Community   **Forums**   TechBlog   TechCenter   TechVideos   Ideas   Tech Alerts   Developer   Resource

Centrify Express

Community support for Centrify Express for Mac, Centrify Express for
Linux and UNIX and Centrify Express for CAC Smart Cards.

TSYS
Proxy Messages

Blogs   Support   Community   [LOGIN]   [TRY IT NOW]

The Internet Site you are accessing is
only being made available for
business use under the provisions of the

Why Centrify   Products   Solutions   Customers   Partners   Company

Infrastructure Services - Secure Remote Access

Welcome to the Centrify Community! [Announcement]: Important Centrify Website Account Changes after January 6th

COMMUNITY → FORUMS → EXPRESS → RUNNING CENTRIFYDC IN DOCKER CONTAINER →

Running centrifydc in docker container

| Search Community... 🔍 | Board ▾ |

Reply   Topic Options ⚙▾   ⟨ Message Listing   ⟨ Previous Topic   Next Topic ⟩

⟨ Previous   **1**   2   Next ⟩

rafajot
Participant II

Posts: 5
Registered: 01-20-2015

#1 of 17 6,885   01-20-2015 05:33 AM - last edited 12-21-2015 02:40 AM   Options ⚙▾

Hello,

Is there any recomendation/is it a supported scenario to run centrifydc in a docker container?
At the moment I have the following setup:
Docker version 1.4.1, build 5bc2ff8
Description: Ubuntu 14.04.1 LTS
centrifydc   5.2.1-301   amd64   Centrify DirectControl Agent

When I install centrifydc inside docker container it seems to work fine but adjoin command fails with the following error message:

```
root@mydocker-container:/#  adjoin -i -w --force --user myusername --password mypasswd -D mydocker-container.mydomain mydc
Using LDAP to create computer name larger than 15 characters.
This requires Windows Administrator privileges.
Try -N option if you cannot use an Administrator account.

Using domain controller: mydc.mydomain writable=true
Join to domain:mydomain, zone:Auto Zone successful
```

and when I run strace for adjoin process (running inside container) on docker host I get the following output:

```
root@mydocker-host:~# strace -p 15624
Process 15624 attached
restart_syscall(<... resuming interrupted call ...>) = 0
socket(PF_LOCAL, SOCK_STREAM, 0)         = 3
fcntl(3, F_GETFL)                        = 0x2 (flags O_RDWR)
fcntl(3, F_SETFL, O_ACCMODE|O_NONBLOCK) = 0
connect(3, {sa_family=AF_LOCAL, sun_path="/var/centrifydc/daemon"}, 24) = -1 ENOENT (No such file or directory)
close(3)                                 = 0
nanosleep({0, 500000000}, NULL)          = 0
socket(PF_LOCAL, SOCK_STREAM, 0)         = 3
fcntl(3, F_GETFL)                        = 0x2 (flags O_RDWR)
fcntl(3, F_SETFL, O_ACCMODE|O_NONBLOCK) = 0
connect(3, {sa_family=AF_LOCAL, sun_path="/var/centrifydc/daemon"}, 24) = -1 ENOENT (No such file or directory)
close(3)                                 = 0
nanosleep({0, 500000000}, NULL)          = 0
socket(PF_LOCAL, SOCK_STREAM, 0)         = 3
fcntl(3, F_GETFL)                        = 0x2 (flags O_RDWR)
fcntl(3, F_SETFL, O_ACCMODE|O_NONBLOCK) = 0
connect(3, {sa_family=AF_LOCAL, sun_path="/var/centrifydc/daemon"}, 24) = -1 ENOENT (No such file or directory)
close(3)                                 = 0

[...]
```

And I have to admit /var/centrifydc/daemon socket is not present in docker container:

```
root@mydocker-container:/# ls -l /var/centrifydc/
total 56
-rw-r--r-- 1 root root  423 Jan 20 12:12 kset.dc.mydomain
-rw------- 1 root root   54 Jan 20 12:12 kset.des.salt
-rw-r--r-- 1 root root   17 Jan 20 12:12 kset.domain
-rw-r--r-- 1 root root   32 Jan 20 12:12 kset.domaincontroller
-rw-r--r-- 1 root root   17 Jan 20 12:12 kset.forest
-rw-r--r-- 1 root root   32 Jan 20 12:12 kset.globalcatalog
-rw-r--r-- 1 root root   41 Jan 20 12:12 kset.host
-rw-r--r-- 1 root root    8 Jan 20 12:12 kset.licensemode
-rw-r--r-- 1 root root   15 Jan 20 12:12 kset.prew2k.host
-rw-r--r-- 1 root root    9 Jan 20 12:12 kset.schema
-rw-r--r-- 1 root root   11 Jan 20 12:12 kset.site
-rw-r--r-- 1 root root   32 Jan 20 12:12 kset.zone
-rw-r--r-- 1 root root   26 Jan 20 12:12 kset.zonename
drwxrwxrwt 2 root root 4096 Jan 20 12:12 user
root@mydocker-container:/#
```

Thank you,
Rafał Jankowski

Report Inappropriate Content

Labels:　Express for UNIX - Linux

Reply

Kudos

Traditionally support is driven from the paid version and if there are no major architectural changes it's simultaneously available to the community version.

In general, and admitting that I have a miniscule exposure to dockers, I expect us to be a shared component among dockers (or selectively exposing it, based on the requirement), rather than joining an individual docker. If that even makes sense :)

This will post will be escalated.

R.P

Want to learn more about practical Centrify examples? Check out my blog at http://centrifying.blogspot.com

Follow Centrify:

Report Inappropriate Content

Reply

○ **Kudos**

---

rafajot
Participant II

Posts: 5
Registered: 01-20-2015

#3 of 17 6,875   01-20-2015 07:11 AM   Options

Robertson,

Do I understand correctly that in the solution you are planning the docker host will join domain and it will have shared component that will allow docker containers running on this host to join the same domain?

If so it is some reasonable solution but it is also seems to be kind of limitation - different docker containers running on the same host won't be able to join different domains or even different Organizational Units within the same domain etc.

Regards,
Rafał

Report Inappropriate Content

Reply

○ **Kudos**

Robertson
Centrify Guru I

Posts: 2,034
Registered: 07-26-2012

#4 of 17 6,859   01-20-2015 10:37 AM   Options

Great feedback :-)

That Rafal is why we let our bigger customers outline their customer stories and use cases before we develop and productize capabilities.

Let's hope we have something cooking and maybe by the summer we can have an update for you.

R.P

Want to learn more about practical Centrify examples? Check out my blog at http://centrifying.blogspot.com

Follow Centrify:

It would be helpful to understand how you've implemented the container and what it is you're trying to accomplish.

By better understanding your use case, we will be able to provide you with better guidance and provide a better solution in the future.

Regards,

Felderi Santiago
Technical Director - NA East, LATAM
Centrify Corporation
Found my response helpful? Click the Kudos button!

Follow Centrify:

Fel
Centrify Guru I

Posts: 907
Topics: 3
Kudos: 230
Blog Posts: 4
Ideas: 0
Solutions: 119

Registered: 07-06-2010

Report Inappropriate Content

Reply

○ Kudos

---

rafajot
Participant II

Posts: 5
Registered: 01-20-2015

#6 of 17 6,849   01-20-2015 12:31 PM   Options

My goal is to run docker host with couple of docker containers. Each container I would like to access (SSH, Apache with basic authentication) with AD credentials. So actually scenario described by Robertson would be quite satisfactionary for me - at the moment I don't need sepearate domains for different containers running on the same host. However I would like to have different login permissions (for example pam.allow.groups) among different Docker containers.

I'm not sure if it answers your question - if not please let me know.

Regards,
Rafał

Report Inappropriate Content

Reply

○ Kudos

Fel
Centrify Guru I

Posts: 907
Topics: 3
Kudos: 230
Blog Posts: 4
Ideas: 0
Solutions: 119

Registered: 07-06-2010

#7 of 17 6,817   01-20-2015 05:13 PM   Options

Thanks,

I took a closer look at this and I am able to reproduce your issue. We're looking into why adjoin is unable to start adclient after the join but a workaround for now is to start adclient manually by running "/usr/sbin/adclient".

Running adinfo should now show status as connected.

We will post more information here as it becomes available.

Hope this helps,

Felderi Santiago
Technical Director - NA East, LATAM
Centrify Corporation

Community   Forums   TechBlog   TechCenter   TechVideos   Ideas   Tech Alerts   Developer   Resource

leoliou
Centrify Contributor II

Posts: 15
Registered: 07-08-2010

#8 of 17 6,778

01-21-2015 03:44 PM   Options

the issue is that within docker container, there is no init process. upstart is not working at all.

for example:
root@752b259cc603:/# initctl start rsyslogd; echo $?; ps -ef
0
UID   PID PPID C STIME TTY   TIME CMD
root   1   0 0 21:00 ?   00:00:00 bash
root   58   1 0 23:38 ?   00:00:00 ps -ef

notice bash has pid of 0, and init is no where to be seen.
notice also, that rc=0 from initctl, but rsyslogd is not started.

and then:
root@752b259cc603:/# /sbin/init 2
init: Failed to connect to socket /com/ubuntu/upstart: Connection refused

that is why adjoin complained that it cannot talk to adclient, because it is never started, even though when adjoin invoked initctl to start adclient, it got rc=0.
this is why starting adclient manually, everything just worked.

we will keep looking into this, but technically, this is docker issue as it appears upstart is crippled within docker container.

Report Inappropriate Content

Reply

5 **Kudos**

leoliou
Centrify Contributor II

Posts: 15
Registered: 07-08-2010

#9 of 17 6,777

01-21-2015 03:47 PM   Options

saw the typo in command, tried again:

root@752b259cc603:/# initctl start rsyslog; echo $?; ps -ef
0
UID   PID PPID C STIME TTY   TIME CMD
root   1   0 0 21:00 ?   00:00:00 bash
root   60   1 0 23:46 ?   00:00:00 ps -ef

note, bash is because of command:
root@leo-u1404-s64a:~# docker run -t -i myubuntu:cdc-installed bash

Report Inappropriate Content

Reply

5 **Kudos**

leoliou

#10 of 17 6,749

01-22-2015 11:33 AM   Options

Within it, use CMD directive to invoke a script that starts the services and applications you need when the container gets started.
you then invoke docker run with -d (detach) and -P (publish) to expose the container ports.

Report Inappropriate Content

Reply

○ Kudos ➕⭐

◄ Previous 1 2 Next ►

◄ Message Listing ◄ Previous Topic Next Topic ►

powered by Lithium

1.669.444.5200

✉ Contact Us

PRODUCTS

Identity Service

Privilege Service

Server Suite

Mac Management

Federal CAC Reader

Free Trials

Free Products

COMPANY

About Us

Blogs

Management

News and Events

Investors

Careers

Contact

SERVICES

Overview

Professional Services

Training

SUPPORT

Support Portal Login

Support Plans

Centrify Trust

Cloud Status

COMMUNITIES

Centrify

Developer

Express

RESOURCES

White Papers

Webinars

Demo Videos

Documentation