Wazuh Agent

Info

- `agent-auth` is a wrapper for `ossec-authd`
- Config File: `/var/ossec/etc/ossec.conf`.
- Registering Agents

Setup

Linux

- Install Docs

Before `wazuh-agent` can be started, it needs to register as an agent with the API. It registers over SSL with a symmetric key. If it's not registered, you'll get this error on startup:

```
ossec-agentd: CRITICAL: (1751): File client.keys not found or empty.
```

To set this password, enter it through the CLI:

```
/var/ossec/bin/agent-auth -d -m chip-wz.adatechnologists.com -P PUT_PASSWORD_HERE
```

It will write the password to a file locally. Then start the agent.

Windows

- https://documentation.wazuh.com/current/installation-guide/installing-wazuh-agent/wazuh_agent_windows.html

Install

Registering with the GUI won't work because the protocol for registration is hardcoded to `UDP` .

```
PATH_TO_MSI_INSTALLER /q ADDRESS="chip-wz.adatechnologists.com" AUTHD_SERVER="chip-
```

Uninstall

```
msiexec.exe /x PATH_TO_MSI_INSTALLER /qn
```

Useful Commands

Tail logs

```
/var/ossec/logs/ossec.(log|json)
```

Get Agent Version

```
/var/ossec/bin/agent-auth -V
```

Run Configuration Test

```
/var/ossec/bin/ossec-agentd -t
```

REST API

Remove Agent

- https://documentation.wazuh.com/current/user-manual/agents/restful-api/remove.html

```
curl -k -u chipper:PASSWORD_HERE -X DELETE "https://chip-wz.adatechnologists.com:55

{"error":0,"data":{"msg":"All selected agents were removed","affected_agents":["004
```