Variables references

Elasticseach

elasticsearch_cluster_name

Name of the Elasticsearch cluster

Default wazuh

elasticsearch_node_name

Name of the Elasticsearch node

Default node-1

elasticsearch_http_port

ElasticSearch listening port

Default 9200

elasticsearch_network_host

ElasticSearch, listening ip address

Default 127.0.0.1

elasticsearch_jvm_xms

JVM heap size

Default null

elastic_stack_version

Version of Elasticsearch to install

Default 5.6.3

elasticsearch_shards

Set number of shards for indices

Default 5

elasticsearch_replicas

Set number of shards for indices

Default 1

Kibana

elasticsearch_http_port

Elasticsearch node port.

Default 9200

elasticsearch_network_host

IP address or hostname of Elasticsearch node.

Default 127.0.0.1

kibana_server_host

Listening IP address of Kibana.

Default 0.0.0.0

kibana_server_port

Listening port of Kibana.

Default 5601

elastic_stack_version

Version of Kibana to install

Default 5.6.3

Logstash

logstash_create_config

Generate or not Logstash config.

Defaults true

logstash_input_beats

When is set to true, it will configure Logstash to use Filebeat input. Otherwise it will use File input.

Defaults false

elasticsearch_network_host

Ip address or hostname of Elasticsearch node.

Default 127.0.0.1

elasticsearch_http_port

Port of Elasticsearch node.

Default 9200

elasticsearch_shards

Set number of shards for indices

Default 5

elasticsearch_replicas

Set number of shards for indices

Default 1

elastic_stack_version

Version of Logstash to install

Default 5.6.3

logstash_ssl

Using ssl between filebeat and logstash

Default false

logstash_ssl_dir

Folder where the SSL key and cert will be stored.

Default /etc/pki/logstash

logstash_ssl_certificate_file

SSL certificate file to be copied from Ansible server to logstash server.

Default null

logstash_ssl_key_file

SSL key file to be copied from Ansible server to logstash server.

Default null

Filebeat

filebeat_create_config:

Generate or not Filebeat config.

Default true

filebeat_prospectors:

Set filebeat propectors to fetch data.

Example:

```
filebeat_prospectors:
- input_type: log
  paths:
    - "/var/ossec/logs/alerts/alerts.json"
  document_type: json
  json.message_key: log
  json.keys_under_root: true
  json.overwrite_keys: true
```

filebeat_output_elasticsearch_enabled:

Send output to Elasticsearch node(s).

Default false

filebeat_output_elasticsearch_hosts:

Elasticsearch node(s) to send output.

Example:

```
filebeat_output_elasticsearch_hosts:
- "localhost:9200"
- "10.1.1.10:9200"
```

filebeat_output_logstash_enabled:

Send output to Logstash node(s).

Default true

filebeat_output_logstash_hosts:

Logstash node(s) to send output.

Example:

```
filebeat_output_logstash_hosts:
- "10.1.1.10:5000"
- "10.1.1.11:5000"
```

filebeat_enable_logging:

Enable/disable logging.

Default true

filebeat_log_level:

Set filebeat log level.

Default debug

filebeat_log_dir:

Set filebeat log directory.

Default: /var/log/mybeat

filebeat_log_filename:

Set filebeat log filename.

Default mybeat.log

filebeat_ssl_dir:

Set the folder containing SSL certs.

Default /etc/pki/logstash

filebeat_ssl_certificate_file:

Set certificate filename.

Default null

filebeat_ssl_key_file:

Set certificate key filename.

Default null

filebeat_ssl_insecure:

Verify validity of the server certificate hostname.

Default false

Wazuh Manager

wazuh_manager_fqdn:

Set Wazuh Manager fqdn hostname.

Default wazuh-server

wazuh_manager_config:

This store the Wazuh Manager configuration.

Example:

```
wazuh_manager_config:
  json_output: 'yes'
  alerts_log: 'yes'
  logall: 'no'
  log_format: 'plain'
  connection:
  - type: 'secure'
    port: '1514'
    protocol: 'tcp'
  authd:
  enable: false
  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'
  email_notification: 'no'
  mail_to:
  - 'admin@example.net'
  mail_smtp_server: localhost
  mail_from: wazuh-server@example.com
  extra_emails:
  - enable: false
    mail_to: 'admin@example.net'
    format: full
    level: 7
    event_location: null
    group: null
    do_not_delay: false
    do_not_group: false
    rule_id: null
  reports:
  - enable: false
    category: 'syscheck'
    title: 'Daily report: File changes'
    email_to: 'admin@example.net'
    location: null
    group: null
    rule: null
    level: null
    srcip: null
    user: null
    showlogs: null
  syscheck:
  frequency: 43200
  scan_on_start: 'yes'
  auto_ignore: 'no'
  alert_new_files: 'yes'
  ignore:
    - /etc/mtab
    - /etc/mnttab
    - /etc/hosts.deny
    - /etc/mail/statistics
    - /etc/random-seed
    - /etc/random.seed
    - /etc/adjtime
    - /etc/httpd/logs
    - /etc/utmpx
    - /etc/wtmpx
    - /etc/cups/certs
    - /etc/dumpdates
    - /etc/svc/volatile
  no_diff:
    - /etc/ssl/private.key
  directories:
    - dirs: /etc,/usr/bin,/usr/sbin
      checks: 'check_all="yes"'
    - dirs: /bin,/sbin
      checks: 'check_all="yes"'
  rootcheck:
  frequency: 43200
  openscap:
  timeout: 1800
  interval: '1d'
  scan_on_start: 'yes'
  log_level: 1
  email_level: 12
  localfiles:
  - format: 'syslog'
    location: '/var/log/messages'
  - format: 'syslog'
    location: '/var/log/secure'
  - format: 'command'
    command: 'df -P'
    frequency: '360'
  - format: 'full_command'
    command: 'netstat -tln | grep -v 127.0.0.1 | sort'
    frequency: '360'
  - format: 'full_command'
    command: 'last -n 20'
    frequency: '360'
  globals:
  - '127.0.0.1'
  - '192.168.2.1'
  commands:
  - name: 'disable-account'
    executable: 'disable-account.sh'
    expect: 'user'
    timeout_allowed: 'yes'
  - name: 'restart-ossec'
    executable: 'restart-ossec.sh'
    expect: ''
    timeout_allowed: 'no'
  - name: 'win_restart-ossec'
    executable: 'restart-ossec.cmd'
    expect: ''
    timeout_allowed: 'no'
  - name: 'firewall-drop'
    executable: 'firewall-drop.sh'
    expect: 'srcip'
    timeout_allowed: 'yes'
  - name: 'host-deny'
    executable: 'host-deny.sh'
    expect: 'srcip'
    timeout_allowed: 'yes'
  - name: 'route-null'
    executable: 'route-null.sh'
    expect: 'srcip'
    timeout_allowed: 'yes'
  - name: 'win_route-null'
    executable: 'route-null.cmd'
    expect: 'srcip'
    timeout_allowed: 'yes'
  active_responses:
  - command: 'restart-ossec'
    location: 'local'
    rules_id: '100002'
  - command: 'win_restart-ossec'
    location: 'local'
    rules_id: '100003'
  - command: 'host-deny'
    location: 'local'
    level: 6
    timeout: 600
  syslog_outputs:
  - server: null
    port: null
    format: null
```

wazuh_agent_configs:

This store the different settings and profiles for centralized agent configuration via Wazuh Manager.

Example:

```
- type: os
  type_value: Linux
  syscheck:
    frequency: 43200
    scan_on_start: 'yes'
    auto_ignore: 'no'
    alert_new_files: 'yes'
    ignore:
    - /etc/mtab
    - /etc/mnttab
    - /etc/hosts.deny
    - /etc/mail/statistics
    - /etc/svc/volatile
    no_diff:
      - /etc/ssl/private.key
    directories:
      - dirs: /etc,/usr/bin,/usr/sbin
        checks: 'check_all="yes"'
      - dirs: /bin,/sbin
        checks: 'check_all="yes"'
  rootcheck:
    frequency: 43200
    cis_distribution_filename: null
  localfiles:
    - format: 'syslog'
      location: '/var/log/messages'
    - format: 'syslog'
      location: '/var/log/secure'
    - format: 'syslog'
      location: '/var/log/maillog'
    - format: 'apache'
      location: '/var/log/httpd/error_log'
    - format: 'apache'
      location: '/var/log/httpd/access_log'
    - format: 'apache'
      location: '/var/ossec/logs/active-responses.log'
- type: os
  type_value: Windows
  syscheck:
    frequency: 43200
    scan_on_start: 'yes'
    auto_ignore: 'no'
    alert_new_files: 'yes'
    windows_registry:
      - key: 'HKEY_LOCAL_MACHINE\Software\Classes\batfile'
        arch: 'both'
      - key: 'HKEY_LOCAL_MACHINE\Software\Classes\Folder'
  localfiles:
    - format: 'Security'
      location: 'eventchannel'
    - format: 'System'
      location: 'eventlog'
```

cdb_lists:

Configure CDB lists used by the Wazuh Manager (located at `ansible-wazuh-manager/vars/cdb_lists.yml`).

Example:

```
cdb_lists:
- name: 'audit-keys'
  content: |
    audit-wazuh-w:write
    audit-wazuh-r:read
    audit-wazuh-a:attribute
    audit-wazuh-x:execute
    audit-wazuh-c:command
```

⚠ Warning

We recommend the use of Ansible Vault to protect Wazuh, agentless and authd credentials.

agentless_creeds:

Credentials and host(s) to be used by agentless feature.

Example:

```
agentless_creeds:
  - type: ssh_integrity_check_linux
    frequency: 3600
    host: root@example.net
    state: periodic
    arguments: '/bin /etc/ /sbin'
    passwd: qwerty
```

⚠ Warning

We recommend the use of Ansible Vault to protect Wazuh, agentless and authd credentials.

wazuh_api_user:

Wazuh API credentials.

Example:

```
wazuh_api_user:
- foo:$apr1$/axqZYWQ$Xo/nz/IG3PdwV82EnfYKh/
- bar:$apr1$hXE97ag.$8m0koHByattiGKUKPUgcZ1
```

⚠ Warning

We recommend the use of Ansible Vault to protect Wazuh, agentless and authd credentials.

authd_pass:

Wazuh authd service password.

Example:

```
authd_pass: foobar
```

Wazuh Agent

wazuh_manager_ip:

Set Wazuh Manager server IP address to be used by the agent.

Default null

wazuh_profile:

Configure what profiles this agent will have.

Default null

Multiple profiles can be included, separated by a comma and a space, by example:

```
wazuh_profile: "centos7, centos7-web"
```

wazuh_agent_authd:

Set the agent-authd facility. This will enable or not the automatic agent registration, you could set various options in accordance of the authd service configured in the Wazuh Manager.

```
wazuh_agent_authd:
  enable: false
  port: 1515
  ssl_agent_ca: null
  ssl_agent_cert: null
  ssl_agent_key: null
  ssl_auto_negotiate: 'no'
```

wazuh_notify_time

Set the <notify_time> option in the agent.

Default null

wazuh_time_reconnect

Set <time-reconnect> option in the agent.

Default null

wazuh_winagent_config

Set the Wazuh Agent installation regarding Windows hosts.

```
install_dir: 'C:\wazuh-agent\'
version: '2.1.1'
revision: '2'
repo: https://packages.wazuh.com/windows/
md5: fd9a3ce30cd6f9f553a1bc71e74a6c9f
```

wazuh_agent_config:

Wazuh Agent related configuration.

Example:

```
log_format: 'plain'
syscheck:
  frequency: 43200
  scan_on_start: 'yes'
  auto_ignore: 'no'
  alert_new_files: 'yes'
  ignore:
    - /etc/mtab
    - /etc/mnttab
    - /etc/hosts.deny
    - /etc/mail/statistics
    - /etc/random-seed
    - /etc/random.seed
    - /etc/adjtime
    - /etc/httpd/logs
    - /etc/utmpx
    - /etc/wtmpx
    - /etc/cups/certs
    - /etc/dumpdates
    - /etc/svc/volatile
  no_diff:
    - /etc/ssl/private.key
  directories:
    - dirs: /etc,/usr/bin,/usr/sbin
      checks: 'check_all="yes"'
    - dirs: /bin,/sbin
      checks: 'check_all="yes"'
  windows_registry:
    - key: 'HKEY_LOCAL_MACHINE\Software\Classes\batfile'
      arch: 'both'
    - key: 'HKEY_LOCAL_MACHINE\Software\Classes\Folder'
rootcheck:
  frequency: 43200
openscap:
  disable: 'yes'
  timeout: 1800
  interval: '1d'
  scan_on_start: 'yes'
localfiles:
  - format: 'syslog'
    location: '/var/log/messages'
  - format: 'syslog'
    location: '/var/log/secure'
  - format: 'command'
    command: 'df -P'
    frequency: '360'
  - format: 'full_command'
    command: 'netstat -tln | grep -v 127.0.0.1 | sort'
    frequency: '360'
  - format: 'full_command'
    command: 'last -n 20'
    frequency: '360'
```

⚠ Warning

We recommend the use of Ansible Vault to protect authd credentials.

authd_pass:

Wazuh authd credentials for agent registration.

Example:

```
authd_pass: foobar
```