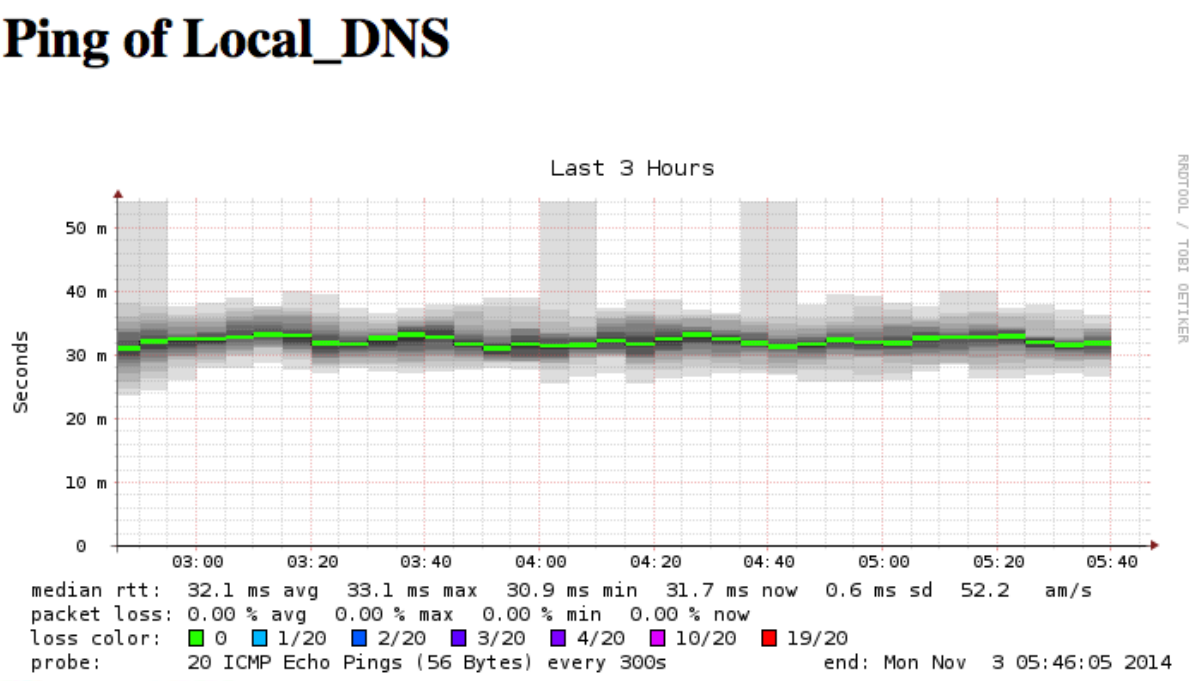
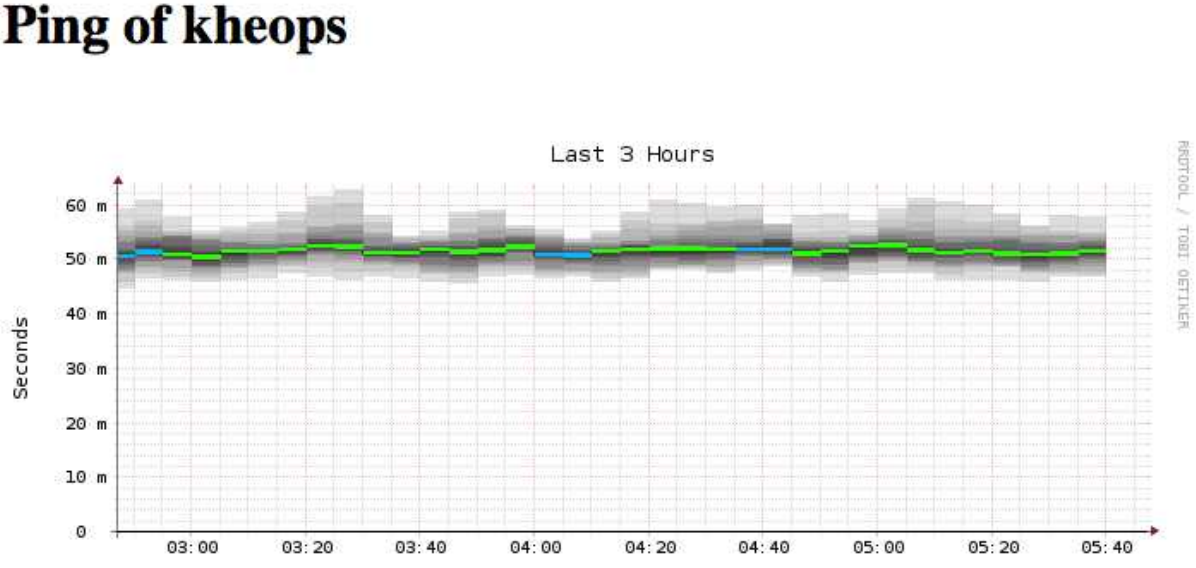
Smokeping, SNMP

Smokeping

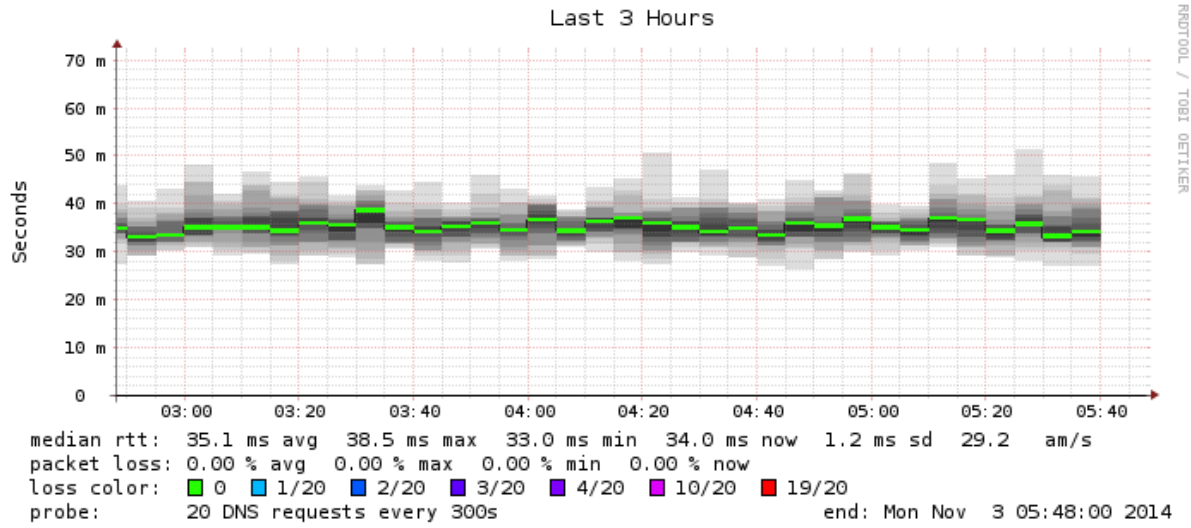
Dans cet exercice, nous allons analyser les graphes fournis par smokeping qui ont été obtenus depuis une machine qui est raccordée via un accès ADSL.
Smokeping a été paramétré pour fournir les indicateurs suivants :

- Niveau réseau
  - ping vers kheops.unice.fr
  - ping vers resolver DNS de l'opérateur
- Niveau application
  - DNS
    - Interrogation du resolver DNS de l'opérateur pour résoudre www.google.fr
    - Interrogation du resolver ouvert de Google (8.8.8.8) pour résoudre kheops.unice.fr
  - HTTP
    - téléchargement page kheops.unice.fr
  - HTTPs
    - téléchargement page d'accueil de kheops.unice.fr

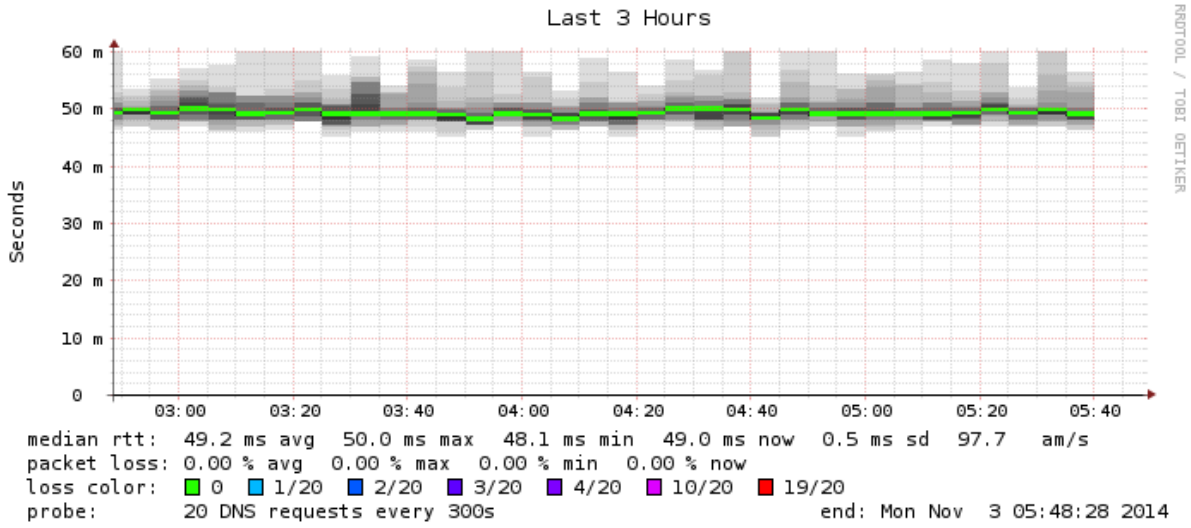




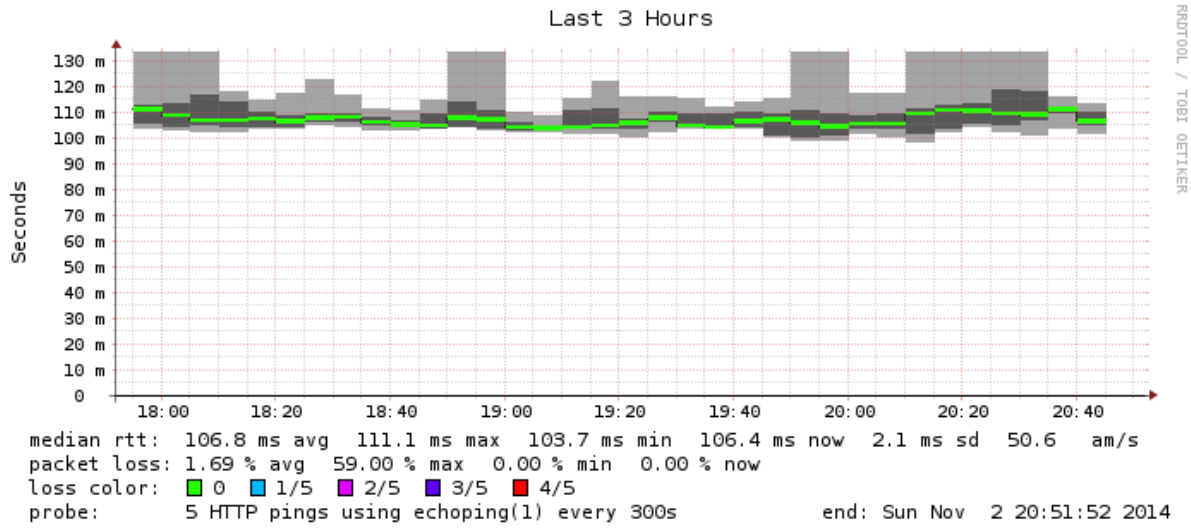
DNS lookup for Google from Local DNS



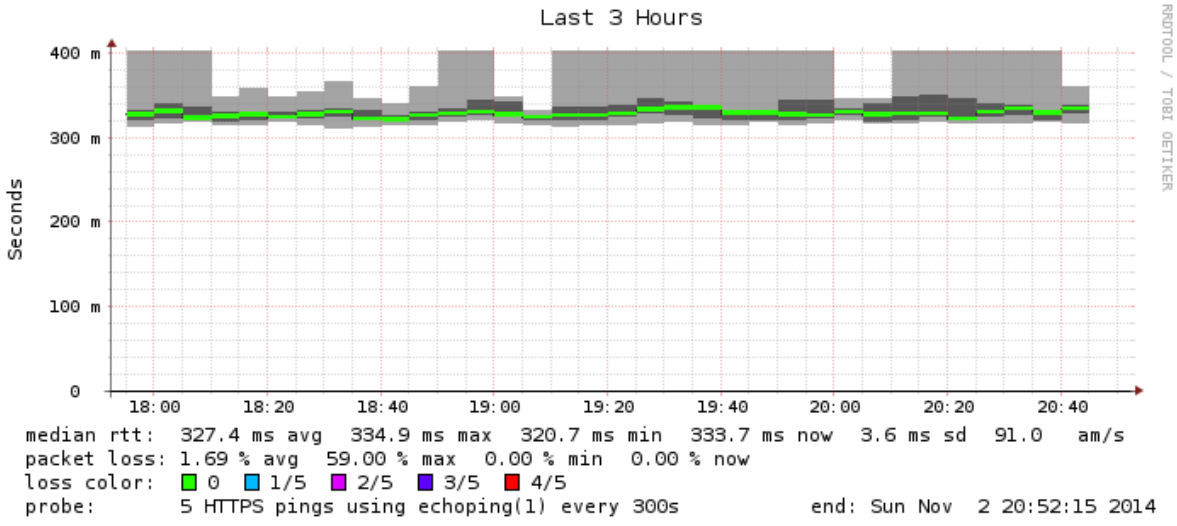
DNS lookup for kheops from Google open DNS



HTTP for Kheops



HTTPs for Kheops



*Q 1 : en quoi peut-on dire que smokeping est une généralisation de ping ?

*Q 2 : accès ADSL
Toutes les mesures effectuées passent au travers du lien d'accès ADSL. Voici un traceroute effectué depuis la machine.

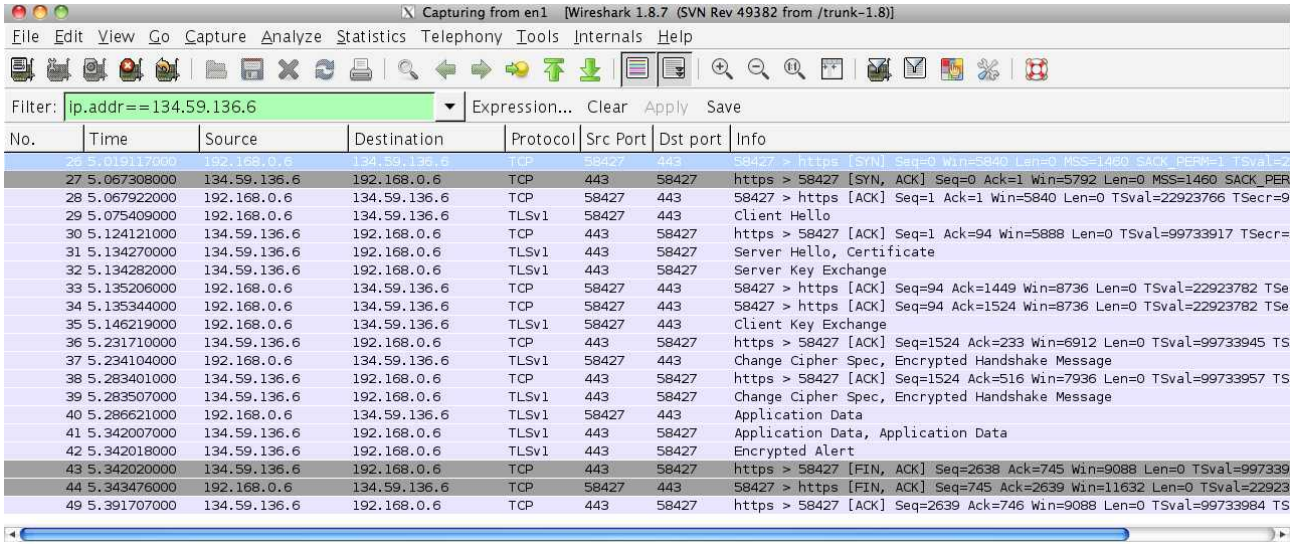
```
guillaume@~:traceroute www.google.fr
traceroute to www.google.fr (74.125.136.94), 64 hops max, 52 byte packets
 1  192.168.0.254 (192.168.0.254)  3.227 ms  1.499 ms  1.618 ms
 2  82.238.189.254 (82.238.189.254)  22.462 ms  22.608 ms  23.447 ms
 3  78.254.5.190 (78.254.5.190)  57.356 ms  28.126 ms  34.682 ms
 4  ant06-1-v902.intf.nra.proxad.net (78.254.254.154)  22.296 ms  21.869 ms  22.433 ms
 5  nice-6k-1-v900.intf.nra.proxad.net (78.254.254.158)  23.228 ms  22.856 ms  23.427 ms
 6  marseille-crs8-1-be1006.intf.routers.proxad.net (194.149.160.137)  26.911 ms  26.948 ms  28.392 ms
 7  p11-crs16-1-be1102.intf.routers.proxad.net (78.254.249.89)  36.027 ms  35.220 ms  35.947 ms
 8  th2-9k-1-be1001.intf.routers.proxad.net (78.254.249.6)  35.185 ms  36.780 ms  35.686 ms
 9  * ix-15-547.tcore1.pvu-paris.as6453.net (195.219.241.173)  76.658 ms  76.883 ms
10  * * *
11  72.14.239.145 (72.14.239.145)  88.513 ms  88.723 ms  91.281 ms
12  * * 209.85.245.81 (209.85.245.81)  86.731 ms
13  209.85.245.87 (209.85.245.87)  85.244 ms  86.358 ms
    216.239.51.112 (216.239.51.112)  87.183 ms
14  72.14.236.135 (72.14.236.135)  108.451 ms
    209.85.240.220 (209.85.240.220)  88.782 ms  98.841 ms
15  209.85.255.85 (209.85.255.85)  91.499 ms
    216.239.48.104 (216.239.48.104)  90.741 ms
    209.85.255.87 (209.85.255.87)  91.015 ms
16  216.239.49.38 (216.239.49.38)  90.906 ms
    216.239.49.28 (216.239.49.28)  92.234 ms
    216.239.49.38 (216.239.49.38)  91.763 ms
17  * * *
18  * ea-in-f94.1e100.net (74.125.136.94)  92.919 ms  91.183 ms
```

** Q2.1 Quel est le RTT sur le lien d'accès ADSL ?
** Q2.2 Comment ce résultat varie en fonction de l'accès ADSL d'après vous (opérateur, distance, qualité du lien?)

Q3 : DNS
** Q3.0 Qu'est-ce qu'un resolver DNS ?
** Q3.1 Quelle est la part de la latence d'accès au serveur par rapport au temps de résolution DNS du serveur ?
** Q3.2 Relier le temps de résolution en lui-même avec le schéma typique de résolution DNS vu en cours.
** Q3.3 Y a-t-il du caching DNS ?

Q 4 : HTTP
** Q4.1 Faites un diagramme temporel correspondant au téléchargement de l'objet demandé.
** Q4.2 Faites le lien entre le diagramme précédent, le temps de ping et le temps du HTTPping pour kheops.

Q 5 : HTTPs
** Q5.1 Quel est le surcout du HTTPs par rapport au HTTP.
** Q5.2 Voici les traces wiresharks pour kheops. Relier le surcout en temps avec les échanges réseau et le temps de ping.



Exercice 3 : SNMP

Q: Quel est l'intérêt d'avoir un arbre de référence qui soit unique ?

Q: Tous les objets de l'arbre de référence doivent ils être implémentés dans une Mib?

Note : On trouvera en annexe les extraits utiles de la MIB-II ; on a supprimé certaines variables pour simplifier, considérez que seules les variables indiquées existent.

Q : On considère la variable ipForwarding. Quelle est le « Object Identifier »(OID) sous forme numérique qui permet d'accéder à la valeur correspondante de l'agent (argument d'un échange snmpget). Quelles valeurs peuvent-elles être rendues ?

Q: Par quel appel SNMP peut on modifier ipForwarding pour faire de la machine un routeur ?

6. Definitions

```
RFC1155-SMI DEFINITIONS ::= BEGIN

EXPORTS -- EVERYTHING
        internet, directory, mgmt,
        experimental, private, enterprises,
        OBJECT-TYPE, ObjectName, ObjectSyntax, SimpleSyntax,
        ApplicationSyntax, NetworkAddress, IpAddress,
        Counter, Gauge, TimeTicks, Opaque;

 -- the path to the root

 internet      OBJECT IDENTIFIER ::= { iso org(3) dod(6) 1 }

 directory     OBJECT IDENTIFIER ::= { internet 1 }

 mgmt          OBJECT IDENTIFIER ::= { internet 2 }

 experimental  OBJECT IDENTIFIER ::= { internet 3 }

 private       OBJECT IDENTIFIER ::= { internet 4 }
 enterprises   OBJECT IDENTIFIER ::= { private 1 }
```



```
--
--      SIZE (0..255)

PhysAddress ::=
    OCTET STRING
-- This data type is used to model media addresses.  For many
-- types of media, this will be in a binary representation.
-- For example, an ethernet address would be represented as
-- a string of 6 octets.


-- groups in MIB-II

system       OBJECT IDENTIFIER ::= { mib-2 1 }

interfaces   OBJECT IDENTIFIER ::= { mib-2 2 }

at           OBJECT IDENTIFIER ::= { mib-2 3 }

ip           OBJECT IDENTIFIER ::= { mib-2 4 }

icmp         OBJECT IDENTIFIER ::= { mib-2 5 }

tcp          OBJECT IDENTIFIER ::= { mib-2 6 }

udp          OBJECT IDENTIFIER ::= { mib-2 7 }

egp          OBJECT IDENTIFIER ::= { mib-2 8 }

-- historical (some say hysterical)
-- cmot      OBJECT IDENTIFIER ::= { mib-2 9 }

transmission OBJECT IDENTIFIER ::= { mib-2 10 }

snmp         OBJECT IDENTIFIER ::= { mib-2 11 }


-- the System group

-- Implementation of the System group is mandatory for all
-- systems.  If an agent is not configured to have a value
-- for any of these variables, a string of length 0 is
-- returned.
```

```
            ::= { atEntry 3 }


        -- the IP group

        -- Implementation of the IP group is mandatory for all
        -- systems.

        ipForwarding OBJECT-TYPE
            SYNTAX  INTEGER {
                        forwarding(1),    -- acting as a gateway
                        not-forwarding(2) -- NOT acting as a gateway
                    }
            ACCESS  read-write
            STATUS  mandatory
            DESCRIPTION
                    "The indication of whether this entity is acting
                    as an IP gateway in respect to the forwarding of
                    datagrams received by, but not addressed to, this
                    entity.  IP gateways forward datagrams.  IP hosts
                    do not (except those source-routed via the host).

                    Note that for some managed nodes, this object may
                    take on only a subset of the values possible.
                    Accordingly, it is appropriate for an agent to
                    return a `badValue' response if a management
                    station attempts to change this object to an
                    inappropriate value."
            ::= { ip 1 }

        ipDefaultTTL OBJECT-TYPE
            SYNTAX  INTEGER
            ACCESS  read-write
            STATUS  mandatory
            DESCRIPTION
                    "The default value inserted into the Time-To-Live
                    field of the IP header of datagrams originated at
                    this entity, whenever a TTL value is not supplied
                    by the transport layer protocol."
            ::= { ip 2 }
```

M3105 : Ansible

Guillaume Urvoy-Keller

September 19, 2019

1 Objectifs

1. Faites un croquis expliquant le fonctionnement d'Ansible avec :
   - La machine d'administration.
   - Les serveurs à configurer: est-ce que ce sont des serveurs physiques? virtuels? des containers?
   - Les playbooks/rôles, c'est à dire l'ensemble des recettes à appliquer.
   - Le protocole utilisé entre la machine d'administration et les serveurs à configurer pour l'envoi des commandes Ansible?
2. Pourquoi utiliser Ansible et ne pas simplement créer des images de machines virtuelles (une pour le serveur Web, l'autre pour la base de données, etc) qui contiennent directement tous les logiciels nécéssaires?
3. Ansible fonctionne en mode Push (on pousse les configurations vers les serveurs) alors que les autres (Chef, Puppet, Salt, etc) fonctionnent en mode Pull (c'est le serveur qui contacte la machine d'administration). Quelle est la conséquence sur la configuration logicielle des serveurs à configurer avec Chef, Puppet, Salt, etc?

2 Connexion SSH via une clé publique

Utiliser une paire clé publique/privée permet de se connecter sans que l'utilisateur ait à donner son mot de passe. La mise en oeuvre de la connexion en SSH via une clé est le suivant :

- A faire une seule fois, avant la première connexion :
  - On créé une paire de clé publique/privée Pub/Priv sur la machine Admin A. Soit un message M, on a la propriété suivante : Priv(Pub(M))=M.
  - On copie la clé **publique** sur le serveur S.
- A chaque connexion :
  - A fait coucou à S et lui dit qu'il veut s'authentifier via une clé privée
  - S génère un nombre aléatoire N, le crypte avec Pub et envoie à S Pub(M)
  - A décrypte N et le renvoie à S.

1. Pourquoi cela fonctionne?
2. Du point de vue d'Ansible, que faut-il faire pour gérer un parc de machines?

3 Ansible vs. scripting

Les outils de gestion logicielle des infrastructures comme Ansible, Salt, Chef, Puppet... sont "en concurrence" avec la méthode traditionnelle de gestion qui se fait par des scripts.

Considérons un exemple simple : un serveur sur lequel on veut a) mettre à jour le système de paquets et b) installer un serveur Web nginx.

On peut le faire via Ansible avec la commande suivante :

```
$ ansible all --inventory "localhost," --module-name apt --args "name=nginx update_cache=yes"
```

L'application de la commande donne :

```
root@ansible:~# ansible all --inventory "localhost," --module-name apt --args "name=nginx
    update_cache=yes"
localhost | SUCCESS => {
    "cache_update_time": 1566892162,
    "cache_updated": true,
    "changed": true,
    "stderr": "debconf: delaying package configuration, since apt-utils is not installed\n",
    "stderr_lines": [
        "debconf: delaying package configuration, since apt-utils is not installed"
    ],
    "stdout": "Reading package lists...\nBuilding dependency tree...\nReading state information...\
        nThe following NEW packages will be installed:\n  nginx\n0 upgraded, 1 newly installed, 0 to
         remove and 35 not upgraded.\nNeed to get 3596 B of archives.\nAfter this operation, 44.0 kB
         of additional disk space will be used.[....]
       "stdout_lines": [
        "Reading package lists...",
        "Building dependency tree...",
        "Reading state information...",
        "The following NEW packages will be installed:",
        "  nginx",
        "0 upgraded, 1 newly installed, 0 to remove and 35 not upgraded.",
 [....]
```

Alternativement, on aurait pu utiliser le script python suivant :

```
#!/usr/bin/env python3

import paramiko

PORT = 22

def run_ssh_cmd(username, hostname, cmd,port=PORT):
    ssh_client = paramiko.SSHClient()
    ssh_client.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh_client.load_system_host_keys()
    ssh_client.connect(hostname, port, username, key_filename='/root/.ssh/id_rsa')
    stdin, stdout, stderr = ssh_client.exec_command(cmd)
    while not stdout.channel.exit_status_ready():
                if stdout.channel.recv_ready():
                    alldata = stdout.channel.recv(1024)
                    while stdout.channel.recv_ready():
                        alldata += stdout.channel.recv(1024)
                    print(str(alldata, "utf8"))

if __name__ == '__main__':
    hostname = input("Target: ")
    username = 'root'
    cmd = input("Command:")
    run_ssh_cmd(username, hostname, cmd)
```

Pour comprendre la différence entre Ansible et l'utilisation du script, répondez aux questions ci-après

1. Que se passe-t-il avec le script si la connexion SSH ne peut pas être établie?
2. Comment y remédier?
3. En regardant la sortie fournie par Ansible dans l'application de la commande précédente, que se passe-t-il si l'installation du paquet échoue?
4. Que faut-il modifier au script python pour obtenir le même résultat?

4 Configuration d'un serveur Web

```
- name: Configure webserver with nginx
  hosts: testserver
  become: yes
  tasks:
    - name: install nginx
      apt: name=nginx update_cache=yes
    - name: restart nginx
      service: name=nginx state=restarted
```

1. Quels sont les modules utilisés?
2. Dans quels cas la seconde tâche est-elle déclenchée?
3. Quel est l'intérêt de la version 2 du script ci-après?

```
- name: Configure webserver with nginx
  hosts: testserver
  become: yes
  tasks:
    - name: install nginx
      apt: name=nginx update_cache=yes
      notify: restart nginx
  handlers:
    - name: restart nginx
      service: name=nginx state=restarted
```

5 Inventaire

Ansible est capable d'adapter automatiquement les commandes qu'il joue au serveur visé. Pour ce faire, il fait un inventaire du serveur avec la commande :

```
root@ansible:~# ansible all --inventory "localhost," -m setup
localhost | SUCCESS => {
    "ansible_facts": {
        "ansible_all_ipv4_addresses": [
            "172.17.0.3"
        ],
        "ansible_architecture": "x86_64",
        "ansible_bios_date": "03/14/2014",
        "ansible_bios_version": "1.00",
        "ansible_cmdline": {
            "BOOT_IMAGE": "/boot/kernel",
            "console": "ttyS1",
            "page_poison": "1",
            "panic": "1",
            "root": "/dev/sr0",
            "text": true,
            "vsyscall": "emulate"
        },
        "ansible_date_time": {
            "date": "2019-08-26",
            "day": "26",
            "epoch": "1566837209",
            "hour": "16",
            "year": "2019"
        },
        "ansible_default_ipv4": {
            "address": "172.17.0.3",
            "alias": "eth0",
            "broadcast": "172.17.255.255",
            "gateway": "172.17.0.1",
            "interface": "eth0",
            "macaddress": "02:42:ac:11:00:03",
            "mtu": 1500,
            "netmask": "255.255.0.0",
            "network": "172.17.0.0",
            "type": "ether"
        },
      [.....]
```

Question : comment les informations ont-elles été obtenues?

6 Idempotence

Définition: idempotence is "the property of certain operations in mathematics and computer science that can be applied multiple times without changing the result beyond the initial application".

Quel est le script idempotent entre les versions v1 et v2 ci-dessous?

```
# Script v1
echo "127.0.0.1 localhost" >> /etc/hosts

# Script v2
If (!grep -q 127.0.0.1 /etc/hosts); then echo "127.0.0.1 localhost" >> /etc/hosts; fi
```

Est-ce que la commande Ansible ci-dessous est idempotent?

```
ansible all --inventory "localhost," -m command -a "touch toto, creates=toto"
localhost | SUCCESS | rc=0 >>
skipped, since toto exists
```