

Accessing Spark History Server

This document contains the steps to access Spark History Server in AWS EMR.

1. Go to the homepage for your EMR cluster. Then under the cluster information page, click on the **security groups of the master node**.

Security and access

Key name: RHEL

EC2 instance profile: EMR_EC2_DefaultRole

EMR role: EMR_DefaultRole

Visible to all users: All [Change](#)

Security groups for Master: [sg-00fcc219431b5c0a6](#) [🔗](#) (ElasticMapReduce-master)

Security groups for Core & Task: [sg-0a724c5cb4e439160](#) [🔗](#) (ElasticMapReduce-slave)

2. Click on the 'security group' and you will land on a similar page. Here, click on the security group of the **Elastic MapReduce-master node** as highlighted in the image below.

Security Groups (2) [Info](#)

🔍 *Filter security groups*

search: [sg-00fcc219431b5c0a6](#) ✕ [Clear filters](#)

<input type="checkbox"/>	Name ▾	Security group ID ▾	Security group name ▾	VPC ID ▾
<input type="checkbox"/>	-	sg-00fcc219431b5c0a6	ElasticMapReduce-master	vpc-069954fb4011801ca 🔗
<input type="checkbox"/>	-	sg-0a724c5cb4e439160	ElasticMapReduce-slave	vpc-069954fb4011801ca 🔗

3. Clicking on the security group will land you on the corresponding security information page. Click on 'Edit inbound rules' to add a new rule.

sg-00fcc219431b5c0a6 - ElasticMapReduce-master Actions ▾

Details

Security group name ElasticMapReduce-master	Security group ID sg-00fcc219431b5c0a6	Description Master group for Elastic MapReduce created on 2021-03-16T22:01:30.781Z	VPC ID vpc-069954fb4011801ca
Owner 367134191692	Inbound rules count 21 Permission entries	Outbound rules count 1 Permission entry	

Inbound rules | Outbound rules | Tags

Inbound rules (21) Manage tags Edit inbound rules

- Here, you need to add a new rule. Click on **Add rule** towards the bottom of all the rules. Clicking on the 'add rule' will add a new row as shown in the figure below.

sgr-049e72c7217cd27d1	All TCP	TCP	0 - 65535	Custom	72.21.198.64/29		Delete
sgr-0aa1d8567077864f9	All ICMP - IPv4	ICMP	All	Custom	sg-00fcc219431b5c0a6		Delete
sgr-0522ea2084a15dc38	Custom TCP	TCP	8443	Custom	sg-0a724c5cbac439160		Delete
sgr-0e4552cd2b814d5be	Custom TCP	TCP	8443	Custom	207.171.167.26/32		Delete
-	Custom TCP	TCP	0	Custom	72.21.217.0/24		Delete

Add rule

- Now, here you need to set the rule for **Custom TCP**, and then for the port, you need to type **18080**. Next, you need to keep the Source as **'My IP'** for this rule.

Custom TCP	TCP	18080	My IP	223.182.167.217/32		Delete
------------	-----	-------	-------	--------------------	--	--------

- Now you can click on **Save rules** and then **go back to the EMR cluster homepage**.
- Go to the **Application User Interfaces** tab for your AWS EMR cluster.

8. Copy the **User interface URL** corresponding to **Spark History Server** under the **On-cluster application user interfaces**.

Amazon EMR

EMR Studio
EMR Serverless [New](#)

EMR on EC2
Clusters
Notebooks
Git repositories
Security configurations
Block public access
VPC subnets
Events

EMR on EKS
Virtual clusters

Help
What's new

EMR Serverless is now GA.
With EMR Serverless, get the benefits of Amazon EMR such as open source compatibility, latest versions and performance optimized runtime for popular frameworks along with easy provisioning, quick job startup, automatic capacity management, and simple cost controls. [Get Started with EMR Serverless](#)

Persistent application user interfaces

Applications installed on the Amazon EMR cluster publish user interfaces (UI) as web sites to monitor cluster activity. Persistent UI logs are available for 30 days after an application ends. Persistent UI don't required SSH tunneling. They are hosted off of the cluster.

Application user interface

[YARN timeline server](#)
[Spark history server](#)

On-cluster application user interfaces

On-cluster UI are available only while clusters are running. Because they are hosted on the master node, on-cluster UI require a connection via SSH tunneling. Set up SSH tunneling before accessing these application UI. [Learn more](#)

Application	User interface URL	Status
HDFS Name Node	http://ec2-3-210-199-65.compute-1.amazonaws.com:9870/	SSH tunnel not enabled
JupyterHub	https://ec2-3-210-199-65.compute-1.amazonaws.com:9443/	SSH tunnel not enabled
Spark History Server	http://ec2-3-210-199-65.compute-1.amazonaws.com:18080/	SSH tunnel not enabled
Livy	http://ec2-3-210-199-65.compute-1.amazonaws.com:8998/	SSH tunnel not enabled
Resource Manager	http://ec2-3-210-199-65.compute-1.amazonaws.com:8088/	SSH tunnel not enabled

The following table lists web interfaces you can view on the task nodes:

Application	User interface URL
-------------	--------------------

9. Now you can copy the URL on another tab of your web browser and click on **Enter**. You will see the following page appear.

History Server

Event log directory: `hdfs://var/log/spark/apps`
Last updated: 2022-08-01 19:10:22
Client local time zone: Asia/Calcutta

Search:

Version	App ID	App Name	Started	Completed	Duration	Spark User	Last Updated	Event Log
3.1.2-amzn-1	application_1659348629157_0002	livy-session-1	2022-08-01 17:01:00	2022-08-01 18:51:37	1.8 h	livy	2022-08-01 18:51:37	Download
3.1.2-amzn-1	application_1659348629157_0005	livy-session-4	2022-08-01 18:30:19	2022-08-01 18:36:56	6.6 min	livy	2022-08-01 18:36:56	Download
3.1.2-amzn-1	application_1659348629157_0003	livy-session-2	2022-08-01 17:55:16	2022-08-01 18:00:35	5.3 min	livy	2022-08-01 18:00:35	Download
3.1.2-amzn-1	application_1659348629157_0001	livy-session-0	2022-08-01 16:45:21	2022-08-01 16:58:06	13 min	livy	2022-08-01 16:58:06	Download

Showing 1 to 4 of 4 entries
[Show incomplete applications](#)

10. Here, you need to click on **Show incomplete applications**. All applications which haven't been finished will show here. Your job might also be present as a completed job in which case you don't need to find it in incomplete applications.

11. From here, you can check the applications and their DAGs and access any job on the history server.