

LABYRINTH DECEPTION PLATFORM Release Notes v. 1.2.0

Feature list	1
Last Seen Seeder Agent (Отображение даты последней связи с Seeder)	1
Seeder Tasks refactoring	2
Close alerts functionality	2
Unavailable worker location notification	3
Refactoring: Alerts timeline (List)	3
Bugfixes list	5
Network scan failure during generate	5
Point menu Start Services menu incorrect message	5
Honeynet creation on error issue	6
Incorrect location in Datacenter field of Honeynet	6
Wrong IP address in nodes list (указание реальных IP адресов всех нод системы)	6
Roadmap features	7

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.

Hostname	IP Address	OS	Arch	Last Registration	Last Seen At	Current User
DESKTOP-HUPFDM	192.168.200.238	windows	amd64	2020-10-20 23:21:05	2020-10-20 23:21:05	DESKTOP-HUPFDM\vlakas
DESKTOP-1JMIVUU	192.168.100.247	windows	amd64	2020-10-20 23:21:05	2020-10-28 09:59:31	DESKTOP-1JMIVUU\seeker
ultrabook	192.168.200.238	linux	amd64	2020-10-06 14:14:48	2020-10-06 14:14:48	seeker
WIN-7NKAEEU28JR	192.168.200.182	windows	amd64	2020-07-09 11:14:22	2020-07-09 11:14:22	WIN-7NKAEEU28JR\Administrator
sustain	192.168.200.238	linux	amd64	2020-06-26 21:48:13	2020-06-28 01:32:33	vlakas
seeder-host-1	192.168.200.205	linux	amd64	2020-03-12 23:05:52	2020-05-29 00:32:36	root
seeder-host-2	192.168.200.204	linux	amd64	2020-03-12 23:05:30	2020-05-29 00:32:36	root

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:

The screenshot shows the 'Alerts' section of the Labyrinth interface. At the top, there are four status filters: 'Open' (highlighted with a red box), 'In Progress', 'Closed', and 'Ignored'. Below the filters is a search bar and a 'Change alert state' button. The main area contains a table of alerts:

Timestamp	Status	Alert Score	Risk Score	Point ID	Point IP	Point Type	Alert reason
27.10.2020 23:07:11	closed	2	2870	askod-c48e116c	192.168.200.32	askod	Potentially dangerous HTTP method (POST, PUT or DELETE)
27.10.2020 23:06:34	open	2	2866	askod-c48e116c	192.168.200.32	askod	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:41:55	in progress	2	2865	sshd-17d747ad	192.168.200.33	sshd	Port scan detected (TCP SYN, e.g. nmap -sS -T4)

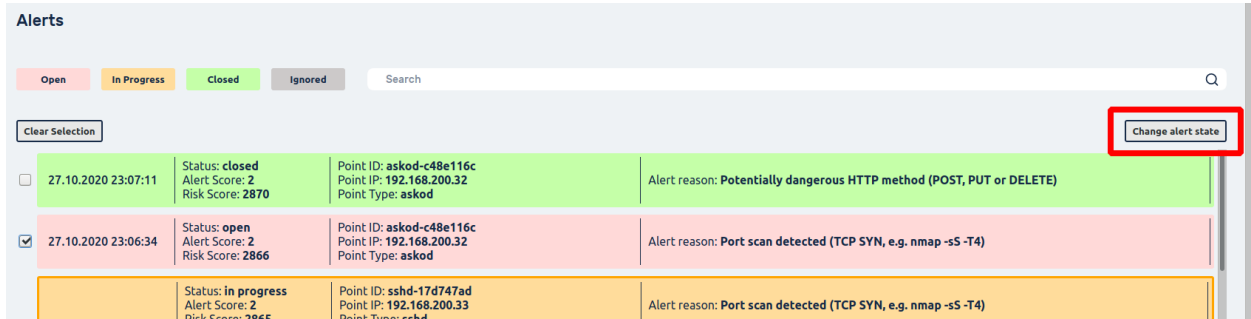
Below the 'in progress' alert, there is a section titled 'Events related to the Alert' with a scrollable list of events:

- Timestamp 2020-10-27 22:43:10. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 43598. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:09. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 27101. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:09. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 60423. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:08. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 34598. TCP Flags SYN.

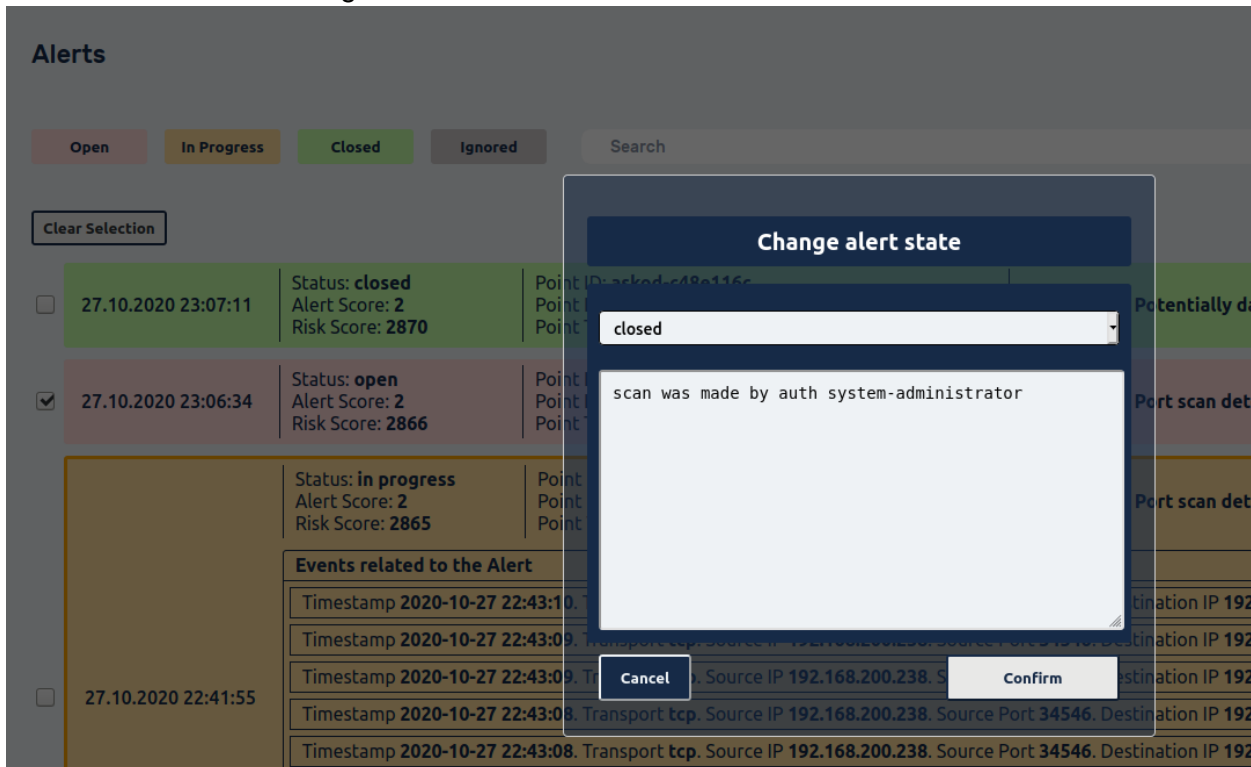
To change the status, you need to select Alert:

This screenshot is identical to the previous one, but the checkbox next to the 'open' alert (27.10.2020 23:06:34) is now checked, indicating it has been selected for a status change.

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):

Time	Status	Alert Score	Risk Score	Point ID	Point IP	Point Type	Alert reason
27.10.2020 23:07:11	closed	2	2870	askod-c48e116c	192.168.200.32	askod	Potentially dangerous HTTP method (POST, PUT or DELETE)
27.10.2020 23:06:34	open	2	2866	askod-c48e116c	192.168.200.32	askod	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:41:55	in progress	2	2865	sshd-17d747ad	192.168.200.33	sshd	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:41:54	ignored	2	2864	sshd-cd31ac5d	192.168.200.34	sshd	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:41:54	open	2	2863	askod-c48e116c	192.168.200.32	askod	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:41:54	open	2	2862	askod-1c771609	192.168.200.35	askod	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:38:55	open	2	2861	askod-1c771609	192.168.200.35	askod	Port scan detected (TCP SYN, e.g. nmap -sS -T4)

Displaying detailed information about an event:

Time	Status	Alert Score	Risk Score	Point ID	Point IP	Point Type	Alert reason
27.10.2020 23:07:11	closed	2	2870	askod-c48e116c	192.168.200.32	askod	Potentially dangerous HTTP method (POST, PUT or DELETE)
27.10.2020 23:06:34	open	2	2866	askod-c48e116c	192.168.200.32	askod	Port scan detected (TCP SYN, e.g. nmap -sS -T4)
27.10.2020 22:41:55	in progress	2	2865	sshd-17d747ad	192.168.200.33	sshd	Port scan detected (TCP SYN, e.g. nmap -sS -T4)

Events related to the Alert

- Timestamp 2020-10-27 22:43:10. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 43598. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:09. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 27101. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:09. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 60423. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:08. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 34598. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:08. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 48474. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:07. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 15039. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:06. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 24806. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:06. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 11504. TCP Flags SYN.
- Timestamp 2020-10-27 22:43:05. Transport tcp. Source IP 192.168.200.238. Source Port 34546. Destination IP 192.168.200.33. Destination Port 59526. TCP Flags SYN.

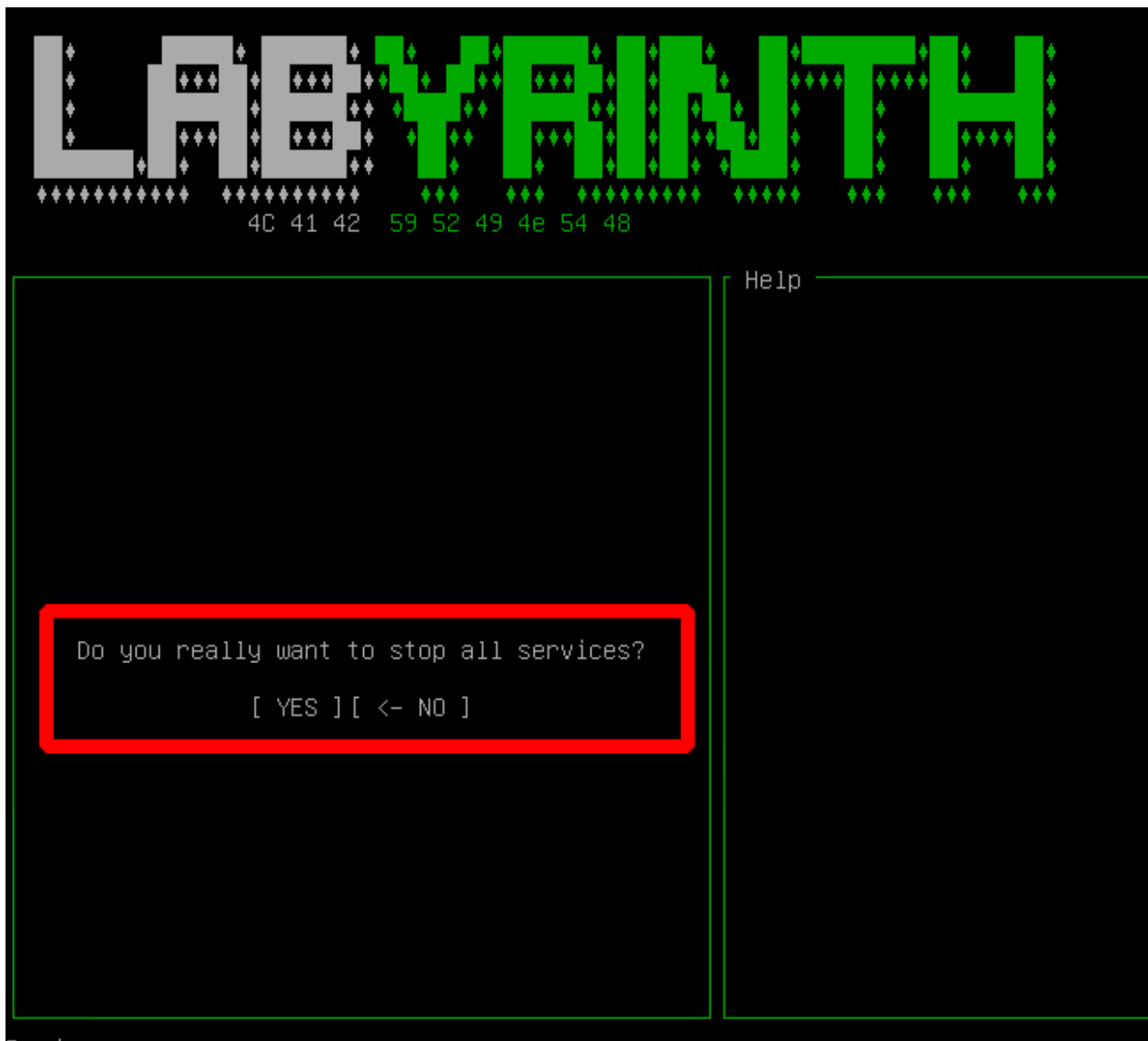
Bugfixes list

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.

id	Datacenter	Hostname	ipv4_address	Status
44919ab8-2400-d55d-60b5-064f0487c90d	dc1	updatestest-worker	10.255.254.2	ready
fa9e43ec-9c15-3c40-ba2d-3f591f5db20c	dc1	updatestest-admin	10.255.254.1	ready

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

id	Location	Description	Subnet	Gateway
honeynet01	updatestest	Test net	192.168.200.0/24	192.168.200.1

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).

id	Datacenter	Hostname	ipv4_address	Status
44919ab8-2400-d55d-60b5-064f0487c90d	updatestest	updatestest-worker	192.168.200.210	ready
fa9e43ec-9c15-3c40-ba2d-3f591f5db20c		updatestest-admin	192.168.200.209	ready

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.