CUNY Academic Commons - Feature #2142

Setup for new WP installation for commonsinabox.org

2012-09-24 09:00 AM - Boone Gorges

Status:	Resolved		**Start date:**	2012-09-24
Priority name:	High		**Due date:**	
Assignee:			**% Done:**	0%
Category name:	Server		**Estimated time:**	0.00 hour
Target version:	Not tracked			

Description

Hi André,

Part of the Commons In A Box launch will include a public website that contains documentation as well as community space for support, sharing development ideas, etc. Currently, we are hosting commonsinabox.org on the Commons, but we'd like to migrate to a standalone WP installation, so we can have a separate BuddyPress community, with different logins, etc. I can do the software setup, but we'll need the server space set aside first.

1) New webroot directory. It doesn't much matter to me how this is set up. It's probably most secure (and maybe easiest for you?) if we have a new Linux user ('cbox', maybe), with a public_html subdirectory in the user's /home/ directory. (If this is a symlink that points somewhere else on the filesystem, that's OK by me.) We'll need some permissions tweaks to the WP installation so that Apache can read/write the necessary stuff, but that'll have to wait until after I set up WP.
2) A new database, and a new MySQL user with all privileges on it.
3) Change the current vhost setting for commonsinabox.org and its sister domains (listed here http://redmine.gc.cuny.edu/issues/1617) so that it points to this new directory. It's OK if commonsinabox.org has some downtime between the time when you switch it over and the time I set up the WP install - we see very little traffic anyway, and it'll just take me a few minutes to set up WP and migrate over our old content.

Because this is a production site, it probably makes the most sense to put it on main Commons server 146.96.128.200, but I'm not particular about this - whatever you think is best. My guess is that it will never be more than a low-traffic site, so there should be no resource issues (especially in the near future).

In the future, we'll probably want a staging mirror set up. But for now, it's probably easiest for our team to develop the site's content on the production site (we'll leave the unfinished stuff unpublished for now). That way, it'll be easy to create the staging site down the road by simply copying the database and doing the necessary search-and-replaces.

Marking this High priority, because I'd like to make sure our team has plenty of time to develop their content in the shared commonsinabox.org space. By the end of this week would be great. Thanks so much, André!

History

#1 - 2012-09-24 09:00 AM - Boone Gorges

- Subject changed from Setup for new WP installation to Setup for new WP installation for commonsinabox.org

#2 - 2012-09-24 09:20 AM - Matt Gold

Many thanks for starting this ticket, Boone, and thanks in advance for your thoughts and your work, André.

#3 - 2012-09-24 10:08 AM - local admin

Ok, no problem.

1. Added new local UNIX user:

```
[root@commons ~]# useradd cbox
[root@commons ~]#
[root@commons ~]# passwd cbox
Changing password for user cbox.
Enter new UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully.
```

2. Added remote login permission for new account:

```
account sufficient      pam_succeed_if.so user = cbox
```

...more soon.

#4 - 2012-09-24 10:12 AM - local admin

3. Copied ssh authorized keys from commons user to new user, to allow Boone to login passwordless.

```
[root@commons ~]# cp -R /home/commons/.ssh/ /home/cbox/
```

...more soon.

#5 - 2012-09-28 02:41 AM - Matt Gold

Thanks so much, André!

#6 - 2012-10-01 05:19 PM - Boone Gorges

Hi André,

Just wanted to touch base on this one. Had a chance to set up the new DB and mysql user for me yet? Once I've got that, and you've redirected the vhost, I think I'll be golden :)

#7 - 2012-10-02 09:05 AM - local admin

4. Generated new mySQL user and database named cbox.

#8 - 2012-10-02 09:33 AM - local admin

- Status changed from Assigned to Reporter Feedback

5. Generated public www directory, with full privileges assigned to cbox user:

```
[root@commons ~]# mkdir /home/cbox/www
[root@commons ~]# chmod -R 775 /home/cbox/www
[root@commons ~]# ll  /home/cbox/
total 4
drwxrwxr-x. 2 root root 4096 Oct  2 09:28 www
[root@commons ~]# chcon -t httpd_sys_content_t /home/cbox/
[root@commons ~]# chown -R cbox:cbox /home/cbox/
```

6. Re-configured vhost pointing to new directory:

```
<VirtualHost *:80>
        DocumentRoot /home/cbox/www
        ServerName commonsinabox.org
        ServerAlias commonsinabox.net commons-in-a-box.com commons-in-a-box.org commons-in-a-box.net commonsin
abox.com
        ServerSignature email
        DirectoryIndex index.php index.html index.htm
        CustomLog logs/cbox_log combined
        CustomLog logs/cbox_access_log common
</VirtualHost>
```

7. Reloaded Apache configuration:

```
[root@commons ~]# service httpd reload
Reloading httpd:
```

#9 - 2012-10-02 09:35 AM - local admin

Please let me know if there are any other ssh keys to be authorized for this account and let me know how it goes!

#10 - 2012-10-02 01:37 PM - Boone Gorges

- Status changed from Reporter Feedback to Assigned

Thanks, André!

I just checked out a copy of the WordPress codebase to the web directory. But when I try to access it at commonsinabox.org or any of its aliases, I get a 403: Forbidden.

Files are there, and should be readable by apache:

```
[cbox@commons www]$ ls -l /home/cbox/www/
```

```
total 164
-rw-rw-r--.  1 cbox cbox   395 Oct  2 13:34 index.php
-rw-rw-r--.  1 cbox cbox 19929 Oct  2 13:34 license.txt
-rw-rw-r--.  1 cbox cbox  9177 Oct  2 13:34 readme.html
-rw-rw-r--.  1 cbox cbox  4264 Oct  2 13:34 wp-activate.php
drwxrwxr-x. 10 cbox cbox  4096 Oct  2 13:34 wp-admin
-rw-rw-r--.  1 cbox cbox  1354 Oct  2 13:34 wp-app.php
-rw-rw-r--.  1 cbox cbox   271 Oct  2 13:34 wp-blog-header.php
-rw-rw-r--.  1 cbox cbox  3522 Oct  2 13:34 wp-comments-post.php
-rw-rw-r--.  1 cbox cbox  3177 Oct  2 13:34 wp-config-sample.php
drwxrwxr-x.  5 cbox cbox  4096 Oct  2 13:34 wp-content
-rw-rw-r--.  1 cbox cbox  2726 Oct  2 13:34 wp-cron.php
drwxrwxr-x.  9 cbox cbox  4096 Oct  2 13:34 wp-includes
-rw-rw-r--.  1 cbox cbox  1997 Oct  2 13:34 wp-links-opml.php
-rw-rw-r--.  1 cbox cbox  2395 Oct  2 13:34 wp-load.php
-rw-rw-r--.  1 cbox cbox 29084 Oct  2 13:34 wp-login.php
-rw-rw-r--.  1 cbox cbox  7712 Oct  2 13:34 wp-mail.php
-rw-rw-r--.  1 cbox cbox  9916 Oct  2 13:34 wp-settings.php
-rw-rw-r--.  1 cbox cbox 18299 Oct  2 13:34 wp-signup.php
-rw-rw-r--.  1 cbox cbox  3700 Oct  2 13:34 wp-trackback.php
-rw-rw-r--.  1 cbox cbox  2788 Oct  2 13:34 xmlrpc.php
```

Any ideas?

#11 - 2012-10-02 01:38 PM - local admin

Try now!

#12 - 2012-10-02 01:39 PM - Boone Gorges

Same:

```
Forbidden

You don't have permission to access /index.php on this server.

Additionally, a 403 Forbidden error was encountered while trying to use an ErrorDocument to handle the request
.
Apache/2.2.15 (Red Hat) Server at commonsinabox.net Port 80
```

#13 - 2012-10-02 01:40 PM - Dominic Giglio

From comment 8:

> [root@commons ~]# chown -R cbox:cbox /home/cbox/

Shouldn't that directory be owned by the apache user?

#14 - 2012-10-02 01:41 PM - local admin

Try now!

> Shouldn't that directory be owned by the apache user?

I believe just being readable is enough...

#15 - 2012-10-02 01:43 PM - Boone Gorges

> Try now!

Same 403 :(

#16 - 2012-10-02 01:45 PM - local admin

Hmm... I'm seeing an odd modsecurity warning:

```
[Tue Oct 02 13:44:11 2012] [error] [client 146.96.33.245] ModSecurity: Warning. Operator GE matched 5 at TX:ou
tbound_anomaly_score. [file "/etc/httpd/modsecurity.d/base_rules/modsecurity_crs_60_correlation.conf"] [line "
38"] [msg "Outbound Anomaly Score Exceeded (score 15): The application is not available"] [hostname "commonsin
abox.org"] [uri "/index.php"] [unique_id "UGsn65JggMgAAD4O-l0AAAD2"]
```

..let me see what I can dig up on that.

#17 - 2012-10-03 10:56 AM - local admin

I still haven't been able to figure out what exactly modsecurity doesn't like about this, but I went ahead and exempted the whole vhost not to hold development back.

#18 - 2012-10-03 10:57 AM - local admin

Ah, please let me know what files/folders should be writable by Apache.

#19 - 2012-10-03 02:36 PM - Boone Gorges

Hi André -

Getting close!

1) I was able to install WP. I then set up the installation as a Git checkout and attempted to push to Github. Linux threw an error about permissions on my .ssh directory:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@        WARNING: UNPROTECTED PRIVATE KEY FILE!        @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0755 for '/home/cbox/.ssh/id_rsa' are too open.
It is recommended that your private key files are NOT accessible by others.
This private key will be ignored.
bad permissions: ignore key: /home/cbox/.ssh/id_rsa
```

Could you sudo chmod that directory to 600? I'm pretty sure that's right.

2) Apache needs write permissions to:
- /home/cbox/www/wp-content/uploads
- /home/cbox/www/wp-content/blogs.dir

I'm thinking that the following setup will make it so that Apache can write there, and the cbox user will also be able to muck about as necessary in those directories:

```
chmod -R g+w /home/cbox/www/wp-content/uploads
chmod -R g+w /home/cbox/www/wp-content/blogs.dir
chgrp -R cbox /home/cbox/www/wp-content/uploads
chgrp -R cbox /home/cbox/www/wp-content/blogs.dir
chown -R apache /home/cbox/www/wp-content/uploads
chown -R apache /home/cbox/www/wp-content/blogs.dir
```

But you're the expert :)

#20 - 2012-10-03 02:46 PM - local admin

> Linux threw an error about permissions on my .ssh directory:

Ah ok, fixed it now.

> I'm thinking that the following setup [...]

Ok, went with that :)

#21 - 2012-10-03 09:22 PM - Boone Gorges

Hm, now I can't SSH in using my public key - I'm getting prompted for the cbox password, rather than for my public key password. Maybe 600 was not right?

#22 - 2012-10-04 02:54 AM - Matt Gold

Hi Boone,

The http://commonsinabox.org/ URL is live and it's a URL that is already circulating. is there anyway you can migrate our previous install (which I'm assuming is still available on the commons) there until we have thing set up as a real cbox install?

#23 - 2012-10-04 07:39 AM - Boone Gorges

I'll have the setup in place as soon as I can.

#24 - 2012-10-04 08:52 AM - local admin

    Maybe 600 was not right?

I'm pretty sure the permissions are ok, as I just copied what's there for commons where it presumably works ok.

Just to double-check, is this your public key?

```
AAAAB3NzaC1yc2EAAAABIwAAAQEAvNzSpxfdnnCNh4FQKtcncoOVxFOASaSpxG4sFEutRIafujMfI4cfosw6fmUTgZvqHp1jfDc8R0OwiNSXHb
CLK87UxfY8yf9I0s6Qbjyud0xmb90ix/VCzkrjt/0/UUjNSVSL71cHmhCdFkODGgyMRb8fmwdY7l3tgmBjIvm5zyq3ecxZD83jxB2PhJQe88RL
/mAiE9elIc8vOh0CcPTBII0s/Gv2JmQEECnEp8FHMsedzyCG0yctNLGZvMxoJXecR7pHYi8row75FOe/cGvY/h96S7cIBW22L4WmFtJgUSEqeI
hqoGvGsL7DsINFI6ZL4v4zmrtR/PEuTOCIt3aIx
```

Please try it with the -v flag and send me the output. Perhaps we can connect live via voice or chat and sort this out?

#25 - 2012-10-04 10:28 AM - Boone Gorges

Hi André -

```
$ ssh -v cbox@commonsinabox.org
OpenSSH_6.1p1, OpenSSL 1.0.1c 10 May 2012
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Connecting to commonsinabox.org [146.96.128.200] port 22.
debug1: Connection established.
debug1: identity file /home/bgorges/.ssh/id_rsa type 1
debug1: identity file /home/bgorges/.ssh/id_rsa-cert type -1
debug1: identity file /home/bgorges/.ssh/id_dsa type -1
debug1: identity file /home/bgorges/.ssh/id_dsa-cert type -1
debug1: identity file /home/bgorges/.ssh/id_ecdsa type -1
debug1: identity file /home/bgorges/.ssh/id_ecdsa-cert type -1
debug1: Remote protocol version 2.0, remote software version OpenSSH_5.3
debug1: match: OpenSSH_5.3 pat OpenSSH_5*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_6.1
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: server->client aes128-ctr hmac-md5 none
debug1: kex: client->server aes128-ctr hmac-md5 none
debug1: SSH2_MSG_KEX_DH_GEX_REQUEST(1024<1024<8192) sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
debug1: Server host key: RSA 63:02:8f:4d:56:19:e0:5e:4e:f8:c8:79:d0:65:cb:7e
debug1: Host 'commonsinabox.org' is known and matches the RSA host key.
debug1: Found key in /home/bgorges/.ssh/known_hosts:67
debug1: ssh_rsa_verify: signature correct
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Next authentication method: publickey
debug1: Offering RSA public key: /home/bgorges/.ssh/id_rsa
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Trying private key: /home/bgorges/.ssh/id_dsa
debug1: Trying private key: /home/bgorges/.ssh/id_ecdsa
debug1: Next authentication method: password
cbox@commonsinabox.org's password:
```

    Perhaps we can connect live via voice or chat and sort this out?

I can maybe connect up sometime in the mid-afternoon. I'll let you know. Thanks for your help so far :)

#26 - 2012-10-04 10:38 AM - local admin

Ok, but please give it one last try now if you have a moment. Thanks.

#27 - 2012-10-04 10:44 AM - local admin

I think the problem was that /home/cbox needed to be non-world-readable as well...

#28 - 2012-10-04 10:54 AM - Boone Gorges

Ok, but please give it one last try now if you have a moment. Thanks.

Sure - still the same problem.

#29 - 2012-10-05 03:26 PM - local admin

Sure - still the same problem.

Hmm... in order to run the website from /home/cbox/www, apache needs to be able to read /home/cbox, but it seems that ssh doesn't want anybody to be able to read it other than the owner. So I moved the website to /var/www/cbox instead, then reset the permissions on /home/cbox. Another try?

#30 - 2012-10-05 03:46 PM - Boone Gorges

Hm, still not working:

```
$ ssh cbox@commonsinabox.org -v
OpenSSH_6.1p1, OpenSSL 1.0.1c 10 May 2012
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: Connecting to commonsinabox.org [146.96.128.200] port 22.
debug1: Connection established.
debug1: identity file /home/bgorges/.ssh/id_rsa type 1
debug1: identity file /home/bgorges/.ssh/id_rsa-cert type -1
debug1: identity file /home/bgorges/.ssh/id_dsa type -1
debug1: identity file /home/bgorges/.ssh/id_dsa-cert type -1
debug1: identity file /home/bgorges/.ssh/id_ecdsa type -1
debug1: identity file /home/bgorges/.ssh/id_ecdsa-cert type -1
debug1: Remote protocol version 2.0, remote software version OpenSSH_5.3
debug1: match: OpenSSH_5.3 pat OpenSSH_5*
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_6.1
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: server->client aes128-ctr hmac-md5 none
debug1: kex: client->server aes128-ctr hmac-md5 none
debug1: SSH2_MSG_KEX_DH_GEX_REQUEST(1024<1024<8192) sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_GROUP
debug1: SSH2_MSG_KEX_DH_GEX_INIT sent
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY
debug1: Server host key: RSA 63:02:8f:4d:56:19:e0:5e:4e:f8:c8:79:d0:65:cb:7e
debug1: Host 'commonsinabox.org' is known and matches the RSA host key.
debug1: Found key in /home/bgorges/.ssh/known_hosts:67
debug1: ssh_rsa_verify: signature correct
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: SSH2_MSG_NEWKEYS received
debug1: Roaming not allowed by server
debug1: SSH2_MSG_SERVICE_REQUEST sent
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Next authentication method: publickey
debug1: Offering RSA public key: /home/bgorges/.ssh/id_rsa
debug1: Authentications that can continue: publickey,gssapi-keyex,gssapi-with-mic,password
debug1: Trying private key: /home/bgorges/.ssh/id_dsa
debug1: Trying private key: /home/bgorges/.ssh/id_ecdsa
debug1: Next authentication method: password
cbox@commonsinabox.org's password:
```

#31 - 2012-10-05 08:24 PM - local admin

So sorry, Boone. I did 600 instead of of 700 on /home/cbox/.ssh. To avoid any further hassle on this I added my own key to authorized_keys and verified it finally, definitely works. Go for it.

#32 - 2012-10-06 09:36 AM - Boone Gorges

Awesome, I am in! The 600 may have been my fault, I think I suggested it above :-/

Thanks :)

#33 - 2012-10-08 01:21 PM - Boone Gorges

Hi André - I've just set up the site, and I think we're just about done. The last thing is that we need to change permissions on certain directories that need to be Apache-writable. They are:

```
/home/cbox/www/wp-content/blogs.dir/
/home/cbox/www/wp-content/uploads/
```

I think the schema we've used in the past is: chown these dirs to apache, and make sure they're group-writable (and that the cbox user is a member of the group).

Thanks again for your patience and persistence with this one!

#34 - 2012-10-09 10:29 AM - local admin

hey Boone, no "problemo" and I thank you too :)

re: apache writability, I believe this is already set. Did it fail on testing?

```
bash-4.2# ssh commons
Last login: Fri Oct  5 20:09:50 2012 from cpe-72-229-162-211.nyc.res.rr.com
  _
 / `_  _ _  _ _  _  _   _
/_,/_// / // / //_// /_\

[root@commons ~]# ll /home/cbox/www/wp-content/
total 20
drwxrwxr-x.  2 apache cbox   4096 Oct  3 14:33 blogs.dir
-rwxr-xr-x.  1 cbox   apache   28 Oct  2 13:34 index.php
drwxr-xr-x. 12 cbox   apache 4096 Oct  8 11:55 plugins
drwxr-xr-x.  7 cbox   apache 4096 Oct  8 11:49 themes
drwxrwxr-x.  4 apache cbox   4096 Oct  8 11:56 uploads
[root@commons ~]# ll -d /home/cbox/www/wp-content/blogs.dir/
drwxrwxr-x. 2 apache cbox 4096 Oct  3 14:33 /home/cbox/www/wp-content/blogs.dir/
```

#35 - 2012-10-09 11:18 AM - Boone Gorges

- Status changed from Assigned to Resolved

Right you are, André! I never actually tested, I was just listing the next thing that needed to be done - didn't realize you would read my mind :)

Thanks again. Marking this ticket Resolved.

#36 - 2012-10-09 11:19 AM - local admin

You're very kind. Appreciated.

#37 - 2012-10-10 09:54 PM - Boone Gorges

- Status changed from Resolved to Assigned

Hey André - Scott was doing some work on commonsinabox.org and discovered that rewrite permalinks weren't working (eg http://commonsinabox.org/bbpress). I have an .htaccess file in the webroot that should do the work, but the permissions on it are a bit off. Maybe that's the problem? Would you mind having a look?

#38 - 2012-10-12 10:34 AM - local admin

It seems like there's some redirect issue with this:

```
[Fri Oct 12 10:33:36 2012] [error] [client 146.96.33.245] Request exceeded the limit of 10 internal redirects
due to probable configuration error. Use 'LimitInternalRecursion' to increase the limit if necessary. Use 'Log
Level debug' to get a backtrace.
```

#39 - 2012-10-12 10:36 AM - local admin

> I have an .htaccess file in the webroot that should do the work, but the permissions on it are a bit off. Maybe that's the problem?

I don't see anything wrong with the permission there...

```
[root@commons ~]# ll /home/cbox/www/.htaccess
-rwxrwxr-x. 1 cbox cbox 236 Oct  8 11:49 /home/cbox/www/.htaccess
```

#40 - 2012-10-15 10:12 AM - Boone Gorges

- Status changed from Assigned to Resolved

Turns out this was my fault - I created the .htaccess file locally, and then checked it into the git repo. So the rewrite rules were set up for my local machine, where I was visiting the site under a different URL. I've fixed the problem and the pages are now visible.

André, sorry for the confusion. Scott, it's all yours :)