



StrongDM + AWS Workshop

July 31, 2025



John Martinez
Technical Evangelist
StrongDM



Ashok Mahajan
Sr Partner SA
AWS



Catherine Lo
Sr Solutions Engineer
StrongDM

Meet the Team



Mario Perozo
Sr Solutions Engineer
StrongDM

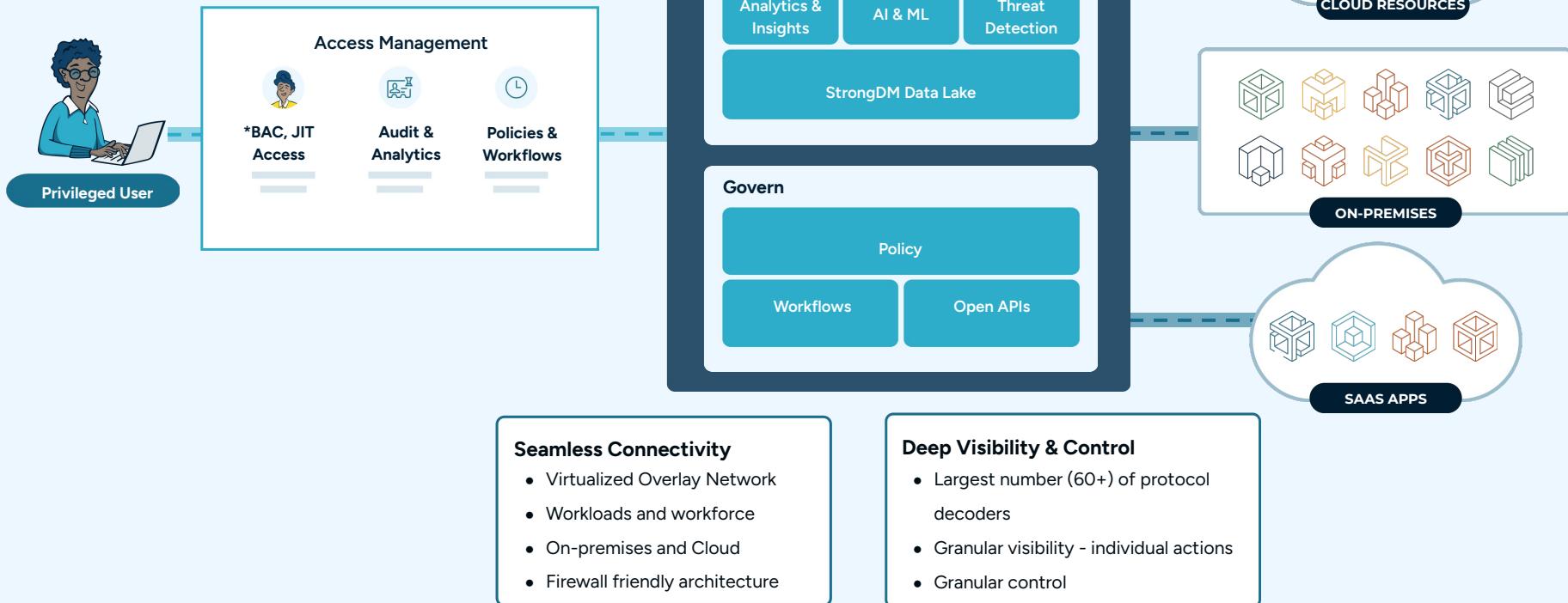
Housekeeping

- All content material is in the Resources tab (and GitHub)
- When in doubt, ask the team
- Please ask questions in the Q&A tab
- The StrongDM tenant is shared, please clearly identify your resources, and do not modify others'
- GitHub rep link: <https://github.com/strongdm/aws-workshops>
- Both the AWS account and StrongDM tenant will be available until 3pm PT today
- Duration of live session is 1.5 hours, but will be flexible if help is needed

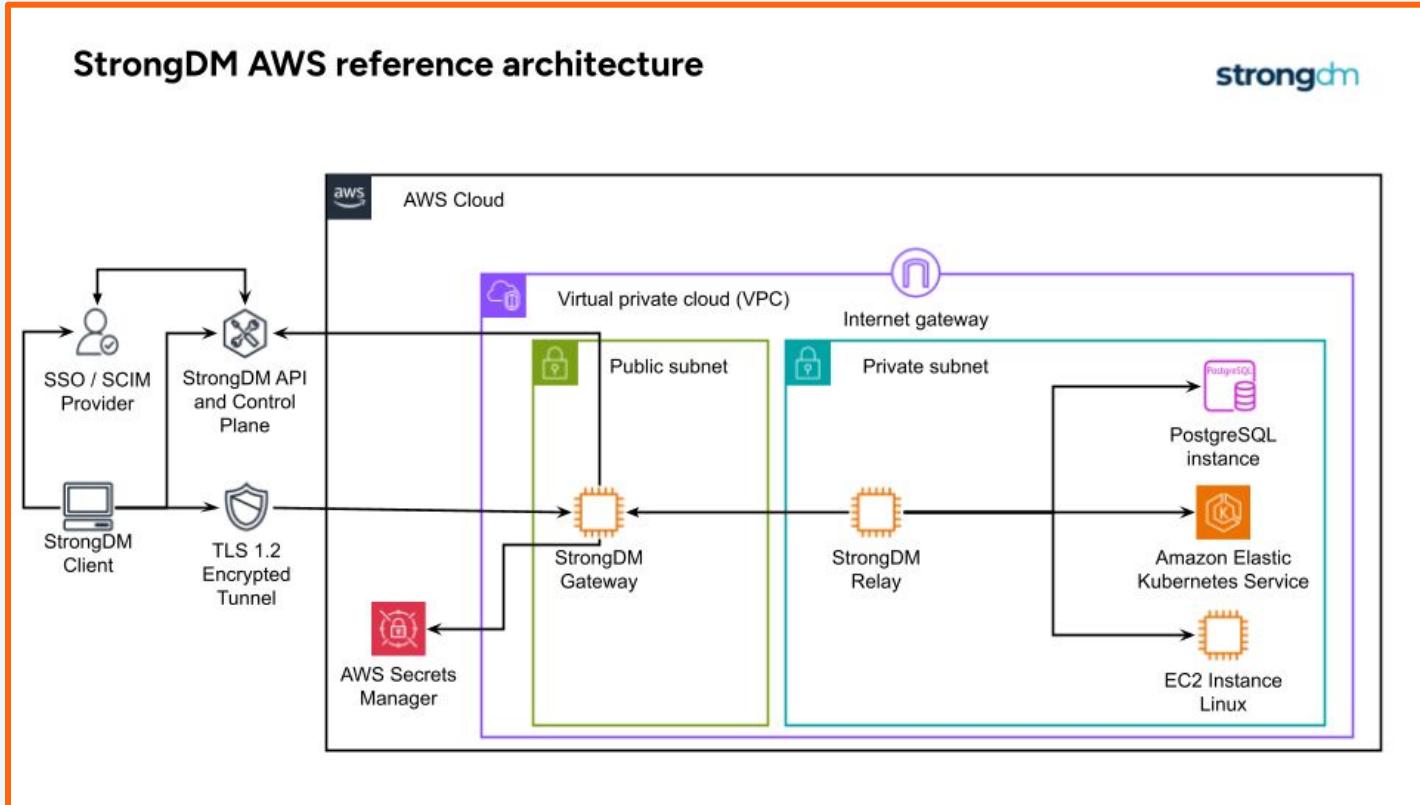
What are we covering today?

1. Logging in to your AWS account (Link provided in chat)
2. Logging in to your StrongDM tenant (Link provided in email)
3. Downloading and logging in to the StrongDM Desktop client
4. Fixing some IAM permissions (excuse our dust!)
5. Launching a self-registering CloudFormation stack
6. Checking for a running StrongDM Gateway
7. Adding the SSH resource to StrongDM
8. Adding the RDS PostgreSQL resource to StrongDM
9. Granting temporary access to those resources
10. Connecting to the resources
11. Advanced: Just-In-Time Access to those resources
12. Advanced: StrongDM policies

StrongDM Zero Trust



AWS Reference Architecture



Log in to AWS

Use the link provided to launch the AWS Workshop Studio site and register with your email address

Once registered, click on "AWS Console"

The screenshot shows a web browser window titled 'Workshop Studio' with the URL 'catalog.us-east-1.prod.workshops.aws'. The page features a dark header with the AWS logo and the text 'aws workshop studio'. On the right side, there's a user profile section for 'john.martinez'. The main content area has a heading 'AWS Workshop Studio' and subtext 'Join hands-on events and workshops'. Below this, a callout box says 'All you need is an event access code to join and get started with your event' with a 'Get started' button. Another callout box on the right lists 'What can you do here' with items like 'Join a scheduled customer engagement, such as a workshop, an Immersion Day, a bootcamp, an AWS GameDay, a hackathon, etc.' and 'Take a self-paced workshop via public URL'. At the bottom, a diagram titled 'How AWS Workshop Studio works' shows four steps: 1. Receive event access code (key icon), 2. Join event by entering the code (monitor icon), 3. Access provided AWS Account (laptop icon), and 4. Complete the workshop (monitor icon). The footer contains copyright information and links to 'Privacy policy', 'Terms of use', and 'Cookie preferences'.

Setting up AWS

Navigate to IAM on the top AWS Console search bar

Go to IAM Roles, search for WSParticipant

Attack **AmazonRDSFullAccess** and **AWSCloudFormationFullAccess** policies under **Add Permissions**

Log out, and log back in

Navigate to EC2 -> Key Pairs

Create key pair, give it a recognizable name, and download it

The screenshot shows the 'Add permissions' dialog in the AWS IAM console. The URL is `us-east-1.console.aws.amazon.com/iam/home?region=us-east-1#/roles/details/WSParticipantRole/attach-policies`. The role 'WSParticipantRole' is selected. The 'Attach policy to WSParticipantRole' section shows 'Current permissions policies (9)' and 'Other permissions policies (1/1058)'. A search bar at the top of the list is set to 'CloudFormation'. The 'AWSCloudFormationFullAccess' policy is selected and highlighted with a blue border. Other policies listed include 'AmazonSageMakerPartnerServiceCatalogProductsCloudFormationPolicy', 'AmazonSageMakerServiceCatalogProductsCloudFormationPolicy', 'AWSCloudFormationReadOnlyAccess', 'AWSCodeDeployRoleForCloudFormation', and 'AWSDeepRacerCloudFormationAccessPolicy'. At the bottom right are 'Cancel' and 'Add permissions' buttons.

Log in to StrongDM

Look for the welcome email in your inbox

Follow the instructions to log in to the StrongDM Admin UI

Download the StrongDM client from the “Download & Install” tab in the Admin UI, or from the link in the email

Once downloaded, sign in and use the same email address + password as the Admin UI

You have been invited to join Workshop [Inbox](#)



StrongDM Support <noreply@strongdm.com>
to Emilio ▾

4:28 PM (0 minutes ago)



Welcome to StrongDM!

You have been invited to join the Workshop account.

This invitation expires in 48 hours.

Please [set a password](#) and login.

Once you're logged in, [download](#) and install the StrongDM client.

- [Windows setup instructions](#)
- [Mac setup instructions](#)
- [Linux setup instructions](#)

See our [user guide](#) for instructions on how to connect to servers and databases.

If you have any questions, please contact your administrator.

Thank you!

Team StrongDM

Reply

Reply all

Forward

StrongDM Token

Navigate to Principals -> Tokens

Click Add Token

Name the token something attributable to you

Expiration can be anything

Select Relays (all) permissions

Click Create

Copy token and save to a local file

The screenshot shows the StrongDM web application interface. The left sidebar contains navigation links: Reports, Principals (selected), Users, Roles, Tokens (selected), Identity Sets, Resources, Access, Requests, Logs, Networking, Integrations, Settings, Diagnostics, Documentation, Download & Install, and Support. The version is listed as 109.98.0.

The main content area is titled "Create Admin Token". It displays a list of permissions grouped by category:

- Relays:** List (List relay tokens), Create (Create new relay tokens)
- Access Workflows:** Read (List and read access workflows), Write (Create, delete, and update access workflows)
- Organization:** View Settings (View settings), Edit Settings (Edit settings)
- Grants:** Read (List and read resource access grants), Write (Create and delete resource access)
- Secret Stores:** List (List secrets stores), Create (Create new secret stores), Update (Update existing secret stores), Delete (Delete secrets stores)
- Identities:** Read Identity Sets (List and read identity sets), Write Identity Sets (Create, delete, and update identity sets), Read Identity Aliases (List and read identity aliases), Write Identity Aliases (Create, delete, and update identity aliases)
- Approval Workflows:** Read (List and read approval workflows), Write (Create, delete, and update approval workflows)
- Policies:** Read (List and read policies), Write (Create, delete, and update policies)
- Secret Engines:** List (List secrets engines)
- Managed Secrets:** List (List managed secrets)

AWS CloudFormation (1)

Download the template
[sdm-aws-workshop.yml](#) from the GitHub Repo

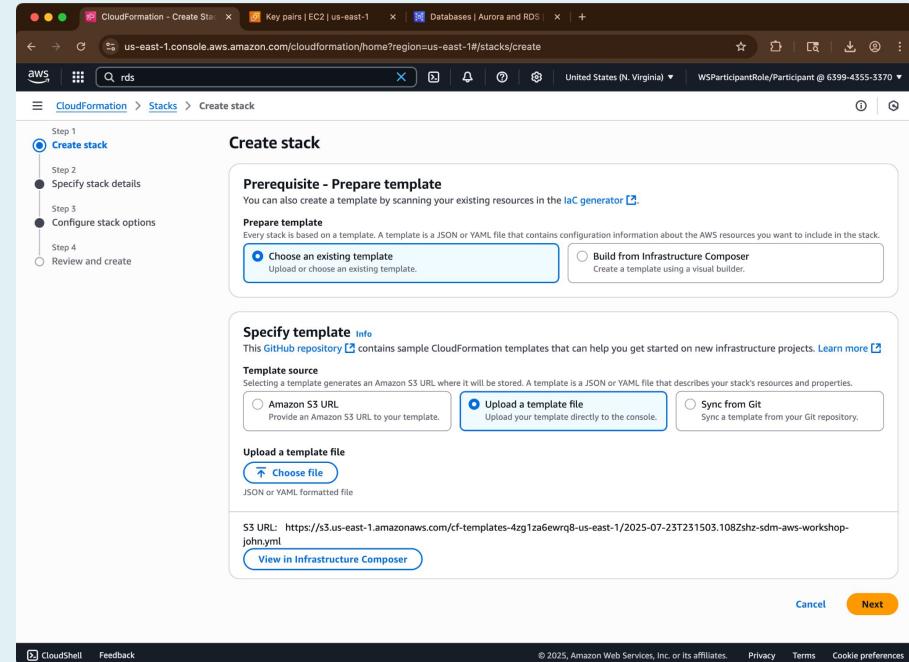
Edit the template locally

- replace the string “XXXXX” after “**SDM_ADMIN_TOKEN=**” with the contents of the token you created in StrongDM
- replace “XXXXX” after **MasterUserPassword** for RDS

In the AWS Console, navigate to CloudFormation and create a new stack

Select Upload Template File and select the edited template

Click Next



AWS CloudFormation (2)

Give your stack a recognizable name

Select the Default VPC and first Subnet in the parameters drop downs

Select the Key pair you created earlier

Select two the first two RDS subnets

Click Next

CloudFormation - Create Stack | Key pairs | EC2 | us-east-1 | Databases | Aurora and RDS | +

us-east-1.console.aws.amazon.com/cloudformation/home?region=us-east-1#/stacks/create

CloudFormation > Stacks > Create stack

Step 2: Specify stack details

Provide a stack name

Stack name: sdm-aws-workshop-johnm

Stack name must contain only letters (a-z, A-Z), numbers (0-9), and hyphens (-) and start with a letter. Max 128 characters. Character count: 22/128.

Parameters

Parameters are defined in your template and allow you to input custom values when you create or update a stack.

DefaultVPC
Select the default VPC
vpc-09cfa3c8c289fe209

EC2PublicSubnet
Select a public subnet for the EC2 instance
subnet-04b9dfb2d5c44bbbf

KeyName
Name of an existing EC2 KeyPair to enable SSH access to the instance
workshop-key-johnm

RDSSubnets
Select exactly two subnets for the RDS DB Subnet Group
Select List<AWS::EC2::Subnet>

subnet-04b9dfb2d5c44bbbf X subnet-026fe73155d0b01cd X

Cancel Previous Next

AWS CloudFormation (3)

You don't need to configure Stack Options, unless you'd like to add additional tags (do not use "Name", as it is used in the template)

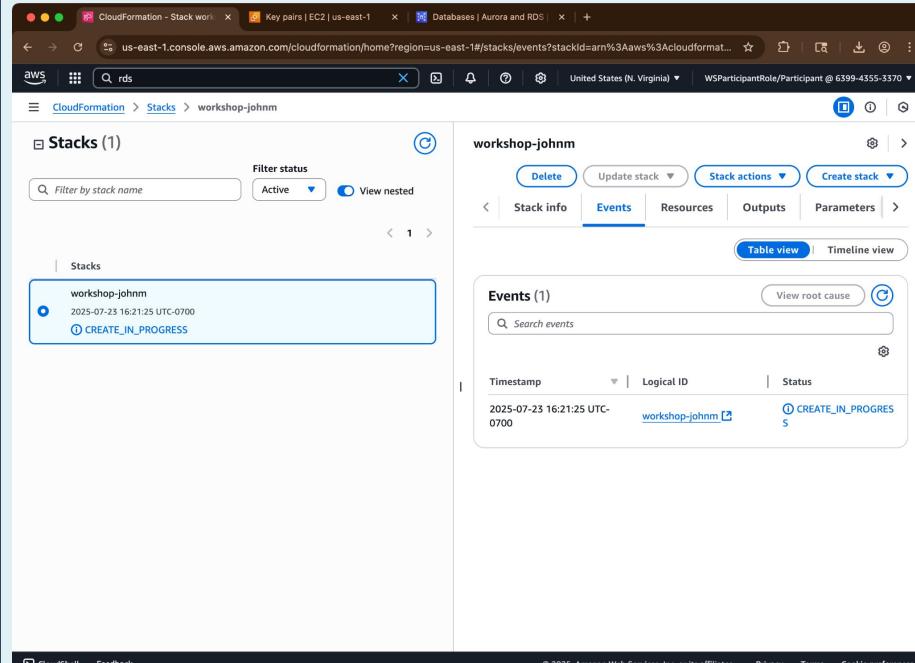
Click Submit

The Stack will begin creating

This will deploy:

- 1 StrongDM Gateway instance
- 1 Ubuntu Linux instance
- 1 RDS PostgreSQL Database

This process will take around 10 minutes, have a beverage!



AWS CloudFormation (3)

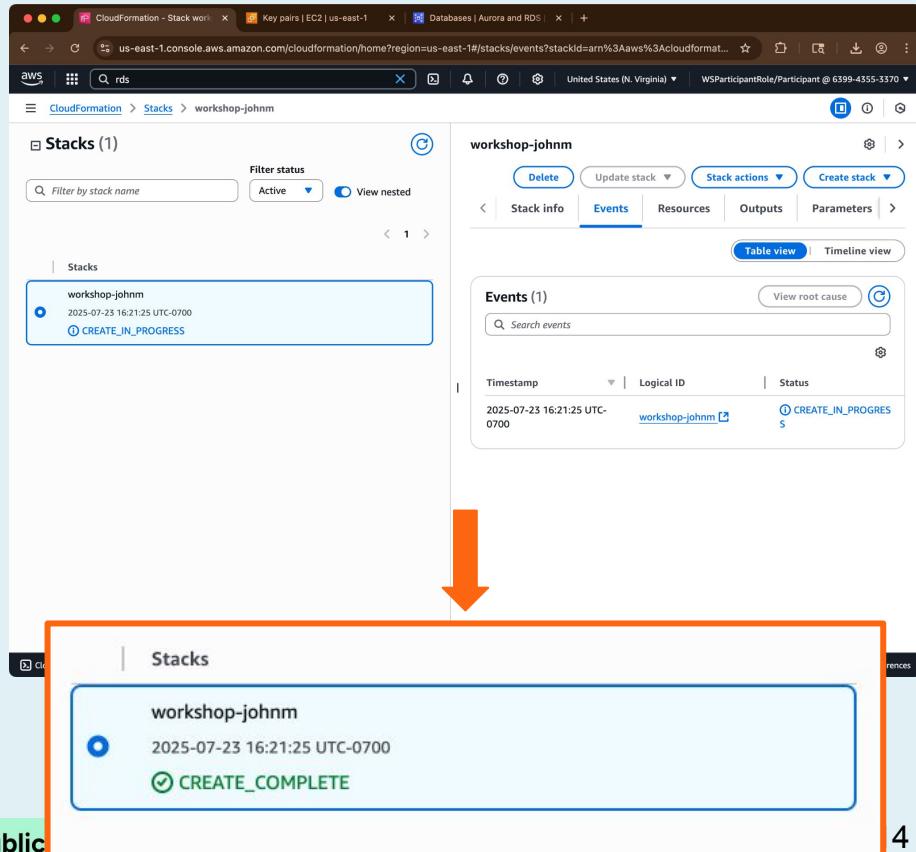
You don't need to configure Stack Options, unless you'd like to add additional tags (do not use "Name", as it is used in the template)

Click Submit

The Stack will begin creating

This will deploy:

- 1 StrongDM Gateway instance
- 1 Ubuntu Linux instance
- 1 RDS PostgreSQL Database



StrongDM Gateway

In the StrongDM Admin UI, navigate to Networking -> Gateways

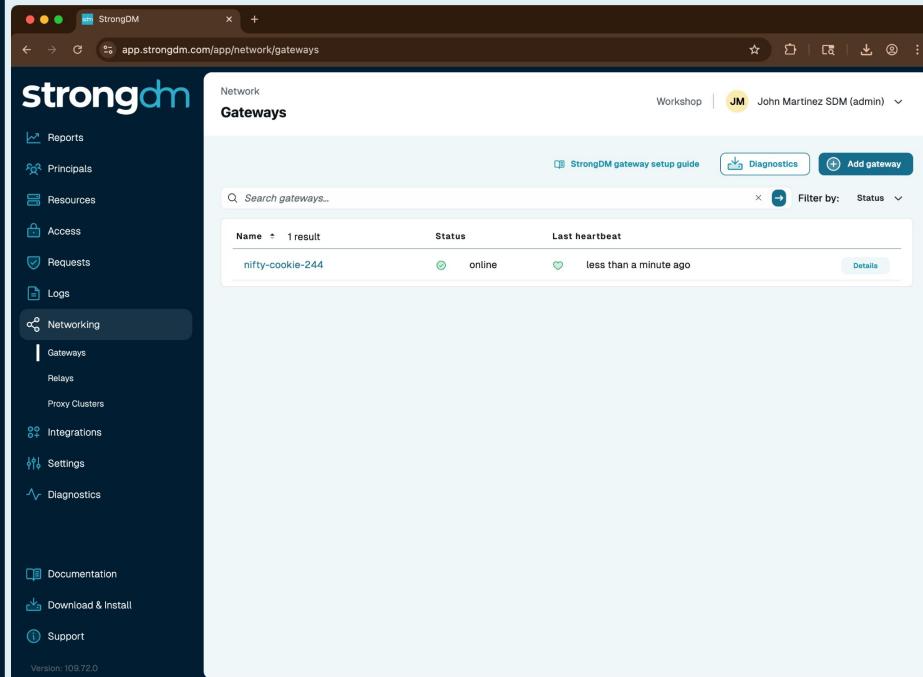
Look for your gateway

If there are more multiple gateways, look for your gateway's public IP address from the list

If you don't know your gateway's public IP, look for it in the AWS EC2 Console

You should rename your gateway to a recognizable name

Ensure that your gateway is "online"



The screenshot shows the StrongDM Admin UI interface. The left sidebar has a dark theme with white text and icons. It includes sections for Reports, Principals, Resources, Access, Requests, Logs, Networking (which is currently selected and highlighted in blue), Gateways, Relays, Proxy Clusters, Integrations, Settings, and Diagnostics. Below the sidebar are links for Documentation, Download & Install, and Support, along with a note about the current version (109.72.0). The main content area has a light background. At the top right, there are buttons for 'Workshop' (with a yellow profile icon), 'John Martinez SDM (admin)', 'Diagnostics', and '+ Add gateway'. Below these are buttons for 'StrongDM gateway setup guide', 'Search gateways...', 'Filter by: Status', and 'Details'. A table lists one gateway entry:

Name	Status	Last heartbeat
nifty-cookie-244	online	less than a minute ago

StrongDM Gateway (Manual Optional Setup)

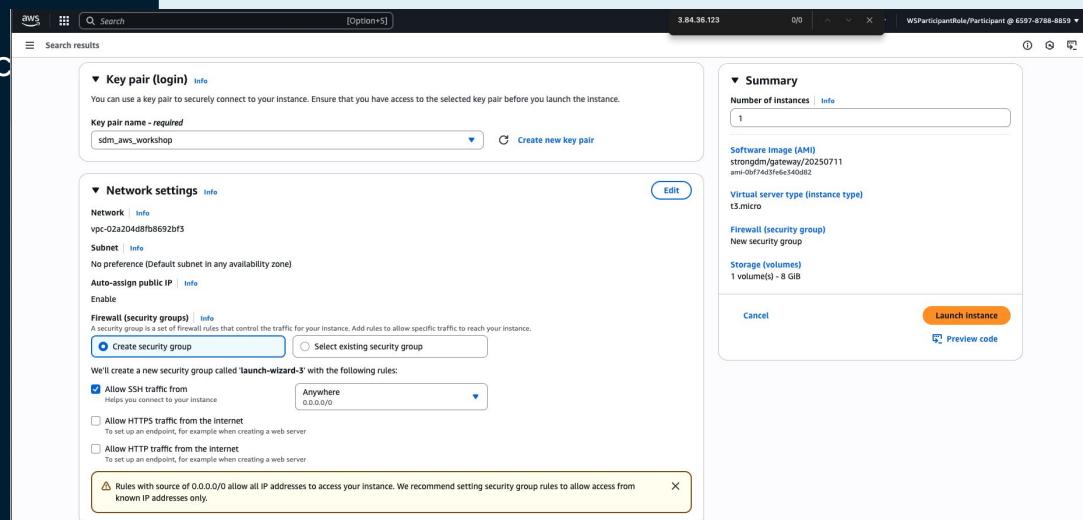
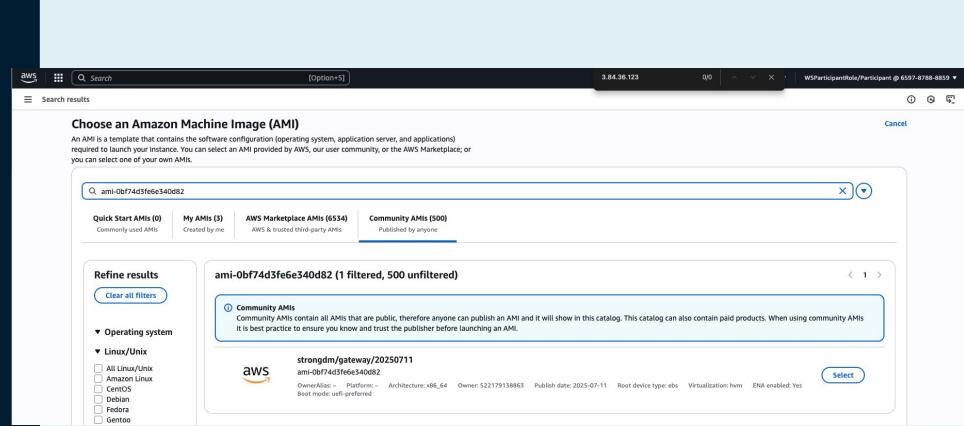
Follow the instructions in the [StrongDM Gateway AMI Installation Guide](#)

Launch an EC2 instance with the StrongDM Gateway AMI (**us-east-1** **ami-0bf74d3fe6e340d82**), Ensure a public IP address is assigned

Ensure that the Gateway token is passed in user-data

You should rename your gateway to a recognizable name

Check that your gateway is "online"



You may rename your gateway to a recognizable name

Public Data

SSH Resource (1)

In the StrongDM Admin UI, navigate to Resources -> Servers

Click on Add server

Give it a name attributable to you

Server type: SSH (Customer Managed Key)

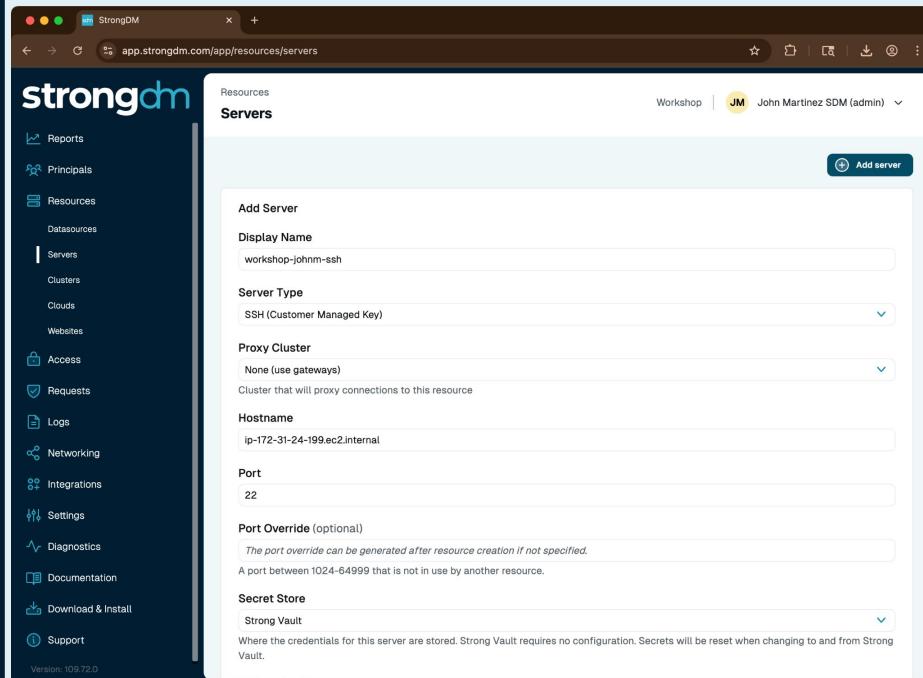
Hostname: Your private EC2 DNS name

Authentication: Leased Credentials /

Username "Ubuntu"

Private Key: the downloaded key from AWS

Click Create



SSH Resource (2)

Find your SSH resource in the list

Click on the name of the resource

In Diagnostics, click the green Check Health button

The resource should turn to "Healthy"

The screenshot shows the StrongDM web application interface. On the left is a sidebar with navigation links: Reports, Principals, Resources, Datasources, Servers (selected), Clusters, Clouds, Websites, Access, Requests, Logs, Networking, Integrations, Settings, Diagnostics (selected), Documentation, Download & Install, and Support. The main content area has a header 'Resources / Servers' and a sub-header 'workshop-johnm-ssh'. It displays the following information:

Status	Type	Created at
Healthy	SSH (Customer Managed Key)	Today at 4:34 PM PST

Below this is a 'Diagnostics' tab, which contains a message: 'The server is online and accessible via one or more gateways or relays.' A 'Check health' button is located at the bottom right of this section. The 'Settings' tab is also visible. At the bottom of the main content area, there is a table with the following data:

Node name	1 result	Type	Status	Reachable	Connection	Last Checked
nifty-cookie-244		Gateway	Healthy	SUCCESS	SUCCESS	today -

At the very bottom of the page, it says 'Version: 109.72.0'.

Postgres Resource (1)

In the StrongDM Admin UI, navigate to Resources -> Datasources

Click on Add datasource

Give it a name attributable to you

Datasource type: PostgreSQL

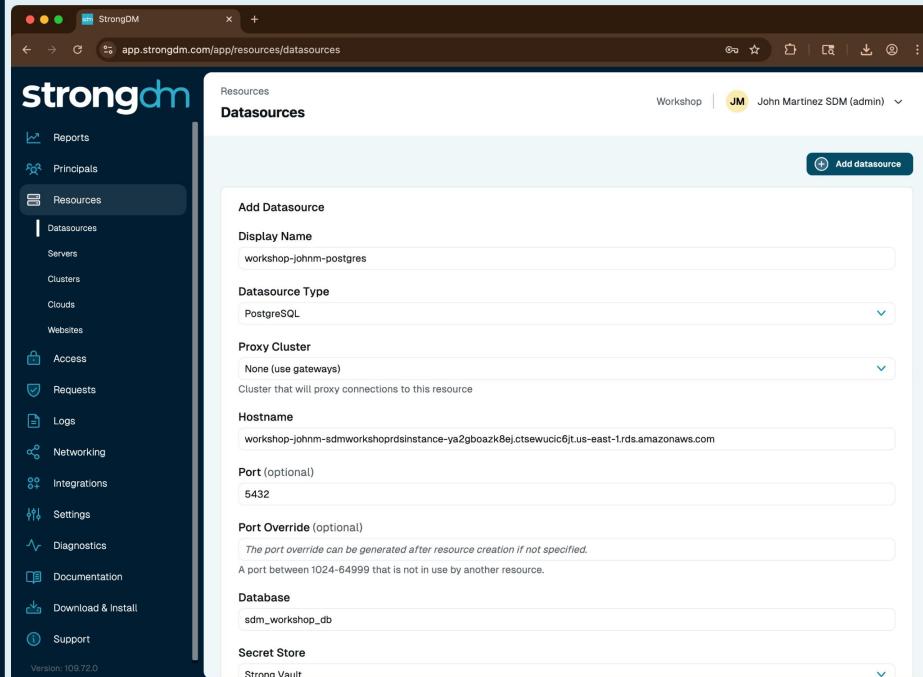
Hostname: RDS DB Endpoint

Database: Retrieve from CloudFormation file (DBName)

Username: Retrieve from CloudFormation file (MasterUsername)

Password: Retrieve from CloudFormation file (MasterUserPassword)

Click Create



Postgres Resource (2)

Find your Postgres resource in the list

Click on the name of the resource

In Diagnostics, click the green Check Health button

The resource should turn to "Healthy"

The screenshot shows the StrongDM web application interface. On the left is a sidebar with various navigation links: Reports, Principals, Resources (which is selected), Datasources, Servers, Clusters, Clouds, Websites, Access, Requests, Logs, Networking, Integrations, Settings, Diagnostics (which is expanded), Documentation, Download & Install, and Support. The main content area has a header 'Resources / Datasources' and a sub-header 'workshop-johnm-postgres'. It displays the following information:

Status	Type	Created at
Healthy	PostgreSQL	Today at 4:37 PM PST

Below this is a 'Diagnostics' tab, which contains a message: 'The datasource is online and accessible via one or more gateways or relays.' A 'Check health' button is located at the bottom right of this section. The 'Diagnostics' table lists one result:

Node name	Type	Status	Reachable	Connection	Last Checked
nifty-cookie-244	Gateway	Healthy	SUC...	SUC...	today...

Grant Temporary Access

Find your User entry in Principals -> Users in the StrongDM Admin UI

Click on Grant Temporary Access

Follow the UI to find your Ubuntu and Postgres resources for a finite amount of time

Once granted, both resources will appear in the StrongDM Desktop App, click on the connect icon for Postgres

strongdm

Reports

Principals

Users

Roles

Tokens

Identity Sets

Resources

Access

Requests

Logs

Networking

Integrations

Settings

Diagnostics

strongdm

Workshop | JM John Martinez SDM (admin)

Principals

Users

Search: suspended:false

Filter by: Role Permission level Activity

Name	Email	Permission Level	Roles	Temporary Access	Device Trust
Jason, Patterson	mpattjas+sdmworkshop@amazon.com	Admin	no roles	-	Actions
Katz, Tracy	tracy+workshop@strongdm.com	Admin	no roles	-	Actions
Lo, Cat	catherine.lo+workshop@strongdm.com	Admin	no roles	-	Actions
Lupascu, Alin	alin+workshop@strongdm.com	Admin	no roles	-	Actions
Mahajan, Ashok	ashok.mag+sdmworkshop@amazon.com	Admin	no roles	-	Actions
Mangubat SDM, Calvin	calvin.mangubat+workshop@strongdm.com	Admin	no roles	-	Actions
<input checked="" type="checkbox"/> Martinez SDM, John	john.martinez+workshop@strongdm.com	Admin	no roles	-	Actions
Morris, Jared	jared.morris+workshop@strongdm.com	Admin	no roles	-	Actions
Pearson, Josh	joshua.pearson+workshop@strongdm.com	Admin	no roles	-	Actions

Grant temporary access

Martinez SDM, John
john.martinez+workshop@strongdm.com

View details
Set roles
Remove from all roles

StrongDM - Login

John Martinez SDM

Resources

Favorites All

Search resources...

2 Resources

PostgreSQL

workshop-johnm-postgres
127.0.0.1:10002 ⚡

SSH (Customer Managed Key)

workshop-johnm-ssh
127.0.0.1:10001 ⚡

Connected to StrongDM

StrongDM Public Data

Public Data

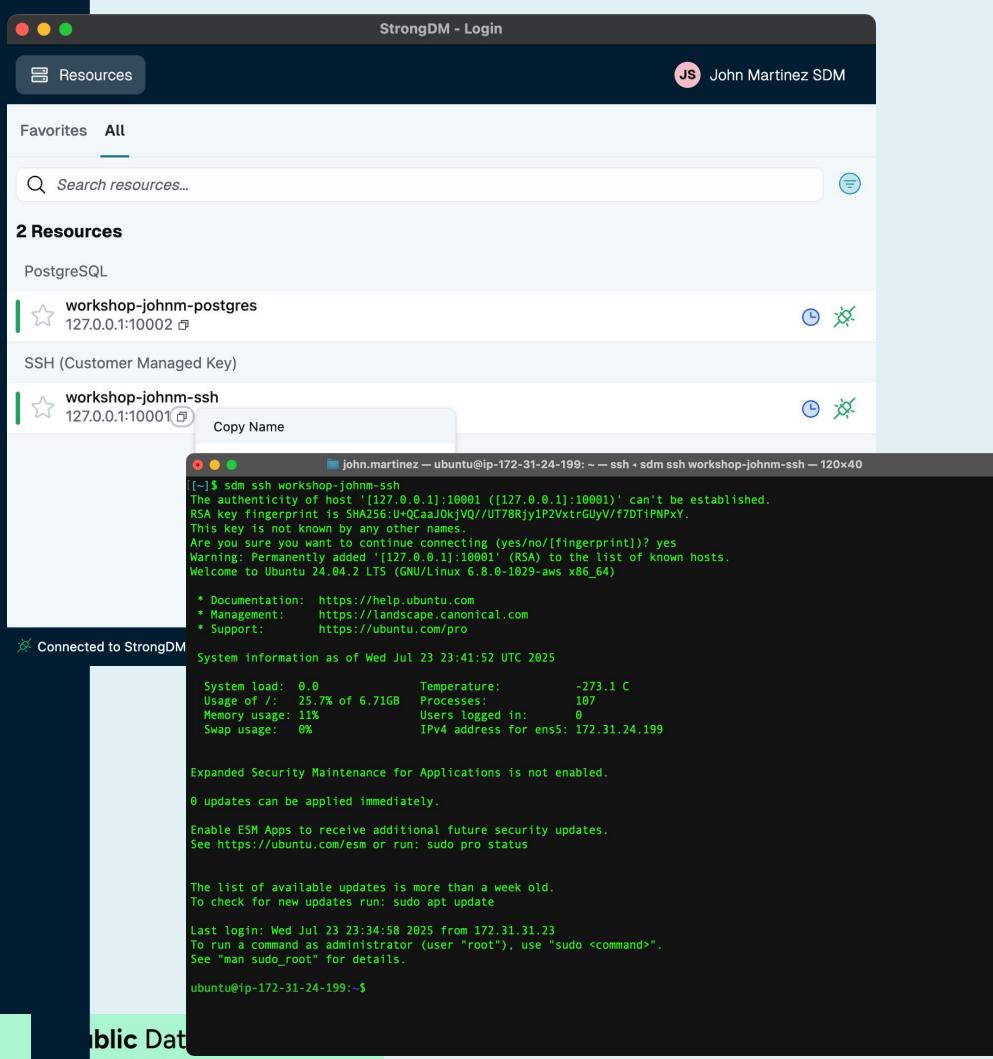
Connect to SSH

In the StrongDM Desktop App, copy the name of the SSH resource

Use the StrongDM CLI (**sdm**) command connect to the resource

If **sdm** is not found, you can use the OS builtin **ssh** command to connect, by using the IP address (127.0.0.1) and port as found in the desktop UI to connect

```
ssh -p <port> ubuntu@127.0.0.1
```



Connect to Postgres

In the StrongDM Desktop App, copy the port of the Postgres resource (similar to the SSH example)

Download a GUI database client such as Beekeeper Studio ([community edition](#))

Follow the GUI to connect to a PostgreSQL database

Leave user name blank

IP address/Hostname: 127.0.0.1
Port: From the StrongDM Desktop App

The StrongDM Desktop App interface shows a list of resources. A context menu is open over the 'workshop-johnm-postgres' resource, which has the IP address 127.0.0.1 and port 10002. The menu options are: Copy Name, Copy IP:Port, Copy IP, and Copy Port. The 'Copy IP:Port' option is highlighted.

The Beekeeper Studio application is shown below. It has a sidebar with a 'New Connection' button and a 'SAVED' section containing several database connections. In the main area, there is a 'New Connection' dialog for a PostgreSQL connection. The 'Connection Type' is set to 'Postgres', 'Host' is 'localhost', 'Port' is '10002', and 'User' is left blank. There are buttons for 'Test' and 'Connect'.

Advanced Use Cases

Just-In-Time Access

Follow the instructions in the Create and Use JIT Access Workflows section of the manual Workshop document

[https://github.com/strongdm/aws-workshops/
blob/main/index.en.md#create-and-use-jit-access-workflows](https://github.com/strongdm/aws-workshops/blob/main/index.en.md#create-and-use-jit-access-workflows)

StrongDM Policies

Follow the links to the Policies documentaiton in the Create Policies section of the manual Workshop document

[https://github.com/strongdm/aws-workshops/
blob/main/index.en.md#optional-create-policies](https://github.com/strongdm/aws-workshops/blob/main/index.en.md#optional-create-policies)