Mitchell Anicas
Nov 5, 2014

61 11

Share

How To Connect To Your Droplet with SSH

Tags: Getting Started, Linux Basics, DigitalOcean

Tutorial Series

This tutorial is part 1 of 3 in the series: New Ubuntu 14.04 Server Checklist
This tutorial is part 1 of 3 in the series: New CentOS 7 Server Checklist

Introduction

If you have recently created a DigitalOcean Droplet, and you are new to working with Linux servers, you will need to learn how to use SSH to connect to and manage it. SSH, which stands for *Secure Shell*, is an encrypted network protocol that is used to for, among other things, remote server login and command execution. It is the standard method used for accessing and interacting with Linux servers.

This quick tutorial will show you how to connect to your new Linux cloud server for the first time, by logging into it using an SSH client.

Prerequisites

The prerequisites section describes everything that you need know about to follow this tutorial. Of course, you will need to have created a new Droplet through the DigitalOcean Control Panel.

Server Information and Login Credentials

In order to connect to a remote Linux server via SSH, you must have following:

- **User name**: The remote user to log in as. The default admin user, or *Superuser*, on most Linux servers is `root`
- **Password and/or SSH Key**: The password that is used to authenticate the user that you are logging in as. If you added a public SSH key to your droplet when you created it, you must have the private SSH key of the key pair (and passphrase, if it has one)
- **Server IP address**: This is the address that uniquely identifies your server on the Internet, and can be found in your DigitalOcean Droplets page

If you did not add an SSH key to your Droplet when you created it, you should have received an email from DigitalOcean with the aforementioned connection information and credentials. The emailed password is temporary, and must be changed after the first login.

SSH Client Software

There are a variety of SSH clients that you can use to connect to a Linux server. We will cover the following two:

- **OpenSSH** *(Linux and Mac OS X)*: A collection of software that ships with most Unix-like operating systems that includes the `ssh` command
- **PuTTY** *(Windows)*: A free SSH client that can run on Windows, and is available for download on the PuTTY Download Page. `putty.exe` is the SSH client, and `puttygen.exe` should also be downloaded if you want to use SSH keys.

Web2PDF
converted by Web2PDFConvert.com

SSH Login as Root

Now that you have all of the required information and software, you are now ready to log in to your server for the first time. Make sure to only follow the instructions that are relevant to your SSH client.

Option 1: OpenSSH (Linux and Mac OS X)

The OpenSSH `ssh` client is a command-line tool, so open a Terminal window to get started.

Step 1—Initiate the Connection

At the command prompt, enter the following command to attempt to connect to your server as the `root` user (subsitute the highlight word with your server's IP address):

```
ssh root@SERVER_IP_ADDRESS
```

For example, if the server IP address was `123.234.123.234`, the command would look like this: `ssh root@123.234.123.234`.

The first time you attempt to connect to your server, you will likely see a warning that looks like this:

```
The authenticity of host '123.123.123.123 (123.123.123.123)' can't be established.
ECDSA key fingerprint is
79:95:46:1a:ab:37:11:8e:86:54:36:38:bb:3c:fa:c0.
Are you sure you want to continue connecting (yes/no)?
```

Go ahead and type `yes` to continue to connect. Here, your computer is telling you that the remote server is not recognized. Since this is your first time connecting, this is completely expected. Skip to step 2, Authentication.

If you happened to destroy a droplet directly prior to creating the one that you are connecting to, you may see a warning like this:

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
...
```

If this is the case, your new droplet probably has the same IP address as the old, destroyed droplet, but a different host SSH key. This is fine, and you can remove the warning, by deleting the old droplet's host key from your system, by running this command:

```
ssh-keygen -R SERVER_IP_ADDRESS
```

Now try connecting to your server again.

Step 2—Authenticate

The authentication step involves providing a password and/or a private SSH key to prove that you are authorized to log in as `root`.

If you **added an SSH key** to your Droplet, and you have the private key installed on your computer, OpenSSH will attempt to use the key to authenticate to the `root` account. If you used a key with a passphrase, you will need to provide the passphrase to complete the login process. At this point, if you are unable to log in, you may need to start your `ssh-agent` and add your SSH keys to it with the following command (assuming your key is called "id_rsa"), then go back to *Step 1*:

Web2PDF
converted by Web2PDFConvert.com

```
eval `ssh-agent -s`
ssh-add ~/.ssh/id_rsa
```

If you **did not add an SSH key** to your Droplet, you will be prompted for the temporary password, and you will also be required to change it. Follow these steps to complete the login process:

1. Copy the temporary password from the email, and paste it into the password prompt
2. At the `(current) UNIX password` prompt, paste in the temporary password again
3. At the `Enter new UNIX password` prompt, enter a strong password
4. At the `Retype new UNIX password` prompt, enter the same strong password that you just entered

Don't forget the new password that you set.

You're now logged in! Skip to the *Where To Go From Here?* section of this tutorial to read about what your next steps with your server should be.

Option 2: PuTTY (Windows)

Run `putty.exe` by double-clicking on it, which will start the program and take you to the configuration screen.

Note: These steps do not cover using SSH keys with PuTTY. If you need to use SSH keys with PuTTY, use PuTTYgen to generate and load keys. A tutorial on this subject can be found here: How To Use SSH Keys with PuTTY.

Step 1—Configure the Connection

To properly configure the the SSH connection in putty, ensure that the following settings are set:

- **Host Name (or IP address)**: Enter your server's IP address here
- **Port**: 22 (default)
- **Connection Type**: SSH (default)

You may now name and save this particular connection for future use by typing a name in the "Saved Sessions" field, and clicking "save".

Step 2—Initiate the Connection

To initiate the connection, double-click on the session name, and accept the security alert (this will only appear the first time you connect to a server).

Step 3—Authenticate

The authentication step involves providing the login credentials, the user name and temporary password, to connect to the server. Following the initial connection, you will be required to change the password.

Follow these steps to complete the login process:

1. At the `login as` prompt, enter `root`
2. At the `Password prompt`, enter the password that was emailed to you (copy and paste it)
3. At the `(current) UNIX password` prompt, paste in the temporary password again
4. At the `Enter new UNIX password` prompt, enter a strong password
5. At the `Retype new UNIX password` prompt, enter the same strong password that you just entered

Don't forget the new password that you set.

Web2PDF
converted by Web2PDFConvert.com

Where To Go From Here?

Congratulations! You are logged in to your server over SSH!

The next steps are to set up some basic security measures to protect your server from being compromised. These steps are covered in these distribution-specific tutorials:

- Initial Server Setup with Ubuntu 14.04
- Initial Server Setup with CentOS 7

Heart 61 Share Subscribe

Author:
Mitchell Anicas

Tutorial Series

New Ubuntu 14.04 Server Checklist

When creating a new Ubuntu 14.04 server, there are some basic steps that you should take to ensure that your server is secure and configured properly. The tutorial series covers connecting to your server and general security best practices, and provides links to articles that will help you start running your own web server or application.

1. How To Connect To Your Droplet with SSH — November 4, 2014
   ♡ 61 11 By Mitchell Anicas
2. Initial Server Setup with Ubuntu 14.04 — April 17, 2014
   ♡ 306 120 By Justin Ellingwood
3. Additional Recommended Steps for New Ubuntu 14.04 Servers — November 3, 2014
   ♡ 134 19 By Justin Ellingwood

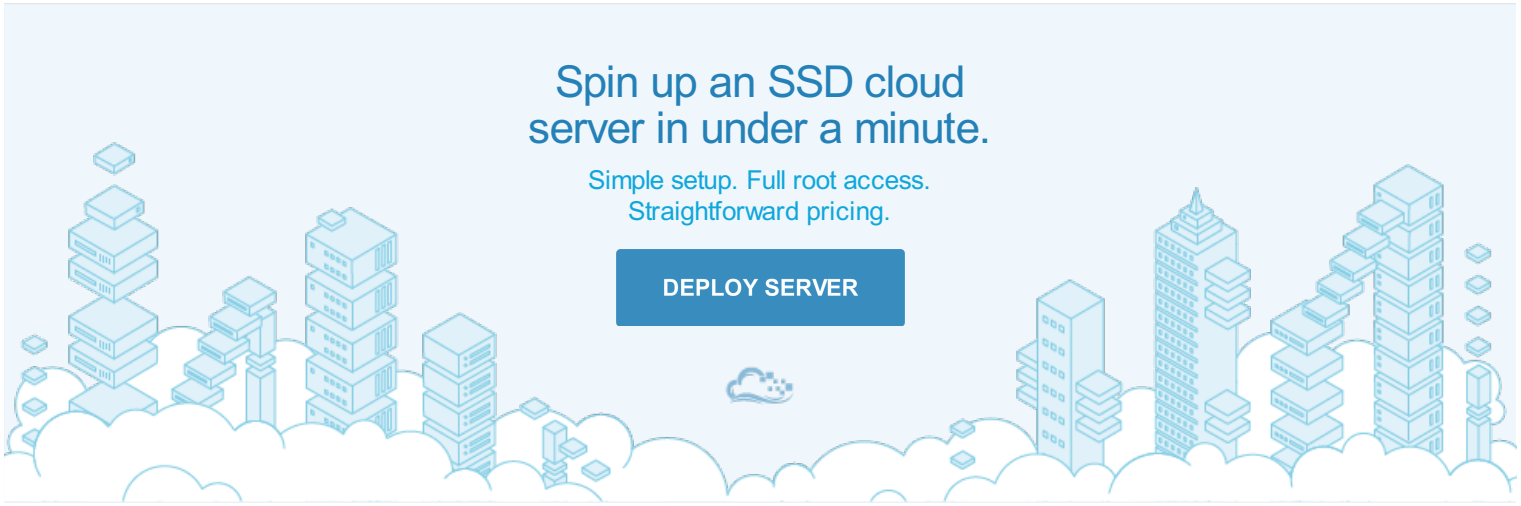
New CentOS 7 Server Checklist

When creating a new CentOS 7 server, there are some basic tasks that you should take to ensure that your server is secure and configured properly. The tutorial series covers connecting to your server and general security best practices, and provides links to articles that will help you start running your own web server or application.

1. How To Connect To Your Droplet with SSH — November 4, 2014
   ♡ 61 11 By Mitchell Anicas
2. Initial Server Setup with CentOS 7 — July 21, 2014
   ♡ 44 49 By Mitchell Anicas
3. Additional Recommended Steps for New CentOS 7 Servers — November 5, 2014

Web2PDF
converted by Web2PDFConvert.com

♡ 25 13 By Justin Ellingwood



Related Tutorials

Initial Server Setup with Debian 8

Automating the Deployment of a Scalable WordPress Site

Initial Setup of a Fedora 21 Server

How To Use the API to Deploy Droplets From a Master Snapshot

How To Resize Your Droplets on DigitalOcean

11 Comments

B I </> Leave a comment...

Log In to Comment

jnsyellow *November 16, 2014*

Every time I try and SSH I get this and it wont let me in:

Web2PDF
converted by Web2PDFConvert.com

```
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
-RSA KEY I HAVE TAKEN OUT-
Please contact your system administrator.
Add correct host key in /Users/Jonathan/.ssh/known_hosts to get rid of this message.
Offending RSA key in /Users/Jonathan/.ssh/known_hosts:6
RSA host key for -MY IP I TOOK OUT- has changed and you have requested strict checking.
Host key verification failed.

[Process completed]
```

I highly doubt I am getting attacked. I had tried installing a key previously and had to spin up a new server.

Also, I spun up a new server and tried doing no SHH, tried that and my connection got rejected?

♡ Reply

manicas MOD *November 17, 2014*

Did you delete and create a new server in a short amount of time? Each time a server is created, it generates a unique "host key". The first time you try and SSH to a server, your computer associates the IP address and host key in the `.ssh/known_hosts` file. Your computer probably has the old server's host key, and is warning you that the new server's host key doesn't match that.

To remove the warning, by deleting the original server's host key on your computer, use this command (replace the highlighted part with your server's IP address:

```
ssh-keygen -R <IP_ADDRESS>
```

After running this command, connect to your server as usual.

♡ 1

franciscojfs *December 2, 2014*

Hi Mitchell.

Thanks for the tutorial. Unfortunately I am facing a problem when trying to connect.

After providing the connection string `ssh root@xxx.xxx.xxx.xxx` I got a `Connection closed by xxx.xxx.xxx.xxx`.

I didn't create a droplet using SSH, but added a SSH later to my Digital Ocean control panel.

Also, when do a `cat /var/log/auth.log` I see some erros at the last lines, like `couldn't load host keys` and `No supported key exchange algorithms [preauth]`.

When I execute `ssh -vvv root@xxx.xxx.xxx.xxx` I get:

OpenSSH*6.2p2, OSSLShim 0.9.8r 8 Dec 2011*
*debug1: Reading configuration data /etc/ssh*config
debug1: /etc/ssh*config line 20: Applying options for **
*debug2: ssh*connect: needpriv 0
debug1: Connecting to xxx.xxx.xxx.xxx [xxx.xxx.xxx.xxx] port 22.
debug1: Connection established.
debug3: Incorrect RSA1 identifier
debug3: Could not load "/Users/lucasrezende/.ssh/id*rsa" as a RSA1 public key*
*debug1: identity file /Users/lucasrezende/.ssh/id*rsa type 1
debug1: identity file /Users/lucasrezende/.ssh/id*rsa-cert type -1*
*debug1: identity file /Users/lucasrezende/.ssh/id*dsa type -1
debug1: identity file /Users/lucasrezende/.ssh/id*dsa-cert type -1*
debug1: Enabling compatibility mode for protocol 2.0
*debug1: Local version string SSH-2.0-OpenSSH*6.2

Web2PDF
converted by Web2PDFConvert.com

debug1: Remote protocol version 2.0, remote software version OpenSSH*6.6.1p1 Ubuntu-2ubuntu2*
*debug1: match: OpenSSH*6.6.1p1 Ubuntu-2ubuntu2 pat OpenSSH*
debug2: fd 3 setting O*NONBLOCK*
*debug3: load*hostkeys: loading entries for host "xxx.xxx.xxx.xxx" from file "/Users/lucasrezende/.ssh/known*hosts"*
*debug3: load*hostkeys: loaded 0 keys
debug1: SSH2*MSG*KEXINIT sent
Connection closed by xxx.xxx.xxx.xxx

Do you have any idea of what could be happening?

Take care!!!

♡ Reply

nycJacob *December 27, 2014*

just created a ubuntu droplet without an ssh key. I logged in with password and then read about ssh keys. I have an ssh key from an AWS instance on my linux home system. I added that key to my droplet now but every time I ssh to my droplet it still asks for a password and doesn't seem to verify the key.

♡

manicas MOD *December 30, 2014*

If you are adding an already existing public SSH key (e.g. `id_rsa.pub`) to your server, follow step 3 of this tutorial How to set up SSH keys. Be sure to substitute the appropriate user, if you are not using `root`.

♡

nycJacob *December 31, 2014*

thanks I got it now

♡

TreadLightly *January 29, 2015*

If you aren't logging in with root I might add that you need to create a new user with the "adduser" command.

♡ Reply

fishb6nes *April 6, 2015*

I'm completely lost as to how to do a first time login on an Ubuntu 14.04x32 droplet where I did specifiy an SSH key on creation. It is still asking me for a password, which in this case was not emailed to me.

♡ Reply

manicas MOD *April 6, 2015*

Are you specifying `root` as the user, e.g. `ssh root@xxx.xxx.xxx.xxx`?

The other thing to check is if your private key exists, in the proper location. Assuming you called it "id*rsa", it should be located in your home directory at* `.ssh/id`rsa (`ls -la ~/.ssh/`). If it is in there, try running this command:

```
eval `ssh-agent -s`
ssh-add ~/.ssh/id_rsa
```

Then try connecting as root again.

♡ 1

fishb6nes *April 6, 2015*

nvm, this is what I was looking for https://www.digitalocean.com/community/tutorials/how-to-use-ssh-keys-with-putty-on-digitalocean-droplets-windows-users

Thanks nontheless!

♡ 1

wangshengbing *April 16, 2015*

but why i can not connect to my server by PuTTY ,the error is: network error,connection timed out,can you tell me how to solve this?

♡ Reply

Web2PDF
converted by Web2PDFConvert.com

Leave a comment...

Log In to Comment

This work is licensed under a Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License.

Copyright © 2015 DigitalOcean™ Inc.

Web2PDF
converted by Web2PDFConvert.com