

Cloudbrink Connector - AWS

Cloudbrink's [Software Defined Mobility](#) enables enterprises to deliver best-in-class quality of experience and security for their end users in the new mobile-first and cloud-native world. Cloudbrink achieves this through three simple components:

1. The Brink Agent is installed on end user devices, with all major platforms supported.
2. Enterprise access points are automatically created via machine learning in close proximity to the end user, enabling Cloudbrink's revolutionary overlay protocol to overcome the most challenging last-mile network conditions, delivering best-in-class, high fidelity quality of experience for the end-user no matter the network they are connected to.
3. To provide end-to-end security, a Cloudbrink Connector is deployed in the customer's data center or cloud environment, creating a dark tunnel connection from the end user to their applications.

This document covers deploying the Cloudbrink Connector in an AWS environment.

Introduction

This document will guide you to create a Cloudbrink Connector in AWS. Steps 1 through 14 must be completed twice if deploying an active-standby Connector pair.

Prerequisites

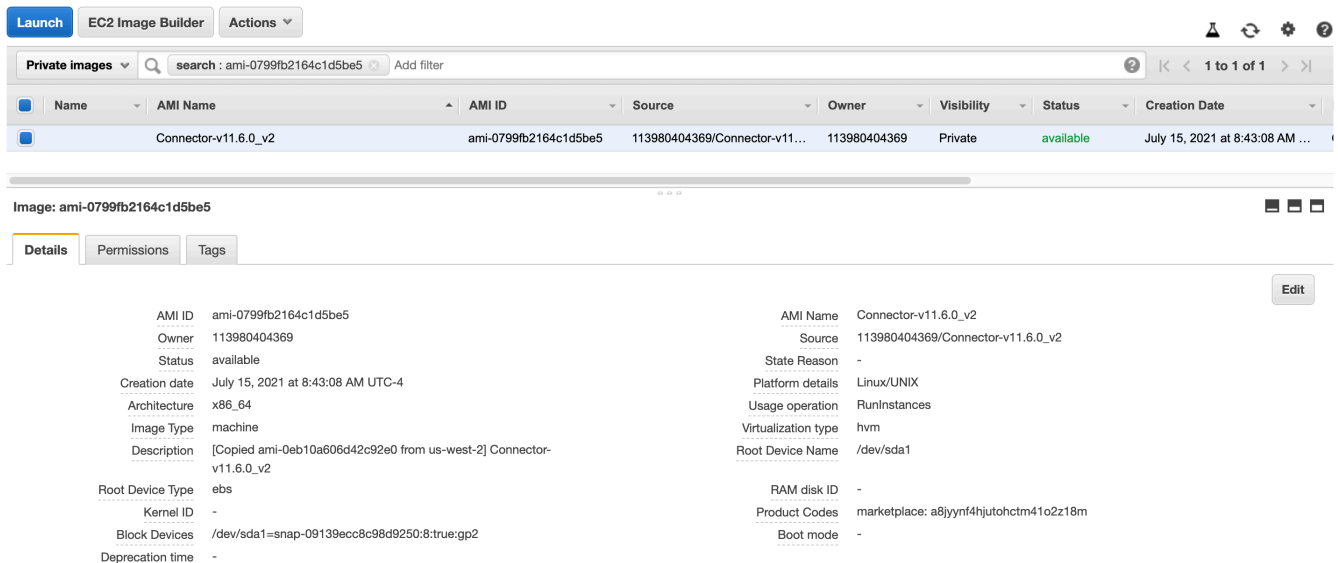
- An AWS account with necessary quota to deploy one (or two if active-standby pair) instance(s) with the below compute requirements
- Cloudbrink Connector AMI(s) have been shared your AWS Account (please notify Cloudbrink if additional regions are required)
- A Connector and corresponding OTP token has been generated in the Cloudbrink Admin Portal, or alternatively a cloud-init customization script has been separately provided by Cloudbrink

Connector VM Requirements

- OS: Ubuntu 20.04
- Compute: c5.xlarge (4 CPU and 8GiB RAM)
- Networking:
 - Inbound port 22 must be open between Connector instances if deploying an active-standby pair
 - Outbound ports 443 (TCP), and 9993-4 (UDP) to Cloudbrink SaaS and Edges
- Username: cbrink (required for hardening scripts)
- User Data cloud-init script

Create Connector VM from AWS AMI

1. Navigate to the **EC2** section of the AWS Console, and under **Images** in the left pane, select **AMIs**.
2. Search for the Connector AMI ID provided separately via email, and click the blue **Launch** button.



Launch EC2 Image Builder Actions

Private images search: ami-0799fb2164c1d5be5 Add filter

Name	AMI Name	AMI ID	Source	Owner	Visibility	Status	Creation Date
Connector-v11.6.0_v2	ami-0799fb2164c1d5be5	113980404369/Connector-v11...	113980404369	Private	available	July 15, 2021 at 8:43:08 AM ...	

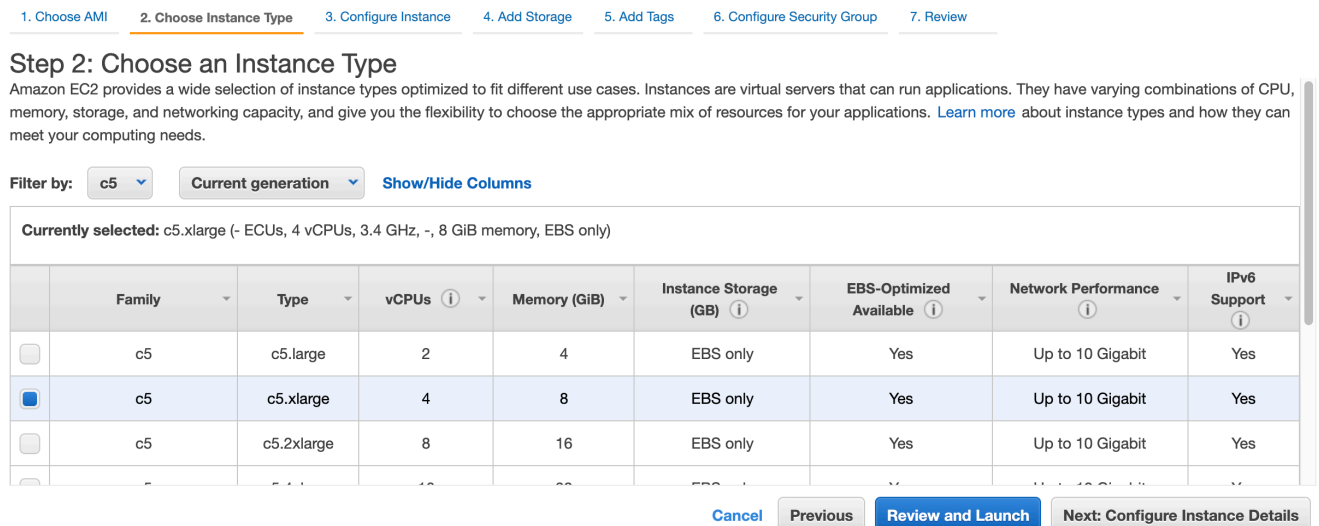
Image: ami-0799fb2164c1d5be5

Details Permissions Tags

AMI ID	ami-0799fb2164c1d5be5	AMI Name	Connector-v11.6.0_v2
Owner	113980404369	Source	113980404369/Connector-v11.6.0_v2
Status	available	State Reason	-
Creation date	July 15, 2021 at 8:43:08 AM UTC-4	Platform details	Linux/UNIX
Architecture	x86_64	Usage operation	RunInstances
Image Type	machine	Virtualization type	hvm
Description	[Copied ami-0eb10a606d42c92e0 from us-west-2] Connector-v11.6.0_v2	Root Device Name	/dev/sda1
Root Device Type	ebs	RAM disk ID	-
Kernel ID	-	Product Codes	marketplace: a8jymf4hjutohctm41o2z18m
Block Devices	/dev/sda1=snap-09139ecc8c98d9250:8:true:gp2	Boot mode	-
Deprecation time	-		

Edit

3. On **Step 2: Choose an Instance Type**, select **c5.xlarge**, and click the gray **Next: Configure Instance Details** button.



1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Step 2: Choose an Instance Type

Amazon EC2 provides a wide selection of instance types optimized to fit different use cases. Instances are virtual servers that can run applications. They have varying combinations of CPU, memory, storage, and networking capacity, and give you the flexibility to choose the appropriate mix of resources for your applications. [Learn more](#) about instance types and how they can meet your computing needs.

Filter by: c5 Current generation Show/Hide Columns

Currently selected: c5.xlarge (- ECUs, 4 vCPUs, 3.4 GHz, -, 8 GiB memory, EBS only)

	Family	Type	vCPUs	Memory (GiB)	Instance Storage (GB)	EBS-Optimized Available	Network Performance	IPv6 Support
<input type="checkbox"/>	c5	c5.large	2	4	EBS only	Yes	Up to 10 Gigabit	Yes
<input checked="" type="checkbox"/>	c5	c5.xlarge	4	8	EBS only	Yes	Up to 10 Gigabit	Yes
<input type="checkbox"/>	c5	c5.2xlarge	8	16	EBS only	Yes	Up to 10 Gigabit	Yes

Cancel Previous Review and Launch Next: Configure Instance Details

4. On **Step 3: Configure Instance Details**, ensure **Number of instances** is set to **1**, even if deploying an active-standby pair (each instance will have a unique OTP token).

- Still on **Step 3**, under the **Advanced Details** section, paste in the **User data** script as text, with the appropriate OTP Token for your environment. If unsure of this value, please contact Cloudbrink Support.

Example Script:

```
#cloud-config
runcmd:
  - [bash, /opt/scripts/brink_connector_deploy_cloud.sh, -o, "<OTP_TOKEN>", -a, "1"]
```

Advanced Details

Enclave ⓘ	<input type="checkbox"/> Enable
Metadata accessible ⓘ	Enabled
Metadata version ⓘ	V1 and V2 (token optional)
Metadata token response hop limit ⓘ	1
User data ⓘ	<input checked="" type="radio"/> As text <input type="radio"/> As file <input type="checkbox"/> Input is already base64 encoded

```
#cloud-config
runcmd:
  - [bash, /opt/scripts/brink_connector_deploy_cloud.sh, -o, "87c2b909-68a2-4bf6-84a3-a4f7132cd7c2", -a, "1"]
```

- Fill out the rest of **Step 3** per business requirements, and then click **Next: Add Storage**.
- On **Step 4: Add Storage**, change the **Size** value from 8 GiB to **50 GiB**.

1. Choose AMI
2. Choose Instance Type
3. Configure Instance
4. Add Storage
5. Add Tags
6. Configure Security Group
7. Review

Step 4: Add Storage

Your instance will be launched with the following storage device settings. You can attach additional EBS volumes and instance store volumes to your instance, or edit the settings of the root volume. You can also attach additional EBS volumes after launching an instance, but not instance store volumes. [Learn more](#) about storage options in Amazon EC2.

Volume Type ⓘ	Device ⓘ	Snapshot ⓘ	Size (GiB) ⓘ	Volume Type ⓘ	IOPS ⓘ	Throughput (MB/s) ⓘ	Delete on Termination ⓘ	Encryption ⓘ
Root	/dev/sda1	snap-09139ecc8c98d9250	50	General Purpose SSD (gp2)	150 / 3000	N/A	<input checked="" type="checkbox"/>	Not Encrypt

Cancel
Previous
Review and Launch
Next: Add Tags

- Click the gray **Next: Add Tags** button.
- On **Step 5: Add Tags**, add any required tags per business requirements.
- Click the gray **Next: Configure Security Group** button.
- Configure the instance security group per business requirements. All Connector communication happens in the outboud direction (it must be able to talk outwards to

Cloudbrink Edges and SaaS), so opening inbound ports from the internet is not required.

12. Click the blue **Review and Launch** button.
13. Ensure all settings match the above steps and business requirements. Click **Launch**.
14. In the key pair pop-up, either generate a new key pair or use an existing pair for SSH access, per business requirements. The Connector instance is hardened, with SSH only supported for the user `cbrink`. Click **Launch Instance**.