

Autodiscovery

SAYMON allows you to describe the infrastructure of any complexity in terms of objects and links between them. This infrastructure is then filled with information received from monitoring agents, widgets with current metrics and graphs, painted in the colors of the states.

However, creating an infrastructure map manually is often too tiring, because it can contain thousands of objects. To solve this problem, SAYMON provides mechanisms for auto-detection of objects. With their help, you can add most of the objects of interest to the user on the infrastructure map automatically, without time-consuming manual “clicking” in the Web interface.

In SAYMON there are two types of auto-detection of objects. The first type is built-in mechanisms that work without any effort from the user. These include, for example, the network autodiscovery mechanism, which displays in the diagram all the hosts available on the local network.

The second type is the methods in the [REST API](#) that can be used by client automation scripts to create objects in SAYMON. Using such scripts, you can implement any autodetection algorithm for any kind of infrastructure objects.

We'll take a look at both autodetection mechanisms here.

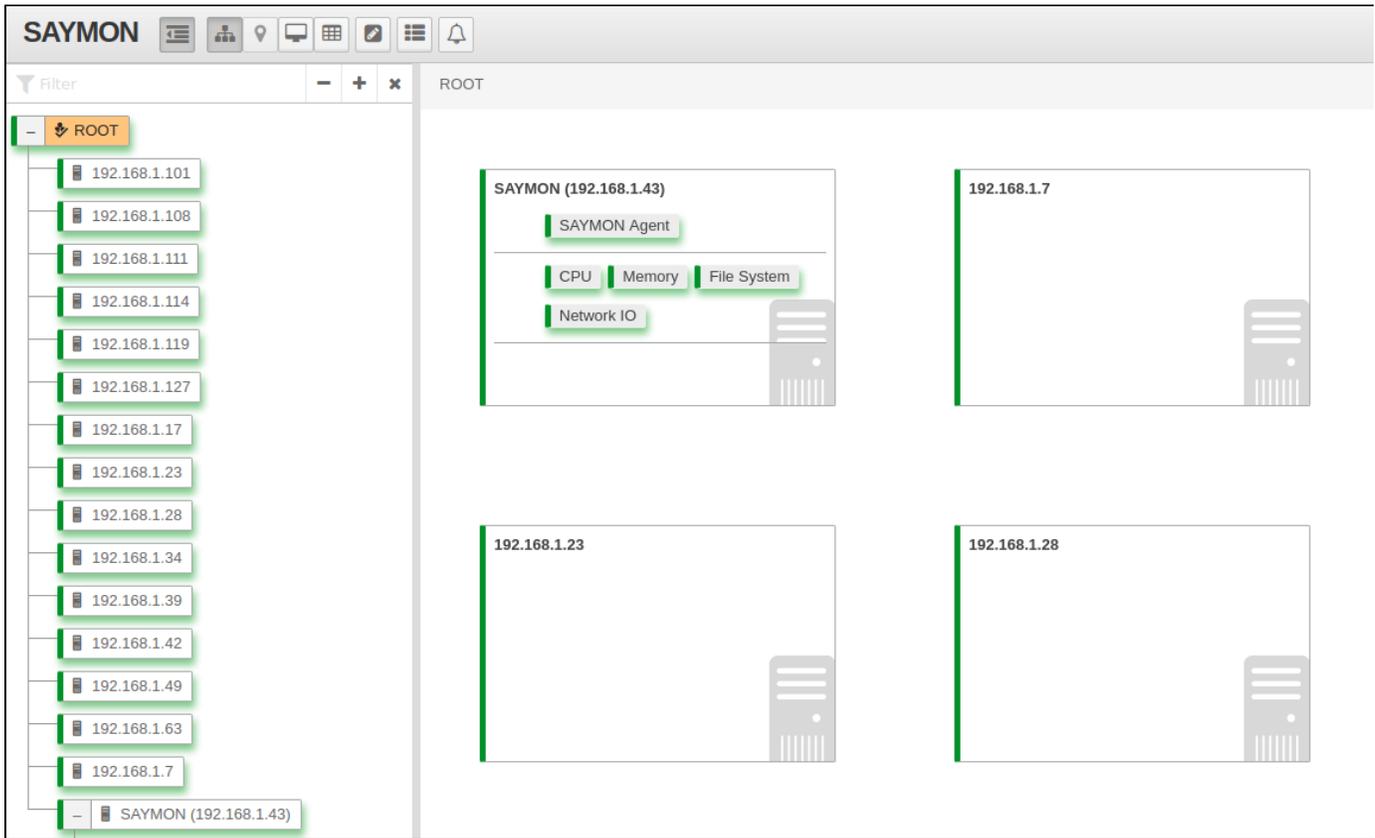
Built-in autodiscovery

The built-in autodiscovery mechanisms are implemented inside SAYMON and work automatically when the system is started (unless they are disabled by the system administrator).

SAYMON's built-in autodiscovery mechanisms include network autodiscovery. Also in the development process are the autodiscovery mechanisms of system services and the autodiscovery mechanism via SNMP.

Network Autodiscovery

The network autodiscovery mechanism works as follows. The agent scans the local subnet and sends to the server information on all IP addresses available for a TCP connection or available via PING. Host objects with corresponding addresses are created in SAYMON and displayed on the infrastructure map. For them, monitoring is also automatically enabled using a [Ping sensor](#).



In the agent, network autodiscovery is enabled and disabled using the `agent.discoveryEnabled` option (enabled by default). To disable network autodiscovery on an agent, you must set this option to **false**:

```
agent.discoveryEnabled=false
```

Autodiscovery via API

It is impossible to foresee all autodiscovery options for the whole variety of existing infrastructures. However, in SAYMON there is an open [REST API](#), using which the client can implement any suitable mechanism of objects autodiscovery using an automatic script (script). SAYMON's [REST API](#) works over HTTP, so the script can be implemented in any language or platform where there is an HTTP client.

The simplest example is a bash script with sending REST requests to SAYMON via curl.

Adding objects via REST

Suppose you have a script that can detect a certain type of objects in the infrastructure (these can be network devices or software services). You can add detected objects to SAYMON using the **POST / node / api / objects** REST method. Below is an example of how this can be done in a bash script.

```
# Code to detect the object...
# ...

# Object detected, create it in SAYMON.
curl -v -u admin:saymon -H "Content-Type: application/json" -X POST \
  --data '{"name": "Detected object", "discovery_id": "Object_id"}' \
  http://saymon/node/api/objects
```

An important parameter when detecting an object is **discovery_id**. This is a string that uniquely identifies an object in the infrastructure and avoids its re-creation in SAYMON. If at the time of creating an object in SAYMON an object already exists with the specified **discovery_id**, it is simply modified with new data, and a new object is not created. This allows you to run an autodiscovery script multiple times (for example, on a schedule) and be sure that objects already detected will not be created again in SAYMON.

In the case of network devices, the device's IP address or MAC address can be the `discovery_id`.