LESSON WORKBOOK

AWS Fundamentals 02 - Your First EC2 Lab, from Budget to Cleanup

AWS Fundamentals

Study the lesson, work through the lab, and check your understanding with the quiz. Keep the reference sheet nearby as you practice.

Includes the complete lesson, guided lab, knowledge check, answer explanations, and quick reference.

Lesson

AWS Fundamentals 02 - Your First EC2 Lab, from Budget to Cleanup

CloudComputingTutor · Beginner · 25-minute reading + 45-60-minute lab
Prerequisites: `aws-fundamentals-01`, basic `pwd`, `ls`, `cat`, and `cd`. **Outcome:** Connect to an Amazon Linux instance through Session Manager, explain its identity and network path, collect operating-system evidence, and remove the resources you created. **Publication state:** New teaching material; the live AWS lab has not been executed as part of preparing this lesson. Sources checked **2026-09-18**.

1. Give Shutterbird one small job

In AWS Fundamentals 01, Shutterbird was our fictional photo-sharing startup. Its architecture had compute, storage, identity, and networking boxes. Today we inspect one compute box. The assignment is deliberately modest: create a temporary Linux workstation, identify its operating system and storage, write a short observation file, and clean up.

There is no website to expose yet. There is no reason to open SSH to the world. The success condition is a repeatable sequence you can explain: **choose -> connect -> inspect -> prove -> remove**. A running server alone is only the middle of the exercise.

An EC2 instance is a virtual machine. An Amazon Machine Image, or AMI, supplies its starting operating system. The instance type supplies a capacity shape. An EBS volume supplies its persistent block storage. Your subnet locates it in one Availability Zone; its security group controls network traffic. These choices describe different parts of the same machine. EC2 concepts and launch workflow

2. Two identities and one connection path

Your signed-in AWS identity controls whether you may start a session. Separately, the instance has an IAM role that lets its SSM Agent communicate with Systems Manager. Giving the instance a role does not automatically grant your human identity session access.

We use an EC2 instance profile containing a role with `AmazonSSMManagedInstanceCore`. The agent makes outbound HTTPS connections. For this lab the path is instance -> public subnet -> internet gateway -> regional Systems Manager services. It needs a public IPv4 address for this IPv4 internet-gateway route. We will allow no inbound security-group rules. Public addressing and permission to accept inbound traffic are different decisions. Instance permissions, internet-gateway routing

Session Manager avoids a downloaded SSH key in this exercise, but it is powerful administrative access. On an unmodified supported Linux image, sessions normally run as `ssm-user`, which can

have sudo privileges. Treat that shell accordingly. Later lessons can introduce private subnets and interface endpoints; those have additional configuration and potential charges. Session Manager prerequisites

3. Lab preflight: establish the boundaries

Use an authorized personal learning account or an instructor-provided sandbox, never a production account. Protect the root account with MFA and sign in through your normal temporary/federated learning identity. You need console access and permission to launch/terminate EC2, inspect networking and volumes, create/delete this lab's security group, and create/tag/delete this lab's role and instance profile. Passing that role to EC2 requires `iam:PassRole`. Session access needs the human-side Systems Manager permissions described in the official example policies.

If an instructor supplies resources, ask them to supply the tagged profile, network, and session permission before class. Do not attach administrator access to the instance to overcome a failed step. A permission error is a preflight issue, not a reason to broaden the lab. No cloud account or no suitable permissions? Complete Section 10's tabletop route.

Choose a single AWS commercial Region, such as `us-east-1`, and record it. Verify a default VPC and default subnet exist there. In the VPC console, confirm DNS resolution is enabled, the subnet's effective route table has `0.0.0.0/0` targeting an attached internet gateway, and its default network ACL allows inbound and outbound traffic. A custom restrictive ACL must allow HTTPS requests and their ephemeral return traffic; use the instructor's approved network instead of improvising changes. If there is no suitable default network, take the tabletop route until one is provisioned.

Finally, review current EC2, EBS, and public IPv4 rates for your account/Region. Credits and eligibility vary. This lesson does not promise a free lab. Set a 45-minute local reminder to check your resource inventory. A reminder costs nothing and works even if a billing notification is delayed. Public IPv4 pricing

4. Step 1 - Set visibility before provisioning

Open Billing and Cost Management -> Budgets. If you have budget permissions, create a monthly cost budget for this learning account with a small amount you are comfortable spending, such as USD 5. Choose an actual-cost email notification at 50% and 100%; add a forecast notification if available. Use an inbox you monitor and complete any confirmation requested. If the account owner manages budgets, record the existing budget and the responsible person instead.

Record budget name, thresholds, recipient, and today's starting displayed spend. **This is a notification configuration, not a hard spending cap.** AWS updates cost information periodically; an email can arrive after usage has accumulated. Closing your browser does not stop resource charges. Your controls are small resources, limited duration, and verified cleanup. AWS Budgets behavior

Expected evidence: a budget configuration screenshot with personal/account details redacted. A configuration screenshot proves setup, not successful delivery of a threshold email that has not occurred.

5. Step 2 - Create the instance role and security group

In IAM -> Roles -> Create role, choose **AWS service**, then the **EC2** use case. Select only `AmazonSSMManagedInstanceCore`. Name the role `cct-ec2-lab-role` and tag it `Project=CloudComputingTutor` and `Purpose=aws-fundamentals-02`. The EC2 console workflow creates the corresponding instance profile. Record its name. If that name already exists, use a unique lab suffix and record the actual name instead of changing an existing role.

In the chosen Region's EC2 console, create `cct-ec2-lab-sg` inside your selected VPC. Give it **zero inbound rules**. Replace its default outbound rule with HTTPS/TCP 443 to `0.0.0.0/0`. This allows service connections over HTTPS; it does not constrain destinations to AWS alone. AWS-provided DNS in this default VPC is handled separately from ordinary security-group filtering. Keep the unmodified default ACL identified in preflight. Record the security-group ID.

Expected evidence: the role's service trust is EC2, its permissions show the SSM managed policy, and the security-group inbound list is empty. Naming and tagging are inventory aids, not security controls by themselves.

6. Step 3 - Launch a deliberately small instance

Open EC2 -> Instances -> Launch instances. Set the name to `cct-shutterbird-lab`. Choose the latest **Amazon Linux 2023 standard AMI**, published by Amazon, with **x86_64** architecture. Choose `t3.micro` where available and permitted; otherwise use an instructor-approved compatible small type after reviewing its price. An architecture mismatch between AMI and type prevents launch. Instance-type concepts

Select **Proceed without a key pair** because this procedure uses Session Manager. In network settings, explicitly select your VPC, public default subnet, **Auto-assign public IP: Enable**, and the security group from Step 2. Do not accept the wizard's suggested SSH inbound rule. Keep one small root `gp3` EBS volume at the AMI's default size, enable encryption, and verify **Delete on termination** is enabled. Record its volume ID after launch.

In Advanced details select your IAM instance profile, require IMDSv2 for instance metadata, and, for T3, select **Standard** credit mode for this low-CPU exercise. Keep detailed monitoring off and leave user data empty. Review the instance count: **one**. Launch only after confirming the settings. Record the instance ID, Region, AZ, launch time, role, security group, and root volume ID.

Expected result: `pending` becomes `running`; status checks pass. SSM registration can take additional minutes. Do not launch another machine merely because the first takes time to register.

7. Step 4 - Connect and inspect Linux

Select that exact instance -> Connect -> **Session Manager** -> Connect. The browser shell is the Linux instance, not your laptop. Run the following one command at a time:

```
whoami
pwd
cat /etc/os-release
uname -r
hostname
lsblk
df -h /
free -h
systemctl is-active amazon-ssm-agent
```

Expected observations: the identity is usually `ssm-user`; `/etc/os-release` names Amazon Linux 2023; `lsblk` displays block devices, possibly with NVMe-style names; `df` describes the mounted root filesystem; `free` reports memory; the agent reports `active`. Exact hostnames, kernel versions, available memory, and disk names vary. Capture your observations rather than copying an example value.

Now make an isolated folder with a collision-resistant name:

```
LAB_DIR=$(mktemp -d /tmp/cct-observation.XXXXXX)
printf '%s\n' 'Shutterbird lab: connected through Session Manager.' > "$LAB_DIR/observation.txt"
cat "$LAB_DIR/observation.txt"
ls -l "$LAB_DIR/observation.txt"
```

Explain each command in a sentence. `mktemp` makes the folder; `printf` produces text; redirection writes the file; `cat` reads it; `ls -l` exposes permissions and ownership. These Linux actions do not require you to download or display AWS credentials. Do not run `aws configure` or retrieve metadata credentials for this lab.

8. Step 5 - Troubleshoot by layer

If Connect is unavailable, check the selected account, Region, instance ID, role attachment, and agent registration first. Confirm the public IPv4 address exists, the subnet route really targets an attached internet gateway, outbound 443 is allowed, and the ACL is unchanged. The endpoints include regional `ssm` and `ssmmessages`; older configurations can also involve `ec2messages`. Then check whether your human identity may start a session. A permissions denial differs from a node that is not online.

If a session opens but a command fails, read the error. A mistyped unit name is different from an inactive service. Avoid adding inbound SSH or replacing policies with administrator access as a generic fix. Keep one observation log: attempted action, actual message, suspected layer, and next read-only check. That log is more valuable than a screenshot of a green status alone.

9. Step 6 - Finish with cleanup evidence

Copy your observation text and selected screenshots into your portfolio before termination. This lab contains no valuable application data. End the browser session. Select the recorded instance ID in EC2 and choose **Instance state -> Terminate (delete)**. Confirm the correct target. Wait until it is terminated; then check the recorded root volume no longer exists. If a lab-owned volume remains, verify its ID and that it is unattached before deleting it. Stopping an instance retains EBS storage and is not equivalent to removing the lab. Termination behavior

Check Elastic IPs and snapshots: this lesson should have created neither. Confirm the auto-assigned public IPv4 address is released. Delete only the dedicated lab security group after its network interface is gone. Remove the dedicated IAM role/profile if no instance uses it; preserve anything an instructor supplied or shared. Keep the budget for future learning. Leave the default VPC, subnet, route table, and internet gateway in place.

Record termination time and the inventory checks. Check Billing again after cost data refreshes; a zero immediately afterward is not proof of zero cost. If you immediately continue AWS Fundamentals 03, you may reuse the instance and role during the same supervised session, record that handoff, and perform the combined cleanup there. Otherwise terminate now.

10. Offline route and portfolio handoff

Without AWS, draw the browser identity, regional service, instance role, agent, subnet, internet gateway, security group, and EBS volume. Label the direction of the HTTPS connection. Use this simulated incident: "The instance is running, inbound rules are empty, no public IPv4 exists, and there are no NAT gateways or interface endpoints." Explain why this lab's internet route cannot work and name the missing component.

Write a fictional inventory with clearly labeled sample IDs, a cost checklist, and a teardown order. On local Linux you may inspect `/etc/os-release`, memory, and disk using the read-only commands above; macOS output and utilities differ, so describe those as local observations. Do not claim an AWS deployment occurred. Your tabletop evidence is the diagram, reasoning, and predicted outcomes.

Submit five items: the architecture sketch, preflight/budget record, Linux observation file, one troubleshooting explanation, and cleanup inventory. A learner passes when they can explain **both identities**, the outbound network path, one OS observation, and why cost checks continue after deletion. Next, Shutterbird gives this machine a narrowly defined job in a private S3 bucket.

Knowledge check and answers

AWS Fundamentals 02 - Scenario Quiz

Answer before reading the explanation. Score one point per correct choice; aim for 6/8, then repeat the lab decisions behind any missed question.

1. The forgotten tab

Shutterbird's intern closes the Session Manager tab but leaves EC2 running. What happens?

A. EC2 terminates automatically. B. The shell connection ends, while cloud resources can continue incurring charges. C. EBS is deleted. D. The monthly budget stops the instance.

Answer: B. A browser session and an EC2 resource have separate lifecycles. Cleanup requires the recorded instance's termination and verification of related storage/address resources.

2. The invisible instance

The instance is running in a public subnet, its route targets an internet gateway, and outbound HTTPS is allowed. It has no public IPv4 and this IPv4-only lab has no NAT or interface endpoints. Why is SSM registration failing?

A. No inbound port 22. B. The instance lacks the address required for this internet-gateway path. C. An EBS volume is always public. D. It needs a bigger instance.

Answer: B. A route alone does not give an IPv4 instance internet connectivity. This specific lab also requires a public IPv4. Private-subnet alternatives need their own complete connectivity design.

3. Two permissions checks

The SSM Agent is online, but Mira receives AccessDenied when starting a session. Which permission should be investigated next?

A. Her human/federated identity's session permissions. B. Anonymous internet access. C. The file's Unix execute bit. D. The AMI's publisher name.

Answer: A. Instance-side service permissions and human-side session authorization are distinct. An online agent does not authorize every person to open a shell.

4. A budget misconception

A USD 5 budget has notifications configured. A teammate says, "Spending cannot exceed five dollars." What is the best correction?

A. Budgets only work for S3. B. Email budgets are visibility tools with delayed cost data; resource usage can exceed the threshold. C. Budgets disable IAM. D. Five dollars always buys one month of EC2.

Answer: B. Notifications are not a real-time spending cap. Choose resource size and duration deliberately and verify cleanup.

5. A plausible cleanup failure

The instance is stopped and its root volume is still listed. Which next action best matches a completed disposable lab?

A. Leave it stopped indefinitely. B. Rename the instance. C. Save needed evidence, terminate the exact lab instance, and verify its lab-owned volume is removed. D. Delete the account's default VPC.

Answer: C. Stopped machines retain attached EBS volumes, which can remain billable. Do not delete shared networking merely to clean up one exercise.

6. Evidence from Linux

The learner wants the distribution name and the root filesystem's usage. Which pair is most direct?

A. `cat /etc/os-release` and `df -h /`. B. `hostname` and `whoami`. C. `pwd` and `cd /`. D. `ls` and `echo done`.

Answer: A. The OS-release file identifies the distribution; `df` reports mounted filesystem capacity/use. A hostname does not reliably identify the OS distribution.

7. The broad fix

Session Manager is unavailable. Someone suggests opening all inbound ports and attaching AdministratorAccess to the instance. What should happen first?

A. Accept it because this is temporary. B. Launch five more instances. C. Check role, agent, outbound path, account/Region, and human permissions in order. D. Publish the root password.

Answer: C. Those checks target the actual dependencies. Broad permissions and inbound exposure do not diagnose the failing layer.

8. An honest portfolio

A learner completed the tabletop route but has never created an AWS instance. Which portfolio statement fits the evidence?

A. "Deployed and operated EC2 in production." B. "Designed a Session Manager lab, explained its dependencies, and documented predicted cleanup." C. "Reduced my employer's AWS bill." D. "Measured AWS network throughput."

Answer: B. It accurately describes a useful planning artifact. Live claims require live observations; the exercise explicitly supports either route.

Instructor extension: Ask the learner to draw the failed path from Question 2, then distinguish an IAM denial from an offline managed node without changing any settings.

Quick reference

First EC2 Lab - Desk Reference

Shutterbird goal: inspect one temporary Linux machine; produce evidence; remove it.
Prerequisite: authorized learning identity, MFA, budget visibility, approved default network.
Source check: **2026-09-18**.

Component	Choice / check
Region	One recorded commercial Region
AMI	Amazon-published Amazon Linux 2023 standard, x86_64
Instance	One small compatible type; review current pricing
Subnet	Default public subnet, route to attached internet gateway
Network	Public IPv4 enabled; DNS works; default allow ACL
Security group	No inbound; outbound TCP 443
Machine identity	EC2 role/profile with AmazonSSMManagedInstanceCore
Human identity	Permission to start/manage own Session Manager sessions
Root disk	Small gp3, encrypted, delete on termination
Advanced	IMDSv2 required; T3 Standard credits; no user data

Path: human -> Session Manager service ← outbound HTTPS ← SSM Agent on EC2. Both IAM permission sets matter.

```
whoami                          # Linux user
pwd                             # Current working directory
cat /etc/os-release             # Distribution/version
uname -r                        # Kernel
hostname                        # Machine name
lsblk                           # Block devices
df -h /                         # Mounted root filesystem
free -h                         # Memory
systemctl is-active amazon-ssm-agent
```

Connection not ready? Check account/Region -> exact instance -> role/profile -> agent -> address/route/DNS/outbound 443/ACL -> human permission. Keep the inbound list empty.

Cost check: EC2 + EBS + public IPv4 + possible data transfer. Account credits vary. A budget notification is not a spending cap and is not immediate.

Before cleanup: save your observations and record instance, volume, security-group, role/profile IDs. End session -> terminate exact lab instance -> verify volume deletion and automatic address release -> delete only dedicated lab security group/role/profile. Preserve shared network and budget. Recheck cost data after it refreshes.

Portfolio evidence: diagram, budget setup, OS observations, one failure diagnosis, cleanup inventory. Tabletop work must be labeled simulated.

Sources: EC2 launch, Session prerequisites, instance role, human permissions, budgets, termination.