

# **Cisco Spaces: Connector AMI**

• Launch Connector 3 as an EC2 Instance from AMI , on page 1

## Launch Connector 3 as an EC2 Instance from AMI

This chapter provides information about how to launch a connector 3 as an EC2 instance from Amazon Machine Images (AMI), configure the connector 3 instance, and finally obtain a URL to log in to the connector connector and CLI.

Step 1 Log in to your Amazon Web Services account and navigate to the EC2 Dashboard. In the left-navigation pane, choose Images > AMI Catalog.

Step 2 In the AMIs search area, click AWS MarketPlace AMIs and enter DNA Spaces Connector. Press Enter.

## Figure 1: Configuration



- **Step 3** Click the displayed image and click **Select**.
- Step 4 In the Cisco DNA Spaces Connector window displayed, click Continue.

## Figure 2: AWS MarketPlace AMIs

Overview			
	Product details Pricing	Usage Support	
he Cisco DNA Sp vithout missing a	aces: Connector enables Cisco DNA : ny client information	Spaces to communicate with multiple controllers eff	iciently, by allowing each controller to transmit client da
ypical total price		Latest version	Video
0.093/Hr		Cisco DNA Spaces Connector3 October2023	Product Video 🖸
otal pricing per inst	ance for services hosted on t2.large in	Delivery methods	Categories
s-east-1. ee additional pricin	g information.	Amazon Machine Image (i) Operating systems	Network Infrastructure
		Other AlmaLinux 8	
		CentOS 7	

Step 5 In the Image Summary window displayed, click Launch Instance from AMI

## Figure 3: Launch Instance from AMI

EC2 > AMIs > ami-0fd326aca1b04cf96			
Image summary for ami-Ofd326aca1b04cf96 (	Connector3-b84-Jan-QA-Img)	🔀 EC2 Image Bu	ilder Actions <b>V</b> Launch instance from AMI
AMI ID D ami-Ofd326aca1b04cf96 (Connector3-b84-Jan-QA-Img)	image type machine	Platform details Linux/UNIX	Root device type EBS
AMI name  Crisco-dna-spaces-connector3-b84-jan2023-8.4.0-22- DEV	Owner account ID	Architecture x86_64	Usage operation Runinstances
Root device name	Status Ø Available	Source D 038249548279/cisco-dna-spaces-connector3-b84- jan2023-8.4.0-22-DEV	Virtualization type hvm
Boot mode -	State reason -	Creation date	Kernel ID -
Block devices Block devices devices devices devices Block devices	Description	Product codes	RAM disk ID -
Deprecation time -	Last launched time –		

**Step 6** In the Launch an Instance window displayed, enter an instance name, and add any additional labels for your instance by clicking the Add Additional tags button.

#### Figure 4: Launch Instance from AMI

Jer Services	<b>Q</b> Search				[Option+S]	
Launch Amazon EC2 a following the	allows you to simple steps	create virtual ma below.	chines, or instances	5, that run on the A	WS Cloud. Quick	ly get started by
Name aı	nd tags In	fo				
Name	7 414 0				Add	dditional tags
Connecto	ors-Ami-Dev-	Instance- I			Add a	autional tags
Q Se	arch our full d	catalog including	1000s of applicatio	n and OS images		
Q Se	arch our full o	Recents	1000s of applicatio	n and OS images Quick Start		
Q se	arch our full d from catalog	age (AMI)	1000s of applicatio	n and OS images Quick Start		Q
Amazor connect ami-086	arch our full o from catalog n Machine Im- tor3-packer-a dd6727207b	atalog including Recents age (AMI) Ilmalinux-ami-dev 37c54	1000s of applicatio	n and OS images Quick Start	Bro Incl AWS t	Q wse more AMIs uding AMIs from Marketplace and he Community
Ami Amazor connect ami-084	n Machine Ima tor3-packer-a dd6727207b	atalog including Recents age (AMI) Ilmalinux-ami-dev 37c54	1000s of application	n and OS images Quick Start Root device	Bro Incl AWS t ENA Enabled	Q wse more AMIs uding AMIs from , Marketplace and he Community

Step 7Choose an instance with the corresponding Type as t2.medium that has vCPU value as 2 and Memory (GB) as 4.<br/>Click Next: Configure Instance Details.

t2.medium corresponds to a standard window with 2vCPUs and 4-GB memory and is the recommended setting.

#### Figure 5: Configure Instance Details

aws	Services	Q Search [	Option+S]
=	▼ Instar	ice type Info	
	Instance type		
	<b>t2.mediun</b> Family: t2 On-Deman On-Deman	n 2 vCPU 4 GiB Memory d Linux pricing: 0.0454 USD per Hour d Windows pricing: 0.0644 USD per Hour	Compare instance types
	▼ Key p	air (login) Info use a key pair to securely connect to your instance. Ensure that you have access to the	selected key pair before you launch
	the insta	nce.	
	connector	-ami-test-key	C Create new key pair

- **Note** You can have a more advanced configuration by choosing an option with higher vCPU and memory, by choosing an instance type with one of the following configurations. If an exact match is unavailable, you can choose a configuration with the next-available vCPU or memory:
  - 4 vCPUs and 8-GB memory (referred to in this document as Advanced1)
  - 8 vCPUs and 16-GB memory (referred to in this document as Advanced2)

Step 8 Choose a Network and a Subnet. Click Next: Add Storage.

## Figure 6: Add Storage

<ul> <li>Network settings</li> </ul>	Info				
/PC - required Info					
vpc-	·····		•	C	
Subnet Info					
automat.		eV			
subnet-				$\sim$	
VPC: vpc-02	Owner: 199547563901		•	G	Create new subnet 🗹

**Step 9** Enter the value of **Size(GB)** as 120. Click **Next: Configure Security Group**.

## Figure 7: Configure Storage

▼ Configure storage Info	Advanced
1x 120 GiB gp2 ▼ Root volume (Encrypted) Add new volume	
0 x File systems	Edit

- **Step 10** Configure a security group by following these steps:
  - a) Create a new security group or modify an existing one by clicking the respective radio button.

aws	Services Q Search	[Option+S]
=	▼ Network settings Info	Edit
	Network Info vpc- Not used - defau	t
	Subnet Info No preference (Default subnet in any availat Auto-assign public IP Info Enable	ility zone)
	Firewall (security groups) Info A security group is a set of firewall rules that contro instance. Create security group	the traffic for your instance. Add rules to allow specific traffic to reach your Select existing security group
	Security groups Info	
	Select security groups	Compare security
	launch-wizard-69 sg-( VPC: vpt	r X group rules

b) Configure rules permitting inbound traffic to specific ports, as shown in the following image. You can allow inbound traffic to these ports for all IP addresses or choose to restrict them for specific IP addresses.

Figure 9: Configure These Inbound Rules Permitting Traffic to Specific Ports

lr I	bound rules (6 Q Filter security gr	5) roup rules				C Manage tags	Edit inbound rules
	Name	$\nabla$	Security group rule $\nabla$	IP version	⊽ Туре	⊽ Protocol	
	-		sgr-0497e0b5ee57ae7	IPv4	HTTPS	ТСР	443
	-		sgr-0b120f3989c477140	IPv4	Custom UDP	UDP	2003
	-		sgr-084f5c1391adb52fa	IPv4	Custom TCP	ТСР	8000
	-		sgr-02070569e30bbd	IPv4	Custom UDP	UDP	161
	-		sgr-0bb0c8051cee0daf8	IPv4	SSH	ТСР	22
	-		sgr-0c502fa77173670d8	IPv4	Custom TCP	TCP	8004

- **Note** Using an inbound rule, you can also specify the network subnet range that can access this instance (For example, through SSH).
- c) Configure the outbound rule shown in the following image.

## Figure 10: Configure This Outbound Rule

Inbound rules	Outbound rules Tag	IS			
<ol> <li>You can now</li> </ol>	check network connectivity wi	th Reachability Analyzer		Run Reach	nability Analyzer X
Outbound ru	<b>les</b> (1/1)			C Manage tags	Edit outbound rules
<b>Q</b> Filter securit	ty group rules				< 1 > @
IP version	⊽ Туре	▼ Protocol		▽ Destination	
IPv4	All traffic	All	All	0.0.0/0	-

- **Note** For various connector services to work, you must open specific ports. See the respective **Information About Open Ports** section of the connector service for more information.
- **Step 11** In the displayed **Select an existing key pair or create a new key pair** dialog box, do either of the following:
  - Choose **Create a new key pair** from the drop-down list. Provide a **Key pair name** and click **Download Key Pair** to download it. Then click **Launch Instance** to launch the instance.
  - Choose **Choose an existing key pair** from the drop-down list. Select the previously downloaded key pair from the **Select a key Pair** drop-down list. Then click **Launch Instance** to launch the instance.

1. Choose AMI Step 7: F	2. Choose Instance Type Review Instance	3. Configure Ins	tance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review				
All select	ed security groups inbou	and rules					
Туре 🤅		Protoco		Des	cription (i)		
HTTP		TCP	Select an existing key pair or create a new key pair ×				
HTTP		TCP		-			
Custom	TCP Rule	TCP	A key pair consists of a public key that AWS stores, and a private key file that you store. Together,				
Custom	TCP Rule	TCP	they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the paseword used to lea into your instance. For Linux AMIs, the private key file allows you to				
Custom	TCP Rule	TCP	securely SSH into your instance.				
Custom	TCP Rule	TCP					
SSH		TCP	Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more				
SSH		TCP	about removing existing key pairs norm a public Alvin.				
HTTPS		TCP	Create a new key pair				
HTTPS		TCP	Key1				
ALICME	- IPv4	All	Download Key Pair				
All ICME	- IPv4	All					
<ul> <li>Instance</li> </ul>	Details	Pui	You have to download the private key file (".pern file) before you can continue. Store it in a secure and accessible location. You will not be able to download the file again after it's created.			Ed	t instance details
Storage							Edit storage
▶ Tags			Cancel Launch Instances				Edit tags
						Cancel Pre	vious Launch

Figure 11: Create a New Key Pair

#### Figure 12: Choose an Existing Key Pair

se AMI 2. Choose Instance Ty	vpe 3. Configure Inst	ance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review			
7: Review Instand	ce Launch				
selected security groups inb	ound rules				
/pe 🕕	Protoco		Description (i)		
ПТР	TCP	Select an existing key pair or create a new key pair ×	-		
TP	TCP				
ustom TCP Rule	TCP	A key pair consists of a public key that AWS stores, and a private key file that you store. Together,			
stom TCP Rule	TCP	they allow you to connect to your instance securely. For Windows AMIs, the private key file is required to obtain the password used to log into your instance. For Linux AMIs, the private key file allows you to			
stom TCP Rule	TCP	securely SSH into your instance.			
stom TCP Rule	TCP				
н	TCP	Note: The selected key pair will be added to the set of keys authorized for this instance. Learn more about removing existing key pairs from a public AMI			
Η	TCP				
TPS	TCP	Select a key pair			
TPS	TCP	ConnectorAMI			
ICMP - IPv4	All	I acknowledge that I have access to the selected private key file (ConnectorAMI.pem), and			
I ICMP - IPv4	All	that without this file, I won't be able to log into my instance.			
ance Details		Cancel Launch Instances		Edit	instance de
rage					Edit sto

**Step 12** After you have downloaded the key pair (.pem) file to your system, navigate to the file location. Configure appropriate permissions for the .PEM file using the **chmod** command.

chmod 400 /path/to/MyAccessKey1.pem

**Step 13** Review the instance and click **Launch**.

Figure 13: Review Instance and Launch

Number o	f instances Info
1	
Software	Image (AMI)
<b>cisco-dna-</b> ami-0ff1550	•spaces-connector3-b8read more 022ef237286
Virtual ser	rver type (instance type)
t2.mediun	n
Circurall /-	
FILEWALL (S	ecurity aroun)
eWLC	ecurity group)
eWLC	ecurity group)
eWLC Storage (v	ecurity group) rolumes)
eWLC Storage (v 1 volume(	ecurity group) rolumes) s) - 120 GiB
eWLC Storage (v 1 volume(	rolumes) s) - 120 GiB e tier: In your first year includes 750
Firewall (S eWLC Storage (v 1 volume( i Fre hou	ecurity group) volumes) s) - 120 GiB e tier: In your first year includes 750 × urs of t2.micro (or t3.micro in the
eWLC Storage (v 1 volume( Fre hou Reg inst	e tier: In your first year includes 750 urs of t2.micro (or t3.micro in the pions in which t2.micro is unavailable) ance usage on free tier AMIs per
Firewall (S eWLC Storage (v 1 volume( ist Reg inst mo	ecurity group) volumes) (s) - 120 GiB e tier: In your first year includes 750 urs of t2.micro (or t3.micro in the pions in which t2.micro is unavailable) :ance usage on free tier AMIs per nth, 30 GiB of EBS storage, 2 million
Firewall (S eWLC Storage (v 1 volume( int Reg inst mo IOs	ecurity group) rolumes) (s) - 120 GiB e tier: In your first year includes 750 urs of t2.micro (or t3.micro in the pions in which t2.micro is unavailable) :ance usage on free tier AMIs per nth, 30 GiB of EBS storage, 2 million , 1 GB of snapshots, and 100 GB of
eWLC Storage (v 1 volume( ist Reg inst mo IOs bar	ecurity group) volumes) (s) - 120 GiB e tier: In your first year includes 750 urs of t2.micro (or t3.micro in the pions in which t2.micro is unavailable) :ance usage on free tier AMIs per nth, 30 GiB of EBS storage, 2 million , 1 GB of snapshots, and 100 GB of indwidth to the internet.

**Step 14** On the EC2 dashboard, wait for the instance to finish launching and the status to change to **Running**. Alternatively, you can see the running instances on the **Instances** page. Click the instance to obtain the IPv4 address of the instance.

#### Figure 14: Obtain IPv4 Address of Instance

Services Q Search	[Option+S]	D A <sup>*</sup> Ø N. Virginia ▼
Instances (1/1) Info		C Connect Instance state V Actions V Launch instances V
Q. Find instance by attribute or tag (case-sensitive)		< 1 > @
Instance ID = I-094538a13d1d19edf X Clear filters		
✓ Name ▼ Instance I	D Instance state v I Instance type v I Status o	check   Alarm status   Availability Zone V   Public IPv4 DNS V   Public IPv4
Connector3-AMI-Dev-Instance-1 i-094538a	13d1d19edf ⊘ Running ® ⊖ t2.medium ⊘ 2/2 o	checks passed No alarms + us-east-1f
Instance: i-094538a13d1d19edf (Connector3-AMI-Dev-	instance-1) =	⊗ >
▼ Instance summary Info		
Instance ID i-094538a13d1d19edf (Connector3-AMI-Dev-Instance-1)	Public IPv4 address open address	Private IPv4 addresses
IPv6 address	Instance state	Public IPv4 DNS
-		🗇 ec 🛛 open address 🗹
Hostname type	Private IP DNS name (IPv4 only)	
IP name: ternal	🗇 ip- nternal	
Answer private resource DNS name	Instance type	Elastic IP addresses
IPv4 (A)	t2.medium	-
Auto-assigned IP address	VPC ID	AWS Compute Optimizer finding
ablic IP]	0 (it) 🖸	🚯 Opt-in to AWS Compute Optimizer for recommendations.   Learn more 🖄
IAM Role	Subnet ID	Auto Scaling Group name
-	0	-
▼ Instance details Info		
Platform	AMLID	Monitoring
Linux/UNIX (Inferred)	G •	disabled
Platform details	AMI name	Termination protection

- **Step 15** Perform initial setup to configure a hostname, and change passwords for **spacesadmin** and **root** users.
  - a) Log in to the connector using the ssh -i command and the following parameters:
    - The .PEM key pair downloaded in Step 11
    - ec2-user
    - The IPv4 address obtained in Step 14

ssh -i /path/to/key/MyAccessKey1.pem ec2-user@IPv4-address

- b) Change passwords for **spacesadmin** and **root** users. Avoid a BAD PASSWORD prompt by complying with the following password requirements:
  - Length is more than 14 characters.
  - Includes at least one uppercase letter.
  - · Includes at least one lowercase letter.
  - Includes at least one special character.

The following is a sample output of the command:

```
Welcome to Cisco Spaces Connector Setup
Changing password for user spacesadmin.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
Password changed successfully
Setting rbash...
Restarting docker...
Changing shell for root.
Shell changed.
Changing shell for spaces.
```

```
Remove default users...
Relabeled /etc/sudoers from unconfined_u:object_r:user_tmp_t:s0 to unconfined_u:object_r:etc_t:s0
```

Cisco Spaces Connector UI: https://XX.XXX.XXX Username log in: spacesadmin The install is complete, a reboot will occur in 10 seconds...

Once the installation is complete, a reboot occurs within 10 seconds. Note down the public IP address before reboot.

**Step 16** Log in to the connector and configure the connector further. Do one of the following using the public IPv4 address from the previous step (Step 15):

- Log in to the connector GUI using the browser window and the address https://public-ipv4-address
- Log in to the connector CLI using the SSH command and the username **spacesadmin**. Use the command **ssh spacesadmin**@*public-ipv4-address*. When prompted, use the password configured for the **spacesadmin** user.