Security Network Analytic Stand Up helper

User guide

Last Revision No. & Date (see revision history): Rev 1.0 – 14/06/2021

**Revision History:**

(NOTE: Include final entries from each party for comments at signoff)

|  |  |  |  |
| --- | --- | --- | --- |
| **Revision Level** | **Description** | **Author(s)** | **Comments(NOTES)** |
| 1.0 | Initial | Dario Cavallaro | Initial Draft (full document) |
|  |  |  |  |

Table of Contents

[Table of Figures 4](#_Toc74840243)

[Problems Solved by service/software 5](#_Toc74840244)

[General Description of service/software 5](#_Toc74840245)

[High Level Design of service/software 5](#_Toc74840246)

[Requirements or Targeted Features/Outcomes 6](#_Toc74840247)

[Overview of Design 6](#_Toc74840248)

[External Interactions 6](#_Toc74840249)

[Packaging of Components 6](#_Toc74840250)

[Install/Deployment of Components 6](#_Toc74840251)

[Hardware/Platforms support & requirements 6](#_Toc74840252)

[Dependencies 6](#_Toc74840253)

[Performance Goals or targets 7](#_Toc74840254)

[Anticipated Limitations & Functional Exceptions 7](#_Toc74840255)

[Level of Effort for first release 7](#_Toc74840256)

# Problems Solved by service/software

Accelerate Secure Network Analytics setup through a wizard based approach that populates basic configuration items at setup time.

# General Description of software and requirements

Python script that collects data of network settings and public information to populate basic Host group information. It uses these libraries:

* ipwhois
* ipaddress
* requests
* pip
* Python 3+
* wmi (Windows)
* netifaces (MAC)

V1 will support only Windows 10 and Mac OS 12 (Monterey) and Cisco Secure Network Analytics v7.3+. This script is not tested on versions prior 7.3 or Cisco Secure Cloud Analytics.

The minimum requirements of the Host Machine are:

* 4 CPU Cores
* 4 GB Memory
* 100 GB Hard Disk Space

Network connectivity to SNA and internet. Credentials of an admin user of SNA are required.

# High Level Flow description

The first time a user approaches SNAaC, it is best to download the latest version from github. Before running the script, please make sure all the requirements are satisfied. The requirements-[platform] files will help with that, ie.: pip install -r requirements-win.txt

Once requirements are installed, it is possible to run the programme with: python snaac.py.

The script will collect the network settings of the host it is running on and the whois information available on the public IP the host is accessing internet with.

Finally, the programme will ask for the IP address of the SMC and its administrative credentials.

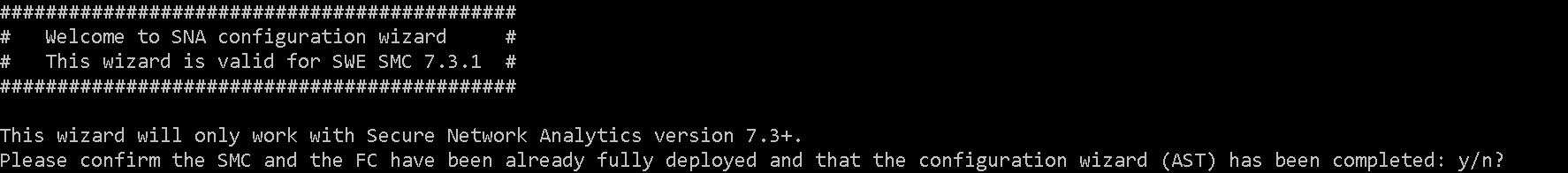
The programme will ask for confirmation of the changes that will apply to the host group configuration. The settings are always added. No old configuration is overwritten or cancelled.

# Low Level Description

First of all pull the git repository from: [todo: add url and full command]. Please see here for more information about git: https://git-scm.com/downloads.

Use pip -r requirements-win.txt to install all the required packages based on the platform. Swap win with mac if you are running this on Mac OS. This command requires Python 3+, pip installed and working and an internet connection. Please see here for more information on how to install Python 3+: <https://www.python.org>. Please see here for more information on how to install pip: <https://pip.pypa.io/en/stable/installation/>.

Once all the requirements are installed, run the programme using python snaac.py from the directory that contains the repository.

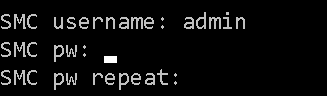
The programme will first ask for confirmation that Secure Network Analytics’ SMC and FC have been already fully deployed and that the first configuration wizard (AST) has been completed successfully. 

More information about Secure Network Analytics and the AST here: <https://www.cisco.com/c/en/us/support/security/stealthwatch/series.html#InstallandUpgrade>.

Once the information collection has been completed, it will ask for the IP address of the SMC:



After it will ask for the credentials of the administrative user. NOTE: a check on the user has been implemented. Also the password has to be submitted twice to avoid typos.



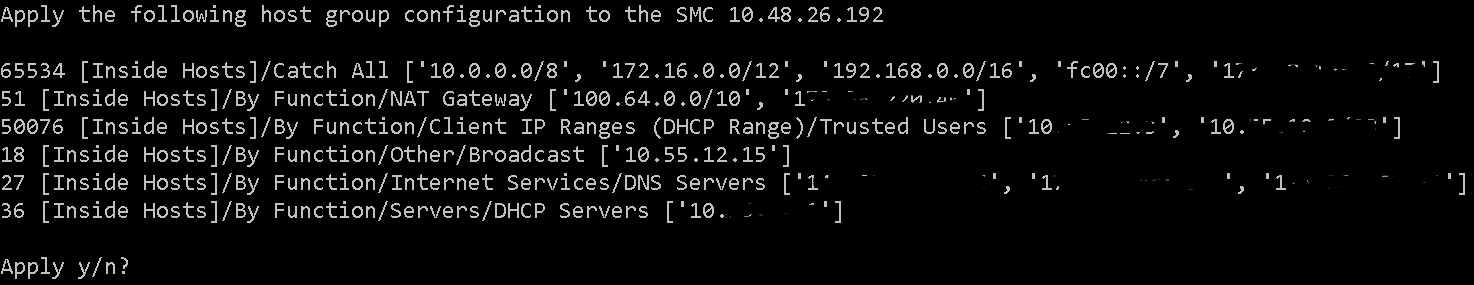
It will ask confirmation of the domain ID. Confirm if you don’t know what this means. Only useful if you have deployed multiple domains on SNA:



If this is not the first time you are running the programme, it will ask if you want to reuse the configuration in cache or refresh the configuration:



Otherwise, it will ask for confirmation about the configuration items it will update:



Please make sure the information displayed is correct. If you need to change this information manually, you can answer no, edit the file snaac\_config.json and run again the programme to import the cached items.

After a successful run, SNA’s Host groups will be populated with basic information that will allow a more accurate generation of alarms. Also it is a great first step for tuning Secure Network Analytics.