

Accessing DigitalOcean Droplets via Command Line Using SSH Keys on OSX

As you get rolling with using DigitalOcean and other VPS providers, one of the features that many folks see in the configuration is the “user SSH key to access your instance” options. The trick is that many newcomers to using cloud instances aren’t totally comfortable or fully understand setting up an SSH key for password-less access to your instance.

Is it Secure Without a Password?

A resounding yes! In fact, it’s much more secure. You’ve uploaded the public side of your key to the instance already from within the cloud infrastructure and you’re now using the private side to match up for access. By not using a password, you’re removing the risk of sending authentication information over the public network. Brute force attacks are not as effective with public/private key pairs whereas they are successful in password hacking attempts.

It’s assumed that you’ve already uploaded your key. I won’t dig into all the different providers and ways to upload the keys. Make sure to do that for your individual provider to create and upload a key from your machine.

Adding your key to the SSH agent from the command line for OSX

When you launch your instance through the GUI, make sure that you have a SSH key selected to match the private key you have on your local machine. I’ve nicknamed mine as Eric-MacbookPro. For extra safety, I also keep copies of the keys in an offsite vault to ensure that I never lose access to

Add your SSH keys ?

New SSH Key



Eric-MacbookPro

the instances that are attached to that key.

When your DigitalOcean droplet is launched, the key is added as part of the init process. Once you have your IP address, you just have a quick process to run to set your key up. Because I use a key that is stored in a folder that isn’t the default, it has to be added to the ssh agent.

Run the `eval `ssh-agent -s`` command. NOTE: those are backspaces, not apostrophes. That character is found on the same key as the tilde (~) symbol.

The second command you run is `ssh-add [yourkeyname]` where [yourkeyname] is the full filename and path of your private key. IN my case, I have it stored in my Documents folder under a keys subfolder. This is my process:

```
ssh-add ~/Documents/keys/id_rsa
```

```
[Eric's-MacBook-Pro:Documents discoposse]$  
[Eric's-MacBook-Pro:Documents discoposse]$ eval `ssh-agent -s`  
Agent pid 5630  
[Eric's-MacBook-Pro:Documents discoposse]$ ssh-add ~/Documents/keys/id_rsa  
Identity added: /Users/discoposse/Documents/keys/id_rsa (/Users/discoposse/Docum  
ents/keys/id_rsa)  
[Eric's-MacBook-Pro:Documents discoposse]$
```

Connecting to your DigitalOcean Droplet via SSH with your Private Key

Now we simply run the command line ssh using the administrative account. For CentOS and Ubuntu on DigitalOcean, it is the root account. For CoreOS instances, you use the core account.

My Ubuntu instance is accessible now by the ssh root@ip-address:

```
[Eric's-MacBook-Pro:keys discoposse]$  
[Eric's-MacBook-Pro:keys discoposse]$ ssh root@162.243.18.7  
The authenticity of host '162.243.18.7' (162.243.18.7) can't be established.  
ECDSA key fingerprint is SHA256:LslxnclqimgGtj50FfVKr0yESqy2kEKIt1aVmZ  
Are you sure you want to continue connecting (yes/no)? yes  
Warning: Permanently added '162.243.18.7' (ECDSA) to the list of known hosts.  
Welcome to Ubuntu 16.04.1 LTS (GNU/Linux 4.4.0-57-generic x86_64)  
  
* Documentation:  https://help.ubuntu.com  
* Management:    https://landscape.canonical.com  
* Support:       https://ubuntu.com/advantage  
  
Get cloud support with Ubuntu Advantage Cloud Guest:  
http://www.ubuntu.com/business/services/cloud  
  
0 packages can be updated.  
0 updates are security updates.  
  
The programs included with the Ubuntu system are free software;  
the exact distribution terms for each program are described in the  
individual files in /usr/share/doc/*/copyright.  
  
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by  
applicable law.  
root@webserver:~#
```

Now you're in! Keep your keys safe, and keep your DigitalOcean droplets safe with those keys. Happy SSHing!