იოსებ ქართველიშვილი

ინფორმაციის დაცვა და კიბერუსაფრთხოების სისტემები

(პრაქტიკულის მეთოდური მითითებანი)

„სტუ-ს IT კონსალტინგის სამეცნიერო ცენტრი”

საქართველოს ტექნიკური უნივერსიტეტი

იოსებ ქართველიშვილი

სადოქტორო პროგრამა „ინფორმატიკა“

ინფორმაციის დაცვა და კიბერუსაფრთხოების სისტემები

(პრაქტიკული სამუშაოს მეთოდური მითითებანი)

დამტკიცებულია:

სტუ-ს „IT კონსალტინგის სამეცნიერო ცენტრის “სარედაქციო კოლეგიის მიერ

ოქმი N7, 15 ოქტომბერი 2020

თბილისი

2020

უაკ 004.5

განხილულია ინფორმაციის დაცვისა და კიბერუსაფრთხოების ძირითადი მოთხოვნების საკითხები, მათი რეალიზაციის მეთოდები და ინსტრუმენტული საშუალებები, ორგანიზაციებში მათი დანერგვისა და გამოყენების პრობლემები და სამართლებრივ ბაზაზე დაყრდნობით გადაწყვეტის გზები. წარმოდგენილია ინფორმაციული უსაფრთხოების კონცეფციის ჩამოყალიბება და კომპლექსური დაცვის სისტემის უზრუნველყოფა თანამედროვე ღრუბლოვანი ტექნოლოგიებით. შემოთავაზებულია ლაბორატორიული პრაქტიკუმის მეთოდური მითითებები ისეთ საკითხებზე, როგორიცაა: მონაცემთა შიფრირება და კრიპტოგრაფიული ალგორითმის პროგრამული პროდუქტი VeraCrypt-ის ბაზაზე; რისკების მენეჯმენტი ღრუბლოვან ტექნოლოგიებში, NextCloud პროგრამული პაკეტის გამოყენებით, სისტემის სრულფასოვანი კონფიგურირება და ადმინისტრირება; სერვერულ ოპერაციულ სისტემებში ჯგუფური პოლიტიკები და მათი მართვა. დამხმარე მეთოდური სახელმძღვანელო რეკომენდებულია ინფორმატიკის სპეციალობის დოქტორანტებისათვის, ინფორმაციული და კომუნიკაციური ტექნოლოგიების სფეროში (ICT 0613).

რეცენზენტები:

პროფ. **ო. შონია** (სტუ)
ასოც. პროფ: **კ. ოდიშარია** (სტუ)

რედკოლეგია:

ა. ფრანგიშვილი (თავმჯდომარე), მ. ახობაძე, გ. გოგიჩაიშვილი, ზ. ბოსიკაშვილი, ე. თურქია, რ. კაკუბავა, ნ. ლომინაძე, ჰ. მელაძე, თ. ობგაძე, გ. სურგულაძე (რეადაქტორი), გ. ჩაჩანიძე, ა. ცინცაძე, ზ. წვერაიძე

ISBN 978-9941-8-2867-6

სასწავლო კურსის მიზანი

ინფორმაციის დაცვისა და უსაფრთხოების ძირითადი მოთხოვნების შესწავლა. ამ მოთხოვნათა რეალიზაციის მეთოდებისა და საშუალებების არჩევის, მათი დანერგვისა და გამოყენების შესწავლა. მოქმედ ორგანიზაციულ სამართლებრივ ბაზაზე დაყრდნობით, ნებისმიერი ტიპის ორგანიზაციის ინფორმაციული უსაფრთხოების კონცეფციის ჩამოყალიბება და კომპლექსური დაცვის სისტემის უზრუნველყოფა სხადასხვა მეთოდებითა და საშუალებებით. თანამედროვე ღრუბლოვანი ტექნოლოგიების საბაზისო ცოდნის მიღება. კიბერუსაფრთხოების საბაზისო ცოდნის მიღება, თანამედროვე კიბერშეტევების ვექტორების იდენტიფიცირება. კიბერუსაფრთხოებაში გამოყენებული მანქანური სწავლების მეთოდების გაცნობა. ინფორმაციული და ქსელური რესურსების დაცულობის ანალიზის მეთოდიკის შესწავლა. თანამედროვე სოციალური ქსელებისა და მობილური ტექნოლოგიების ეფექტურად გამოყენების საბაზისო ცოდნის მიღება.

საგნის შესწავლის შედეგად მიღებული ცოდნა და შეძენილი უნარები

1. ჩამოთვლის პერსონალური მონაცემების დაცვის მეთოდებს, საშუალებებს და ძირითად პრინციპებს. მსჯელობს ინფორმაციის შეფასების კრიტერიუმებისა და ინფორმაციული რესურსების კლასიფიკაციის შესახებ.

2. ახდენს კონკრეტული ინფორმაციული ინფრასტრუქტურის დაცვის ძირითდი მექანიზმების გამოყენების რაციონალურობის შეფასებას და ნაკლოვანებების გამოვლენას.

3. ახორციელებს კონკრეტული დანიშნულების ნებისმიერი მასშტაბის კომპიუტერული ქსელების დაცულობის გამოვლენას საკანონმდებლო, ადმინისტრაციულ, პროცედურულ და პროგრამულ-ტექნიკურ დონეზე, არსებული გადახრების გამოვლენაა და მათი გამოსწორების უახლესი მეთოდების მოძიებას.

4. აანალიზებს და საზღვრავს ორგანიზაციაში ღრუბლოვანი ტექნოლოგიების დანერგვის საჭიროების დონეს.

5. ახორციელებს გამოკვლევების საფუძველზე დავალებული კონკრეტული პროგრამული პროდუქტების დაცულობის ძირითადი მექანიზმების გამოყენებას რაციონალურობის შეფასებას და ნაკლოვანებების აღმოფხვრას შესაბამისი კომპლექსური ღონისძიებების გატარებით

6. ჩამოთვლის არსებული ინფორმაციის შეფასების კრიტერიუმებს. ახდენს ინფორმაციული რესურსების კლასიფიკაციას, კიბერ ინციდენტების იდენტიფიცირებას.

7. აანალიზებს და ადგენს თუ რა ტიპის კიბერშეტევას ჰქონდა ადგილი.

8. ჩამოთვლის სოციალური ქსელებისა და მობილური ტექნოლოგიების არასათანადო გამოყენებისას გამოწვეულ რისკებს და საფრთხეებს.

9. მანქანური სწავლების საფუძველზე აყალიბებს ქსელური რესურსების ადაპტური ანალიზის ჩატარების მექანიზმებს.

10. მსჯელობს კიბერუსაფრთხოებაში მანქანური სწავლების პრობლემებზე.

11. აანალიზებს მანქანური სწავლების ტექნოლოგიით უკვე განხორციელებულ კიბერთავდასხმებს და ინტელექტუალური ანალიზის საფუძველზე გეგმავს ქსელის დაცვის ზომების შემუშავების შემდგომ მექანიზმებს.

12. შეუძლია ცოდნის გაფართოება ახალ სფეროში და შესაბამისი უნარ-ჩვევების გამომუშავება უკვე მიღებული ცოდნისა და გამოცდილების საფუძველზე.

13. ახალ სფეროში პრაქტიკაში იყენებს უკვე მიღებულ ცოდნასა და გამოცდილებას.

14. კეთილსინდისიერად და დამოუკიდებლად ახდენს პრაქტიკული დავალებებისა და სხვადასხვა სახის ამოცანების შესრულებას.

საათების განაწილება (სტუდენტის დატვირთვა)

კრედიტების რაოდენობა 8. ლექცია -15 სთ., სე,მინარი (ჯგფში მუშაობა) -30 სთ., პრაქტიკული (კომპიუტერულ კლასში) – 15 სთ. დამოუკიდებელი მუშაობა 137 სთ.

პრაქტიკული სამუშაოს თემები:

1. პერსონალური მონაცემების დამუშავებისას სპეციალური რეკომენდაციების მომზადების პროცესის მიმოხილვა, რომლებიც როგორც საჯარო, ისე კერძო ორგანიზაციებისთვისაა განკუთვნილი. პერსონალური მონაცემების დამუშავებისას გამოყენებული პროგრამული პროდუქტების მიმოხილვა.

2. ორგანიზაციებში ინფორმაციის დაცვისა და უსაფრთხოების პრაქტიკული უზრუნველყოფა. ფაილებისა და საქაღალდეების დაშიფრვა კრიპტოგრაფიული ალგორითმების გამოყენებით, პროგრამული პროდუქტის VeraCrypt-ის გამოყენებით.

3. პროგრამული პროდუქტის - Wireshark (პროტოკოლების ანალიზატორი) დანიშნულება და ინტერფეისის მიმოხილვა. უტილიტა Wireshark-ის გამართვა. ფილტრები, ოფციები და სტატისტიკები.

4. პროგრამული პროდუქტის - PRTG Administrator Tools დანიშნულება და ინტერფეისის მიმოხილვა. პროგრამის სენსორების განხილვა. JFLOW სენსორის გამართვა.

5. რისკების მენეჯმენტი ღრუბლოვან ტექნოლოგიებში. ღია კოდის მქონე ღრუბლოვანი ტექნოლოგიის NextCloud პროგრამული პაკეტის დაყენება ოპერაციულ სისტემაზე. სისტემის სრულფასოვანი კონფიგურირება და ადმინისტრირების საშუალებების ძირითადი პრინციპების გაცნობა.

6. ვირტუალიზაციის მეთოდი. პროგრამული პროდუქტი VMware Workstation-ის დანიშნულება და მისი გამართვა. პროგრამა VMware Workstation-ის გამოყენებით ვირტუალური მანქანის შექმნა.

7. სერვერული ოპერაციული სისტემის ძირითადი ცნობები და სერვერის მენეჯერთან (Server Manager) მუშაობის შესწავლა პრაქტიკული მაგალითების გამოყენებით.

8. სერვერულ ოპერაციულ სისტემებში ჯგუფური პოლიტიკები და მათი მართვა. ჯგუფურ პოლიტიკებთან სამუშაო სპეციალურ კონსოლთან მუშაობის შესწავლა.

9. დაცილებული კომპიუტერის მართვა. Remote Desktop Connection და ვირტუალური კერძო ქსელის (VPN) აგების კონცეფცია, ქსელის ფუნქციები და მათი კლასიფიკაცია. Cisco VPN Client კონსოლთან მუშაობის შესწავლა.

10. ორგანიზაციის ვებსერვერზე კიბერშეტევების დროს სერვერის ე.წ. „access log“ ფაილის ანალიზის მეთოდები შეტევის მომენტის ინციდენტის დეტალების დასადგენად.

11. მარშრუტიზატორის საწყისი პარამეტრების კონფიგურაცია და მისი სტანდარტული კონფიგურაციის შემოწმება. ქსელის უსაფრთხოების საკითხების გამოკვლევა.

12. საეჭვო აპლიკაციის იდენტიფიცირება რეალური აპლიკაციების გარემოცვაში. ვირტუალურ მანქანაში დაყენებული მობილური ოპერაციული სისტემის ქვეშ დაყენებული აპლიკაციების გადარჩევა და მათში საეჭვო აპლიკაციის იდენტიფიცირება.

13. კიბერუსაფრთხოების გადაწყვეტილებების მიმოხილვა. ბოროტად გამოყენების / ხელმოწერის გამოვლენა. ანომალიის გამოვლენა. ჰიბრიდული გამოვლენა. სკანირების გამოვლენა.

14. ფართომასშტაბიანი ქსელების მოდელირება. საფრთხეების აღმოჩენა. ქსელის დინამიკა და კიბერ შეტევა. კონფიდენციალურობის დაცვა მონაცემთა მოპოვებაში. კოჰონენის ნეირონული ქსელები.

15. ანონიმურობის შენარჩუნება ინლაინში ყოფნისას: Kali-Linux-ში იდენტობის დამალვის სხვადასხვა გზები (TOR, VPN, PROXY CHAINS). Nmap - ქსელური სკანირების პროგრამა Nmap-ის განსაზღვრება, მისი შესაძლებლობები და გამოყენების გზები.

პრაქტიკული სამუშაოს შესრულების ნიმუში

პრაქტიკული N2

მონაცემთა შიფრირება, კრიპტოგრაფიული ალგორითმის პროგრამული პროდუქტი VeraCrypt-ის დაინსტალირება და მისი მართვა

VeraCrypt for Windows - ეს არის პროგრამული პროდუქტი, რომელიც გამოიყენება სხვადასხვა სახის ფაილების შიფრირებისათვის. პროგრამა დაშიფვრავს თქვენს მონაცემებს ისეთი სახით, რომ სხვა მომხმარებლები ვერ შეძლებენ მისადმი წვდომას პაროლის გარეშე. იგი წააგავს ელექტრონულ სეიფს, სადაც შესაძლებელია ფაილების შენახვა და დარწმუნებული იყოთ მათ უსაფრთხოებაში.

VeraCrypt პროგრამა შიფრირებას უკეთებს ფაილებს და იცავს მათ პაროლის დახმარებით. დაცული მოცულობა იწოდება - "ტომად". კომპიუტერზე ისინი გამოიყურება, როგორც მიერთებული დისკი. სინამდვილეში, ტომი მდებარეობს ერთადერთი ფაილის (კონტეინერის) ქვეშ, რომელიც შესაძლებელია პაროლის მითითებით გაიხსნას და დაიკეტოს. კონტეინერის შიგნით ფაილი მდებარეობს უსაფრთხოდ.

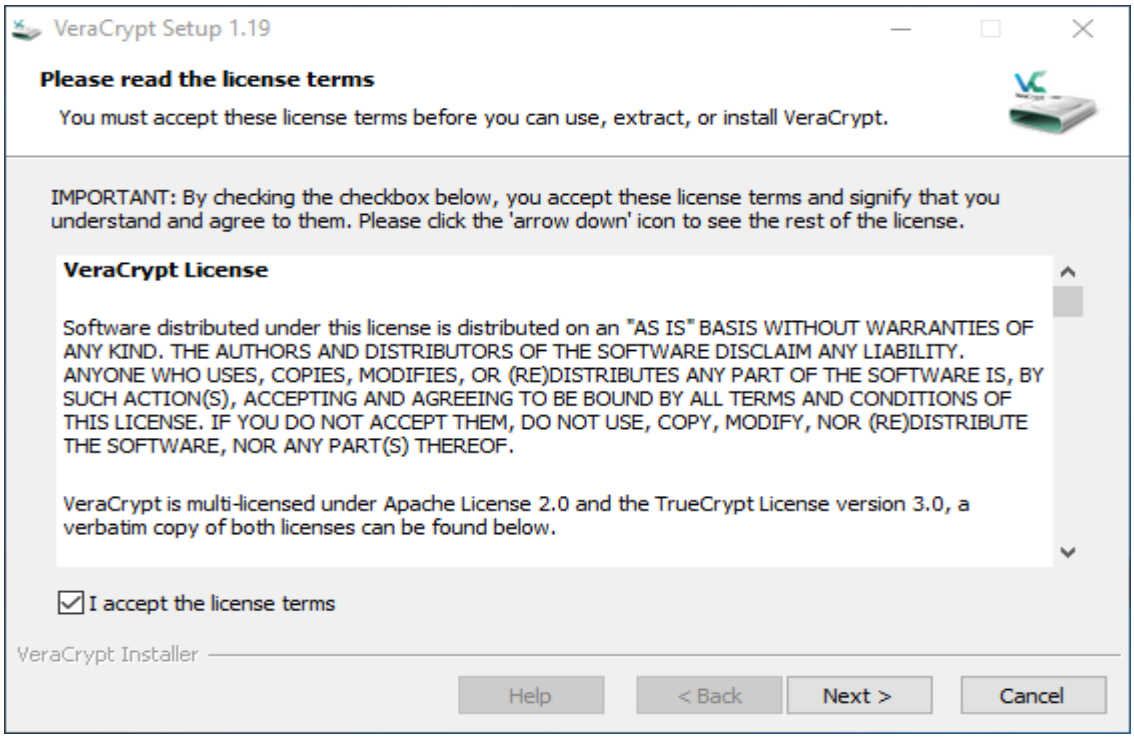
<u>შენიშვნა:</u> თუ დაგავიწყდებათ პაროლი, მაშინ დაკარგავთ მონაცემებთან წვდომას. დავიწყებული პაროლის აღდგენა შეუძლებელია.

<u>VeraCrypt პროგრამის დაინსტალირება:</u>

ბიჯი 1: გაუშვით საინსტალაციო ფაილი - "VeraCrypt Setup 1.19.exe" .

ნახ.1

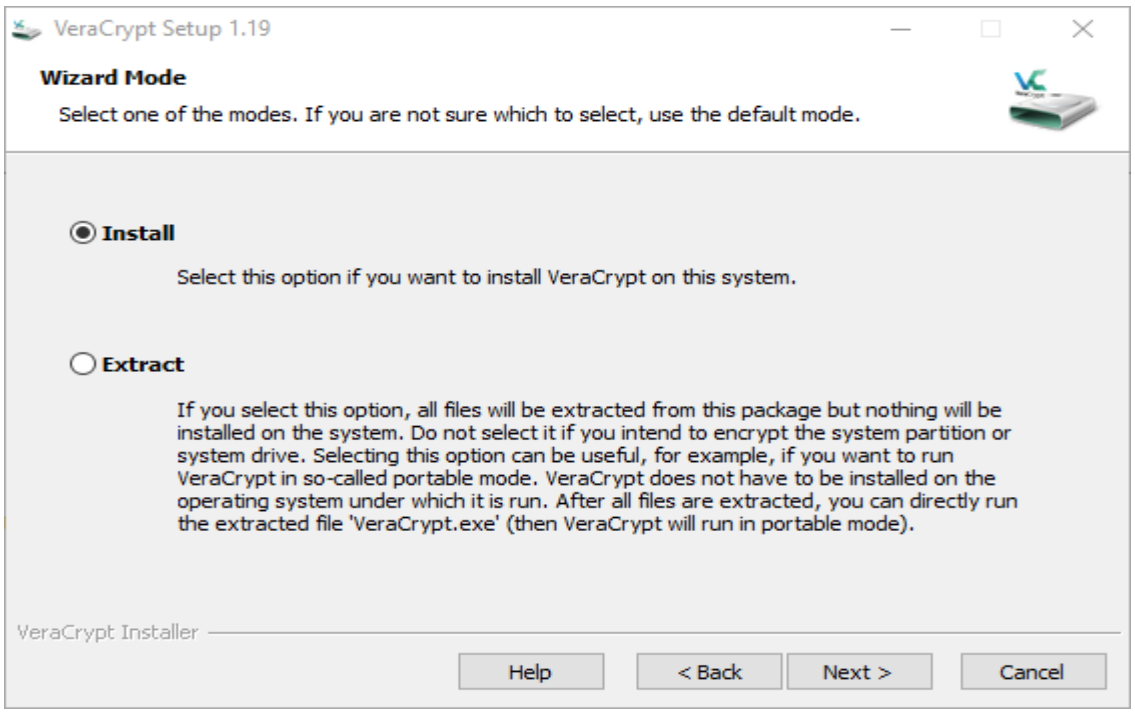
ფაილის გაშვების შემდეგ გამოდის ლიცენზიის ფანჯარა (ნახ.2).



ნახ.2

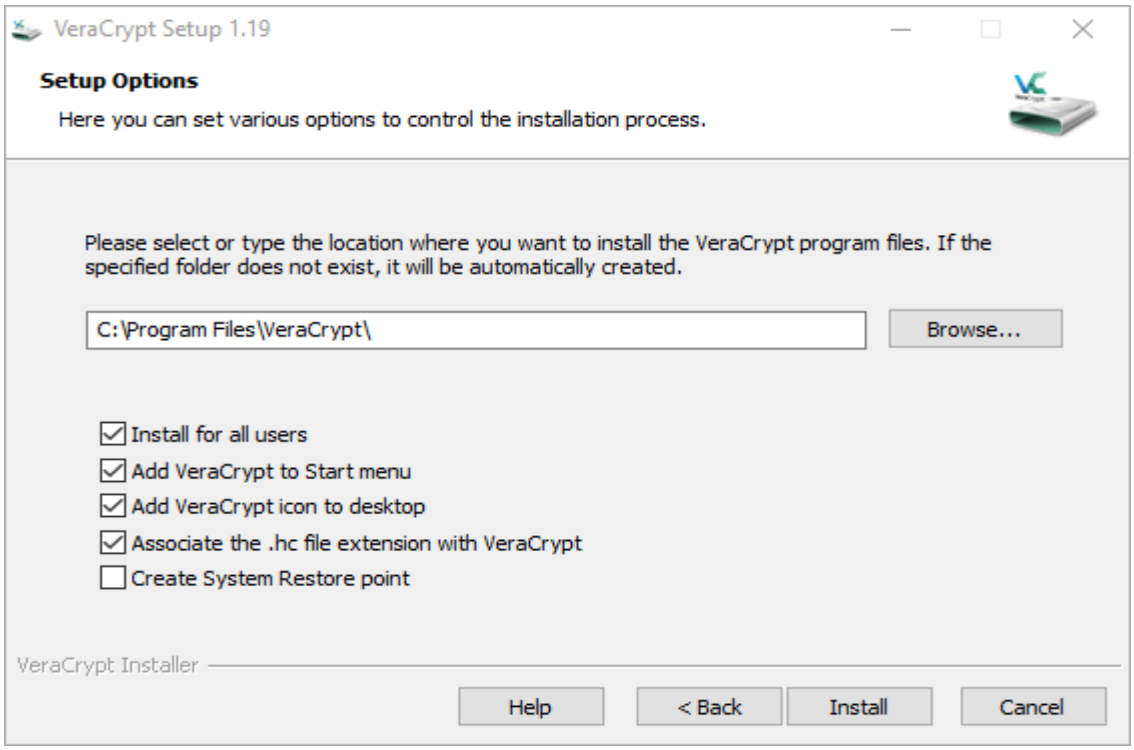
ბიჯი 2: მოვნიშნოთ ალამი - *I accept the license terms* და დავაჭიროთ ღილაკს - Next. გამოდის არჩევანის ფანჯარა, სადაც ვირჩევთ რომ პროგრამა დაინსტალირდეს მთლიანად ან დავაყენოთ პროგრამის პორტატიული ვერსია.

ბიჯი 3: ჩვენს შემთხვევაში ავირჩიოთ პირველი პუნქტი, მოვნიშნოთ ალამი - Install და დავაჭიროთ ღილაკს - Next (ნახ.3).



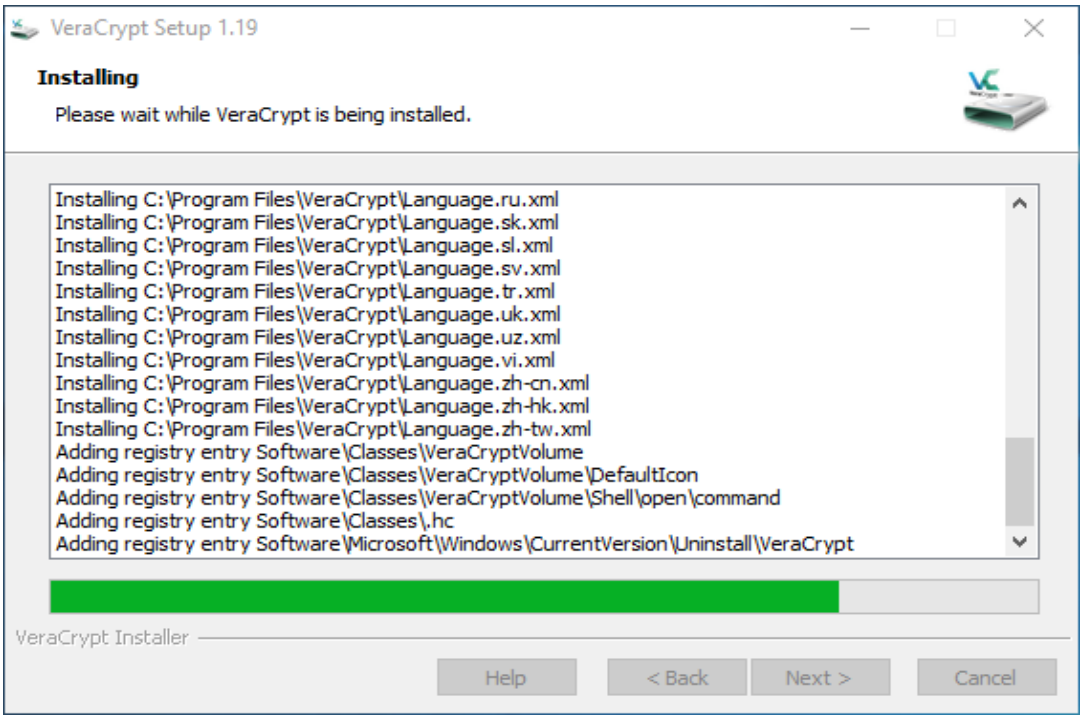
ნახ.3

რის შემდეგაც გამოდის ფანჯარა, სადაც ვირჩევთ მისამართს, თუ სად უნდა დაყენდეს პროგრამა (ნახ.4).



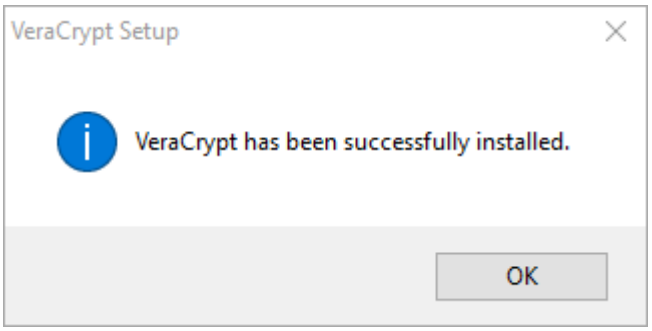
ნახ.4

ბიჯი 4: მისამართი და დანარჩენი ალმები დავტოვოთ უცვლელად და დავაჭიროთ ღილაკს - Install, შედეგად დაიწყება ინსტალაციის პროცესი (ნახ.5).



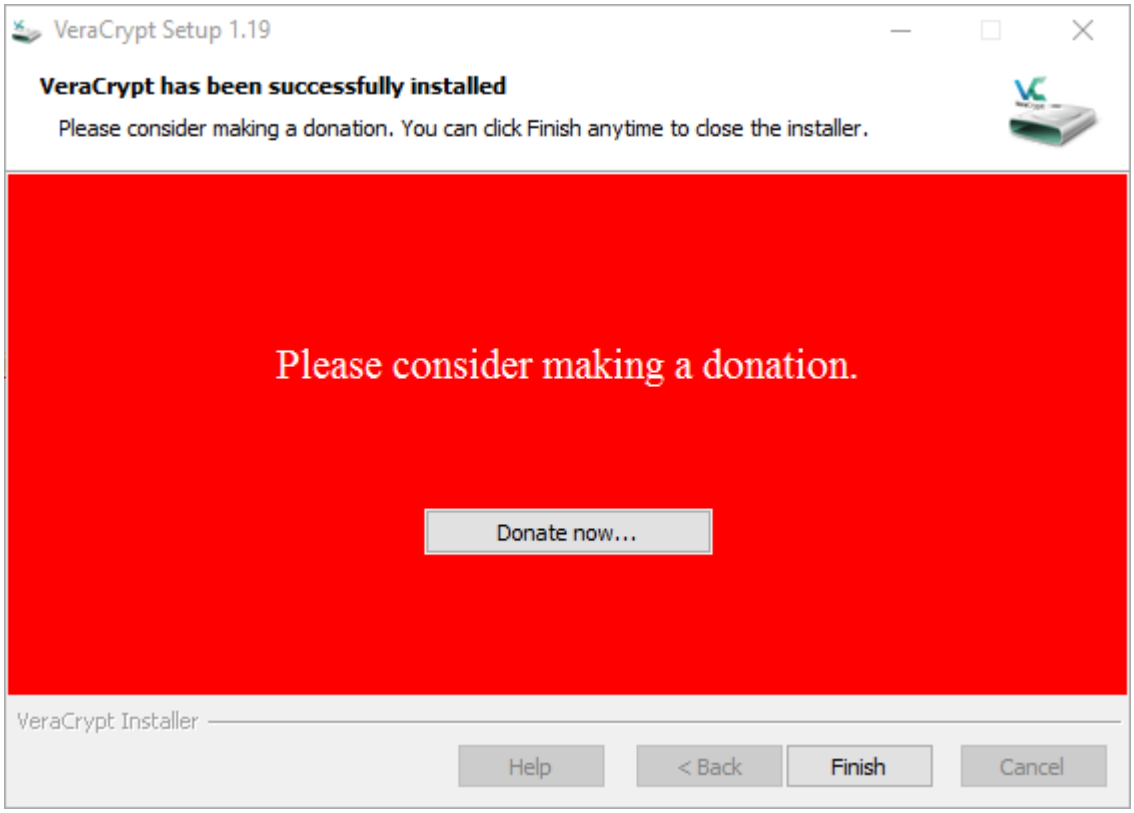
ნახ.5

ბიჯი 5: ინსტალაციის დასრულების შემდეგ გამოდის შეტყობინება:



ნახ.6

ბიჯი 6: დავაჭიროთ ღილაკს - OK და გამოდის შემდეგი ფანჯარა:



ნახ.7

ბიჯი 7: დავაჭიროთ ღილაკს - Finish, რომ დასრულდეს ინსტალაციის პროცესი და სამუშაო მაგიდაზე გაჩნდება **VeraCrypt**-ის იარლიყი:

ნახ.8

ჩვეულებრივი ტომის შექმნა:

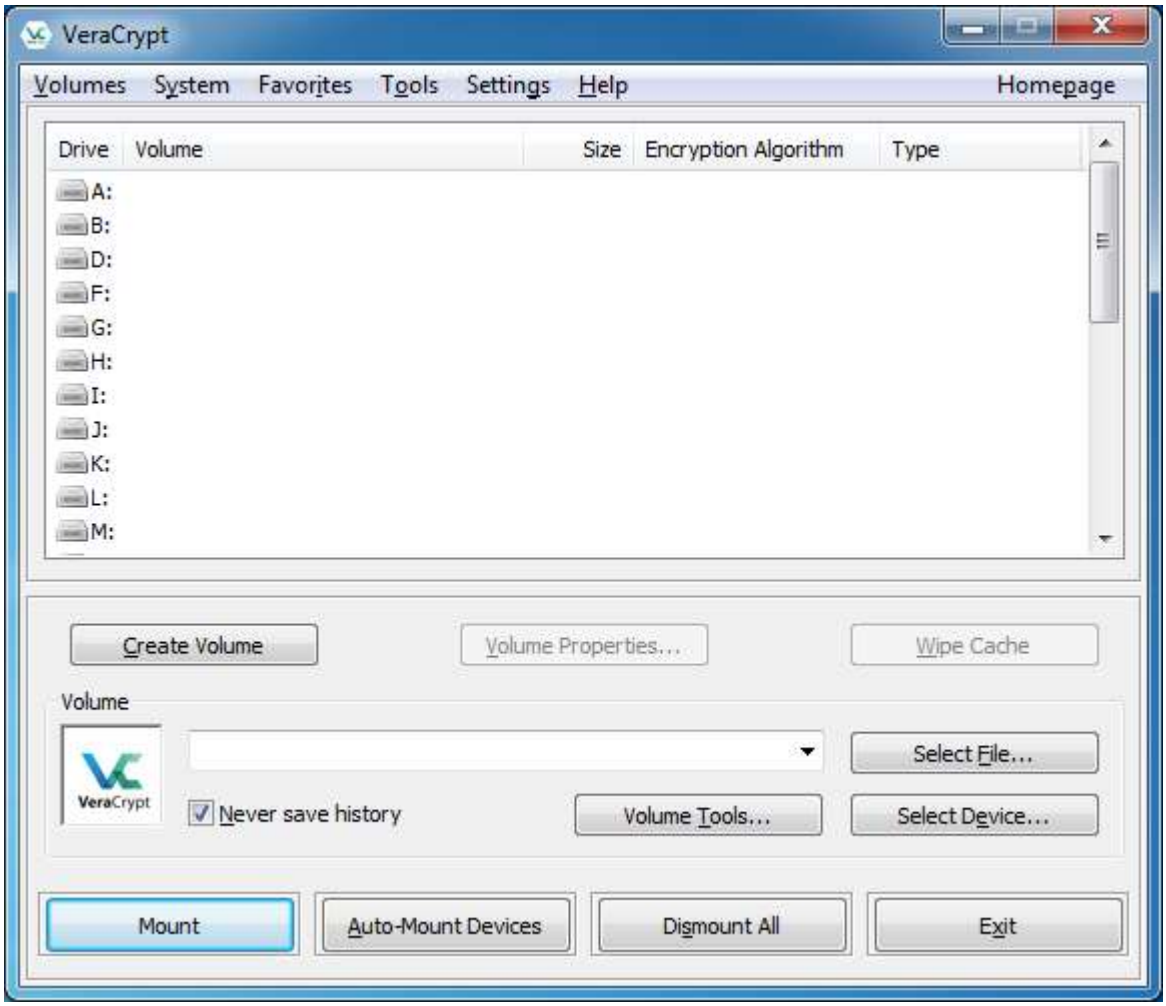
პროგრამა VeraCrypt საშუალებას იძლევა შექმნათ ორი სახის ტომი: **ფარული** და **ჩვეულებრივი**.

- **ჩვეულებრივი ტომი** იცავს თქვენს ფაილებს პაროლით. ეს პაროლი უნდა შეიყვანოთ ყოველ ჯერზე, როდესაც დაიწყებთ დაშიფრული VeraCrypt-ის ტომთან მუშაობას.

- **ფარულ ტომი** აქვს ორი პაროლი. თქვენ შეგიძლიათ გამოიყენოთ ერთი მათგანი, რათა გახსნათ მასკირირებული ჩვეულებრივი ტომი, სადაც ინახება ნაკლებად მნიშვნელოვანი მონაცემები და რომლის დაკარგვა ან სხვის ხელში ჩაგდება არ გამოიწვევს რაიმე პრობლემას. მეორე პაროლი იძლევა წვდომას იმ ფარულ ტომზე, სადაც ინახება ყველაზე მნიშვნელოვანი მონაცემები.

თავდაპირველად განვიხილოთ, თუ როგორ ხდება **ჩვეულებრივი ტომის** შექმნა. ამისათვის შევასრულოთ შემდეგი ნაბიჯები:

ბიჯი 1: სამუშაო მაგიდიდან გავუშვათ პროგრამა VeraCrypt. გაიხსნება პროგრამის ძირითადი ფანჯარა.

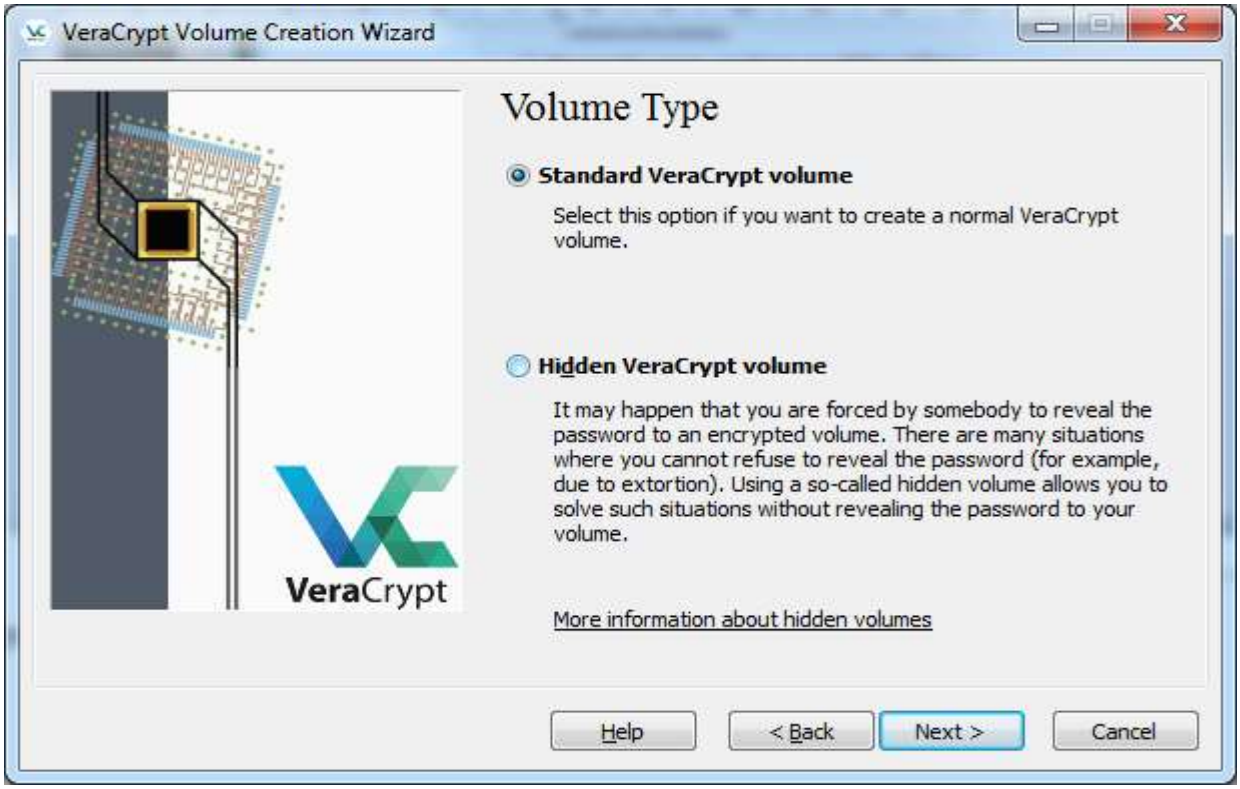


ნახ.9

ბიჯი 2: დავაჭიროთ ღილაკს - Create Volume, რომ შევქმნათ ახალი ტომი.

ნახ.10

ბიჯი 3: გამოსულ ფანჯარაში დავტოვოთ მონიშნული ალამი უცვლელად და დავაჭიროთ ღილაკს - Next.

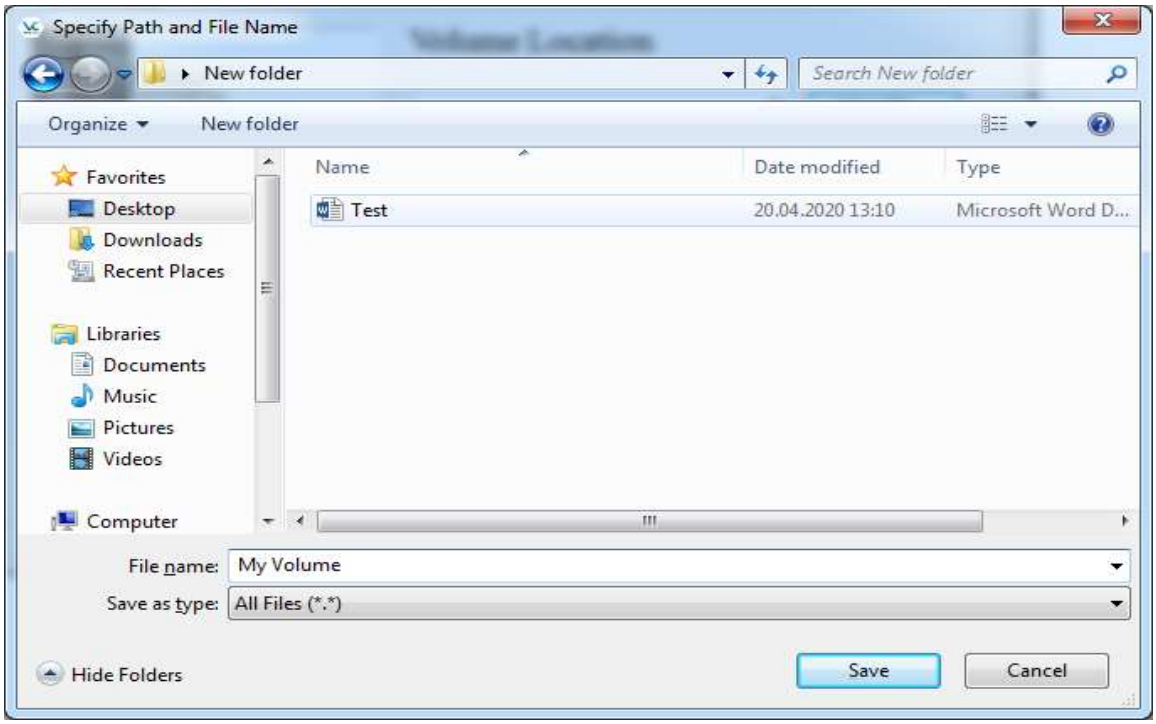


ნახ.11

ბიჯი 4: ფანჯარაში დავტოვოთ მონიშნული ალამი უცვლელად, რაც ნიშნავს რომ ვქმნით ჩვეულებრივ ტომს და დავაჭიროთ ღილაკს - Next.

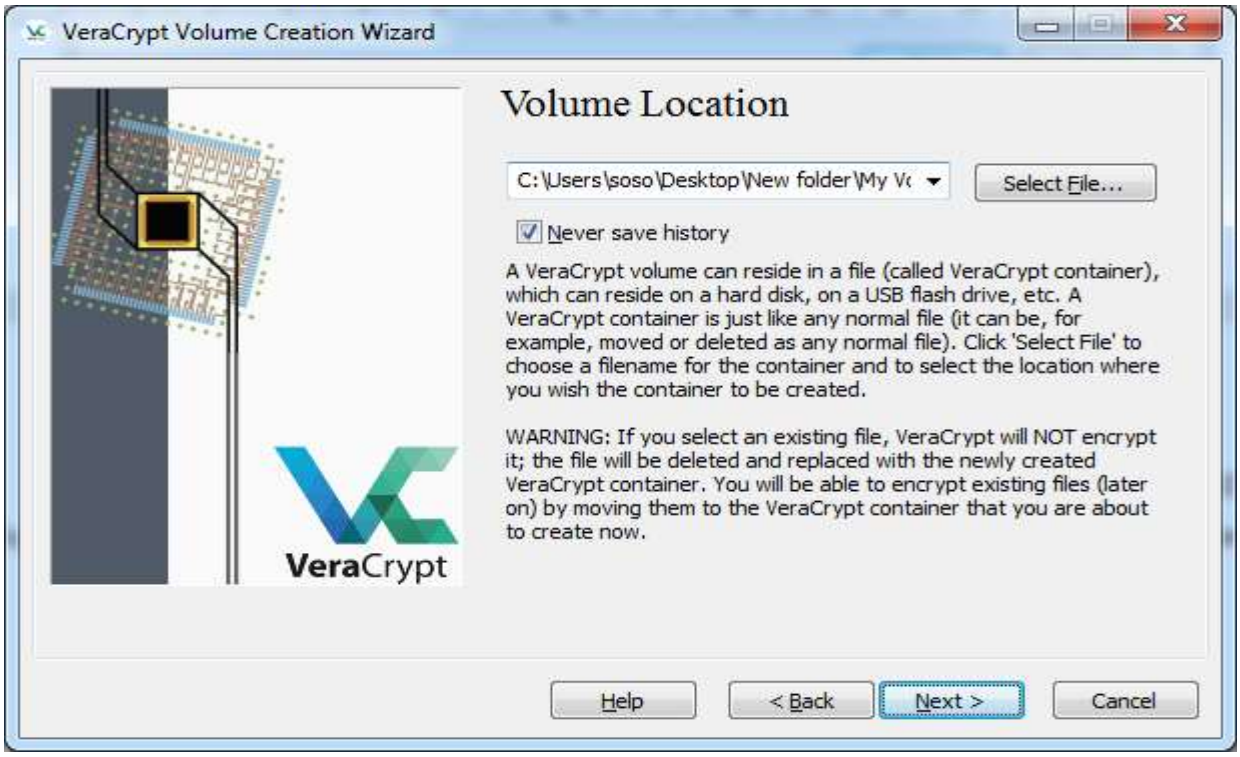
ნახ.12

ბიჯი 5: დავაჭიროთ ღილაკს - Select File.... და ავირჩიოთ ადგილმდებარეობა და ფაილის სახელი, სადაც უნდა განთვსდეს VeraCrypt-ის კონტეინერი.



ნახ.13

ბიჯი 6: ფაილის სახით შეგვიძლია ავირჩიოთ ნებისმიერი დასახელება, ჩვენი მაგალითის შემთხვევაში ფაილს დავარქვათ - My Volume და დავაჭიროთ ღილაკს - Save.



ნახ.14

ბიჯი 7: დავაჭიროთ ღილაკს - Next და დავაყენოთ შიფრირების პარამეტრები.

ნახ.15

ბიჯი 8: გამოსულ ფანჯარაში შესაძლებელია კონტეინერში არსებული ფაილების დაშიფვრისა და ამოშიფვრის ალგორითმის მეთოდის შეცვლა. ჩვენი მაგალითის

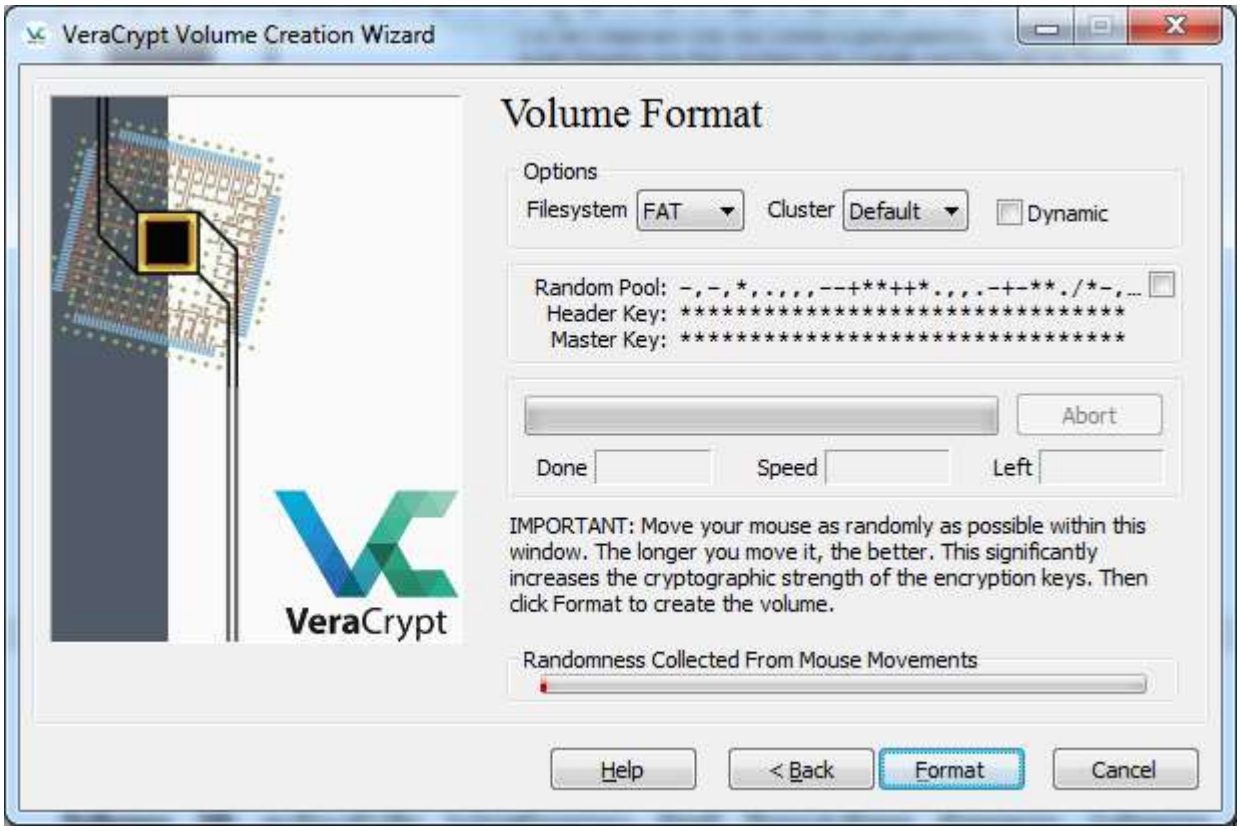
შემთხვევაში დავტოვოთ უცვლელად პარამეტრები და დავაჭიროთ ღილაკს - Next, სადაც შესაძლებელი იქნება მოვახდინოთ ტომის ზომის დაყენება.

ნახ.16

ბიჯი 9: გამოსულ ფანჯარაში უნდა დავაყენოთ შესაქმნელი კონტეინერის ზომა, სადაც უნდა განთავსდეს დასაშიფრი ფაილები. ჩვენი მაგალითის შემთხვევაში დავაყენით 250 მბ და დავაჭიროთ ღილაკს - Next, რათა მოვახდინოთ პაროლის შეტანა.

ნახ.17

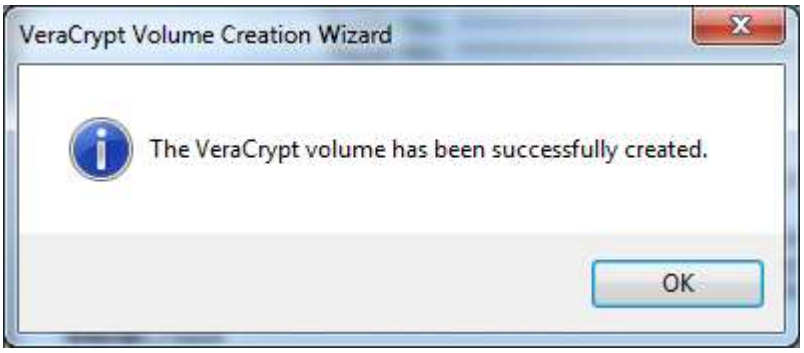
ბიჯი 10: ფანჯარაში სასურველია რომ შევიტანოთ რთული პაროლი და დავაჭიროთ ღილაკს - Next.



ნახ.18

ბიჯი 11: როდესაც ფაილების ზომა 4 გბ-ს აღემატება, მაშინ სასურველია გამოსულ ფანჯარაში ფაილური სისტემის შეცვლა, სხვა შემთხვევაში დავტოვოთ პარამეტრები უცვლელად და დავაჭიროთ ღილაკს - Format, რომ მოხდეს ჩვეულებრივი ტომის შექმნა.

პროცესის დასრულების შემდეგ პროგრამა ქმნის ფაილს - My Volume. ეს არის VeraCrypt-ის კონტეინერი, ზომით - 250 მბ, სადაც შესაძლებელია მნიშვნელოვანი მონაცემების შენახვა და გამოდის შეტყობინების ფანჯარა.



ნახ.19

ბიჯი 12: დავაჭიროთ ღილაკს - OK. გამოდის შეტყობინების ფანჯარა, რომ ტომი იქნა შემნილი.

ნახ.20

ბიჯი 13: დავაჭიროთ ღილაკს - Exit და დავბრუნდეთ პროგრამის ძირითად ფანჯარაზე.

ამით **ჩვეულებრივი ტომის** შექმნის პროცესი დასრულებულია და ჩვენს მიერ მითითებულ მისამართზე იქმნება 250 მბ-იანი ფაილი - My Volume.

ნახ.21

<u>ფარული ტომის შექმნა:</u>

პროგრამა VeraCrypt-ში ფარული ტომი მოთავსებულია დაშიფრული ჩვეულებრივი ტომის შიგნით, რომლის არსებობაც შეიძლება ძნელი მისახვედრი იყოს უცხო პირისთვის. მაშინაც კი, როდესაც თქვენი ჩვეულებრივი ტომი არის ამოშიფრული, შეუძლებელია იმის დადგენა, არის თუ არა მასში ფარული ტომი, თუ არ იცით მისი პაროლი. ჩვეულებრივი და ფარული ტომის პაროლები განსხვავებულია.

ფარული ტომი გარკვეულწილად წააგავს საიდუმლო ნაწილს. ბოროტგანმზრახველმა შეიძლება მოიპოვოს ჩვეულებრივი ტომის პაროლი და ვერც კი წარმოიდგინოს, რომ მასში არსებობს ფარული ტომი, სადაც ინახება მნიშვნელოვანი ინფორმაცია.

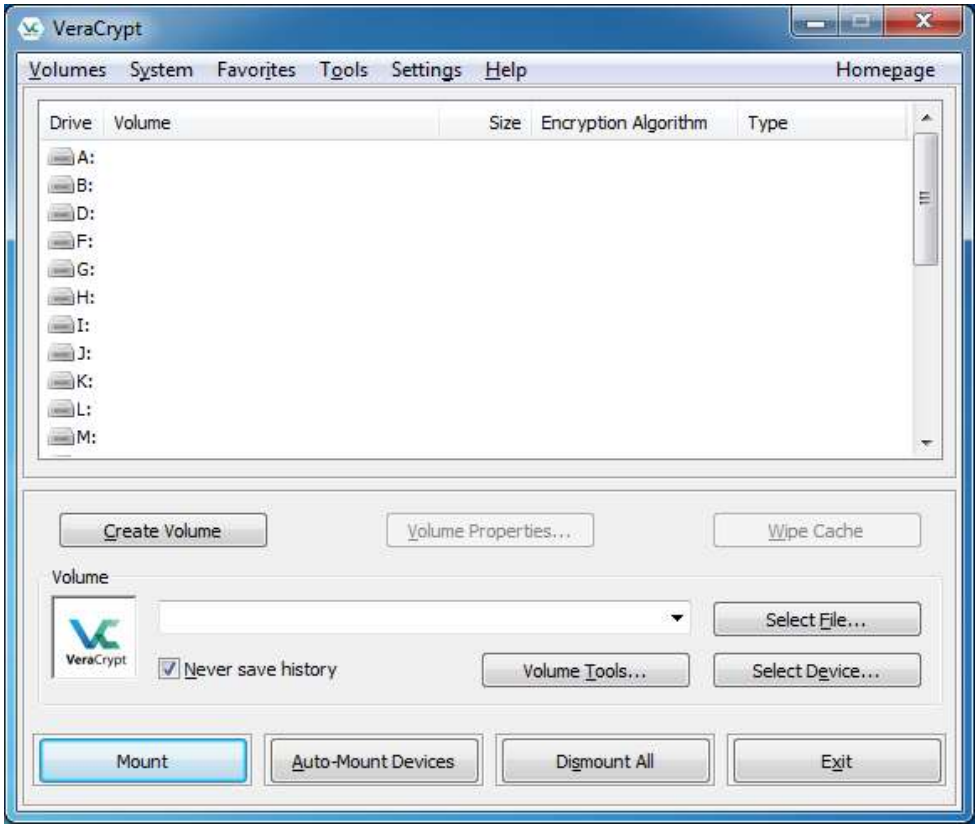
ფარული ტომის შესაქმნელად ორი მიდგომა არსებობს. ორივე მათგანი ძალიან გავს ჩვეულებრივი ტომის შექმნის პროცესს.

ჩვეულებრივი რეჟიმი: ამ დროს იქმნება ჩვეულებრივი ტომი, შემდეგ კი მის შიგნით ფარული ტომი.

პირდაპირი რეჟიმი: თქვენ უკვე გაქვთ ჩვეულებრივი ტომი, რომლის შიგნითაც თქვენ შექმნით ფარული ტომს.

ჩვენი მაგალითის შემთხვევაში გამოვიყენოთ პირდაპირი რეჟიმი.

ბიჯი 1: სამუშაო მაგიდიდან გავუშვათ პროგრამა VeraCrypt. გაიხსნება პროგრამის ძირითადი ფანჯარა.

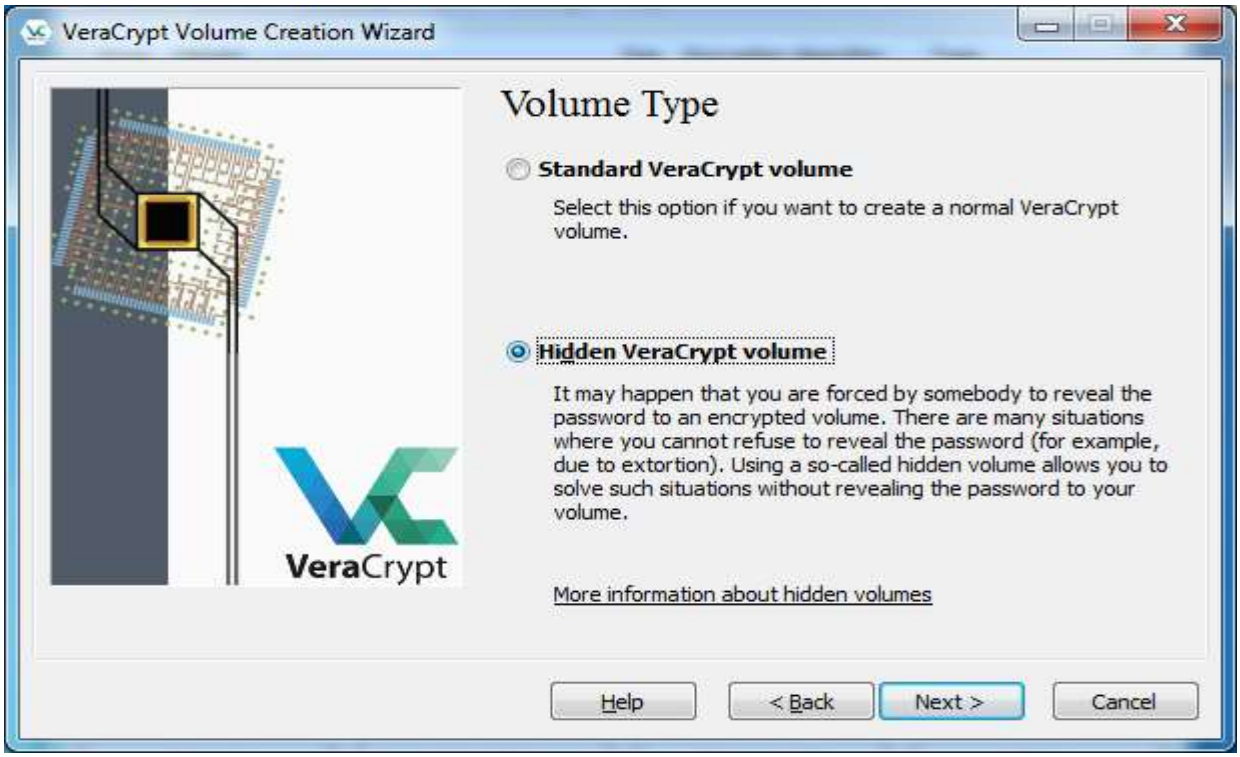


ნახ.22

ბიჯი 2: დავაჭიროთ ღილაკს - Create Volume, რომ შევქმნათ ახალი ტომი.

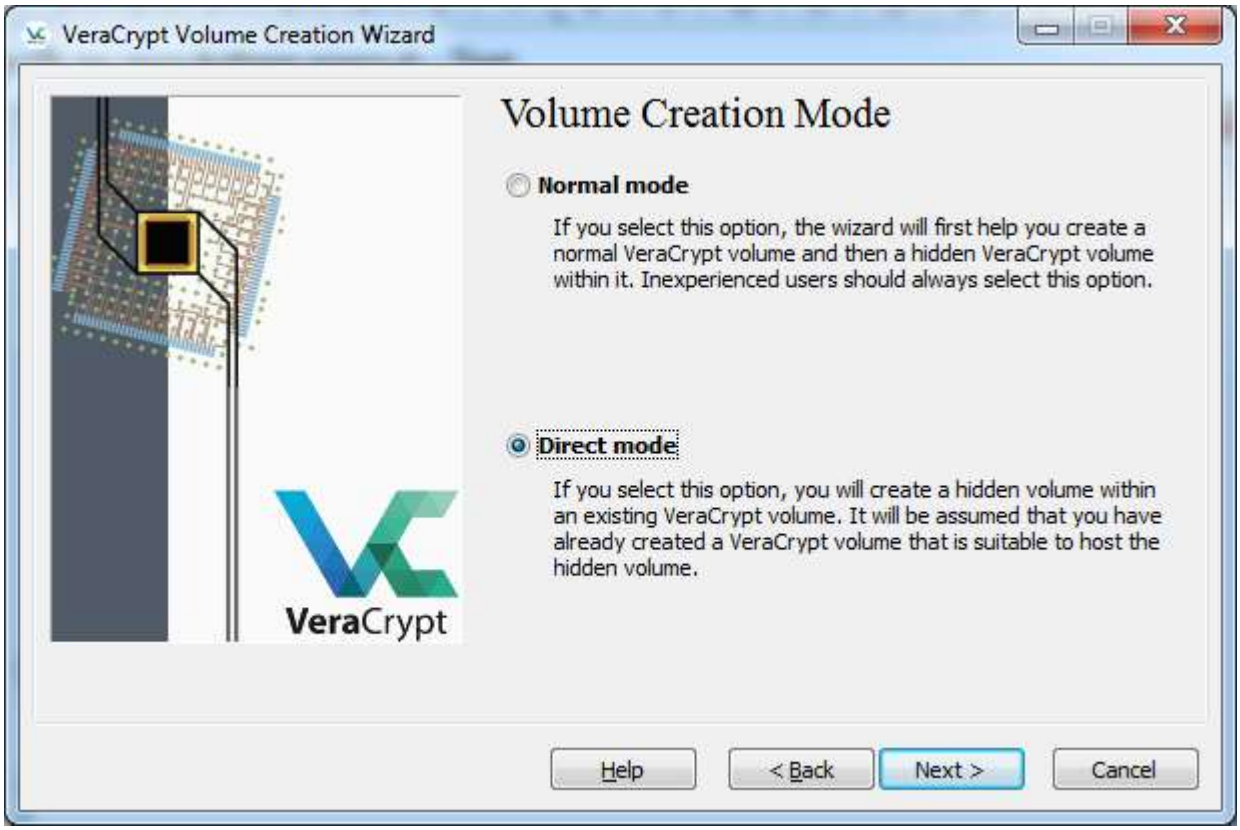
ნახ.23

ბიჯი 3: გამოსულ ფანჯარაში დავტოვოთ მონიშნული ალამი უცვლელად და დავაჭიროთ ღილაკს - Next.



ნახ.24

ბიჯი 4: ფანჯარაში მოვნიშნოთ მეორე ალამი, რაც ნიშნავს რომ ვქმნით ფარულ ტომს და დავაჭიროთ ღილაკს - Next.

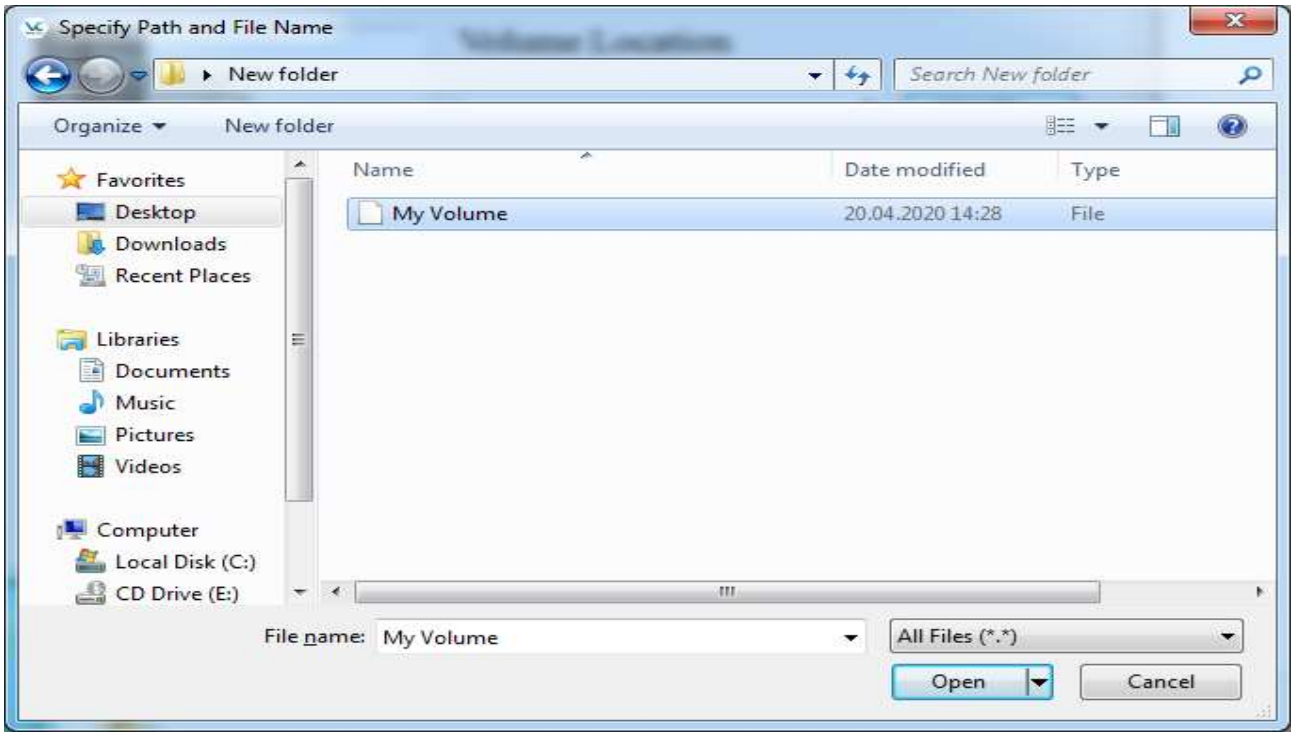


ნახ.25

ბიჯი 5: ფანჯარაში მოვნიშნოთ "Direct mode" ალამი, რაც ნიშნავს რომ ვირჩევთ პირდაპირ რეჟიმს და დავაჭიროთ ღილაკს - Next.

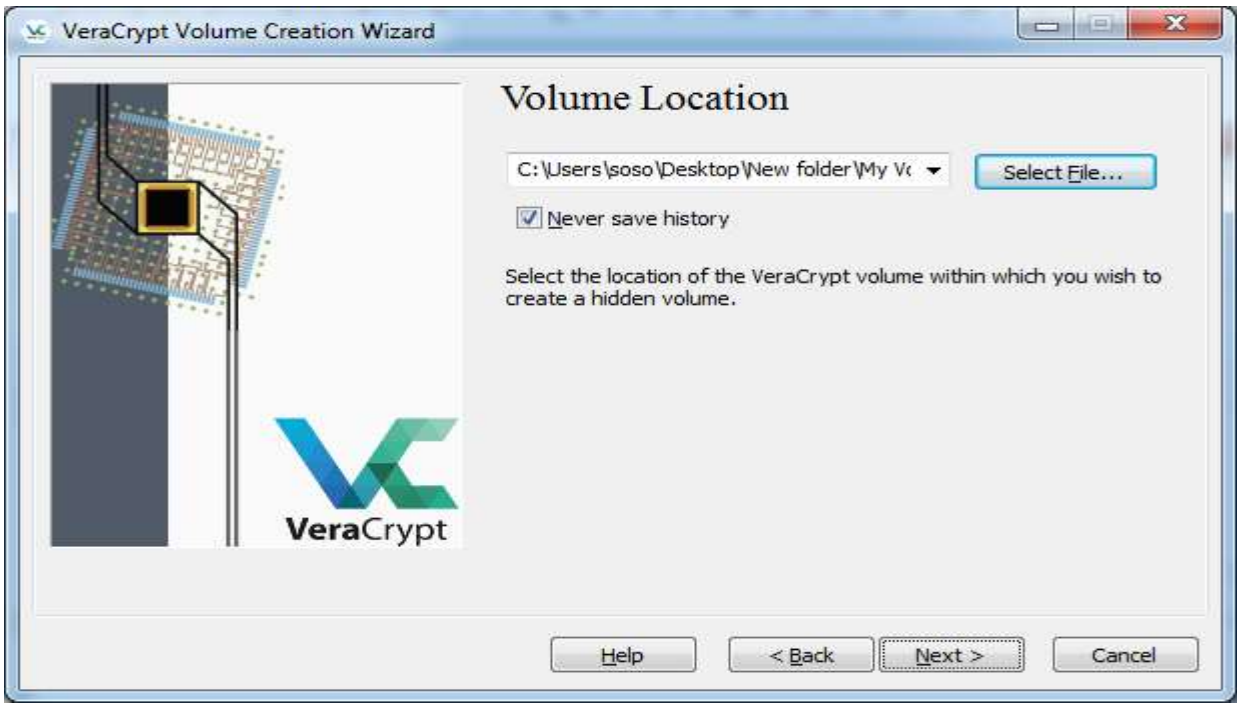
ნახ.26

ბიჯი 6: დავაჭიროთ ღილაკს - Select File.... ავირჩიოთ ჩვეულებრივი ტომით შექმნილი ფაილ-კონტეინერი.



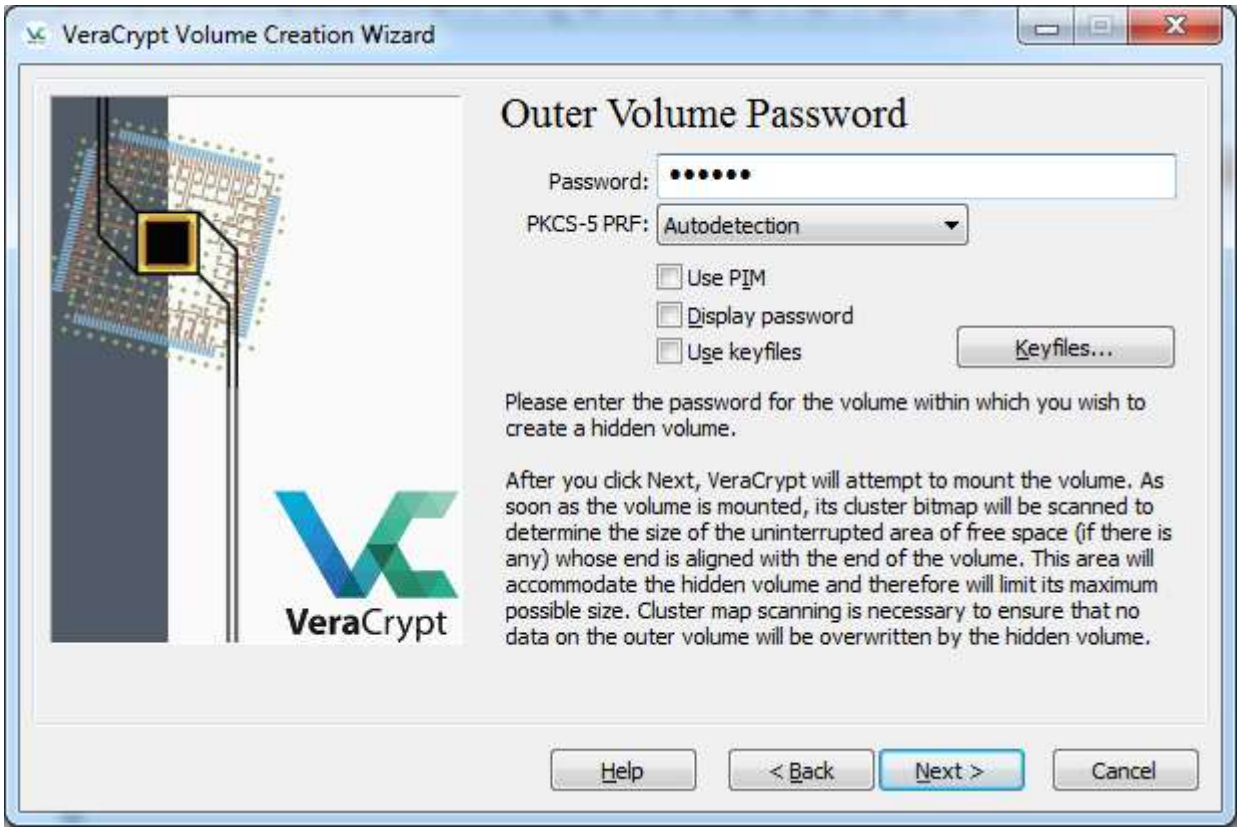
ნახ.27

ბიჯი 7: დავაჭიროთ ღილაკს - Open.



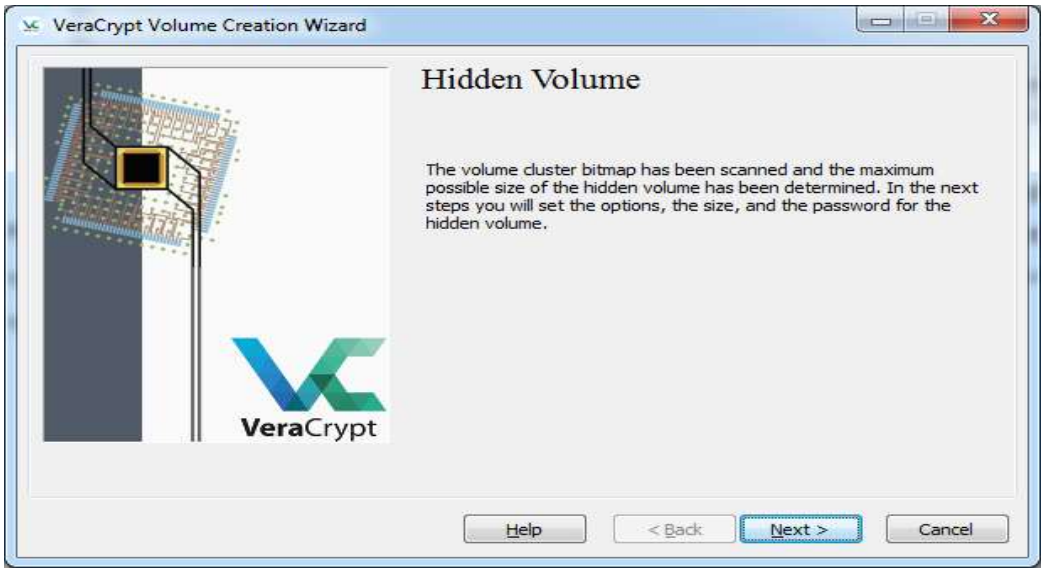
ნახ.28

ბიჯი 8: დავაჭიროთ ღილაკს - Next და დავაყენოთ შიფრირების პარამეტრები.



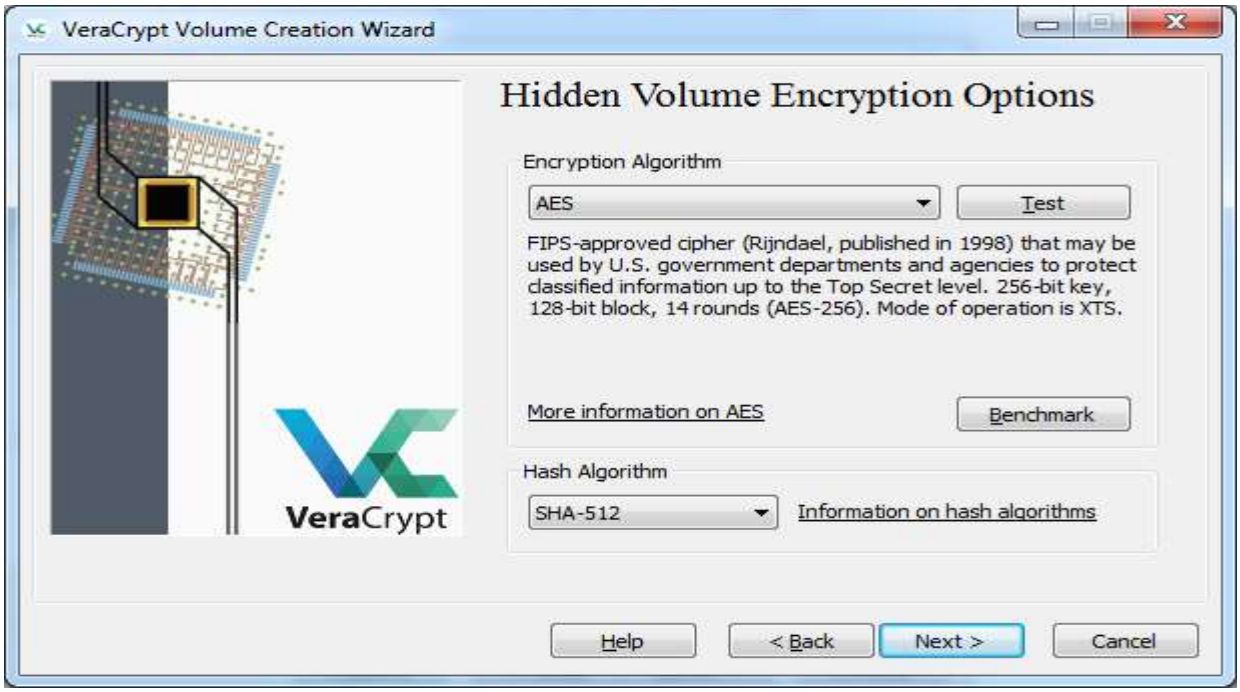
ნახ.29

ბიჯი 9: Password ფანჯარაში შეიტანება პაროლი, რომელიც გამოვიყენეთ ჩვეულებრივი ტომის შექმნის დროს. დანარჩენი პარამეტრები დავტოვოთ უცვლელად და დავაჭიროთ ღილაკს - Next, რათა მოვამზადოთ ჩვეულებრივი ტომი, იმისათვის რომ დაემატოს ფარული ტომი.



ნახ.30

ბიჯი 10: დავაჭიროთ ღილაკს - Next, რათა მოვახდინოთ ფარული ტომისთვის შიფრირების პარამეტრების დაყენება.



ნახ.31

ბიჯი 11: შიფრირების ალგორითმების პარამეტრები დავტოვოთ უცვლელად და დავაჭიროთ ღილაკს - Next, რათა მოვახდინოთ ფარული ტომისთვის ზომის დაყენება.

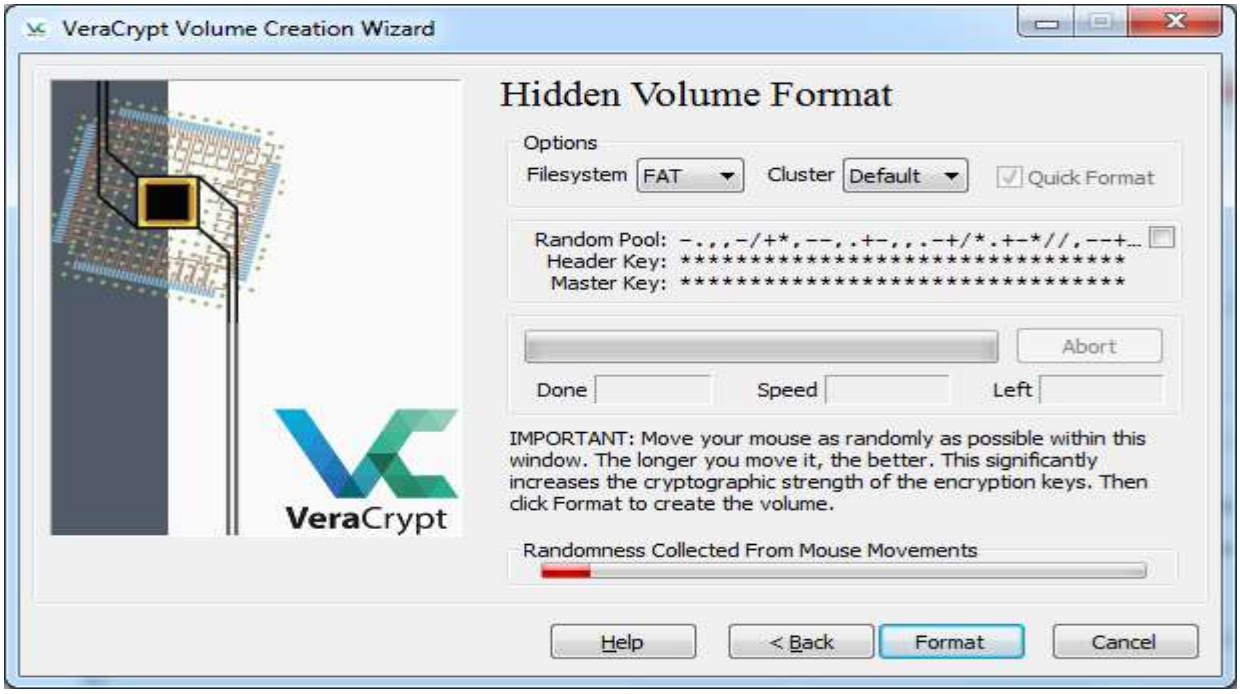
ნახ.32

ბიჯი 12: გამოსულ ფანჯარაში ფარული ტომისთვის უნდა დავაყენოთ შესაქმნელი კონტეინერის ზომა, სადაც უნდა განთავსდეს დასაშიფრი ფაილები. სასურველია რომ ზომა

იყოს ჩვეულებრივ ტომზე ნაკლები. ჩვენი მაგალითის შემთხვევაში დავაყენით 200 მბ და დავაჭიროთ ღილაკს - Next, რათა მოვახდინოთ პაროლის შეტანა.

ნახ.33

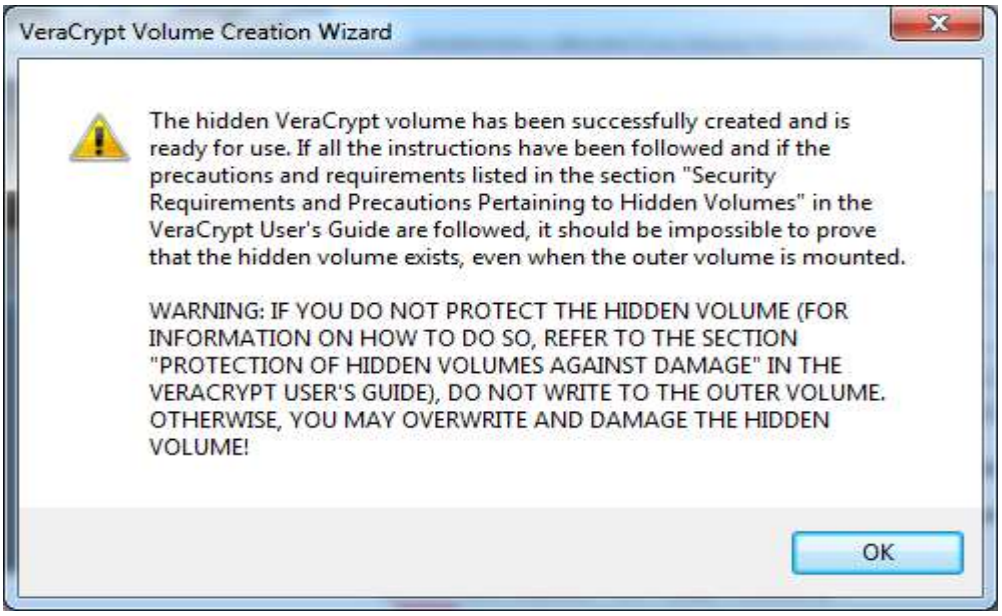
ბიჯი 13: ფანჯარაში ფარული ტომისთვის უნდა შევიტანოთ პაროლი, რომელიც უნდა გასხვავდებოდეს ჩვეულებრივი ტომის პაროლისაგან. სასურველია რომ აქაც შევიტანოთ რთული პაროლი და დავაჭიროთ ღილაკს - Next.



ნახ.34

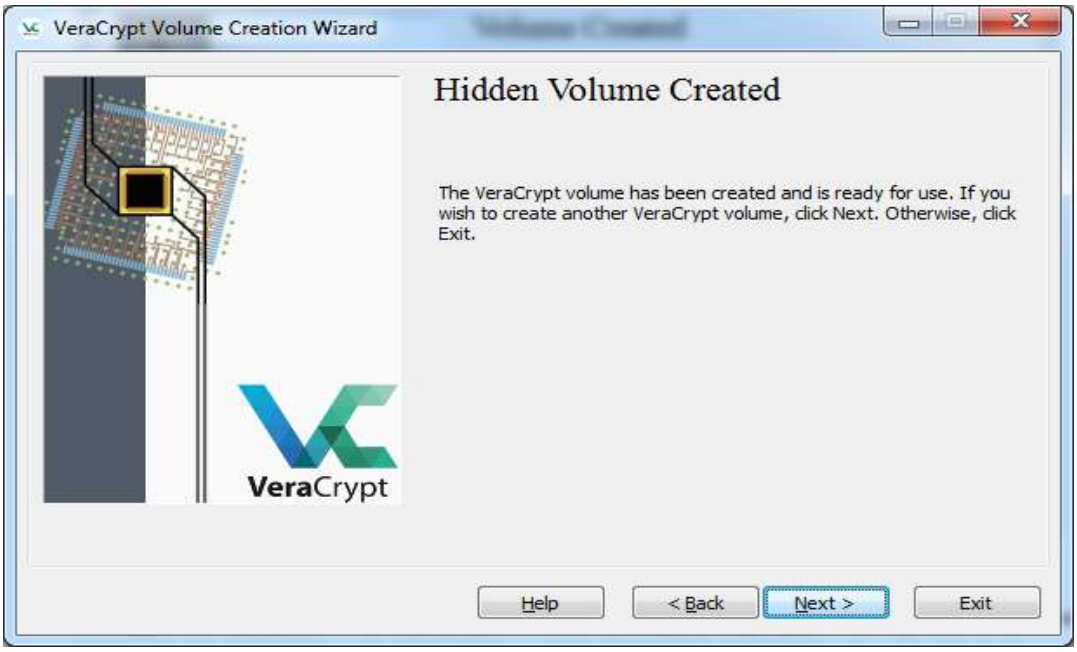
ბიჯი 14: დავტოვოთ პარამეტრები უცვლელად და დავაჭიროთ ღილაკს - Format, რომ მოხდეს ფარული ტომის შექმნა.

პროცესის დასრულების შემდეგ გამოდის შეტყობინება ფარული ტომის შესახებ:



ნახ.35

ბიჯი 15: დავაჭიროთ ღილაკს - OK. გამოდის შეტყობინების ფანჯარა, რომ ფარული ტომი იქნა შემნილი.



ნახ.36

ბიჯი 13: დავაჭიროთ ღილაკს - Exit და დავბრუნდეთ პროგრამის ძირითად ფანჯარაზე.

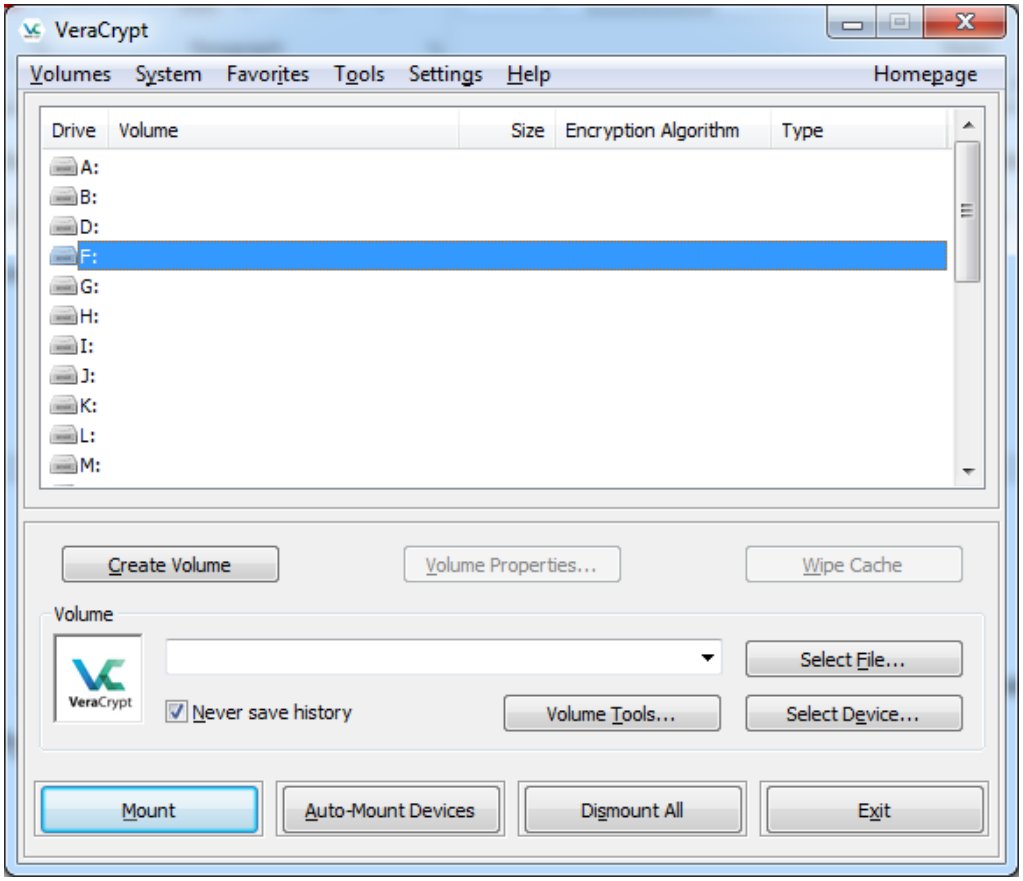
ამით **ფარული ტომის** შექმნის პროცესი დასრულებულია.

დაშიფრული ტომის გახსნა:

პროგრამა VeraCrypt-ში როდესაც მოხდება დაშიფრული ტომის წარმატებით გახსნა (ამოშიფვრა), სისტემაში გაიხსნება ახალი პორტატიული დისკი, სადაც შესაძლებელი იქნება ფაილებისა და ფოლდერების ჩაწერა, დათვალიერება, შეცვლა და წაშლა. ფაილებთან სამუშაოს დასრულების შემდეგ უნდა მოხდეს გახსნილი ტომის ისევ დაშიფვრა და სისტემიდან გაქრება მიერთებული დისკი. ჩვეულებრივი და ფარული ტომის ამოშიფვრა ხდება ერთნაირად. პაროლის შეტანის შესაბამისად გაიხსნება შესაბამისი ტომი, ვინაიდან ჩვეულებრივი და ფარული ტომის პაროლები არის სხვადასხვა.

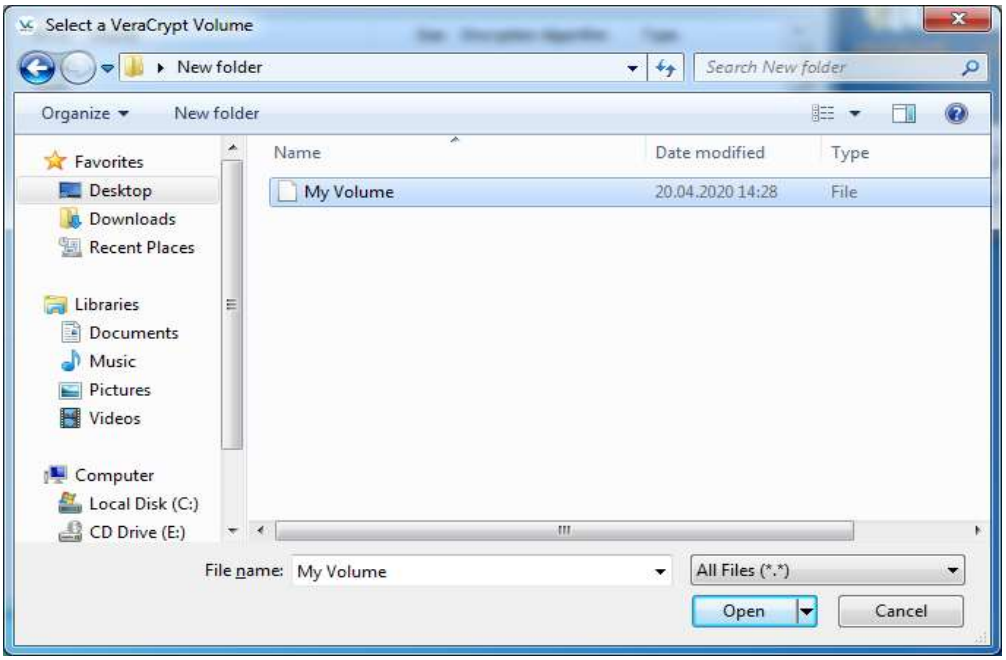
განვიხილოთ პროცესი, თუ როგორ ხდება ტომის ამოშიფვრა:

ბიჯი 1: გავხსნათ VeraCrypt პროგრამის ძირითადი ფანჯარა და მასში მოვნიშნოთ რომელიმე დისკის დასახელება.



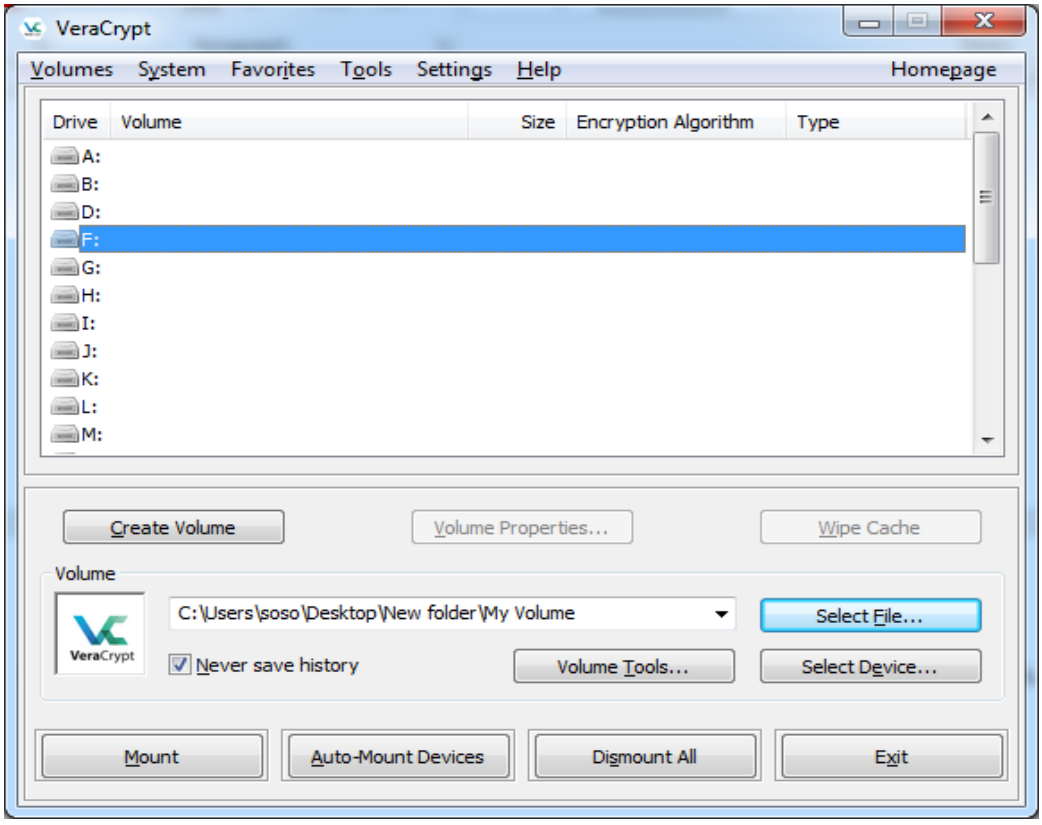
ნახ.37

ბიჯი 2: დავაჭიროთ ღილაკს - Select File და ავირჩიოთ ჩვენს მიერ შექმნილი ფაილ-კონტეინერი.



ნახ.38

ბიჯი 3: დავაჭიროთ ღილაკს - Open და დავუბრუნდეთ ძირითად ფანჯარას.

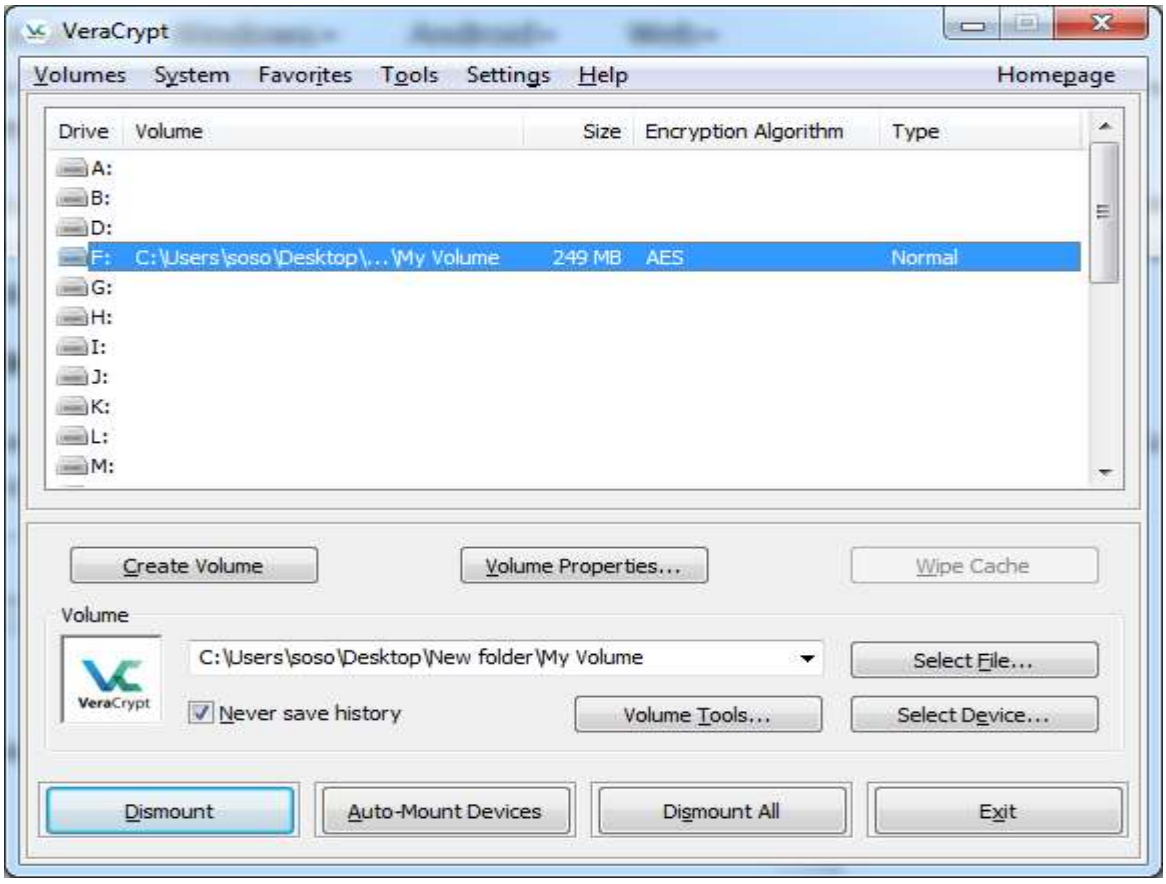


ნახ.39

ბიჯი 4: დავაჭიროთ ღილაკს - Mount.

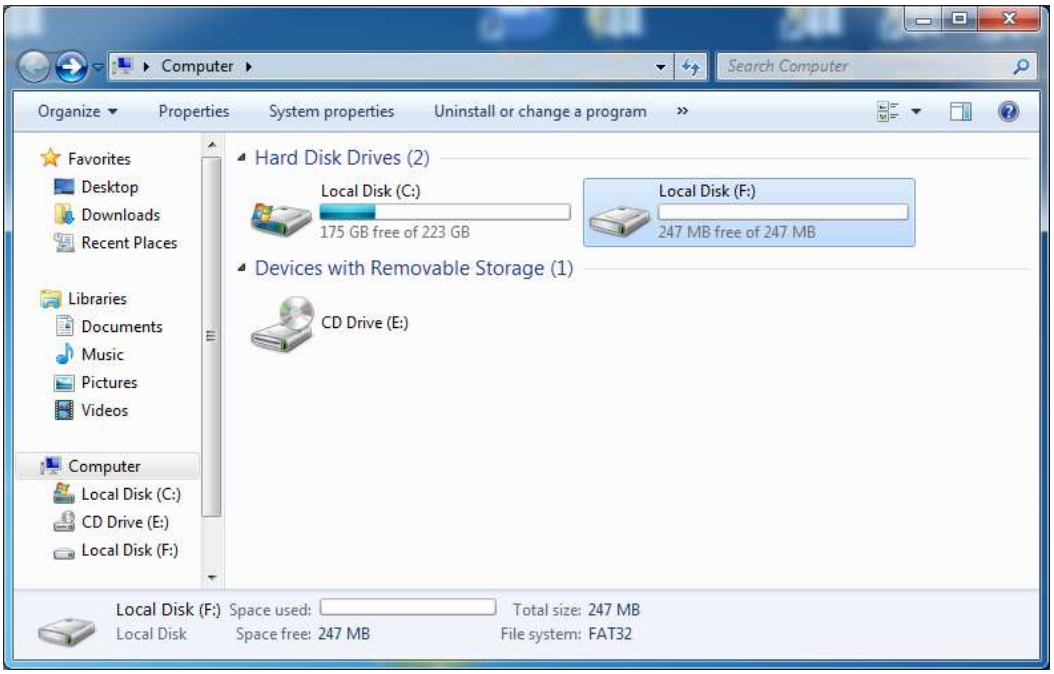
ნახ.40

ბიჯი 5: თუ გვინდა რომ ამოვშიფროთ ჩვეულებრივი ტომი, შეგვაქვს შესაბამისი პაროლი, ხოლო ფარული ტომის შემთხვევაში შეგვაქვს მისი შესაბამისი და დავაჭიროთ ღილაკს - OK. რის შემდეგაც მოხდება შესაბამისი ტომის ამოშიფვრა და მიებმება არჩეულ დისკს.



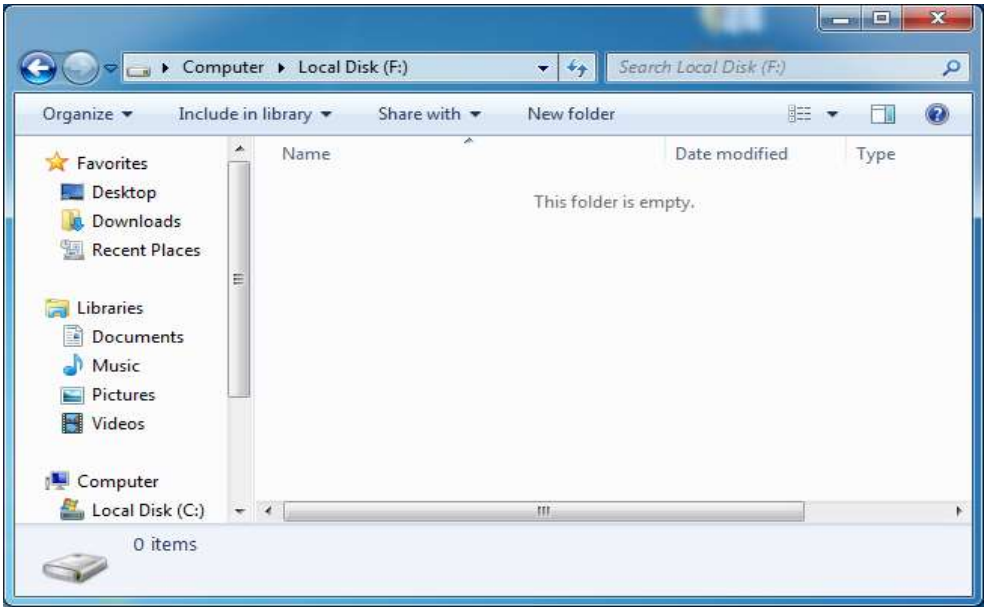
ნახ.41

ბიჯი 6: იმისათვის, რომ მოვახდინოთ არჩეული დისკის გახსნა, ორჯერ უნდა დავკლიკოთ ძირითადი ფანჯრის შესაბამის ჩანაწერზე ან დისკების დასახელებებიდან ავირჩიოთ შესაბამისი დისკი.



ნახ.42

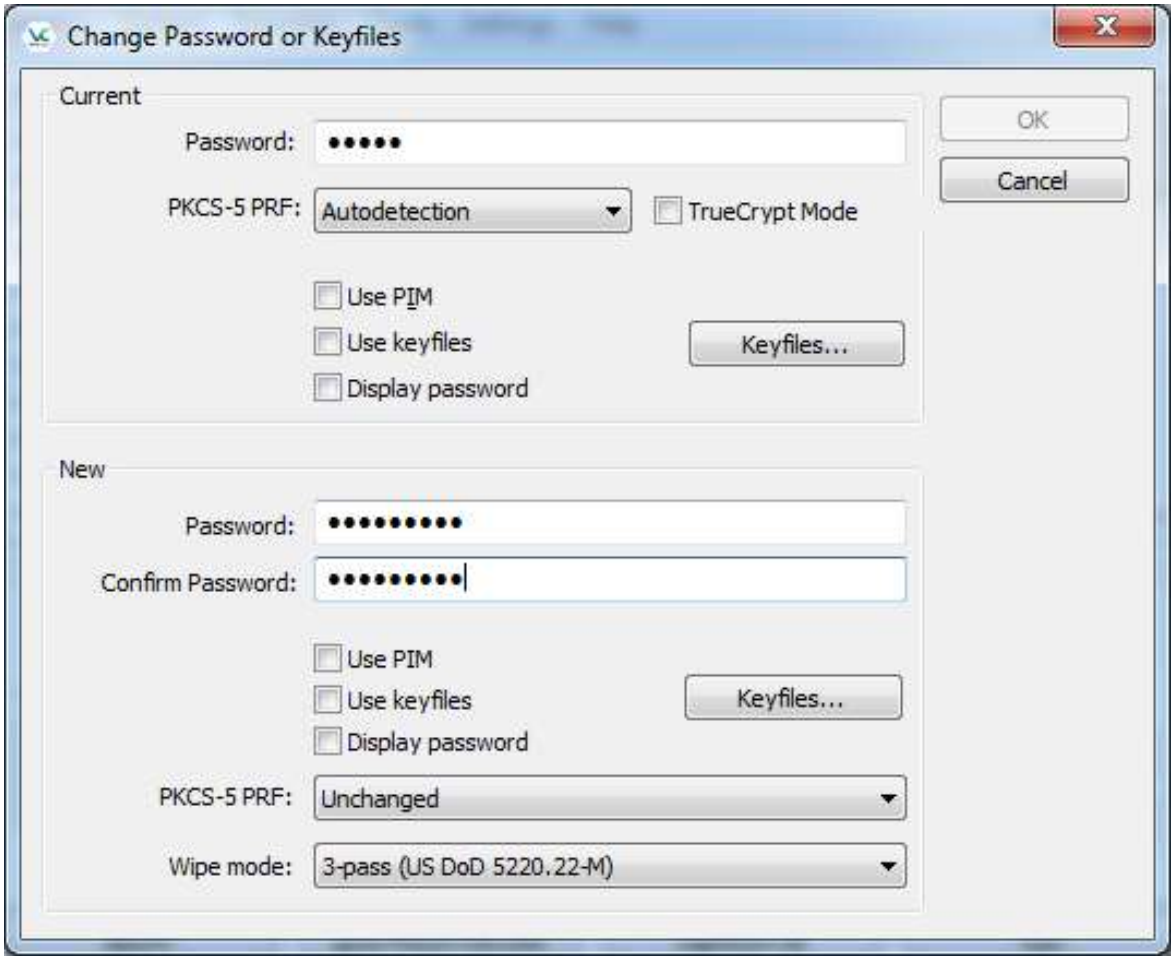
ბიჯი 7: დისკის გახსნის შემდეგ თვდაპირველად ვნახავთ, რომ ცარიელი იქნება და მასში შეგვიძლია განვახორციელოთ ფაილებისა და ფილდერების ჩაწერა, დათვალიერება, რედაქტირება და წაშლის ოპერაციები.



ნახ.43

ბიჯი 8: ვირტუალურ დისკში ფაილების მანიპულაციის შემდეგ უნდა მოვახდინოთ მისი ჩაკეტვა (დაშიფვრა), ამისათვის ძირითად ფანჯარაზე დავაჭიროთ ღილაკს - Dismount.

ჩვეულებრივ ან ფარულ ტომზე პაროლის შესაცვლელად ძირითად ფანჯარაზე არჩეულ დისკს უნდა მივაბათ შესაბამისი ფაილ-კონტეინერი, შემდეგ შევდივართ Volumes მენიუში და ვირჩევთ Change Password of Keyfiles პუნქტს.



ნახ.44

Password ფანჯარაში შეგვყავს იმ ტომის პაროლი, რომლის შეცვლაც გვინდა და New განყოფილების ფანჯრებში შეგვყავს ახალი პაროლი. ბოლოს OK ღილაკის დახმარებით ხდება ძველი პაროლის ჩანაცვლება ახალი პაროლით.

პრაქტიკული N5

რისკების მენეჯმენტი ღრუბლოვან ტექნოლოგიებში.

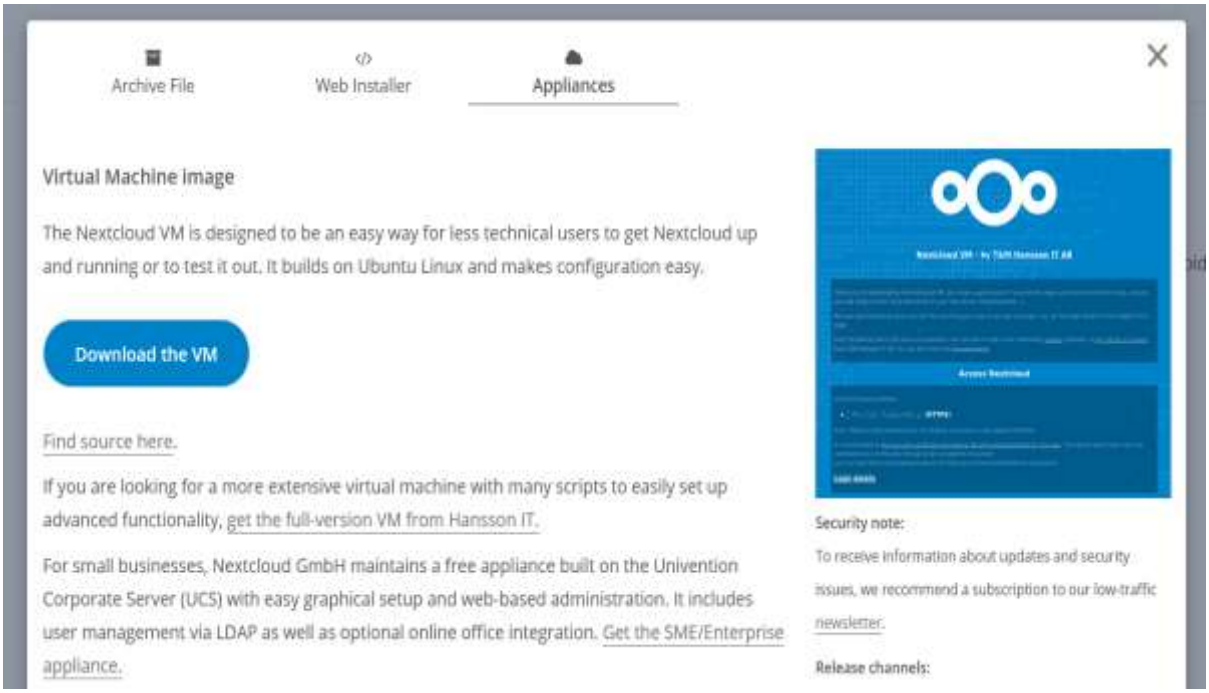
მიზანი: ღია კოდის მქონე ღრუბლოვანი ტექნოლოგიის NextCloud პროგრამული პაკეტის დაყენება ოპერაციულ სისტემაზე. სისტემის სრულფასოვანი კონფიგურირება და ადმინისტრირების საშუალებების ძირითადი პრინციპების გაცნობა.

Nextcloud არის საჯაროდ ხელმისაწვდომი ღრუბლოვანი ტექნოლოგიების პლატფორმა, რომელიც შესაძლებელია ჩვენს ორგანიზაციაში იქნას დანერგილი. სისტემას გააჩნია მომხმარებლების სამართავი მექანიზმები, რაც საშუალებას იძლევა ორგანიზაციის შიგნით, შიდა ქსელის მეშვეობით, ერთმანეთში ფაილების მიმოცვლის კონფიდენციალურობის გარანტიას.

Nextcloud სისტემა არსებობს როგორც პროგრამული პაკეტის სახით, ასევე ვირტუალური მანქანის სახითაც. მოცემულ პრაქტიკულ სამუშაოში განხილულია Nextcloud სისტემის ინსტალაცია ვირტუალური მანქანის გარემოცვაში.

ოფიციალური ვებ-გვერდიდან შესაძლებელია ვირტუალური მანქანის გადმოწერა „OVA“ ფაილურ ფორმატში, რომლის მხარდაჭერა გააჩნია როგორც VMware-ს, ასევე VirtualBox ვირტუალიზაციის პროგრამებს.

გადმოსაწერი ბმული: https://download.nextcloud.com/vm/Nextcloud-VM.ova

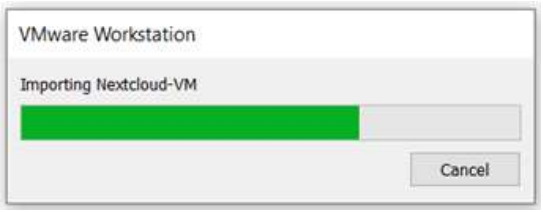


ნახ.1

გადმოწერილი ფაილის დასახელება იქნება „**Nextcloud-VM.ova**“, ხოლო მისი მოცულობა დაახლოებით 1GB შეადგენს (ნახ.2).

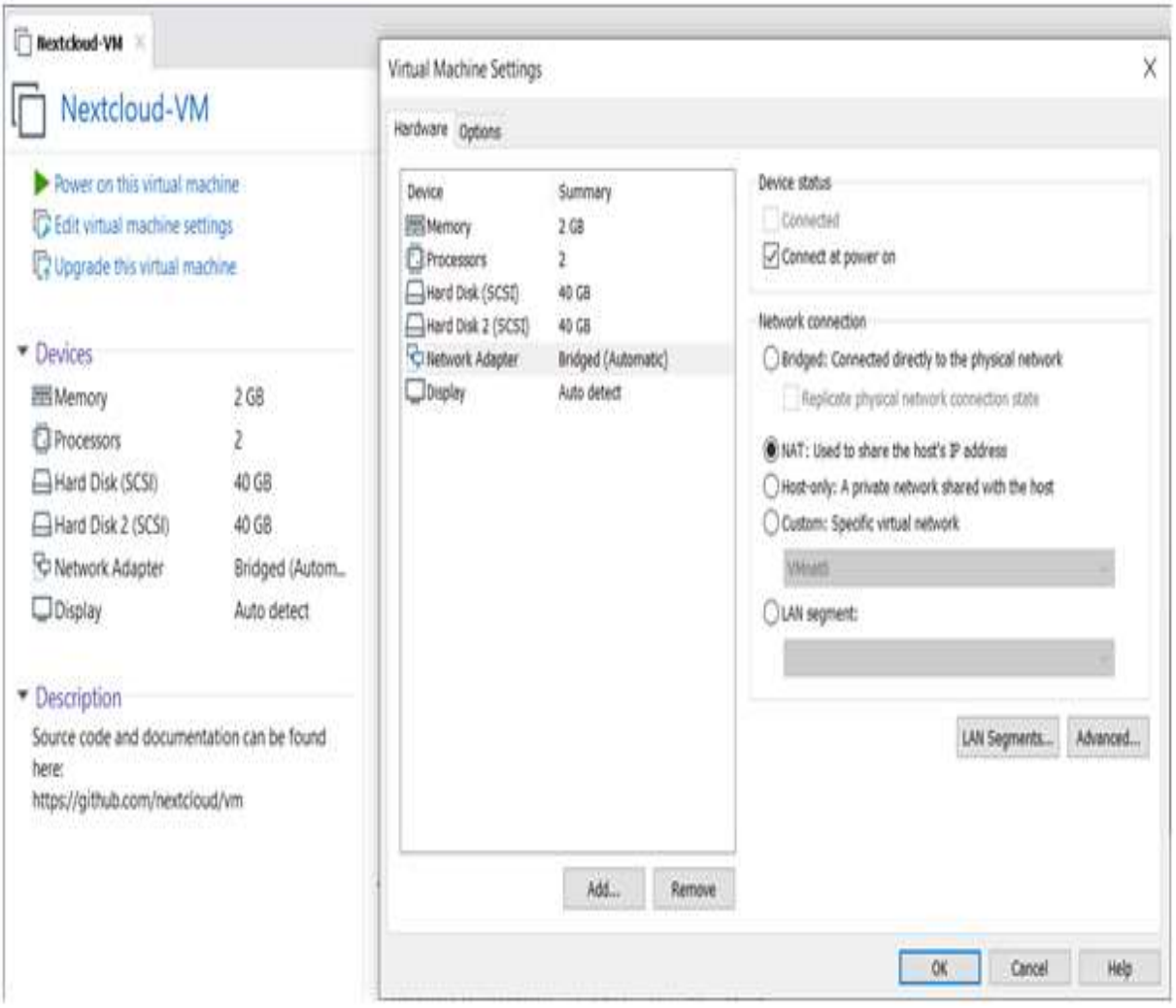
გადმოწერილ ფაილზე ორჯერ დაწკაპუნებით დაიწყება იმიჯის იმპორტირება VMware პროგრამაში (ნახ.3).

ნახ.2



ნახ.3

იმპორტირებას დაახლოებით 5 წუთი სჭირდება. შედეგად მივიღებთ ვირტუალურ მანქანას „**Nextcloud-VM**“ დასახელებით. სანამ მას ჩავრთავთ, საჭიროა კონფიგურაციის გადამოწმება. რეკომენდირებულია „Network Adapter“ პარამეტრის შეცვლა „Bridged“ ვარიანტიდან „NAT“ ვარიანტზე (ნახ.4).

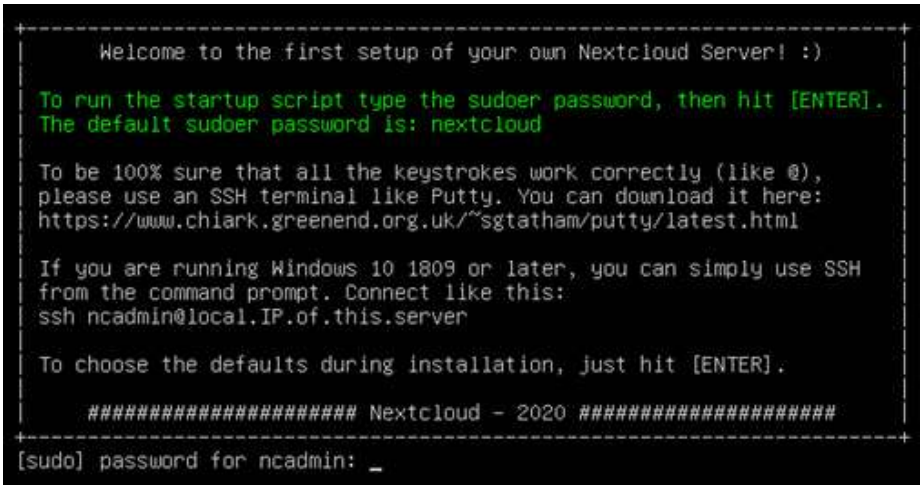


ნახ.4

კონფიგურაციის შემდეგ შეგვიძლია ჩავრთოთ ვირტუალური მანქანა. ჩართვისას გამოდის შეტყობინება სერვერის IP მისამართის, სტანდარტული მომხმარებლის სახელისა და პაროლის შესახებ (ნახ.5).

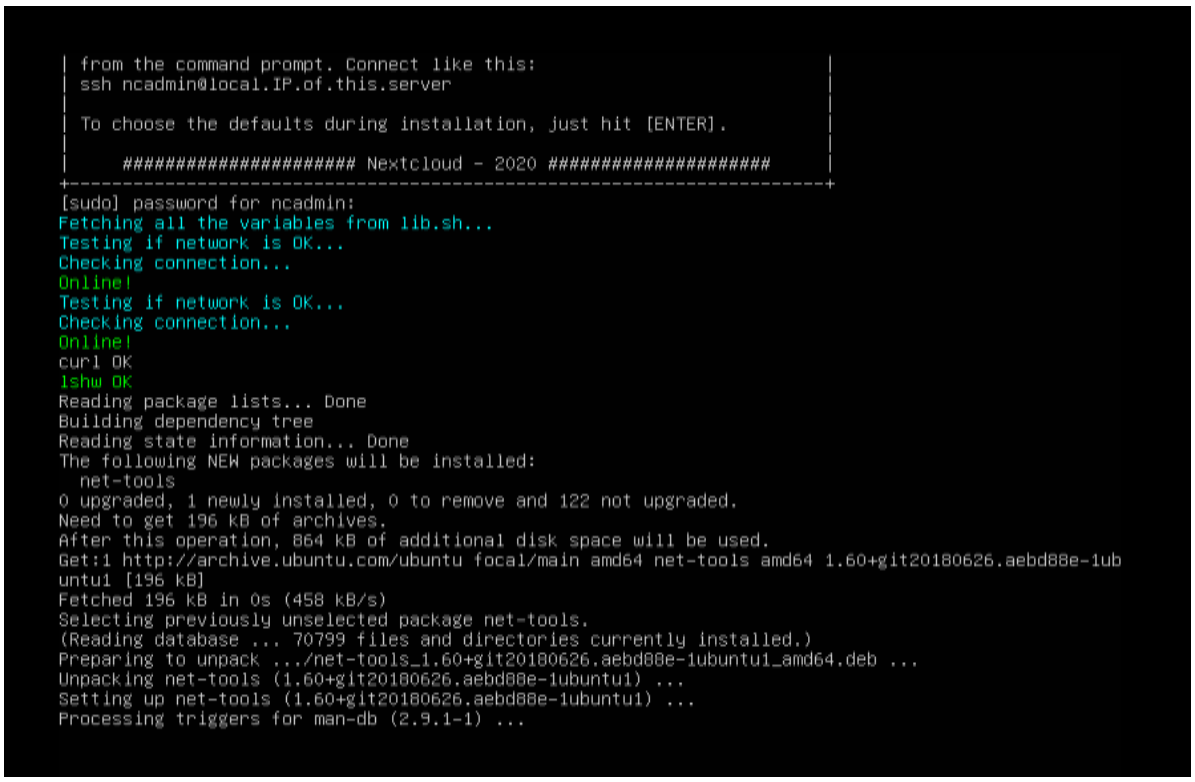
ნახ.5

ავტორიზაციის გავლის შემდეგ, დაიწყება სისტემის ინსტალაციის პროცესი (ნახ.6).



ნახ.6

თავდაპირველად მოწმდება ინტერნეტთან კავშირი, შემდეგ კი ხდება სისტემისთვის საჭირო მოდულების გადმოწერა (ნახ.7).



ნახ.7

გამოდის შეტყობინება პარტიციების კონფიგურირების შესახებ (ნახ.8).

ნახ.8

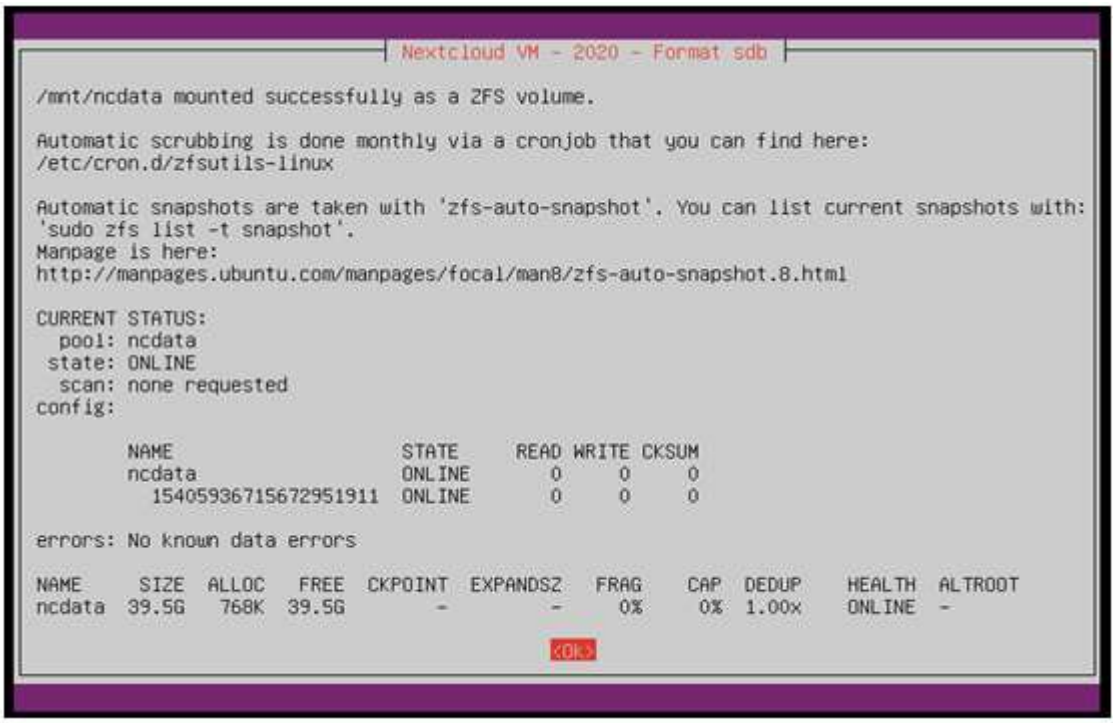
შესაძლებელია ავირჩიოთ როგორც ავტომატური კონფიგურაცია, ასევე ნებისმიერი სხვა მყარი დისკის მითითება, რომელიც ღრუბლოვან საცავში არსებული ფაილების შესანახად გამოიყენება (ნახ.9).

ნახ.9

საჭიროა დაფიქსირებული ვარიანტის დადასტურება, რომელიც არჩეულ დისკს დააფორმატებს (ნახ.10).

ნახ.10

ფორმატირების შემდეგ გამოდის შეტყობინება პროცესის დასრულების შესაბამისი სტატუსით (ნახ.11).



ნახ.11

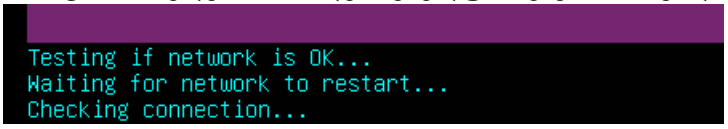
შემდგომ ეტაპზე საჭიროა DNS Resolver პარამეტრის არჩევა. ამ შემთხვევაში არის სამი ვარიანტი:

1. „Quad9“ სერვისის გამოყენება;
2. „Cloudflare“ სერვისის გამოყენება;
3. ლოკალური DNS სერვერის გამოყენება.

ნახ.12

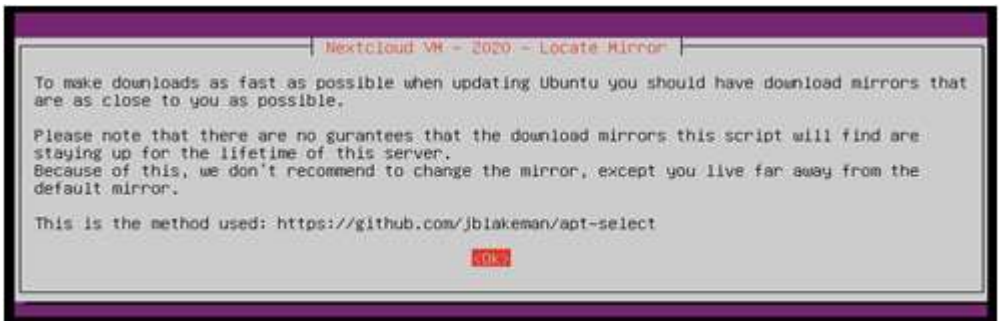
რეკომენდირებულია ლოკალური DNS სერვერის ვარიანტის არჩევა, თუმცა წინა ორი ვარიანტიდან რომელიმეს არჩევაც არ წარმოადგენს პრობლემას.

არჩეული ვარიანტის მიხედვით მოხდება ქსელური კავშირის გადამოწმება.



ნახ.13

შემდეგ ეტაპზე საჭიროა ავირჩიოთ სისტემისთვის საჭირო პაკეტების გადმოსაწერი რეპოზიტორიის მისამართი (ნახ.14-16).

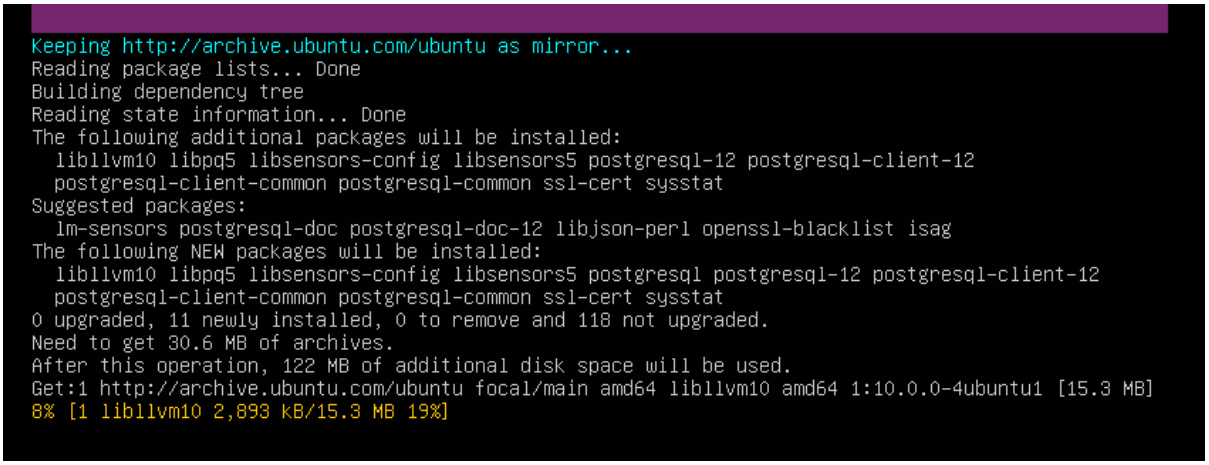


ნახ.14

ნახ.15

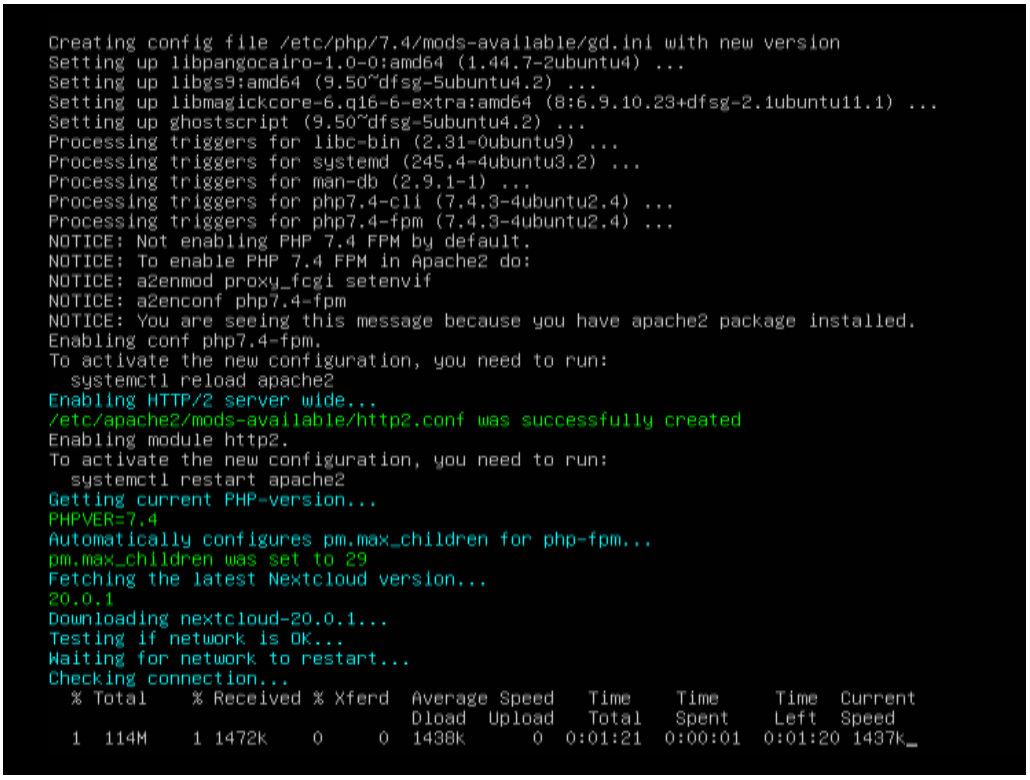
ნახ.16

შესაძლებელია დავტოვოთ სტანდარტული „ubuntu.com“-ის რეპოზიტორი, ან შევცვალოთ სასურველით (ნახ.17).



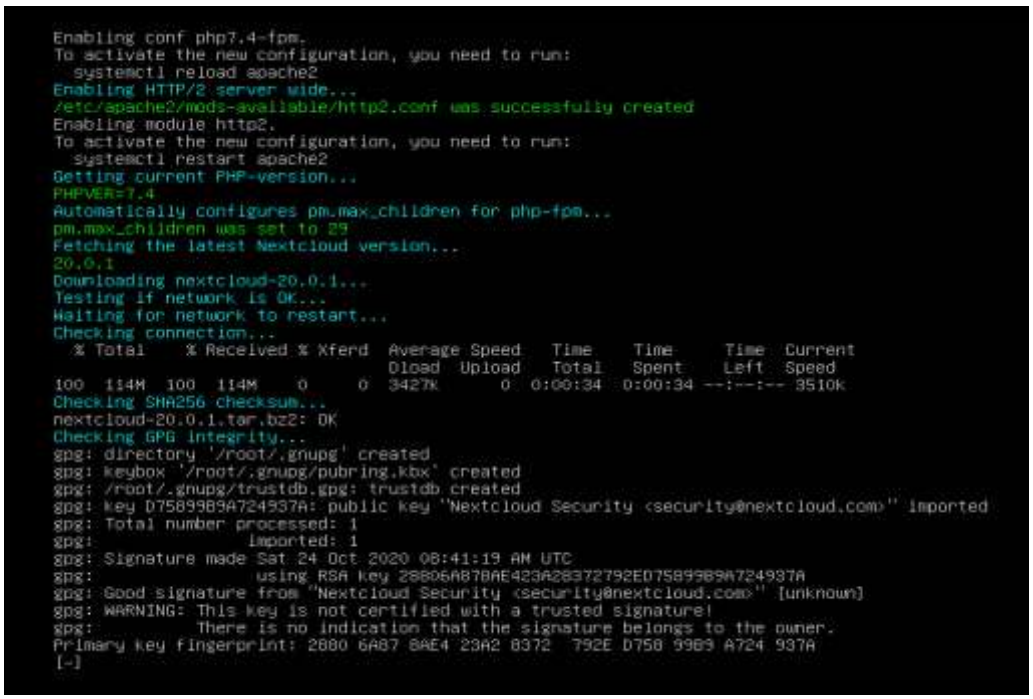
ნახ.17

არჩეული ვარიანტის შესაბამისად მოხდება სისტემისთვის საჭირო მოდულების გადმოწერა (ნახ.18).



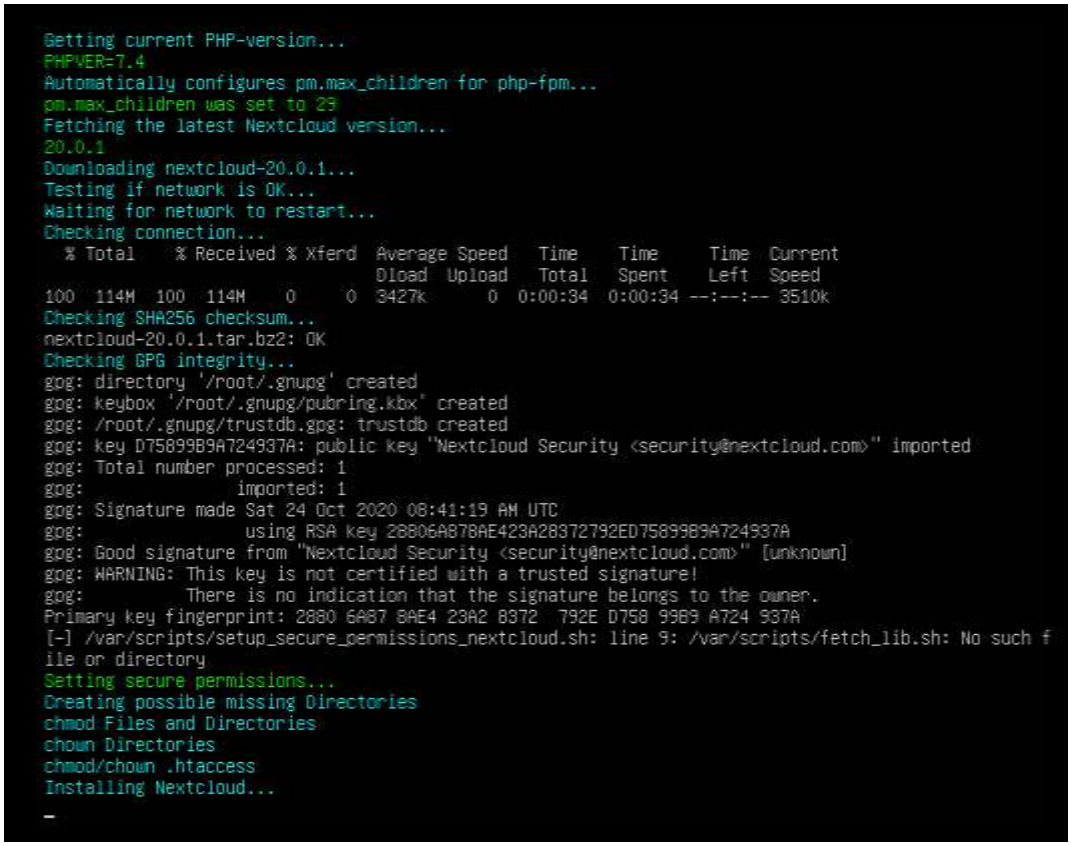
ნახ.18

პროცესის მიმდინარეობისას ჩანს, რომ ინსტალირდება „PHP“ პროგრამული ენის მხარდაჭერა, „Apache“ ვებ-სერვერი და შემდგომ ხდება Nextcloud სისტემის უახლესი ვერსიის ჩამოტვირთვა (ნახ.19).



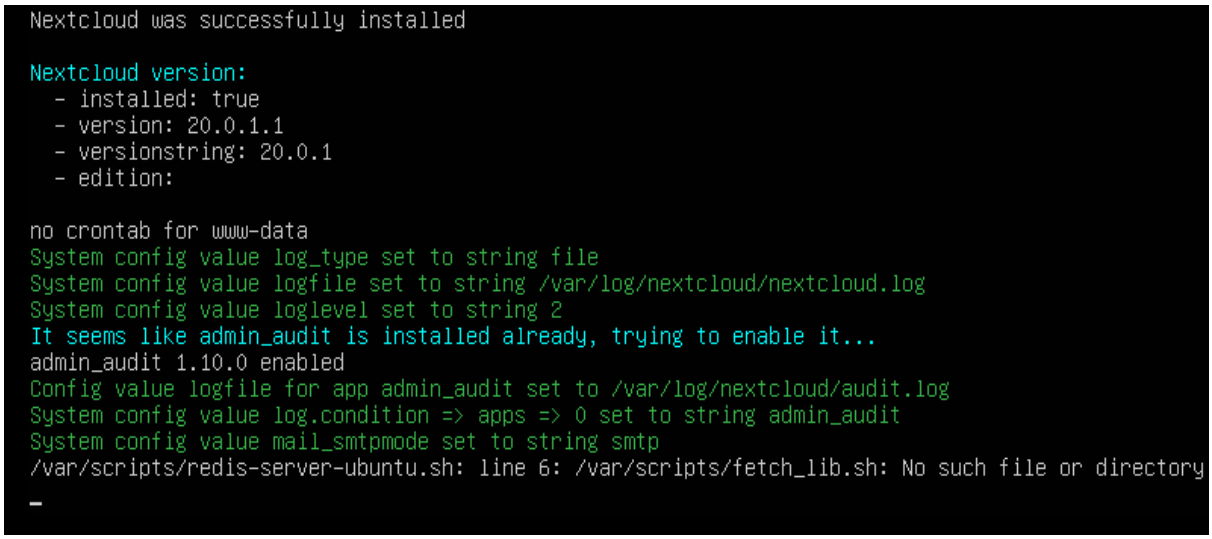
ნახ.19

Nextcloud სისტემის ჩამოტვირთვის შემდგომ მოწმდება მისი მთლიანობა „GPG“ გასაღების მეშვეობით (ნახ/20).



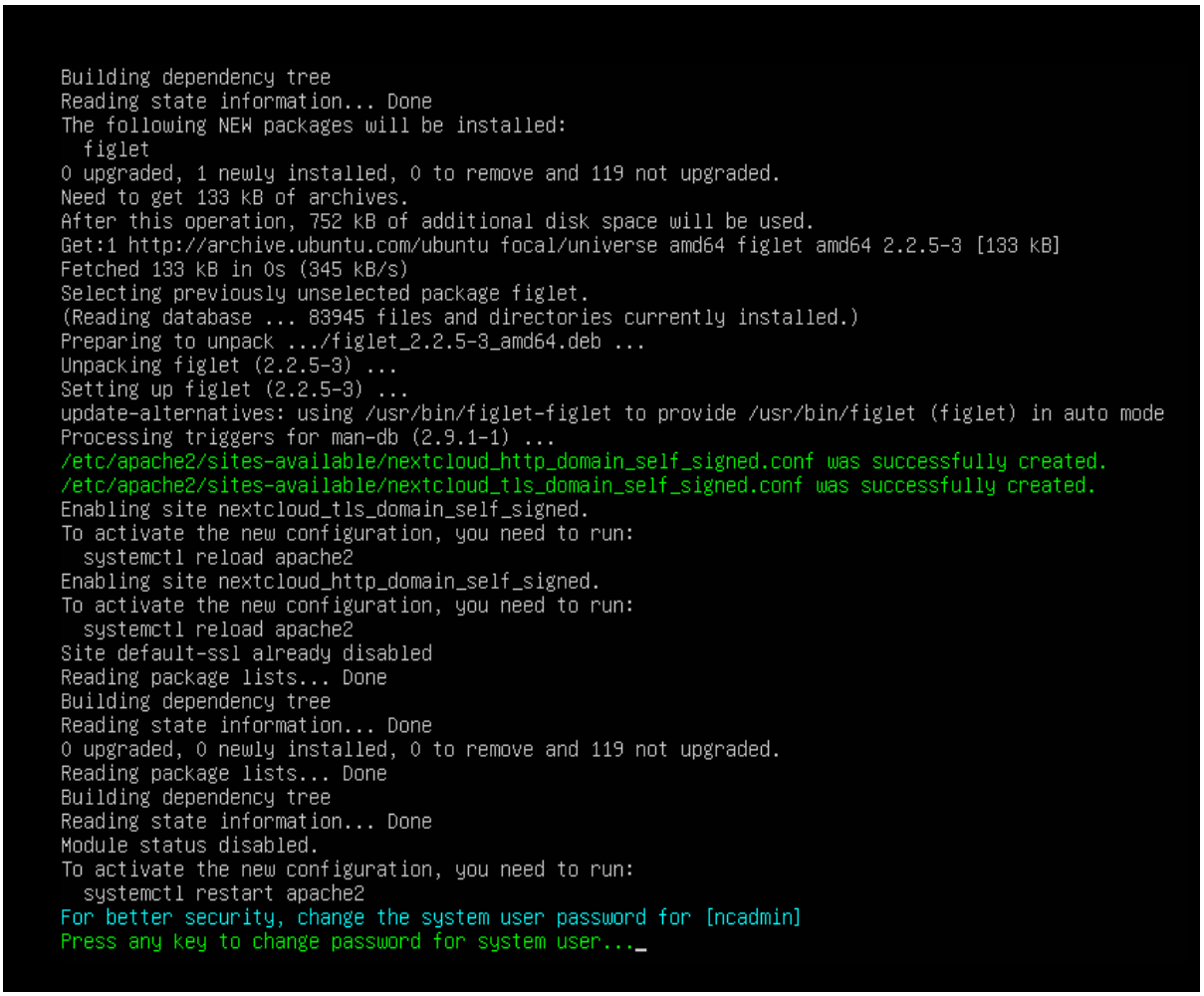
ნახ.20

შემდგომ იქმნება საჭირო დირექტორიები და ეთითება შესაბამისი უფლებები (ნახ.21).



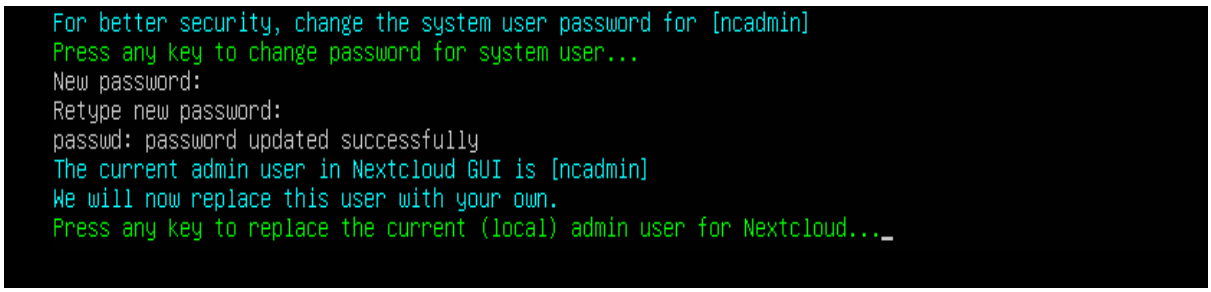
ნახ.21

კიდევ ერთხელ ხდება სისტემისთვის საჭირო მოდულების გადმოწერა (ნახ.22).



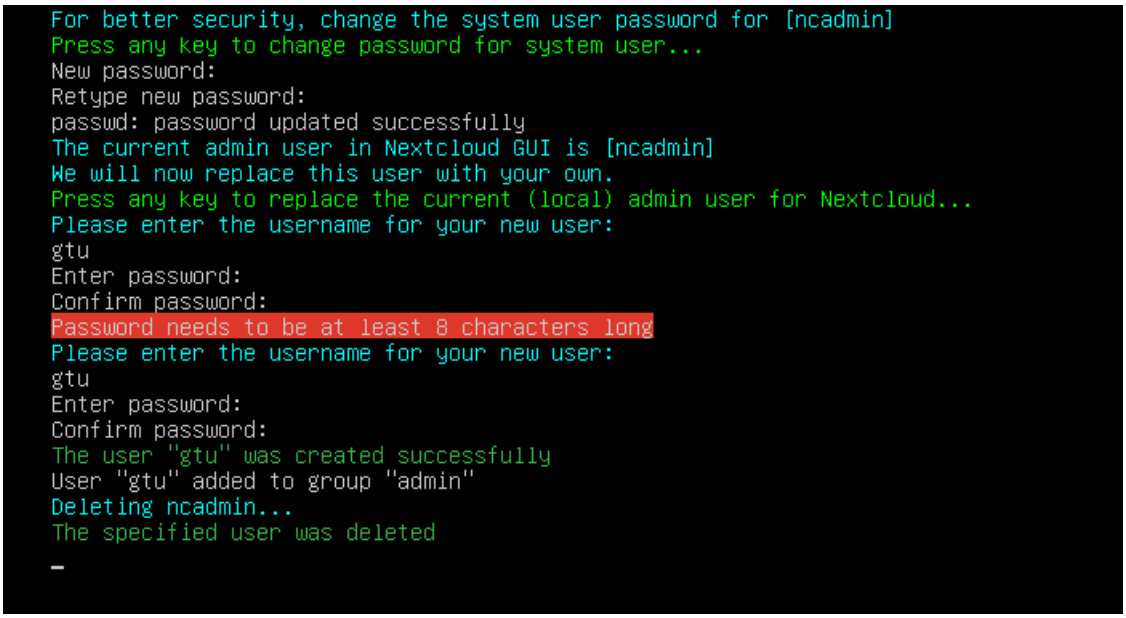
ნახ.22

უსაფრთხოების მიზნით, სისტემა მოგვთხოვს ადმინისტრატორის „ncadmin“ მომხმარებლის პაროლის შეცვლას (ნახ.23).



ნახ.23

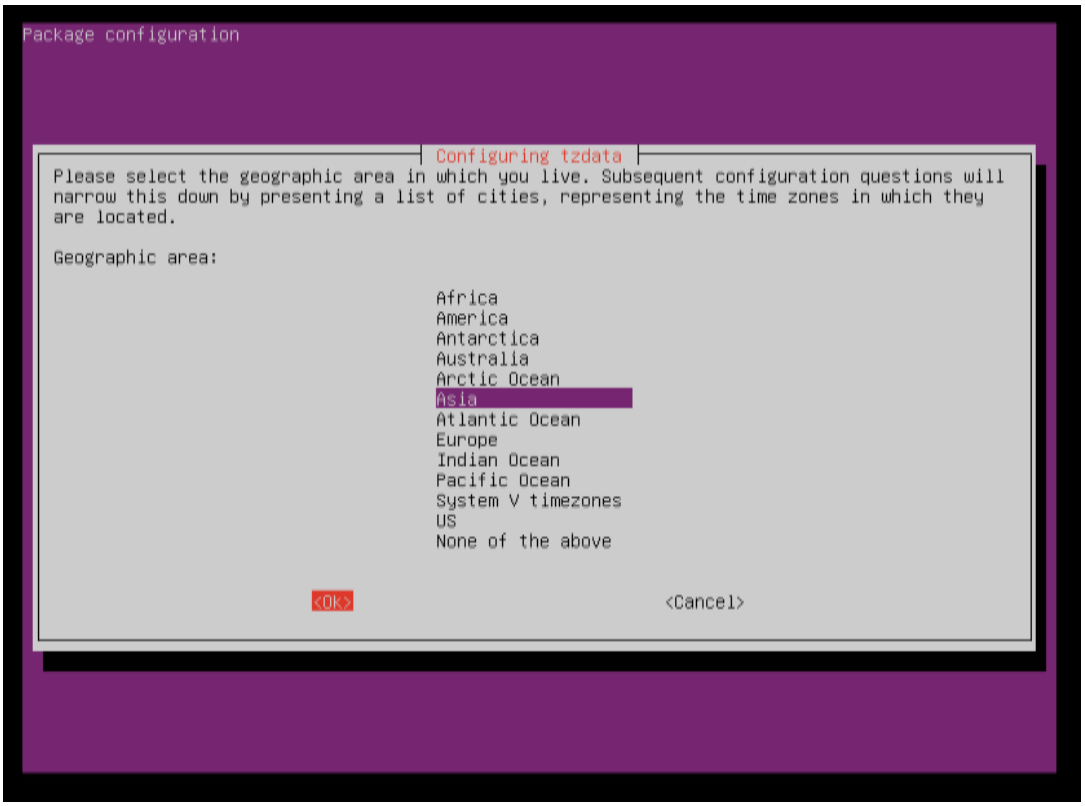
უსაფრთხოების მიზნით, სისტემა მოგვთხოვს ახალი ადმინისტრატორის სახელის მითითებას (ნახ.24).



ნახ.24

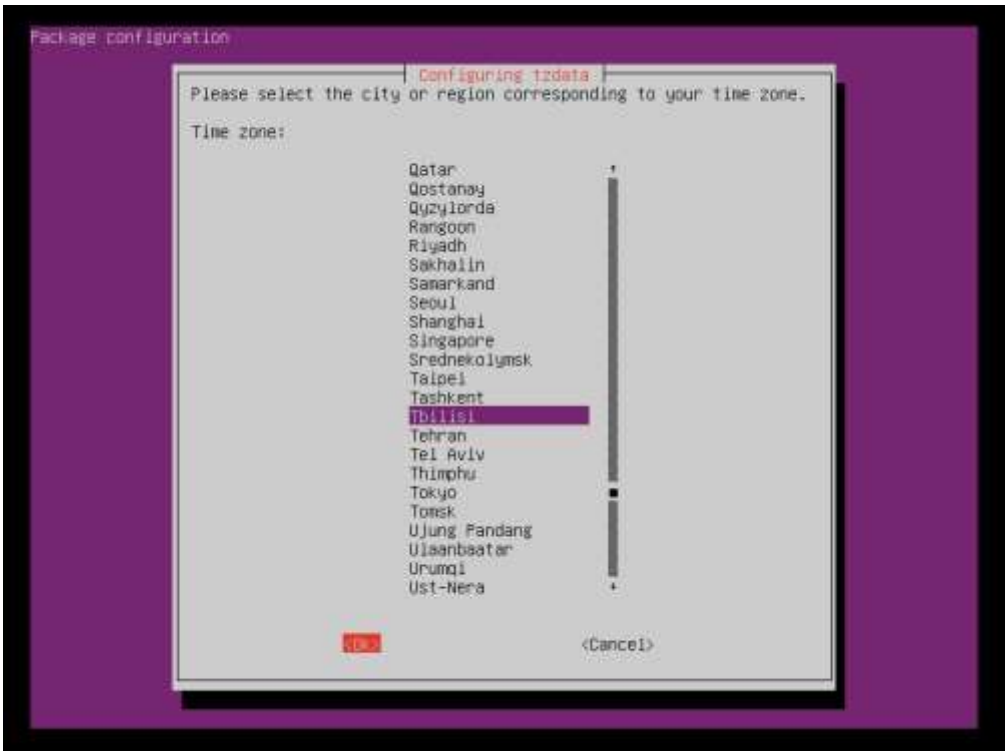
შეიქმნება ახალი ადმინისტრატორის ანგარიში და წაიშლება არსებული სტანდარტული „ncadmin“ ანგარიში.

საბოლოო ეტაპზე საჭიროა სერვერის გეოლოკაციის მითითება. ავირჩიოთ „Asia“.



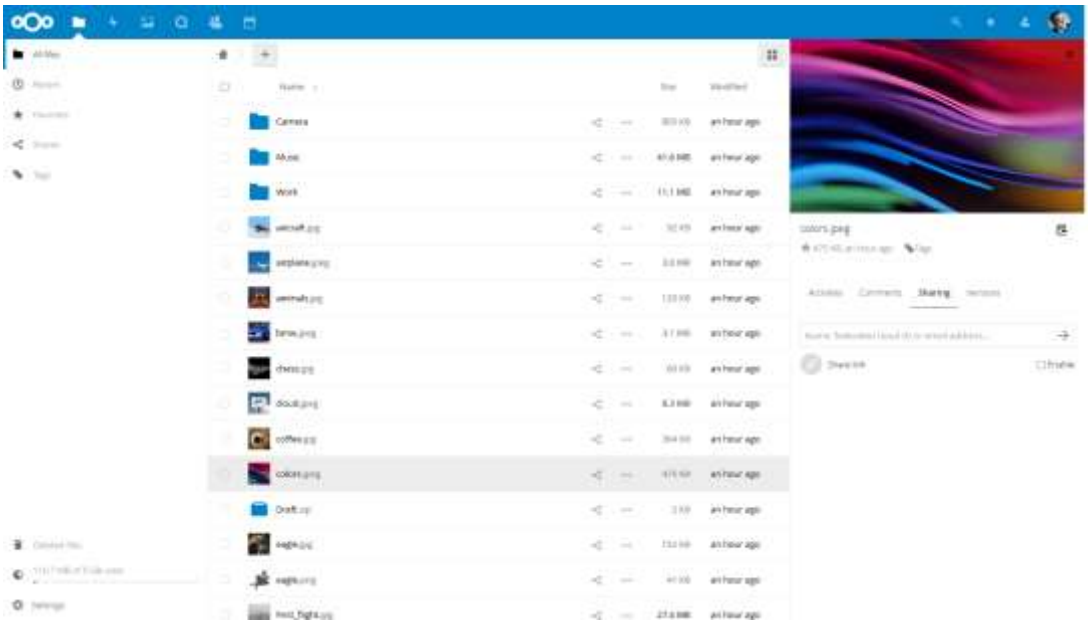
ნახ.25

შემდგომ კი ავირჩიოთ „Tbilisi“.



ნახ.26

ამით ინსტალაციის პროცედურა წარმატებით დასრულდება. სერვერის IP მისამართზე ვებ-ბრაუზერით შესვლისას გამოჩნდება Nextcloud სისტემის ვებ-გვერდი.



ნახ.27

შემდგომ შეგვიძლია დავარეგისტრიროთ მომხმარებლები და მივანიჭოთ მათ შესაბამისი უფლებები.

პრაქტიკული N8

სერვერულ ოპერაციულ სისტემებში ჯგუფური პოლიტიკები და მათი მართვა.

მიზანი: ჯგუფურ პოლიტიკებთან სამუშაო სპეციალურ კონსოლთან მუშაობის შესწავლა.

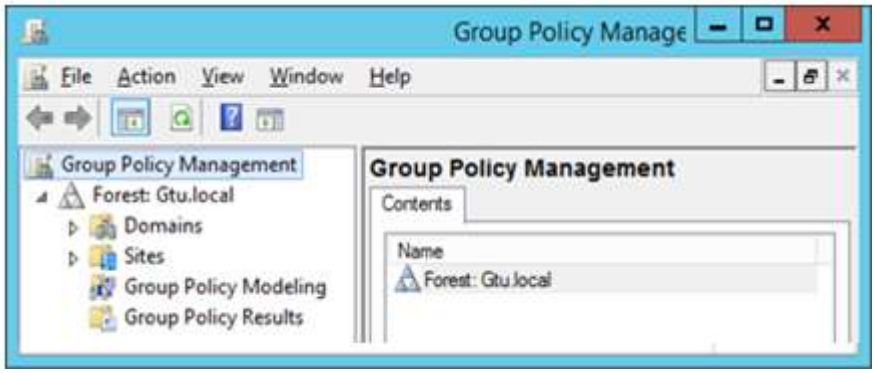
ჯგუფური პოლიტიკა (Group Policy) ეს არის Active Directory-ის ერთ-ერთი მთავარი შემადგენელი ნაწილი. მისი მართვის მთავარ ინსტრუმენტს წარმოადგენს ჯგუფური პოლიტიკების მართვის კონსოლი (GPMC). სისტემის ადმინისტრატორების მიერ ხდება ჯგუფური პოლიტიკის ობიექტების აგება (Group Policy Object - GPO). GPO – ეს არის როგორც სხვადასხვა აწყობების კონტეინერი (პოლიტიკების აწყობები), რომლებიც შეიძლება გამოყენებული იქნას მომხმარებლებისა და კომპიუტერების სააღრიცხვო ჩანაწერებზე Active Directory -ის საშუალებით. ჯგუფური პოლიტიკის ობიექტების აგება ხდება ჯგუფური პოლიტიკების მართვის რედაქტორის (Group Policy Management Editor - GPME) გამოყენებით, რომელიც გაეშვება GPO-ს ობიექტის რედაქტირების დროს GPMჩ კონსოლიდან. GPO-ს ერთ ობიექტზე შესაძლებელია მიეთითოს იმ პროგრამების ნაკრები, რომლებიც გათვალისწინებულია ყველა მომხმარებლების სამუშაო მაგიდაზე განთავსებისთვის. აგრეთვე, შესაძლებელია რეალიზება გაუკეთდეს მკაცრ პოლიტიკას დისკების კვოტებთან დაკავშირებით, შეიქმნას პაროლებისა და სააღრიცხვო ჩანაწერების ბლოკირების პოლიტიკა, რომელიც ფუნქციონირებს დომენის ქვეშ.

GPO-ს ობიექტი შედგება ორი ნაწილისაგან, კვანძების სახით:

- Computer Configuration (კომპიუტერის კონფიგურაცია). ისინი მართავენ იმ აწყობებს, რომლებიც სპეციფიკურია კომპიუტერებისათვის. როგორებიცაა მაგალითად, დისკების კვოტები, უსაფრთხოების აუდიტი და მოვლენების ჟურნალის შექმნა.

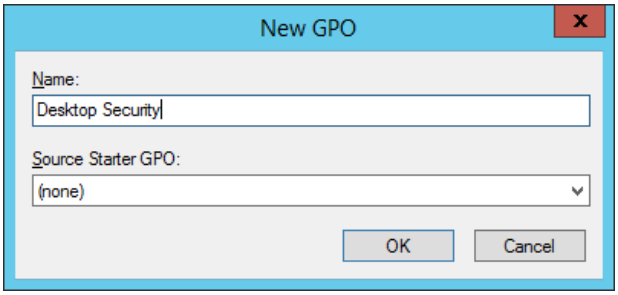
- User Configuration (მომხმარებლის კონფიგურაცია). ისინი მართავენ იმ აწყობებს, რომლებიც სპეციფიკურია მომხმარებ¬ლისთვის. როგორებიცაა მაგალითად, დანართების კონფიგურაცია, Start მენიუს მართვა და ფოლდერების გადამისამართება.

განვიხილოთ, თუ რა ეტაპები უნდა გავიაროთ, რომ შევქმნათ და რედაქტირება მოვახდინოთ დომენური GPO-ს ობიექტებზე. ყველა დომენური GPO-ს ობიექტების სამართა¬ვად გამოიყენება GPMC კონსოლი, რომლის გამოძახება ხდება Tools მენიუდან და გაიხსნება კონსოლის ფანჯარა, რომლის მარცხენა ნაწილში აისახება დომენის დასახელება (ნახ.1).



ნახ.1

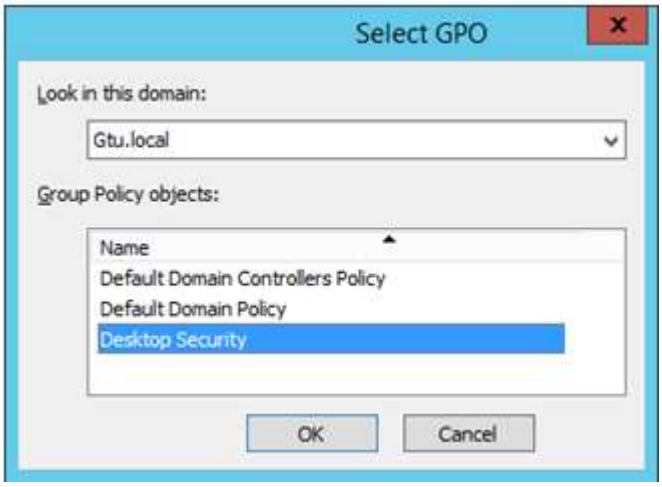
იმისათვის რომ შევქნას ახალი GPO-ს ობიექტი ხის ტრუქტურაში უნდა გავშალოთ Domains დასახელება და გამოვაჩინოთ ყველა კვანძები. შემდეგ უნდა დავდგეთ Group Policy Modeling კვანძზე და კონტექსტურ მენიუში ავირჩიოთ პუნქტი New. გამოდის New GPO დიალოგური ფანჯარა, სდაც დასახელებაში შევიტანოთ მაგალითად, Desktop Security და დავაჭიროთ ღილაკს OK (ნახ.2).



ნახ.2

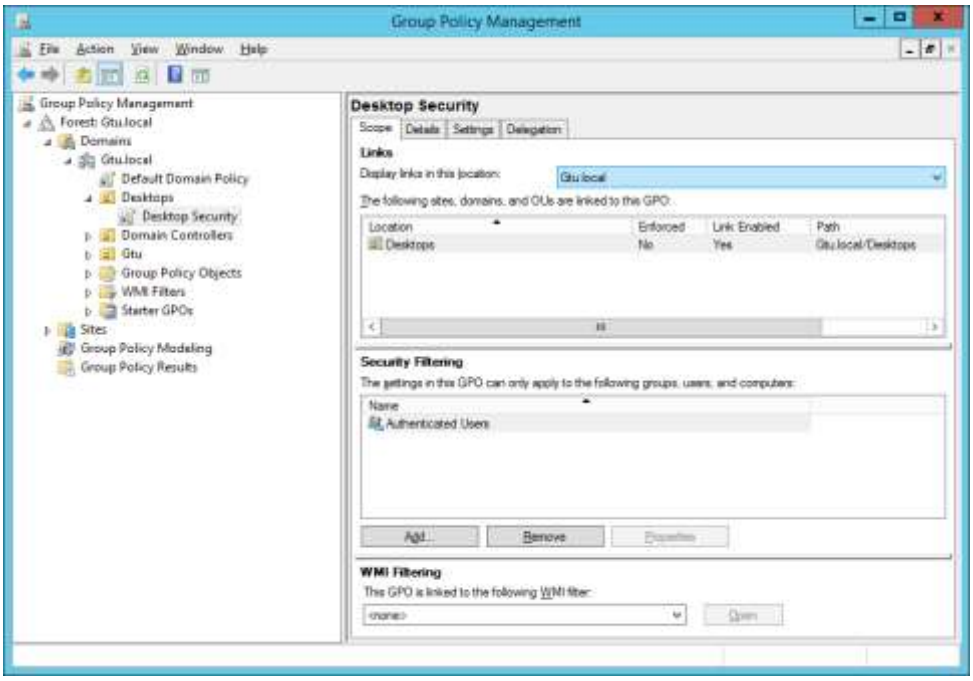
შედეგად იქმნება GPO-ს ცარიელი ობიექტი Desktop Security დასახელებით, რომელიც ჯერჯერობით არავისთან კავშირში არ არის. ამ მომენტისათვის უნდა მოხდეს ამ GPO ობიექტის კონფიგურაციის აწყობა და შემდეგ კავშირი დამყარდეს დომენთან ან ორგანიზაციულ ერთეულთან.

შემდგომ ეტაპზე გავხსნათ ახალი ორგანიზაციული ერთეული (კვანძი), მაგალითად Desktops დასახელებით და დავაკავშიროთ GPO ობიექტს. ამისათვის გამოვიძახოთ Desktops-ის კონტექსტური მენიუ და ავირჩიოთ Link an Existing GPO (დაუკავშირდეს არსებულ GPO ობიექტს). დიალოგურ ფანჯარაში Select GPO ავირჩიოთ GPO ობიექტი Desktop Security დასახელებით და დავაჭიროთ ღილაკს OK (ნახ.3).



ნახ.3

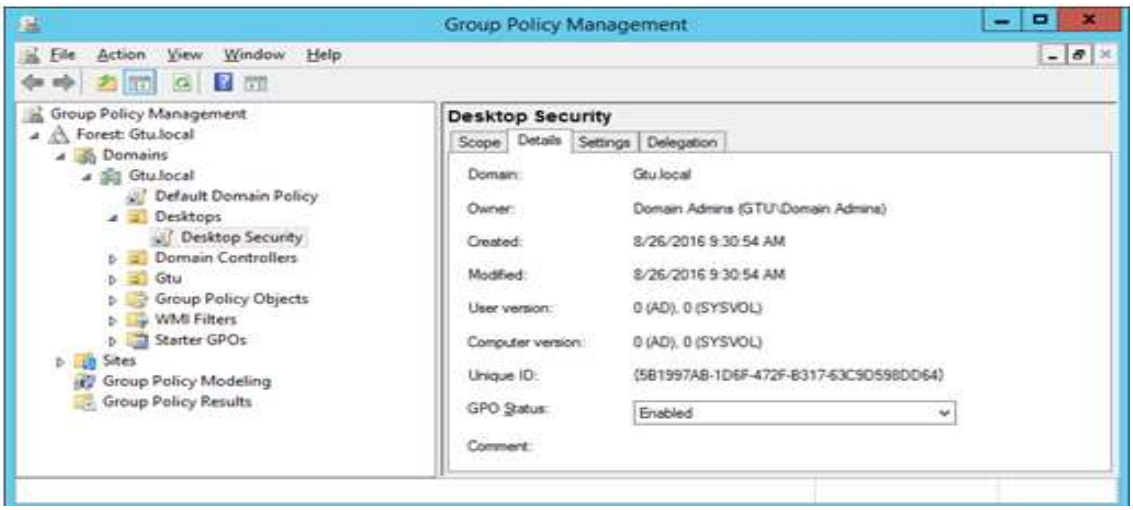
ამ პროცედურის ჩატარების შემდეგ ორგანიზაციულ ერთეულში Desktops-ში მოხდება GPO ობიექტის ასოცირება. მოვნიშნოთ GPO ობიექტი Desktop Security და თუ დავაკვირდებით, მარჯვენა პანელზე გამოჩნდება რამოდენიმე ჩანართი და თვისებები. ყველა GPO ობიექტს გააჩნია 4 სახის ჩანართი: Scope (მოქმედების არეალი), Details (დეტალები),Settings (აწყობები) და Delegation (დელეგირება) (ნახ.4).



ნახ.4

Scope ჩანართი გვეხმარება GPO ობიექტის ასპექტების ჩამოყალიბებაში. იგი შედგება ორი მთავარი განყოფილებისაგან: Links (ლინკი) და Security Filtering (უსაფრთხოების ფილტრაცია). Links განყოფილებაში მოთავსებულია ის საიტები, დომენები და ორგანიზაციული ერთეულები, რომლებზეც მიმდინარე მომენტში დაკავშირებულია GPO ობიექტი, ხოლო Security Filtering გამოსახულია ის ჩამონათვალი, თუ რომელ ჯგუფებს და მომხმარებლებს აქვთ უფლება გამოიყენონ GPO ობიექტის აწყობები. მესამე განყოფილება WMI Filtering (WMI ფილტრაცია), მიეთითება ფილტრი, რაზედაც GPO ობიექტს გააჩნია ლინკი, თუ ის გათვალისწინებულია.

Details ჩანართში გამოსახულია სხვადასხვა ცნობები GPO ობიექტის შესახებ, რომელიც ეხება მის შექმნას და მდგომარეობას (ნახ.5).

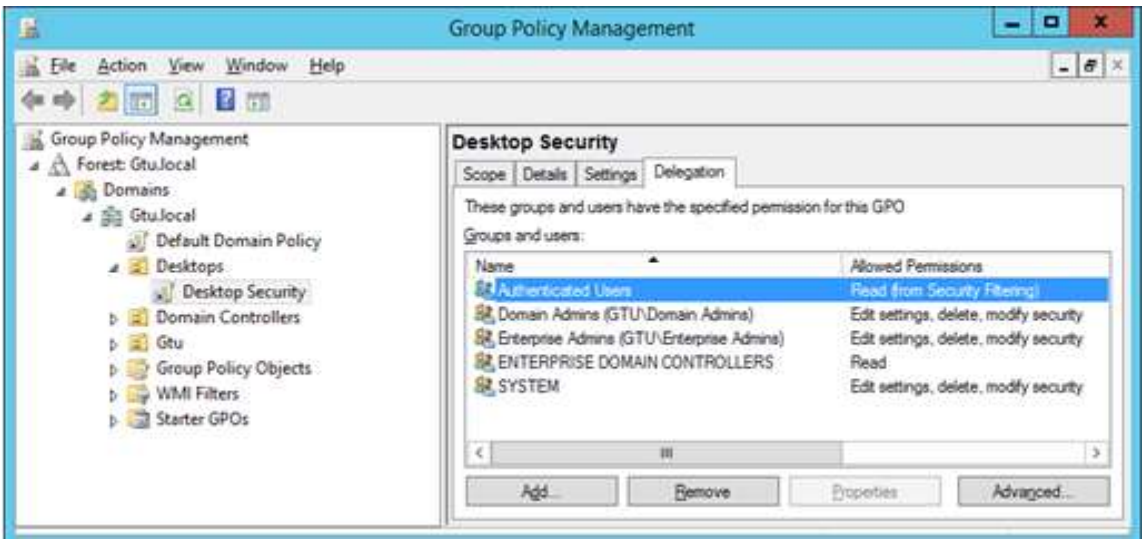


ნახ.5

Settings ჩანართი შეიცავს დინამიურ მონაცემებს აწყობების შესახებ, რომელიც დაკონფიგურირებულია GPO ობიექტზე (ნახ.6).

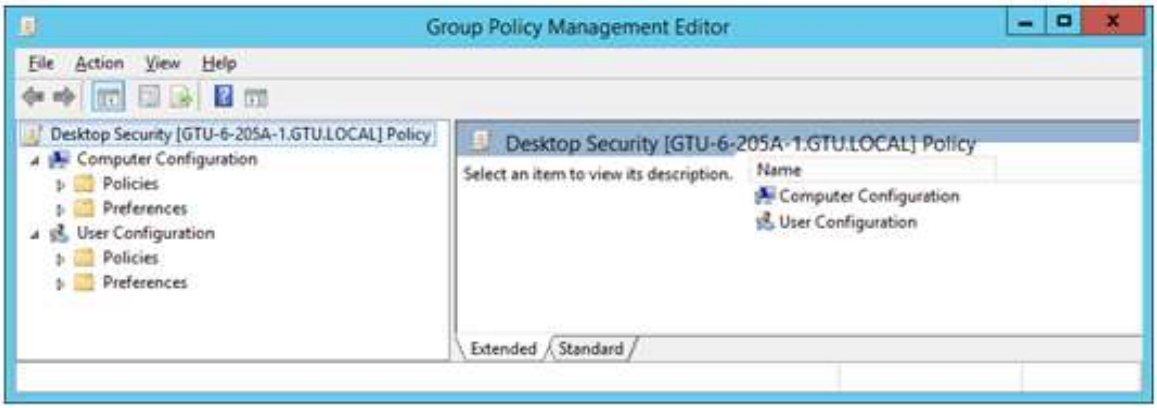
ნახ.6

ბოლოს Delegation ჩანართი გვიჩვენებს, თუ ვის შეუძლია შეასრულოს GPO ობიექტის ადმინისტრირება (ნახ.7).



ნახ.7

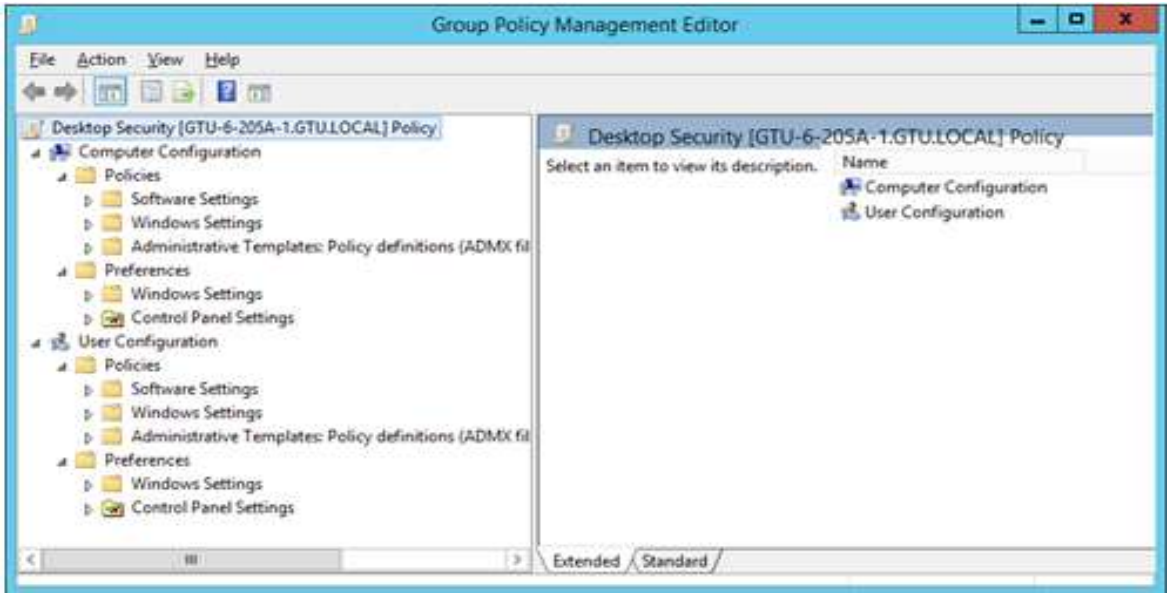
შემდეგ ეტაპზე განვიხილოთ, თუ როგორ ხდება GPO ობიექტის მოდიფიცირება. ამისათვის გადავიდეთ Group Policy Objects კვანძზე, გამოვიძახოთ მასში GPO ობიექტის კონტექსტური მენიუ და ავირჩიოთ Edit, რის შემდეგაც გახისნება ჯგუფური პოლიტიკების მართვის რედაქტორი GPME, რომლის მარცხენა ზედა ნაწილში ეწერება GPO ობიექტის დასახელება, ჩვენს შემთხვევაში – Desktop Security [GTU-6-205A-1.GTU.Local] Policy, რომელიც ხის სტრუქტურის სახით შეიცავს GPO ობიექტის აუცილებელ კვანძებს (ნახ.8).



ნახ.8

როგორც ადრე აღვნიშნეთ არსებობს GPO-ს ობიექტის აწყობების ორი ტიპი: Computer Configuration (კომპიუტერის კონფიგურაცია) და User Configuration (მომხმარებლის კონფიგურაცია). ისინი ხის სტრუქტურაში წარმოდგენილია ორი ძირითადი კვანძების სახით, რომლებიც თავის მხრივ შეიცავენ ქვეკვანძებს. კონფიგურაციის აწყობების შემდეგ უბრალოდ დაიხურება GPME რედაქტორი, რის შემდეგაც ცვლილებები ჩაიწერება GPO ობიექტში.

მართვის რედაქტორის ორივე ძირითადი კვანძი შეიცავს შემდეგ ქვეკავნძებს: Policies (პოლიტიკები) და Preferences (პარამეტრები).Policies ქვეკვანძი თავის მხრივ შეიცავს შემდეგ ქვეკვანძებს: Software Settings (პროგრამული უზრუნველყოფის აწყობები), Windows Settings (Windows აწყობები) და Administrative Templates (ადმინისტრაციული შაბლონები). Preferences ქვეკვანძი დაყოფილია შემდეგ ქვეკვანძებად: Control Panel (მართვის პანელი) და Windows Settings (Windows აწყობები) (ნახ.9).



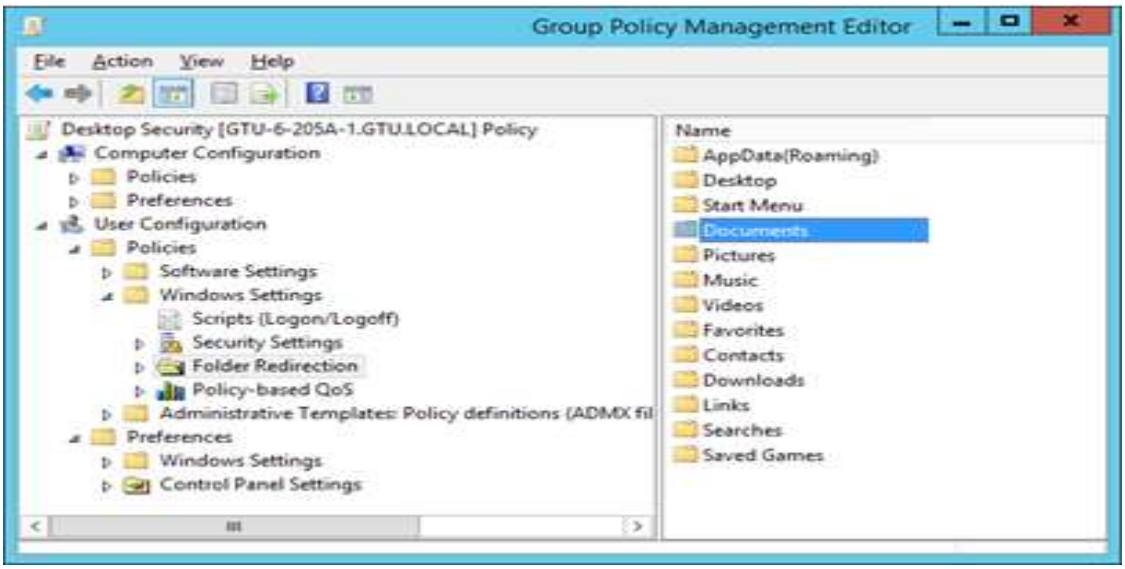
ნახ.9

ძირითად კვანძებს შორის განსხვავება არის ის, რომ აწყობები User Configuration-ისთვის ვრცელდება მომხმარებლების სააღრიცხვო ჩანაწერებისთვის, ხოლო Computer Configuration-ისთვის ვრცელდება კომპიუტერების სააღრიცხვო ჩანაწერებისთვის.

არსებობს ძალიან ბევრი სახის GPO ობიექტის აწყობები. განვიხილოთ ზოგიერთი მათგანი, რომლებიც ყველაზე ხშირად გამოიყენება.

- **ფოლდერების გადამისამართება.** ეს არის User Configuration-ის ერთ-ერთი სასარგებლო სამუშაო ჯგუფურ პოლიტიკაში, რომელიც ეხება ისეთი ხშირად გამოყენებადი ფოლდერების მოწესრიგებას, როგორებიცაა: AppData, Desktop, Start Menu, Documents და Favorites ... კერძოდ, ნებისმიერ მომხმარებლისთვის, არა აქვს მნიშვნელობა რომელ კომპიუტერთან იჯდება იგი, ყოველთვის ხელმისაწვდომი იქნება ეს ფოლდერები თავისი ინფორმაციით. ეს ფოლდერები ნებისმიერი მომხმარებლისთვის წარმოადგენს მნიშვნელოვან ელემენტს, რომელშიც ინახება მომხმარებლისთვის აუცილებელი მიმდინარე ინფორმაცია და სასურველია რომ მას ნებისმიერი კომპიუტერიდან ჰქონდეს წვდომა ამ ფოლდერებთან. აქედან გამომდინარე კარგი იქნება, რომ ეს ფილდერები განთავსდეს ქსელში რომელიმე სერვერზე, სადაც უფრო დაცული იქნება მასში არსებული ინფორმაცია და მომხმარებლისთვის სისტემაში შესვლის დროს მოხდება გადამისამართება აღნიშნული სერვერის შესაბამის ფილდერებზე და ყველა მომხმარებლისთვის ავტომატურად იქნება გახსნილი თავისი ქვეფოლდერები. აღნიშნული პროცედურების ჩატარება Documents ფოლდერის მაგალითზე, GPME რედაქტორში ხდება შემდეგნაირად:

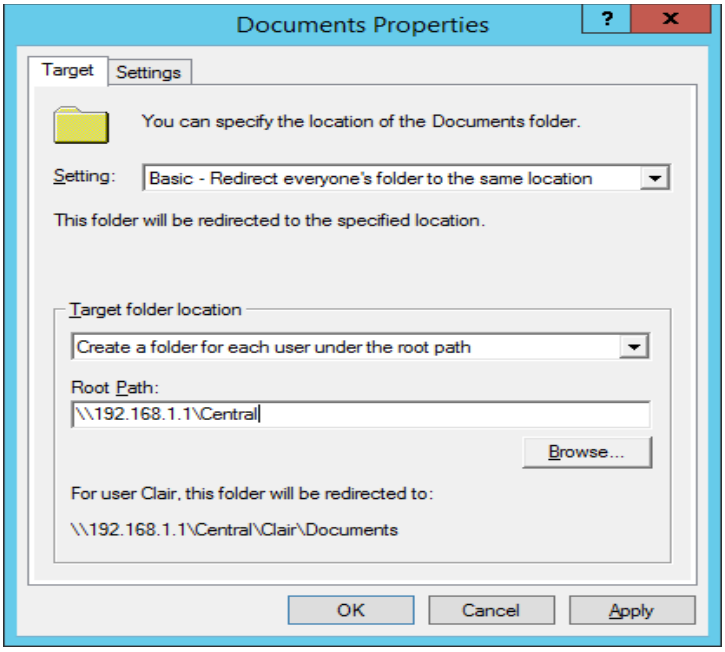
ხის სტრუქტურაში ვდგებით კვანზძე User Configuration\Policies\Windows Settings\Folder Redirection და ფანჯრის მარჯვენა მხარეს ვირჩევთ Documents (ნახ.10).



ნახ.10

შევდივართ მის კონტექსტურ მენიუში და ავირჩიოთ პუნქტი Properties. გაიხსნება დიალოგური ფანჯარა, Setting პუნქტში ავირჩიოთ Basic, რათა განვსაზღვროთ Documents ფოლდერის უნიკალური ადგილმდებარეობა, რომელიც ერთობლივად იქნება გამოყენებული მომხმარებლების მიერ. Target Folder Location პუნქტში ავირჩიოთ Create a folder for each user under the root path (ყველა მომხმარებლისთვის შეიქმნას ფილდერი მითითებულ მისამართზე) და Root Path ველში იწერება Documents ფოლდერის

ადგილმდებარეობის მისამართი სერვერზე. ასეთი აწყობების შემთხვევაში, სისტემა მითითებულ მისამართში ავტომატურად შექმნის ქვეფოლდერს მომხმარებლის სახელით. Settings ჩანართზე არსებული აწყობები დავტოვოთ უცვლელად (ნახ.11).

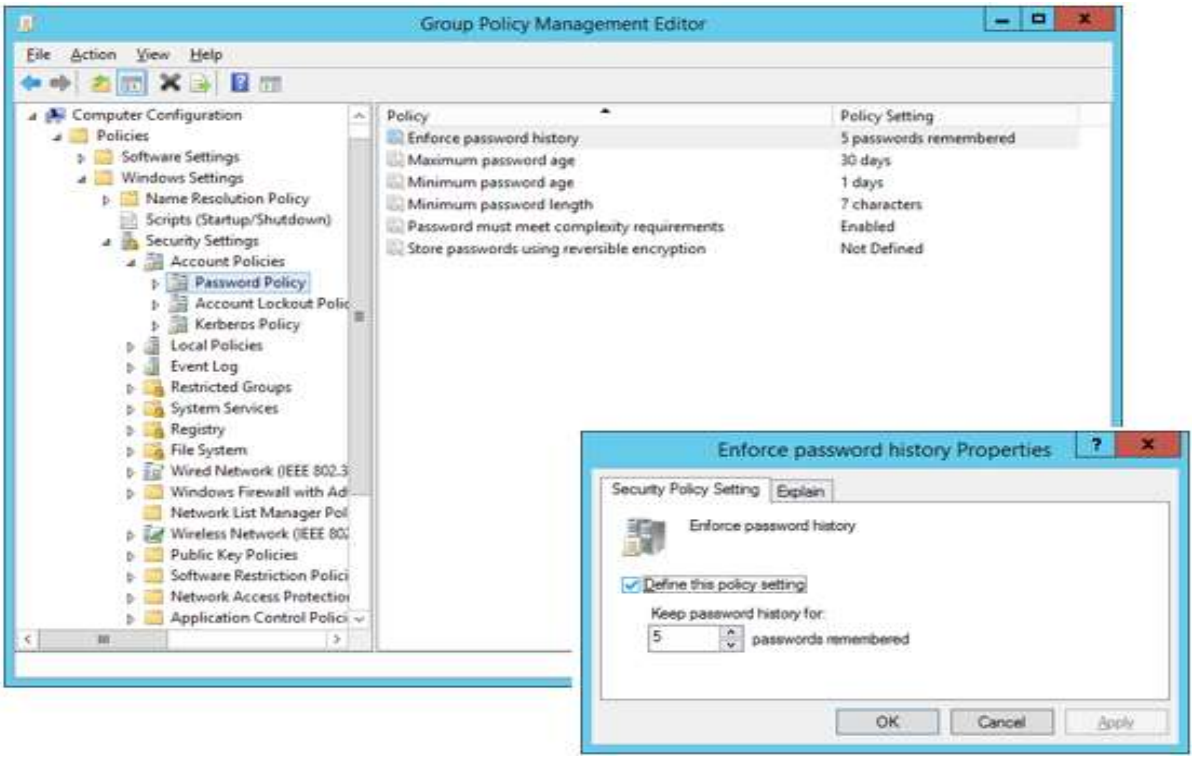


ნახ.11

- **უსაფრთხოების აწყობები.** სხვადასხვა ორგანიზაციებსა თუ კომპანიებში უსაფრთხოების მიზნით ხშირ შემთხვევებში მიღებულია ისეთი პოლიტიკა, რომ მომხმარებლებს პაროლი ჰქონდეთ გართულებული სახით და რაღაც პერიოდის განმავლობაში ახდენდნენ მის შეცვლას. მაგალითად, გვსურს რომ დომეინის მომხმარებელს ჰქონდეს მინიმუმ 7 სიმბოლოიანი პაროლი, აქედან ერთი მაინც უნდა იყოს მთავრული ასოიანი და შეიცავდეს რიცხვებს. პაროლი უნდა მოქმედებდეს 1 თვის განმავლობაში და შემდეგ უნდა ხდებოდეს მისი ცვლილება. სისტემის მიერ უნდა ხდებოდეს 5 პაროლის დამახსოვრება, რათა მომხმარებელმა არ გაიმეოროს ერთი და იგივე პაროლი დაყენება. ყველაფერი ეს შესაძლებელია განხორციელდეს ჯგუფური პოლიტიკის დახმარებით, რომელიც GPME რედაქტორში ხდება შემდეგნაირად:

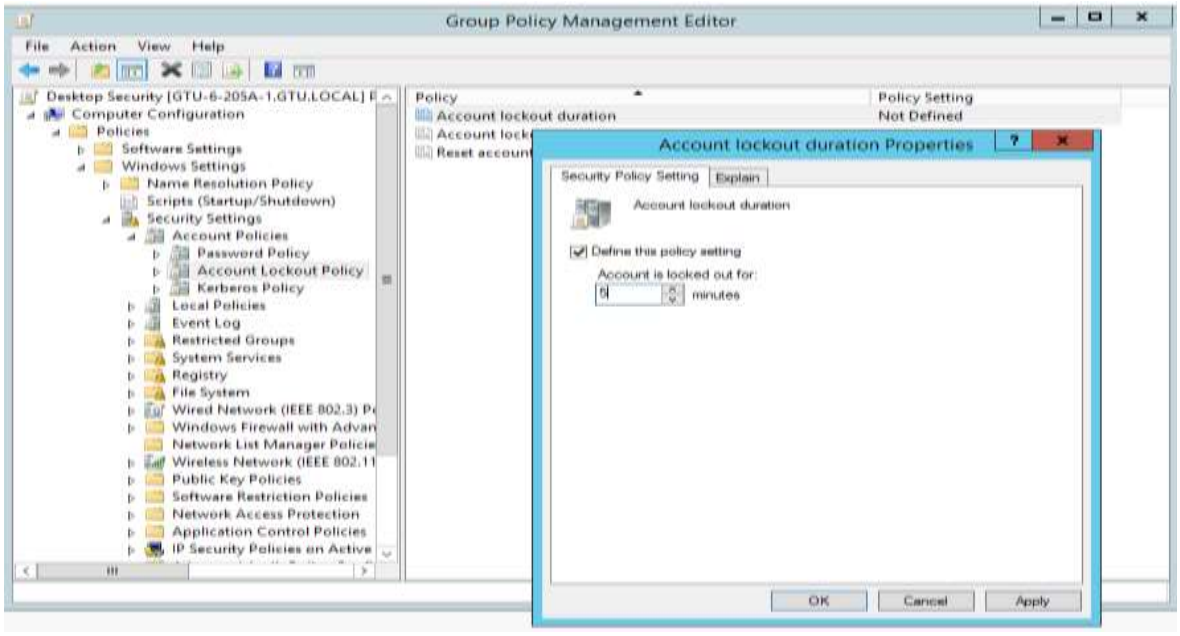
ხის სტრუქტურაში ვდგებით კვანზძე Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy და ფანჯრის მარჯვენა მხარეს Policy ჩამონათვალებში Policy Setting სვეტებში Properties საშუალებით ვაყენებთ შემდეგ მონაცემებს: Enforce password history Documents ვაფიქსირებთ 5 passwords remembered, Maximum password age – 30 days, Minimum password age – 1 days, Minimum password length – 7 characters da password must meet complexity requrements – Enabled (ნახ.12).

- **სააღრიცხვო ჩანაწერის ბლოკირება.** გამოვიყენოთ ისეთი პოლიტიკა, რომელიც ახდენს სააღრიცხვო ჩანაწერების ბლოკირებას 5 წუთით იმ შემთხვევაში, თუ მიმდევრობით სამჯერ იქნა დაშვებული შეცდომა სისტემაში შესასვლელად.



ნახ.12

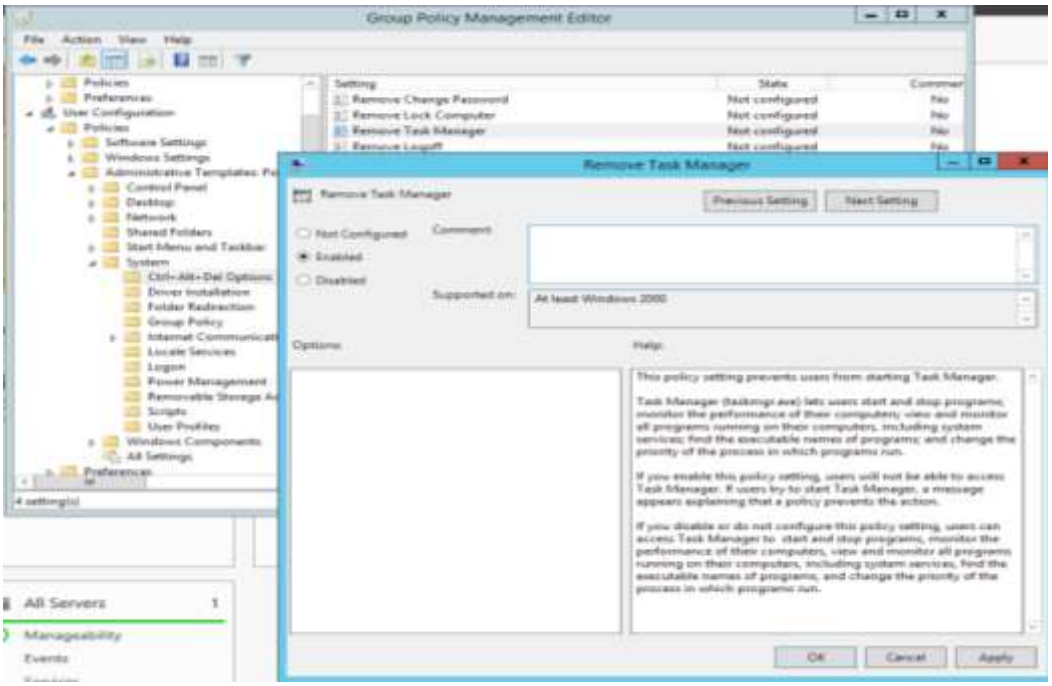
ამისათვის ვირჩევთ Computer Configuration\Policies\ Windows Settings\Security Settings\Account Policies\ Account Lockout Policy და მარჯვენა მხარეს ვირჩევთ Account lockout duration (ნახ.13).



ნახ.13

- **Task Manager -ის ბლოკირება**. ვთქვათ გვინდა რომ მომხმარებლებს ჩაეკეტოს Task Manager-ის გამოყენება.

ამისათვის ვირჩევთ User Configuration\Policies\ Administrative Templates\System \Ctrl+Alt+Del Options და მარჯვენა მხარეს ვირჩევთ Remove Task Manager (ნახ.14).



ნახ.14

რომელი კომპიუტერიდანაც არ უნდა შევიდეს აღნიშნული მომხმარებელი, მისთვის ყოველთვის ჩეკეტილი იქნება Task Manager-ის გამოყენება.

ყველა GPO ობიექტის აწყობები შეგიძლიათ იხილოთ https://www.microsoft.com/en-us/download/details.aspx?id=25250 Web-მისამართზე.

რეკომენდებული ლიტერატურა:

1. შონია ო., თოფურია ნ. „მონაცემთა დაცვის ლოკალური და ღრუბლოვანი სერვისები“, თბილისი, 2017. 004.056(02)/21.

2. შონია ო., ქართველიშვილი ი., ნარეშელაშვილი გ. უსადენო ქსელების უსაფრთხოება. თბილისი, სტუ 2018. 115 გვ. ბიბლ. ინდექსი: CD-3975.

3. შონია ო., ქართველიშვილი ი. ქსელებისა და მონაცემთა ბაზების მართვის სისტემების უსაფრთხოების სკანირება. თბილისი, სტუ 2018. CD-3974.

4. სვანაძე ვ. კიბერსივრცე და კიბერუსაფრთხოების გამოწვევები. თბილისი, 2015. CD-5679. https://gipa.ge/uploads/files/Cyber_Protection.pdf

5. Tim Güneysu, Helena Handschuh. Cryptographic Hardware and Embedded Systems, ISBN: 978-3-662-48324-4, U.S.A. 2015. CD-4118.

6. Martti Lehto, Pekka Neittaanmäki. Cyber Security: Analytics, Technology and Automation, ISBN: 978-3-319-18302-2, U.S.A. 2015. CD-4120.

გადაეცა წარმოებას 12..11.2020. ხელმოწერილია დასაბეჭდად 20.11.2020. ოფსეტური ქაღალდის ზომა 60X84 1/16. პირობითი ნაბეჭდი თაბახი 3. ტირაჟი 100 ეგზ.

სტუ-ს „IT კონსალტინგის ცენტრი“ (თბილისი, მ.კოსტავას 77)

ISBN 978-9941-8-2867-6