datatap

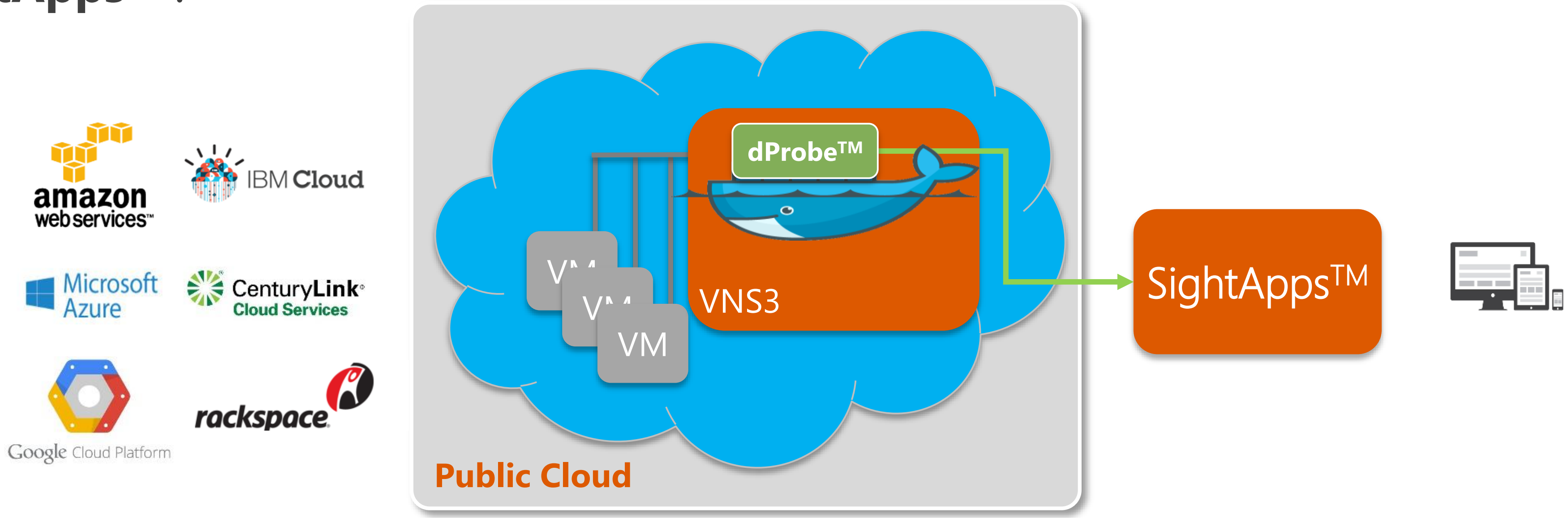
dPobe^{TM} for Docker Configuration Guide

Contents

Introduction

dProbe™ is a lightweight packet inspection probe that performs L3-L7 header analysis. Depending on the expected traffic load to analyze, different versions of the dProbes are employed.

For the Cloud environments where networking features such as SPAN and traffic tunneling are not offered, dProbe can be deployed as a Docker instance in a multi-purpose VPN/Gateway/Firewall/Switch/Router solution such as **VNS3** from **CohesiveFT**. Following is a picture that illustrates how the dProbe runs in a docker container environment reporting to **SightApps™**.



Server Requirements

dProbe is optimized to run in resource constrained environments keeping up with rate of network traffic. System requirements for a dProbe instance are as following:

- At the most 150Mbytes of RAM for docker instance
- At the most 30% of computing cycles from docker host system
- Around 1Gbyte disk space – dProbe docker instance does not store any data locally

Docker Host:

dProbe docker instance is based on CentOS 6.5. Following are some of the expected characteristics of the Docker host environment:

- Docker version of at least 1.4 on the host
- Docker host should have the capability to supply network traffic to dProbe instance (Steps to do this are described for VNS3/CohesiveFT to give you an idea. For other docker hosts, you need to identify the steps to enable this.)
- Docker host should be able to allow outbound communication from dProbe to SightApps

Getting Started – Docker Host

If you have a Docker host environment, follow the steps below:

- Contact support@datatapsolutions.com to get a link to dProbe Docker image
- DataTap Support provides you with a link to **image** as well as a **keyfile** to access the docker instance. Please save this **keyfile** for later consumption.
- Import the image: **docker import** <HTTP-LINK-TO-dProbe-Image>

```
[root@dockerhost ~]# docker import http://www.datatapsolutions.com/jklcdjoijoijckd89jlkcd989cd889cdjoicd80.tar.gz
```

- Verify that the image is imported with a **datatap/datatap** tag: **docker images**

```
[root@dockerhost ~]# docker images
REPOSITORY      TAG           IMAGE ID       CREATED          VIRTUAL SIZE
datatap/dProbe  latest        f9913d335b23     2 days ago        637.5 MB
```

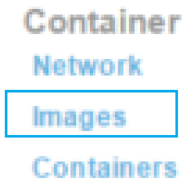
- Run the dProbe docker instance

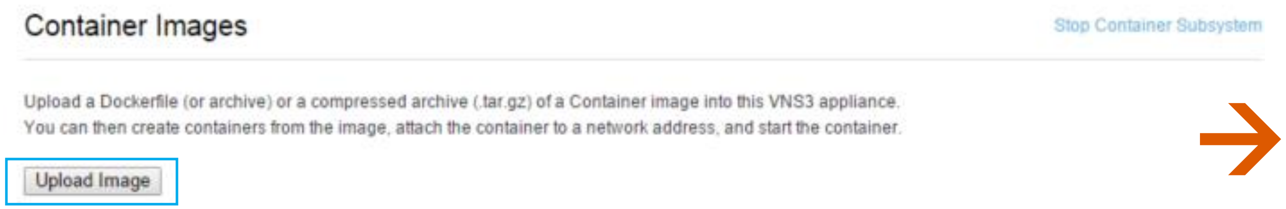
```
[root@dockerhost ~]# docker run -i –t f99
'Supervisord is running as root and it is searching '
2015-01-10 22:10:13,925 CRIT Supervisor running as root (no user in config file)
2015-01-10 22:10:13,937 INFO supervisord started with pid 1
2015-01-10 22:10:14,954 INFO spawned: 'sshd' with pid 8
2015-01-10 22:10:14,991 INFO spawned: 'datatapProbe' with pid 9
2015-01-10 22:10:15,997 INFO success: sshd entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
2015-01-10 22:10:15,997 INFO success: datatapProbe entered RUNNING state, process has stayed up for > than 1 seconds (startsecs)
```

VNS3/CohesiveFT (1/3)

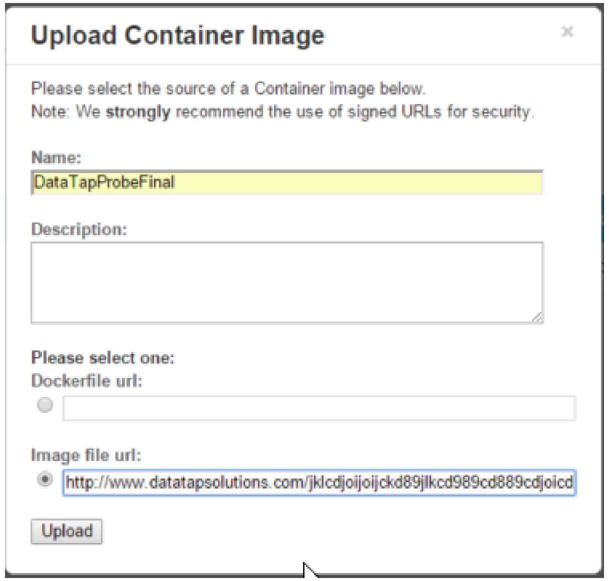
If you have a VNS3 in your environment, follow the steps below:

- Contact support@datatapsolutions.com to get a link to dProbe Docker image
- Importing the dProbe image
  - Log into VNS3 (If you do not have Container license contact CohesiveFT support)
  - From left hand menu, go to ‘Container’ section and click on ‘Images’
  - Click on ‘Upload Image’ and enter the details as shown below
  - Click ‘Upload’ to get the dProbe image on to VNS3




Container Images

Upload a Dockerfile (or archive) or a compressed archive (.tar.gz) of a Container image into this VNS3 appliance.
You can then create containers from the image, attach the container to a network address, and start the container.


Upload Container Image

Please select the source of a Container image below.
Note: We **strongly** recommend the use of signed URLs for security.

Name: DataTapProbeFinal

Description:

Please select one:

Dockerfile url:
○

Image file url:
● http://www.datatapsolutions.com/jklcdjoijoijckd89jlkcd989cd889cdjoicd

VNS3/CohesiveFT (2/3)

- Start the dProbe instance with following steps:
  - From left hand menu, go to ‘Container’ section and click on ‘Images’
  - Find the dProbe image by the name you have given
  - Clock on ‘Action’ button and ‘Allocate’ a new Container as shown below

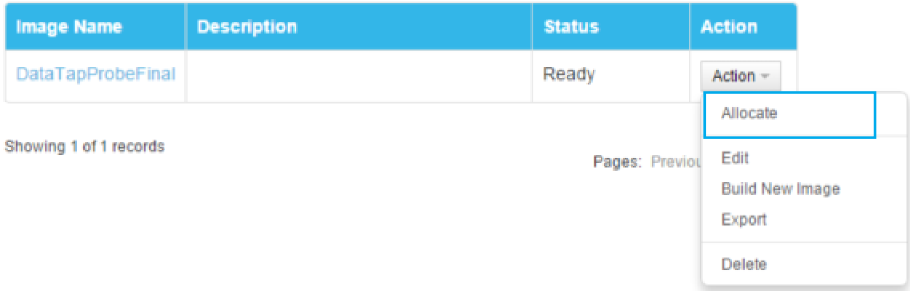
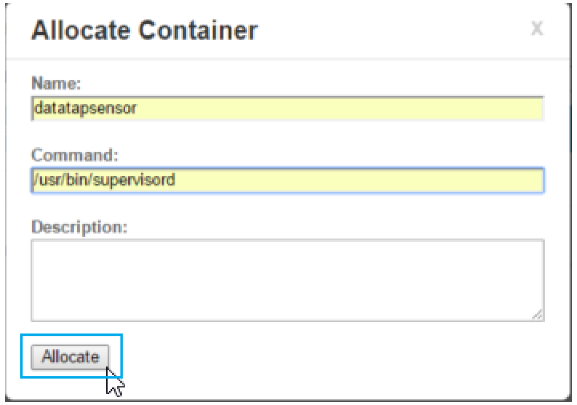


Image Name	Description	Status	Action
DataTapProbeFinal		Ready	Action

Showing 1 of 1 records

Pages: Previou



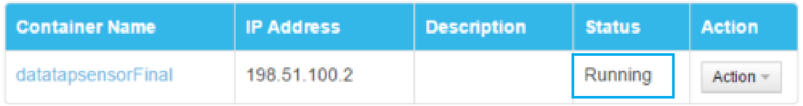
Allocate Container

Name: datatapsensor

Command: /usr/bin/supervisord

Description:

  - Now go to newly created container from menu – Container → Containers and find the dProbe container running.



Container Name	IP Address	Description	Status	Action
datatapsensorFinal	198.51.100.2		Running	Action

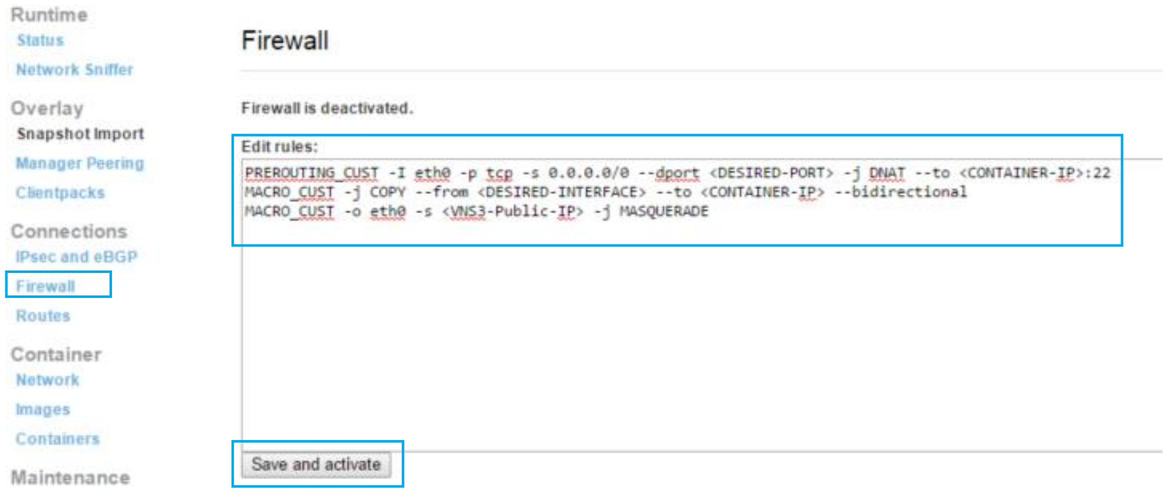
VNS3/CohesiveFT (3/3)

- VNS3 configuration to enable dProbe instance:
  - From left hand menu, go to 'Connections' section and click on 'Firewall'
  - Enter following rules respectively:
    - Enable SSH Access on the DESIRED-PORT on Docker Host (VNS3) (Required for Certificate, Licensing and Remote Support)

      PREROUTING_CUST -I eth0 -p tcp -s 0.0.0.0/0 --dport <DESIRED-PORT> -j DNAT --to <CONTAINER-IP>:22
    - Copy tunnel traffic from DESIRED-INTERFACE on host (eth0 or tun0) to dProbe container (Required to analyze the traffic)

      MACRO_CUST -j COPY --from <DESIRED-INTERFACE> --to <CONTAINER-IP> --bidirectional
    - Let the Docker Subnet Access the Internet via the Managers Public IP (Required to enable communications to SightApps)

      MACRO_CUST -o eth0 -s <VNS3-Public-IP> -j MASQUERADE



Firewall

Firewall is deactivated.

Edit rules:

```
PREROUTING_CUST -I eth0 -p tcp -s 0.0.0.0/0 --dport <DESIRED-PORT> -j DNAT --to <CONTAINER-IP>:22
MACRO_CUST -j COPY --from <DESIRED-INTERFACE> --to <CONTAINER-IP> --bidirectional
MACRO_CUST -o eth0 -s <VNS3-Public-IP> -j MASQUERADE
```

Restricted Shell Access

DataTapSolutions provides restricted shell access to dProbe docker instance. This enables customers exchange information with dProbe using file transfer (scp) command. Following are the steps to communicate with dProbe instance:

- Make sure you have enabled access to port 22 on dProbe instance. If you are on a docker host command line, use 22 directly for SSH-PORT. If on VNS3 use the DESIRED-PORT as described in VNS3 docker section for SSH-PORT.
- Using the SSH Private Keyfile provided along with dProbe docker image, execute following command to transfer files to and from dProbe instance
  - Transfer file in to dProbe Instance:

```
[root@dockerhost ~]# scp -P <SSH-PORT> -i <PATH-TO-KEYFILE> test.file deployer@<CONTAINER-IP>:/home/deployer
```

  - Transfer file out of dProbe Instance

```
[root@dockerhost ~]# scp -P <SSH-PORT> -i <PATH-TO-KEYFILE> deployer@<CONTAINER-IP>:/home/deployer/test.file .
```

Note: There is a "." at the end of the command when transferring files out of dProbe instance

SightApps Pairing

Once the dProbe Docker instance is up and running, it's time for SightApps pairing of the server.

- Log into SightApps Administration interface (refer to SightApps Administration guide) and download the Certificate file (Also called SightApps Probe Signature)
  - Save the Certificate file from SightApps as **server.cer**

- Using the Restricted Shell Access, put the server.cer file into dProbe instance

```
[root@dockerhost ~]# scp -P <SSH-PORT> -i <PATH-TO-KEYFILE> server.cer deployer@<CONTAINER-IP>:/home/deployer
```

Probe Licensing

Once the dProbe Docker instance SightApps pairing is completed, it's time for licensing the server.

- Using the Restricted Shell Access, get the licenseSeed.lic file from dProbe instance

```
[root@dockerhost ~]# scp -P <SSH-PORT> -i <PATH-TO-KEYFILE> deployer@<CONTAINER-IP>:/home/deployer/licenseSeed.lic .
```

- Contact support@datatapsolutions.com with above file to get dProbe Docker instance license
- Using the Restricted Shell Access, put the license.lic file into dProbe instance

```
[root@dockerhost ~]# scp -P <SSH-PORT> -i <PATH-TO-KEYFILE> license.lic deployer@<CONTAINER-IP>:/home/deployer
```

Note: There step is going to be automated to control from a SightApps server in future releases.

Remote Support

In the instances where DataTap support personnel require to access the dProbe command-line tools, we ask you to follow the procedure below to enable access:

- Make sure you have enabled access to port 22 on dProbe instance. If you are using VNS3 use the DESIRED-PORT as described in VNS3 docker section for SSH-PORT and communicate the same to DataTap Support.
- Enable access to SSH-PORT on the Docker host to DataTap support IP range (Typically done through your network settings)
- To access your dProbe instance, DataTap Support needs to know the Docker host Public IP address as well as SSH-PORT.

WARNING: Please disable the Remote support (by disabling DataTap Support IP range and SSH-PORT) after your issue is resolved.

Email us at support@datatapsolutions.com for

Help Now ➔

Learn more at http://www.datatapsolutions.com