FAQ

Is there a noticeable performance impact when the OpenSCAP wodle is enabled on an agent?

The OpenSCAP wodle is designed to be very efficient, but the performance will depend on how fast oscap is (the scanner). Depending on the chosen policy, oscap can consume significant resources. We recommend you test your policies on a test agent before deploying them to production systems.

Are evaluations executed in parallel?

No, each evaluation is executed sequentially. Also, each profile of an evaluation is executed sequentially. This makes scans take somewhat longer but also reduces the load on agents caused by those scans.

How does the interval work?

The interval is the intended amount of time between the commencements of subsequent OpenSCAP scans on an agent. If a scan takes longer than the configured interval, an "interval overtaken" log message will be written to `/var/ossec/log/ossec.log`, and when the scan is finished, it will start again immediately.

Are the policies evaluated when OSSEC starts?

Yes, by default, policies are evaluated when the wodle starts. You can change this by setting <scan-on-start> to 'no'. In this case, the next evaluation will be executed after the interval specified. The wodle state is saved when OSSEC is stopped.

Where are the policies?

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