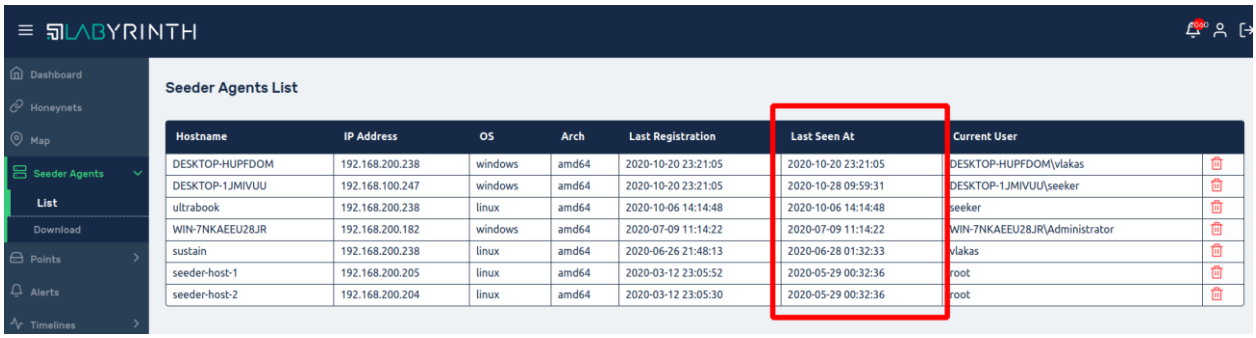
LABYRINTH DECEPTION PLATFORM Release Notes v. 1.2.0

Feature list

Last Seen Seeder Agent (Display the date of the last communication with Seeder)

Added the Last Seen At field to the list of Seeder agents, which shows the last time the agent contacted the server.



Alerts search result format
The format of the returned alert search results has been changed at the server API level.

Seeder Tasks refactoring

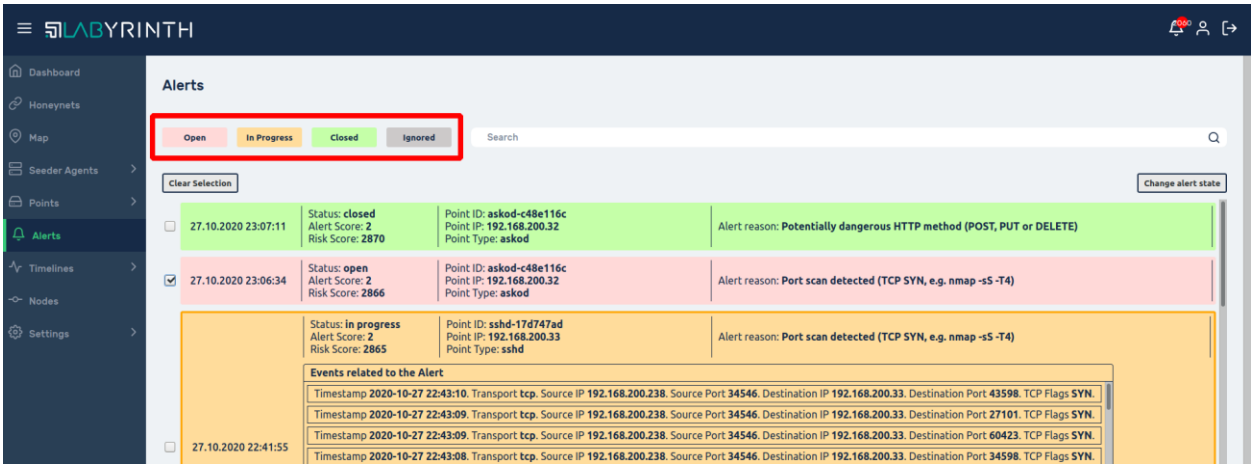
Additional checks have been added to the work of Seeder agents and Seeder API:

- Verification of all generated files before and after sending via Seeder
- Checking the availability of a set of files for a specific Seeder by its ID

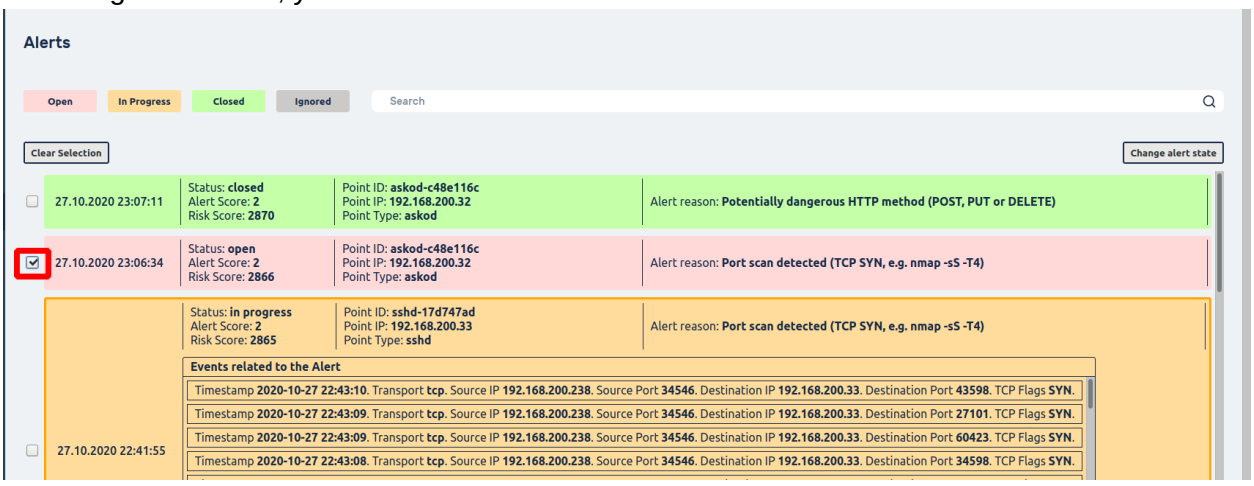
Close alerts functionality

Starting from this release, alerts status changes is performed from both an integrated IRMS system, and directly through the platform's WEB interface.

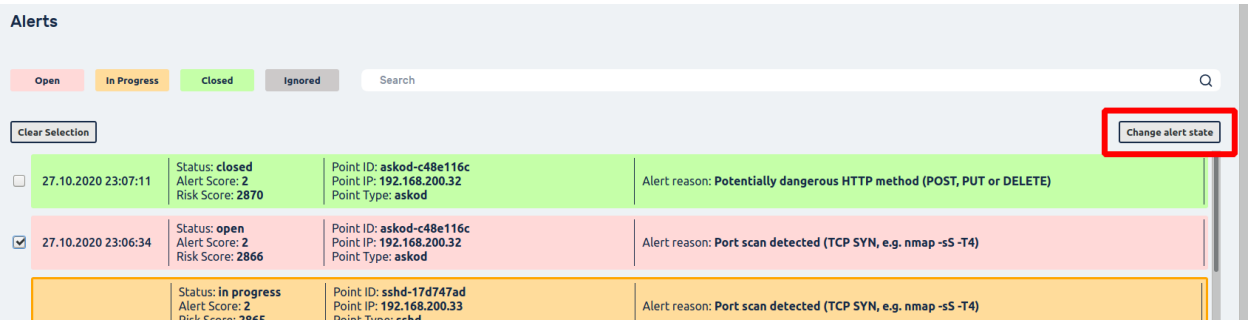
There are 4 states for Alerts:



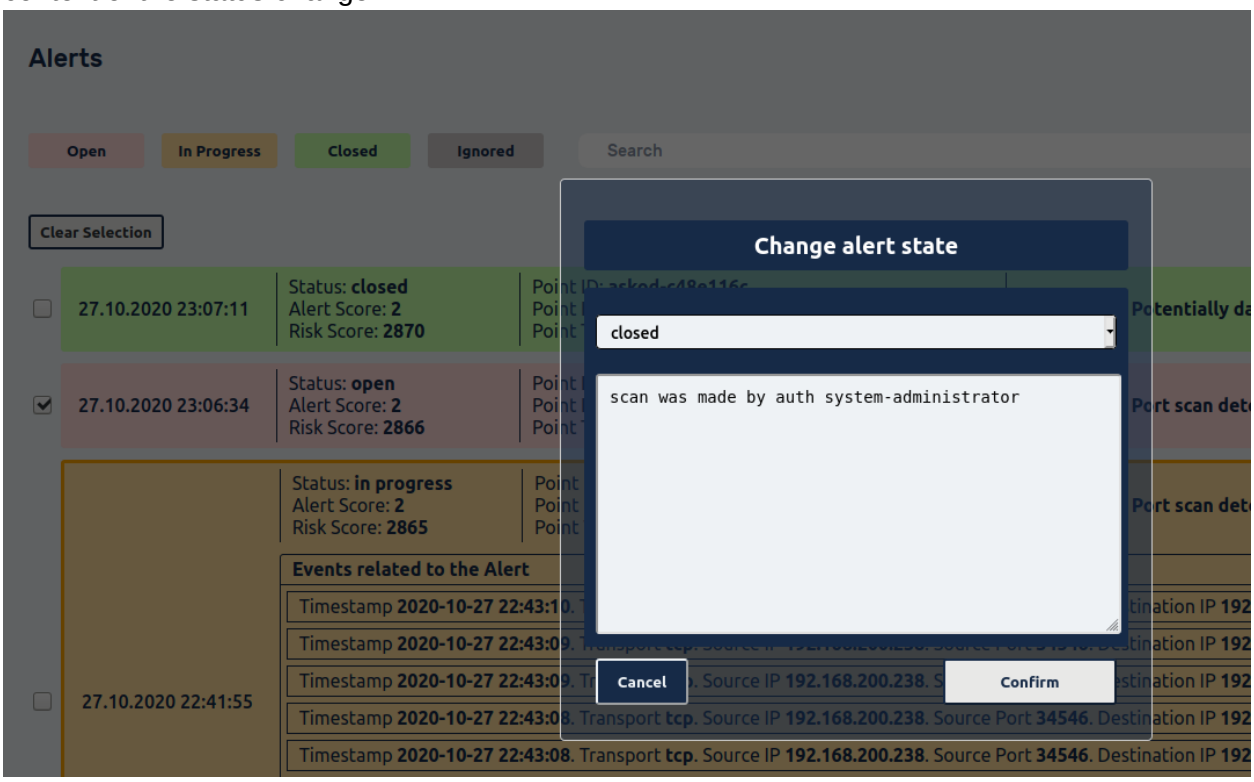
To change the status, you need to select Alert:



Then click on the button “Change alert state”:



It is necessary to indicate a new status for the Alert and give a short description for the informational context of the status change:



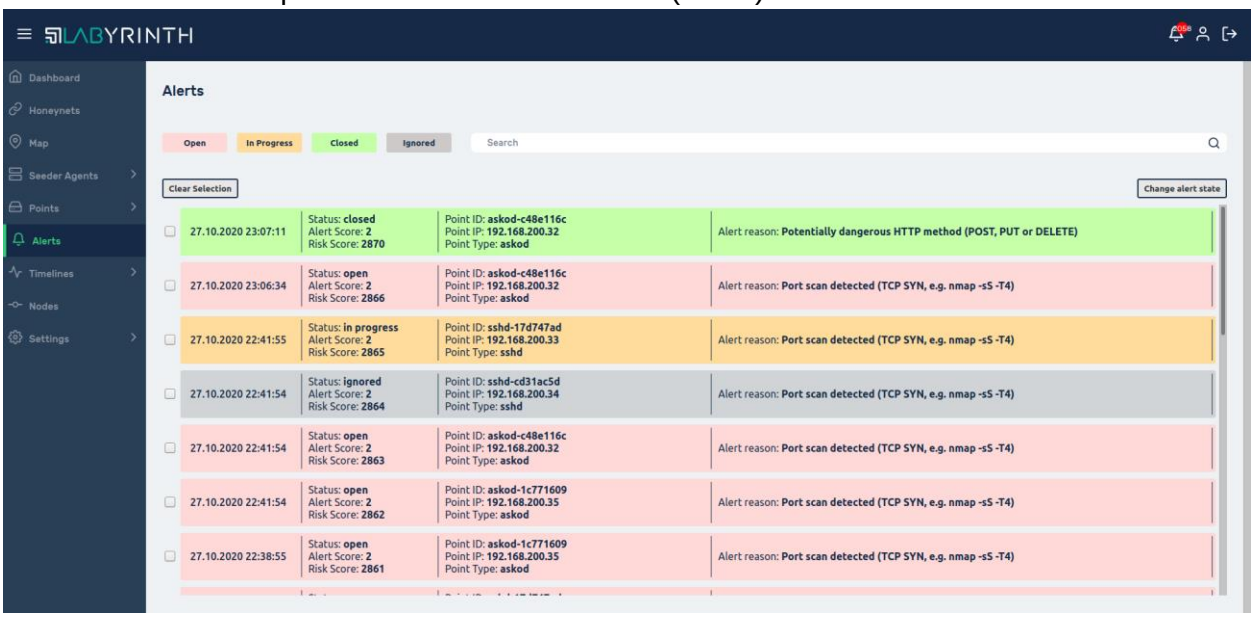
Unavailable worker location notification

Honeynet and Worker Node communicate through the Location parameter. If there is a Honeynet with Location Abc, then a Worker Node with Location Abc must be present. When you try to create a Honeynet for which there are no workers, a notification about this will be displayed during generation process.

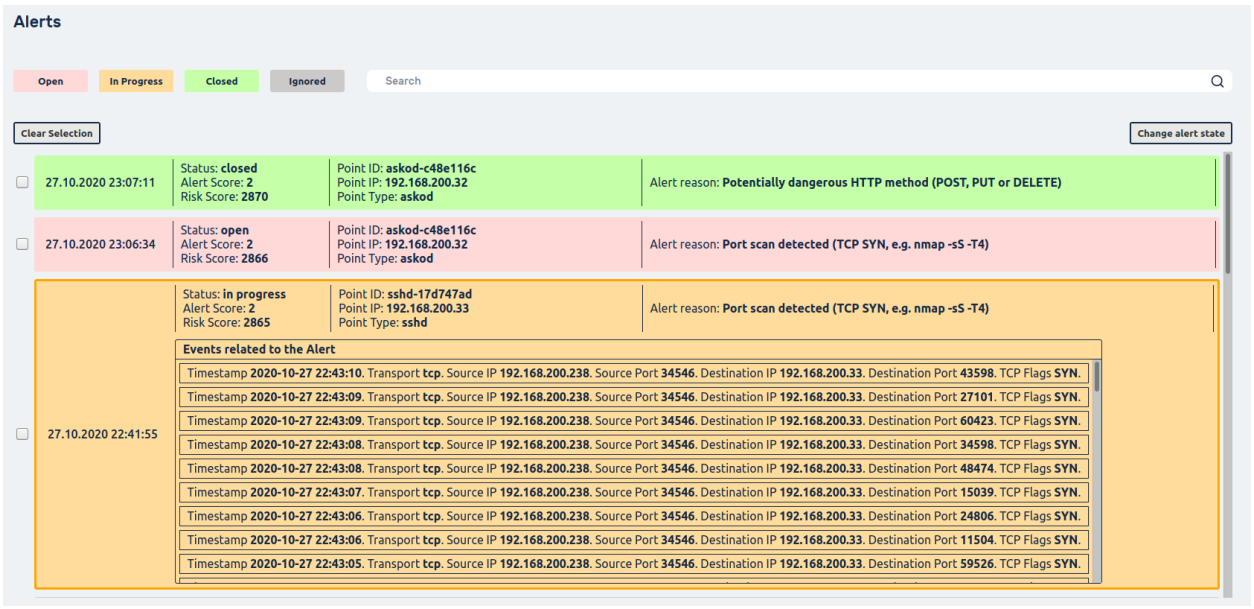
Refactoring: Alerts timeline (List)

The appearance of the Alerts list has been redesigned to increase informativeness and improve the content of detected events.

General view of the updated list of detected events (Alerts):



Displaying detailed information about an event:



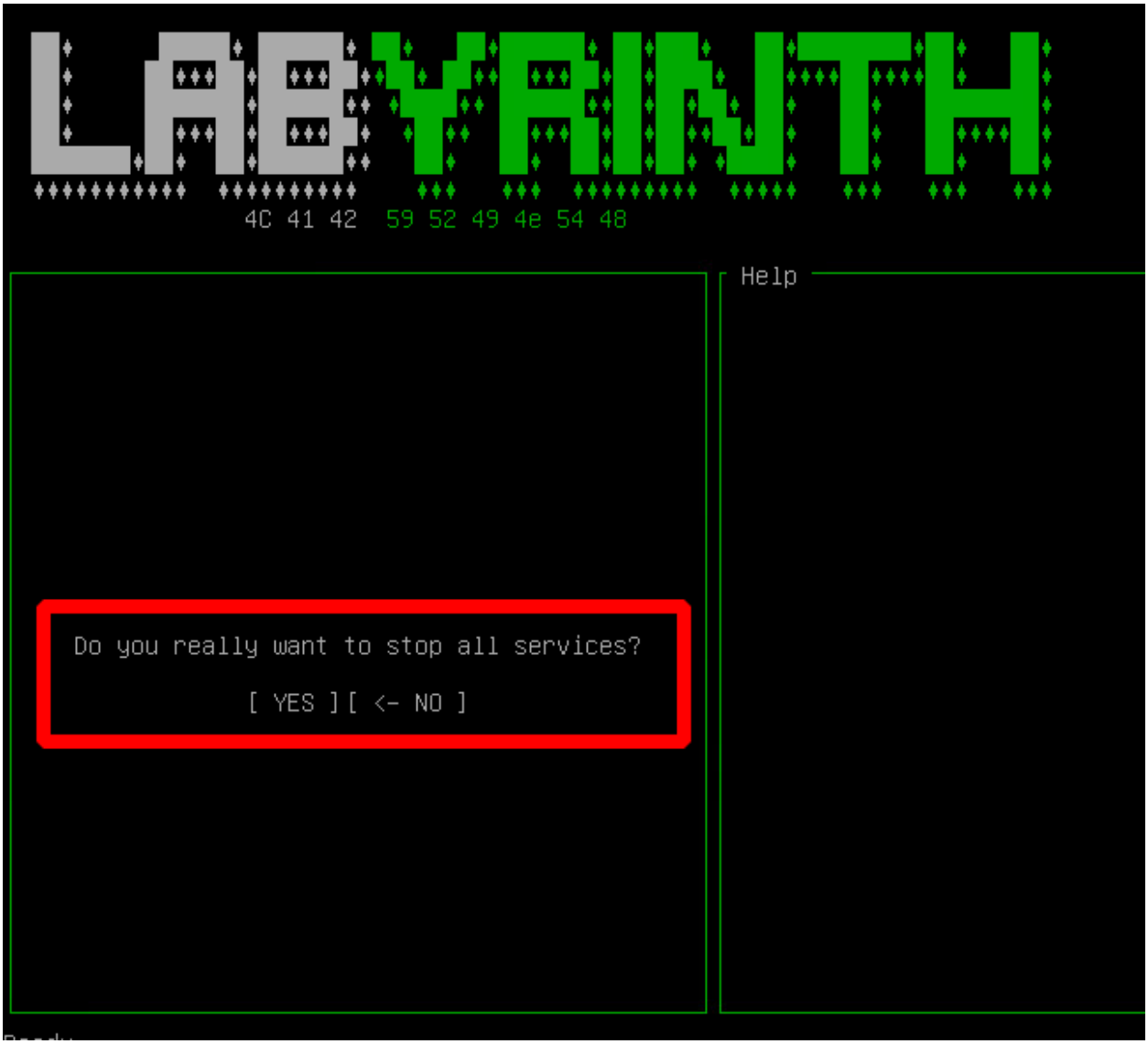
Bugfixes list

Network scan failure during generate

Removed potential errors during the initial scan of a network during the "Generate" process, that could lead to a long time for Labyrinth generation. Many of the built-in verifications relate to scanning WEB services / applications running over HTTPS and having non-standard certificates.

Point menu Start Services menu incorrect message

Fixed syntax error of the console menu in the content of notifications about stopping / starting internal services on the server:

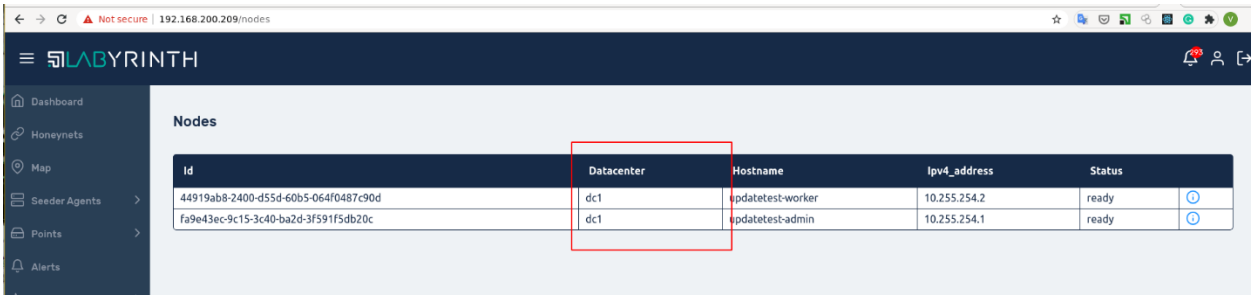


Honeynet creation on error issue

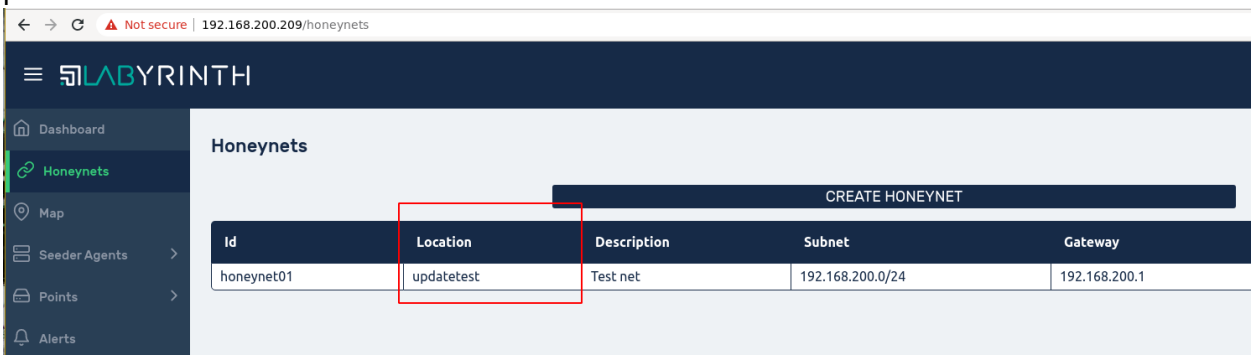
Fixed potential race-condition (logic error) when creating / deleting multiple Honeynets. Additional verifications have been added to eliminate potential side-effects.

Incorrect location in Datacenter field of Honeynet

Previously, in the interface of the list of system nodes, data about a data center of the Worker was displayed.

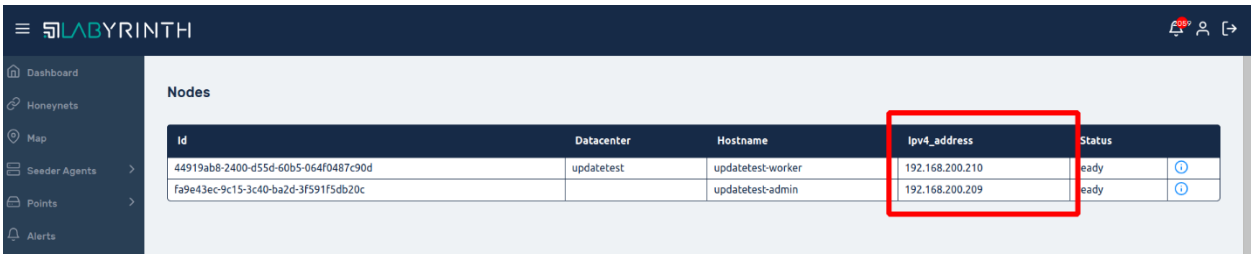


This field has been replaced by the Location field, due to its greater importance during a Honeynet creation process:



Wrong IP address in nodes list (specifying the real IP addresses of all nodes in the system)

Previously, the addresses used to form a secure connection between nodes were indicated. Now the operator is shown in the WEB interface the real IP of the hosts that make up the Labyrinth system (admin & worker).



Planned features for the next release

1. An ability to regulate the automated generate process, specifically to control the number of generated points of certain types.
2. An ability to specify a list of IP addresses, based on which points of the Universal Web type will be created.
3. A list of all created breadcrumbs with information about name, permissions, location, timestamp, owner.