

MODALIDADE:	Aprendizagem +	Não aplicável	
CURSO:	Técnico/a de Cibersegurança		
UC:	Gerir sistemas de deteção de intrusos (IDS)	CÓDIGO UC:	UC01486
FORMADOR/A:	Bruno Silva	DATA:	

#### OBJETIVOS

- Saber como instalar e configurar um sistema de gestão de eventos e informações de segurança / sistema de deteção de intrusões IDS

O Wazuh é uma plataforma de código aberto, direcionada para a área de cibersegurança, usada para deteção de ameaças, monitorização e resposta a incidentes.

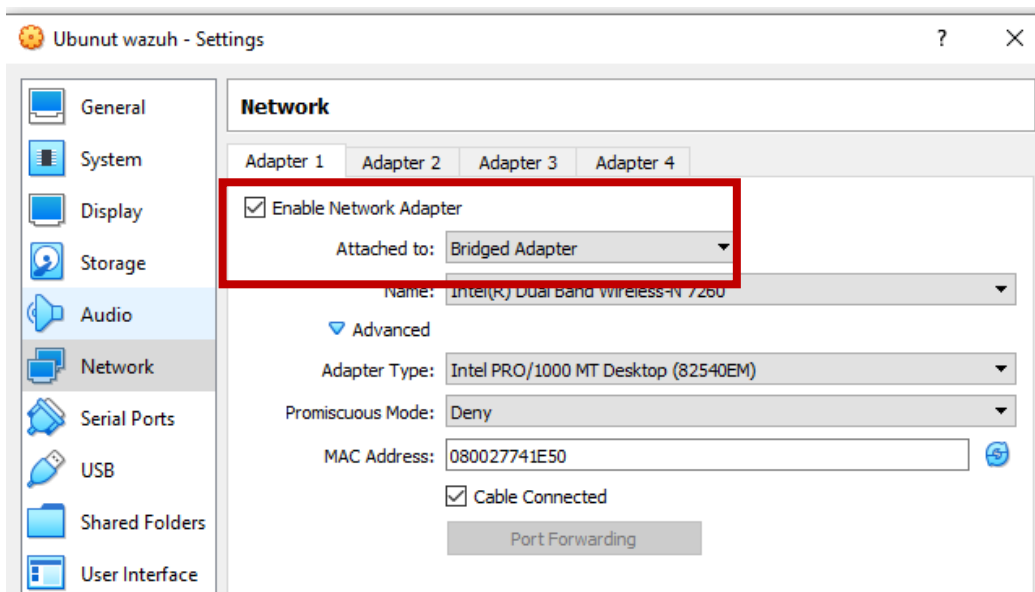
Na prática, esta plataforma é considerada um sistema de gestão de eventos e informações de segurança (SIEM) e também um sistema de deteção de intrusão (IDS).

Esta plataforma disponibiliza recursos para análise de logs, monitorização da integridade de ficheiros, deteção de intrusões, deteção de vulnerabilidades e muito mais. O Wazuh é baseado no Elastic Stack (anteriormente conhecida como ELK Stack), que integra o Elasticsearch, Logstash e Kibana para gestão e visualização de logs.

Inclui também agentes que recolhem dados dos endpoints, enviando-os para um servidor central para análise. O Wazuh ajuda as organizações a melhorar a sua postura de segurança, disponibilizando funções que permitem acompanhar em tempo real a sua infraestrutura de TI e responder prontamente a incidentes de segurança.

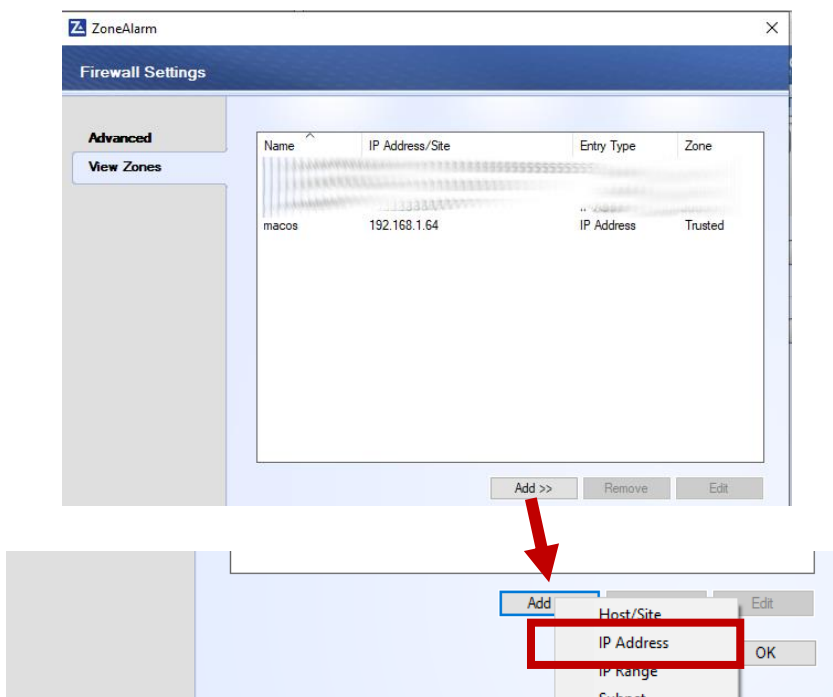
### Parte 1 – Pré-requisitos

**Passo 1** - Caso use o **software virtual box**, nas configurações da placa de rede da máquina virtual deve colocar o adaptador de rede em **bridge adapter**

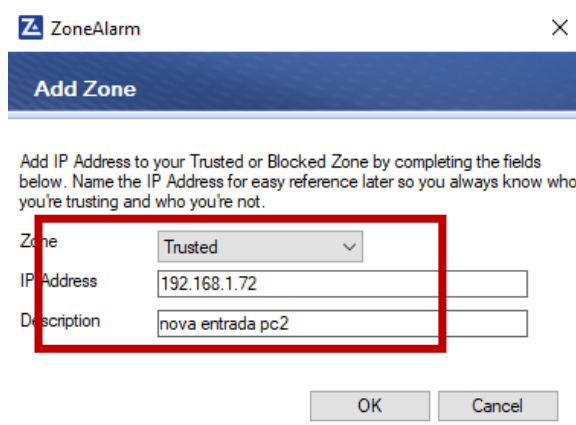


**Passo 2** - Os computadores da LAN **podem não conseguir entrar na máquina virtual**. Isto deve-se ao fato da firewall ou antivírus bloquear as ligações que podem ser potencialmente perigosas. Para tal, deverá verificar:

- **Caso 1** - Na firewall do Windows, verificar se tem permissão na partilha de ficheiros e rede;
- **Caso 2** - Se tiver um software Firewall como Zone Alarm ou outro parecido, deve ir as configurações da Firewall e pedir para criar uma nova exceção para o computador que pretende aceder ao computador onde está a máquina virtual;



No **campo IP Address**, deve colocar o IP da máquina que está a tentar comunicar com o sistema onde está a máquina virtual.



## Parte 2 – Instalação Wazuh (Ubuntu)

**Passo 1** - Fazer a atualização dos repositórios do Ubuntu: **`apt update && apt upgrade`**

**Passo 2** - Fazer instalação das ferramentas de rede: **`apt install net-tools`**

**Passo 3** - Fazer instalação do gestor de tarefas (via linha de comandos): **`apt install htop`**

**Passo 4** - Instalar a ferramenta para transferir dados dos servidores via URL e outros protocolos: **`apt-get install curl`**

**Passo 5** - Fazer download do software Wazuh e instalação dos pacotes:

**`curl -sO https://packages.wazuh.com/4.14/wazuh-install.sh && sudo bash ./wazuh-install.sh -a`**

**Nota importante 1:** Este processo demora alguns minutos, pois está a descarregar o conteúdo e no final irá instalar, ativar serviços e associar outras aplicações.

```
20/11/2023 17:04:54 INFO: Starting Wazuh installation assistant. Wazuh version:
4.6.0
20/11/2023 17:04:54 INFO: Verbose logging redirected to /var/log/wazuh-install.l
20/11/2023 17:05:01 INFO: --- Dependencies ---
20/11/2023 17:05:01 INFO: Installing gawk.
^[H./wazuh-install.sh: linha 987: [: : expressão inteira esperada
20/11/2023 17:05:16 INFO: Wazuh web interface port will be 443.
20/11/2023 17:05:22 INFO: --- Dependencies ---
20/11/2023 17:05:22 INFO: Installing apt-transport-https.
^[H20/11/2023 17:05:29 INFO: Wazuh repository added.
20/11/2023 17:05:29 INFO: --- Configuration files ---
20/11/2023 17:05:29 INFO: Generating configuration files.
^[H20/11/2023 17:05:32 INFO: Created wazuh-install-files.tar. It contains the W
azuh cluster key, certificates, and passwords necessary for installation.
20/11/2023 17:05:32 INFO: --- Wazuh indexer ---
20/11/2023 17:05:32 INFO: Starting Wazuh indexer installation.
```

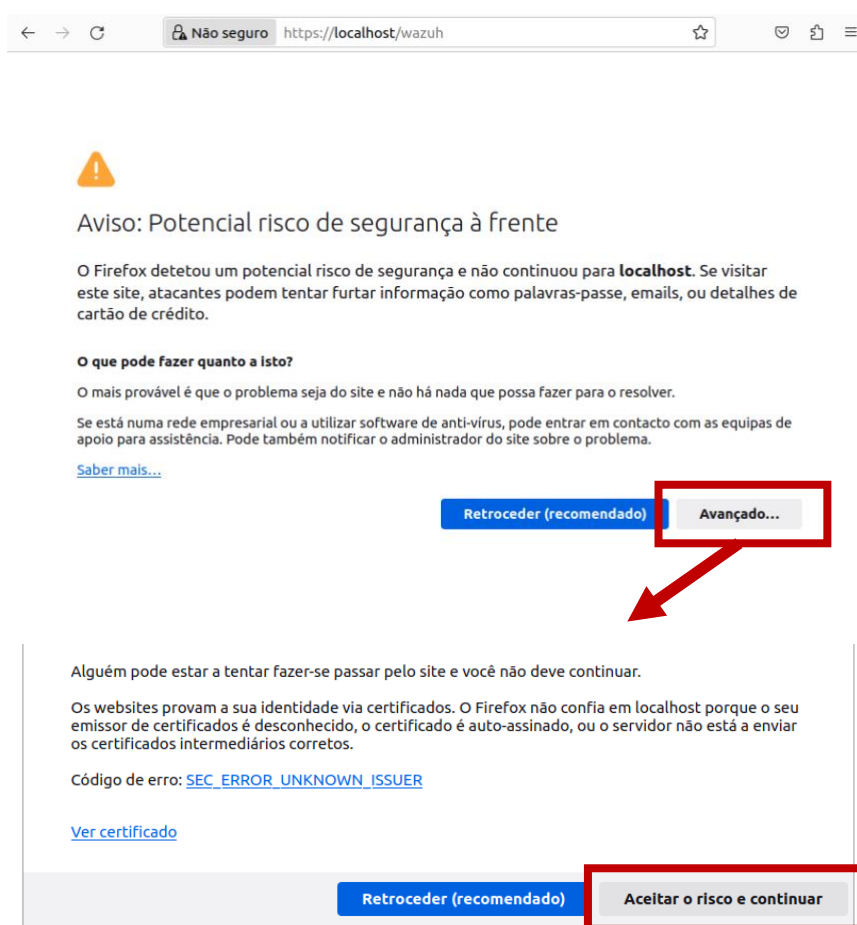
**Passo 6** - No final da instalação, este vai exibir os dados de acesso ao portal na consola. **Grave os dados de acesso num ficheiro de texto para saber como aceder a plataforma Wazuh!**

```
20/11/2023 17:16:08 INFO: wazuh-dashboard service started.
20/11/2023 17:16:38 INFO: Initializing Wazuh dashboard web application.
20/11/2023 17:16:39 INFO: Wazuh dashboard web application initialized.
20/11/2023 17:16:39 INFO: --- Summary ---
20/11/2023 17:16:39 INFO: You can access the web interface https://<wazuh-dashbo
ard-ip>:443
User: admin
Password: RGJvhowWwk47zX3x2Ym?xG?5kn0?1X3K
20/11/2023 17:16:39 INFO: Installation finished.
root@silva-VirtualBox:/home/silva#
```

**Passo 7** - Para aceder à plataforma, basta colocar o endereço iniciado sempre por `https://` e de seguida colocar uma das duas formas:

- `https://localhost`
- `https://<endereço_ip_da_maquina>`

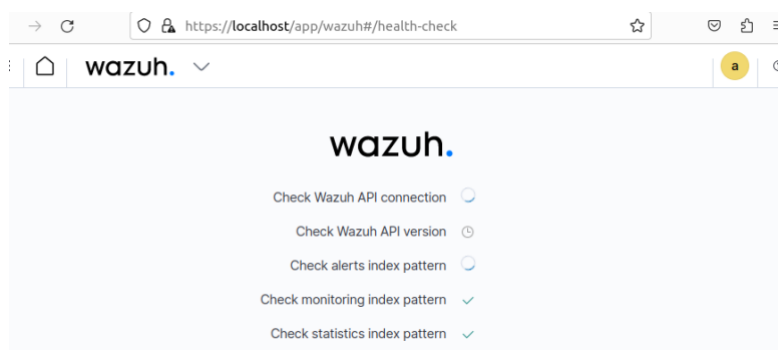
Ao aceder ao portal do Wazuh, este irá exibir um aviso devido ao certificado de segurança, pois trata-se de uma norma de segurança. Para ultrapassar esta situação, precisamos de dar confirmação, bastando clicar no botão **Avançado** e de seguida **Aceitar o risco e continuar**:



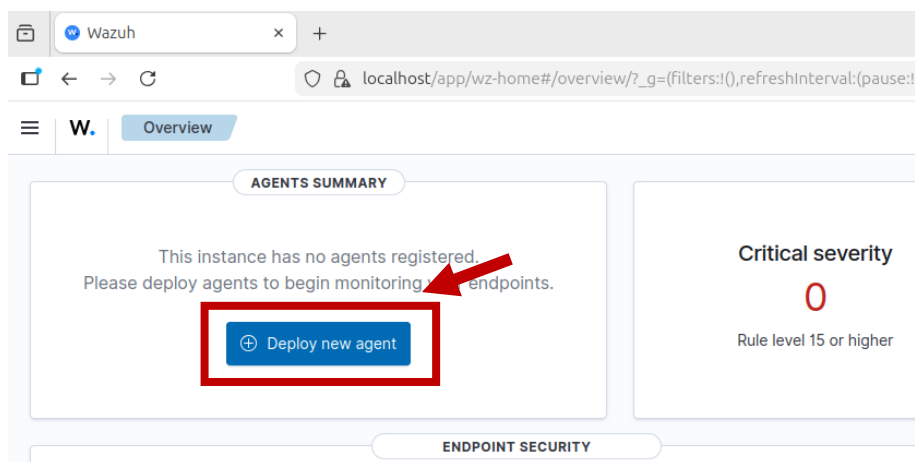
**Passo 8** - Feitos os passos anteriores, será aberta a página principal do qual devem utilizar os dados de acesso que foi dado anteriormente, mais especificamente, no passo 6.



**Passo 9** – Quando entra no portal, este irá verificar os serviços e estado da plataforma:

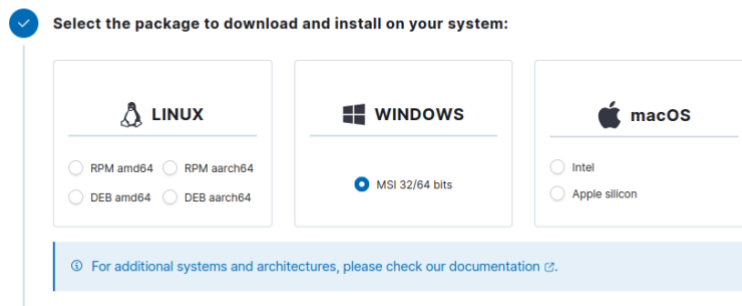


**Passo 10** – No ambiente de trabalho da plataforma ainda não tem nada reportado. Para tal, vamos começar pela operação mais básica que será adicionar agentes. Os agentes são os dispositivos que vão estar a ser monitorizados pela aplicação. Para tal vamos clicar na opção **Add Agent**:



**Passo 11** – Selecionar qual a plataforma do agente em causa (reparem que até abrange os processadores de nova geração):

Deploy new agent



**Passo 12** – Indicar o endereço IP máquina **onde está instalado o Wazuh** (pois podemos estar a aceder a plataforma de uma máquina diferente). Se não sabe o IP abra um terminal e coloque a instrução **ifconfig**:

```

silva@silva-VirtualBox: ~
silva@silva-VirtualBox:~$ ifconfig
enp0s8: flags=4096<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::eef:c022:123c:92a2 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:74:1e:50 txqueuelen 1000 (Ethernet)
    RX packets 1947 bytes 649216 (649.2 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 2192 bytes 352569 (352.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

enp0s8: flags=4096<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.1.70 netmask 255.255.255.0 broadcast 192.168.1.255
    inet6 2001:0000:0000:5200:bcb1:91e1:99ca:b936 prefixlen 64 scopeid 0x0<
    ether 08:00:00:00:00:00 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

global>
    inet6 2001:0000:0000:5200:40fc:fb85:7570:ed5a prefixlen 64 scopeid 0x0<
    ether 08:00:00:00:00:00 txqueuelen 0 (Ethernet)
    RX packets 0 bytes 0 (0.0 KB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 0 bytes 0 (0.0 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
  
```

✓ **Server address**

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

Assign a server address ⓘ

✓ **Optional settings**

The deployment sets the endpoint hostname as the agent name by default. Optionally, you can set your own name in the field below.

Assign an agent name ⓘ

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

**Passo 13** – O código para instalar o agente é automaticamente gerado com as opções que selecionou previamente. Podem clicar em cima dos dois comandos, do qual irá copiar os códigos:

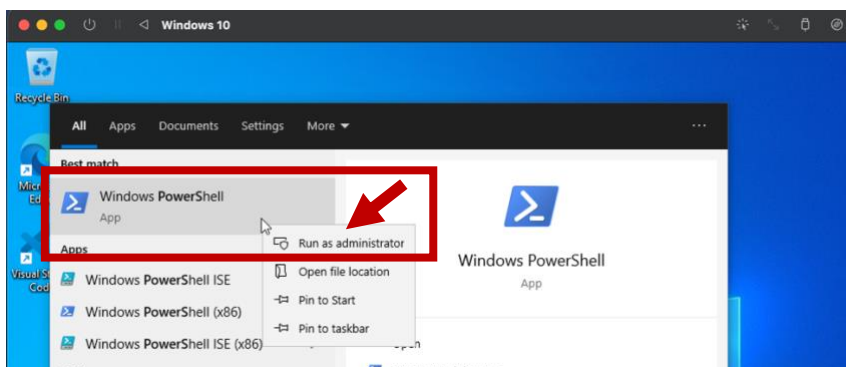
4 Run the following commands to download and install the Wazuh agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.6.0-1.msi -OutFile $(env:tmp)\wazuh-agent; msisexec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='192.168.1.70' WAZUH_AGENT_NAME='Windows_Mac_UTM' WAZUH_REGISTRATION_SERVER='192.168.1.70'
```

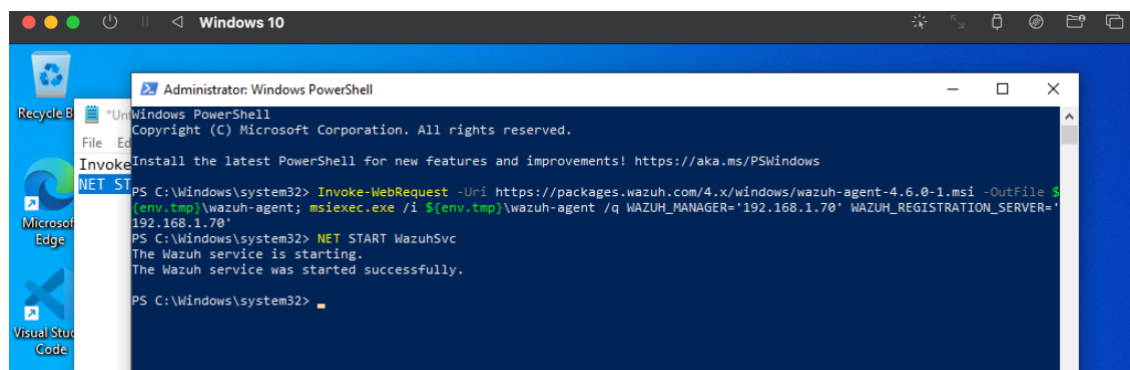
5 Start the Wazuh agent:

```
NET START WazuhSvc
```

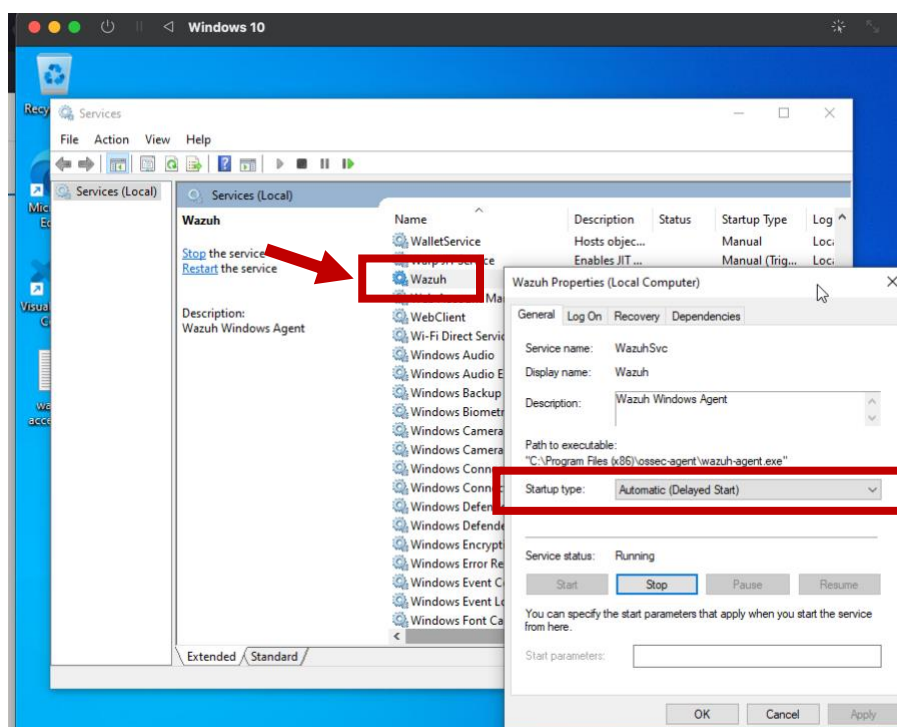
**Passo 14** – No computador “agente” deve abrir uma aplicação chamada Powershell e em modo de administrador (clique em cima da aplicação com o lado direito do rato):



**Colocar os códigos que foram gerados no passo anterior:**

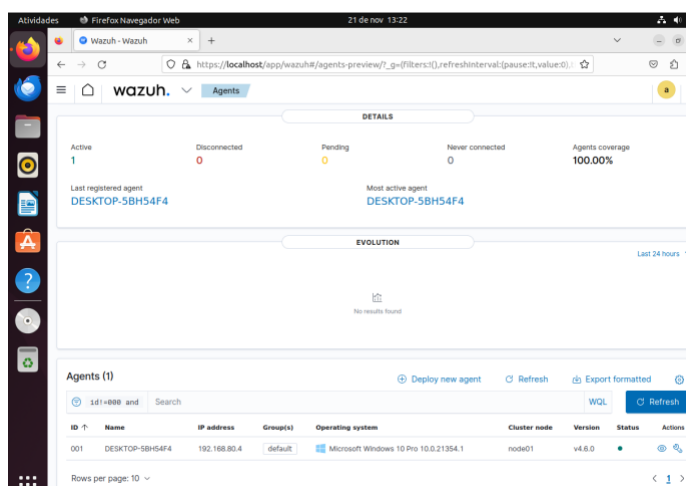


Feito os passos anteriores, será exibida a janela dos serviços que estão a correr no Windows e devem selecionar um serviço (basta clicar uma vez com o lado esquerdo do rato num dos serviços) e depois escrever nas teclas as iniciais “waz” e automaticamente este irá para o serviço mais próximo com a expressão de digitou no teclado. Quando detetar o serviço do Wazuh, dê dois cliques com o lado esquerdo do rato e irá ver a seguinte imagem:



**Se**, na opção Startup type não estiver a mesma opção está na imagem mais acima, deverá carregar no botão stop e alterar o valor para “Automatic (Delayed Start)” e clicar no botão Start.

**Passo 15** – Depois da mensagem de sucesso, vamos a plataforma do Wazuh e verificar se já está anexado o novo agente:



Eventualmente se não conseguir detetar alguma coisa (especialmente com sistemas recentes), significa que temos de verificar alguns pontos importantes, pois **só isso, pode não ser o suficiente para detetar automaticamente os agentes.**

A firewall do Windows 11 ou o antivírus podem bloquear as comunicações de saída. O Wazuh precisa das portas **1514** (ligação do Agente) e **1515** (registo/enrollment) abertas via TCP.

**Abra o PowerShell no Windows 11 como Administrador e execute:**

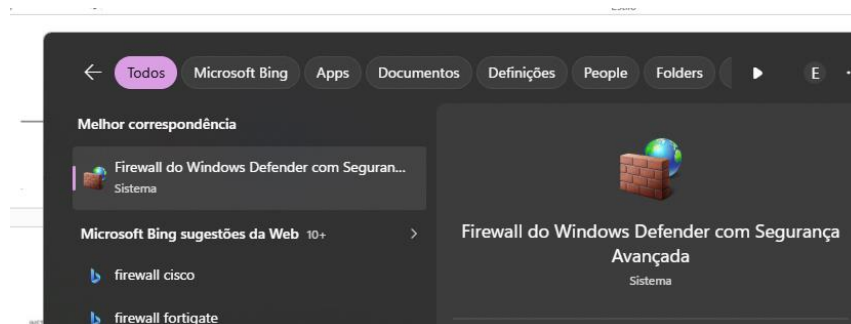
Test-NetConnection -ComputerName ip\_servidor\_wazuh -Port 1514

```
PS C:\WINDOWS\system32> Test-NetConnection -ComputerName 192.168.1.74 -Port 1514
WARNING: TCP connect to (192.168.1.74 : 1514) failed
WARNING: Ping to 192.168.1.74 failed with status: 11050

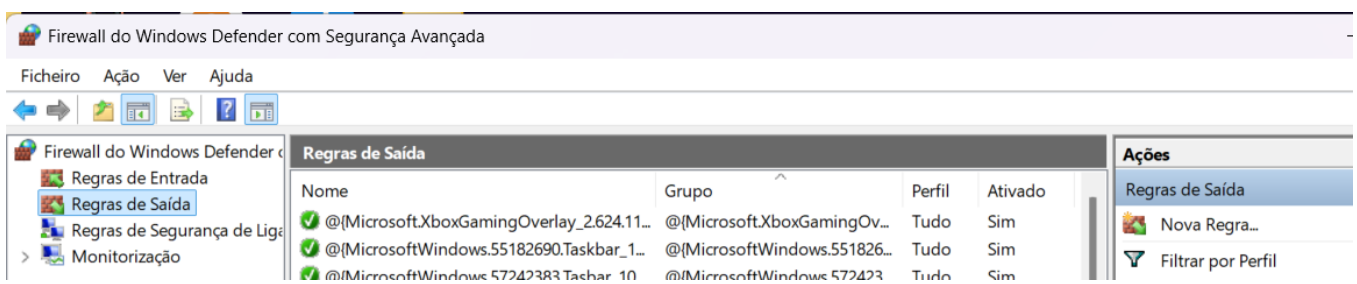
ComputerName           : 192.168.1.74
RemoteAddress           : 192.168.1.74
RemotePort              : 1514
InterfaceAlias          : Ethernet
SourceAddress           : 192.168.1.74
PingSucceeded           : False
PingReplyDetails (RTT) : 0 ms
TcpTestSucceeded        : False
```

Se der ligação falhada, vamos ter de abrir uma exceção na firewall (no Ubuntu e no Windows). Como tal, vamos dazer o seguinte:

**Passo 1 – Abrir a firewall do sistema Windows:**



**Passo 2 – Do lado esquerdo seleccione a opção Regras de Saída e depois no lado direito clique em nova regra:**



**Passo 3 – Peça para adicionar uma nova regra pela porta:**

Assistente de Novas Regras de Saída

### Tipo de Regra

Especifique o tipo de regra de firewall a criar.

**Passos:**

- Tipo de Regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Que tipo de regra gostaria de criar?

Programa  
Regra que controla as ligações para um programa.

Porta  
Regra que controla as ligações para uma porta TCP ou UDP.

### Protocolo e Portas

Especifique os protocolos e portas a que esta regra se aplica.

**Passos:**

- Tipo de Regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Esta regra é aplicada ao protocolo TCP ou UDP?

TCP

UDP

Esta regra é aplicada a todas as portas remotas ou a portas remotas espe

Todas as portas remotas

Portas remotas específicas:   
Exemplo: 80, 443, 5000-5010

Assistente de Novas Regras de Saída

### Ação

Especifique a ação a executar quando uma ligação corresponde às condições especificadas na regra.

**Passos:**

- Tipo de Regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Que ação deve ser executada quando uma ligação corresponde às condições especif

Permitir a ligação  
Isto inclui ligações protegidas, ou não, com IPsec.

Permitir a ligação se for segura  
Isto inclui apenas ligações autenticadas através da utilização de IPsec. As ligações protegidas utilizando as definições de propriedades IPsec e as regras no nó de Reg Segurança da Ligação.

Bloquear a ligação

**Perfil**  
Especifique os perfis para os quais esta regra se aplica.

**Passos:**

- Tipo de Regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Quando é que esta regra é aplicada?

- Domínio**  
É aplicada quando um computador está ligado ao respetivo domínio empresarial.
- Privado**  
É aplicada quando um computador está ligado a uma localização de rede privada, tal como uma casa ou um local de trabalho.
- Público**  
É aplicada quando um computador está ligado a uma localização de redes públicas.

 Assistente de Novas Regras de Saída

**Nome**  
Especifique o nome e descrição desta regra.

**Passos:**

- Tipo de Regra
- Protocolo e Portas
- Ação
- Perfil
- Nome

Nome:  
Wazuh Saida Agente

**Faça o mesmo para a porta 1515 e coloque o nome “Wazuh Saida Sincronização Agente”**

**Passo 4** – Peça para adicionar uma nova regra de entrada (mesmo processo anterior) com as seguintes informações:

- **Adicionar porta 1514 e coloque o nome “Wazuh Entrada Agente”**
- **Adicionar porta 1515 e coloque o nome “Wazuh Entrada Sincronização Agente”**

**Passo 5** – Só isto ainda não é necessário, pois ainda falta abrir as portas do lado do servidor. Como tal, vamos abrir um terminal no ubuntu e colocar as seguintes regras (porta 1514 e 1515):

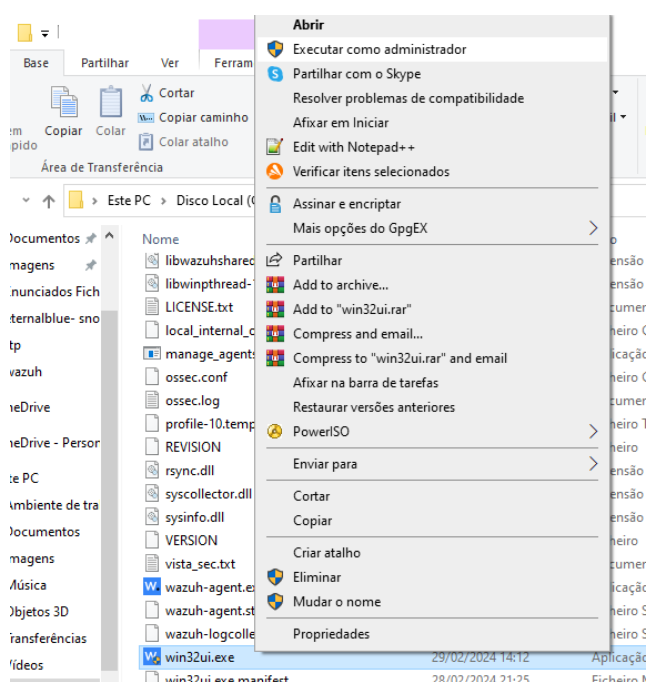
**ufw allow 1514/tcp**

**ufw allow 1515/tcp**

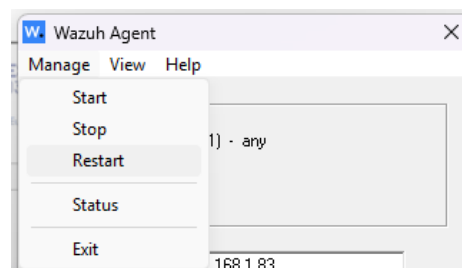
```
root@bruno-VirtualBox:/home/bruno# ufw allow 1514/tcp
Regra adicionada
Regra adicionada (v6)
root@bruno-VirtualBox:/home/bruno# ufw allow 1515/tcp
Regra adicionada
Regra adicionada (v6)
```

**Passo 6** – Agora precisamos de reiniciar o serviço do agente que está instalado no Windows, mais especificamente, no diretório **C: → Programas x86 → pasta ossec-agent:**

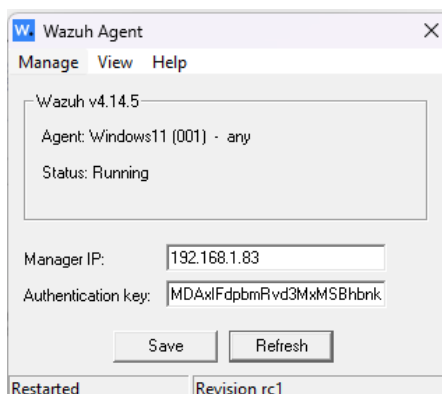
Dentro deste ficheiro (perto do final da pasta), temos o programa win32ui.exe. Esta é uma interface gráfica para ajudar gerir o agente e deve ser executado em modo de administrador:



Ao abrir a aplicação, peça para reiniciar o serviço do agente:

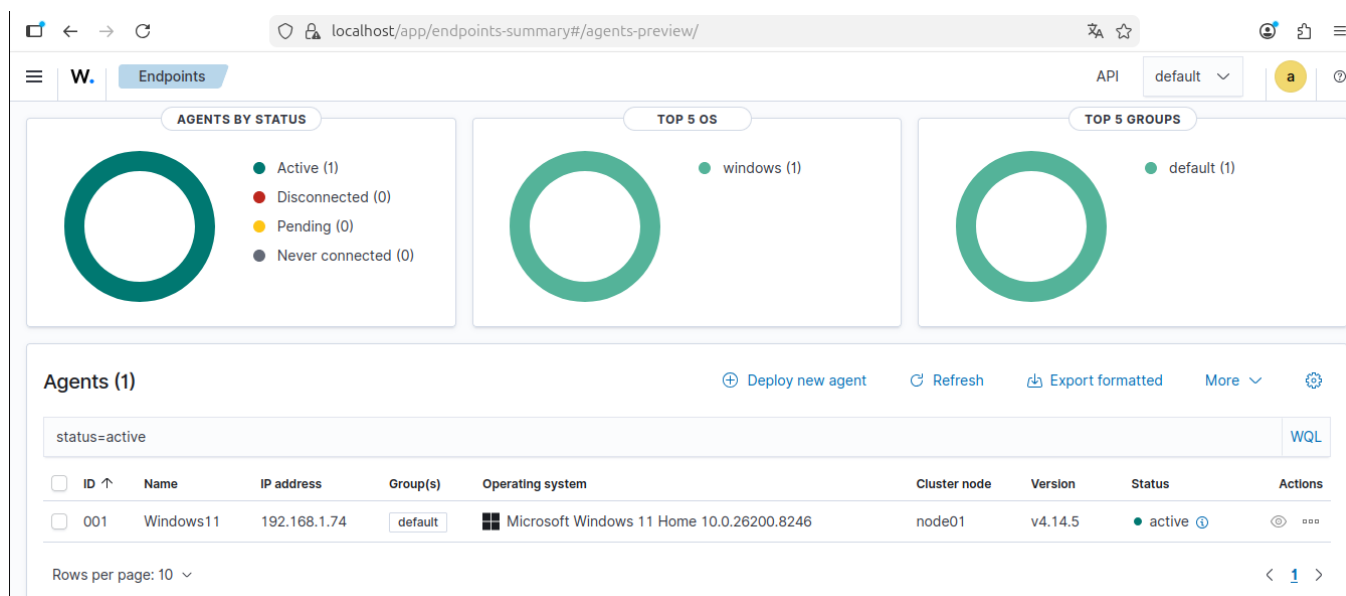
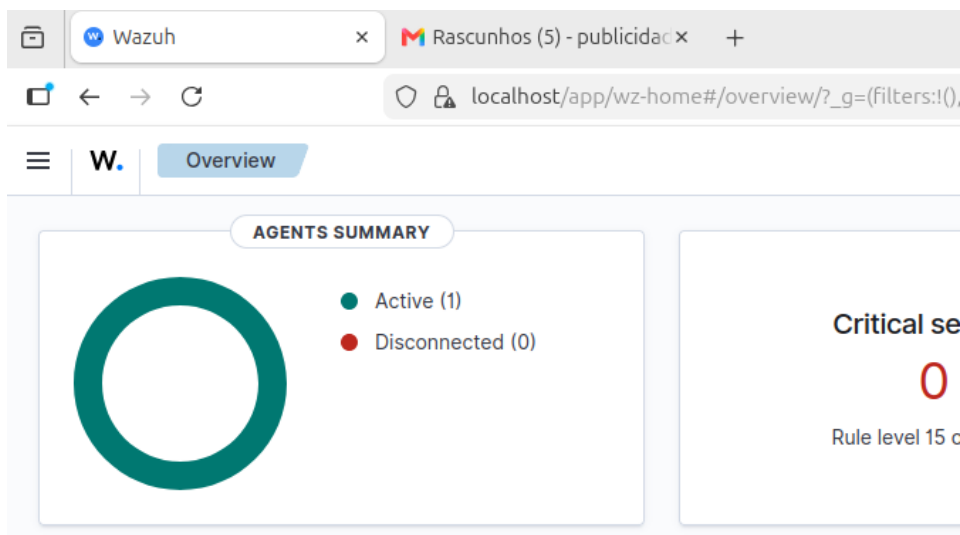


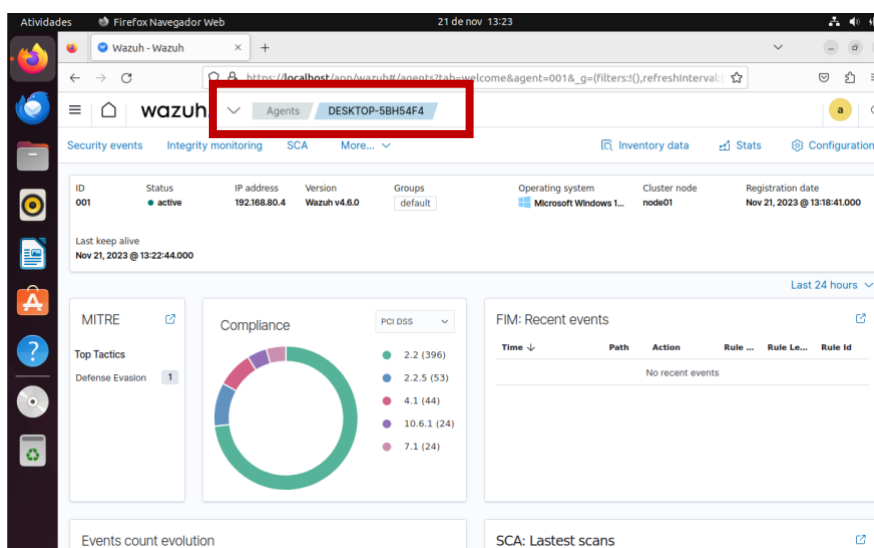
E logo de seguida, o campo “Authentication Key” deve colocar a chave de sincronização:



Volte a carregar a página do wazuh no Ubuntu e veja a deteção do equipamento.

**Passo 17** – Com o novo agente associado, podemos aceder as informações da Máquina Agente, como demonstra a seguinte imagem:

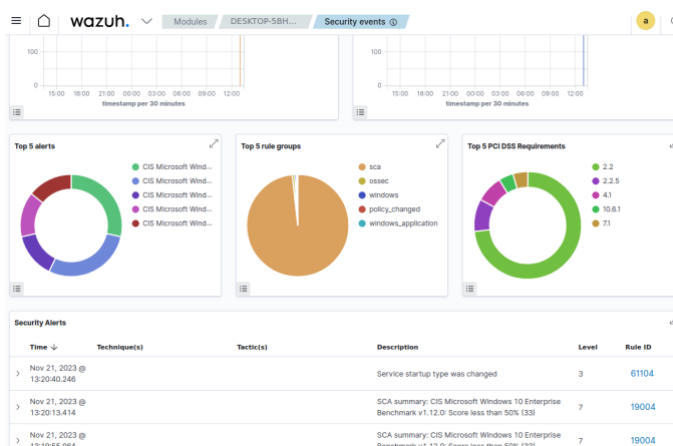




**Passo 17** – Quando estiver dentro de um agente, terá uma barra de navegação, do qual, pode consultar informações como eventos de segurança, monitorização, entre outros parâmetros. Vamos explorar o ambiente de trabalho!



Quando entrar dentro de cada opção o conteúdo mais abaixo, será modificado com base na opção selecionada. Para este exemplo, temos o ecrã inicial (de cada agente), do qual, tem os menus de navegação e os relatórios do que aconteceu nos últimos tempos:

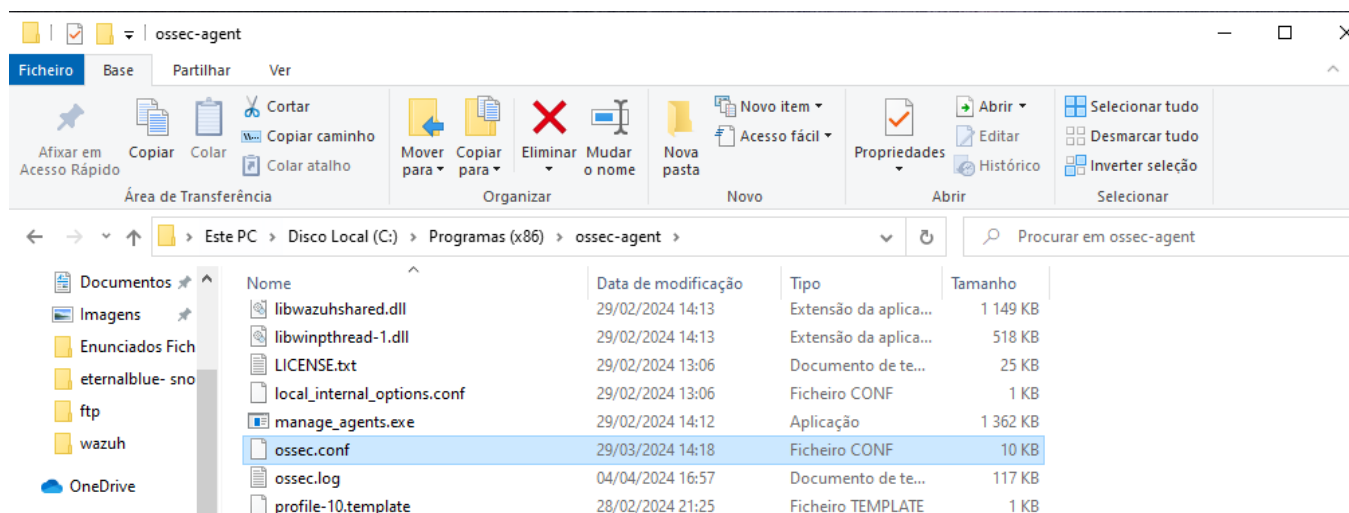


Se eventualmente reiniciar o computador agente. Quando iniciar o sistema, na plataforma do Wazuh, a seção dos Security Alerts mostra as notificações do fim de sessão na máquina e não só:

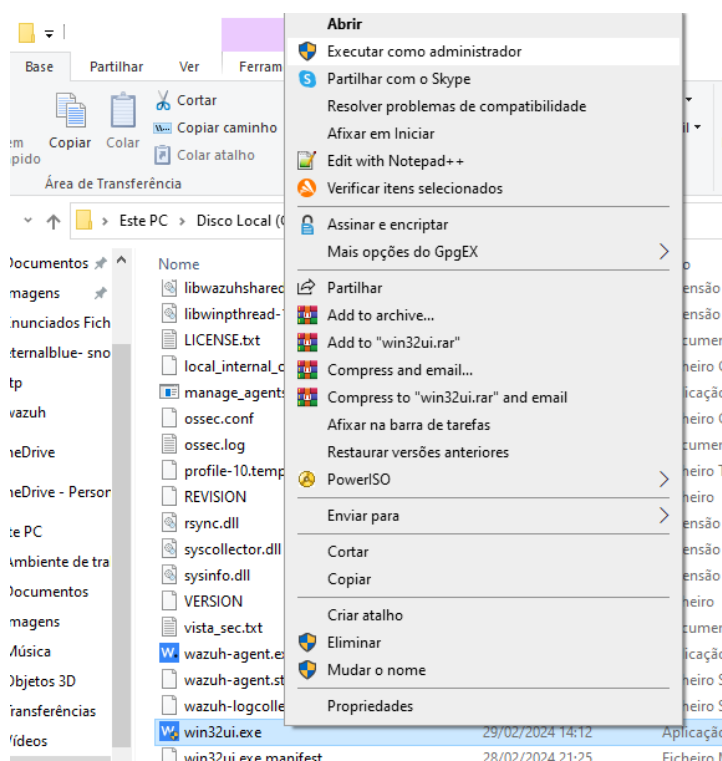
Time ↓	Technique(s)	Tactic(s)	Description	Level	Rule ID
> Nov 21, 2023 @ 13:25:13.589			Windows application error event.	9	60602
> Nov 21, 2023 @ 13:25:13.192			SessionEnv was unavailable to handle a notification event.	5	60775
> Nov 21, 2023 @ 13:25:13.113			WSearch was unavailable to handle a notification event.	5	60775
> Nov 21, 2023 @ 13:25:12.998			Windows User Logoff.	3	60137
> Nov 21, 2023 @ 13:24:44.883			The Windows logon process has failed to terminate currently logged on user's processes.	5	60789
> Nov 21, 2023 @ 13:23:24.686			Software protection service scheduled successfully.	3	60642

### Parte 3 – Sincronização de informação

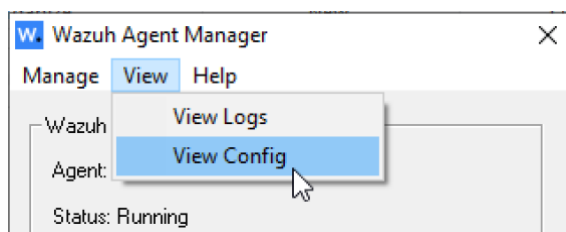
Quando o agente é instalado no Windows, este fica alojado no diretório C:, mais especificamente, na pasta Programas x86 → pasta ossec-agent:



Dentro deste ficheiro (perto do final da pasta), temos o programa win32ui.exe. Esta é uma interface gráfica para ajudar gerir o agente e deve ser executado em modo de administrador:

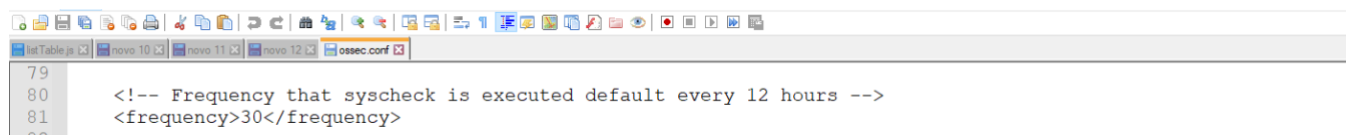


Dentro desta aplicação, vamos ao menu View e selecione a opção View Config, para modificar as propriedades do agente:



Por norma, o agente vem com configurações pré-desenvolvidas na instalação do agente, mas, agora queremos alterar algumas dessas propriedades, como por exemplo:

- O tempo de sincronização (em segundos) do qual deve mudar para 30 segundos:



- Mais abaixo, inserir uma linha de monitorização do ambiente de trabalho do agente. Para tal, vamos adicionar uma nova linha (normalmente linha 98 até costuma estar em branco):

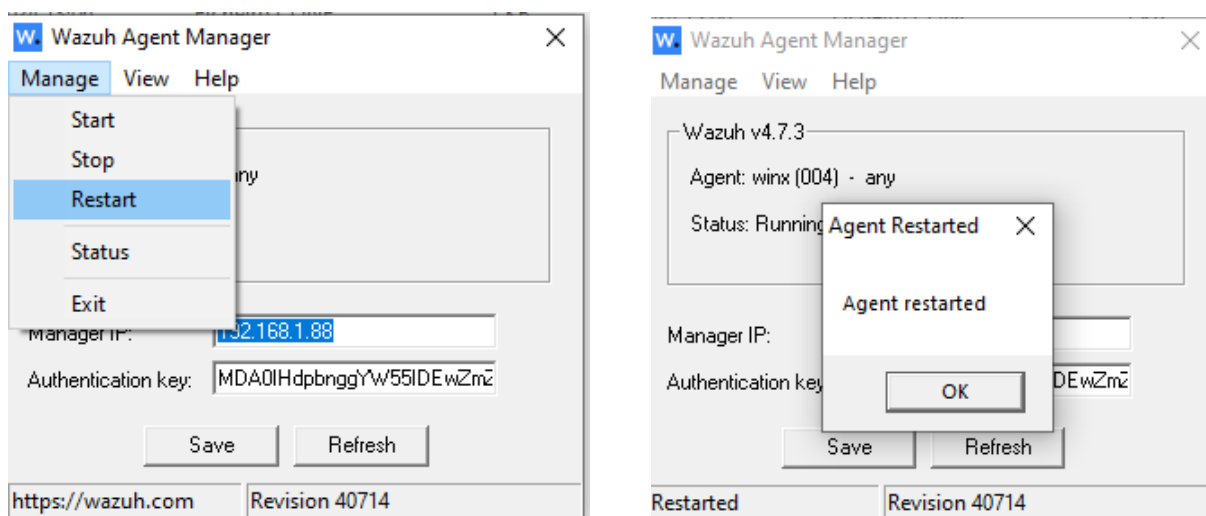
**<directories realtime="yes" report\_changes="yes" check\_all="yes">localização do ambiente de trabalho</directories>**

```

79
80 <!-- Frequency that syscheck is executed default every 12 hours -->
81 <frequency>30</frequency>
82
83 <!-- Default files to be monitored. -->
84 <directories recursion_level="0" restrict="regedit.exe$|system.ini$|win.ini$" %WINDIR%</directories>
85
86 <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$
87 <directories recursion_level="0">%WINDIR%\SysNative\drivers\etc</directories>
88 <directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\SysNative\wbem</directories>
89 <directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\SysNative\WindowsPowerShell\v1.0</direc
90 <directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\SysNative</directories>
91
92 <!-- 32-bit programs. -->
93 <directories recursion_level="0" restrict="at.exe$|attrib.exe$|cacls.exe$|cmd.exe$|eventcreate.exe$|ftp.exe$
94 <directories recursion_level="0">%WINDIR%\System32\drivers\etc</directories>
95 <directories recursion_level="0" restrict="WMIC.exe$" %WINDIR%\System32\wbem</directories>
96 <directories recursion_level="0" restrict="powershell.exe$" %WINDIR%\System32\WindowsPowerShell\v1.0</direct
97 <directories recursion_level="0" restrict="winrm.vbs$" %WINDIR%\System32</directories>
98 <directories realtime="yes" report_changes="yes" check_all="yes">C:\Users\Silva</directories>
99 <directories realtime="yes">%PROGRAMDATA%\Microsoft\Windows\Start Menu\Programs\Startup</directories>
100

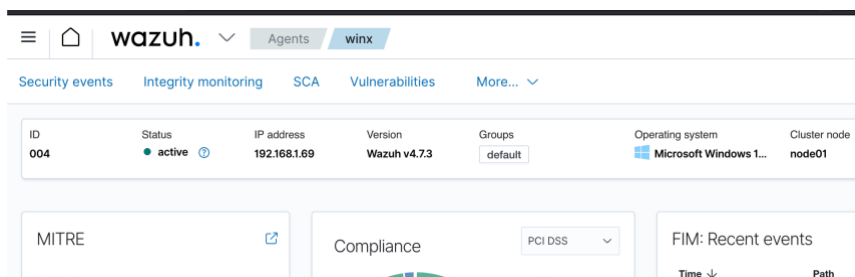
```

**No final grave as alterações e feche o editor das configurações e deve reiniciar o agente Wazuh. Para tal, faça os seguintes passos:**

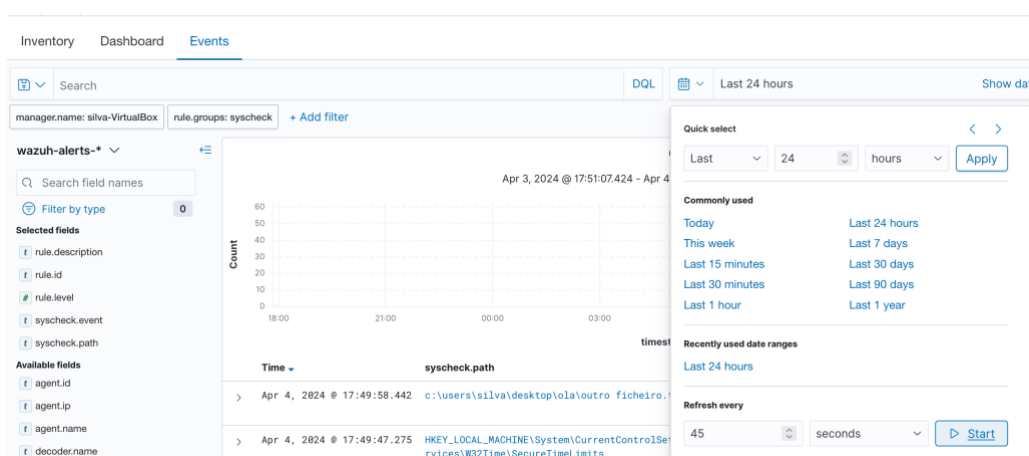


#### Parte 4 – Verificar estados e registos

**Passo 1** – Aceda a página do Wazuh e entre dentro do agente ativo. De seguida, no meu superior, vamos clicar na opção “Integrity Monitoring”:



**Passo 2** – Após clicar na opção “Events”, localize o botão do calendário e depois de clicar no mesmo, vamos pedir para fazer sincronização a cada 30 ou 45 segundos e clique no botão Start:



**Passo 3** – No computador onde está o agente, deve criar um ficheiro no ambiente de trabalho e no wazuh deve verificar se aparece a confirmação da criação do ficheiro:



```

f syscheck.attrs_after      ARCHIVE

f syscheck.changed_attributes size, mtime, md5, sha1, sha256

f syscheck.diff             ---
> ja viram como funciona?

f syscheck.event            modified

f syscheck.md5_after        99d8891f0419b0ef9c3bf36969dd0404
    
```