Quickstart on AWS

Date of Publish: 2019-05-28

Contents

Prerequisites on AWS

In order to launch Cloudbreak from the CloudFormation template you must:

- Have an existing an AWS account.

  If you don't have an account, you can create one at https://aws.amazon.com/.
- Import an existing SSH key pair or generate a new SSH key pair in the AWS region which you are planning to use for launching Cloudbreak and clusters. If you don't have a key pair, you can create or import it by using the following steps:

  1. Navigate to the Amazon EC2 console at https://console.aws.amazon.com/ec2/.
  2. Check the region listed in the top right corner to make sure that you are in the correct region.
  3. In the left pane, find NETWORK AND SECURITY and click Key Pairs.
  4. Do one of the following:

     - Click Create Key Pair to create a new key pair. Your private key file will be automatically downloaded onto your computer. Make sure to save it in a secure location. You will need it to SSH to the cluster nodes. You may want to change access settings for the file using chmod 400 my-key-pair.pem.
     - Click Import Key Pair to upload an existing public key and then select it and click Import. Make sure that you have access to its corresponding private key.
- In order to access Cloudbreak web UI, you should use one of the following supported browsers: Chrome, Firefox, or Safari.

Related Information
Amazon EC2 key pairs (AWS)

Launch Cloudbreak from the quickstart template on AWS

Launch Cloudbreak from a CloudFormation template by using the following steps. This is the quickstart deployment option.

⚠️ **Attention:** As of December 31, 2021, Cloudbreak reached end of support. For more information, see Support lifecycle policy. Cloudera recommends that you migrate your workloads to CDP Public Cloud.

Note:

The quickstart option cannot be used with AWS GovCloud. You must use the production deployment option.

Steps

1. Click on the link to launch the CloudFormation template that will create the AWS resources, including an EC2 Instance runningCloudbreak:

Region	Link
us-east-1 (N. Virginia)	Launch the CloudFormation Template in US East
us-west-1 (N. California)	Launch the CloudFormation Template in US West (N. California)
us-west-2 (Oregon)	Launch the CloudFormation Template in US West (Oregon)
eu-central-1 (Frankfurt)	Launch the CloudFormation Template in EU Central
eu-west-1 (Dublin)	Launch the CloudFormation Template in EU West
sa-east-1 (São Paulo)	Launch the CloudFormation Template in South America
ap-northeast-1 (Tokyo)	Launch the CloudFormation Template in Asia Pacific (Tokyo)

Region	Link
ap-southeast-1 (Singapore)	Launch the CloudFormation Template in Asia Pacific (Singapore)
ap-southeast-2 (Sydney)	Launch the CloudFormation Template in Asia Pacific (Sydney)

2. The **Create stack** wizard is launched in the Amazon CloudFormation management console:

3. You do not need to change any template parameters on the Select Template page, but check the region name in the top right corner to confirm the region in which you want to launch Cloudbreak:

Note:

If needed, you may change the region if needed by using the dropdown in the top right corner.

4. Click Next to display the Specify Details page.

5. On the Specify Details page, enter the following information:

Parameter	Description
Specify Details section	
Stack name	Enter name for your stack. It must be unique in your AWS environment.
General Configuration section	
Controller Instance Type	EC2 instance type to use for the cloud controller.
Email Address	Username for the Admin login. Must be a valid email address.
Admin Password	Password for Admin login. Must be at least 8 characters containing letters, numbers, and symbols.
Security Configuration section	
SSH Key Name	Name of an existing EC2 key pair to enable SSH to access the instances. Key pairs are region-specific, so only the key pairs that you created for a selected region will appear in the dropdown.
Remote Access	Allow connections to the cloud controller ports from this address range. Must be a valid CIDR IP. For example: • 192.168.27.0/24 will allow access from 192.168.27.0 through 192.168.27.255. • 192.168.27.10/32 will allow access from 192.168.27.10. • 0.0.0.0/0 will allow access from all. Refer to Cloudbreak instance security groups for more information on the inbound ports that are used with Cloudbreak.

6. Click Next to display the Options page.

7. On he Options page, if you expand the Advanced section, there is an option to Rollback on failure.

   • By default, this option is set to Yes, which means that if there are any event failures when creating the stack, all the AWS resources created so far are deleted (i.e. rolled back) to avoid unnecessary charges.

   • If you set this option to No, if there are any event failures when creating the stack, the resources are left intact (i.e. not rolled back). Select the No option to aid in troubleshooting. Note that in this case you are responsible for deleting the stack later.

8. Click Next to display the Review page.

9. On the Review page, click the I acknowledge… checkbox.

10. Click Create.

> **Note:**
> The Stack Name is shown in the table with a CREATE_IN_PROGRESS status. You can click on the Stack Name and see the specific events that are in progress. The create process takes about 10 minutes and once ready, you will see CREATE_COMPLETE.
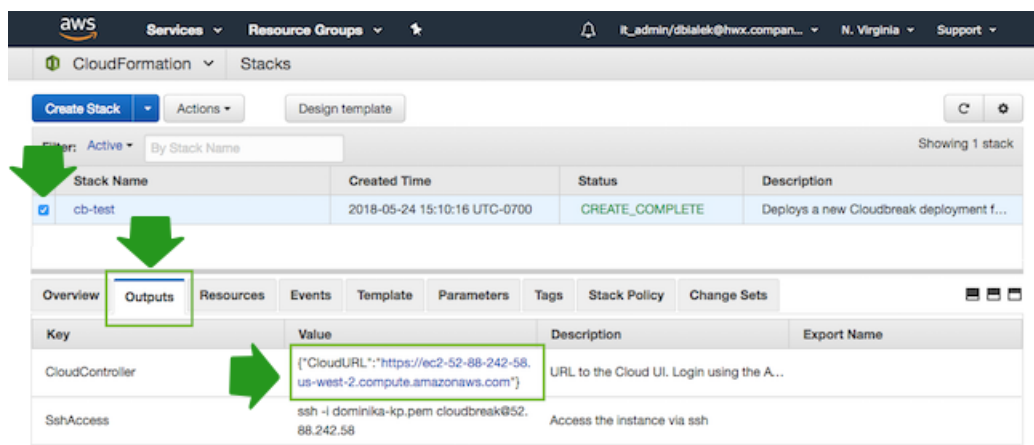
Related Information

CIDR IP calculator

Cloudbreak instance security group

Access Cloudbreak web UI on AWS

Follow these steps to obtain Cloudbreak VM's public IP address and log in to the Cloudbreak web UI.

Steps

1. Once the stack creation is complete, Cloudbreak is ready to use. You can obtain the URL to Cloudbreak from the Outputs tab:

Note:

If the Outputs tab is blank, refresh the page.

2. Paste the link in your browser's address bar.

   **a.** Confirm the security exception to proceed to the Cloudbreak web UI.

    The first time you access Cloudbreak web UI, Cloudbreak automatically generates a self-signed certificate, due to which your browser warns you about an untrusted connection and asks you to confirm a security exception.

Browser	Steps
Firefox	Click Advanced > Click Add Exception… > Click Confirm Security Exception
Safari	Click Continue
Chrome	Click Advanced > Click Proceed…

    b. The login page is displayed:
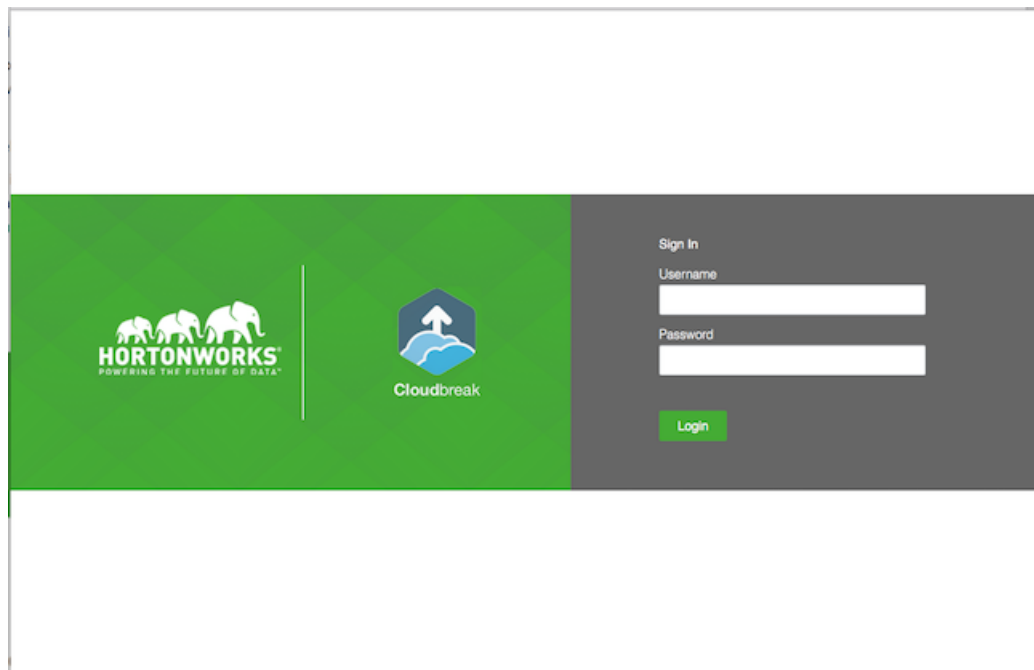
    c. Log in to the Cloudbreak web UI using the credential that you configured in the CloudFormation template.

    d. Upon a successful login, you are redirected to the dashboard:
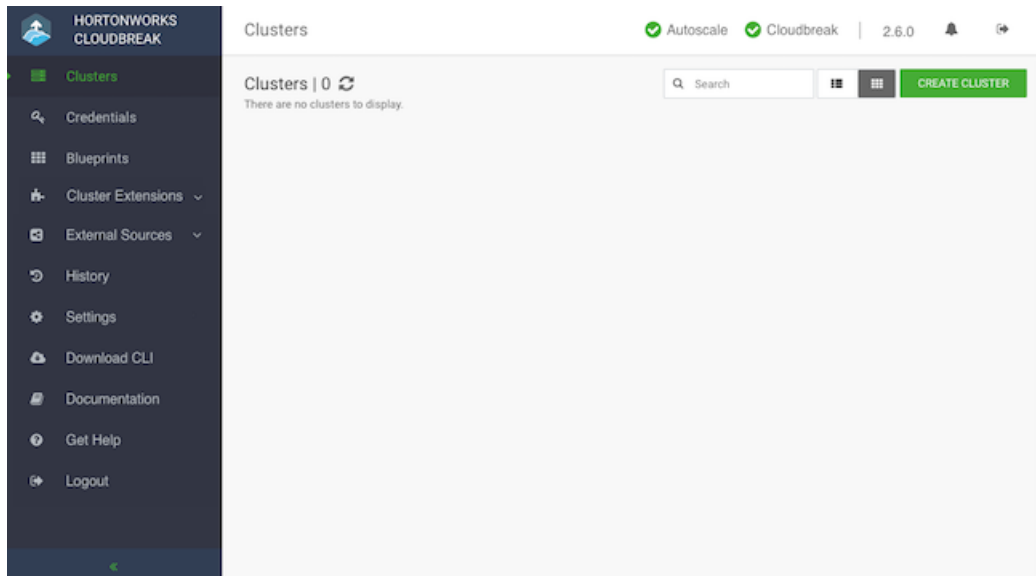
Next steps

After launching Cloudbreak, you must configure an external Cloudbreak database (if using Cloudbreak for production) and then create a Cloudbreak credential.

Configuring an external Cloudbreak database

By default, Cloudbreak, uses an embedded PostgreSQL database to persist data related to Cloudbreak, configuration and so on. This database is only suitable for non-production Cloudbreak, deployments. For production, you must configure an external Cloudbreak database.

Creating a Cloudbreak credential

This step is required. Only after you've performed it, you can start creating clusters. There are two ways to create a Cloudbreak credential on AWS. If you are just getting started with Cloudbreak, we recommend using the easier key-based credential method. For Cloudbreak credential options on AWS, refer to Credential options on AWS.

Related Information
External Cloudbreak database
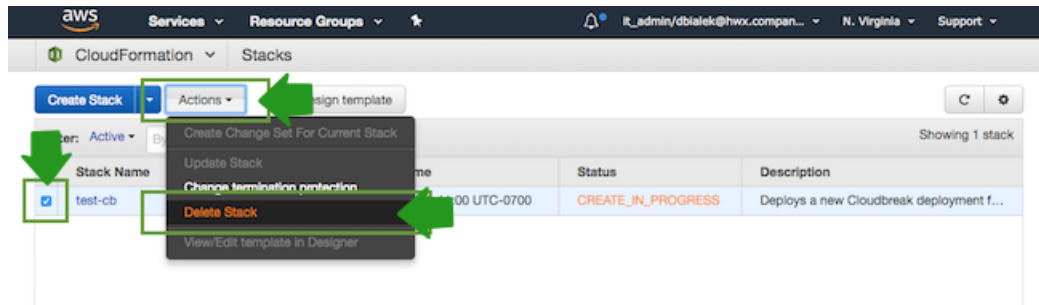Cloudbreak credential options on AWS

Delete Cloudbreak on AWS

If you want to delete Cloudbreak deployment, you can do so by deleting the stack in the CloudFormation console.

Steps

1. Log in to the CloudFormation console.
2. Select the deployment that you want to delete.
3. Select Actions > Delete Stack:

4. Click Yes, Delete to confirm.

All resources created as part of this stack (such as the Cloudbreak VM) will be deleted.