

**ENTERPRISE ENDPOINT SECURITY SOLUTION FOR LARGE  
ORGANIZATION WITH HIGH AVAILABILITY (ACTIVE-PASSIVE)**

**BY**

**Allin Arzoo  
ID: 193-25-819**

This Report Presented in Partial Fulfillment of the Requirements for the  
Degree of Masters of Science in Computer Science and Engineering

Supervised By

**Md. Abbas Ali Khan**  
Senior Lecturer  
Department of CSE  
Daffodil International University

Co-Supervised By

**Md. Tarek Habib**  
Assistant Professor  
Department of CSE  
Daffodil International University



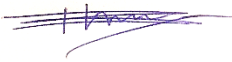
**DAFFODIL INTERNATIONAL UNIVERSITY  
DHAKA, BANGLADESH  
MAY 2021**

## **APPROVAL**

This Project titled “**Enterprise Endpoint security solution for large Organization with High availability (Active-passive)**”, submitted by **Allin Arzoo** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of M.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on “03-06-2021”

### **BOARD OF EXAMINERS**

**Chairman**

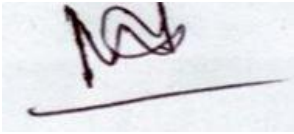


---

**Dr. Touhid Bhuiyan**  
**Professor and Head**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University

**Internal Examiner**



---

**Dr. Md. Ismail Jabiullah**  
**Professor**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University



**Internal Examiner**

---

**Dr. Sheak Rashed Haider Noori**  
**Associate Professor and Associate Head**

Department of Computer Science and Engineering  
Faculty of Science & Information Technology  
Daffodil International University



**Dr. Shamim H Ripon**

**Professor**

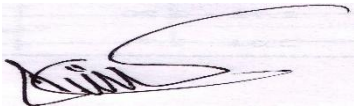
Department of Computer Science and Engineering  
East West University

**External Examiner**

## DECLARATION

I hereby declare that, this project has been done by us under the supervision of **Mr. Md. Abbas Ali Khan, Senior Lecturer, Department of CSE** Daffodil International University. I also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

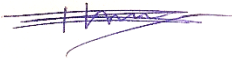
**Supervised by:**



---

**Mr. Md. Abbas Ali Khan**  
Senior Lecturer  
Department of CSE  
Daffodil International University

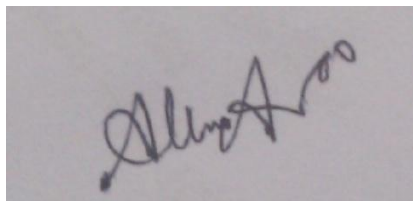
**Co-Supervised by:**



---

**Md. Tarek Habib**  
Assistant Professor  
Department of CSE  
Daffodil International University

**Submitted by:**



---

**Allin Arzoo**  
ID: -193-25-819  
Department of CSE  
Daffodil International University

## ACKNOWLEDGEMENT

First I express my heartiest thanks and gratefulness to almighty Allah for His divine blessing makes us possible to complete the final year project/internship successfully.

I am really grateful and wish our profound our indebtedness to **Md Abbas Ali Khan, Senior Lecturer**, Department of CSE Daffodil International University, Dhaka. Deep Knowledge & keen interest of our supervisor in the field of “Cyber Security and network” to carry out this project. His endless patience ,scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior draft and correcting them at all stage have made it possible to complete this project.

I would like to express our heartiest gratitude to **Dr. Touhid Bhuiyan, Professor** and Head, Department of CSE, for his kind help to finish this project and also to other faculty member and the staff of CSE department of Daffodil International University.

I would like to thank our entire course mate in Daffodil International University, who took part in this discuss while completing the course work.

Finally, I must acknowledge with due respect the constant support and patients of our parents.

## **ABSTRACT**

Endpoint security is very important and unavoidable security tool for any Organization. Now a day we cannot think an enterprise network without it. In this project we are providing Enterprise Endpoint security solution for large Organization and also provide active passive solution for High availability. In first part of this paper we will discuss about Endpoint security solution for large Organization who has separated internet and intranet connection and second part active passive solution for high availability will. Sometimes managing the endpoint security can be complicated because of the network architecture of certain organization and requirements changes after the network architecture. In this report we will discuss about endpoint security solution for an organization using separated internet and intranet connection network be using Kaspersky Endpoint security. Beside this active passive Datacenter is a very common concept now a day's which contains a main Datacenter and another Passive Data Center & if any problem occurs to the main data center the services will run from passive data center. Antivirus Companies doesn't provide active passive solution for this active passive environment. In this project we are providing an Enterprise Endpoint security solution for active passive Datacenter environment with Kaspersky Endpoint Security.

## TABLE OF CONTENTS

<b>CONTENTS</b>	<b>PAGE</b>
Board of Examiners	ii
Declaration	iii
Acknowledgements	iv
Abstract	v
<b>CHAPTER</b>	
<b>CHAPTER 1: INTRODUCTION</b>	<b>1-2</b>
1.1 Introduction	1
1.2 Objective	1
1.3. Motivation	1
1.4 Report Layout	2
<b>CHAPTER 2:BACKGROUND</b>	<b>3-3</b>
2.1 Introduction	3
2.2 Why Choose Kaspersky	3
2.3 Related Work	3
2.4 Challenges	3
<b>CHAPTER 3: ENDPONT SECURITY REGULER STRUCTURE AND OUR PROPOSED STRUCTURE</b>	<b>4-6</b>
3.1 Introduction	4
3.2 Endpoint Security	4
3.3 Kaspersky Endpoint Security	4
3.4 Kaspersky Security Center	4
3.5Kaspersky Endpoint Software in Client End	5
3.6 Kaspersky Endpoint Security Structure	5
3.7Proposed Design for The Mentioned Network Structure	5

<b>CHAPTER 4: INSTALLATION AND OPERATION OF KES</b>	<b>7-23</b>
4.1 Introduction	7
4.2Installing Kaspersky Security Center	7
4.3Install Kaspersky Endpoint Security in Client End	11
4.4Operation with Kaspersky Security Center	15
4.5Add Slave Server	22
4.6Proposed Solution for The Discussed Environment	23
<b>CHAPTER 5: KASPERSKY SECURITY CENTER BACKUP</b>	<b>24-29</b>
5.1 Introduction	24
5.2Kaspersky Security Center Backup Tool	24
5.3Active-Passive Datacenter Concept	26
5.3 Endpoint Security in Active Passive Datacenter Concept	27
5.4 Solution For The Backup	27
5.6 Pre-requisites of Backup and Restore of Active Passive Data Center	28
5.7 Network Configuration	28
5.8 Working Procedure of Backup	28
<b>CHAPTER 6: CONCLUSION AND FUTURE STUDY</b>	<b>30-31</b>
6.1 Summary of Study	30
6.2 Conclusion	30
6.3 Recommendation	30
6.4 Further study	31
<b>REFERENCES</b>	<b>32</b>



## **LIST OF FIGURES**

<b>FIGURES</b>	<b>PAGE</b>
Diagram 3.1: Basic Structure of Endpoint Security System	5
Diagram 3.2: Proposed Structure of Endpoint Security System	6
Diagram 2.1: Active Passive Data Center Theory	26
Figure 4.1: SQL Server Installation	8
Figure 4.2: SQL Server Installation, Stand Alone	9
Figure 4.3: Kaspersky Security Center Installation	9
Figure 4.4: Kaspersky Security Center Installation Dashboard	10
Figure 4.5: Kaspersky Security Center Management Console.	11
Figure 4.6: Kaspersky Network agent IP	12
Figure 4.7: KES Installation	13
Figure 4.8: KES Custom Installation	14
Figure 4.9: Kaspersky Security Endpoint Security Dashboard in Client End	15
Figure 4.10: Kaspersky Security Center Management	16
Figure 4.11 Group Add in KSC	17
Figure 4.12: Manage Policy in Kaspersky Security Center	18
Figure 4.13: Host in Kaspersky Security Center	19
Figure 4.14: Manage Device in Kaspersky Security Center	20
Figure 4.15: Host Status	21
Figure 1.11: Running Task a Selective User in Kaspersky Security Center	22
Figure 1.12: Add Slave Server in Kaspersky Security Center	23
Figure 5.1: Backup and Restore Tool of Kaspersky Security Center	24
Figure 5.2: Backup and Restore Tool of Kaspersky Security Center	25
Figure 5.3: Backup and Restore Tool of KSC	26
Figure 5.4: Backup KSC in another Server With Backup and Restore Tool of KSC	29

## **LIST OF ABBREVIATION**

DIU – Daffodil International University

CSE – Computer Science and Engineering

EN – Endpoint Security

KES – Kaspersky Endpoint Security

KSC – Kaspersky Security Center

NAT – Network Address Translator

# **CHAPTER 1**

## **INTRODUCTION**

### **1.1 Introduction**

Endpoint Security solution is sometimes complicated as the way the network is designed. In many organization internal network and external network is differentiate, normal users don't have internet connection there and that is the main challenge of endpoint security because endpoint security needs internet connection for virus database update. Beside this many endpoint security available in market like CISCO Amp, ESET need internet connection for active the software license. Here we are going to introduce Endpoint Security solution for an organization where there is no internet after DMZ zone or no internet in Distribution network. We will also discuss the active passive data center concept and backup and restore of Kaspersky Security Center in active passive data center environment.

### **1.2 Objective**

- Learn about Endpoint Security Solution
- Learn about Kaspersky Endpoint Security
- Installation and work with Kaspersky Endpoint Security
- Endpoint Security Solution for company has no internet in Distribution Zone
- Use Kaspersky Backup and restore tool
- Active passive Data Center Concept
- Backup and restore in Active Passive Data Center Environment

### **1.3 Motivation**

I work in a company with large user network with intranet, there is no internet after DMZ zone or from distribution there is no internet. I had to designed and implement endpoint security solution this kind of network. Our company also has active passive Data center and I had also make a solution for active passive data center backup and restore but not only Kaspersky but also the other vendors don't have any support for this so I had to make the concept of backup of KSC server in active passive data center environment.

## **1.4 Report Layout**

Report layout describes a summary of all chapters. A brief summary of all chapters are given below:

Chapter 1: Discusses about my thesis introduction, objective and motivation.

Chapter 2: In chapter two I will discuss the background, related work and challenges

Chapter 3: In the chapter three I will introduce the Endpoint Security, Kaspersky endpoint security, regular structure of KES and the proposed plan for an organization has no internet in distribution.

Chapter 4: In the chapter four I will introduce how to establish KES, how it download the update and then the main part of this chapter, how to set up an endpoint security for an environment where there is no internet in distribution zone.

Chapter 5: In Chapter five I will discuss about the Backup and restore of KES, Active–Passive Data Center Environment and Backup and restore of KES for Active-Passive Data Center Environment.

Chapter 6: In Chapter Six there will be consist of Summary of this project, Conclusion and Future Study.

## **CHAPTER 2**

### **BACKGROUND**

#### **2.1 Introduction**

There are different types of Endpoint Security Software available. Their working procedure is about same. Endpoint Security Software's management console running on a server and we can manage the whole system from the management console. Endpoint Security Software's another important work is to download the signature updates from the vendor's site via internet and management console distributes the updates to the hosts. As we mentioned earlier we are working on an environment where there is no internet on distribution so the Endpoint Security Software won't be run in its normal way.

#### **2.2 Why choose Kaspersky**

In many of the Endpoint Security Software, host need to connect in internet for making the license active like ESET, CISCO Amp, MacAfee but Kaspersky provide the License file to the customer and with this file Endpoint Security Endpoint Security Software can be activated without internet. So environment like us Kaspersky is very suitable. Beside this Kaspersky is very easy to manage and it is very scalable.

#### **2.3 Related work**

Endpoint Security Software companies do research on their products for make them better and stay alive in this challenging market. Beside this very little work has done in this field without the Endpoint Security Vendor companies.

#### **2.4 Challenges**

Network stability is one of the big challenges for this project. It is very important in time of remote installation, download updates and virus scan. It is also very much important in active passive backup because in this process we are copying the backup from one server to another server through network share so unstable network, spike or packet loss could be the reason of failure of total work

## **CHAPTER 3**

### **ENDPONT SECURITY REGULER STRUCTURE AND OUR PROPOSED STRUCTURE**

#### **3.1 Introduction**

In this chapter I will going to discuss about the Endpoint Security, Kaspersky Endpoint Security, Kaspersky Security Center and Kaspersky Endpoint software in client end, Kaspersky Endpoint Security Structure and then our proposed structure for an environment where there is no internet in DMZ Zone or no internet after DMZ zone.

#### **3.2Endpoint Security**

Endpoint security or endpoint protection is a process where the devices of computer networks are remotely connected to client devices. Endpoint security is a software that helps to identify and manage the computer and data access over a corporate network and provide protection against virus, male-ware and threats.

#### **3.3 Kaspersky Endpoint Security**

Kaspersky Endpoint Security for Business Core is an on premise and cloud-based security solution for small and medium-sized businesses that includes anti-malware, a firewall and a central administration control. It's very efficient and fit for different type of Network Structure.

#### **3.4 Kaspersky Security Center**

Kaspersky Security Center is a single administration console for managing and controlling all Kaspersky solution and administration tools. It makes every endpoint and device on your network more visible, simplifies IT administration tasks. It also downloads all virus update. We need to install the Security Center in a windows server.

#### **3.5 Kaspersky Endpoint software in client end**

In client end we need to install two software, one is Kaspersky network agent and another is Kaspersky endpoint security. Kaspersky endpoint security is the antivirus software and the network agent is the connector which connects the client to Kaspersky security Center.

### 3.6 Kaspersky Endpoint Security Structure

Kaspersky Endpoint security is client-server based system, Kaspersky Security Center is installed in the server & all antivirus administration is done with this. Signature updates can be download and install in computers via server or directly from internet.

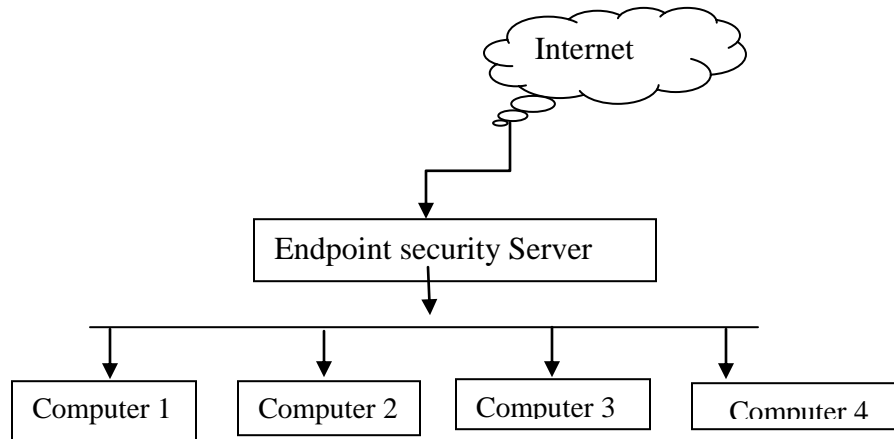


Diagram 3.1: Basic structure of Endpoint security system

### 3.7 Proposed design for the mentioned Network Structure

But in our environment, internet is not available in distribution zone or more specific there will be no internet after DMZ. So here my solution is to install a server in DMZ zone which can connect internet but only the Endpoint security vendor's site with specific port, which will download all updates from internet. After this there will be another server in distribution zone with will be connected to the DMZ zone server. The distribution server has basically two role one is to manage all computers, and another is download updates from DMZ server and distribute it to computers. We can manage the KES from the distribution zone server.

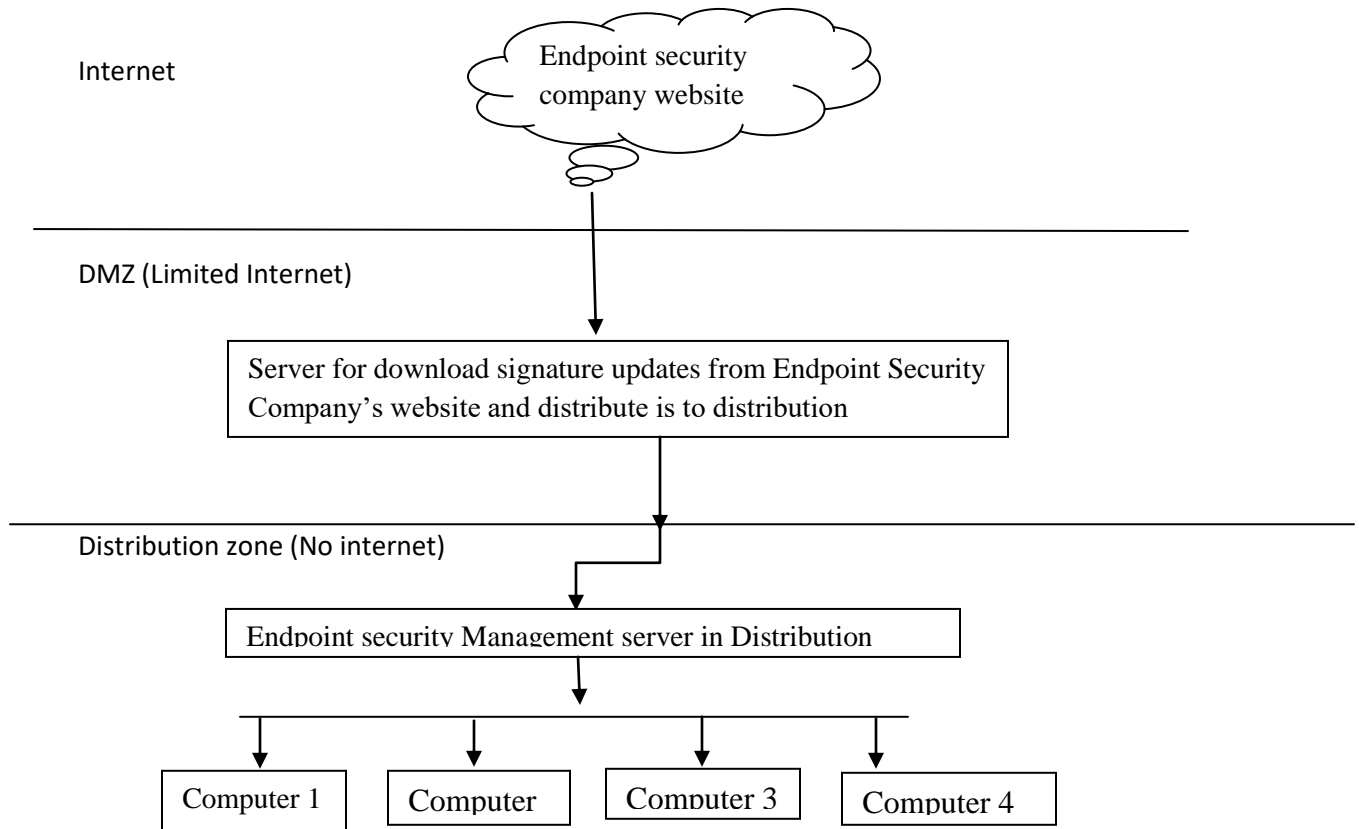


Diagram 3.2: Proposed structure of Endpoint security system



## **CHAPTER 4**

### **INSTALLATION AND OPERATION OF KES**

#### **4.1 Introduction**

In this Chapter we will show the installation procedure of Kaspersky Endpoint Security and set up Kaspersky Endpoint Security for an environment where there is no internet in distribution zone.

#### **4.2 Installing Kaspersky Security Center**

We need to install Kaspersky Security Center on windows server. For Kaspersky Security Center 12 minimum Hardware requirement is 4GB RAM and 10GB free storage. OS versions have to be Windows server 2012, Windows server 2016, Windows server 2019 and Windows 10, Windows 8 & Windows 7 service pack 1. Kaspersky Security Center also need Database Server installed on OS. Database server versions have to be MS SQL Server 2012 and above, it also supports Maria DB and RDS. For installing Kaspersky Security Center at first we will install MS SQL Server We will go for SQL standalone installation

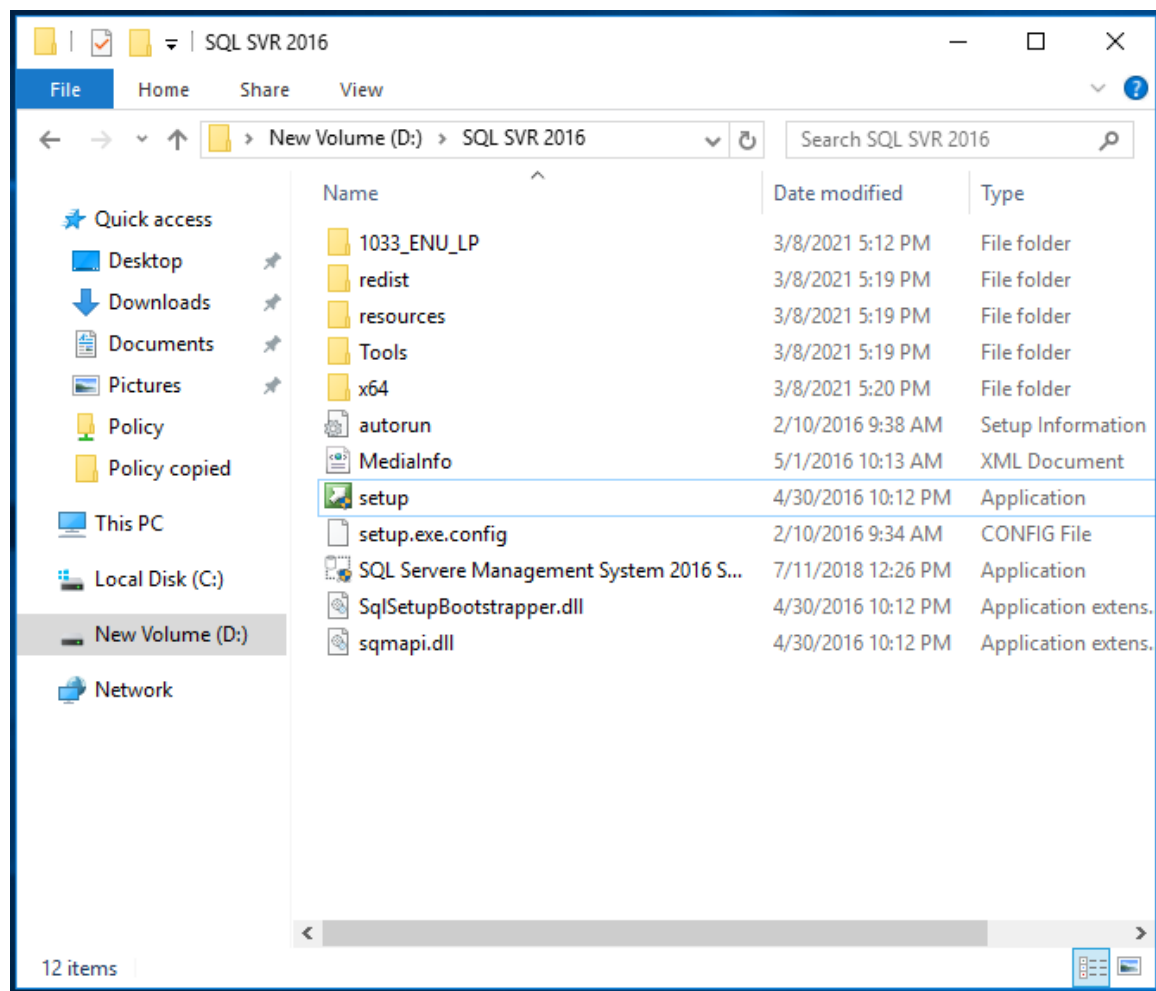


Figure 4.1: SQL Server installation

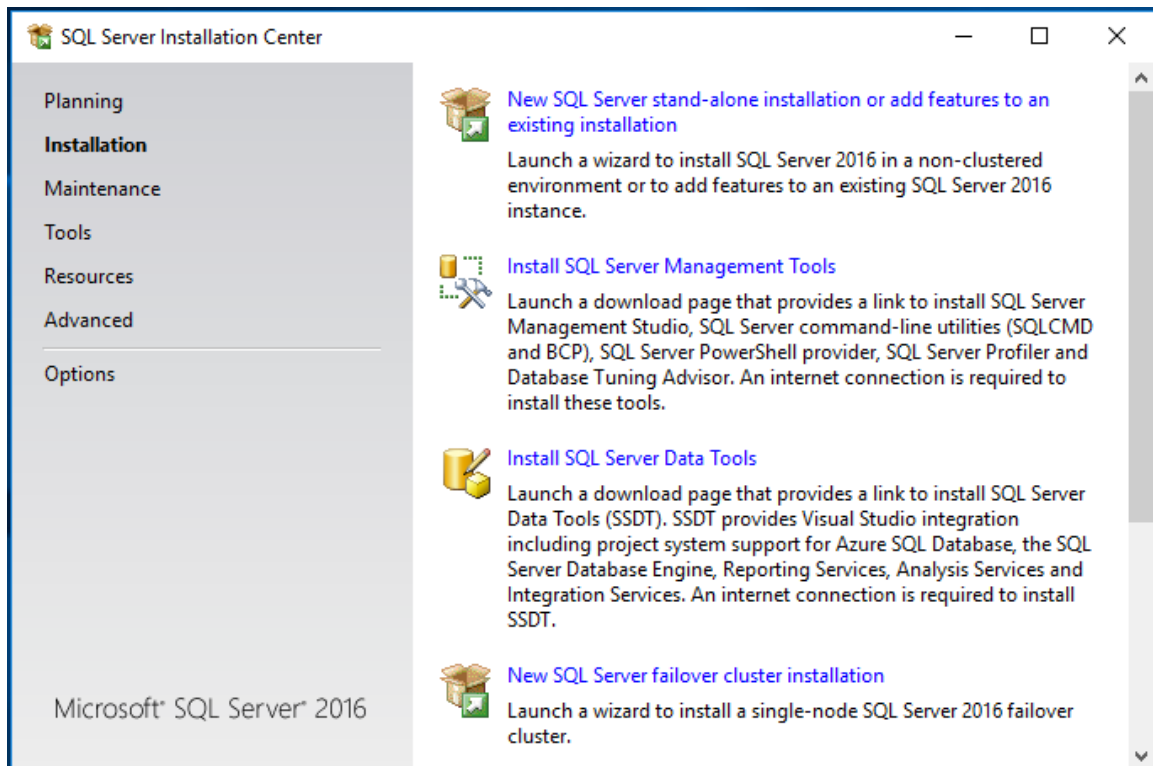


Figure 4.2: SQL Server Installation, Stand Alone

After finishing the SQL installation we will go for Kaspersky Security Center Installation

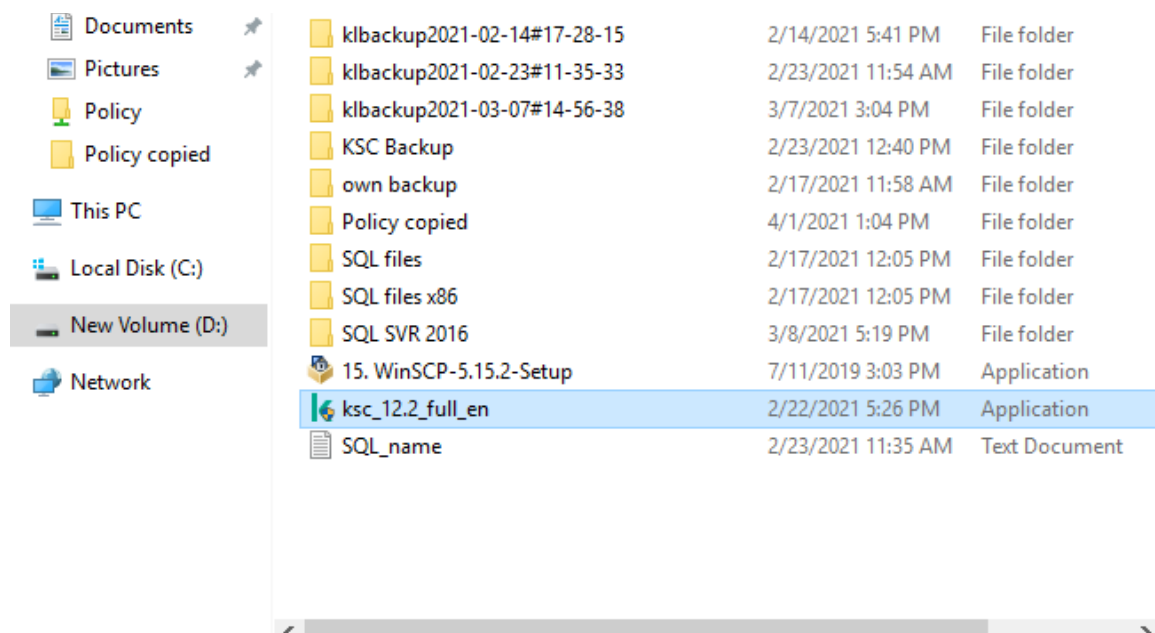


Figure 4.3: Kaspersky Security Center Installation

Here I am installing Kaspersky Security Center 12.2, I have to make sure that I'm installing with the administrator privilege. By Clicking Install Kaspersky Security Center 12 we will start the installation.



Figure 4.4: Kaspersky Security Center Installation Dashboard

After finishing the installation we can open Kaspersky Security Center with the console or Web browser. Kaspersky prefers the Console most.

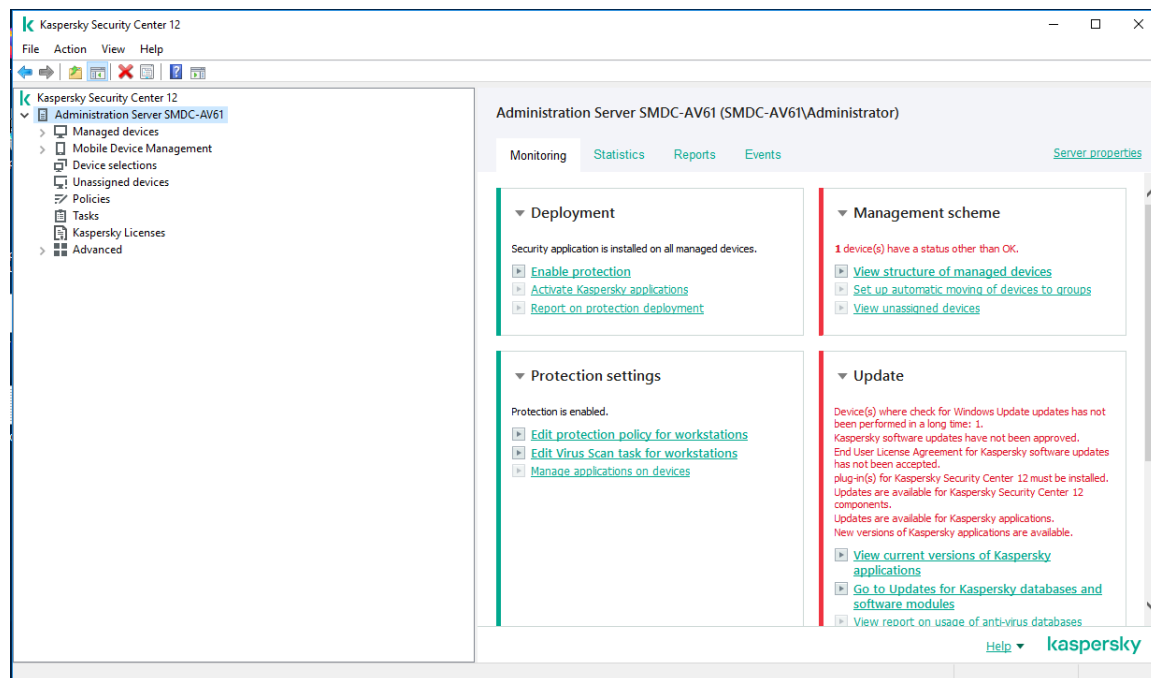


Figure 4.5: Kaspersky Security Center management Console.

### 4.3 Install Kaspersky Endpoint Security in client end

In Client device we need to install two software one in the Kaspersky Network Agent and another in Kaspersky Endpoint Security commonly known as KES. The Kaspersky Network Agent is the connector between the user device and Kaspersky Security Center. At first we will install the network agent then we will go for KES.

In time of installing the network agent we have to put the server address or Kasperskysecurity center server address (IP address of the server) and then it will be able to connect to the server. For this project we will recommend to create a mapping for Kaspersky Security Center IP address and connect the host's with the mapping IP. After the installation of network agent we need to add the device in Kaspersky Security Center.

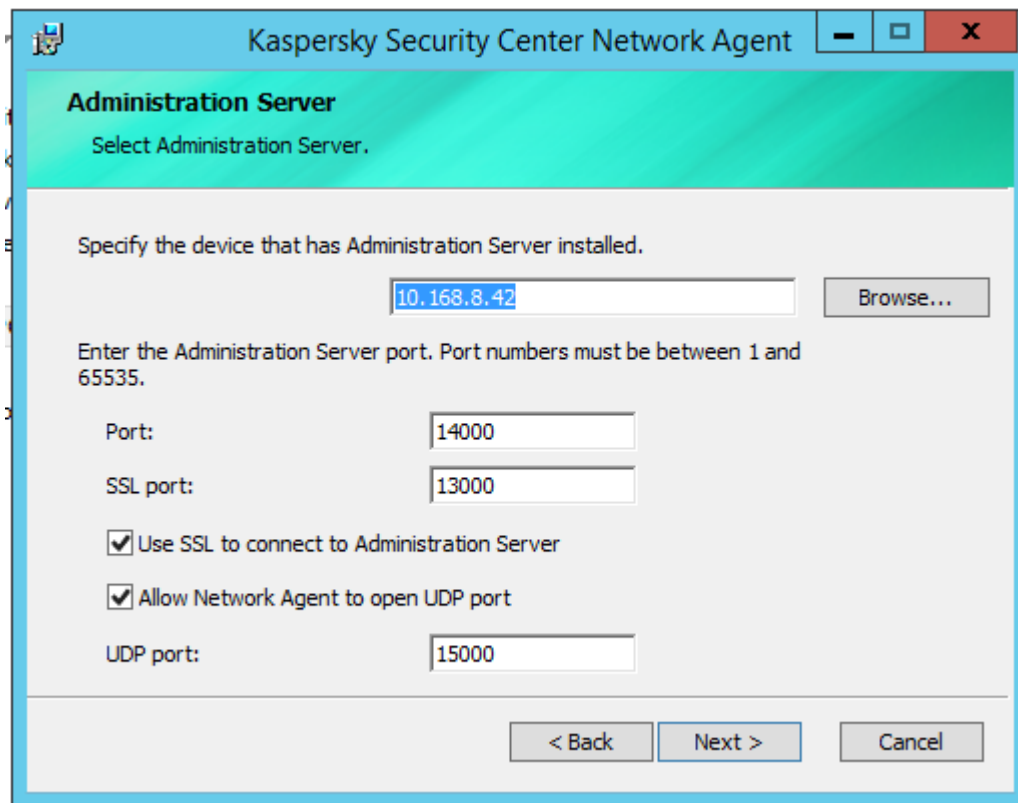


Figure 4.6: Kaspersky Network agent IP

After connecting the server to the Kaspersky Security Center we can install the KES software in user device remotely from Kaspersky Security Center or install it manually. If the network connection is slow or not stable then it's better to install the KES manually.

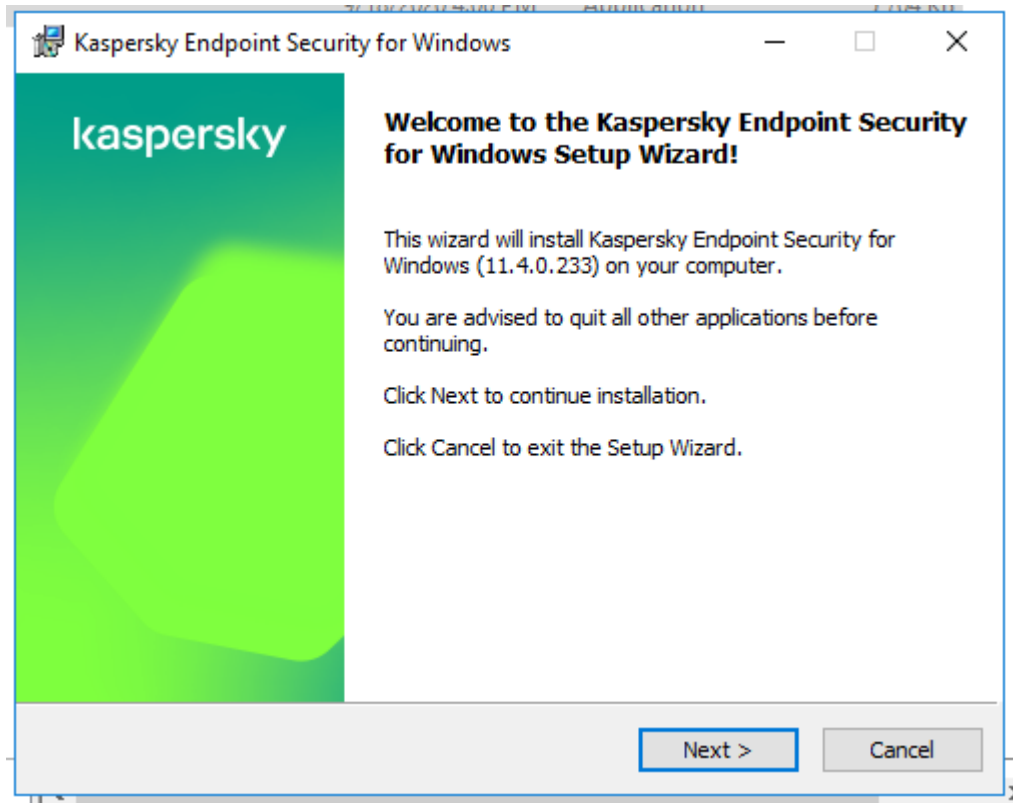


Figure 4.7: KES Installation

Installing the KES is very simple, have to agree with the license argument and have to select which features of the application you want from custom selection.

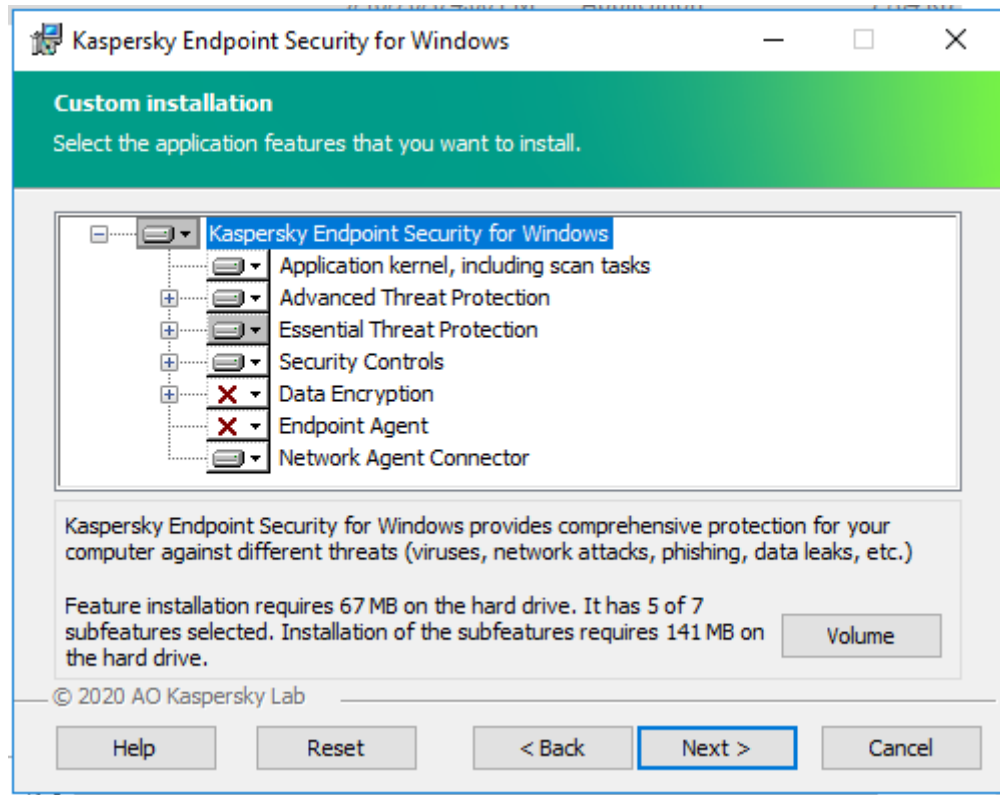


Figure 4.8: KES Custom Installation

User can also select more features like if he/she wants Citrix provisioning, KSN server etc.



After finishing the installation we will find below dashboard in the user device.

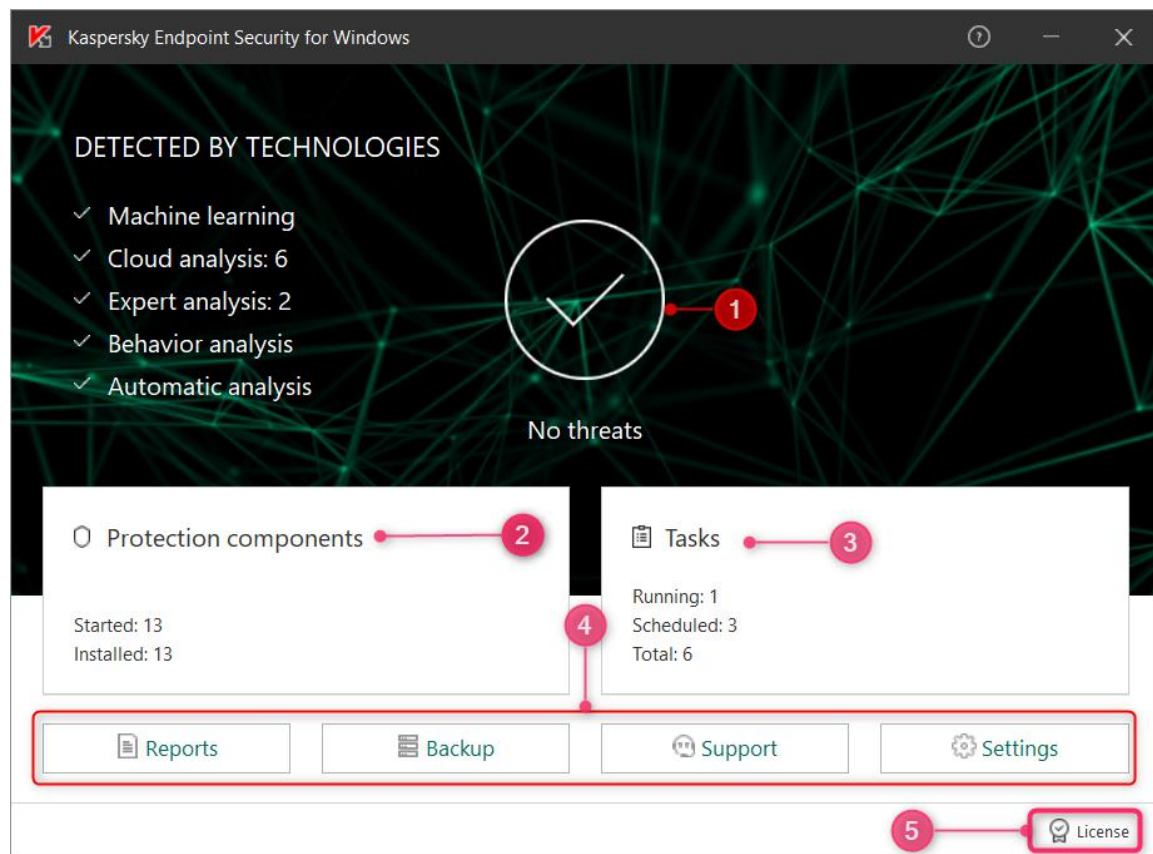


Figure 4.9: Kaspersky Security Endpoint Security Dashboard in client end

From the dashboard we can check different status, task and license. We can activate the Antivirus License from Kaspersky Security Center or we can activate or we can activate it manually from key file or license code but Kaspersky recommend activation of license from Kaspersky Security Center.

#### 4.4 Operation with Kaspersky Security Center

For manage the user Devices we have to add them in Kaspersky Security Center but before adding the devices we need to create group for proper management and apply policy.

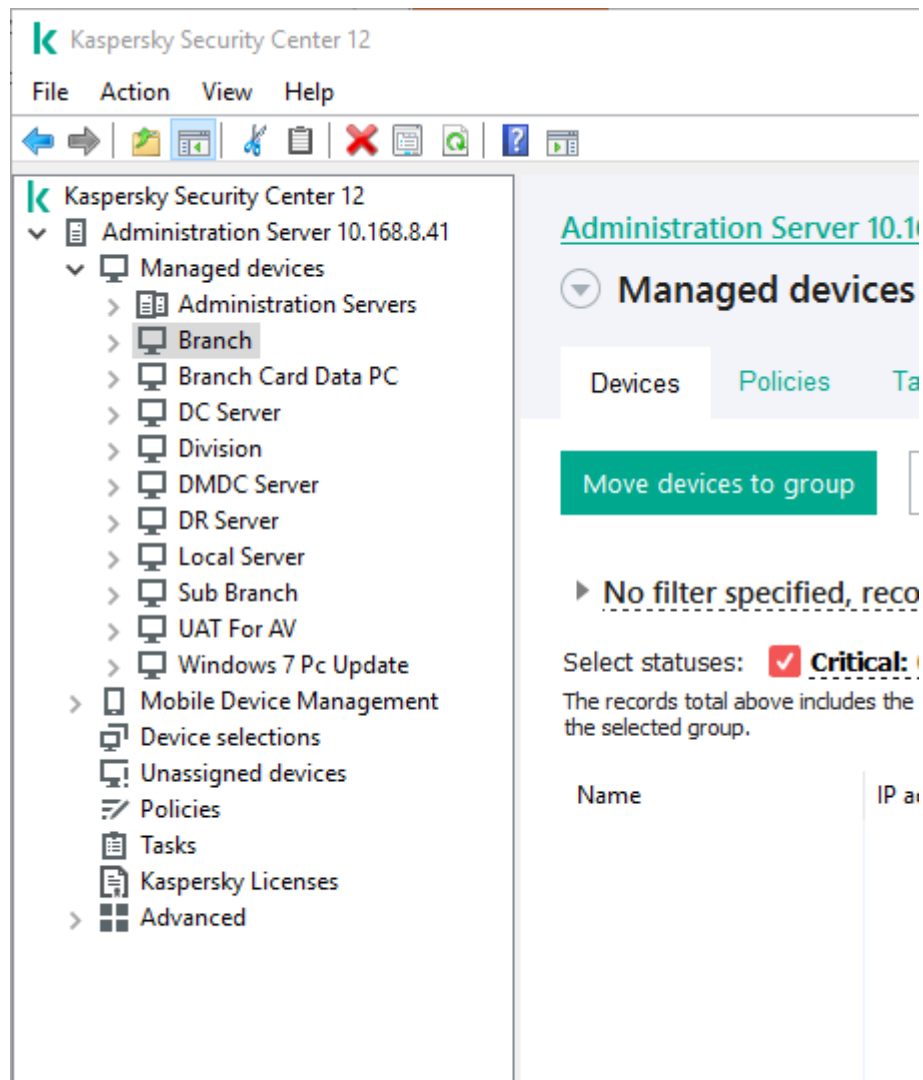


Figure 4.10: Kaspersky Security Center Management

From the manage device we can create group as per our requirement.

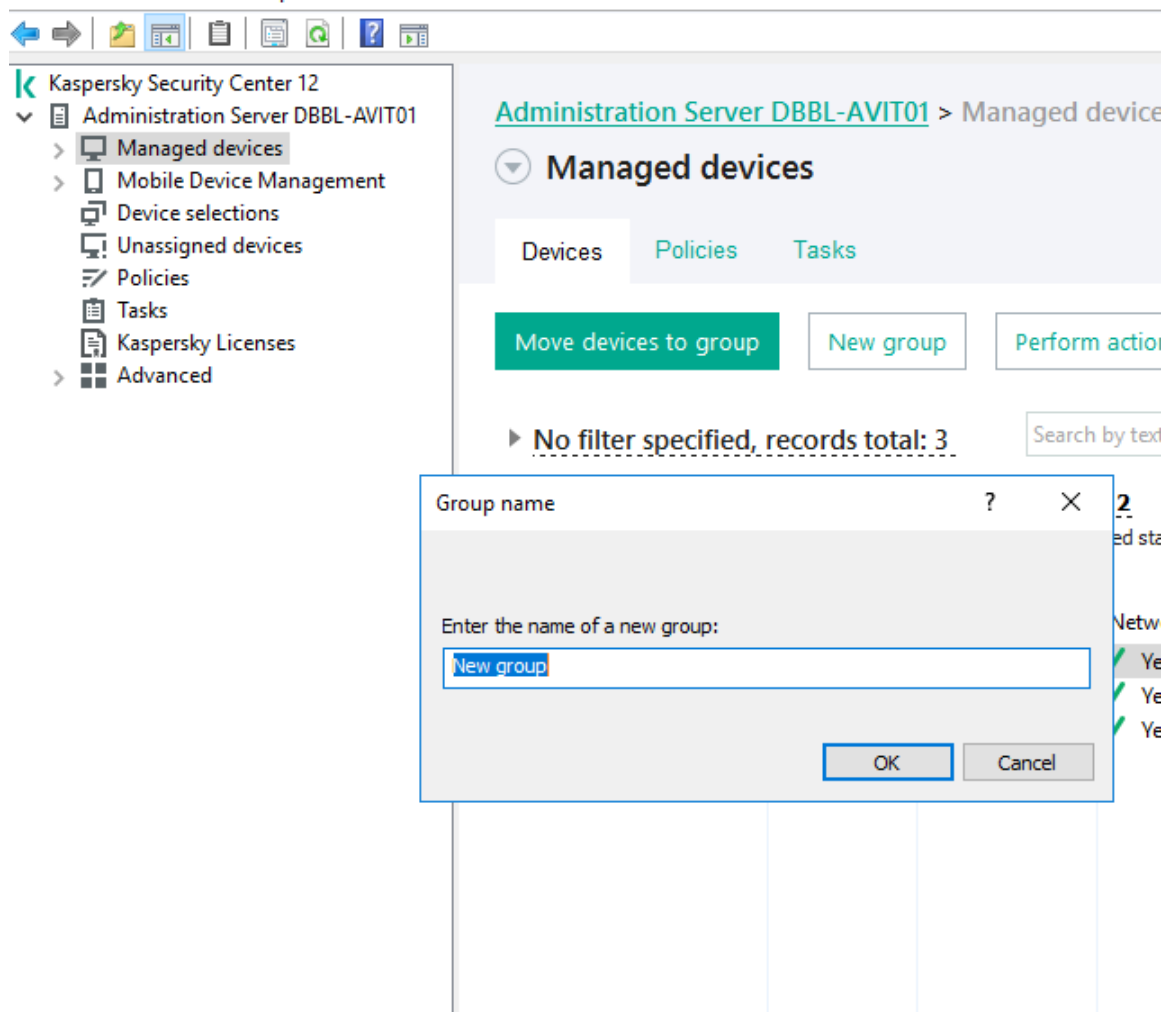


Figure 4.11 Group Add in KSC

After creating group we need to add policy for the specific group. Policy is basically depends on the OS versions of the users devices and KES versions. The automatic update schedule & scan schedule is also manage in policy

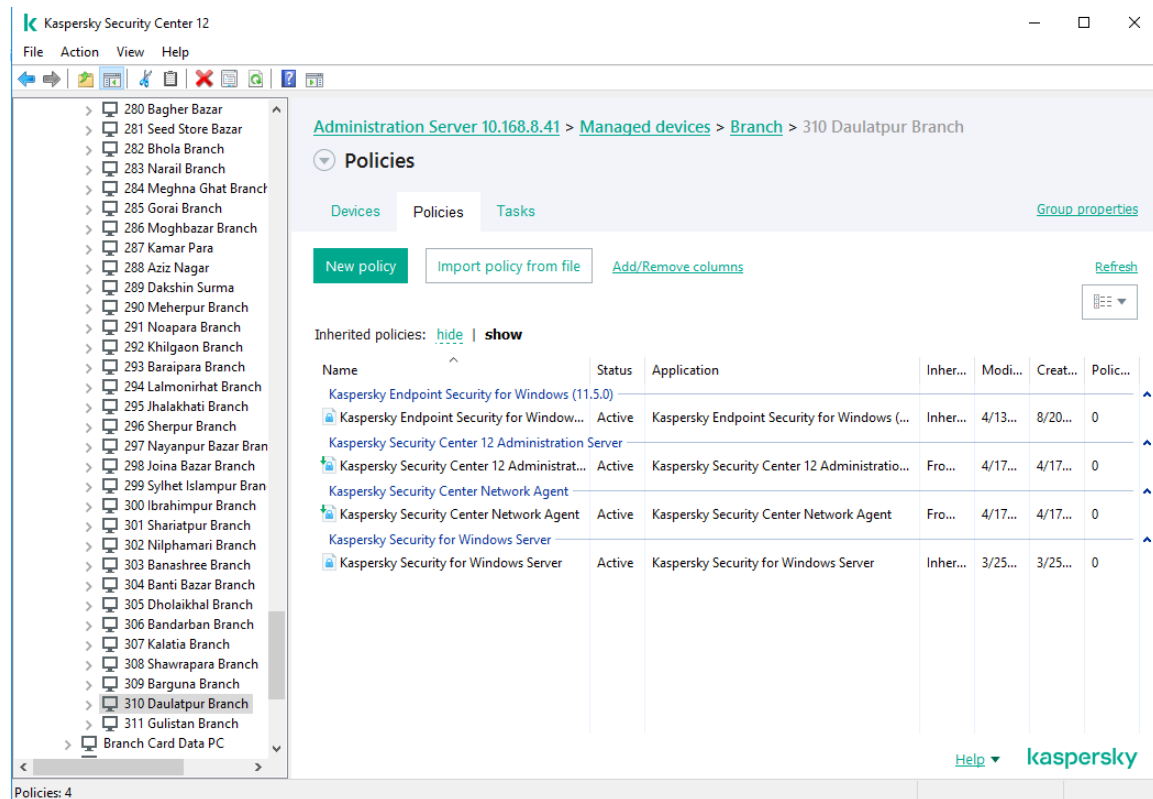


Figure 4.12: Manage Policy in Kaspersky Security Center

After making the policies we will add device to the groups. We can add devices by using device hostname or IP address.

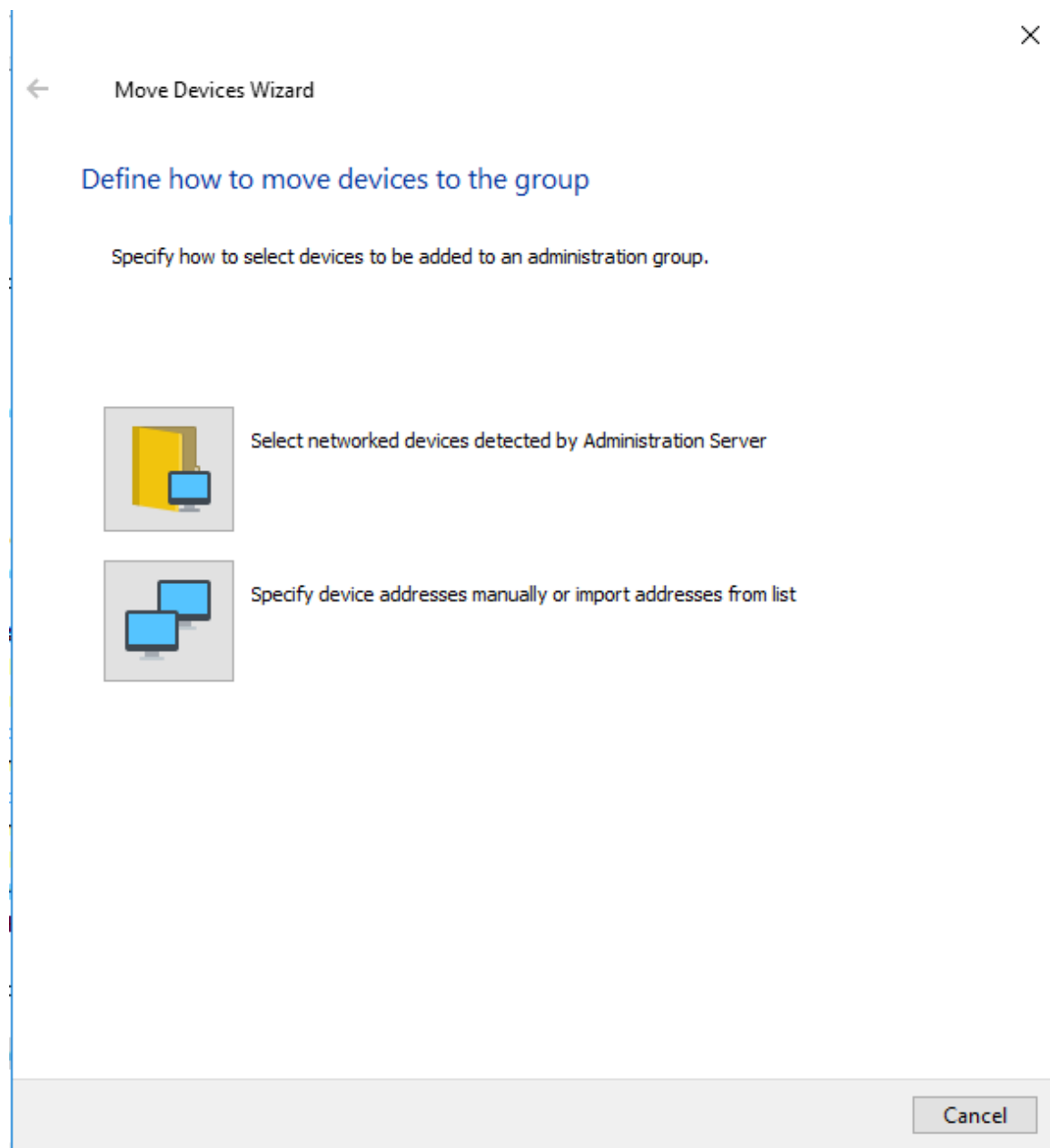


Figure 4.13: Host in Kaspersky Security Center

After adding devices we can see their status from the group under the managed server.

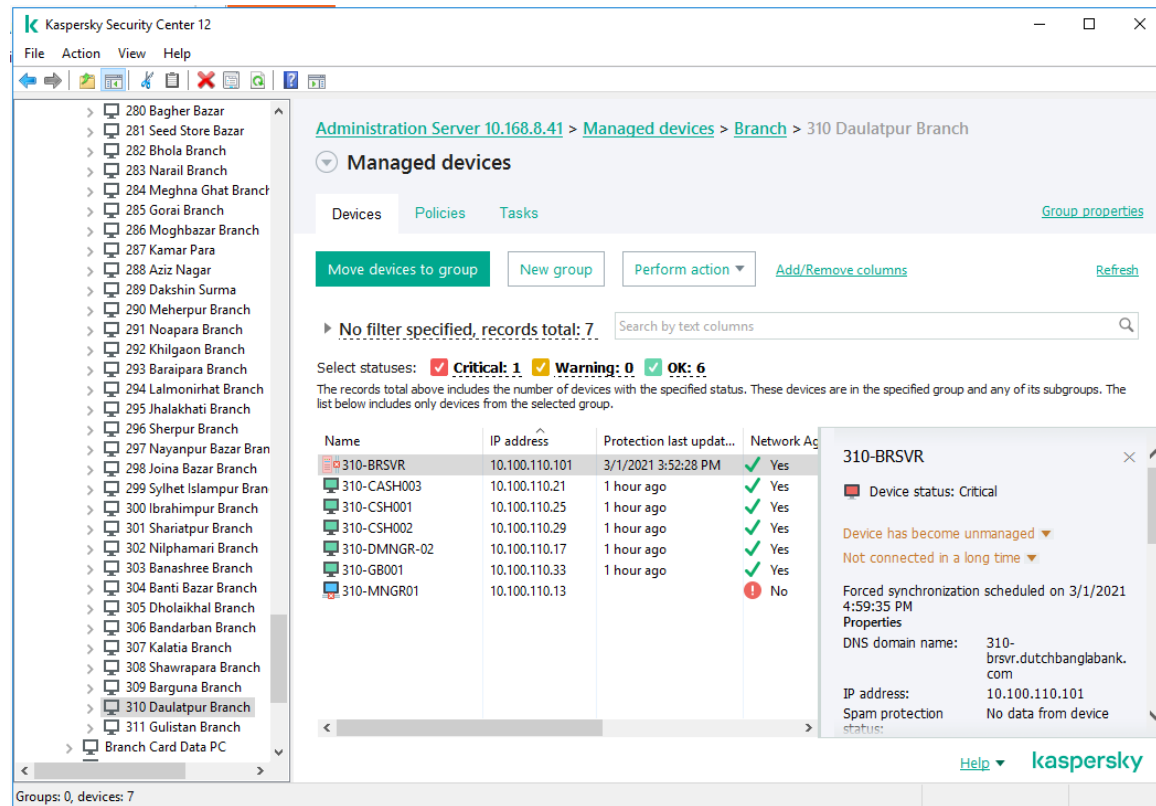


Figure 4.14: Manage Device in Kaspersky Security Center

We can find individual host of a group and there status

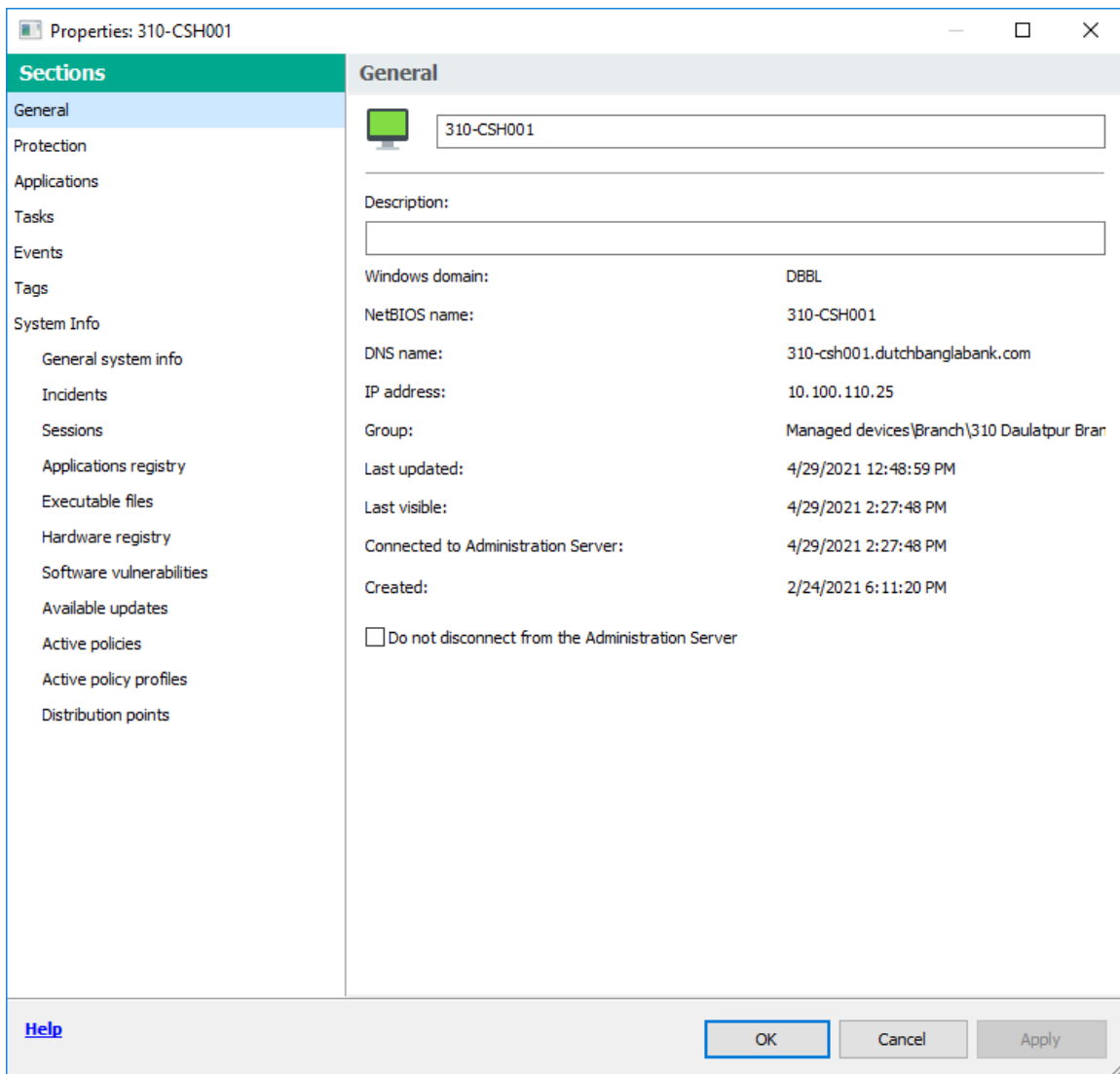


Figure 4.15: Host Status

From task we can run different task in it, like instant virus scan, update, add license etc.

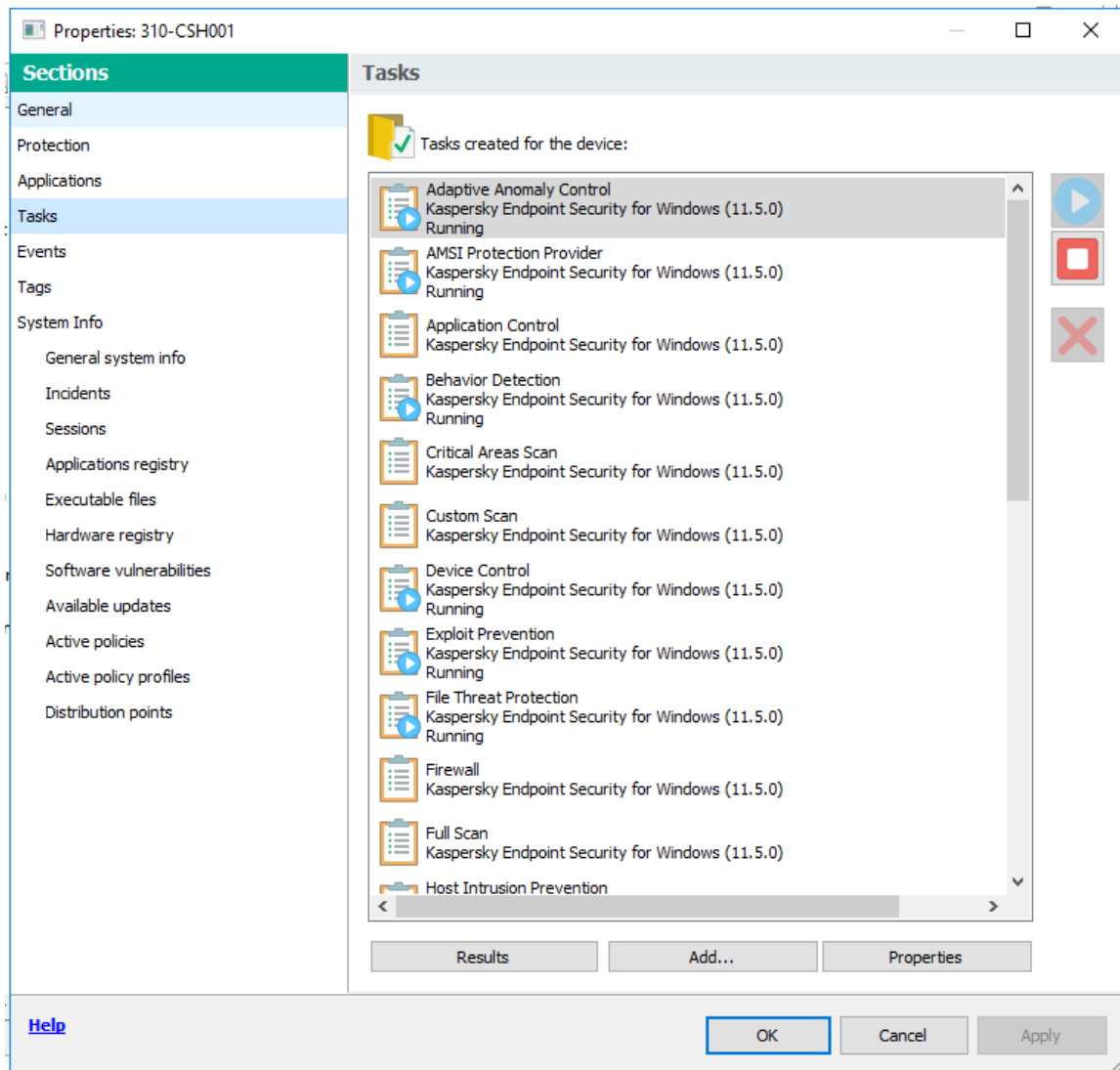


Figure 4.16: Running Task on a selective user in Kaspersky Security Center

## 4.5 Add Slave Server

Slave server is depending on master slave technology. We can add slave server under the master. Main role of master server here is to download the virus database update from Kaspersky site and distribute in slave server or servers. A Master server can have more the one slave. We can add slave server from the Kaspersky Security Center.



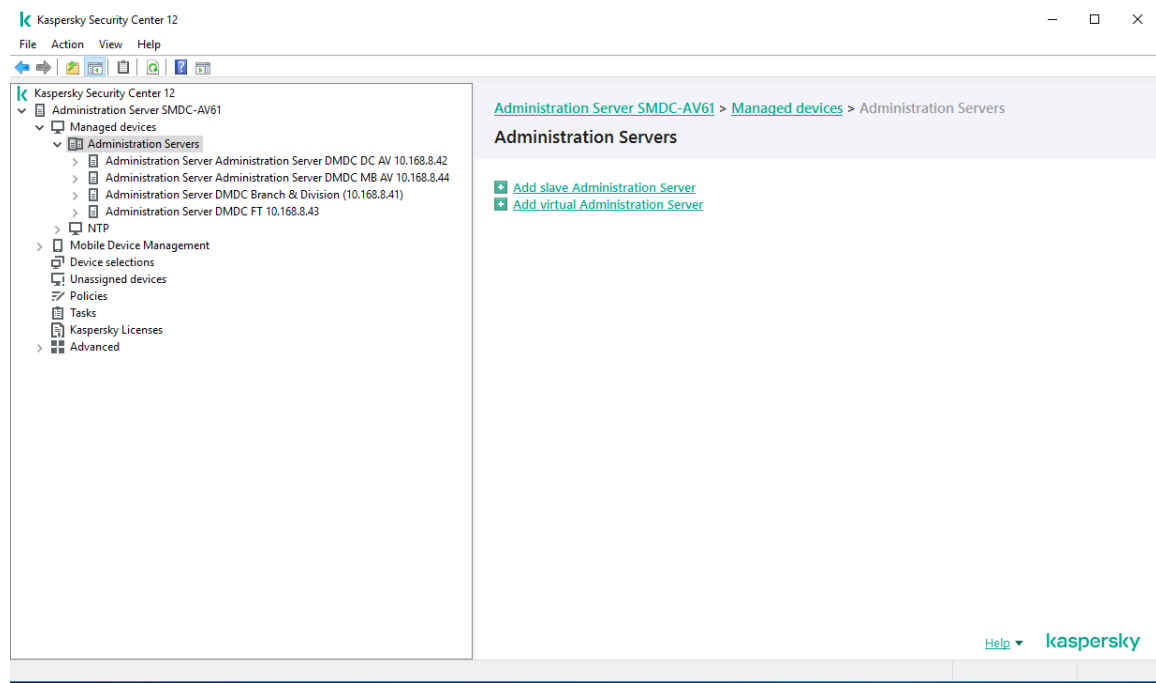


Figure 4.17: Add Slave Server in Kaspersky Security Center

**4.6 Proposed Solution for the Discussed environment:** As per I mentioned earlier that we are proposing a solution where there is no internet after DMZ and internet and intranet is separated. For any kind of antivirus software virus update is must and for downloading the updates we must need internet but in this type of environment where there is no internet in distribution zone how we can download the update. So our proposed solution is locate the Master Server in DMZ zone, where there is internet, the master server will download the update. The slave servers will be on the distribution zone where there is no internet but though they are connected with the master they can download the regular virus update and distribute it to the user devices. All user devices managed from the slave server and the role of the master is to download the update and distribute it to slave.

## CHAPTER 5

### KASPERSKY SECURITY CENTER BACKUP

#### 5.1 Introduction

Though all user device related information and policies are saved in Kaspersky Security Center so it's important to take Backup of Kaspersky Security Center.

#### 5.2 Kaspersky Security Center Backup tool

Kaspersky Security Center has a backup tool for keep the data backup in the same server where is situated.

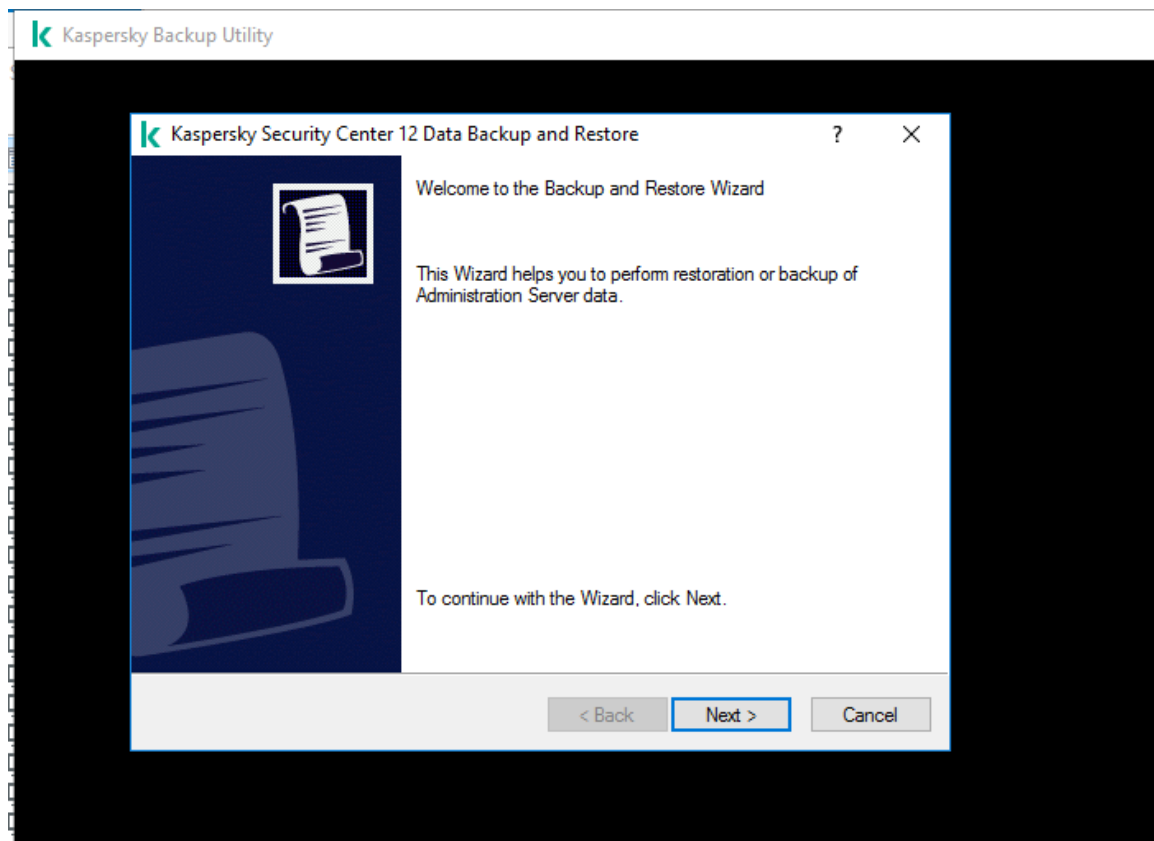


Figure 5.1: Backup and restore tool of Kaspersky Security Center

This Backup tool copies the Backup of Security Center in a shared location in the server.

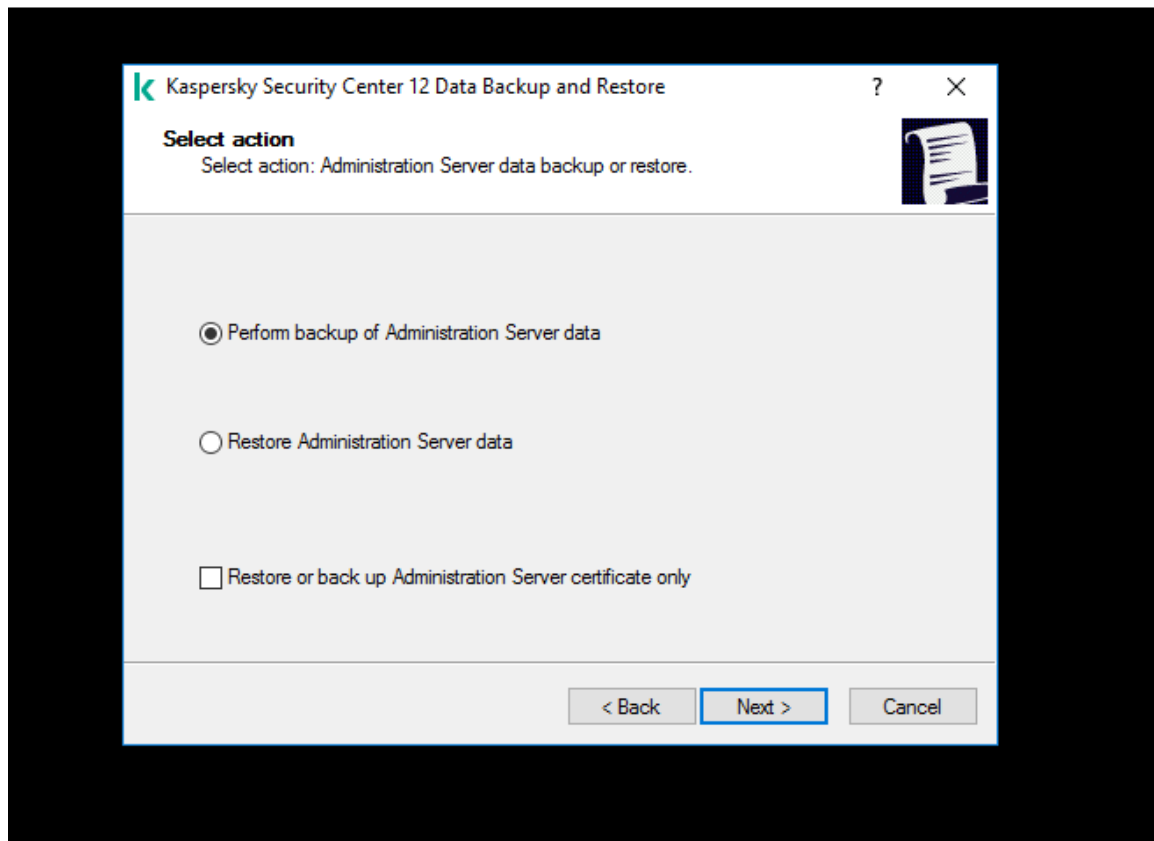


Figure 5.2: Backup and restore tool of Kaspersky Security Center 2

If any problem occurs to the system then we can restore the Kaspersky Security Center from the backup by this tool.

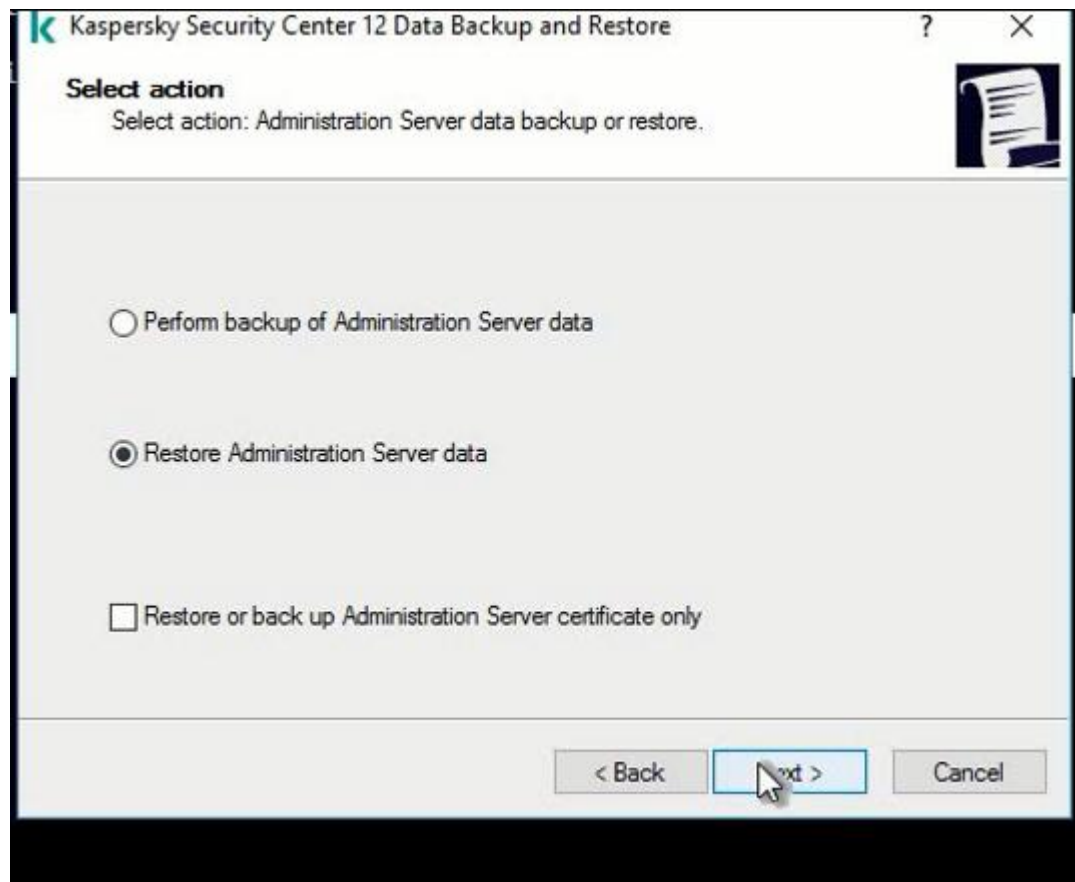


Figure 5.3: Backup and Restore Tool of KSC

### 5.3 Active-Passive Datacenter concept

Active passive Datacenter is a concept where there are two same kind of data center for an organization and both Data Centers are connected to each other. The operation runs from the main data center but all data is stored in both Data center equally. If the main data Center falls then all services can run from the other datacenter with stored Data.

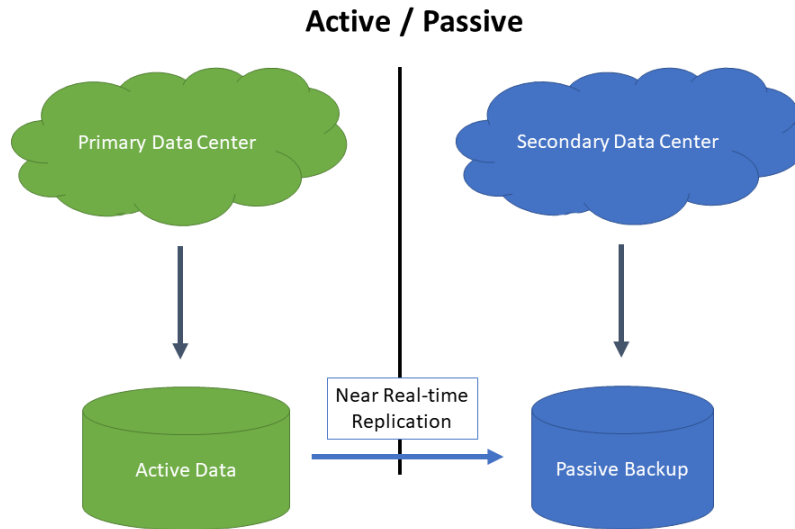


Diagram 5.3: Active passive Data Center theory

#### 5.4 Endpoint Security in Active Passive Datacenter Concept

Kaspersky Security Center keep backup on the same server where it's situated. Not only Kaspersky but also Endpoint Security Systems are also work the same way. They do not have any tool or process to keep backup of the Kaspersky Security Center in another server or location. So in active passive concept there is no data backup policy provided by the Vendors.

#### 5.5 Our Solution for the Backup

As I mentioned earlier, with the Kaspersky Backup tool we can take backup of Kaspersky Security Center data in a shared location of the same server. In active-passive concept both Datacenter are connected to each other. With the backup tool we will take backup of the Kaspersky Security Center server of main Data Center but will keep the backup in the passive Datacenter server through network share. If any disaster occurs in the main data Center we will restore Kaspersky Security Center from the passive Data Center server.

#### 5.6 Pre-requisites of Backup and Restore of Active Passive Data Center

For take backup and restore, in the Main Data Center and the Passive data Center we have to make the same Kaspersky Security Center server. In both side Kaspersky Security Center server's name will be the same but IP will be different.

### **5.7 Network Configuration**

All host devices need to connect to the server with the mapping IP address. Mapping IP address is a concept where there will be a private IP address against the IP of the Server or network device. Suppose our KSC server in distribution zone has IP 168.8.10.41 but we will map it with the private IP address 10.99.10.41. In host PC or device in time of installing network agent we will put the private IP address 10.99.10.41. After restoring the KSC server from passive data center we need to change the real ip against the mapping IP from active Datacenter IP to Passive data Center IP by NAT. SO if our KSC server of passive data center is 192.90.40.10 then we have to map IP address 10.99.10.41 to 192.90.40.10 from 168.8.10.41. By doing this there will be no effect of KSC server IP changing in host end.

### **5.8 Working Procedure of Backup**

As I mentioned earlier backup tool keep the backup in a shared network place so we will make a share folder in the passive data center server. In the backup tool we will put the share location of the share folder of the passive data center server. Though the hostname of the both servers are same so restore will be done normally and as I mentioned earlier that host will connect to the server with mapping IP, we will change the mapping IP of the Kaspersky Security Center server from Active Datacenter Server IP to Passive Datacenter Server IP. Then the host will be able to connect with the Kaspersky Security Center server in passive data center side.

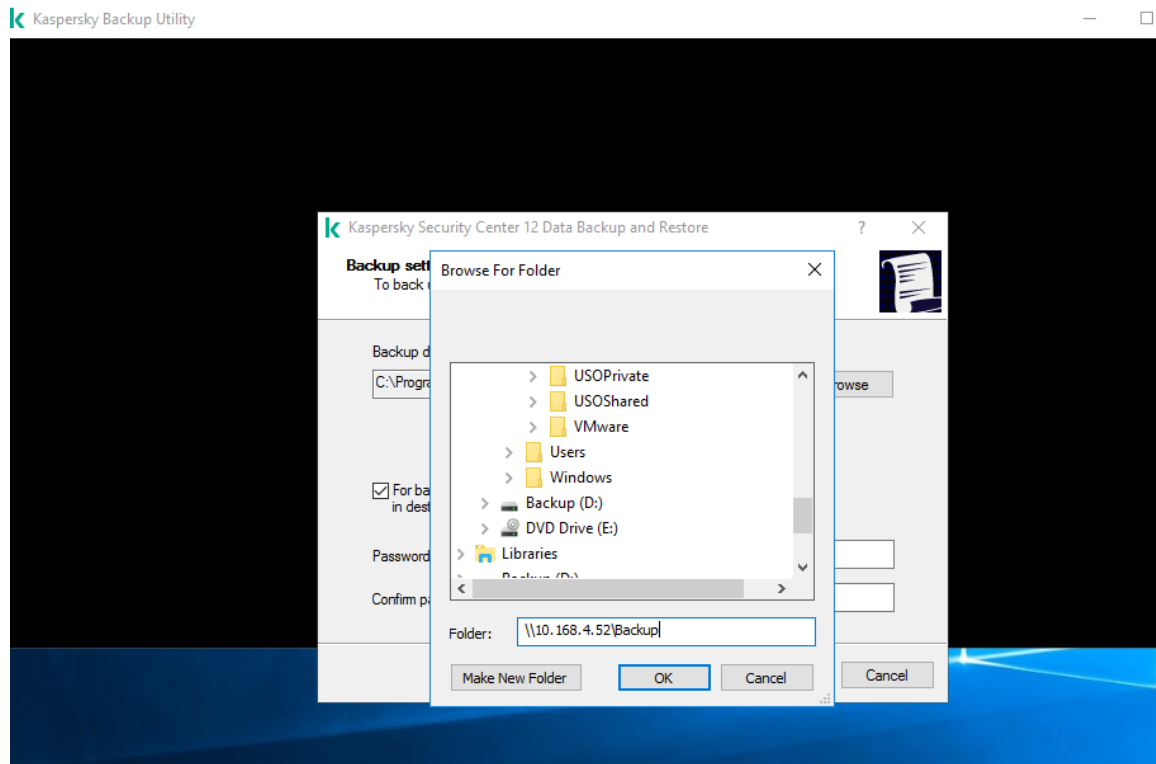


Figure 5.4: Backup KSC in another Server with Backup and Restore Tool of Kaspersky Security Center

## **CHAPTER 06**

### **CONCLUSION AND FURTHER STUDY**

#### **6.1 Summary of the Study**

To complete my project I have work with endpoint security solution, managing endpoint protection from security center server and how it manage in different type of network structure.

I have also work with active passive solution, gained knowledge about it. I have come up with a solution for active-passive backup and restore of Kaspersky endpoint security which was a unique idea and make it happened.

#### **6.2 Conclusion**

During this project I have discovered some drawbacks of Kaspersky endpoint security. When the scheduled update and remote installation going on, the network need to be very stable a single packet loss can undone the whole project.

Network stability is also important in active passive backup because in this process we are copping the backup from one server to another server through network share so unstable network, spike or packet loss could be the reason of failure of total work.

#### **6.3 Recommendations**

Though I mention some related work. It was very hard for me to make things happen. I am very thankful for the company DBBL where I work because for DBBL I have got the opportunity to work with different endpoint Security Solutions and the environment to implement the project. With the total journey if this research Work my supervisor Mr. Md. Abbas Ali Khan helped me a lot and guided me for making this research project successful.



#### **6.4 Future Study**

In this project I have come with a backup solution of active-passive network structure and also restore it in future I will work for endpoint security backup and solution for Active-Active environment.

## REFERENCES

- [1] Kaspersky Cyber Security Solution, available at << <https://kaspersky.com> >>, last accessed on 02-03-2021 at 10PM.
- [2] Active passive clustering, available at <<<https://www.sanitysolutions.com>>>, last accessed on 01-03-2021 at 8 PM.
- [3] Endpoint Solution, available at <<<https://www.mcafee.com>>>, last accessed on 01-02-2021 at 9 PM.
- [4] Backup and restore, available at <<<https://csguide.cs.princeton.edu/storage/backup>>>, last accesses on 04-02021 at 5 PM.
- [5] Active-Active clustering, available at <<<https://www.purestorage.com/au/knowledge/>>>, last accessed on 03-04-2021 at 11 PM.

## ENTERPRISE ENDPOINT SECURITY SOLUTION FOR LARGE ORGANIZATION WITH HIGH AVAILABILITY (ACTIVE-PASSIVE)

### ORIGINALITY REPORT

5%	%	%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

### PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	4%
2	Submitted to Sheffield Hallam University Student Paper	1%
3	Submitted to Oaklands College Student Paper	<1%

Exclude quotes Off  
Exclude bibliography Off

Exclude matches Off