

Licenciatura em Engenharia Informática

Gestão de Redes



AthTek NetWalk

AThTek Ip-Mac Scanner

Ansible

Francisco Amaral 21280426

Índice

2. Introdução	3
3. Processo de instalação	4
3.1 AthTek IP-Mac Scanner	4
3.2 AthTek NetWalk Enterprise	6
3.3 Ansible	7
4. Processo de configuração	8
4.1 AthTek IP-MAC Scanner	8
4.2 AthTek NetWalk Enterprise	8
4.3 Ansible	8
5. Funcionalidades	9
5.1 AthTek IP-Mac Scanner	9
5.2 AthTek NetWalk Enterprise	10
5.3 Ansible	13
6. Conclusão	16
6.1 AthTek IP-MacScanner	16
6.2 AthTek NetWalk Enterprise	16
6.3 Ansible	16
7. Bibliografia	17

2. Introdução

Foi proposto a realização de um trabalho sobre algumas ferramenta de gestão de redes. Neste projeto foram escolhidas duas ferramentas da mesma empresa, AthTek, e uma ferramenta de monitoramento de websites, o Pingdom, da SolarWinds.

O **IP/Mac Scanner** suporta a análise dos resultados da digitalização para rastrear clientes desconhecidos. Uma ferramenta de ping está incluída no IP - MAC Scanner, para que se possa efetuar pings de forma facilitada, a quaisquer endereços IP a partir dos resultados da verificação. Também é possível encontrar funções de controle remoto e notificação por e-mail no scanner IP - MAC lateral.

O **AthTek NetWalk** é uma ferramenta de análise de infraestrutura de rede que ajuda no gerenciamento, manutenção e solução de problemas de todos os tipos de redes. É particularmente útil para novos administradores de rede que desejam obter um conhecimento profundo sobre a infraestrutura e gerenciamento de rede.

Contém representações gráficas da rede, usando advanced packet sniffing, para ajudar a projetar o estado da rede em formato estatístico e gráfico.

Permite também que os usuários configurem warnings para ocorrer eventos, tal como envio de e-mails, programas em execução etc. Se houver uma comunicação de rede não confiável, basta configurar um filtro no gerenciamento de eventos para identificá-lo, ou até mesmo bloqueá-lo.

O **Ansible** é uma ferramenta gratuita em open source para automatizar, configurar servidores e instalar aplicações a partir de uma localização central.

3. Processo de instalação

3.1 AthTek IP-Mac Scanner



Figura 1



Figura 2 - Ferramenta instalada

Quando a ferramenta é instalada aparece um pedido de registo, pois tem um limite de trial de 15 dias. Aqui, é seleccionada a opção Trial se não tiver comprado ou registrado.

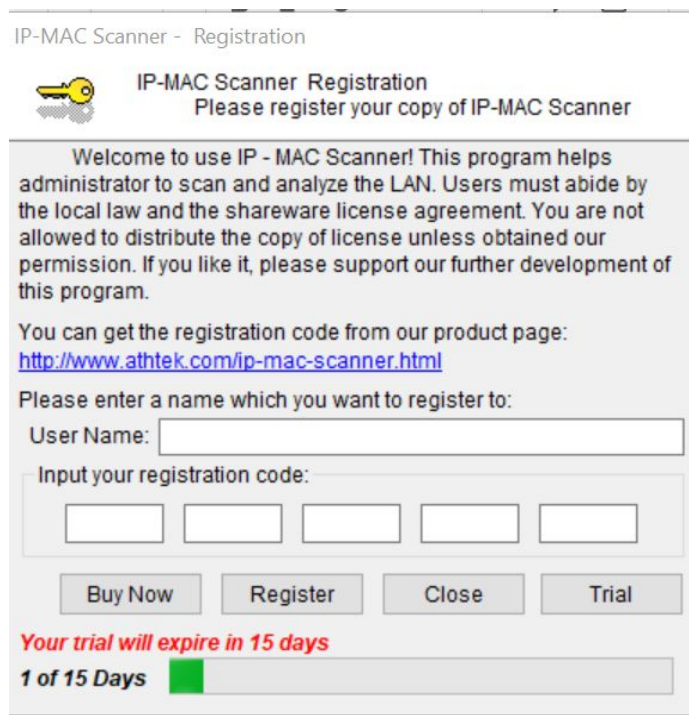


Figura 3

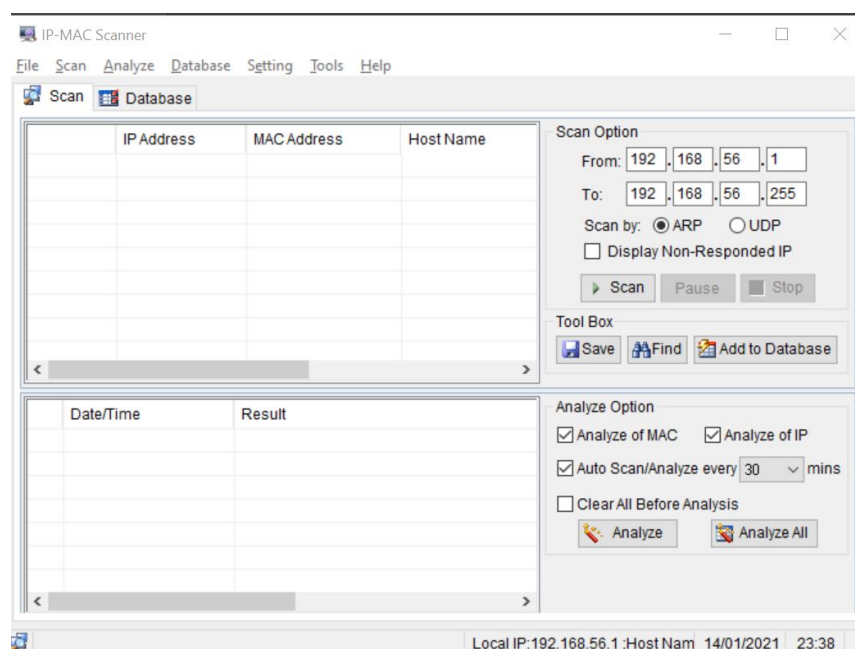


Figura 4 - Ferramenta instalada e pronta a ser usada.

3.2 AthTek NetWalk Enterprise

Igualmente ao IP-Mac Scanner, e como seria de esperar visto que são da mesma empresa, é pedido o registo ou a compra do produto, porém para este projeto e testes foi usado a versão trial(Opção Try).

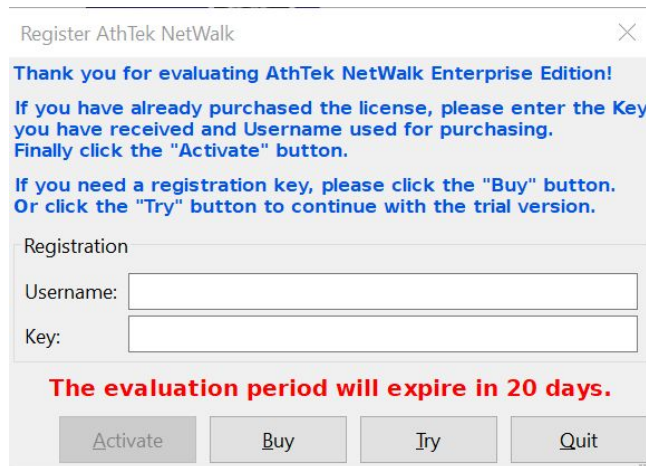


Figura 5

3.3 Ansible

Primeiro é feita a instalação do python3

```
francisco@francisco-VirtualBox:~$ sudo apt-get install python3-pip
```

Figura 6 - Instalação de python3

De seguida instala-se o ansible (pip3 install ansible e sudo apt install ansible)

```
francisco@francisco-VirtualBox:~$ pip3 install ansible
Collecting ansible
  Downloading ansible-2.10.5.tar.gz (29.1 MB)
    | 29.1 MB 6.5 MB/s
Collecting ansible-base<2.11,>=2.10.4
  Downloading ansible-base-2.10.4.tar.gz (5.7 MB)
    | 5.7 MB 3.1 MB/s
Requirement already satisfied: PyYAML in /usr/lib/python3/dist-packages (from ansible-base<2.11,>=2.10.4->ansible) (5.3.1)
Requirement already satisfied: cryptography in /usr/lib/python3/dist-packages (from ansible-base<2.11,>=2.10.4->ansible) (2.8)
Collecting jinja2
  Downloading Jinja2-2.11.2-py2.py3-none-any.whl (125 kB)
    | 125 kB 8.2 MB/s
Collecting packaging
  Downloading packaging-20.8-py2.py3-none-any.whl (39 kB)
Requirement already satisfied: MarkupSafe>=0.23 in /usr/lib/python3/dist-packages (from jinja2->ansible-base<2.11,>=2.10.4->ansible) (1.1.0)
Collecting pyparsing>=2.0.2
  Downloading pyparsing-2.4.7-py2.py3-none-any.whl (67 kB)
    | 67 kB 3.0 MB/s
Building wheels for collected packages: ansible, ansible-base
  Building wheel for ansible (setup.py) ... done
  Created wheel for ansible: filename=ansible-2.10.5-py3-none-any.whl size=47721392 sha256=8aca49e0f95d46338e063d4adba3d3235906608649ddf6ab464b597cf3e47b27
  Stored in directory: /home/francisco/.cache/pip/wheels/2d/ee/2b/3f9436f9fc4a6a226b7ae4fdc716703b6e5b39dad30e93324
  Building wheel for ansible-base (setup.py) ... done
  Created wheel for ansible-base: filename=ansible_base-2.10.4-py3-none-any.whl size=1868520 sha256=476def211dbceab6b92241b331ebae76a8634429e42f5d3aa83cb7902c111f6
  Stored in directory: /home/francisco/.cache/pip/wheels/06/63/a2/bda2e97bcb84ab543994ab4bb8552866d0f1c074a3a0794979
Successfully built ansible ansible-base
Installing collected packages: jinja2, pyparsing, packaging, ansible-base, ansible
Successfully installed ansible-2.10.5 ansible-base-2.10.4 jinja2-2.11.2 packaging-20.8 pyparsing-2.4.7
francisco@francisco-VirtualBox:~$
```

```
francisco@francisco-VirtualBox:/etc$ sudo apt install ansible
```

Figura 7 e 8- Ansible instalado com sucesso

4. Processo de configuração

4.1 AthTek IP-MAC Scanner

Como foi visto na figura 5, temos um GUI que nos permite escolher a pool de IPs onde a pesquisa de IPs/MACs vai ocorrer.

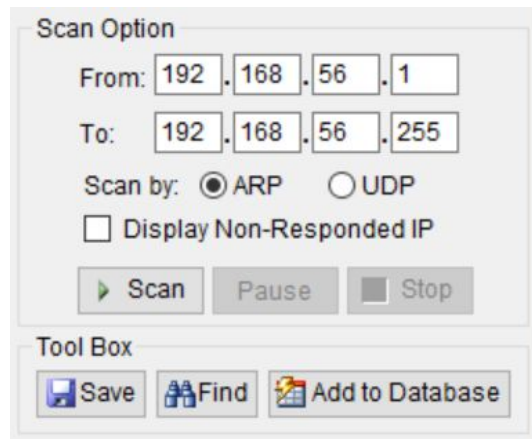


Figura 9

4.2 AthTek NetWalk Enterprise

Quando a ferramenta é aberta pela primeira vez é preciso escolher qual o adaptador de rede é que ele irá funcionar sobre.

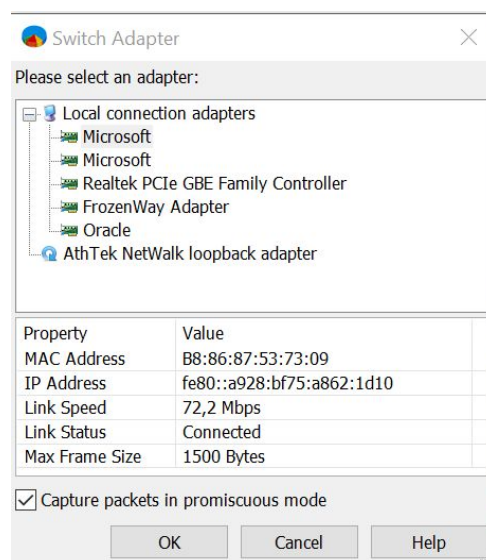


Figura 10

4.3 Ansible

Para começar a configurar o Ansible, existem dois ficheiros distintos, **ansible.cfg** e **hosts**. Estes ficheiros estão na diretoria `/etc/ansible/`, como podemos ver na imagem.

```
francisco@francisco-VirtualBox:~$ cd /etc/ansible/  
francisco@francisco-VirtualBox:/etc/ansible$ ls  
ansible.cfg  hosts
```

Figura 11

Como é óbvio, o `ansible.cfg` é onde estão as configurações do Ansible e o `hosts` contém a lista de servidores que irão ser “controlados”.

O ficheiro `hosts` é bastante importante, sendo também conhecido como Inventário, pois contém a lista de máquinas linux, routers, switches que irão ser controlados.

No ficheiro `hosts`, pode fazer grupos de hosts com elementos `[]`, por exemplo

```
# Ex 2: A collection of hosts belonging to the 'webservers' group

#[webservers]
#alpha.example.org
#beta.example.org
#192.168.1.100
#192.168.1.110
```

Figura 12

No exemplo para teste, usei simplesmente a própria máquina (localhost) para verificar o comando do Ansible. Basta acrescentar isto ao ficheiro de `hosts`.

```
localhost ansible_connection=local
```

Figura 13

5. Funcionalidades

5.1 AthTek IP-Mac Scanner

Depois de carregar em “Scan” é visível todos os ips e macs que estão na pool de IPs que foi escolhida pelo utilizador.

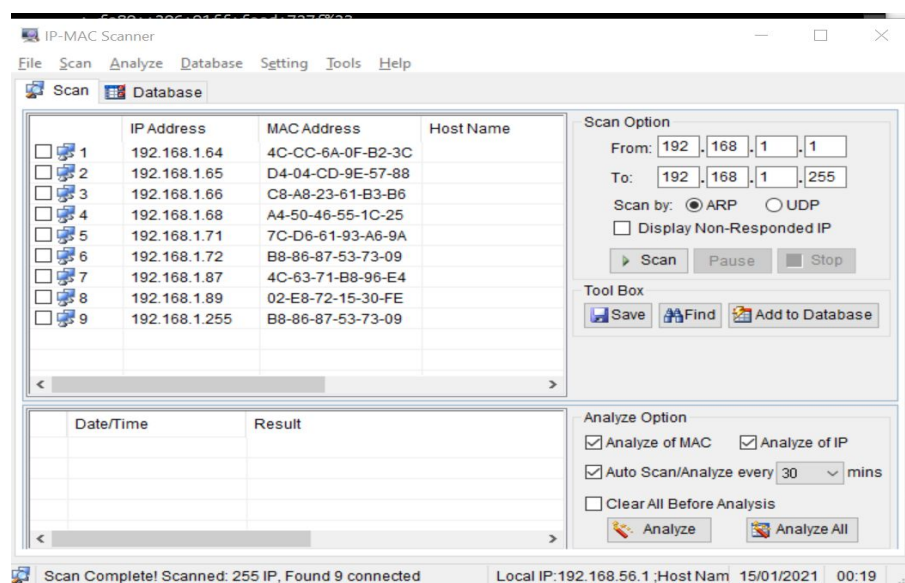


Figura 14

É possível adicionar estes IPs/MACs a uma base de dados da ferramenta, e também convertê-los numa tabela excel (Opção Export to Excel)

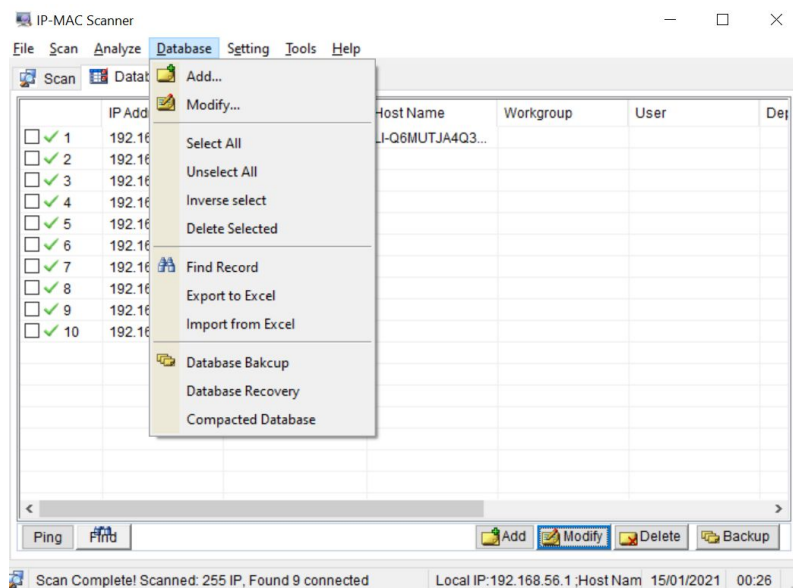


Figura 15

Depois há um conjunto de ferramentas que se pode aplicar sobre os IPs selecionados.

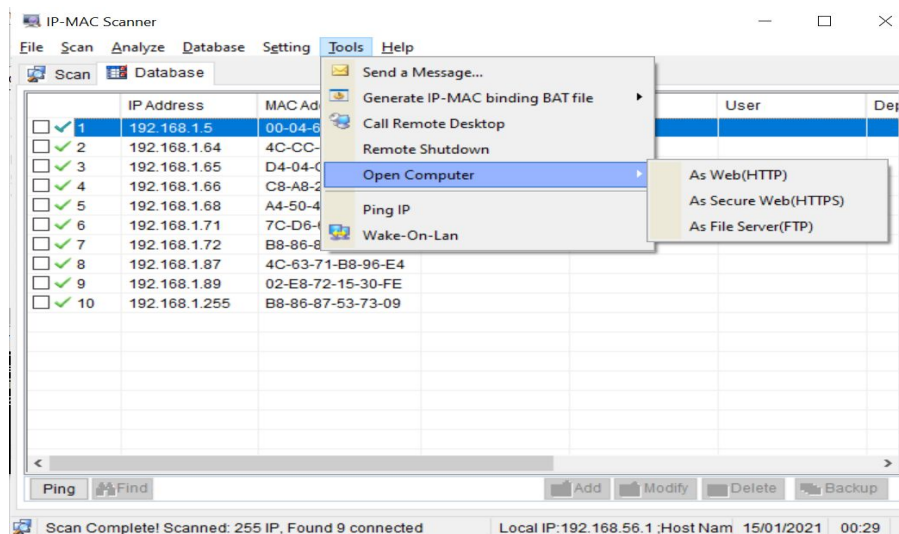


Figura 16

5.2 AthTek NetWalk Enterprise

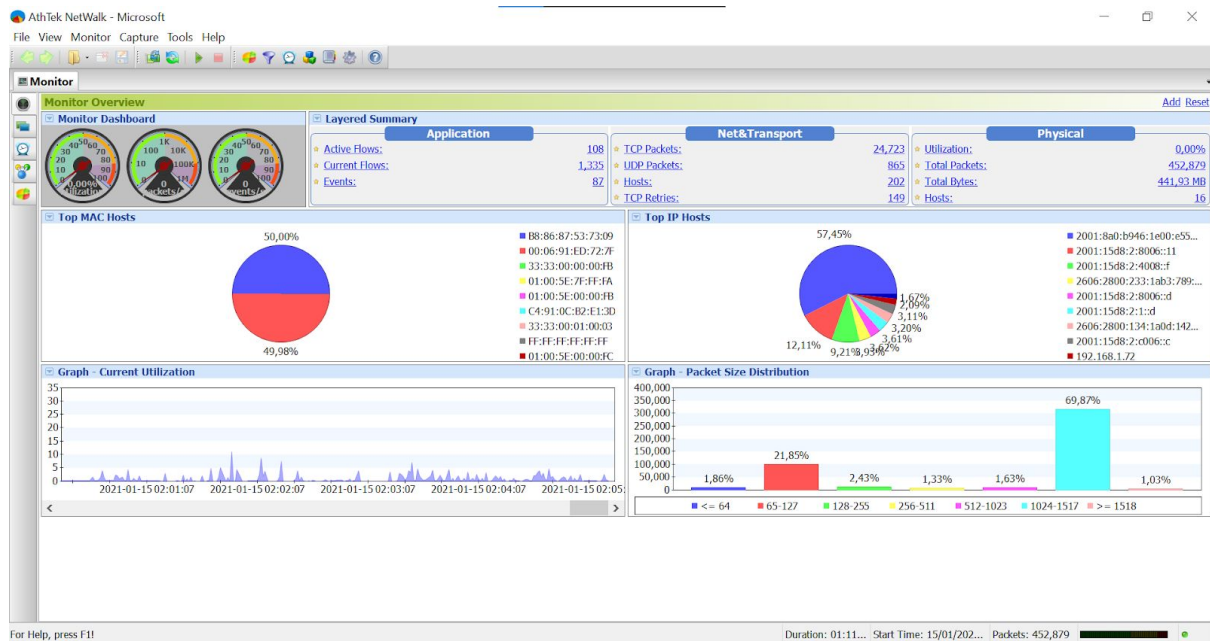


Figura 17 - Página inicial/Overview

No lado direito da ferramenta é possível escolher a opção Layered View, onde se pode escolher sobre qual das camadas se pretende ter informação (Physical, Net Transport, Application). Permite ter uma informação bastante detalhada sobre protocolos (HTTP, DNS, POP3, SMTP e muitos mais), e também permite fazer o download dos gráficos para imagens.

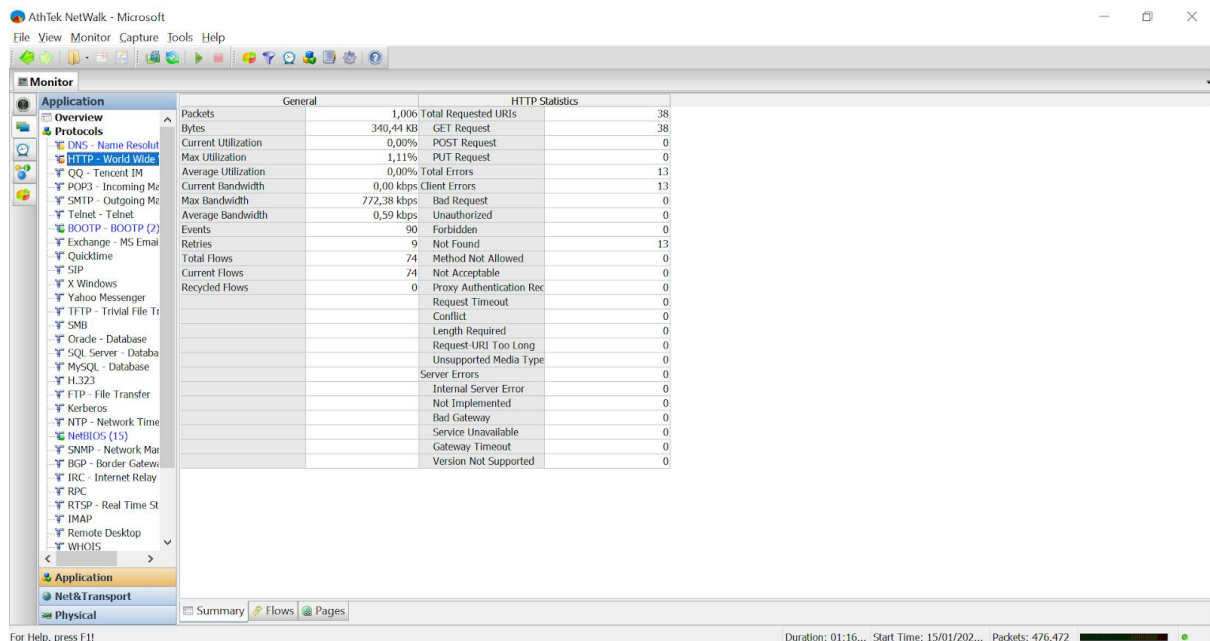


Figura 18 - Layered View

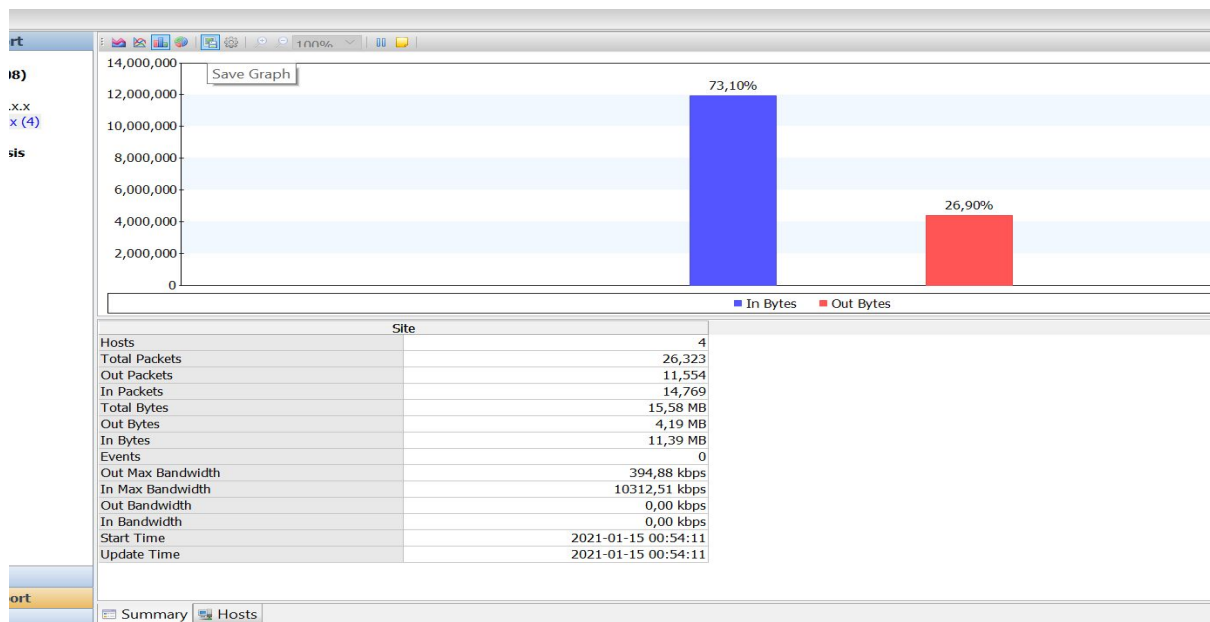


Figura 19 - Layered View em modo gráfico

Também é possível ver eventos das três camadas na opção “Events” do lado direito. A ferramenta automaticamente conta e classifica os eventos de acordo com a sua importância.

Total Count:	3,502	2,220	385	897	0	Filter:	All
Time	Description	Src. Address	Src. P...	Dst. Address	Dst. P...	Type	Layer
2021-0...:54:24	TCP Retransmission	88.221.65.150	443	192.168.1.72	51,289	Advanced	Net&Tra...rt Layer
2021-0...:54:25	TCP Retransmission	2a03:28...00c:0:2	443	2001:8a...14:7482	50,785	Advanced	Net&Tra...rt Layer
2021-0...:54:26	TCP Server Timeout	192.168.1.72	51,255	gateway...cord.gg	443	Advanced	Net&Tra...rt Layer
2021-0...:54:26	TCP Retransmission	gateway...cord.gg	443	192.168.1.72	51,255	Advanced	Net&Tra...rt Layer
2021-0...:54:29	TCP Server Timeout	2001:8a...14:7482	51,283	2a03:28...0:25de	443	Advanced	Net&Tra...rt Layer
2021-0...:54:57	TCP Retransmission	2001:8a...14:7482	50,785	2a03:28...00c:0:2	443	Advanced	Net&Tra...rt Layer
2021-0...:54:58	TCP Retransmission	2a03:28...00c:0:2	443	2001:8a...14:7482	50,785	Advanced	Net&Tra...rt Layer
2021-0...:55:03	TCP Keepalive	2001:8a...14:7482	51,266	2606:47...12:1ad3	443	Advanced	Net&Tra...rt Layer
2021-0...:55:03	TCP Keepalive ACK	2606:47...12:1ad3	443	2001:8a...14:7482	51,266	Advanced	Net&Tra...rt Layer
2021-0...:55:07	TCP Server Timeout	192.168.1.72	51,255	gateway...cord.gg	443	Advanced	Net&Tra...rt Layer
2021-0...:55:14	TCP Keepalive	2001:8a...14:7482	51,294	2a00:14...c::200e	443	Advanced	Net&Tra...rt Layer
2021-0...:55:14	TCP Keepalive	2001:8a...14:7482	51,286	2a00:14...a::2016	443	Advanced	Net&Tra...rt Layer
2021-0...:55:14	TCP Keepalive ACK	2a00:14...c::200e	443	2001:8a...14:7482	51,294	Advanced	Net&Tra...rt Layer
2021-0...:55:15	TCP Keepalive ACK	2a00:14...a::2016	443	2001:8a...14:7482	51,286	Advanced	Net&Tra...rt Layer
2021-0...:55:22	TCP Retransmission	gateway...cord.gg	443	192.168.1.72	51,255	Advanced	Net&Tra...rt Layer
2021-0...:55:25	TCP Keepalive	2001:8a...14:7482	50,974	2606:47...2:1bd3	443	Advanced	Net&Tra...rt Layer
2021-0...:55:31	TCP Keepalive	2001:8a...14:7482	51,284	2001:15...0c:0:a7	443	Advanced	Net&Tra...rt Layer
2021-0...:55:31	TCP Keepalive ACK	2001:15...0c:0:a7	443	2001:8a...14:7482	51,284	Advanced	Net&Tra...rt Layer
2021-0...:55:33	TCP Keepalive	192.168.1.72	51,276	130.211.19.189	443	Advanced	Net&Tra...rt Layer
2021-0...:55:34	TCP Keepalive ACK	130.211.19.189	443	192.168.1.72	51,276	Advanced	Net&Tra...rt Layer
2021-0...:55:34	TCP Keepalive	2001:8a...14:7482	50,763	2a00:14...c00::bc	5,228	Advanced	Net&Tra...rt Layer
2021-0...:55:34	TCP Keepalive ACK	2a00:14...c00::bc	5,228	2001:8a...14:7482	50,763	Advanced	Net&Tra...rt Layer
2021-0...:55:42	TCP Server Timeout	2606:47...12:1ad3	443	2001:8a...14:7482	51,266	Advanced	Net&Tra...rt Layer
2021-0...:55:48	TCP Server Timeout	192.168.1.72	51,255	gateway...cord.gg	443	Advanced	Net&Tra...rt Layer
2021-0...:55:59	TCP Keepalive	2001:8a...14:7482	51,294	2a00:14...c::200e	443	Advanced	Net&Tra...rt Layer
2021-0...:56:00	TCP Keepalive	2001:8a...14:7482	51,286	2a00:14...a::2016	443	Advanced	Net&Tra...rt Layer
2021-0...:56:00	TCP Keepalive ACK	2a00:14...c::200e	443	2001:8a...14:7482	51,294	Advanced	Net&Tra...rt Layer
2021-0...:56:00	TCP Keepalive ACK	2a00:14...a::2016	443	2001:8a...14:7482	51,286	Advanced	Net&Tra...rt Layer
2021-0...:56:11	TCP Keepalive	2001:8a...14:7482	50,974	2606:47...2:1bd3	443	Advanced	Net&Tra...rt Layer
2021-0...:56:11	TCP Keepalive ACK	2606:47...2:1bd3	443	2001:8a...14:7482	50,974	Advanced	Net&Tra...rt Layer
2021-0...:56:14	TCP Retransmission	2a03:28...00c:0:2	443	2001:8a...14:7482	50,785	Advanced	Net&Tra...rt Layer
2021-0...:56:16	TCP Server Timeout	2001:15...0c:0:a7	443	2001:8a...14:7482	51,284	Advanced	Net&Tra...rt Layer
2021-0...:56:16	TCP Retransmission	2001:15...0c:0:a7	443	2001:8a...14:7482	51,284	Advanced	Net&Tra...rt Layer
2021-0...:56:19	TCP Keepalive	192.168.1.72	51,276	130.211.19.189	443	Advanced	Net&Tra...rt Layer

Figura 20 - Eventos

A opção Matrix Map fica possível ver tráfego de rede ao longo de uma circunferência. Cada nó representa o “peso” de cada comunicação e quando está com cor verde representa que há tráfego ativo no último segundo. Há a opção de

gravar esta Matrix Map como imagem. Se for efetuado um duplo clique em cima do MAC address é possível ter mais informações sobre o que está a acontecer.

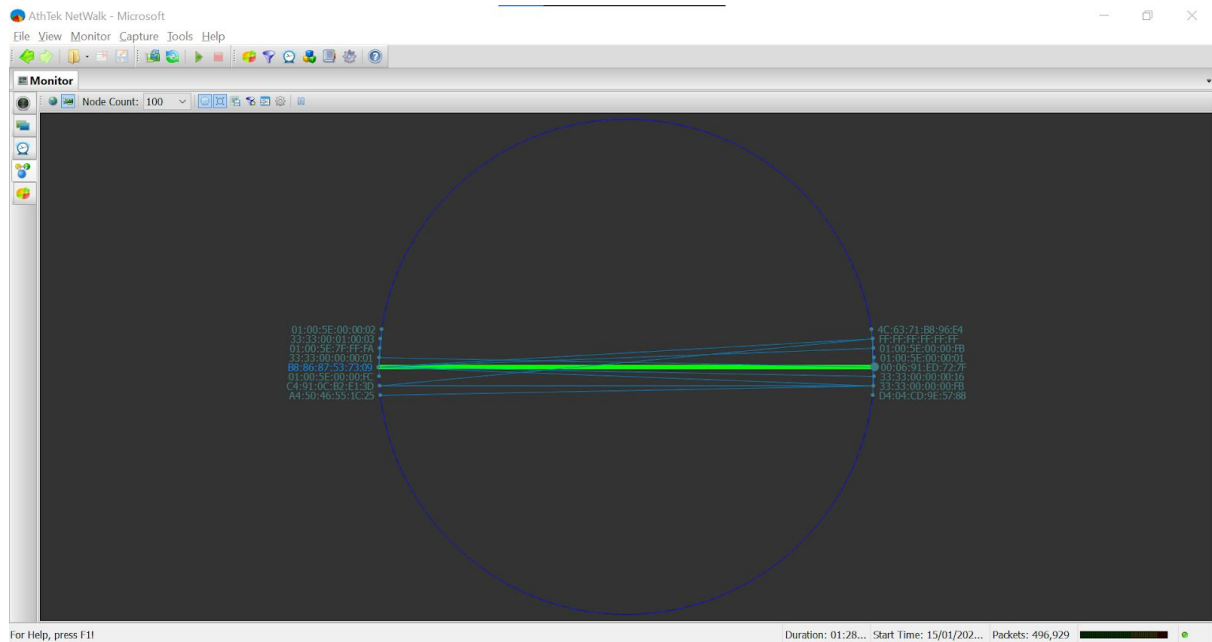


Figura 21 - Matrix Map

5.3 Ansible

Como é possível ver na imagem, o Ansible funciona de forma correta, pingando o localhost.

```
francisco@francisco-VirtualBox:/etc/ansible$ ansible all -m ping
localhost | SUCCESS => {
  "ansible_facts": {
    "discovered_interpreter_python": "/usr/bin/python3"
  },
  "changed": false,
  "ping": "pong"
}
```

Figura 22 - Comandos Ad-Hoc com o Ansible

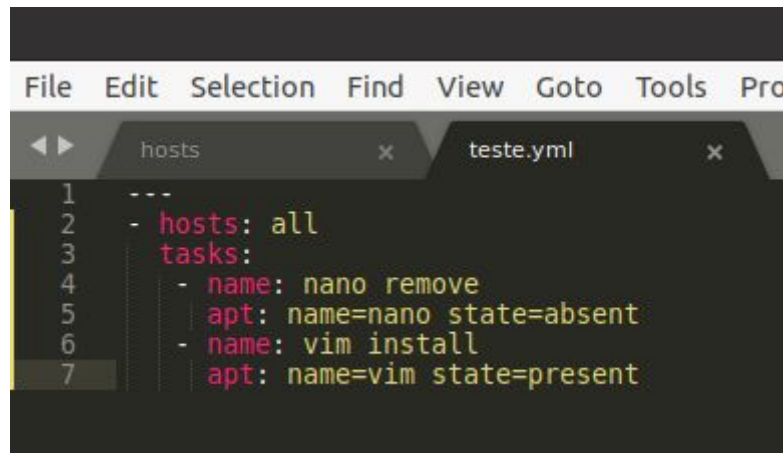
Isto são chamados comandos ad-hoc. No Ansible permitem a execução de tarefas simples na linha de comando em um ou todos os seus hosts. Um comando ad-hoc consiste em dois parâmetros; o grupo de hosts que define em quais máquinas executar a tarefa e o módulo Ansible a ser executado.

Porém, existe uma forma melhor e mais “poderosa” de utilizar o Ansible, com os chamados Playbooks. Um Playbook tem um conjunto de “jogadas” que por sua vez contém Tasks, e é um ficheiro YAML.

Quando este playbook for executado, vai garantir que a última versão do nano está nas máquinas.

Na opção hosts é possível introduzir o grupo criado com os elementos [] no ficheiro de hosts, como explicado em cima. Neste caso de teste somente no localhost.

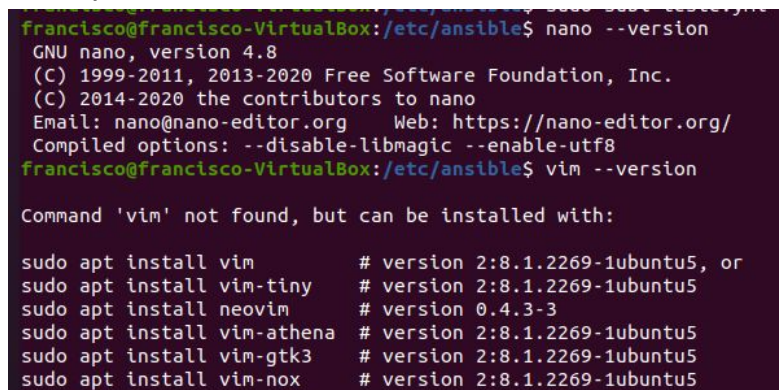
Para efeito de teste, foi criado um playbook com o efeito de desinstalar o nano e instalar o vim.



```
File Edit Selection Find View Goto Tools Pro
hosts x teste.yml x
1 ---
2 - hosts: all
3   tasks:
4     - name: nano remove
5       apt: name=nano state=absent
6     - name: vim install
7       apt: name=vim state=present
```

Figura 23 - Playbook para teste

Como é possível ver, a máquina neste momento não tem o vim instalado.



```
francisco@francisco-VirtualBox:/etc/ansible$ nano --version
GNU nano, version 4.8
(C) 1999-2011, 2013-2020 Free Software Foundation, Inc.
(C) 2014-2020 the contributors to nano
Email: nano@nano-editor.org Web: https://nano-editor.org/
Compiled options: --disable-libmagic --enable-utf8
francisco@francisco-VirtualBox:/etc/ansible$ vim --version
Command 'vim' not found, but can be installed with:

sudo apt install vim          # version 2:8.1.2269-1ubuntu5, or
sudo apt install vim-tiny     # version 2:8.1.2269-1ubuntu5
sudo apt install neovim      # version 0.4.3-3
sudo apt install vim-athena  # version 2:8.1.2269-1ubuntu5
sudo apt install vim-gtk3    # version 2:8.1.2269-1ubuntu5
sudo apt install vim-nox     # version 2:8.1.2269-1ubuntu5
```

Figura 24 - Demonstração que o vim não está instalado e o nano sim

Para correr o playbook é simplesmente necessário escrever **ansible-playbook NomeDaPlaybook.yml** no terminal.



```
francisco@francisco-VirtualBox:/etc/ansible$ sudo ansible-playbook teste.yml

PLAY [all] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [nano remove] *****
changed: [localhost]

TASK [vim install] *****
changed: [localhost]

PLAY RECAP *****
localhost : ok=3  changed=2  unreachable=0  failed=0  skipped=0  rescued=0  ignored=0
```

Figura 25- Correr o playbook e o seu efeito final

Como é possível ver na imagem, as duas tasks que tinham o nome de nano remove e nano install foram executadas com sucesso.

No play recap é possível ver que houve 2 alterações, ou seja uma quando o nano foi removido e uma quando o vim foi instalado.

```
francisco@francisco-VirtualBox:/etc/ansible$ vim --version
VIM - Vi IMproved 8.1 (2018 May 18, compiled Apr 15 2020 06:40:31)
Included patches: 1-2269
Modified by team+vim@tracker.debian.org
Compiled by team+vim@tracker.debian.org
Huge version without GUI.  Features included (+) or not (-):
```

Figura 26- Vim instalado com sucesso.

```
francisco@francisco-VirtualBox:/etc/ansible$ nano --version
bash: /usr/bin/nano: No such file or directory
```

Figura 27 - Nano já não existe na máquina.

Se por algum motivo o utilizador quiser voltar a correr a playbook, o Ansible não faz mudança nenhuma sem ser necessário, e como o vim já estava instalado e o nano removido, há 0 changes ocorridas.

```
bash: /usr/bin/nano: No such file or directory
francisco@francisco-VirtualBox:/etc/ansible$ sudo ansible-playbook teste.yml

PLAY [all] *****

TASK [Gathering Facts] *****
ok: [localhost]

TASK [nano remove] *****
ok: [localhost]

TASK [vim install] *****
ok: [localhost]

PLAY RECAP *****
localhost                : ok=3    changed=0    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Figura 28 - 0 changes feitos na máquina

6. Conclusão

6.1 AthTek IP-MacScanner

Pontos Fortes:

- Rápido a fazer um scan de IP/MAC em uma lan.
- Teste de ping.
- Possibilidade de guardar os dados obtidos do scan na base de dados.
- Possibilidade de guardar os dados obtidos em tabelas excel.
- Leve.
- Possibilidade de mandar uma mensagem a outro computador numa lan.

Pontos Fracos:

- Pago(Só possui um trial gratuito de 15 dias)

O AthTek IP-Mac Scanner é uma ferramenta de utilização bastante simples, o que é bastante bom para utilizadores sem experiência prévia que queiram gerir a sua LAN, porém tem o downside de ser pago.

6.2 AthTek NetWalk Enterprise

Pontos Fortes:

- Gráficos em tempo real de endereços IP's, pacotes capturados, e fluxo de tráfego.
- Excelente para packet sniffing(Usa wireshark)
- Possibilidade de guardar os dados obtidos em imagens.
- Tem análises detalhadas de praticamente todos os protocolos(HTTP,DNS,SMTP,POP3 e muitos mais..)
- De utilização simples, o que permite iniciantes aprenderem e usarem a ferramenta sem qualquer problema.

Pontos Fracos:

- Pago

O AthTek NetWalk Enterprise é uma ferramenta de utilização bastante simples, o que é bastante bom para utilizadores sem experiência prévia que queiram gerir a sua LAN,ter dados e estatística sobre a mesma.

Funciona em conjunto com o Wireshark e com o WinPcap, e tem uma performance incrível em packet sniffing e análise da rede, porém tem o downside de ser pago.

6.3 Ansible

Pontos Fortes:

- Excelente para automação de tarefas
- Gratuito, simples e open-sourced

O Ansible é uma ferramenta bastante simples, excelente para automação de tarefas, gratuito, sendo na minha opinião uma ferramenta excelente e sem pontos fracos.

7. Bibliografia

<https://www.ansible.com/>

http://www.athtek.com/netwalk.html?fbclid=IwAR2wrTBZD32dFCVIJROA29Bj0TW0e_gS_N9bF-k6FmWxpyGseFXQm7nBrcwuW

<https://gist.github.com/ryantuck/9771990cfd16b016929>

<http://www.athtek.com/ip-mac-scanner.html>