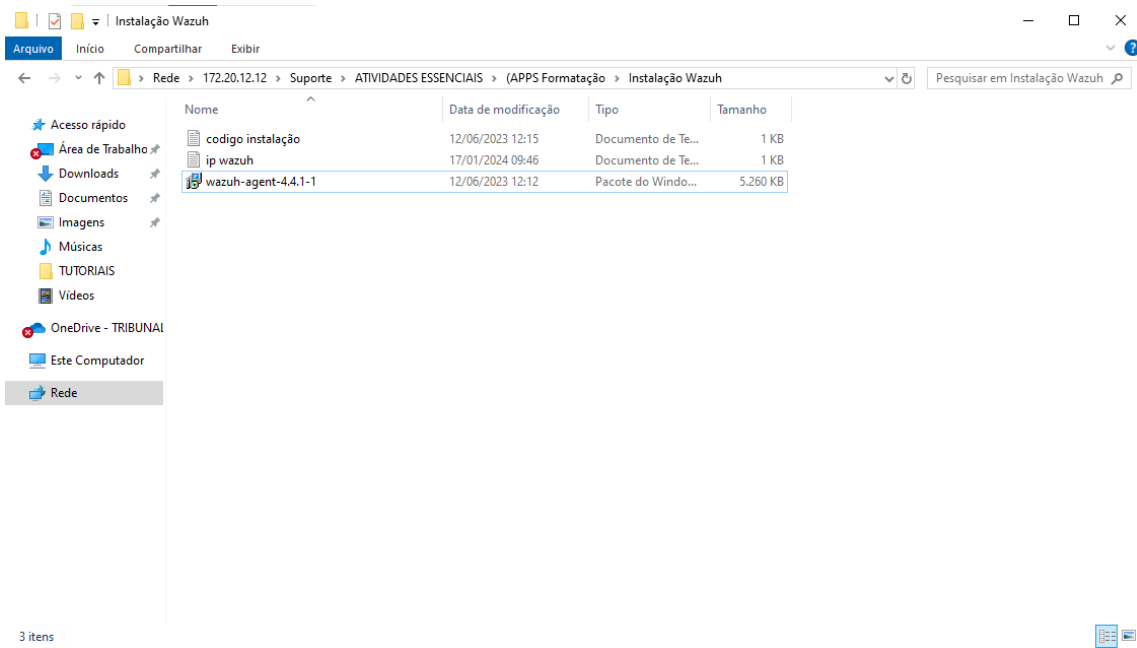


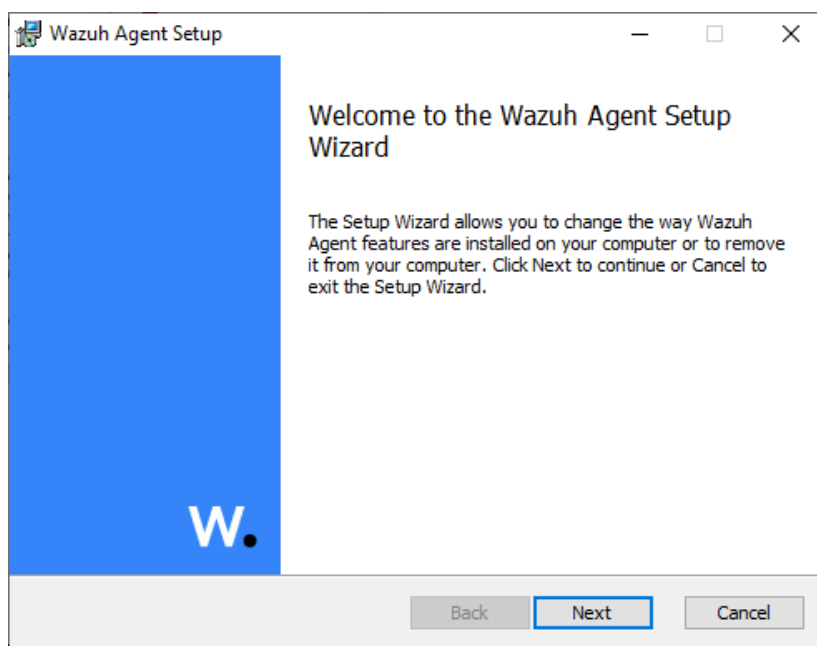
MA_SM-04		Código MA_SM-04	Rev 01	 TRIBUNAL DE CONTAS DO ESTADO DO ACRE
Nome do documento INSTALAÇÃO E MANUTENÇÃO DO WAZUH				

Elaboração		Aprovação	
Assinatura	Data	Assinatura	Data
Iago da Silva Ferreira	23/01/2024		
Nome: Cargo:	Iago da Silva Ferreira Estagiário	Nome: Cargo:	Claudio Pontes Diretor - DTI

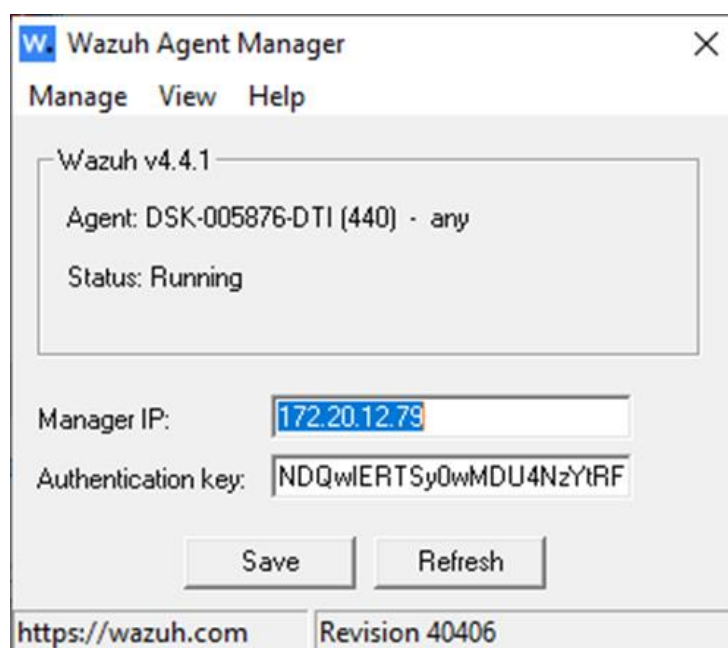
INSTALAÇÃO E MANUTENÇÃO DO WAZUH



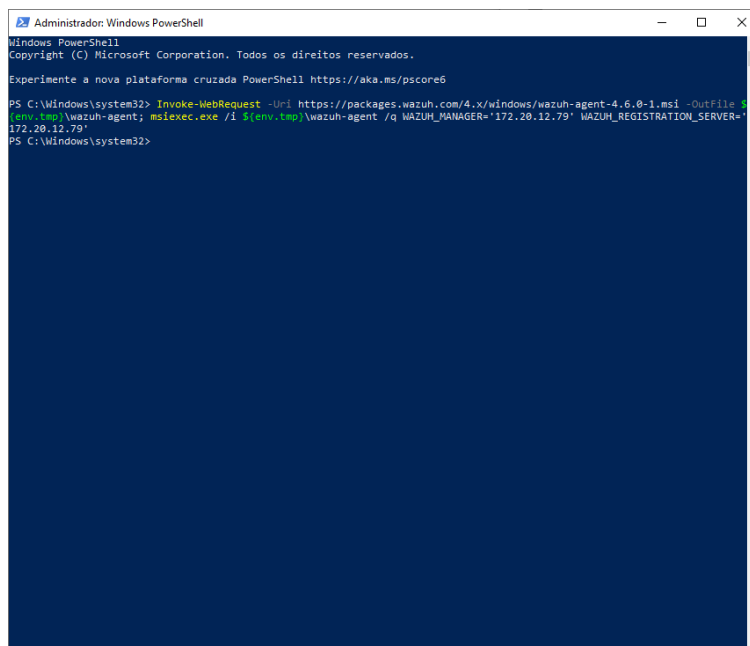
Passo 1: Procure o agente na pasta do suporte (<\\172.20.12.12>) - Ele vai ser encontrado no endereço “\\172.20.12.12\Suporte\ATIVIDADES ESSENCIAIS\APPS Formatação\Instalação Wazuh” o agente é o programa “wazuh-agent-4.4.1-1.msi”.



Passo 2: Inicie a instalação - Execute ele e se necessário dê a permissão de administrador.



Passo 3: Configure o agente - Vá em "C:\Program Files (x86)\ossec-agent" e execute o programa "win32ui.exe" e coloque o seguinte ip "172.20.12.79", logo após isso salve no botão "Save" e vá em "Manage" e "Restart", logo após fique apertando Refresh até aparecer a chave criptografada.



```

Administrador: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. Todos os direitos reservados.

Experimente a nova plataforma cruzada PowerShell https://aka.ms/pscore6

PS C:\Windows\system32> Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.6.0-1.msi -OutFile $(env:tmp)\wazuh-agent; msixec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER='172.20.12.79' WAZUH_REGISTRATION_SERVER='172.20.12.79'
PS C:\Windows\system32>

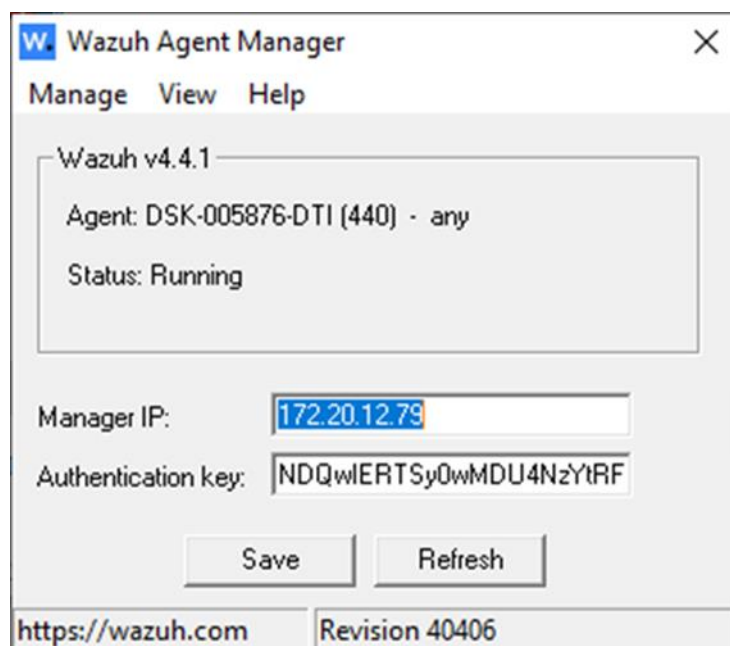
```

Passo 4(Opcional): Executar instalação via comando PowerShell - Execute o PowerShell como administradore e coloque o seguinte comando: "Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.6.0-1.msi -OutFile \$(env:tmp)\wazuh-agent; msixec.exe /i \$(env:tmp)\wazuh-agent /q WAZUH_MANAGER='172.20.12.79' WAZUH_REGISTRATION_SERVER='172.20.12.79'" e logo em seguida execute "NET START WazuhSvc" para iniciar o programa.

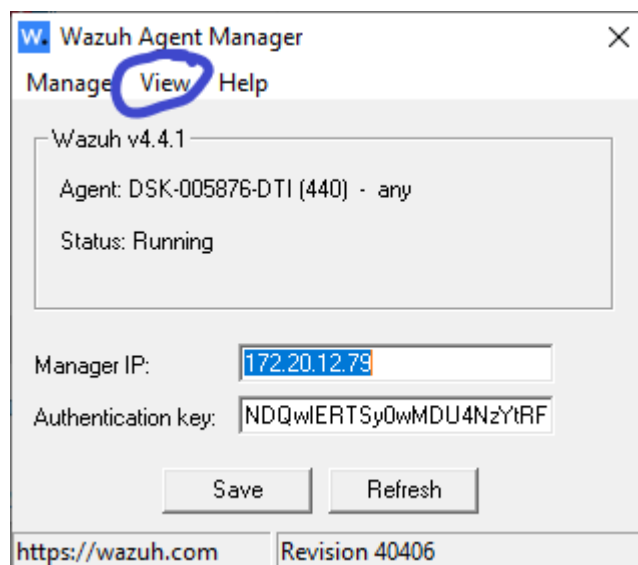


Manutenção - Em caso de erros e perda de conexão será comunicado pela infraestrutura, o passo a passo para resolver é o que será documentado abaixo.





Passo 1: Abra o programa de configuração - Vá em "C:\Program Files (x86)\ossec-agent" e execute o programa "win32ui.exe"



Passo 2: Abra as configurações - Para isso vá em "View" e abra "View Config"

```

ossec.conf - Bloco de Notas
Arquivo  Editar  Formatar  Exibir  Ajuda
k!--
Wazuh - Agent - Default configuration for Windows
More info at: https://documentation.wazuh.com
Mailing list: https://groups.google.com/forum/#!forum/wazuh
-->

<ossec_config>

<client>
  <server>
    <address>172.20.12.79</address>
    <port>1514</port>
    <protocol>tcp</protocol>
  </server>
  <config-profile>windows, windows10</config-profile>
  <config-profile>windows, windows10</config-profile>
  <crypto_method>aes</crypto_method>
  <notify_time>10</notify_time>
  <time-reconnect>60</time-reconnect>
  <auto_restart>yes</auto_restart>
  <enrollment>
    <enabled>yes</enabled>
    <manager_address>172.20.12.79</manager_address>
    <manager_address>172.20.12.79</manager_address>
  </enrollment>
  <enrollment>
    <enabled>yes</enabled>
    <manager_address>172.20.12.79</manager_address>
  </enrollment>
</client>

<!-- Agent buffer options -->
<client_buffer>
  <disabled>no</disabled>
  <queue_size>5000</queue_size>

```

Passo 3: Edite as configurações em protocolo - Procure pela linha "Protocol" e se estiver como "udp" passe para "tcp"