DIATEAM

MILITARY & CIVIL CYBERSECURITY SOLUTIONS

ACTION MANAGER

2.6

www.diateam.net – contact@diateam.net - @DIATEAM_Labs

INTRODUCTION

- CROSS PLATFORM PRODUCT

- PRODUCT USED IN THE HYNESIM ENVIRONNEMENT

Why

- ActionManager's main objective is to remotely execute "actions" in hynesim VMs (Virtual Machines)

- Execute multiple script in several entities easily

- Retrieve VM Files to host without network connection

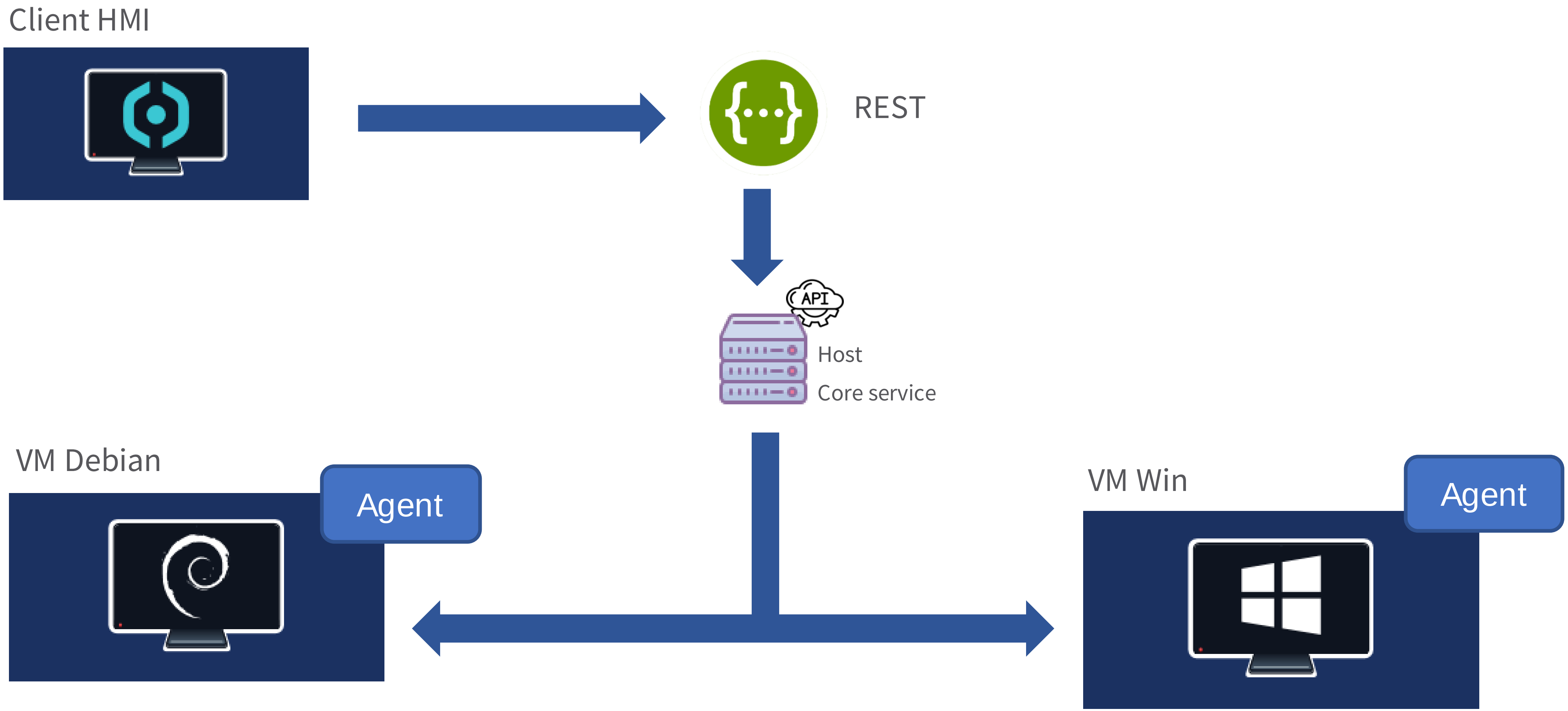
- Actions will generate logs
  - The exit status of the script will be saved
  - History of executed Actions in HMI / API

- Create a script that can be execute on all registered entities
  - One script for everybody
  - Good Maintainability

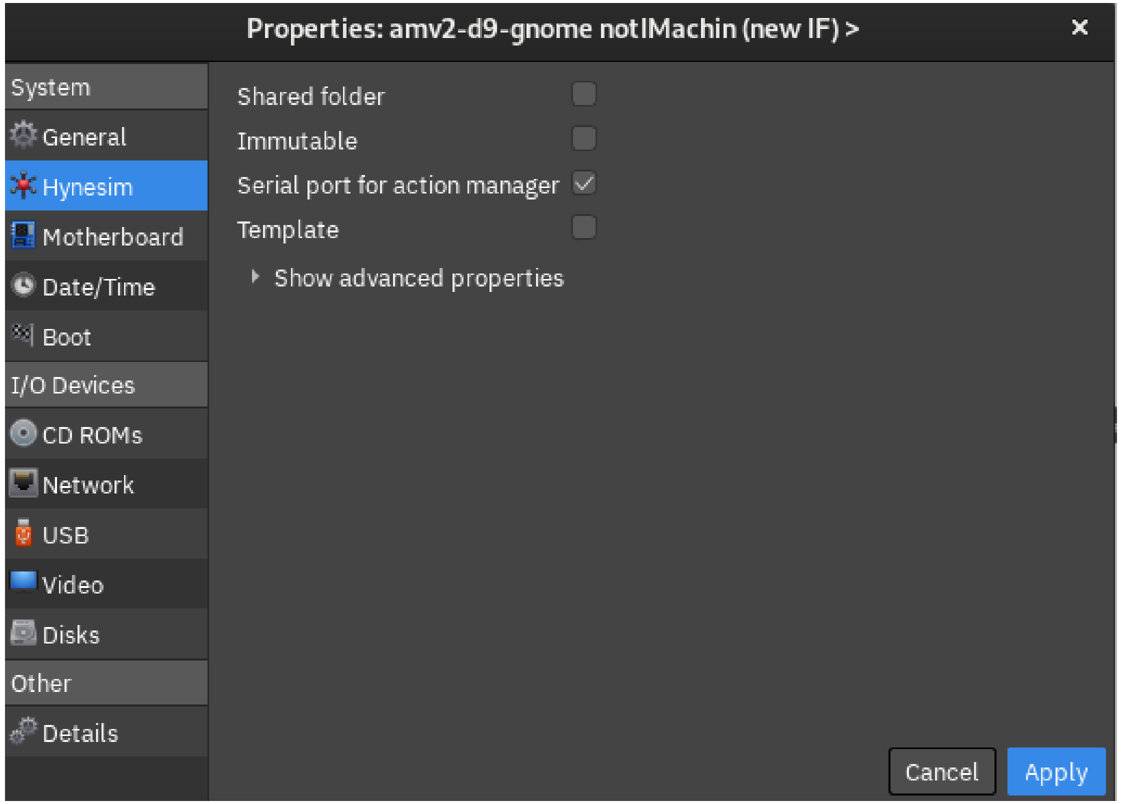
- Execute an Action at a specific date (Scheduler)

- Run an action as root or as a specific user

How it works


Client HMI
REST
API
Host
Core service
VM Debian
Agent
VM Win
Agent

Works without network connection



Properties: amv2-d9-gnome notIMachin (new IF) >

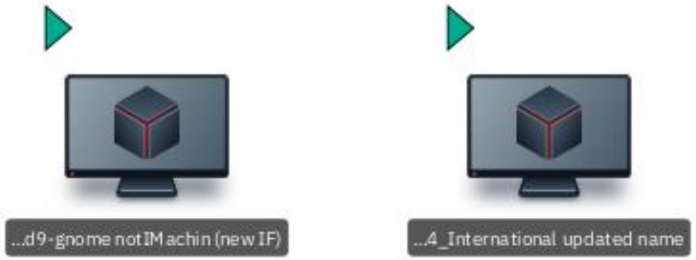
Shared folder □

Immutable □

Serial port for action manager ☑

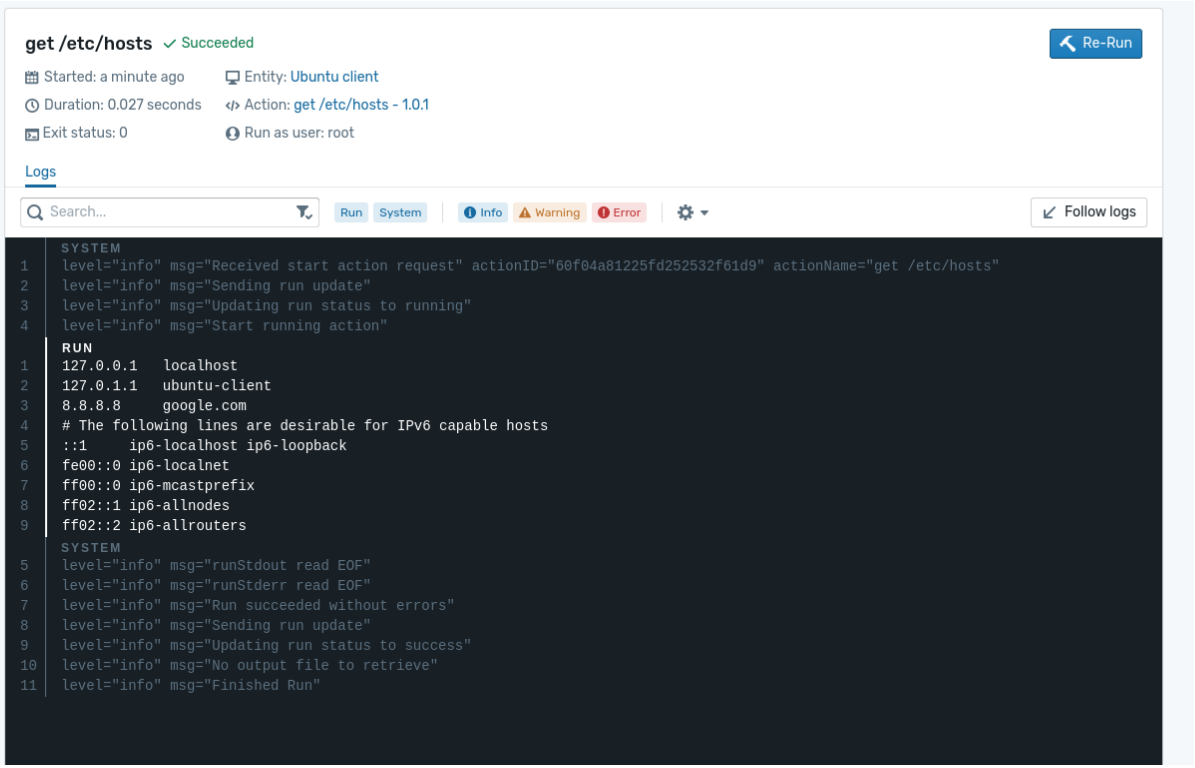
Template □

▸ Show advanced properties


...d9-gnome notIMachin (new IF)
...4_International updated name

Execute "Actions" from client to VM

Client

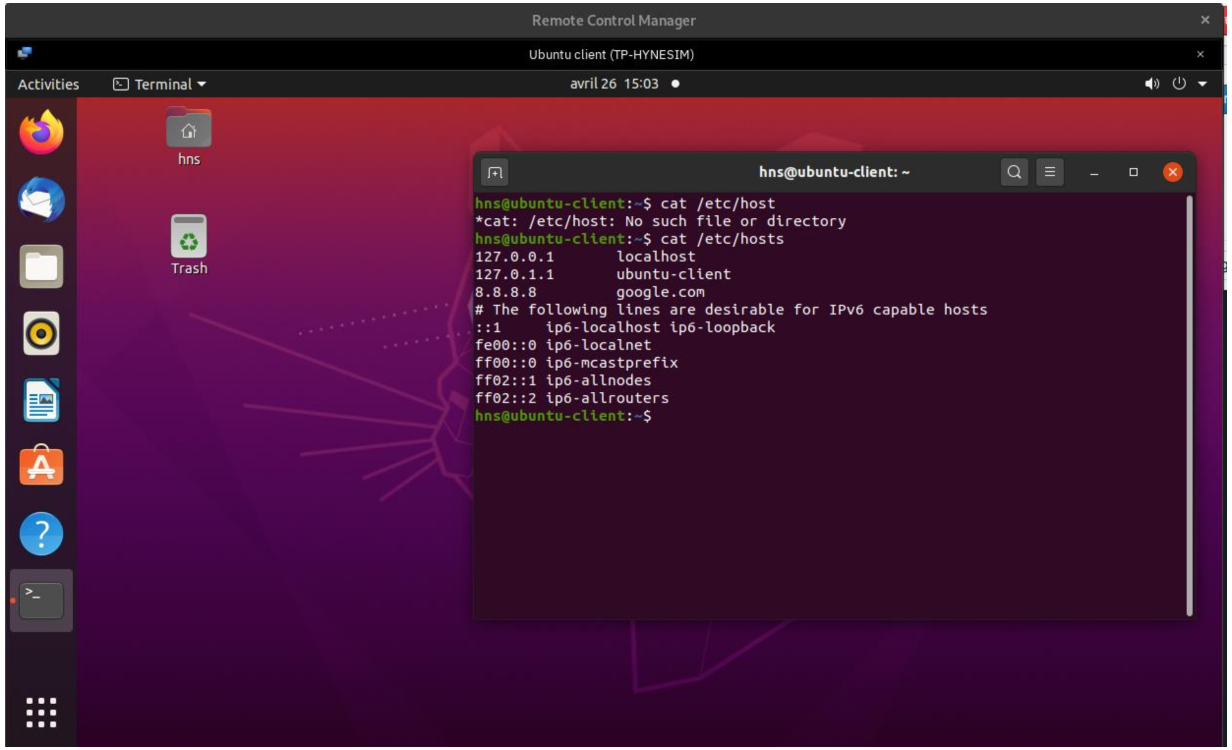


get /etc/hosts ✓ Succeeded

Started: a minute ago
Duration: 0.027 seconds
Exit status: 0
Entity: Ubuntu client
Action: get /etc/hosts - 1.0.1
Run as user: root

```
SYSTEM
level="info" msg="Received start action request" actionID="60f04a81225fd252532f61d9" actionName="get /etc/hosts"
level="info" msg="Sending run update"
level="info" msg="Updating run status to running"
level="info" msg="Start running action"
RUN
127.0.0.1   localhost
127.0.1.1   ubuntu-client
8.8.8.8     google.com
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
SYSTEM
level="info" msg="runStdout read EOF"
level="info" msg="runStderr read EOF"
level="info" msg="Run succeeded without errors"
level="info" msg="Sending run update"
level="info" msg="Updating run status to success"
level="info" msg="No output file to retrieve"
level="info" msg="Finished Run"
```

VM

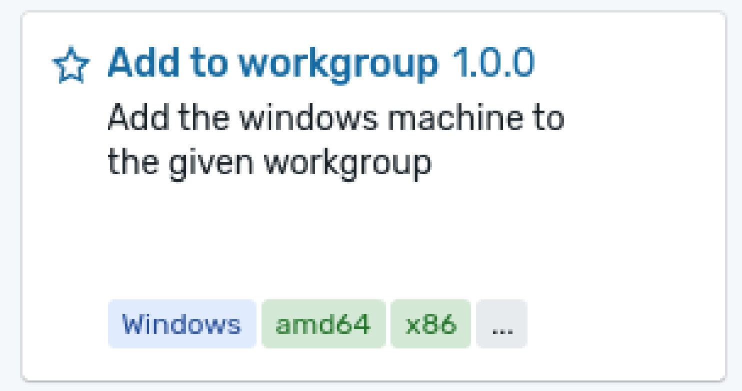


```
hns@ubuntu-client:~$ cat /etc/host
*cat: /etc/host: No such file or directory
hns@ubuntu-client:~$ cat /etc/hosts
127.0.0.1       localhost
127.0.1.1       ubuntu-client
8.8.8.8         google.com
# The following lines are desirable for IPv6 capable hosts
::1     ip6-localhost ip6-loopback
fe00::0 ip6-localnet
ff00::0 ip6-mcastprefix
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters
hns@ubuntu-client:~$
```

DIATEAM

ACTION

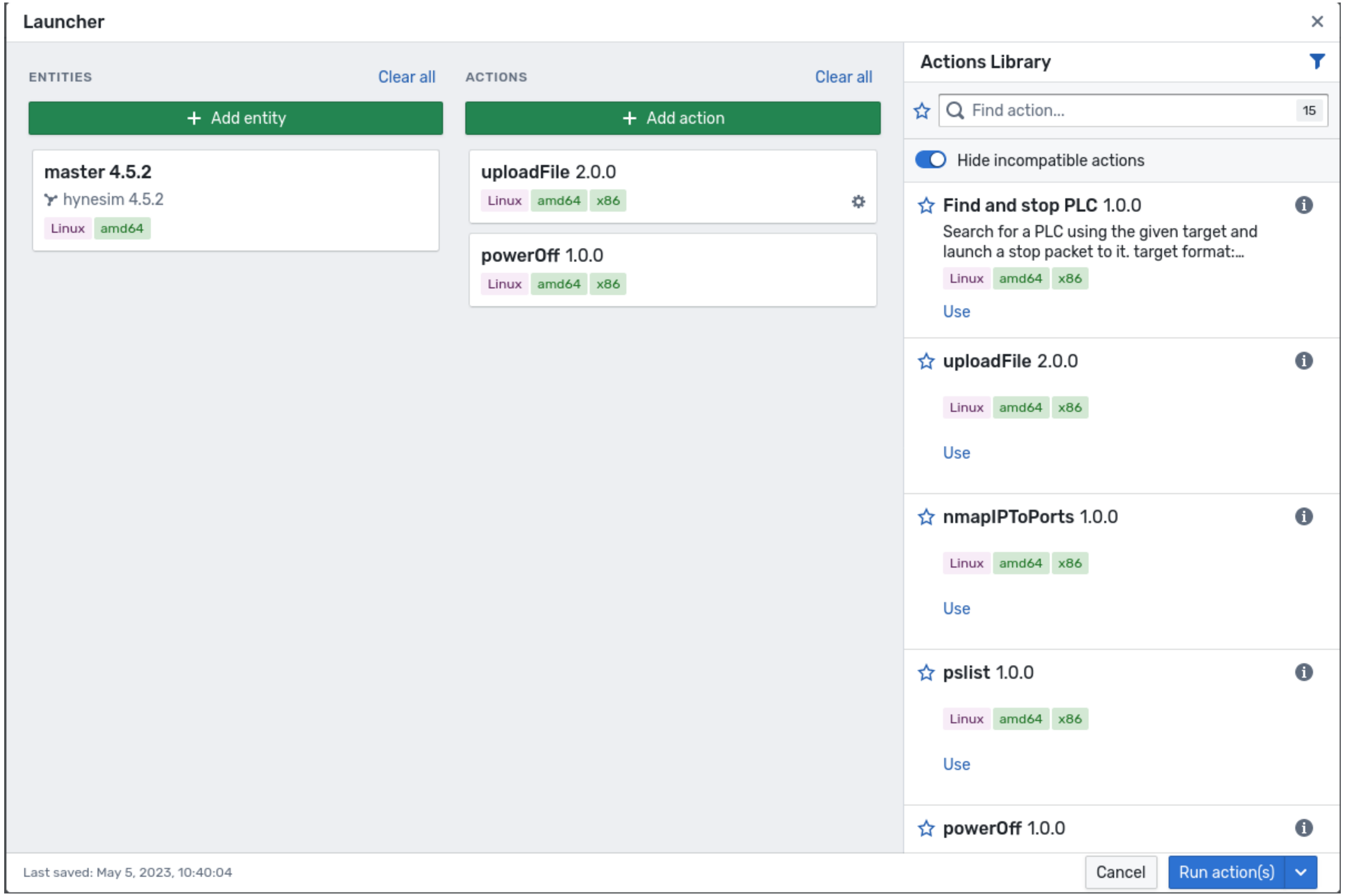
- Executable
  - Bash
  - Python
  - Powershell
- JSON
  - Describe the action and its inputs, resources…
- Executed in an Entity



☆ Add to workgroup 1.0.0

Add the windows machine to the given workgroup

Run multiple Actions



Launcher

ENTITIES Clear all

+ Add entity

master 4.5.2
hynesim 4.5.2
Linux amd64

ACTIONS Clear all

+ Add action

uploadFile 2.0.0
Linux amd64 x86

powerOff 1.0.0
Linux amd64 x86

Actions Library

Find action... 15

Hide incompatible actions

Find and stop PLC 1.0.0
Search for a PLC using the given target and launch a stop packet to it. target format:...
Linux amd64 x86
Use

uploadFile 2.0.0
Linux amd64 x86
Use

nmapIPToPorts 1.0.0
Linux amd64 x86
Use

pslist 1.0.0
Linux amd64 x86
Use

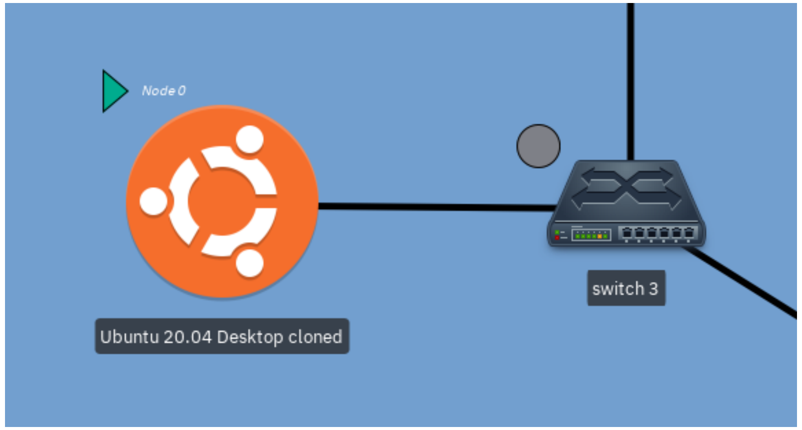
powerOff 1.0.0

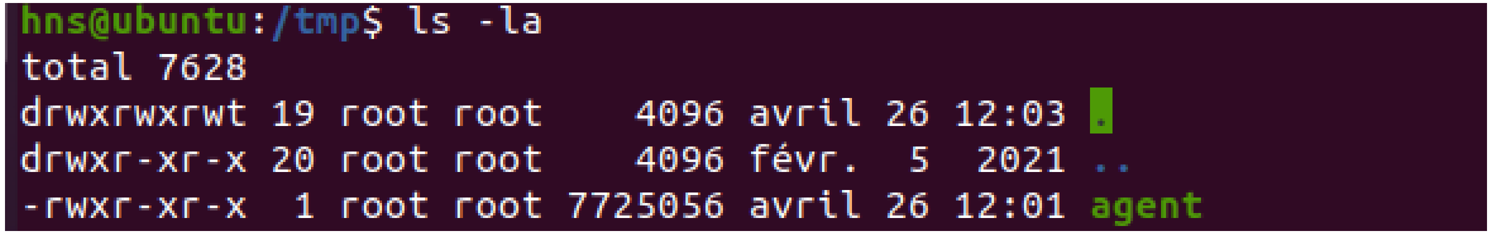
Last saved: May 5, 2023, 10:40:04

Cancel Run action(s)

AGENTS

- Run inside Entities
- Cross Platform (Windows / GNU Linux)
- Execute "Actions"
- Connected through serial port





```
hns@ubuntu:/tmp$ ls -la
total 7628
drwxrwxrwt 19 root root    4096 avril 26 12:03 .
drwxr-xr-x 20 root root    4096 févr.  5  2021 ..
-rwxr-xr-x  1 root root 7725056 avril 26 12:01 agent
```

DIATEAM

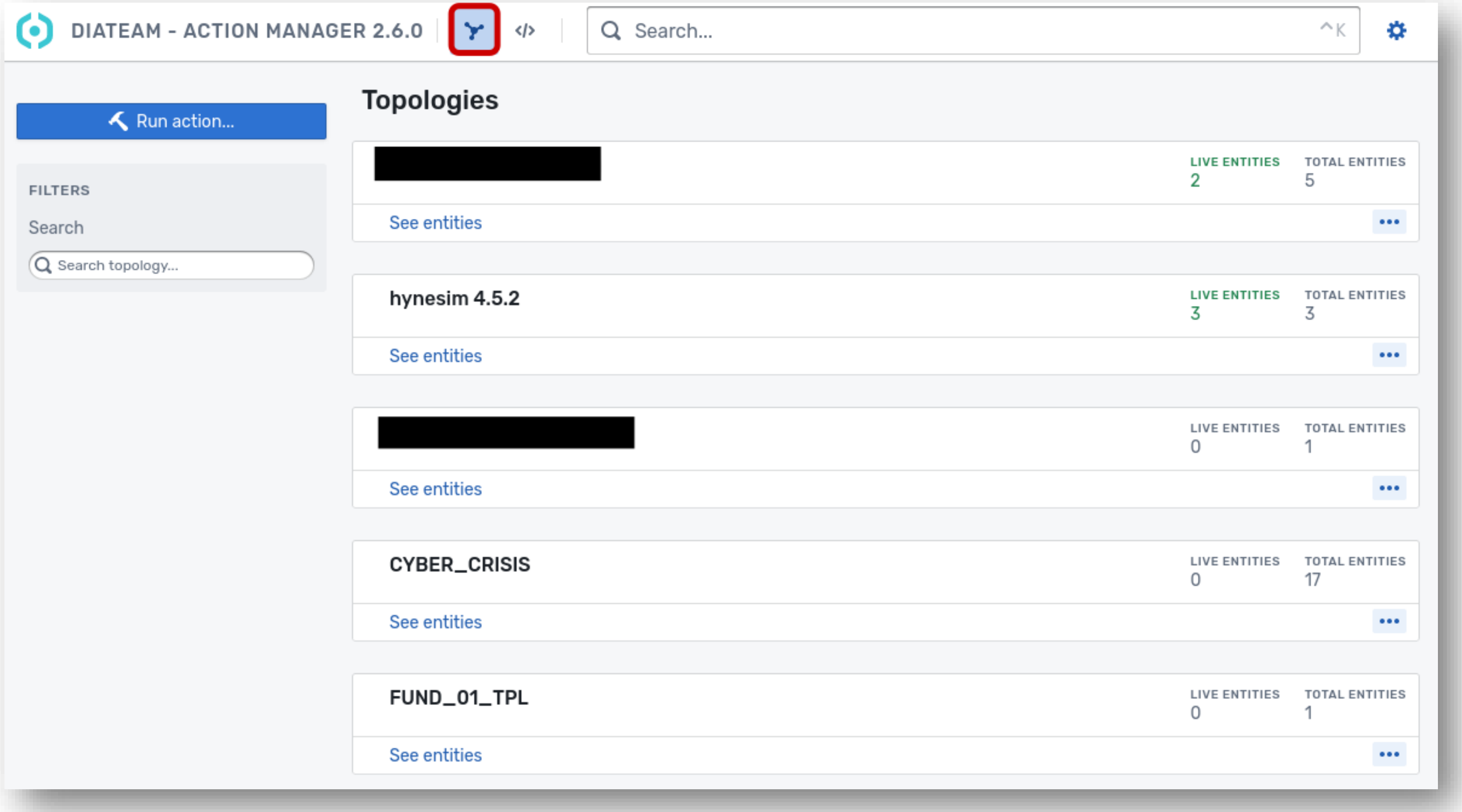
MILITARY & CIVIL CYBERSECURITY SOLUTIONS

MAIN USAGE

www.diateam.net – contact@diateam.net - @DIATEAM_Labs

MAIN USAGE

- TOPOLOGIES PAGE
  - Run actions
  - Entities information & runs
- AM “AGENT” MUST BE RUNNING
- RUN ACTIONS FROM ANYWHERE



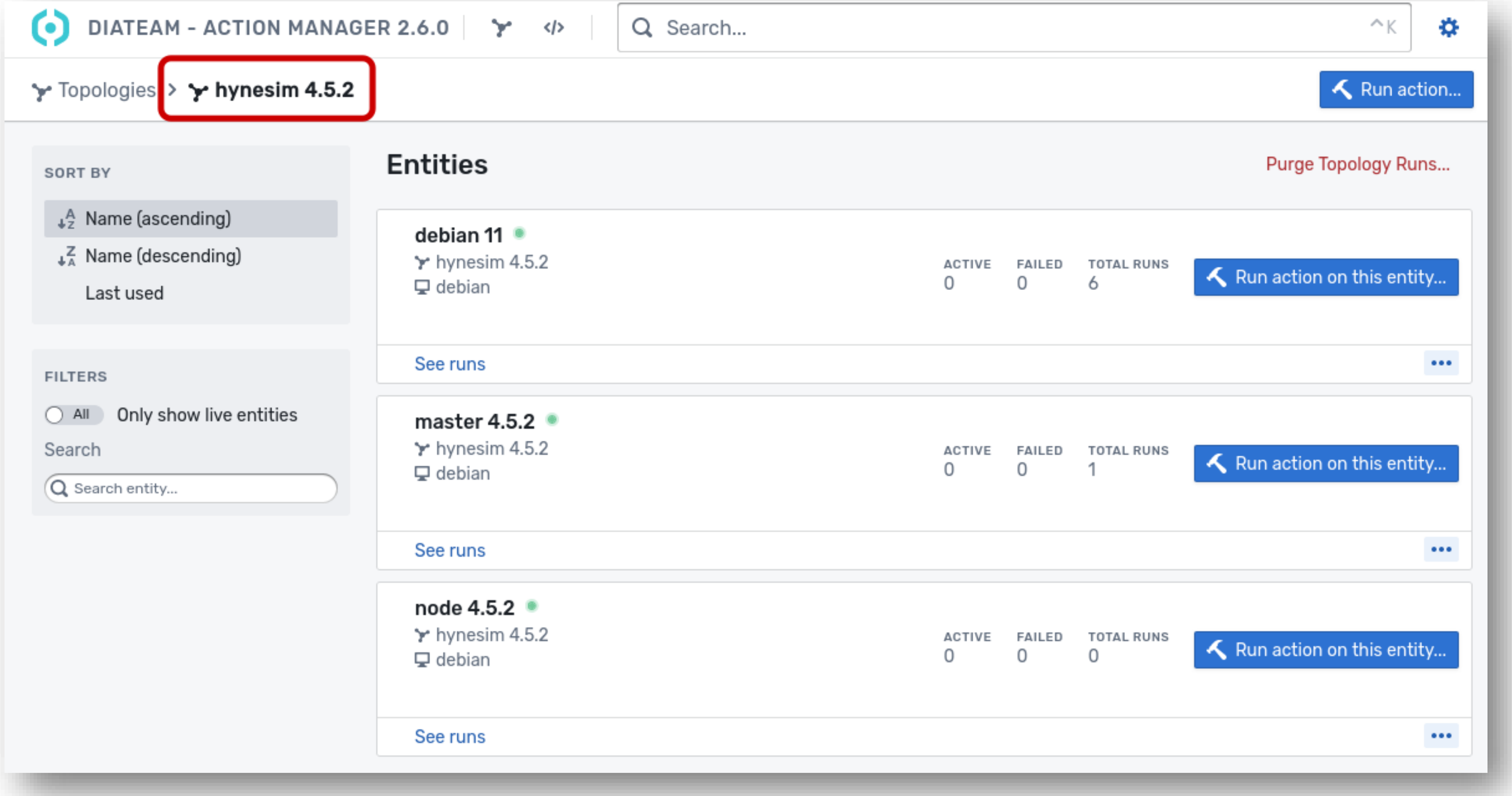
Topologies

	LIVE ENTITIES	TOTAL ENTITIES
[redacted]	2	5
hynesim 4.5.2	3	3
[redacted]	0	1
CYBER_CRISIS	0	17
FUND_01_TPL	0	1

See entities

MAIN USAGE

- ENTITIES PAGE
  - Run actions
  - Entities information & runs



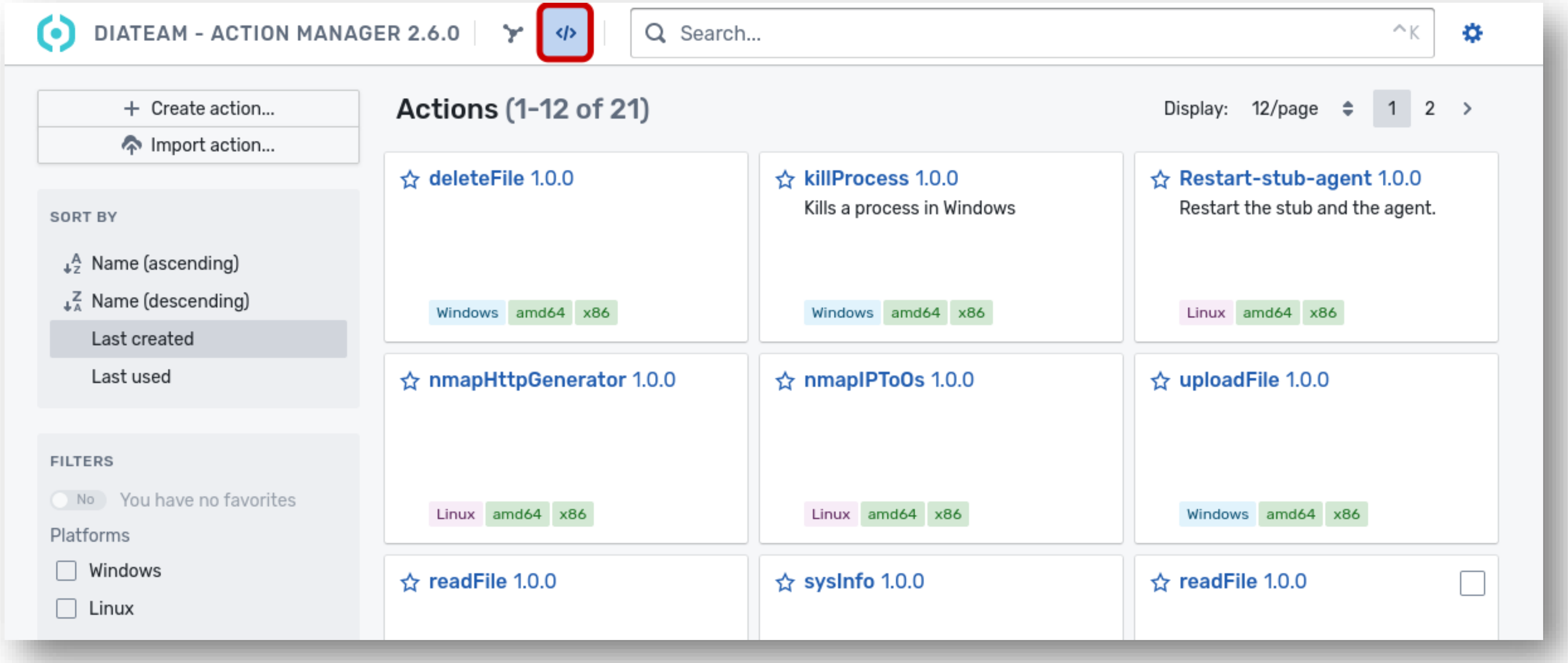
	ACTIVE	FAILED	TOTAL RUNS
debian 11 hynesim 4.5.2 debian	0	0	6
master 4.5.2 hynesim 4.5.2 debian	0	0	1
node 4.5.2 hynesim 4.5.2 debian	0	0	0

- AM "AGENT" MUST BE RUNNING
- RUN ACTIONS FROM ANYWHERE

DIATEAM

MAIN USAGE

- ACTIONS PAGE
  - Create and import actions
  - Actions information
- WINDOWS
  - BAT or Powershell
- LINUX
  - Any executable file



DIATEAM - ACTION MANAGER 2.6.0

Search...

Actions (1-12 of 21)

Display: 12/page 1 2

☆ deleteFile 1.0.0 — Windows amd64 x86

☆ killProcess 1.0.0 — Kills a process in Windows — Windows amd64 x86

☆ Restart-stub-agent 1.0.0 — Restart the stub and the agent. — Linux amd64 x86

☆ nmapHttpGenerator 1.0.0 — Linux amd64 x86

☆ nmapIPToOs 1.0.0 — Linux amd64 x86

☆ uploadFile 1.0.0 — Windows amd64 x86

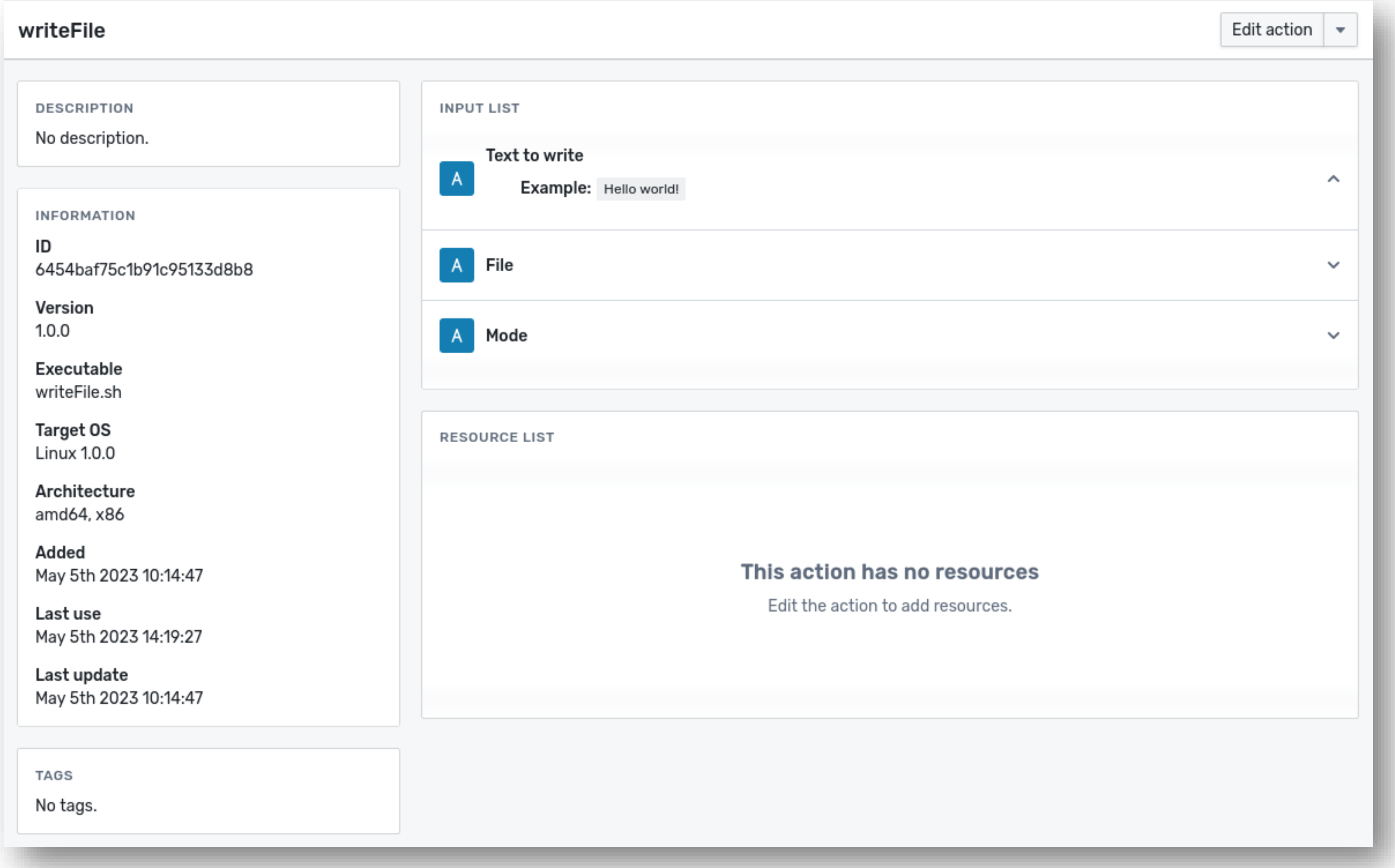
☆ readFile 1.0.0

☆ sysInfo 1.0.0

☆ readFile 1.0.0 □

MAIN USAGE

- ACTION PAGE
  - inputs details
  - Version, exec file…



writeFile

DESCRIPTION

No description.

INFORMATION

ID
6454baf75c1b91c95133d8b8

Version
1.0.0

Executable
writeFile.sh

Target OS
Linux 1.0.0

Architecture
amd64, x86

Added
May 5th 2023 10:14:47

Last use
May 5th 2023 14:19:27

Last update
May 5th 2023 10:14:47

TAGS

No tags.

INPUT LIST

A **Text to write**
Example: Hello world!

A **File**

A **Mode**

RESOURCE LIST

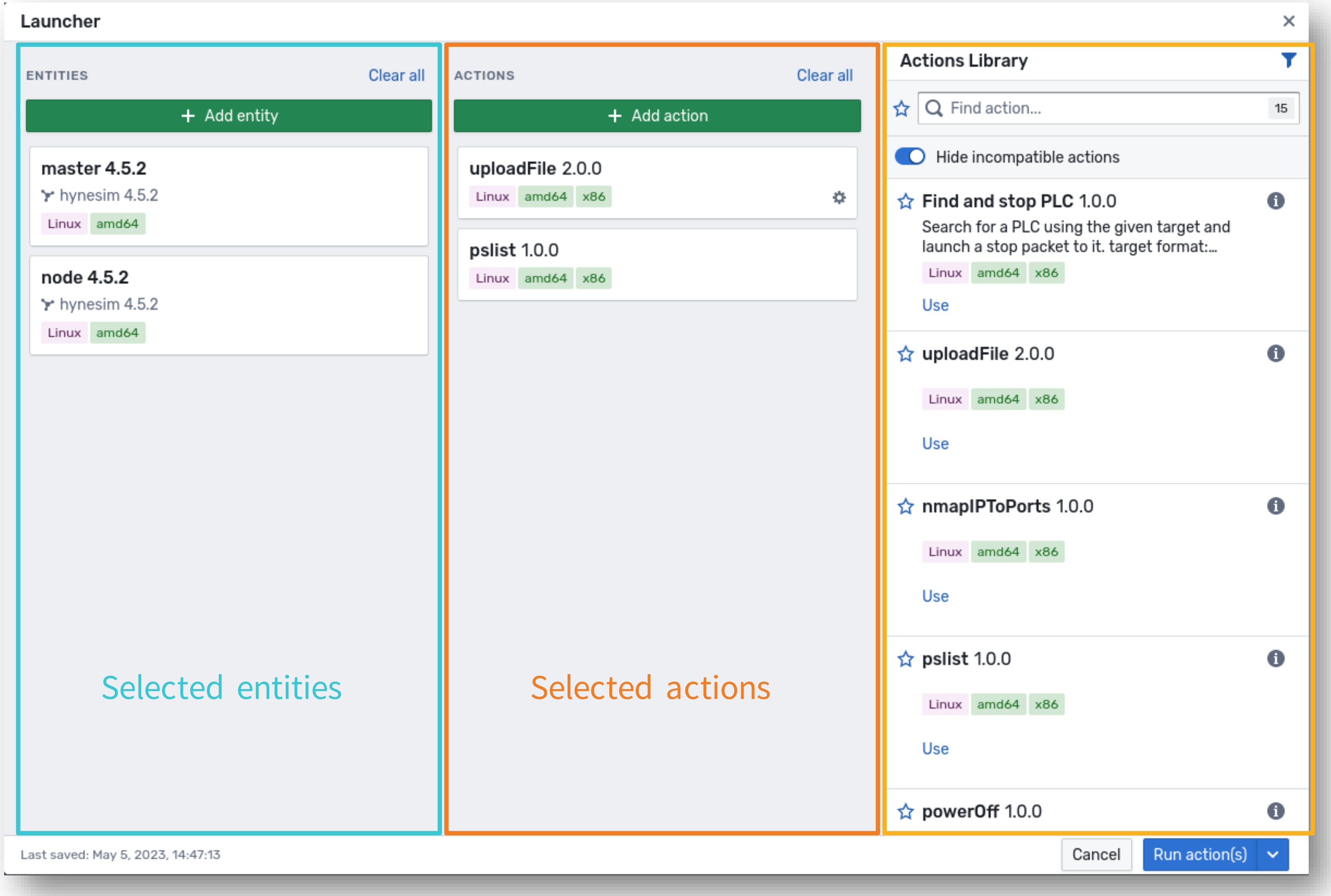
This action has no resources

Edit the action to add resources.

MAIN USAGE

- LAUNCHER
  - Select entities
  - Select actions
  - Configure actions

- LAUNCHER CAN BE ACCESSED FROM ANYWHERE



Launcher

ENTITIES — Clear all

+ Add entity

master 4.5.2
hynesim 4.5.2
Linux amd64

node 4.5.2
hynesim 4.5.2
Linux amd64

Selected entities

ACTIONS — Clear all

+ Add action

uploadFile 2.0.0
Linux amd64 x86

pslist 1.0.0
Linux amd64 x86

Selected actions

Actions Library

Find action... 15

Hide incompatible actions

Find and stop PLC 1.0.0
Search for a PLC using the given target and launch a stop packet to it. target format:...
Linux amd64 x86
Use

uploadFile 2.0.0
Linux amd64 x86
Use

nmapIPToPorts 1.0.0
Linux amd64 x86
Use

pslist 1.0.0
Linux amd64 x86
Use

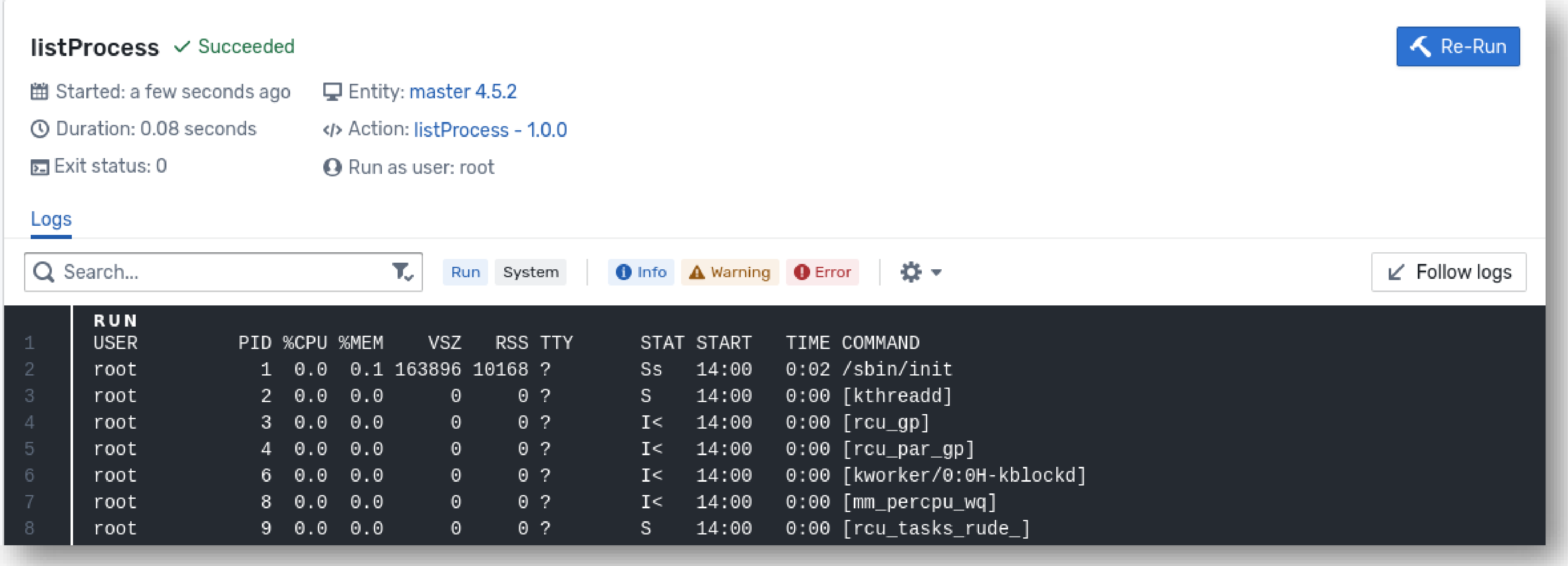
powerOff 1.0.0

Last saved: May 5, 2023, 14:47:13

Cancel — Run action(s)

MAIN USAGE

- RUN RESULT
  - System logs & action logs
  - Execution duration
  - User



listProcess ✓ Succeeded

Started: a few seconds ago

Duration: 0.08 seconds

Exit status: 0

Entity: master 4.5.2

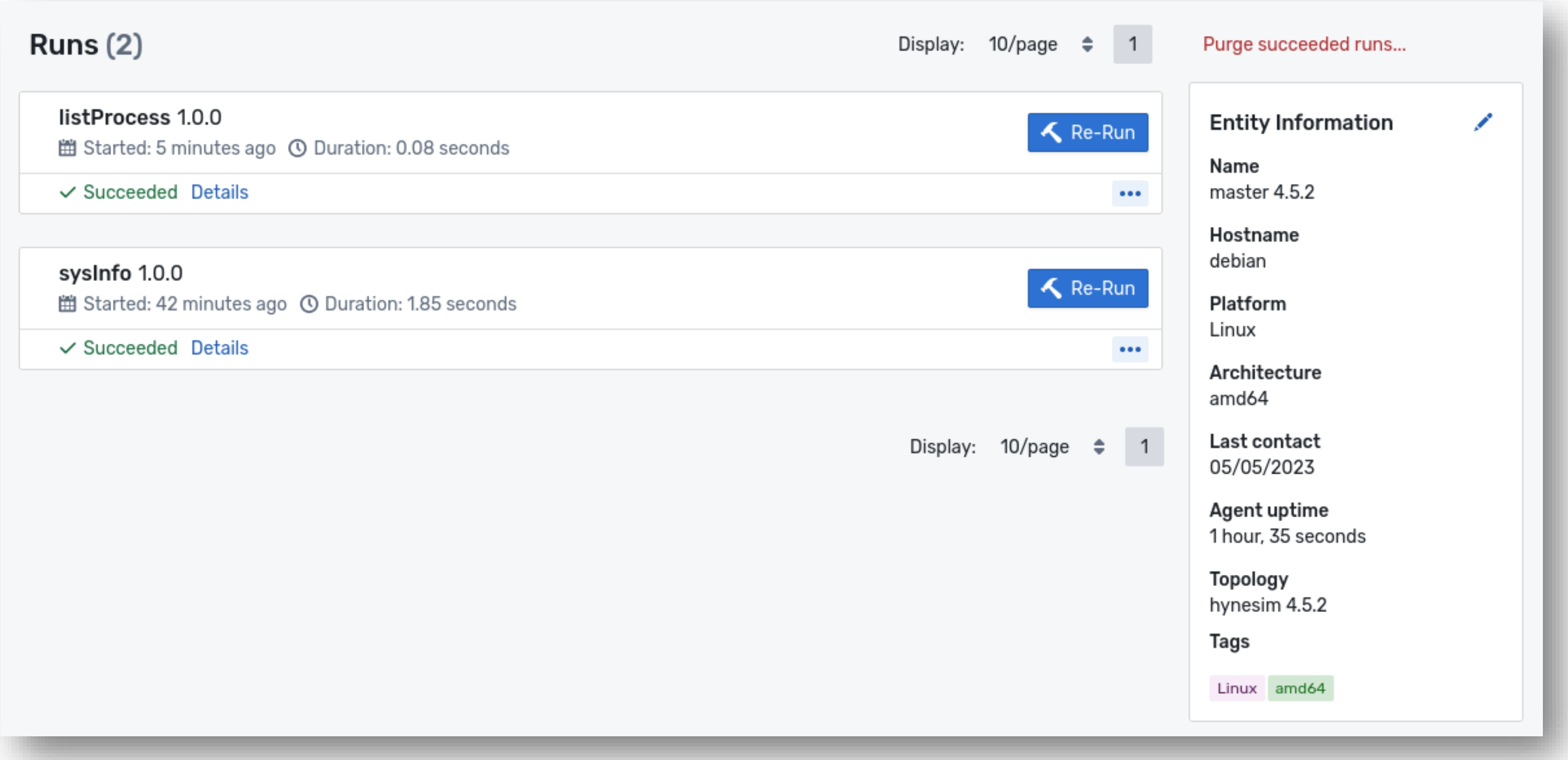
Action: listProcess - 1.0.0

Run as user: root

```
RUN
USER         PID %CPU %MEM    VSZ   RSS TTY      STAT START   TIME COMMAND
root           1  0.0  0.1 163896 10168 ?        Ss   14:00   0:02 /sbin/init
root           2  0.0  0.0      0     0 ?        S    14:00   0:00 [kthreadd]
root           3  0.0  0.0      0     0 ?        I<   14:00   0:00 [rcu_gp]
root           4  0.0  0.0      0     0 ?        I<   14:00   0:00 [rcu_par_gp]
root           6  0.0  0.0      0     0 ?        I<   14:00   0:00 [kworker/0:0H-kblockd]
root           8  0.0  0.0      0     0 ?        I<   14:00   0:00 [mm_percpu_wq]
root           9  0.0  0.0      0     0 ?        S    14:00   0:00 [rcu_tasks_rude_]
```

MAIN USAGE

- ENTITY RUNS PAGE
  - Sorted by date
  - Run an action again



Runs (2)

listProcess 1.0.0
Started: 5 minutes ago Duration: 0.08 seconds
✓ Succeeded Details

sysInfo 1.0.0
Started: 42 minutes ago Duration: 1.85 seconds
✓ Succeeded Details

Entity Information

Name
master 4.5.2

Hostname
debian

Platform
Linux

Architecture
amd64

Last contact
05/05/2023

Agent uptime
1 hour, 35 seconds

Topology
hynesim 4.5.2

Tags
Linux amd64

DIATEAM

MILITARY & CIVIL CYBERSECURITY SOLUTIONS

DEMONSTRATION

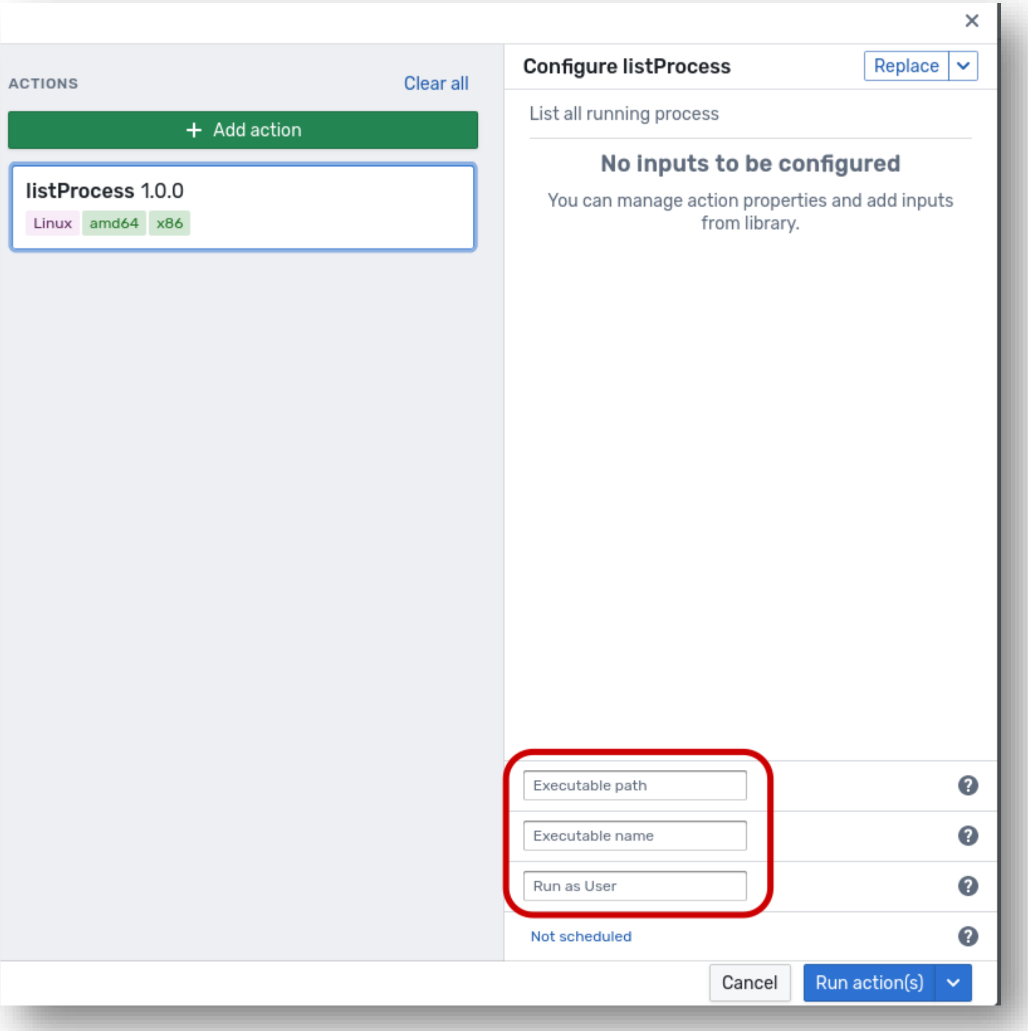
DIATEAM

MILITARY & CIVIL CYBERSECURITY SOLUTIONS

ADVANCED FEATURES

ADVANCED FEATURES

- USER ACTION
  - Default: root/nt authority
  - Allows to execute an action as a user
    - Launch graphical softwares
    - Create/Update content as a user
  - Allow to change the location that the action will be runed
    - Default in the temporary directory
  - Allow to change the executable name
    - Default name "exec"



ACTIONS

listProcess 1.0.0

Configure listProcess

List all running process

No inputs to be configured

You can manage action properties and add inputs from library.

Executable path

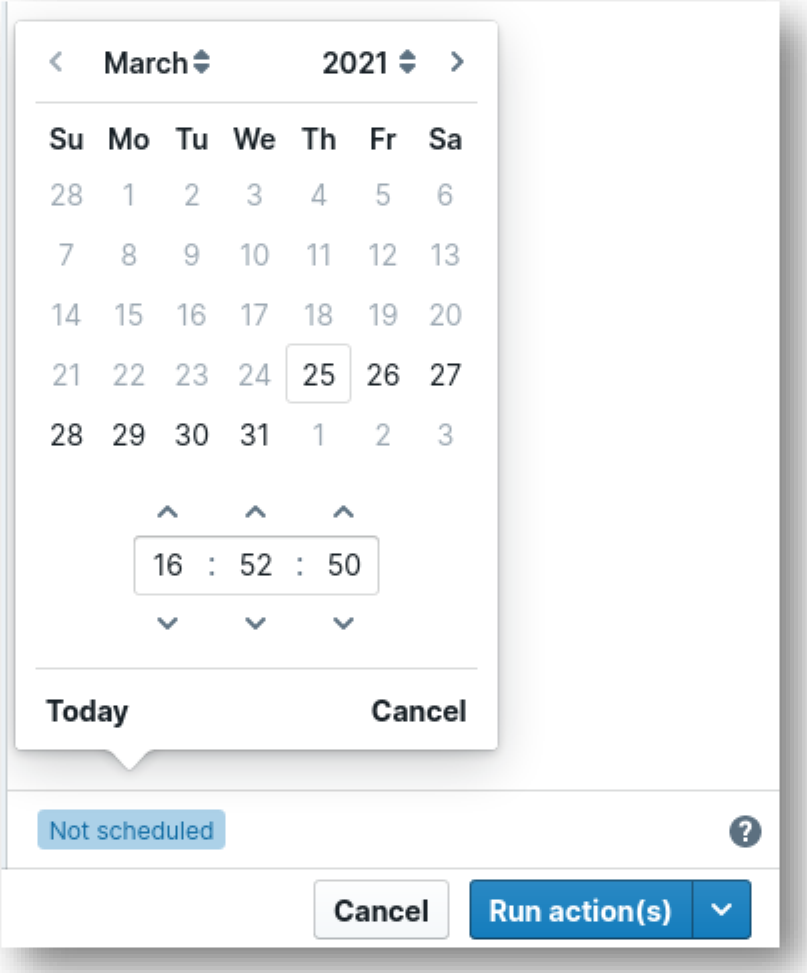
Executable name

Run as User

Not scheduled

ADVANCED FEATURES

- SCHEDULER
  - Prepare your actions



March 2021

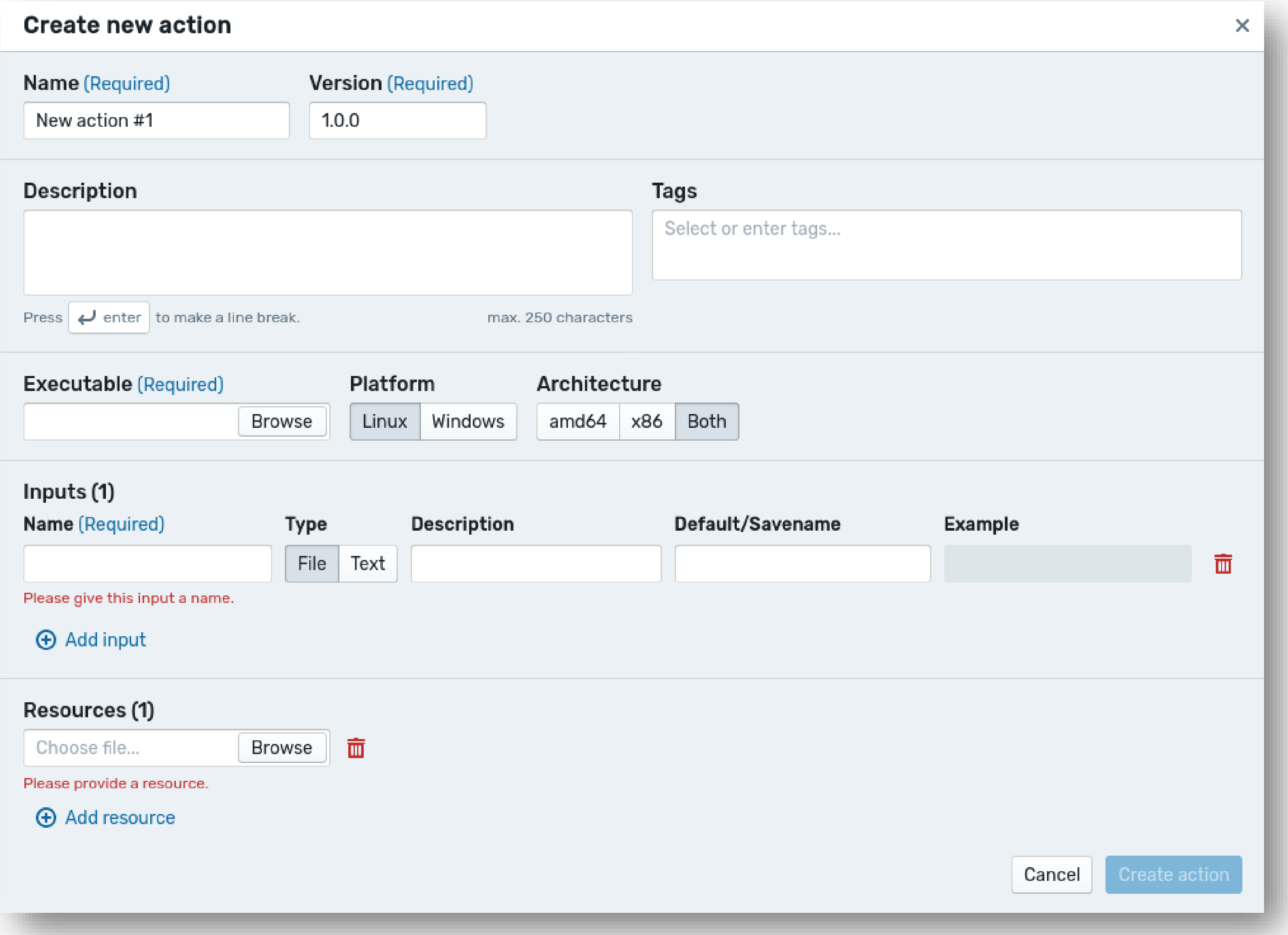
Su	Mo	Tu	We	Th	Fr	Sa
28	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23	24	25	26	27
28	29	30	31	1	2	3

16 : 52 : 50

Not scheduled

ADVANCED FEATURES

- FILES
  - Exchange files between the server and the VM
  - Input files
  - output files
  - resources



Create new action

Name (Required): New action #1

Version (Required): 1.0.0

Description

Tags: Select or enter tags...

Press ↵ enter to make a line break. max. 250 characters

Executable (Required)

Platform: Linux | Windows

Architecture: amd64 | x86 | Both

Inputs (1)

Name (Required)	Type	Description	Default/Savename	Example
	File / Text			

Please give this input a name.

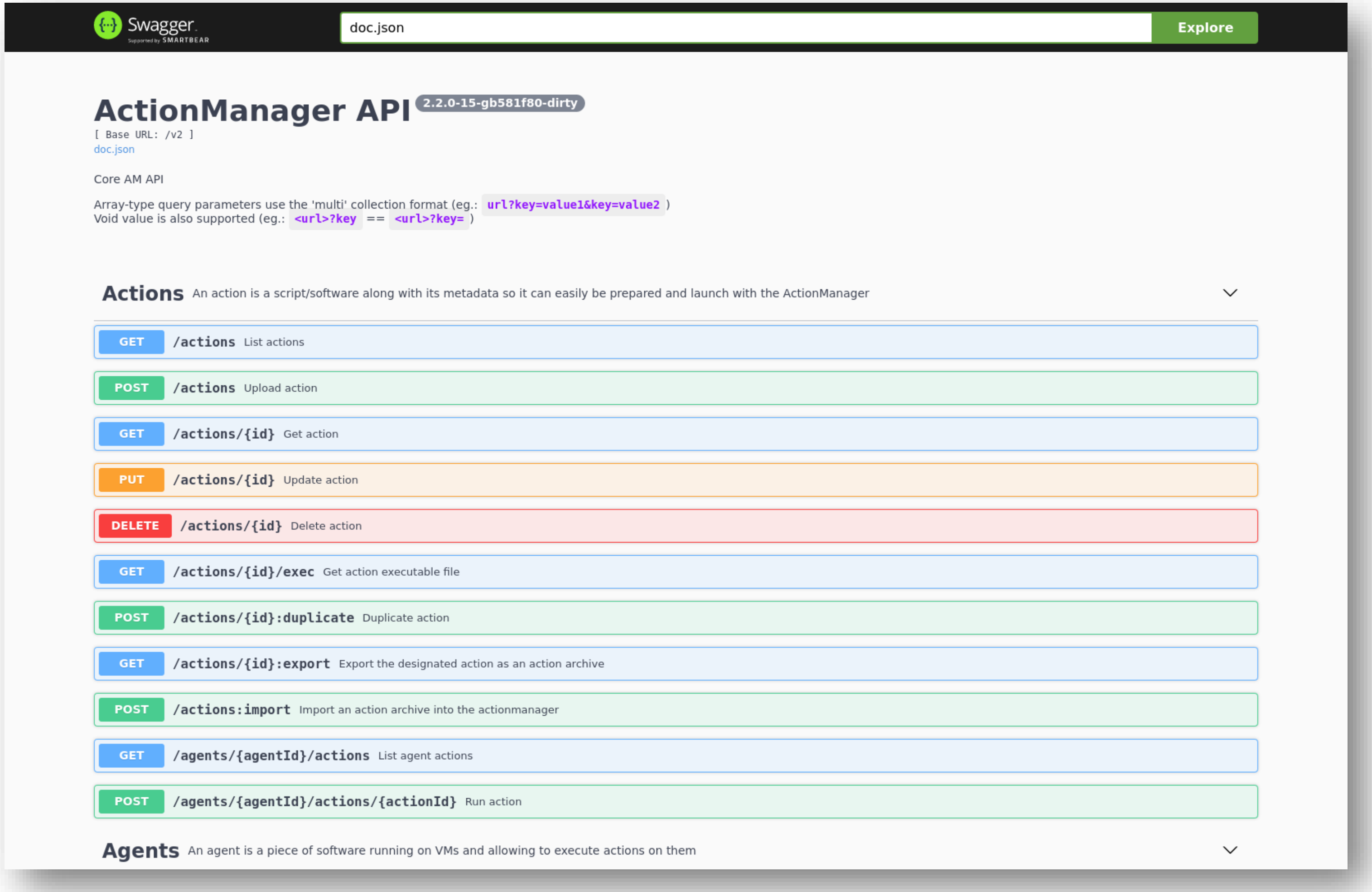
Resources (1)

Choose file...

Please provide a resource.

ADVANCED FEATURES

- SWAGGER
  - Delivered with AM server
  - Browse & test the API



ActionManager API 2.2.0-15-gb581f80-dirty

[Base URL: /v2]
doc.json

Core AM API

Array-type query parameters use the 'multi' collection format (eg.: `url?key=value1&key=value2`)
Void value is also supported (eg.: `<url>?key` == `<url>?key=`)

Actions An action is a script/software along with its metadata so it can easily be prepared and launch with the ActionManager

GET `/actions` List actions
POST `/actions` Upload action
GET `/actions/{id}` Get action
PUT `/actions/{id}` Update action
DELETE `/actions/{id}` Delete action
GET `/actions/{id}/exec` Get action executable file
POST `/actions/{id}:duplicate` Duplicate action
GET `/actions/{id}:export` Export the designated action as an action archive
POST `/actions:import` Import an action archive into the actionmanager
GET `/agents/{agentId}/actions` List agent actions
POST `/agents/{agentId}/actions/{actionId}` Run action

Agents An agent is a piece of software running on VMs and allowing to execute actions on them

DIATEAM

MILITARY & CIVIL CYBERSECURITY
SOLUTIONS

MANY THANKS !
QUESTIONS ?

www.diateam.net – contact@diateam.net - @DIATEAM_Labs