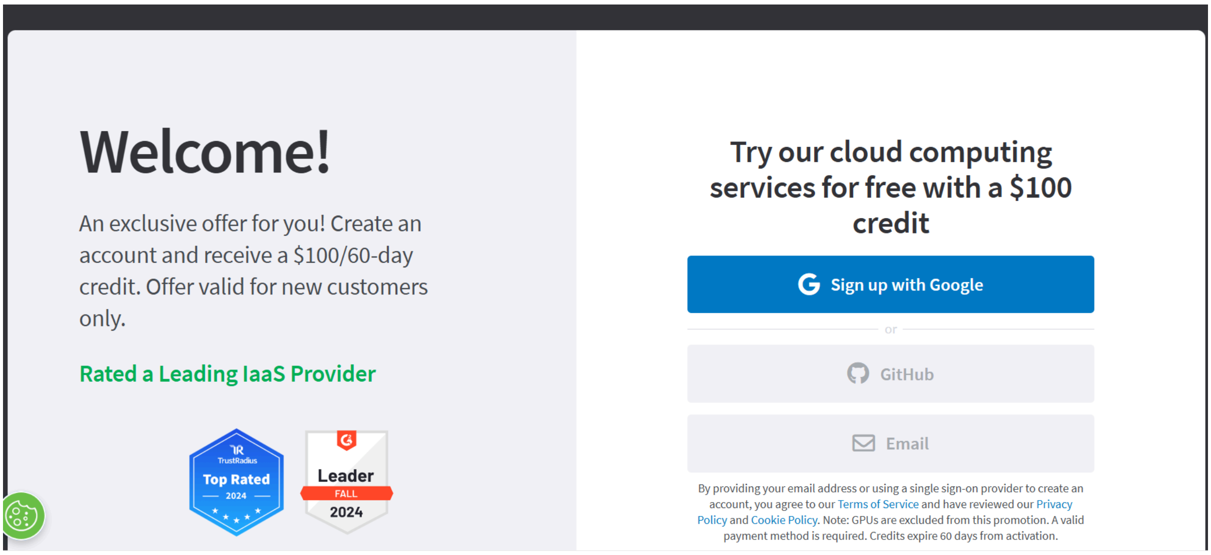


Welcome!

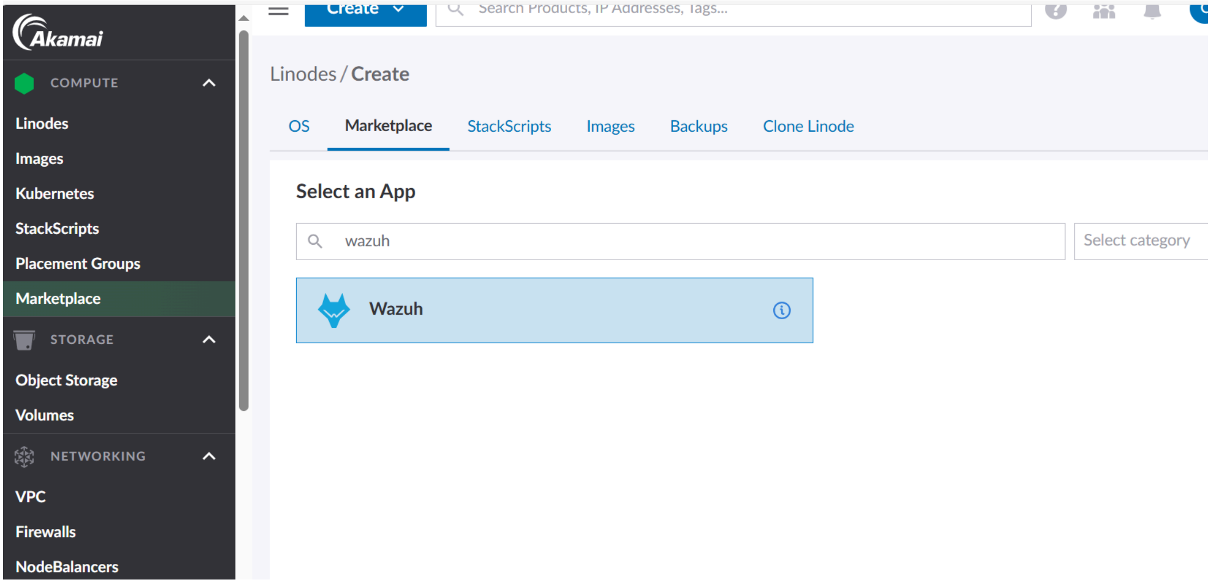
An exclusive offer for you! Create an account and receive a $100/60-day credit. Offer valid for new customers only.

Rated a Leading IaaS Provider

Try our cloud computing services for free with a $100 credit

By providing your email address or using a single sign-on provider to create an account, you agree to our Terms of Service and have reviewed our Privacy Policy and Cookie Policy. Note: GPUs are excluded from this promotion. A valid payment method is required. Credits expire 60 days from activation.

Setting up an account on wazuh as i receive $100 free credit to use to set up the virtual machine where wazuh will be hosted.

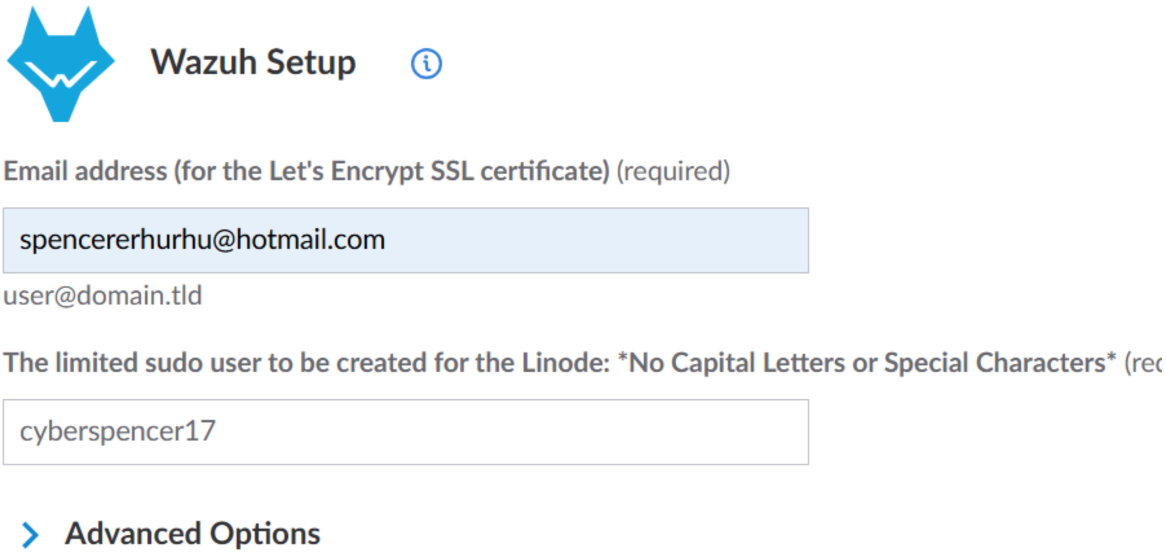


Linodes / Create

Select an App

wazuh

Above the account is created and I select wazuh and begin configurations.



Wazuh Setup

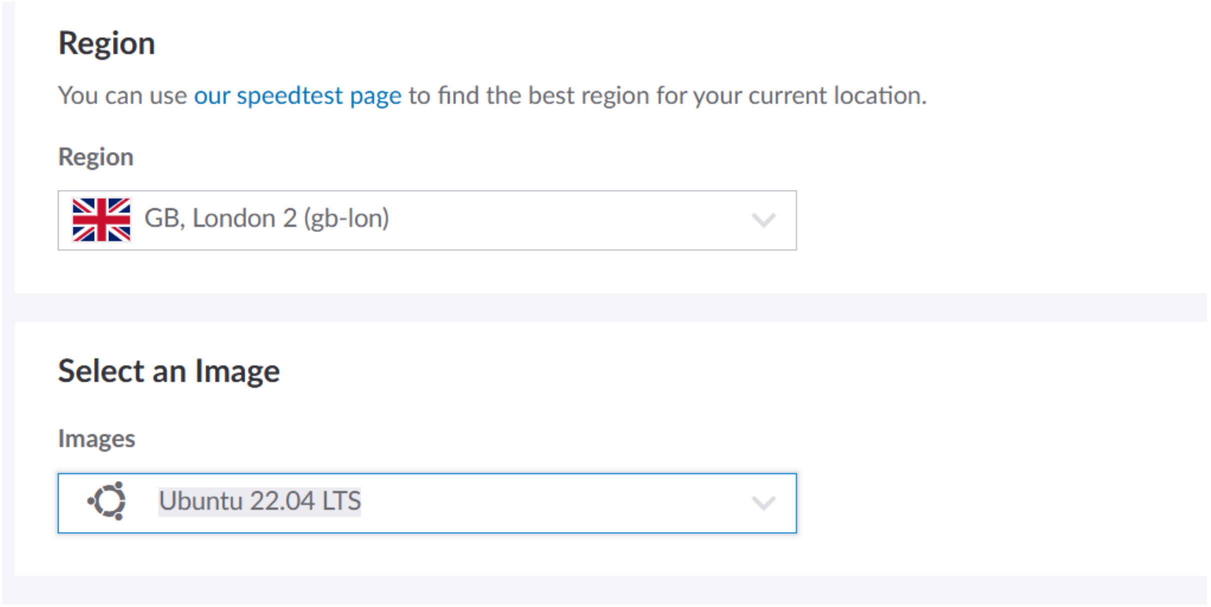
Email address (for the Let's Encrypt SSL certificate) (required)

spencererhurhu@hotmail.com

user@domain.tld

The limited sudo user to be created for the Linode: *No Capital Letters or Special Characters* (rec

cyberspencer17



Region

You can use our speedtest page to find the best region for your current location.

Region

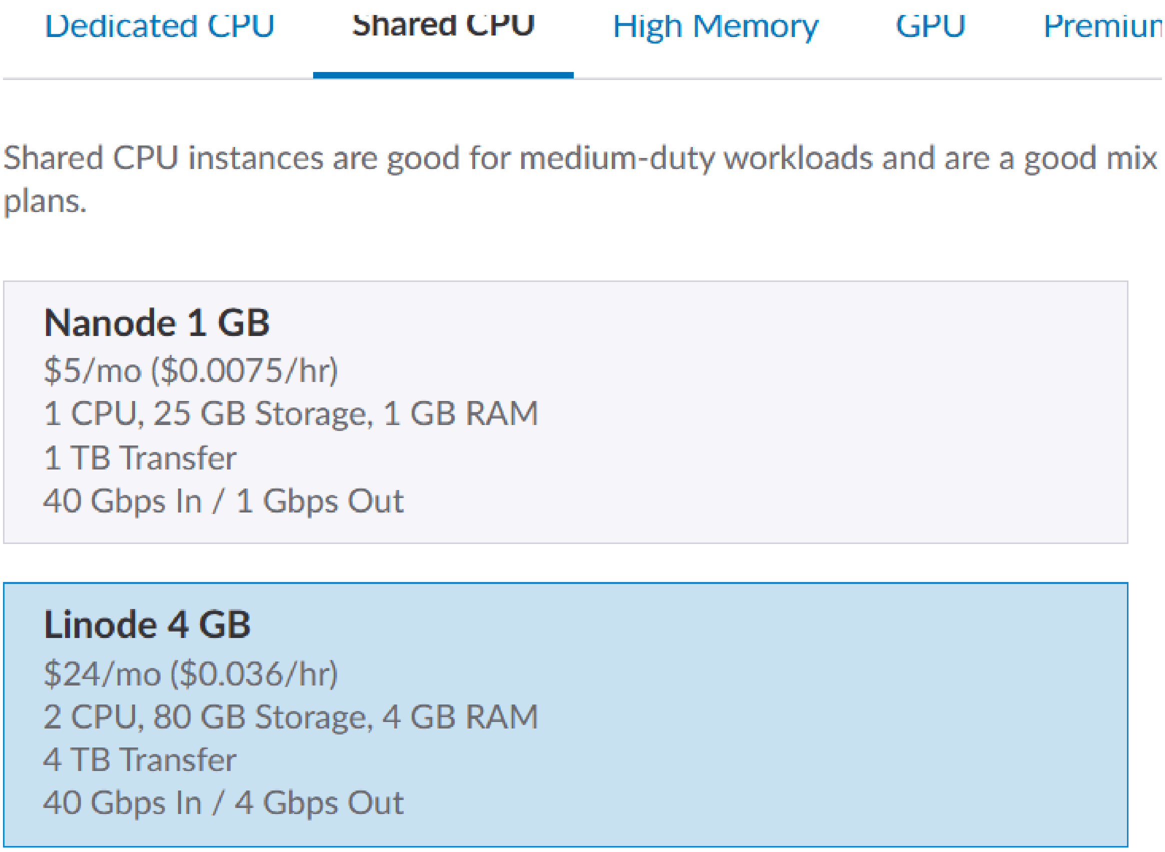
GB, London 2 (gb-lon)

Select an Image

Images

Ubuntu 22.04 LTS

In the images above I set configurations for the vm and choose the uk as the region because it will make transfers quicker.

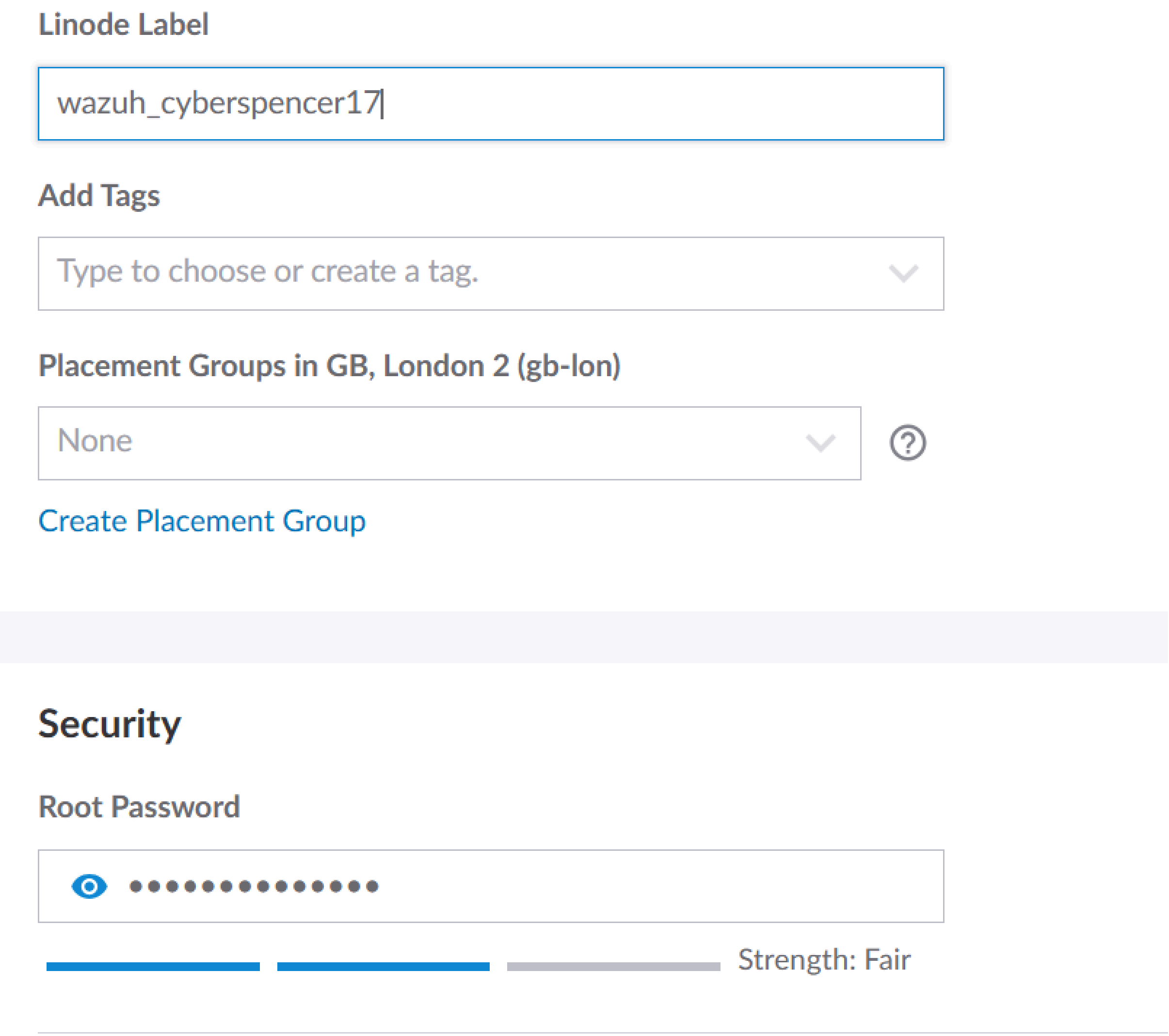


Shared CPU instances are good for medium-duty workloads and are a good mix
plans.

Nanode 1 GB
$5/mo ($0.0075/hr)
1 CPU, 25 GB Storage, 1 GB RAM
1 TB Transfer
40 Gbps In / 1 Gbps Out

Linode 4 GB
$24/mo ($0.036/hr)
2 CPU, 80 GB Storage, 4 GB RAM
4 TB Transfer
40 Gbps In / 4 Gbps Out

I chose 4gb to make sure the wahuz had enough operational resources to run without issues. I also chose a shared cpu because it is cheaper.



Linode Label

wazuh_cyberspencer17

Add Tags

Type to choose or create a tag.

Placement Groups in GB, London 2 (gb-lon)

None

Create Placement Group

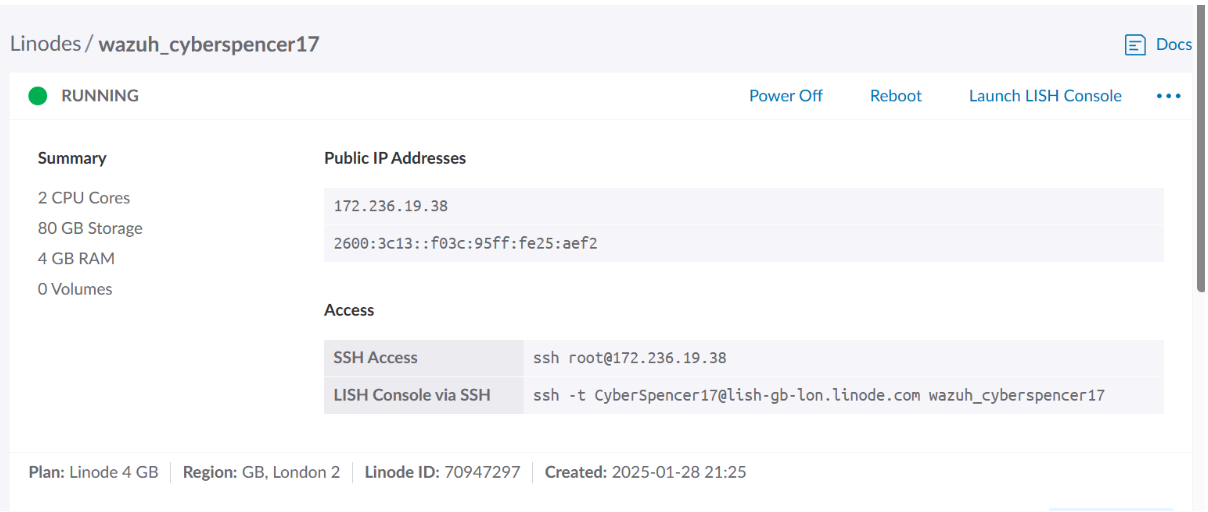
Security

Root Password

••••••••••••••

Strength: Fair

Above I gave it a name and set a password.



Linodes / **wazuh_cyberspencer17**

● RUNNING

Summary

2 CPU Cores
80 GB Storage
4 GB RAM
0 Volumes

Public IP Addresses

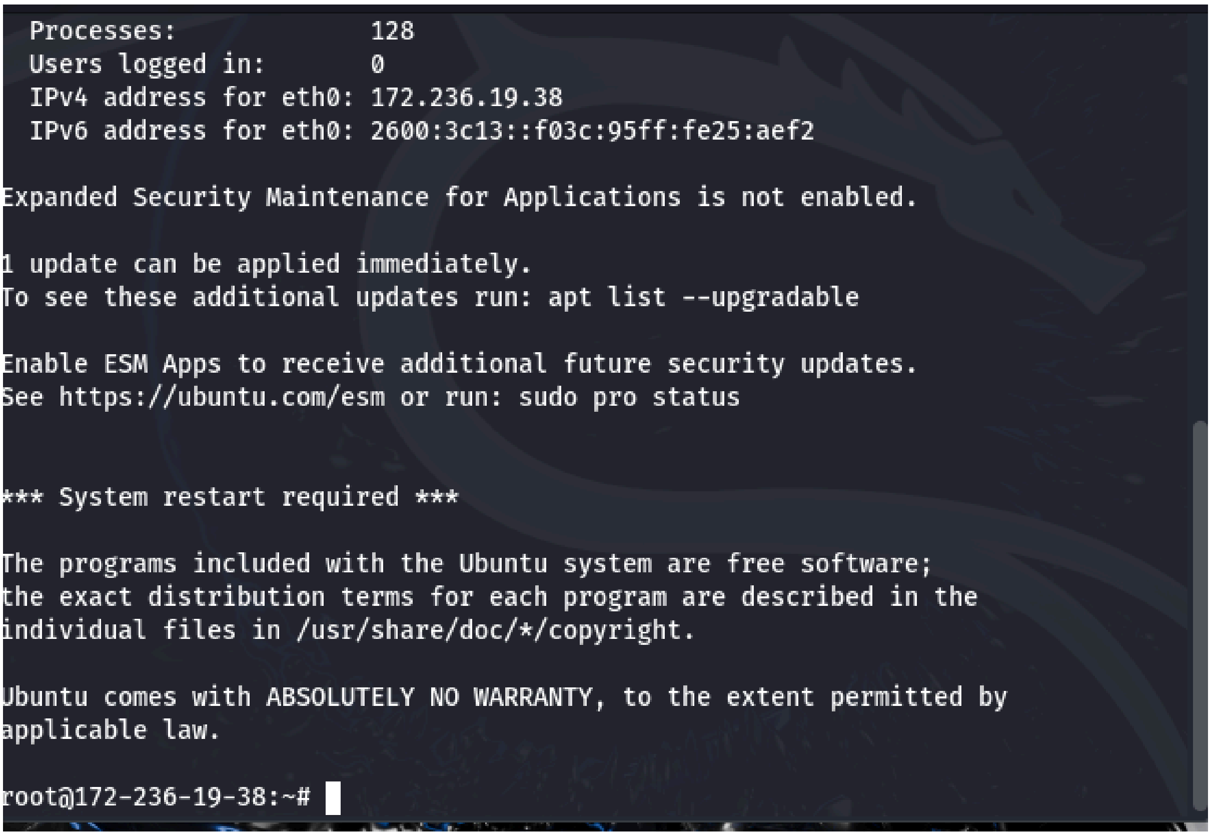
```
172.236.19.38
2600:3c13::f03c:95ff:fe25:aef2
```

Access

SSH Access	`ssh root@172.236.19.38`
LISH Console via SSH	`ssh -t CyberSpencer17@lish-gb-lon.linode.com wazuh_cyberspencer17`

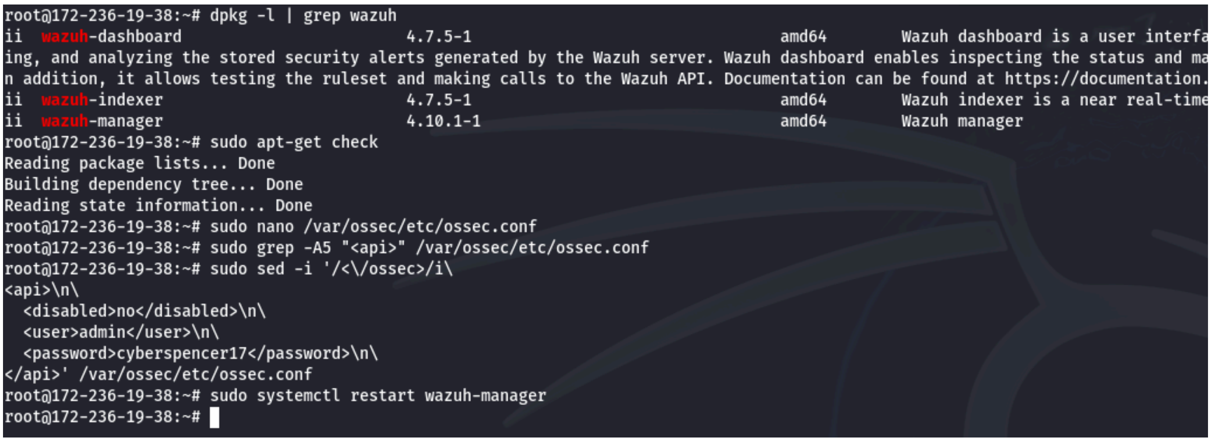
Plan: Linode 4 GB | **Region:** GB, London 2 | **Linode ID:** 70947297 | **Created:** 2025-01-28 21:25

Successfully a virtual machine has been launched in the cloud and I have been given ssh information for logins and other communications. I'm now going to connect to it using the ssh.



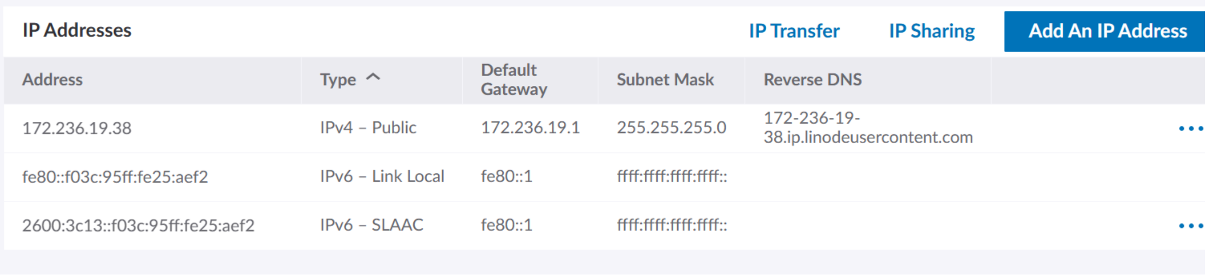
```
  Processes:              128
  Users logged in:        0
  IPv4 address for eth0: 172.236.19.38
  IPv6 address for eth0: 2600:3c13::f03c:95ff:fe25:aef2

Expanded Security Maintenance for Applications is not enabled.

1 update can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

root@172-236-19-38:~# 
```

Here I have successfully logged in.



```
root@172-236-19-38:~# dpkg -l | grep wazuh
ii  wazuh-dashboard                     4.7.5-1                           amd64        Wazuh dashboard is a user interfa
ing, and analyzing the stored security alerts generated by the Wazuh server. Wazuh dashboard enables inspecting the status and ma
n addition, it allows testing the ruleset and making calls to the Wazuh API. Documentation can be found at https://documentation.
ii  wazuh-indexer                       4.7.5-1                           amd64        Wazuh indexer is a near real-time
ii  wazuh-manager                       4.10.1-1                          amd64        Wazuh manager
root@172-236-19-38:~# sudo apt-get check
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
root@172-236-19-38:~# sudo nano /var/ossec/etc/ossec.conf
root@172-236-19-38:~# sudo grep -A5 "<api>" /var/ossec/etc/ossec.conf
root@172-236-19-38:~# sudo sed -i '/<\/ossec>/i\
<api>\n\
  <disabled>no</disabled>\n\
  <user>admin</user>\n\
  <password>cyberspencer17</password>\n\
</api>' /var/ossec/etc/ossec.conf
root@172-236-19-38:~# sudo systemctl restart wazuh-manager
root@172-236-19-38:~# 
```

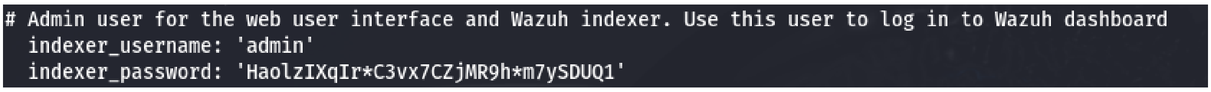
Manually set a username and password for the wazuh login.



IP Addresses

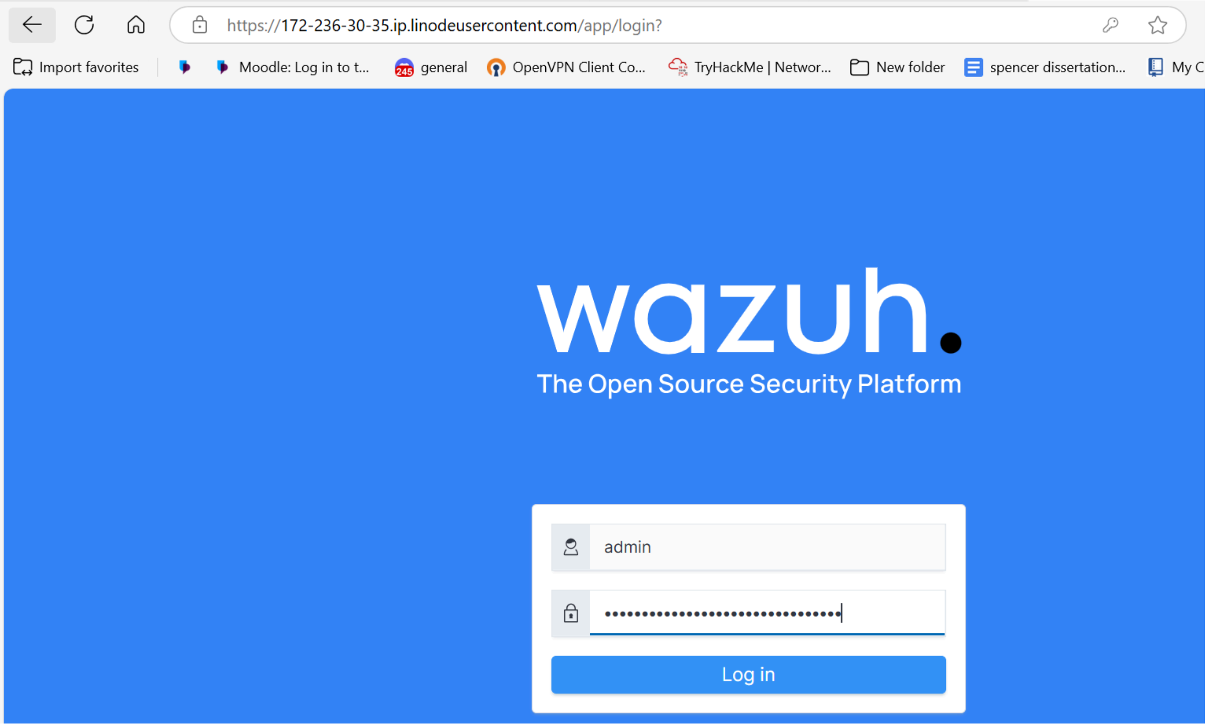
Address	Type	Default Gateway	Subnet Mask	Reverse DNS
172.236.19.38	IPv4 – Public	172.236.19.1	255.255.255.0	172-236-19-38.ip.linodeusercontent.com
fe80::f03c:95ff:fe25:aef2	IPv6 – Link Local	fe80::1	ffff:ffff:ffff:ffff::	
2600:3c13::f03c:95ff:fe25:aef2	IPv6 – SLAAC	fe80::1	ffff:ffff:ffff:ffff::	

Here I located the reverse dns to access the platform.



```
# Admin user for the web user interface and Wazuh indexer. Use this user to log in to Wazuh dashboard
  indexer_username: 'admin'
  indexer_password: 'HaolzIXqIr*C3vx7CZjMR9h*m7ySDUQ1'
```

In linux I navigated to the file with the credentials for me to log into the wazuh interface.

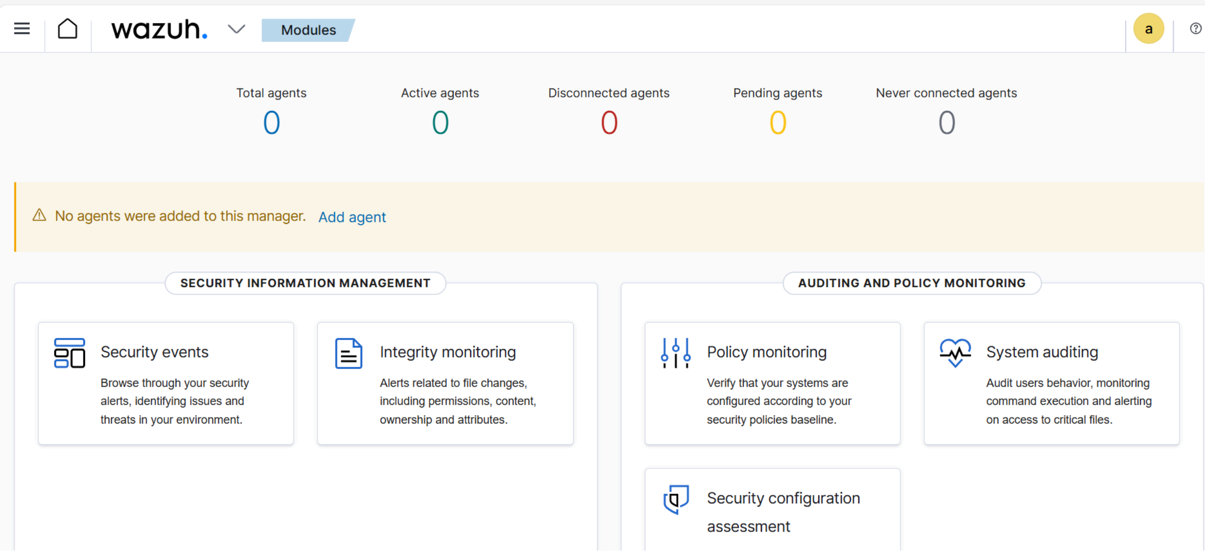


https://172-236-30-35.ip.linodeusercontent.com/app/login?

admin

••••••••••••••••••••••••••••••••

Here I enter the reverse dns and the login credentials.



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

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.

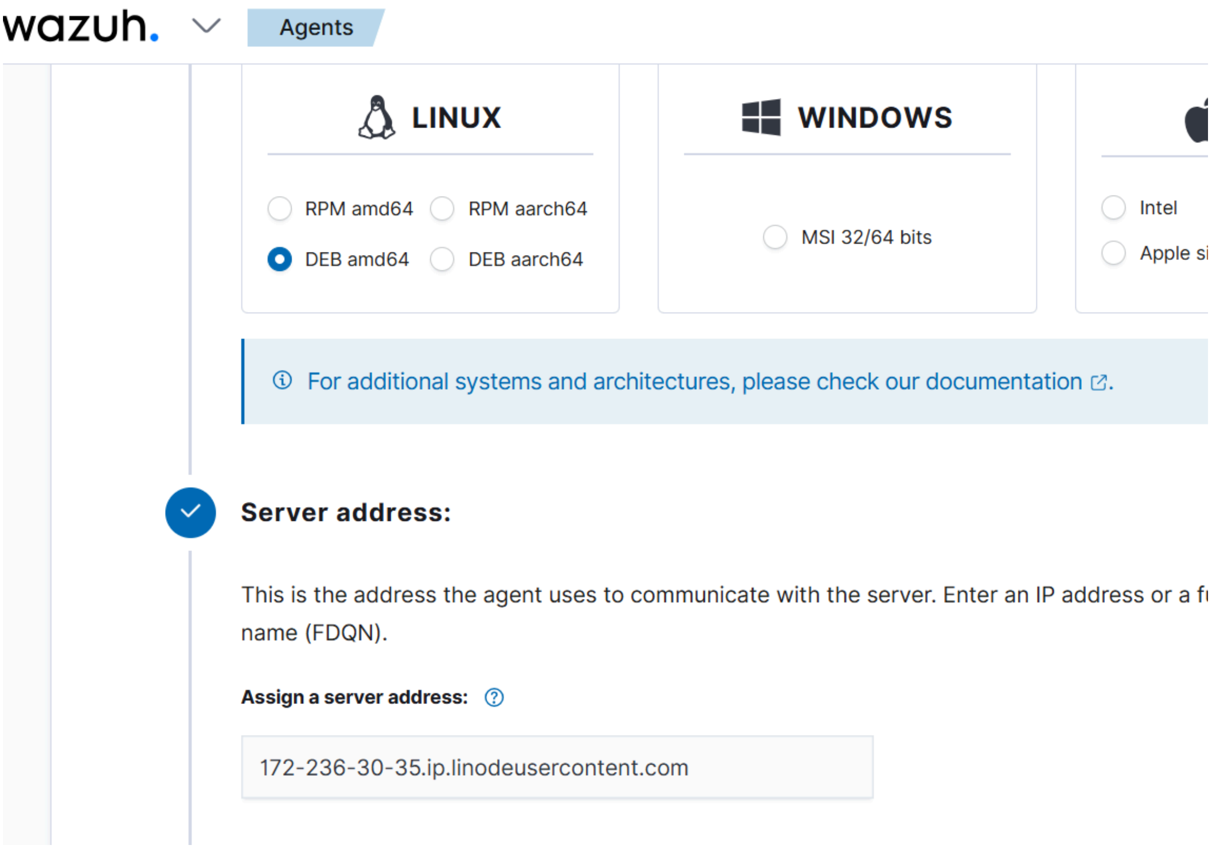
AUDITING AND POLICY MONITORING

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.

Security configuration assessment

Now that wazuh has successfully launched, I will now add agents that we can monitor.



LINUX

○ RPM amd64 ○ RPM aarch64
● DEB amd64 ○ DEB aarch64

WINDOWS

○ MSI 32/64 bits

○ Intel
○ Apple si

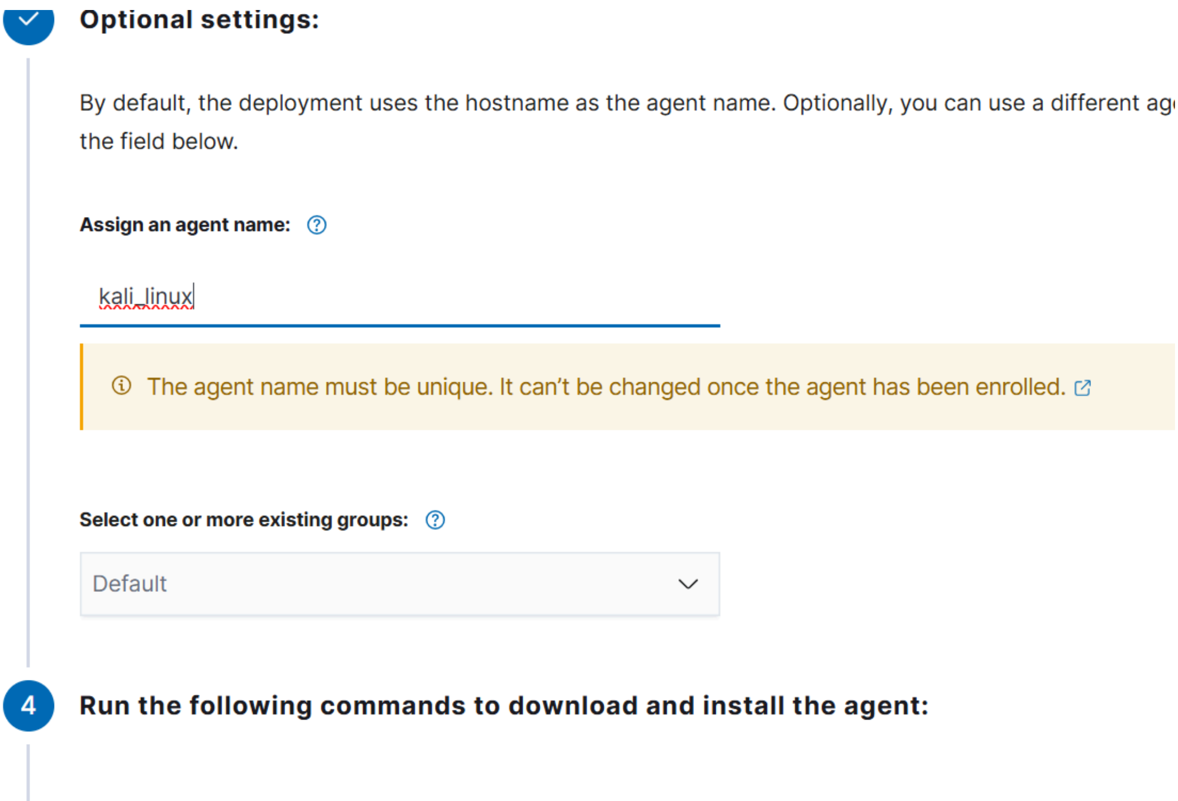
ⓘ For additional systems and architectures, please check our documentation.

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fu name (FDQN).

Assign a server address:

172-236-30-35.ip.linodeusercontent.com



Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different ag
the field below.

Assign an agent name: ⓘ

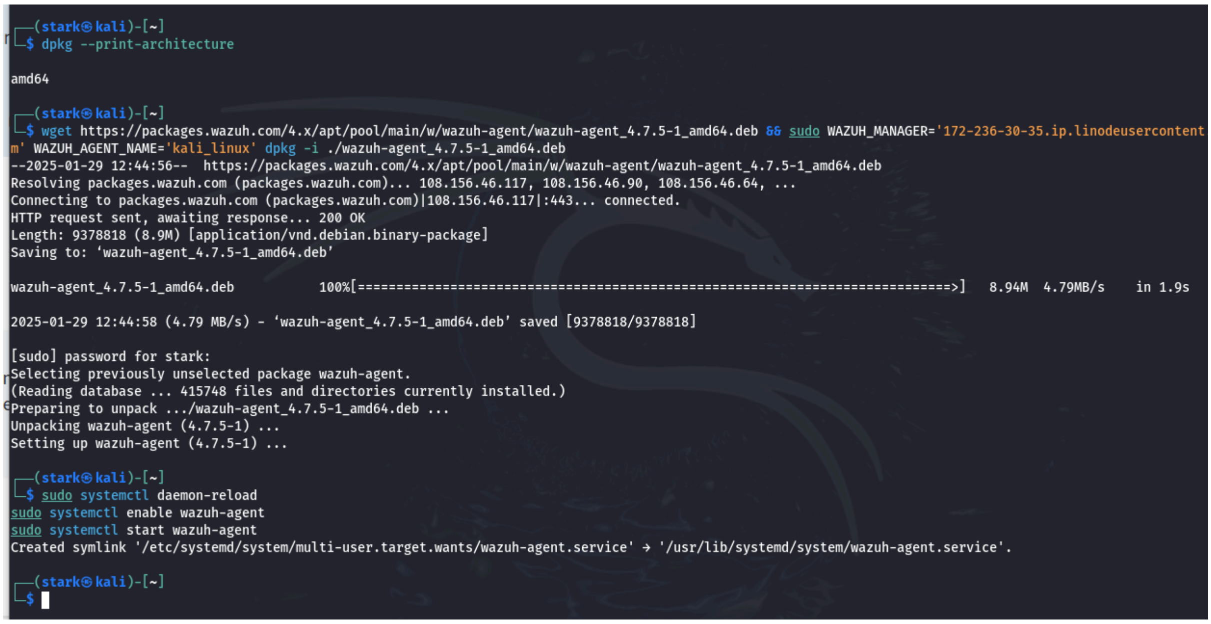
kali_linux

ⓘ The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups: ⓘ

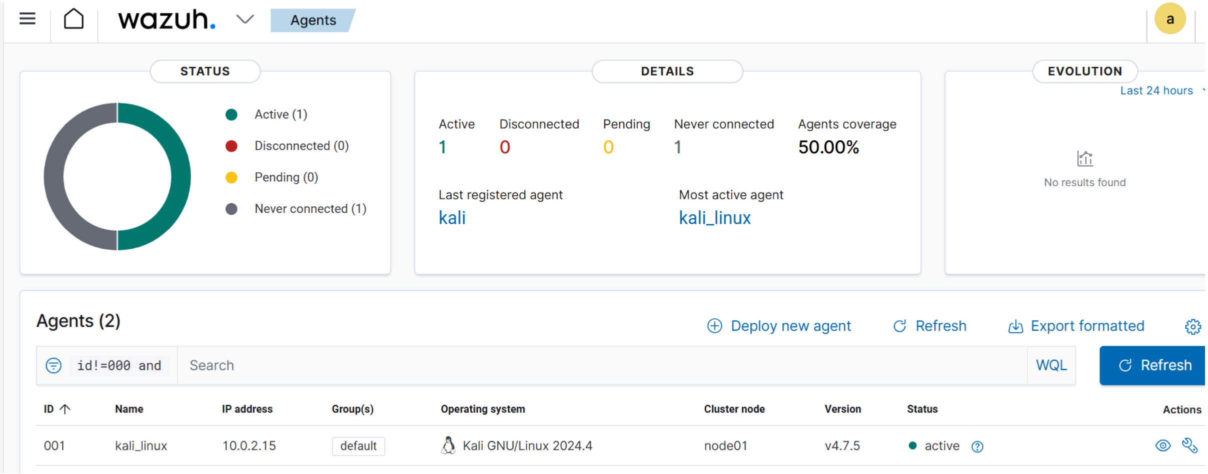
Default

4 **Run the following commands to download and install the agent:**



```
┌──(stark㉿kali)-[~]
└─$ dpkg --print-architecture

amd64

┌──(stark㉿kali)-[~]
└─$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb && sudo WAZUH_MANAGER='172-236-30-35.ip.linodeusercontent
m' WAZUH_AGENT_NAME='kali_linux' dpkg -i ./wazuh-agent_4.7.5-1_amd64.deb
--2025-01-29 12:44:56--  https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.7.5-1_amd64.deb
Resolving packages.wazuh.com (packages.wazuh.com)... 108.156.46.117, 108.156.46.90, 108.156.46.64, ...
Connecting to packages.wazuh.com (packages.wazuh.com)|108.156.46.117|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 9378818 (8.9M) [application/vnd.debian.binary-package]
Saving to: 'wazuh-agent_4.7.5-1_amd64.deb'

wazuh-agent_4.7.5-1_amd64.deb          100%[=============================================================================>]   8.94M  4.79MB/s    in 1.9s

2025-01-29 12:44:58 (4.79 MB/s) - 'wazuh-agent_4.7.5-1_amd64.deb' saved [9378818/9378818]

[sudo] password for stark:
Selecting previously unselected package wazuh-agent.
(Reading database ... 415748 files and directories currently installed.)
Preparing to unpack .../wazuh-agent_4.7.5-1_amd64.deb ...
Unpacking wazuh-agent (4.7.5-1) ...
Setting up wazuh-agent (4.7.5-1) ...

┌──(stark㉿kali)-[~]
└─$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink '/etc/systemd/system/multi-user.target.wants/wazuh-agent.service' → '/usr/lib/systemd/system/wazuh-agent.service'.

┌──(stark㉿kali)-[~]
└─$ █
```

In the images above I set the configuration details so that the kali linux machine would be added as an agent to monitor.



Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	1	50.00%

Last registered agent: kali

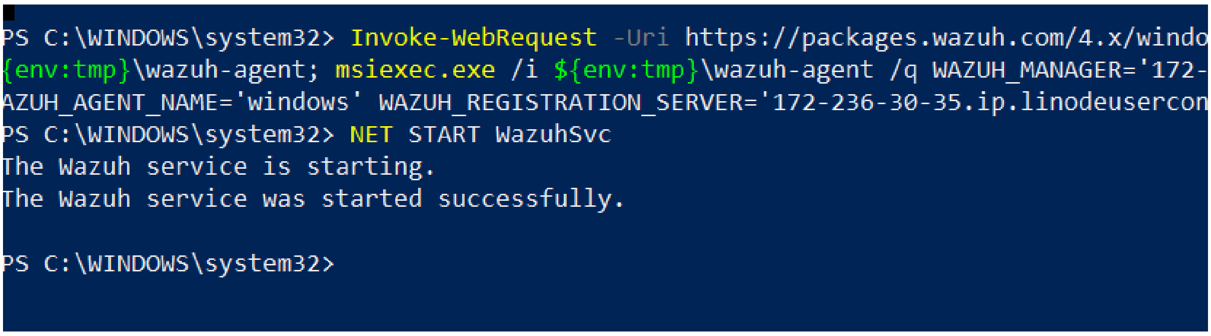
Most active agent: kali_linux

Agents (2)

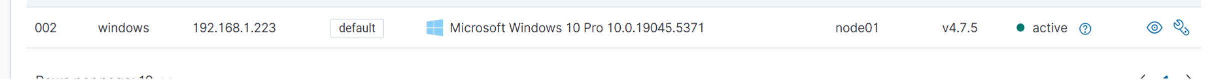
id!=000 and Search

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	kali_linux	10.0.2.15	default	Kali GNU/Linux 2024.4	node01	v4.7.5	● active	

Here the agent has been successfully added.

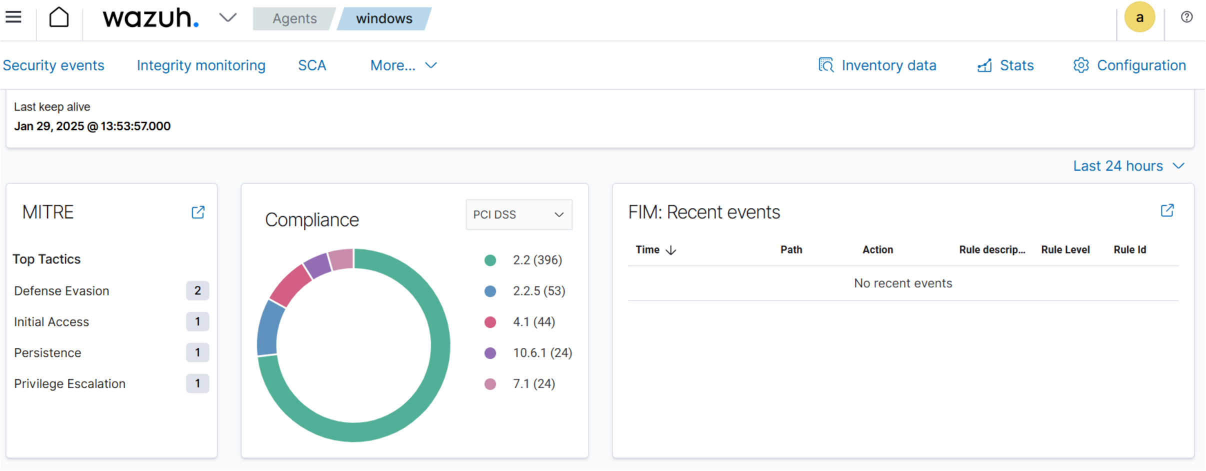


```
PS C:\WINDOWS\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windo
{env:tmp}\wazuh-agent; msiexec.exe /i ${env:tmp}\wazuh-agent /q WAZUH_MANAGER='172-
AZUH_AGENT_NAME='windows' WAZUH_REGISTRATION_SERVER='172-236-30-35.ip.linodeusercon
PS C:\WINDOWS\system32> NET START WazuhSvc
The Wazuh service is starting.
The Wazuh service was started successfully.

PS C:\WINDOWS\system32>
```



002	windows	192.168.1.223	default	Microsoft Windows 10 Pro 10.0.19045.5371	node01	v4.7.5	● active

Above I installed my windows machine as an agent as well.



Last keep alive
Jan 29, 2025 @ 13:53:57.000

Top Tactics

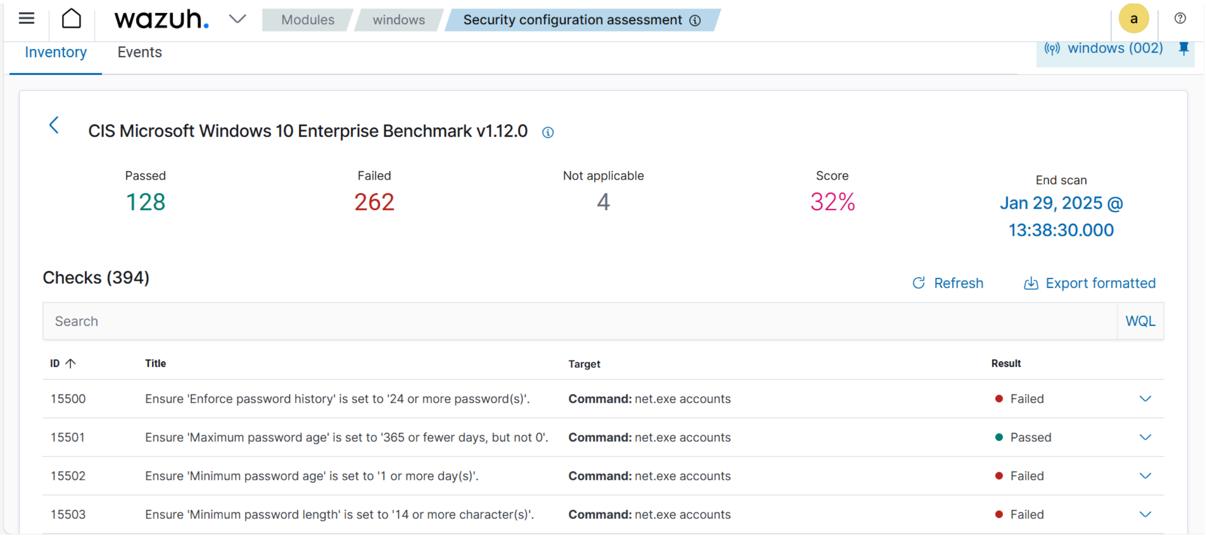
Defense Evasion	2
Initial Access	1
Persistence	1
Privilege Escalation	1

●	2.2 (396)
●	2.2.5 (53)
●	4.1 (44)
●	10.6.1 (24)
●	7.1 (24)

Time	Path	Action	Rule descrip...	Rule Level	Rule Id

No recent events

Here we look at one of the agents. It displays the windows systems companies' level to certain policies such as gdpr and other regulations. On the left we have the mitre top tactics that bad actors are using against the system and here it displays defensive evasion. This mitre display is useful for showing the top attack strategies hackers are using against your system.



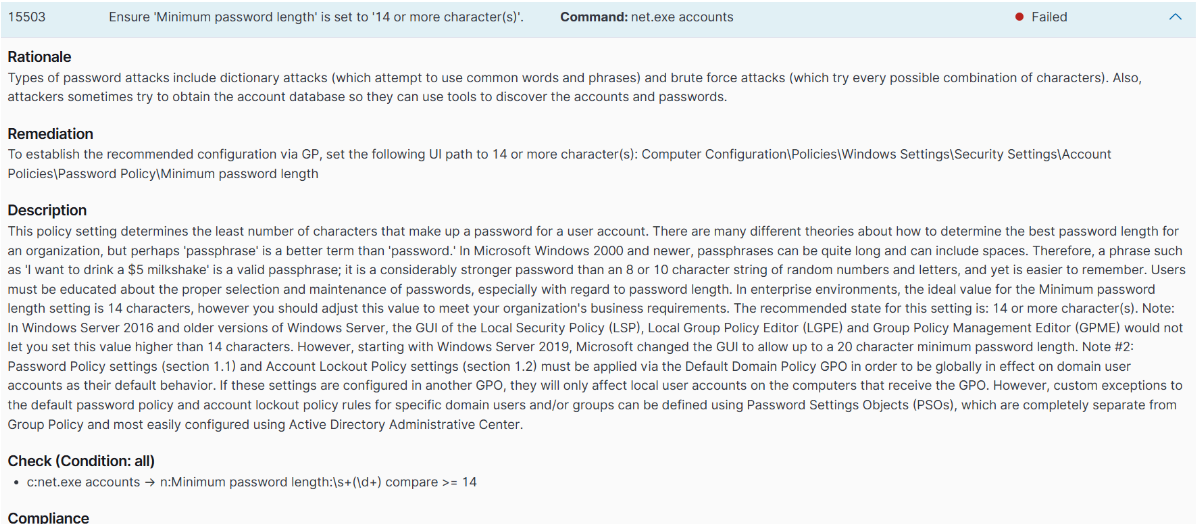
CIS Microsoft Windows 10 Enterprise Benchmark v1.12.0

Passed	Failed	Not applicable	Score	End scan
128	262	4	32%	Jan 29, 2025 @ 13:38:30.000

Checks (394)

ID ↑	Title	Target	Result
15500	Ensure 'Enforce password history' is set to '24 or more password(s)'.	**Command:** net.exe accounts	● Failed
15501	Ensure 'Maximum password age' is set to '365 or fewer days, but not 0'.	**Command:** net.exe accounts	● Passed
15502	Ensure 'Minimum password age' is set to '1 or more day(s)'.	**Command:** net.exe accounts	● Failed
15503	Ensure 'Minimum password length' is set to '14 or more character(s)'.	**Command:** net.exe accounts	● Failed

The security configuration assessment tells me whether the system is configured securely and gives me a score based on the configuration tests. Here it shows me all the checks I have passed and failed. Then I can select a check for more detailed explanation of the issue.



15503 Ensure 'Minimum password length' is set to '14 or more character(s)'. **Command:** net.exe accounts ● Failed

Rationale

Types of password attacks include dictionary attacks (which attempt to use common words and phrases) and brute force attacks (which try every possible combination of characters). Also, attackers sometimes try to obtain the account database so they can use tools to discover the accounts and passwords.

Remediation

To establish the recommended configuration via GP, set the following UI path to 14 or more character(s): Computer Configuration\Policies\Windows Settings\Security Settings\Account Policies\Password Policy\Minimum password length

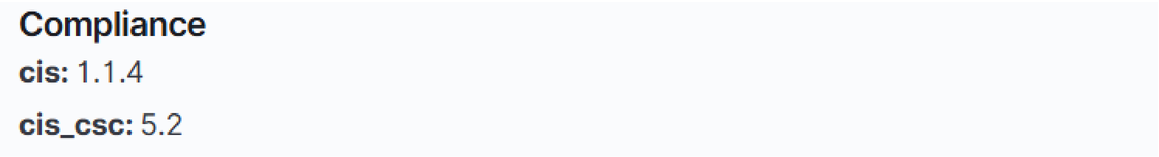
Description

This policy setting determines the least number of characters that make up a password for a user account. There are many different theories about how to determine the best password length for an organization, but perhaps 'passphrase' is a better term than 'password.' In Microsoft Windows 2000 and newer, passphrases can be quite long and can include spaces. Therefore, a phrase such as 'I want to drink a $5 milkshake' is a valid passphrase; it is a considerably stronger password than an 8 or 10 character string of random numbers and letters, and yet is easier to remember. Users must be educated about the proper selection and maintenance of passwords, especially with regard to password length. In enterprise environments, the ideal value for the Minimum password length setting is 14 characters, however you should adjust this value to meet your organization's business requirements. The recommended state for this setting is: 14 or more character(s). Note: In Windows Server 2016 and older versions of Windows Server, the GUI of the Local Security Policy (LSP), Local Group Policy Editor (LGPE) and Group Policy Management Editor (GPME) would not let you set this value higher than 14 characters. However, starting with Windows Server 2019, Microsoft changed the GUI to allow up to a 20 character minimum password length. Note #2: Password Policy settings (section 1.1) and Account Lockout Policy settings (section 1.2) must be applied via the Default Domain Policy GPO in order to be globally in effect on domain user accounts as their default behavior. If these settings are configured in another GPO, they will only affect local user accounts on the computers that receive the GPO. However, custom exceptions to the default password policy and account lockout policy rules for specific domain users and/or groups can be defined using Password Settings Objects (PSOs), which are completely separate from Group Policy and most easily configured using Active Directory Administrative Center.

Check (Condition: all)

- c:net.exe accounts → n:Minimum password length:\s+(\d+) compare >= 14

Compliance

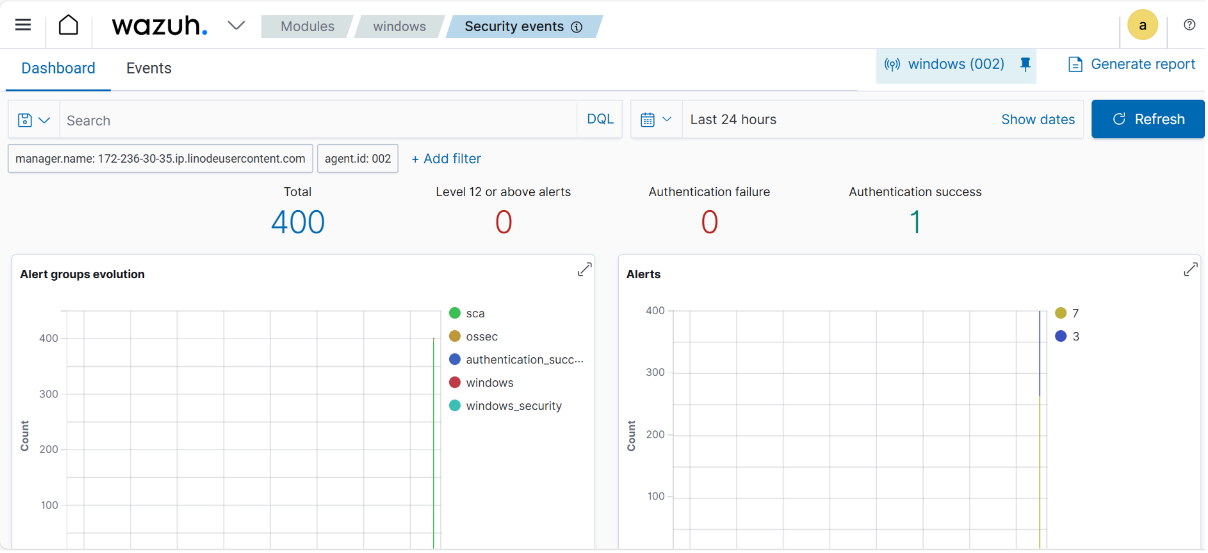


Compliance

cis: 1.1.4

cis_csc: 5.2

Above it tells me the rationale for the check,how to remediate it and why it is important. Furthermore, it tells me the compliance number for it. This is extremely useful to fortify your cyber defenses as it shows you how not complying to these checks can leave open doors for hackers to take advantage of. To ensure the maximum level of security, it is recommended to ensure all checks are passed.

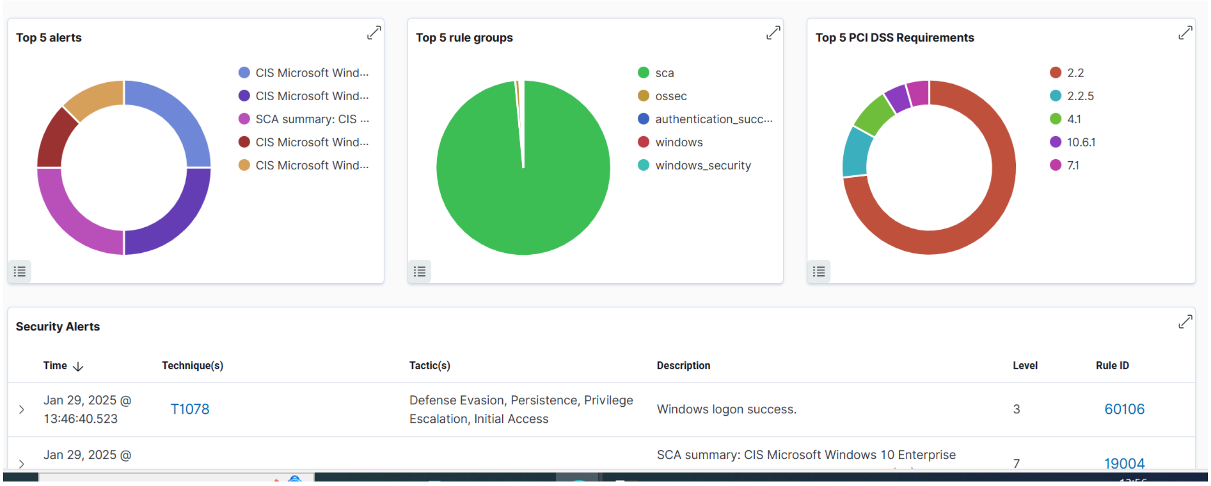


manager.name: 172-236-30-35.ip.linodeusercontent.com

agent.id: 002

Total	Level 12 or above alerts	Authentication failure	Authentication success
400	0	0	1

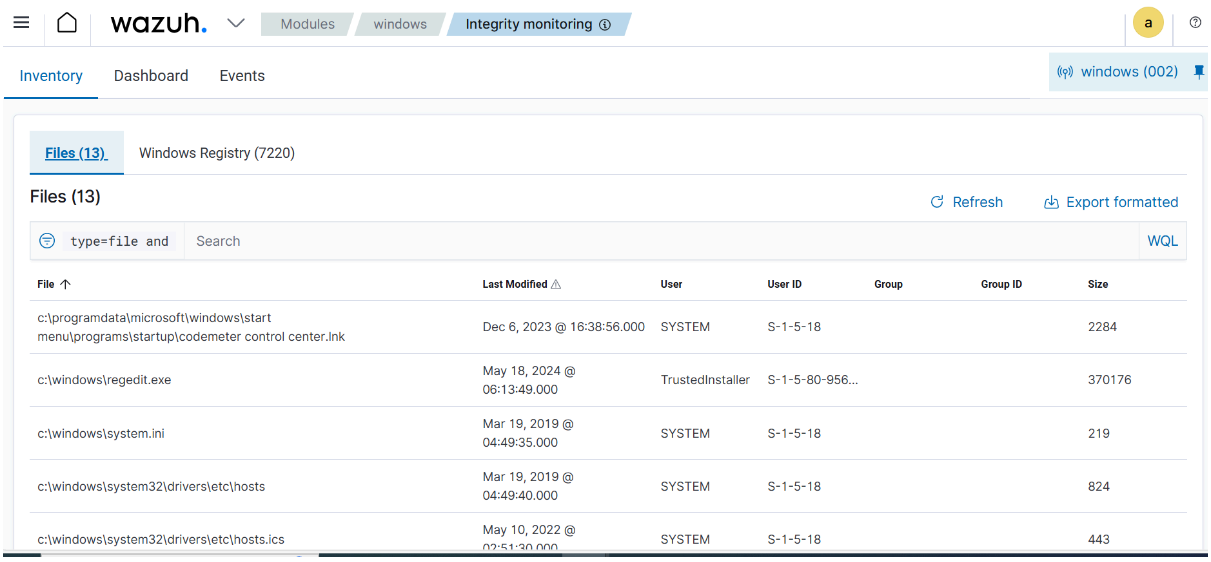
Here within security alerts I can see stuff such as total amount of events, authentication failed and successful attempts.



Security Alerts

Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
Jan 29, 2025 @ 13:46:40.523	T1078	Defense Evasion, Persistence, Privilege Escalation, Initial Access	Windows logon success.	3	60106
Jan 29, 2025 @			SCA summary: CIS Microsoft Windows 10 Enterprise	7	19004

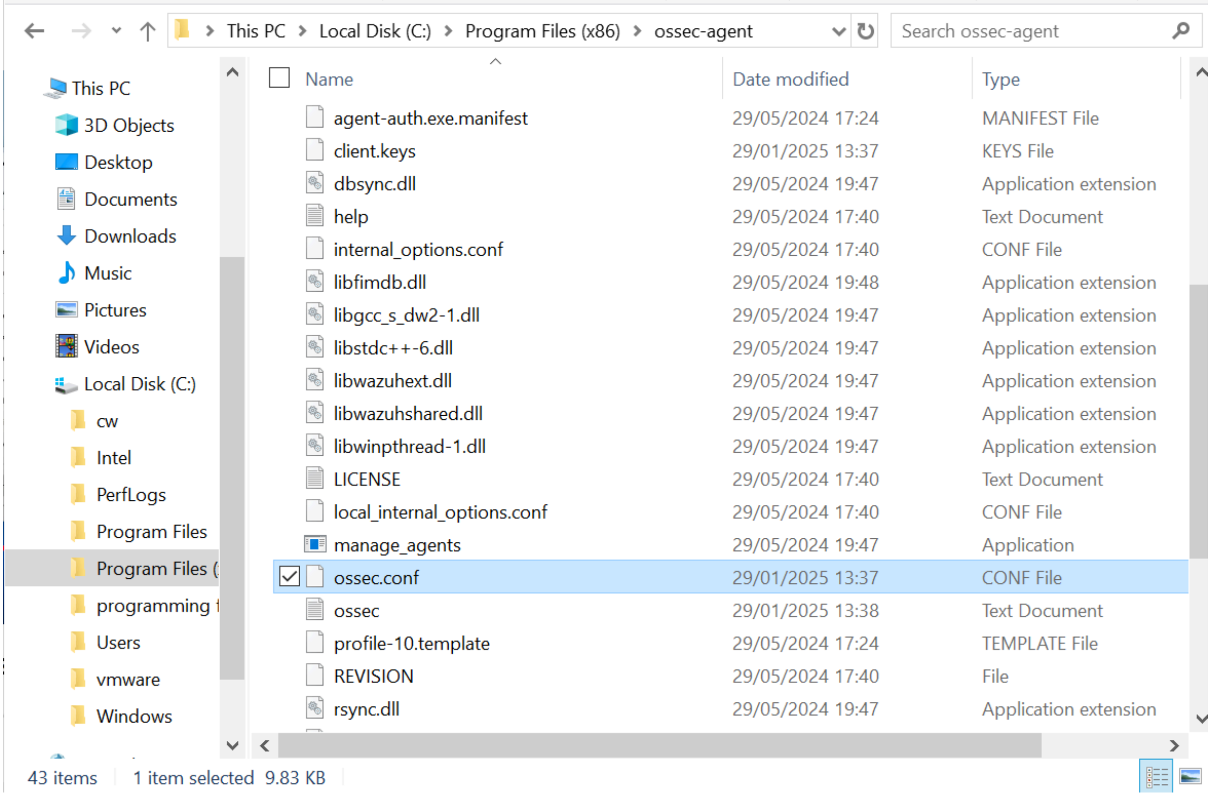
Above it shows me top 5 alerts along with a list of security alerts, the mitre tactic and a description for better diagnosis.



Files (13)

File	Last Modified	User	User ID	Group	Group ID	Size
c:\programdata\microsoft\windows\start menu\programs\startup\codemeter control center.lnk	Dec 6, 2023 @ 16:38:56.000	SYSTEM	S-1-5-18			2284
c:\windows\regedit.exe	May 18, 2024 @ 06:13:49.000	TrustedInstaller	S-1-5-80-956...			370176
c:\windows\system.ini	Mar 19, 2019 @ 04:49:35.000	SYSTEM	S-1-5-18			219
c:\windows\system32\drivers\etc\hosts	Mar 19, 2019 @ 04:49:40.000	SYSTEM	S-1-5-18			824
c:\windows\system32\drivers\etc\hosts.ics	May 10, 2022 @ 02:51:30.000	SYSTEM	S-1-5-18			443

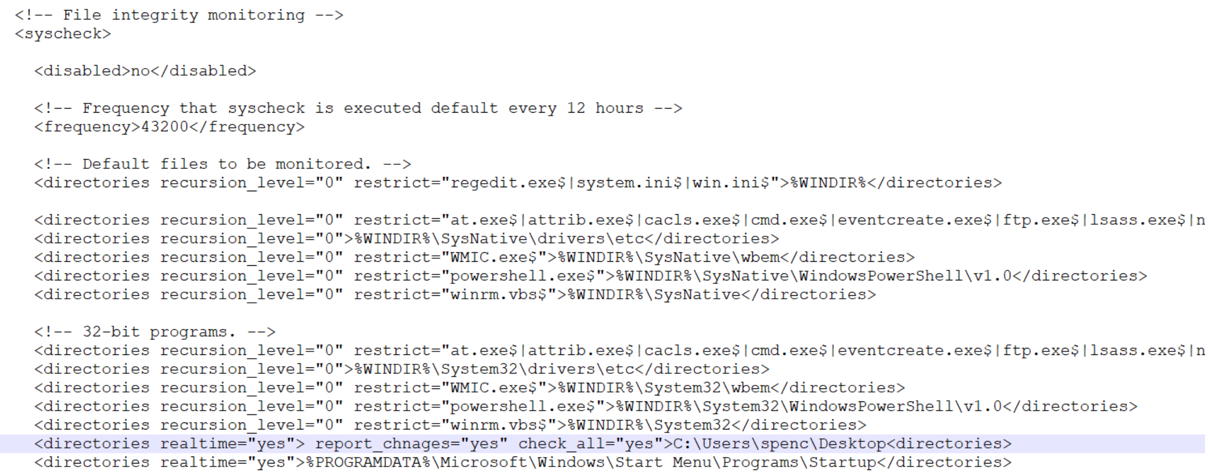
An important module for windows is the integrity monitoring module. The module monitors the field and registry keys on the windows and alerts when a modification is made. This simulates when an authorised individual modified a file on the system. You can also set the time frame for how often it will scan the files and registry keys.   I will now demonstrate how to modify it to alert in real time.



Name	Date modified	Type
agent-auth.exe.manifest	29/05/2024 17:24	MANIFEST File
client.keys	29/01/2025 13:37	KEYS File
dbsync.dll	29/05/2024 19:47	Application extension
help	29/05/2024 17:40	Text Document
internal_options.conf	29/05/2024 17:40	CONF File
libfimdb.dll	29/05/2024 19:48	Application extension
libgcc_s_dw2-1.dll	29/05/2024 19:47	Application extension
libstdc++-6.dll	29/05/2024 19:47	Application extension
libwazuhext.dll	29/05/2024 19:47	Application extension
libwazuhshared.dll	29/05/2024 19:47	Application extension
libwinpthread-1.dll	29/05/2024 19:47	Application extension
LICENSE	29/05/2024 17:40	Text Document
local_internal_options.conf	29/05/2024 17:40	CONF File
manage_agents	29/05/2024 19:47	Application
☑ ossec.conf	29/01/2025 13:37	CONF File
ossec	29/01/2025 13:38	Text Document
profile-10.template	29/05/2024 17:24	TEMPLATE File
REVISION	29/05/2024 17:40	File
rsync.dll	29/05/2024 19:47	Application extension

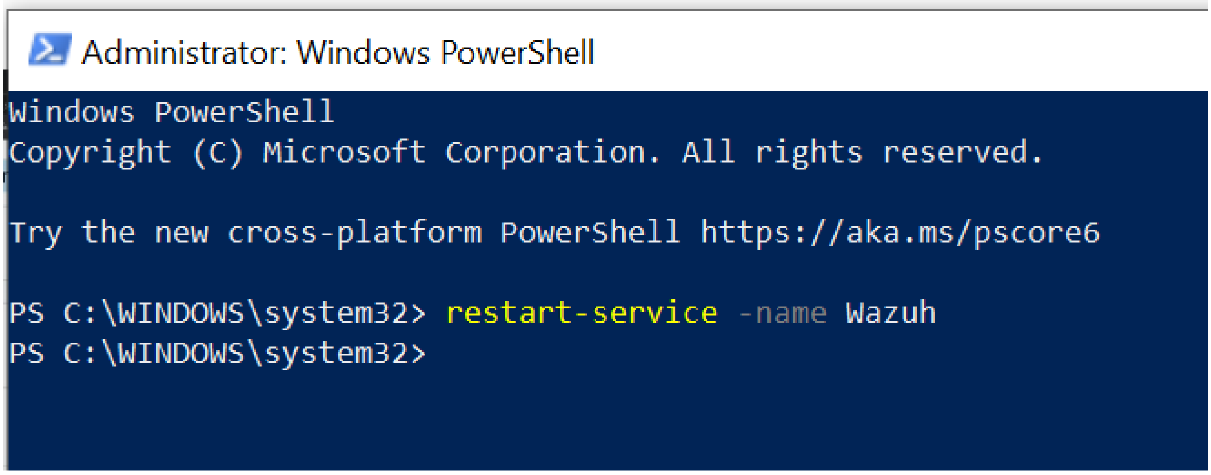
43 items   1 item selected 9.83 KB

I navigate to the ossec.conf file which is the configuration file for my agent.



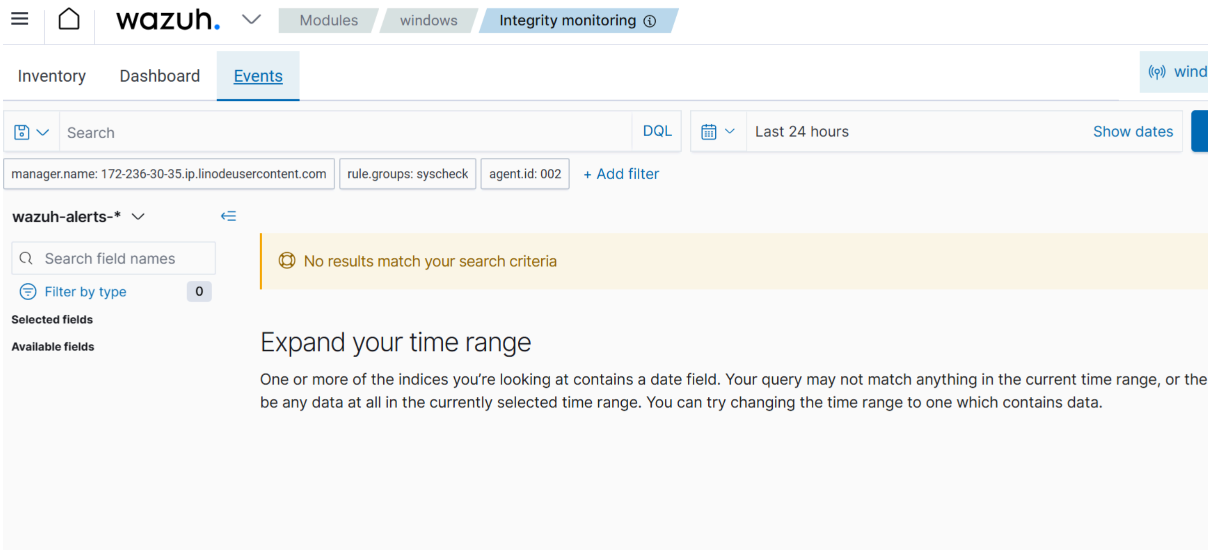
```
<!-- File integrity monitoring -->
<syscheck>

  <disabled>no</disabled>

  <!-- Frequency that syscheck is executed default every 12 hours -->
  <frequency>43200</frequency>

  <!-- Default files to be monitored. -->
  <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$">%WINDIR%</directories>

  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\SysNative\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\SysNative\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\SysNative</directories>

  <!-- 32-bit programs. -->
  <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$|lsass.exe$|n
  <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
  <directories recursion_level="0" restrict="WMIC.exe$">%WINDIR%\System32\wbem</directories>
  <directories recursion_level="0" restrict="powershell.exe$">%WINDIR%\System32\WindowsPowerShell\v1.0</directories>
  <directories recursion_level="0" restrict="winrm.vbs$">%WINDIR%\System32</directories>
  <directories realtime="yes"> report_chnages="yes" check_all="yes">C:\Users\spenc\Desktop<directories>
  <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
```

Here I navigated to the syscheck section under integrity monitoring. I added a new directory which is highlighted in purple. Here I specified a directory and gave it options. I told it to monitor the desktop directory of the user spenc. I then saved the file and restarted the service.



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> restart-service -name Wazuh
PS C:\WINDOWS\system32>
```

Service is restarted.



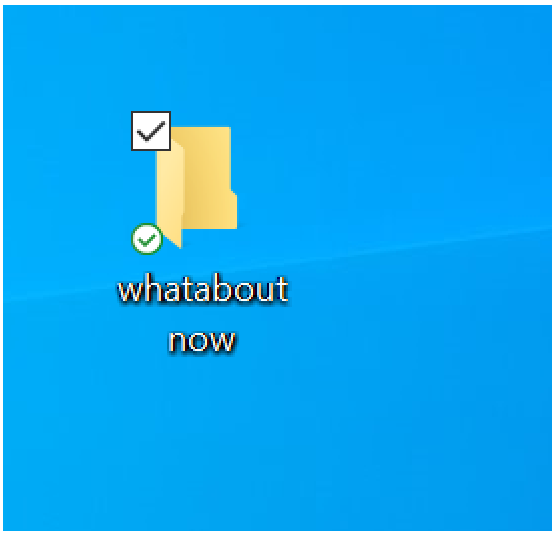
manager.name: 172-236-30-35.ip.linodeusercontent.com | rule.groups: syscheck | agent.id: 002

No results match your search criteria

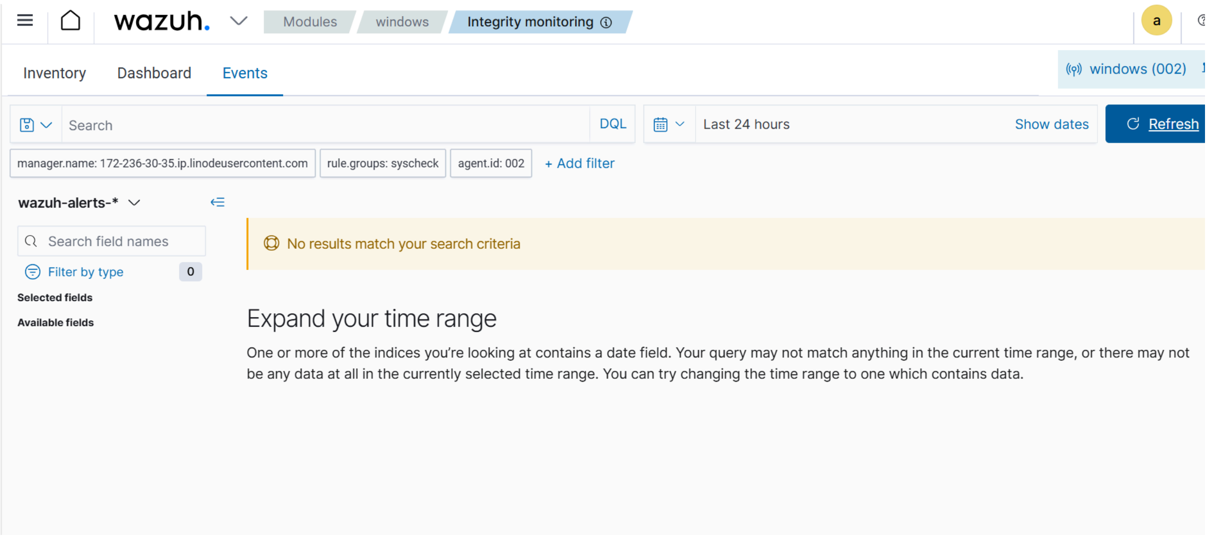
Expand your time range

One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or the be any data at all in the currently selected time range. You can try changing the time range to one which contains data.

Currently there are no events that have happened on the desktop.



Here I added a random folder on the desktop.



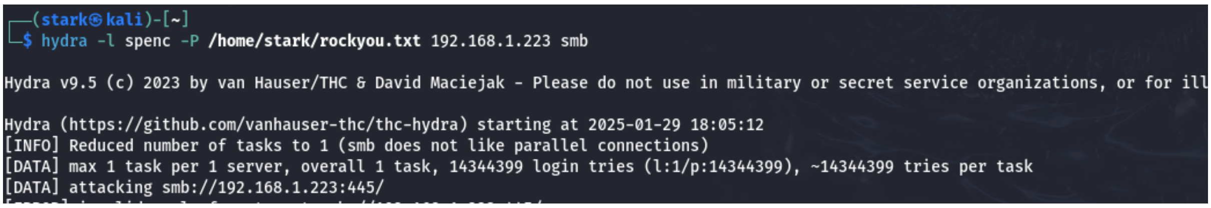
manager.name: 172-236-30-35.ip.linodeusercontent.com | rule.groups: syscheck | agent.id: 002

No results match your search criteria

Expand your time range

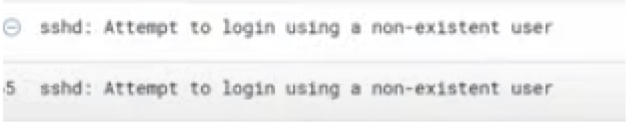
One or more of the indices you're looking at contains a date field. Your query may not match anything in the current time range, or there may not be any data at all in the currently selected time range. You can try changing the time range to one which contains data.

Now all that's left is to refresh and all the events will be logged here. I'm now going to attempt a brute force attack and see if it gets logged.



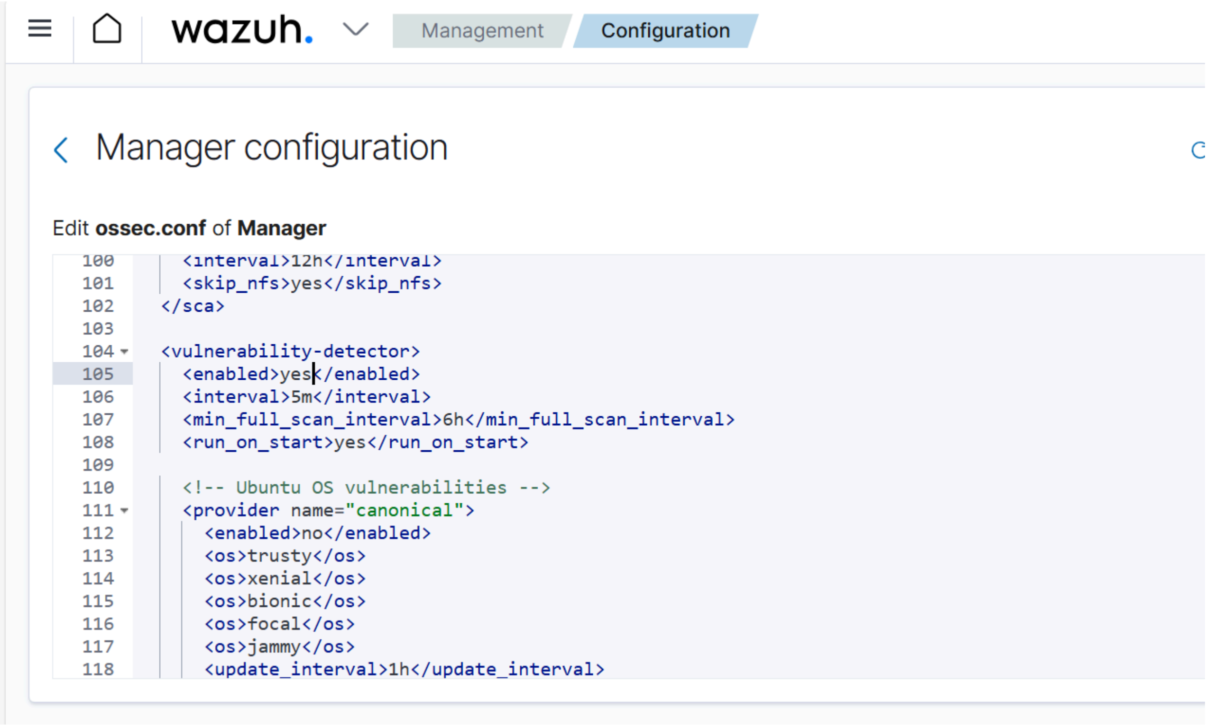
```
┌──(stark㉿kali)-[~]
└─$ hydra -l spenc -P /home/stark/rockyou.txt 192.168.1.223 smb

Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for ill

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-01-29 18:05:12
[INFO] Reduced number of tasks to 1 (smb does not like parallel connections)
[DATA] max 1 task per 1 server, overall 1 task, 14344399 login tries (l:1/p:14344399), ~14344399 tries per task
[DATA] attacking smb://192.168.1.223:445/
```

Here I used the hydra tool to attempt the brute force.



```
sshd: Attempt to login using a non-existent user
5  sshd: Attempt to login using a non-existent user
```

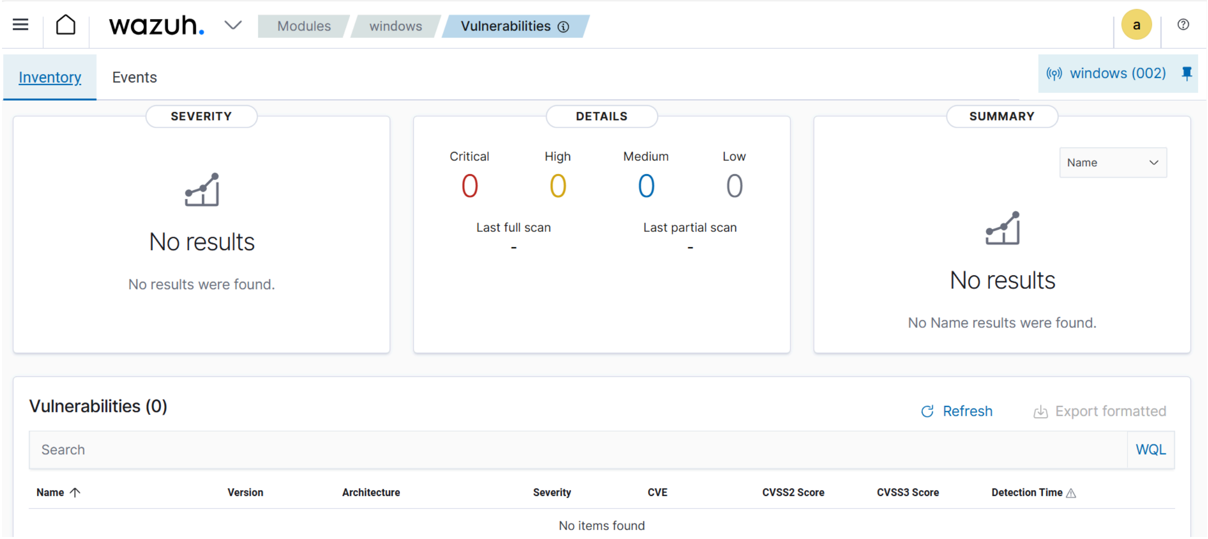
Here successfully the brute force attack was logged.



Edit **ossec.conf** of **Manager**

```
    <interval>12h</interval>
    <skip_nfs>yes</skip_nfs>
  </sca>

  <vulnerability-detector>
    <enabled>yes</enabled>
    <interval>5m</interval>
    <min_full_scan_interval>6h</min_full_scan_interval>
    <run_on_start>yes</run_on_start>

    <!-- Ubuntu OS vulnerabilities -->
    <provider name="canonical">
      <enabled>no</enabled>
      <os>trusty</os>
      <os>xenial</os>
      <os>bionic</os>
      <os>focal</os>
      <os>jammy</os>
      <update_interval>1h</update_interval>
```

Here I edited the configuration file so that the wazuh would scan the agents for vulnerabilities.



No results

No results were found.

Critical	High	Medium	Low
0	0	0	0

Last full scan -

Last partial scan -

No results

No Name results were found.

Vulnerabilities (0)

Name	Version	Architecture	Severity	CVE	CVSS2 Score	CVSS3 Score	Detection Time

No items found

Above there are no vulnerabilities that were detected by the wazuh. Any would be displayed here. This dashboard is especially useful because it relays what vulnerabilities are on your system that attacks can take advantage of. It relays a score of the vulnerability as well relaying how severe the vulnerability is.

Furthermore alerts can be configured to places such as email or slack to notify you when an alert has been flagged.