

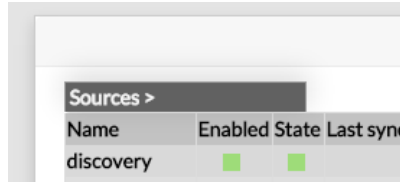


Shinken Enterprise allows you to detect network checks and physical type of your servers located in your IT.

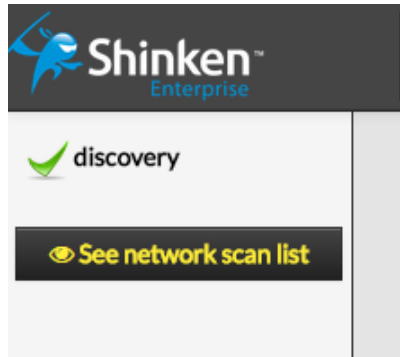
## Edit and add new network scan list

The network scan can be setup directly in the [Administration Interface](#).

First click on the discovery source in the home page.

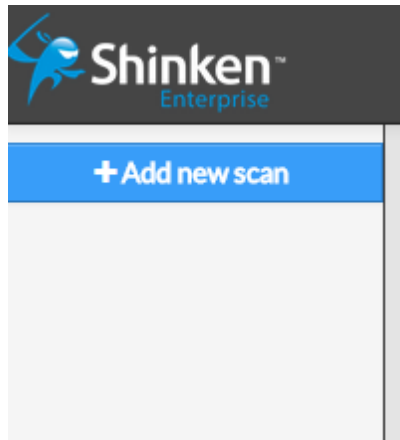


Then click on the "See network scan list" button:



You can list the current network scan in the **Discovery** menu.

You can enable new scan with the **Add new scan** button.



And you will see the configuration of a new scan:

Generic

Name

IP Range

Scan Interval (min) 60

Notes

Enabled  On  Off

You must set up the following parameters:

- Name
- IP range: must match a *nmap* command range definition

 for example: 172.16.1.1-254

- Scan interval, in minutes
- You can setup notes about this scan

Adding a new scan will automatically enable it and your new hosts or your new tags will appear in a few minutes.

## Add new port to host template rule

Without rules, the raw data that is being generated by the discovery scripts is useless. The rules are defined in the `/etc/shinken/discovery_rules.cfg` file.

Here is an example of how to set the ftp host template for anything that is detected by nmap with the TCP/21 port open:

There are three main parts for a rule:

- **discoveryrule\_name**: should be unique
- **creation\_type**: should be host
- **openports**: regexp about the port that will be match. The `^` and `$` is for the regexp thing, so `21` and only `21` will be match, and not `210` for example.
- **+use**: This mentions the template from which the generated object will inherit from. You can add as many properties as you want.

```
define discoveryrule {
    discoveryrule_name    FtpRule
    creation_type          host
    openports              ^21$
    +use                   ftp
}
```

**Here is the list of the default port to Host templates rules:**

Port	Host template
27017	<i>mongodb</i>
53	<i>dns</i>
25	<i>smtp</i>
465	<i>smtps</i>
3306	<i>mysql</i>
22	<i>ssh</i>
110	<i>pop3</i>
995	<i>pop3s</i>
9100	<i>printer-hp</i>
1521	<i>oracle</i>
80	<i>http</i>
443	<i>https</i>
1433	<i>mssql</i>
2301	<i>hp-asm</i>
143	<i>imap</i>
993	<i>imaps</i>
389	<i>ldap</i>
636	<i>ldaps</i>

**Security:  
nmap  
command  
parameters**

Here are the the parameters used by the nmap command used by this module:

- -sU
- -sT
- --min-rate 1000
- --max-retries 3
- -T4
- -O