Wazuh Manager

This role will install and configure Wazuh Manager and Wazuh API, there are several variables you can use to customize the installation or configuration, by example:

- **json_output:** enabling or not JSON output (default: `yes`)

- **email_notification:** enabling email notifications (default: `no`)

- **mail_to:** email notifications recipients (array, defaults: `admin@example.net`)

- **mail_smtp_server:** SMTP server to be used by email notifications (defaults: `localhost`)

- **mail_from:** email notification sender (defaults: `ossec@example.com`)

By creating a YAML file `wazuh-manager.yml` you can be set the usage of this role:

```
- hosts: wazuh-manager
  roles:
    - ansible-wazuh-manager
    - ansible-role-filebeat
```

Setting the variables on a separate YAML file is recommended when configuring the installation. For this example we used: `vars-production.yml` :

```
filebeat_output_logstash_hosts: '10.1.1.11:5000'

wazuh_manager_fqdn: "wazuh-server"

wazuh_manager_config:
  json_output: 'yes'
  alerts_log: 'yes'
  logall: 'no'
  log_format: 'plain'
  connection:
    - type: 'secure'
      port: '1514'
      protocol: 'tcp'
  authd:
    enable: true
    port: 1515
    use_source_ip: 'no'
    force_insert: 'no'
    force_time: 0
    purge: 'no'
    use_password: 'no'
    ssl_agent_ca: null
    ssl_verify_host: 'no'
    ssl_manager_cert: null
    ssl_manager_key: null
    ssl_auto_negotiate: 'no'
```

You can configure **Wazuh API** user credentials, this could be done by setting the file: `ansible-wazuh-manager/vars/wazuh_api_creds.yml` located on your Ansible control server, the credentials are in `htpasswd` format:

```
# Be sure you encrypt this file with ansible-vault
wazuh_api_user:
- foo:$apr1$/axqZYWQ$Xo/nz/IG3PdwV82EnfYKh/
- bar:$apr1$hXE97ag.$8m0koHByattiGKUKPUgcZ1
```

Also, you can configure **agentless** host credentials via the file: `ansible-wazuh-manager/vars/agentless_creeds.yml` , set many as you need:

```
# Be sure you encrypt this file with ansible-vault.
agentless_creeds:
  - type: ssh_integrity_check_linux
    frequency: 3600
    host: root@example1.net
    state: periodic
    arguments: '/bin /etc/ /sbin'
    passwd: qwerty
  - type: ssh_integrity_check_bsd
    frequency: 3600
    host: user@example2.net
    state: periodic
    arguments: '/bin /etc/ /sbin'
    passwd: qwerty
```

And the `authd` service password could be set in the file `ansible-wazuh-manager/vars/authd_pass.yml` :

```
# Be sure you encrypt this file with ansible-vault
authd_pass: foobar
```

> ⚠️ Warning
>
> We recommend the use of Ansible Vault to protect Wazuh API and agentless credentials.

Next, run the playbook:

```
$ ansible-playbook wazuh-manager.yml -e@vars-production.yml
```

The example above will install Wazuh Manager and Filebeat, Filebeat will be configured to forward data to `10.1.1.11:5000` as Logstash node, also it will set various `agentless` hosts configurations including their credentials, the Wazuh API and the `authd` will be configured as well.

Please review the references section to see all variables available for this role.