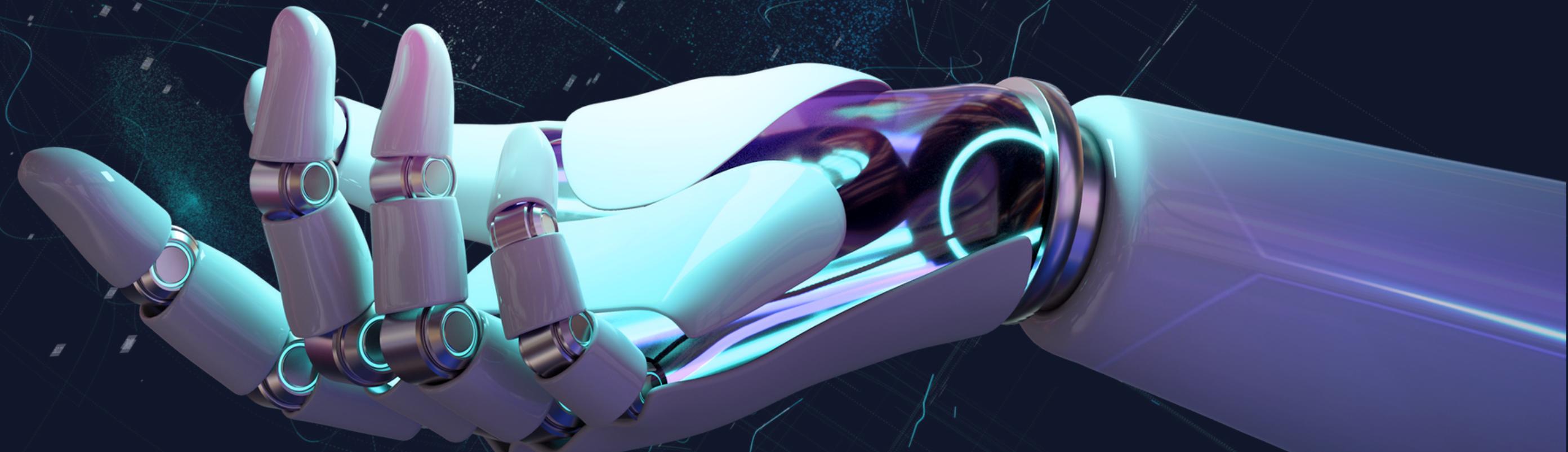


بسم الرحمن الرحيم

تثبيت واعداد  
Wazuh  
وتحديث واعداد  
Sysmon

by: Abdulrahman.



# شرح اعداد و تثبيت wazuh على virtualbox

Google search results for "wazuh ova". A large white circle with the number 1 is overlaid on the search bar, and a white arrow points from it to the first search result.

wazuh ova

All Videos Images News Maps More Tools

About 3.180 results (0,40 seconds)

[https://documentation.wazuh.com › deployment-options](https://documentation.wazuh.com/deployment-options)

**Virtual Machine (OVA) - Installation alternatives**

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (**OVA**) format. This can be directly imported to VirtualBox or other **OVA** compatible ...

Wazuh website screenshot showing the "Virtual Machine (OVA)" page. A large white circle with the number 2 is overlaid on the sidebar menu, and a white arrow points from it to the "Virtual Machine (OVA)" link under "Installation alternatives".

Platform Cloud Services Partners Blog Company Version 4.3 (current)

Search

Getting started Quickstart Installation guide

**Installation alternatives**

- ▶ **Virtual Machine (OVA)**
- Amazon Machine Images (AMI)
- Deployment on Docker
- Deployment on Kubernetes
- Offline installation
- Installation from sources
- Installing Wazuh with Elastic
- Stack basic license

انقر هنا وسوف يتم تحميل السيرفر بشكل تلقائي

Virtual Machine (OVA)

Wazuh provides a pre-built virtual machine image in Open Virtual Appliance (OVA) format. This can be directly imported to VirtualBox or other OVA compatible hosts. Take into account that this VM only runs on 64-bit systems and does not support distributed deployment. Be aware that some components may not work out of the box. However, these can be implemented by using a distributed deployment.

Download the [virtual appliance \(OVA\)](#), which contains the following components:

- CentOS 7
- Wazuh manager 4.3.6
- Wazuh indexer 4.3.6
- Filebeat-OSS 7.10.2
- Wazuh dashboard 4.3.6

ON THIS PAGE

- [Virtual Machine \(OVA\)](#)
- Hardware requirements
- Import and access the virtual machine
- Access the Wazuh dashboard
- Configuration files
- VirtualBox time configuration
- Upgrading the VM

Search


[/ Quickstart](#)

## Hardware

Hardware requirements highly depend on the number of protected endpoints and cloud vs on-premises deployment. The number of agents can help estimate how much data will be analyzed and how many security alerts will be indexed.

Following this quickstart implies deploying the Wazuh server, the Wazuh indexer, and the Wazuh agent on the same host. This is usually enough for monitoring up to 100 endpoints and for 90 days of queryable/indexed alert data. The table below shows the recommended hardware for a quick deployment:

Agents	CPU	RAM	Storage (90 days)
1-25	4 vCPU	8 GiB	50 GB
25-50	8 vCPU	8 GiB	100 GB
50-100	8 vCPU	8 GiB	200 GB

هذا يوضح استخدام السيرفر على مدار 90 يوم من حيث مساحة الذاكرة  
وقدرة المعالج والرامات وتدل "Agents" على عدد الأجهزة المستعنة على  
السيرفر

Getting started

## Quickstart

Installation guide

Installation alternatives

Upgrade guide

Migration guide

Wazuh Cloud service

User manual

Cloud security

Container security

Development

Compliance

هذا يوضح الحد الأدنى "Minimum" من حجم الرايم والمعالج  
واعداد الموصى به "Recommended" من حجم الرايم والمعالج



wazuh.

Platform Cloud Services Partners

Search



Getting started

Quickstart

## Installation guide

Wazuh indexer

## Wazuh server

Wazuh installation  
assistant

Step-by-step installation

Wazuh dashboard

Wazuh agent

/ Installation guide / Wazuh server

Red Hat Enterprise Linux 7, 8, 9

Ubuntu 16.04, 18.04, 20.04, 22.04

## Hardware requirements

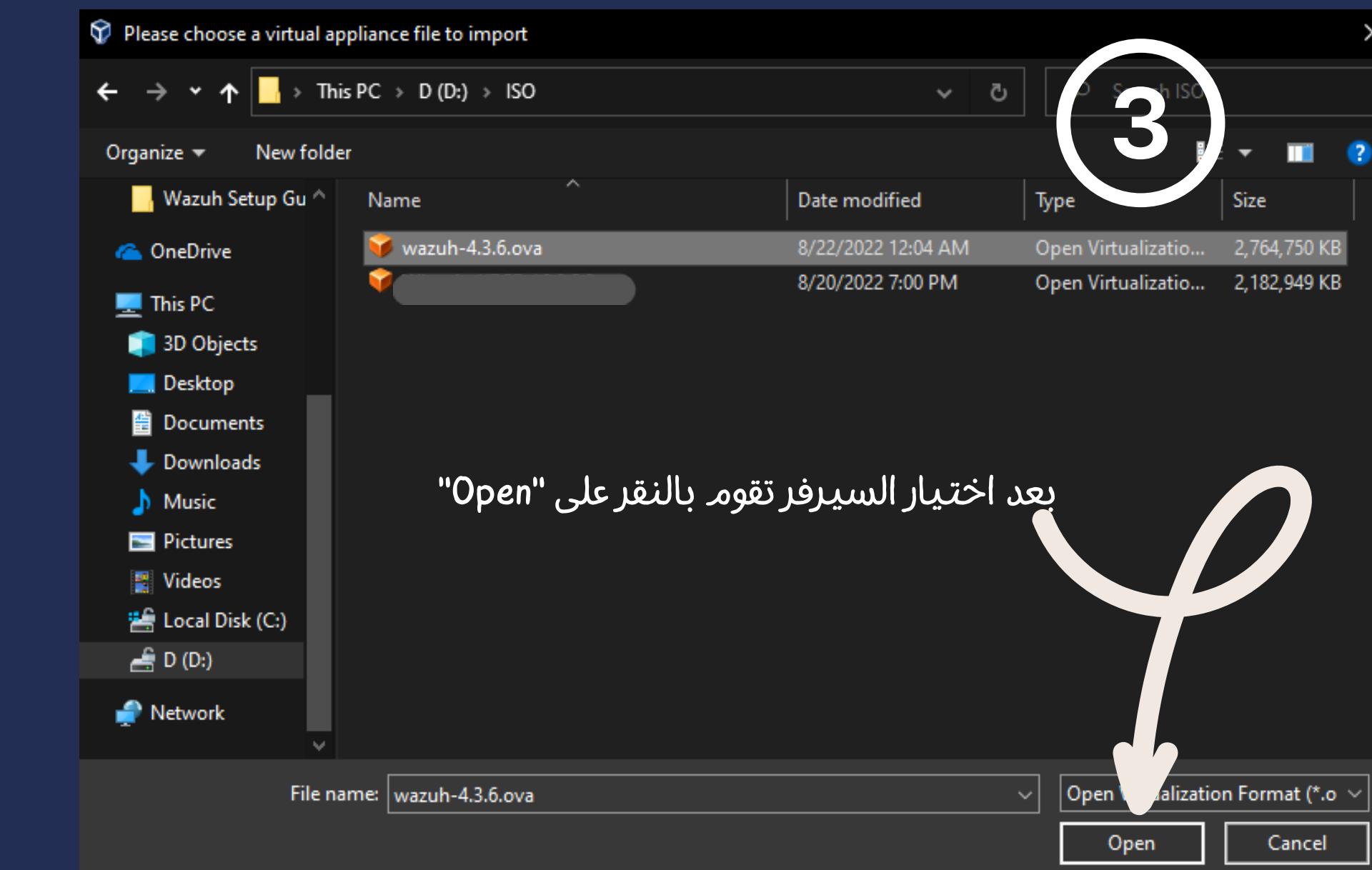
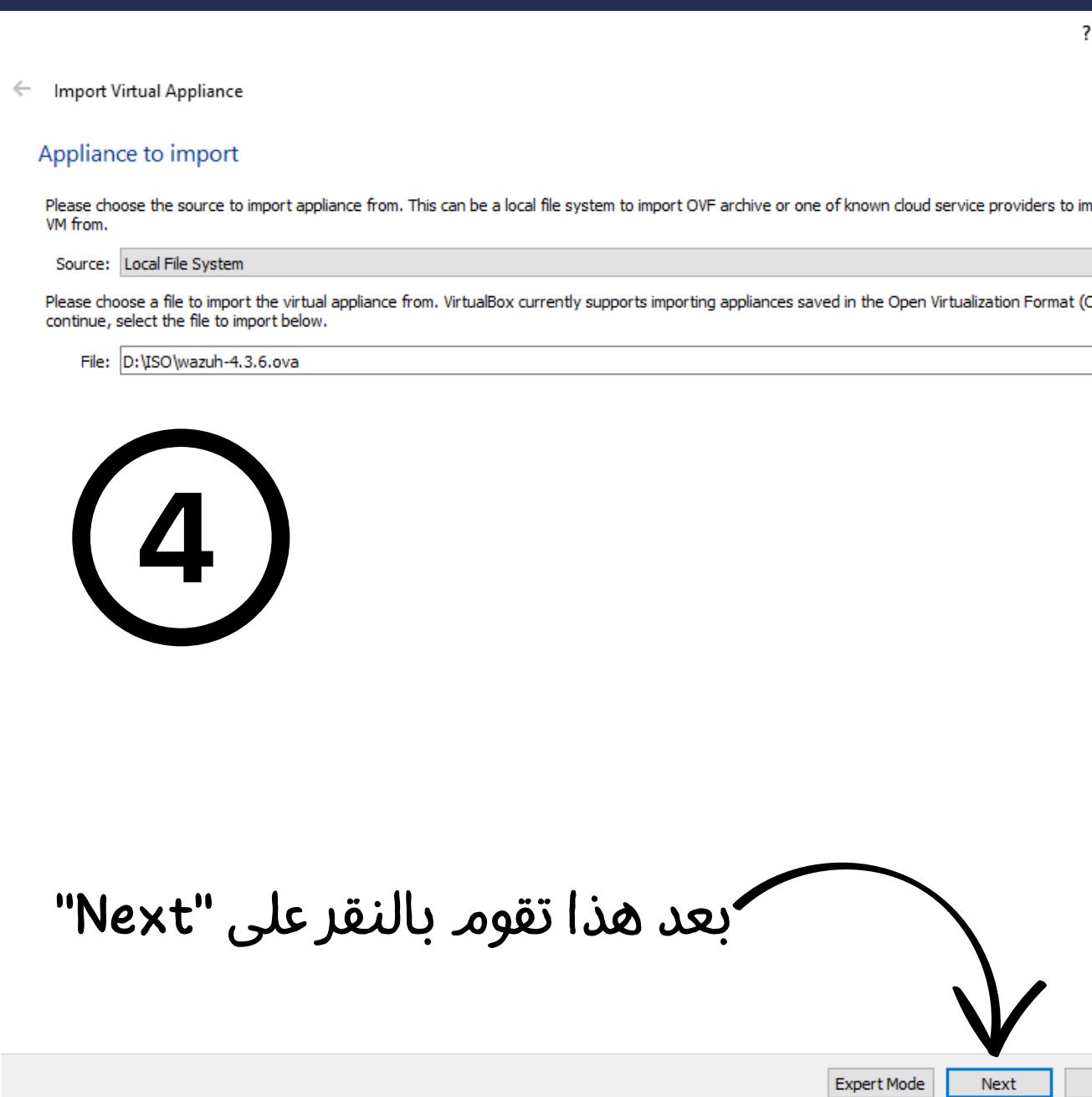
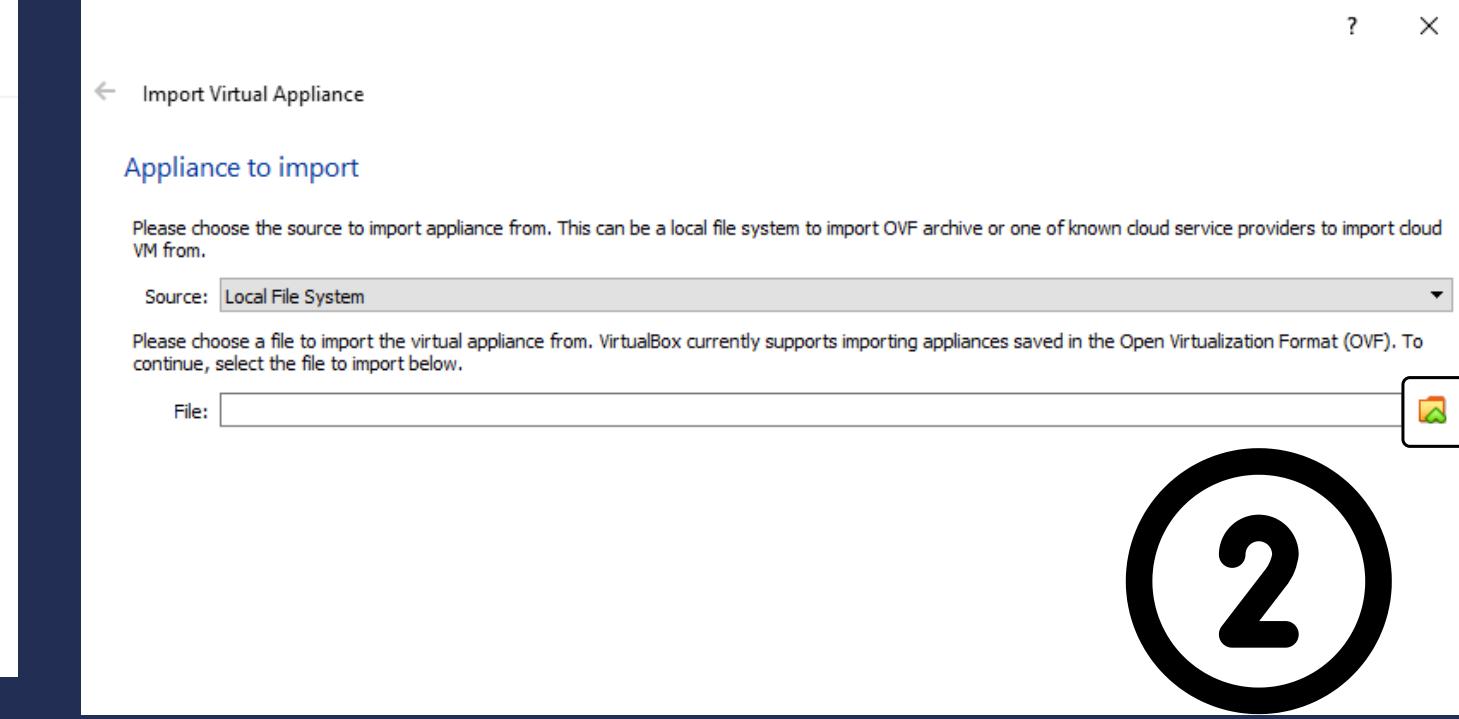
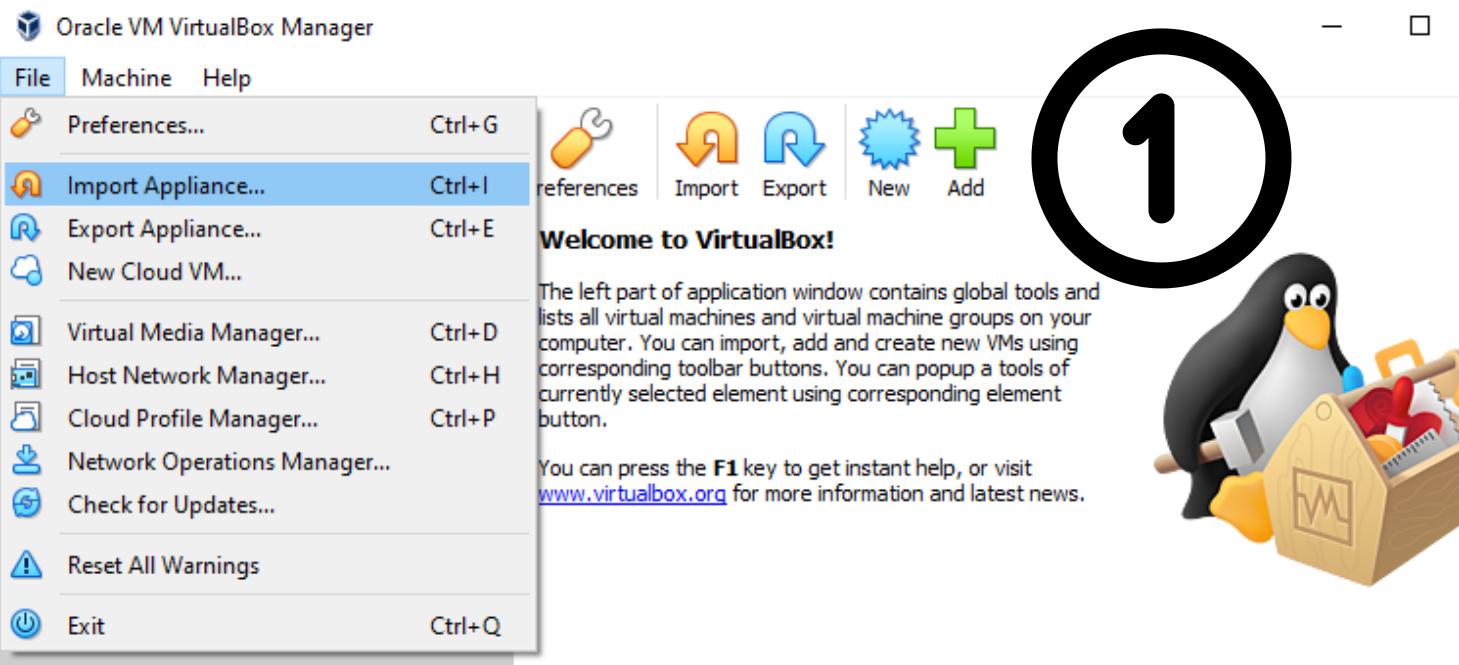
The Wazuh server can be installed as a single-node or as a multi-node cluster.

- Hardware recommendations

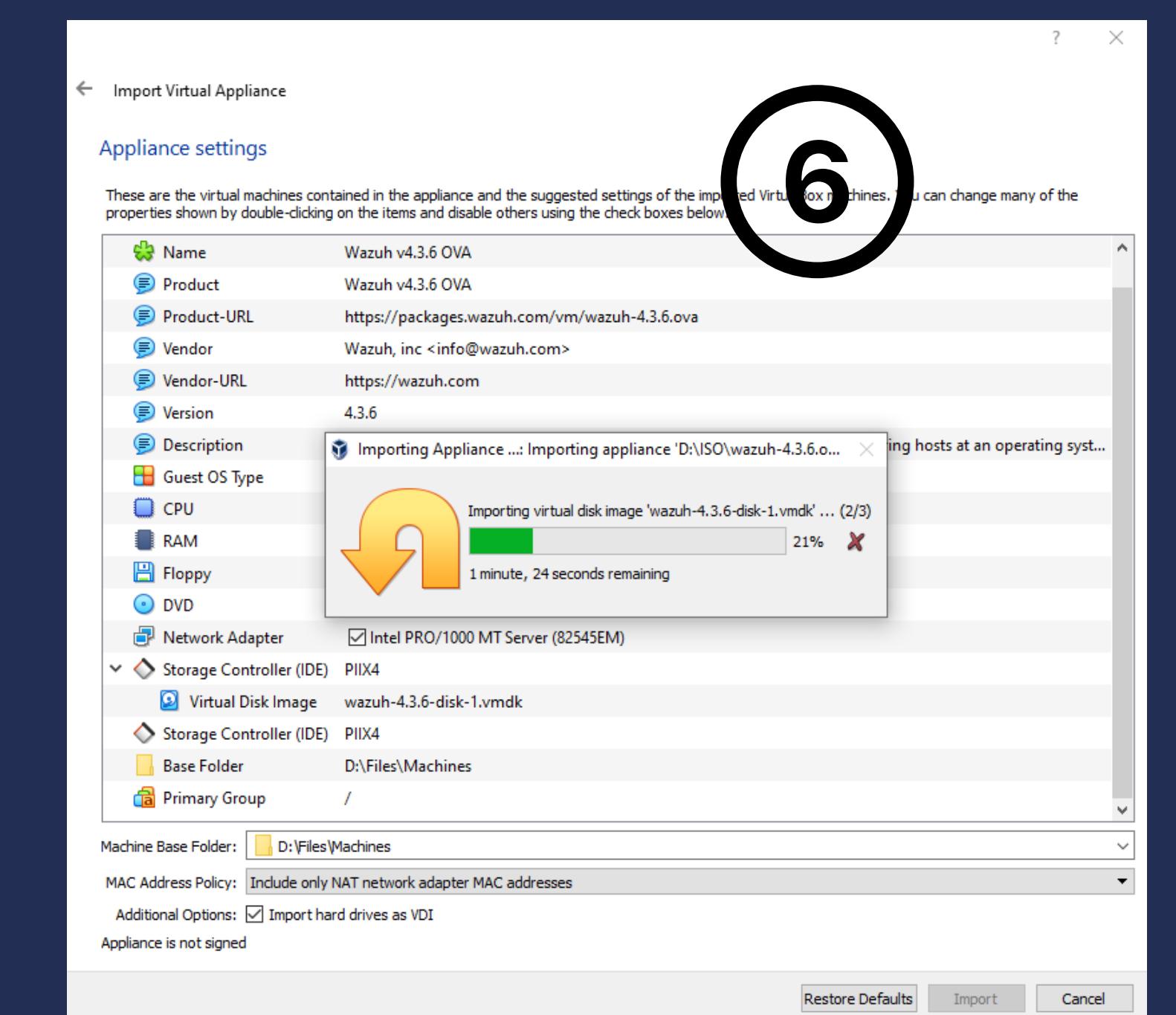
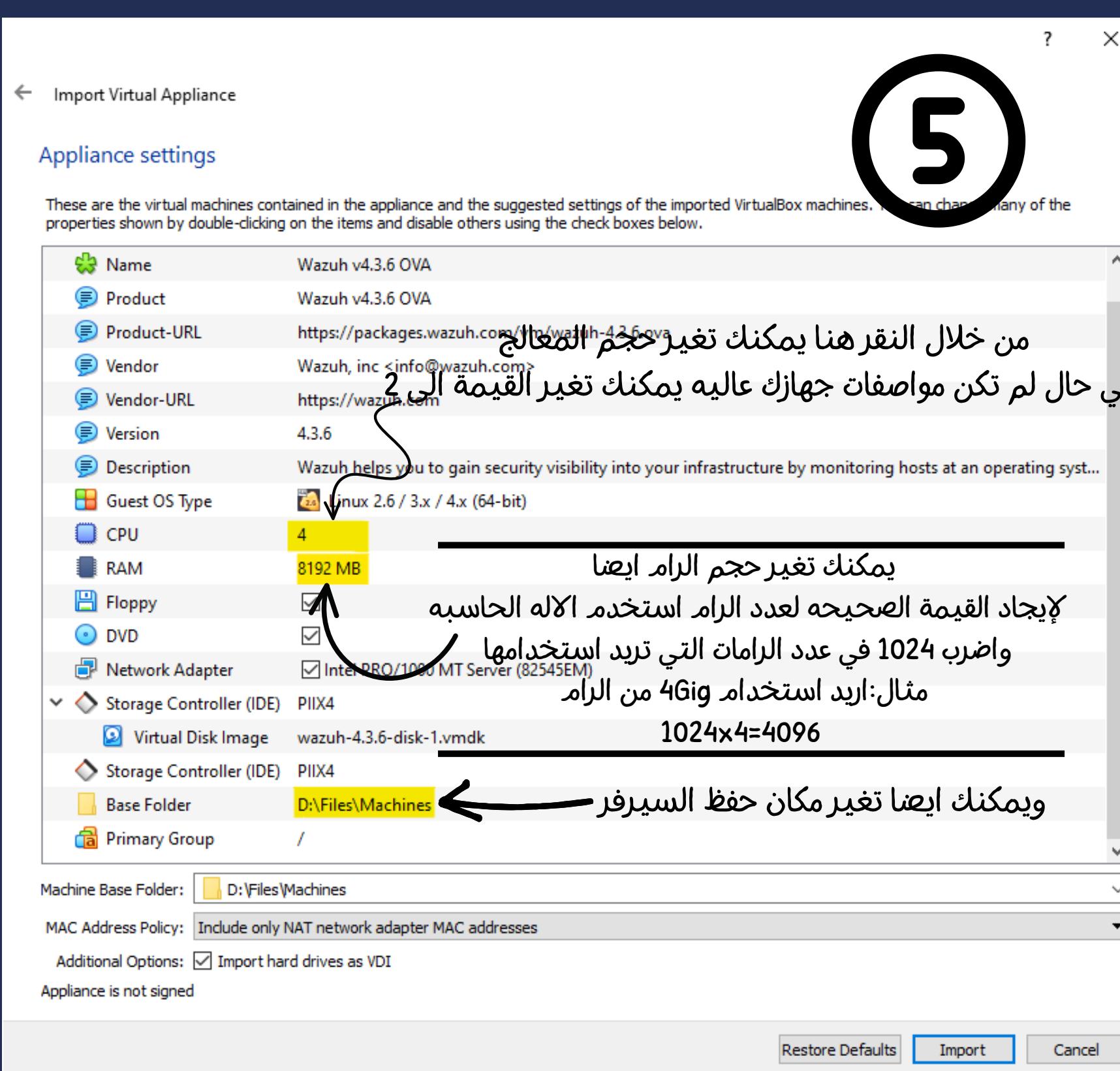
Component	Minimum	Recommended	RAM (GB)	CPU (cores)
	RAM (GB)	CPU (cores)		
Wazuh server	2	2	4	8



اتقد هنـا وسـوف تـبـثـق لـك زـافـذـه وسـوف  
تـقـوم بـأـخـتـيـار مـكـان السـيرـفـر الـذـي تم  
تـحـمـيلـه مـسـقاـ



"Next"



لمعرفه عنوان السيرفر للدخول عليه من خلال متصفح قم بكتابه الأمر "ip" في حال لم يظهر لك اي عنوان كما هو موضح باللون البرتقالي قم بكتابه الأمر التالي "sudo systemctl restart network"

بعد ذلك قم بكتابه كلمة المدورة اخرى "wazuh" لمنح صلاحيه المسؤول من خلال الامر sudo





## بعد ذلك قم بكتابه الامر

"ssh -l wazuh-user <ip address>"

اسم المستخدم بعد ذلك عنوان الايميل الخاص بالسيرفر

بعد ذلك اكتب 'yes' بعد ذلك سيرسل لك الكلمة المدورة الخاصة باليوزر

**"في حال لم تقم بتغيير كلمة المرور بعد "wazuh**

## ـ "OK" cmd ٿم بکتابه

قم بتشغيل موجه اوامر للاتصال بالسيرفر من خلال بروتوكول ssh لسهولة النسخ والصق لتشغيله من خلال الكيبورد "علامه الويندز + حرف R" بعد ذلك قم

A screenshot of the Windows Run dialog box. The title bar says "Run". The main area has a blue icon of a square with rounded corners and a smaller square inside. To its right is the placeholder text: "Type the name of a program, folder, document, or internet resource, and Windows will open it for you." In the search field below, the text "cmd" is typed. At the bottom are three buttons: "OK" (highlighted with a blue border), "Cancel", and "Browse...". A large black circle with a white number "10" is overlaid on the top right corner of the dialog box.

اًلن سوف نقوم بتغيير كلمة المرور الافتراضيه للمستخدم لحماية السيرفر

نقوم بكتابه الامر "sudo passwd wazh-user"

ملاحظه: الامر sudo في كل مره تكتبه للمره الاوله يطلب من كلمة المرور

الخاصه بالمستخدم بعد ذلك ينفذ لك الامر

ويمنحه مده محدده في حال لم تقم بكتابه sudo سوف يطلب منك ادخال كلمة المرور مره اخرى  
في المثال الموضح في الاسفل استخدمت الامر sudo لمرات عديده والمده الزمنيه بين كل امر لم تكن  
طويله لذلك كما هو موضح لم يطلب ادخال كلمة المرور الخاصه بالمستخدم وانما تم تنفيذ الامر بشكل  
مباشر

ملاحظه: عند كتابه كلمة المرور كنوع من الامان لا تظهر كلمة المرور ولا تظهر عدد الخانات

```
[wazuh-user@wazuh-server ~]$ sudo passwd wazuh-user
Changing password for user wazuh-user.
New password: ادخل كلمة المرور الجديدة
Retype new password: اعد ادخال كلمة المرور
passwd: all authentication tokens updated successfully.
[wazuh-user@wazuh-server ~]$
```

12

ملاحظه: تم وضع كلمة مرور افتراضيه للمستخدم Root

وهي "Wazuh" ويجب تغييرها لتأمين السيرفر

```
[root@wazuh-server ~]# sudo passwd root
Changing password for user root.
New password: 
Retype new password: 
passwd: all authentication tokens updated successfully.
[root@wazuh-server ~]#
```



ملاحظه يوجد اكثرا من اسم مستخدم وكلمة مرور  
افتراضيه تستطيع تسجيل الدخول بها  
سيتم تغييرها لاحقا للتأمين لوحة التحكم

للدخول لواجه الويب والوصول الى لوحة التحكم من خلال  
المتصفح قم بكتابه رقم الايبي الخاص بالسيرفر

"https://<ip address>"

كما هو موضح في الصورة رقم 13

لمعرفه كيف معرفه الايبي في الاسفل صورة رقم 14

## Access the Wazuh dashboard

Shortly after starting the VM, the Wazuh dashboard can be accessed from the web interface by using the following credentials:

URL: `https://<wazuh_server_ip>`  
user: admin  
password: admin

كلمة المرور واسم المستخدم  
للدخول من خلال واجه الويب

You can find `<wazuh_server_ip>` by typing the following command in the VM:

ip a

لمعرفه عنوان الايبي الخاص بالسيرفر





الآن سنقوم بتغيير كلمات المرور المستخدمين الخاصة بالدخول للوحة التحكم لتأمينها من خلال موجه الاوامر 'CMD' بأسستخدام بروتوكول "SSH" وذلك لسهولة النسخ واللصق يمكنك معرفه كيفيه الاتصال من خلال النظر للصورتين في الاعلى

رقم 10,11

سنقوم بـأستخدام سكريبت يساعدنا في عملية تغيير كلمات المرور ويمكن من خلاله تغيير جميع كلمات المرور الخاصة بلوحة التحكم دفعه واحده وانشاء كلمات مرور عشوائيه او تغيير كلمات المرور بشكل محدد



The screenshot shows the Wazuh documentation website. The top navigation bar includes links for Platform, Cloud, Services, Partners, Blog, and Company, with 'Version 4.3 (current)' selected. The main content area displays the 'Change the Wazuh indexer passwords' page under the 'Securing Wazuh' section of the User manual. The page contains instructions and a command-line example for changing indexer passwords.

**Change the Wazuh indexer passwords - Securing Wazuh**

User manual, installation and configuration guides for Wazuh

wazuh. docs.

Change the Wazuh indexer passwords - Securing Wazuh

Platform Cloud Services Partners Blog Company Version 4.3 (current)

Search 

Getting started

Quickstart

Installation guide

Installation alternatives

Upgrade guide

Migration guide

Wazuh Cloud service

User manual

Wazuh server administration

Certificates deployment

Edit on GitHub 

ON THIS PAGE

Change the Wazuh indexer passwords

Change the password for single user

Change the passwords for all users

Change the passwords using a formatted file

## Change the Wazuh indexer passwords

In this section we will show you how to change the passwords of the Wazuh indexer users to secure your installation.

We provide a script to simplify the process of changing passwords, start by downloading it:

```
# curl -so wazuh-passwords-tool.sh https://packages.wazuh.com/4.3/wazuh-passwords-tool.sh
```

The script allows changing the password for either a single user or all the users present on the `/usr/share/wazuh-indexer/plugins/opensearch-security/securityconfig/internal_users.yml` file. It also offers the option to change the password of more than one user at once, getting them from a formatted file.

## سنقوم بتحميل السكريت من خلال الامر التالي

`curl -so wazuh-passwords-tool.sh https://packages.wazuh.com/4.3/wazuh-passwords-tool.sh`

ثم نقوم بكتابه الامر "chmod +x wazuh-passwords-tool.sh"

لتغيير جميع كلمات مرور المستخدمين وانشاء كلمات مرور عشوائية قم باستخدام الامر

"`sudo ./wazuh-passwords-tool.sh -a`"

لتغييركلمة المرور لمستخدم واحد فقط

"`sudo ./wazuh-passwords-tool.sh -u - اسما المستخدم -p -كلمة المرور الجديدة`"

ملاحظه: في حال اردت تغييركلمة مرور بشكل محدد يرجى مراعاة انه لا يسمح

باستخدام جميع الرموز وانما يسمح بالرموز التالية \* . ? . + . -

ويجب ان تكون كلمة المرور بين 8 خانات الى 64 خانه ويجب ان تكون مكونه من احرف صغيره وكبيده ورموز وارقام

وتم تضليل الاخطاء باللون البرتقالي للتوضيح

```
wazuh-user@wazuh-server:~ [wazuh-user@wazuh-server ~]$ curl -so wazuh-passwords-tool.sh https://packages.wazuh.com/4.3/wazuh-passwords-tool.sh
[wazuh-user@wazuh-server ~]$ ls
wazuh-passwords-tool.sh
[wazuh-user@wazuh-server ~]$ chmod +x wazuh-passwords-tool.sh
[wazuh-user@wazuh-server ~]$ ls
wazuh-passwords-tool.sh
[wazuh-user@wazuh-server ~]$ sudo ./wazuh-passwords-tool.sh -a
23/08/2022 01:05:40 INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
23/08/2022 01:05:49 INFO: The password for user admin is G?nGto?h8.Z8eXC3obv0FTp*1.uAm5MA
23/08/2022 01:05:49 INFO: The password for user kibanaserver is *A.WOy*F+Ge07Q6zz*u0jNB1uAEnR2B.
23/08/2022 01:05:49 INFO: The password for user kibano is ImcE.c0e.C?3V8UtYRwUhdHJw6W7nQXF
23/08/2022 01:05:49 INFO: The password for user logstash is ?2biBU6nA6iFDhtc0UNTSfJGH1IxH6LO
23/08/2022 01:05:49 INFO: The password for user readall is YZNb+lc9wQ95epkSWW6uMc0.hHf1NdN+
23/08/2022 01:05:49 INFO: The password for user snapshotrestore is IZUs.6Ze6Qp.eDREF9JINphn1eYqK?no
23/08/2022 01:05:49 WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.
[wazuh-user@wazuh-server ~]$ sudo ./wazuh-passwords-tool.sh -u admin -p ShouldYouChange:) ✘
-bash: syntax error near unexpected token `)'
[wazuh-user@wazuh-server ~]$ sudo ./wazuh-passwords-tool.sh -u admin -p ShouldYouChange ✘
23/08/2022 01:09:05 ERROR: The password must have a length between 8 and 64 characters and contain at least one upper and lower case letter, a number and a symbol(.+?-).
[wazuh-user@wazuh-server ~]$ sudo ./wazuh-passwords-tool.sh -u admin -p ShouldYouChange.123 ✓
23/08/2022 01:09:27 INFO: Generating password hash
```

15

كما هو موضح تمت طباعة كل اسم ويقابلها  
كلمة المرور التي تم انشائها بشكل عشوائي



لتغيير جميع كلمات المرور بشكل عشوائي وطباعتها في ملف قم بكتابه الامر التالي

"sudo ./wazuh-passwords-tool.sh -a -gf"

```
[wazuh-user@wazuh-server ~]$ sudo ./wazuh-passwords-tool.sh -a -gf passwords.txt
24/08/2022 22:30:58 INFO: Wazuh API admin credentials not provided, Wazuh API passwords not changed.
24/08/2022 22:31:10 INFO: The password for user admin is w.DMSZuDptjNCT49R9bmegrm5W9AMV5+
24/08/2022 22:31:10 INFO: The password for user kibanaserver is L0?xD0G5kxdW.2FIjiTfiID+7D+LIH7y
24/08/2022 22:31:10 INFO: The password for user kibana is Rok7PWRZW2Pc?EWsleYFj9oZyL3Rf1gW
24/08/2022 22:31:10 INFO: The password for user logstash is t0HWFCChb5*aQP*d5y?EaiEAAMAjshkY
24/08/2022 22:31:10 INFO: The password for user readall is BBoS7ZWGbTqfKmyh?ucSKt4JcHdK.SQ
24/08/2022 22:31:10 INFO: The password for user snapshotrestore is xjZLGb0rMYEs.1i2HPn3.wV5jvhgbo9X
24/08/2022 22:31:10 WARNING: Wazuh indexer passwords changed. Remember to update the password in the Wazuh dashboard and Filebeat nodes if necessary, and restart the services.
[wazuh-user@wazuh-server ~]$ ls
passwords.txt  wazuh-passwords-tool.sh
[wazuh-user@wazuh-server ~]$ cat passwords.txt
cat: passwords.txt: Permission denied
[wazuh-user@wazuh-server ~]$ sudo cat passwords.txt
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
indexer_username: 'admin'
indexer_password: 'w.DMSZuDptjNCT49R9bmegrm5W9AMV5+'
# Wazuh dashboard user for establishing the connection with Wazuh indexer
indexer_username: 'kibanaserver'
indexer_password: 'L0?xD0G5kxdW.2FIjiTfiID+7D+LIH7y'
```

طباعة الملف الذي تم انشائه ويحتوي على كلمات المرور واسماء المستخدمين ◀

تم اضافة كلمات المرور واسم المستخدم داخل الملف بالطريقة التالية ←



يمكنك نسخ اسم المستخدم وكلمة المرور من خلال الملف الذي تم انشائه وتسجيل الدخول الى لوحة التحكم من خلال المتصفح كما تم الشرح مسبقا في الاعلى في الصورة رقم 13



DEFENSE

بعد تسجيل الدخول ستظهر لوحة التحكم بالشكل التالي  
نقوم بالنقر على "Add agent" لاستعانته نظام تشغيل على السيرفر

Total agents: 0      Active agents: 0      Disconnected agents: 0      Pending agents: 0      Never connected agents: 0

No agents were added to this manager. [Add agent](#)

**18**

#### SECURITY INFORMATION MANAGEMENT

Security events  
Browse through your security alerts, identifying issues and threats in your environment

Integrity monitoring  
Alerts related to file changes, including permissions, content, ownership and attributes.

#### AUDITING AND POLICY MONITORING

Policy monitoring  
Verify that your systems are configured according to your security policies baseline.

System auditing  
Audit users behavior, monitoring command execution and alerting on access to critical files.

#### THREAT DETECTION AND RESPONSE

Vulnerabilities  
Discover what applications in your environment are affected by well-known vulnerabilities.

MITRE ATT&CK  
Security events from the knowledge base of adversary tactics and techniques based on real-world observations

#### REGULATORY COMPLIANCE

PCI DSS  
Global security standard for entities that process, store or transmit payment cardholder data.

NIST 800-53  
National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.



Deploy a new agent

قم ب اختيار نظام التشغيل الذي تريد اضافته

1 Choose the Operating system

Red Hat / CentOS   Debian / Ubuntu   Windows **Windows**   MacOS

2 Wazuh server address

This is the address the agent uses to communicate with the Wazuh server. It can be an IP address or a fully qualified domain name (FQDN).

192.168.1.130   قم ب اضافة عنوان الايبى الخاص بالسيرفر

3 Assign the agent to a group

قم ب تحديد المجموعة التي سوف تستعينف عليها الجهاز في حال كان لديك اجهزه كثير داخل الشبكة

Select one or more existing groups

Default  "Default" 

4 Install and enroll the agent

You can use this command to install and enroll the Wazuh agent in one or more hosts.

If the installer finds another Wazuh agent in the system, it will upgrade it preserving the configuration.

تثبيت "Wazuh Agent" على نظام التشغيل يقوم بنسخ الامر التالي وكل نظام له طريقه مختلف وتحدد الطريقه حسب اختيارنا السابق في حالتنا قمنا ب اختيار "Windows" وهذا هو الامر الخاص بنظام التشغيل ويندوز

Keep in mind you need to run this command in a Windows PowerShell terminal.

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.7-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.7.msi; msieexec.exe /i ${env:tmp}\wazuh-agent-4.3.7.msi /q WAZUH_MANAGER='192.168.1.130' WAZUH_REGISTRATION_SERVER='192.168.1.130' WAZUH_AGENT_GROUP='default'
```

نقوم بنسخ الامر ومن ثم نقوم بتشغيل "Powershell" كمسؤول ونلصق الامر لتنفيذه كما سوف يتم توضيحة انظر الى صوره رقم 21

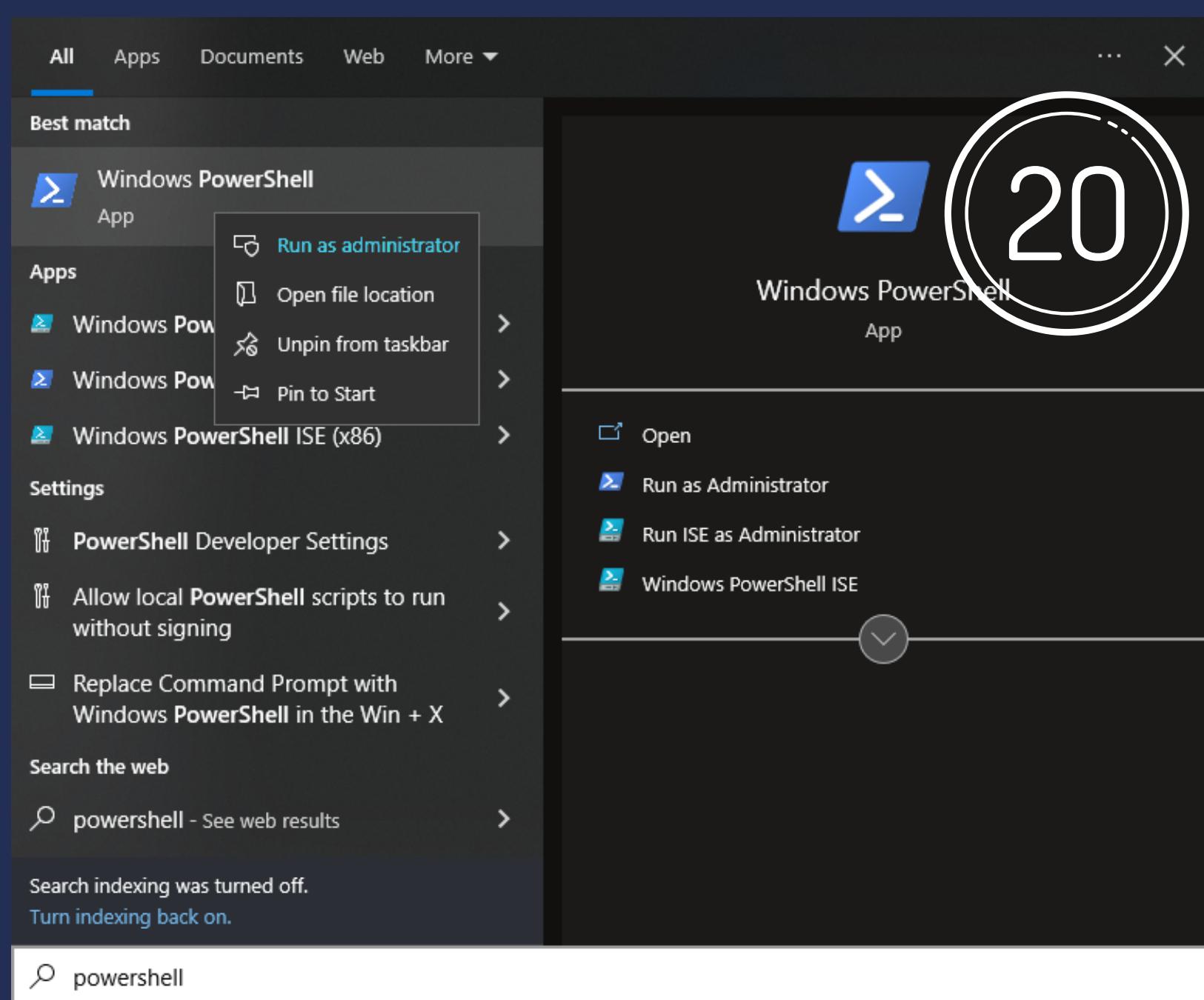
5 Start the agent

NET START WazuhSVC

بعد تثبيت "Wazuh Agent" نقوم بكتابه هذا الامر لتشغيل الخدمة وتلقى التنبيهات على السيرفر



19



```
Administrator: Windows PowerShell
PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.7-1.msi -OutFile ${env:tmp}\wazuh-agent-4.3.7.msi; msiexec.exe /i ${env:tmp}\wazuh-agent-4.3.7.msi /q WAZUH_MANAGER='192.168.1.130' WAZUH_REGISTRATION_SERVER='192.168.1.130' WAZUH_AGENT_GROUP='default'
PS C:\Windows\system32> NET START WazuhSvc
The Wazuh service was started successfully.
PS C:\Windows\system32>
```

A screenshot of a Windows PowerShell window running as Administrator. The title bar says "Administrator: Windows PowerShell". The command entered is: "Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.3.7-1.msi -OutFile \${env:tmp}\wazuh-agent-4.3.7.msi; msiexec.exe /i \${env:tmp}\wazuh-agent-4.3.7.msi /q WAZUH\_MANAGER='192.168.1.130' WAZUH\_REGISTRATION\_SERVER='192.168.1.130' WAZUH\_AGENT\_GROUP='default'". The output shows the command was successful. A large circular badge with the number "21" is overlaid on the bottom right of the window. In the bottom left corner of the image, there is a small watermark or icon containing binary code (01010101 01010100 01010101 01010100).

قم بالرجوع الى الصفحة الرئيسية في لوحة التحكم وقم بتحديث الصفحة وسوف يظهر لك انه تم اضافة جهاز الى السيرفر

wazuh. / Modules

يدل على الاجهزه المعنافية على السيرفر

Total agents  
1

Active agents  
1

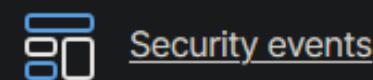
Disconnected agents  
0

Pending agents  
0

Never connected agents  
0

يدل على الاجهزه النشطة على السيرفر

#### SECURITY INFORMATION MANAGEMENT



##### Security events

Browse through your security alerts, identifying issues and threats in your environment



##### Integrity monitoring

Alerts related to file changes, including permissions, content, ownership and attributes.



##### Policy monitoring

Verify that your systems are configured according to your security policies baseline.



##### System auditing

Audit users behavior, monitoring command execution and alerting on access to critical files.

#### THREAT DETECTION AND RESPONSE



##### Vulnerabilities

Discover what applications in your environment are affected by well-known vulnerabilities.



##### MITRE ATT&CK

Security events from the knowledge base of adversary tactics and techniques based on real-world observations



##### PCI DSS

Global security standard for entities that process, store or transmit payment cardholder data.



##### NIST 800-53

National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.



لتحديث السيرفر تقوم بكتابه الامر 'sudo su' او لا ومن ثم كلمه مرور المستخدم  
للوصول للمستخدم المسؤول لتتمكن من تحديث موارد النظام بعد ذلك تقوم  
بكتابه الامر التالي 'yum update'

```
[root@wazuh-server wazuh-user]# yum update
Loaded plugins: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.clarkson.edu
 * extras: packages.oit.ncsu.edu
 * updates: mirror.cogentco.com
Resolving Dependencies
--> Running transaction check
--> Package kernel.x86_64 0:3.10.0-1160.76.1.el7 will be installed
--> Package kernel-devel.x86_64 0:3.10.0-1160.76.1.el7 will be installed
--> Package kernel-headers.x86_64 0:3.10.0-1160.71.1.el7 will be updated
--> Package kernel-headers.x86_64 0:3.10.0-1160.76.1.el7 will be an update
--> Package kernel-tools.x86_64 0:3.10.0-1160.71.1.el7 will be updated
--> Package kernel-tools.x86_64 0:3.10.0-1160.76.1.el7 will be an update
--> Package kernel-tools-libs.x86_64 0:3.10.0-1160.71.1.el7 will be updated
--> Package kernel-tools-libs.x86_64 0:3.10.0-1160.76.1.el7 will be an update
--> Package python-perf.x86_64 0:3.10.0-1160.71.1.el7 will be updated
--> Package python-perf.x86_64 0:3.10.0-1160.76.1.el7 will be an update
--> Package wazuh-dashboard.x86_64 0:4.3.6-1 will be updated
--> Package wazuh-dashboard.x86_64 0:4.3.7-1 will be an update
--> Package wazuh-indexer.x86_64 0:4.3.6-1 will be updated
--> Package wazuh-indexer.x86_64 0:4.3.7-1 will be an update
--> Finished Dependency Resolution

Dependencies Resolved
=====
マسوف يتم تثبيته
```

Package	Arch	Version	Repository	Size
Installing:				
kernel	x86_64	3.10.0-1160.76.1.el7	updates	50 M
kernel-devel	x86_64	3.10.0-1160.76.1.el7	updates	18 M
Updating:				
kernel-headers	x86_64	3.10.0-1160.76.1.el7	updates	9.1 M
kernel-tools	x86_64	3.10.0-1160.76.1.el7	updates	8.2 M
kernel-tools-libs	x86_64	3.10.0-1160.76.1.el7	updates	8.1 M
python-perf	x86_64	3.10.0-1160.76.1.el7	updates	8.2 M
wazuh-dashboard	x86_64	4.3.7-1	wazuh	151 M
wazuh-indexer	x86_64	4.3.7-1	wazuh	361 M

```
Transaction Summary
=====
Install 2 Packages
Upgrade 6 Packages

Total download size: 614 M
Is this ok [y/d/N]: y
```

قم بكتابه حرف "y" لتبعد عملية التحديث

22

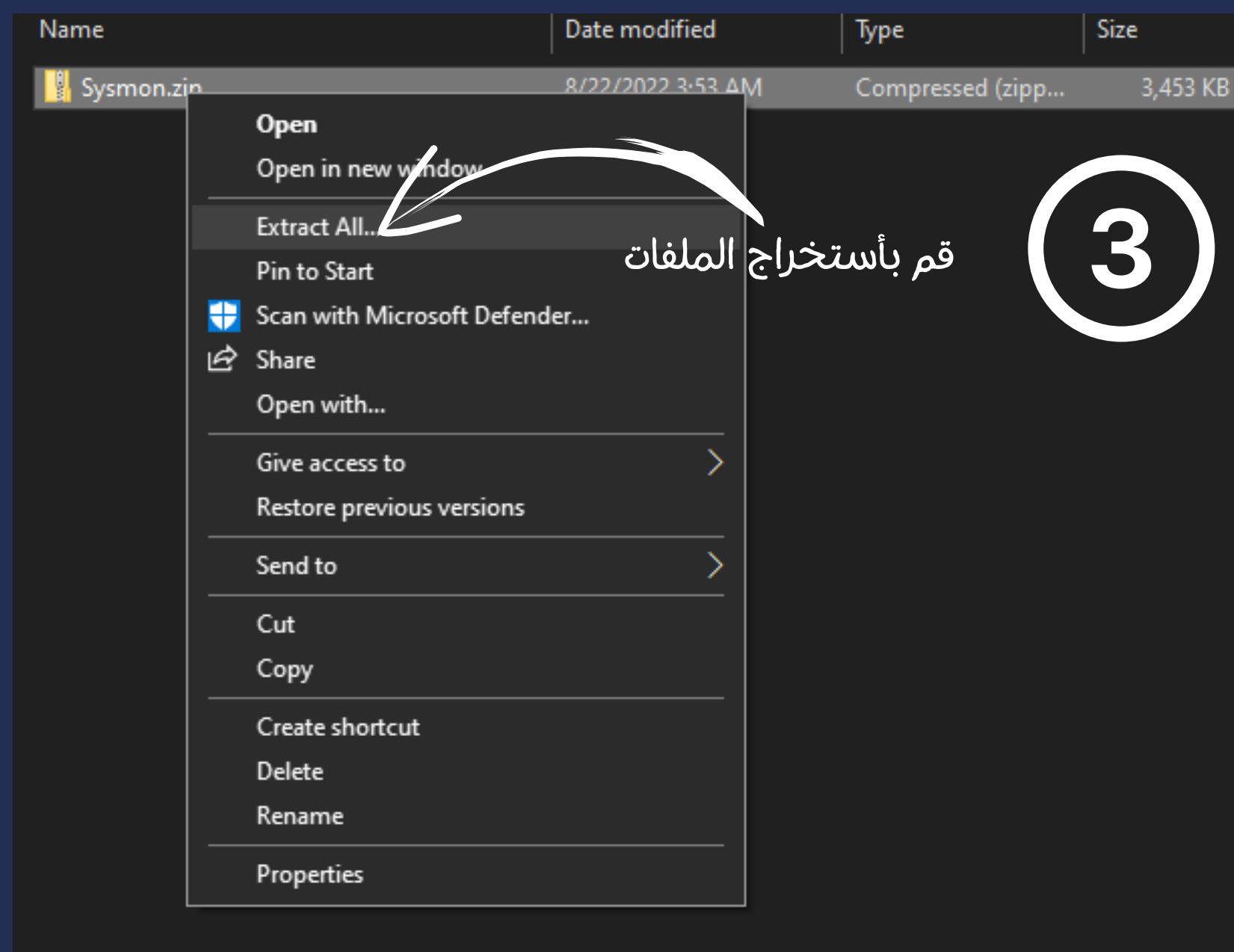
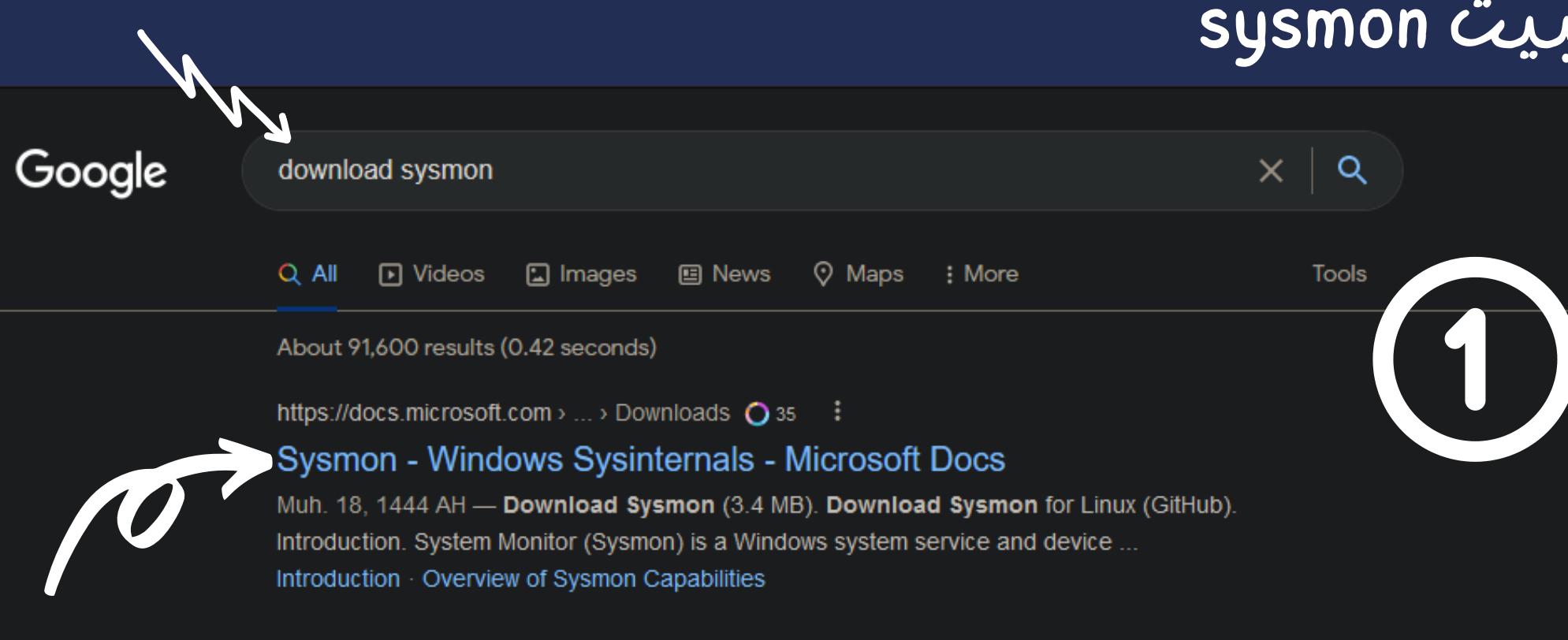
```
[root@wazuh-server wazuh-user]
(8/8): wazuh-indexer-4.3.7-1.x86_64.rpm
-----
Total
Running transaction check
Running transaction test
Transaction test succeeded
Running transaction
  Updating : kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64
  Updating : kernel-tools-3.10.0-1160.76.1.el7.x86_64
  Installing : kernel-3.10.0-1160.76.1.el7.x86_64
  Updating : python-perf-3.10.0-1160.76.1.el7.x86_64
  Installing : kernel-devel-3.10.0-1160.76.1.el7.x86_64
  Updating : kernel-headers-3.10.0-1160.76.1.el7.x86_64
  Updating : wazuh-indexer-4.3.7-1.x86_64
  Updating : wazuh-dashboard-4.3.7-1.x86_64
  Cleanup : kernel-headers-3.10.0-1160.71.1.el7.x86_64
  Cleanup : wazuh-indexer-4.3.6-1.x86_64
  Cleanup : wazuh-dashboard-4.3.6-1.x86_64
  Cleanup : kernel-tools-3.10.0-1160.71.1.el7.x86_64
  Cleanup : kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64
  Cleanup : python-perf-3.10.0-1160.71.1.el7.x86_64
VirtualBox Guest Additions: Building the modules for kernel
3.10.0-1160.76.1.el7.x86_64.
Starting wazuh-indexer service... OK
  Verifying : wazuh-dashboard-4.3.7-1.x86_64
  Verifying : wazuh-indexer-4.3.7-1.x86_64
  Verifying : kernel-headers-3.10.0-1160.76.1.el7.x86_64
  Verifying : kernel-devel-3.10.0-1160.76.1.el7.x86_64
  Verifying : kernel-tools-3.10.0-1160.76.1.el7.x86_64
  Verifying : kernel-tools-libs-3.10.0-1160.76.1.el7.x86_64
  Verifying : python-perf-3.10.0-1160.76.1.el7.x86_64
  Verifying : kernel-3.10.0-1160.76.1.el7.x86_64
  Verifying : kernel-tools-libs-3.10.0-1160.71.1.el7.x86_64
  Verifying : wazuh-indexer-4.3.6-1.x86_64
  Verifying : python-perf-3.10.0-1160.71.1.el7.x86_64
  Verifying : wazuh-dashboard-4.3.6-1.x86_64
  Verifying : kernel-headers-3.10.0-1160.71.1.el7.x86_64
  Verifying : kernel-tools-3.10.0-1160.71.1.el7.x86_64
  Installed: kernel.x86_64 0:3.10.0-1160.76.1.el7
  Updated: kernel-headers.x86_64 0:3.10.0-1160.76.1.el7
  Updated: kernel-tools.x86_64 0:3.10.0-1160.76.1.el7
  Updated: python-perf.x86_64 0:3.10.0-1160.76.1.el7
  Updated: wazuh-dashboard.x86_64 0:4.3.7-1
Complete!
[root@wazuh-server wazuh-user]#
[root@wazuh-server wazuh-user]# clear
[root@wazuh-server wazuh-user]# reboot
Connection to 192.168.1.130 closed by remote host.
Connection to 192.168.1.130 closed.
```

بعد انتهاء عملية التحديث قم باعاده تشغيل 'reboot' السيرفر باستخدام الامر

23



# شرح اعداد و تثبيت sysmon



## Sysmon

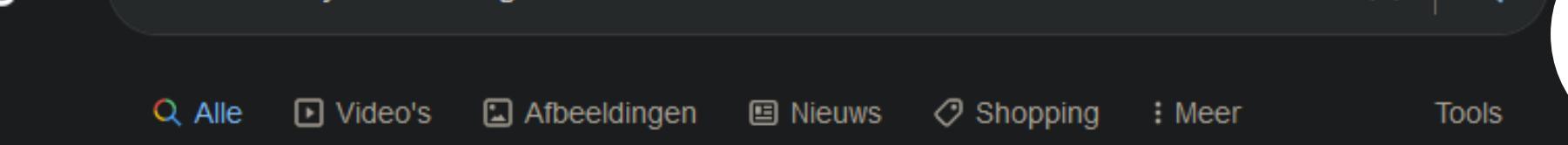
هي اداة من سلسة ادوات Sysinternals وهي الان تابعة لشركة Microsoft تقوم الاداة بتسجيل وتحليل نشاط النظام لتحديد انشطة العناصر او الغير طبيعية ومن خلال تثبيت هذه الاداة وارسال مخرجاتها الى سيرفر Wazuh فسوف نزيد من قدرة تحليل السجل "Logs" لدينا وبالتالي زيادة احتمالية اكتشاف التهديدات .



# Sysmon Config

وهو ملف بصيغة XML يتحكم في كيفية عمل sysmon ويمكنك انشاء ملف تكوين خاص بك بحيث تحكم فيما يتم تسجيله او استبعاده في حالتنا سوف نقوم بتحميل ملف جاهز

جاهز



Google

download sysmon config

X | 

Alle Video's Afbeeldingen Nieuws Shopping Meer Tools

Ongeveer 51.900 resultaten (0,26 seconden)

<https://github.com/sysmon-config> 4 Vertaal deze pagina

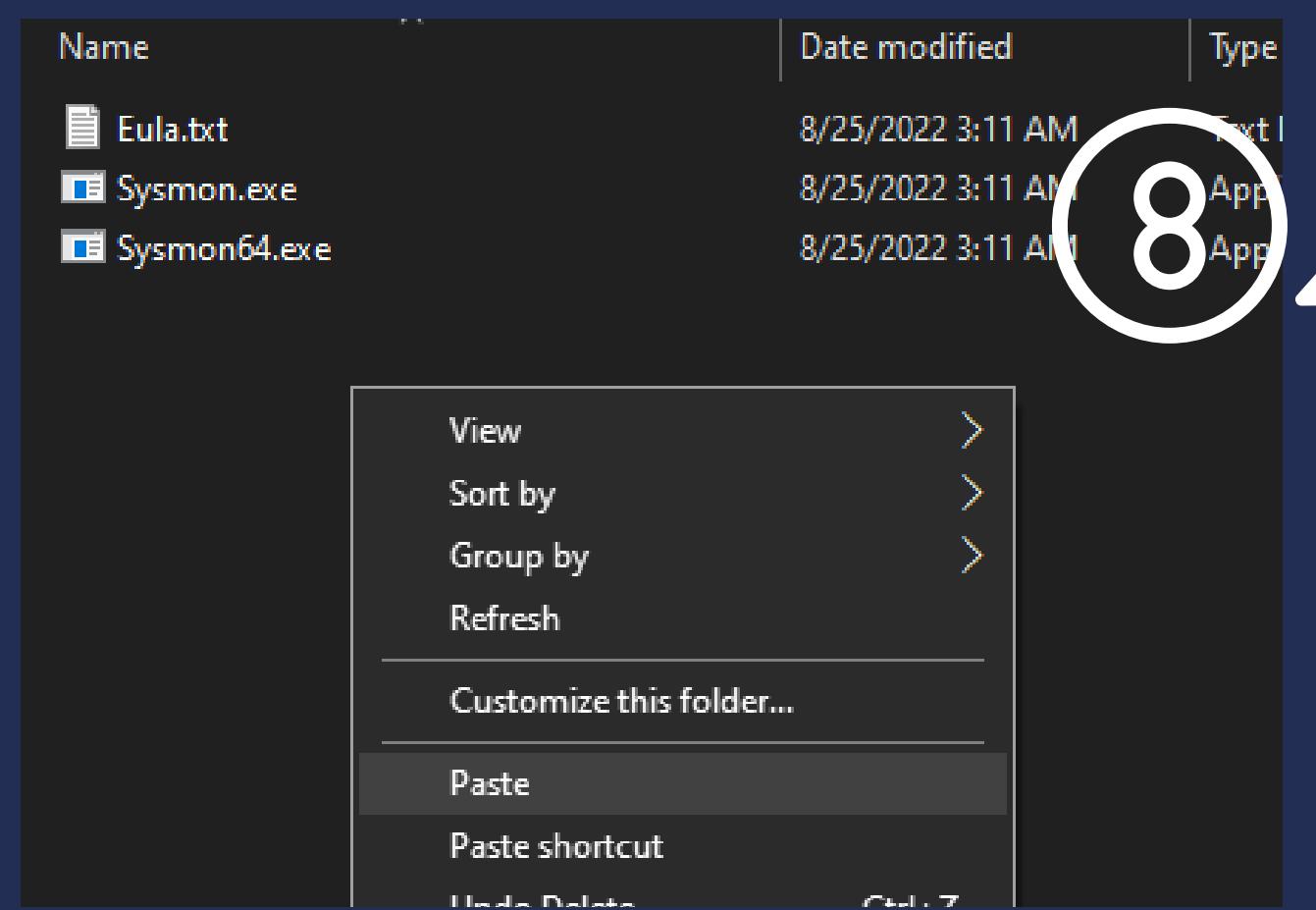
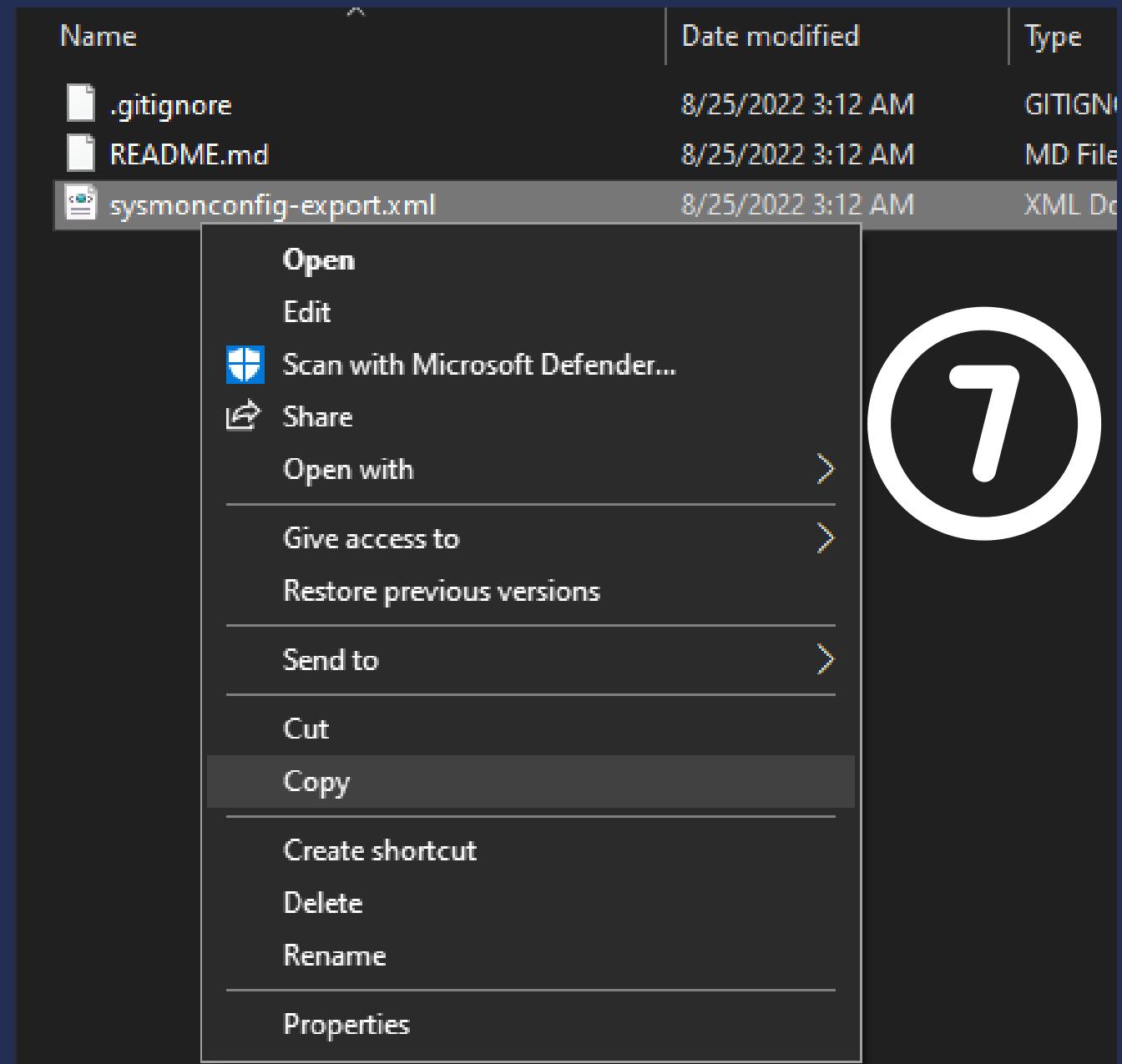
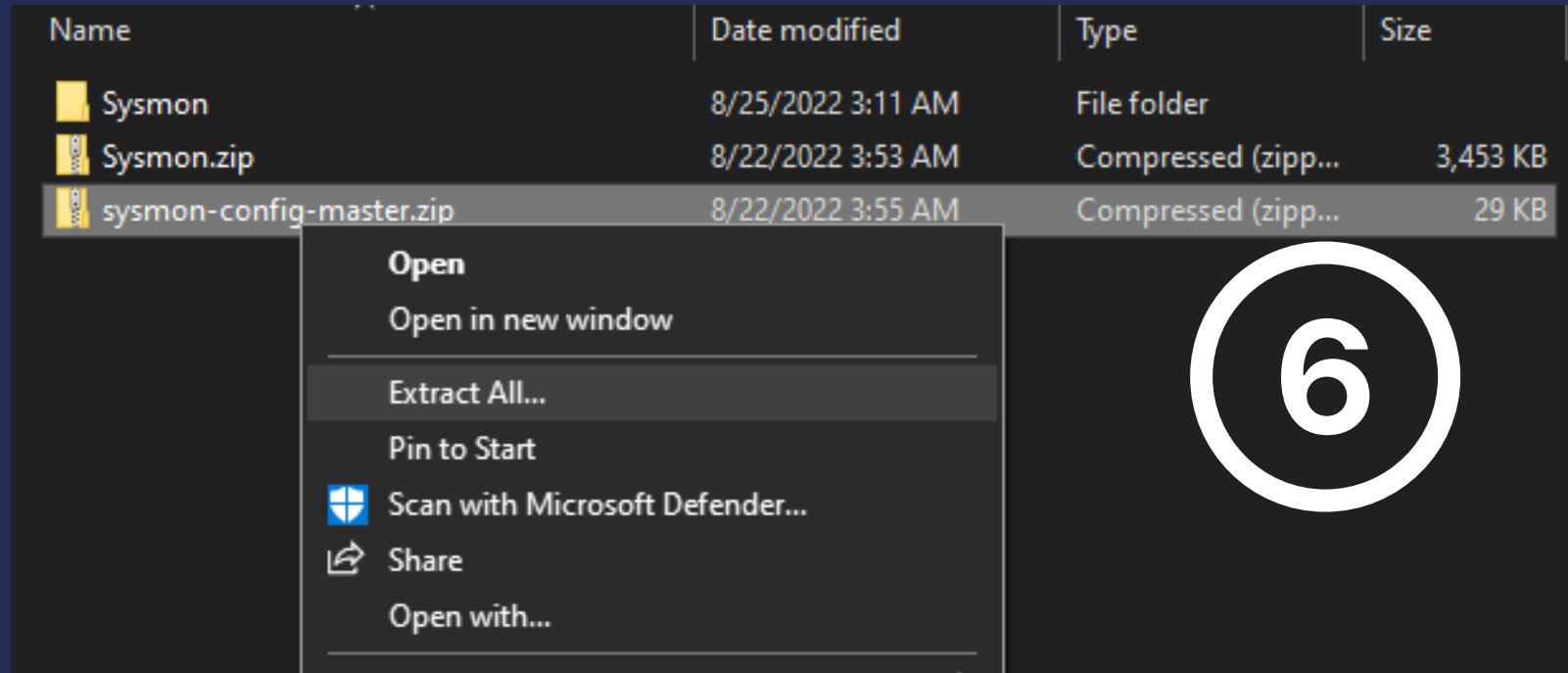
**A Sysmon configuration file for everybody to fork - GitHub**

This is a Microsoft Sysinternals **Sysmon configuration** file template with default high-quality event tracing. The file should function as a great starting ...

Issues 40 · README.md · Pull requests 22

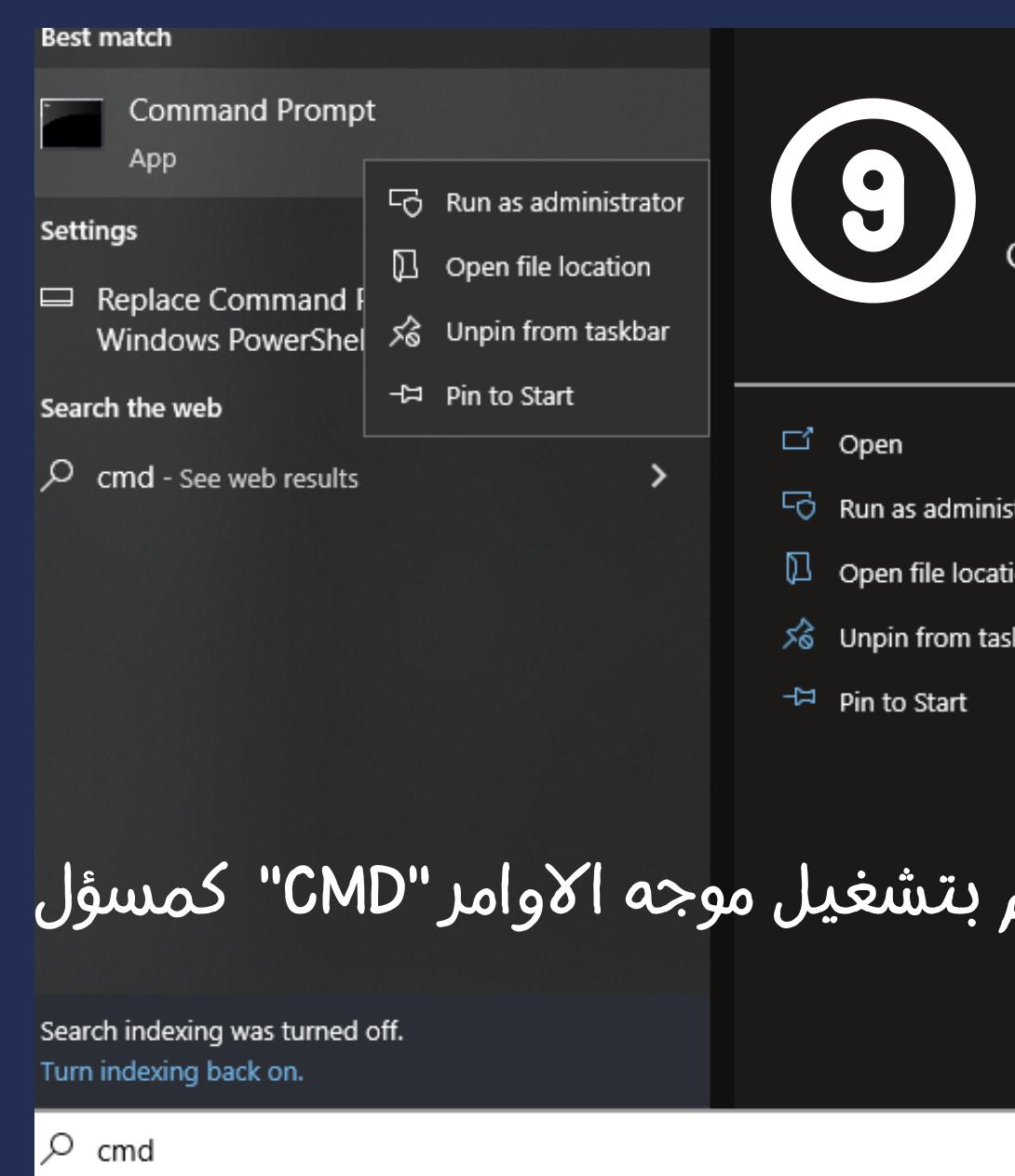
The image shows a GitHub repository page for 'sysmon-config'. At the top right, there is a large white circle containing the number '5'. A white arrow points from the bottom left towards this circle. Below the circle, the word 'Code' is highlighted with a green background and a white border. The repository details include: 'Code' (highlighted), 'Issues 40', 'Pull requests 22', 'Actions', 'Projects', 'Wiki', 'Security', 'Insights', 'master branch', '1 branch', '0 tags', and a 'Clone' menu with options for 'HTTPS' and 'GitHub CLI'. The URL listed is <https://github.com/SwiftOnSecurity/sysmon-config>. The repository description is: 'Sysmon configuration file template with default high-quality event tracing'. It features labels for 'windows', 'monitoring', 'logging', 'sysmon', 'threat-hunting', 'threatintel', 'netsec', and 'sysinternals'. Statistics shown are: '3.7k stars', '348 watching', and '1.4k forks'. The repository title is 'sysmon-config | A Sysmon configuration file for everybody to fork'. The main text area states: 'This is a Microsoft Sysinternals Sysmon configuration file template with default high-quality event tracing. The file should function as a great starting point for system change monitoring in a self-contained and accessible package. This configuration and results should give you a good idea of what's possible for Sysmon. Note that this does not track things like authentication and other Windows events that are also vital for incident investigation.'

بعد ذلك قم بـاستخراج الملفات ونسخ الملف  
**"sysmonconfig-export.xml"**  
 كما هو موضح في الصورة رقم 7



بعد ذلك قم بـلصق الملف الذي تم نسخه  
 الى المجلد الذي يحتوي على اداة sysmon  
 كما هو موضح في الصورة رقم 8

قم بنسخ مسار الملف الذي يحتوي  
اداة sysmon وملف التكوين sysmonconfig



قم بتشغيل موجه الاوامر "CMD" كمسؤول

Search indexing was turned off.  
Turn indexing back on.

cmd



Administrator: Command Prompt

```
C:\Windows\system32>cd C:\Users\{User}\Desktop\{Folder}\Sysmon
C:\Users\{User}\Desktop\{Folder}\Sysmon>sysmon64.exe -accepteula -i sysmonconfig-export.xml
```

System Monitor v14.0 - System activity monitor  
By Mark Russinovich and Thomas Garnier  
Copyright (C) 2014-2022 Microsoft Corporation  
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.  
Sysinternals - www.sysinternals.com

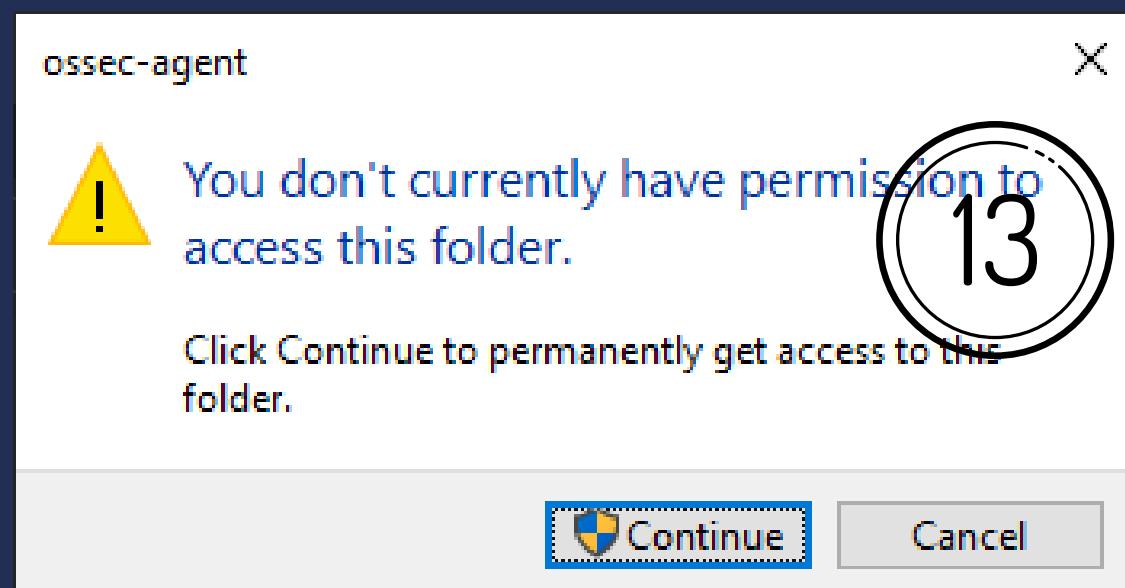
Loading configuration file with schema version 4.50  
Sysmon schema version: 4.82  
Configuration file validated.  
Sysmon64 installed.  
SysmonDrv installed.  
Starting SysmonDrv.  
SysmonDrv started.  
Starting Sysmon64.  
Sysmon64 started.

قم بكتابه هذا امر للتنبيت اداة sysmon64.exe -accepteula -i sysmonconfig-export.xml

11

# الآن سوف نقوم باعداد اعميل wazuh لاستقبال ماسوف يتم تسجيله من خلال sysmon

قم بالذهاب الى هذا المسار وهو المكان الذي تم تثبيت Wazuh agent داخله " القرص C \ البرامج والملفات (x86) \ اسم الملف الذي يحتويه ossec-agent" قد يختلف المسار باختلاف مكان التثبيت حاول الوصول الى الملف وسوف تظهر نافذة كما هو موضح في الصورة رقم 13 انقر على متابعة "Continue" وسوف تظهر نافذة كما هو موضح في الصورة رقم 14 انقر على متابعة "Continue"



This PC > Local Disk (C:) > Program Files (x86) > ossec-agent			
Name	Date modified	Type	Size
wodles	8/25/2022 2:56 AM	File folder	
.agent_info	8/25/2022 2:57 AM	AGENT_INFO File	1 KB
agent-auth.exe	8/19/2022 10:08 AM	Application	985 KB
agent-auth.exe.manifest	8/19/2022 7:51 AM	MANIFEST File	1 KB
client.keys	8/25/2022 2:57 AM	KEYS File	1 KB
dbsync.dll	8/19/2022 8:02 AM	Application exten...	1,294 KB
help.txt	8/19/2022 8:02 AM	Text Document	2 KB
internal_options.conf	8/19/2022 8:02 AM	CONF File	14 KB
libgcc_s_sjlj-1.dll	8/19/2022 8:01 AM	Application exten...	1,090 KB
libwazuhext.dll	8/19/2022 8:01 AM	Application exten...	5,923 KB
libwazuhshared.dll	8/19/2022 8:02 AM	Application exten...	822 KB
libwinpthread-1.dll	8/19/2022 8:01 AM	Application exten...	522 KB
LICENSE.txt	8/19/2022 8:02 AM	Text Document	25 KB
local_internal_options.conf	8/19/2022 8:02 AM	CONF File	1 KB
manage_agents.exe	8/19/2022 10:08 AM	Application	982 KB
ossec.conf	8/25/2022 2:56 AM	CONF File	10 KB
ossec.log	8/25/2022 2:58 AM	Text Document	32 KB
profile.template	8/19/2022 7:51 AM	TEMPLATE File	1 KB
REVISION	8/19/2022 8:02 AM	File	1 KB

14



بعد ذلك ابحث عن ملف باسم "ossec.conf" وقم بفتحه  
باستخدام المفكرة او اي برنامج يستخدم لتحرير النصوص .....

بعد الوصول الى الملف كما هو موضح في الصورة رقم 14  
قم بـأضافة مايلي مع مراعاة مكان الاضافة

<localfile>

location>Microsoft-Windows->

<Sysmon/Operational</location>

<log\_format>eventchannel</log\_format>

<localfile/>

يرجى مراعاة تنسيق الملف  
قم بـأضافة مسافتين هنا

اربع مسافات

اربع مسافات

مسافتين

```

<!-- Log analysis -->
<localfile>
    <location>Application</location>
    <log_format>eventchannel</log_format>
</localfile>

<localfile>
    <location>Security</location>
    <log_format>eventchannel</log_format>
    <query>Event/System[EventID != 5145 and EventID != 5156 and EventID != 5447 and
        EventID != 4656 and EventID != 4658 and EventID != 4663 and EventID != 4660 and
        EventID != 4670 and EventID != 4690 and EventID != 4703 and EventID != 4907 and
        EventID != 5152 and EventID != 5157]</query>
</localfile>

<localfile>
    <location>System</location>
    <log_format>eventchannel</log_format>
</localfile>

<localfile>
    <location>active-response\active-responses.log</location>
    <log_format>syslog</log_format>
</localfile>

<localfile>
    ><location>Microsoft-Windows-Sysmon/Operational</location>
    ><log_format>eventchannel</log_format>
    ></localfile>

<!-- Policy monitoring --> ←———— قم بـأضافة النص فوق هذا السطر تحديداً
<rootcheck>
    <disabled>no</disabled>
    <windows_apps>./shared/win_applications_rcl.txt</windows_apps>
    <windows_malware>./shared/win_malware_rcl.txt</windows_malware>
</rootcheck>

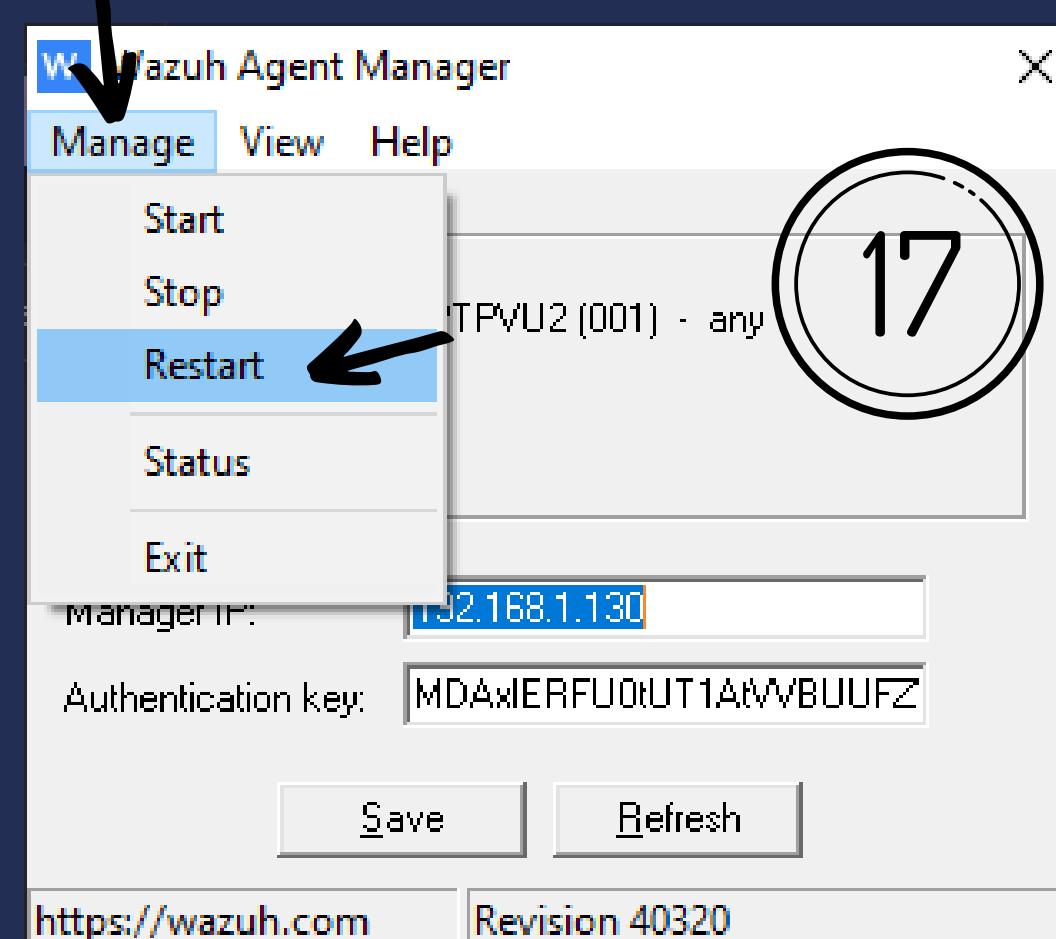
<!-- Security Configuration Assessment -->
<sca>
    <enabled>yes</enabled>
    <scan_on_start>yes</scan_on_start>
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
    .
    .
    .

```



بعد ذلك نقوم بالرجوع للملف الذي يحتوي  
كما تم توضيحة سابقا في الصوره رقم 12

 C:\Program Files (x86)\ossec-agent\



-agent

Share View

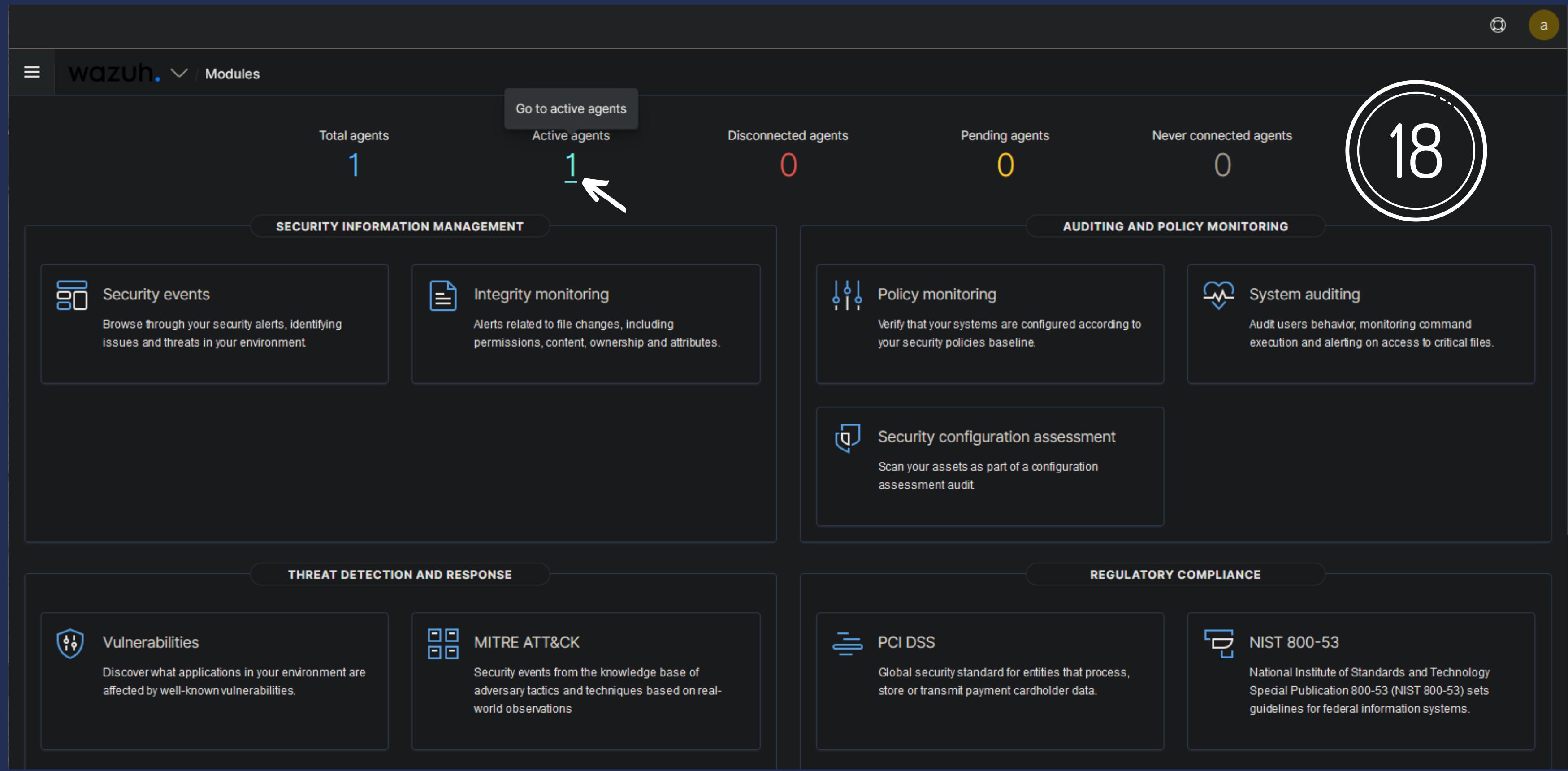
This PC > Local Disk (C:) > Program Files (x86) > ossec-agent >

Name	Date modified	Type	Size
rsync.dll	8/19/2022 8:02 AM	Application exten...	1,167 KB
syscollector.dll	8/19/2022 8:02 AM	Application exten...	1,328 KB
sysinfo.dll	8/19/2022 8:02 AM	Application exten...	1,255 KB
VERSION	8/19/2022 8:02 AM	File	1 KB
vista_sec.txt	8/19/2022 7:51 AM	Text Document	92 KB
wazuh-agent.exe	8/19/2022 10:08 AM	Application	1,883 KB
wazuh-agent.state	8/25/2022 3:31 AM	STATE File	1 KB
wazuh-logcollector.state	8/25/2022 3:30 AM	STATE File	2 KB
win32ui.exe	8/19/2022 10:08 AM	Application	912 KB
win32ui.exe.manifest	8/19/2022 7:51 AM	MANIFEST File	1 KB
wpk_root.pem	8/19/2022 7:51 AM	PEM File	2 KB

بعد ذلك نقوم بتشغيل 'Win32ui.exe'  
ونقوم بعمل اعاده تشغيل لـ Wazuh Agent كما هو موضح  
في الصورة رقم 17



قم بالرجوع للوحة التحكم الخاصه بسيرفر wazuh من خلال المتصفح ومن ثم العملاء النشطين واختار الجهاز المستعاف كما هو موضح صوره رقم 19 لترى التنبيهات والخ..



The screenshot shows the Wazuh web interface with the following details:

- Header:** Shows "wazuh. Modules".
- Top Metrics:**
  - Total agents: 1
  - Active agents: 1 (highlighted with a white arrow)
  - Disconnected agents: 0
  - Pending agents: 0
  - Never connected agents: 0
- Large Number:** A large circular badge on the right side displays the number 18.
- Modules:**
  - SECURITY INFORMATION MANAGEMENT:**
    - Security events: Browse through your security alerts, identifying issues and threats in your environment.
    - Integrity monitoring: Alerts related to file changes, including permissions, content, ownership and attributes.
  - AUDITING AND POLICY MONITORING:**
    - Policy monitoring: Verify that your systems are configured according to your security policies baseline.
    - System auditing: Audit users behavior, monitoring command execution and alerting on access to critical files.
  - THREAT DETECTION AND RESPONSE:**
    - Vulnerabilities: Discover what applications in your environment are affected by well-known vulnerabilities.
    - MITRE ATT&CK: Security events from the knowledge base of adversary tactics and techniques based on real-world observations.
  - REGULATORY COMPLIANCE:**
    - PCI DSS: Global security standard for entities that process, store or transmit payment cardholder data.
    - NIST 800-53: National Institute of Standards and Technology Special Publication 800-53 (NIST 800-53) sets guidelines for federal information systems.

wazuh. / Agents

### STATUS



- Active (1)
- Disconnected (0)
- Pending (0)
- Never connected (0)

### DETAILS

Active	Disconnected	Pending	Never connected	Agents coverage
<b>1</b>	<b>0</b>	<b>0</b>	<b>0</b>	<b>100.00%</b>

Last registered agent  
**DESKTOP-UPTPVU2**

### EVOLUTION

Last 24 hours

**19**

No results found

[status=active](#) × Filter or search agent [Refresh](#)

### Agents (1)

ID ↑	Name	IP	Group(s)	OS	Cluster node	Version	Registration date	Last keep alive	Status	Actions
001	DESKTOP-UPTPVU2	192.168.1.165	default	 Microsoft Windows 10 P...	node01	v4.3.7	Aug 25, 2022 @ ...	Aug 25, 2022 @ ...	● active	





# اكتشف واستمتع



wazuh. / Agents / DESKTOP-UPTPVU2

DESKTOP-UPTPVU2 Security events Integrity monitoring SCA Vulnerabilities MITRE ATT&CK More... Inventory data Stats Configuration

ID 001	Status active	IP 192.168.1.165	Version Wazuh v4.3.7	Groups default	Operating system Microsoft Windows 10 Pr...	Cluster node node01	Registration date Aug 25, 2022 @ 02:57:24.000	Last keep alive Aug 25, 2022 @ 03:35:46.000
-----------	------------------	---------------------	-------------------------	-------------------	--	------------------------	--	--

Last 24 hours

MITRE

Top Tactics

- Defense Evasion
- Persistence
- Privilege Escalation
- Initial Access
- Impact

Compliance

PCI DSS

- 2.2 (470)
- 2.2.5 (53)
- 4.1 (44)
- 10.6.1 (34)
- 7.1 (24)

FIM: Recent events

Time ↓	Path	Action	Rule description	Rule Level	Rule ID
No recent events					

Events count evolution

ملاحظة: ليس بالضرورة أن تكون جميع التنبية دليل على وجود نشاط ضار

SCA: Last scan

Benchmark for Windows audit sca\_win\_audit

This document provides a way of ensuring the security of the Windows systems.

Pass 22	Fail 10	Total checks 71	Score 68%
------------	------------	--------------------	--------------

Start time: Aug 25, 2022 @ 03:32:52.000 Duration: < 1s

10100101  
010001001  
10101010