r/portainer • 4 yr. ago
x_MASE_x

Portainer to portainer-agent connection secure?

Hello,I have a portainer setup in a VPS and secured using nginx SSL with a fqdn like:portainer.example.com

Now I have another VPS running a few docker containers and I would like to see all of my portainer instances inside one dashboard which is the main one portainer.example.com

I searched and found that the agent can only be connected to the first portainer reach it/connect to it.

And there is something called agent secret, but not sure if it is working or not since it is in a very old page.

Anyway, if i connected the agent to my main portainer, does that make the connections between the servers secure/encrypted?

Should I install ngnix on the other VPS/s or my only option is the "Protect Docker daemon socket" ??

Join the conversation

Sort by: Best Search Comments

neilcresswell • 4y ago

Portainer to Agent comms is always using https, with a self-signed cert created by the agent automatically on initial deployment.

On first connection from Portainer to an agent, Portainer shares its digital signature with the agent, and the agent then updates its internal security settings to only allow comms from Portainer instances with that signature (stops a second portainer instance using the same agent). The agent secret is used if you do actually want to have multiple portainer instances sharing the same agent (rare use case).

So, I'm fine with just installing the agent and connecting any portainer to it.

No risks or anything else I should secure?

Since I'll be running nginx proxy manager on the agent and portainer it self.

Do I have to keep any ports open for the agent besides 9001?

Thanks for the replay.

1 Reply ···

2 more replies

mapero84 • 2y ago

Thanks for the explenation. I wonder where the key is stored in the portainer agent, since the agent does not have a volume assosiated. Is it only in memory? When the agent host restarts, the agent basically accepts any portainer instance that comes first?
Thanks and sorry for reviving this thread.

1 Reply ···

1 more reply

Foreign-Celery-8301 • 2mo ago

For everyone stumbling upon this post. NO! Your Portainer agent is NOT SECURE!!! Immediately take action by stopping the agent and monitoring your server. You may have already been a victim of the malware "Perfctl" https://blog.exatrack.com/Perfctl-using-portainer-and-new-persistences/ https://www.aquasec.com/blog/perfctl-a-stealthy-malware-targeting-millions-of-linux-servers/

2 Reply ···

kevdogger • 4y ago

I'd like clarification on this as well. I used agent at first but then reverted and opened the docker daemon to listen with client server self signed ssl certs. Im not sure if the agent is encrypted

1 Reply ···

x_MASE_x OP • 4y ago

Are you using cloudflare or nginx proxy?

The thing is that I'm using all of my domains with cloudflare with strict ssl to only trusted CA.

And the docker daemon ssl seems like a pain in the ass to configure since I have multiple servers.

I would really love if someone can point me to the right direction here.

Jazzlike-Abrocoma-96 • 2y ago

To put it simply the portainer agent interacts with the docker.sock which runs with root privileges. When you add the agent to this you grant the validated connections root access too.

Now this wouldn't be an issue but I've yet to see any kind of authentication of the agent when I've been installing it. It just connects seemingly unauthenticated, and I can't find the documentation that says it authenticates with the license key or something like that either. So, at this point. It looks like a major security risk.

1 Reply ...

voloyev • 3mo ago

It is actually a major security risk. Especially, if you run agent in default mode and expose its port. Example, of such attack https://blog.exatrack.com/Perfctl-using-portainer-and-new-persistences/

1 Reply ...

r/Premiumize • 5 mo. ago

Why do people say you can use this service on multiple ip addresses at the same time?

1 upvote · 45 comments

r/Cryptomator • 1 mo. ago

Confused about how Cryptomator works

8 upvotes · 9 comments

r/applebusinessmanager • 3 mo. ago

DO NOT PUSH DOMAIN CAPTURE

8 upvotes · 15 comments

r/dns • 6 mo. ago

Another alternative DNS that might help some people

8 upvotes · 27 comments

r/hyperacusis • 6 days ago

Overprotection is absolutely a thing

23 upvotes · 21 comments

r/FridayThe13thGame • 21 days ago

What's the new DNS?

35 upvotes · 7 comments

r/redteamsec • 4 mo. ago

I don't know how to start red teaming

12 upvotes · 35 comments

r/AnyDesk • 6 days ago

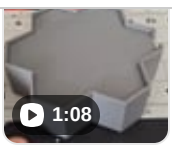
Any Desk detected as Trojan virus

7 upvotes · 6 comments

r/transguns • 3 mo. ago

OPSEC

Overengineered solutions to non-problems



260 upvotes · 56 comments

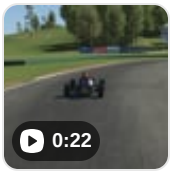
r/dns • 1 mo. ago

Am I configuring this DNS architecture correctly?

8 upvotes · 6 comments

r/Simracingstewards • 2 mo. ago

Protestable?



120 upvotes · 56 comments

r/trouduction • 6 mo. ago

Configuration d'un nouvel ordinateur

35 upvotes · 8 comments

r/FridayThe13thGame • 1 mo. ago

DNS up and running again

87 upvotes · 36 comments

r/talesfromtechsupport • 9 mo. ago

User with a non-issue that was 'fixed' created an actual issue.

620 upvotes · 40 comments

r/cyberpunk2077mods • 10 days ago

Any one recognize the cyberware in this pic?

67 upvotes · 10 comments

24 upvotes · 4 comments

r/SpeedRunnersGame • 9 days ago

Windows detecting as virus

15 upvotes · 5 comments

r/printablescom • 2 mo. ago

Hiding malware

48 upvotes · 21 comments

r/RubenSim • 6 days ago

Ro-cleaner and it's awful opsec

17 upvotes · 6 comments

r/ProPresenter • 2 mo. ago

Pro Presenter File Management

20 upvotes · 10 comments

TOP POSTS

Reddit

reReddit: Top posts of May 6, 2021

Reddit

reReddit: Top posts of May 2021

Reddit

reReddit: Top posts of 2021