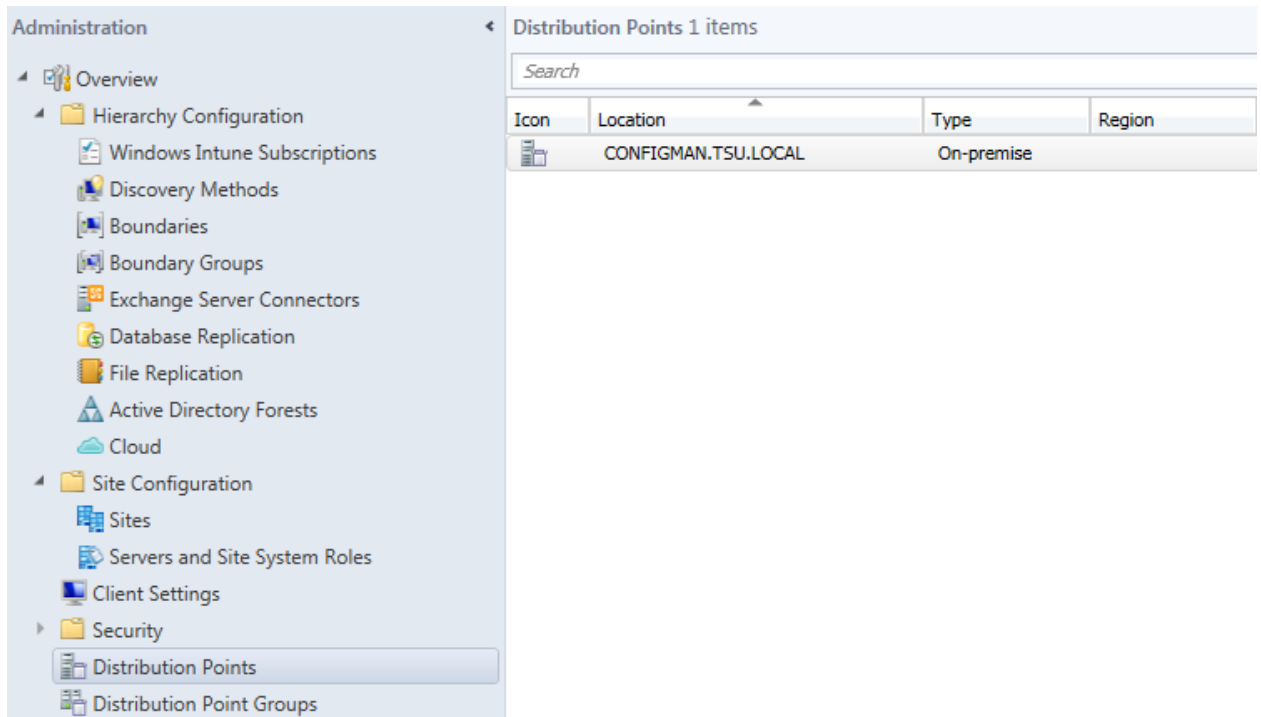


ფუნქციონირების განაწილების ნიმუში Configuration Manager-ში

წარმოვადგინოთ აღწერილი კომპონენტები უშუალოდ პროგრამის გარემოში.

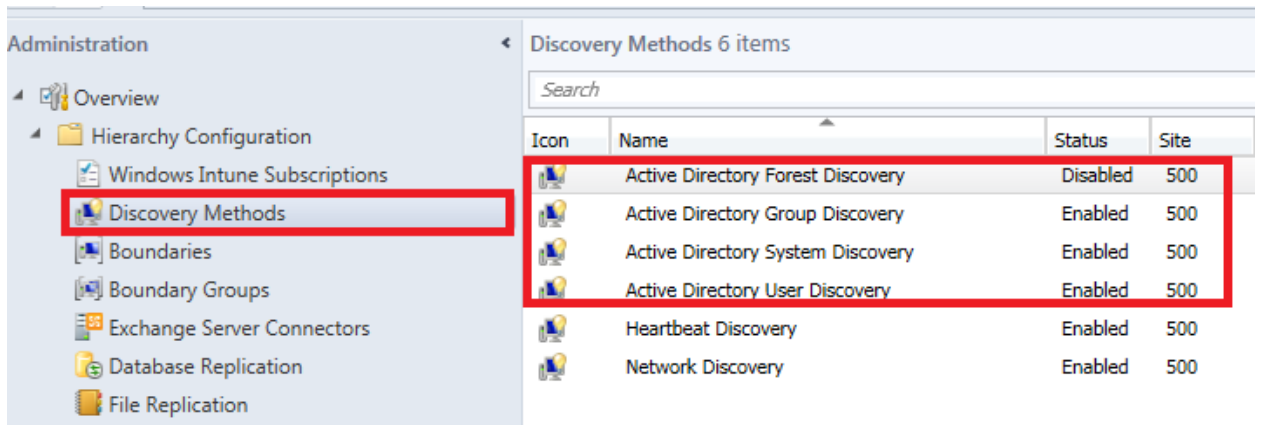


მმართველი სერვერების ინტერფეისი



განაწილების პუნქტების (Distribution Points) ინტერფეისი

სისტემის გამართვის პროცესში მომდევნო მნიშვნელოვან ნაბიჯს IT-ინფრასტრუქტურის შესახებ ინფორმაციის მოპოვება და ერთიან მონაცემთა ბაზაში თავმოყრა წარმოადგენს. როგორც ზემოთ აღვნიშნეთ, Configuration Manager-ის მონაცემთა ბაზისთვის ინფორმაციის ძირითად წყაროს ორგანიზაციის დომენური ინფრასტრუქტურა (Active Directory) წარმოადგენს. ორ სისტემას შორის კავშირი მყარდება მენიუს პუნქტ Administration -> Discovery Methods დახმარებით, რომელშიც შესაბამისი მოდულების (Active Directory User Discovery, Active Directory Group Discovery, Active Directory System Discovery და სხვა) აქტივაციით მოიპოვება და Configuration Manager-ის მონაცემთა ბაზაში თავსდება ინფორმაცია დომენის მომხმარებლების, მომხმარებელთა ჯგუფების, დომენში ჩართული კომპიუტერების და სხვა ობიექტების შესახებ.



ინფორმაციის დაგროვების მეთოდები Configuration Manager-ში

ინფორმაციის მოპოვება სინქრონულ რეჟიმში სრულდება. დომენში განხორციელებული ნებისმიერი ცვლილება (კომპიუტერების, მომხმარებლების, მომხმარებელთა ჯგუფების დამატება, წაშლა, მოდიფიცირება) მაქსიმალურად მოკლე დროში აისახება Configuration Manager-ის მონაცემთა ბაზაში.

სისტემების გამართვის მნიშვნელოვან ეტაპს კლიენტის პროგრამული უზრუნველყოფის დაყენება წარმოადგენს. ნებისმიერი კომპიუტერი ითვლება Configuration Manager-ის კლიენტად, თუ მასზე კლიენტის პროგრამა აყენია. მხოლოდ ამის შემდეგ გვაქვს შესაძლებლობა, მთლიან IT-ინფრასტრუქტურაში ცენტრალიზებული ოპერაციების განხორციელებაზე ვისაუბროთ.

5.3.1.5. მოთხოვნების ფორმირება WQL-ენის საშუალებით

IT-ინფრასტრუქტურის ამა თუ იმ სეგმენტზე Configuration Manager-ის საშუალებით ავტომატიზებული ამოცანების შესასრულებლად თავდაპირველად ამ სეგმენტების (ე.წ. მოწყობილობათა ნაკრებების ანუ **Device Collections**-ების) განსაზღვრაა აუცილებელი. ამ მიზნით სისტემა **Configuration Manager** იყენებს მოთხოვნების სპეციალურ ენას **Windows Management Instrumentation Query Language (WQL)**, რომლის სინტაქსი რელაციური მონაცემთა ბაზების მართვის საყოველთაოდ ცნობილი ენა SQL-ის ბაზაზეა დამყარებული.

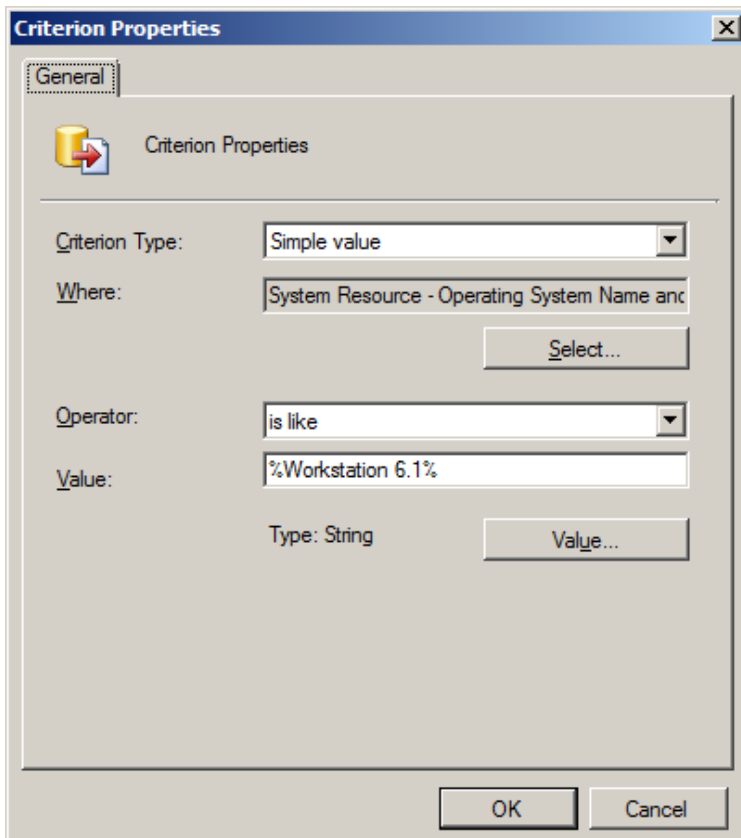
განვიხილოთ WQL-ენაზე შესრულებული მიმართვების და მათი შედეგების რამდენიმე მაგალითი. ქვემოთ, სურათზე ნაჩვენებია რესურსების ფილტრაციის რამდენიმე ბრძანების შედეგი.

Device Collections 17 items						
Search					X	Search
Add Criteria ▾						
Icon	Name	Limiting Collection	Member Count	Members Visible on Site	Referenced Collec	
	All Desktop and Server Clients	All Systems	544	544	0	
	All Mobile Devices	All Systems	0	0	0	
	All Systems		636	636	0	
	All Unknown Computers	All Systems	2	2	0	
	All Windows Servers	All Systems	213	213	3	
	Deploy Server	All Systems	1	1	0	
	Desktop Workstations	All Systems	395	395	3	
	Microsoft SQL Server Collection	All Windows Servers	57	57	0	
	SCCM Server	All Systems	1	1	0	
	Terminal Servers	All Windows Servers	41	41	0	
	VDI Workstations	All Systems	17	17	0	
	Windows 7 Workstations	All Systems	214	214	0	
	Windows Server 2003	All Systems	10	10	0	
	Windows Server 2008	All Systems	152	152	0	
	Windows Server 2012	All Systems	52	52	0	
	Windows Vista Workstation	All Systems	35	35	0	
	Windows XP Workstation	All Systems	162	162	0	

Configuration Manager Device Collection მოდულის ფრაგმენტი

როგორც სკრინშოტზე ჩანს, პროგრამას გამოაქვს მრავალი მნიშვნელოვანი მოწყობილობათა ნაკრებების გაფილტრული სია. აღვნიშნოთ რამდენიმე:

- ყველა კომპიუტერი (636 კომპიუტერი)
- ყველა კომპიუტერი Windows XP-ოპერაციული სისტემით (162 კომპიუტერი);
- ყველა კომპიუტერი Windows 7-ოპერაციული სისტემით (214 კომპიუტერი);
- ყველა კომპიუტერი სერვერული Windows 2008-ოპერაციული სისტემით (152 კომპიუტერი);
- ყველა კომპიუტერი სერვერული Windows 2012-ოპერაციული სისტემით (52 კომპიუტერი);
- ყველა კომპიუტერი, რომელზეც აყენია მონაცემთა ბაზების მართვის სისტემა MS SQL Server (57 კომპიუტერი).



მოწყობილობათა ნაკრების შექმნის გრაფიკული ინტერფეისი

მოწყობილობათა ნაკრების შექმნის ყველაზე მარტივი ხერხია ფილტრაციის ინტერფეისის გამოყენება უამრავი სხვადასხვა კრიტერიუმის მიხედვით, გრაფიკულ რეჟიმში. მაგალითად, მე-6 სურათზე გამოტანილია მოწყობილობათა ნაკრების შექმნის ინტერფეისი Windows 7-სისტემებისთვის, სადაც პარამეტრი:

Where = System Resource – Operating System Name and Version

განსაზღვრავს ფილტრის შინაარსს (ფილტრაცია შესრულდება ოპერაციული სისტემის დასახელებისა

და ვერსიის მიხედვით). ოპერატორი is like და მისი მნიშვნელობა %Workstation% კითხვით, რომ ოპერაციული სისტემის სახელსა და ვერსიაში უნდა ფიგურირებდეს მნიშვნელობა %Workstation%, რომელიც ოპერაციული სისტემა Windows 7-ის „სამუშაო“ დასახელებას წარმოადგენს.

ქვემოთ მოცემულია WQL-ენაზე გენერირებული მოთხოვნების რამდენიმე ნიმუში, რომელთა შესრულების შედეგადაც ზემოთ აღწერილის მსგავსი მოწყობილობათა ნაკრებების მიღება შეგვიძლია.

-- იმ კომპიუტერების სიის გამოტანა, რომლებზე დაყენებულია ოპერაციული სისტემა Windows 7

```
SELECT SMS_R_System.NetbiosName,
SMS_R_System.OperatingSystemNameandVersion from
SMS_R_System where
SMS_R_System.OperatingSystemNameandVersion like "%Workstation 6.1%"
```

-- იმ კომპიუტერების სიის გამოტანა, რომლებზე დაყენებულია Microsoft Excel

```
SELECT SMS_R_System.NetbiosName,
```

```
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName from
SMS_R_System inner join SMS_G_System_ADD_REMOVE_PROGRAMS on
SMS_G_System_ADD_REMOVE_PROGRAMS.ResourceId =
SMS_R_System.ResourceId where
SMS_G_System_ADD_REMOVE_PROGRAMS.DisplayName like "%Excel%"
```

-- ორგანიზაციის ერთერთ განყოფილებაში (OU) შემავალი კომპიუტერების სია

```
SELECT SMS_R_System.NetbiosName,
SMS_R_System.SystemOUName from
SMS_R_System where
SMS_R_System.SystemOUName = "FinanceDepartment"
```

-- Apple-ფირმის ყველა კომპიუტერი

```
Select SMS_R_System.ClientEdition from SMS_R_System where
SMS_R_System.ClientEdition = 5
```

-- ყველა კომპიუტერი UNIX და LINUX ოპერაციული სისტემებით

```
Select SMS_R_System.ClientEdition from SMS_R_System where
SMS_R_System.ClientEdition = 13
```

მოცემული ლისტინგი წარმოადგენს მოწყობილობების, მომხმარებლების და რესურსების ფილტრაციის საშუალებათა ძალიან მცირე ნაწილს. ამ თვალსაზრისით Configuration Manager-ის შესაძლებლობათა სრულად აღწერა მოცემული ნაშრომის ფარგლებში შეუძლებელია.

მოწყობილობათა ნაკრებების შექმნის შემდეგ მათზე მრავალფეროვანი ქმედებების შესრულება შეიძლება, რომელთაგან უმნიშვნელოვანესს პროგრამების და აპლიკაციების ცენტრალიზებული ინსტალაცია წარმოადგენს (იხილეთ მომდევნო ქვეთავი)

5.3.5 აპლიკაციების ცენტრალიზებული ინსტალაცია კლიენტთა კომპიუტერებზე

System Center 2012 Configuration Manager-ის საშუალებით შეიძლება პროგრამული უზრუნველყოფის ცენტრალიზებულად, ერთი ბრძანებით ინსტალაცია დიდი ოდენობით კომპიუტერებზე. ზემოთ აღწერილი პროცედურის ჩატარების (მოწყობილობათა ნაკრებების შექმნა) შემდეგ სისტემის ადმინისტრატორს თავისუფლად შეუძლია ისეთი ოპერაციების ჩატარება, როგორცაა მაგალითად:

- ყველა Windows XP-სისტემიან კომპიუტერზე MS Office 2007-ის დაყენება
- საფინანსო და მატერიალური რესურსების მართვის დეპარტამენტების ყველა კომპიუტერზე წარმოების მართვის (ERP) სისტემა „ორის-მენეჯერის“ დაყენება
- და ასე შემდეგ...

პროცედურის განსახორციელებლად რამდენიმე წინასწარი მოქმედების შესრულებაა აუცილებელი:

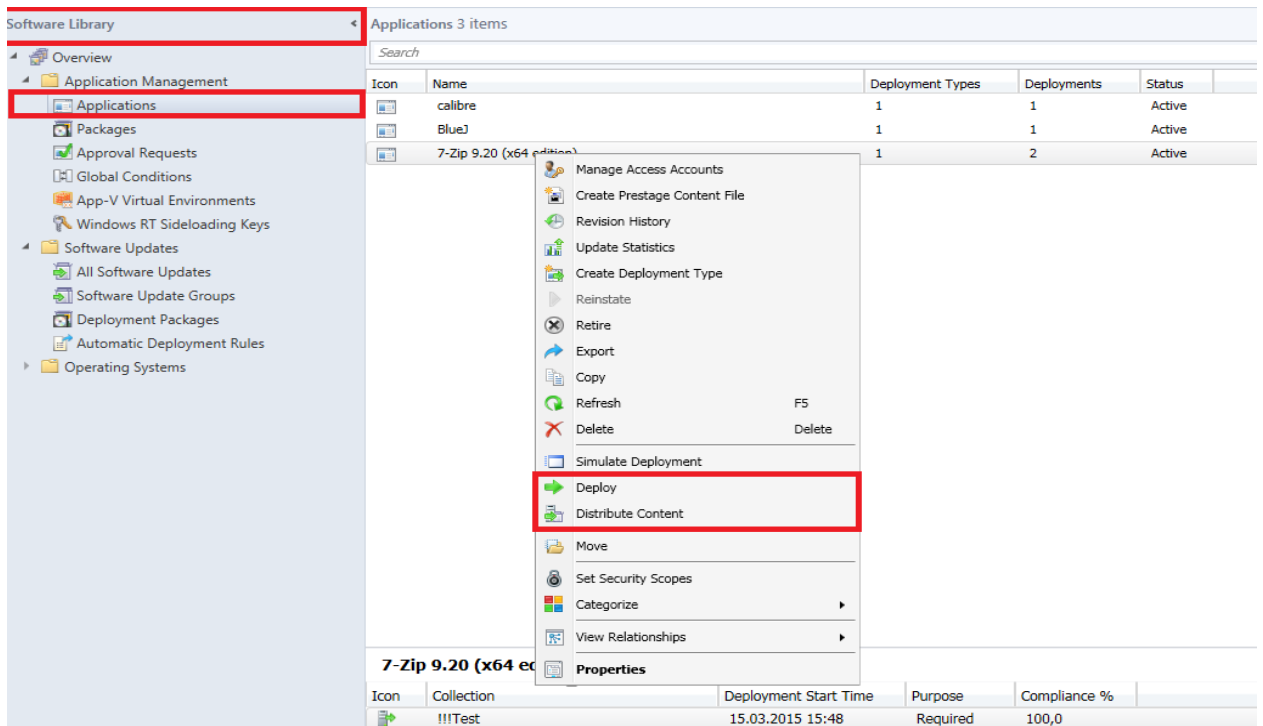
- კომპიუტერებზე კლიენტ-პროგრამების დაყენება
- დასაყენებელი პროგრამის (აპლიკაციის) ჩართვა Configuration Manager-ის საცავში და პარამეტრების განსაზღვრა - მენიუს პუნქტი Software Library -> Applications; ბრძანებები Create Application, Select OS for Installation

• აპლიკაციის გავრცელება განაწილების პუნქტებში (Distribution Points) - იქვე ბრძანება (მაუსის მარჯვენა ღილაკი აპლიკაციაზე -> Distribute Content)

• აპლიკაციის ინსტალაციის პროცედურის გაშვება შერჩეულ მოწყობილობათა ნაკრებზე (კომპიუტერების ქვესიმრავლე) - (მაუსის მარჯვენა ღილაკი აპლიკაციაზე -> Deploy

- პროცესის მონიტორინგი Deployments-განყოფილებაში

პროგრამული ინტერფეისის შესაბამისი ფრაგმენტი ძირითადი ბრძანებებით იხილეთ სურათზე.

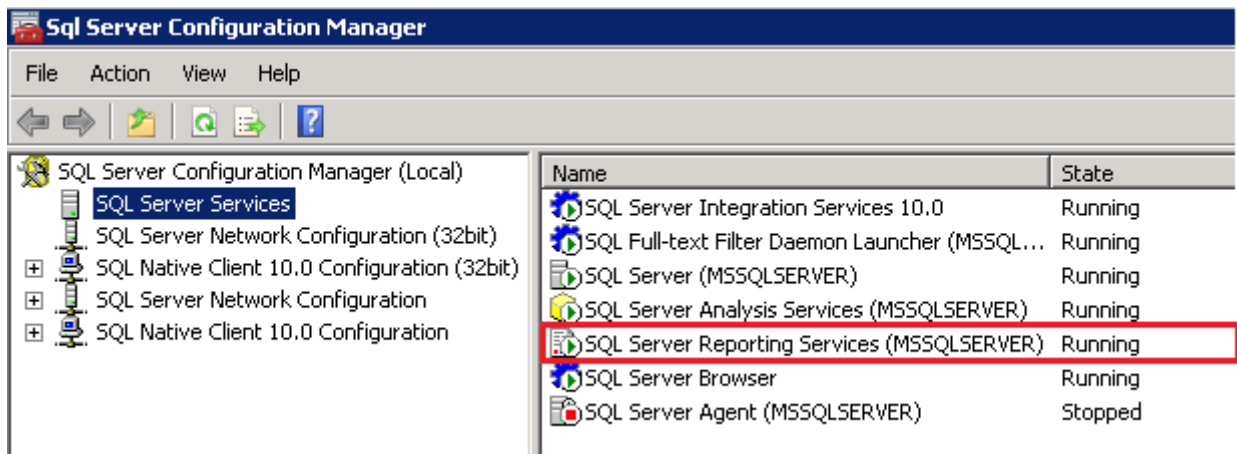


IT-ინფრასტრუქტურაში პროგრამის ცენტრალიზებული ინსტალაციის ინტერფეისი

5.3.2. რეპორტინგი

რეპორტინგი აუცილებელია ნებისმიერი სეროზული ინფორმაციული სისტემისთვის, მითუმეტეს, როცა IT-ინფრასტრუქტურის მართვის ერთიან სისტემაზე ვსაუბრობთ. პროგრამა Configuration Manager მრავალრიცხოვანი რეპორტების გენერირების საშუალებას გვაძლევს მენიუს პუნქტ Monitoring -> Reporting-ის საშუალებით.

რეპორტების გენერირება უშუალოდ მონაცემთა ბაზების მართვის სისტემა MS SQL Server-ის ინსტრუმენტებით, კერძოდ Reporting Service-ბით სრულდება. რეპორტინგის სერვერი მონაცემთა ბაზების მართვის სისტემის ინსტალაციის დროს დასაყენებელი კომპონენტების სიაში უნდა იყოს მითითებული, ხოლო ინსტალაციის დასრულების შემდეგ იგი გამოჩნდება SQL-სერვერთა სიაში, რომლის მართვასაც ემსახურება უტილიტა SQL Server Configuration Manager (იხილეთ სურათი).



რეპორტინგის სერვისის მონაცემთა ბაზების სერვერთა მართვის ინტერფეისში

განვიხილოთ რეპორტის აგების მაგალითი ამოცანისთვის „ორგანიზაციაში მომუშავე ყველა პროგრამა“. რეპორტის გენერირების შემდეგ მიიღება Excel-ის ფაილი, რომელშიც შემდეგი ინფორმაცია აისახება: პროგრამის სახელი, მწარმოებელი, ვერსიის ნომერი და კომპიუტერთა რაოდენობა, რომელზეც ეს პროგრამა აყენია. საყურადღებოა, რომ Excel-ის ფაილშივე შესაბამის ველებთან დაკავშირებულია ბმულები, რომელთა საშუალებითაც დამატებითი ინფორმაციის მიღება შეიძლება. მაგალითად, კომპიუტერების რაოდენობაზე დაწკაპუნებისას იმ კომპიუტერების დასახელებები გამოვა, რომლებზეც მითითებული პროგრამა აყენია. ქვემოთ, სურათზე რეპორტის ფრაგმენტი გამოტანილი.

Software 01A - Summary of installed software in a specific collection

Product Name	Publisher	Version	Count of Software	Software Properties Hash
{{F86C29B6-7D6E-4B49-8955-F38CED3F5C24}}			2	dfca4a082933eecd76411fa6da1864711
7-Zip 4.65			15	87fa8d72a6d23628df37d4a6369980ec
7-Zip 9.20			3	d4e63a83dc30096fc9efff4160a91f36
AC3Filter (remove only)			2	8034ac2232cdc3952326c007fadfc230
Active@ UNDELETE 7			1	bc9d37d9e0795611f57d0174950c926
ActiveXSave Version1.1.3		1.1	2	9dffe0810c82a201f2170d36b380bc5d
Adobe SVG Viewer 3.0		3.0	1	0576353d1470f1c8ed795798aefc8bd5
Advanced IP Scanner v1.5			1	e228bac5876d221a8a828b650d715c3
Advanced Office Password Recovery (remove only)			1	b7c32a6869147c06635813f7e61fa964
Advanced Port Scanner v1.3			1	8f8e6e31e3677fdbc98c0f1b0df98a0d35
Android Commander version 0.7.9.11		0.7	2	bc8e5d36830665f024219f5451722a47
ArchiCAD 11 INT			6	6596db8567258f0b2e45be00d130aa9
ArchiCAD 12 USA			1	255c99e80baae2d2da093a1e4e31fe7
ATI - Software Uninstall Utility		6.14	6	8d6747068cba5c87a3138b20e02e2d0
ATI Catalyst Control Center		1.2	3	7d38470c9fe27e9409933038447035d
ATI Display Driver		8.261	1	7668826b418a198585ed1ec12fa29a5c
ATI Display Driver		8.30-060908a1-036948C-HP	5	46e3a317fd19deb1d1acecf640e51b909
ATI Display Driver		8.471-080225a1-059746C-ATI	3	5e7cfec6fca30b5329cfe8517ec4f536
ATI Display Driver		8.591-090225a-076825C-ATI	2	d9e1c52c4f0f56e282c1f41e1a18b00d
ATI Display Driver		8.593	4	14190da6dbdea69ce9f28df697e09307
Avant Browser (remove only)			4	650a139d774769275d626cea20efa99
BDE			4	b007437d0aef522e9e4f18e2d89aec7e
BIXOLON SLP-D420 Windows Driver			1	faaa696f2d99918118bc41e3833a165d
Bloomberg Excel Tools			1	f94bb46bb92646407a88cd0b647b3cfd
Bloomberg Office Tools (32-bit)			1	beb112d5d6ef18dd70259f4e352b9fbfc
Bloomberg PFM Upload Tool for Microsoft Excel			1	00fcc51ad259c2681330441a1f45a62c
Bloomberg Professional Service			1	3274f6076b48ea5ae8abf5a2f35c6dd1
Bloomberg SFD Data Dictionary			1	f5e2689d46c7e8320e27e8135a241ba
Borland Database Engine Setup			1	29c100d3d8464b4820ae5c1fd5325f75
Bundled software uninstaller			1	734f258443b2323d0050e970257199c
Camera Finder			3	f7f343d55d04a1f743dd6c46d72bb906
				9f755266148dd9bdb1436aec561d736
				5b68f42d35ddb619efa6ee2db4cc9fb5
				172b1359ba5aeac9d017cec3ed56e19

რეპორტი "ყველა პროგრამა"

პრაქტიკული სავარჯიშო

1. შეასრულეთ პროგრამა MS System Center 2012 Configuration Manager-ის ინსტალაცია, დაუკავშირეთ იგი Active Directory-ს და შეასრულეთ მოხმარებლების და კომპიუტერების იმპორტი;
2. შექმენით კოლექცია (Device Collection) WQL-ენის გამოყენებით: ყველა მანქანა ოპერაციული სისტემა Windows 7-ით;
3. შეასრულეთ ანტივირუსული პროგრამა Microsoft Security Essential-ის ცენტრალიზებული ინსტალაცია (Deployment) კლიენტების კომპიუტერებზე Configuration Manager-ის გამოყენებით.

ცოდნის შეფასება

სტუდენტებს მიეცემათ პრაქტიკული დავალება

- შეასრულონ სატესტო სერვერზე ელექტრონული ფოსტის სერვერ MS Exchange 2013-ის, შიდასაკომუნიკაციო სისტემა MS Lync 2010-ის და IT-ინფრასტრუქტურის მართვის სისტემა MS System Center 2012 Configuration Manager-ის ინსტალაცია;
- შექმნან ელ.ფოსტის მონაცემთა ბაზები (სთორები) და ელექტრონული საფოსტო ყუთები (მეილბოქსები). დააწესონ მათთვის მეხსიერების კვოტები და შეზღუდონ გარკვეულ მისართებზე გამგზავ/მიმღებთა სია;
- საკომუნიკაციო სისტემის მართვის პანელში დაამატონ ახალი მოხმარებლები და მათი სახელით კლიენტ-კომპიუტერებზე შეასრულონ რეგისტრაცია Lync-სისტემაში. წარმოადგინონ ტექსტური, აუდიო- და ვიდეო კომუნიკაციის, აგრეთვე ჯგუფური შეხვედრების მაგალითები;
- Configuration Manager-ის გარემოში შექმენით კოლექციები (Device Collections) სხვადასხვა კრიტერიუმების მიხედვით (ყველა პერსონალური კომპიუტერი, ყველა ოპერაციული სისტემა Windows 7). შეასრულეთ კოლექციის შემადგენელ კომპიუტერებზე პროგრამის (მაგ. ანტივირუსი) ერთიანი ინსტალაცია.

შემფასებელი აკვირდება შესაფასებელ პირის მუშაობას პროფესიული სტანდარტით (პროგრამით / მოდულით) განსაზღვრული ამოცანების შესრულების პროცესში. დაკვირვება ხორციელდება კომპიუტერებით აღჭურვილ ლაბორატორიაში,

სადაც შესაფასებელი პირი პრაქტიკულ საქმიანობას ეწევა. შემფასებელმა წინასწარ უნდა დაგეგმოს დაკვირვების პროცესი, იმის დასადგენად, თუ რამდენად სწორად იყენებს შესაფასებელი პირი ცოდნას, უნარებსა და ყველა რესურსს შედეგის მისაღწევად.

შეფასება განხორციელდება პროცესზე დაკვირვებით, წინასწარ განსაზღვრული შეფასების ინდიკატორების საფუძველზე.

დავალების ნიმუში და შეფასების რუბრიკა

პროცესზე დაკვირვება

- ✚ შეასრულოს სხვადასხვა საკომუნიკაციო და ინფრასტრუქტურის მართვის პროგრამების ინსტალაცია
- ✚ გამოიყენოს დაყენებული პრაქტიკული ამოცანებისთვის (ელ.ფოსტის სთორების და მეილბოქსების შექმნა, ტექსტური, ვიდეო- და აუდიო კომუნიკაციის მართვა, IT-ინფრასტრუქტურის მართვა)

სწავლის შედეგი	N	დასახელება	შეფასება	
			კი	არა
საფოსტო და საკომუნიკაციო სერვერების გამართვა	1.	შეასრულა ელ.ფოსტის სერვერის (MS Exchange Server 2012) ინსტალაცია		
	2.	შეასრულა საკომუნიკაციო სერვერის (MS Lync 2010) ინსტალაცია		
	3.	შეასრულა IT-ინფრასტრუქტურის მართვის სერვისის (System Center 2012 Configuration Manager) ინსტალაცია		
	4.	შექმნა ელ. ფოსტის საცავები (სთორები) და საფოსტო ყუთები (მეილბოქსები) Exchange Server-ზე		
	5.	შეასრულა სთორებსა და მეილბოქსებზე გამოყოფილი გარე მეხსიერების კვოტირება Exchange Server-ზე		
	6.	შეასრულა ელ.ფოსტის მისამართზე გაგზავნა/მიღების უფლებების განსაზღვრა ცალკეული ადრესატებისთვის		

7.	შეასრულა Lync-ის კლიენტ-პროგრამების ინსტალაცია საკომუნიკაციო სერვისისთვის და დააკავშირა მომხმარებლები ერთმანეთს ტექსტურ, აუდიო- და ვიდეო რეჟიმებში		
8.	შეასრულა ჯგუფური შეხვედრის ორგანიზება საკომუნიკაციო სერვისის ფარგლებში		
9.	შექმნა მოწყობილობათა კოლექციები (Device Collections) სხვადასხვა კრიტერიუმებით Configuration Manager-ში		
10.	შეასრულა ანტივირუსის ცენტრალიზებული ინსტალაცია Configuration Manager-იდან		

სწავლის შედეგი ჩაითვლება მიღწეულად თუ სტუდენტმა შეძლო შედეგის მინიმუმ 8 პუნქტის შესრულება

6. კონტროლისა და მონიტორინგის სისტემები

6.1. დაშორებული წვდომის სერვისების (Remote Access)

ადმინისტრირება

ვირტუალური დაცული ქსელის (VPN) განთავსება RRAS დახმარებით

დაუცველ ქსელებში გადასაცემი ინფორმაციის დაცვის გავრცელებული მეთოდია ვირტუალური დაცული ქსელის შექმნა (**Virtual Private Network – VPN**), რომელიც არსებითად არის კავშირი ორ კერძო კვანძს ან ქსელში შორის. ის ასრულებს ტრაფიკის დაცვასა და შიფრაციას ორ მხარეს შორის, რათა აკრძალულ იქნას მისი არასანქცირებული „მოსმენა“. მომხმარებლის გადმოსახედიდან **VPN** ჩანს როგორც ჩვეულებრივი კავშირი ქსელის სხვადასხვა სეგმენტს შორის - სწორედ აქედან მოდის ტერმინი ვირტუალური დაცული ქსელი.

VPN-ით გადასაცემი მონაცემები ენკაპსულირდება, ანუ მონაცემებს თავსართში ემატება ველი, რომელიც მიუთითებს მონაცემთა დანიშნულების ადგილს. შემდეგ პაკეტში არსებული ინფორმაცია იშიფრება, მისი შემცველობის დასაცავად. ყოველივე ამის შემდეგ დაშიფრული პაკეტები იგზავნება სერვერის ქსელში ე.წ **VPN** ტუნელის დახმარებით.

დაშორებული წვდომის (**Remote Access**) როლი **Windows Server 2012**-ში უზრუნველყოფს **VPN** ქსელის შექმნას და ინტეგრირდება **NPS** როლთანკლიენტის ეფექტურობის შესამოწმებლად, **VPN** სეანსის შექმნამდე.

ტუნელირების პროტოკოლები

ტუნელირების პროტოკოლი - ეს არის სპეციალური ტექნოლოგია, რომელიც განსაზღვრავს მონაცემების ენკაპსულაციის, გადაცემის და დეკაპსულაციის საშუალებებს, მათი **VPN** კავშირით გადაცემის დროს. არსებობს ტუნელირების პროტოკოლების სხვადასხვა რეალიზაცია, რომლებიც შეესაბამებიან ღია სისტემების ურთიერთქმედების (**Open System Interconnection – OSI**) მოდელის სხვადასხვა დონეს. **OSI**

მოდელი შედგება შვიდი დონისაგან და VPN ტუნელირების პროტოკოლები მონაცემთა გაცვლისთვის იყენებენ მეორე და მესამე დონეებს.

საუკეთესო უსაფრთხო პროტოკოლები უზრუნველყოფენ:

- **მონაცემთა კონფიდენციალურობას (data confidentiality)** - პროტოკოლი შიფრავს მონაცემებს ისე, რომ მესამე პირს არ შეეძლოს მისი წაკითხვა საერთოწვდომის ქსელში გადაცემისას;
- **მონაცემთა მთლიანობას (data integrity)** - ამ ფუნქციის პროტოკოლების გამოყენებისას შევიტყობთ, თუ მესამე პირი შეცვლის მონაცემებს ქსელში გადაცემისას.
- **ხელახალი გადაცემისაგან დაცვას (replay protection)** - გარანტიას იძლევა, რომ ერთი და იგივე მონაცემები გადაცემული იქნება მხოლოდ ერთხელ. **Replay Attack** შეტევისას ბოროტმოქმედი იპარავს გადაცემულ მონაცემებს და შემდეგ ხელახლა აგზავნის.
- **მონაცემთა წყაროს ნამდვილობის შემოწმებას (data origin authentication)** - ინფორმაციის გამგზავნი და მიმღები უნდა იყვნენ დარწმუნებული გადაცემული და მიღებული მონაცემების წარმომავლობაზე.

Windows Server 2012 მხარს უჭერს VPN-ის შემდეგ პროტოკოლებს (პროტოკოლები დალაგებულია უსაფრთხოების ზრდადობის მიხედვით):

- **PPTP (Point-to-Point Tunneling Protocol)** – VPN ქსელი PPTP პროტოკოლით, VPN-ის ყველაზე დაბალი უსაფრთხოების ფორმაა. რამეთუ ისინი არ საჭიროებენ ინფრასტრუქტურასთან საერთოწვდომის გასაღებს (**PKI - public-key infrastructure**), რომლებიც ასევე ნაკლებად გავრცელებულნი არიან. **PPTP** შეერთებაში გამოიყენება ნამდვილობის შესამოწმებელი პროტოკოლები: **MS-CHAP, MS-CHAPv2, EAP** და **PEAP**. მონაცემთა შიფრაციისათვის გამოიყენება **MPPE (Microsoft Point-to-Point Encryption)** პროტოკოლი. **PPTP** შეერთება უზრუნველყოფს მონაცემთა კონფიდენციალურობას, მაგრამ არ იძლევა მათი მთლიანობისა და წყაროს ნამდვილობის შემოწმების გარანტიას. ზოგიერთი მოძველებული **NAT-მოწყობილობა** მხარს არ უჭერს **PPTP**-ს.

L2TP/IPsec (Layer 2 Tunneling Protocol/ Internet Protocol Security) პროტოკოლი უზრუნველყოფს მონაცემთა წყაროს ნამდვილობის შემოწმებას, მთლიანობას,

განმეორებითი გაგზავნისაგან დაცვას და კონფიდენციალურობას თითოეული პაკეტისთვის ცალ-ცალკე. **L2TP/IPsec**-ში გამოიყენება ციფრული სერტიფიკატები, ამიტომ მას სჭირდება წვდომა სერტიფიკატების მომსახურების ინფრასტრუქტურასთან. **L2TP/IPsec** პროტოკოლს მხარს უჭერს სხვა მწარმოებლის უმრავლესი **VPN**-პროდუქტი. **L2TP/IPsec**-ის გამოყენება შეუძლია ყველა **NAT** მოწყობილობას, მხოლოდ იმ შემთხვევაში თუ კლიენტი და სერვერი მხარს უჭერს **IPsec NAT Traversal (NAT-T)**-ს, მაგალითად, **Windows 7, Windows 8.1, Windows Server 2003, Windows Server 2008, Windows Server 2012**. **L2TP** შეიძლება მოიმართოს ნამდვილობის შემოწმებლად, სერტიფიკატების ან საერთო გასაღების საფუძველზე.

- **SSTP** – **VPN** ტუნელები **SSTP** პროტოკოლით იყენებენ **443** პორტს. ეს ნიშნავს იმას, რომ **VPN** ტრაფიკ **SSTP**-ს შეუძლია გაიაროს პრაქტიკულად ყველა ფაიერვოლი, ინტერნეტთან დაშვებული წვდომით, განსახვავებით **PPTP, L2TP/IPsec** და **IKEv2 (Internet Key Exchange version 2)** პროტოკოლებისაგან. **SSTP** აგზავნის ტრაფიკს **HTTPS** პროტოკოლის **SSL**-არხით. ის მხარს უჭერს მონაცემთა წყაროს ნამდვილობის შემოწმებას, მთლიანობას, განმეორებითი გადაგზავნისაგან დაცვას და კონფიდენციალურობას. არასდროს გამოიყენოთ **SSTP** პროტოკოლი **Web-Proxy**-სერვერის გავლით, რომელიც იყენებს ნამდვილობის შემოწმებას.

- **IKEv2** - ეს არის პროტოკოლი, რომელსაც მხარს არ უჭერენ **Windows**-ის ძველი ვერსიები. ის მუშაობს **IPv6** და **VPN Reconnect** ფუნქციებით, მხარს უჭერს **EAP (Extensible Authentication Protocol)** პროტოკოლს და კომპიუტერის სერტიფიკატებს კლიენტის მხრიდან ნამდვილობის შესამოწმებლად. აქ შედიან **PEAP, EAP-MSCHAP v2**, სმარტ-ბარათები და სხვა სერტიფიკატები.

IKEv2 მხარს არ უჭერს ნამდვილობის შემოწმებელ **POP, CHAP** ან **MS-CHAPv2 (EAP-ის გარეშე)** პროტოკოლებს. **IKEv2** უზრუნველყოფს მონაცემთა წყაროს ნამდვილობის შემოწმებას, მთლიანობას, ხელახალი გადაგზავნისაგან დაცვას და კონფიდენციალურობას. **IKEv2** იყენებს **UDP** პორტ **500**-ს.

VPN-ის აქტივაცია RRAS (Routing and Remote Access Server) სერვერზე

Remote Access როლის დასამატებლად შეასრულეთ შემდეგი ეტაპები:

- სერვერების მართვის ფანჯარაში აირჩიეთ **Manage** -> **Add Roles and Features**.
- **Before you Begin** გვერდზე დააწექით **Next** ღილაკს.
- გამოსულ **Select Installation type** გვერდზე აირჩიეთ **Role/Feature Based Install**

ვარიანტი და დააჭირეთ **Next** ღილაკს.

- **Select Destination Server** გვერდზე აირჩიეთ **Select a Server from the Server Pool** ვარიანტი, დააწექით სერვერების სახელებზე, რომლებზეც უნდა დაყენდეს **Remote Access** როლი და დააჭირეთ **Next** ღილაკს.

- მომდევნო **Select Server Roles** ფანჯარაში აირჩიეთ **Remote Access** ვარიანტი და შემდეგ სამჯერ დააჭირეთ **Next** ღილაკს. **Select Role Services** გვერდზე აირჩიეთ **Direct Access and VPN (RAS)** ვარიანტი და დააწექით **Next** ღილაკს.

- **Confirm Installation Selections** გვერდზე დააჭირეთ ღილაკს **Install**.

- მომდევნო **Results** ფანჯარაში შეამოწმეთ ინსტალაციის წარმატებით შესრულება.

იმისათვის, რომ მოვმართოთ **Remote Access** სერვერის ყველაზე გავრცელებული ფუნქცია - **Gateway VPN**, შეასრულეთ შემდეგი მოქმედებები.

- გახსენით **Routing and Remote Access** კონსოლი, სერვერების მართვის **Tools** მენიუდან.

- აირჩიეთ სერვერის ლოკალური სახელი ან დაუკავშირდით **Remote Access** დაშორებულ სერვერს. ამისათვის მაუსის მარჯვენა ღილაკით დააჭირეთ **Routing and Remote Access** პუნქტს და კონტექსტურ მენიუში აირჩიეთ **Add Server**.

- შემდეგ დააჭირეთ **Action** მენიუს და ჩამომლილ მენიუში აირჩიეთ **Configure and enable Routing and Remote Access**.

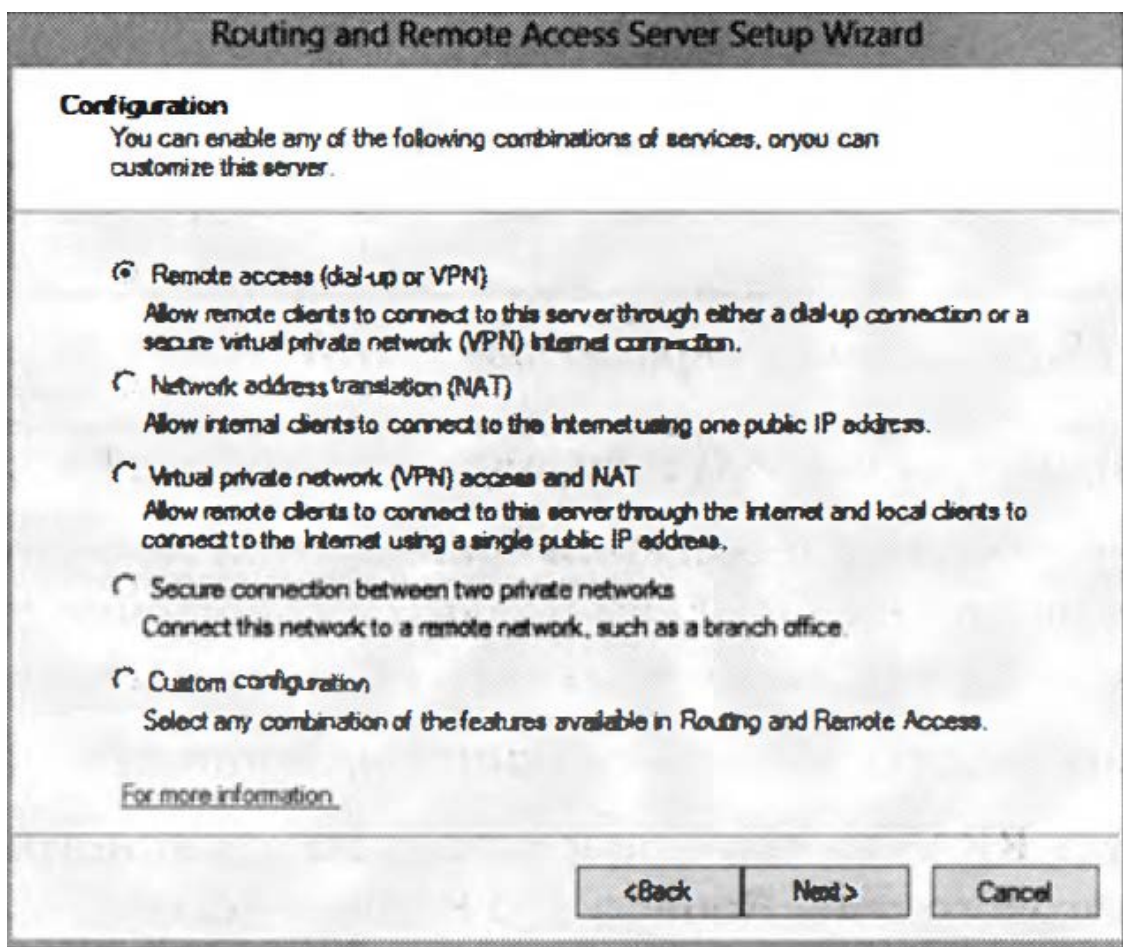
- მომდევნო ფანჯარაში დააჭირეთ **Next** ღილაკს.

- აირჩიეთ პარამეტრების ერთ-ერთი ვარიანტი (სურ. 6.1). განსხვავებულ სიტუაციაში საჭიროა სხვადასხვა პარამეტრები. მაგალითად, საიტთაშორისი **VPN**-ის შესაქმნელად გადამრთველი უნდა დავაყენოთ **Secure Connection Between Two Private Networks** პუნქტზე. ჩვენს შემთხვევაში ვქმნით მარტივ **VPN** ქსელს, ამიტომ აირჩიეთ ვარიანტი **Remote Access (Dial-up or VPN)**.

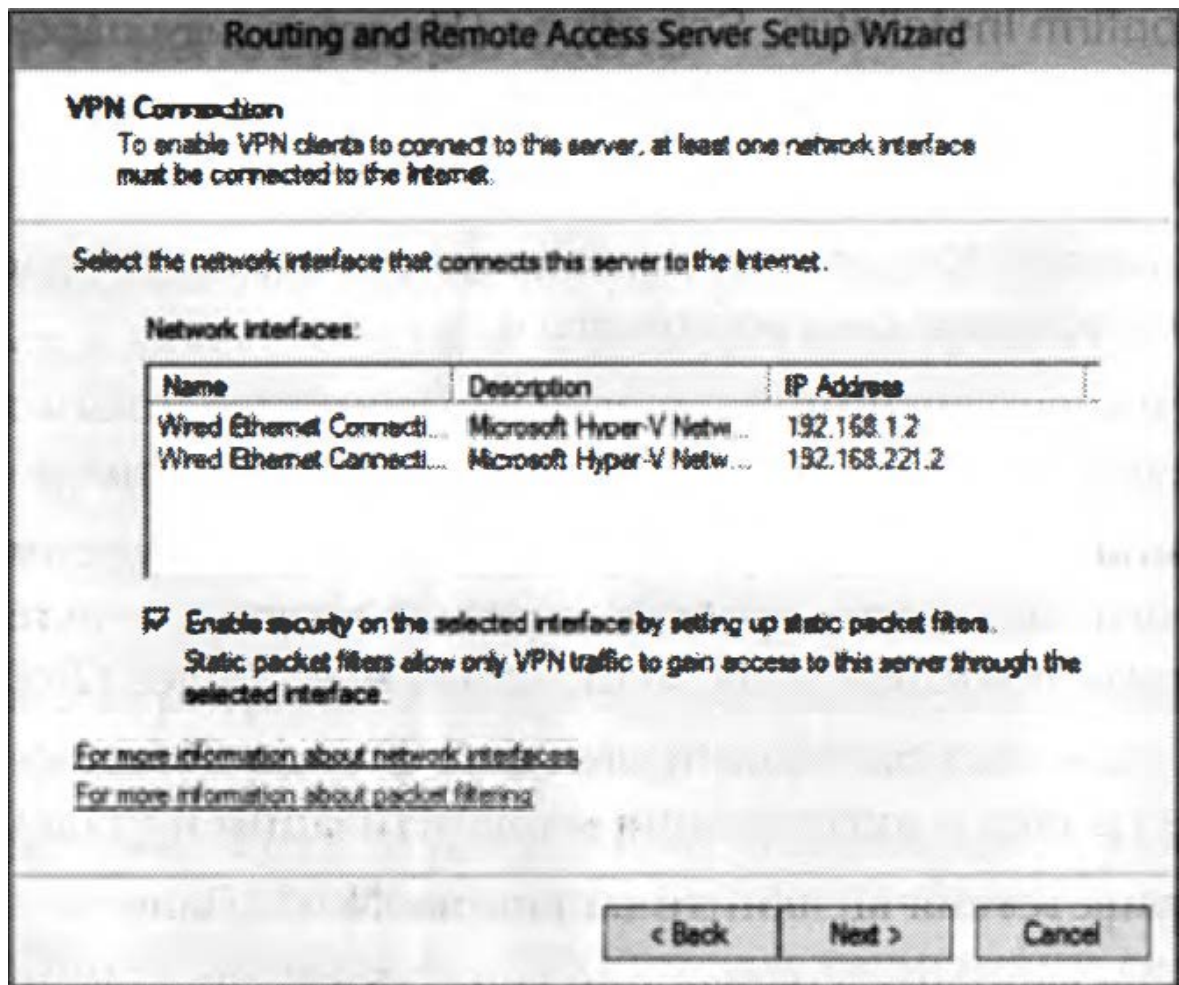
- **Remote Access** გვერდზე მონიშნეთ VPN პუნქტი. კომპიუტერებული შეერთების შესაქმნელად (მაგალითად, თუ VPN კომპუტატორზე მიერთებულია მოდემი) უნდა მოვნიშნოთ ასევე **Dial-up** განყოფილება. დააჭირეთ **Next** ღილაკს.

- **VPN Connection** გვერდზე (სურ. 6.2) მიუთითეთ ქსელში ჩართული ქსელის ადაპტერი, საიდანაც გავლენ VPN კლიენტები. ეს შეიძლება იყოს ინტერნეტი ან დაცული პერიფერიული ქსელი, ისევე როგორც DMZ. დააჭირეთ **Next** ღილაკს.

- მომდევნო **IP Address Assignment** გვერდზე მიუთითეთ თუ როგორ უნდა მიიღონ VPN კლიენტებმა თავიანთი IP მისამართი (როგორც წესი - **Automatically**). რის შემდეგაც უნდა მივუთითოთ ხელით მართვის დიაპაზონი. დააჭირეთ **Next** ღილაკს.

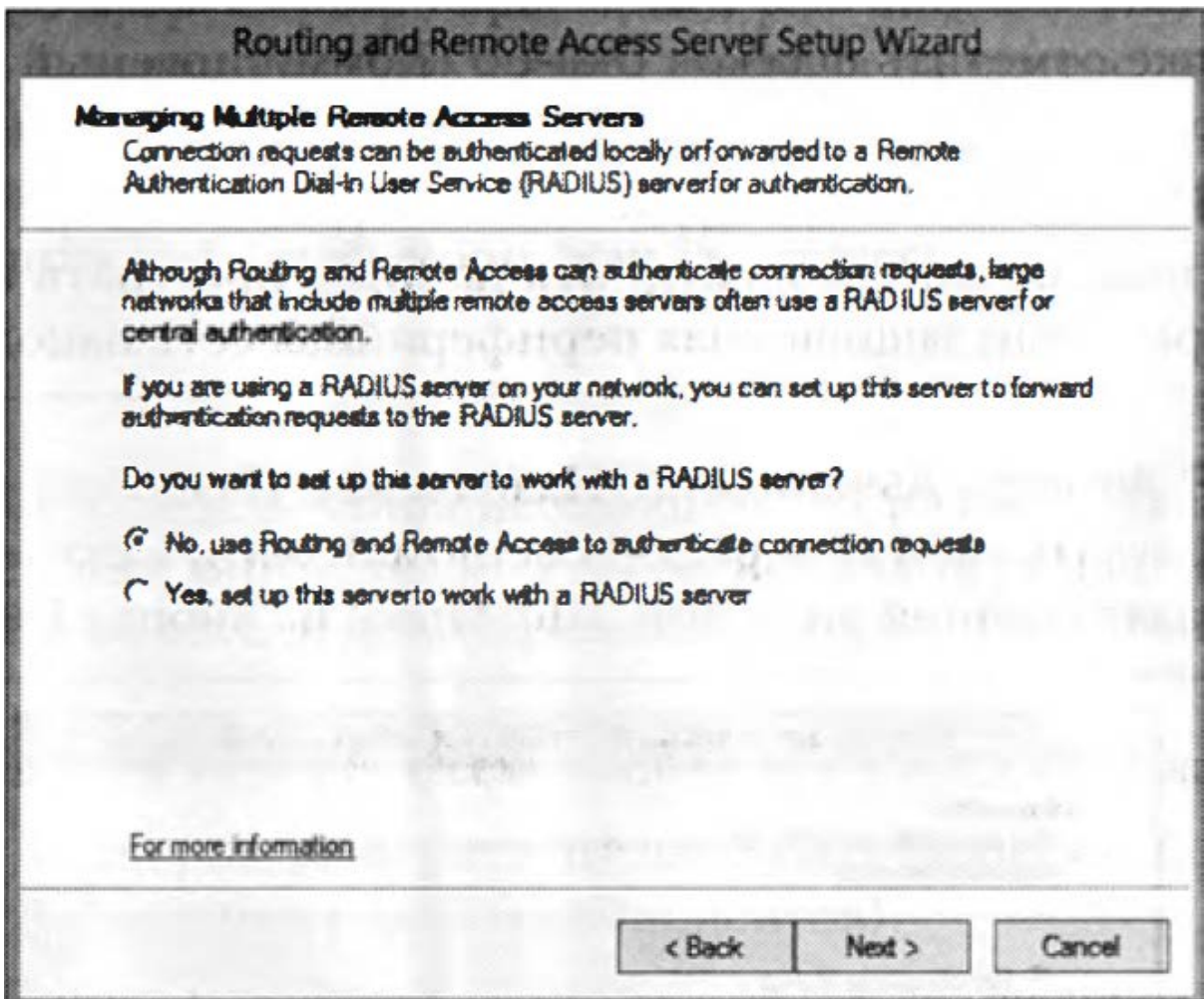


სურ. 6.1. VPN შესაძლებლობების აქტივაცია



სურ. 6.2. ქსელური ბარათის მითითება VPN კლიენტებისათვის

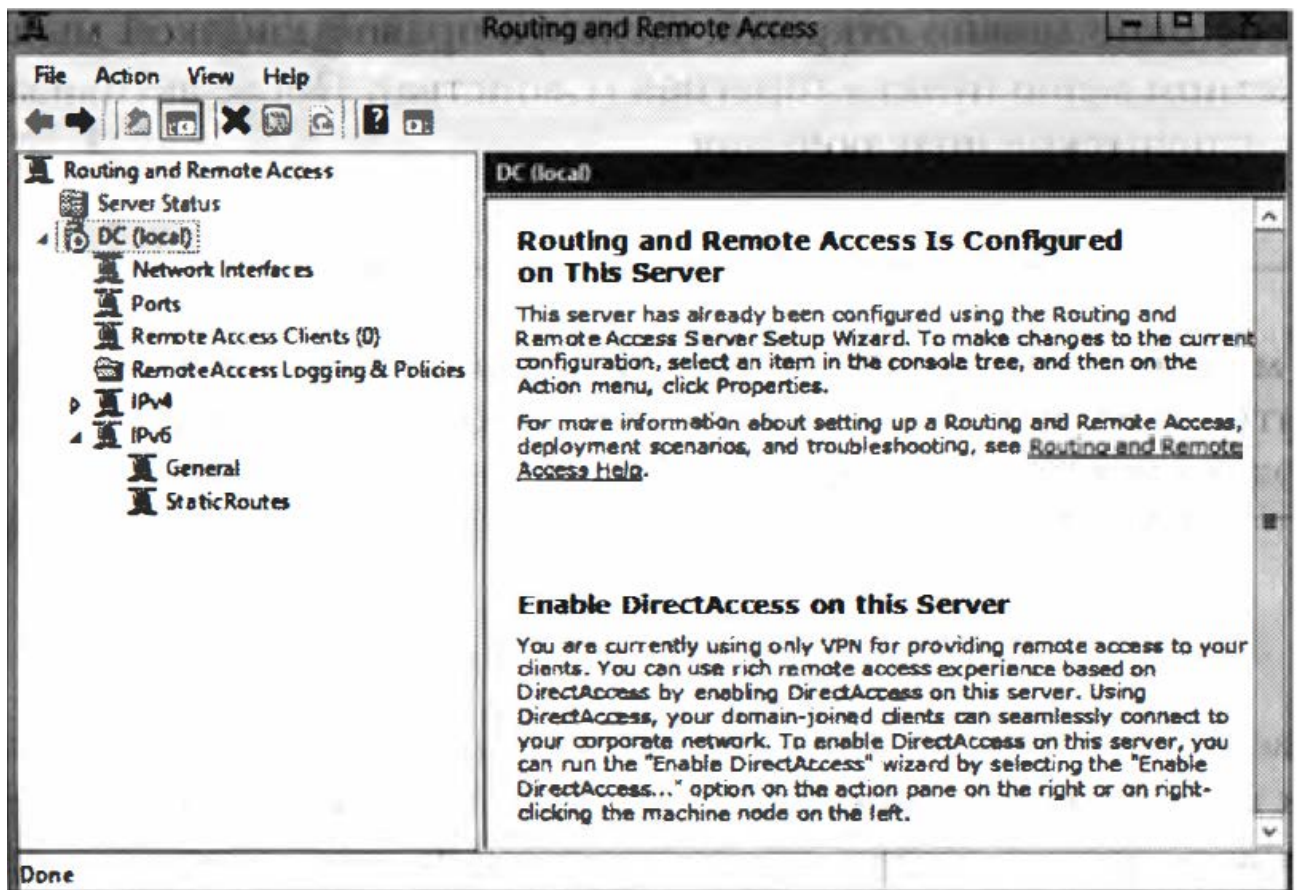
- **Managing Multiple Remote Access Servers** გვერდზე (სურ. 6.3) მიუთითეთ საჭიროა თუ არა ლოკალური აუთენტიფიკაცია **RRAS** დახმარებით ან დაშორებული **RADIUS** სერვერის გამოყენება. დააჭირეთ **Next** ღილაკს.



სურ. 6.3. RADIUS პარამეტრების მითითება VPN სერვერისთვის

- გადახედეთ ოსტატის (Wizard) პარამეტრებს და დააჭირეთ **Finish** ღილაკს.
- სტანდარტული პოლიტიკის შექმნის შესახებ გამოსული შეტყობინების დროს, შეერთების მოთხოვნისთვის დააჭირეთ **OK** ღილაკს. თუ გამოვიდა შეტყობინება **DHCP** რეტრანსლაციის აგენტის შესახებ, ასევე დააწეეთ **OK** ღილაკს.
- ოსტატის მუშაობის დასრულების შემდეგ, დააჭირეთ **Finish** ღილაკს.

ოსტატი გააქტიურებს **RRAS**-ს სერვერზე და დაუშვებს პარამეტრებისა და **VPN** კლიენტების ადმინისტრირებას **Routing and Remote Access** დიალოგური ფანჯრიდან (სურ. 6.4). გახსენით ეს ფანჯარა და დათვალიერეთ პარამეტრები, რათა გაეცნოთ სისტემის კონფიგურაციას.



სურ. 6.4. სერვერის ადმინისტრირება RRAS კონსოლის დახმარებით

6.2. ინტერნეტის კონტროლის და უსაფრთხოების სისტემების (Proxy, Firewall) ინსტალაცია

ფაიერვოლის ძირითადი დავალებაა პაკეტების ფილტრაცია. ის ამოწმებს ყველა პაკეტის თავსართს, რომლებიც გადაიცემა კომპიუტერის ქსელურ ინტერფეისებზე და ამ პაკეტებზე ასრულებს იმ მოქმედებებს, რომლებიც შეესაბამება ფაიერვოლში მომართულ წესებს.

ფაიერვოლი შეიძლება გამოყენებულ იქნას როგორც ერთი კომპიუტერის დასაცავად (მაგალითად ინტერნეტში ჩართული პერსონალური კომპიუტერი), ასევე მთლიანი ქსელის დასაცავად. ქსელის შემთხვევაში ფაიერვოლი ყენდება **Gateway** („კარიბჭე“) - კომპიუტერზე, რომელიც უზრუნველყოფს ქსელის დანარჩენი კომპიუტერების ინტერნეტში წვდომას. მოცემულ თავში ჩვენ არ განვიხილავთ ქსელურ ფაიერვოლს, არამედ განვიხილავთ იქნება **Windows Server 2012** ოპერაციულ სისტემაში ჩაშენებული ფაიერვოლი.

ლოკალური ფაიერვოლის მთავარი ფუნქციებია:

- კომპიუტერის დაცვა ყველა შესაძლო შეტევისაგან;
- კომპიუტერის დაცვა ქსელური „ჭიებისაგან“ (**Worm**);
- ზიანისმომტანი პროგრამების და არასასურველი ტრაფიკის დაბლოკვა.

დაწვრილებით განვიხილოთ ფაიერვოლის მუშაობის პრინციპი. როგორც ვიცით ქსელში მონაცემები გადაიცემიან არა მთლიანად, არამედ პატარა ნაწილებად - პაკეტებად. წარმოიდგინეთ ინფორმაცია ერთიანად რომ გადაიცემოდეს ქსელში - სანამ ქსელის ერთი წევრი იწერს ფილმს, ქსელის ყველა დანარჩენი კლიენტი ელოდება გადმოწერის დასრულებას. ამიტომ გადასაცემი მონაცემები იყოფა პაკეტებად და თითოეული პაკეტი ცალკე გადაიცემა. პაკეტი შედგება ორი ნაწილისაგან - თავსართი (**Header**) და ტანი (**Body** - მონაცემთა სივრცე). თავსართი შეიცავს ისეთ ინფორმაციას როგორცაა: გამგზავნის მისამართი, მიმღების მისამართი, გამგზავნის და მიმღების პორტი, გადასაცემი მონაცემების ზომა და ა.შ. პაკეტის ტანი შეიცავს თვითონ მონაცემებს, მაგალითად, გადასაცემი ფაილის ნაწილი, ელექტრონული ფოსტა, ხმოვანი შეტყობინება და სხვა.

ფაიერვოლი აანალიზებს ყველა პაკეტის თავსართს, რომლებიც გადიან ქსელური ინტერფეისის საშუალებით. თავსართის თითოეული ველი (გამგზავნის IP-მისამართი, მიმღების IP-მისამართი და ა.შ.) ემორჩილება ფაიერვოლის წესების ნაკრებს. წესების ნაკრები (**Rules**) იქმნება სისტემური ადმინისტრატორის მიერ. ნაგულისხმევად, ფაიერვოლს უკვე აქვს წესების ნაკრები, რომელიც აუცილებლობის შემთხვევაში შეგვიძლია შევცვალოთ. ყოველი წესი იძლევა პაკეტების და მოქმედებების შერჩევის კრიტერიუმებს, რომელიც უნდა შესრულდეს პაკეტზე. მაგალითად, გვინდა ავკრძალოთ ყველა შემომავალი კავშირი: ჩვენი კომპიუტერი არ არის სერვერი, ამიტომ ინტერნეტის მომხმარებლებს არა აქვთ მასთან კავშირი; შეგვიძლია ავკრძალოთ რაიმე პროგრამის ინტერნეტთან წვდომა. ასევე შესაძლებელია კონკრეტულ კვანძთან წვდომის აკრძალვა (მაგალითად, მათთან, რომელთაც თვლით საზიანოდ - რათა მასთან წვდომის საშუალება არ ჰქონდეს ჩვენი კომპიუტერის სხვა მომხმარებლებს); შესაძლებლობა გვაქვს ავკრძალოთ განსაზღვრული პორტი, რათა დავხუროთ ქსელის რომელიმე სერვისი, მაგალითად, **5190** ნომრის მქონე პორტის დაბლოკვით, ჩვენ ვკრძალავთ **ICQ** პროგრამასთან მუშაობას.

როგორც უკვე აღვნიშნეთ, ფაიერვოლები აუცილებლად ყენდება **Gateway-**კომპიუტერებზე, რომლებიც უზრუნველყოფენ სხვა კომპიუტერების ინტერნეტთან წვდომას. ასეთი ფაიერვოლები ძირითადად ასრულებენ მარშრუტიზაციის ფუნქციას, ე.ი. პროვაიდერის ქსელიდან პაკეტების გადამისამართებას ინტერნეტის სხვა მარშრუტიზატორებზე. რა თქმა უნდა მათზე ასევე სრულდება პაკეტების ფილტრაცია, იმგვარად რომ პროვაიდერის ქსელის რესურსების გამოყენება შეუძლიათ მხოლოდ მის კლიენტებს და სხვას არავის. მაგრამ ასეთ ფაიერვოლებს არ შეუძლიათ ლოკალური კომპიუტერების დაცვა ქსელური ჭიებისაგან (**Worm**) ან მომხმარებლის კომპიუტერზე რაიმე პროგრამის ინტერნეტთან წვდომის აკრძალვა. ამიტომ კომპიუტერზე პერსონალური ფაიერვოლის გარეშე მუშაობა უბრალოდ არ შეიძლება.

ღირს თუ არა **Windows**-ის პერსონალური ფაიერვოლის გამორთვა და სხვა ფაიერვოლის დაყენება? **Windows XP**-ის ფაიერვოლი არის „საცერის“ მსგავსი ერთი საათი გატარებული ინტერნეტში ანტივირუსის და დამატებითი ფაიერვოლის გარეშე - და ვირუსი უკვე თქვენს კომპიუტერზეა. **Windows 7, 8.1** ფაიერვოლი წარმატებით ართმევს თავს დაკისრებულ მოვალეობებს. ინტერნეტში ოთხთვიანი მუშაობის შემდეგ,

დამატებითი ფაიერვოლისა და ანტივირუსის გარეშე, გადავწყვიტე შემემოწმებინა კომპიუტერი **DrWeb**-ის უტილიტა **CureIt**-ით და შედეგად კომპიუტერში ქსელური ვირუსები არ აღმოჩნდა. **Windows** ოპერაციული სისტემის ფაიერვოლი პარამეტრების მოხერხებული კონფიგურაციით, არ ჩამოუვარდება ფასიან ფაიერვოლებს. სურვილის შემთხვევაში შეგიძლიათ დახარჯოთ დამატებითი რესურსი სხვა ფაიერვოლის შეძენაზე. ყველაზე კარგი ვარიანტია შეიძინოთ **Total Internet Security** ან **Kaspersky Internet Security**. ეს პროგრამული პაკეტი შეიცავს ფაიერვოლის და ანტივირუსის ფუნქციებს, ორივეს ერთად. ასევე შესაძლებელია გამოიყენოთ **Outpost Security Suite Pro** - შესანიშნავი ფაიერვოლი, რომელიც შეგიძლიათ მიმოიხილოთ მოცემულ მისამართზე: www.agnitum.ru/products.

ფაიერვოლების გამოყენება აუცილებელია თქვენი კომპიუტერისათვის. როგორც კი კომპიუტერი დაკავშირდება საზოგადო ქსელში (**public Network**), ავტომატური პროგრამა-სკანერები იწყებენ მისი ქსელური ინტერფეისის შემოწმებას, რათა იპოვონ დაუცველი ადგილები შემოჭრისთვის. დღესდღეისობით მომხმარებლები ხშირად იყენებენ საზოგადო ქსელს (**public Network**), **WiFi**-ს კაფეში ან აეროპორტში. უფასო **WiFi** ქსელში ჩართვისას, ვერ იქნებით დარწმუნებულნი, რომ ორ მაგიდას იქით მჯდარი კლიენტი არ ცდილობს პორტების სკანირებას, რათა აღმოაჩინოს დაუცველი ადგილები თქვენს კომპიუტერში. ფაიერვოლი აუცილებელია მუდმივად, არამარტო საზოგადო ქსელში (**public Network**) ჩართვისას, არამედ ასევე კორპორაციულთანაც, რადგანაც ყოველთვის არსებობს კომპიუტერში შემოჭრის რისკი.

Windows-ის ფაიერვოლი უზრუნველყოფს კომპიუტერის უსაფრთხოებას, ის იცავს მას ოფისის დაცულ ქსელთან (**Home** ან **Work Network**) ან საზოგადო ქსელთან (**public Network**) კაფეებსა და აეროპორტებში მიერთებისას.

ფაიერვოლები განსაზღვრავენ ქსელურ ტრაფიკს მომართული წესების ერთობლიობის საფუძველზე. ეს წესები ცნობილია როგორც გამონაკლისები (**Exception**). როცა ტრაფიკი ხვდება ფაიერვოლით დაცულ ქსელურ ინტერფეისზე, ფაიერვოლი გაანალიზებს და წესების შესაბამისად გაატარებს ან დაბლოკავს მას. **Windows**-ში არის ორი ფაიერვოლი: **Windows Firewall** და **Windows Firewall** უსაფრთხოების გაძლიერებულ რეჟიმში (**WFAS - Windows Firewall with Advanced Security**). მათ შორის ძირითადი განსხვავება დაკავშირებულია წესების სირთულესთან, რომლებიც მოიმართება თვითონ

მოცემულ ფაიერვოლებში. **Windows Firewall**-ში გამოიყენება მარტივი წესები, რომლებიც პირდაპირ უკავშირდება პროგრამას ან სერვისს. **WFAS**-ში გამოიყენება უფრო რთული წესები, რომლებიც ფილტრავენ ტრაფიკს პორტების, პროტოკოლების და მისამართების საფუძველზე.

ფაიერვოლის პრინციპების შესწავლისას გახსოვდეთ: თუ არ არსებობს წესი, რომელიც კონკრეტული სახის ტრაფიკს გაატარებს, ფაიერვოლი უბრალოდ დაბლოკავს მას. ზოგადად დაშვებულია საჭირო ტრაფიკის ფაიერვოლით გატარება, თუმცა შეიძლება შეიქმნას სიტუაცია, როცა აუცილებელია ამკრძალავი წესების შემოღება. ავტომატურად **Windows Firewall**-სა და **WFAS**-ს აქვთ წესების მინიმალური ნაკრები, რომლებიც ქსელებთან ურთიერთქმედების საშუალებას იძლევა. ეს ნიშნავს, რომ თქვენ შეგიძლიათ ფაიერვოლის მომართვის გარეშე დაათვალიეროთ ქსელი, მაგრამ თუ შეეცდებით გამოიყენოთ დანართი, რომლისთვისაც არ არის მომართული წესები, მაგალითად **FTP**, მიიღებთ გამაფრთხილებელ შეტყობინებას. ეს რეჟიმი განსხვავდება **Windows**-ის წინა ვერსიებისგან მაგალითად **Windows XP**-გან, სადაც ფაიერვოლი ბლოკავდა მხოლოდ შემომავალ ტრაფიკებს და არ ბლოკავდა გამავალს. სტანდარტულად **Windows**-ის ფაიერვოლი ბლოკავს შემოსული ტრაფიკის დიდ ნაწილს. პროგრამის პირველად დაბლოკვისას, ფაიერვოლისაგან მიიღებთ შეტყობინებას (სურ. 8.1), რაც საშუალებას იძლევა დავუშვათ გამონაკლისი, რომელიც შემდგომში გაატარებს მოცემული ტიპის ტრაფიკს:

იმისათვის რომ გავარკვიოთ **Windows** ფაიერვოლის მუშაობის პრინციპი, აუცილებელია გავეცნოთ ქსელთან მუშაობის რამდენიმე ძირითად კონცეფციას:

- პროტოკოლი (**protocol**). **Windows Firewall**-ში საწყისი თვალსაზრისით აუცილებელია სამი პროტოკოლი - **TCP (Transmission Control Protocol)**, **UDP (User Datagram Protocol)** და **ICMP (Internet Control Message Protocol)**. **TCP** პროტოკოლი უფრო საიმედოა. ის გამოიყენება ინტერნეტ-ტრაფიკის დიდი ნაწილისთვის. პროტოკოლი **UDP** გამოიყენება ფართომუწყებლობითი და დიდმისამართიანი მონაცემებისთვის, ასევე ტრაფიკისთვის, რომელიც დაკავშირებულია ონლაინ-თამაშებთან. **ICMP** პროტოკოლი ძირითადად გამოიყენება დიაგნოსტიკისთვის.

- პორტი (**port**) ეს არის საიდენტიფიკაციო ნომერი **TCP** ან **UDP** პაკეტის სათაურში. პორტები გამოიყენება იმისათვის, რომ „დავაკავშიროთ“ ქსელური ტრაფიკი კონკრეტულ

სერვისთან ან პროგრამასთან. მაგალითად, **80** ნომერი პორტი დარეზერვებულია **WWW** ტრაფიკისთვის, ხოლო პორტი **25** - ელექტრონული ფოსტის ინტერნეტით გადასაცემად.

- **IPSec (Internet Protocol Security)**. **IPSec** - არის საშუალება, რომელიც უზრუნველყოფს ქსელური ტრაფიკის უსაფრთხოებას შიფრაციის და ციფრული ხელმოწერის მეშვეობით. შიფრაცია გარანტიას იძლევა, რომ ბოროტმოქმედი ვერ შეძლებს წაიკითხოს გადაცემული ტრაფიკი. ხელმოწერა საშუალებას აძლევს ტრაფიკის ადრესატს, ამოიცნოს გამგზავნი.

- ქსელის მისამართი (**network address**). ქსელის ყველა ჰოსტს აქვს საკუთარი მისამართი. ფაიერვოლში შესაძლებელია მოვმართოთ ტრაფიკის სხვადასხვა დამუშავება, მთელი ქსელის გამავალ ტრაფიკთან დამოკიდებულებით ან გამავალი ქსელის შემომავალ ტრაფიკთან დამოკიდებულებით.

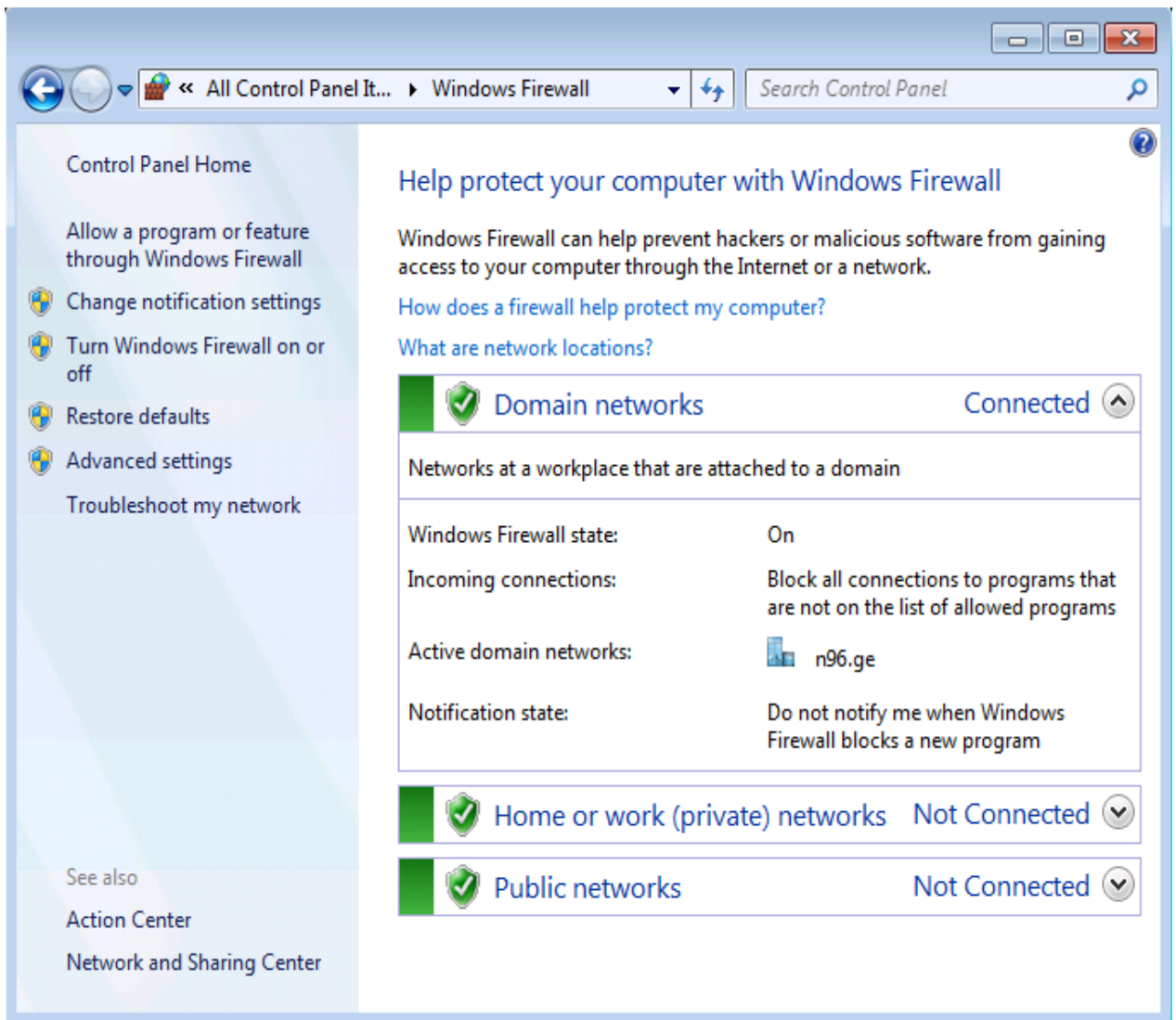
- შემომავალი ტრაფიკი (**inbound traffic**) - ქსელური მონაცემები, რომლებიც გამოდიან გარე ჰოსტიდან და მომართულნი არიან ჩვენს კლიენტ **Windows 7**-ზე.

- გამავალი ტრაფიკი (**outbound traffic**). ტრაფიკი, რომელსაც ჩვენი კლიენტი, **Windows 7**, აგზავნის გარე ჰოსტთან ქსელის საშუალებით.

ქსელური ინტერფეისი (**network interface**). ქსელური ინტერფეისი შეიძლება იყოს ფიზიკურ კავშირში ლოკალური ქსელით, უკაბელო შეერთებით, მოდემის საშუალებით ან ვირტუალური დაცული ქსელის (**VPN**) მეშვეობით.

ქსელის ადგილმდებარეობა

ინფორმაცია ქსელურ ადგილმდებარეობაზე (**Network Location Awareness, NLA**) საშუალებას აძლევს **Windows 7**-ს დანიშნოს ქსელური პროფილი ქსელური შეერთების თვისებების საფუძველზე. როგორც 8.2 სურათზეა ნაჩვენები, **Windows 7** იყენებს სამ ქსელურ პროფილს: დომენურ ქსელს (**Domain Networks**), საშინაო ან სამუშაო (კერძო) ქსელებს (**Home Or Work (Private) Networks**) და საზოგადო ქსელს (**Public Networks**). როცა ვუკავშირდებით ახალ ქსელს, **Windows 7**-ს გამოაქვს დიალოგური ფანჯარა, სადაც უნდა დავაზუსტოთ ქსელის ტიპი - საშინაო, სამუშაო ან საზოგადო. შემდგომში ქსელის ტიპი ასოცირდება მის თვისებებთან რათა ასახულ იქნას კომპიუტერის ამ ქსელში შეერთება მომდევნო ეტაპზე. შესაძლებელია ქსელის ტიპის შეცვლა ქსელის მართვისა და საერთო წვდომის (**Network and Sharing Center**) ფანჯრიდან. დომენური ქსელური პროფილი გამოიყენება **Active Directory Domain Services (AD DS)** დომეინში სამუშაოდ.



სურ. 6.5. Windows Firewall-ის ფანჯარა

ქსელური პროფილები საშუალებას იძლევიან გავრცელდეს ფაიერვოლის სხვადასხვა წესების ერთობლიობა, იმისდა მიხედვით თუ რომელ ქსელშია ჩართული კომპიუტერი. 6.5 სურათზე ნაჩვენებია, რომ **Remote Desktop** უფლება აქტიურია დომენურ (**Domain**) და საშინაო ან სამუშაო (**Home or Work (Private)**) პროფილებში, მაგრამ არაა აქტიური საზოგადო (**Public**) პროფილში.

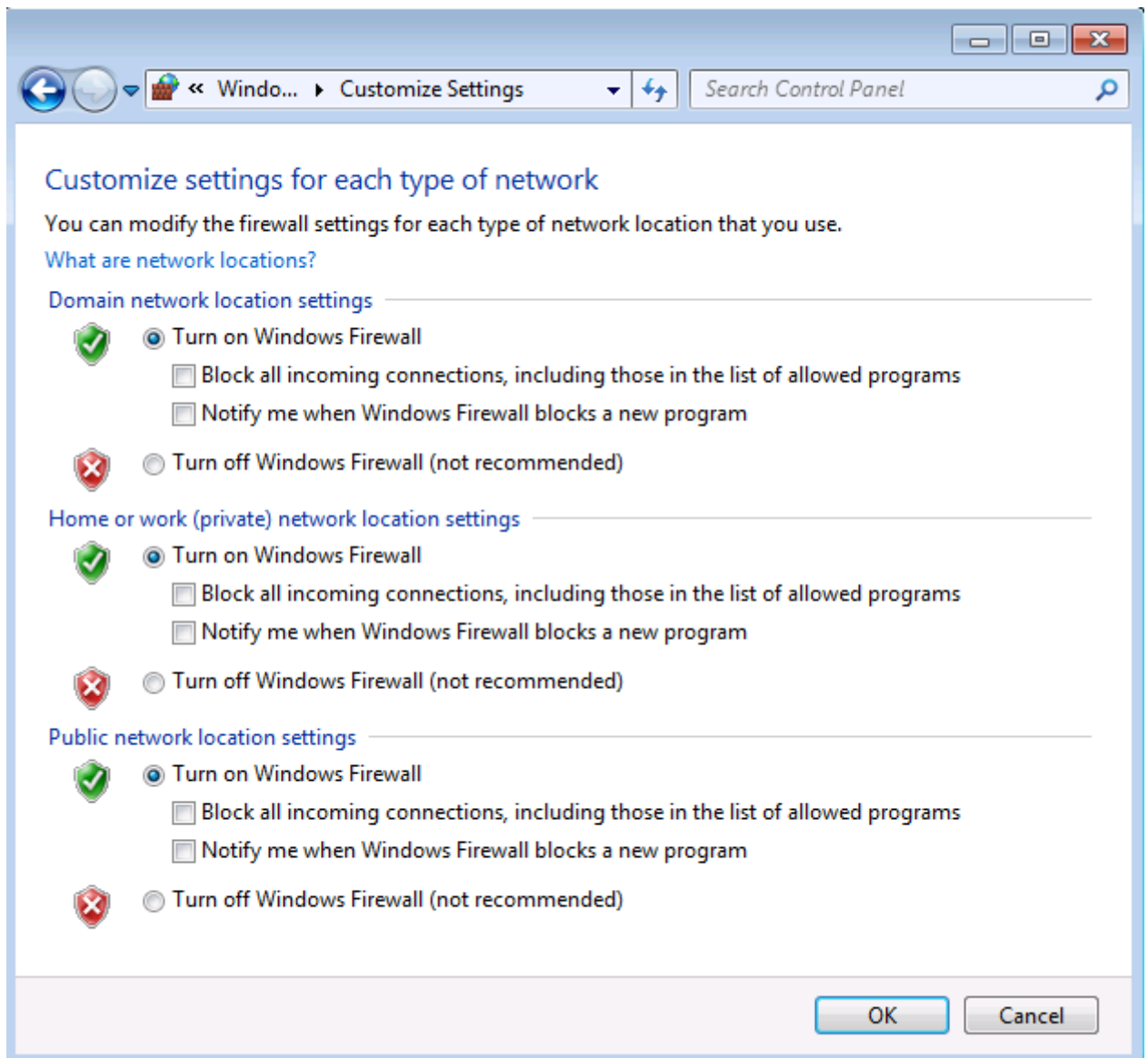
შესაძლებელია შერჩევით გავააქტიუროთ **Windows** ფაიერვოლი თითოეული ქსელური პროფილისათვის, ისე როგორც ნაჩვენებია სურათზე 6.7. ასევე შეგვიძლია თითოეულისთვის მოვმართოთ შემდეგი ორი პარამეტრი:

- **Block all incoming connections, including those in the list of allowed programs** - დაიბლოკოს ყველა შემომავალი კავშირი, იმის გამოკლებით, რომლებიც დაშვებულია ფაიერვოლის წესების ერთობლიობით;

▪ **Notify me when Windows Firewall blocks a new program** - იმ შემთხვევაში თუ ფაიერვოლი დაბლოკავს ახალ პროგრამას, მოხდეს მისი შეტყობინების სახით გამოტანა სამუშაო მაგიდაზე.

მომხმარებლებს შეუძლიათ შექმნან ტრაფიკთან სამუშაო წესები, რომლებზეც ისინი გაფრთხილებულნი იყვნენ ფაიერვოლის მიერ, მხოლოდ იმ შემთხვევაში თუ მათ აქვთ ლოკალური ადმინისტრატორის უფლებები.

როგორც წესი **Windows Firewall**-ი ითიშება ყველა პროფილისათვის იმ შემთხვევაში, თუ თქვენ იყენებთ სხვა მწარმოებლის ფაიერვოლს და გსურთ რომ სწორედ მან დაიცვას თქვენი კომპიუტერი. მნიშვნელოვანია, რომ თქვენ არ გათიშეთ **Windows Firewall**-ი მხოლოდ იმიტომ, რომ ქსელში **Windows 7**-სა და ინტერნეტს შორის არის სხვა ფაიერვოლი, მაგალითად მარშრუტიზატორი ან აპარატურული ფაიერვოლი. სრულიად შესაძლებელია რომ ბოროტმოქმედმა დააინფიცირა ლოკალური ქსელის სხვა კომპიუტერი. უსაფრთხოების თვალსაზრისით ყველა ქსელი უნდა იქნას განხილული როგორც პოტენციურად საშიში.



სურ. 6.7. Windows Firewall-ის შერჩევითი ჩართვა

პროგრამის ინტერნეტთან წვდომის უზრუნველყოფა

არსებობს პროგრამის ინტერნეტთან წვდომის აკრძალვის ან დაშვების ორი ხერხი. პირველი მდგომარეობს იმაში რომ, ვუთითებთ პროგრამის გამშვებ ფაილს და „ვეუბნევით“, რომ ამ პროგრამის ინტერნეტთან წვდომა აკრძალულია ან დაშვებულია. ამ შემთხვევაში ვკრძალავთ ან ვუშვებთ კონკრეტული პროგრამის გამშვები ფაილის წვდომას. დავუშვათ რომ ჩვენ მივეცით ინტერნეტთან წვდომის უფლება **qip.exe** პროგრამას. თუ ვინმე მის გამშვებ ფაილს შეუცვლის სახელს და დაარქმევს **qip1.exe**-ს, ამ შემთხვევაში ასეთი პროგრამის ინტერნეტთან წვდომა იქნება აკრძალული, რამეთუ ფაიერვოლმა არაფერი იცის ამ პროგრამის შესახებ - ის ცნობს მხოლოდ **qip.exe** პროგრამას.

წვდომის აკრძალვა/დაშვების მეორე ხერხი დაფუძნებულია პორტებზე. ამ შემთხვევაში ჩვენ შეგვიძლია დავუშვათ ან აკრძალოთ წვდომა განსაზღვრული კლასის ყველა პროგრამისთვის. მაგალითად, სერვისი **ICQ** იყენებს პორტს **5190**. თუ აკრძალავთ **5190** პორტს, მაშინ ვერცერთი პროგრამა, რომელიც იყენებს ამ პორტს, - იქნება ეს **qip.exe**, **qip1.exe** თუ **icq.exe** - ვერ მიიღებს წვდომას ინტერნეტთან ამ პორტით. მეორე ხერხი უფრო საიმედოა, მაგრამ ამისათვის საჭიროა იმ პორტების ცოდნა, რომლებსაც იყენებს მოცემული პროგრამა. პორტის ნომერი შეგვიძლია დავაზუსტოთ პროგრამის დოკუმენტაციაში ან პროგრამის მწარმოებლის საიტზე. ძირითადი **TCP** პორტები აღწერილია ქვემოთ მოცემულ ცხრილში:

ცხრილი №1

პორტი	სერვისი	რა მოხდება, თუ აკრძალავთ ამ პორტთან წვდომას
21	FTP (File Transfer Protocol)	ვერცერთი FTP კლიენტი ვერ შეძლებს FTP სერვერთან დაკავშირებას. FTP -დან ფაილების გადმოწერა იქნება შეუძლებელი. სასარგებლოა, თუ გსურთ ტრაფიკის ეკონომია - FTP სერვერებზე ინახება უამრავი ტრაფიკი და თუ ჩვენს გარდა კომპიუტერს იყენებს სხვა მომხმარებელიც, მაშინ შესაძლებელია FTP სერვერთან წვდომის აკრძალვა, ზიანის თავიდან ასაცილებლად.
25	SMTP (Simple Mail Transfer Protocol)	მოცემულ პორტთან წვდომის აკრძალვით, ვბლოკავთ ფოსტის გაგზავნას ყველა საფოსტო კლიენტთან.
53	DNS (Domain Name System)	ამ პორტის აკრძალვა არ შეიძლება, რამეთუ სისტემა ვერ შეძლებს დომენური სახელის IP -მისამართებში გარდასახვას, ე.ი. ვერ შევძლებთ ინტერნეტში მუშაობას (ვერ გავხსნით ვებ-გვერდებს, არ მოხდება ელექტრონული ფოსტის გაგზავნა და მიღება და ა.შ.)

80	HTTP (Hyper Transfer Protocol)	ჰიპერტექსტური ინფორმაციის გადაცემის პროტოკოლი. ეს არის WWW-ს ძირითადი პროტოკოლი. ამ პორტთან წვდომის აკრძალვით, ყველა ბრაუზერს ვუკრძალავთ ნებისმიერ საიტზე შესვლას. დანარჩენი სერვისები (ფოსტა, FTP) იმუშავებენ, თუ რა თქმა უნდა ისინიც დაბლოკილი არ გაქვთ.
110	POP (Post Office Protocol)	ეს არის პროტოკოლი რომლითაც ვიღებთ ელექტრონულ ფოსტას. თუ აკრძალავთ ამ პორტის გამოყენებას, ვერ შევძლებთ მოცემული პროტოკოლით ელექტრონული წერილების მიღებას.
443	SSL (Secure Socket Layer)	ამ პორტის აკრძალვის შემდეგ შეგვიძლია დავივიწყოთ უსაფრთხო კავშირი (HTTPS), რომლებიც ყენდება 443 პორტზე
5190	ICQ	მოცემულ პორტს იყენებს შეტყობინებათა სწრაფი გაცვლის პოპულარული კლიენტი ICQ. 5190 პორტის წვდომის შეზღუდვით ვკრძალავთ ინტერნეტ წვდომას ყველა ICQ კლიენტისათვის (ICQ, QIP, Miranda და ა.შ.)
44583	Skype	44583 პორტი გამოიყენება Skype პროგრამის შემომავალი კავშირისთვის. თუ დავბლოკავთ ამ პორტს, Skype აღარ იმუშავებს.

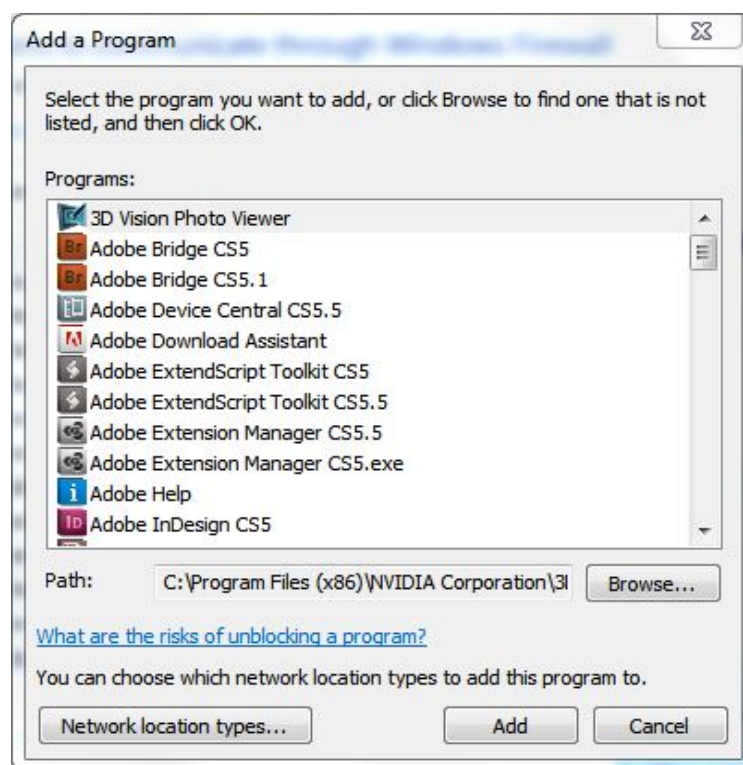
პროგრამების დაშვების უზრუნველყოფა Windows Firewall-ში

Windows Firewall ბრანდმაუერი საშუალებას იძლევა დავუშვათ გამონაკლისები პროგრამებთან მიმართებაში. ამით განსხვავდება იგი Windows Vista-სგან, სადაც ფაიერვოლი საშუალებას იძლეოდა დაეშვა გამონაკლისები პორტის მისამართის მიხედვით.

თქვენ ჯერ კიდევ შეგიძლიათ შექმნათ წესები პორტის მისამართის მიხედვით, WFAS-ის გამოყენებით, რომლის შესახებაც შემდეგში გვექნება საუბარი. ასევე

შეგიძლიათ ფაიერვოლის საშუალებით მუშაობის უფლება დართოთ **Windows 7**-ის კონკრეტულ კომპონენტს, მაგალითად **Windows Virtual PC**. იმისათვის რომ დავამატოთ წესი ნებისმიერი კომპონენტისთვის ან პროგრამებისთვის, დააჭირეთ მაუსის მარცხენა ღილაკი ბრძანებას **Allow A Program Or Feature Through Windows Firewall** (დაშვებულ იქნას პროგრამების და კომპონენტის მუშაობა **Windows Firewall**-ის მეშვეობით), მართვის პანელის **Windows Firewall** განყოფილებაში. დიალოგურ ფანჯარაში (სურ. 8.3) გამოჩნდება დაინსტალირებული პროგრამების და კომპონენტების სია, რომელთათვისაც შექმნილია წესები, ასევე პროფილები, რომელშიც გააქტიურებულია წესი, დაკავშირებული მოცემულ პროგრამებთან და კომპონენტებთან.

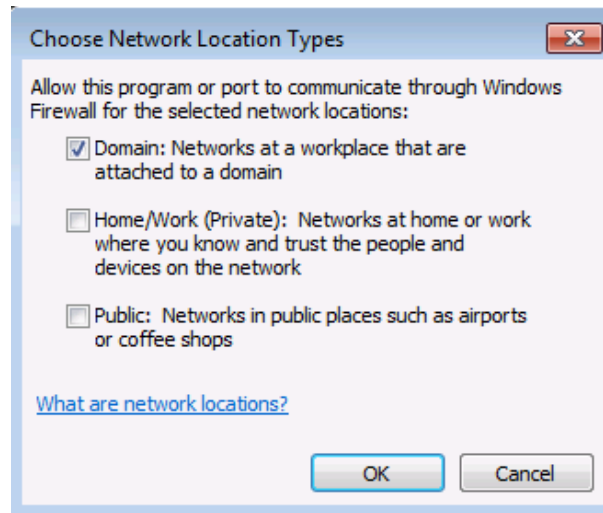
ამ გვერდის პარამეტრების შესაცვლელად დააჭირეთ ღილაკზე **Change Settings**. ფაიერვოლის პარამეტრების ცვლილების უფლება აქვთ მხოლოდ ლოკალური ჯგუფის ადმინისტრატორ წევრებს ან მომხმარებლებს რომლებიც იქნენ დელეგირებულნი შესაბამისი სრულუფლებიანობით.



სურ. 6.8. პროგრამა-გამონაკლისის დამატება

თუ პროგრამა, რომლისთვისაც გვინდა წესის შექმნა, არ არის ამ ჩამონათვალში, დააჭირეთ ღილაკზე **Allow Another Program** (დაშვებულ იქნას სხვა პროგრამა). გაიხსნება დიალოგური ფანჯარა **Add a Program** (სურ. 6.9). თუ ამ სიაშიც არ არის პროგრამა, რომლისთვისაც ვქმნით წესს, დააჭირეთ ღილაკს **Browse**. გამოიყენეთ ღილაკი **Network**

Location Types, რათა მიუთითოთ ქსელური პროფილი, რომლისთვისაც წესი იქნება აქტიური.



სურ. 6.9. ქსელური პროფილის შერჩევა

შენიშვნა: იმისათვის რომ დავაბრუნოთ **Windows Firewall** ან **WFAS** საწყის მდგომარეობაში, **Command Prompt**-ში ჩაწერეთ ბრძანება **netsh advfirewall reset** სისტემური ადმინისტრატორის უფლებით ან მართვის პანელის **Windows Firewall** ფანჯარაში დააჭირეთ მიმართვას **Restore Defaults**.

Windows Server-ის უსაფრთხოება გაძლიერებულ რეჟიმში

Windows Firewall გაძლიერებულ უსაფრთხოების რეჟიმში (**WFAS**) საშუალებას იძლევა შეიქმნას უფრო დეტალიზებული წესი. მომხმარებელთა უმეტესობისთვის კომპიუტერების უსაფრთხოების შესანარჩუნებლად სრულიად საკმარისია პარამეტრები, რომელიც ხელმისაწვდომია ჩვეულებრივი **Windows Firewall**-ით. უფრო რთულის სიტუაციებისთვის გამოიყენება **WFAS (Windows Firewall With Advanced Security)**, რათა:

- მოვმართოთ წესები შემომავალი და გამავალი ტრაფიკისთვის. **Windows Firewall**-ი არ იძლევა საშუალებას შეიქმნას წესი ტრაფიკის ტიპის საფუძველზე;
- მოვმართოთ წესები კონკრეტული პროტოკოლებისთვის ან პორტებისთვის;
- მოვმართოთ წესი იმ ტრაფიკისთვის, რომელიც მიმართულია კონკრეტული სერვისისკენ, და არა კონკრეტული დანართისკენ;
- შევზღუდოთ ტრაფიკის წესის მოქმედების არე განსაზღვრული წყაროსთვის ან განსაზღვრული სამიზნე მისამართისთვის;

- მოვმართოთ წესები, რომლებიც დაუშვებენ მხოლოდ ავტორიზებულ ტრაფიკს.
- მოვმართოთ კავშირის უსაფრთხოების წესები.



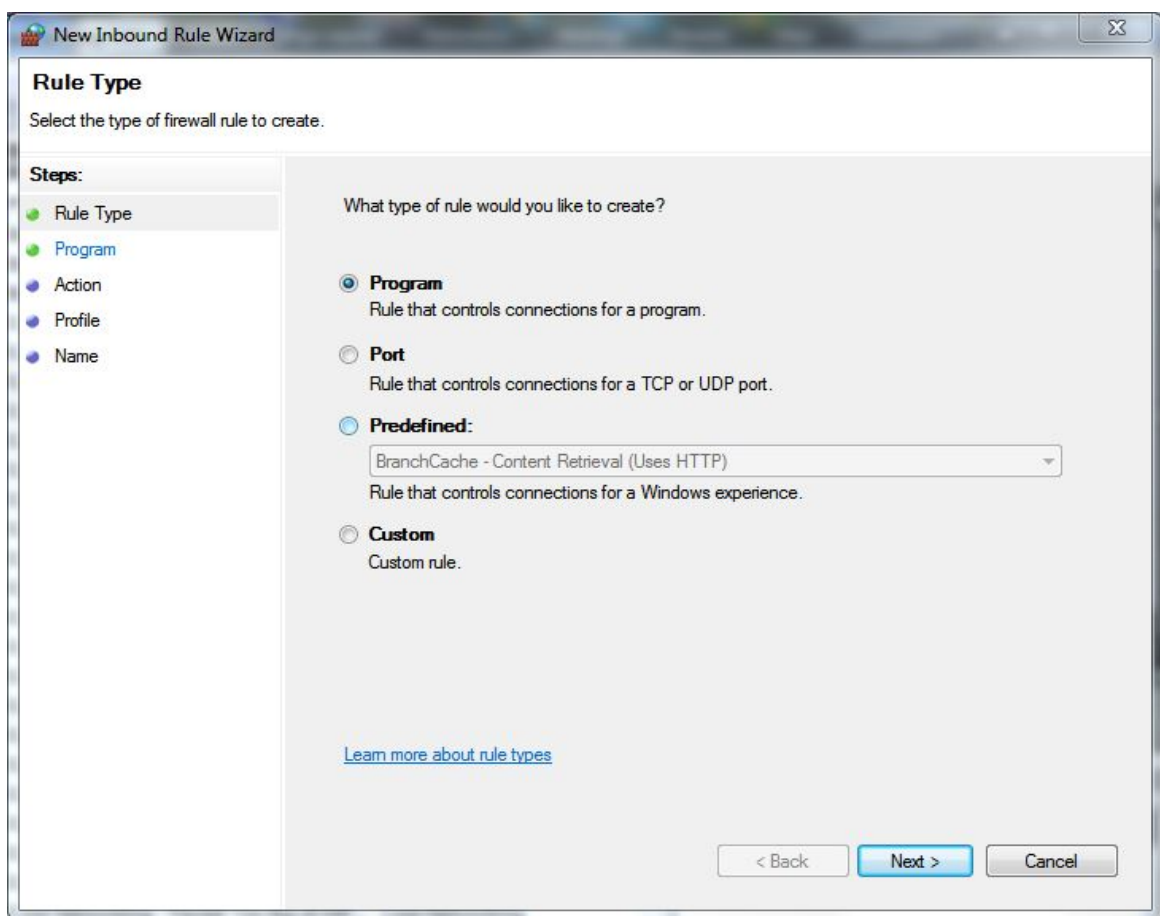
სურ. 6.10. WFAS კონსოლი აქტიურია ორი ქსელური პროფილისთვის

იმისათვის რომ გავხსნათ WFAS კონსოლი, ჩაწერეთ სტარტ მენიუში **Windows Firewall With Advanced Security** ან მართვის პანელის **Windows Firewall** დიალოგურ ფანჯარაში დააჭირეთ მიმართვას **Advanced Settings** (დამატებითი პარამეტრები). WFAS კონსოლში ასახულია ქსელური პროფილები, რომლებიც აქტიურია მოცემულ მომენტში. ისევე როგორც **Windows Firewall**-ის შემთხვევაში, იმისდა მიხედვით როგორი პროფილია აქტიური მოცემულ მომენტში კონკრეტული ქსელური ადაპტერისთვის, მოქმედებს განსხვავებული წესების ნაკრები. მაგალითად 6.10 სურათზე ნაჩვენებია, რომ აქტიურია **Home or Work (Private)** და საზოგადო (**public**) პროფილები. შეგვიძლია გავააქტიუროთ წესი, რომელიც დაუშვებს ტრაფიკს მე-80 პორტიდან დომენური პროფილისთვის, მაგრამ ვერ გავააქტიურებთ მას საზოგადო პროფილისთვის. იგივე დომენში მყოფ ჰოსტებს, რომლებიც დაკავშირებულნი არიან კომპიუტერთან უკაბელო ქსელური ადაპტერით, შეუძლიათ მიიღონ წვდომა მოცემულ კომპიუტერზე განთავსებულ ვებ-სერვერზე, რაც

შეეხება ჰოსტებს, რომლებიც ცდილობენ მიიღონ წვდომა იგივე ვებ-სერვერზე ინტერნეტის საშუალებით, იქნებიან დაბლოკილნი.

WFAS-ისთვის წესის შექმნა

შემომავალი და გამავალი წესების მომართვის პროცესი, ფაქტობრივად, იდენტურია: **WFAS** კონსოლში აირჩიეთ კვანძი, წესის ტიპის შესაბამისად, რომელიც გინდათ რომ შექმნათ და დააჭირეთ ბრძანებას წესის შექმნა (**New Rule**). გაიხსნება წესის შექმნის ოსტატი ახალი შემომავალი (გამავალი) შეერთებისთვის (**New Inbound (or Outbound) Rule**).

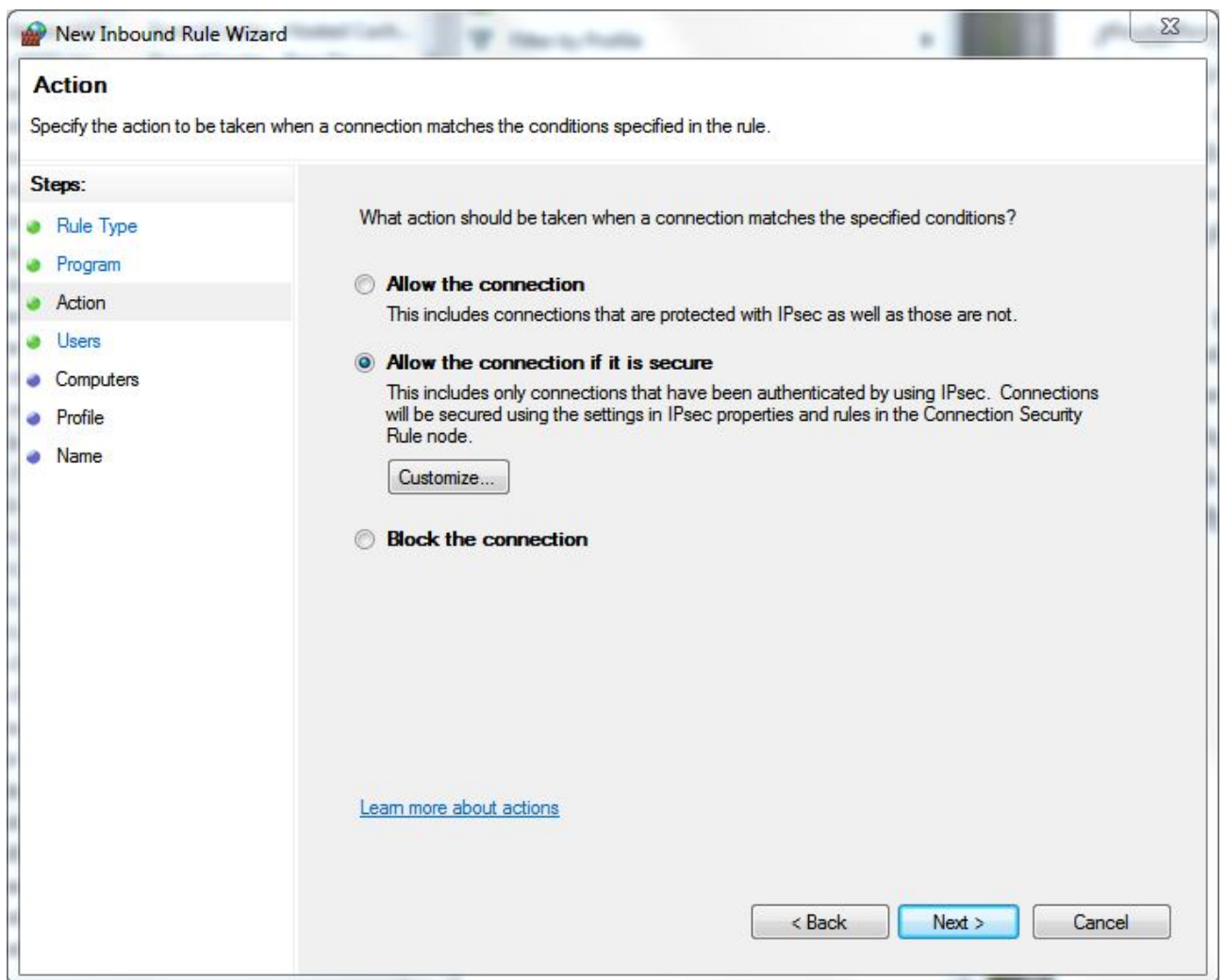


სურ. 6.11. წესის შექმნის ოსტატი ახალი შემომავალი შეერთებისთვის

პირველი გვერდი, რომელიც ნაჩვენებია 6.11 სურათზე, საშუალებას იძლევა დავაზუსტოთ წესის ტიპი, რომელსაც ვქმნით. წესებს შორის შესაძლებელია ავირჩიოთ პროგრამის წესი (**Program**), პორტის წესი (**Port**), წინასწარგანსაზღვრული (**Predefined**) ან მორგებული (**Custom**) წესი. პროგრამების წესები და წინასწარგანსაზღვრული წესები ანალოგიურია, რომლებიც იქმნებიან **Windows Firewall**-ში. მორგებული წესები იქმნება იმ კრიტერიუმების საფუძველზე, რომლებსაც არ შეიცავს სხვა ვარიანტი. ის აუცილებელია

იმ შემთხვევაში, თუ გვჭირდება წესი, რომელიც ვრცელდება კონკრეტულ სერვისზე, და არა პორტზე ან პროგრამაზე. ასევე შეგვიძლია გამოვიყენოთ მორგებული (**Custom**) წესი, თუ გვჭირდება ჩავრთოთ მასში, როგორც კონკრეტული პროგრამა, ასევე პორტების ერთობლიობა. მაგალითად, თუ გსურთ დაუშვათ მონაცემების გაცვლა კონკრეტული პროგრამებისთვის, კონკრეტული პორტით, მაშინ გვჭირდება შექმნათ მორგებული (**Custom**) წესი.

თუ გადაწყვიტეთ შექმნათ წესი პროგრამისთვის, მაშინ აუცილებლად მოგიწევთ იმ პროგრამის მითითება, რომელზეც ვრცელდება წესი. თუ ავირჩევთ პორტის წესს, მაშინ უნდა მივუთითოთ პროტოკოლი (**TCP** ან **UDP**), რომელზეც ვრცელდება წესი, ასევე უნდა დავუზუსტოთ პორტის ნომერი. შემდეგ ეტაპზე ვაზუსტებთ როგორი მოქმედება უნდა ჩატარდეს, როცა ფაიერვოლი დაუპირისპირდება ტრაფიკს, წესების შესაბამისი პირობებით. ხელმისაწვდომია შემდეგი ვარიანტები:

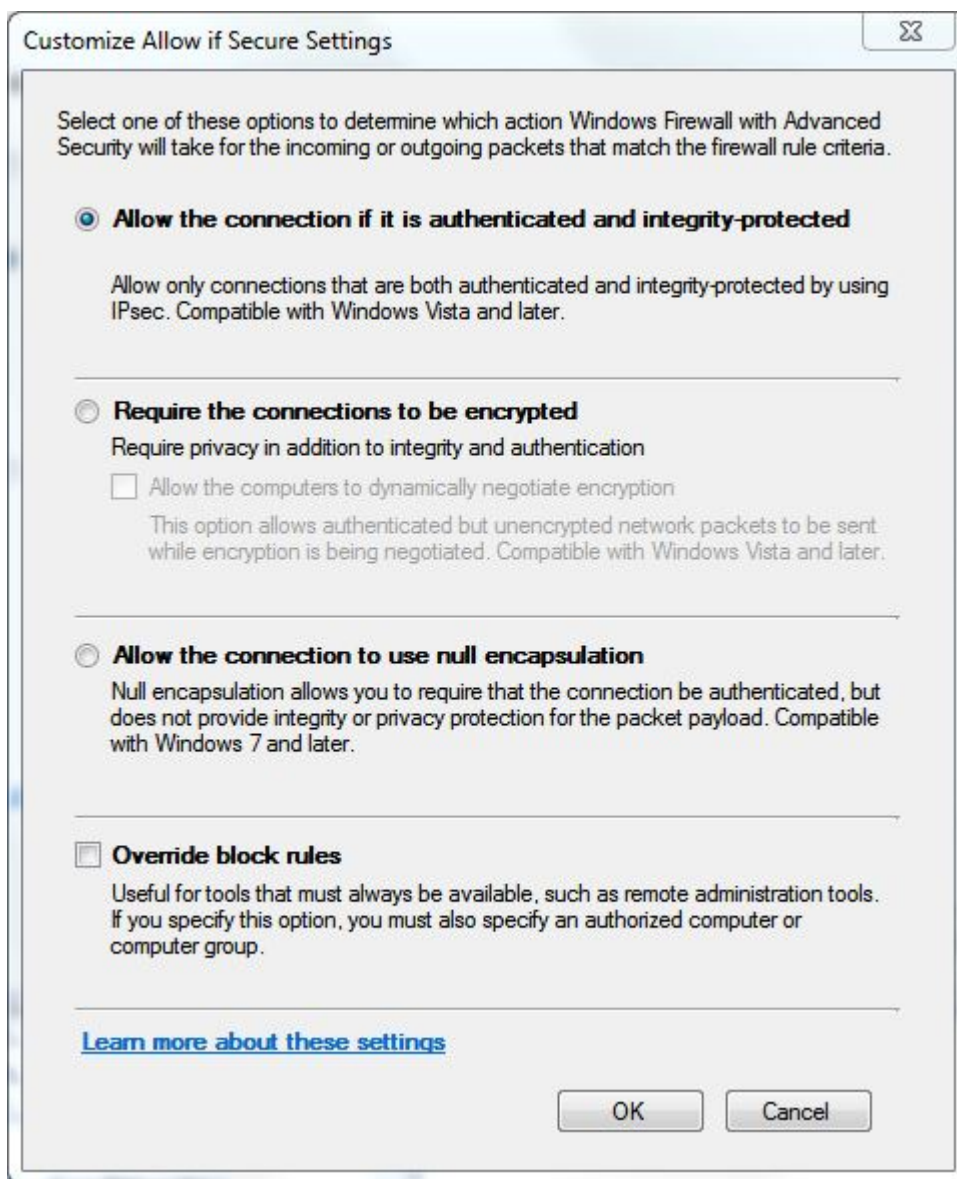


სურ. 6.12

▪ **Allow the connection** (შეერთების დაშვება) - **WFAS** ფაიერვოლი უშვებს შეერთებას, თუ ტრაფიკი შესაბამისობაშია წესების პირობებთან;

▪ **Block the connection** (შეერთების დაბლოკვა) - **WFAS** ფაიერვოლი ბლოკავს შეერთებას, თუ ტრაფიკი შესაბამისობაშია წესების მოთხოვნებთან;

▪ **Allow the connection if it is secure** (დაშვებულ იქნას უსაფრთხო შეერთება) - **WFAS** ფაიერვოლი უშვებს შეერთებას, თუ ტრაფიკი შესაბამისობაშია წესების მოთხოვნებთან და გაიარა ავთენტურობის შემოწმება ერთ-ერთი მეთოდის გამოყენებით, რომელიც მითითებულია შეერთების უსაფრთხოების წესებში. უსაფრთხოების პარამეტრები ნაჩვენებია სურათზე (6.12).



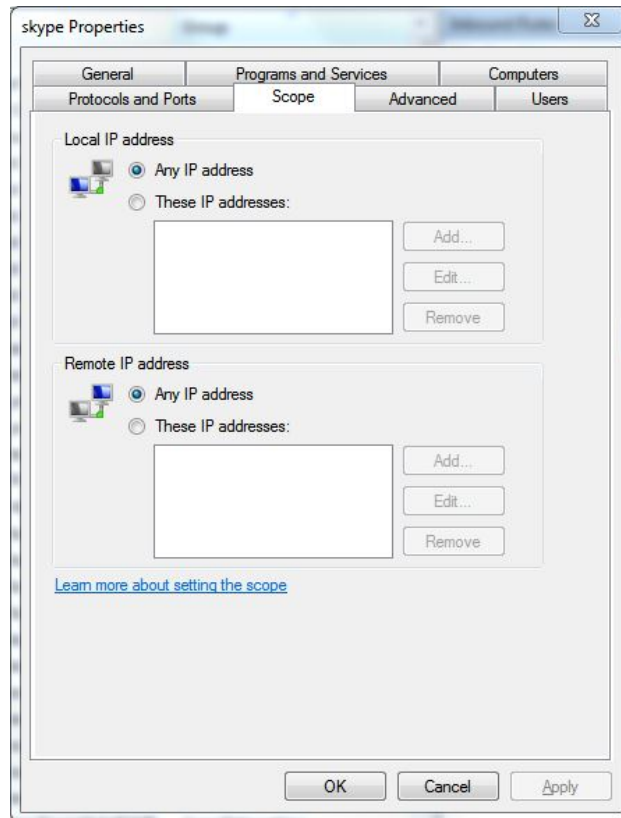
სურ. 6.13. უსაფრთხოების პარამეტრების მომართვა

სტანდარტულად მოთხოვნილია, რომ შეერთებამ გაიაროს შემოწმება ავთენტურობაზე და მთლიანობაზე, რაც შეეხება შიფრაციას, ის არ მოითხოვება. დააყენეთ გადამრთველი **Require The Connection To Be Encrypted** პუნქტზე, თუ გსურთ რომ ფაიერვოლის წესებმა მოითხოვოს არა მხოლოდ ავთენტურობის და მთლიანობის შემოწმება, არამედ მონაცემების შიფრაციაც. დაბლოკვის წესების განსაზღვრა საშუალებას გვაძლევს მივუთითოთ კომპიუტერის სააღრიცხვო ჩანაწერი ან კომპიუტერების ჯგუფი, რომლებსაც შეეძლება გვერდი აუარონ ბლოკირების მოქმედ წესებს.

წესის მოქმედების არე (Rule Scope)

წესის მოქმედების არე (**Rule Scope**) საშუალებას გვაძლევს დავაკონკრეტოთ, ვრცელდება თუ არა წესი კონკრეტულ საწყის და სამიზნე მისამართზე. თუ გსურთ შექმნათ წესი, რომელიც დაუშვებს კონკრეტული ტიპის ტრაფიკს, და შეზღუდოთ იგი კონკრეტული ქსელური მისამართებით, აუცილებელია შეიცვალოს წესების მოქმედების არე. მოქმედების არე შექმნის პროცესში შეიძლება მივუთითოთ მხოლოდ მორგებული (**Custom**) წესისთვის. პროგრამების ან პორტის წესებისთვის სამოქმედო არე მიეთითება შემდეგ, წესის თვისებების რედაქტირების მეშვეობით, როგორც ნაჩვენებია სურათზე 8.11. ჩვენ შეგვიძლია მივუთითოთ **IP**-მისამართი ან **IP**-მისამართების დიაპაზონი, ასევე გამოვიყენოთ ერთი რომელიმე წინასწარგანსაზღვრული იმ კომპიუტერების ერთობლიობიდან, რომლებიც მოიცავენ შლიუზს (**Gateway**), **WINS**-სერვერებს, **DHCP**-სერვერებს, **DNS**-სერვერებს და ლოკალურ ქვექსელს. დიაპაზონებში დაშვებულია როგორც **IPv4**, ასევე **IPv6** მისამართების გამოყენება.

წესის მოქმედების არის შესაცვლელად შევასრულოთ შემდეგი მოქმედებები:

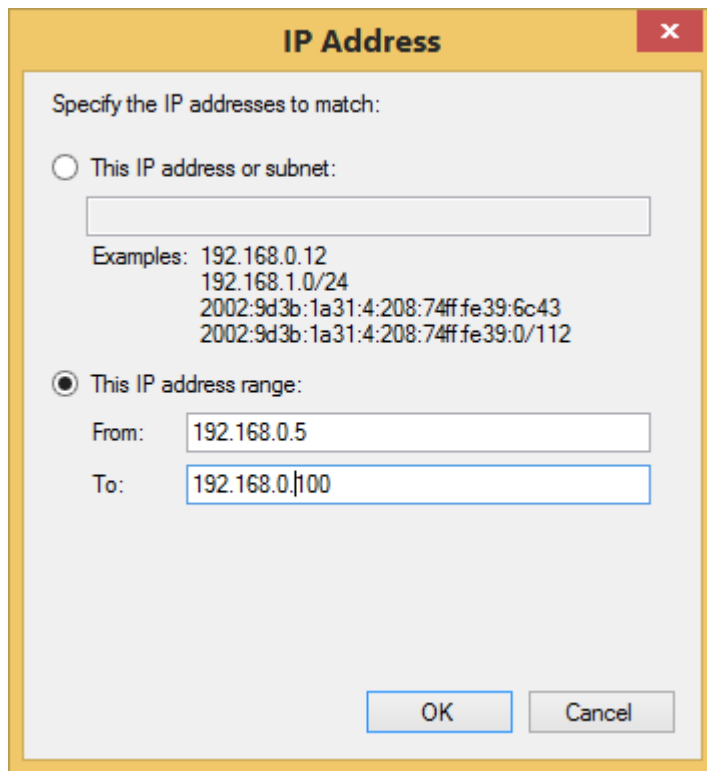


სურ. 6.13

1. **WFAS** კონსოლში მასის მარჯვენა ღილაკით დააჭირეთ წესზე და აირჩიეთ ბრძანება **Properties** (თვისებები). გაიხსნება წესის თვისებების დიალოგური ფანჯარა. გადადით **Scope** ჩანართში;

2. იმისათვის რომ გამოვიყენოთ წესები ლოკალურ **IP** მისამართთან (მაგალითად, იმ შემთხვევაში, როცა ქსელურ ადაპტერს მინიჭებული აქვს რამდენიმე მისამართი ან კომპიუტერზე დაყენებულია რამდენიმე ქსელური ადაპტერი), დააყენეთ გადამრთველი **These IP Addresses** (მითითებული **IP**-მისამართები) **Local IP-Address** განყოფილებაში. დააჭირეთ ღილაკს **Add** (დამატება) და მიუთითეთ, რომელ მისამართსა თუ მისამართებზე ვრცელდება მოცემული წესი;

3. თუ გსურთ შეზღუდოთ წესის მოქმედება დაშორებული **IP** მისამართებისთვის (მაგალითად, წესები უნდა გავრცელდეს მხოლოდ კონკრეტული ქვექსელიდან შემომავალ ტრაფიკებზე), დააყენეთ გადამრთველი **These IP Addresses** (მითითებული **IP**-მისამართები) **Remote IP-Address** განყოფილებაში. დააჭირეთ ღილაკს **Add** (დამატება), რომ მიუთითოთ ცალკეული **IP** მისამართები, ქსელის მისამართი ან **IP** მისამართების დიაპაზონები (სურ.8.12):



სურ. 6.14

წესის თვისებების ფანჯრის **Advanced** ჩანართი საშუალებას იძლევა დავაკონკრეტოთ, რომელ ქსელურ ინტერფეისზე ვრცელდება წესი. ეს პროცედურა ლოკალური IP მისამართების შეზღუდვის ანალოგიურია, რომელშიც ვრცელდება წესი, მაგრამ ამ შემთხვევაში ირჩევა კონკრეტული მოწყობილობა, და არა მისამართი, რომელიც ამ მოწყობილობისთვისაა განკუთვნილი. **Advanced** ჩანართში ასევე მიეთითება, თუ როგორ რეაგირებს წესები იმ ტრაფიკზე, რომელიც გაივლის სასაზღვრო მოწყობილობას, მაგალითად, **NAT** მარშრუტიზატორს. ხელმისაწვდომია შემდეგი ვარიანტები:

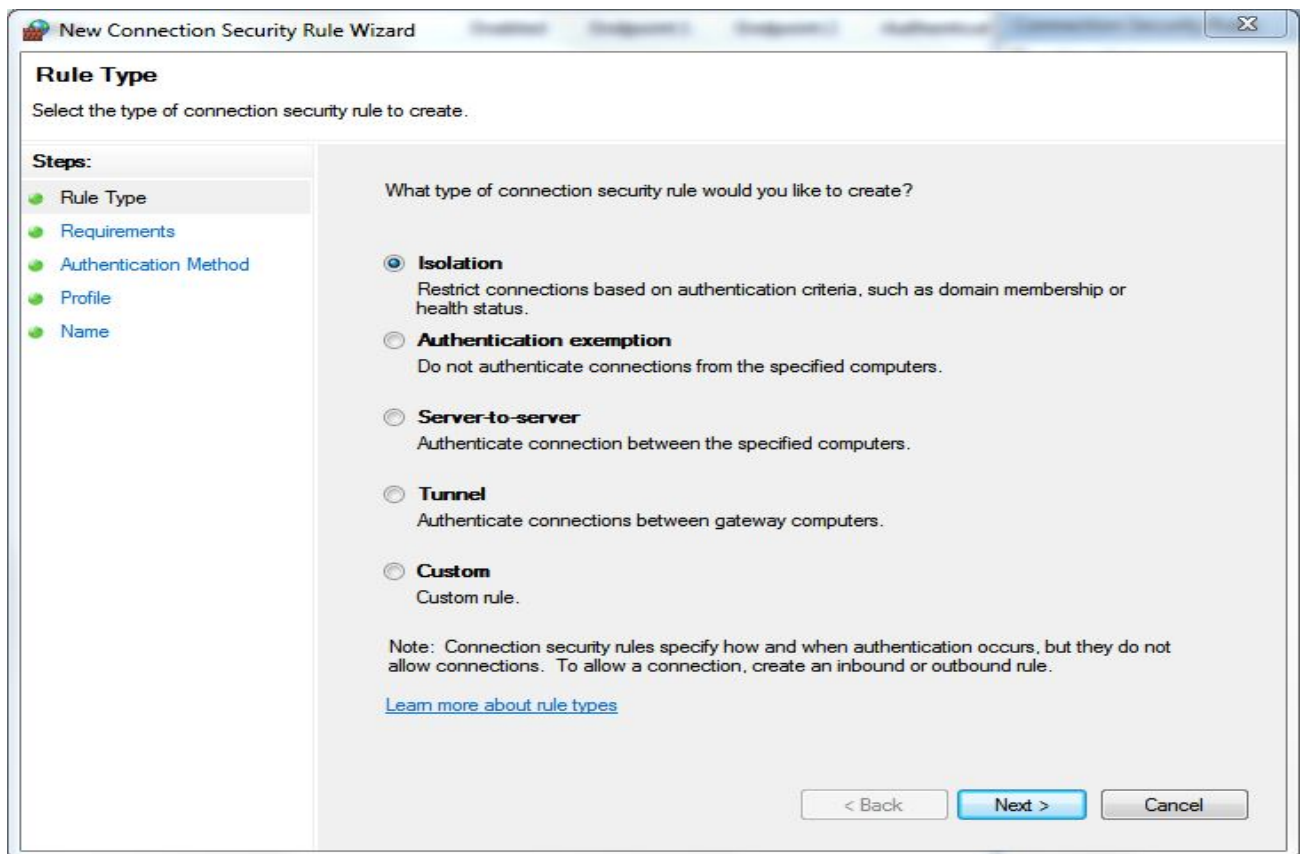
- ბლოკირება კვანძების გვერდის ავლით (**Block edge traversal**) - წესის სამოქმედო ობიექტი იბლოკება ინტერნეტიდან არამოთხოვნილი ტრაფიკი **NAT** მოწყობილობის საშუალებით;
- დაშვება კვანძების გვერდის ავლით (**Allow edge traversal**) - წესის სამოქმედო ობიექტი დაამუშავებს არამოთხოვნილ ტრაფიკს, რომელიც მიღებულია ინტერნეტიდან **NAT** მოწყობილობის საშუალებით;
- მომხმარებლისთვის გადაცემა (**Defer to user**) - მომხმარებელი იღებს შეტყობინებას, რომელიც ატყობინებს **NAT** მოწყობილობიდან ტრაფიკის შემოსვლას. თუ მომხმარებელს

აქვს საკმარისი უფლებამოსილება, მას შეუძლია ხელით დაბლოკოს ან დაუშვას მონაცემთა გაცვლა;

▪ ჩანართებზე გადაცემა (**Defer to application**) - NAT მოწყობილობიდან შემომავალი ტრაფიკის მიღება ან დაბლოკვა განისაზღვრება დანართების პარამეტრებით.

შეერთების უსაფრთხოების წესები

შეერთების უსაფრთხოების წესები (**connection security rules**) - ეს არის წესების განსაკუთრებული ტიპი, რომელიც დაკავშირებულია ტრაფიკის შემოწმების გავლასა და დაშიფრვასთან. შეერთების უსაფრთხოების წესები გამოიყენება კომუნიკაციების სამართავად ქსელის სხვადასხვა ჰოსტებს შორის. მათ შესაქმნელად გამოიყენება წესების შექმნის ოსტატი, ახალი უსაფრთხო შეერთებისათვის (**New Connection Security Rule**), როგორც ნაჩვენებია სურ. 8.13-ზე. შეერთებამ შეიძლება გაიაროს შემოწმება **Kerberos V5** პროტოკოლის დახმარებით, რომელსაც ესაჭიროება წვდომა დომენთან და მომხმარებლის სააღრიცხვო ჩანაწერთან ან კომპიუტერთან რომელიც ზის დომეინში. თუ ავირჩევთ დამატებით პარამეტრებს, შევძლებთ შეერთების ნამდვილობის შემოწმებას **NTMLv2** პროტოკოლის, სერტიფიცირების ცენტრის მიერ გაცემული კომპიუტერის სერტიფიკატების ან წინასწარ არჩეული გასაღების დახმარებით.



სურ. 6.15. შეერთების უსაფრთხოების ახალი წესები

შეერთების უსაფრთხოების სხვადასხვა წესები მუშაობს შემდეგნაირად:

- **იზოლაცია (Isolation)** - იზოლაციის წესები ზღუდავს მხოლოდ ჰოსტების კომუნიკაციას, რომლებმაც გაიარეს შემოწმება ნამდვილობაზე კონკრეტული საადრიცხვო მონაცემების გამოყენებით. მაგალითად, შეგვიძლია გამოვიყენოთ იზოლაციის წესები, იმისათვის რომ გამოვრიცხოთ მონაცემთა გაცვლიდან ის ჰოსტები, რომლებიც არ არიან **Active Directory Domain System (AD DS)**-ს წევრები. იზოლაციის წესებში შეიძლება ჩავრთოთ შემომავალი და გამავალი ტრაფიკების ნამდვილობის შემოწმების მოთხოვნა, მოვითხოვოთ როგორც შემომავალი, ასევე გამავალი შეერთების ნამდვილობის შემოწმება ან მოვითხოვოთ ყველანაირი ტიპის შეერთების ნამდვილობის შემოწმება.

- **ნამდვილობის შემოწმებისაგან განთავისუფლება (Authentication exemption)** - ეს წესები იძლევა იზოლაციის წესებისგან გამონაკლისების დაშვების საშუალებას. ნამდვილობის შემოწმებისგან განთავისუფლების პარამეტრებს მომართავენ იმ შემთხვევაში, მაგალითად, თუ გვინდა დავუშვათ კომპიუტერი დაუკავშირდეს **DHCP** და **DNS** სერვერებს ავტორიზაციის აუცილებლობის გარეშე.

- **სერვერი სერვერთან (Server-to-server)** - ეს წესები იცავენ შეერთებას კონკრეტულ კომპიუტერებს შორის. ისინი განსხვავდებიან იზოლაციის წესებისაგან იმით, რომ ის ვრცელდება არა მთელ შეერთებაზე, არამედ მხოლოდ კონკრეტულ მისამართსა და ჰოსტს შორის შეერთებაზე.

- **გვირაბი (Tunnel)** - ეს წესები **Server-to-server**-ის ანალოგიურია, მაგრამ გამოიყენება დაშორებულ საიტთან „გვირაბული“ შეერთებისას. მაგალითად, საიტიდან საიტზე.

შენიშვნა: ურთიერთობა შეერთების უსაფრთხოების წესებსა და **IPSec** პოლიტიკას შორის ანალოგიურია, **AppLocker**-სა და პროგრამების გამოყენების შეზღუდვის პოლიტიკას შორის ურთიერთობის. წესთა ორივე ნაკრები ასრულებენ ერთი და იგივე ფუნქციას და არჩევანი დამოკიდებულია ოპერაციულ სისტემაზე, რომელსაც იყენებს ჩვენი ორგანიზაციის კლიენტის კომპიუტერი.

6.3. სარეზერვო ასლების ადმინისტრირება

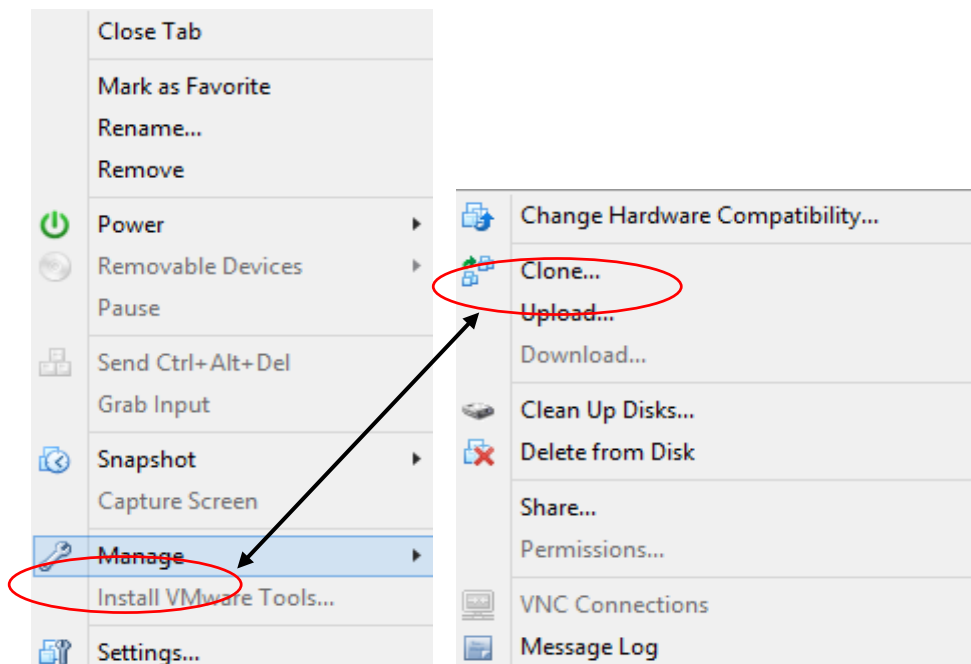
ვირტუალური მანქანის სარეზერვო ასლის შექმნა (Clone)

გარდა ზემოთ აღწერილი ფუნქციებისა, ვირტუალურ მანქანას აქვს ერთი მეტად მნიშვნელოვანი ფუნქცია - მუშაობა კლონებთან (**Clone**). მისი საშუალებით მარტივად და დროის მცირე მონაკვეთში შეგვიძლია ვირტუალური მანქანის სარეზერვო ასლის შექმნა. სარეზერვო ასლში ვირტუალური მანქანის პარამეტრებთან ერთად შევა ოპერაციული სისტემა და მასზე ინსტალირებული ყველა პროგრამა თუ უტილიტა.

ვირტუალური მანქანის, ვირტუალური ოპერაციული სისტემის ან მასში არსებული რაიმე პროგრამული უზრუნველყოფის დაზიანების შემთხვევაში წამებში შეგვიძლია კლონირებული ვირტუალური მანქანის ჩართვა და არ მოგვიწევს სისტემის გამართვა თავიდან, რომელსაც დღეები და შესაძლოა თვეც კი დასჭირდეს. ამ ფუნქციის გამოსაყენებლად უბრალოდ გვჭირდება მეტი მოცულობა მყარ დისკზე.

ვირტუალური მანქანის ასლის შესაქმნელად მივყვით ბრძანებათა თანმიმდევრობას:

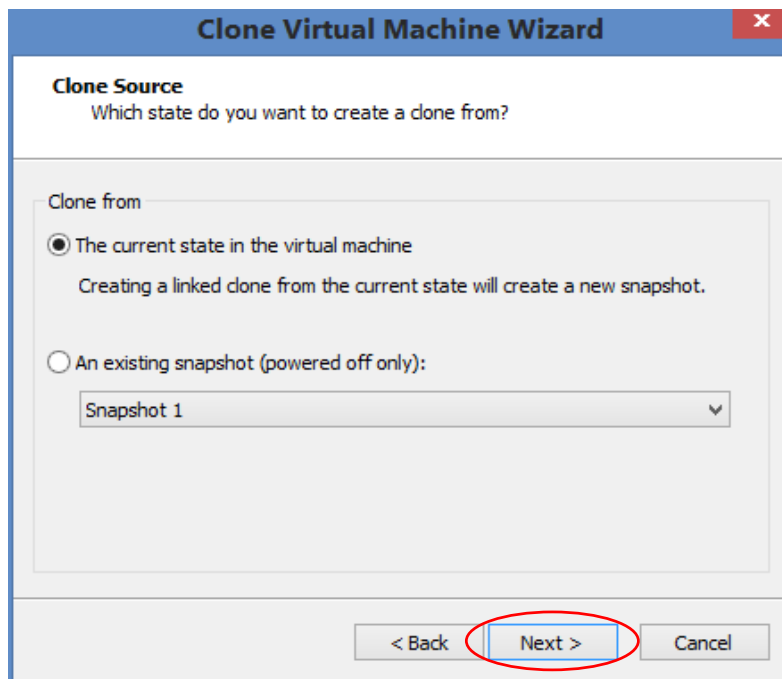
ღეგაბი - **VMware Workstation** პროგრამის მთავარი მენიუს **Library** განყოფილებაში, დავაჭიროთ მაუსის მარჯვენა ღილაკით იმ ოპერაციულ სისტემაზე, რომლის ასლის შექმნაც გვინდა. გამოსულ კონტექსტურ მენიუში ჩამოვშალოთ **Manage** პუნქტი და ავირჩიოთ ბრძანება **Clone** (სურ. 6.3.1:



სურ.6.3.1

II ეტაპი - გამოსულ ფანჯარაში ვაწვებით **Next** ღილაკს;

III ეტაპი - ამ ეტაპზე უნდა დავაკონკრეტოთ ვირტუალური მანქანის, რომელი მდგომარეობის მიხედვით გვინდა ასლის შექმნა, შემოთავაზებული გვაქვს ორი ვარიანტი: ა) **The current state in the virtual machine** - ვირტუალური მანქანის მიმდინარე მდგომარეობის მიხედვით; ბ) **An existing snapshot (powered off only)** - არსებული აღდგენის წერტილის (**Snapshot**) მიხედვით. რადგან ჩვენ გვინდა მიმდინარე მდგომარეობის სარეზერვო ასლი (**Clone**), ვირჩევთ პირველ ვარიანტს და ვაწვებით **Next** ღილაკს (სურ. 6.3.2):



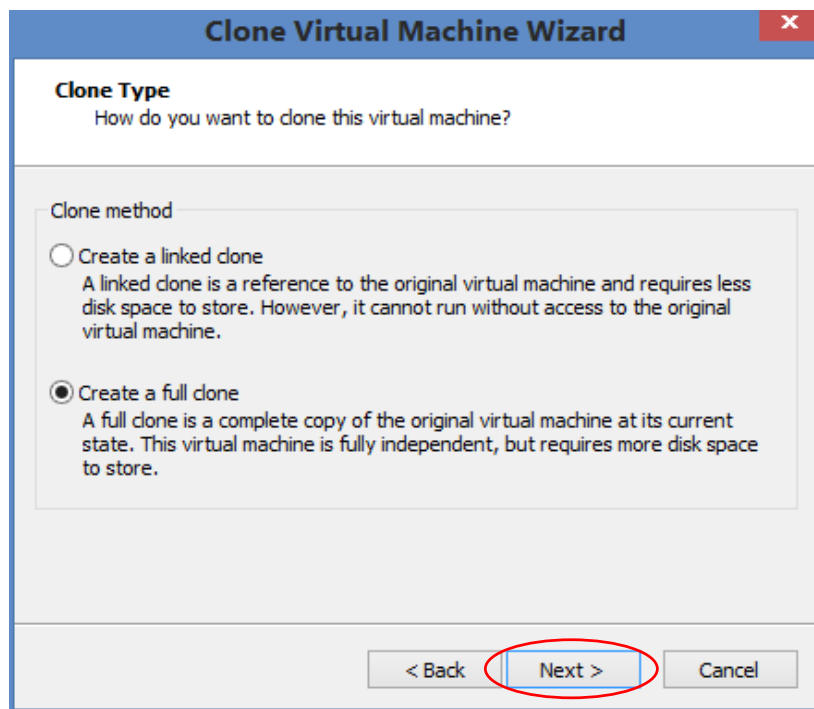
სურ.6.3. 2

IV ეტაპი - ასლის შექმნის მეთოდი (**Clone method**). ამ შემთხვევაშიც გვაქვს ორი ვარიანტი:

ა) **Create a linked clone** (დაკავშირებული კლონის შექმნა) - დაკავშირებული კლონი არის ვირტუალური მანქანის ასლი, რომელიც ანაწილებს მშობელი ვირტუალური მანქანების ვირტუალურ დისკებს ეტაპობრივად, რაც იძლევა მყარ დისკზე მეხსიერების ეკონომიას და საშუალებას აძლევს ვირტუალურ მანქანებს გამოიყენონ პროგრამული უზრუნველყოფის იგივე აპარატურა. დაკავშირებული კლონი შექმნილია მშობელი ვირტუალური მანქანის აღდგენის წერტილიდან (**Snapshot**). ყველა ფაილი, რომელიც ხელმისაწვდომია მშობელ ვირტუალურ მანქანაზე, კადრის (**Snapshot**) შექმნის მომენტში ისევ რჩებიან ხელმისაწვდომნი დაკავშირებული კლონისთვის (**Linked Clone**).

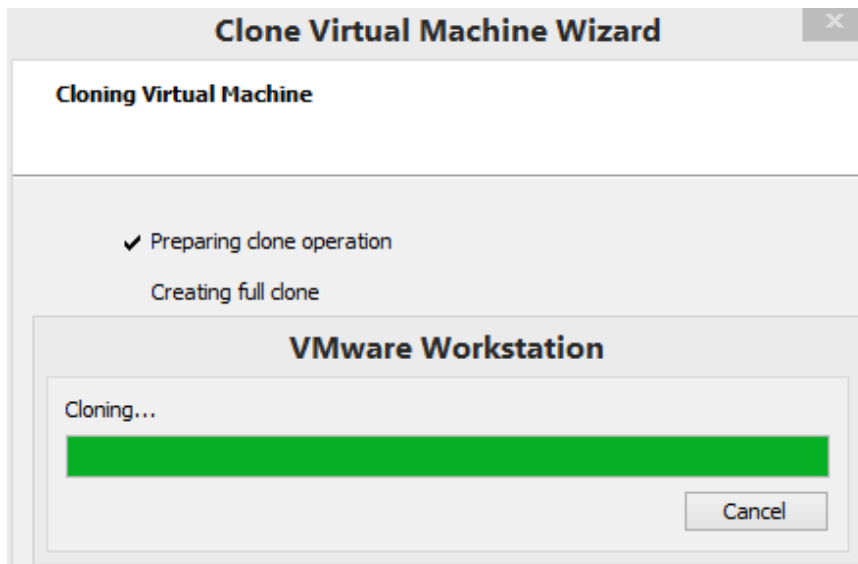
ვირტუალურ დისკზე მიმდინარე ცვლილებები არ ახდენს გავლენას დაკავშირებულ კლონზე და პირიქით, დაკავშირებული კლონის დისკზე ცვლილება გავლენას არ ახდენს მშობელზე.

ბ) **Create a full clone** - სრული კლონი არის ორიგინალი ვირტუალური მანქანის მიმდინარე მდგომარეობის ზუსტი ასლი. ეს ვირტუალური მანქანა არის მთლიანად დამოუკიდებელი, მაგრამ მოითხოვს მეტ სივრცეს მყარ დისკზე.



სურ.6.3. 3

უცვლად - ვარქმევთ სახელს კლონირებულ ვირტუალურ მანქანას და ვუთითებთ მისი განთავსების ადგილს ან ვტოვებთ ორივე პარამეტრს უცვლელად. ვაწვებით **Next** ღილაკს. დაიწყება ასლის შექმნის პროცესი. მისი დასრულების დრო დამოკიდებულია ვირტუალურ მანქანაში არსებული ფაილების ზომაზე.



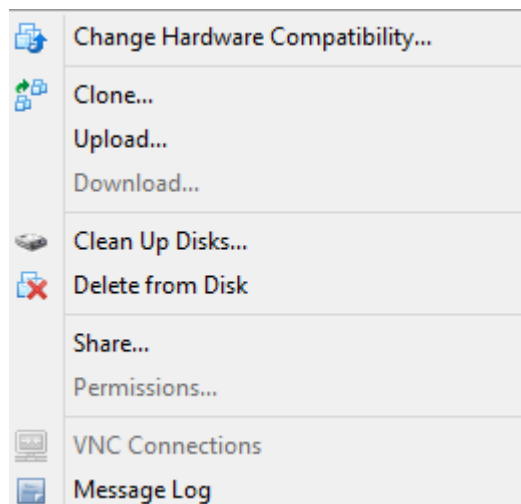
სურ.6.3. 4

პროცესის დასრულების შემდეგ ვაჭერთ **Close** ღილაკს. ამით ვირტუალური მანქანის ასლის შექმნა დამთავრებულია.

ვირტუალური მანქანის წაშლა

იქმნება სიტუაცია, როდესაც უბრალოდ აღარ გვჭირდება შექმნილი ვირტუალური მანქანა ან დაზიანებულია ან კიდევ დიდ ადგილს იკავებს მყარ დისკზე და გვინდა მისი წაშლა ადგილის გამოთავისუფლების მიზნით.

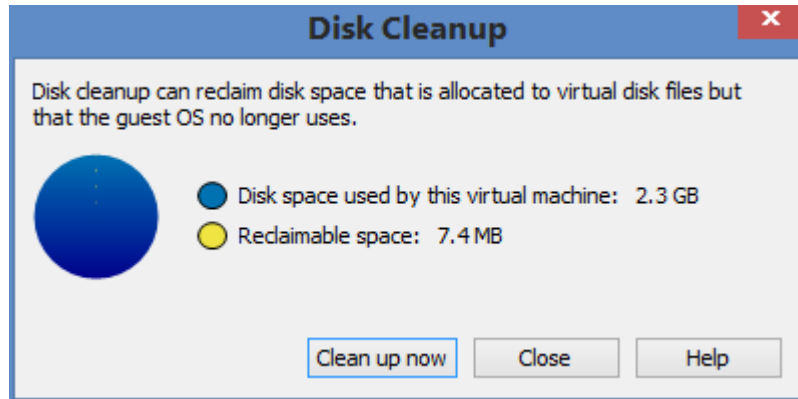
ამისათვის წასაშლელ ვირტუალურ მანქანაზე გამოვიძახოთ კონტექსტური მენიუ და ჩამოვშალოთ **Manage** პუნქტი.



სურ.6.3. 5

გამოვა **Manage** პუნქტის ქვემენიუ (სურ. 6.3.5), საიდანაც ჩვენ გვჭირდება მხოლოდ ორი ბრძანება:

7. **Clean Up Disks...** - მოცემული **Disk Cleanup** ბრძანება მყარი დისკიდან დააბრუნებს იმ სივრცეს, რომელიც გამოყოფილი იყო ვირტუალური დისკის ფაილებისთვის, და რომელსაც სტუმარი ოპერაციული სისტემა აღარ გამოიყენებს. დააჭირეთ **Clean up now** ღილაკს (სურ. 6.3.6) ადგილის გამოსათავისუფლებლად;



სურ.6.3. 6

Delete from Disk - მოცემული ბრძანებით მთლიანად წაიშლება ვირტუალური მანქანა მყარი დისკიდან. გამოთავისუფლდება მყარი დისკის ის მოცულობა, რომელიც თავის დროზე გამოყავით ვირტუალური ოპერაციული

6.3.1 Acronis True Image Home პროგრამის მიმოხილვა

Acronis ეს არის პროგრამების ინტეგრირებული პაკეტი, რომელიც უზრუნველყოფს, კომპიუტერის მთელი ინფორმაციის უსაფრთხოებას. პროგრამა საშუალებას იძლევა შეიქმნას ოპერაციული სისტემის, კონფიგურაციის, სამომხმარებლო პარამეტრების და ყველა არსებული მონაცემების სარეზერვო ასლები, ასევე შესაძლებელია საიმედოდ წაიშალოს ის კონფიდენციალური ინფორმაცია, რომელიც მომხმარებლისთვის უკვე აღარ არის საჭირო. ამ პროგრამული უზრუნველყოფის დახმარებით შესაძლებელია შეიქმნას სარეზერვო ასლები რჩეული ფაილებისა და საქაღალდეების, მაკროსოფტის მომხმარებელთა ელექტრონული ფოსტის პარამეტრებისა და შეტყობინებების, მთლიანი ლოგიკური დისკების და დანაყოფებისა კი. ონლაინ საცავები საშუალებას იძლევა შევინახოთ მნიშვნელოვანი ფაილები დამორებულ საცავებში. მონაცემები დაცულია დაკარგვის, მოპარვის და კომპიუტერის განადგურების შემთხვევაშიც კი. **Acronis**-ის უწყვეტი დაცვა (**Acronis Nonstop Backup**) პერიოდულად (ყოველ 5 წუთში) ინახავს ცვლილებებს, რომელიც მოხდა სისტემაში და ფაილებთან, რაც აუცილებლობის შემთხვევაში საშუალებას იძლევა იოლად დავაბრუნოთ სისტემა დროის ნებისმიერ მომენტში არსებულ მდგომარეობაში.

True Image უზრუნველყოფს ყველა აუცილებელ ინსტრუმენტს კომპიუტერის აღსადგენად მონაცემების დაზიანების, შემთხვევით მნიშვნელოვანი ფაილებისა და საქაღალდეების წაშლის ან მყარი დისკის მწყობრიდან გამოსვლის შემთხვევაში.

კომპანია **Acronis**-ის მიერ შემუშავებული და განხორციელებული უნიკალური ტექნოლოგია საშუალებას იძლევა შეიქმნას ლოგიკური დისკის ზუსტი, სექტორული სარეზერვო ასლები. ასეთი სარეზერვო ასლები მხარს უჭერენ ყველა ოპერაციულ სისტემას, პროგრამებსა და ფაილებს, ასევე პერსონალურ პარამეტრებსა და მონაცემებს.

გარდა ამისა **Acronis**-ი იცავს მომხმარებლის პერსონალურ მონაცემებს. კომპიუტერის ძველი მონაცემების უბრალო წაშლა არ იძლევა გარანტიას, რომ ისინი განადგურდება აღდგენის შესაძლებლობის გარეშე. უტილიტა **Acronis Drive Cleanser**, რომელიც შედის **True Image** შემადგენლობაში სამუდმოდ ანადგურებს ფაილებს და შლის პირად მონაცემებს დანაყოფზე ან მთლიან დისკზე, ხოლო სისტემის გამწმენდი საშუალება შლის მომხმარებლის მიერ კომპიუტერზე **Windows**-ით განხორციელებულ სამუშაოს ყველანაირ კვალს.

გეგმის მიხედვით სარეზერვო ასლის შექმნისას **Acronis** ავტომატურად ირჩევს სარეზერვო ასლის ტიპს (სრული, ინკრემენტული, დიფერენციალური) მომხმარებლის მიერ მომართული სარეზერვო ასლის სქემის შესაბამისად.

სარეზერვო ასლები შეგვიძლია შევინახოთ პერსონალური კომპიუტერის ნებისმიერ შემნახველ მოწყობილობაზე.

ახალი ტექნოლოგია და **Windows**-ის სტილის ინტერფეისი ახალისებს ამ პროგრამასთან მუშაობას. მხოლოდ რამდენიმე უბრალო კითხვაზე პასუხის გაცემა და **True Image** თვითონ იზრუნებს ყველაფერზე, სწრაფად აღადგენს სისტემას.

True Image–ის ძირითადი ცნებები

მოცემული განყოფილება მოიცავს იმ ძირითადი ცნებების მიმოხილვას, რომლებიც გამოიყენება პროგრამის მუშაობისას.

სარეზერვო კოპირება და აღდგენა

სარეზერვო კოპირება (არქივირება) – ეს არის მონაცემთა ასლის შექმნა, დაკარგვის ან დაზიანების შემთხვევაში მათ აღსადგენად.

როგორც წესი, სარეზერვო ასლიდან მონაცემთა აღდგენა ხდება ორ შემთხვევაში: 1)აღდგენა იმ მდგომარეობაში, რომელშიც იმყოფებოდა სისტემა დაზიანებამდე (საავარიო აღდგენა); 2)მცირე რაოდენობის ფაილების აღდგენა მათი შემთხვევით (უნებლიე) წაშლის ან დაზიანების შემთხვევაში.

True Image გვაძლევს ამ ორივე შემთხვევის მოგვარების საშუალებას, ქმნის როგორც დისკებისა და დანაყოფების იმიჯებს, ისე ფაილების სარეზერვო ასლებს.

სარეზერვო ასლების ვერსიები

სარეზერვო ასლების ვერსიები - არის ფაილი ან ფაილები, რომლებიც იქნება სარეზერვო კოპირების ყოველი ოპერაციისას. შექმნილი ვერსიების რაოდენობა ყოველთვის ტოლია სარეზერვო კოპირებისას შესრულებული ოპერაციების რაოდენობისა ან დროში შენახული წერტილების რაოდენობისა (სარეზერვო ასლების გაერთიანების ფუნქციის ამორთვისას).

ამგვარად, ვერსია წარმოადგენს წერტილს დროში, რომლის საშუალებითაც შესაძლებელია სისტემის ან მონაცემების აღდგენა. ერთი სიტყვით, სარეზერვო ასლების ვერსიები წარმოადგენენ სრულ, ინკრემენტულ და დიფერენციალურ სარეზერვო ასლებს.

სარეზერვო ასლების ვერსიები მსგავსია ფაილების ვერსიებისა. ფაილების ვერსიის ცნება ნაცნობია იმ მომხმარებელთათვის, რომლებიც იცნობენ ოპერაციულ სისტემების **Windows Vista**-ს და **Windows 7**-ის ფუნქციას ფაილების წინა ვერსიები (**Previous versions of files**). ეს ფუნქცია საშუალებს იძლევა აღდგეს ფაილი იმ მდგომარეობაში, რომელშიც ის იყო გარკვეული დროის განმავლობაში. სარეზერვო ასლების ვერსია საშუალებას იძლევა აღდგეს მონაცემები მის მსგავსად.

ეს გამოდგება იმ შემთხვევაში, როცა საჭიროა დაზიანებული ან წაშლილი ფაილების მოძებნა. უბრალოდ უნდა დავათვალიეროთ სარეზერვო ასლები **Acronis**-ის სარეზერვო ასლების ბრაუზერში (**Acronis Backup Explorer**), სანამ არ ვიპოვით საჭირო ფაილებიან ვერსიას. გარდა ამისა, შესაძლებელია აღდგეს სხვადასხვა შენახული ვერსიები მოძიებული ფაილებისა.

არსებობს კიდევ ერთი ტიპი ინკრემენტული სარეზერვო ასლების ვერსიების. თუ დანაყოფი ირთვება წაკითხვისა და ჩაწერის რეჟიმში, მაშინ პროგრამა გვთავაზობს, რომ მიერთებული გამოსახულება, სახე, შეიცვლება, და ქმნის ინკრემენტულ ვერსიას ცვლილებების შესანახად. ამ ტიპის ინკრემენტული ვერსიების თვისებები რამდენადმე განსხვავებულია. მაგალითად, არ შეიძლება ასეთი ვერსიების გაერთიანება.

დისკის კლონირება

ამ ოპერაციის დროს სრულდება გადატანა ან კოპირება მთელი დისკისა მეორე დისკზე. მაგალითად, ეს აუცილებელია დიდი მოცულობის მქონე დისკის დაყენებისას. შედეგი კი არის ორი იდენტური დისკი ერთნაირი ფაილური სტრუქტურით. მონაცემთა გადატანა **True Image** –ში ხორციელდება დისკის კლონირების ოსტატის დახმარებით. მთელი ინფორმაცია საწყისი მყარი დისკიდან, ოპერაციული სისტემის ჩათვლით, დაინსტალირებული პროგრამები და მომხმარებლის ფაილები, გადაიტანება მეორე მყარ დისკზე შემდგომი განმეორებითი პროგრამული უზრუნველყოფის დაყენებისა და მომართვის აუცილებლობის გარეშე.

Acronis არ ახდენს კლონირებას მხოლოდ ერთი დანაყოფისა, შესაძლებელია მხოლოდ მთელი დისკის კლონირება.

არსებობს მთელი ინფორმაციის ერთი მყარი დისკიდან მეორეზე გადატანის სხვა საშუალებაც: მყარი დისკის სარეზერვო ასლის შექმნა და მისი აღდგენა ახალი დისკზე.

სარეზერვო ასლის ფაილის ფორმატი

პროგრამა **Acronis**-ის მიერ შექმნილ სარეზერვო ასლებს აქვთ გაფართოება **TIB** და გულისხმობის პრინციპით ხდება მონაცემების შეკუმშვით შენახვა, რის მეშვეობითაც საჭიროა დისკის ნაკლები სივრცე სარეზერვო ასლების შესანახად.

TIB-ფაილის შექმნისას პროგრამა ითვლის მონაცემთა ბლოკების საკონტროლო ჯამის მნიშვნელობებს (**Checksum Values**) და ამატებს ამ მნიშვნელობას შექმნილ სარეზერვო ასლს. საკონტროლო ჯამის მნიშვნელობის დახმარებით შეიძლება მოხდეს მონაცემთა მთლიანობის შემოწმება.

TIB ფორმატის სარეზერვო ასლებიდან მონაცემების აღდგენა შესაძლებელია მხოლოდ **True Image** პროგრამის დახმარებით. მონაცემთა აღდგენა ხდება როგორც **Windows**-ის, ისე აღდგენის გარემოში.

მონაცემთა შენახვა **Acronis**-ში შესაძლებელია ასევე **ZIP** ფორმატით. ეს საშუალებას იძლევა აღდგეს ფაილი სარეზერვო ასლებიდან ნებისმიერ გარემოში პროგრამა **Acronis**-ის გარეშე.

ყველაზე ფართოდ გამოყენებულ ოპერაციულ სისტემებში **Microsoft Windows** და **Mac OS X** არის ჩაშენებული **ZIP** ფორმატის მხარდაჭერა.

Acronis-ის უწყვეტი დაცვისათვის (**Acronis Nonstop Backup**) გამოიყენება მონაცემთა და მეტამონაცემთა სპეციალური ფარული საცავი. სარეზერვო ასლების მონაცემები იკუმშება და იყოფა ფაილებად თითოეული ზომით 1 გბ. ამ ფაილებს ასევე აქვთ ფორმატი **TIB**, ხოლო მათში მოთავსებული მონაცემები შეიძლება აღდგეს მხოლოდ პროგრამა **True Image** -ის დახმარებით.

სარეზერვო ასლის შემოწმება

სარეზერვო ასლების შემოწმების ფუნქცია ადასტურებს, რომ სარეზერვო ასლი არ არის დაზიანებული და შესაძლებელია მონაცემების აღდგენა. სარეზერვო ასლის შექმნისას მას ემატება მონაცემთა ბლოკების საკონტროლო ჯამის მაჩვენებელი (**Checksum Values**). სარეზერვო ასლის მთლიანობა მოწმდება მონაცემთა საკონტროლო ჯამის დათვლით და მიღებული რაოდენობის სარეზერვო ასლის მნიშვნელობასთან

შედარებით. თუ მნიშვნელობები ემთხვევა, ე.ი. სარეზერვო ასლის ფაილები დაზიანებული არ არის და წარმატებით შეიძლება მათი გამოყენება მონაცემთა აღსადგენად.

გაერთიანება

გაერთიანების ოპერაციით შესაძლებელია გამოუსადეგარი სარეზერვო ასლების წაშლა სარეზერვო ასლების ჯაჭვიდან.

გასაერთიანებელ ჯაჭვს შეიძლება წარმოადგენდეს სრული სარეზერვო ასლი და ერთი ან რამდენიმე ინკრემენტული სარეზერვო ასლი.

ჯაჭვიდან სრული სარეზერვო ასლის წაშლისას პროგრამა ქმნის ახალ სრულ სარეზერვო ასლს ყველაზე ძველი დარჩენილი სარეზერვო ასლის მაგივრად. გაერთიანებისას ინახება არჩეული სარეზერვო ასლები და იშლება ნებისმიერი ის სარეზერვო ასლი, რომელიც არ იქნა არჩეული.

გაერთიანების ოპერაციამ შეიძლება მოითხოვოს საკმაოდ დრო და სისტემური რესურსები (დისკის სივრცის ჩათვლით), ამიტომ არ არის რეკომენდებული გაერთიანების გამოყენება ძალიან ხშირად. უმეტეს შემთხვევაში უმჯობესია შეიქმნას ახალი ჯაჭვი სარეზერვო ასლებისა და შემდეგ წაიშალოს ძველი.

Acronis-ის უწყვეტი დაცვის ფუნქციაში გამოიყენება გაერთიანების სხვა მექანიზმი. პროგრამა აერთიანებს იმ მეტამონაცემებს, რომლებსაც ის იყენებს სარეზერვო ასლების მონაცემთა მართვისათვის. რადგან მეტამონაცემთა მოცულობა საკმაოდ ნაკლებია სარეზერვო ასლების მონაცემთა მოცულობაზე, გაერთიანება მოითხოვს საკმაოდ ნაკლებ დროს და სისტემურ რესურსებს.

საავარიო აღდგენა

საავარიო აღდგენისათვის ჩვეულებრივ საჭიროა ჩამტვირთავი მატარებელი და სისტემური დანაყოფის სარეზერვო ასლი.

Acronis აღადგენს სისტემურ მონაცემებს დაზიანების, ვირუსების შეტევის ან მავნე პროგრამებისა და სხვა მიზეზების შედეგად მწყობრიდან გამოსულ სისტემას.

თუ ოპერაციული სისტემა არ იტვირთება, **True Image** აღადგენს სისტემურ დანაყოფს. ჩამტვირთავი კომპაქტ-დისკი, რომლის საშუალებითაც ხდება აღდგენა,

შედის პროდუქტის მიწოდების კომპლექტში. ასევე ჩამტვირთავი მატარებელი (**Rescue media**) შეიძლება შეიქმნას ჩამტვირთავი მატარებლების შემქმნელი ოსტატის (**Media Builder tool**) დახმარებით.

ამოცანის შესრულების დაგეგმვა

სარეზერვო ასლებიდან აღდგენილი მონაცემები უნდა შეიცავდეს აქტუალურ ინფორმაციას, ამიტომ სარეზერვო ასლები რეგულარულად უნდა განახლდეს. სარეზერვო კოპირება უნდა მოხდეს რეგულარულად, მაგალითად დღეში ერთხელ. მიუხედავად იმისა, რომ ხელით სარეზერვო ასლის შექმნა მარტივი პროცესია, შეიძლება შემთხვევით დაგვავიწყდეს მისი შესრულება.

დამგეგმავი (**Sheduler**) დავალებას ასრულებს ავტომატურად მომხმარებლის მონაწილეობის გარეშე, მაგალითად სარეზერვო ასლების რეგულარული, ავტომატური შექმნა. სარეზერვო ასლების შექმნა სრულდება იქამდე, სანამ იქნება საკმარისი სივრცე დისკზე.

სიახლეები True Image –ში

- **Windows 8-ის მხარდაჭერა - True Image** მხარს უჭერს ფირმა მაიკროსოფტის კიდევ ერთ პროდუქტს **Windows 8-ს**. შეგიძლიათ შეიძინოთ და დააყენოთ **Windows 8**, და არ ინერვიულოთ იმაზე, აუცილებლობის შემთხვევაში აღდგება თუ არა სისტემა.

- **სინქრონიზაცია მობილურ მოწყობილობებთან** - ახლა შესაძლებელია მონაცემების სინქრონიზაცია არა მარტო კომპიუტერებს შორის არამედ მობილურ მოწყობილობებთანაც. მხარს უჭერს ისეთ მოწყობილობებს, როგორცაა ტელეფონები და პლანშეტური პერსონალური კომპიუტერები, **iOS** და **Android** პლატფორმაზე. შედით **App Store**-ში ან **Google Play**-ში და დააყენეთ **Acronis**-ის უფასო დანართი, იმისათვის რომ გქონდეთ წვდომა მონაცემებთან ნებისმიერ დროს და ნებისმიერ ადგილას.

- **მარტივი წვდომა ფაილებთან და საქაღალდეებთან - Acronis Cloud** სერვისის მომხმარებლებს შეუძლიათ ფაილების და საქაღალდეების გაცვლა მაუსზე ერთი დაჭერით. ყველაფერი ამისათვის საჭიროა - დავაჭიროთ მაუსის მარჯვენა ღილაკი საჭირო ფაილზე ან საქაღალდეზე და კონტექსტურ მენიუში ავირჩიოთ ბრძანება **Create shared link**. პროგრამა შექმნის საერთოწვდომის ბმულს და განათავსებს მას გაცვლის

ბუფერში. ეს ბმული შესაძლებელია გავუგზავნოთ ნებისმიერ ადამიანს. შეგვიძლია შევქმნათ საერთოწვდომის ბმული ნებისმიერი ფაილისა თუ საქაღალდისთვის, და არა მარტო იმ ფაილებისთვის, რომლებიც ჩართულნი არიან სინქრონიზაციაში ან ონლაინ-საცავის სარეზერვო ასლში.

სისტემური მოთხოვნები და მხარდამჭერი ინფორმაციის მატარებლები

მინიმალური სისტემური მოთხოვნები:

True Image –ის მინიმალური აპარატურული მოთხოვნები შეესაბამება იმ კომპიუტერზე დაყენებულ ოპერაციული სისტემის მოთხოვნებს, რომელზეც გაიშვება იგი. **Acronis** –ის მუშაობისთვის საჭიროა ასევე შემდეგი მოწყობილობები:

- **CD-RW/DVD-RW** - ჩამტვირთავი მოწყობილობების შექმნისათვის;
- მაუსი ან სხვა მისათითებელი მოწყობილობა (რეკომენდებულია).

Acronis–ის უწყვეტი დაცვის სამუშაოდ აუცილებელია მინიმუმ 1 გბ ოპერატიული მეხსიერება.

Acronis–ის აპარატურული მოთხოვნები ჩამტვირთავი მატარებლისადმი:

- 512 მბ ოპერატიული მეხსიერება;
- პროცესორი **Pentium 1** გჰც ან მეტი;
- 1.5 გბ თავისუფალი სივრცე მყარ დისკზე;

ეკრანის რეკომენდებული რეზოლუცია – 1280 x 1024;

ეკრანის მინიმალური რეზოლუცია – 1024 x 768;

მხარდამჭერი ოპერაციული სისტემები

True Image –ს მუშაობის უნარიანობა შემოწმებულია შემდეგ ოპერაციულ სისტემებზე:

- **Windows XP SP3;**
- **Windows XP Professional x64 Edition SP2;**
- **Windows Vista SP2** (ყველა ვერსია);

- **Windows 7** (ყველა ვერსია);
- **Windows 8** (ყველა ვერსია);
- **Windows Home Server 2011**.

Acronis საშუალებას იძლევა შეიქმნას ჩამტვირთავი დისკი **CD-R/DVD-R**, საიდანაც შესაძლებელია სარეზერვო ასლის შექმნა და დისკების ან დანაყოფების აღდგენა ნებისმიერ პროცესორიან – **Intel** ან **AMD** - კომპიუტერზე, რომელიც მუშაობს ნებისმიერი ოპერაციული სისტემის მართვით, მათ შორის **Linux®** (გარდა კომპიუტერებისა **Apple Macintosh Intel**-ის პროცესორით).

ფაილური სისტემები, რომელსაც მხარს უჭერს პროგრამა **Acronis**-ი

- **FAT16/32;**
- **NTFS;**
- **Ext2/Ext3/Ext4***
- **ReiserFS;***
- **Linux SWAP*.**

თუ ფაილურ სისტემას არ აქვს მხარდაჭერა ან დაზიანებულია, მონაცემთა სარეზერვო ასლის შექმნა მოხდება სექტორული რეჟიმით.

* ფაილური სისტემები **Ext2/Ext3/Ext4**, **ReiserFS** ან **Linux SWAP** მხარდაჭერილია მხოლოდ სარეზერვო ასლის შექმნის ოპერაციისთვის და დისკების ან დანაყოფების აღსადგენად. შეუძლებელია **True Image** –ის გამოყენება ფაილების დონეზე ამ ფაილურ სისტემებში (სარეზერვო კოპირება, აღდგენა, ფაილების ძებნა, ასევე იმიჯში ჩამატება და ფაილების აღდგენა ასლიდან). ასევე არ შეიძლება სარეზერვო ასლის შექმნა ამგვარი ფაილურ სისტემებიან დისკებზე ან დანაყოფებზე.

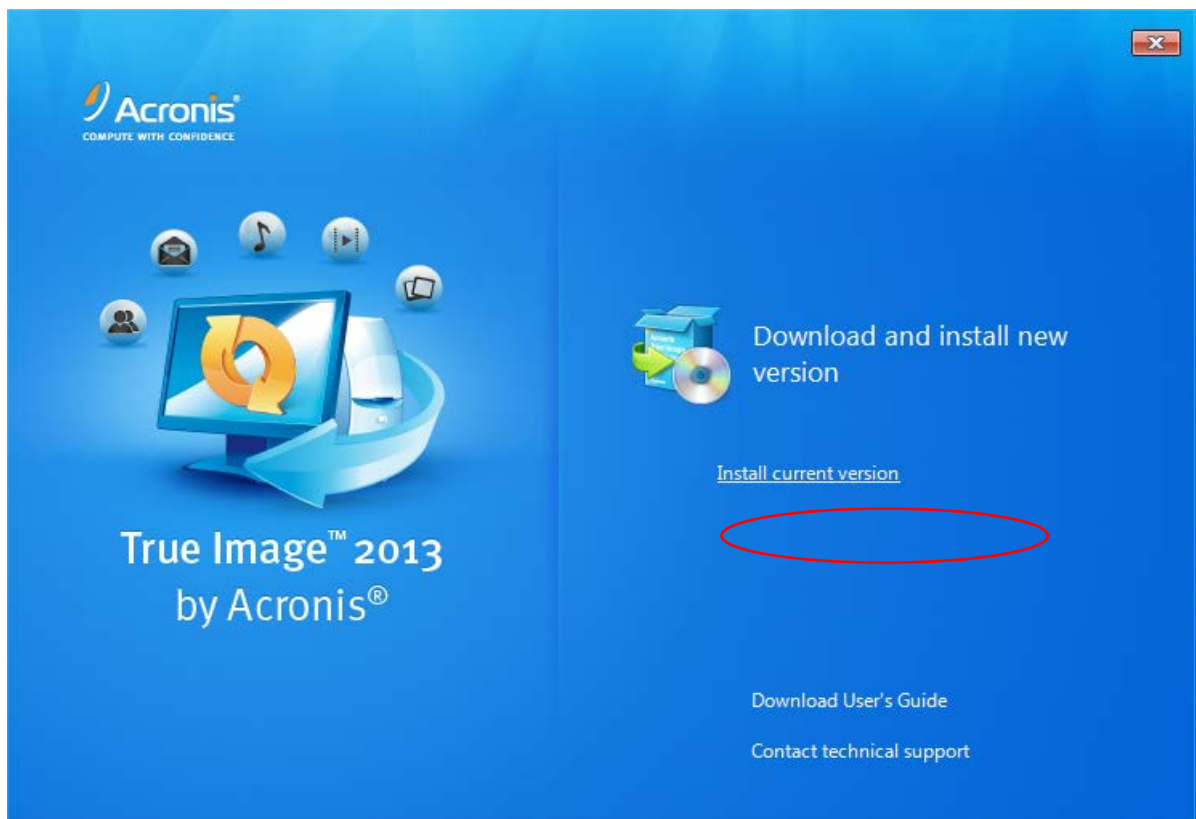
შენახვის მხარდამჭერი მოწყობილობები

- მყარი დისკები
- მყარსხეულიანი დამგროვებლები (**SSD**)
- დაცვის ქსელური მოწყობილობები

- FTP-სერვერები
- CD-R/RW, DVD-R/RW, DVD+R (მათ შორის ორშრიანი DVD+R), DVD+RW, DVD-RAM, BD-R, BD-RE
- USB 1.1/2.0/3.0, FireWire (IEEE-1394) და PC card შემნახავი მოწყობილებები
- REV® და სხვა გადამტანი მატარებლები.

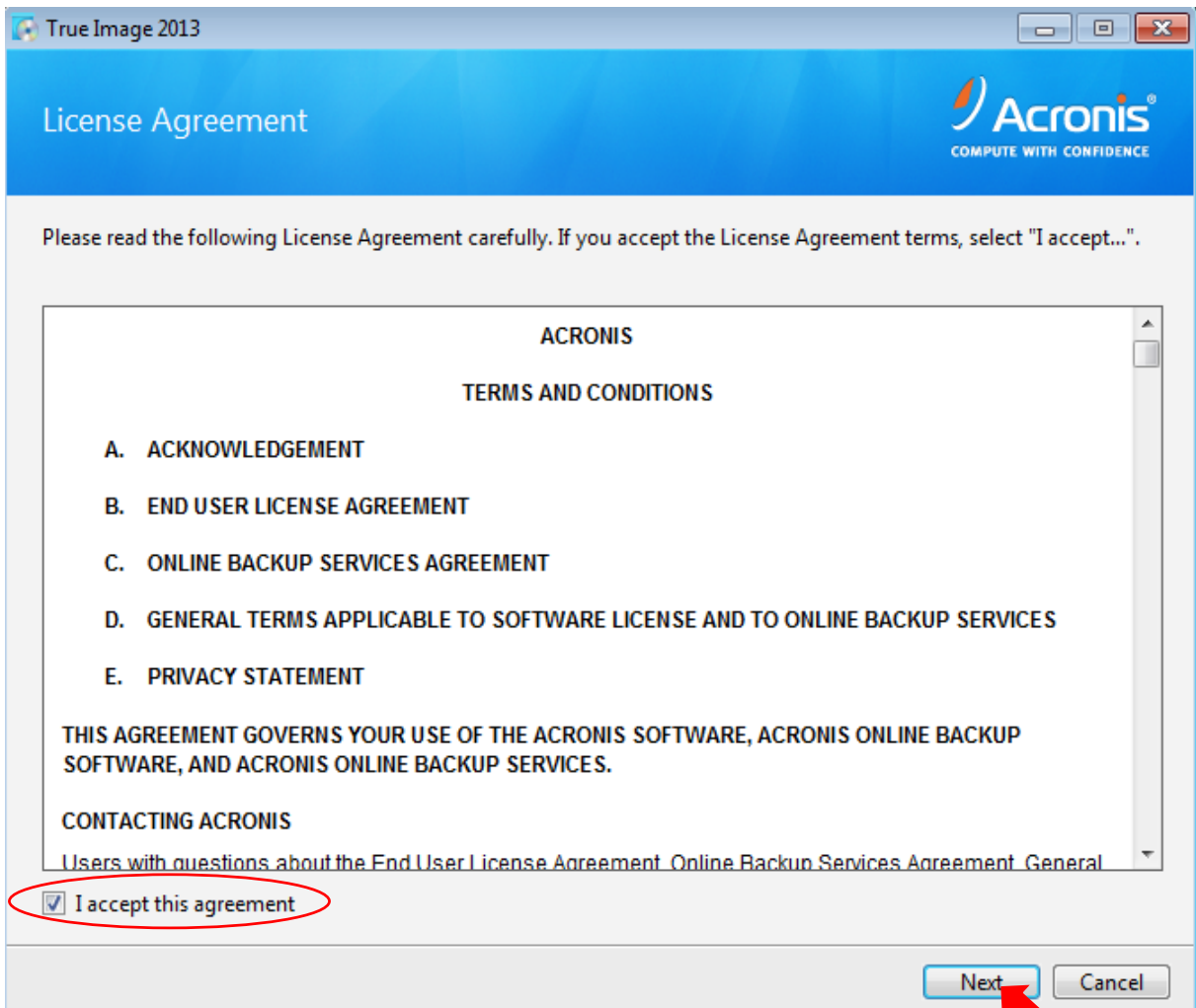
6.3.1.1 Acronis True Image -ის ინსტალაცია და აქტივაცია

პროგრამის დასაყენებლად აუცილებელია მისი გადმოწერა. თუ გსურთ 30 დღიანი საცდელი ვერსიის გამოყენება უმჯობესია მიმართოთ www.acronis.com საიტს. რაც შეეხება გატეხილ ვერსიას მისი გადმოწერა შესაძლებელია შემდეგი მისამართიდან: <http://allshares.ge/download.php?id=3305049551>. გადმოწერის შემდეგ გაუშვით ინსტალატორი, გამოვა შემდეგი ფანჯარა:



თუ დავაჭერთ ღილაკს **Download and install new version**, მაშინ სისტემა თავის საიტზე შეამოწმებს პროგრამის ახალი ვერსიის არსებობას, თუ ასეთი აღმოჩნდა მაშინ მოახდენს მის გადმოწერას ავტომატურ რეჟიმში და გაუშვებს ინსტალაციაზე. თუ არ გვსურს ახალი ვერსიის გადმოწერა (რაც კარგი ვარიანტია თუ გატეხილ ვერსიას ვიყენებთ) მაშინ

უბრალოდ დავაჭიროთ **Install current version** მიმართვას. გამოვა სალიცენზიო შეთანხმების ფანჯარა, რომელშიც აუცილებელია დავეთანხმოთ, წინააღმდეგ შემთხვევაში პროგრამას ვერ დავაყენებთ:



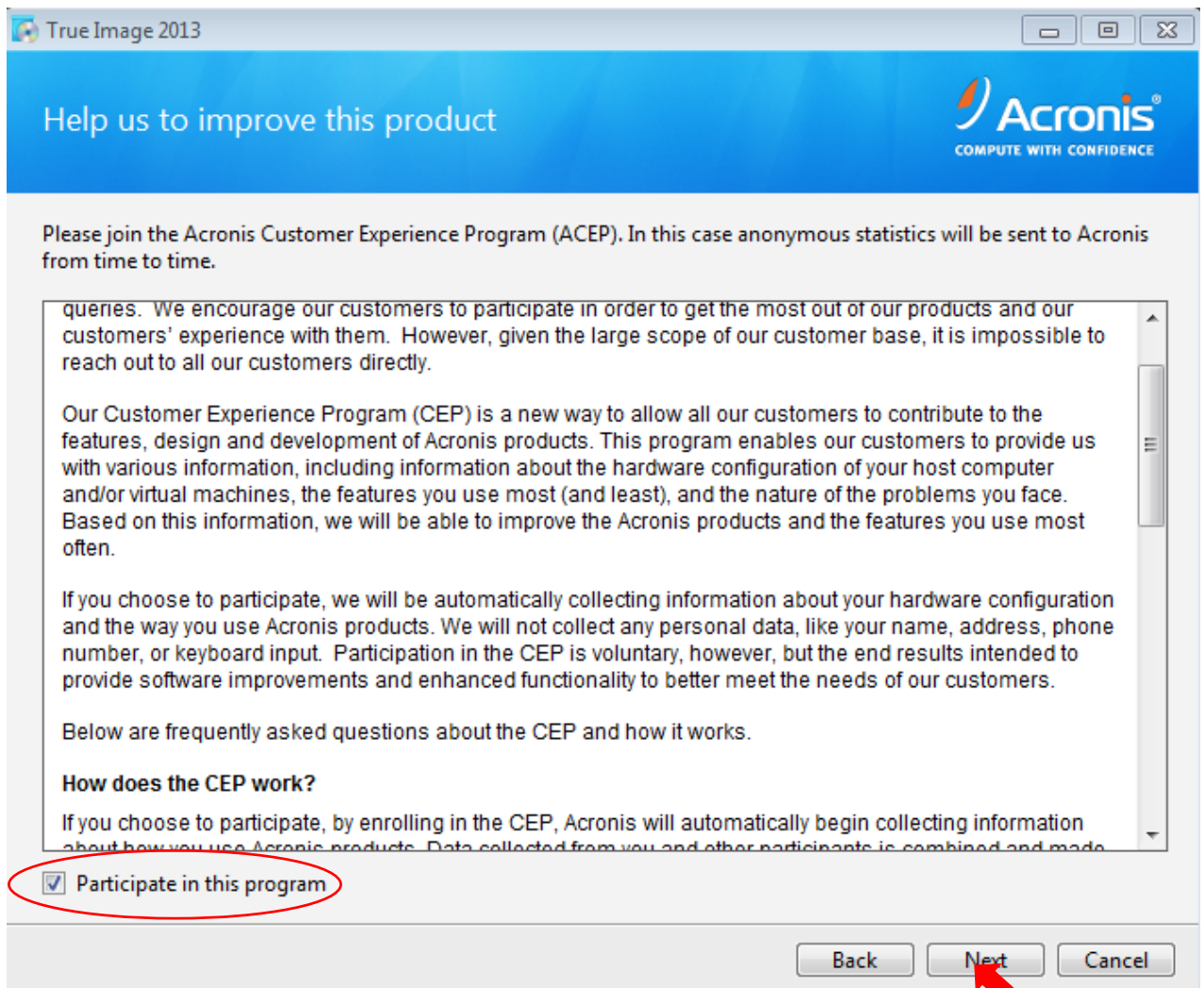
მომდევნო ფანჯარაში შესაძლებელია (სურვილის შემთხვევაში) გავწევრიანდეთ **Acronis Customer Experience Program (ACEP)** პროგრამაში. ამ შემთხვევაში პროგრამა ანონიმურად მოაგროვებს და გააგზავნის **Acronis**-ის საიტზე შემდეგ მონაცემებს:

- ჩვენი კომპიუტერის აპარატურული კონფიგურაცია;
- ჩვენი კომპიუტერის და ვირტუალური მანქანის პროგრამული უზრუნველყოფის კონფიგურაცია (ოპერაციული სისტემის სახელი და ვერსია, ასევე მასზე დაყენებული პროგრამები);

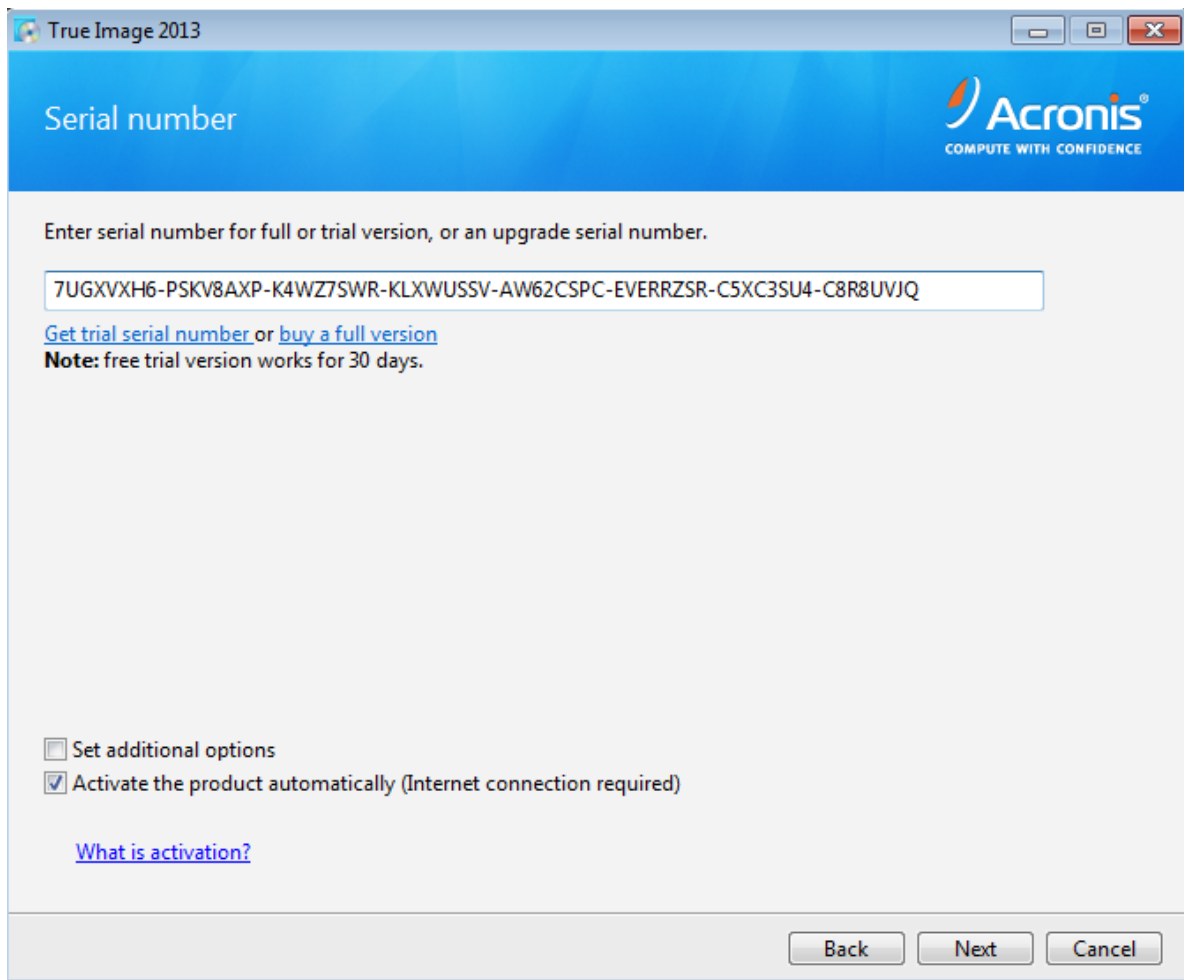
- ვირტუალური მანქანის კონფიგურაცია.

ამით მწარმოებელი ამოწმებს რაიმე კონფლიქტი ხომ არ აქვს **Acronis** პროგრამას სხვა პროგრამებთან და აპარატურასთან, თავსებადობის მხრივ.

ინსტალაციის გასაგრძელებლად დააწექით **Next** ღილაკს.



მომდევნო ეტაპზე უნდა მივუთითოთ მივუთითოთ სერიული ნომერი. მოცემული კოდი პროგრამას მოყვება და ჩაწერილია ტექსტურ დოკუმენტში (Инструкция). დააკოპირეთ და ჩასვით ფანჯრის გამოყოფილ არეში, ისე როგორც ნაჩვენებია სურათზე. დააჭირეთ **Next** ღილაკს.



შემდეგ ფანჯარაში ვაწვებით **Proceed** ღილაკს. დაიწყება ინსტალაციის პროცესი, რომელიც რამდენიმე წამი გაგრძელდება. ინსტალაციის დასრულების შემდეგ დაჭირეთ **Finish** ღილაკს.

მას შემდეგ რაც ინსტალაცია დავასრულეთ, ახლა უნდა ვიზრუნოთ პროგრამის გააქტიურებაზე, წინააღმდეგ შემთხვევაში გვექნება 30-დღიანი საცდელი ვერსია, სადაც ზოგიერთი კომპონენტი არ იქნება ხელმისაწვდომი.

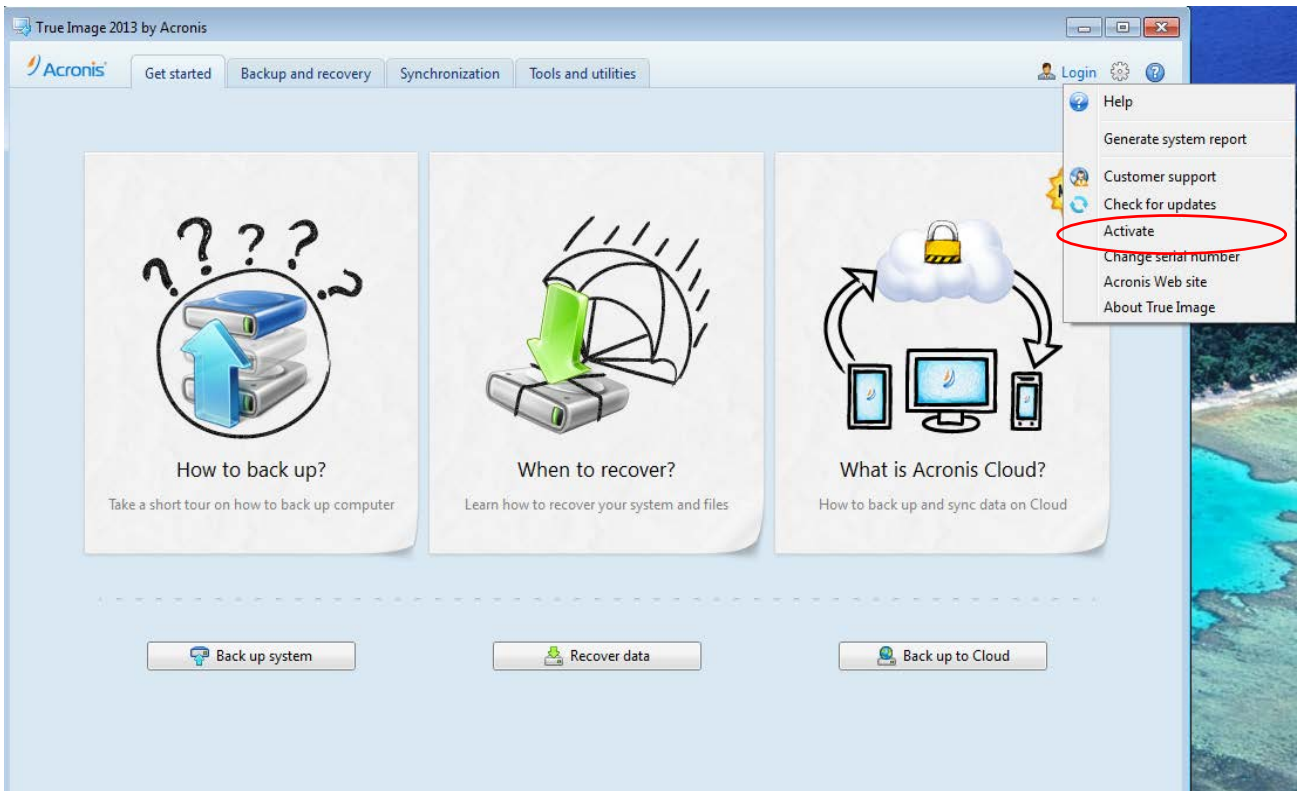
პროგრამის გასააქტიურებლად მიყევით ინსტრუქციას:

1 ეტაპი - გამოიძახეთ შემდეგი საქალაღე **C:\Program Files (x86)\Common Files\Acronis\ Home**. მოძებნეთ **libcrypto10.dll** ფაილი და გადაარქვით სახელი შემდეგნაირად **libcrypto10.dll.bak**;

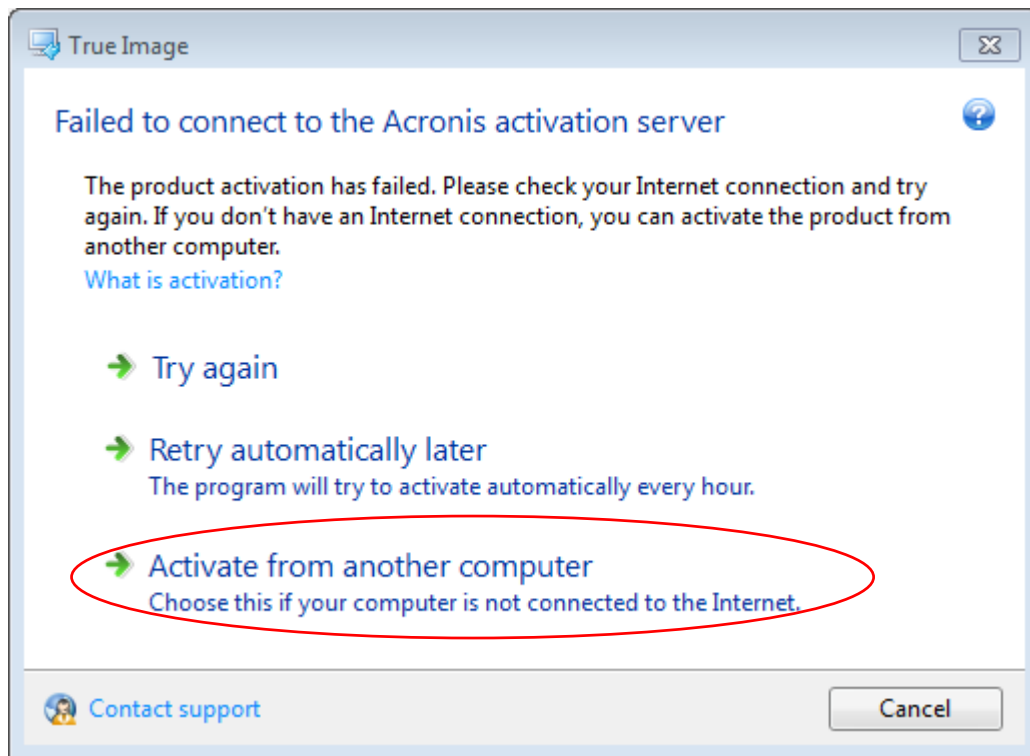
2 ეტაპი - პროგრამის საინსტალაციო პაკეტში მოძებნეთ **libcrypto10.dll** ფაილი, დააკოპირეთ და ჩასვით ზემოთ მოცემულ საქალაღეში;

3 ეტაპი - გადატვირთეთ ოპერაციული სისტემა და როცა ჩაირთვება გათიშეთ ინტერნეტთან წვდომა;

4 ეტაპი - გახსენით **True Image** პროგრამა. გამოსულ ფანჯარაში გამოიძახეთ **Help** მენიუ და აირჩიეთ ბრძანება **Activate**:



დაიწყება აქტივაციის პროცესი, მაგრამ რადგან ინტერნეტთან წვდომა არ გვაქვს გამოიტანს შემდეგ შეტყობინებას. დააჭირეთ **Activate from another computer** ღილაკს. გამოსული ფანჯრის **Type the Activation code** ველში ჩაწერეთ ნებისმიერი კოდი, მაგალითად **12345** და დააწეეთ **Activate** ღილაკს.



5 ეტაპი - გამოიძახეთ შემდეგი საქალაქი **C:\Program Files (x86)\Acronis\TrueImageHome**, მოძებნეთ **license_activator** ფაილი, გადაარქვით სახელი ან საერთოდ წაშალეთ.

6 ეტაპი - ჩართეთ ინტერნეტი და გამოიყენეთ პროგრამა.

6.3.1.2 მონაცემთა სარეზერვო ასლის შექმნა

True Image გვთავაზობს სარეზერვო ასლის შექმნის დიდ შესაძლებლობებს, რაც საკმარისია ინფორმაციული ტექნოლოგიების დარგის პროფესიონალისთვისაც კი, მაგალითად დისკების (დანაყოფების), ფაილებისა და ელექტრონული ფოსტის სარეზერვო ასლების შექმნა. აირჩიეთ სარეზერვო ასლის შექმნის ყველაზე უფრო ხელსაყრელი ხერხი ან გამოიყენეთ ყველა.

განსხვავება ფაილებისა და დისკებისა და დანაყოფების სარეზერვო ასლებს შორის ფაილებისა და საქალაქდების კოპირებისას იკუმშება და ინახება მხოლოდ ფაილები და საქალაქდების დირექტორიები.

დისკებისა და დანაყოფების სარეზერვო ასლები განსხვავდება ფაილებისა და საქალაქდების სარეზერვო ასლებისაგან. **True Image** ინახავს სექტორალურ მომენტალურ სურათს დისკისას ან დანაყოფისას. აქ შედის ოპერაციული სისტემა,

რეესტრი, დრაივერები, პროგრამები, მონაცემთა ფაილები და სისტემური არეები, რომლებიც დაფარულია მომხმარებლისათვის. ამ პროცედურას ეწოდება დისკის ასლის შექმნა, ხოლო მიღებულ სარეზერვო ასლს ხშირად უწოდებენ დისკის ან დანაყოფის ასლს.

ავტომატურად **True Image** ინახავს მყარი დისკის მხოლოდ იმ სექტორებს, რომლებზეც არის ინფორმაცია.

ამასთან, **Acronis**-ს იმიჯში არ შეყავს ოპერაციულ სისტემა **Windows XP**-სა და უფრო ძველი ვერსიების ფაილი **pagefile.sys** და **hiberfil.sys** ფაილი (რომელშიც ინახება ოპერატიული მეხსიერების შემცველობა კომპიუტერის ჰიბერნაციის რეჟიმში გადასვლისას). ეს იძლევა ასლის ზომის შემცირებისა და მისი შექმნისა და აღდგენის სისწრაფის გაზრდის საშუალებას.

დანაყოფის ასლი მოიცავს ყველა ფაილსა და საქალაქებს (მათ შორის ფარულს და სისტემურ ფაილებსაც), ჩამტვირთავ ჩანაწერს და ფაილების განთავსების ცხრილს (**FAT**). ასევე ის მოიცავს ძირეული საქალაქდების ფაილებს და მყარი დისკის ნულოვან ბილიკს მთავარი ჩამტვირთავი ჩანაწერით (**Master Boot Record, MBR**).

დისკის ასლი შეიცავს დისკის ყველა დანაყოფების ასლებს, ასევე ნულოვან ბილიკებს **MBR**-ით.

სრული, ინკრემენტული და დიფერენციალური სარეზერვო ასლები

True Image გვთავაზობს სარეზერვო ასლების შექმნის სამ მეთოდს.

1) **სრული**: სრული სარეზერვო ასლი შეიცავს ყველა მონაცემს, რაც კი მისი შექმნის დროს არსებობდა. ეს რეჟიმი ქმნის საფუძველს მომავალში ინკრემენტული ან დიფერენციალური სარეზერვო ასლების შესაქმნელად; ის ასევე შეიძლება გამოვიყენოთ ავტონომიური სარეზერვო ასლის შექმნისას.

2) **ინკრემენტული**: სარეზერვო ასლში შედის მხოლოდ ის ფაილები, რომლებმაც განიცადეს ცვლილება ბოლო, ნებისმიერი სარეზერვო ასლის შექმნის შემდეგ.

3) **დიფერენციალური**: სარეზერვო ასლში შედის მხოლოდ ის ფაილები, რომლებმაც განიცადეს ცვლილება ბოლო სრული სარეზერვო ასლის შექმნის შემდეგ.

სარეზერვო ასლის შექმნის ამ სამი მეთოდიდან აირჩიეთ ერთ-ერთი:

„სრული“ (Full) - ავტონომიური სრული სარეზერვო ასლის შექმნა შეიძლება იყოს ოპტიმალური გადაწყვეტა, თუკი ხშირად ხდება სისტემის დაბრუნება საწყის მდგომარეობამდე ან არ არის სასურველი დიდი რაოდენობის სარეზერვო ასლების შენახვა.

„ინკრემენტული“ (Incremental) - ინკრემენტული სარეზერვო ასლის შექმნა განსაკუთრებით გამოიყენება იმ შემთხვევაში, თუკი საჭიროა სარეზერვო ასლების ხშირი შექმნა და წარსული დროის კონკრეტულ მომენტში არსებულ მდგომარეობამდე აღდგენის შესაძლებლობის ქონა. სრული სარეზერვო ასლის შექმნის შემდეგ თუ თვის ყოველ დღეს შევქმნით ინკრემენტულ სარეზერვო ასლს, მიიღება იგივე შედეგი, როგორც თითქოს თვის ყოველ დღეს სრულდებოდა სრული სარეზერვო ასლის შექმნა. როგორც წესი, ინკრემენტული სარეზერვო ასლები არსებითად მცირეა სრულ ან დიფერენციალურთან შედარებით.

სარეზერვო ასლის შექმნის ამ მეთოდის გამოყენების სცენარს შეიძლება წარმოადგენდეს სისტემის ყოველკვირეული სრული სარეზერვო ასლის შექმნა მხოლოდ იმ მონაცემთა სარეზერვო ასლების შექმნის ყოველდღიური ინტერვალით, რომლებმაც განიცადეს ცვლილება ბოლო სარეზერვო ასლის შექმნის შემდეგ.

მოცემული სცენარის უპირატესობას წარმოადგენს საცავის სივრცისა და დროის ეკონომია, რაც საჭიროა ყოველდღიური სარეზერვო ასლის შექმნისას. თუმცა, სისტემის დაზიანების შემთხვევაში მის აღდგენას მეტი რესურსი დასჭირდება. თუ დაზიანება მოხდება ხუთშაბათს, მაშინ საჭირო გახდება ორშაბათის, სამშაბათის და ოთხშაბათის ბოლო სრული სარეზერვო ასლის აღდგენა.

დიფერენციალური - იგი წარმოადგენს შუალედურ მეთოდს წინა ორ მეთოდს შორის. დიფერენციალური სარეზერვო ასლი მოიცავს მხოლოდ იმ ფაილებს, რომლებმაც განიცადეს ცვლილება ბოლო სრული სარეზერვო ასლის შექმნის შემდეგ. ეს მეთოდი შესაძლებელია საჭიროებს ნაკლებ დროსა და ადგილს სრული სარეზერვო ასლის შექმნასთან შედარებით, მაგრამ მეტს ინკრემენტულთან შედარებით. აღდგენა უფრო მარტივია, ვიდრე მეორე მეთოდის გამოყენებისას, რადგან საკმარისი იქნება ბოლო სრული და დიფერენციალური სარეზერვო ასლის აღდგენა.

სარეზერვო ასლის შექმნის მეთოდის ასარჩევად აუცილებელია სარეზერვო ასლის შექმნის სამომხმარებლო სქემის აგება.

დისკის დეფრაგმენტაციის შემდეგ შექმნილი ინკრემენტული ან დიფერენციალური სარეზერვო ასლი შეიძლება იყოს საკმაოდ დიდი ზომის, ვიდრე ჩვეულებრივი. ეს იმით არის გამოწვეული, რომ დეფრაგმენტაციის პროგრამა ცვლის ფაილების მდებარეობას დისკზე და ეს ცვლილებები აისახება სარეზერვო ასლში. ამიტომ რეკომენდებულია დისკის დეფრაგმენტაციის შემდეგ სრული სარეზერვო ასლის ხელახლა შექმნა.

შენიშვნა: ინკრემენტული სარეზერვო ასლის დაკარგვის ან დაზიანების შემთხვევაში ყველა მომდევნო ინკრემენტული ასლის გამოყენება შეუძლებელი გახდება.

დისკებისა და დანაყოფების სარეზერვო ასლის შექმნა

დანაყოფებისა და დისკების სარეზერვო ასლების შესაქმნელად დააჭირეთ **Disk and partition backup** მიმართვას ჩანართში **Backup and recovery**. გამოვა **Disk Backup** ფანჯარა:

დისკის/დანაყოფების რეკონსტრუქციის გადართვით
საშუალებას იძლევა ავირჩიოთ დანაყოფები ან მთლიანად დისკი

მონაცემთა წყაროს არჩევა სარეზერვო კოპირებისთვის:
ვირჩევთ დანაყოფს ან მთლიანად დისკს სარეზერვო კოპირებისთვის

არჩევანის რეკონსტრუქციის გადართვით:
დააჭირეთ მითითებულ ადგილას, რათა ავირჩიოთ ერთი დანაყოფი

შენახვის ადგილი:
სარეზერვო ასლი შეიქმნება მითითებულ ადგილას.

სარეზერვო ასლის პარამეტრები:
დამატებითი პარამეტრების მოსამართლად დააჭირეთ მიმართვას.

სარეზერვო ასლის დასახელების ველი:
შეიცვანეთ სარეზერვო ასლის საურველი სახელი.

ადწერილობა და გეგმა:
საშუალებას იძლევა მხარი დაუჭიროს ასლის განახლებებს და ოპტიმიზირება გაუკეთოს სარეზერვო ასლის გეგმას

დააჭირეთ მითითებულ დილაქს ყველა პარამეტრის მომართვის შემდეგ

შემდგომ მოცემულია გამოსახულების სარეზერვო ასლის შექმნის პარამეტრების გამოყენებით სარეზერვო ასლის შექმნის მომართვის ინსტრუქცია.

1. აირჩიეთ დანაყოფი სარეზერვო ასლის შექმნისათვის, შესაბამისი ალმის დაყენებით. თუ ერთზე მეტი დანაყოფის სარეზერვო ასლის შექმნაა საჭირო, დააჭირეთ **Multiple partition selection**. თუ დისკზე არის რამდენიმე დანაყოფი და აუცილებელია მთლიანი დისკის სარეზერვო ასლის შექმნა, დააჭირეთ **Switch to disk mode** ზედა მარჯვენა კუთხეში, და ამის შემდეგ ჩააყენეთ დისკის ალამი. დანაყოფის არჩევის რეჟიმში დასაბრუნებლად, აირჩიეთ **Switch to partition mode**.

2. აირჩიეთ სარეზერვო ასლის შენახვის ადგილი (დატოვეთ შემოთავაზებული შენახვის ადგილი ან მიუთითეთ სხვა ადგილი, მიმდინარე შენახვის ადგილის მარჯვენა ქვედა ისარზე დაჭერით და აირჩიეთ პუნქტი **Browse**).

თუ სარეზერვო ასლის შენახვის ადგილს წარმოადგენს გადამტანი მატარებელი (ფლემ-მატარებელი (USB), დისკი CD, DVD და სხვ.), ხელმისაწვდომი გახდება ალამი **Make this media bootable**. თუ ალამს დააყენებთ, გადამტან მატარებელზე შეიქმნება აღდგენის ჩამტვირთავი გარემო და დაემატება **True Image** –ის ჩამტვირთავი ვერსია. **Acronis**-ი შეიძლება გაიშვას გადამტანი მატარებლიდან კომპიუტერზე ოპერაციული სისტემის გარეშე ან დაზიანებულ კომპიუტერზე, რომელიც ვერ იტვირთება.

3. იმ შემთხვევაში, თუ საჭიროა სარეზერვო ასლის გეგმის მიხედვით შესრულება, დააჭირეთ **Shedule** პუნქტის მარჯვნივ ბმულს, ჩართეთ დაგეგმვა და აირჩიეთ აუცილებელი განრიგი.

4. ავტომატური სარეზერვო ასლის შექმნის სქემის შესაცვლელად, გადადით შესაბამის ბმულზე.

5. სარეზერვო ასლიდან შეიძლება გამოირიცხოს დამალული და სისტემური ფაილები და საქალაქდები, ასევე შეგვიძლია მივუთითოთ თუ რა გაფართოების ფაილები გამოიტოვოს სარეზერვო ასლის შექმნისას. გულისხმობის პრინციპით მითითებულია დროებითი და **.tib** (შექმნილი ასლი) გაფართოების მქონე ფაილები.

6. აუცილებლობის შემთხვევაში შეიტანეთ სარეზერვო ასლის ახალი სახელი შესაბამის ველში.

სახელის დარქმევის დროს შეგვიძლია მივუთითოთ საჭირო ინფორმაცია, როგორცაა:

- **@date@** - სარეზერვო ასლის შექმნის თარიღი;
- **@time@** - სარეზერვო ასლის შექმნის ზუსტი დრო;
- **@user@** - მიმდინარე მომხმარებლის სახელი;
- **@machine@** - კომპიუტერის სახელი;
- **@task@** - დავალების სახელი, რომელიც გაუშვებს სარეზერვო ასლის მიმდინარე

პროცესს;

- **@exec@** - გაშვებული დავალების ნომერი;

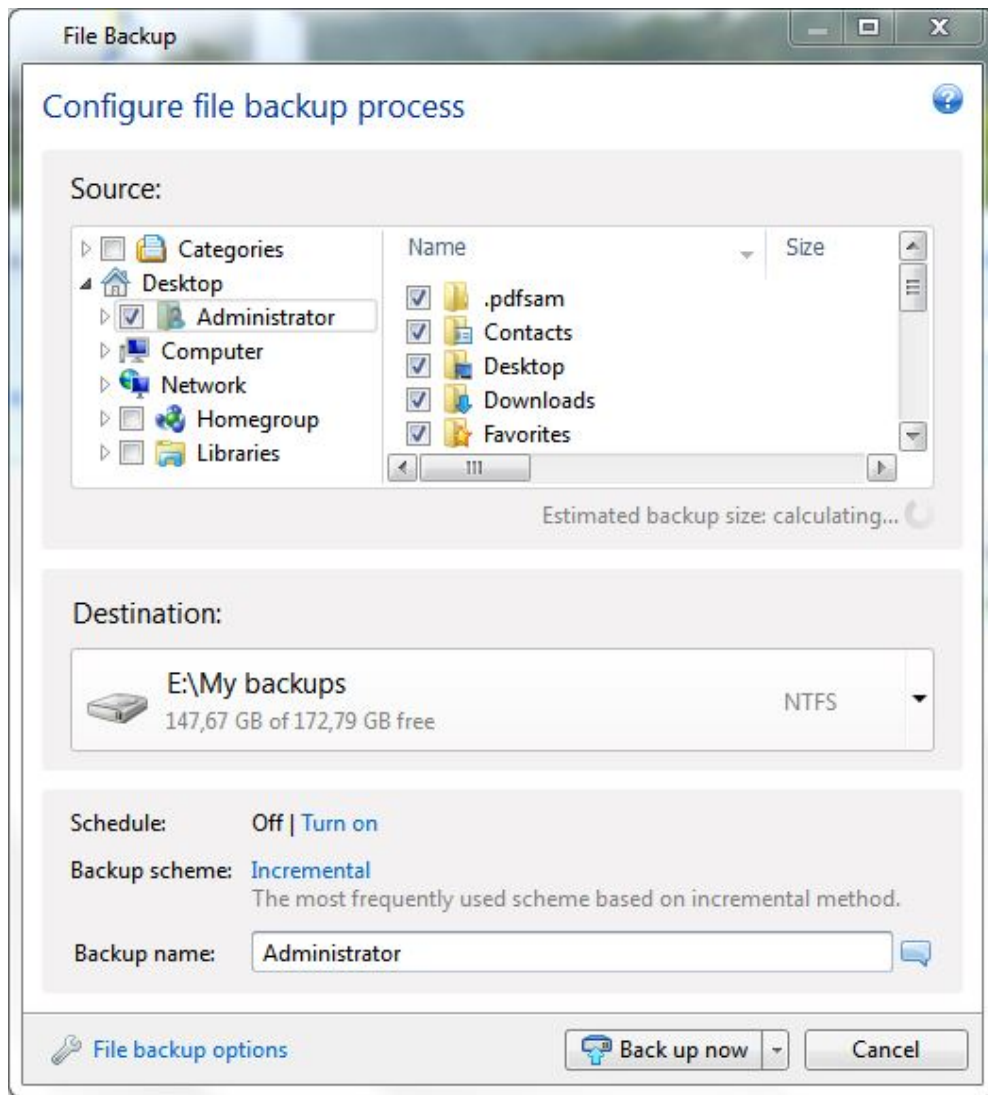
ამისათვის აირჩიეთ ბრძანება **Browse** და ჩაწერეთ ბრძანება რომელიც დაამატებს თქვენთვის საჭირო ინფორმაციას.

7. აირჩიეთ დისკის სარეზერვო ასლის პარამეტრები, რომ მოვმართოთ სარეზერვო ასლის პარამეტრები. მაგალითად, თუ მონაცემთა დისკი შეიცავს კონფიდენციალურ მონაცემებს, შესაძლებელია მათი დაცვა დაშიფრვის საშუალებით. ასევე შეგვიძლია ავირჩიოთ სარეზერვო ასლის დაუყოვნებლივი შემოწმება, მისი შექმნისთანავე, თუმცა მისი გაკეთება მოგვიანებითაც შეიძლება.

8. სარეზერვო ასლის პარამეტრების მომართვის დასრულების შემდეგ უკვე შეგვიძლია გავუშვათ შექმნილი დავალება, **Buck up now** ღილაკზე დაჭერით.

ფაილების და საქალაქდების სარეზერვო ასლის შექმნა

იმისათვის რომ შევქმნათ ფაილების და საქალაქდების სარეზერვო ასლი, მოცემულ ფანჯარაში მონიშნეთ **Other backups** (სხვა სარეზერვო ასლი)



გაიხსნება შესაბამისი ფანჯარა, სადაც ვირჩევთ იმ ფაილებს და საქალაქებს რომელთა ასლის შექმნაც გვინდა და ზემოთ აღწერილი მეთოდით ვქმნით მათ ასლს.

ZIP ფორმატის მხარდაჭერა

თუ სარეზერვო ასლი შენახულია ZIP ფორმატით და არა TIB-ით, მაშინ ფაილების ამოღება სარეზერვო ასლიდან შესაძლებელია ნებისმიერ გარემოში, True Image -ის პროგრამის გამოყენების გარეშე.

მაგალითად, ფაილის სარეზერვო ასლი, რომელიც შეიქმნა ოფისში ფლემ-დამგროვებელზე (USB), შეიძლება აღდგეს სახლში ნოუთბუქზე Acronis-ის დაყენების გარეშე. ეს შესაძლებელია იმის წყალობით, რომ ყველაზე ფართოდ გამოყენებულ ოპერაციულ სისტემებში MS Windows და Mac OS X არის ჩამენებული ZIP ფორმატის მხარდაჭერა.

ZIP ფაილების მხარდაჭერა ოპერაციულ სისტემა *Windows*-ში არ ვრცელდება მრავალტომიან *ZIP* არქივებზე, ასევე *ZIP* არქივებზე, რომელთა ზომა აღემატება 4 გბ, ან რომლებიც შეიცავენ ფაილებს 4 გბ-ზე მეტი ზომით. ამიტომ თუ *ZIP* სარეზერვო ასლის ზომა აღემატება 4 გბ, მისგან შეუძლებელია ფაილების აღდგენა *Acronis*-ის გამოყენების გარეშე.

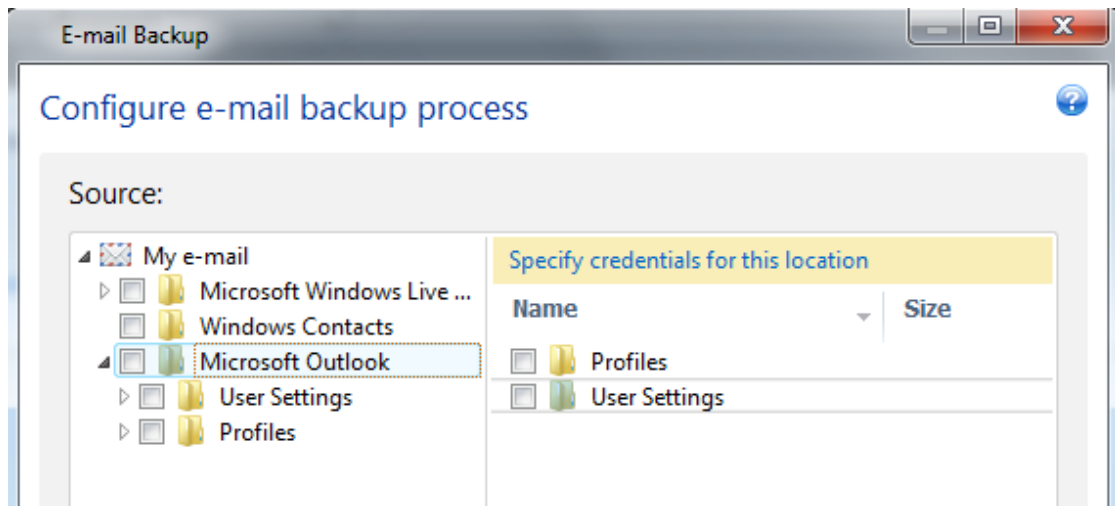
სარეზერვო ასლის შენახვა *ZIP* ფორმატში შესაძლებელია ფაილების, საქაღალდეების, ასევე დუბლიკატების სარეზერვო ასლის შექმნისას.

True Image უზრუნველყოფს *ZIP* ფორმატის სრულ ფუნქციონირებას *tib*-თან. *ZIP* ფორმატის სარეზერვო ასლისთვის შესაძლებელია შემდეგი ოპერაციები: სარეზერვო ასლის შექმნა გეგმის მიხედვის, ფაილებისა და საქაღალდეების აღდგენა და შემოწმება, ინკრიმენტული და დიფერენციული სარეზერვო ასლის შექმნა და ასე შემდეგ. მხარს არ უჭერს პაროლითა და დაშიფვრით დაცვას.

Acronis-ი მხარს უჭერს სარეზერვო კოპირებას და შემოწმებას მხოლოდ იმ *ZIP* ფაილებისას, რომლებიც შეიქმნენ მის დახმარებით. შეუძლებელია *ZIP* პროგრამის საშუალებით შექმნილი *ZIP* არქივის **True Image** -ის პროგრამით აღდგენა და შემოწმება.

6.3.1.3 ელექტრონული ფოსტის სარეზერვო კოპირება

Acronis ახორციელებს შეტყობინებების, სააღრიცხვო ჩანაწერებისა და **Microsoft Outlook 2000, 2002, 2003, 2007, 2010**-ის, **Microsoft Outlook Express**-ის, **Windows Mail** და **Windows Live**-ის მომართვების (პარამეტრების) სარეზერვო კოპირებას. ელექტრონული ფოსტის სარეზერვო კოპირებისას პროგრამა თვითონ არჩევს საქაღალდეს, რომლებიც სარეზერვო ასლის შექმნისათვისაა განკუთვნილი, მომხმარებელს თითქმის არაფრის არჩევა არ მოეთხოვება. აუცილებლობის შემთხვევაში აირჩიეთ **Microsoft Outlook**-ის გარკვეული კომპონენტები და საქაღალდეები:



ხელმისაწვდომია შემდეგი ელემენტები:

- შეტყობინებები, რომლებიც ინახება PST/DBX-ფაილებში მონაცემების გარეშე.
- ელექტრონული ფოსტის საადრიცხვო ჩანაწერები.

Microsoft Office Outlook 2000, 2002, 2003, 2007, 2010-ისათვის:

- საფოსტო საქაღალდეები
- კალენდარი
- კონტაქტები
- დავალებები
- შენიშვნები
- ხელმოწერები
- სიახლეები
- მომხმარებლის მომართვები
- სამისამართო წიგნი.
- **Microsoft Outlook Express-ისათვის:**
- საფოსტო საქაღალდე
- სამისამართო წიგნი (აირჩიეთ **Windows Address Book**).

True Image -ს აქვს შესაძლებლობა შექმნას IMAP-ის (Internet Messages Access Protocol) სარეზერვო ასლი პროგრამა **Microsoft Outlook-ისათვის**. ეს ნიშნავს, რომ შესაძლებელია სარეზერვო ასლის შექმნა საქაღალდისა, რომელიც საფოსტო სერვერზე ინახება. **Microsoft Outlook Express-ის** და **Windows Mail-ისათვის** შესაძლებელია მხოლოდ იმ საფოსტო საქაღალდეების კოპირება, რომლებიც ლოკალურ კომპიუტერზე ინახება.

True Image არ უჭერს მხარს უნიკოდის სიმბოლოებს იმ ელემენტებისათვის, რომლებისთვისაც იქმნება **E-Mail Backup** ტიპის სარეზერვო ასლები.

როგორ შევქმნათ ელ-ფოსტის სარეზერვო ასლი:

1. ჩანართზე **Backup and recovery** დააჭირეთ **Other backups** და აირჩიეთ **Mail backup**. გაიხსნება ფანჯარა **E-mail Backup**.

2. აირჩიეთ **What to back up**-ში საჭირო ობიექტები. პანელის პირველ გვერდზე აისახება ელემენტის შემადგენლობა ყველა არჩეული ობიექტით. ამორთეთ ალამი ჩადგმულ ელემენტებთან, რომლებიც არ საჭიროებენ სარეზერვო ასლში მოთავსებას.

3. აირჩიეთ სარეზერვო ასლის შენახვის ადგილი (დატოვეთ სისტემის მიერ შემოთავაზებული ან მიუთითეთ სხვა, შენახვის მიმდინარე ადგილის მარჯვენა ქვედა ისარზე დაჭერით და **Browse...** პუნქტის არჩევით).

4. პროგრამა სარეზერვო ასლის ფაილს სახელს ანიჭებს გულისხმობის პრინციპით. თუ აუცილებელია სხვა სახელის გამოყენება, შეიყვანეთ იგი **Backup name** ველში.

5. დააჭირეთ ღილაკს **Back up now** სარეზერვო ასლის შესაქმნელად. სარეზერვო ასლის შექმნის 6 საათით გადასადებად, დააჭირეთ ისარს ქვემოთ ამ ღილაკის მარჯვნივ და აირჩიეთ ჩამოშლილი სიიდან დალოდების პერიოდი.

აუცილებელია **Windows**-ის სააღრიცხვო ჩანაწერის საკუთარი სახელი და პაროლი, კონფიდენციალურობის დასაცავად.

გულისხმობის პრინციპით მოცემული სარეზერვო ასლის შექმნის პარამეტრების შესაცვლელად დააჭირეთ **E-mail backup options** და შეცვალეთ პარამეტრები. სისტემის მიერ შემოთავაზებული სარეზერვო კოპირების სქემის შესაცვლელად გადადით შესაბამის მიმართვაზე.

განრიგის მიხედვით სარეზერვო ასლის შესაქმნელად დააჭირეთ მიმართვას **Turn on** განრიგის მოსამართლად. სარეზერვო ასლი რომ განრიგის მიხედვით შეიქმნას, დააჭირეთ ქვემოთ მიმართულ ისარს **Back up now** ღილაკის მარჯვნივ და აირჩიეთ ჩამოშლილი სიიდან პუნქტი **Later**. მომართული პარამეტრებით სარეზერვო ასლი შეიქმნება შედგენილი განრიგით. მისი გაშვება შეიძლება ხელით მოგვიანებით **Backup and recovery** ჩანართიდან.

Acronis-ის უწყვეტი დაცვის ფუნქციის გამოყენება

Acronis-ის უწყვეტი დაცვის ფუნქცია (**Acronis Nonstop backup**) საშუალებას გვაძლევს მარტივად დავიცვათ დისკები და ფაილები. მისი დახმარებით შეიძლება დისკების, ფაილებისა და მათი ვერსიების აღდგენა.

Acronis-ის უწყვეტი დაცვის ფუნქციის მთავარი მიზანია მონაცემთა (ფაილები, საქაღალდეები, კონტაქტები და სხვ.) უწყვეტი დაცვა, მაგრამ მისი დახმარებით შეიძლება ასევე დანაყოფების დაცვაც. მთელი დანაყოფის დაცვის არჩევისას, შესაძლებელია ამ დანაყოფის სრული აღდგენა, ასლის (**Image**) აღდგენის პროცედურის არჩევის გამოყენებით.

Acronis Nonstop Backup-ის გამოყენება შეუძლებელია იმ მონაცემთა დასაცავად, რომლებიც გარე მყარ დისკებზეა მოთავსებული.

მუშაობის პრინციპი

Acronis Nonstop Backup-ის გაშვების შემდეგ, პროგრამა იწყებს დასაცავად არჩეული მონაცემების საწყისი სრული სარეზერვო ასლის შექმნას. დაცული ფაილების ცვლილებების (მათ შორის გახსნილი ფაილების) შენახვა ხდება ყოველ ხუთ წუთში, ამიტომ, სისტემის აღდგენა შესაძლებელია დროის ნებისმიერ მომენტში.

როგორც წესი, დაცული მონაცემთა სარეზერვო ასლის შექმნა ხდება 24 საათის განმავლობაში 5-წუთიანი ინტერვალით.

ძველი სარეზერვო ასლები გაერთიანდება ისე, რომ **True Image** შეინახავს ბოლო 30 დღის ყოველდღიურ და ყოველკვირეულ სარეზერვო ასლებს იქამდე, სანამ არ მოხდება უწყვეტი სარეზერვო ასლების საცავის თავისუფალი სივრცის გამოყენება.

თუ **Acronis Nonstop Backup** ფუნქცია გამოყენებულია არასისტემურ დანაყოფთან და სარეზერვო ასლის შექმნიდან 5 წუთის განმავლობაში არ მომხდარა არავითარი ცვლილება, შემდგომი დაგეგმილი სარეზერვო ასლის შექმნა გამოიტოვება. **Acronis Nonstop Backup** დაელოდება მონაცემთა მნიშვნელოვან ცვლილებებს და შექმნის ახალ ინკრემენტულ სარეზერვო ასლს მხოლოდ მაშინ, როცა ასეთ ცვლილებას აღმოაჩენს. ამ შემთხვევაში დროის რეალური ინტერვალის აჭარბებს 5 წუთს. გარდა ამისა, თუ

მაგალითად რედაქტორ **Word**-ის მუშაობისას შენახვა არ მომხდარა ერთი საათის განმავლობაში, **Word**-ის დოკუმენტში ცვლილებების სარეზერვო ასლი არ შეიქმნება ყოველ ხუთ წუთში, რადგან **True Image** აღიქვამს ფაილის ცვლილებებს დისკზე და არა ოპერატიულ მეხსიერებაში.

გაერთიანება ხდება ყოველ დღე ღამის 12-იდან 1 საათამდე. პირველი გაერთიანება მოხდება მას შემდეგ, რაც **Acronis Nonstop Backup** -ის მუშაობა შეადგენს არანაკლებ 24 საათს. მაგალითად, **Acronis Nonstop Backup** (უწყვეტი დაცვა) ჩაერთო 12 ივლისს დილის 10 საათზე. მაშინ პირველი გაერთიანება მოხდება 14 ივლისს ღამის 12-იდან 1 საათამდე. შემდეგ პროგრამა მონაცემებს გაერთიანებს ყოველ დღე ერთსა და იმავე დროს. კომპიუტერის ღამის 12-იდან 1 საათამდე გამორთვისას, გაერთიანება დაიწყება კომპიუტერის ჩართვისას. **Acronis Nonstop Backup**-ის გარკვეული დროით გამორთვის შემთხვევაში, გაერთიანება მოხდება მისი ხელახლა ჩართვისას.

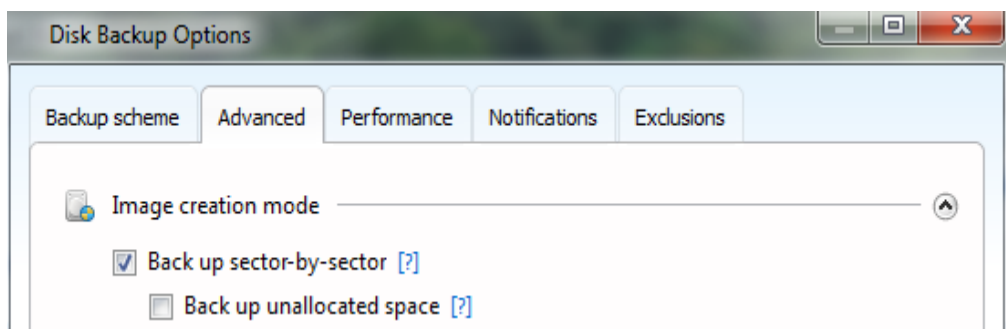
შეიძლება ვიფიქროთ, რომ ასეთი სიჩქარით სარეზერვო ასლის შექმნისას საცავი სწრაფად აივსება. მაგრამ ეს ასე არ არის, რადგან **True Image** სარეზერვო ასლს ქმნის ე.წ. „დელტების“ საშუალებით. ეს ნიშნავს, რომ სარეზერვო ასლებში ინახება მხოლოდ სხვაობა ძველსა და ახალ ვერსიებს შორის, და არა მთლიანი შეცვლილი ფაილი. მაგალითად, **Microsoft Outlook** ან **Windows Mail**-ის გამოყენებისას, არსებული **PST**-ფაილი შეიძლება იყოს ძალიან დიდი. გარდა ამისა, ის იცვლება ელექტრონული ფოსტით შეტყობინების ყოველი მიღება-გაგზავნის დროს. **PST**-ფაილის სრულმა სარეზერვო ასლმა შეიძლება დაიკავოს საცავის უსაზღვროდ დიდი სივრცე, ამიტომ **Acronis** მხოლოდ ფაილის ცვლილებიანი ნაწილის სარეზერვო ასლს ქმნის, პირველად შექმნილ სარეზერვო ასლზე დამატებით.

პარამეტრების მომართვა სარეზერვო ასლის შექმნისას

ასლის (Image) შექმნის რეჟიმი

ამ პარამეტრების გამოყენებით შეიძლება მონაცემების შემცველი არა მარტო სექტორის, არამედ მთლიანი დანაყოფებისა და მყარი დისკების ზუსტი ასლების შექმნა. პარამეტრი **Back up unallocated space** ხელმისაწვდომია მხოლოდ მაშინ, როცა ჩართულია ალამი **Back up sector-by-sector**.

- ყველა სექტორის სარეზერვო ასლის შესაქმნელად ჩართეთ ალამი **Back up sector-by-sector**. ავტომატურად დაკოპირდება მყარის დისკის მხოლოდ ის სექტორები, რომლებზეც არის მონაცემები. თუმცა ხელსაყრელია მყარი დისკის ყველა სექტორის სარეზერვო ასლის შექმნა. მაგალითად, შეცდომით წაგვეშალა ზოგიერთი ფაილი და შესაბამისი უტილიტების გამოყენებით აღდგენის ოპერაციის დაწყებამდე გვსურს დისკის ასლის შექმნა, რადგან ზოგჯერ აღდგენით შეიძლება დაირღვეს ფაილთა სისტემა. მყარი დისკის როგორც გამოყენებული, ასევე გამოუყენებელი სექტორების ამ რეჟიმში კოპირებისას იზრდება დამუშავების დრო და ჩვეულებრივ მიიღება დიდი ზომის ასლი (**Image**).



- **Back up unallocated space** მისაწვდომი ხდება თუ არჩეულია წინა **Back up sector-by-sector** პარამეტრი. ავტომატურად სექტორულ რეჟიმში ასლის შექმნისას დისკის დაუყოფელი სივრცე არ ემატება სარეზერვო ასლს. ამ პარამეტრის არჩევისას სარეზერვო ასლში შევა მყარი დისკის მთელი დაუყოფელი სივრცე.

სარეზერვო ასლების დაცვა

სარეზერვო ასლის დაცვა შესაძლებელია პაროლით. ავტომატური დაცვა პაროლით სარეზერვო ასლისთვის არ არის მომართული.

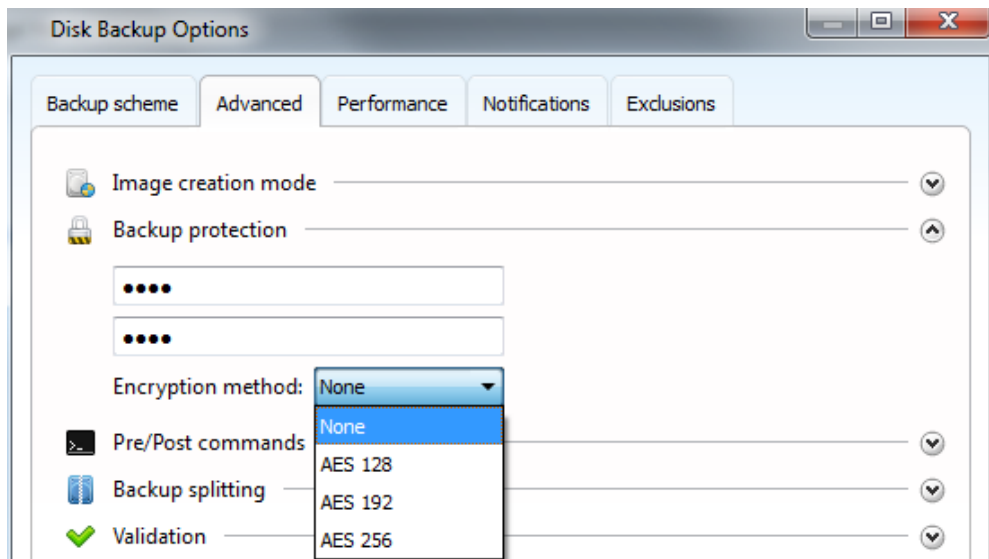
როგორ დავიცვათ სარეზერვო ასლი

- შეიყვანეთ სარეზერვო ასლის პაროლი ველში **Password**. საიმედოდ დაცვისათვის პაროლი უნდა შედგებოდეს არანაკლებ რვა სიმბოლოსგან, როგორც ასოების (მთავრული და პატარა), ისე ციფრების კომბინაციისგან.

- შეიყვანეთ ხელახლა პაროლი ველში **Confirm**.

- კონფიდენციალური მონაცემების საიმედოდ დასაცავად დაშიფრეთ სარეზერვო ასლები საიმედო კრიპტოგრაფული **AES** ალგორითით, რომელიც წარმოადგენს დარგობრივ სტანდარტს. **AES** ალგორითმი მოწოდებულია გასაღების სამი სიგრძით (128,

192 და 256 ბიტი), რაც წარმოადგენს და დაცვას შორის კომპრომისის მონახვის საშუალებას იძლევა:



უმეტესწილად საკმარისია დაშიფვრა 128-ბიტისანი გასაღებით. რაც უფრო გრძელია დაშიფვრის გასაღები, მით უფრო კარგადაა დაცული მონაცემები. თუმცა 192- და 256-ბიტისანი გასაღებების გამოყენება მნიშვნელოვნად ანელებს სარეზერვო ასლის შექმნის პროცესს.

AES დაშიფვრის გამოყენების აუცილებლობის შემთხვევაში, აირჩიეთ ერთ-ერთი ამ სამი ვარიანტიდან:

- **AES 128** – 128-ბიტისანი დაშიფრული გასაღები;
- **AES 192** – 192-ბიტისანი დაშიფრული გასაღები;
- **AES 256** – 256-ბიტისანი დაშიფრული გასაღები.

თუ დაშიფვრა აუცილებელი არ არის და საკმარისია მისი მხოლოდ პაროლით დაცვა, აირჩიეთ **None**.

დაცვის პარამეტრების მითითების შემდეგ დააჭირეთ **OK**-ს.

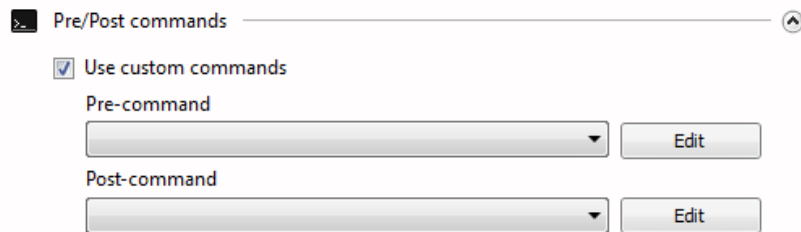
მიაქციეთ ყურადღება, რომ პაროლით დაცული სარეზერვო ასლის შექმნის შემდეგ, მისი პაროლის შეცვლა შეუძლებელია.

პაროლით დაცული სარეზერვო ასლებიდან ინფორმაციის აღსადგენად აუცილებელია პაროლის შეყვანა (რათა მისაწვდომი იყოს მხოლოდ ავტორიზებული მომხმარებლისათვის).

ბრძანებები სარეზერვო ასლების შექმნამდე და შექმნის შემდეგ

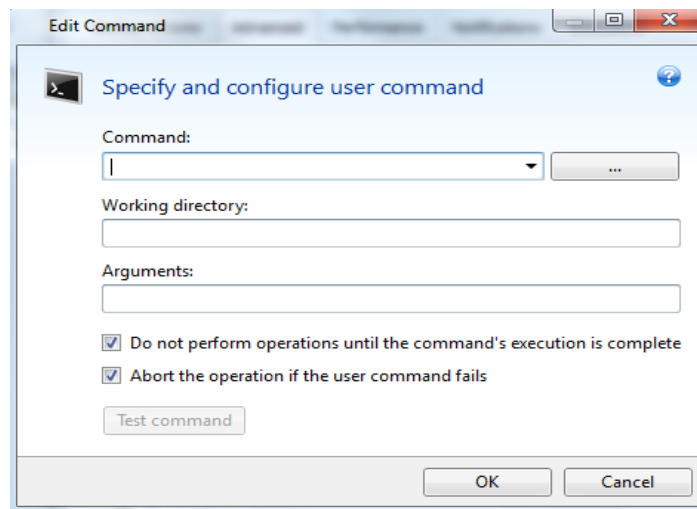
შეიძლება ბრძანებების ან ფაილთა ჯგუფის მითითება, რომლებიც ავტომატურად შესრულდება სარეზერვო ასლის შექმნამდე და შექმნის შემდეგ.

მაგალითად, შესაძლებელია **Windows**-ის გარკვეული პროცესების გაშვება ან შეჩერება ან სარეზერვო ასლის შექმნამდე მონაცემთა შემოწმება:



ბრძანებების (ფაილების პაკეტის) მისათითებლად საჭიროა:

- ველში **Pre-command** აირჩიეთ ბრძანება, რომელიც შესრულდება სარეზერვო ასლის შექმნის პროცესის გაშვებამდე. ახალი ბრძანების შესაქმნელად ან ფაილთა პაკეტის ასარჩევად, დააჭირეთ ღილაკს **Edit**:



- ველში **Post-command** აირჩიეთ ბრძანება, რომელიც შესრულდება სარეზერვო ასლის შექმნის დასრულების შემდეგ. ახალი ბრძანების შესაქმნელად ან ფაილთა პაკეტის ასარჩევად დააჭირეთ ღილაკს **Edit**.

ნუ ეცდებით ინტერაქტიული ბრძანებების შესრულებას, ე.ი. ბრძანებების, რომლებიც მომხმარებლის ჩარევას საჭიროებენ (მაგალითად, „**pause**“). მათი მოქმედება შეუძლებელია.

სარეზერვო ასლის შექმნისას შესასრულებელი სამომხმარებლო ბრძანებების რედაქტირება

სარეზერვო ასლის შექმნამდე და შექმნის შემდეგ სამომხმარებლო ბრძანებების მისათითებლად:

- ველში **Command** შეიყვანეთ ბრძანება ან აირჩიეთ ჩამონათვალიდან. ფაილთა ჯგუფის ასარჩევად დააჭირეთ ღილაკს ...

- ველში **Working directory** შეიყვანეთ „გზა“ (path) ბრძანებების შესასრულებლად ან აირჩიეთ გამოყენებული „გზის“ ჩამონათვალიდან.

- ველში **Arguments** შეიყვანეთ ან აირჩიეთ შესასრულებელი ბრძანებების ჩამონათვალიდან არგუმენტები.

პარამეტრიდან **Do not perform operations until the command's execution is complete** აღმის მოხსნა (რომელიც სარეზერვო ასლის შექმნამდე შესასრულებელი ბრძანებებისათვის ავტომატურადაა ჩართული) საშუალებას იძლევა, სარეზერვო ასლის შექმნის პროცესი ერთდროულად მიმდინარეობდეს სამომხმარებლო ბრძანებების შესრულებასთან ერთად.

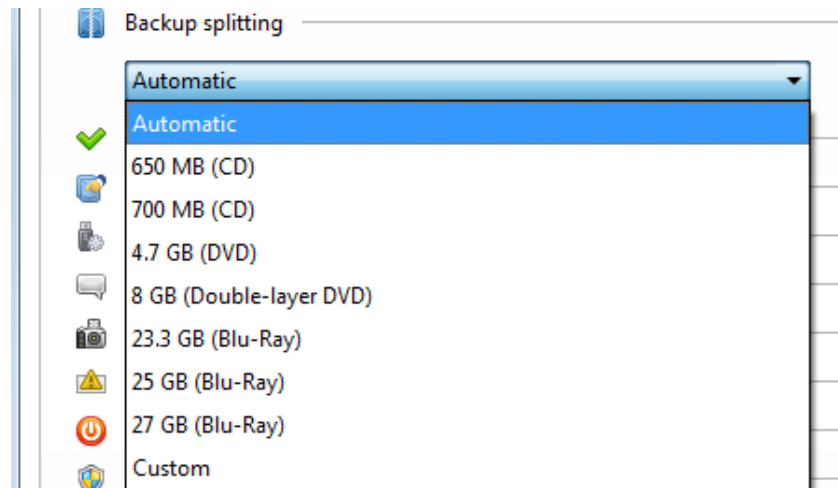
პარამეტრი **Abort the operation if the user command fails** (რომელიც ავტომატურადაა ჩართული) წყვეტს პროცედურას ბრძანების შესრულების დროს რაიმე სახის შეცდომის აღმოჩენისას.

შექმნილი ბრძანების შესამოწმებლად დააჭირეთ ღილაკს **Test command**.

სარეზერვო ასლების დაყოფა

True Image -ს არ შეუძლია დაყოს უკვე შექმნილი სარეზერვო ასლები. მათი დაყოფა შესაძლებელია მხოლოდ მათი შექმნისას.

დიდი ზომის სარეზერვო ასლები შეიძლება დაიყოს რამდენიმე ფაილად, რომლებიც ერთად წარმოადგენენ საწყის სარეზერვო ასლს. სარეზერვო ასლის დაყოფა ხდება ასევე გადასატან მატარებელზე ჩაწერისთვის:



გულისხმობის პრინციპით შემოთავაზებულია **Automatic**. აღნიშნულ პარამეტრს **True Image** შემდეგნაირად იყენებს:

- თუ არჩეულ დისკზე საკმარისი ადგილია და მისი ფაილური სისტემა მხარს უჭერს ფაილებს, რომელთა ზომა შეესაბამება სარეზერვო ასლისთვის პროგნოზირებულ ზომას, მაშინ იქმნება სარეზერვო ასლის მხოლოდ ერთი ფაილი.

- თუ დისკზე საკმარისი ადგილია, მაგრამ მისი ფაილური სისტემა არ უჭერს მხარს ფაილის პროგნოზირებულ ზომას, ასლი (**Image**) ავტომატურად გაიყოფა რამდენიმე ფაილად.

- თუ მყარ დისკზე არასაკმარისი თავისუფალი ადგილია, პროგრამა გამოიტანს შეტყობინებას და დაელოდება თქვენს შემდგომ გადაწყვეტილებას. შეეცადეთ გაანთავისუფლოთ დამატებითი ადგილი დისკზე ან აირჩიეთ სხვა დისკი და შემდეგ გააგრძელეთ პროცესი.

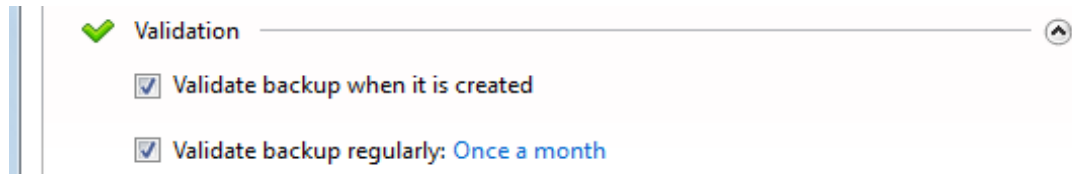
თუ დისკზე არ არის საკმარისი თავისუფალი ადგილი, **Acronis** მოგთხოვთ მომდევნო დისკის ჩადებას.

ფაილის მოთხოვნილი ზომა შეიძლება ავირჩიოთ ჩამოშლილი ჩამონათვალიდან ამრიგად, სარეზერვო ასლი დაიყოფა მითითებული ზომის რამდენიმე ფაილად. ეს ხელსაყრელია მაშინ, როცა სარეზერვო ასლი ინახება მყარ დისკზე შემდგომ ოპტიკურ CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE-ზე დისკებზე ჩასაწერად.

CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE დისკებზე ჩასაწერად შექმნილ ასლს (image) უფრო მეტი დრო სჭირდება, ვიდრე მხოლოდ მყარ დისკზე შესანახად განკუთვნილს.

სარეზერვო ასლების შემოწმება

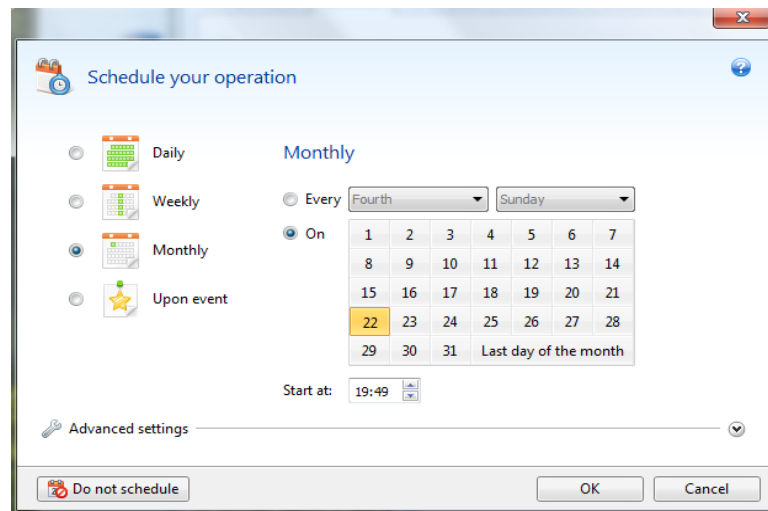
მიუთითეთ შემოწმების დამატებითი პარამეტრები: **Validate backup when it is created:**



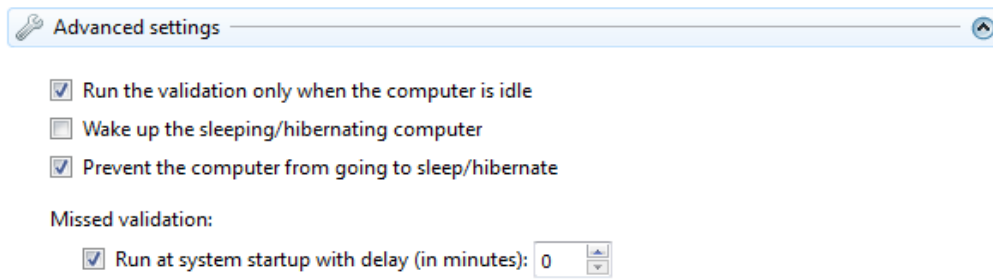
როცა ეს პარამეტრია ჩართული, სარეზერვო ასლის ან მისი დამატებითი ვერსიის შექმნისთანავე ხდება მისი მთლიანობის შემოწმება. კრიტიკულად მნიშვნელოვანი მონაცემების სარეზერვო ასლების, დისკის ან დანაყოფის ასლის შექმნისას მკაცრად არის რეკომენდებული ამ ფუნქციის ჩართვა, რათა გარანტირებულ იქნეს სარეზერვო ასლის ვარგისიანობა დაზიანებული მონაცემების აღდგენის შემთხვევაში.

რეგულარული შემოწმება

სარეზერვო ასლის საიმედოობისათვის მომართეთ რეგულარული შემოწმება. რეგულარული შემოწმება ავტომატურადაა ჩართული და მას აქვს შემდეგი პარამეტრები, რომლის შეცვლაც შეგვიძლია სურვილისამებრ:



- პერიოდულობა: თვეში ერთხელ.
- დღე: სარეზერვო ასლის შექმნის თარიღი.
- დრო: სარეზერვო ასლის შექმნის დაწყებას დამატებული 15 წთ.
- დამატებითი პარამეტრები: ალამი დაყენებულია **Run the validation only when the computer is idle:**

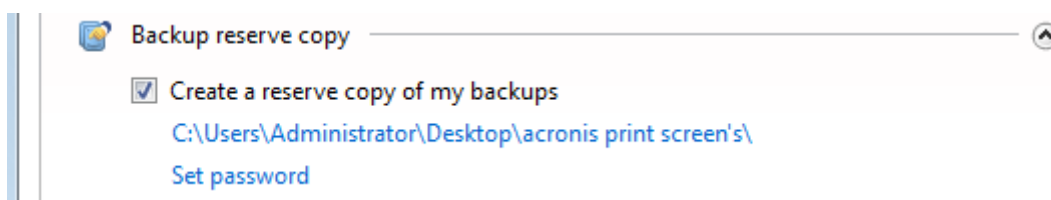


მაგალითად, სარეზერვო ასლის შექმნის ოპერაცია დაიწყო 15 ივლისს 12:00-ზე. სარეზერვო ასლი შეიქმნა 12:05. ამ ვერსიის შემოწმება მოხდება 12:15-იდან, თუ კომპიუტერი იმყოფება „დამცველი ფარდის“ (screen saver) რეჟიმში. წინააღმდეგ შემთხვევაში შემოწმება არ მოხდება. მომდევნო შემოწმება მოხდება ერთი თვის შემდეგ, 15 აგვისტოს 12:15-ზე. როგორც ადრე, მაშინაც კომპიუტერი უნდა იყოს „დამცველი ფარდის“ რეჟიმში. იგივე ოპერაცია განმეორდება 15 სექტემბერს და ასე შემდეგ.

შესაძლებელია ავტომატურად მომართული პარამეტრების შეცვლა და საკუთარი განრიგის დადგენა. ეს ხელსაყრელია, თუ სარეზერვო ასლის შექმნის მომხმარებლის სქემა ინკრემენტულ ვერსიასთან ერთად არის მომართული. მაგალითად, შესაძლებელია დაიგეგმოს სარეზერვო ასლის ყველა ვერსიის (საწყისი სრული და ყველა მომდევნო ინკრემენტული ვერსიის) შემოწმება კვირაში ერთხელ.

სარეზერვო ასლების დუბლირება

სარეზერვო ასლების დუბლიკატების შექმნა და შენახვა შესაძლებელია კომპიუტერის ფაილურ სისტემაში, ქსელურ დისკზე ან USB ფლეშ-დამგროვებელზე.



სარეზერვო ასლის დუბლიკატის შესაქმნელად საჭიროა:

- **Create a reserve copy of my backups** ალმის ჩართვა.
- დააჭირეთ **Set location...** და მიუთითეთ სარეზერვო ასლის შენახვის ადგილი.

შესაძლებელია TIB დუბლიკატის დამატებით პაროლით დაცვა. ამისათვის, დააჭირეთ ღილაკს **Set password** და მიუთითეთ პაროლი დუბლიკატისათვის.

პროგრამა დუბლიკატის შექმნისას საწყისი მონაცემების სრულ სარეზერვო ასლს ქმნის. შეუძლებელია დუბლიკატის ინკრემენტული ან დიფერენციალური სარეზერვო ასლის სახით შექმნა, **TIB** ფორმატითაც კი.

სარეზერვო ასლების დუბლირებას მონაცემთა უსაფრთხოებისა და მოხერხებულობის გამო უფრო მეტი დრო სჭირდება, ვიდრე დუბლირების გარეშე სარეზერვო ასლის შექმნას, რადგანაც ჩვეულებრივ სარეზერვო კოპირება და დუბლიკატის შექმნა სრულდება თანმიმდევრულად და არა ერთდროულად.

მოსახსნელი ინფორმაციის მატარებლის პარამეტრების მომართვა

სარეზერვო ასლის შენახვამდე ინფორმაციის მოსახსნელ დამგროვებელზე (**Removable Storage**), ის უნდა გავხადოთ ჩამტვირთავი, რამდენიმე კომპონენტის დამატებით. რაც გვადლევს საშუალებას არ შევქმნათ ცალკე ჩამტვირთავი დისკი.

პარამეტრები, რომლებიც ხელმისაწვდომია ასარჩევად:

- ინფორმაციის მატარებელზე **True Image** -ის (სრული ვერსია) განთავსება.

True Image (სრული ვერსია) მხარს უჭერს **USB**, **PC**-ბარათებს (ადრინდელ **PCMCIA**) და **SCSI** ინტერფეისებს, ასევე მათზე მიერთებულ მონაცემთა შემნახველ მოწყობილობებს.

- ინფორმაციის მატარებელზე **Acronis System Report**- ის განთავსება

Acronis System Report - საშუალებას იძლევა შეიქმნას ანგარიში სისტემის მდგომარეობაზე, პროგრამულ უზრუნველყოფასთან დაკავშირებული პრობლემების შემთხვევაში. შეცდომების შესახებ ანგარიშის შექმნა შესაძლებელია **Acronis**-ის ჩამტვირთავი მატარებლიდან გაშვების წინ. შექმნილი სისტემური ანგარიშის შენახვა შესაძლებელია **USB**-ფლეშ დამგროვებელზე.

- **Place Acronis One-Click Restore on media**

მოდული **Acronis One-Click Restore** საშუალებას იძლევა ჩატვირთვა შესრულდეს ჩამტვირთავი დამგროვებლიდან და მოხდეს მონაცემთა აღდგენა მასზე არსებულ ასლზე მაუსის ერთი დაწკაპუნებით. ჩატვირთვისა და **Recover** დილაკზე დაჭერით მონაცემები დაუყოვნებლივ აღდგება ძველ ადგილას. აღდგენის რაიმე სახის პარამეტრების რედაქტირება, მაგალითად, აღსადგენი დანაყოფების ზომების შეცვლა, შეუძლებელია.

Acronis-ის სწრაფი აღდგენის მოდული შეიძლება დაემატოს ჩამტვირთავ მატარებელს მხოლოდ დისკის სარეზერვო ასლის ან დისკი ასლის (**Image**) შექმნისას. არ შეიძლება მისი დამატება ინკრემენტული ან დიფერენციალური სარეზერვო ასლის შექმნისას, ასევე დისკის დანაყოფის სარეზერვო ასლის შექმნისას.

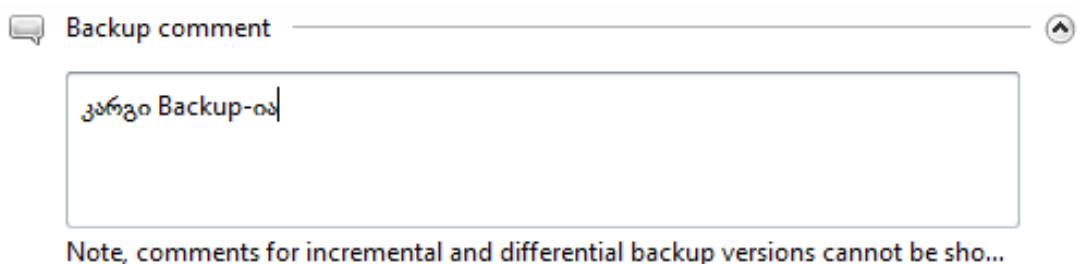
▪ **Ask for first media while creating backups on removable media**

აირჩიეთ, გამოიტანს თუ არა პროგრამა მოთხოვნას „**Insert First Media**” გადამტან მოწყობილობაზე სარეზერვო ასლის შექმნისას. ავტომატურად გადამტან მოწყობილობაზე არჩივის შექმნა მომხმარებლის გარეშე შეუძლებელია, რადგან პროგრამა ელოდება **OK** ღილაკზე დაჭერას, მოთხოვნის ფანჯარაში. ამიტომ განრიგის მიხედვით სარეზერვო ასლის შექმნის დაგეგმვისას გამორთეთ ეს ფუნქცია. იმ შემთხვევაში, როცა გადამტანი მოწყობილობა (მაგალითად, დისკი დევს დისკვანაში) ხელმისაწვდომია, ოპერაცია შესრულდება მომხმარებლის ჩარევის გარეშე.

თუ კომპიუტერზე **Acronis**-ის სხვა პროდუქტია დაყენებული, ამ პროგრამების ჩამტვირთავი ვერსიების კომპონენტების არჩევა შესაძლებელია მოცემულ ფანჯარაში.

კომენტარები სარეზერვო ასლებზე

ამ პარამეტრით შესაძლებელია კომენტარების დამატება სარეზერვო ასლებზე, რაც საშუალებას იძლევა გავარჩიოთ ერთმანეთისგან ასლები (ორი და მეტის არსებობის შემთხვევაში):

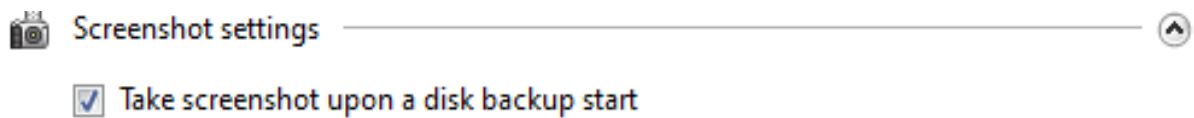


თუ სარეზერვო ასლებს არ აქვთ კომენტარები, შეიტანეთ ისინი შესაბამის ადგილას და დააჭირეთ **Save**-ს. თუ უკვე არსებობს ისინი, შესაძლებელია მათი შეცვლა **Edit** ღილაკზე დაჭერით. რედაქტირების დასრულების შემდეგ დააჭირეთ **Save** ღილაკს ცვლილების შესანახად.

კომენტარები ავტომატურად ენიჭება სარეზერვო ასლების ყველა ვერსიას. სარეზერვო ასლების გარკვეული ვერსიების კომენტარების შეცვლა შეიძლება სარეზერვო ასლების გამცილებლის (**Backup Explorer**) საშუალებით.

Screenshot (კადრის) პარამეტრები

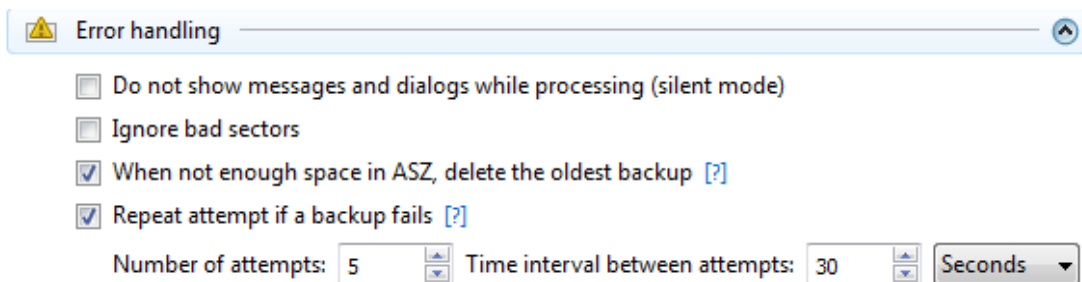
არქივებს კომენტარებთან ერთად, **Screenshot** ეხმარება მონაცემთა წინარე მდგომარეობის ამოცნობაში, რომელთა აღდგენა აუცილებელია. **True Image** იძლევა **Screenshot**-ის შექმნის საშუალებას დისკის ან დანაყოფის სარეზერვო ასლის გაშვების მომენტში. ამ პარამეტრის ჩასართავად, დააყენეთ ალაში **Take screenshot upon a disk backup start.**



Screenshot-ი აისახება სარეზერვო ასლების ბრაუზერის დისკებისა და დანაყოფების ჩანართში. ეკრანის ყოველი კადრი შეესაბამება დისკის ცალკეულ სარეზერვო ასლს. ამრიგად, სარეზერვო ასლების ვერსიებს შორის დროის შკალაზე გადასვლისას შესაძლებელია ეკრანის სხვადასხვა კადრების დანახვა და ამით სარეზერვო ასლებიდან საჭირო ვერსიის სწრაფი მონახვა.

შეცდომების დამუშავება (Error handling)

თუ პროგრამა სარეზერვო ასლების შექმნისას უშვებს შეცდომებს, პროცესი ჩერდება და გამოდის მომხმარებლის პასუხის მომლოდინე შეტყობინება იმის შესახებ, როგორ მოვიქცეთ ამ შეცდომის დროს. თუკი დაყენებულია შეცდომების დამუშავების პოლიტიკა, პროგრამა არ შეწყვეტს კოპირების პროცესს და არც შეტყობინებით გაგვაფრთხილებს შეცდომის შესახებ, მარტივად დაამუშავებს შეცდომას წესების არსებული ნაკრების შესაბამისად და გააგრძელებს მუშაობას:



შეცდომების დამუშავების პოლიტიკა:

▪ **Do not show messages and dialogs while processing (silent mode)** (ავტომატურად ამორთულია) - ჩართეთ ეს ფუნქცია, სარეზერვო ასლის შექმნისას შეცდომების იგნორირებისათვის. ეს შესაძლებლობა გამოიყენება ძირითადად მომხმარებლის გარეშე სარეზერვო ასლის შექმნისას, როცა შეუძლებელია კოპირების პროცესის გაკონტროლება. ამ რეჟიმში შეტყობინება ასლის შექმნისას წარმოქმნილი შეცდომების შესახებ არ გამოვა. ყველა ოპერაციის შესახებ დაწვრილებითი ანგარიშის ნახვა შესაძლებელია სარეზერვო ასლის შექმნის შემდეგ.

▪ **Ignore bad sectors** (ავტომატურად ამორთულია) - ეს რეჟიმი გამოიყენება მხოლოდ დისკებისა და დანაყოფების სარეზერვო ასლების შექმნისას. ის იძლევა სარეზერვო ასლის შექმნის საშუალებას მაშინაც კი, როცა მყარ დისკზე არსებობს დაზიანებული სექტორები. უმეტეს მყარ დისკებზე დაზიანებული სექტორები არ არის, მაგრამ ისინი შეიძლება გაჩნდეს მათი ექსპლუატაციის საკმაოდ დროის გასვლის შემდეგ. თუ მყარი დისკი გამოსცემს უცნაურ ხმებს (მაგალითად, ხმაურს მუშაობის დროს), ეს მის გამოუსწორებლობაზე მიუთითებს. მყარი დისკის მწყობრიდან სრულიად გამოსვლისას შეიძლება უმნიშვნელოვანესი მონაცემები დაიკარგოს, ამიტომ საჭიროა რაც შეიძლება სწრაფად შეიქმნას სარეზერვო ასლი. თუმცა ამ დროს შეიძლება შეიქმნას პრობლემა - დაშლის პირას მისულ დისკზე შეიძლება უკვე იყოს დაზიანებული სექტორები. თუ ჩართული არ არის **Ignore bad sectors**, წაკითხვის ან ჩაწერისას დაზიანებულ სექტორებზე შეცდომების არსებობისას, სარეზერვო ასლის შექმნა შეწყდება. მყარ დისკზე დაზიანებული სექტორების არსებობისას აღნიშნული ფუნქცია იძლევა სარეზერვო ასლის შექმნისა და რაც შეიძლება მეტი მოცულობის მყარი დისკის მონაცემების შენახვის საშუალებას.

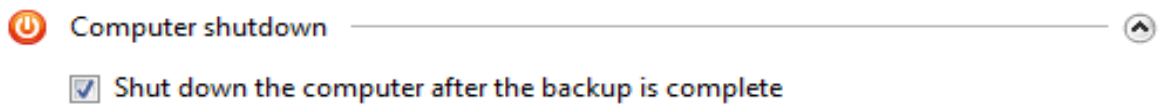
▪ **When not enough space in ASZ, delete the oldest backup** (ავტომატურად ჩართულია) - როცა ეს ფუნქცია ამორთულია და **Acronis**-ის უსაფრთხოების ზონაში არ არის საკმარისი ადგილი სარეზერვო ასლის ფაილისათვის, პროგრამა გამოიტანს დიალოგურ ფანჯარას, რომ დაცვის ზონა (**Secure Zone**) სავსეა და საჭიროა მომხმარებლის ჩარევა. სარეზერვო ასლის შექმნა შეწყდება მანამ, სანამ მომხმარებელი არ ამოირჩევს სასურველ მოქმედებას, ამის გამო შეუძლებელია სარეზერვო ასლის შექმნა მომხმარებლის გარეშე. ეს დიალოგური ფანჯარა გამოდის **Do not show messages and dialogs while processing (silent mode)** ფუნქციის ჩართვისას. ამიტომ მომხმარებლის გარეშე სარეზერვო ასლის შექმნის

განრიგის შედგენისას **Acronis**-ის უსაფრთხოების ზონაში ჩართეთ **When not enough space in ASZ, delete the oldest backup** ფუნქცია.

▪ **Repeat attempt if a backup fails** - ამ პარამეტრით შესაძლებელია სარეზერვო ასლის შექმნის მცდელობის გამეორება, თუკი რაიმე მიზეზით მისი შესრულება ვერ მოხერხდება. ამ პარამეტრის მომართვა ითვალისწინებს ორ მნიშვნელობას - მცდელობის რაოდენობას და დროის ინტერვალს მცდელობათა შორის. ამ პარამეტრების საშუალებით, **Acronis**-ი შეეცდება შექმნას სარეზერვო ასლი მანამ, სანამ წარმატებით არ დაასრულებს ოპერაციას. მაგრამ თუ შეცდომა, რომელიც ელოდება სარეზერვო ასლის შექმნას, არ გაქრება, სარეზერვო ასლი არ შეიქმნება.

კომპიუტერის გამორთვა

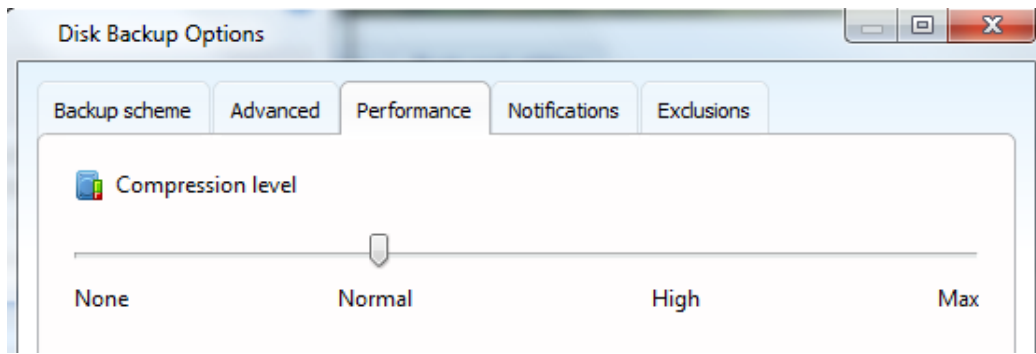
თუ ცნობილია, რომ დაგეგმილი სარეზერვო ასლის შექმნას დიდი დრო დასჭირდება, ჩართეთ **Shut down the computer after the backup is complete** ფუნქცია. ამ შემთხვევაში არ არის საჭირო ოპერაციის დასრულების მოლოდინი. პროგრამა შეასრულებს დაგეგმილ სარეზერვო ასლის შექმნას და ავტომატურად გამორთავს კომპიუტერს.



ეს პარამეტრი ხელსაყრელია სარეზერვო ასლის შექმნის დაგეგმისთვისაც. მაგალითად, საჭიროა სარეზერვო ასლის შექმნა სადამოკებით ყოველ სამუშაო დღეს მთელი სამუშაოს შესანახად. დაგეგმეთ სარეზერვო ასლის შექმნა და დააყენეთ ალამი. ამ შემთხვევაში შეიძლება სამუშაოს დასრულება და წასვლა, თან გეცოდინება, რომ შეიქმნება ძალიან მნიშვნელოვანი ინფორმაციის სარეზერვო ასლები და მერე კომპიუტერიც გაითიშება.

სარეზერვო ასლის ოპერაციის წარმადობა

Performance ჩანართიდან შეიძლება შემდეგი პარამეტრების დაყენება:

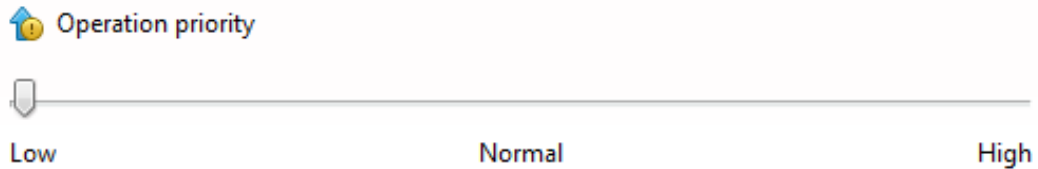


- **None** - მონაცემები დაკოპირდება შეკუმშვის გარეშე, რაც არსებითად გაზრდის სარეზერვო ასლის ფაილის ზომას.
- **Normal** - მონაცემთა შეკუმშვის რეკომენდებული დონე (ავტომატურად ჩართული).
- **High** - შეკუმშვის უფრო მაღალი დონე, სარეზერვო ასლის შესაქმნელად საჭირო ხანგრძლივი დროით.
- **Maximum** - შეკუმშვის მაქსიმალური დონე, სარეზერვო ასლის შესაქმნელად საჭირო მაქსიმალურად ხანგრძლივი დრო.

მონაცემთა შეკუმშვის ოპტიმალური დონე დამოკიდებულია ფაილების ტიპზე, რომლებიც სარეზერვო ასლში ინახება. მაგალითად, შეკუმშვის მაქსიმალური დონეც კი უმნიშვნელოდ შეამცირებს იმ სარეზერვო ასლების ზომას, თუკი ისინი შეიცავს თავიდანვე შეკუმშულ ფაილებს, ისეთებს როგორცაა **JPG, PDF** ან **MP3**.

ოპერაციის პრიორიტეტები

სარეზერვო ასლის შექმნის ან აღდგენის ოპერაციის პრიორიტეტის შეცვლამ შეიძლება დააჩქაროს ან შეანელოს პროცესი (იმისდა მიხედვით, პრიორიტეტი გაიზარდა თუ შემცირდა), ასევე არსებით ზეგავლენას ახდენს სხვა შემსრულებელი პროგრამების წარმადობაზე. სისტემაში გავლილი ყოველი პროცესის პრიორიტეტი განისაზღვრება ამ პროცესისთვის გამოყოფილი სისტემური რესურსებისა და პროცესორული დროის წილით. ოპერაციის პრიორიტეტის შემცირება გამოათავისუფლებს რესურსებს კომპიუტერის მიერ სხვა ამოცანისათვის შესასრულებლად. სარეზერვო ასლის შექმნის ან აღდგენის პრიორიტეტის გაზრდა, პირიქით, დააჩქარებს პროცესს პარალელური ამოცანების რესურსების მითვისების ხარჯზე. თუ რამდენად გამოვლინდება ეს ეფექტი, დამოკიდებულია პროცესის საერთო დატვირთვასა და სხვა ფაქტორებზე:



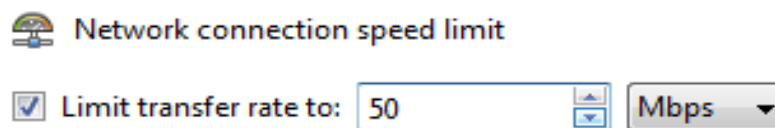
ოპერაციების პრიორიტეტები

- **Low** (ავტომატურად არჩეული) - სარეზერვო ასლის შექმნის ან აღდგენის პროცესი შესრულდება ნელა, მაგრამ სხვა პროცესების შესრულების სიჩქარე იქნება მაღალი.
- **Normal** - სარეზერვო ასლის შექმნის ან აღდგენის პროცესი შესრულდება პრიორიტეტით, რომელიც შეესაბამება სისტემის სხვა პროცესების პრიორიტეტებს.
- **High** - სარეზერვო ასლის შექმნის ან აღდგენის პროცესი შესრულდება სწრაფად სხვა პროცესების წარმადობის შემცირების ხარჯზე. ამ ვარიანტის არჩევისას **Acronis**-მა შეიძლება გამოიყენოს კომპიუტერის რესურსების 100%.

ქსელური მიერთების სიჩქარე

ქსელურ დისკებსა და **FTP**-სერვერზე სარეზერვო ასლების ხშირად შექმნისას რეკომენდებულია შეიზღუდოს **Acronis** -ის მიერ გამოყენებული ქსელის გატარების უნარი.

შეიყვანეთ ქსელში ინფორმაციის სარეზერვო ასლის გადაცემის სიჩქარის შეზღუდვა (კილობაიტ/წამებში).



შეტყობინება სარეზერვო ასლის შექმნისას

ზოგჯერ სარეზერვო ასლის შექმნა ან აღდგენა შეიძლება გაგრძელდეს ერთ საათს ან მეტხანს. **True Image** ოპერაციის დასრულება შესაძლებელია ელფოსტით გვაცნობოს. ასევე შეიძლება გაიგზავნოს შეტყობინების დუბლიკატი, რომელიც პროგრამის მუშაობის პროცესში გამოვა და ასევე ოპერაციის სრული ჟურნალი მისი დასრულების შემდეგ.

ავტომატურად ნებისმიერი შეტყობინების გაგზავნა გამორთულია.

დისკური სივრცის მოცულობის თავისუფალი ზღვარი

შეტყობინების მიღება მომართეთ მაშინ, როცა სარეზერვო ასლების საცავში თავისუფალი ადგილი შემცირდება იმაზე მეტად, ვიდრე მითითებული ზღვრული მნიშვნელობა. თუ სარეზერვო ასლის შექმნის დაწყების შემდეგ **True Image** აღმოაჩენს, რომ თავისუფალი სივრცე სარეზერვო ასლისთვის არჩეულ საცავში მცირეა, ვიდრე მითითებული იყო, პროგრამა არ დაიწყებს სარეზერვო ასლის შექმნის პროცესს, მაგრამ დაუყოვნებლივ შეგატყობინებთ ამის შესახებ, შესაბამისი შეტყობინების გამოტანით. ასეთი შეტყობინება გვთვავობს მოქმედების სამ ვარიანტს: იგნორირება და სარეზერვო ასლის შექმნის გაგრძელება, სხვა შესაძლებელი ადგილის არჩევა ან სარეზერვო ასლის შექმნის შეწყვეტა.

თუ თავისუფალი სივრცე შემცირდება მითითებულ მნიშვნელობასთან შედარებით სარეზერვო ასლის შექმნის პროცესში, პროგრამა მოგვაწვდის ასეთსავე შეტყობინებას და მოგვთხოვს ერთ–ერთი გადაწყვეტილების მიღებას.

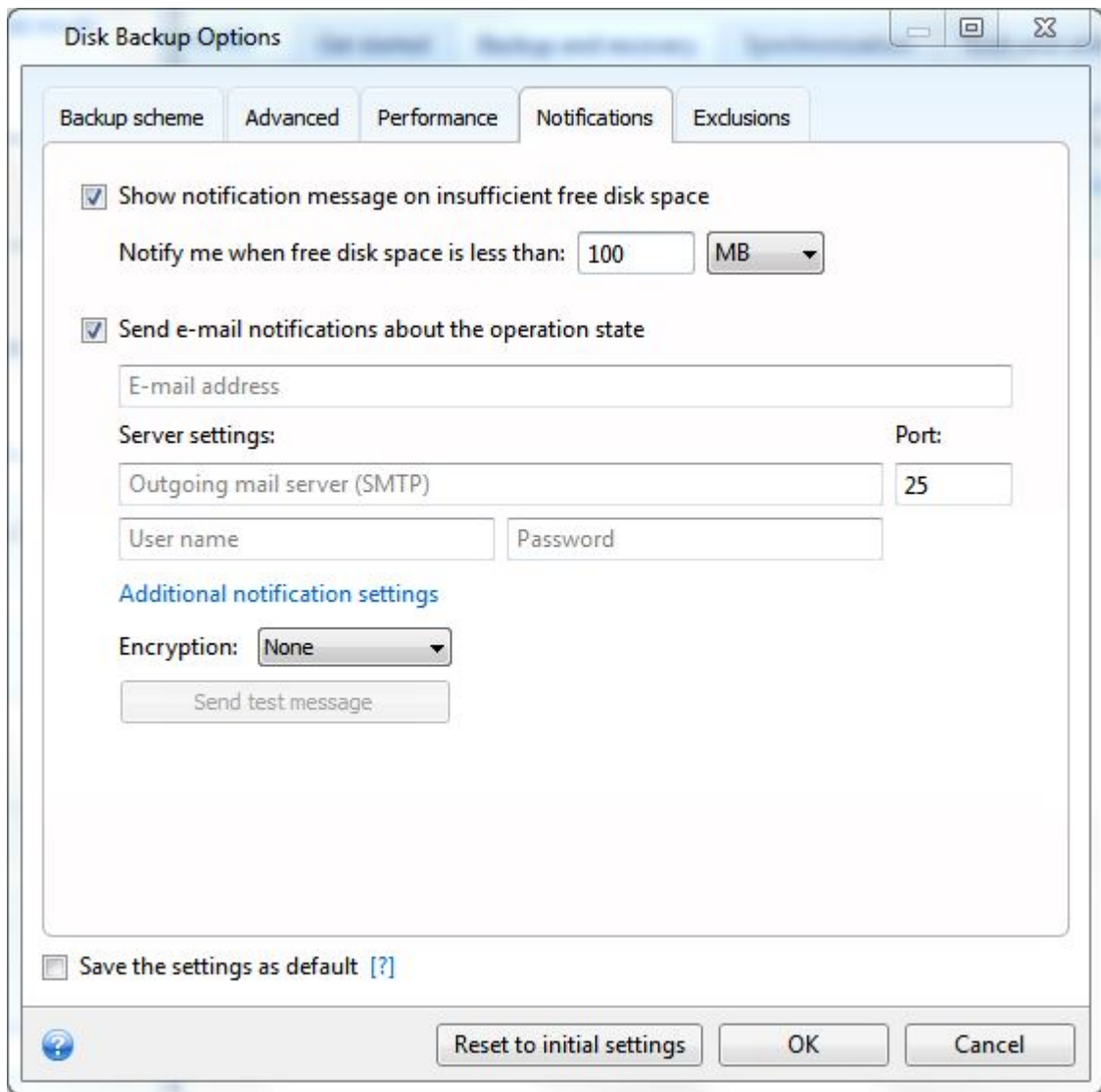
Acronis–ს შეუძლია მოიძიოს თავისუფალი სივრცე შენახვის შემდეგ მოწყობილობებზე:

- ლოკალური მყარი დისკები;
- **USB** ინტერფეისიანი დისკვამყვანები და დამგროვებლები;
- ქსელური რესურსები (**SMB/NFS**).

*შეტყობინება თავისუფალი სივრცის ზღვრთან მიახლოების შესახებ არ გამოვა, თუ პარამეტრებში **Error handling** დაყენებულია ალამი **Do not show messages and dialogs while processing (silent mode)**. შეტყობინება თავისუფალი სივრცის ზღვრთან მიახლოების შესახებ არ მუშაობს **FTP**–სერვერის და **CD/DVD**–დისკებისთვის.*

შეტყობინება ელექტრონულ ფოსტით

მიუთითეთ საადრიცხვო ჩანაწერი ელფოსტის, რომელიც სარეზერვო ასლის შექმნის შედეგების შესახებ შეტყობინების მისაღებად იქნება გამოყენებული.



ელფოსტის პარამეტრების მისათითებლად –

- აირჩიეთ ალამი **Send e-mail notifications about the operation state** შეიყვანეთ ელფოსტის მისამართი ველში **E-mail address** რამდენიმე მისამართი გამოყავით წერტილ-მძიმით.

- მიუთითეთ გამავალი ფოსტის სერვერი (SMTP) ველში **Outgoing mail server (SMTP)**

- გამავალი ფოსტისთვის მიუთითეთ საფოსტო სერვერის პორტი. ავტომატურად გამოიყენება პორტი 25.

- შეიყვანეთ მომხმარებლის სახელი ველში **User name**

- შეიყვანეთ პაროლი ველში **Password**

- პარამეტრების სისწორის შესამოწმებლად დააჭირეთ ღილაკს **Send test message**

შეტყობინების დამატებითი პარამეტრები:

- პროცესის დასრულების შესახებ შეტყობინების გასაგზავნად დააყენეთ ალამი **Send notification upon operation's successful completion;**

- პროცესის ჩავარდნის შემთხვევაში შეტყობინების გასაგზავნად დააყენეთ ალამი **Send notification upon operation failure;**

- ოპერაციის შესახებ შეტყობინებებიანი გზავნილის გასაგზავნად დააყენეთ ალამი **notification when user interaction is required;**

- ოპერაციის სრულ ჟურნალთან ერთად გზავნილის გადასაცემად დააყენეთ ალამი **Add full log to the notification.**

სარეზერვო ასლიდან ელემენტების ამოღება

გამოუსადეგარი ფაილების სარეზერვო ასლიდან ამოსაღებად საჭიროა შესაბამისი ფაილების მითითება სარეზერვო ასლის პარამეტრების ფანჯრის ჩანართში **Disk and partitions backup**. ამოკლების მითითება შესაძლებელია განყოფილებებში **File Backup** ან **Online Backup**.

ავტომატური პარამეტრების გამოყენება

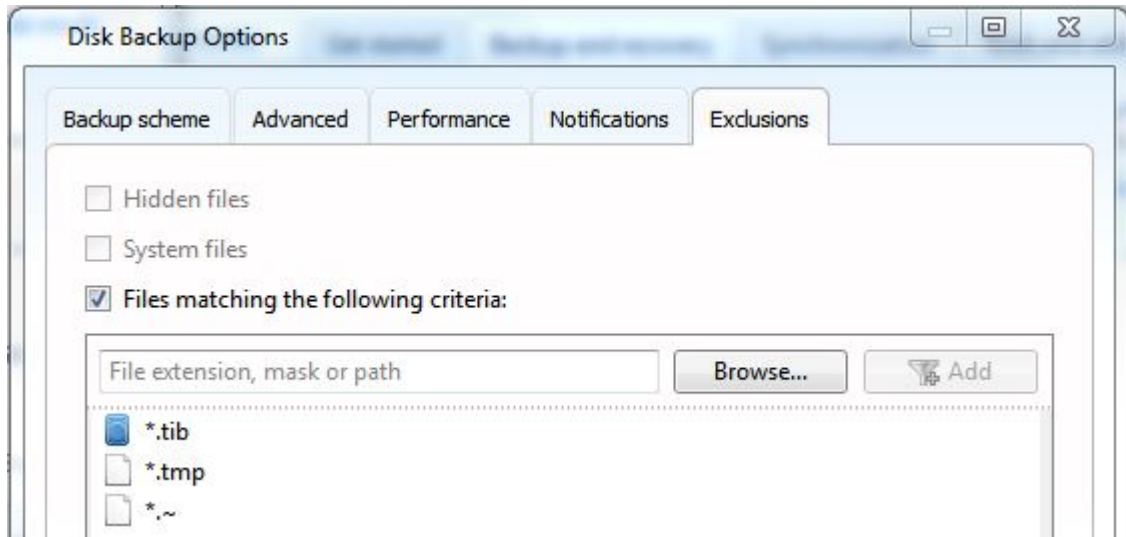
ამოკლების ყველა პარამეტრისთვის, ჩანართის მომართვის შემდეგ არჩეულია თავდაპირველი მნიშვნელობა. ამ პარამეტრების შეცვლა შესაძლებელია მხოლოდ სარეზერვო ასლის შექმნის მიმდინარე ოპერაციის შესრულების დროს ან ყველა სხვა მომდევნო ოპერაციისას. დააყენეთ ალამი **Save as default**, სარეზერვო ასლის ყველა მომდევნო ოპერაციის პარამეტრების ავტომატურად შესაცვლელად. პროდუქტის დაყენებისას მომართული თავდაპირველი მნიშვნელობის დასაბრუნებლად დააჭირეთ ღილაკს **Reset to initial settings**.

რა და როგორ უნდა ამოვაკლოთ

1. სარეზერვო ასლიდან შეიძლება ამოვრიცხოთ ფარული და სისტემური ფაილები (სისტემური დანაყოფების სარეზერვო ასლების ფარული და სისტემური ფაილების გარდა), შესაბამისი ალმების დაყენებით.

2. შეიძლება ამოირიცხოს ფაილები, რომლებიც ესადაგება გარკვეულ კრიტერიუმს. ამისათვის დააყენეთ ალამი **Files matching the following criteria**, შეიყვანეთ გამონაკლისი კრიტერიუმი, ამის შემდეგ დააჭირეთ ღილაკს **Add**.

პროგრამა სარეზერვო ასლებიდან ავტომატურად აგდებს ფაილებს ~, TMP, TIB გაფართოებით:



ამოირიცხვის კრიტერიუმის დამატება

- სარეზერვო ასლიდან ამოსარიცხი ფაილის სახელი შეიძლება მიეთითოს სრულად:
- **file.ext** – ყველა ფაილი ამ სახელწოდებითა და გაფართოებით ამოვარდება
- **c:\file.ext** - C: დისკის ფაილი **file.ext** ამოვარდება.
- შეიძლება ჩასასმელი ნიშნების გამოყენება (* და ?):
- ***.ext** - ყველა ფაილი **.ext** გაფართოებით გამოირიცხება.
- **??name.ext** - გამოირიცხება ყველა ფაილი **.ext** გაფართოებით, რომელთა სახელი ექვსი ასოსაგან შედგება (რომელიც ნებისმიერი ორი სიმბოლოთი იწყება (??) და მთავრდება **name**-ით).
- საქაღალდის ამოსარიცხად დააჭირეთ ღილას **Browse**, აირჩიეთ ამოსაკლები საქაღალდე, დააჭირეთ **OK**, შემდეგ კი ღილაკს **OK**

კრიტერიუმების ამოსაკლებად, მაგალითად შეცდომით დამატებული, დააჭირეთ ნიშანს „Add“ კრიტერიუმის მარჯვნივ.

Windows-ის სააღრიცხვო ჩანაწერი

სარეზერვო ასლის შექმნისას შეიძლება **Windows**-ის სააღრიცხვო ჩანაწერის შექმნა, რომლის სახელითაც შესრულდება სარეზერვო ასლის შექმნის ოპერაცია. ეს იმ

შემთხვევაშია გამოსაყენებელი, როცა კომპიუტერით სხვაც სარგებლობს. ამ შემთხვევაში ხშირად თითოეულ მომხმარებელს აქვს თავისი საკუთარი დოკუმენტები, ელფოსტის სააღრიცხვო ჩანაწერები, პარამეტრები და სხვა პირადი მონაცემები. ავტომატურად **True Image** მიმდინარე მომხმარებელის მონაცემთა სარეზერვო ასლების კოპირებას ახდენს. მიზანშეწონილია ამ მომართვის შეცვლა, თუ მოცემულ მომენტში მომხმარებელი შევიდა სხვისი სააღრიცხვო ჩანაწერით. პროგრამა ქმნის მხოლოდ იმ მონაცემთა სარეზერვო ასლს, რომლებიც ეხება მოცემულ სააღრიცხვო ჩანაწერს. სხვა სააღრიცხვო ჩანაწერების მონაცემების ასლების შექმნა არ მოხდება.

მონაცემთა აღდგენა

სარეზერვო ასლის შექმნის მიზანი სარეზერვო ასლიდან მონაცემთა აღდგენაა იმ შემთხვევაში, თუ რაიმე მიზეზით თავდაპირველი ფაილი დაზიანდა, მაგალითად ფაილის შემთხვევით წაშლა, მოწყობილობის მწყობრიდან გამოსვლა, ხანძარი ან ქურდობა.

თუ მონაცემთა სარეზერვო ასლები **True Image** –ით შექმენით, არაფერი დაიკარგება.

სისტემის აღდგენა ავარიის შემდეგ

თუ კომპიუტერი არ იტვირთება, ეცადეთ ჯერ მონახოთ ამის მიზეზი. თუ მწყობრიდან გამოსვლა ოპერაციული სისტემის გამო მოხდა, გამოიყენეთ სარეზერვო ასლი სისტემის აღსადგენად. მოემზადეთ აღდგენისათვის და შეუდექით სისტემის აღდგენას.

გაუმართაობის მიზეზის დადგენა

სისტემის საავარიო გაუმართაობა გამოწვეული შეიძლება იყოს ორი მიზეზით. პირველი შესაძლო მიზეზი – მოწყობილობის გაუმართაობა. მეორე – დაზიანებულია ოპერაციული სისტემა, **Windows** არ იტვირთება.

პირველ შემთხვევაში უმჯობესია თუ აღდგენით სამუშაოებს ჩაატარებს სერვის-ცენტრი. თუმცა შესაძლებელია გარკვეული სტანდარტული ტესტის ჩატარება. შეამოწმეთ კაბელები, გასართი, გარემოწყობილობების კვება და სხვა. შემდეგ გადატვირთეთ კომპიუტერი. თვითტესტირების პროცედურა **POST**-ის (**Power-On Self Test**) კვების ჩართვისას, რომელიც კომპიუტერის ჩართვისთანავე გაიშვება, უზრუნველყოფს მოწყობილობის სისტემის შემოწმებას. თუ პროცედურის დროს **POST** მოწყობილობა გაჩერდება, მოგვიწვეს კომპიუტერის სერვის-ცენტრში მიტანა.

თუ **POST** არ აღმოაჩენს მოწყობილობის ხარვეზებს, შევა სისტემა **BIOS** და შეამოწმებს, ხედავს თუ არა სისტემა მყარ დისკს. **BIOS**-ში შესასვლელად, დააჭირეთ კლავიშთა შესაბამის კომბინაციას (**Del**, **F1**, **Ctrl+Alt+Esc**, **Ctrl+Esc** ან სხვას **BIOS**-ის ტიპის მიხედვით) **POST** პროცედურის შესრულების დროს. როგორც წესი, კლავიშთა მოთხოვნილი კომბინაცია აისახება კომპიუტერის ჩართვისთანავე. ამ კლავიშებზე დაჭერით შევდივართ პარამეტრების მენიუში. გადადით მყარი დისკის ავტომატურად აღმოჩენ უტილიტზე, რომელიც ჩვეულებრივ „**CMOS** სტანდარტულ პარამეტრებში“ ან „**CMOS**-ს გაფართოებული პარამეტრებშია მოთავსებული. თუ უტილიტი ვერ აღმოაჩენს

სისტემურ დისკს, ეს ნიშნავს სისტემური დისკის დაზიანებას და საჭიროა მისი გამოცვლა.

თუ უტილიტმა სწორად აღმოაჩინა სისტემური მყარი დისკი, მაშინ ავარიული გათიშვა შეიძლება გამოწვეული იყოს ვირუსის, მავნე პროგრამის ან ჩატვირთვისათვის საჭირო სისტემური ფაილის დაზიანების გამო.

თუ სისტემური დისკი მუშაუნარიანია, მაშინ ვცადოთ სისტემის აღდგენა სისტემური დისკის ან სისტემური დანაყოფის სარეზერვო ასლიდან. რადგან **Windows** არ იტვირთება, მოგვიწვევს **Acronis** ჩამტვირთავი მატარებლის გამოყენება.

დაზიანებული მყარი დისკის შეცვლის შემდეგაც ასევე საჭიროა სისტემის აღმდგენი სისტემური დისკის სარეზერვო ასლი.

აღდგენისათვის მომზადება

ა) დაასკანირეთ კომპიუტერი ვირუსზე, თუ არსებობს ეჭვი, რომ ავარიული გათიშვა მოხდა ვირუსის ან მავნე პროგრამების შეტევის შედეგად მოხდა.

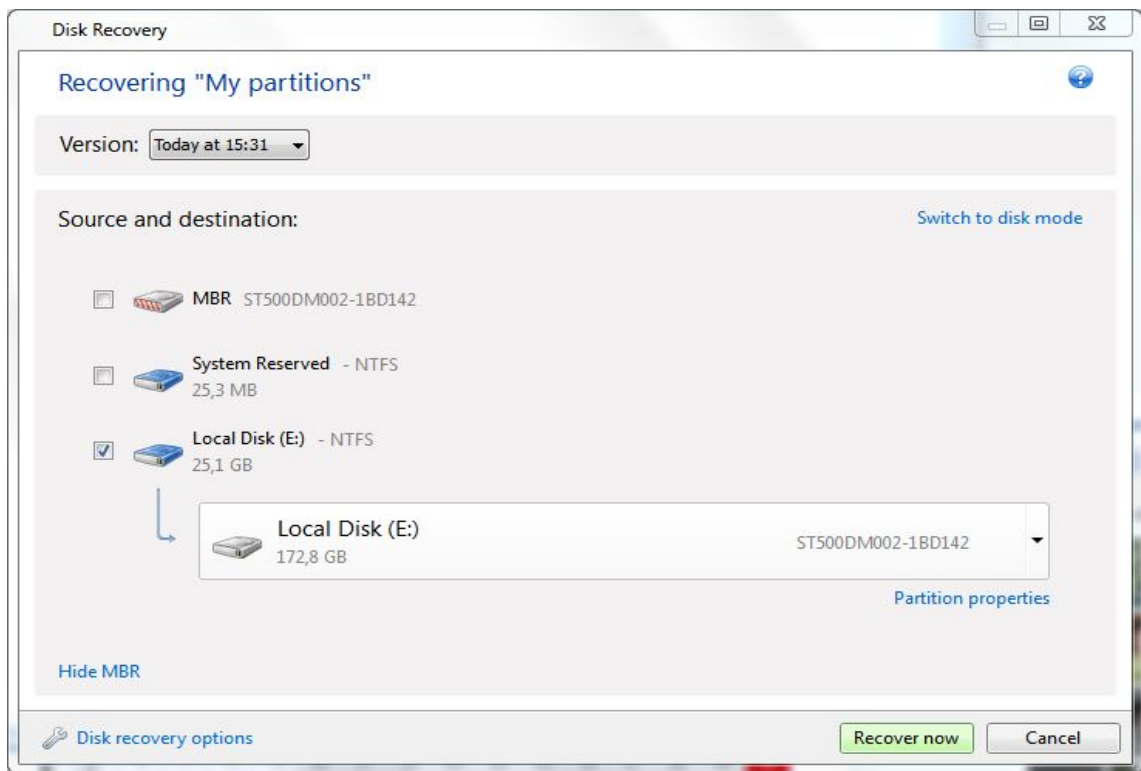
ბ) ჩაიტვირთეთ მატარებლიდან, შეამოწმეთ აღსადგენი სარეზერვო ასლი მთლიანობაზე. ეს აუცილებელია, რადგან სარეზერვო ასლის შემოწმების დროს პროგრამის აღდგენის პირობებში ზოგჯერ მასში აღმოაჩენს ხოლმე დაზიანებებს, მიუხედავად იმისა, რომ ასლმა შემოწმება **Windows**-ში წარმატებით გაიარა. შეიძლება მიზეზი ისაა, რომ **True Image OS Windows**-ში და აღდგენის გარემოში გამოიყენებს მოწყობილობათა სხვადასხვა დრაივერებს. თუ **True Image** აღმოაჩენს დაზიანებებს სარეზერვო ასლში, აღდგენა ვერ გაგრძელდება.

დისკებისა და დანაყოფების აღდგენა

დისკებისა და დანაყოფების აღდგენა ასლიდან შეიძლება მოხდეს როგორც ჩანართიდან **Backup and recovery**, ისე **Acronis**-ის სარეზერვო ასლის ბრაუზერიდან **Acronis Backup Explorer**-იდან. **Backup and recovery** ჩანართიდან აღდგენის გასაშვებად, დააყენეთ ალამი აღსადგენი დანაყოფის ასლის შემცველ სარეზერვო ასლის გასწვრივ. დააჭირეთ ღილაკზე **Recover** (ან ნიშანზე **Recover**, თუ სარეზერვო ასლის პანელი ჩაკეცილია). გაიხსნება ფანჯარა „დისკის აღდგენა“.

თუ საჭიროა დანაყოფის აღდგენა წარსული დროის რაიმე თარიღის მიხედვით, დააჭირეთ სამკუთხა ნიშნაკზე **Operations** მენიუში და აირჩიეთ ბრძანება **Explore and**

recover. გამოვა სარეზერვო ასლის ბრაუზერი, საიდანაც შეგვიძლია შესაბამის დროში შექმნილი ასლის ვერსიის არჩევა. საჭირო ვერსიის არჩევის შემდეგ დააჭირეთ ღილაკს **Recover** და გამოვა ფანჯარა **Explore and recover.**



1. დააყენეთ ალამი აღსადგენი დანაყოფის გასწვრივ.

თუ მთელი დისკის სარეზერვო ასლია შექმნილი, შესაძლებელია მთელი დისკის აღდგენის არჩევა, **Switch to disk mode** დაჭერით. დანაყოფების ასარჩევ გრაფაში დასაბრუნებლად დააჭირეთ **Switch to partition mode**.

2. აღდგენის გზის ველში დანაყოფის სახელით აირჩიეთ მთელი დანაყოფი. დანაყოფები, რომელზეც მოთავსდება აღდგენილი დანაყოფი, ინიშნება შავი ასოებით. ხოლო სხვა დანაყოფები ინიშნება წითელი ასოებით. მთელ დანაყოფზე ყველა მონაცემი იკარგება, რადგან აღდგენილი მონაცემებითა და სისტემური ფაილებით ხდება ხდება მათი ჩანაცვლება.

იმისათვის, რომ ასლი აღდგეს საწყის დანაყოფზე ზომის შეცვლის გარეშე, ამისათვის ამ დანაყოფში თავისუფალი ადგილი უნდა იყოს არანაკლებ 5%-ისა. წინააღმდეგ შემთხვევაში ღილაკი **Recover now** მიუწვდომელი იქნება.

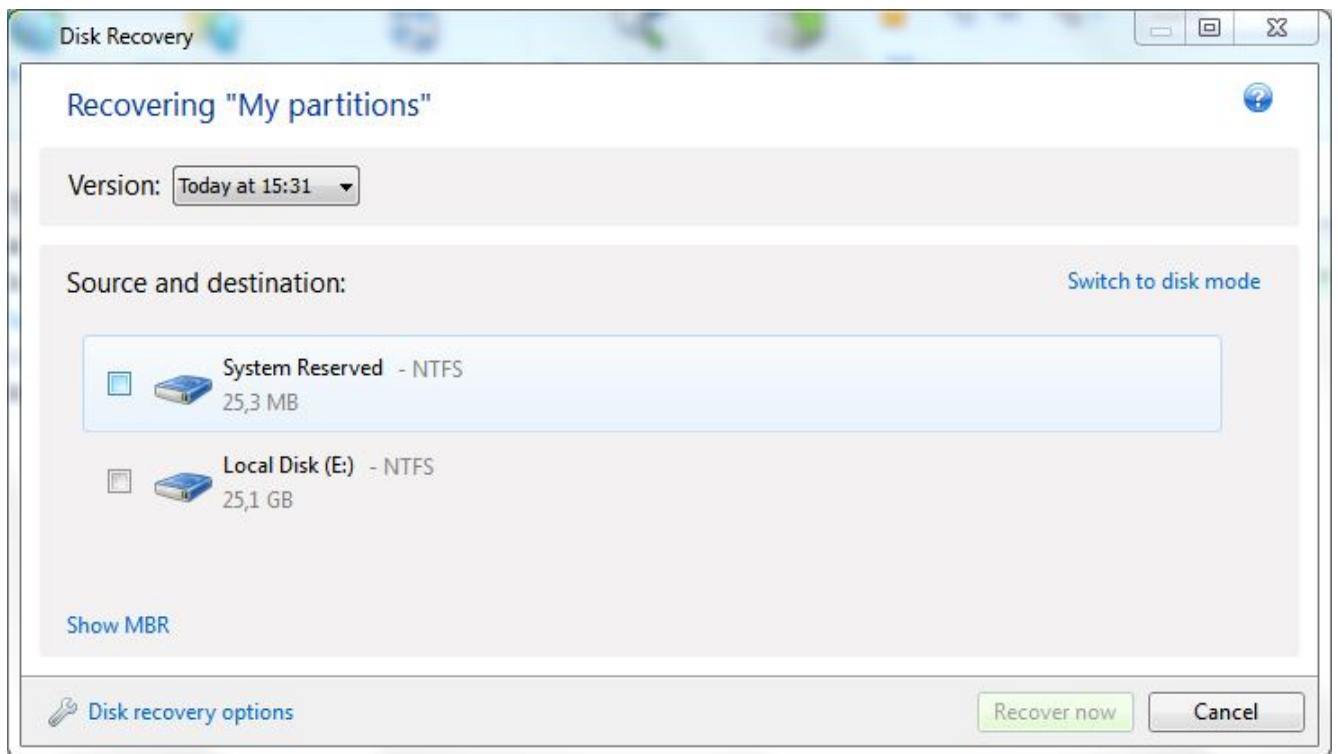
3. არჩევის დასრულების შემდეგ, აღდგენის დასაწყებად დააჭირეთ ღილას **Recover now**.

ზოგჯერ საჭიროა ძირითადი ჩამთვირთავი ჩანაწერის (MBR) აღდგენა. ეს საჭიროა მაგალითად მაშინ, როცა აღდგენის შემდეგ OS Windows არ იტვირთება. MBR-ის აღსადგენად დააჭირეთ **Show MBR** ღილაკს და ჩააყენეთ ალამი MBR.

ერთდროულად რამდენიმე დანაყოფის აღდგენა

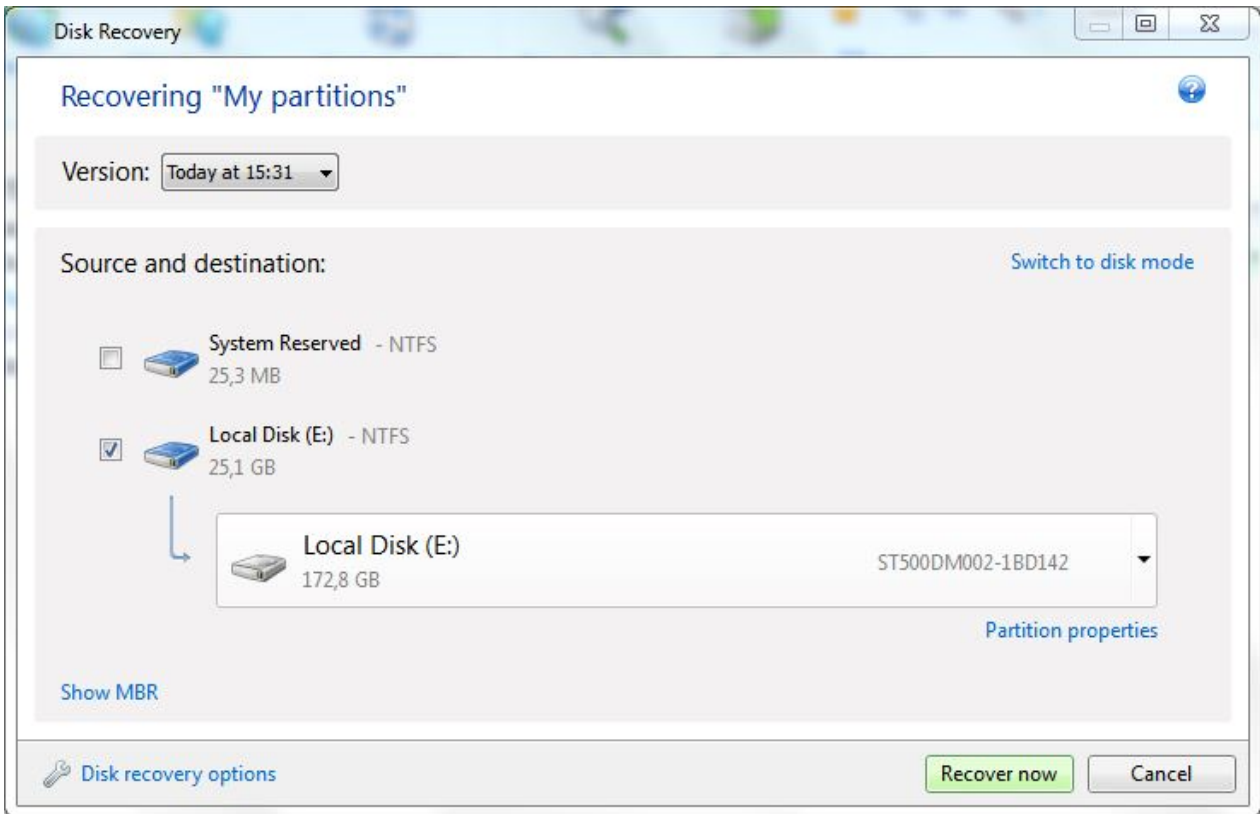
ქვემოთ მოცემულია ორი დანაყოფის აღდგენის მაგალითი. თუ სარეზერვო ასლში შესულია ორზე მეტი დანაყოფი, აღდგენის პროცედურა იქნება ანალოგიური.

1. Acronis პროგრამის **Backup and recovery** ჩანართში დააჭირეთ ღილაკს **Recover**. შემდეგ აირჩიეთ ის სარეზერვო ასლი, რომელიც შეიცავს რამდენიმე დანაყოფს და ისევ **Recover**. გამოვა **Disk Recovery** ფანჯარა:

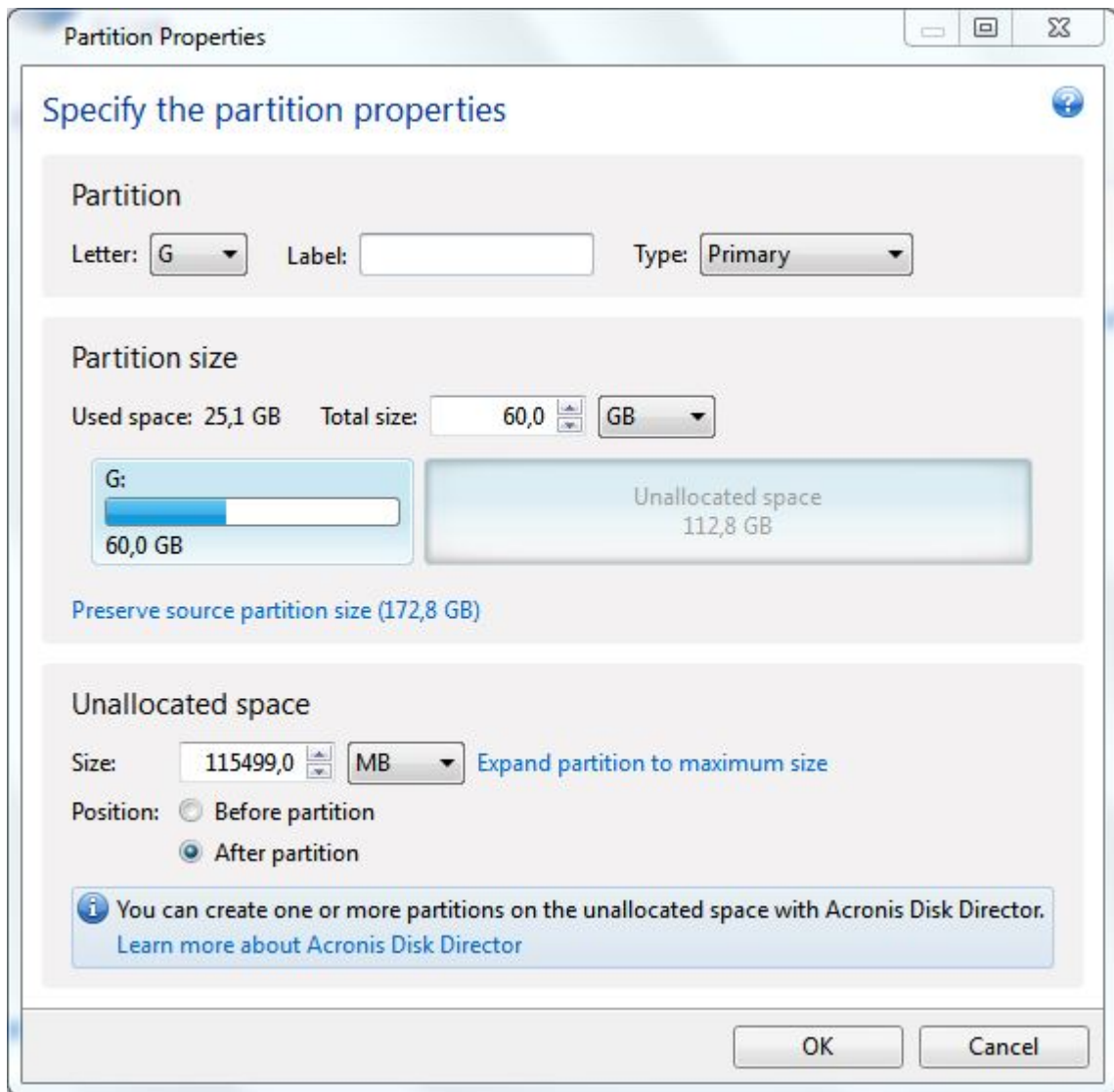


2. ფანჯრის ზედა მარცხენა კუთხეში დააჭირეთ **Version** ელემენტის გასწვრივ მდებარე სამკუთხა ღილაკს და თარიღისა და დროის მიხედვით აირჩიეთ ის სარეზერვო ასლი, რომელიც გვინდა რომ აღვადგინოთ.

3. აირჩიეთ დანაყოფი, რომლის აღდგენაც უნდა მოხდეს. დანაყოფის დასახელებაზე ან ზომაზე დაჭერით ჩამოიშლება მენიუ, საიდანაც მიეთითება აღდგენის ადგილი.



4. დაჭირეთ სამკუთხა ღილაკს და აირჩიეთ სამიზნე მყარი დისკი. აღსადგენი დანაყოფი ჩაიწერება არჩეულ ლოგიკურ დისკზე. ის მოიცავს ყველა ხელმისაწვდომ დისკურ სივრცეს. იმისათვის რომ შევამციროთ დანაყოფის ზომა და დავტოვოთ საკმარისი დისკური სივრცე დანარჩენი დანაყოფებისთვის, დაჭირეთ **Partition properties** მიმართვას. გაიხსნება შესაბამისი ფანჯარა:



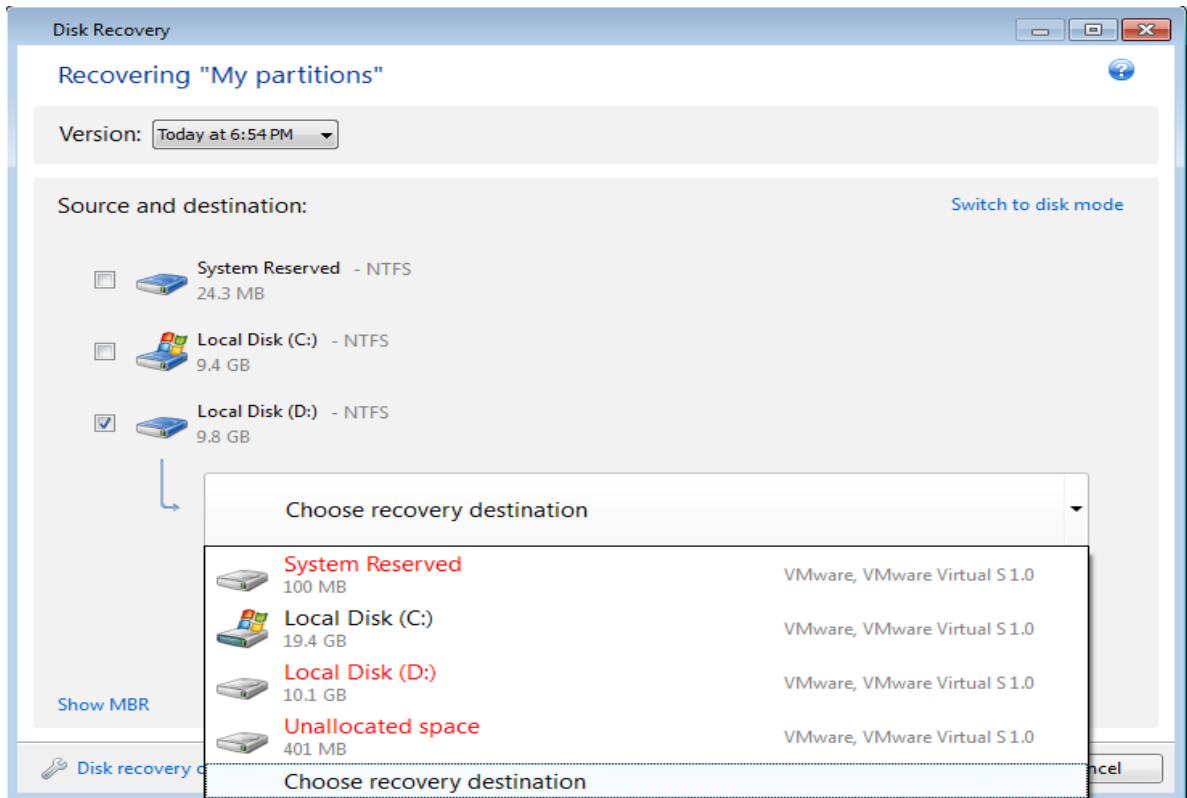
5. დანაყოფის ზომის შესაცვლელად დააწეკით მაუსის მარცხენა ღილაკს მის ბოლოში და ხელის აუღებლად გადაადგილეთ მარცხნივ საჭირო ზომამდე.

დანაყოფის განსაზღვრული ზომის მისათითებლად, შეიყვანეთ საჭირო რიცხვი **Total size** ველში.

დანაყოფის ზომის ცვლილების შემდეგ აუცილებლად დატოვეთ იმდენი თავისუფალი სივრცე, რამდენიც საჭიროა დარჩენილი დანაყოფისთვის. აირჩიეთ დისკის ასოთი დასახელება და დანაყოფის ტიპი. როცა პარამეტრები იქნება მითითებული, დააჭირეთ **OK** ღილაკს, რითაც დადასტურებთ ცვლილებებს და დაბრუნდებით **Disk Recovery** ფანჯარაში.

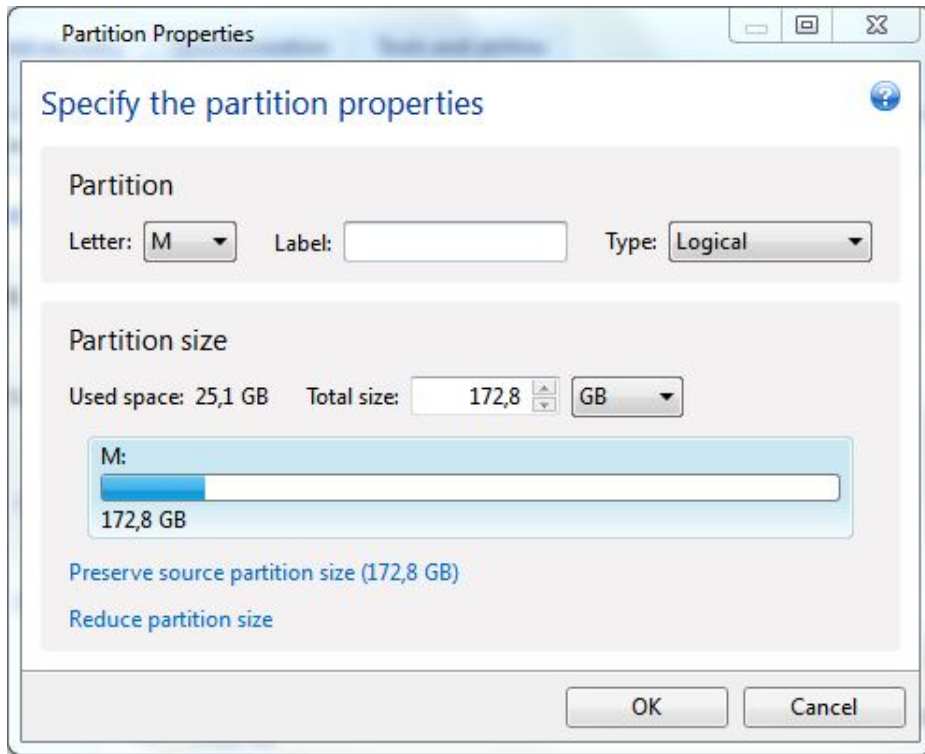
6. დააყენეთ ალამი მომდევნო დანაყოფზე.

7. აირჩიეთ დაუყოფელი სივრცე მთელს მყარ დისკზე. პროგრამა შექმნის დანაყოფს, რომელიც მოიცავს ყველა დაუმისამართებელ სივრცეს.

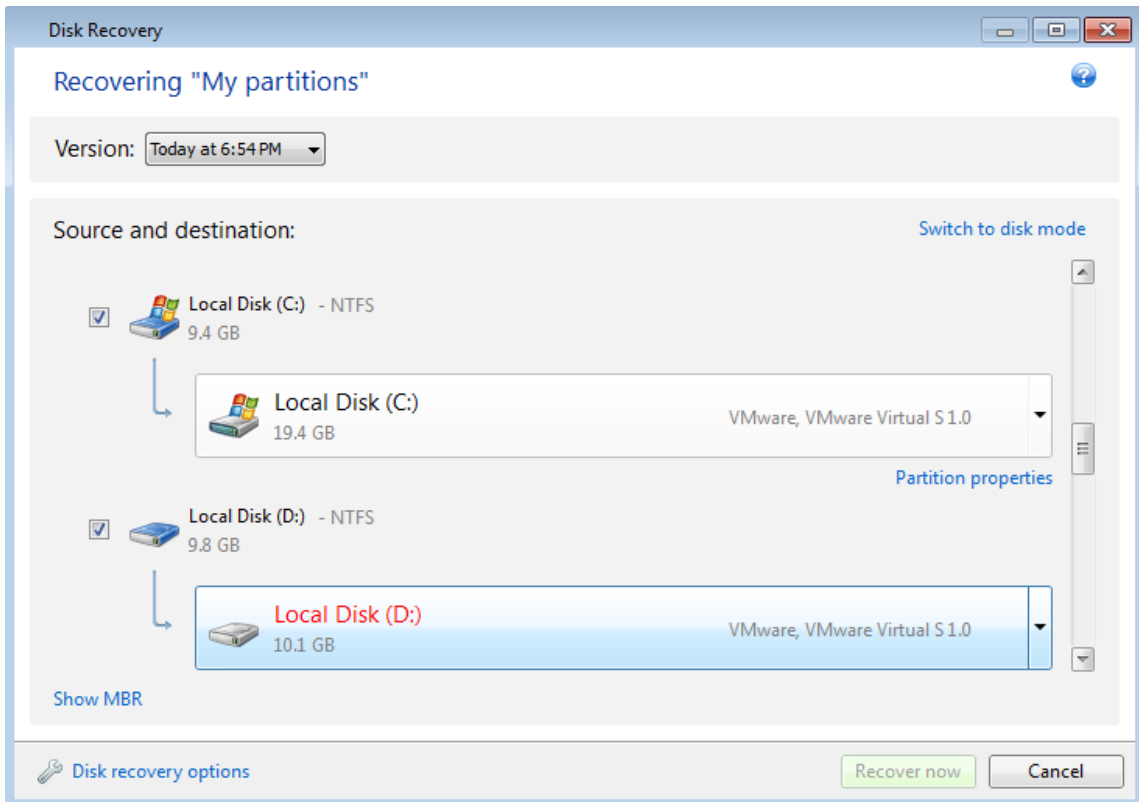


8. დააჭირეთ მიმართვას **Partition Properties** და მომართეთ პარამეტრები. აირჩიეთ დისკის ასოითი დასახელება და დანაყოფის ტიპი. როცა პარამეტრების მომართვას დაამთავრებთ დააჭირეთ **OK** ღილაკს მთავარ მენიუში დასაბრუნებლად.

თუკი იმიჯი შეიცავს ორზე მეტ დანაყოფს, მაშინ დატოვეთ საკმარისი თავისუფალი სივრცე სხვა დანაყოფებისთვის, რომლებიც აუცილებლად უნდა აღდგეს, და გაიმეორეთ 5-7 პუნქტები, სანამ ყველა დანაყოფისთვის არ იქნება პარამეტრები მომართული.



9. დავაჭიროთ ღილაკს **Recover now**, რათა აღვადგინოთ დანაყოფები მთელს მყარ დისკზე.



6.3.1.4 ოპერაციული სისტემის სარეზერვო ასლის შექმნა Flash ან CD/DVD

ჩამტვირთავი მედია საშუალებით

სარეზერვო ასლის შექმნას ვერ დავიწყებთ თუ არ და დავაყენებთ საწყის ჩამტვირთავად **CD\DVD** ან **FLASH** (სადაც გვიწერია **True image** პროგრამა) და არ ჩავიტვირთებთ მითითებული მოწყობილობიდან .

იმისათვის, რომ მივანიჭოთ პრიორიტეტი რომელიმე მოწყობილობას (**CD\DVD** ან **FLASH**), საჭიროა შევიდეთ ბიოსში (**BIOS**). გვაქვს ბიოსში შესასვლელი რამდენიმე ღილაკი, სტანდარტულად ითვლება **DELETE** ღილაკი, ხოლო ნოუთბუქებისთვის გამოიყენება **ESC** ან **F2** ღილაკი. ბიოსში შესვლის შემდეგ უნდა განვსაზღვროთ მოწყობილობების პრიორიტეტი, რისთვისაც გადავდივართ **Boot** ჩანართში:

PhoenixBIOS Setup Utility							
Main	Advanced	Security	Boot	Exit			
+Removable Devices +Hard Drive CD-ROM Drive Network boot from AMD Am79C970A				Item Specific Help			
				Keys used to view or configure devices: <Enter> expands or collapses devices with a + or - <Ctrl+Enter> expands all <+> and <-> moves the device up or down. <n> May move removable device between Hard Disk or Removable Disk <d> Remove a device that is not installed.			
F1	Help	↑↓	Select Item	-/+	Change Values	F9	Setup Defaults
Esc	Exit	↔	Select Menu	Enter	Select ► Sub-Menu	F10	Save and Exit

მოცემულ ფანჯარაში გვაქვს:

- ა) **Removable Devices** – **Flash** მეხსიერება
- ბ) **Hard Drive** - მყარი დისკი (ვინჩესტერი)
- გ) **CD\DVD Drive** -**CD\DVD** წამკითხველი
- დ) **Network Boot** - ქსელიდან ჩატვირთვა

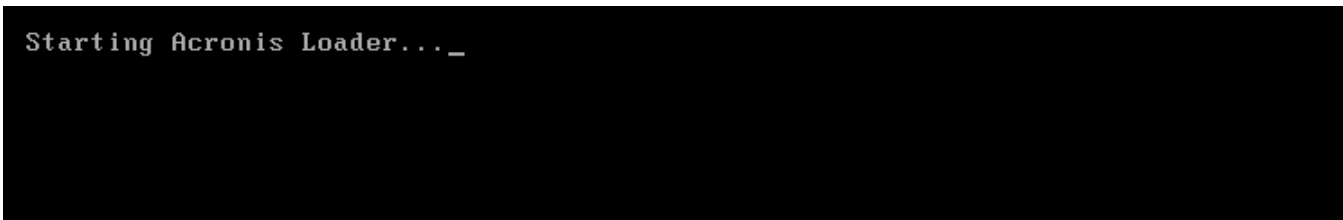
ჩვენს შემთხვევაში პირველ ადგილზე ვაყენებთ **CD\DVD**. ამისათვის ჩამოვდივართ **CD\DVD-Drive**-ზე და + ან - ღილაკით აგვაქვს ზევით 1-ლ ადგილზე, ხოლო მეორეზე ვტოვებთ ვინჩესტერს (**Hard Drive**).

ამ ყველაფრის შემდეგ უნდა მოხდეს ცვლილებების შენახვა. გვაქვს ორი ვარიანტი:

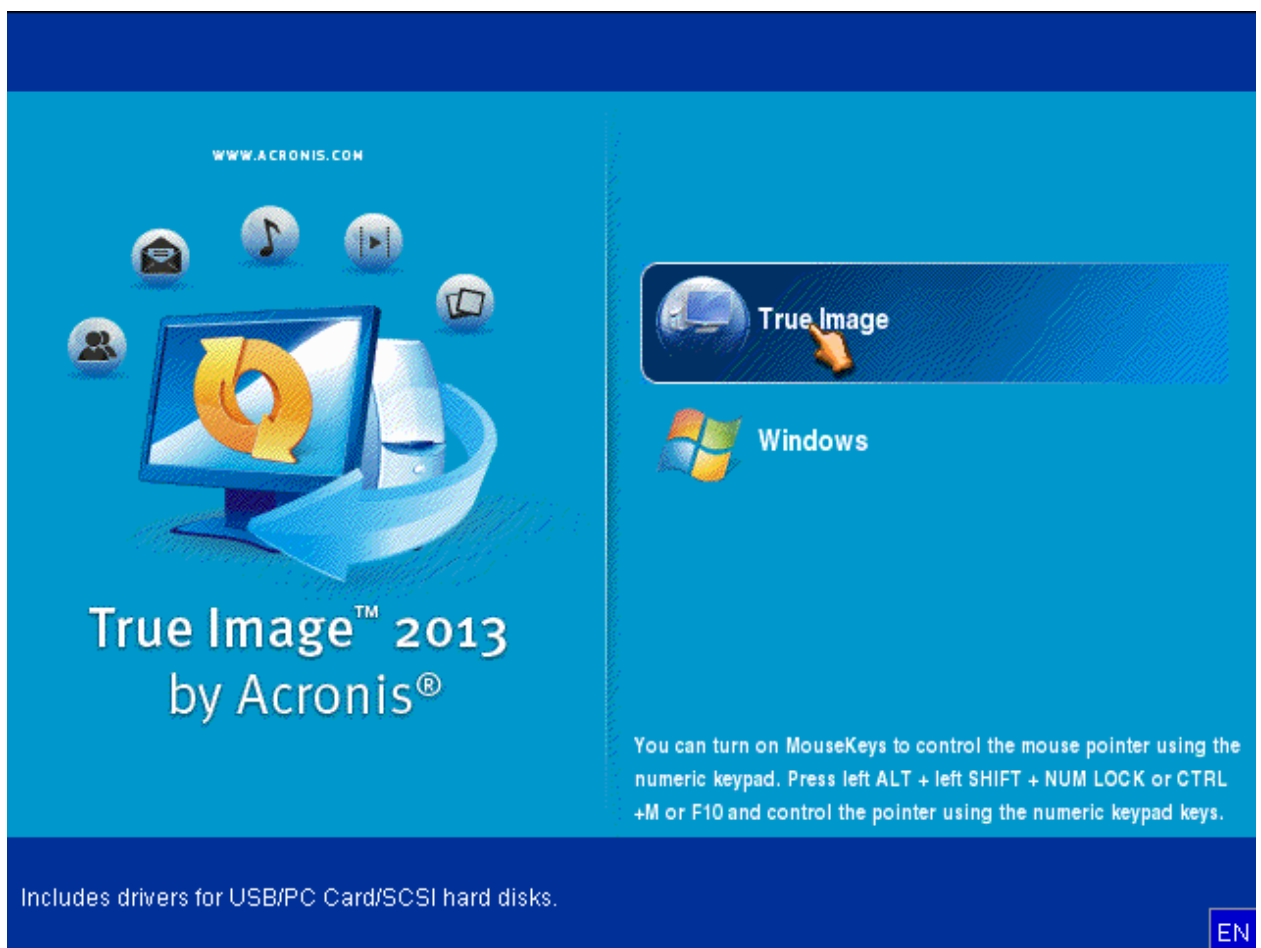
- 1) ვაწვებით **F10** ღილაკს და გამოსულ მენიუში ვაჭერთ **OK** ღილაკზე;
- 2) გადავდივართ **EXIT** მენიუში და ვირჩევთ **Exit Saving Changes** და შემდეგ **OK**

შენიშვნა: თუ აგვერია ბიოსში რაიმე ვაწყებთ **Discard Changes** (ცვლილებების უგულებელყოფა) და ვინახავთ.

მას შემდეგ რაც **BIOS**-ში პირველ წამკითხველ აპარატურად დავაყენებთ **CD/DVD**-ს, ჩავდოთ დისკი და ჩავიტვირთოთ:



მას შემდეგ რაც ჩატვირთვა დასრულდება, გამოჩნდება ფანჯარა:



გვაქვს 2 ვარიანტი:

- 1) **True Image** - ჩაიტვირთება პროგრამა **Acronis**-ი;
- 2) **Windows** - ჩაიტვირთება ოპერაციული სისტემა, რომელიც გვიყენია კომპიუტერზე.

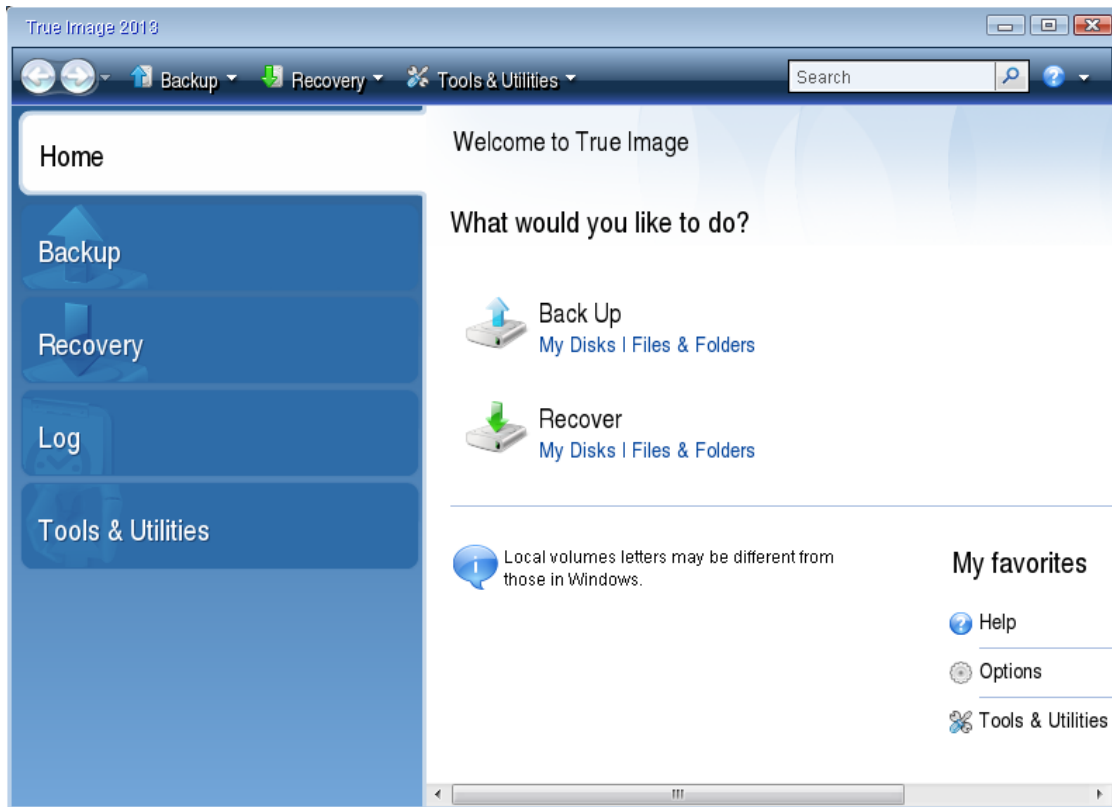
ჩვენს შემთხვევაში გვინდა პირველი: **True Image**.

დაიწყება **Acronis**-ის ჩატვირთვა, რომელიც რამოდენიმე წამი გაგრძელდება (დამოკიდებულია თქვენს ოპერატიულ მეხსიერებაზე).



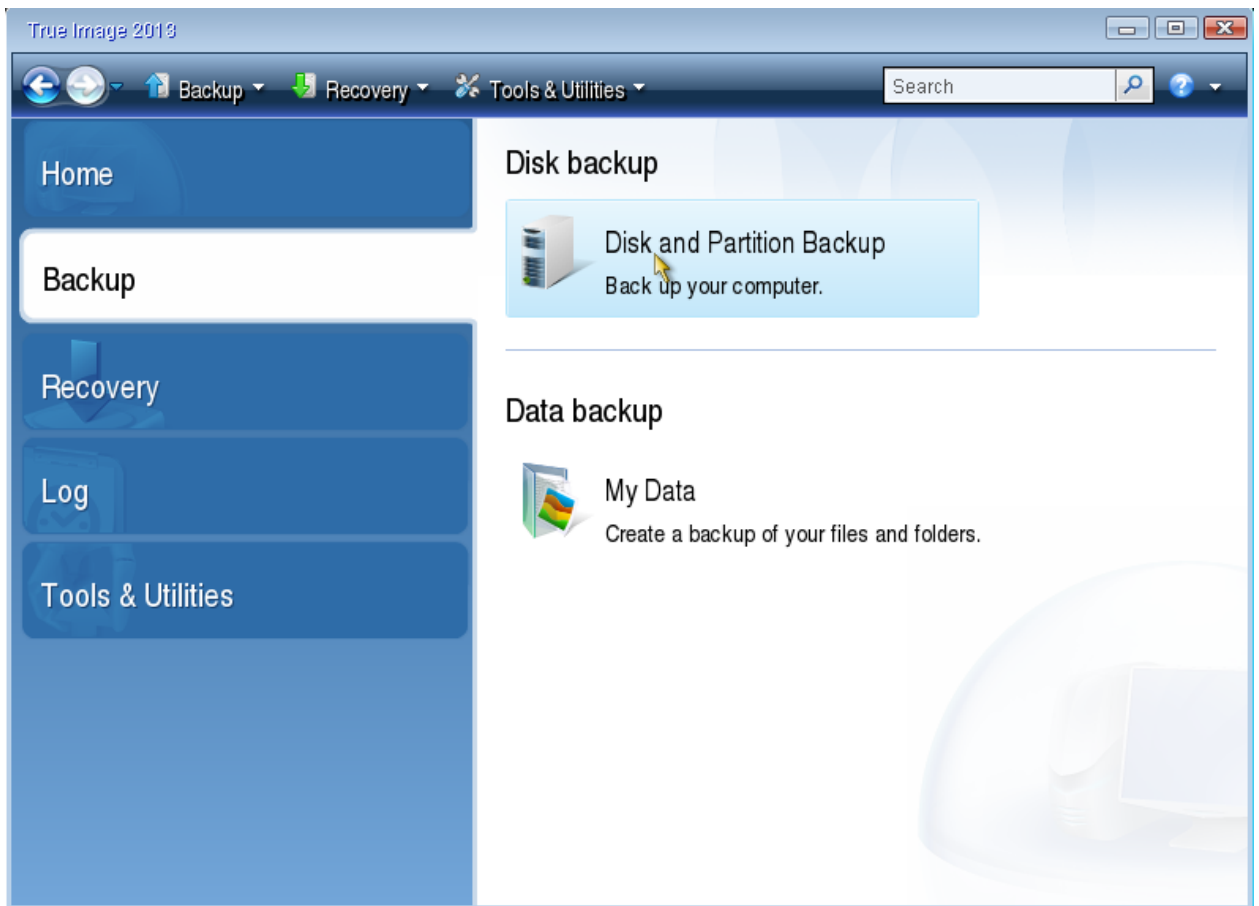
გამოვა შემდეგი ფანჯარა, სადაც უნდა ავირჩიოთ რისი გაკეთება გვინდა:

- **Back Up** – სარეზერვო ასლის შექმნა;
- **Recover** - აღდგენა;



იმ შემთხვევაში თუ ასლი შექმნილი გვაქვს, შექმნის ეტაპი შეგვიძლია გამოვტოვოთ, წინააღმდეგ შემთხვევაში მივყვეთ ინსტრუქციებს. გვაქვს ასლის შექმნის ორი ვარიანტი:

- 1) **Disk and Partition Backup** - მთლიანი ვინჩესტერის ან რომელიმე ლოგიკური დისკის ასლის შექმნა;
- 2) **My Data** - კონკრეტული ფაილების ან ფოლდერების ასლის შექმნა.

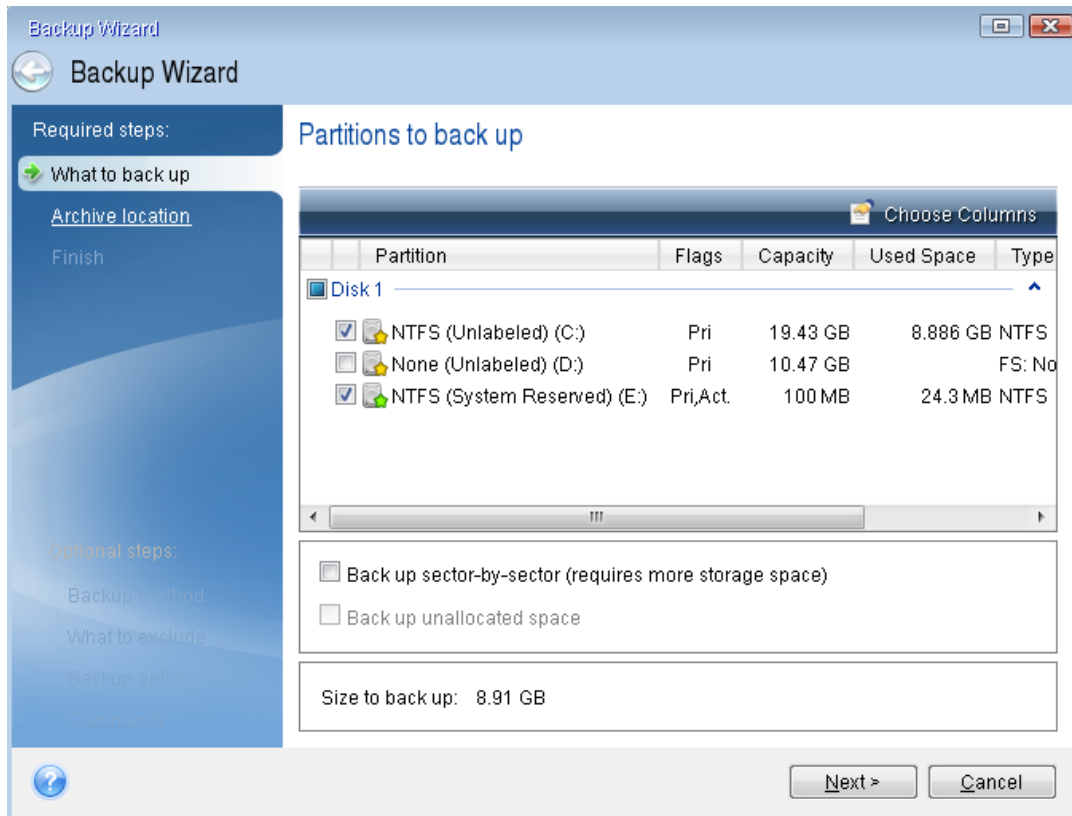


პირველი ვარიანტის არჩევის შემთხვევაში (**Disk and Partition Backup**) გამოჩნდება ის ლოგიკური დანაყოფები, რომელიც გვაქვს მყარ დისკზე. მოვნიშნოთ ის დანაყოფ(ებ)ი, რომლის ასლის შექმნაც გვსურს. ფანჯრის ქვედა მხარეს გვაქვს ორი პარამეტრი:

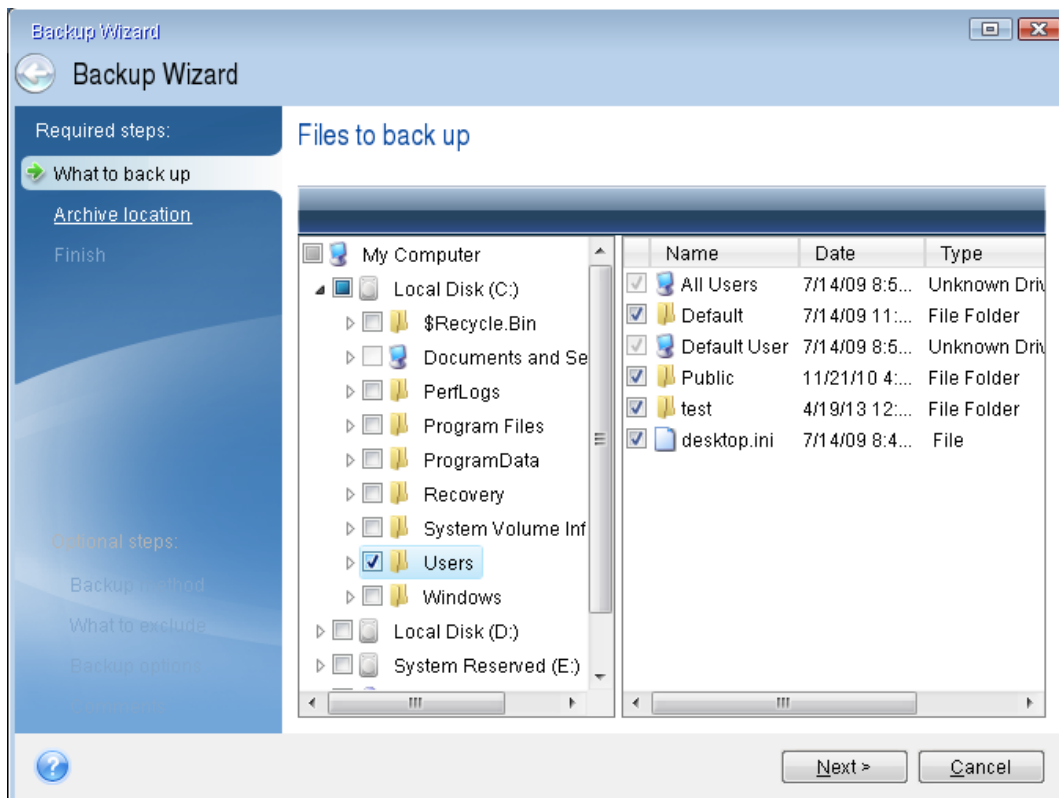
- ყველა სექტორის სარეზერვო ასლის შესაქმნელად ჩართეთ ალამი **Back up sector-by-sector**. ავტომატურად დაკოპირდება მყარის დისკის მხოლოდ ის სექტორები, რომლებზეც არის მონაცემები. თუმცა ხელსაყრელია მყარი დისკის ყველა სექტორის სარეზერვო ასლის შექმნა. მაგალითად, შეცდომით წაგვეშალა ზოგიერთი ფაილი და შესაბამისი უტილიტების გამოყენებით აღდგენის ოპერაციის დაწყებამდე გვსურს დისკის ასლის შექმნა, რადგან ზოგჯერ აღდგენით შეიძლება დაირღვეს ფაილთა სისტემა. მყარი დისკის როგორც გამოყენებული, ასევე გამოუყენებელი სექტორების ამ რეჟიმში კოპირებისას იზრდება დამუშავების დრო და ჩვეულებრივ მიიღება დიდი ზომის ასლი (**Image**);

- **Back up unallocated space** მისაწვდომი ხდება თუ არჩეულია წინა **Back up sector-by-sector** პარამეტრი. ავტომატურად სექტორულ რეჟიმში ასლის შექმნისას დისკის დაუყოფელი სივრცე არ ემატება სარეზერვო ასლს. ამ პარამეტრის არჩევისას სარეზერვო ასლში შევა მყარი დისკის მთელი დაუყოფელი სივრცე

Size to back up - გვიჩვენებს მონიშნული ლოგიკური ნაწილის ზომას ასლის შექმნამდე.



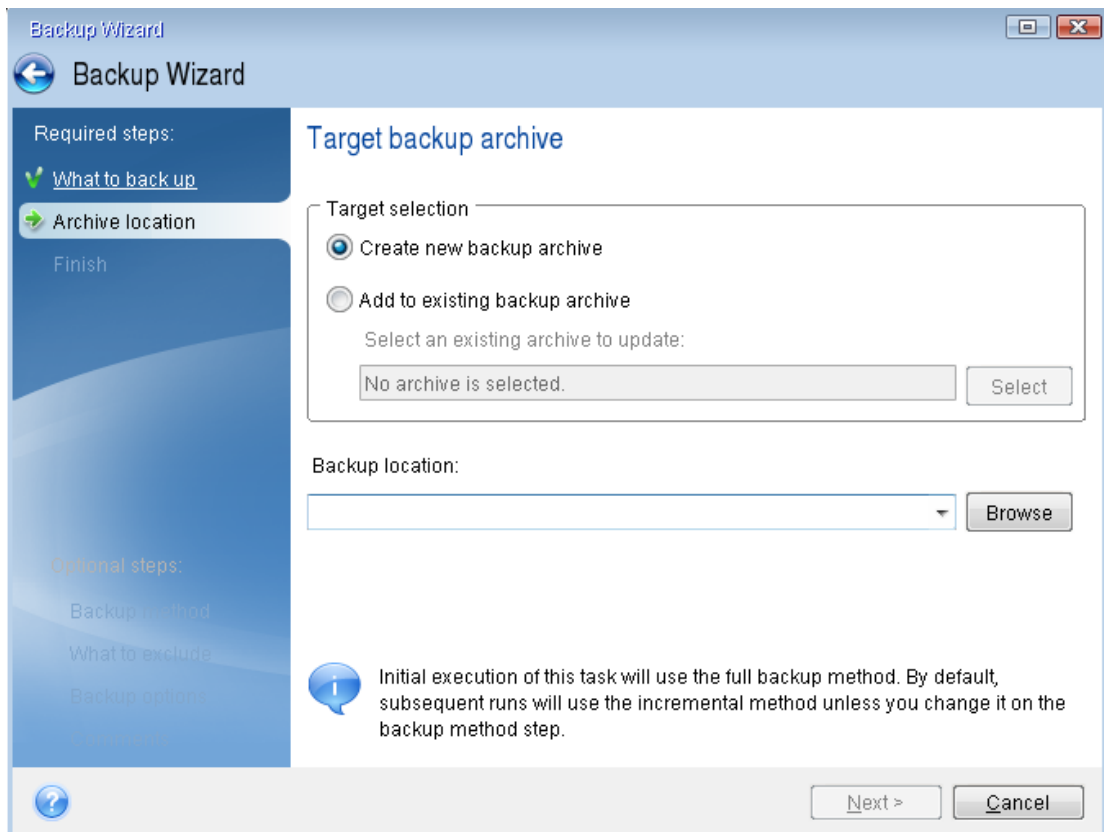
მეორე ვარიანტის არჩევის შემთხვევაში (**My Data**), გვეძლევა შესაძლებლობა შევქმნათ კონკრეტული საქალაქის სარეზერვო ასლი. საჭიროა მონიშნოთ მთლიანად საქალაქი ან ქვესაქალაქი. ასევე სურვილის შემთხვევაში შესაძლებელია რამდენიმეს მონიშვნაც.



რომელი ვარიანტიც არ უნდა ავირჩიოთ **Next** ღილაკზე დაჭერის შემდეგ გამოდის ფანჯარა, სადაც ვირჩევთ ერთ-ერთს:

- **Create new backup archive** - შევქმნათ ახალი ასლი. ამ შემთხვევაში ვაწვევით **Browse** ღილაკს და ვუთითებთ ადგილს თუ სად უნდა მოხდეს ასლის შენახვა.

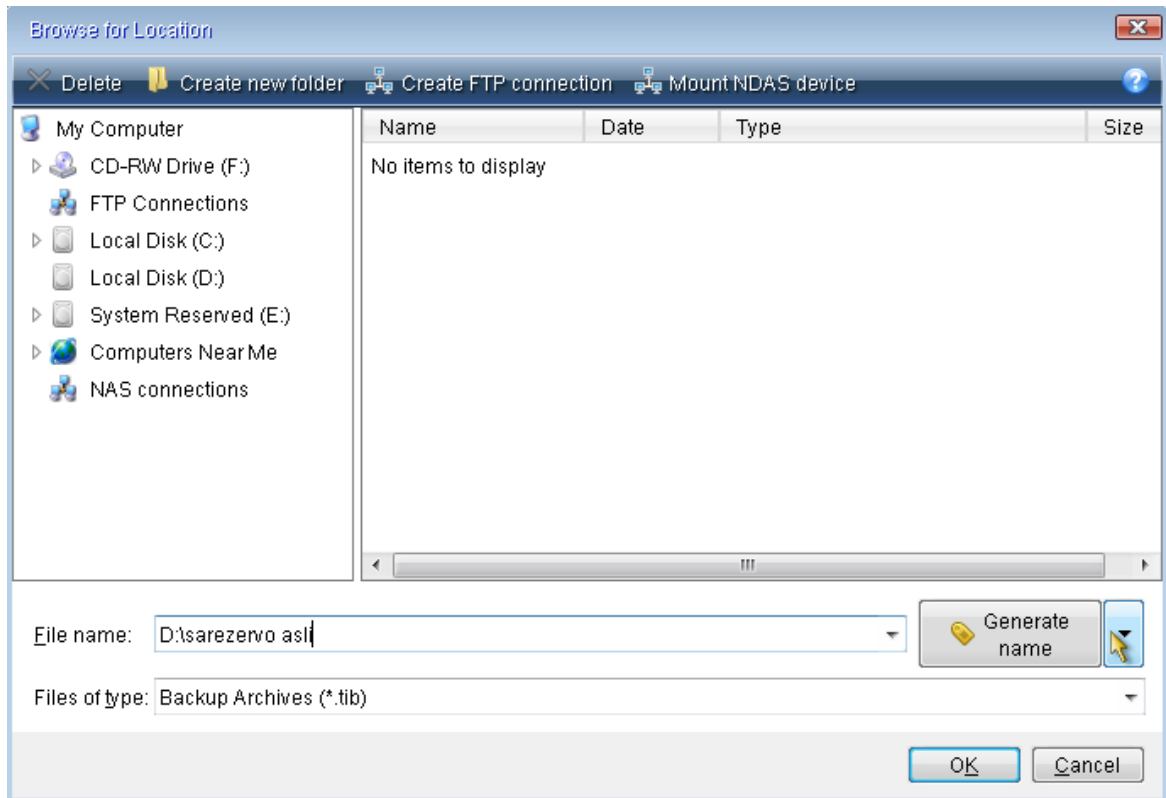
- **Add to existing backup archive** - დავამატოთ ახალი ცვლილებები ადრე შექმნილ ასლს. ამ შემთხვევაში ვაწვევით **Select** ღილაკს და ვუთითებთ ადგილს სადაც გვიჩერია ძველი ასლი (ანუ რისი გაახლებაც უნდა მოხდეს).



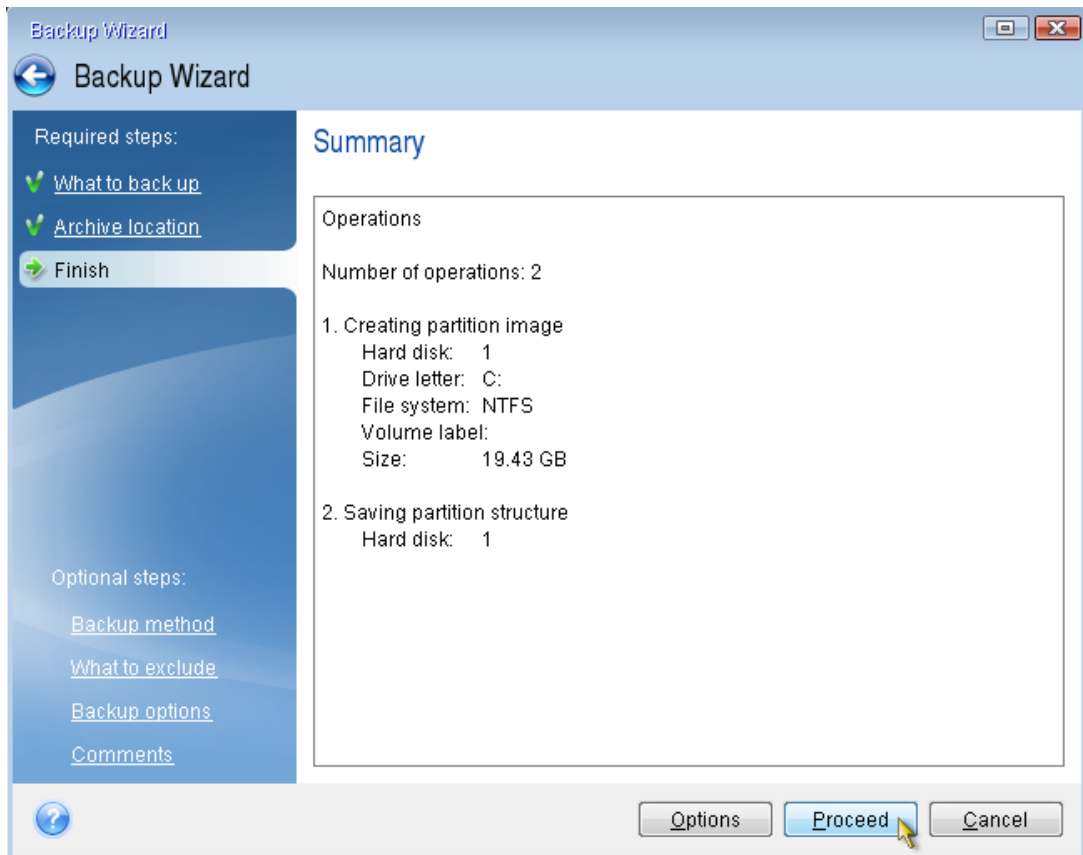
ჩვენს შემთხვევაში გვინდა ახალი ასლის შექმნა, ამიტომ ვირჩევთ **Create new backup archive** და ვაწვებით **Browse** ღილაკს. გამოსულ ფანჯარაში ავირჩიოთ ადგილი სადაც ხდება ასლის შენახვა, დავაწვით **OK**-ს და შემდეგ **Next**.

შენიშვნა: 1) ასლი არ შეინახოთ იმ ლოგიკურ დანაყოფზე რომლის ასლსაც აკეთებთ (ან გიყენიათ ოპერაციული სისტემა). 2) სახელი დაარქვით ისე, რომ იყოს ადვილად მისაგნები.

3) შექმნილი არქივის გაფართოება არის **.tib**



ბოლო ეტაპზე შეგიძლიათ დააწვით ღილაკს **Proceed** დაიწყება ასლის შექმნა. ამ შემთხვევაში პარამეტრები არის გაწერილი ავტომატურად და არაფერში ჩარევა არ გვჭირდება, მაგრამ თუ გსურთ შეცვალოთ რაიმე, მაშინ უნდა განვიხილოთ **Optional steps** მენიუ და მისი ქვემენიუები:



I ეტაპი - Backup method:

True Image გთავაზობს სარეზერვო ასლების შექმნის სამ მეთოდს.

1) **სრული:** სრული სარეზერვო ასლი შეიცავს ყველა მონაცემს, რაც კი მისი შექმნის დროს არსებობდა. ეს რეჟიმი ქმნის საფუძველს მომავალში ინკრემენტული ან დიფერენციალური სარეზერვო ასლების შესაქმნელად; ის ასევე შეიძლება გამოვიყენოთ ავტონომიური სარეზერვო ასლის შექმნისას.

2) **ინკრემენტული:** სარეზერვო ასლში შედის მხოლოდ ის ფაილები, რომლებმაც განიცადეს ცვლილება ბოლო, ნებისმიერი სარეზერვო ასლის შექმნის შემდეგ.

3) **დიფერენციალური:** სარეზერვო ასლში შედის მხოლოდ ის ფაილები, რომლებმაც განიცადეს ცვლილება ბოლო სრული სარეზერვო ასლის შექმნის შემდეგ.

სარეზერვო ასლის შექმნის ამ სამი მეთოდიდან აირჩიეთ ერთ-ერთი:

„სრული“ (Full) - ავტონომიური სრული სარეზერვო ასლის შექმნა შეიძლება იყოს ოპტიმალური გადაწყვეტა, თუკი ხშირად ხდება სისტემის დაბრუნება საწყის მდგომარეობამდე ან არ არის სასურველი დიდი რაოდენობის სარეზერვო ასლების შენახვა.

„ინკრემენტული“ (Incremental) - ინკრემენტული სარეზერვო ასლის შექმნა განსაკუთრებით გამოიყენება იმ შემთხვევაში, თუკი საჭიროა სარეზერვო ასლების ხშირი შექმნა და წარსული დროის კონკრეტულ მომენტში არსებულ მდგომარეობამდე აღდგენის შესაძლებლობის ქონა. სრული სარეზერვო ასლის შექმნის შემდეგ თუ თვის ყოველ დღეს შექმნით ინკრემენტულ სარეზერვო ასლს, მიიღება იგივე შედეგი, როგორც თითქოს თვის ყოველ დღეს სრულდებოდა სრული სარეზერვო ასლის შექმნა. როგორც წესი, ინკრემენტული სარეზერვო ასლები არსებითად მცირეა სრულ ან დიფერენციალურთან შედარებით.

სარეზერვო ასლის შექმნის ამ მეთოდის გამოყენების სცენარს შეიძლება წარმოადგენდეს სისტემის ყოველკვირეული სრული სარეზერვო ასლის შექმნა მხოლოდ იმ მონაცემთა სარეზერვო ასლების შექმნის ყოველდღიური ინტერვალით, რომლებმაც განიცადეს ცვლილება ბოლო სარეზერვო ასლის შექმნის შემდეგ.

მოცემული სცენარის უპირატესობას წარმოადგენს საცავის სივრცისა და დროის ეკონომია, რაც საჭიროა ყოველდღიური სარეზერვო ასლის შექმნისას. თუმცა, სისტემის

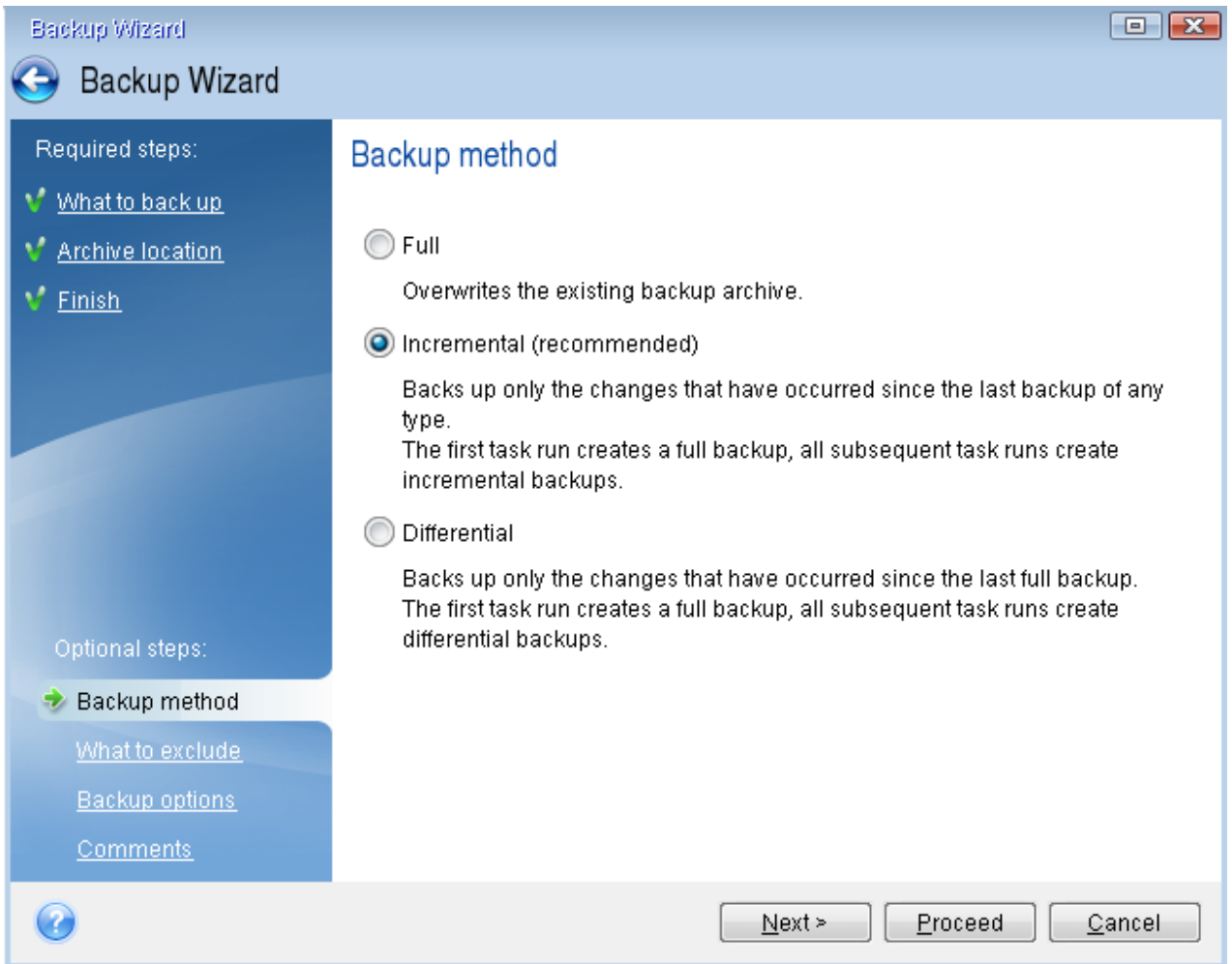
დაზიანების შემთხვევაში მის აღდგენას მეტი რესურსი დასჭირდება. თუ დაზიანება მოხდება ხუთშაბათს, მაშინ საჭირო გახდება ორშაბათის, სამშაბათის და ოთხშაბათის ბოლო სრული სარეზერვო ასლის აღდგენა.

დიფერენციალური - იგი წარმოადგენს შუალედურ მეთოდს წინა ორ მეთოდს შორის. დიფერენციალური სარეზერვო ასლი მოიცავს მხოლოდ იმ ფაილებს, რომლებმაც განიცადეს ცვლილება ბოლო სრული სარეზერვო ასლის შექმნის შემდეგ. ეს მეთოდი შესაძლებელია საჭიროებს ნაკლებ დროსა და ადგილს სრული სარეზერვო ასლის შექმნასთან შედარებით, მაგრამ მეტს ინკრემენტულთან შედარებით. აღდგენა უფრო მარტივია, ვიდრე მეორე მეთოდის გამოყენებისას, რადგან საკმარისი იქნება ბოლო სრული და დიფერენციალური სარეზერვო ასლის აღდგენა.

სარეზერვო ასლის შექმნის მეთოდის ასარჩევად აუცილებელია სარეზერვო ასლის შექმნის სამომხმარებლო სქემის აგება.

დისკის დეფრაგმენტაციის შემდეგ შექმნილი ინკრემენტული ან დიფერენციალური სარეზერვო ასლი შეიძლება იყოს საკმაოდ დიდი ზომის, ვიდრე ჩვეულებრივი. ეს იმით არის გამოწვეული, რომ დეფრაგმენტაციის პროგრამა ცვლის ფაილების მდებარეობას დისკზე და ეს ცვლილებები აისახება სარეზერვო ასლში. ამიტომ რეკომენდებულია დისკის დეფრაგმენტაციის შემდეგ სრული სარეზერვო ასლის ხელახლა შექმნა.

შენიშვნა: ინკრემენტული სარეზერვო ასლის დაკარგვის ან დაზიანების შემთხვევაში ყველა მომდევნო ინკრემენტული ასლის გამოყენება შეუძლებელი გახდება.



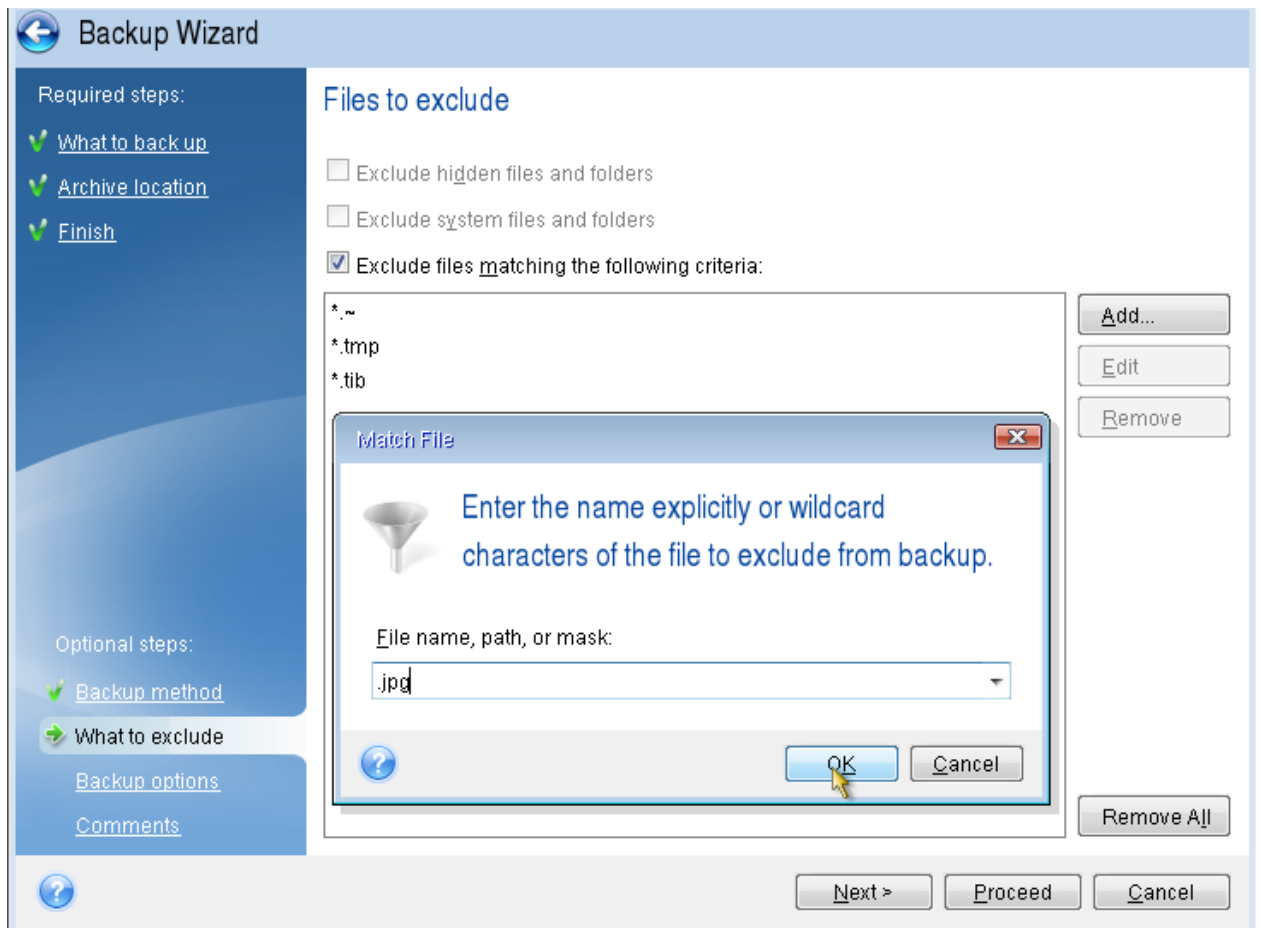
II ეტაპი - What to exclude (რომელი ფაილების ან ფოლდერების გამოტოვება მოხდეს სარეზერვო ასლის შექმნის მომენტში):

რა და როგორ უნდა ამოვაკლოთ

1. სარეზერვო ასლიდან შეიძლება ამოვრიცხოთ ფარული და სისტემური ფაილები (სისტემური დანაყოფების სარეზერვო ასლების ფარული და სისტემური ფაილების გარდა), შესაბამისი ალმების დაყენებით.

2. შეიძლება ამოირიცხოს ფაილები, რომლებიც ესადაგება გარკვეულ კრიტერიუმს. ამისათვის დააყენეთ ალამი **Exclude files matching the following criteria**, ამის შემდეგ დააჭირეთ **Add** ღილაკს და შეიყვანეთ გამონაკლისი კრიტერიუმები.

პროგრამა სარეზერვო ასლებიდან ავტომატურად აგდებს ფაილებს ~, **TMP**, **TIB** გაფართოებით:



ამორიცხვის კრიტერიუმის დამატება

- სარეზერვო ასლიდან ამოსარიცხი ფაილის სახელი შეიძლება მიეთითოს სრულად:
- **file.ext** – ყველა ფაილი ამ სახელწოდებითა და გაფართოებით ამოვარდება;
- **c:\file.ext** - C: დისკის ფაილი **file.ext** ამოვარდება;
- შეიძლება ჩასასმელი ნიშნების გამოყენება (* და ?):
- ***.ext** - ყველა ფაილი **.ext** გაფართოებით გამოირიცხება.
- **??name.ext** - გამოირიცხება ყველა ფაილი **.ext** გაფართოებით, რომელთა სახელი ექვსი ასოსაგან შედგება (რომელიც ნებისმიერი ორი სიმბოლოთი იწყება (??) და მთავრდება **name**-ით).

• საქალაქის ამოსარიცხად დააჭირეთ ღილას **Browse**, აირჩიეთ ამოსაკლები საქალაქი, დააჭირეთ **OK**, შემდეგ კი ღილაკს **OK**;

კრიტერიუმების ამოსაკლებად, მაგალითად შეცდომით დამატებული, დააჭირეთ ნიშანს „Add“ კრიტერიუმის მარჯვნივ.

III ეტაპი - Backup options, რომელსაც აქვს ქვემენიუები:

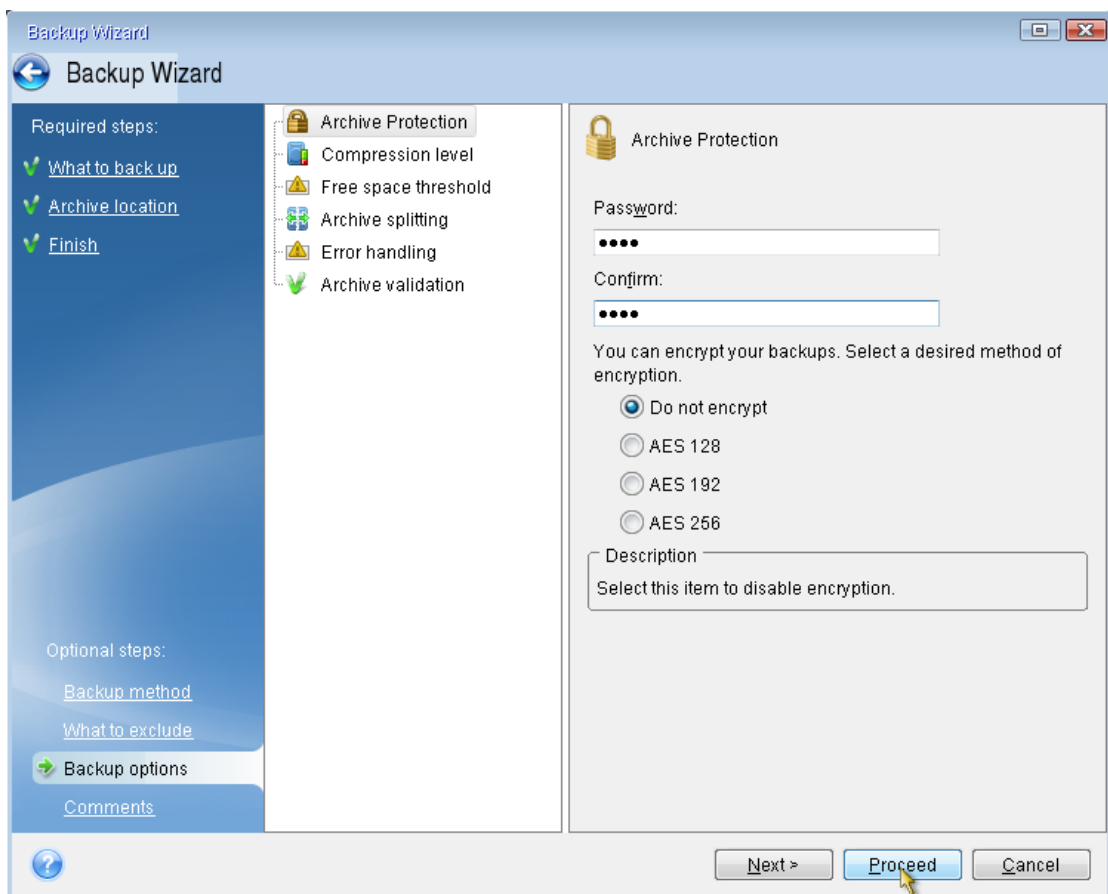
ა) Archive Protection - სარეზერვო ასლის დაცვა პაროლით:

სარეზერვო ასლის დაცვა შესაძლებელია პაროლით. ავტომატური დაცვა პაროლით სარეზერვო ასლისთვის არ არის მომართული.

როგორ დავიცვათ სარეზერვო ასლი

- შეიყვანეთ სარეზერვო ასლის პაროლი ველში **Password**. საიმედოდ დაცვისათვის პაროლი უნდა შედგებოდეს არანაკლებ რვა სიმბოლოსგან, როგორც ასოების (მთავრული და პატარა), ისე ციფრების კომბინაციისგან.

- შეიყვანეთ ხელახლა პაროლი ველში **Confirm**.



კონფიდენციალური მონაცემების საიმედოდ დასაცავად დაშიფრეთ სარეზერვო ასლები საიმედო კრიპტოგრაფული **AES** ალგორითით, რომელიც წარმოადგენს დარგობრივ სტანდარტს. **AES** ალგორითმი მოწოდებულია გასაღების სამი სიგრძით (128,

192 და 256 ბიტი), რაც წარმადობასა და დაცვას შორის კომპრომისის მონახვის საშუალებას იძლევა:

უმეტესწილად საკმარისია დაშიფვრა 128-ბიტის გასაღებით. რაც უფრო გრძელია დაშიფვრის გასაღები, მით უფრო კარგადაა დაცული მონაცემები. თუმცა 192- და 256-ბიტის გასაღებების გამოყენება მნიშვნელოვნად ანელებს სარეზერვო ასლის შექმნის პროცესს.

AES დაშიფვრის გამოყენების აუცილებლობის შემთხვევაში, აირჩიეთ ერთ-ერთი ამ სამი ვარიანტიდან:

- **AES 128** – 128-ბიტის დაშიფვრული გასაღები;
- **AES 192** – 192-ბიტის დაშიფვრული გასაღები;
- **AES 256** – 256-ბიტის დაშიფვრული გასაღები.

თუ დაშიფვრა აუცილებელი არ არის და საკმარისია მისი მხოლოდ პაროლით დაცვა, აირჩიეთ **None**.

დაცვის პარამეტრების მითითების შემდეგ დააჭირეთ **OK**-ს.

მიაქციეთ ყურადღება, რომ პაროლით დაცული სარეზერვო ასლის შექმნის შემდეგ, მისი პაროლის შეცვლა შეუძლებელია.

პაროლით დაცული სარეზერვო ასლებიდან ინფორმაციის აღსადგენად აუცილებელია პაროლის შეყვანა (რათა მისაწვდომი იყოს მხოლოდ ავტორიზებული მომხმარებლისათვის).

ბ) Compression level - შეკუმშვის დონე. გვაქვს 4 დონე.

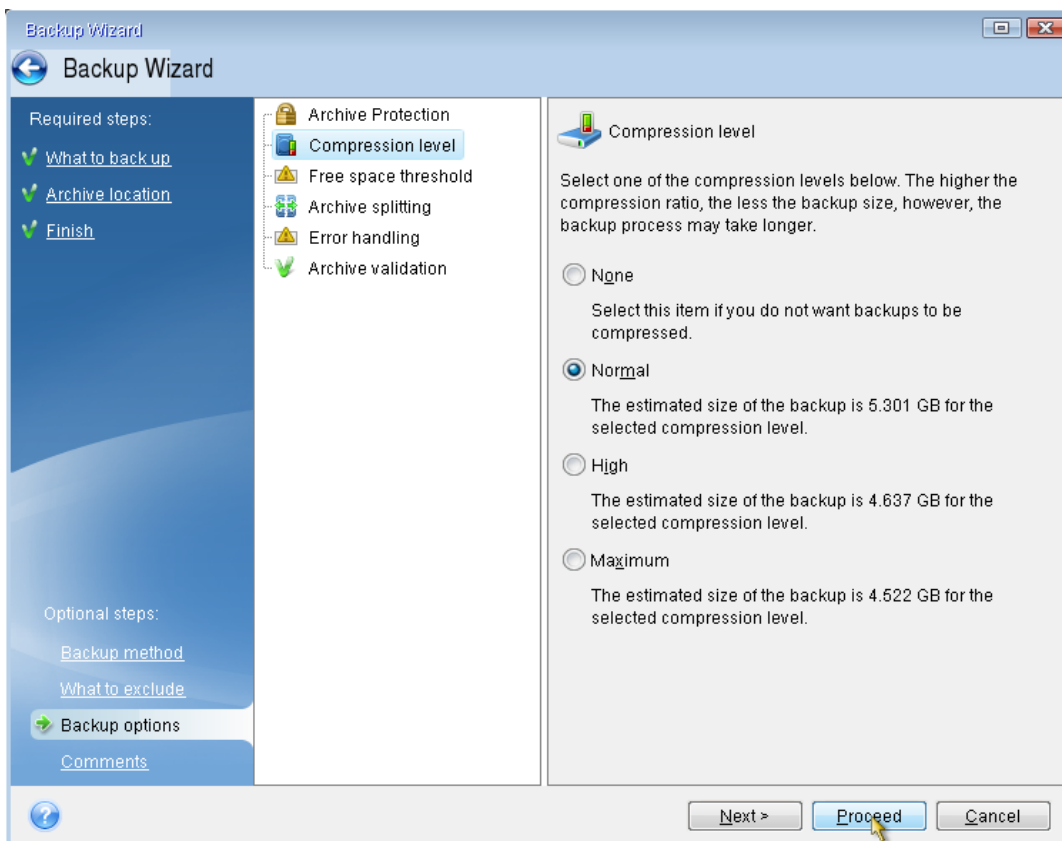
▪ **None** - მონაცემები დაკოპირდება შეკუმშვის გარეშე, რაც არსებითად გაზრდის სარეზერვო ასლის ფაილის ზომას.

▪ **Normal** - მონაცემთა შეკუმშვის რეკომენდებული დონე (ავტომატურად ჩართული).

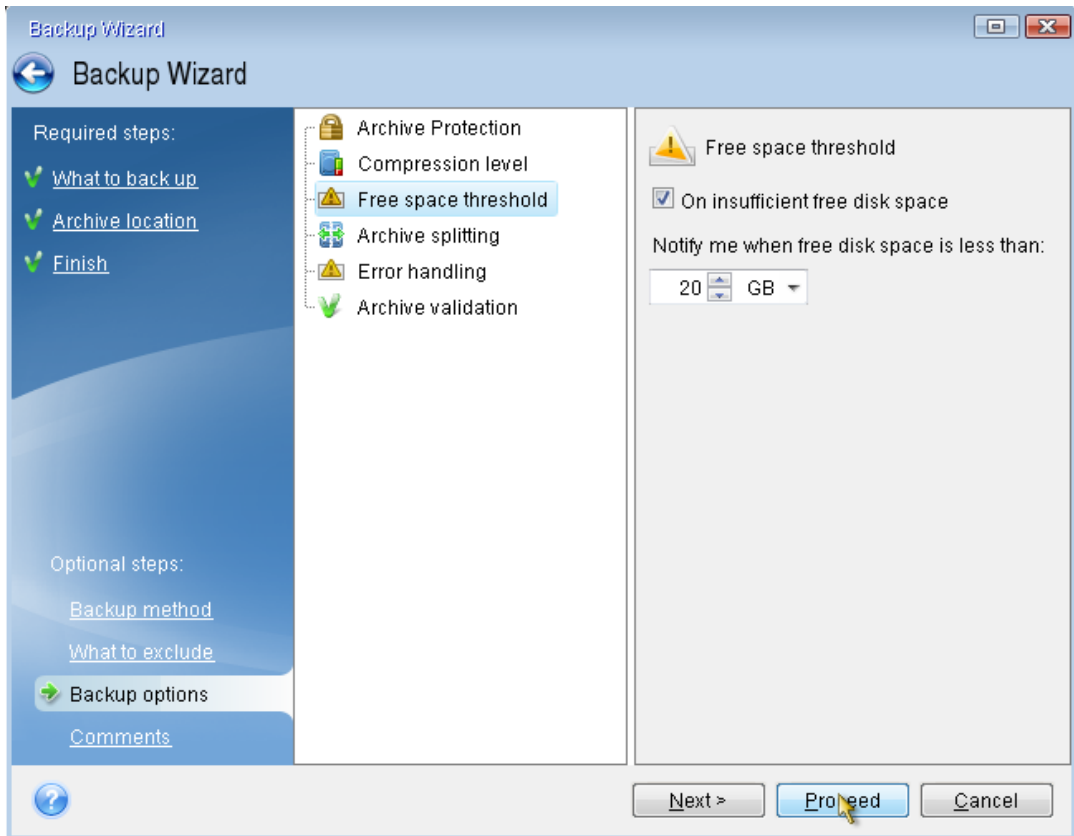
▪ **High** - შეკუმშვის უფრო მაღალი დონე, სარეზერვო ასლის შესაქმნელად საჭირო ხანგრძლივი დროით.

▪ **Maximum** - შეკუმშვის მაქსიმალური დონე, სარეზერვო ასლის შესაქმნელად საჭირო მაქსიმალურად ხანგრძლივი დრო.

მონაცემთა შეკუმშვის ოპტიმალური დონე დამოკიდებულია ფაილების ტიპზე, რომლებიც სარეზერვო ასლში ინახება. მაგალითად, შეკუმშვის მაქსიმალური დონეც კი უმნიშვნელოდ შეამცირებს იმ სარეზერვო ასლების ზომას, თუკი ისინი შეიცავს თავიდანვე შეკუმშულ ფაილებს, ისეთებს როგორცაა **JPG, PDF ან MP3**.



გ) **Free space threshold** - დისკური სივრცის მოცულობის თავისუფალი ზღვარი:



შეტყობინების მიღება მომართეთ მაშინ, როცა სარეზერვო ასლების საცავში თავისუფალი ადგილი შემცირდება იმაზე მეტად, ვიდრე მითითებული ზღვრული მნიშვნელობა. თუ სარეზერვო ასლის შექმნის დაწყების შემდეგ **True Image** აღმოაჩენს, რომ თავისუფალი სივრცე სარეზერვო ასლისთვის არჩეულ საცავში მცირეა, ვიდრე მითითებული იყო, პროგრამა არ დაიწყებს სარეზერვო ასლის შექმნის პროცესს, მაგრამ დაუყოვნებლივ შეგატყობინებთ ამის შესახებ, შესაბამისი შეტყობინების გამოტანით. ასეთი შეტყობინება გვთვავობს მოქმედების სამ ვარიანტს: იგნორირება და სარეზერვო ასლის შექმნის გაგრძელება, სხვა შესაძლებელი ადგილის არჩევა ან სარეზერვო ასლის შექმნის შეწყვეტა.

თუ თავისუფალი სივრცე შემცირდება მითითებულ მნიშვნელობასთან შედარებით სარეზერვო ასლის შექმნის პროცესში, პროგრამა მოგვაწვდის ასეთსავე შეტყობინებას და მოგვთხოვს ერთ-ერთი გადაწყვეტილების მიღებას.

Acronis-ს შეუძლია მოიძიოს თავისუფალი სივრცე შენახვის შემდეგ მოწყობილობებზე:

- ლოკალური მყარი დისკები;
- **USB** ინტერფეისიანი დისკვამყვანები და დამგროვებლები;

დ) **Archive splitting** – სარეზერვო ასლის დაყოფა ნაწილებად:

True Image -ს არ შეუძლია დაყოს უკვე შექმნილი სარეზერვო ასლები. მათი დაყოფა შესაძლებელია მხოლოდ მათი შექმნისას.

დიდი ზომის სარეზერვო ასლები შეიძლება დაიყოს რამდენიმე ფაილად, რომლებიც ერთად წარმოადგენენ საწყის სარეზერვო ასლს. სარეზერვო ასლის დაყოფა ხდება ასევე გადასატან მატარებელზე ჩაწერისთვის.



გულისხმობის პრინციპით შემოთავაზებულია **Automatic**. აღნიშნულ პარამეტრს **True Image** შემდეგნაირად იყენებს:

- თუ არჩეულ დისკზე საკმარისი ადგილია და მისი ფაილური სისტემა მხარს უჭერს ფაილებს, რომელთა ზომა შეესაბამება სარეზერვო ასლისთვის პროგნოზირებულ ზომას, მაშინ იქმნება სარეზერვო ასლის მხოლოდ ერთი ფაილი.

- თუ დისკზე საკმარისი ადგილია, მაგრამ მისი ფაილური სისტემა არ უჭერს მხარს ფაილის პროგნოზირებულ ზომას, ასლი (**Image**) ავტომატურად გაიყოფა რამდენიმე ფაილად.

- თუ მყარ დისკზე არასაკმარისი თავისუფალი ადგილია, პროგრამა გამოიტანს შეტყობინებას და დაელოდება თქვენს შემდგომ გადაწყვეტილებას. შეეცადეთ

განთავისუფლოთ დამატებითი ადგილი დისკზე ან აირჩიეთ სხვა დისკი და შემდეგ გააგრძელეთ პროცესი.

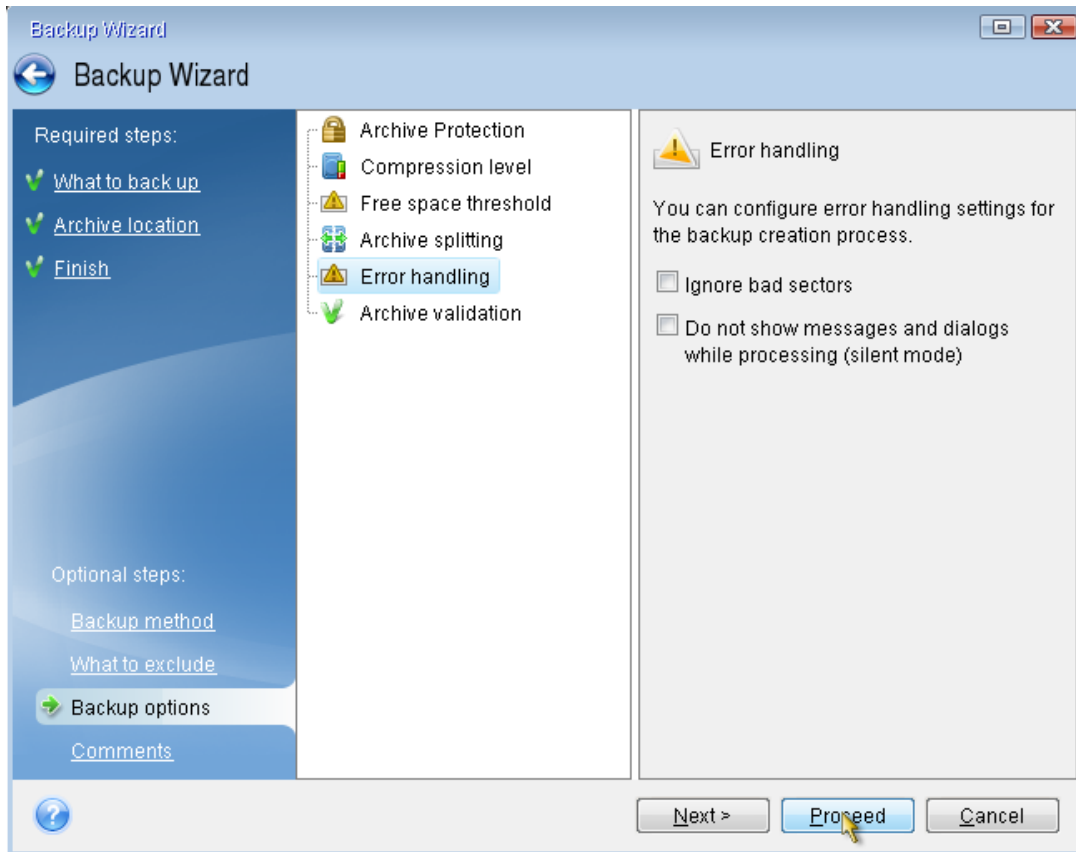
თუ დისკზე არ არის საკმარისი თავისუფალი ადგილი, **Acronis** მოგთხოვთ მომდევნო დისკის ჩადებას.

ფაილის მოთხოვნილი ზომა შეიძლება ავირჩიოთ ჩამოშლილი ჩამონათვალიდან. ამრიგად, სარეზერვო ასლი დაიყოფა მითითებული ზომის რამდენიმე ფაილად. ეს ხელსაყრელია მაშინ, როცა სარეზერვო ასლი ინახება მყარ დისკზე შემდგომ ოპტიკურ **CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE**-ზე დისკებზე ჩასაწერად.

CD-R/RW, DVD-R/RW, DVD+R/RW, BD-R/RE დისკებზე ჩასაწერად შექმნილ ასლს (image) უფრო მეტი დრო სჭირდება, ვიდრე მხოლოდ მყარ დისკზე შესანახად განკუთვნილს.

ე) Error handling - შეცდომების დამუშავება:

თუ პროგრამა სარეზერვო ასლების შექმნისას უშვებს შეცდომებს, პროცესი ჩერდება და გამოდის მომხმარებლის პასუხის მომლოდინე შეტყობინება იმის შესახებ, როგორ მოვიქცეთ ამ შეცდომის დროს. თუკი დაყენებულია შეცდომების დამუშავების პოლიტიკა, პროგრამა არ შეწყვეტს კოპირების პროცესს და არც შეტყობინებით გაგვაფრთხილებს შეცდომის შესახებ, მარტივად დაამუშავებს შეცდომას წესების არსებული ნაკრების შესაბამისად და გააგრძელებს მუშაობას:



შეცდომების დამუშავების პოლიტიკა:

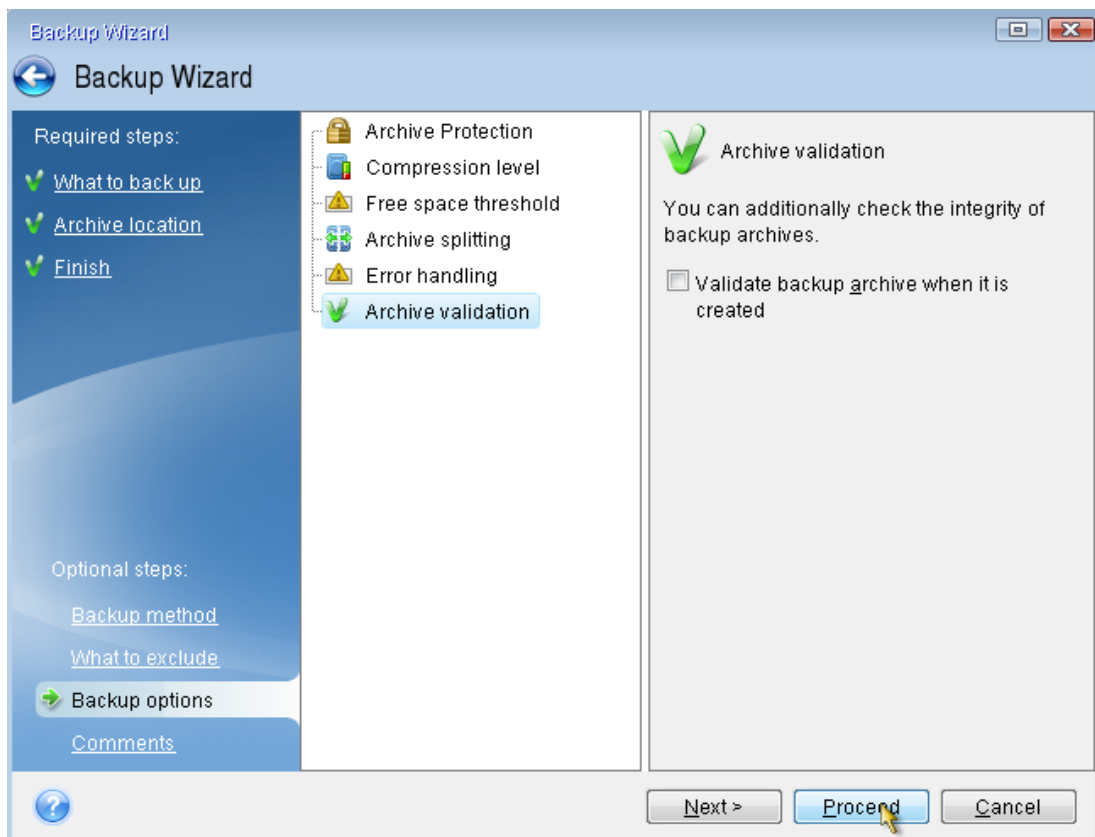
- **Do not show messages and dialogs while processing (silent mode)** (ავტომატურად ამორთულია) - ჩართეთ ეს ფუნქცია, სარეზერვო ასლის შექმნისას შეცდომების იგნორირებისათვის. ეს შესაძლებლობა გამოიყენება ძირითადად მომხმარებლის გარეშე სარეზერვო ასლის შექმნისას, როცა შეუძლებელია კოპირების პროცესის გაკონტროლება. ამ რეჟიმში შეტყობინება ასლის შექმნისას წარმოქმნილი შეცდომების შესახებ არ გამოვა. ყველა ოპერაციის შესახებ დაწვრილებითი ანგარიშის ნახვა შესაძლებელია სარეზერვო ასლის შექმნის შემდეგ.

- **Ignore bad sectors** (ავტომატურად ამორთულია) - ეს რეჟიმი გამოიყენება მხოლოდ დისკებისა და დანაყოფების სარეზერვო ასლების შექმნისას. ის იძლევა სარეზერვო ასლის შექმნის საშუალებას მაშინაც კი, როცა მყარ დისკზე არსებობს დაზიანებული სექტორები. უმეტეს მყარ დისკებზე დაზიანებული სექტორები არ არის, მაგრამ ისინი შეიძლება გაჩნდეს მათი ექსპლუატაციის საკმაოდ დროის გასვლის შემდეგ. თუ მყარი დისკი გამოსცემს უცნაურ ხმებს (მაგალითად, ხმაურს მუშაობის დროს), ეს მის გამოუსწორებლობაზე მიუთითებს. მყარი დისკის მწყობრიდან სრულიად გამოსვლისას შეიძლება უმნიშვნელოვანესი მონაცემები დაიკარგოს, ამიტომ საჭიროა რაც შეიძლება სწრაფად შეიქმნას სარეზერვო ასლი. თუმცა ამ დროს შეიძლება შეიქმნას პრობლემა -

დაშლის პირას მისულ დისკზე შეიძლება უკვე იყოს დაზიანებული სექტორები. თუ ჩართული არ არის **Ignore bad sectors**, წაკითხვის ან ჩაწერისას დაზიანებულ სექტორებზე შეცდომების არსებობისას, სარეზერვო ასლის შექმნა შეწყდება. მყარ დისკზე დაზიანებული სექტორების არსებობისას აღნიშნული ფუნქცია იძლევა სარეზერვო ასლის შექმნისა და რაც შეიძლება მეტი მოცულობის მყარი დისკის მონაცემების შენახვის საშუალებას.

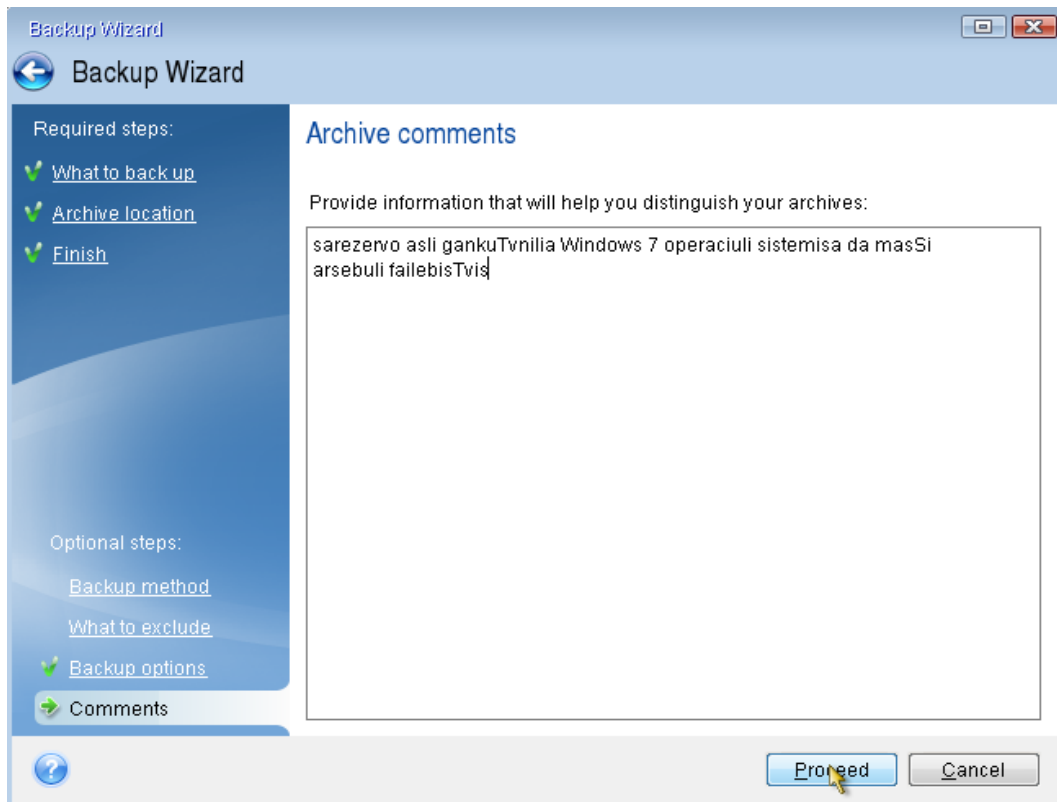
ვ) **Archive validation** - სარეზერვო ასლის შემოწმება

მიუთითეთ შემოწმების დამატებითი პარამეტრები: **Validate backup archive when it is created**:

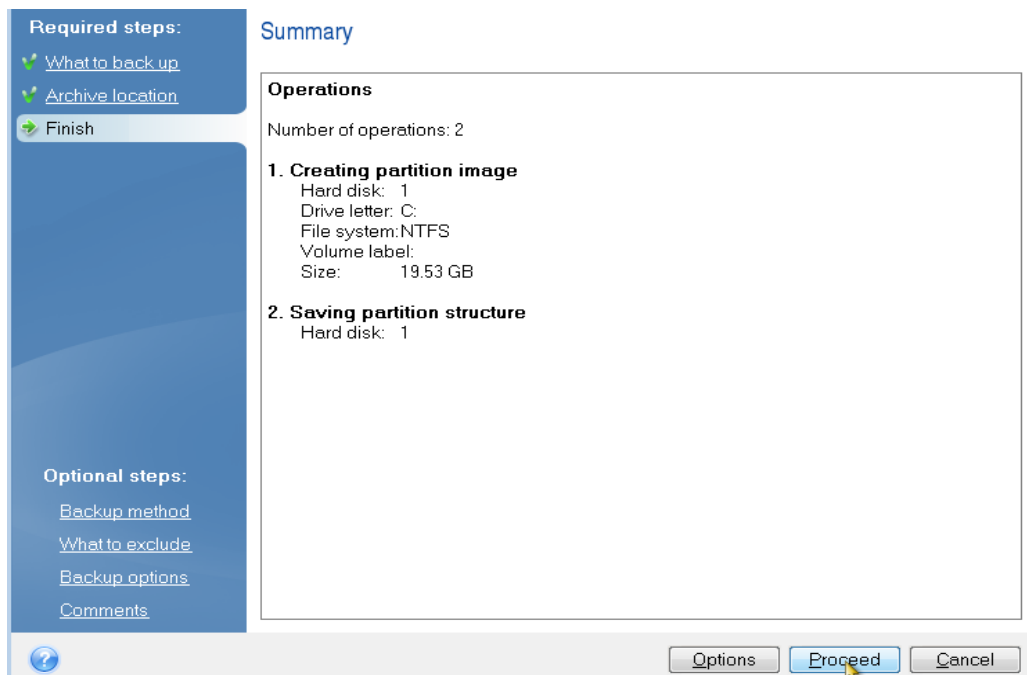


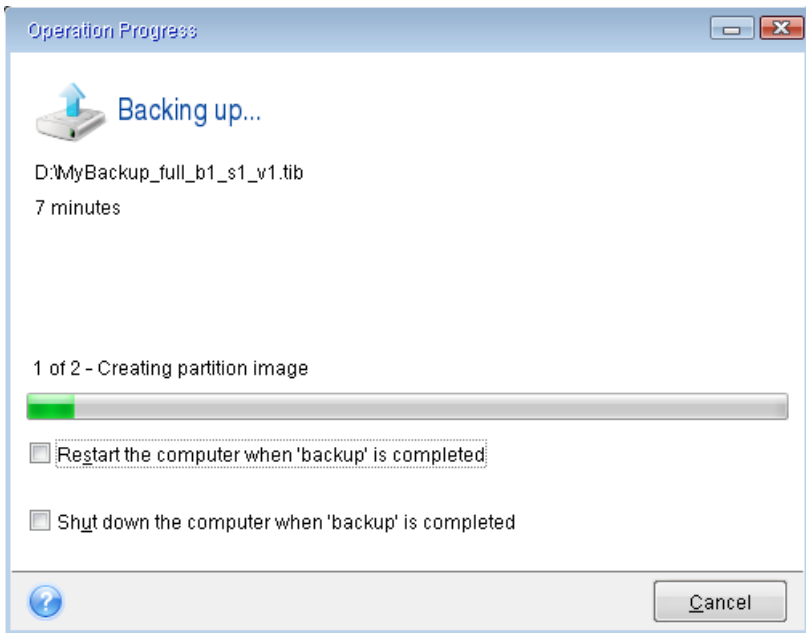
როცა ეს პარამეტრია ჩართული, სარეზერვო ასლის ან მისი დამატებითი ვერსიის შექმნისთანავე ხდება მისი მთლიანობის შემოწმება. კრიტიკულად მნიშვნელოვანი მონაცემების სარეზერვო ასლების, დისკის ან დანაყოფის ასლის შექმნისას მკაცრად არის რეკომენდებული ამ ფუნქციის ჩართვა, რათა გარანტირებულ იქნეს სარეზერვო ასლის ვარგისიანობა დაზიანებული მონაცემების აღდგენის შემთხვევაში.

IV ეტაპი - **Comments** - ამ პარამეტრით შესაძლებელია კომენტარების დამატება სარეზერვო ასლებზე, რაც საშუალებას იძლევა გავარჩიოთ ერთმანეთისგან ასლები (ორი და მეტის არსებობის შემთხვევაში):



მას შემდეგ რაც მოვმართეთ ჩვენთვის საჭირო პარამეტრები, ვაწვებით **Proceed** ღილაკს და დაიწყება სარეზერვო ასლის შექმნა.





Shut down the computer when

"backup" is completed მონიშვნის შემთხვევაში, სარეზერვო ასლის შექმნის შემდეგ კომპიუტერი დაიწყებს გათიშვას, რაზედაც გამოვა შეტყობინება, რომ 15 წამში გაითიშება კომპიუტერი. ჩვენ შეგვიძლია დავაჩქაროთ ეს პროცესი და დავაწვეთ დილაკს **Shutdown**.

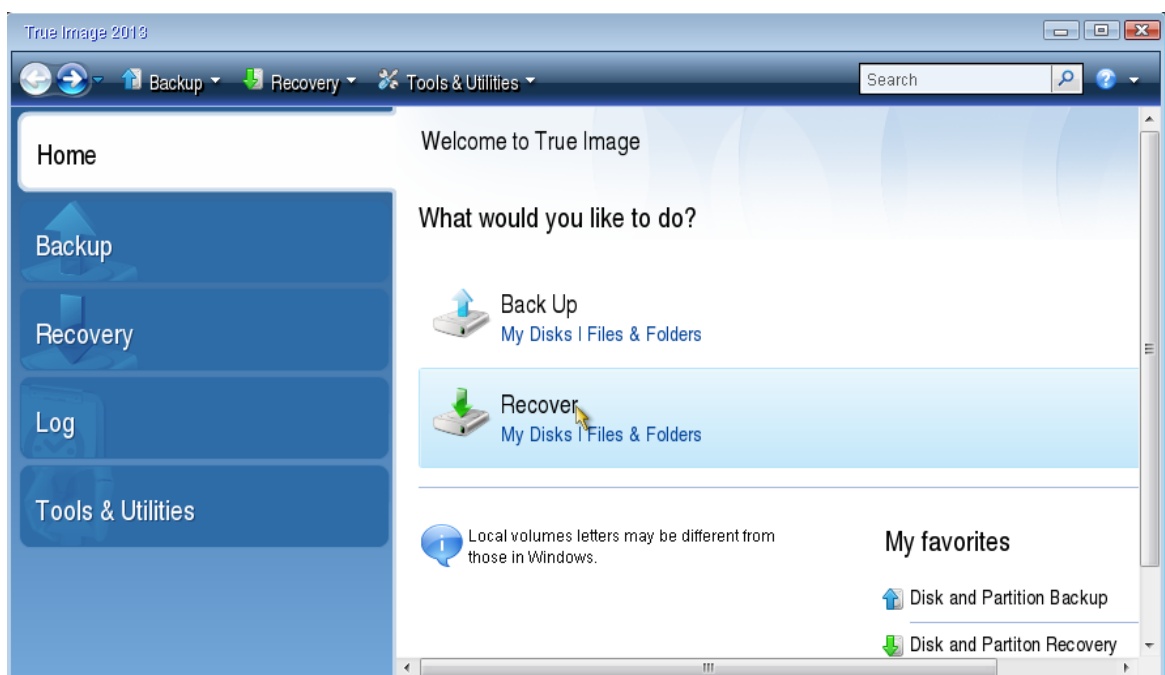
Restart the computer when "backup" is completed - სარეზერვო ასლის შექმნის შემდეგ კომპიუტერი გადაიტვირთება.

ოპერაციული სისტემის ან კონკრეტული საქალაქების სარეზერვო ასლის აღდგენა

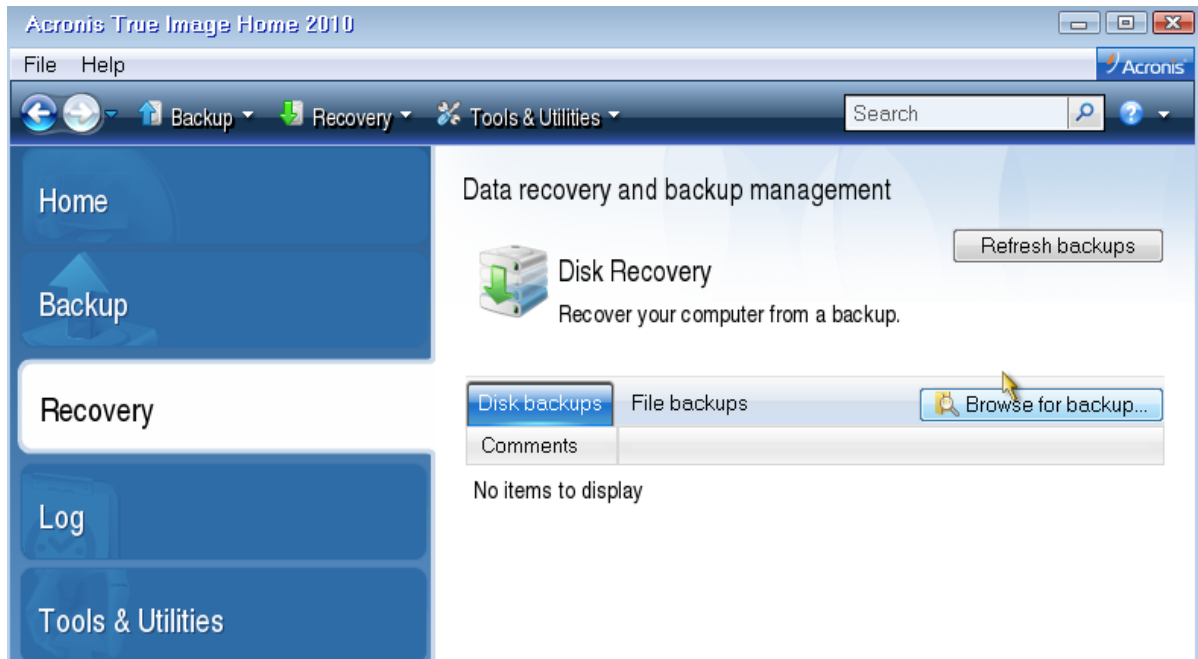
სარეზერვო ასლის აღდგენა შეიძლება დაგვჭირდეს:

- **Windows**-ის ფაილების გაფუჭების ან ნებისმიერი პროგრამული უზრუნველყოფის დაზიანების შემთხვევაში;
- წაგვეშალა ისეთი დოკუმენტები, რომელიც ჩავაყოფეთ სარეზერვო ასლში;
- უბრალოდ გვინდა ამ ასლის აღდგენა სხვა ლოგიკურ დისკზე ან სხვა კომპიუტერზე.

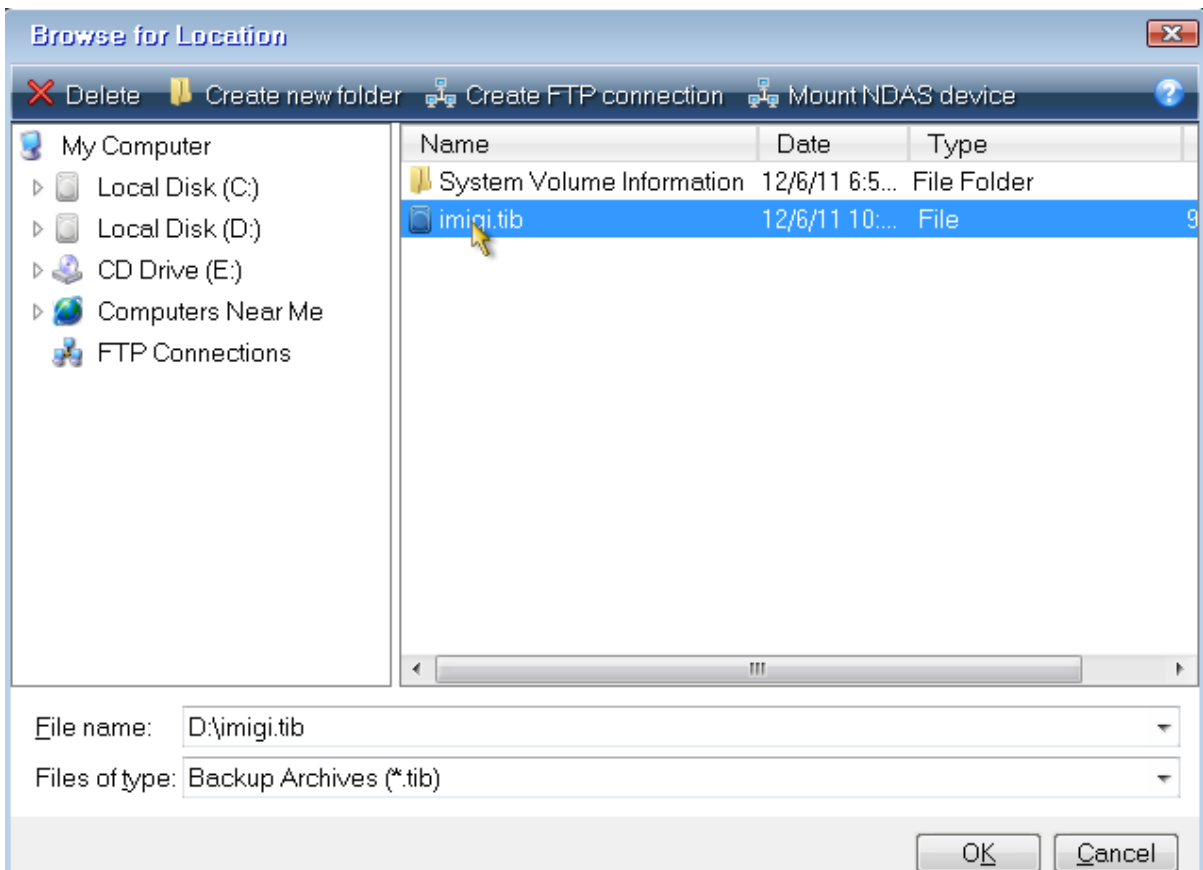
ასლის აღდგენისათვის ვატარებთ იგივე პროცედურებს რომელიც ეხება დისკიდან ჩატვირთვას და გამოსულ მენიუში უკვე ვირჩევთ **Recover** ბრძანებას:



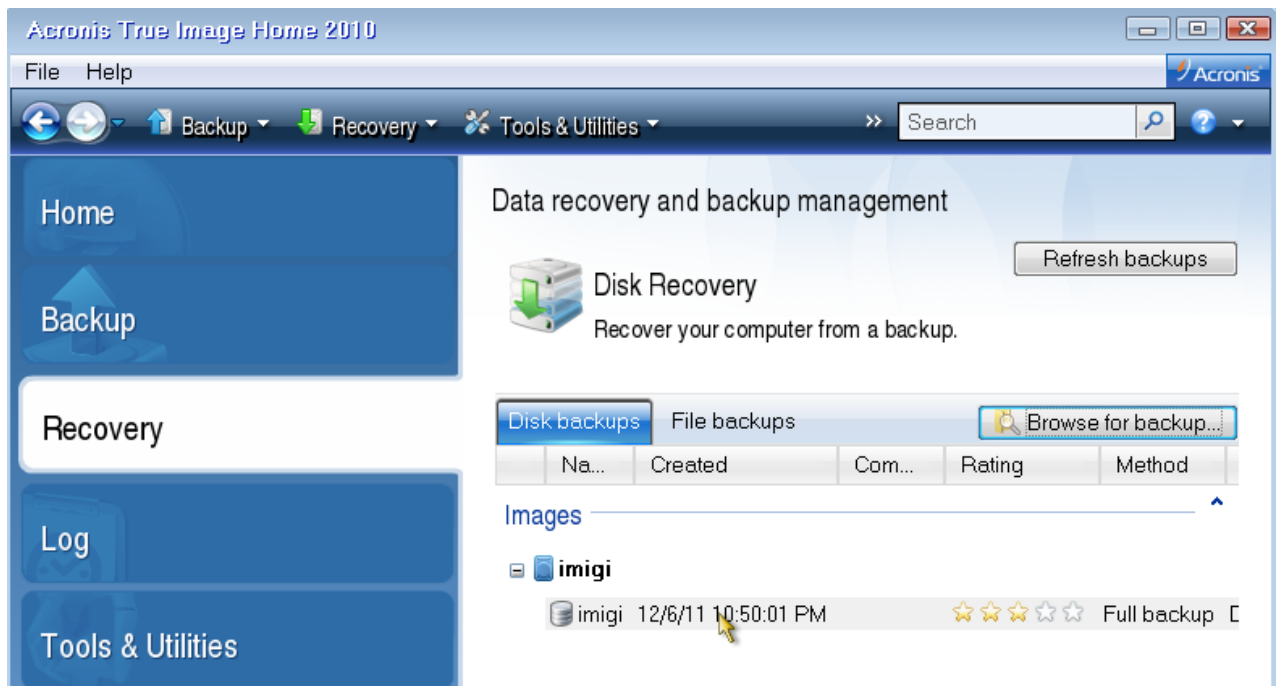
ქვემოთ მოცემულ ფანჯარაში ვაწვებით **Browse for backup**



ვირჩევთ იმ ადგილს სადაც იმყოფება სარეზერვო ასლი (ჩვენს შემთხვევაში ვირჩევთ **D:** დისკს, მოვნიშნავთ სასურველ ასლს (ჩვენს შემთხვევაში გვაქვს ერთი - **imigi.tib**, მაგრამ შეგიძლიათ იქონიოთ რამოდენიმე) და ვაწვებით **OK**-ის.



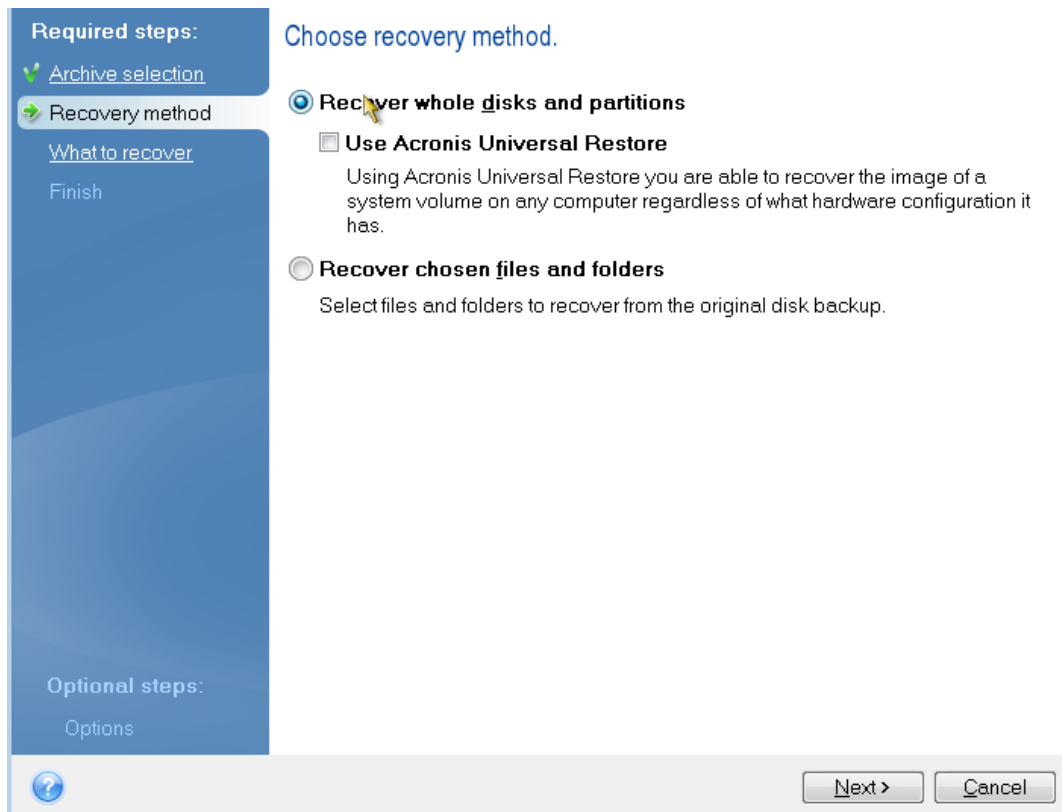
შემდეგ ფანჯარაში მაუსის მარჯვენა ღილაკით დააწექით სარეზერვო ასლს და გამოსულ კონტექსტურ მენიუში აირჩიეთ **Restore**:



მომდევნო ეტაპზე ვირჩევთ აღდგენის მეთოდს. გვაქვს ორი ვარიანტი:

I ვარიანტი - Recover whole disks and partitions - მთლიანი დისკის და დანაყოფების აღდგენა;

➤ **Use Acronis Universal Restore** - ამ ფუნქციის გამოყენებით თქვენ შეგიძლიათ აღადგინოთ სარეზერვო ასლი ნებისმიერი კომპიუტერის სისტემურ დანაყოფზე, მიუხედავად იმისა რა აპარატურული მოწყობილობები აყენია ზედ.



Acronis Universal Restore ფუნქცია სისტემის ჩამტვირთავი ასლის სხვა მოწყობილობაზე აღდგენის საშუალებას იძლევა. მოცემული პარამეტრის არჩევა ხდება სისტემური დისკის აღდგენისას კომპიუტერზე, რომლისთვისაც შეიქმნა სარეზერვო ასლი, მაგრამ მასზე მოხდა პროცესორის, დედაპლათის ან მეხსიერების სხვა მოწყობილობების შეცვლა. ეს ფუნქცია გამოიყენება მაშინ, როცა მაგალითად მოხდა დაზიანებული დედაპლათის შეცვლა ან პერსონალური კომპიუტერიდან ნოუთბუქზე მოხდა სისტემის გადატანა. **Acronis Universal Restore** გამოიყენება სისტემური დისკის აღსადგენად როგორც **TIB** ფაილებიდან, ისე **VHD** ფაილებიდან. ოპერაციული სისტემის ჩასატვირთად საჭიროა მყარი დისკის კონტროლერისა და ახალი დედაპლათის ჩიფსეტის დრაივერები, ამიტომ აღდგენის დაწყებამდე მოიმარაგეთ ისინი, **EXE, CAB, ZIP** ფორმატის შემთხვევაში ამოარქივით ისინი. დრაივერების ფაილებს უნდა ჰქონდეთ **INF, SYS** ან **OEM** გაფართოება.

სისტემის აღსადგენად უმეტესად ხელსაყრელია ჩამტვირთავი მატარებლის გამოყენება, რომელიც უნდა შეიცავდეს **Acronis Universal Restore-ის** დამატებით კომპონენტს. ამიტომ **Acronis True Image Home Plus Pack** დაყენების შემდეგ აუცილებელია ჩამტვირთავი მატარებლის ხელახლა შექმნა.

Acronis Universal Restore-ის დანიშნულება

Acronis Universal Restore შედის **Acronis True Image Home Plus Pack**-ის ცალკე დამატებით მოდულში. **Acronis True Image Home Plus Pack** ინსტალირდება ცალკე საინსტალაციო ფაილიდან და მოითხოვს ცალკე ლიცენზირებას. დამატება **Acronis Universal Restore**-ის ჩამტვირთავი მატარებლიდან აღდგენის გარემოში გამოსაყენებლად, საჭიროა ჩამტვირთავი მატარებლის ხელახლა შექმნა.

ოპერაციული სისტემისა და მონაცემების აღდგენა მარტივად შეიძლება იმავე ან მსგავსი კონფიგურაციის მქონე კომპიუტერზე ადრე შექმნილი ასლიდან. მაგრამ თუ შეიცვლება სისტემური პლატა ან პროცესორი, რაც სრულიად შესაძლებელია მოწყობილობის დაზიანების შემთხვევაში, აღდგენილი სისტემა შეიძლება არ ჩაიტვირთოს.

მცდელობა სისტემის ახალ, უფროპროდუქტულ კომპიუტერზე გადატანისა იმავე შედეგთან მიგვიყვანს. ეს ხდება ასლის მკაცრად აუცილებელი დრაივერების შეუთავსებლობით ახალი მოწყობილობის დრაივერებთან.

Microsoft System Preparation Tool (Sysprep) ინსტრუმენტის გამოყენება ვერ გადაჭრის ამ პრობლემას. ინსტრუმენტი **Sysprep** მხოლოდ **Plug-and-Play** მოწყობილობების დრაივერების შეცვლის საშუალებას იძლევა (ხმის, ქსელური, ვიდეო კარტის და სხვა).

მაგრამ მოწყობილობის აბსტრაგირების ფენა (**Hardware Abstraction Layer, HAL**) და მესხიერების მოწყობილობა უნდა იყოს იდენტური თავდაპირველ და სამიზნე კომპიუტერებზე.

Acronis Universal Restore ტექნოლოგია ეფექტურად წყვეტს სისტემის აპარატურულ-დამოუკიდებელ აღდგენას მოწყობილობის აბსტრაგირებული ფენის სისტემური დრაივერებისა და მესხიერების მოწყობილობის დრაივერების შეცვლის გზით.

ტიპური სიტუაციები, როდესაც გამოიყენება **Acronis Universal Restore**:

- ◆ მწყობრიდან გამოსული სისტემის სწრაფი აღდგენა სხვა მოწყობილობაზე.
- ◆ ოპერაციული სისტემების აპარატურულ-დამოუკიდებელი კლონირება.

შეზღუდვები Acronis Universal Restore-ის გამოყენებისას

1. **Acronis Universal Restore**-ით აღდგენილი სისტემა შეიძლება არ ჩაიტვირთოს, თუ დანაყოფების სტრუქტურა ასლში ან სამიზნე დისკზე არ ემთხვევა საწყისი დისკის დანაყოფების სტრუქტურას. ასლიდან აღდგენილი ჩამტვირთავი მიუთითებს არასწორ დანაყოფს და სისტემა არ ჩაიტვირთება ან არასწორად იმუშავებს.

ასეთი რამ შეიძლება მოხდეს, თუ:

- ასლი შეიცავს მხოლოდ ზოგიერთ დანაყოფს და არა დისკს მთლიანად;
- აღდგენილ იქნა მხოლოდ ზოგიერთი დანაყოფი და არა დისკი მთლიანად.

ზოგჯერ, განსაკუთრებით მაშინ, როცა სისტემა არ არის მოთავსებული საწყის დანაყოფზე, ამან შეიძლება დაარღვიოს ჩამტვირთავის მუშაობა და აღდგენილი სისტემას არ შეუძლია ჩატვირთვა.

ამგვარი პრობლემების თავიდან ასაცილებლად რეკომენდებულია მთელი სისტემური დისკის ასლის შექმნა და მთელი დისკის აღდგენა.

2. ფუნქცია **Acronis Universal Restore** არ მუშაობს, თუ სამიზნე კომპიუტერი იტვირთება **Acronis Startup Recovery Manage**-ის (კლავიში **F11**) დახმარებით ან სარეზერვო ასლი მოთავსებულია აკრონისის უსაფრთხოების ზონაში (**Acronis Secure Zone**). ეს იმიტომ ხდება, რომ **Acronis Startup Recovery Manage** და **Acronis Secure Zone** განკუთვნილია ძირითადად ერთსა და იმავე კომპიუტერზე მონაცემთა აღსადგენად.

Acronis Universal Restore მუშაობის პრინციპი

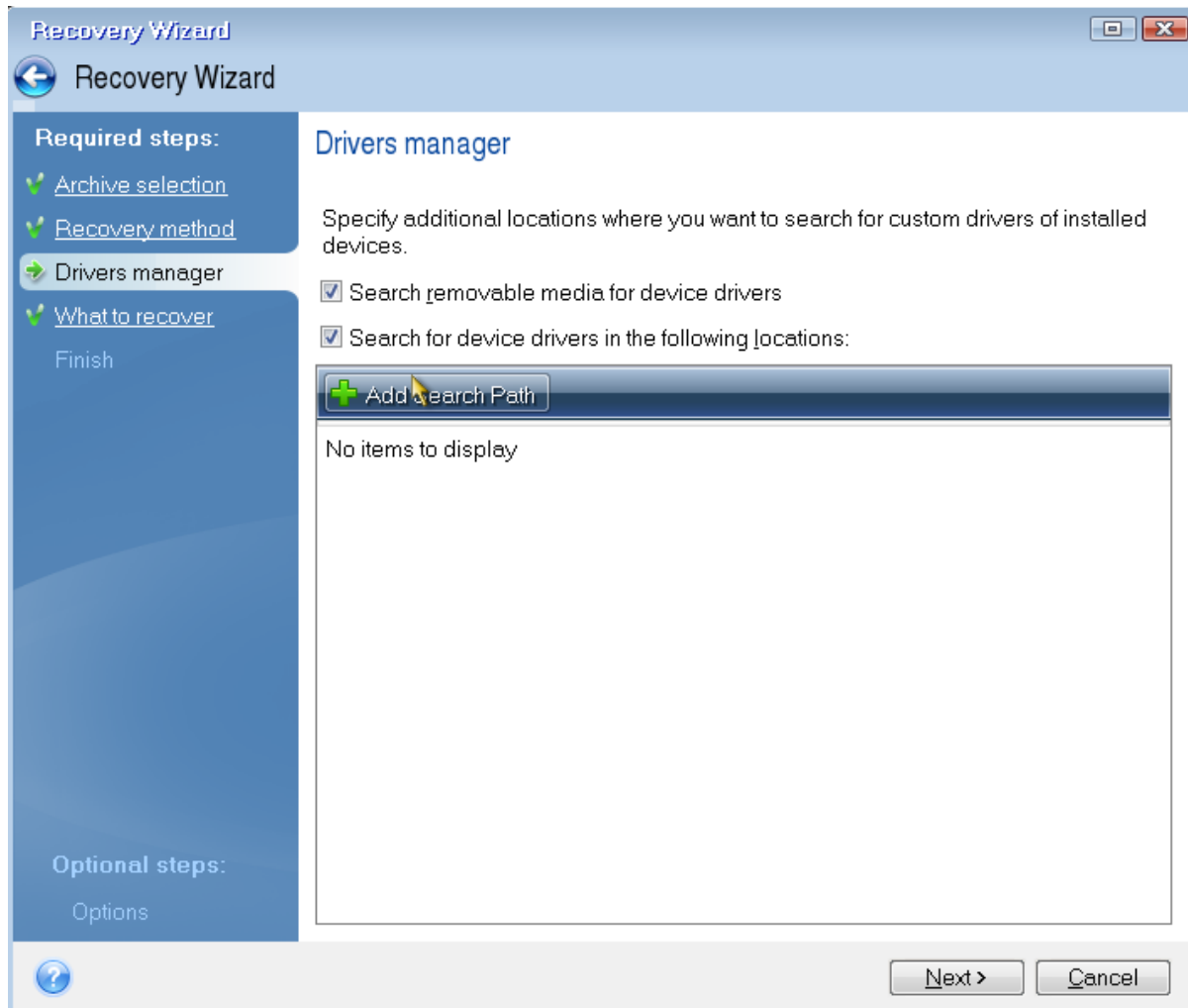
1. აპარატულ-დამოკიდებული დონის (**HAL**) და მეხსიერების მოწყობილების ავტომატური არჩევა.

Acronis Universal Restore ახდენს **HAL**-ის და მეხსიერების მოწყობილობის დრაივერის ძიებას **Windows**-ის დრაივერების შენახვის სტანდარტულ ადგილებში (აღსადგენი სისტემის ასლში) და აყენებს მთელი კომპიუტერის აპარატულ ნაწილთან ყველაზე უფრო მისადაგებულ დრაივერებს.

შესაძლებელია დრაივერების შენახვის სხვა ადგილების მითითებაც (ქსელურ დისკის საქალაქდები ან **CD**), სადაც ასევე მოხდება დრაივერების ძიება. **Acronis Universal Restore**-ს შეუძლია დრაივერების ძებნა გადამტან მატარებლებზე.

2. **Plug-and-Play** მოწყობილობების დრაივერების დაყენებისას **Acronis Universal Restore**-ში გამოიყენება **Plug-and-Play**-ის აღმოჩენისა და დაყენების ჩაშენებული მექანიზმი მოწყობილობის კონფიგურაციის სხვაობის აღმოსაჩენად, სისტემის არა კრიტიკული გაშვებისთვის. ასეთ მოწყობილობებს მიეკუთვნება ვიდეო, აუდიო და **USB**-მოწყობილობები. სისტემაში შესვლის მოთხოვნის გამოსახვისას მართვა გადაეცემა

აღდგენილ **Windows** ოპერაციულ სისტემას. თუ ახალი მოწყობილობების ნაწილი არ მონახება ან არ დაყენდება, მათი დრაივერების მომართვა შესაძლებელია ხელით.



თუ მოვნიშნავთ **Use Acronis Universal Restore** პუნქტს და დავაწვებით **Next** ღილაკს, გამოგვივა ფანჯარა, სადაც შეგვიძლია განვსაზღვროთ დამატებითი ადგილი სადაც გვსურს რომ სისტემამ მოძებნოს დაყენებული მოწყობილობების დრაივერები. გვაქვს ორი ვარიანტი:

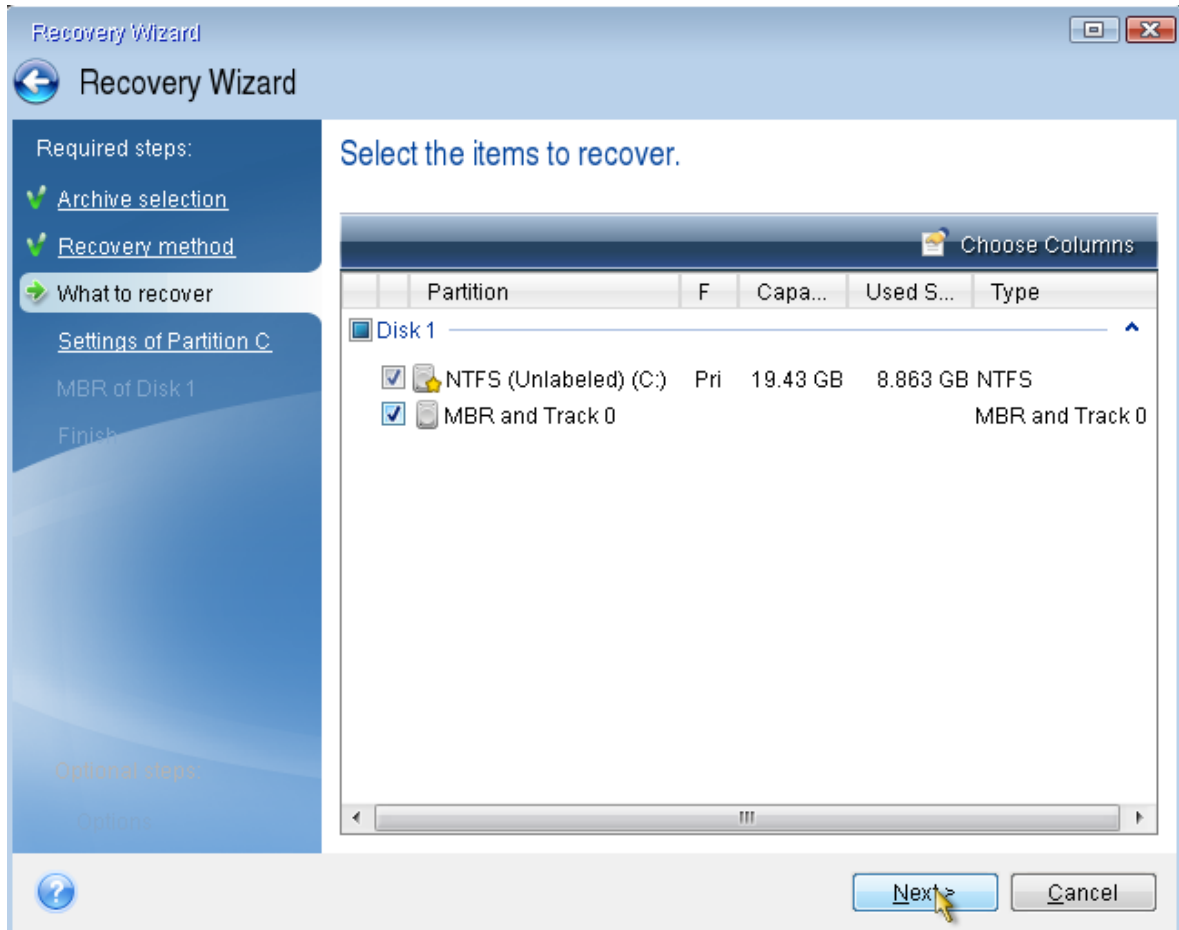
- **Search removable media for device drivers** - მოძებნოს მოწყობილობების დრაივერები ფლემ მებსიერებაზე.

- **Search for device drivers in the following locations** - მოძებნოს მოწყობილობათა დრაივერები მითითებული ადგილიდან. ამ პუნქტის მონიშვნის შემთხვევაში გააქტიურდება ღილაკი **Add Search Path**, სადაც შეგვიძლიათ მიუთითოთ დრაივერების ზუსტი მდებარეობა.

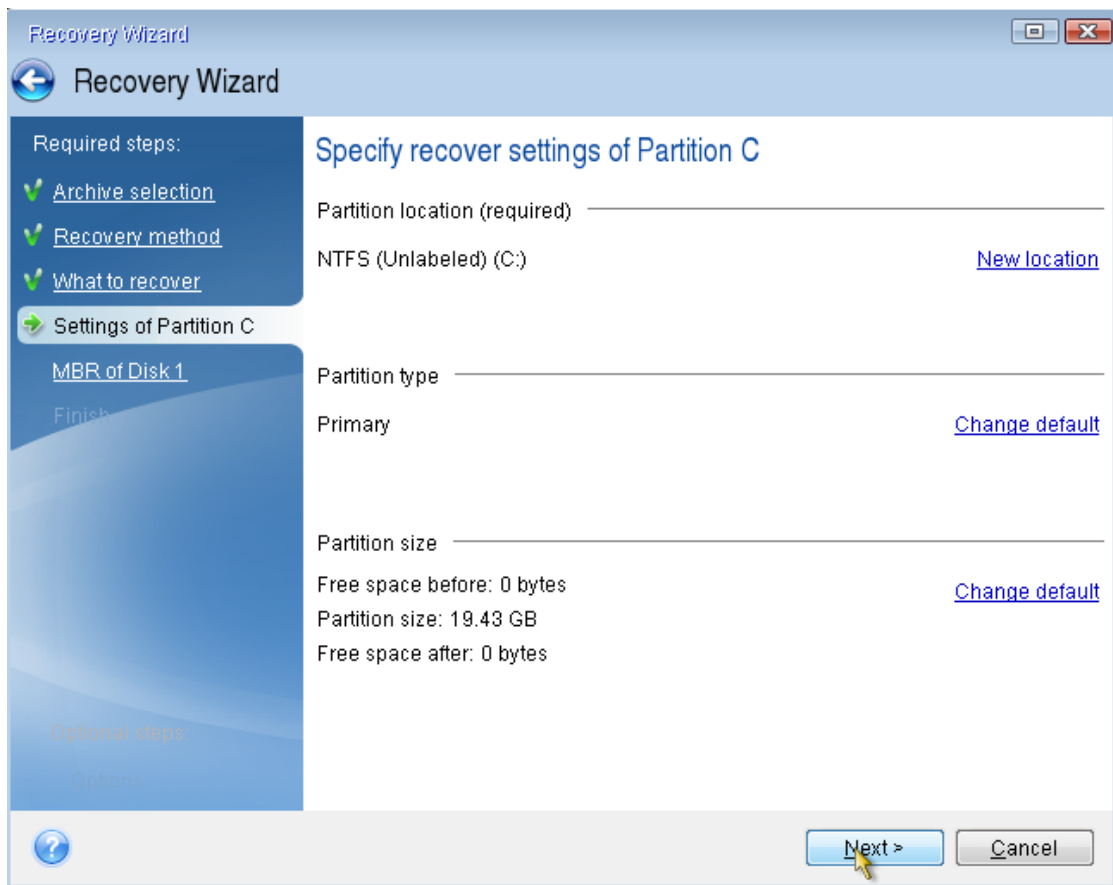
II ვარიანტი - Recover chosen files and folders - შერჩეული ფაილების და ფოლდერების აღდგენა. ამ პუნქტის მონიშვნის შემთხვევაში თუ დავაჭერთ **Next** ღილაკს, გამოვა

ფანჯარა, სადაც შეგვიძლია ავირჩიოთ ის საქალაქე ან საქალაქეები, რომელთა აღდგენაც გვინდა შექმნილი ასლიდან.

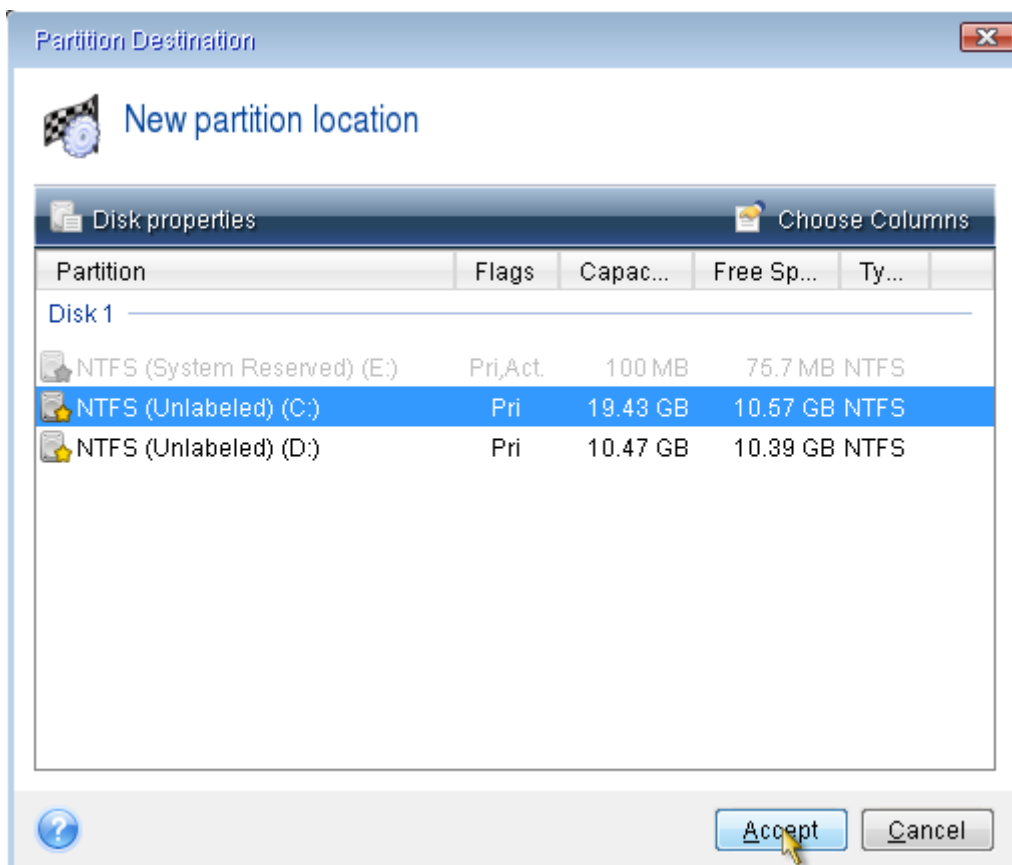
თუ ავირჩევთ I ვარიანტს (**Recover whole disks and partitions**), მაშინ **Next** ლილაკზე დაჭერის შემდეგ გამოსულ ფანჯარაში უნდა ავირჩიოთ დანაყოფი ან დანაყოფები რომელთა აღდგენაც გვინდა.



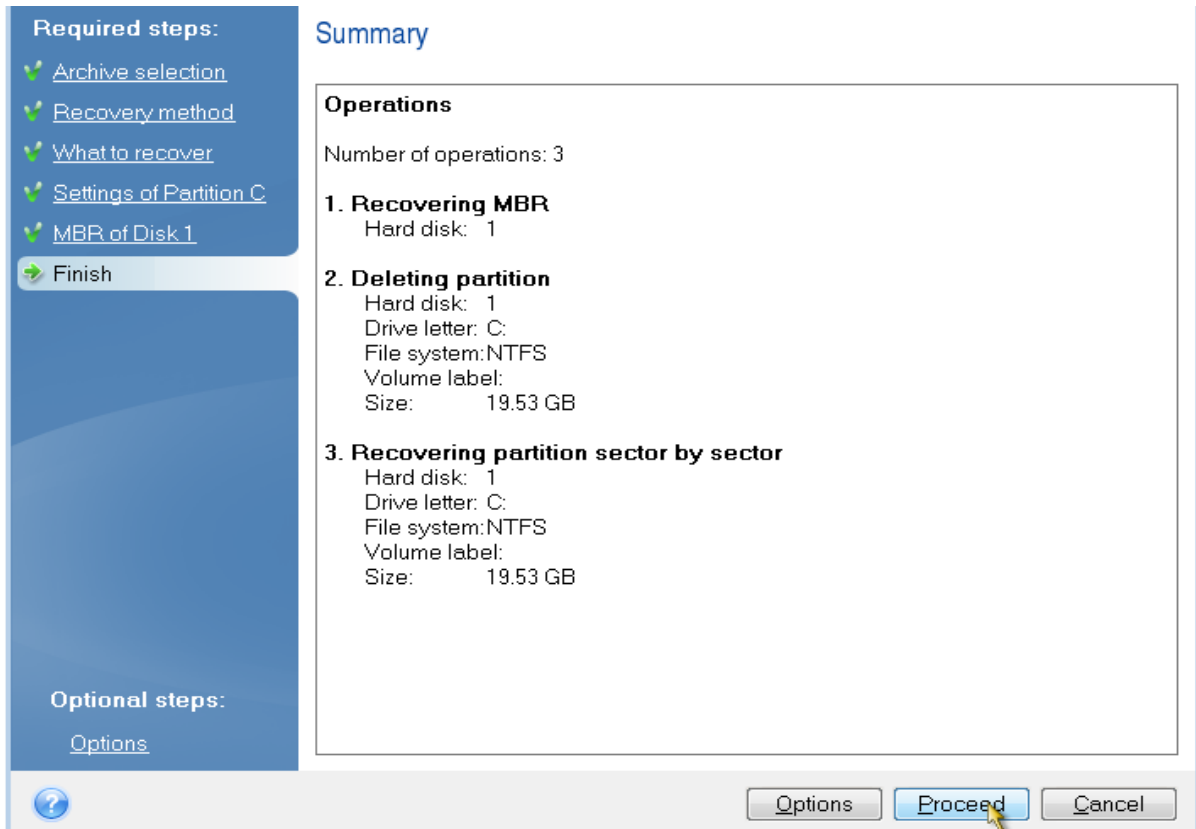
მომდევნო ფანჯარაში უნდა მოვმართოთ იმ დანაყოფის პარამეტრები სადაც ხდება აღდგენა, ამისთვის ვაწვევით **New Location** მიმართვას.



გამოსულ ფანჯარაში ფანჯარაში ვუთითებთ აღდგენის ზუსტ მდებარეობას, შემდეგ ვაწვებით **Accept** და **Next**.

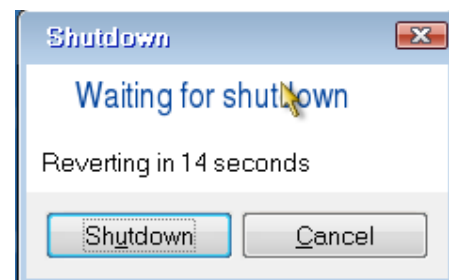
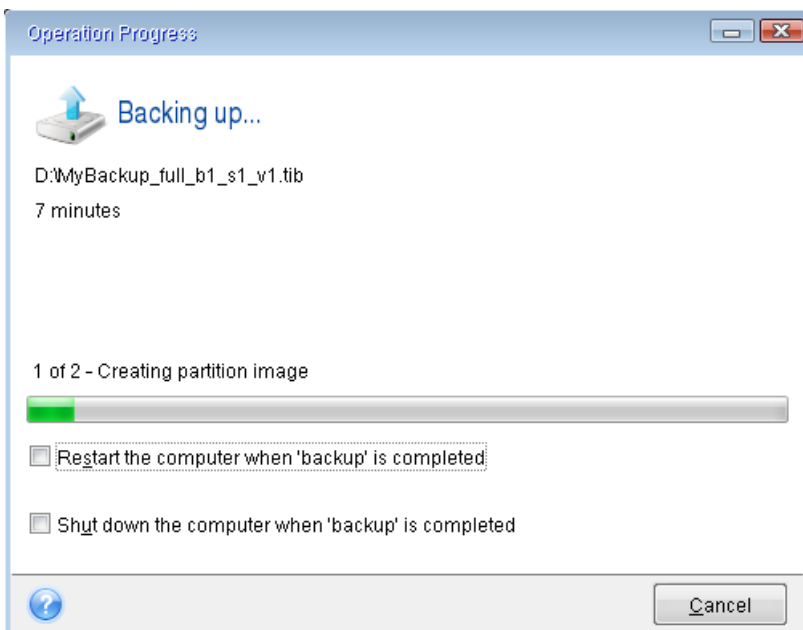


ბოლოს ვაწვებით **Proceed** ღილაკს აღდგენის დასაწყებად:



Shut down the computer when "backup" is completed მონიშვნის შემთხვევაში, სარეზერვო ასლის აღდგენის შემდეგ კომპიუტერი დაიწყებს გათიშვას, რაზედაც გამოვა შეტყობინება, რომ 15 წამში გაითიშება კომპიუტერი. ჩვენ შეგვიძლია დავაჩქაროთ ეს პროცესი და დავაწვეთ ღილაკს **Shutdown**.

Restart the computer when "backup" is completed - სარეზერვო ასლის შექმნის შემდეგ კომპიუტერი გადაიტვირთება.



6.4 არსებული სისტემების მონიტორინგი

სერვერების მონიტორინგი, მონაცემთა შემგროვებელი ნაკრებების (**Data Collector Sets**), შეტყობინებებისა და ღონისძიებების გამოყენებით საშუალებას გვაძლევს თვალი ვადევნოთ სერვერების წარმადობასა და კონფიგურაციას. თუმცა ეფექტურმა მონიტორინგმა ნაკლებად სავარაუდოა შეაჩეროს სერვერზე მიმდინარე პრობლემები. ის იძლევა გამაფრთხილებელ სიგნალებს განვითარებული პრობლემების შესახებ, და გაძლევთ შანსს გამოასწოროთ ისინი სერვისის მუშაობის შეფერხებამდე.

მონაცემთა შეგროვების ნაკრებების - Data Collector Sets კონფიგურაცია

მონაცემთა შემგროვებელი ნაკრებები საშუალებას გვაძლევს შევაგროვოთ წარმადობის მონაცემები, სისტემის კონფიგურაციის მონაცემები და სტატისტიკები ერთ ფაილში. თქვენ შეგიძლიათ გამოიყენოთ **Performance Monitor** ან სხვა გამომცემლის უტილიტები ამ ინფორმაციის ანალიზისთვის რათა შევამოწმოთ სერვერის ფუნქციურობა მიცემული დატვირთვის შემთხვევაში.

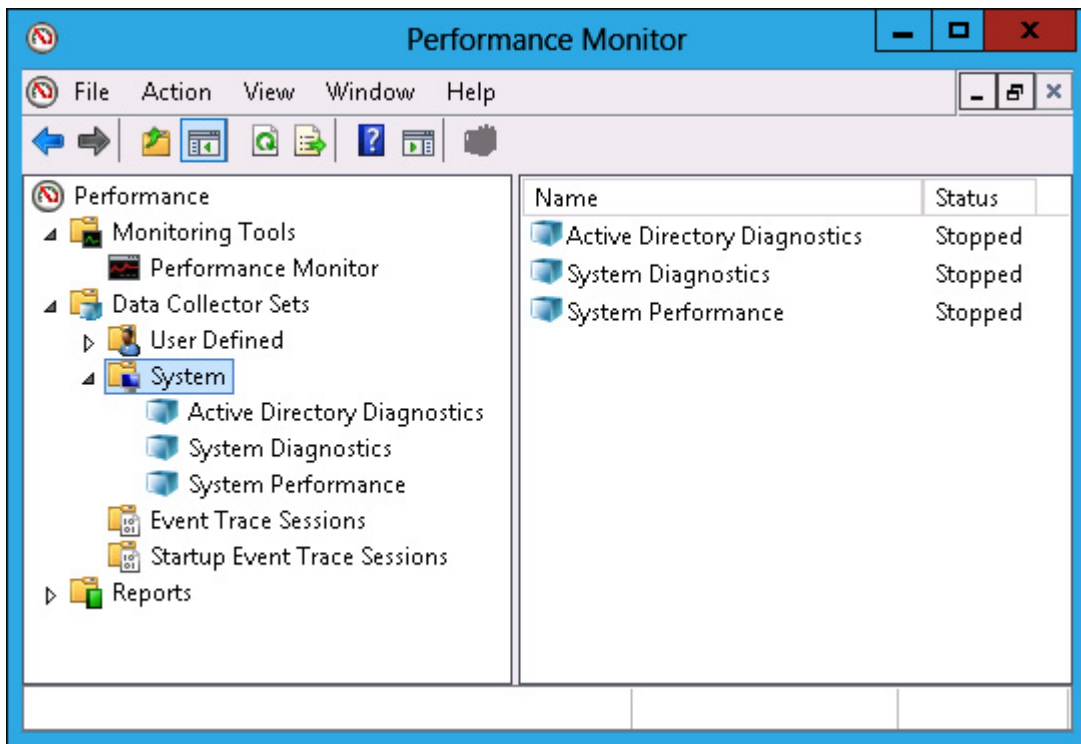
თქვენ შეგიძლიათ დააკონფიგუროთ მონაცემების შეგროვების ჯგუფი, მათ შორის:

- **Performance counter data** - წარმადობის მონაცემების მთვლელი - მონაცემების შეგროვების ჯგუფი მოიცავს არამარტო კონკრეტული წარმადობის მთვლელს, არამედ მონაცემებს, რომლებიც მიღებულ იქნა ამ მთვლელების დახმარებით.

- **Event trace data** - ღონისძიების თვალთვალის მონაცემი - საშუალებას იძლევა თვალყური ადევნოთ ღონისძიებებს და სისტემის აქტივობებს. ღონისძიების თვალთვალის მონაცემი შესაძლოა სასარგებლო იყოს ცუდ მდგომარეობაში მყოფი აპლიკაციებისა თუ სერვისების პრობლემის მოძიებისა და აღმოფხვრის პროცესში.

- **System configuration information** - სისტემის კონფიგურაციის ინფორმაცია - საშუალებას გაძლევთ თვალყური ადევნოთ რეგისტრის დანაყოფების მდგომარეობას და ჩაიწეროთ ამ დანაყოფებში გაკეთებული ნებისმიერი ცვლილება.

Windows Server 2012 და **Windows Server 2012 R2** მოიცავთ ქვემოთ მოცემულ ინტეგრირებულ მონაცემების შეგროვების ნაკრებს.



სურ.6.4. 1

▪ **Active Directory diagnostics** - ხელმისაწვდომია თუ თქვენ კომპიუტერზე დაინსტალირებული გაქვთ დომენური კონტროლერი; ის იძლევა მონაცემებს აქტიური დირექტორიის სიჯანსაღესა (**health**) და საიმედოობაზე.

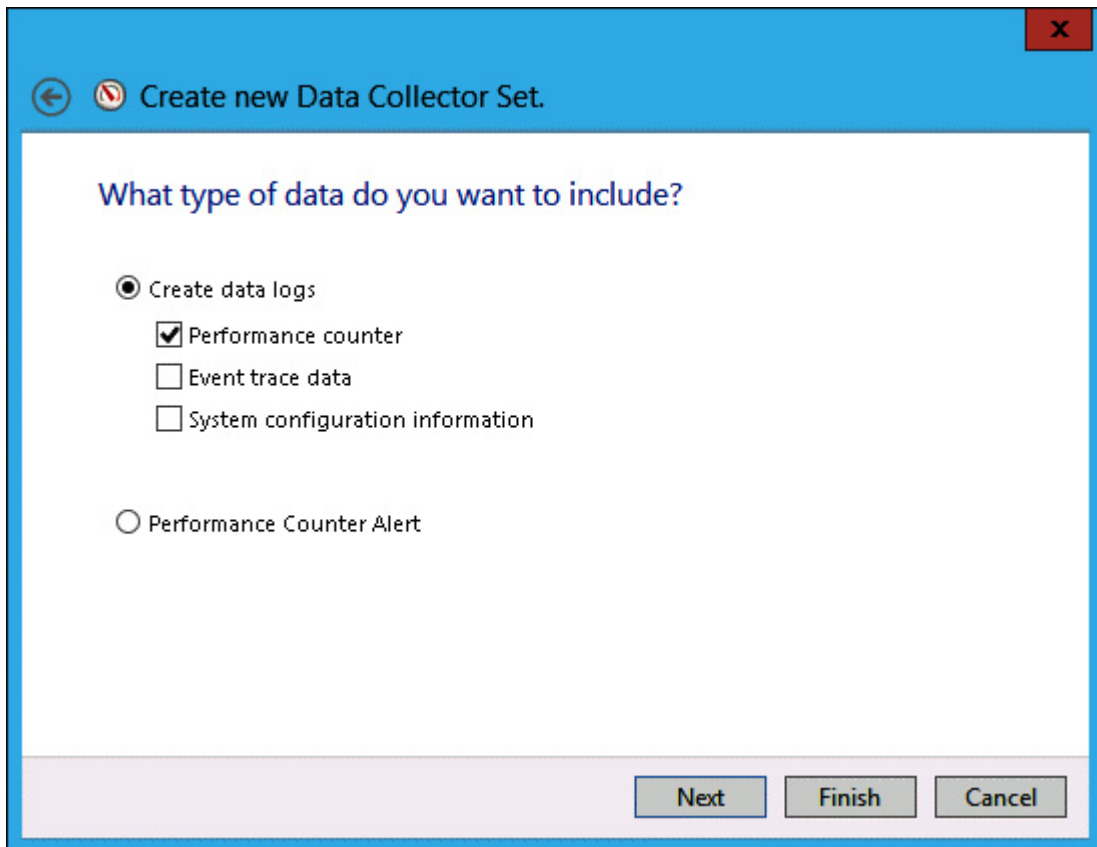
▪ **System diagnostics** - საშუალებას გაძლევთ მოიძიოთ და აღმოფხვრათ ტექნიკასთან, დრაივერებთან და წყვეტის შეცდომებთან დაკავშირებული პრობლემები.

▪ **System performance** - საშუალებას იძლევა დასვათ მძიმედ მომუშავე სისტემის წარმადობის პრობლემის დიაგნოზი. თქვენ შეგიძლიათ დაადგინოთ რომელმა პროცესებმა, სერვისებმა თუ ტექნიკურმა უზრუნველყოფან გამოიწვია წარმადობის შემცირება.

მონაცემთა შემგროვებელი ჯგუფის შესაქმნელად შეასრულეთ შემდეგი ეტაპები:

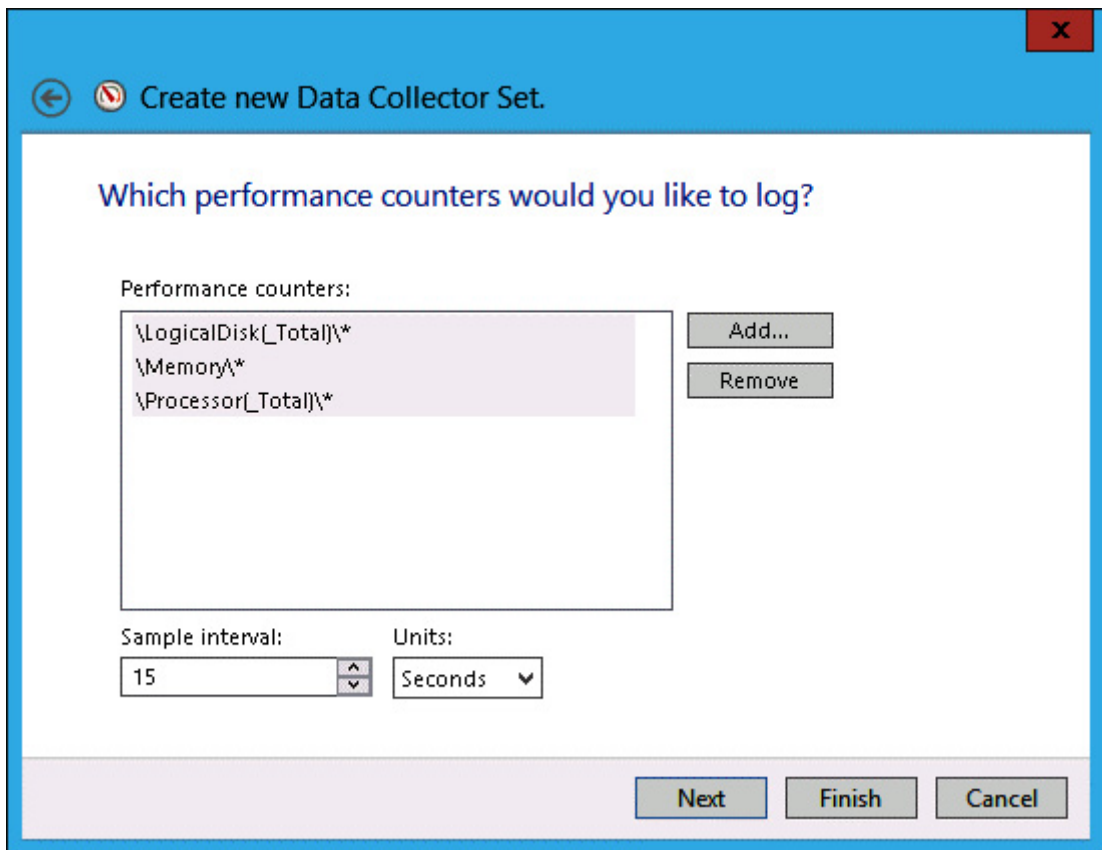
1. **Server Manager console**-ის **Tools** მენიუდან გახსენით **Performance Monitor**;
2. გახსენით მონაცემთა შემგროვებელი ჯგუფი.
3. დააჭირეთ **User Defined** პარამეტრს. **Action** მენიუში დააჭირეთ **New** ღილაკს და შემდეგ აირჩიეთ **Data Collector Set**.
4. თქვენ გეძლევათ შესაძლებლობა შექმნათ მონაცემთა შემგროვებელი ჯგუფი შაბლონიდან, რომელიც საშუალებას მოგცემთ აირჩიოთ არსებული მონაცემთა

შემგროვებელი ჯგუფიდან ან შექმნათ მონაცემთა შემგროვებელი ჯგუფი ხელით. თუ აირჩევთ მონაცემთა შემგროვებელ ნაკრებს ხელით, თქვენ გეყენებათ მონაცემთა ჟურნალის (Log) შექმნის საშუალება, რომელიც შეიძლება შეიცავდეს წარმადობის მთვლელს (Performance Counter), ღონისძიების თვალყურისდევნების მონაცემს (Event Trace Data), და სისტემის კონფიგურაციის ინფორმაციას ან წარმადობის მთვლელის გაფრთხილებას



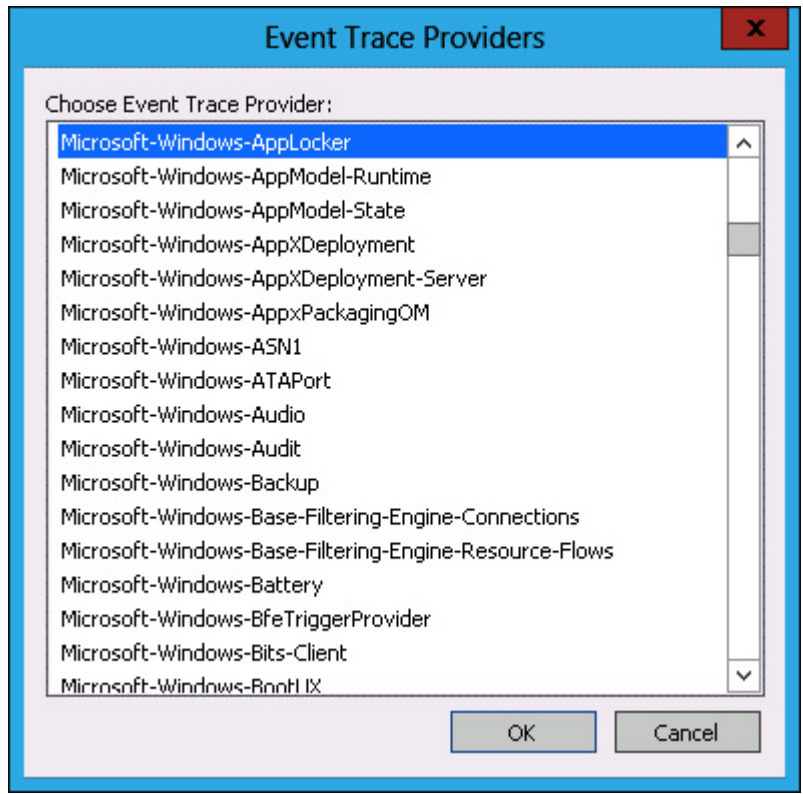
სურ.6.4. 2

5. თუ თქვენ მონიშნავთ **Performance Counter**-ს, შემდეგ თქვენ უნდა აირჩიოთ წარმადობის რომელი მთვლელეები უნდა დაემატოს მონაცემთა შემგროვებელ ნაკრებს. თქვენ ასევე უთითებთ რა სიხშირით მოახდინოს **Windows**-მა მონაცემების შეგროვება წარმადობის მთვლელეებიდან. როგორც სურათზეა ნაჩვენები, მონაცემები გროვდება ყოველ 15 წამში.



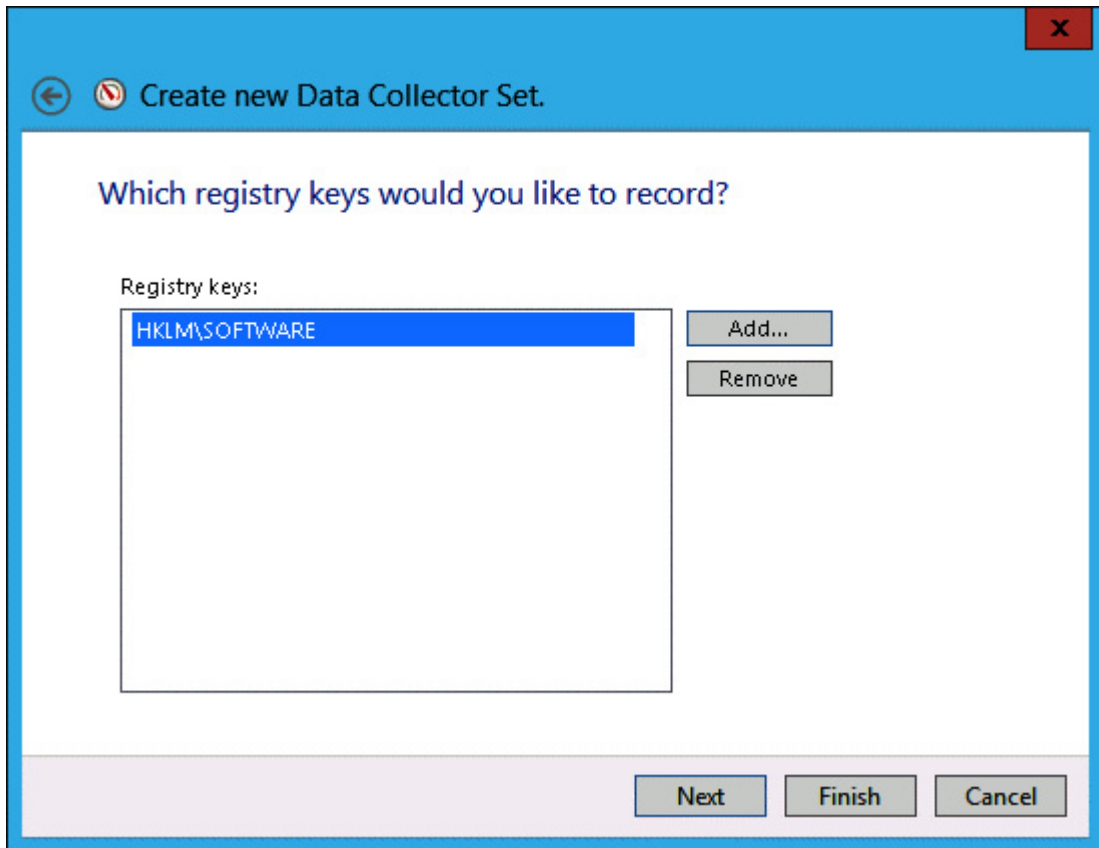
სურ.6.4. 3

6. თუ გადაწყვეტთ ჩართოთ ღონისძიებების თვალთვალის მონაცემი, თქვენ უნდა ჩართოთ ღონისძიების თვალთვალის მომწოდებლები (**Event Trace Providers**). როგორც სურათზეა ნაჩვენები, დიდი რაოდენობით ღონისძიების თვალთვალის მომწოდებლებია ხელმისაწვდომი **Windows Server 2012 R2**-ით. თქვენ იყენებთ ღონისძიების თვალთვალის მომწოდებლებს კონკრეტული პრობლემის მოძიებისა და აღმოფხვრის პროცესში. მაგალითად, **Microsoft Windows-AppLocker** ღონისძიების თვალთვალის პროვაიდერი დაგეხმარებათ დასვათ დიაგნოზი და აღმოფხვრათ **AppLocker**-თან დაკავშირებული პრობლემები.



სურ.6.4. 4

7. თუ აირჩევთ სისტემის კონფიგურაციის ინფორმაციის მონიტორინგს, თქვენ შეძლებთ აირჩიოთ რეგისტრების გასაღებები საკონტროლოდ, ისე როგორც ნაჩვენებია სურათზე. მშობელი გასაღების არჩევით საშუალება გეძლევათ აკონტროლოთ ყველა რეგისტრის ცვლილება, რომელიც ფიქსირდება მაშინ, როდესაც მონაცემის შემგროვებელი ჯგუფი არის გაშვებული.

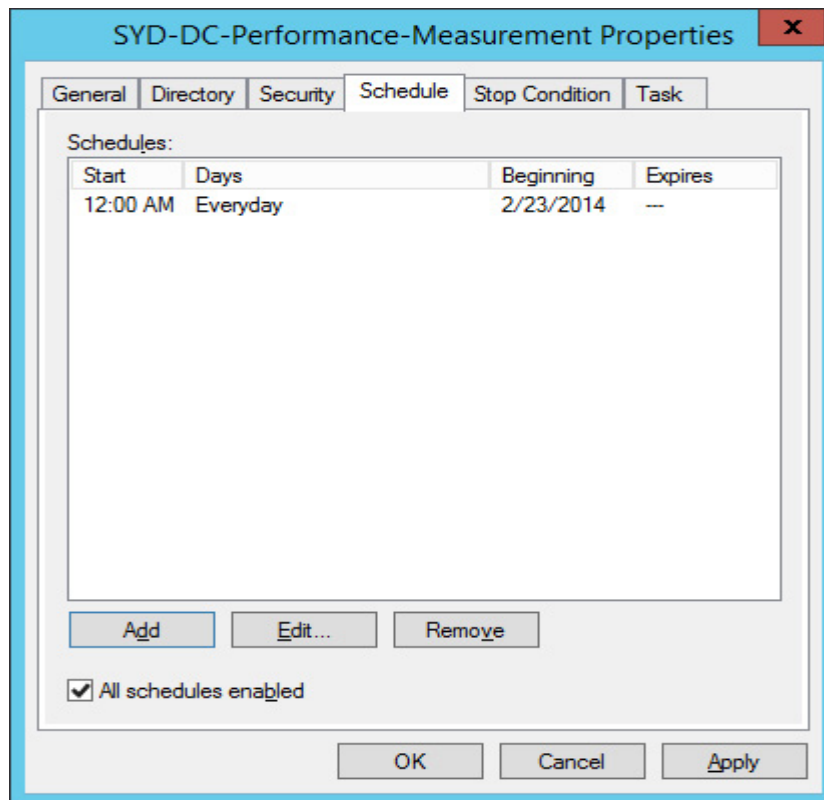


სურ.6.4. 5

8. შემდეგ ეტაპზე თქვენ უნდა მიუთითოთ სად გსურთ მონაცემის შემგროვებელი ჯგუფის მიერ თავმოყრილი მონაცემების განთავსება. ნაგულისხმევი ადგილი **%systemdrive%\PerfLogs\Admin** საქალაღდე. თუ განიზრახეთ მონაცემის შეგროვების ჯგუფის გაშვება დიდი ხნით, თქვენ უნდა მოათავსოთ მონაცემები იმ დანაყოფზე, რომელზეც არ არის ინსტალირებული ოპერაციული სისტემა.

9. მონაცემთა შემგროვებელი ჯგუფის პარამეტრების მომართვის ბოლო ეტაპია იმ სააღრიცხვო ჩანაწერის მითითება, რომლითაც მონაცემის შემგროვებელი ჯგუფი გაეშვება. ნაგულისხმევად დაყენებულია **Local System**, მაგრამ შეგიძლიათ დააკონფიგუროთ ისე, რომ მონაცემის შემგროვებელმა ნაკრებმა გამოიყენოს ნებისმიერი სხვა სააღრიცხვო ჩანაწერი ვისზეც გაქვთ წვდომის უფლება.

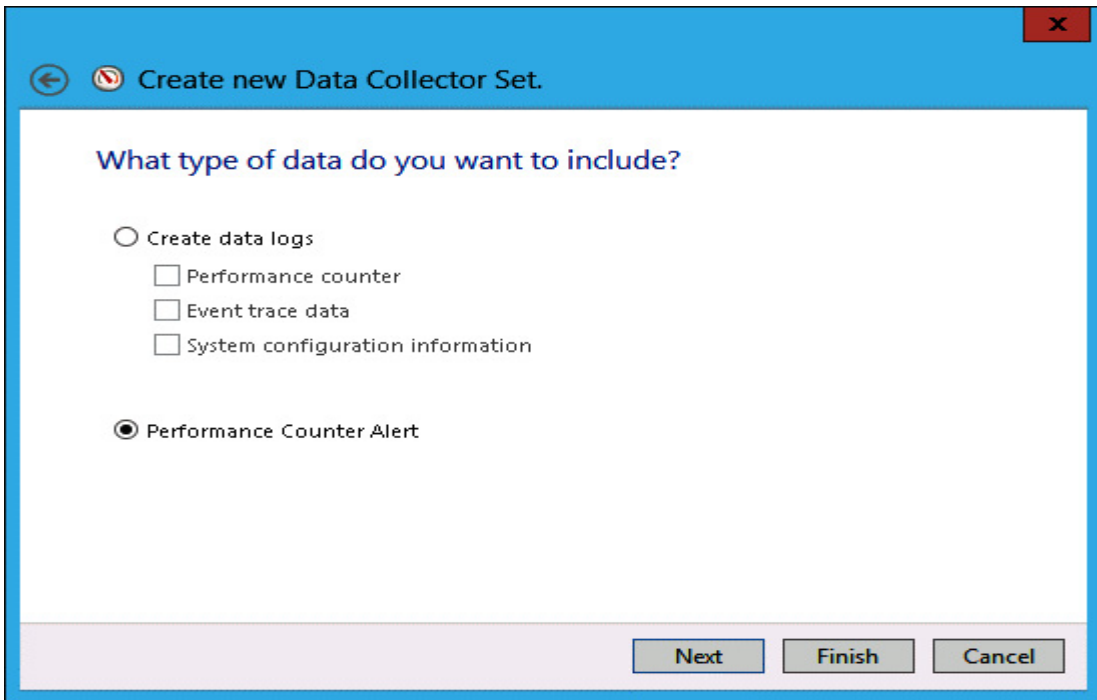
მონაცემის შემგროვებელი ჯგუფის თვისებების **Schedule** ჩანართიდან შეგიძლიათ დაგეგმოთ თუ როდის გაეშვას მონაცემის შემგროვებელი ჯგუფი



სურ.6.4. 6

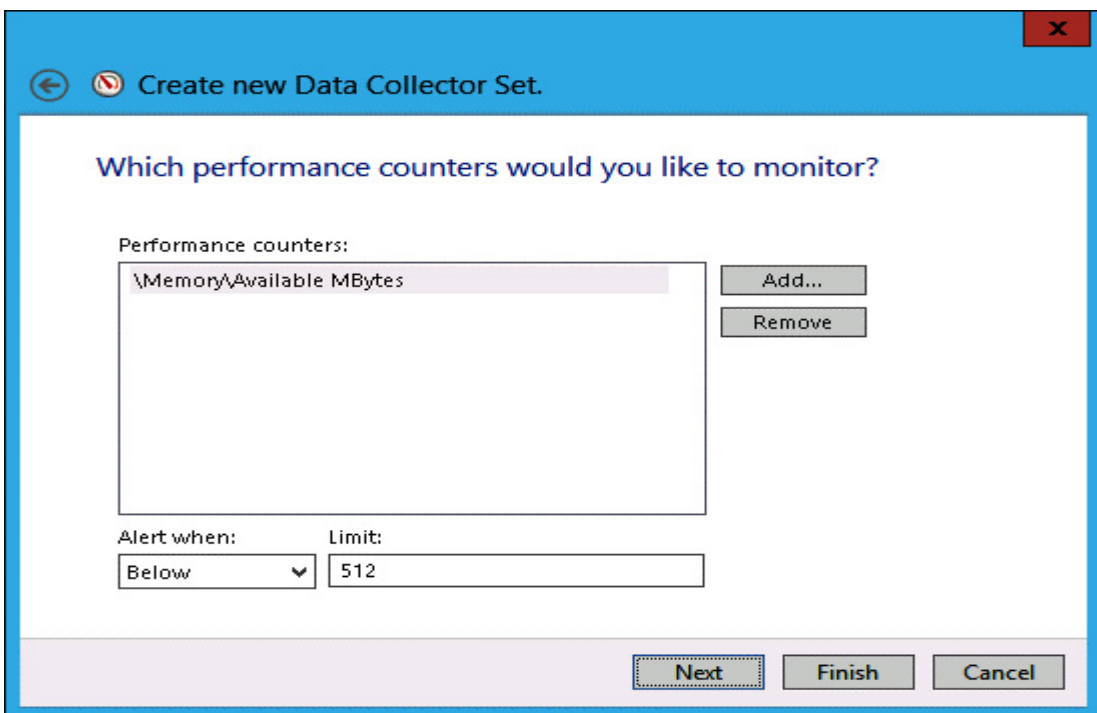
შეტყობინებების მართვა

წარმადობის მთვლელი შეტყობინებები საშუალებას გვაძლევენ დავაკონფიგუროთ დავალება ისე რომ მოხდეს მისი გაშვება, როდესაც წარმადობის მთვლელი, როგორცაა ხელმისაწვდომი დისკური სივრცე ან მეხსიერება ჩამოსცდება ან გადააჭარბებს კონკრეტულ მნიშვნელობას. წარმადობის მთვლელის შეტყობინების დასაკონფიგურებლად, ქმნით ახალ მონაცემთა შემგროვებელ ჯგუფს, ირჩევთ ხელით შექმნის პარამეტრს და ნიშნავთ **Performance Counter Alert** - წარმადობის მთვლელი შეტყობინების პარამეტრს, ისე როგორც ნაჩვენებია სურათზე.



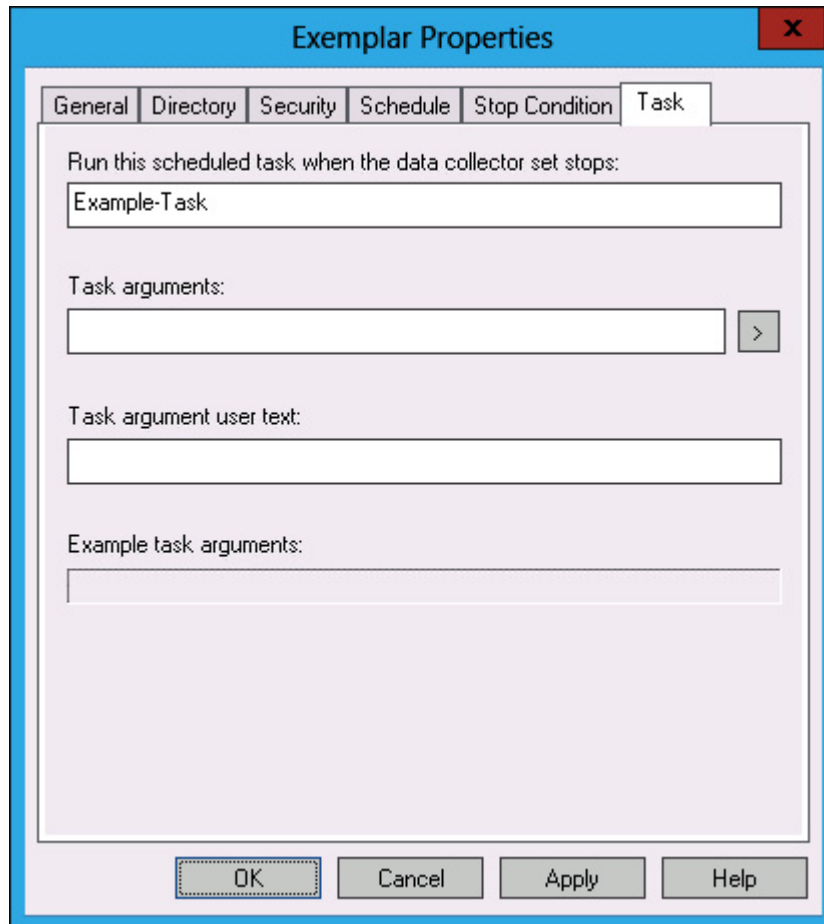
სურ.6.4. 7

თქვენ ამატებთ წარმადობის მთვლელს, მნიშვნელობის ზღვარს და უნდა იქნას თუ არა გაშვებული გაფრთხილება, თუ მნიშვნელობა გადააჭარბებს ან ჩამოსცდება ქვემოთ მოცემულ მნიშვნელობას. სურათზე ნაჩვენებია გაფრთხილება, რომელიც მოქმედებაში მოდის, მაშინ როცა ხელმისაწვდომი მეხსიერების რაოდენობა ჩამოსცდება 512 მეგაბაიტს.



სურ.6.4. 8

როდესაც შექმნით გაფრთხილებას, ყველა მათგანი, რომელიც გამოწვეულ იქნება, დაემატება შესაბამისი ღონისძიება, ღონისძიებების ჟურნალში. თქვენ ასევე შეგიძლიათ ასევე დააკონფიგუროთ გაფრთხილება, ისე რომ გაუშვას დაგეგმილი დავალება, როდესაც მოხდება გაფრთხილების გაშვება. ამის გაკეთება შეგიძლიათ გაფრთხილების თვისებების რედაქტირებითა და დაგეგმილი დავალების სახელის მინიჭებით, **Task** ჩანართში, ისე როგორც ნაჩვენებია სურთზე.



სურ.6.4. 9

პრაქტიკული სავარჯიშო

1. შეასრულეთ ვირტუალური დაცული ქსელის (VPN) სერვისის ინსტალაცია და კონფიგურაცია, გააქტიურეთ VPN კლიენტის გამოყენების შესაძლებლობები, მომართეთ კავშირისთვის საჭირო უსაფრთხოების პარამეტრების კონფიგურაცია, განახორციელეთ VPN-ის მომხმარებლების რეგისტრაცია და დაშორებული ოფისების გაერთიანება ერთ VPN ქსელში;
2. მოახდინეთ Windows Firewall with Advanced Security-ის კონფიგურაცია, დააინსტალირეთ Proxy სისტემა და მოახდინეთ მისი კონფიგურაცია, პოლიტიკის შესაბამისდ შეზღუდეთ საიტებზე წვდომა, გაანაწილეთ ინტერნეტ ტრაფიკი;
3. შეასრულეთ Windows Deployment Services ინსტალაცია და კონფიგურაცია, შექმენით სისტემის სარეზერვო ასლი, საჭიროების შემთხვევაში მოახდინეთ მისი აღდგენა, შექმენით ყოველდღიური AD DS სარეზერვო ასლი, შეასრულეთ Windows RE დავალება.
4. სისტემაში დაამატეთ Windows System Resource Manager უტილიტა, დააკონფიგურეთ Windows System Resource Manager ტერმინალ სერვისებისათვის, მოახდინეთ მონიტორინგის სხვა უტილიტების ინსტალაცია, მომართეთ Performance Monitor და Monitoring Event Logs დანერგვა და კონფიგურაცია.

ცოდნის შეფასება

სტუდენტებს მიეცემათ პრაქტიკული დავალება

- შეასრულონ ვირტუალური დაცული ქსელის (VPN) სერვისის ინსტალაცია და კონფიგურაცია, გააქტიურონ VPN კლიენტის გამოყენების შესაძლებლობები, მომართონ კავშირისთვის საჭირო უსაფრთხოების პარამეტრების კონფიგურაცია, განახორციელონ VPN-ის მომხმარებლების რეგისტრაცია და დაშორებული ოფისების გაერთიანება ერთ VPN ქსელში;
- მოახდინონ Windows Firewall with Advanced Security-ის კონფიგურაცია, დააინსტალირონ Proxy სისტემა და მოახდინონ მისი კონფიგურაცია,

პოლიტიკის შესაბამისდ შეზღუდონ საიტებზე წვდომა, გაანაწილონ ინტერნეტ ტრაფიკი;

- შეასრულონ Windows Deployment Services ინსტალაცია და კონფიგურაცია, შექმნან სისტემის სარეზერვო ასლი, საჭიროების შემთხვევაში მოახდინონ მისი აღდგენა, შექმნან ყოველდღიური AD DS სარეზერვო ასლი, შეასრულონ Windows RE დავალება.
- სისტემაში დაამატონ Windows System Resource Manager უტილიტა, დააკონფიგურონ Windows System Resource Manager ტერმინალ სერვისებისათვის, მოახდინონ მონიტორინგის სხვა უტილიტების ინსტალაცია, მომართონ Performance Monitor და Monitoring Event Logs დანერგვა და კონფიგურაცია.

შემფასებელი აკვირდება შესაფასებელ პირის მუშაობას პროფესიული სტანდარტით (პროგრამით / მოდულით) განსაზღვრული ამოცანების შესრულების პროცესში. დაკვირვება ხორციელდება კომპიუტერებით აღჭურვილ ლაბორატორიაში, სადაც შესაფასებელი პირი პრაქტიკულ საქმიანობას ეწევა. შემფასებელმა წინასწარ უნდა დაგეგმოს დაკვირვების პროცესი, იმის დასადგენად, თუ რამდენად სწორად იყენებს შესაფასებელი პირი ცოდნას, უნარებსა და ყველა რესურსს შედეგის მისაღწევად.

შეფასება განხორციელდება პროცესზე დაკვირვებით, წინასწარ განსაზღვრული შეფასების ინდიკატორების საფუძველზე.

დავალების ნიმუში და შეფასების რუბრიკა

პროცესზე დაკვირვება

- ✚ შეასრულოს სხვადასხვა საკომუნიკაციო და ინფრასტრუქტურის მართვის პროგრამების ინსტალაცია
- ✚ გამოიყენოს დაყენებული პრაქტიკული ამოცანებისთვის (ელ.ფოსტის სთორების და მეილბოქსების შექმნა, ტექსტური, ვიდეო- და აუდიო კომუნიკაციის მართვა, IT-ინფრასტრუქტურის მართვა)

სწავლის შედეგი	N	დასახელება	შეფასება	
			კი	არა
კონტროლისა და მონიტორინგის სისტემები	1.	შეასრულა ვირტუალური დაცული ქსელის (VPN) სერვისის ინსტალაცია,		
	2.	შეასრულა VPN კლიენტის გამოყენების შესაძლებლობების აქტივაცია და კავშირისთვის საჭირო უსაფრთხოების პარამეტრების კონფიგურაცია		
	3.	შეასრულა VPN-ის მომხმარებლების რეგისტრაცია და დაშორებული ოფისების გაერთიანება ერთ VPN ქსელში;		
	4.	შეასრულა Windows Firewall with Advanced Security-ის კონფიგურაცია, ,		
	5.	შეასრულა Proxy სისტემის ინსტალაცია და მისი კონფიგურაცია		
	6.	შეასრულა პოლიტიკის შესაბამისი საიტებზე წვდომის შეზღუდვები, ინტერნეტ ტრაფიკის განაწილება;		
	7.	შეასრულა Windows Deployment Services ინსტალაცია და კონფიგურაცია,		
	8.	შეასრულა სისტემის სარეზერვო ასლი, შემნა ყოველდღიური AD DS სარეზერვო ასლი, შეასრულა Windows RE დავალება.		
	9.	დაამატა Windows System Resource Manager უტილიტა და დააკონფიგურა Windows System Resource Manager ტერმინალ სერვისებისათვის		
	10.	მოახდინა მონიტორინგის სხვა უტილიტების ინსტალაცია, მომართა Performance Monitor და Monitoring Event Logs დანერგვა და კონფიგურაცია.		

სწავლის შედეგი ჩაითვლება მიღწეულად თუ სტუდენტმა შეძლო შედეგის მინიმუმ 8 პუნქტის შესრულება

დასკვნა

სახელმძღვანელოში თანამედროვე ინფორმაციული ტექნოლოგიების უმნიშვნელოვანესი მიმართულება - კორპორაციული კომპიუტერული ქსელების სერვერული სისტემების არქიტექტურა იქნა განხილული. ქსელურად შენახული ინფორმაციის მოცულობა და კრიტიკულობა გახდა მთავარი მამოძრავებელი ძალა გასული საუკუნის ბოლოდან დამკვიდრებული ახალი მეთოდებისა სერვერული სისტემების დაპროექტებისა და აგების პროცესში.

სახელმძღვანელოში გათვალისწინებულ იქნა „სისტემების ადმინისტრატორის“ პროფესიულ საგანმანათლებლო პროგრამაში შემავალი მოდულების თემატიკა და შესაბამისი სწავლის შედეგები Windows სისტემების ბაზაზე.

სახელმძღვანელო რეკომენდირებულია პროფესიული სასწავლებლების „სისტემების ადმინისტრატორი“ საგანმანათლებლო პროგრამის სტუდენტებისთვის, სისტემების ადმინისტრატორებისთვის. აღნიშნული სახელმძღვანელოს პოტენციური მომხმარებელი შეიძლება იყოს ნებისმიერი პიროვნება, რომელიც თავისი პირადი თუ პროფესიული საქმიანობის სფეროში იყენებს ინფორმაციულ ტექნოლოგიებს.

სახელმძღვანელოში განხილული თემატიკა პროგრამული უზრუნველყოფის მოწინავე მწარმოებელთა შეუწელებელი ყურადღების საგანს წარმოადგენს. ამ მიმართულებით ახალი ტექნოლოგიების განვითარებას და დანერგვას ახლო მომავალში უნდა ველოდოთ.

გამოყენებული ლიტერატურა

1. Microsoft® Windows Server® 2012 - Rand Morimoto, Ph.D., MCITP, MVP Michael Noel, MVP, MCITP Guy Yardeni, MCITP, CISSP, MVP Omar Droubi, MCSE, MCTS Andrew Abbate, MCITP Chris Amaris, MCITP, MCTS, CISSP
2. http://en.wikipedia.org/wiki/World_Wide_Web
3. <http://office.microsoft.com/en-us/windows-sharepoint-services-help/working-with-sharepoint-lists-part-1-HA001119988.aspx>
4. *გოჩა ჩოგოვაძე, ვია სურგულაძე, ოთარ შონია* მონაცემთა და ცოდნის ბაზების აგების საფუძვლები. თბილისი, გამომცემლობა „განათლება“, 1996
5. *А.В.Кузовкин, А.А.Цыганов, Б.А.Щукин* Управление данными. Москва, Издательский центр «Академия», 2010
6. <http://db-engines.com/en>
7. http://ru.wikipedia.org/wiki/Система_мгновенного_обмена_сообщениями
8. http://en.wikipedia.org/wiki/Microsoft_Lync
9. *Keith Hanna, Nathan Winters* Mastering Microsoft Lync Server 2013; ISBN: 978-1-118-52132-8 888 pages, May 2013
10. *Omar Kudovic*. MS Lync Presentations. Quipu Workshop – 24-27.03.2014, Frankfurt-am-Main
11. *დავით გულუა* "ორგანიზაციის IT-ინფრასტრუქტურის მართვის ავტომატიზაცია ITIL-ტექნოლოგიის გამოყენებით", ლექციების კონსპექტი, თბილისი, 2013.
12. *Brian Mason, Greg Ramsey* Microsoft System Center 2012 Configuration Manager: Administration Cookbook, Packt Publishing, 2012
13. https://en.wikipedia.org/wiki/System_Center_Configuration_Manager