TP ANSIBLE NAGIOS SECURITE

Procédures préalables :

- **Attribution d'un nom à chaque machine :**

Indispensable car on utilisera la variable 'ansible invenory_hostname' qui y fait directement appel dans la partie apache (fichier index.html) et dans la partie sécurité pour les configurations ssh des serveurs web (fichier main.yml):

```
[root@localhost ~]# vi /etc/hostname
```

```
svr****
```

- **Mise à jour des packages sur toutes les machines :**

```
[root@svr*** ~]# yum install epel-release
[root@svr*** ~]# yum -y update (pour distributions RedHat)
[root@svr*** ~]# apt-get update -y (pour distributions Debian)
[root@svr*** ~]# yum -y install vim
[root@svr*** ~]# apt-get install vim
```

- **Pour les serveurs distributions debian**
  - **Installation d'un pare-feu compatible avec Ansible**

```
[root@svrftp ~]#  apt-get install ufw
```

  - **Ce pare-feu par défaut bloque les ports ssh ; il faut les autoriser :**

```
[root@svrftp ~]#  ufw allow ssh
```

  - **Autoriser la connexion ssh à root :**

```
root@svrftp:~# vim /etc/ssh/sshd_config
```

Ligne 32

```
PermitRootLogin yes
```

N.B : Le rôle firewallftp.yml comprend l'installation de ufw. Néanmoins la vérification échoue si il n'est pas installé en amont

ANSIBLE

- **Installation de tree (facultatif)**

```
[root@svransible ~]# yum install -y tree
```

- **Edition du fichier /etc/hosts pour faire correspondre adresses IP et nom de machine**

```
[root@svransible etc]# vim /etc/hosts
```

```
172.32.1.255    svransible
172.32.2.3      svrnagios
172.32.2.16     svrweb1
172.32.2.20     svrweb2
172.32.2.27     svrftp
```

- **Echanges de clés ssh pour permettre la connexion avec le serveur ansible :**

```
[root@svransible ~]# ssh-keygen -t rsa
[root@svransible ~]# ssh-copy-id -i svrweb1
[root@svransible ~]# ssh-copy-id -i svrweb2
[root@svransible ~]# ssh-copy-id -i svrftp
[root@svransible ~]# ssh-copy-id -i svrnagios
```

- **Edition du fichier hosts de Ansible pour renseigner les machines sur lesquelles opérer :**

```
[root@svransible ~]# vim /etc/ansible/hosts
```

```
[ftp]
svrftp

[nagios]
svrnagios

[web]
svrweb1
svrweb2
```

- **Verification que la connexion via Ansible s'effectue correctement :**

```
[root@svransible ~]# ansible -m ping all --one-line
```

```
svrftp | SUCCESS => {"changed": false, "ping": "pong"}
svrweb1 | SUCCESS => {"changed": false, "ping": "pong"}
svrweb2 | SUCCESS => {"changed": false, "ping": "pong"}
svrnagios | SUCCESS => {"changed": false, "ping": "pong"}
```

- **Création du playbook cloud.yml qui utilisera des rôles :**

```
[root@svransible ~]# cd /etc/ansible
[root@svransible ansible]# vim cloud.yml
```

```
- hosts: all, localhost
  roles:
    - addusers
    - nrpe
    - securite
- hosts: web
  roles:
    - apache
- hosts: nagios
  roles:
    - nagios
- hosts: ftp
  roles:
     - vsftpd
```

- **Création d'un template de rôles puis création de l'arborescence pour nos différents rôles :**

```
[root@svransible ~]# cd /etc/ansible/roles
[root@svransible roles]# ansible-galaxy init common
```

```
  common was created successfully
```

```
[root@svransible roles]# ls
```

```
Common
```

```
[root@svransible roles]# cp -r common addusers
[root@svransible roles]# cp -r common nagios
```

```
[root@svransible roles]# cp -r common apache
[root@svransible roles]# cp -r common firewall
[root@svransible roles]# cp -r common nrpe
[root@svransible roles]# cp -r common vsftp
[root@svransible roles]# mv common securite
[root@svransible roles]# ls
```

```
addusers  apache  firewall  nagios  nrpe  securite  vsftpd
```

- **Visualisation de l'arborescence avant incrémentation des fichiers :**

```
[root@svransible ansible]# tree
```

```
.
├── ansible.cfg
├── cloud.yml
├── hosts
└── roles
    ├── addusers
    │   ├── defaults
    │   │   └── main.yml
    │   ├── files
    │   ├── handlers
    │   │   └── main.yml
    │   ├── meta
    │   │   └── main.yml
    │   ├── README.md
    │   ├── tasks
    │   │   └── main.yml
    │   ├── templates
    │   ├── tests
    │   │   ├── inventory
    │   │   └── test.yml
    │   └── vars
    │       └── main.yml
    ├── apache
    │   ├── defaults
    │   │   └── main.yml
    │   ├── files
    │   ├── handlers
    │   │   └── main.yml
    │   ├── meta
    │   │   └── main.yml
    │   ├── README.md
    │   ├── tasks
    │   │   └── main.yml
    │   ├── templates
    │   │   └── index.html
    │   ├── tests
    │   │   ├── inventory
```

```
│   │   └── test.yml
│   └── vars
│       └── main.yml
├── securite
│   ├── defaults
│   │   └── main.yml
│   ├── files
│   ├── handlers
│   │   └── main.yml
│   ├── meta
│   │   └── main.yml
│   ├── README.md
│   ├── tasks
│   │   └── main.yml
│   ├── templates
│   ├── tests
│   │   ├── inventory
│   │   └── test.yml
│   └── vars
│       └── main.yml
├── firewall
│   ├── defaults
│   │   └── main.yml
│   ├── files
│   ├── handlers
│   │   └── main.yml
│   ├── meta
│   │   └── main.yml
│   ├── README.md
│   ├── tasks
│   │   └── main.yml
│   ├── templates
│   ├── tests
│   │   ├── inventory
│   │   └── test.yml
│   └── vars
│       └── main.yml
├── nagios
│   ├── defaults
│   │   └── main.yml
│   ├── files
│   ├── handlers
│   │   └── main.yml
│   ├── meta
│   │   └── main.yml
│   ├── README.md
│   ├── tasks
│   │   └── main.yml
│   ├── templates
│   ├── tests
│   │   ├── inventory
```

```
│   │   └── test.yml
│   └── vars
│       └── main.yml
├── nrpe
│   ├── defaults
│   │   └── main.yml
│   ├── files
│   ├── handlers
│   │   └── main.yml
│   ├── meta
│   │   └── main.yml
│   ├── README.md
│   ├── tasks
│   │   └── main.yml
│   ├── templates
│   ├── tests
│   │   ├── inventory
│   │   └── test.yml
│   └── vars
│       └── main.yml
└── vsftpd
    ├── defaults
    │   └── main.yml
    ├── files
    ├── handlers
    │   └── main.yml
    ├── meta
    │   └── main.yml
    ├── README.md
    ├── tasks
    │   └── main.yml
    ├── templates
    ├── tests
    │   ├── inventory
    │   └── test.yml
    └── vars
        └── main.yml
```

APACHE

- **Création de la page d'accueil indiquant bonjour et le nom de la machine**

```
[root@svransible templates]# cp index.html
/etc/ansible/roles/apache/templates
[root@svransible templates]# vi index.html
```

```
<html>
  <head><title>Page de garde de
{{inventory_hostname}}</title></head>
  <body>
    <hr>
    <center><h1>Machine  {{inventory_hostname}}</h1>
             du domaine  {{ansible_domain}}</center>
    <br><hr>
    <center><b>
<br> Bonjour {{ansible_user_id}}
<br>
<br> La distribution est : {{ansible_distribution}}
<br> La taille de la memoire est : {{ansible_memtotal_mb}}
<br> La taille de la swap est : {{ansible_memory_mb.swap.total}}
<br>
<br> La liste des adresses IP :<br>
  {% for element in ansible_all_ipv4_addresses %}
    {{element}}
  {% endfor %}
<br> La liste des interfaces resaux :<br>
  {% for element in ansible_interfaces %}
    interface : {{element}}<br>
  {% endfor %}
<br><hr>
    </b></center>
  </body>
</html>
```

- **Création des tâches pour le serveur Apache :**

```
[root@svransible tasks]# cd /etc/ansible/roles/apache/tasks

[root@svransible tasks]# vim main.yml
```

```
# tasks file for apache

  - name: "Installation du package apache si distribution RedHat"
    yum:
      name: "httpd"
      state: "latest"
    when: ansible_os_family == 'RedHat'
```

```
  - name: "Installation du package apache si distribution Debian"
    apt:
      name: "apache2"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "Installation de la page de garde"
    template:
      src: "index.html"
      dest: "/var/www/html/index.html"
      owner: "apache"
      group: "apache"
    register: confapache

  - name: "Redemarrage du service apache si distribution RedHat"
    service:
      name: "httpd"
      state: "started"
      enabled: yes
    when: confapache.changed

  - name: "Redemarrage du service apache si distribution Debian"
    service:
      name: "apache2"
      state: "started"
      enabled: yes
    when: confapache.changed

  - name: "Ouverture des ports Apache"
    include_tasks:
"/etc/ansible/roles/firewall/tasks/firewallweb.yml"

  - name: "Ouverture des ports nrpe"
    include_tasks:
"/etc/ansible/roles/firewall/tasks/firewallnrpe.yml"

  - name: "Installation de l'antivirus clamav si distribution
RedHat"
    yum:
      name: clamav
      state: "latest"
    when: ansible_os_family == 'RedHat'

  - name: "Installation de l'antivirus clamav si distribution
Debian"
    apt:
      name: "clamav"
      state: "latest"
    when: ansible_os_family == 'Debian'
...
```

NAGIOS

- **Création des tâches pour le serveur Nagios :**

```
[root@svransible nagios]# cd tasks
[root@svransible tasks]# vim main.yml
```

```yaml
---
# tasks file for intalling nagios

  - name: "Installation de Nagiossur Debian"
    apt:
      name: "nagios-nrpe-server"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "Installation de Nagios sur Redhat"
    yum:
      name: "nagios"
      state: "latest"
    when: ansible_os_family == 'Redhat'

  - name: "Installation du fichier de configuration nagios"
    template:
      src: "nagios.cfg"
      dest: "/etc/nagios/nagios.cfg"
      owner: "root"
      group: "root"

  - name: "Installation du fichier de configuration commands"
    template:
      src: "commands.cfg"
      dest: "/etc/nagios/objects/commands.cfg"
      owner: "root"
      group: "root"

  - name: "Installation du fichier de configuration contacts"
    template:
      src: "contacts.cfg"
      dest: "/etc/nagios/objects/contacts.cfg"
      owner: "root"
      group: "root"

  - name: "Installation du fichier de configuration hosts"
    template:
      src: "hosts.cfg"
      dest: "/etc/nagios/objects/hosts.cfg"
      owner: "root"
      group: "root"

  - name: "RE-Demarrage du service Nagios"
    service:
```

```
      name: "nagios"
      state: "started"
      enabled: yes

  - name: "Ouverture des ports Apache"
    include_tasks:
"/etc/ansible/roles/firewall/tasks/firewallweb.yml"

  - name: "Ouverture des ports nrpe"
    include_tasks:
"/etc/ansible/roles/firewall/tasks/firewallnrpe.yml"
...
```

[root@svransible etc]# cd ansible/roles/nagios/templates/
[root@svransible templates]# ls

```
commands.cfg  contacts.cfg  hosts.cfg  nagios.cfg
```

[root@svransible templates]# vim commands.cfg

On ajoute ces lignes au fichier template

```
################################################################################
#
# SAMPLE REMOTE HOST CHECK COMMANDS
#
################################################################################
# 'check_nrpe' command definition
define command{
        command_name check_nrpe
        command_line $USER1$/check_nrpe -H $HOSTADDRESS$ -c $ARG1$
}
```

[root@svransible templates]# vim contacts.cfg

On édite le fichier template à sa guise

```
define contact{
        contact_name                    nagiosadmin
        use                             generic-contact
        alias                           Nagios Admin
        service_notification_period     24x7
        host_notification_period        24x7
        service_notification_options    w,u,c,r,f,s
        host_notification_options       d,u,r,f,s
        service_notification_commands   notify-service-by-email
```

```
        host_notification_commands      notify-host-by-email

        email                           nagios@localhost
        }
```

[root@svransible templates]# vim hosts.cfg

```
# Define a host for the remote machine

define host{
        use                     linux-server
        host_name               svransible
        alias                   svransible
        address                 172.32.1.255
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command           check-host-alive
        notification_period     workhours
        notification_interval   120
        notification_options    d,u,r
        contact_groups          admins
        }

define host{
        use                     linux-server
        host_name               svrweb1
        alias                   svrweb1
        address                 172.32.2.16
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command           check-host-alive
        notification_period     workhours
        notification_interval   120
        notification_options    d,u,r
        contact_groups          admins
        }

define host{
        use                     linux-server
        host_name               svrweb2
        alias                   svrweb2
        address                 172.32.2.20
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command           check-host-alive
        notification_period     workhours
        notification_interval   120
        notification_options    d,u,r
```

```
        contact_groups          admins
        }

define host{
        use                     linux-server
        host_name               svrftp
        alias                   svrftp
        address                 172.32.2.27
        check_period            24x7
        check_interval          5
        retry_interval          1
        max_check_attempts      10
        check_command           check-host-alive
        notification_period     workhours
        notification_interval   120
        notification_options    d,u,r
        contact_groups          admins
        }
##############################################################################
#############
##############################################################################
#############
#
# HOST GROUP DEFINITION
#
##############################################################################
#############
##############################################################################
#############

# Define an optional hostgroup for Linux machines

define hostgroup{
        hostgroup_name  servers
        alias           servers
        members         svransible, svrweb1, svrweb2, svrftp
        }



##############################################################################
#############
##############################################################################
#############
#
# SERVICE DEFINITIONS
#
##############################################################################
#############
##############################################################################
#############


# Define a service to "ping" the remote machine
```

```
define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             PING
        check_command
check_ping!100.0,20%!500.0,60%
        }


# Define a service to check the disk space of the remote partition

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             Remote Partition
        check_command                   check_nrpe!check_disk
        }


# Define a service to check the number of users on the remote
machine

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             Current Users
        check_command                   check_nrpe!check_users
        }


# Define a service to check the number of currently remote running
procs

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             Total Processes
        check_command
check_nrpe!check_total_procs
        }



# Define a service to check the load on the remote machine.

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             Current Load
        check_command                   check_nrpe!check_load!
        }
```

```
# Define a service to check the swap usage the remote machine.

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             Swap Usage
        check_command                   check_nrpe!check_swap
        }



# Define a service to check SSH on the remote machine.
# Disable notifications for this service by default, as not all
users may have SSH enabled.

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             SSH
        check_command                   check_ssh
        notifications_enabled           0
        }



# Define a service to check HTTP on the remote machine.
# Disable notifications for this service by default, as not all
users may have HTTP enabled.

define service{
        use                             generic-service
        hostgroup_name                  servers
        service_description             HTTP
        check_command                   check_http
        notifications_enabled           0
        }
```

[root@svransible templates]# vim nagios.cfg

```
# Definitions for monitoring the local (Linux) host
cfg_file=/etc/nagios/objects/hosts.cfg
```

NRPE

- **Création des tâches pour installer nrpe sur les machines à contrôler :**

```
[root@svransible nrpe]#
[root@svransible tasks]# vim main.yml
```

```yaml
---
# tasks file for installing nrpe
# Par défaut sur les distributions Debian l installation du plugin
nrpe ne cree
# pas le dossier /etc/nagios c est pourquoi il faut installer
nagios egalement

  - name: "Installation de nrpe sur les distributions RedHat"
    yum:
      name: "nagios-plugins*"
      state: "latest"
    when: ansible_os_family == 'RedHat'

  - name: "Installation de nagios sur les distributions Debian"
    apt:
      name: "nagios-nrpe-server"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "Installation de nrpe sur les distributions Debian"
    apt:
      name: "nagios-nrpe-plugin"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "Installation du fichier de configuration nrpe"
    template:
      src: "nrpe.cfg"
      dest: "/etc/nagios/nrpe.cfg"
      owner: "root"
      group: "root"
    register: confnrpe

  - name: "Demarrage du service nrpe"
    service:
      name: "nrpe"
      state: "started"
      enabled: yes
    when: confnrpe.changed
...
```

[root@svransible templates]# vim nrpe.cfg

```
ligne 117
allowed_hosts=127.0.0.1, 172.32.2.3
ligne 133
dont_blame_nrpe=1
ligne 314
command[check_disk]=/usr/lib64/nagios/plugins/check_disk -w 20% -c
10% -p /dev/sda1
command[check_swap]=/usr/lib64/nagios/plugins/check_swap -w 20% -c
10%
```

VSFTPD

- **Création des tâches pour le serveur FTP :**

```
[root@svransible tasks]# cd /etc/ansible/roles/vsftpd/tasks
[root@svransible tasks]# vim main.yml
```

```
---
# tasks file installation  vsftpd sur distribution Debians
  - name: "Installation du serveur vsftpd pour les distributions
Debian"
    apt:
      name: "vsftpd"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "installation du serveur vsftpd pour les distributions
RedHat"
    yum:
      name: "vsftpd"
      state: "latest"
    when: ansible_os_family == 'RedHat'

  - name: "demarrage du serveur ftp"
    service:
      name: "vsftpd"
      state: "started"
      enabled: "yes"

  - name: "Installation du parefeu ufw pour les distributions
Debian"
    apt:
      name: "ufw"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "Ouverture des ports ftp"
    include_tasks:
"/etc/ansible/roles/firewall/tasks/firewallftp.yml"

  - name: "Ouverture des ports nrpe"
    include_tasks:
"/etc/ansible/roles/firewall/tasks/firewallnrpe.yml"
...
```

USERS

- **Création des tâches pour ajouter les utilisateurs :**

```
[root@svransible ansible]# cd roles/addusers/tasks
[root@svransible tasks]# vim main.yml
```

```yaml
---
# tasks file for adding users
  - name: "Creation des groupes"
    group:
      name: "projet{{ item }}"
    with_items:
      - 1
      - 2

  - name: "installation du fichier login.defs pour renouvellement
password"
    template:
      src: "login.defs"
      dest: "/etc/login.defs"
      owner: "root"
      group: "root"

  - name: "installation du template bash"
    template:
      src: "bashrc"
      dest: "/etc/bashrc"
      owner: "root"
      group: "root"

  - name: "installation du template .bashrc"
    template:
      src: ".bashrc"
      dest: "/etc/skel/.bashrc"
      owner: "root"
      group: "root"

  - name:
    yum:
      name: "ksh"
      state: "latest"
    when: ansible_os_family == 'RedHat'

  - name:
    apt:
      name: "ksh"
      state: "latest"
    when: ansible_os_family == 'Debian'

  - name: "installation du template ksh"
    template:
      src: "kshrc"
```

```
      dest: "/etc/kshrc"
      owner: "root"
      group: "root"

  - name: "installation du template .kshrc"
    template:
      src: ".kshrc"
      dest: "/etc/skel/.kshrc"
      owner: "root"
      group: "root"

  - name: "installation du fichier de bienvenue"
    template:
      src: "bienvenue.txt"
      dest: "/etc/skel/bienvenue.txt"
      owner: "root"
      group: "root"

  - name: "Ajout des utilisateurs sur les differents serveurs"
    include_tasks: "addusers.yml"

...
```

[root@svransible tasks]# more addusers.yml

```
---
# Ajout d'utilsateurs sur distributions redhat
# le mot de passe par defaut de tous les utilisateurs est Pa$$w0rd

  - name: "Ajout des utilisateurs chefs de projet en shell ksh"
    user:
      name: "cp1"
      state: "present"
      groups: "projet1"
      comment: "chef de projet"
      uid: "10001"
      shell: "/bin/ksh"
      createhome: yes
      password:
"$6$/1/RIl3p$PTgsfk60ZClLbdAJJPsoA60u2sOrlCex.JX7Ay4y/GXlMLeULQnPw
82CzcLsHWbqv4YSJOGIu6WfM/Wo1yJr80"

  - name: "Ajout des utilisateurs chefs de projet en shell bash"
    user:
      name: "cp2"
      state: "present"
      groups: "projet2"
      comment: "chef de projet"
      uid: "10002"
      shell: "/bin/bash"
      createhome: yes
      password:
"$6$/1/RIl3p$PTgsfk60ZClLbdAJJPsoA60u2sOrlCex.JX7Ay4y/GXlMLeULQnPw
82CzcLsHWbqv4YSJOGIu6WfM/Wo1yJr80"
```

```
  - name: "ajouter des utilisateurs developpeurs ksh"
    user:
      name: "dev{{ item }}"
      state: "present"
      groups: "projet1"
      comment: "developpeur"
      uid: "100{{ item }}"
      shell: "/bin/ksh"
      createhome: yes
      password:
"$6$/1/RIl3p$PTgsfk60ZClLbdAJJPsoA60u2sOrlCex.JX7Ay4y/GXlMLeULQnPw
82CzcLsHWbqv4YSJOGIu6WfM/Wo1yJr80"
    with_items:
      - 10
      - 11
      - 12
      - 13
      - 14
      - 15

  - name: "ajouter des utilisateurs developpeurs bash"
    user:
      name: "dev{{ item }}"
      state: "present"
      groups: "projet2"
      comment: "developpeur"
      uid: "100{{ item }}"
      shell: "/bin/bash"
      createhome: yes
      password:
"$6$/1/RIl3p$PTgsfk60ZClLbdAJJPsoA60u2sOrlCex.JX7Ay4y/GXlMLeULQnPw
82CzcLsHWbqv4YSJOGIu6WfM/Wo1yJr80"
    with_items:
      - 20
      - 21
      - 22
      - 23
      - 24
      - 25
...
```

[root@svransible templates]# vim bashrc

Ajouter les lignes :

```
# clobber setting
set -o noclobber
```

[root@svransible templates]# vim kshrc

Ajouter les lignes :

```
# clobber setting
set +o clobber
```

[root@svransible templates]# vim .bashrc (ET vim .kshrc)

```
# aliases
alias h='history'
alias ll='ls -lrt'
```

[root@svransible templates]# vim login.defs

Modifier les lignes 25-28

```
PASS_MAX_DAYS   60
PASS_MIN_DAYS   55
PASS_MIN_LEN    5
PASS_WARN_AGE   6
```

FIREWALL

Création des tâches pour ouvrir les ports sur les différents serveurs :

```
[root@svransible ansible]# cd roles/firewall/tasks/
```

```
[root@svransible tasks]# vim firewallweb.yml
```

```yaml
---
# Ouvertures des ports http et nrpe sur les serveurs apache
  - name: "Ouverture des ports apache pour les distributions
RedHat"
    firewalld:
      service: http
      permanent: true
      state: enabled
    when: ansible_os_family == 'RedHat'

  - name: "Ouverture des ports apache pour les distributions
Debian"
    ufw:
      rule: allow
      port: 80
      proto: tcp
      state: enabled
    when: ansible_os_family == 'Debian'
...
```

```
[root@svransible tasks]# vim firewallnagios.yml
```

```yaml
---
# Ouvertures des ports NRPE

  - name: "Ouverture des ports nrpe sur les distributions Debian"
    ufw:
      rule: allow
      port: 5666
      proto: tcp
      state: enabled
    when: ansible_os_family == 'Debian'

  - name: "Ouverture des ports nrpe sur les distributions RedHat"
    firewalld:
      service: nrpe
      permanent: true
      state: enabled
    when: ansible_os_family == 'RedHat'
...
```

[root@svransible tasks]# vim firewallftp.yml

```yaml
---
# Ouverture des ports FTP pour serveur ftp

  - name: "Ouverture des ports vsftp sur les distributions RedHat"
    ufw:
      rule: allow
      port: 21
      proto: tcp
      state: enabled
    when: ansible_os_family == 'Debian'

  - name: "Ouverture des ports vsftp sur les distributions RedHat"
    firewalld:
      service: http
      permanent: true
      state: enabled
    when: ansible_os_family == 'RedHat'
...
```

NB : Cette section est conçue pour être opérationnelle quelle que soit la distribution (RedHat ou Debian) du serveur sur laquelle on va l'appliquer.

SECURITE

Création des tâches pour sécuriser les différents serveurs :

```
[root@svransible ansible]# cd roles/securite/tasks/
[root@svransible tasks]# vim main.yml
```

```
---
# tasks pour la securite
  - name: "installation du fichier system-auth pour memoriser les
6 derniers password"
    template:
      src: "system-auth"
      dest: "/etc/pam.d/system-auth"
      owner: "root"
      group: "root"

  - name: "installation du fichier pwquality definissant les
caracteres obligatoires du password"
    template:
      src: "pwquality.conf"
      dest: "/etc/security/pwdquality.conf"
      owner: "root"
      group: "root"

  - name: "config ssh pour serveur web1"
    include_tasks: sshweb1.yml
    when: inventory_hostname == svrweb1

  - name: "config ssh pour serveur web2"
    include_tasks: sshweb2.yml
    when: inventory_hostname == svrweb2


  - name: "config ssh pour serveur Nagios"
    include_tasks: sshnagans.yml
    when: inventory_hostname == svrnagios

  - name: "config ssh pour serveur Ansible"
    include_tasks: sshnagans.yml
    when: inventory_hostname == svransible
...
```

```
[root@svransible tasks]# vim sshweb1.yml
```

```
---
#configuration des acces ssh pour svrweb1

  - name: "installation du fichier pam.d sshd"
    template:
      src: "sshd"
```

```
      dest: "/etc/pam.d/sshd"
      owner: "root"
      group: "root"


  - name: "installation du fichier pam.d sshd"
    template:
      src: "ssh_users_allowweb1"
      dest: "/etc/ssh/ssh_users_allow"
      owner: "root"
      group: "root"
...
```

[root@svransible tasks]# vim sshweb2.yml

```
---
#configuration des acces ssh pour svrweb1

  - name: "installation du fichier pam.d sshd"
    template:
      src: "sshd"
      dest: "/etc/pam.d/sshd"
      owner: "root"
      group: "root"


  - name: "installation du fichier pam.d sshd"
    template:
      src: "ssh_users_allowweb2"
      dest: "/etc/ssh/ssh_users_allow"
      owner: "root"
      group: "root"
...
```

[root@svransible tasks]# vim sshnagans.yml

```
---
#configuration des acces ssh pour serveurs nagios et ansible

  - name: "installation du fichier pam.d sshd"
    template:
      src: "sshd"
      dest: "/etc/pam.d/sshd"
      owner: "root"
      group: "root"


  - name: "installation du fichier pam.d sshd"
    template:
      src: "ssh_users_allownagans"
      dest: "/etc/ssh/ssh_users_allow"
      owner: "root"
```

```
      group: "root"
...
```

[root@svransible roles]# vim securite/templates/ssh_users_allowweb1

```
#Utilisateurs autorisés a se connecter via ssh au serveur web1
dev10
dev11
dev12
dev13
dev14
dev15
```

[root@svransible roles]# vim securite/templates/ssh_users_allowweb2

```
#Utilisateurs autorisés a se connecter via ssh au serveur web2
dev20
dev21
dev22
dev23
dev24
dev25
```

[root@svransible roles]# vim securite/templates/ssh_users_allownagans

```
# Utilisateurs autorisés a se connecter via ssh aux serveurs
nagios et web
cp1
cp2
```

[root@svransible roles]# vim securite/templates/sshd

Modifier Ligne 2 du fichier original comme suit

```
auth       required     pam_listfile.so item=user sense=deny
file=/etc/ssh/ssh_users_allow onerr=succeed
```

[root@svransible roles]# vim securite/templates/system-auth

Modifier Ligne 3 du fichier original comme suit

```
auth        requisite     pam_succeed_if.so uid != 0 quiet
```

[root@svransible roles]# vim securite/templates/pwquality.conf

Editer le fichier original comme suit :

```

# Minimum acceptable size for the new password (plus one if
```

```
# credits are not disabled which is the default). (See
pam_cracklib manual.)
# Cannot be set to lower value than 6.
minlen = 8
#
# The maximum credit for having digits in the new password. If
less than 0
# it is the minimum number of digits in the new password.
dcredit = -2
#
# The maximum credit for having uppercase characters in the new
password.
# If less than 0 it is the minimum number of uppercase characters
in the new
# password.
ucredit = -1
```

Visualisation de l'arborescence finale :

```
[root@svransible ansible]# tree -af
.
├── ./ansible.cfg
├── ./cloud.yml
├── ./hosts
├── ./hosts.rpmnew
└── ./roles
    ├── ./roles/addusers
    │   ├── ./roles/addusers/defaults
    │   │   └── ./roles/addusers/defaults/main.yml
    │   ├── ./roles/addusers/files
    │   ├── ./roles/addusers/handlers
    │   │   └── ./roles/addusers/handlers/main.yml
    │   ├── ./roles/addusers/meta
    │   │   └── ./roles/addusers/meta/main.yml
    │   ├── ./roles/addusers/README.md
    │   ├── ./roles/addusers/tasks
    │   │   ├── ./roles/addusers/tasks/addusers.yml
    │   │   └── ./roles/addusers/tasks/main.yml
    │   ├── ./roles/addusers/templates
    │   │   ├── ./roles/addusers/templates/bashrc
    │   │   ├── ./roles/addusers/templates/.bashrc
    │   │   ├── ./roles/addusers/templates/bienvenue.txt
    │   │   ├── ./roles/addusers/templates/kshrc
    │   │   ├── ./roles/addusers/templates/.kshrc
    │   │   └── ./roles/addusers/templates/login.defs
    │   ├── ./roles/addusers/tests
    │   │   ├── ./roles/addusers/tests/inventory
    │   │   └── ./roles/addusers/tests/test.yml
    │   └── ./roles/addusers/vars
    │       └── ./roles/addusers/vars/main.yml
    └── ./roles/apache
        ├── ./roles/apache/defaults
        │   └── ./roles/apache/defaults/main.yml
        ├── ./roles/apache/files
        ├── ./roles/apache/handlers
        │   └── ./roles/apache/handlers/main.yml
        ├── ./roles/apache/meta
        │   └── ./roles/apache/meta/main.yml
        ├── ./roles/apache/README.md
        ├── ./roles/apache/tasks
        │   └── ./roles/apache/tasks/main.yml
        ├── ./roles/apache/templates
        │   └── ./roles/apache/templates/index.html
        ├── ./roles/apache/tests
        │   ├── ./roles/apache/tests/inventory
        │   └── ./roles/apache/tests/test.yml
        └── ./roles/apache/vars
            └── ./roles/apache/vars/main.yml
```

```
├── ./roles/firewall
│   ├── ./roles/firewall/defaults
│   │   └── ./roles/firewall/defaults/main.yml
│   ├── ./roles/firewall/files
│   ├── ./roles/firewall/handlers
│   │   └── ./roles/firewall/handlers/main.yml
│   ├── ./roles/firewall/meta
│   │   └── ./roles/firewall/meta/main.yml
│   ├── ./roles/firewall/README.md
│   ├── ./roles/firewall/tasks
│   │   ├── ./roles/firewall/tasks/firewallftp.yml
│   │   ├── ./roles/firewall/tasks/firewallnrpe.yml
│   │   ├── ./roles/firewall/tasks/firewallweb.yml
│   │   └── ./roles/firewall/tasks/main.yml
│   ├── ./roles/firewall/templates
│   ├── ./roles/firewall/tests
│   │   ├── ./roles/firewall/tests/inventory
│   │   └── ./roles/firewall/tests/test.yml
│   └── ./roles/firewall/vars
│       └── ./roles/firewall/vars/main.yml
├── ./roles/nagios
│   ├── ./roles/nagios/defaults
│   │   └── ./roles/nagios/defaults/main.yml
│   ├── ./roles/nagios/files
│   ├── ./roles/nagios/handlers
│   │   └── ./roles/nagios/handlers/main.yml
│   ├── ./roles/nagios/meta
│   │   └── ./roles/nagios/meta/main.yml
│   ├── ./roles/nagios/README.md
│   ├── ./roles/nagios/tasks
│   │   └── ./roles/nagios/tasks/main.yml
│   ├── ./roles/nagios/templates
│   │   ├── ./roles/nagios/templates/commands.cfg
│   │   ├── ./roles/nagios/templates/contacts.cfg
│   │   ├── ./roles/nagios/templates/hosts.cfg
│   │   └── ./roles/nagios/templates/nagios.cfg
│   ├── ./roles/nagios/tests
│   │   ├── ./roles/nagios/tests/inventory
│   │   └── ./roles/nagios/tests/test.yml
│   └── ./roles/nagios/vars
│       └── ./roles/nagios/vars/main.yml
├── ./roles/nrpe
│   ├── ./roles/nrpe/defaults
│   │   └── ./roles/nrpe/defaults/main.yml
│   ├── ./roles/nrpe/files
│   ├── ./roles/nrpe/handlers
│   │   └── ./roles/nrpe/handlers/main.yml
│   ├── ./roles/nrpe/meta
│   │   └── ./roles/nrpe/meta/main.yml
│   ├── ./roles/nrpe/README.md
│   ├── ./roles/nrpe/tasks
│   │   └── ./roles/nrpe/tasks/main.yml
│   ├── ./roles/nrpe/templates
│   │   └── ./roles/nrpe/templates/nrpe.cfg
```

```
│   ├── ./roles/nrpe/tests
│   │   ├── ./roles/nrpe/tests/inventory
│   │   └── ./roles/nrpe/tests/test.yml
│   └── ./roles/nrpe/vars
│       └── ./roles/nrpe/vars/main.yml
├── ./roles/securite
│   ├── ./roles/securite/defaults
│   │   └── ./roles/securite/defaults/main.yml
│   ├── ./roles/securite/files
│   ├── ./roles/securite/handlers
│   │   └── ./roles/securite/handlers/main.yml
│   ├── ./roles/securite/meta
│   │   └── ./roles/securite/meta/main.yml
│   ├── ./roles/securite/README.md
│   ├── ./roles/securite/tasks
│   │   ├── ./roles/securite/tasks/main.yml
│   │   ├── ./roles/securite/tasks/sshnagans.yml
│   │   ├── ./roles/securite/tasks/sshweb1.yml
│   │   └── ./roles/securite/tasks/sshweb2.yml
│   ├── ./roles/securite/templates
│   │   ├── ./roles/securite/templates/pwquality.conf
│   │   ├── ./roles/securite/templates/sshd
│   │   ├── ./roles/securite/templates/ssh_users_allownagans
│   │   ├── ./roles/securite/templates/ssh_users_allowweb1
│   │   ├── ./roles/securite/templates/ssh_users_allowweb2
│   │   └── ./roles/securite/templates/system-auth
│   ├── ./roles/securite/tests
│   │   ├── ./roles/securite/tests/inventory
│   │   └── ./roles/securite/tests/test.yml
│   └── ./roles/securite/vars
│       └── ./roles/securite/vars/main.yml
└── ./roles/vsftpd
    ├── ./roles/vsftpd/defaults
    │   └── ./roles/vsftpd/defaults/main.yml
    ├── ./roles/vsftpd/files
    ├── ./roles/vsftpd/handlers
    │   └── ./roles/vsftpd/handlers/main.yml
    ├── ./roles/vsftpd/meta
    │   └── ./roles/vsftpd/meta/main.yml
    ├── ./roles/vsftpd/README.md
    ├── ./roles/vsftpd/tasks
    │   └── ./roles/vsftpd/tasks/main.yml
    ├── ./roles/vsftpd/templates
    ├── ./roles/vsftpd/tests
    │   ├── ./roles/vsftpd/tests/inventory
    │   └── ./roles/vsftpd/tests/test.yml
    └── ./roles/vsftpd/vars
        └── ./roles/vsftpd/vars/main.yml

64 directories, 85 files
```

Vérification :

[root@svransible ansible]# ansible-playbook --check cloud.yml

```
PLAY [all, localhost]
*********************************************************************

TASK [Gathering Facts]
*********************************************************************
ok: [svrftp]
ok: [localhost]
ok: [svrweb1]
ok: [svrnagios]
ok: [svrweb2]

TASK [addusers : Creation des groupes]
*****************************************
changed: [svrftp] => (item=1)
changed: [svrweb2] => (item=1)
changed: [svrweb1] => (item=1)
changed: [svrnagios] => (item=1)
changed: [localhost] => (item=1)
changed: [svrftp] => (item=2)
changed: [svrweb1] => (item=2)
changed: [svrnagios] => (item=2)
changed: [svrweb2] => (item=2)
changed: [localhost] => (item=2)

TASK [addusers : installation du fichier login.defs pour
renouvellement password] ***
changed: [svrftp]
changed: [svrweb2]
changed: [svrnagios]
changed: [svrweb1]
changed: [localhost]

TASK [addusers : installation du template bash]
*********************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [svrnagios]
changed: [localhost]

TASK [addusers : installation du template .bashrc]
*****************************
changed: [svrftp]
changed: [svrweb2]
changed: [svrweb1]
```

```
changed: [localhost]
changed: [svrnagios]

TASK [addusers : yum]
*********************************************************
skipping: [svrftp]
changed: [localhost]
changed: [svrweb1]
changed: [svrnagios]
changed: [svrweb2]

TASK [addusers : apt]
*********************************************************
skipping: [svrweb1]
skipping: [svrweb2]
skipping: [svrnagios]
skipping: [localhost]
changed: [svrftp]

TASK [addusers : installation du template ksh]
*********************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [addusers : installation du template .kshrc]
*******************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [addusers : installation du fichier de bienvenue]
*************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [addusers : Ajout des utilisateurs sur les differents
serveurs] ***********
included: /etc/ansible/roles/addusers/tasks/addusers.yml for
svrftp, svrweb1, svrweb2, svrnagios, localhost

TASK [addusers : Ajout des utilisateurs chefs de projet en shell
ksh] **********
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [svrnagios]
```

```
changed: [localhost]

TASK [addusers : Ajout des utilisateurs chefs de projet en shell
bash] *********
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [addusers : ajouter des utilisateurs developpeurs ksh]
*********************
changed: [svrftp] => (item=10)
changed: [svrweb1] => (item=10)
changed: [svrweb2] => (item=10)
changed: [svrnagios] => (item=10)
changed: [localhost] => (item=10)
changed: [svrftp] => (item=11)
changed: [svrweb1] => (item=11)
changed: [svrweb2] => (item=11)
changed: [svrnagios] => (item=11)
changed: [svrftp] => (item=12)
changed: [localhost] => (item=11)
changed: [svrnagios] => (item=12)
changed: [svrweb2] => (item=12)
changed: [svrweb1] => (item=12)
changed: [svrftp] => (item=13)
changed: [localhost] => (item=12)
changed: [svrweb1] => (item=13)
changed: [svrftp] => (item=14)
changed: [svrnagios] => (item=13)
changed: [svrweb2] => (item=13)
changed: [localhost] => (item=13)
changed: [svrftp] => (item=15)
changed: [svrweb1] => (item=14)
changed: [svrweb2] => (item=14)
changed: [svrnagios] => (item=14)
changed: [localhost] => (item=14)
changed: [localhost] => (item=15)
changed: [svrnagios] => (item=15)
changed: [svrweb2] => (item=15)
changed: [svrweb1] => (item=15)

TASK [addusers : ajouter des utilisateurs developpeurs bash]
*********************
changed: [svrftp] => (item=20)
changed: [svrweb1] => (item=20)
changed: [svrweb2] => (item=20)
changed: [svrnagios] => (item=20)
changed: [localhost] => (item=20)
changed: [svrftp] => (item=21)
changed: [svrweb1] => (item=21)
changed: [svrnagios] => (item=21)
changed: [svrweb2] => (item=21)
```

```
changed: [svrftp] => (item=22)
changed: [localhost] => (item=21)
changed: [svrweb1] => (item=22)
changed: [svrnagios] => (item=22)
changed: [svrweb2] => (item=22)
changed: [svrftp] => (item=23)
changed: [localhost] => (item=22)
changed: [svrweb1] => (item=23)
changed: [svrftp] => (item=24)
changed: [svrweb2] => (item=23)
changed: [svrnagios] => (item=23)
changed: [localhost] => (item=23)
changed: [svrftp] => (item=25)
changed: [svrweb1] => (item=24)
changed: [svrweb2] => (item=24)
changed: [svrnagios] => (item=24)
changed: [localhost] => (item=24)
changed: [svrweb1] => (item=25)
changed: [svrnagios] => (item=25)
changed: [svrweb2] => (item=25)
changed: [localhost] => (item=25)

TASK [nrpe : Installation de nrpe sur les distributions RedHat]
*****************
skipping: [svrftp]
changed: [localhost]
changed: [svrnagios]
changed: [svrweb2]
changed: [svrweb1]

TASK [nrpe : Installation de nagios sur les distributions Debian]
***************
skipping: [svrweb1]
skipping: [svrweb2]
skipping: [svrnagios]
skipping: [localhost]
changed: [svrftp]

TASK [nrpe : Installation de nrpe sur les distributions Debian]
*****************
skipping: [svrweb1]
skipping: [svrweb2]
skipping: [svrnagios]
skipping: [localhost]
changed: [svrftp]

TASK [nrpe : Installation du fichier de configuration nrpe]
*********************
changed: [svrftp]
changed: [localhost]
changed: [svrweb2]
changed: [svrnagios]
changed: [svrweb1]
```

```
TASK [nrpe : Demarrage du service nrpe]
*****************************************
changed: [svrftp]
changed: [localhost]
changed: [svrweb2]
changed: [svrweb1]
changed: [svrnagios]

TASK [securite : installation du fichier system-auth pour
memoriser les 6 derniers password] ***
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [securite : installation du fichier pwquality definissant les
caracteres obligatoires du password] ***
changed: [svrftp]
changed: [localhost]
changed: [svrweb2]
changed: [svrweb1]
changed: [svrnagios]

TASK [securite : config ssh pour serveur web1]
**********************************
included: /etc/ansible/roles/securite/tasks/sshweb1.yml for
svrftp, svrweb1, svrweb2, svrnagios, localhost

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [localhost]
changed: [svrweb2]
changed: [svrnagios]

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [securite : config ssh pour serveur web2]
**********************************
included: /etc/ansible/roles/securite/tasks/sshweb2.yml for
svrftp, svrweb1, svrweb2, svrnagios, localhost

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [localhost]
```

```
changed: [svrweb2]
changed: [svrweb1]
changed: [svrnagios]

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [securite : config ssh pour serveur Nagios]
*******************************
included: /etc/ansible/roles/securite/tasks/sshnagans.yml for
svrftp, svrweb1, svrweb2, svrnagios, localhost

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [localhost]
changed: [svrweb2]
changed: [svrnagios]

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [localhost]
changed: [svrweb2]
changed: [svrnagios]

TASK [securite : config ssh pour serveur Ansible]
*******************************
included: /etc/ansible/roles/securite/tasks/sshnagans.yml for
svrftp, svrweb1, svrweb2, svrnagios, localhost

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [svrweb2]
changed: [localhost]
changed: [svrnagios]

TASK [securite : installation du fichier pam.d sshd]
****************************
changed: [svrftp]
changed: [svrweb1]
changed: [localhost]
changed: [svrweb2]
changed: [svrnagios]
```

```
PLAY [web]
*********************************************************************
***

TASK [Gathering Facts]
*********************************************************
ok: [svrweb1]
ok: [svrweb2]

TASK [apache : Installation du package apache si distribution
RedHat] **********
changed: [svrweb2]
changed: [svrweb1]

TASK [apache : Installation du package apache si distribution
Debian] **********
skipping: [svrweb1]
skipping: [svrweb2]

TASK [apache : Installation de la page de garde]
*******************************
changed: [svrweb1]
changed: [svrweb2]

TASK [apache : Redemarrage du service apache si distribution
RedHat] ***********
changed: [svrweb1]
changed: [svrweb2]

TASK [apache : Redemarrage du service apache si distribution
Debian] ***********
changed: [svrweb1]
changed: [svrweb2]

TASK [apache : include_tasks]
*************************************************
included: /etc/ansible/roles/firewall/tasks/firewallweb.yml for
svrweb1, svrweb2

TASK [apache : Ouverture des ports apache pour les distributions
RedHat] *******
changed: [svrweb2]
changed: [svrweb1]

TASK [apache : Ouverture des ports apache pour les distributions
Debian] *******
skipping: [svrweb1]
skipping: [svrweb2]

TASK [apache : include_tasks]
*************************************************
included: /etc/ansible/roles/firewall/tasks/firewallnrpe.yml for
svrweb1, svrweb2
```

```
TASK [apache : Ouverture des ports nrpe sur les distributions
Debian] **********
skipping: [svrweb1]
skipping: [svrweb2]

TASK [apache : Ouverture des ports nrpe sur les distributions
RedHat] **********
changed: [svrweb1]
changed: [svrweb2]

TASK [apache : Installation de l'antivirus clamav si distribution
RedHat] ******
changed: [svrweb1]
changed: [svrweb2]

TASK [apache : Installation de l'antivirus clamav si distribution
Debian] ******
skipping: [svrweb1]
skipping: [svrweb2]

PLAY [nagios]
*********************************************************************

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

TASK [nagios : Installation de Nagiossur Debian]
*******************************
skipping: [svrnagios]

TASK [nagios : Installation de Nagios sur Redhat]
*******************************
skipping: [svrnagios]

TASK [nagios : Installation du fichier de configuration nagios]
*****************
changed: [svrnagios]

TASK [nagios : Installation du fichier de configuration commands]
**************
changed: [svrnagios]

TASK [nagios : Installation du fichier de configuration contacts]
**************
changed: [svrnagios]

TASK [nagios : Installation du fichier de configuration hosts]
******************
changed: [svrnagios]

TASK [nagios : RE-Demarrage du service Nagios]
*********************************
changed: [svrnagios]
```

```
TASK [nagios : include_tasks]
*************************************************
included: /etc/ansible/roles/firewall/tasks/firewallweb.yml for
svrnagios

TASK [nagios : Ouverture des ports apache pour les distributions
RedHat] *******
changed: [svrnagios]

TASK [nagios : Ouverture des ports apache pour les distributions
Debian] *******
skipping: [svrnagios]

TASK [nagios : include_tasks]
*************************************************
included: /etc/ansible/roles/firewall/tasks/firewallnrpe.yml for
svrnagios

TASK [nagios : Ouverture des ports nrpe sur les distributions
Debian] **********
skipping: [svrnagios]

TASK [nagios : Ouverture des ports nrpe sur les distributions
RedHat] **********
changed: [svrnagios]

PLAY [ftp]
*********************************************************************
***

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

TASK [vsftpd : Installation du serveur vsftpd pour les
distributions Debian] ***
changed: [svrftp]

TASK [vsftpd : installation du serveur vsftpd pour les
distributions RedHat] ***
skipping: [svrftp]

TASK [vsftpd : demarrage du serveur ftp]
****************************************
changed: [svrftp]

TASK [vsftpd : Installation du parefeu ufw pour les distributions
Debian] ******
ok: [svrftp]

TASK [vsftpd : Ouverture des ports]
*********************************************
included: /etc/ansible/roles/firewall/tasks/firewallftp.yml for
```

```
svrftp

TASK [vsftpd : Ouverture des ports vsftp sur les distributions
RedHat] *********
ok: [svrftp]

TASK [vsftpd : Ouverture des ports vsftp sur les distributions
RedHat] *********
skipping: [svrftp]

TASK [vsftpd : include_tasks]
**************************************************
included: /etc/ansible/roles/firewall/tasks/firewallnrpe.yml for
svrftp

TASK [vsftpd : Ouverture des ports nrpe sur les distributions
Debian] **********
ok: [svrftp]

TASK [vsftpd : Ouverture des ports nrpe sur les distributions
RedHat] **********
skipping: [svrftp]

PLAY RECAP
**********************************************************************
***
localhost          : ok=31   changed=25   unreachable=0    failed=0
svrftp             : ok=40   changed=28   unreachable=0    failed=0
svrnagios          : ok=41   changed=32   unreachable=0    failed=0
svrweb1            : ok=41   changed=32   unreachable=0    failed=0
svrweb2            : ok=41   changed=32   unreachable=0    failed=0
```

COMMENTAIRES

Coté Serveurs il reste des paramétrages à faire pour fonctionner avec SeLinux:

- **Serveurs Apache :**

[root@svrwebX]# setsebool -P antivirus_can_scan_system 1
[root@svrwebX]# setsebool -P clamd-use_jit 1

```
Boolean clamd                                   use_jit is not defined
```

[root@svrwebX]# setsebool -P clamd_use_jit 1
[root@svrwebX]# getsebool -a | grep antivirus

```
antivirus_can_scan_system   -- -> on
antivirus_use_jit           -- -> on
```

- **Serveur Nagios : Pour permettre le fonctionnement de l'interface web :Attention Procédure non vérifiée**

Source :
https://fportase.wordpress.com/selinux-policies/nagios-and-rhel-5-xx-and-6-xx-working-with-selinux-enabled/

- create custom nagios plugin

```
# cd /etc/selinux/targeted
# mkdir nagios
# cd !$
# vi nagios_plugin.te
```

```
module nagios_ 1.4;
require {
        type nagios_t;
        type nagios_log_t;
        type var_t;
        type ping_t;
        type httpd_t;
        type httpd_sys_content_t;
        type httpd_nagios_script_t;
        type procmail_t;
        type system_mail_t;
```

```
        type nagios_services_plugin_t;
        type postfix_local_t;
        type nagios_checkdisk_plugin_t;
        type nagios_system_plugin_t;
        class process { signal sigkill ptrace };
        class dir { read write search add_name remove_name };
        class file manage_file_perms;
        class fifo_file { read write create open getattr };
}
#============= httpd_nagios_script_t ================
allow httpd_nagios_script_t var_t:file { open read getattr };
allow httpd_nagios_script_t var_t:fifo_file { open write getattr };
#============= nagios_services_plugin_t ==============
allow nagios_services_plugin_t var_t:file { read write };
#============= httpd_t ==============
allow httpd_t var_t:file { open read getattr };
#============= nagios_t ==============
#allow nagios_t self:process ptrace;
allow nagios_t system_mail_t:process { signal sigkill };
allow nagios_t httpd_sys_content_t:file { write getattr };
allow nagios_t var_t:dir { read write add_name remove_name };
allow nagios_t var_t:fifo_file { read write create open getattr };
allow nagios_t var_t:file manage_file_perms;
#============= ping_t ==============
allow ping_t var_t:file { read write };
#============= procmail_t ==============
allow procmail_t nagios_log_t:dir search;
#============= postfix_local_t ==============
allow postfix_local_t nagios_log_t:dir search;
#============= nagios_checkdisk_plugin_t ==============
allow nagios_checkdisk_plugin_t var_t:file { open read write };
#============= nagios_system_plugin_t ==============
allow nagios_system_plugin_t var_t:file { open read write };
```

- compile plugin (selinux-devel should be installed)

```
# make -f /usr/share/selinux/devel/Makefile
```

If compilation process finished OK we'll get a new file nagios_plugin.pp

```
# setenforce 0
```

- load compiled plugin

```
# semodule -i  nagios_plugin.pp

# setenforce 1
```

Now Nagios should work in enforced mode without any problems:

Il faut egalement redefinir le mot de passe pour acceder à l'interface web :

```
# htpassword –c /etc/nagios/passwd nagiosadmin
```