How it works

The Security Content Automation Protocol (SCAP) is a specification for expressing and manipulating security data in standardized ways. SCAP jointly uses several specifications in order to automate continuous monitoring, vulnerability management, and reporting on results of security compliance scans.

Components of the security compliance evaluation process:

- **SCAP scanner**: This is an application that reads a SCAP policy and checks whether or not the system is compliant with it. There are many tools to scan your systems against SCAP policies. This wodle is an integration with the NIST-certified scanner called **OpenSCAP**.
- **Security policies (SCAP content)**: These determine how a system must be set up and what to check for. These policies contain machine-readable descriptions of the rules which your system will be required to follow.
- **Profiles**: Each security policy can contain multiple profiles, which provide sets of rules and values in line with a specific security baseline. You can think of a profile as a particular subset of rules within the policy; the profile determines which rules defined in the policy will be actually used and what values will be used during the evaluation.
- **Evaluation (scan)**: This is the process performed by the OpenSCAP scanner on an agent according to a specific security policy and profile. It usually takes only a few minutes, depending on the number of rules selected in the profile.

Requirements

This wodle is executed on the agent, so each agent must meet the following requirements:

OpenSCAP In order to perform SCAP evaluations, we need the scanner. As we mentioned above, we use OpenSCAP. You can install it with this command:

a. For RPM-based distributions:

```
sudo yum install openscap-scanner
```

b. For Debian-based distributions:

```
sudo apt-get install libopenscap8 xsltproc
```

Python 2.6+ Python is a core part of this wodle. Currently all Linux distributions come with python, so it should not be an inconvenience.

Default policies

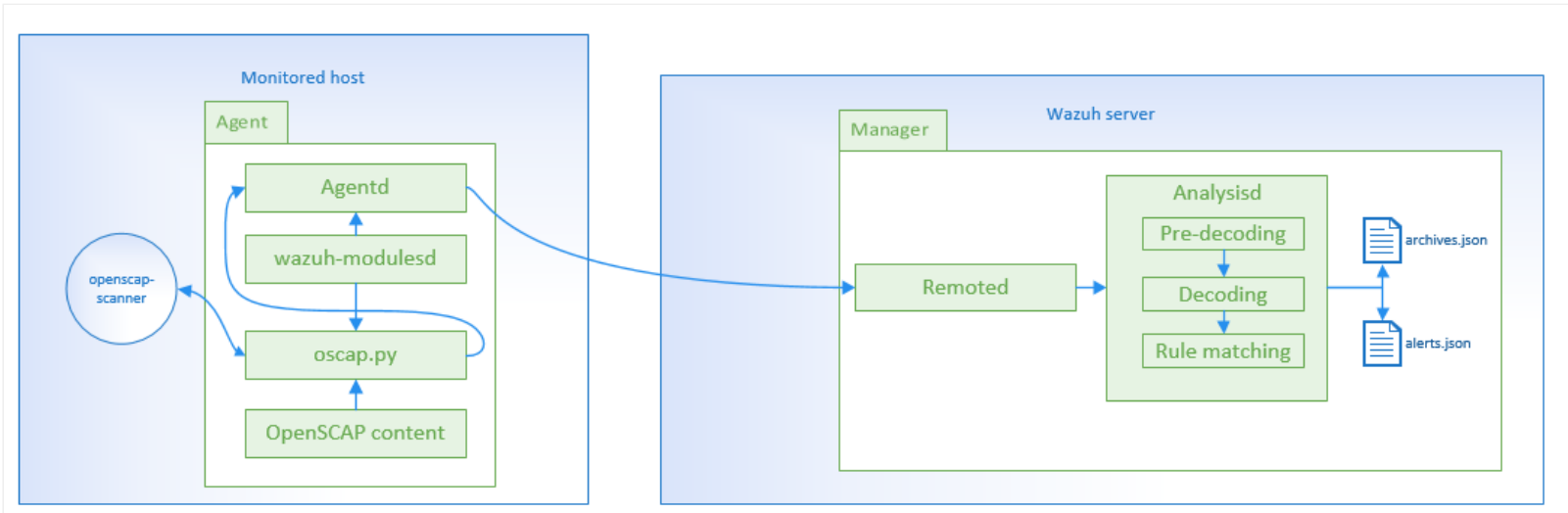
These are the Security Policy includes by default on Wazuh:

SO	Version	File name	Main profiles	Vulnerability assessment
CentOS	6	ssg-centos-6-ds.xml	Server, PCI	N/A
	7	ssg-centos-7-ds.xml	Common, PCI	N/A
RedHat	6	ssg-rhel-6-ds.xml	Server, PCI	N/A
		cve-redhat-6-ds.xml	N/A	Y
	7	ssg-rhel-7-ds.xml	Common , PCI	N/A
		cve-redhat-7-ds.xml	N/A	Y
Debian	8	ssg-debian-8-ds.xml	Common	N/A
Ubuntu	xenial	ssg-ubuntu-1604-ds.xml	Common	N/A
	trusty	cve-debian-oval.xml	N/A	Y

SO	Version	File name	Main profiles	Vulnerability assessment
	precise	cve-debian-oval.xml	N/A	Y
Fedora	24	ssg-fedora-ds.xml	Common	N/A

Each agent must have its policies in `/var/ossec/wodles/oscap/content`.

Wodle flow



The agent will run *openscap-scanner* periodically according to the configuration. Each result of the scan will be sent to the Manager and it will generate an alert if the status of the result is fail. It is possible to tuning the rules to send the pass result too.

```
{
  "timestamp": "2017-03-20T15:59:43-0700",
  "rule": {
    "level": 7,
    "description": "OpenSCAP: Set Lockout Time For Failed Password Attempts (not passed)",
    "id": "81530",
    "firedtimes": 5,
    "groups": [
      "oscap",
      "oscap-result"
    ],
    "pci_dss": [
      "2.2"
    ]
  },
  "agent": {
    "id": "1040",
    "name": "ip-10-0-0-76",
    "ip": "10.0.0.76"
  },
  "manager": {
    "name": "vpc-ossec-manager"
  },
    "full_log": "oscap: msg: \"xccdf-result\", scan-id: \"10401490050781\", content: \"ssg-centos-7-
ds.xml\", title: \"Set Lockout Time For Failed Password Attempts\", id:
\"xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_unlock_time\", result: \"fail\",
severity: \"medium\", description: \"To configure the system to lock out accounts after a number of
incorrect login attempts and require an administrator to unlock the account using pam_faillock.so, modify
the content of both /etc/pam.d/system-auth and /etc/pam.d/password-auth as follows: add the following line
immediately before the pam_unix.so statement in the AUTH section: auth required pam_faillock.so preauth
silent deny= unlock_time= fail_interval= add the following line immediately after the pam_unix.so statement
in the AUTH section: auth [default=die] pam_faillock.so authfail deny= unlock_time= fail_interval= add the
following line immediately before the pam_unix.so statement in the ACCOUNT section: account required
pam_faillock.so\", rationale: \"Locking out user accounts after a number of incorrect attempts prevents
direct password guessing attacks. Ensuring that an administrator is involved in unlocking locked accounts
draws appropriate attention to such situations.\" references: \"AC-7(b)
(http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf), 47
(http://iase.disa.mil/stigs/cci/Pages/index.aspx)\", identifiers: \"CCE-26884-7 (http://cce.mitre.org)\",
oval-id: \"oval:ssg:def:166\", benchmark-id: \"xccdf_org.ssgproject.content_benchmark_RHEL-7\", profile-id:
\"xccdf_org.ssgproject.content_profile_pci-dss\", profile-title: \"PCI-DSS v3 Control Baseline for CentOS
Linux 7\".",
    "oscap": {
      "scan": {
        "id": "10401490050781",
        "content": "ssg-centos-7-ds.xml",
        "benchmark": {
          "id": "xccdf_org.ssgproject.content_benchmark_RHEL-7"
        },
        "profile": {
          "id": "xccdf_org.ssgproject.content_profile_pci-dss",
          "title": "PCI-DSS v3 Control Baseline for CentOS Linux 7"
        }
      },
      "check": {
        "title": "Set Lockout Time For Failed Password Attempts",
        "id": "xccdf_org.ssgproject.content_rule_accounts_passwords_pam_faillock_unlock_time",
        "result": "fail",
        "severity": "medium",
        "description": "To configure the system to lock out accounts after a number of incorrect login
attempts and require an administrator to unlock the account using pam_faillock.so, modify the content of
both /etc/pam.d/system-auth and /etc/pam.d/password-auth as follows: add the following line immediately
before the pam_unix.so statement in the AUTH section: auth required pam_faillock.so preauth silent deny=
unlock_time= fail_interval= add the following line immediately after the pam_unix.so statement in the AUTH
section: auth [default=die] pam_faillock.so authfail deny= unlock_time= fail_interval= add the following
line immediately before the pam_unix.so statement in the ACCOUNT section: account required
pam_faillock.so",
        "rationale": "Locking out user accounts after a number of incorrect attempts prevents direct
password guessing attacks. Ensuring that an administrator is involved in unlocking locked accounts draws
```

```
appropriate attention to such situations.",
        "references": "AC-7(b) (http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf),
47 (http://iase.disa.mil/stigs/cci/Pages/index.aspx)",
        "identifiers": "CCE-26884-7 (http://cce.mitre.org)",
        "oval": {
          "id": "oval:ssg:def:166"
        }
      }
    },
    "decoder": {
      "parent": "oscap",
      "name": "oscap"
    },
    "location": "wodle_open-scap"
}
```


When the scan finishes, a report event is sent which generates an alert:


```
{
    "timestamp": "2017-03-20T15:59:43-0700",
    "rule": {
      "level": 5,
      "description": "OpenSCAP Report overview: Score less than 80",
      "id": "81542",
      "firedtimes": 2,
      "groups": [
        "oscap",
        "oscap-report"
      ],
      "pci_dss": [
        "2.2"
      ]
    },
    "agent": {
      "id": "1040",
      "name": "ip-10-0-0-76",
      "ip": "10.0.0.76"
    },
    "manager": {
      "name": "vpc-ossec-manager"
    },
    "full_log": "oscap: msg: \"xccdf-overview\", scan-id: \"10401490050797\", content: \"ssg-centos-7-
ds.xml\", benchmark-id: \"xccdf_org.ssgproject.content_benchmark_RHEL-7\", profile-id:
\"xccdf_org.ssgproject.content_profile_common\", profile-title: \"Common Profile for General-Purpose
Systems\", score: \"75.000000\".",
    "oscap": {
      "scan": {
        "id": "10401490050797",
        "content": "ssg-centos-7-ds.xml",
        "benchmark": {
          "id": "xccdf_org.ssgproject.content_benchmark_RHEL-7"
        },
        "profile": {
          "id": "xccdf_org.ssgproject.content_profile_common",
          "title": "Common Profile for General-Purpose Systems"
        },
        "score": "75.000000"
      }
    },
    "decoder": {
      "parent": "oscap",
      "name": "oscap"
    },
    "location": "wodle_open-scap"
}
```