



## AWS Projects Group 4

### Names:

- هاجر سعيد السيد علي
- اسامه جمال عبدالعزيز
- محمد احمد محمود
- محمد سعد محمد علي

# Project 6 : Exploring AWS Identity and Access Management (IAM)

## **Open the Environment on CLI**

we are using the AWS CLI in a terminal environment. Make sure the AWS CLI is installed and configured with AWS credentials and region.

- Open Terminal
- Configure AWS CLI

\* Provide the necessary inputs for:

- AWS Access Key ID
- AWS Secret Access Key
- Default region name (e.g., us-east-1)
- Default output format (e.g., json)

## **Task 1: Explore Users**

### **and Groups Step 1: List**

#### **IAM Users**

List all the IAM users to get an overview of pre-created users.

```
C:\Users\Hagar>aws configure
AWS Access Key ID [*****DPS5]:
AWS Secret Access Key [*****CzsZ]:
Default region name [us-east-1]:
Default output format [json]

C:\Users\Hagar>aws iam list-users
{
  "Users": [
    {
      "Path": "/spl66/",
      "UserName": "user-1",
      "UserId": "AIDA5GVR5MQNA56TN2X4",
      "Arn": "arn:aws:iam::907684963232:user/spl66/user-1",
      "CreateDate": "2024-10-12T17:51:43+00:00"
    },
    {
      "Path": "/spl66/",
      "UserName": "user-2",
      "UserId": "AIDA5GVR5MQLL02LE6L4",
      "Arn": "arn:aws:iam::907684963232:user/spl66/user-2",
      "CreateDate": "2024-10-12T17:51:43+00:00"
    },
    {
      "Path": "/spl66/",
      "UserName": "user-3",
      "UserId": "AIDA5GVR5MQA6RJ6ZRWG",
      "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
      "CreateDate": "2024-10-12T17:51:43+00:00"
    }
  ]
}
```

## Step 2: List IAM Groups

Retrieve a list of all IAM groups

```
C:\Users\Hagar>aws iam list-groups
{
  "Groups": [
    {
      "Path": "/spl66/",
      "GroupName": "EC2-Admin",
      "GroupId": "AGPA5GVR5MQQOMLH4ID5L",
      "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Admin",
      "CreateDate": "2024-10-12T17:51:43+00:00"
    },
    {
      "Path": "/spl66/",
      "GroupName": "EC2-Support",
      "GroupId": "AGPA5GVR5MQQMWF7F632E",
      "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Support",
      "CreateDate": "2024-10-12T17:51:43+00:00"
    },
    {
      "Path": "/spl66/",
      "GroupName": "S3-Support",
      "GroupId": "AGPA5GVR5MQQCSTASWKGX",
      "Arn": "arn:aws:iam::907684963232:group/spl66/S3-Support",
      "CreateDate": "2024-10-12T17:51:43+00:00"
    }
  ]
}

C:\Users\Hagar>
C:\Users\Hagar>
```

### **Step 3: View User Details**

To inspect a specific user, use the following command by replacing <user\_name>with the actual username.

**comand : aws iam get-user --user-name <user\_name>**

```
C:\Users\Hagar>aws iam get-user --user-name user-1
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-1",
        "UserId": "AIDA5GVR5MOQNA56TN2X4",
        "Arn": "arn:aws:iam::907684963232:user/spl66/user-1",
        "CreateDate": "2024-10-12T17:51:43+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a335854817935416t1w907684963232"
            }
        ]
    }
}

C:\Users\Hagar>aws iam get-user --user-name user-2
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-2",
        "UserId": "AIDA5GVR5MOQLL02LE6L4",
        "Arn": "arn:aws:iam::907684963232:user/spl66/user-2",
        "CreateDate": "2024-10-12T17:51:43+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a335854817935416t1w907684963232"
            }
        ]
    }
}

C:\Users\Hagar>aws iam get-user --user-name user-3
{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDA5GVR5MOQA6RJ6ZRWG",
        "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
        "CreateDate": "2024-10-12T17:51:43+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a335854817935416t1w907684963232"
            }
        ]
    }
}
```

## Step 4: List Users in a Specific Group

To get a list of all users that belong to a specific group,

command : **aws iam get-group --group-name <group\_name>**

```
C:\Users\Hagar>
C:\Users\Hagar>aws iam get-group --group-name EC2-Admin
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA5GVR5MQQOMLH4ID5L",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}

C:\Users\Hagar>aws iam get-group --group-name EC2-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA5GVR5MQQMWF7F632E",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}

C:\Users\Hagar>aws iam get-group --group-name S3-Support
{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA5GVR5MQCSTASWKGX",
        "Arn": "arn:aws:iam::907684963232:group/spl66/S3-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}
```

## Task 2: Inspect IAM Policies

Step 1: List Attached Policies for a Group

```
C:\Users\Hagar>aws iam list-attached-group-policies --group-name EC2-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}

C:\Users\Hagar>aws iam list-attached-group-policies --group-name S3-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        }
    ]
}

C:\Users\Hagar>aws iam list-attached-group-policies --group-name EC2-Admin
{
    "AttachedPolicies": []
}

C:\Users\Hagar>
```

## Step 2: View Policy Details

To view the details of a specific policy attached to the group, use the policy's ARN(Amazon Resource Name) from the previous command's output

```
C:\Users\Hagar>aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess
{
  "Policy": {
    "PolicyName": "AmazonEC2ReadOnlyAccess",
    "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
    "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 1,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
    "CreateDate": "2015-02-06T18:40:17+00:00",
    "UpdateDate": "2024-02-14T18:43:53+00:00",
    "Tags": []
  }
}

C:\Users\Hagar>aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
{
  "Policy": {
    "PolicyName": "AmazonS3ReadOnlyAccess",
    "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
    "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
    "Path": "/",
    "DefaultVersionId": "v3",
    "AttachmentCount": 1,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "Description": "Provides read only access to all buckets via the AWS Management Console.",
    "CreateDate": "2015-02-06T18:40:59+00:00",
    "UpdateDate": "2023-08-10T21:31:39+00:00",
    "Tags": []
  }
}

C:\Users\Hagar>
```

## Task 3: Add Users to Groups

add users to specific groups according to their role requirements.

### Step 1: Add User-1 to S3-Support Group

Grant User-1 read-only access to S3 by adding them to the S3-Support group.

### Step 2: Add User-2 to EC2-Support Group

assign User-2 permissions to read-only access to EC2 resources.

### **Step 3: Add User-3 to EC2-Admin Group**

Assign User-3 permissions to view, start, and stop EC2 instances by adding them to the EC2-Admin group.

```
C:\Users\Hagar>aws iam add-user-to-group --group-name S3-Support --user-name User-1  
C:\Users\Hagar>aws iam add-user-to-group --group-name EC2-Support --user-name User-2  
C:\Users\Hagar>  
C:\Users\Hagar>aws iam add-user-to-group --group-name EC2-Admin --user-name User-3  
C:\Users\Hagar>  
C:\Users\Hagar>
```

### **Step 4: Verify Users are Added to Groups**

Verify that the users are properly added to the groups by listing users within each group

```
C:\Users\Hagar>aws iam get-group --group-name S3-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA5GVR5MQNA56TN2X4",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-1",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA5GVR5MOQCSTASWKGX",
        "Arn": "arn:aws:iam::907684963232:group/spl66/S3-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}

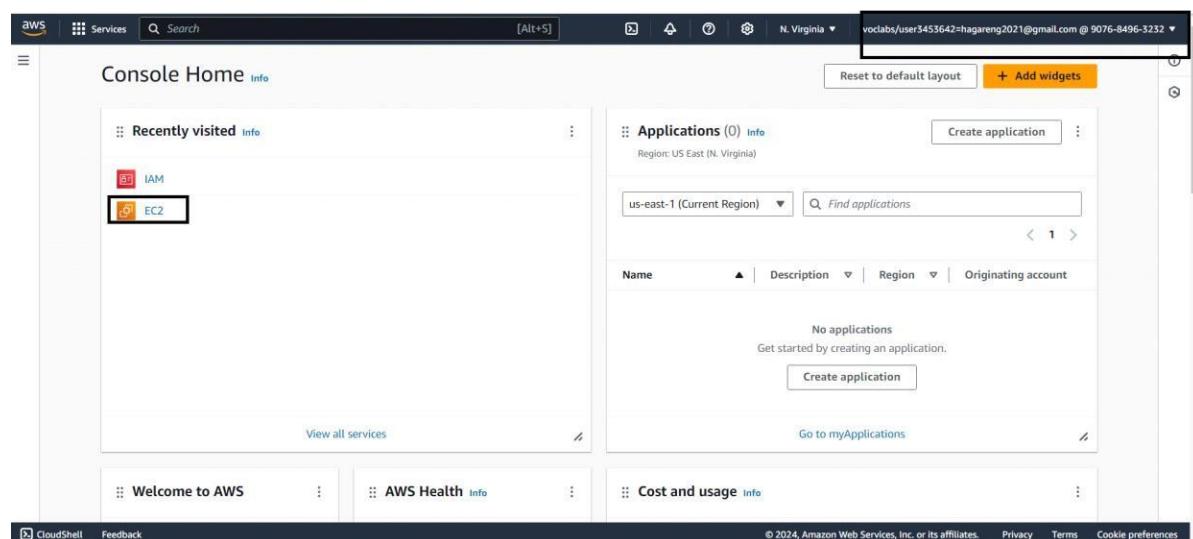
C:\Users\Hagar>aws iam get-group --group-name EC2-Support
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA5GVR5MQA6RJ6ZRWG",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA5GVR5MOQLL02LE6L4",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-2",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA5GVR5MOQMNZ7F632E",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Support",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}
```

```
C:\Users\Hagar>aws iam get-group --group-name EC2-Admin
{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA5GVR5MQQA6RJ6ZRWG",
            "Arn": "arn:aws:iam::907684963232:user/spl66/user-3",
            "CreateDate": "2024-10-12T17:51:43+00:00"
        }
    ],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA5GVR5MQQ0MLH4ID5L",
        "Arn": "arn:aws:iam::907684963232:group/spl66/EC2-Admin",
        "CreateDate": "2024-10-12T17:51:43+00:00"
    }
}
```

```
C:\Users\Hagar>
```

## Task 4: Test Permissions

### Step 1: Get the console sign-in URL



The screenshot shows the AWS IAM Dashboard. On the left, a sidebar lists navigation options like 'Identity and Access Management (IAM)', 'Access management', and 'Access reports'. The main area displays 'IAM resources' (User groups: 3, Users: 3, Roles: 16, Policies: 0, Identity providers: 0) and an 'AWS Account' section with details such as Account ID (907684963232), Account Alias (Create), and a 'Sign-in URL for IAM users' (https://907684963232.signin.aws.amazon.com/console). A red box highlights the sign-in URL field.

## Step 2: User-1 Test S3 Read-only Access:

- Sign in to AWS Management Console as User-1 using the IAM sign-in URL.
- Navigate to the S3 service and try to list buckets.
- Try to perform any write operations (like deleting bucket), which should fail due to read-only access

The screenshot shows the AWS sign-in page for 'User-1'. It includes fields for 'Account ID (12 digits) or account alias' (907684963232), 'IAM user name' (user-1), 'Password', and a 'Remember this account' checkbox. A 'Sign in' button is at the bottom. To the right, there's a sidebar with an 'Amazon Lightsail' advertisement featuring a cartoon robot and the text 'Lightsail is the easiest way to get started on AWS'.

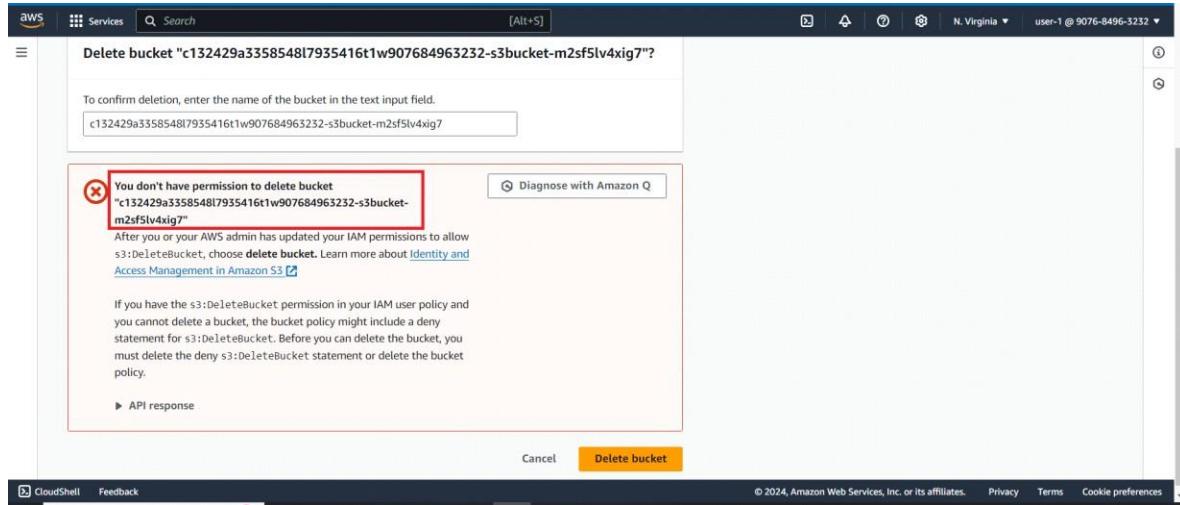
The screenshot shows the AWS Console Home page. At the top right, the user's email 'user-1 @ 9076-8496-3232' is displayed with a red box around it. Below the header, there are several sections: 'Recently visited' (with S3 highlighted), 'Applications' (empty), 'Welcome to AWS', 'AWS Health', and 'Cost and usage'. A search bar and a 'Reset to default layout' button are also present.

The screenshot shows the Amazon S3 service dashboard. On the left, a sidebar lists options like Buckets, Access Grants, and Storage Lens. The main area displays an 'Account snapshot - updated every 24 hours' with a link to 'View Storage Lens dashboard'. Below this is a table for 'General purpose buckets' (1). The first row shows a bucket named 'c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7' with details: AWS Region 'US East (N. Virginia) us-east-1', IAM Access Analyzer 'View analyzer for us-east-1', and Creation date 'October 14, 2024, 00:26:03 (UTC+03:00)'. A red box highlights the bucket name in the table.

The screenshot shows the AWS S3 console interface. On the left, the navigation pane includes sections for Buckets, Storage Lens, and Feature spotlight. The main content area displays a bucket named 'c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7'. The 'Objects' tab is selected, showing a table with one row: 'No objects'. Below the table is a large 'Upload' button. The top right corner shows the user's email: 'user-1 @ 9076-8496-3232'.

This screenshot shows the same AWS S3 console interface. The 'General purpose buckets' section is highlighted with a red arrow labeled '1'. The table lists a single bucket: 'c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7'. A red box highlights the 'Delete' button in the actions column. The top right corner shows the user's email: 'user-1 @ 9076-8496-3232'.

This screenshot shows the 'Delete bucket' confirmation dialog. It contains a warning message about the不可逆性 of deleting a bucket. The user has entered the bucket name 'c132429a3358548l7935416t1w907684963232-s3bucket-m2sf5lv4xig7' into the input field. A red arrow points to this input field. At the bottom are 'Cancel' and 'Delete bucket' buttons, with the latter being highlighted by a red box.



### Step 3: User-2 Test EC2 Read-only Access:

- Sign in as User-2.
- Navigate to the EC2 dashboard.
- Check if User-2 can view instances but cannot modify (start/stop) them

Google Chrome isn't your default browser [Set as default](#)

Try the new sign in UI  
See our new improved Amazon Web Services sign in experience before we officially launch. [Enable new sign in](#)

**aws**

**Sign in as IAM user**

Account ID (12 digits) or account alias

IAM user name

Password

Remember this account

**Sign in**

[Sign in using root user email](#)  
[Forgot password?](#)

**Amazon Lightsail**

Lightsail is the easiest way  
to get started on AWS

[Learn more »](#)



Screenshot of the AWS Console Home page:

The top navigation bar shows "N. Virginia" and the user "user-2 @ 9076-8496-3232".

The "Recently visited" section shows "EC2" and "IAM".

The "Applications" section shows 0 applications, with a message: "Access denied".

The "Cost and usage" section shows 1 instance.

The sidebar includes "Welcome to AWS", "AWS Health", and "CloudShell".

Screenshot of the EC2 Dashboard:

The left sidebar shows "Instances" selected.

The main "Resources" section displays the following table:

Instances (running)	1	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	1
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	3	Snapshots	0	Volumes	1

The "Launch instance" button is highlighted with a red arrow.

The "Service health" section shows an error message: "An error occurred" with a red arrow pointing to it.

The "Account attributes" and "Explore AWS" sections are also visible.

Screenshot of the AWS EC2 Instances page showing a single instance named "i-07157fdb3e25eb54". The instance is running, t2.micro, in us-east-1a, with a Public IPv4 address of ec2-44-220-177-252. A modal window titled "Select an instance" is open over the main list.

EC2 Dashboard | EC2 Global View | Events | Instances | Instance Types | Launch Templates | Spot Requests | Savings Plans | Reserved Instances | Dedicated Hosts | Capacity Reservations | Images | AMIs | AMI Catalog | Elastic Block Store | Volumes | Snapshots | Lifecycle Manager | CloudShell

Last updated 1 minute ago | Connect | Instance state | Actions | Launch instances

Find Instance by attribute or tag (case-sensitive) | All states

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPV4
i-07157fdb3e25eb54	i-07157fdb3e25eb54	Running	t2.micro	2/2 checks passed	View alarms	us-east-1a	ec2-44-220-177-252

Select an instance

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Instances page showing the detailed "Instance summary" for the instance "i-07157fdb3e25eb54". The instance is running, t2.micro, with a Public IPv4 address of 44.220.177.252 and a Private IP DNS name of ip-10-1-11-171.ec2.internal. It is associated with a VPC ID of vpc-0dfid59c61855d73fa (Lab VPC).

EC2 Dashboard | EC2 Global View | Events | Instances | Instance Types | Launch Templates | Spot Requests | Savings Plans | Reserved Instances | Dedicated Hosts | Capacity Reservations | Images | AMIs | AMI Catalog | Elastic Block Store | Volumes | Snapshots | Lifecycle Manager | Feedback

EC2 > Instances > i-07157fdb3e25eb54

Instance summary for i-07157fdb3e25eb54

Updated 1 minute ago

Instance ID i-07157fdb3e25eb54	Public IPv4 address 44.220.177.252 [open address]	Private IPv4 addresses 10.1.11.171
IPv6 address -	Instance state Running	Public IPv4 DNS ec2-44-220-177-252.compute-1.amazonaws.com [open address]
Hostname type IP name: ip-10-1-11-171.ec2.internal	Private IP DNS name (IPv4 only) ip-10-1-11-171.ec2.internal	Elastic IP addresses -
Answer private resource DNS name -	Instance type t2.micro	AWS Compute Optimizer finding <small>User: arn:aws:iam::907684963232:user/spl66/user-2 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: * because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action</small>
Auto-assigned IP address 44.220.177.252 [Public IP]	VPC ID vpc-0dfid59c61855d73fa (Lab VPC)	Retry
IAM Role -	Subnet ID subnet-026d5b063839be271 (Public Subnet 1)	Auto Scaling Group name -

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Instances (1/1) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Instance state ▲ Actions ▲ Launch Instances ▲

Stop instance Start instance Reboot instance Hibernate instance

Availability Zone ▲ Public IP

us-east-1a ec2-44-220-177-252.compute-1.amazonaws.com

1 Instances

2 i-07157fdbbe3e25eb54

3 Running t2.micro

4 Terminate (delete) instance

Instances (1/1) Info

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Instance state ▲ Actions ▲ Launch Instances ▲

Stop instance Start instance Reboot instance Hibernate instance

Availability Zone ▲ Public IP

us-east-1a ec2-44-220-177-252.compute-1.amazonaws.com

1 Instances

2 i-07157fdbbe3e25eb54

3 Terminating

4 Terminate (delete) instance

5

6

7

8

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

29

30

31

32

33

34

35

36

37

38

39

40

41

42

43

44

45

46

47

48

49

50

51

52

53

54

55

56

57

58

59

60

61

62

63

64

65

66

67

68

69

70

71

72

73

74

75

76

77

78

79

80

81

82

83

84

85

86

87

88

89

90

91

92

93

94

95

96

97

98

99

100

101

102

103

104

105

106

107

108

109

110

111

112

113

114

115

116

117

118

119

120

121

122

123

124

125

126

127

128

129

130

131

132

133

134

135

136

137

138

139

140

141

142

143

144

145

146

147

148

149

150

151

152

153

154

155

156

157

158

159

160

161

162

163

164

165

166

167

168

169

170

171

172

173

174

175

176

177

178

179

180

181

182

183

184

185

186

187

188

189

190

191

192

193

194

195

196

197

198

199

200

201

202

203

204

205

206

207

208

209

210

211

212

213

214

215

216

217

218

219

220

221

222

223

224

225

226

227

228

229

230

231

232

233

234

235

236

237

238

239

240

241

242

243

244

245

246

247

248

249

250

251

252

253

254

255

256

257

258

259

260

261

262

263

264

265

266

267

268

269

270

271

272

273

274

275

276

277

278

279

280

281

282

283

284

285

286

287

288

289

290

291

292

293

294

295

296

297

298

299

300

301

302

303

304

305

306

307

308

309

310

311

312

313

314

315

316

317

318

319

320

321

322

323

324

325

326

327

328

329

330

331

332

333

334

335

336

337

338

339

340

341

342

343

344

345

346

347

348

349

350

351

352

353

354

355

356

357

358

359

360

361

362

363

364

365

366

367

368

369

370

371

372

373

374

375

376

377

378

379

380

381

382

383

384

385

386

387

388

389

390

391

392

393

394

395

396

397

398

399

400

401

402

403

404

405

406

407

408

409

410

411

412

413

414

415

416

417

418

419

420

421

422

423

424

425

426

427

428

429

430

431

432

433

434

435

436

437

438

439

440

441

442

443

444

445

446

447

448

449

450

451

452

453

454

455

456

457

458

459

460

461

462

463

464

465

466

467

468

469

470

471

472

473

474

475

476

477

478

479

480

481

482

483

484

485

486

487

488

489

490

491

492

493

494

495

496

497

498

499

500

501

502

503

504

505

506

507

508

509

510

511

512

513

514

515

516

517

518

519

520

521

522

523

524

525

526

527

528

529

530

531

532

533

534

535

536

537

538

539

540

541

542

543

544

545

546

547

548

549

550

551

552

553

554

555

556

557

558

559

560

561

562

563

564

565

566

567

568

569

570

571

572

573

574

575

576

577

578

579

580

581

582

583

584

585

586

587

588

589

590

591

592

593

594

595

596

597

598

599

600

601

602

603

604

605

606

607

608

609

610

611

612

613

614

615

616

617

618

619

620

621

622

623

624

625

626

627

628

629

630

631

632

633

634

635

636

637

638

639

640

641

642

643

644

645

646

647

648

649

650

651

652

653

654

655

656

657

658

659

660

661

662

663

664

665

666

667

668

669

670

671

672

673

674

675

676

677

678

679

680

681

682

683

684

685

686

687

688

689

690

691

692

693

694

695

696

697

698

699

700

701

702

703

704

705

706

707

708

709

710

711

712

713

714

715

716

717

718

719

720

721

722

723

724

725

726

727

728

729

730

731

732

733

734

735

736

737

738

739

740

741

742

743

744

745

746

747

748

749

750

751

752

753

754

755

756

757

758

759

760

761

762

763

764

765

766

767

768

769

770

771

772

773

774

775

776

777

778

779

780

781

782

783

784

785

786

787

788

789

790

791

792

793

794

795

796

797

798

799

800

801

802

803

804

805

806

807

808

809

810

811

812

813

814

815

816

817

818

819

820

821

822

823

824

825

826

827

828

829

830

831

832

833

834

835

836

837

838

839

840

841

842

843

844

845

846

847

848

849

850

851

852

853

854

855

856

857

858

859

860

861

862

863

864

865

866

867

868

869

870

871

872

873

874

875

876

877

878

879

880

881

882

883

884

885

886

887

888

889

890

891

892

893

894

895

896

897

898

899

900

901

902

903

904

905

906

907

908

909

910

911

912

913

914

915

916

917

918

919

920

921

922

923

924

925

926

927

928

929

930

931

932

933

934

935

936

937

938

939

940

941

942

943

944

945

946

947

948

949

950

951

952

953

954

955

956

957

958

959

960

961

962

963

964

965

966

967

968

969

970

971

972

973

974

975

976

977

978

979

980

981

982

983

984

985

986

987

988

989

990

991

992

993

994

995

996

997

998

999

1000

The screenshot shows the AWS EC2 Instances page. On the left, a sidebar lists various services: EC2 Dashboard, EC2 Global View, Events, Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), and Elastic Block Store (Volumes, Snapshots, Lifecycle Manager). The main content area displays a single instance, **i-07157fdbbe3e25eb54**. The instance summary table includes the following details:

	Value
Instance ID	i-07157fdbbe3e25eb54
IPv6 address	-
Hostname type	Private IP/DNS name (IPv4 only)
Public IPv4 address	44.220.177.252   open address
Instance state	Running
Private IPv4 addresses	10.1.11.171
Public IPv4 DNS	ec2-44-220-177-252.compute-1.amazonaws.com   open address

Below the table, there are links for Details, Status and alarms, Monitoring, Security, Networking, Storage, and Tags. At the bottom of the page, there are links for © 2024, Amazon Web Services, Inc. or its affiliates., Privacy, Terms, and Cookie preferences.

## Step 4: User-3 Test EC2 Admin Access:

- Sign in as User-3.
- Navigate to the EC2 dashboard.
- Verify that User-3 can view, start, and stop EC2 instances

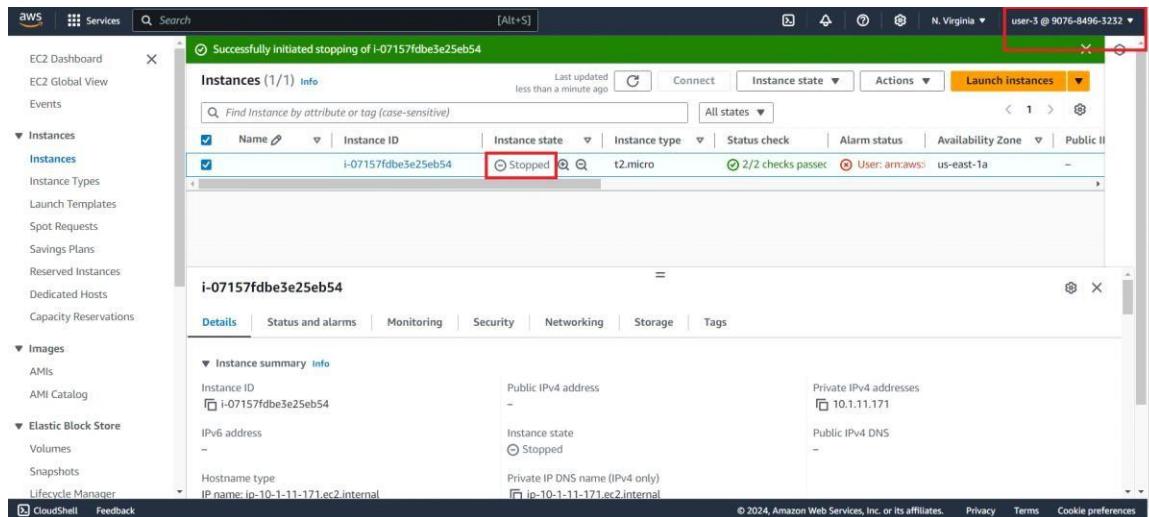
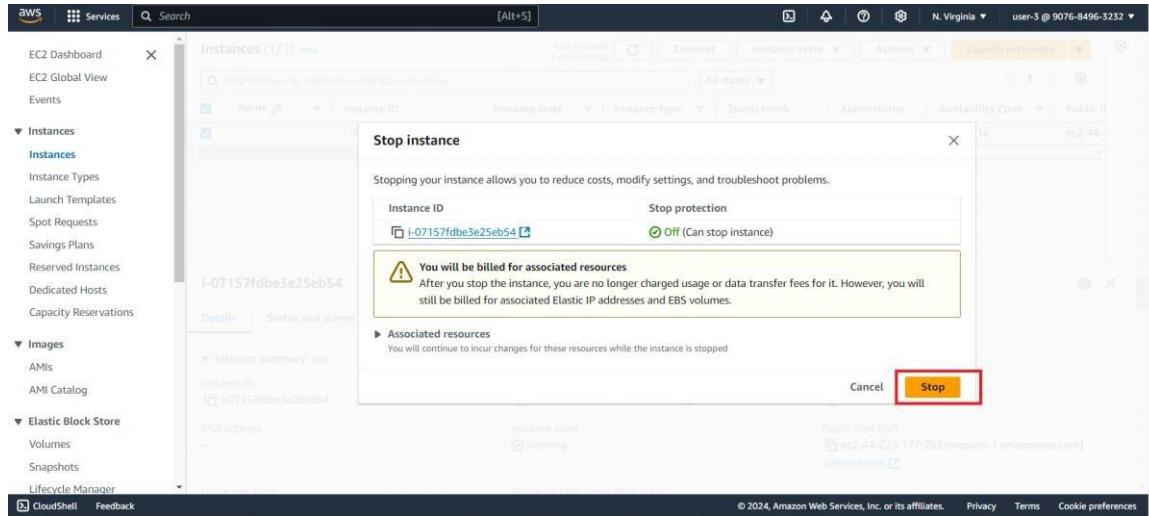
The screenshot shows the AWS sign-in page. At the top, there is a message: "Try the new sign in UI! See our new improved Amazon Web Services sign in experience before we officially launch." Below this is a "Enable new sign in" button. The main form is titled "Sign in as IAM user". It contains the following fields:

- Account ID (12 digits) or account alias: 907684963232
- IAM user name: user-3
- Password: [REDACTED]
- Remember this account

At the bottom of the form is a "Sign in" button. To the right of the form, there is a promotional banner for "Amazon Lightsail" with the text: "Lightsail is the easiest way to get started on AWS" and a "Learn more »" button. There is also a cartoon robot icon.

The screenshot shows the AWS Console Home page. At the top right, the user information "user-3 @ 9076-8496-3232" is highlighted with a red box. Below it, there are two main sections: "Recently visited" (IAM, EC2) and "Applications (0)". The "EC2" link in the "Recently visited" section is also highlighted with a red box. The "Applications" section shows a single entry for "us-east-1 (Current Region)" with a search bar "Find applications". A message "Access denied" is displayed in a box. At the bottom, there are links for "View all services", "Go to myApplications", "Welcome to AWS", "AWS Health", and "Cost and usage". The footer includes links for "CloudShell", "Feedback", and copyright information "© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences".

The screenshot shows the AWS EC2 Instances page. On the left, the navigation menu is expanded to show "Instances" (selected and highlighted with a red box), "Images", and "Elastic Block Store". Under "Instances", sub-options like "Instance Types", "Launch Templates", and "Spot Requests" are listed. The main content area displays a table titled "Instances (1/1) Info" with one row for instance "i-07157fdbbe3e25eb54", which is "Running". The "Actions" dropdown menu is open, with the "Stop instance" option highlighted with a red box. The "Actions" menu also includes "Start instance", "Reboot instance", "Hibernate instance", and "Terminate (delete) instance". The instance details page for "i-07157fdbbe3e25eb54" is shown below, with tabs for "Details", "Status and alarms", "Monitoring", "Security", "Networking", "Storage", and "Tags". The "Details" tab is active, showing "Instance summary" with fields for Instance ID, Public IPv4 address (44.220.177.252), Private IPv4 addresses (10.1.11.171), Instance state (Running), Public IPv4 DNS (ec2-44-220-177-252.compute-1.amazonaws.com), and Private IP DNS name (IPv4 only). The footer includes "CloudShell" and "Feedback" links.



AWS Academy

ACAv3EN... > Assignments  
Guided Lab: Exploring AWS Identity and Access Management (IAM)

Home Modules Discussions Grades Lucid (Whiteboard)

Dashboard Calendar Inbox History Help

Guided Lab: Exploring AWS Identity and Access Management (IAM)

Due No Due Date Points 56 Submitting an external tool

AWS 00:54 Start Lab End Lab AWS Details Details

EN\_US

**Guided Lab:  
Exploring AWS  
Identity and Access  
Management (IAM)**

**Lab overview and  
objectives**

Total score 15/15

[Task 2A] Check user-1 iam group 5/5

[Task 2B] Check user-2 iam group 5/5

[Task 2C] Check user-3 iam group 5/5

Submission Oct 12 at 10:45pm Submission Details

Grade: 56 (56 pts possible)  
Graded Anonymously: no

Comments: No Comments

This screenshot shows the AWS Academy interface for a guided lab titled 'Exploring AWS Identity and Access Management (IAM)'. The left sidebar includes links for Account, Dashboard, Calendar, Inbox, History, and Help. The main content area displays the lab title and objectives. At the top right, there are submission details: 'Oct 12 at 10:45pm', 'Submission Details', 'Grade: 56 (56 pts possible)', and 'Graded Anonymously: no'. Below these are 'Comments' and 'No Comments'. The central part of the screen shows the lab results with a total score of 15/15. The results list three tasks: 'Check user-1 iam group' (5/5), 'Check user-2 iam group' (5/5), and 'Check user-3 iam group' (5/5). The bottom of the page has navigation links for Start Lab, End Lab, AWS Details, and Details.

# Project 6 :Identity and Access Management (IAM) lab

## 1. Open the Environment on CLI

Start by ensuring you are using the AWS CLI in a terminal environment. Make sure the AWS CLI is installed and properly configured with the correct AWS credentials and region.

- Open Terminal
- Configure AWS CLI
  - Provide the necessary inputs for:
  - AWS Access Key ID
  - AWS Secret Access Key
  - Default region name (e.g., us-east-1)
  - Default output format (e.g., json)



The screenshot shows a terminal window titled 'root@kali: ~'. The window has a dark theme with white text. The terminal is running the command 'aws configure'. It displays four configuration prompts:

- AWS Access Key ID [\*\*\*\*\*2GBN]:
- AWS Secret Access Key [\*\*\*\*\*ffno]:
- Default region name [us-east-1]:
- Default output format [json]:

The user has not yet entered any values for these fields.

## 2. Task 1: Explore Users and Groups

### Step 1: List IAM Users

List all the IAM users to get an overview of pre-created users.

```
(root㉿kali)-[~]
# aws iam list-users

{
    "Users": [
        {
            "Path": "/spl66/",
            "UserName": "user-1",
            "UserId": "AIDA2CTFHBEV4AUHZGIZZ",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-2",
            "UserId": "AIDA2CTFHBEV6W4MDCTIL",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        },
        {
            "Path": "/spl66/",
            "UserName": "user-3",
            "UserId": "AIDA2CTFHBEV3D3PPDNGT",
            "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
            "CreateDate": "2024-09-27T12:23:54+00:00"
        }
    ]
}
```

## Step 2: List IAM Groups

Retrieve a list of all IAM groups.

```
(root㉿kali)-[~]
# aws iam list-groups

{
  "Groups": [
    {
      "Path": "/spl66/",
      "GroupName": "EC2-Admin",
      "GroupId": "AGPA2CTFHBEVWF7N6KMVY",
      "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
      "CreateDate": "2024-09-27T12:23:54+00:00"
    },
    {
      "Path": "/spl66/",
      "GroupName": "EC2-Support",
      "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
      "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
      "CreateDate": "2024-09-27T12:23:54+00:00"
    },
    {
      "Path": "/spl66/",
      "GroupName": "S3-Support",
      "GroupId": "AGPA2CTFHBEV7R2X36ALH",
      "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
      "CreateDate": "2024-09-27T12:23:54+00:00"
    }
  ]
}
```

### Step 3: View User Details

To inspect a specific user, use the following command by replacing <user\_name> with the actual username.

**aws iam get-user --user-name <user\_name>**

```
(root㉿kali)-[~]
└─# aws iam get-user --user-name user-1

{
  "User": {
    "Path": "/spl66/",
    "UserName": "user-1",
    "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
    "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
    "CreateDate": "2024-09-27T12:23:54+00:00",
    "Tags": [
      {
        "Key": "cloudlab",
        "Value": "c132429a3358548l7753975t1w692775749931"
      }
    ]
  }
}
```

```
(root㉿kali)-[~]
└─# aws iam get-user --user-name user-2

{
  "User": {
    "Path": "/spl66/",
    "UserName": "user-2",
    "UserId": "AIDA2CTFHBEV6W4MDCTIL",
    "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
    "CreateDate": "2024-09-27T12:23:54+00:00",
    "Tags": [
      {
        "Key": "cloudlab",
        "Value": "c132429a3358548l7753975t1w692775749931"
      }
    ]
  }
}
```

```
[root@kali]~]
# aws iam get-user --user-name user-3

{
    "User": {
        "Path": "/spl66/",
        "UserName": "user-3",
        "UserId": "AIDA2CTFHBEV3D3PPDNGT",
        "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
        "CreateDate": "2024-09-27T12:23:54+00:00",
        "Tags": [
            {
                "Key": "cloudlab",
                "Value": "c132429a3358548l7753975t1w692775749931"
            }
        ]
    }
}
```

#### Step 4: List Users in a Specific Group

To get a list of all users that belong to a specific group, replace <group\_name> with the group name.

aws iam get-group --group-name <group\_name>

```
[root@kali]~]
# aws iam get-group --group-name S3-Support

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "S3-Support",
        "GroupId": "AGPA2CTFHBEV7R2X36ALH",
        "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}

[root@kali]~]
# aws iam get-group --group-name EC2-Support

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Support",
        "GroupId": "AGPA2CTFHBEVRVQG2MSMB",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}

[root@kali]~]
# aws iam get-group --group-name EC2-Admin

{
    "Users": [],
    "Group": {
        "Path": "/spl66/",
        "GroupName": "EC2-Admin",
        "GroupId": "AGPA2CTFHBEVWF7N6KMYV",
        "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
        "CreateDate": "2024-09-27T12:23:54+00:00"
    }
}
```

### 3. Task 2: Inspect IAM Policies

#### Step 1: List Attached Policies for a Group

This command lists all policies attached to a specific group.

```
└─(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name S3-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonS3ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess"
        }
    ]
}

└─(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name EC2-Support
{
    "AttachedPolicies": [
        {
            "PolicyName": "AmazonEC2ReadOnlyAccess",
            "PolicyArn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess"
        }
    ]
}

└─(root㉿kali)-[~]
└─# aws iam list-attached-group-policies --group-name EC2-Admin
{
    "AttachedPolicies": []
}
```

#### Step 2: View Policy Details

To view the details of a specific policy attached to the group, use the policy's ARN (Amazon Resource Name) from the previous command's output.

```
└─(root㉿kali)-[~]
└─# aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonEC2ReadOnlyAccess",
        "PolicyId": "ANPAIGDT4SV4GSETWTBZK",
        "Arn": "arn:aws:iam::aws:policy/AmazonEC2ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v1",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to Amazon EC2 via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:17+00:00",
        "UpdateDate": "2024-02-14T18:43:53+00:00",
        "Tags": []
    }
}
```

```
[root@kali]# aws iam get-policy --policy-arn arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess
{
    "Policy": {
        "PolicyName": "AmazonS3ReadOnlyAccess",
        "PolicyId": "ANPAIZTJ4DXE7G6AGAE6M",
        "Arn": "arn:aws:iam::aws:policy/AmazonS3ReadOnlyAccess",
        "Path": "/",
        "DefaultVersionId": "v3",
        "AttachmentCount": 1,
        "PermissionsBoundaryUsageCount": 0,
        "IsAttachable": true,
        "Description": "Provides read only access to all buckets via the AWS Management Console.",
        "CreateDate": "2015-02-06T18:40:59+00:00",
        "UpdateDate": "2023-08-10T21:31:39+00:00",
        "Tags": []
    }
}
```

#### 4. Task 3: Add Users to Groups

Now, add users to specific groups according to their role requirements.

##### Step 1: Add User-1 to S3-Support Group

Grant User-1 read-only access to S3 by adding them to the S3-Support group.

```
[root@kali]# aws iam add-user-to-group --user-name User-1 --group-name S3-Support
```

##### Step 2: Add User-2 to EC2-Support Group

Give User-2 read-only access to EC2 resources.

```
[root@kali]# aws iam add-user-to-group --user-name User-2 --group-name EC2-Support
```

##### Step 3: Add User-3 to EC2-Admin Group

Assign User-3 permissions to view, start, and stop EC2 instances by adding them to the EC2-Admin group.

```
[root@kali]# aws iam add-user-to-group --user-name User-3 --group-name EC2-Admin
```

## Step 4: Verify Users are Added to Groups

Verify that the users are properly added to the respective groups by listing users within each group.

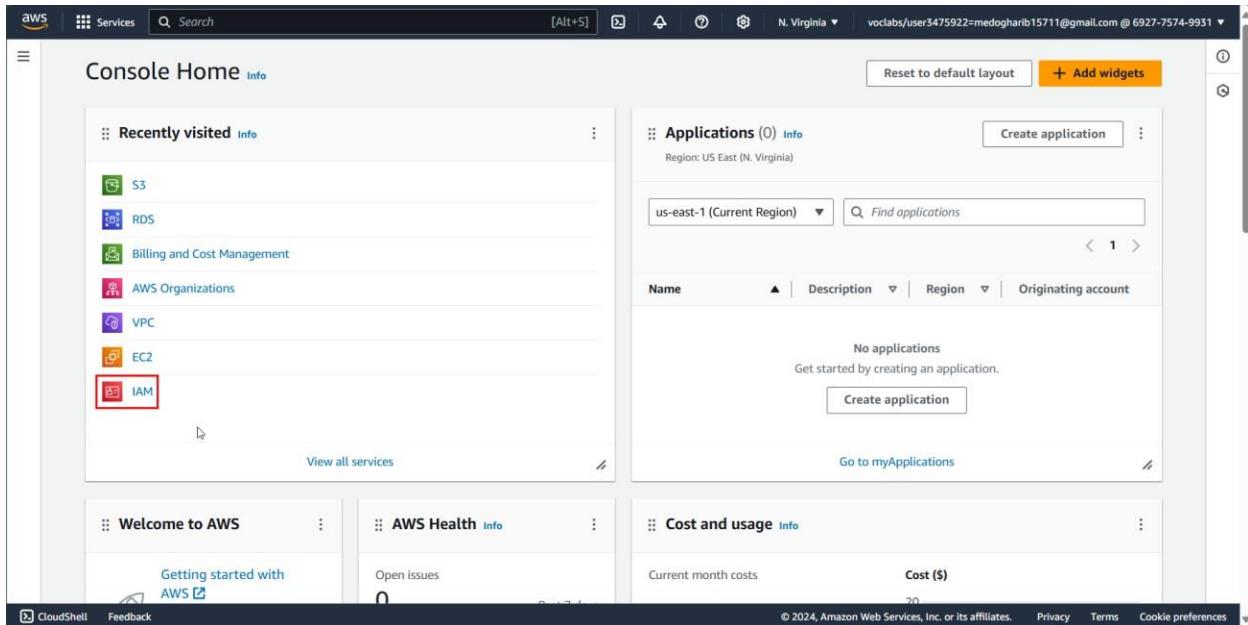
```
[root@kali)-[~]
└─# aws iam get-group --group-name S3-Support
{
  "Users": [
    {
      "Path": "/spl66/",
      "UserName": "user-1",
      "UserId": "AIDA2CTFHBEV4AUHZGIZ2",
      "Arn": "arn:aws:iam::692775749931:user/spl66/user-1",
      "CreateDate": "2024-09-27T12:23:54+00:00"
    }
  ],
  "Group": {
    "Path": "/spl66/",
    "GroupName": "S3-Support",
    "GroupId": "AGPA2CTFHBEV7R2X36ALH",
    "Arn": "arn:aws:iam::692775749931:group/spl66/S3-Support",
    "CreateDate": "2024-09-27T12:23:54+00:00"
  }
}
```

```
[root@kali)-[~]
└─# aws iam get-group --group-name EC2-Support
{
  "Users": [
    {
      "Path": "/spl66/",
      "UserName": "user-2",
      "UserId": "AIDA2CTFHBEV6W4MDCTIL",
      "Arn": "arn:aws:iam::692775749931:user/spl66/user-2",
      "CreateDate": "2024-09-27T12:23:54+00:00"
    }
  ],
  "Group": {
    "Path": "/spl66/",
    "GroupName": "EC2-Support",
    "GroupId": "AGPA2CTFHBEVRVQG2M5MB",
    "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Support",
    "CreateDate": "2024-09-27T12:23:54+00:00"
  }
}
```

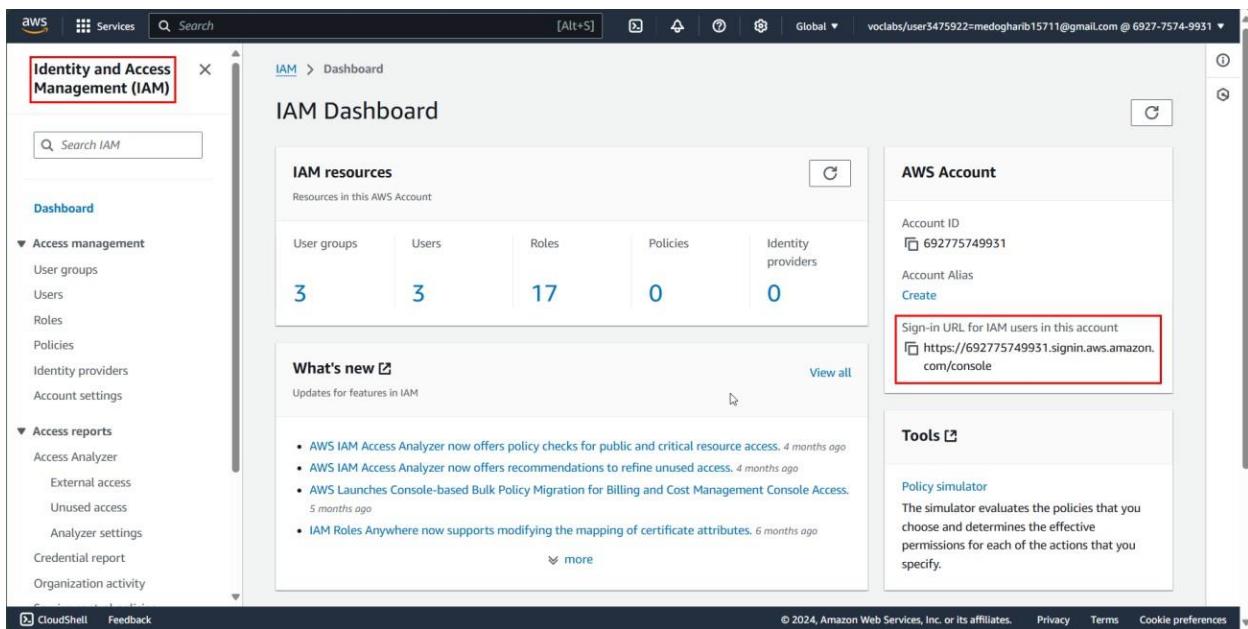
```
[root@kali)-[~]
└─# aws iam get-group --group-name EC2-Admin
{
  "Users": [
    {
      "Path": "/spl66/",
      "UserName": "user-3",
      "UserId": "AIDA2CTFHBEV3D3PPDNGT",
      "Arn": "arn:aws:iam::692775749931:user/spl66/user-3",
      "CreateDate": "2024-09-27T12:23:54+00:00"
    }
  ],
  "Group": {
    "Path": "/spl66/",
    "GroupName": "EC2-Admin",
    "GroupId": "AGPA2CTFHBEWF7N6KMVY",
    "Arn": "arn:aws:iam::692775749931:group/spl66/EC2-Admin",
    "CreateDate": "2024-09-27T12:23:54+00:00"
  }
}
```

## 5. Task 4: Test Permissions

### Step 1: Get the console sign-in URL



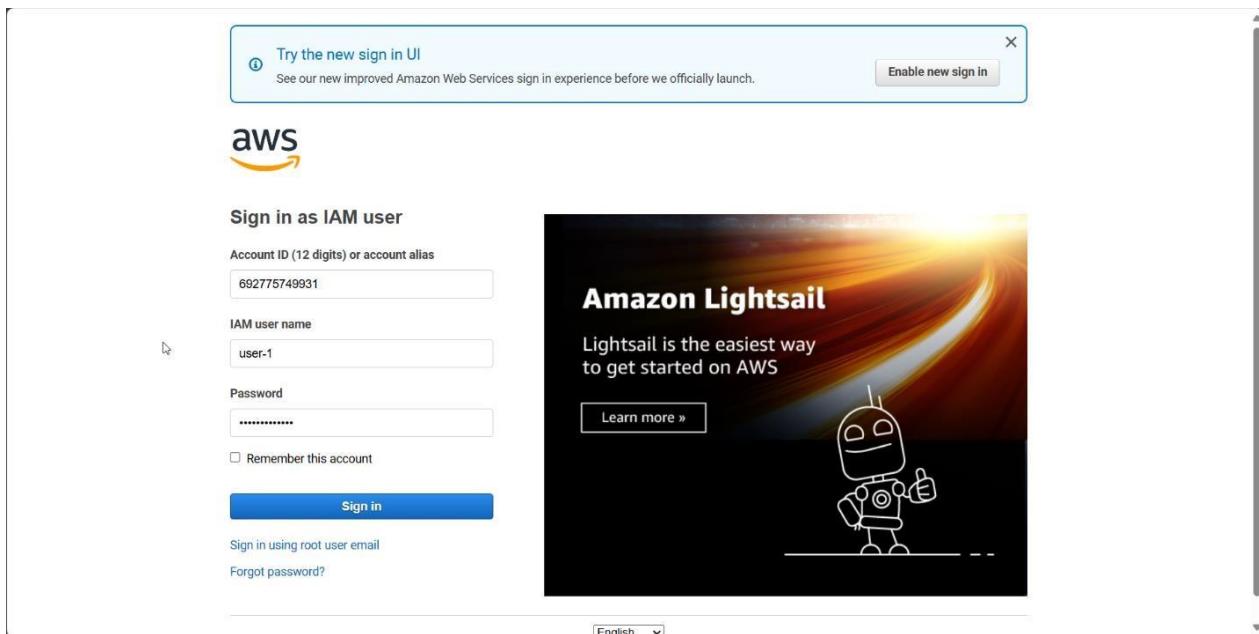
The screenshot shows the AWS Console Home page. On the left, under 'Recently visited' services, 'IAM' is highlighted with a red box. Other visible services include S3, RDS, Billing and Cost Management, AWS Organizations, VPC, and EC2. To the right, there's a section for 'Applications' which is currently empty. Below that is a 'Cost and usage' summary showing current month costs of \$20. At the bottom, there are links for CloudShell, Feedback, and cookie preferences.



The screenshot shows the IAM Dashboard. The left sidebar has 'Identity and Access Management (IAM)' selected with a red box. Under 'Access management', 'User groups', 'Users', 'Roles', 'Policies', 'Identity providers', and 'Account settings' are listed. Under 'Access reports', 'Access Analyzer', 'External access', 'Unused access', 'Analyzer settings', 'Credential report', and 'Organization activity' are listed. The main dashboard shows 'IAM resources' with counts: User groups (3), Users (3), Roles (17), Policies (0), and Identity providers (0). A 'What's new' section lists recent updates. On the right, the 'AWS Account' panel displays the account ID (692775749931) and a 'Sign-in URL for IAM users in this account' field containing the URL <https://692775749931.signin.aws.amazon.com/console>. The 'Tools' panel includes a 'Policy simulator' link.

## Step 2: User-1 Test S3 Read-only Access:

- Sign in to AWS Management Console as User-1 using the IAM sign-in URL.
- Navigate to the S3 service and try to list buckets.
- Try to perform any write operations (like deleting bucket), which should fail due to read-only access.



The screenshot shows the AWS Console Home page. In the top left, under 'Recently visited', the 'S3' icon is highlighted with a red box. Other items in this section include 'EC2'. On the right side, there is a 'Applications' section showing '(0)' applications, with a note 'Access denied' in a red box. Below this, there are sections for 'Cost and usage' (showing 'Access denied' for both current month costs and cost breakdown) and 'Welcome to AWS' (with a link to 'Getting started with AWS'). The bottom of the page includes standard navigation links like CloudShell, Feedback, and copyright information.

AWS Services Search [Alt+S] N. Virginia user-1 @ 6927-7574-9931

### Amazon S3

Buckets Access Grants Access Points Object Lambda Access Points Multi-Region Access Points Batch Operations IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens Dashboards Storage Lens groups AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

CloudShell Feedback

### Amazon S3

Account snapshot - updated every 24 hours All AWS Regions Storage lens provides visibility into storage usage and activity trends. Learn more View Storage Lens dashboard

General purpose buckets Directory buckets

General purpose buckets (1) Info All AWS Regions Buckets are containers for data stored in S3.

Name	AWS Region	IAM Access Analyzer	Creation date
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2	US East (N. Virginia) us-east-1	View analyzer for us-east-1	October 6, 2024, 03:41:13 (UTC+03:00)

Find buckets by name

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the AWS S3 service page. On the left, there's a sidebar with navigation links like Buckets, Storage Lens, and Feature spotlight. The main area displays an account snapshot and a list of general purpose buckets. One bucket is highlighted with a red box: 'c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2'. This bucket is located in the US East (N. Virginia) region and was created on October 6, 2024, at 03:41:13 UTC+03:00. The bucket name is also highlighted with a red box.

AWS Services Search [Alt+S] N. Virginia user-1 @ 6927-7574-9931

### Amazon S3

Buckets Access Grants Access Points Object Lambda Access Points Multi-Region Access Points Batch Operations IAM Access Analyzer for S3

Block Public Access settings for this account

Storage Lens Dashboards Storage Lens groups AWS Organizations settings

Feature spotlight

AWS Marketplace for S3

CloudShell Feedback

### Amazon S3 > Buckets > c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2

#### c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2

Objects Properties Permissions Metrics Management Access Points

Objects (0) Info

Upload Copy S3 URI Copy URL Download Open Actions Create folder

Objects are the fundamental entities stored in Amazon S3. You can use [Amazon S3 inventory](#) to get a list of all objects in your bucket. For others to access your objects, you'll need to explicitly grant them permissions. [Learn more](#)

Find objects by prefix

Name	Type	Last modified	Size	Storage class
No objects				
You don't have any objects in this bucket.				

Upload

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

The screenshot shows the details page for a specific S3 bucket. The left sidebar is identical to the previous screenshot. The main area shows the bucket name 'c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2' and its location. Below this, there's a tab bar with 'Objects' selected. The 'Objects (0)' section shows a table with columns for Name, Type, Last modified, Size, and Storage class. A message indicates 'No objects' and 'You don't have any objects in this bucket.' There's also a prominent 'Upload' button.

Screenshot of the AWS S3 Buckets page.

The left sidebar shows:

- Buckets
- Access Grants
- Access Points
- Object Lambda Access Points
- Multi-Region Access Points
- Batch Operations
- IAM Access Analyzer for S3
- Block Public Access settings for this account
- Storage Lens
- Dashboards
- Storage Lens groups
- AWS Organizations settings

The main content area shows the "General purpose buckets" section with one item:

Name	AWS Region	IAM Access Analyzer	Creation date
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2	US East (N. Virginia) us-east-1	<a href="#">View analyzer for us-east-1</a>	October 6, 2024, 03:41:13 (UTC+03:00)

Actions available for the bucket include: Copy ARN, Empty, Delete (highlighted with a red box), and Create bucket.

Screenshot of the "Delete bucket" confirmation dialog.

The top navigation bar shows the path: Amazon S3 > Buckets > c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2 > Delete bucket.

The dialog title is "Delete bucket" with an info link.

A warning message box contains:

- ⚠ Deleting a bucket cannot be undone.
- Bucket names are unique. If you delete a bucket, another AWS user can use the name.
- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

[Learn more](#)

The main content area asks: "Delete bucket \"c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2\"?"

To confirm deletion, enter the name of the bucket in the text input field:  
c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2

Buttons: Cancel (grayed out), Delete bucket (highlighted with a red box).

aws Services Q Search [Alt+S] N. Virginia user-1 @ 6927-7574-9931 ⓘ

☰

- If this bucket is used with a Multi-Region Access Point in an external account, initiate failover before deleting the bucket.
- If this bucket is used with an access point in an external account, the requests made through those access points will fail after you delete this bucket.

[Learn more](#) ⓘ

Delete bucket "c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2"

To confirm deletion, enter the name of the bucket in the text input field.

c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2

 You don't have permission to delete bucket  
"c132429a3358548l7753975t1w692775749931-s3bucket-wzacuw342nr2" ⓘ

[Diagnose with Amazon Q](#)

After you or your AWS admin has updated your IAM permissions to allow s3:DeleteBucket, choose **delete bucket**. Learn more about [Identity and Access Management in Amazon S3](#) ⓘ

If you have the s3:DeleteBucket permission in your IAM user policy and you cannot delete a bucket, the bucket policy might include a deny statement for s3:DeleteBucket. Before you can delete the bucket, you must delete the deny s3:DeleteBucket statement or delete the bucket policy.

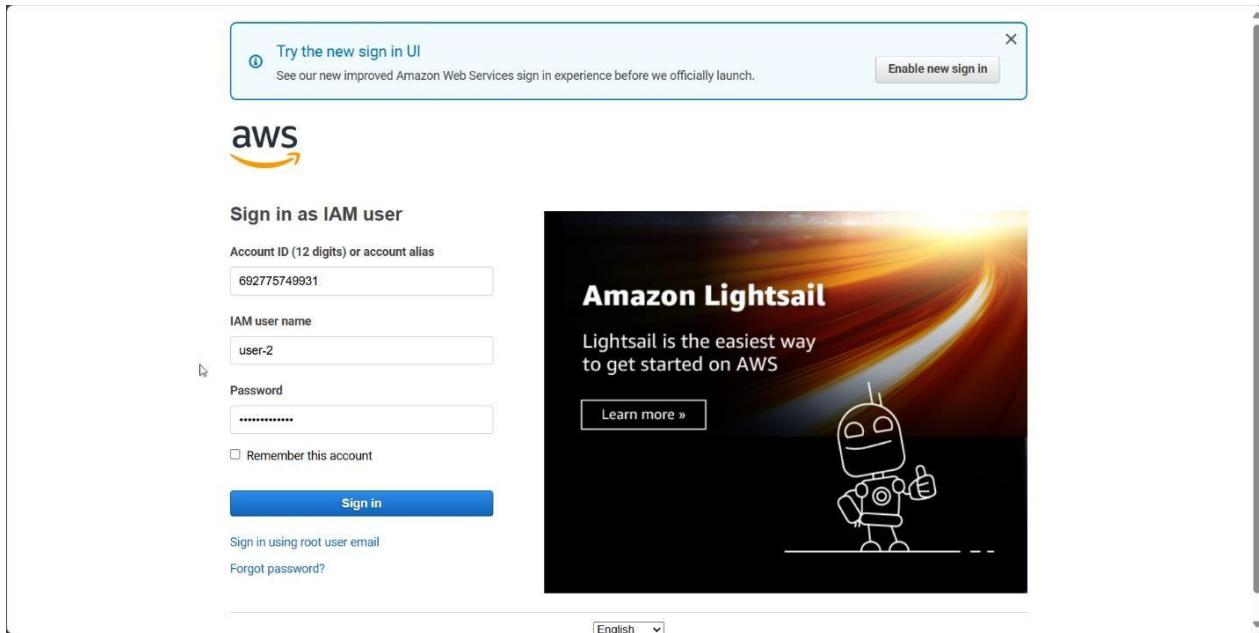
▶ API response

Cancel **Delete bucket**

CloudShell Feedback ⓘ © 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

### Step 3: User-2 Test EC2 Read-only Access:

- Sign in as User-2.
- Navigate to the EC2 dashboard.
- Check if User-2 can view instances but cannot modify (start/stop) them.



The screenshot shows the AWS Console Home page for User-2. The top navigation bar includes 'Services', a search bar, and a region selector set to 'N. Virginia'. The user's email, 'user-2 @ 692775749931', is also shown. The main dashboard features several cards: 'Recently visited' (with 'EC2' highlighted in red), 'Applications' (0), 'Welcome to AWS' (with a 'Getting started with AWS' link), 'AWS Health' (with a heart icon), and 'Cost and usage' (with cost breakdown sections). A prominent red box highlights the 'Access denied' message in the Applications card. The bottom of the page includes standard footer links like 'CloudShell', 'Feedback', and copyright information: '© 2024, Amazon Web Services, Inc. or its affiliates.'

**EC2 Dashboard**

EC2 Global View

Events

Console-to-Code [Preview](#)

Instances

Instances **Instances**

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

CloudShell Feedback

**Resources**

You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

Instances (running)	1	Auto Scaling Groups	0	Capacity Reservations	0
Dedicated Hosts	0	Elastic IPs	0	Instances	1
Key pairs	1	Load balancers	0	Placement groups	0
Security groups	3	Snapshots	0	Volumes	1

**Launch instance**

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

**Service health**

AWS Health Dashboard

**An error occurred**

An error occurred retrieving service health information

[Diagnose with Amazon Q](#)

**Zones**

Zone name	Zone ID
us-east-1a	use1-az1

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

**EC2 Dashboard**

EC2 Global View

Events

Console-to-Code [Preview](#)

Instances

Instances **Instances**

Instance Types

Launch Templates

Spot Requests

Savings Plans

Reserved Instances

Dedicated Hosts

Capacity Reservations

Images

AMIs

AMI Catalog

Elastic Block Store

Volumes

Snapshots

Lifecycle Manager

Network & Security

Security Groups

CloudShell Feedback

**Instances (1) Info**

Last updated less than a minute ago

Find Instance by attribute or tag (case-sensitive)

Name	Instance ID	Instance state	Instance type	Status check	Alarm status	Availability Zone	Public IPv4 DNS
	i-02bf558e035784452	Running	t2.micro	2/2 checks passed	<a href="#">View alarms</a> +	us-east-1a	ec2-44-200-200-178.co...

**Select an instance**

© 2024, Amazon Web Services, Inc. or its affiliates. [Privacy](#) [Terms](#) [Cookie preferences](#)

**EC2 Instances Detail View**

**Instance summary for i-02bf538e035784452**

Instance ID	i-02bf538e035784452	Public IPv4 address	44.200.200.178   open address
IPv6 address	-	Instance state	Running
Hostname type	IP name: ip-10-1-11-80.ec2.internal	Private IP DNS name (IPv4 only)	ip-10-1-11-80.ec2.internal
Answer private resource DNS name	-	Instance type	t2.micro
Auto-assigned IP address	-	VPC ID	vpc-08b10f72ecc9b9112 (Lab VPC)
IAM Role	-	Subnet ID	subnet-0a9c02318bb235b6e (Public Subnet 1)
IMDSv2	Required	Instance ARN	arnaws:ec2:us-east-1:692775749931:instance/i-02bf538e035784452

**AWS Compute Optimizer finding**

User: arnawsiam:692775749931:user/spl66/user-2 is not authorized to perform: compute-optimizer:GetEnrollmentStatus on resource: \* because no identity-based policy allows the compute-optimizer:GetEnrollmentStatus action

**Actions**

Connect, Instance state, Actions

**EC2 Instances List View**

**Instances (1/1) Info**

Name	Instance ID	Instance state	Instance type	Status check
<input checked="" type="checkbox"/> i-02bf538e035784452	i-02bf538e035784452	Running	t2.micro	2/2 checks passed

**Actions**

Stop instance, Start instance, Reboot instance, Hibernate instance, Terminate (Delete) instance

**Instance Details**

**i-02bf538e035784452**

Details	Status and alarms	Monitoring	Security	Networking	Storage	Tags
Instance ID	i-02bf538e035784452	Public IPv4 address	44.200.200.178   open address	Private IP4 addresses	10.1.11.80	
IPv6 address	-	Instance state	Running	Private IP4 DNS	ec2-44-200-200-178.compute-1.amazonaws.com   open address	
Hostname type	IP name: ip-10-1-11-80.ec2.internal	Private IP DNS name (IPv4 only)	ip-10-1-11-80.ec2.internal	Elastic IP addresses	-	
Answer private resource DNS name	-	Instance type	-	-	-	

**Actions**

Launch instances, Instance state, Actions

Screenshot of the AWS EC2 Instances page showing a termination dialog.

**Instances (1/1) Info**

**Terminate (delete) instance?**

On an EBS-backed instance, the default action is for the root EBS volume to be deleted when the instance is terminated. Storage on any local drives will be lost.

Are you sure you want to terminate these instances?

Instance ID	Termination protection
i-02bf538e035784452	Disabled

To confirm that you want to delete the instances, choose the terminate button below. Instances with termination protection enabled will not be terminated. Terminating the instance cannot be undone.

**Cancel** **Terminate (delete)**

Details Status and alarms Monitoring Security Networking Storage Tags

Instance ID: i-02bf538e035784452  
 IPv4 address: -  
 Hostname type: IP name: ip-10-1-11-80.ec2.internal  
 Instance state: Running  
 Private IP/DNS name (IPv4 only): ip-10-1-11-80.ec2.internal  
 Instance type: t2.micro  
 Elastic IP addresses: Public IPv4 DNS: ec2-44-200-200-178.compute-1.amazonaws.com | open address  
 Private IPv4 addresses: 10.1.11.80  
 Public IPv4 DNS: ec2-44-200-200-178.compute-1.amazonaws.com | open address

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

Screenshot of the AWS EC2 Instances page showing a failed termination attempt due to insufficient permissions.

**Failed to terminate (delete) an instance: You are not authorized to perform this operation. User: arnaws:iam::692775749931:user/spl66/user-2 is not authorized to perform: ec2:TerminateInstances on resource: arnaws:ec2:us-east-1:692775749931:instance/i-02bf538e035784452 because no identity-based policy allows the ec2:TerminateInstances action. Encoded authorization failure message: F4PB1TD08YVpvCgj4cOVED\_jhzxqkUT\_XwdrN68SogtsEHXzGncdx-muwkomAk0lMf-hj6AcvU8-9e7BQyM00ogu0DDele0I57Yz4dHdBVz0JyksSelBQk4JBZfT0DDQz\_QTw\_jB5-JcByWLRx0JzjneQzYQFN\_vPaAyW4lk2zTYUM8lJLQmfKX5a-GCGtwKNYbAGDVx87PtofgB8Bmwz1EZG31JkefSm7PnNsP82noWgkffOp17BBSUGKcdLs82Y0knQOOGjBewoCoQJ\_aVh0EDfLE5kGNADwvjBCKy\_N2u529pVBz\_vrZ9LMQGIN7xPjbeW2A44n4nwP1VpytuZHcCxwgjEAm148k1Us1328aKj7272znDqJ0JtzlkWJ1UHkhfTeIP008Q-uF55m66DcCf64t2FkK7r7l51-k84Kve56rgLog4vLSqgQ18OVWLKn5poQfjtPS4AjPm-\_gurCllhOx7-1UAJd/dAxzwXw0Jh9nCOObcvVLDdUmqrLbswNq2-WtEHuYQq58RCh/jVb9-hp\_AafM2zPa94093zxF-RVYDA\_4P5jQodpwg2dDgIAuyDef0zunQqjCT1EgwVP\_b4uf7f7z-ClePz155VlV1PfOyVzMo\_lAPVttlBrhN00laUoQrnJQmQ2331zyrxW02YBT0zyLrTyOkh04v\_-FBQge9g-bMin-ujBgBYOKXhQ6hd4YICpnbUlPEd15QghlhQdHEoATC/EWw0IDDrxTHm7TQVQyvCzbsaHHZdhH0u\_ykQ9trJhBQdfalHmDQu4masp-VRqCLt5y5OGODaS8W-Xxa68cZKQg0x41yQLwRCGG1PKY9kMSJSRske0DEKw3K-pwwhhB3ef7zmh4UBxjQ3RSkm6hr204MVU8pV1uphIuteTMxzdqCkQrMvv7ej4obFBi2fIymQZY0RgB1-bhmJAyZi8vp7py11kv42RKSS7uLo5Q-QkQ8k8K\_shZdzDjRqN1tyTPZYkfQJFUJ7lqPQ**

**Instances (1/1) Info**

**Diagnose with Amazon Q**

**i-02bf538e035784452**

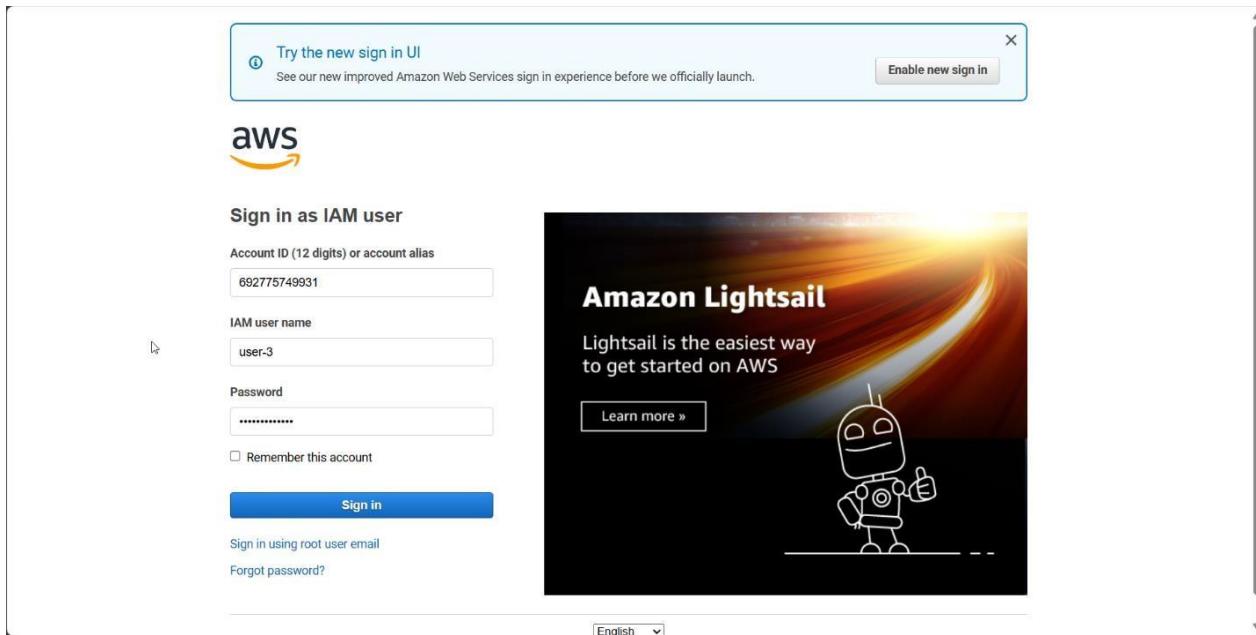
Details Status and alarms Monitoring Security Networking Storage Tags

Instance ID: i-02bf538e035784452  
 IPv4 address: 44.200.200.178 | open address  
 Hostname type: IP name: ip-10-1-11-80.ec2.internal  
 Instance state: Running  
 Private IP/DNS name (IPv4 only): ip-10-1-11-80.ec2.internal  
 Instance type: t2.micro  
 Elastic IP addresses: Public IPv4 DNS: ec2-44-200-200-178.compute-1.amazonaws.com | open address  
 Private IPv4 addresses: 10.1.11.80  
 Public IPv4 DNS: ec2-44-200-200-178.compute-1.amazonaws.com | open address

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

## Step 4: User-3 Test EC2 Admin Access:

- Sign in as User-3.
- Navigate to the EC2 dashboard.
- Verify that User-3 can view, start, and stop EC2 instances.



The image shows the AWS Console Home page. At the top, there's a navigation bar with 'Services', a search bar, and a user profile 'user-3 @ 6927-7574-9931'. Below the navigation is the 'Console Home' section. On the left, under 'Recently visited', the 'EC2' service is highlighted with a red box. In the center, the 'Applications' section shows '(0)' applications with a 'Create application' button. A message 'Access denied' is displayed in a red box. At the bottom of the page, there are sections for 'Welcome to AWS', 'AWS Health', and 'Cost and usage', each with its own set of metrics and 'Access denied' messages. The footer includes links for 'CloudShell', 'Feedback', 'Privacy', 'Terms', and 'Cookie preferences'.

The screenshot shows the AWS EC2 Instances page. On the left, a sidebar navigation includes: EC2 Dashboard, EC2 Global View, Events, Console-to-Code (Preview), Instances (selected), Instance Types, Launch Templates, Spot Requests, Savings Plans, Reserved Instances, Dedicated Hosts, Capacity Reservations, Images (AMIs, AMI Catalog), Elastic Block Store (Volumes, Snapshots, Lifecycle Manager), Network & Security (Security Groups), CloudShell, and Feedback.

The main content area displays the 'Instances (1/1) Info' table. It shows one instance: i-02bf538e035784452, which is Running, t2.micro, and has 2/2 checks passed. The 'Actions' dropdown menu is open, with the 'Stop instance' option highlighted by a red box and a red circle labeled '3'. A modal window titled 'Stop instance' is displayed, containing the instance ID (i-02bf538e035784452) and a 'Stop protection' toggle set to 'Off (Can stop instance)'. A warning message states: 'You will be billed for associated resources. After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.' The 'Stop' button in the modal is highlighted by a red box and a red circle labeled '4'.

The screenshot shows the 'Stop instance' confirmation dialog. It contains the following text: 'Stopping your instance allows you to reduce costs, modify settings, and troubleshoot problems.' Below this is a table with two columns: 'Instance ID' (i-02bf538e035784452) and 'Stop protection' (set to 'Off (Can stop instance)'). A warning message box contains the text: 'You will be billed for associated resources. After you stop the instance, you are no longer charged usage or data transfer fees for it. However, you will still be billed for associated Elastic IP addresses and EBS volumes.' At the bottom right of the dialog is a 'Cancel' button and a large red-bordered 'Stop' button.

Successfully initiated stopping of i-02bf538e035784452

Last updated less than a minute ago

Connect Instance state Actions Launch instances

Instances (1/1) Info Find Instance by attribute or tag (case-sensitive)

Name Instance ID Instance state Instance type Status check Alarm status Availability Zone Public IPv4 DNS

i-02bf538e035784452 Stopped t2.micro 2/2 checks passed User: arn:aws:us-east-1a

i-02bf538e035784452

Details Status and alarms Monitoring Security Networking Storage Tags

Instance summary

Instance ID	Public IPv4 address	Private IPv4 addresses
i-02bf538e035784452	-	10.1.11.80
IPv6 address	Instance state	Public IPv4 DNS
-	Stopped	-
Hostname type	Private IP DNS name (IPv4 only)	Elastic IP addresses
IP Name: ip-10-1-11-80.ec2.internal	ip-10-1-11-80.ec2.internal	-
Answer private resource DNS name	Instance type	
-	t2.micro	

© 2024, Amazon Web Services, Inc. or its affiliates. Privacy Terms Cookie preferences

CloudShell Feedback

## Guided Lab: Exploring AWS Identity and Access Management (IAM)

Due No Due Date Points 56 Submitting an external tool

AWS 01:05 ► Start Lab ■ End Lab i AWS Details i Details ×

EN\_US

## Guided Lab: Exploring AWS Identity and Access Management (IAM)

### Lab overview and objectives

In this lab, you explore users and groups and inspect the associated policies in the AWS Identity and Access Management (IAM) service. You also add users to the groups and verify the permissions that are inherited by them.

After completing this lab, you should be able to do the following:

Total score 15/15

[Task 2A] Check user-1 iam group 5/5

[Task 2B] Check user-2 iam group 5/5

[Task 2C] Check user-3 iam group 5/5

Guided Lab: Exploring AWS Identity and Access Management (IAM)  
Lab Assignments

Sep 27 at  
5:18pm

56 / 56



# Project 9 : Creating an Amazon virtual private cloud (VPC)

## Access and

### Configure AWS CLI

#### Step 1: Open the

#### Lab Environment

- Start your lab

session as directed. Step

2: Run the Lab

• Initiate the lab session by clicking the "Run Lab" button. Step 3:

Access AWS CLI

- Navigate to the AWS Details panel.

- Locate the AWS CLI section and click

"Show" to reveal the CLI credentials. Step 4:

Configure AWS CLI

- Open Command Prompt (cmd) on your Windows machine.

- Enter the following command to start the configuration process: When prompted, input the AWS credentials provided:

**“aws configure”**

- AWS Access Key ID: [Enter your aws\_access\_key\_id]

- AWS Secret Access Key: [Enter your aws\_secret\_access\_key]

- Default region name: [Enter the desired AWS region, e.g., us-west-2]

- Default output format: [Enter your preferred output format, e.g., json]

The screenshot shows a Kali Linux terminal window with root privileges. The user is running the command `aws configure`. The output is as follows:

```
root@kali:~# aws configure
AWS Access Key ID [*****LVYS]: 
AWS Secret Access Key [*****aObB]: 
Default region name [us-east-1]: 
Default output format [json]:
```

Below the terminal, there is a file viewer window titled "EN\_US" showing a file named ".aws/credentials". The contents of the file are:

```
[default]
aws_access_key_id=ASIA2G3Q4JISKGFLVYS
aws_secret_access_key=Iie2akKEzr
region=us-east-1
output=json
```

On the right side of the screen, there is a sidebar with the title "Lab overview and objectives".

## Task 1: Creating a VPC

### 1. Create the VPC:

```
(root@kali)-[~]
└─# aws ec2 create-vpc --cidr-block 10.0.0.0/16 --tag-specifications 'ResourceType=vpc,Tags=[{Key=Name,Value=Lab VPC}]'

{
    "Vpc": {
        "CidrBlock": "10.0.0.0/16",
        "DhcpOptionsId": "dopt-07314e6443821a60c",
        "State": "pending",
        "VpcId": "vpc-0c3d8065af0fccdba",
        "OwnerId": "701951435345",
        "InstanceTenancy": "default",
        "Ipv6CidrBlockAssociationSet": [],
        "CidrBlockAssociationSet": [
            {
                "AssociationId": "vpc-cidr-assoc-07b8d3a6d54b43723",
                "CidrBlock": "10.0.0.0/16",
                "CidrBlockState": {
                    "State": "associated"
                }
            }
        ],
        "IsDefault": false,
        "Tags": [
            {
                "Key": "Name",
                "Value": "Lab VPC"
            }
        ]
    }
}
```

### 2. Enable DNS hostnames for the VPC: First, get the VPC ID:

### 3. Use the VPC ID to enable DNS hostnames:

```
File Actions Edit View Help
root@kali: ~
└─# aws ec2 describe-vpcs --filters "Name=cidr-block,Values=10.0.0.0/16" --query 'Vpcs[0].VpcId' --output text
vpc-01dcc1827af9ef5af

└─# aws ec2 modify-vpc-attribute --vpc-id vpc-01dcc1827af9ef5af --enable-dns-hostnames "{\"Value\":true}"

```

## Task 2: Creating Subnets

### Task 2.1: Creating a Public Subnet

#### 1. Create the Public Subnet:

```
(root㉿kali)-[~]
└─# aws ec2 create-subnet --vpc-id vpc-01dcc1827af9ef5af --cidr-block 10.0.0.0/24 --availability-zone us-east-1a --tag-specifications 'ResourceType=subnet,Tags=[{"Key=Name,Value=Public Subnet"}]'

{
    "Subnet": {
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "AvailableIpAddressCount": 251,
        "CidrBlock": "10.0.0.0/24",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-094f06a9e81c23778",
        "VpcId": "vpc-01dcc1827af9ef5af",
        "OwnerId": "701951435345",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "Public Subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-east-1:701951435345:subnet/subnet-094f06a9e81c23778",
        "EnableDns64": false,
        "Ipv6Native": false,
        "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        }
    }
}
```

#### 2. Enable Auto-assign Public IP for Public Subnet: Get the subnet ID for the public subnet:

#### 3. Enable auto-assign public IPv4:

```
(root㉿kali)-[~]
└─# aws ec2 describe-subnets --filters "Name=cidr-block,Values=10.0.0.0/24" --query 'Subnets[0].SubnetId' --output text
subnet-094f06a9e81c23778

(root㉿kali)-[~]
└─# aws ec2 modify-subnet-attribute --subnet-id subnet-094f06a9e81c23778 --map-public-ip-on-launch
```

## Task 2.2: Creating a Private Subnet

### 1. Create the Private Subnet:

```
(root@kali)-[~]
└─# aws ec2 create-subnet --vpc-id vpc-01dcc1827af9ef5af --cidr-block 10.0.2.0/23 --availability-zone us-east-1a --tag-specifications 'ResourceType=subnet,Tags=[{Key=Name,Value=Private Subnet}]'

{
    "Subnet": {
        "AvailabilityZone": "us-east-1a",
        "AvailabilityZoneId": "use1-az4",
        "AvailableIpAddressCount": 507,
        "CidrBlock": "10.0.2.0/23",
        "DefaultForAz": false,
        "MapPublicIpOnLaunch": false,
        "State": "available",
        "SubnetId": "subnet-0941035c8b8e97a9a",
        "VpcId": "vpc-01dcc1827af9ef5af",
        "OwnerId": "701951435345",
        "AssignIpv6AddressOnCreation": false,
        "Ipv6CidrBlockAssociationSet": [],
        "Tags": [
            {
                "Key": "Name",
                "Value": "Private Subnet"
            }
        ],
        "SubnetArn": "arn:aws:ec2:us-east-1:701951435345:subnet/subnet-0941035c8b8e97a9a",
        "EnableDns64": false,
        "Ipv6Native": false,
        "PrivateDnsNameOptionsOnLaunch": {
            "HostnameType": "ip-name",
            "EnableResourceNameDnsARecord": false,
            "EnableResourceNameDnsAAAARecord": false
        }
    }
}
```

## Task 3: Creating an Internet Gateway

### 1. Create the Internet Gateway:

```
(root㉿kali)-[~]
└─# aws ec2 create-internet-gateway --tag-specifications 'ResourceType=internet-gateway,Tags=[{Key=Name,Value=Lab IGW}]'

{
    "InternetGateway": {
        "Attachments": [],
        "InternetGatewayId": "igw-03222a7d8b12fd926",
        "OwnerId": "701951435345",
        "Tags": [
            {
                "Key": "Name",
                "Value": "Lab IGW"
            }
        ]
    }
}
```

### 2. Attach the Internet Gateway to the VPC: Get the Internet Gateway ID:

### 3. Attach the Internet Gateway to the VPC:

```
(root㉿kali)-[~]
└─# aws ec2 describe-internet-gateways --filters "Name=tag:Name,Values=Lab IGW" --query 'InternetGateways[0].InternetGatewayId' --output text
igw-03222a7d8b12fd926

(root㉿kali)-[~]
└─# aws ec2 attach-internet-gateway --vpc-id vpc-01dcc1827af9ef5af --internet-gateway-id igw-03222a7d8b12fd926
```

## Task 4: Configuring Route Tables

### 1. Create a Public Route Table:

```
(root㉿kali)-[~]
└─# aws ec2 create-route-table --vpc-id vpc-01dcc1827af9ef5af --tag-specifications 'ResourceType=route-table,Tags=[{Key=Name,Value=Public Route Table}]'

{
  "RouteTable": {
    "Associations": [],
    "PropagatingVgws": [],
    "RouteTableId": "rtb-05a5135d3a02ed2af",
    "Routes": [
      {
        "DestinationCidrBlock": "10.0.0.0/16",
        "GatewayId": "local",
        "Origin": "CreateRouteTable",
        "State": "active"
      }
    ],
    "Tags": [
      {
        "Key": "Name",
        "Value": "Public Route Table"
      }
    ],
    "VpcId": "vpc-01dcc1827af9ef5af",
    "OwnerId": "701951435345"
  },
  "ClientToken": "132b3571-6c76-45f6-bfcc-8c0935e61bb0"
}
```

### 2. Add Route to Internet Gateway: Get the Route Table ID:

```
(root㉿kali)-[~]
└─# aws ec2 describe-route-tables --filters "Name>tag:Name,Values=Public Route Table" --query 'RouteTables[0].RouteTableId' --output text

rtb-05a5135d3a02ed2af

(root㉿kali)-[~]
└─# aws ec2 create-route --route-table-id rtb-05a5135d3a02ed2af --destination-cidr-block 0.0.0.0/0 --gateway-id igw-03222a7d8b12fd926

{
  "Return": true
}
```

### 3. Add a route to the Internet Gateway:

### 4. Associate Public Subnet with Public Route Table: Associate the public subnet to the route table:

```
[root@kali:~]
# aws ec2 associate-route-table --route-table-id rtb-05a5135d3a02ed2af --subnet-id subnet-094f06a9e81
c23778
{
    "AssociationId": "rtbassoc-09576b1b8fa4f852b",
    "AssociationState": {
        "State": "associated"
    }
}
```

## Task 5: Creating a Security Group for the Application Server

### 1. Create a Security Group:

```
[root@kali]# aws ec2 create-security-group --group-name App-SG --description "Allow HTTP traffic" --vpc-id vpc-01dccc1827af9ef5af
{
    "GroupId": "sg-0ad65ec95b3c3e833"
}
```

### 2. Allow HTTP (port 80) traffic: Get the Security Group ID:

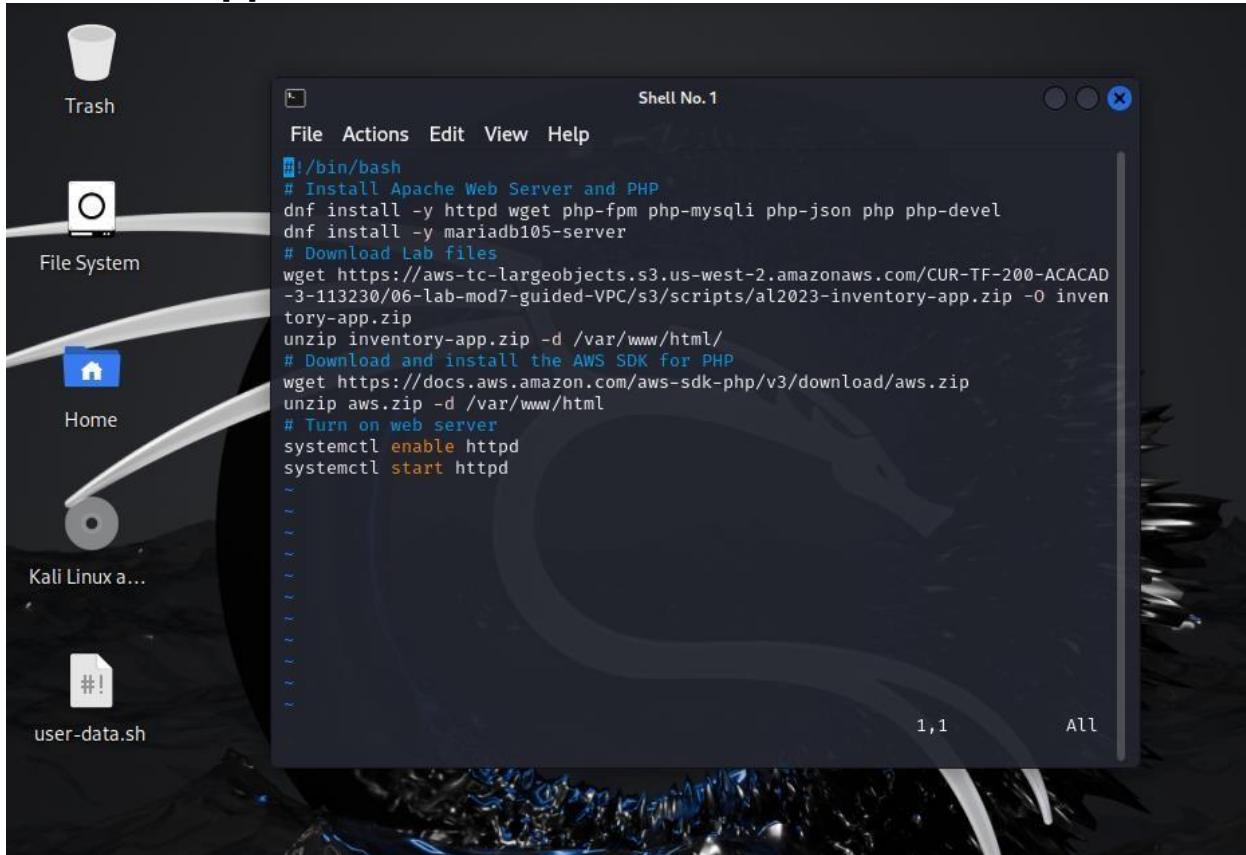
### 3. Add the inbound rule for HTTP:

```
[root@kali]# aws ec2 describe-security-groups --filters "Name=group-name,Values=App-SG" --query 'SecurityGroups[0].GroupId' --output text
sg-0ad65ec95b3c3e833

[root@kali]# aws ec2 authorize-security-group-ingress --group-id sg-0ad65ec95b3c3e833 --protocol tcp --port 80 --cidr 0.0.0.0/0
{
    "Return": true,
    "SecurityGroupRules": [
        {
            "SecurityGroupRuleId": "sgr-0d4e66c3cdd468003",
            "GroupId": "sg-0ad65ec95b3c3e833",
            "GroupOwnerId": "701951435345",
            "IsEgress": false,
            "IpProtocol": "tcp",
            "FromPort": 80,
            "ToPort": 80,
            "CidrIpv4": "0.0.0.0/0"
        }
    ]
}
```

## Task 6: Launching an Application Server in the Public Subnet

1. **Prepare User Data Script:** Create a user-data.sh file that contains the script to install and configure the web application



```
#!/bin/bash
# Install Apache Web Server and PHP
dnf install -y httpd wget php-fpm php-mysql php-json php php-devel
dnf install -y mariadb105-server
# Download Lab files
wget https://aws-tc-largeobjects.s3.us-west-2.amazonaws.com/CUR-TF-200-ACACAD-3-113230/06-lab-mod7-guided-VPC/s3/scripts/al2023-inventory-app.zip -O inventory-app.zip
unzip inventory-app.zip -d /var/www/html/
# Download and install the AWS SDK for PHP
wget https://docs.aws.amazon.com/aws-sdk-php/v3/download/aws.zip
unzip aws.zip -d /var/www/html/
# Turn on web server
systemctl enable httpd
systemctl start httpd
~
```

## 2. Launch EC2 Instance:

```
[root@kali]~# aws ec2 run-instances \
--image-id ami-007868005aea67c54 \
--instance-type t2.micro \
--key-name vockey \
--security-group-ids sg-0ad65ec95b3c3e833 \
--subnet-id subnet-094f06a9e81c23778 \
--associate-public-ip-address \
--user-data ~/Desktop/user-data.sh \
--tag-specifications 'ResourceType=instance,Tags=[{Key=Name,Value=App Server}]'
{
    "Groups": [],
    "Instances": [
        {
            "AmiLaunchIndex": 0,
            "ImageId": "ami-007868005aea67c54",
            "InstanceId": "i-0ca3fde2164238343",
            "InstanceType": "t2.micro",
            "KeyName": "vockey",
            "LaunchTime": "2024-10-10T07:52:51+00:00",
            "Monitoring": {
                "State": "disabled"
            },
            "Placement": {
                "AvailabilityZone": "us-east-1a",
                "GroupName": "",
                "Tenancy": "default"
            },
            "PrivateDnsName": "ip-10-0-0-252.ec2.internal",
            "PrivateIpAddress": "10.0.0.252",
            "ProductCodes": [],
            "PublicDnsName": "",
            "State": {
                "Code": 0,
                "Name": "pending"
            },
            "StateTransitionReason": "",
            "SubnetId": "subnet-094f06a9e81c23778",
            "VpcId": "vpc-01dcc1827af9ef5af",
            "Architecture": "x86_64",
            "BlockDeviceMappings": [],
            "ClientToken": "1844436c-229c-42ff-8136-7f2d88ad71f4",
            "EbsOptimized": false,
            "EnaSupport": true,
            "Hypervisor": "xen",
        }
    ]
}
```

```
root@kali: ~
File Actions Edit View Help
    "EbsOptimized": false,
    "EnaSupport": true,
    "Hypervisor": "xen",
    "NetworkInterfaces": [
        {
            "Attachment": {
                "AttachTime": "2024-10-10T07:52:51+00:00",
                "AttachmentId": "eni-attach-0d8efb18964b72730",
                "DeleteOnTermination": true,
                "DeviceIndex": 0,
                "Status": "attaching",
                "NetworkCardIndex": 0
            },
            "Description": "",
            "Groups": [
                {
                    "GroupName": "App-SG",
                    "GroupId": "sg-0ad65ec95b3c3e833"
                }
            ],
            "Ipv6Addresses": [],
            "MacAddress": "0a:ff:fa:cb:ce:0f",
            "NetworkInterfaceId": "eni-085b1e8bec9242d43",
            "OwnerId": "701951435345",
            "PrivateDnsName": "ip-10-0-0-252.ec2.internal",
            "PrivateIpAddress": "10.0.0.252",
            "PrivateIpAddresses": [
                {
                    "Primary": true,
                    "PrivateDnsName": "ip-10-0-0-252.ec2.internal",
                    "PrivateIpAddress": "10.0.0.252"
                }
            ],
            "SourceDestCheck": true,
            "Status": "in-use",
            "SubnetId": "subnet-094f06a9e81c23778",
            "VpcId": "vpc-01dcc1827af9ef5af",
            "InterfaceType": "interface"
        },
        {
            "RootDeviceName": "/dev/xvda",
            "RootDeviceType": "ebs",
            "SecurityGroups": [
                {
                    "GroupName": "App-SG",
                    "GroupId": "sg-0ad65ec95b3c3e833"
                }
            ]
        }
    ]
}
```

```
root@kali:~  
File Actions Edit View Help  
    "RootDeviceType": "ebs",  
    "SecurityGroups": [  
        {  
            "GroupName": "App-SG",  
            "GroupId": "sg-0ad65ec95b3c3e833"  
        }  
    ],  
    "SourceDestCheck": true,  
    "StateReason": {  
        "Code": "pending",  
        "Message": "pending"  
    },  
    "Tags": [  
        {  
            "Key": "Name",  
            "Value": "App Server"  
        }  
    ],  
    "VirtualizationType": "hvm",  
    "CpuOptions": {  
        "CoreCount": 1,  
        "ThreadsPerCore": 1  
    },  
    "CapacityReservationSpecification": {  
        "CapacityReservationPreference": "open"  
    },  
    "MetadataOptions": {  
        "State": "pending",  
        "HttpTokens": "optional",  
        "HttpPutResponseHopLimit": 1,  
        "HttpEndpoint": "enabled",  
        "HttpProtocolIpv6": "disabled",  
        "InstanceMetadataTags": "disabled"  
    },  
    "EnclaveOptions": {  
        "Enabled": false  
    },  
    "PrivateDnsNameOptions": {  
        "HostnameType": "ip-name",  
        "EnableResourceNameDnsARecord": false,  
        "EnableResourceNameDnsAAAARecord": false  
    },  
    "MaintenanceOptions": {  
        "AutoRecovery": "default"  
    },  
    "CurrentInstanceBootMode": "legacy-bios"  
:
```

```
root@kali:~  
File Actions Edit View Help  
        }  
    ],  
    "SourceDestCheck": true,  
    "StateReason": {  
        "Code": "pending",  
        "Message": "pending"  
    },  
    "Tags": [  
        {  
            "Key": "Name",  
            "Value": "App Server"  
        }  
    ],  
    "VirtualizationType": "hvm",  
    "CpuOptions": {  
        "CoreCount": 1,  
        "ThreadsPerCore": 1  
    },  
    "CapacityReservationSpecification": {  
        "CapacityReservationPreference": "open"  
    },  
    "MetadataOptions": {  
        "State": "pending",  
        "HttpTokens": "optional",  
        "HttpPutResponseHopLimit": 1,  
        "HttpEndpoint": "enabled",  
        "HttpProtocolIpv6": "disabled",  
        "InstanceMetadataTags": "disabled"  
    },  
    "EnclaveOptions": {  
        "Enabled": false  
    },  
    "PrivateDnsNameOptions": {  
        "HostnameType": "ip-name",  
        "EnableResourceNameDnsARecord": false,  
        "EnableResourceNameDnsAAAARecord": false  
    },  
    "MaintenanceOptions": {  
        "AutoRecovery": "default"  
    },  
    "CurrentInstanceBootMode": "legacy-bios"  
},  
],  
"OwnerId": "701951435345",  
"ReservationId": "r-0d9458c5de6c23470"  
}  
(END)
```

### 3. Validate Setup:

- Get the public DNS of the instance:

```
[root@kali:~]
# aws ec2 describe-instances --filters "Name=tag:Name,Values=App Server" --query 'Reservations[0].Instances[0].PublicDnsName' --output text
ec2-3-208-22-89.compute-1.amazonaws.com
```

# Project 14: Automating Infrastructure Deployment with AWS CloudFormation

---

## Task 1: Deploying a Networking Layer

1. **Download and inspect** the lab-network.yaml CloudFormation template, which defines the VPC, subnets, and networking components.
  2. **Deploy the template** by creating a new stack in AWS CloudFormation:
    - o **Stack Name:** lab-network
    - o **Template Source:** Upload the lab-network.yaml file.
    - o **Tags:** Add a tag with Key=application and Value=inventory.
  3. **Monitor** the stack creation process and review the resources created, including the VPC and public subnet.
  4. **Inspect the Outputs** tab for resource IDs and explore how values are exported for use in other stacks.
- 

## The Code

```
bash
Copy code
#!/bin/bash

# Create lab-network stack
echo "Creating lab-network
stack..." aws cloudformation
create-stack \
--stack-name lab-network \
--template-body file://lab-network.yaml \
--tags Key=application,Value=inventory
```

```
# Wait for lab-network stack creation to complete
echo "Waiting for lab-network stack creation to complete..."
aws cloudformation wait stack-create-complete --stack-name lab-
network
```

---

## The Output

```
bash
Copy code
$ ./script.sh
Creating lab-network stack...
arn:aws:cloudformation:us-east-1:202792838471:stack/lab-
network/abbed460- 8cc9-11ef-b978-0ee756e81a1d
```

Waiting for lab-network stack creation to  
complete... lab-network stack creation  
completed.

## Images for Task 1:

The screenshot shows the AWS CloudFormation console interface. At the top, there's a navigation bar with 'CloudFormation > Stacks > lab-network'. Below it is a search bar with 'lab-ne' and a dropdown for 'Active' status. A blue box highlights the 'lab-network' stack, which was created on '2024-10-17 23:52:07 UTC+0300' and is in 'CREATE\_COMPLETE' status.

Below the stack list, there are tabs for 'Stack info', 'Events', 'Resources' (which is selected), 'Outputs', 'Parameters', 'Template', 'Change sets', and 'Git sync'. The 'Resources' tab displays a table with 8 items:

Logical ID	Physical ID	Type	Status	Module
InternetGateway	<a href="#">igw-08a96c780a346d436</a>	AWS::EC2::InternetGateway	<span>✓ CREATE_COMPLETE</span>	-
PublicRoute	<a href="#">rtb-01b077920a9bd4229 0.0.0/0</a>	AWS::EC2::Route	<span>✓ CREATE_COMPLETE</span>	-
PublicRouteTable	<a href="#">rtb-01b077920a9bd4229</a>	AWS::EC2::RouteTable	<span>✓ CREATE_COMPLETE</span>	-
PublicSubnet	<a href="#">subnet-01dc7e72ba71b2b64</a>	AWS::EC2::Subnet	<span>✓ CREATE_COMPLETE</span>	-
PublicSubnetNetworkAclAssociation	<a href="#">aclassoc-0ba0dd3e5673cf1b5</a>	AWS::EC2::SubnetNetworkAclAssociation	<span>✓ CREATE_COMPLETE</span>	-
PublicSubnetRouteTableAssociation	<a href="#">rtbassoc-0b132229e4c5ce64e</a>	AWS::EC2::SubnetRouteTableAssociation	<span>✓ CREATE_COMPLETE</span>	-
VPC	<a href="#">vpc-07506a5a343052659</a>	AWS::EC2::VPC	<span>✓ CREATE_COMPLETE</span>	-

---

## Task 2: Deploying an Application Layer

1. **Download and inspect** the lab-application.yaml template, which sets up an EC2 instance and security group within the previously created VPC.

2. **Deploy the application layer** by creating a new stack:
    - o **Stack Name:** lab-application
    - o Ensure that the application stack references the lab-network stack to import VPC and subnet IDs.
  3. **Verify the deployment** by accessing the Outputs tab, copying the URL, and testing the application in your browser.
- 

## The Code

```
bash
Copy code
#!/bin/bash

# Create lab-application stack
echo "Creating lab-application
stack..." aws cloudformation create-
stack \
--stack-name lab-application \
--template-body file://lab-application.yaml \
--parameters
ParameterKey=NetworkStackName,ParameterValue=lab-network \
--tags Key=application,Value=inventory

# Wait for lab-application stack creation to complete
echo "Waiting for lab-application stack creation to complete..."
aws cloudformation wait stack-create-complete --stack-name lab-
application echo "lab-application stack creation completed."

# Retrieve outputs for lab-application stack
echo "Retrieving outputs for lab-application stack..."
aws cloudformation describe-stacks --stack-name lab-
application --query 'Stacks[0].Outputs' --output table
```

---

## The Output

```
bash
Copy code
```

Creating lab-application stack...

arn:aws:cloudformation:us-east-1:202792838471:stack/lab-application/d3f5c830- 8cc9-11ef-94e1-0affe95ac3a5

Waiting for lab-application stack creation to complete... lab-application stack creation completed.

Retrieving outputs for lab-application stack...

	DescribeStacks	
Description	-- URL of the sample website-----	
+ OutputKey	+ URL	+
OutputValue	http://ec2-44-212-10-252.compute-1.amazonaws.com	
++		+

## Images for Task 2:

The screenshot shows the AWS CloudFormation Stacks page. The URL is [CloudFormation > Stacks > lab-application](#). The page displays a list of stacks with one item: "lab-application". The stack details are as follows:

- Created: 2024-10-17 23:53:14 UTC+0300
- Status: UPDATE\_COMPLETE

The screenshot shows the AWS CloudFormation Outputs page for the "lab-application" stack. The URL is [lab-application](#). The "Outputs" tab is selected. There is one output entry:

Key	Value	Description	Export name
URL	<a href="http://ec2-44-212-10-252.compute-1.amazonaws.com">http://ec2-44-212-10-252.compute-1.amazonaws.com</a>	URL of the sample website	-



**Congratulations, you have successfully launched the AWS CloudFormation sample.**

lab-application						
		Delete	Update	Stack actions ▾	Create stack ▾	
Stack info	Events	Resources	Outputs	Parameters	Template	Change sets
Git sync						
<b>Resources (4)</b>						
<input type="text" value="Search resources"/> <span>⟳</span> <span>1</span> <span>&gt;</span> <span>⚙️</span>						
Logical ID	▲	Physical ID	▼	Type	▼	Status
DiskMountPoint		vol-0e5915cb0cd1003b1j-0d157901c900d9efa		AWS::EC2::VolumeAttachment		<span>✓ CREATE_COMPLETE</span>
DiskVolume		vol-0e5915cb0cd1003b1	🔗	AWS::EC2::Volume		<span>✓ CREATE_COMPLETE</span>
WebServerInstance		i-0d157901c900d9efa	🔗	AWS::EC2::Instance		<span>✓ CREATE_COMPLETE</span>
WebServerSecurityGroup		sg-0def9734f9d383b82	🔗	AWS::EC2::SecurityGroup		<span>✓ UPDATE_COMPLETE</span>

## Task 3: Updating a Stack

1. **Download the updated lab-application2.yaml template** that adds HTTPS traffic permissions to the security group.
2. **Update the lab-application stack** using the new template to modify the security group without replacing it.
3. **Verify the changes** by inspecting the security group's inbound rules in the EC2 console.

## The Code

```
bash
Copy code
#!/bin/bash

# Create change set for updating the lab-
application stack CHANGE_SET_NAME="lab-
application-changeset-$(date +%s)"

echo "Creating change set for lab-application
update..." aws cloudformation create-change-set
\
```

```

--stack-name lab-application \
--template-body file://lab-application2.yaml \
--parameters ParameterKey=NetworkStackName,ParameterValue=lab-network \
--tags Key=application,Value=inventory \
--change-set-name $CHANGE_SET_NAME \
--change-set-type UPDATE

# Wait for the change set creation to complete
echo "Waiting for the change set creation to
complete..." aws cloudformation wait change-
set-create-complete \
--stack-name lab-application \
--change-set-name $CHANGE_SET_NAME
echo "Change set created: $CHANGE_SET_NAME"

# Display the details of the change set (resources that will be
updated) echo "Showing changes for the update..."
aws cloudformation describe-change-set \
--stack-name lab-application \
--change-set-name $CHANGE_SET_NAME \
--query
'Changes[*].ResourceChange.{Action:Action,LogicalResourceId:Log
icalResourceId
,ResourceType:ResourceType,Replacement:Replacement}' \
--output table

# Confirm if the user wants to apply the change set
read -p "Do you want to execute the change set?
(yes/no): " choice
if [ "$choice" == "yes" ]; then
# Execute the change set
echo "Executing the change set..."
aws cloudformation execute-change-set \
--stack-name lab-application \
--change-set-name $CHANGE_SET_NAME

# Wait for lab-application stack update to complete
echo "Waiting for lab-application stack update to complete..."
aws cloudformation wait stack-update-complete --stack-name lab-
application
echo "lab-application stack update completed."
else
echo "Change set not
executed." fi

```

---

## The Output

bash

Copy code

Creating change set for lab-application update...

arn:aws:cloudformation:us-east-

1:202792838471:changeSet/lab-application- changeset-

1729198493/7ddf8425-2c94-4144-95fd-f599b7ab0406

arn:aws:cloudformation:us-east-1:202792838471:stack/lab-

application/d3f5c830- 8cc9-11ef-94e1-0affe95ac3a5

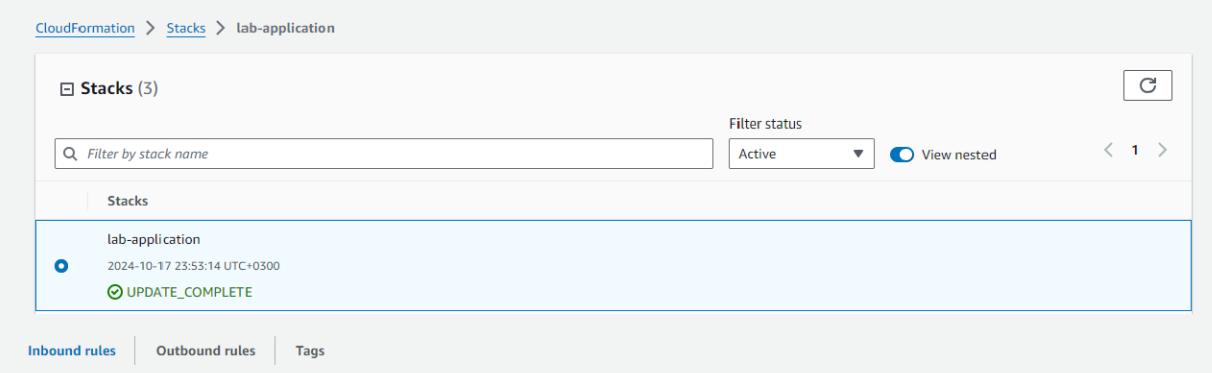
Waiting for the change set creation to  
complete... Change set created: lab-application-  
changeset-1729198493 Showing changes for  
the update...

DescribeChangeSet			
Action	LogicalResourceId	Replacement	ResourceType
Modify	WebServerSecurityGroup	False	AWS::EC2::SecurityGroup

Do you want to execute the change set?  
 (yes/no): yes Executing the change set...  
 Waiting for lab-application stack update to complete... lab-application stack update completed.

## Images for Task 3:

Include screenshots of the following for Task 3:



The screenshot shows the AWS CloudFormation Stacks page. The 'lab-application' stack is selected, indicated by a blue dot next to its name. The status is shown as 'UPDATE\_COMPLETE'. The page includes filters for stack name, status (Active), and nested stacks, along with buttons for creating a new stack and viewing tags.

Inbound rules	Outbound rules	Tags																								
<b>Inbound rules (2)</b> <table border="1"> <thead> <tr> <th colspan="6">Inbound rules (2)</th> </tr> <tr> <th><input type="checkbox"/></th> <th>Name</th> <th>Security group rule...</th> <th>IP version</th> <th>Type</th> <th>Protocol</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>sgr-0102cd391fb3f9ac7</td> <td>IPv4</td> <td>HTTPS</td> <td>TCP</td> </tr> <tr> <td><input type="checkbox"/></td> <td>-</td> <td>sgr-0832210ac6c87ff51</td> <td>IPv4</td> <td>HTTP</td> <td>TCP</td> </tr> </tbody> </table>			Inbound rules (2)						<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol	<input type="checkbox"/>	-	sgr-0102cd391fb3f9ac7	IPv4	HTTPS	TCP	<input type="checkbox"/>	-	sgr-0832210ac6c87ff51	IPv4	HTTP	TCP
Inbound rules (2)																										
<input type="checkbox"/>	Name	Security group rule...	IP version	Type	Protocol																					
<input type="checkbox"/>	-	sgr-0102cd391fb3f9ac7	IPv4	HTTPS	TCP																					
<input type="checkbox"/>	-	sgr-0832210ac6c87ff51	IPv4	HTTP	TCP																					

lab-application

Delete Update Stack actions ▾ Create stack ▾

Stack info | Events | **Resources** | Outputs | Parameters | Template | Change sets | Git sync

### Resources (4)

Logical ID	Physical ID	Type	Status	Module
DiskMountPoint	vol-0e5915cb0cd1003b1 i-0d157901c900d9efa	AWS::EC2::VolumeAttachment	<span>✓ CREATE_COMPLETE</span>	-
DiskVolume	vol-0e5915cb0cd1003b1	AWS::EC2::Volume	<span>✓ CREATE_COMPLETE</span>	-
WebServerInstance	i-0d157901c900d9efa	AWS::EC2::Instance	<span>✓ CREATE_COMPLETE</span>	-
WebServerSecurityGroup	sg-0def9734f9d383b82	AWS::EC2::SecurityGroup	<span>✓ UPDATE_COMPLETE</span>	-

lab-application

Delete Update Stack actions ▾ Create stack ▾

Stack info | **Events** | Resources | Outputs | Parameters | Template | Change sets | Git sync

### Events (24)

Timestamp	Logical ID	Status	Detailed status	Status r
2024-10-18 00:19:13 UTC+0300	lab-application	<span>✓ UPDATE_COMPLETE</span>	-	-
2024-10-18 00:19:12 UTC+0300	lab-application	<span>ℹ UPDATE_COMPLETE_CLEANUP_IN_PROGRESS</span>	-	-
2024-10-18 00:19:09 UTC+0300	WebServerSecurityGroup	<span>✓ UPDATE_COMPLETE</span>	-	-
2024-10-18 00:19:08 UTC+0300	WebServerSecurityGroup	<span>ℹ UPDATE_IN_PROGRESS</span>	-	-
2024-10-18 00:19:05 UTC+0300	lab-application	<span>ℹ UPDATE_IN_PROGRESS</span>	-	User In

---

## Task 4: Exploring Templates with AWS CloudFormation Designer

1. **Open the AWS CloudFormation Designer tool** to visualize and edit templates.
  2. **Upload the lab-application2.yaml template** to explore its components and relationships.
  3. **Experiment with adding new resources**, editing configurations, and connecting resources visually.
- 

### Images for Task 4:

Specify template [Info](#)

A template is a JSON or YAML file that describes your stack's resources and properties.

Template source

Selecting a template generates an Amazon S3 URL where it will be stored.

Amazon S3 URL  
Provide an Amazon S3 URL to your template.

Upload a template file  
Upload your template directly to the console.

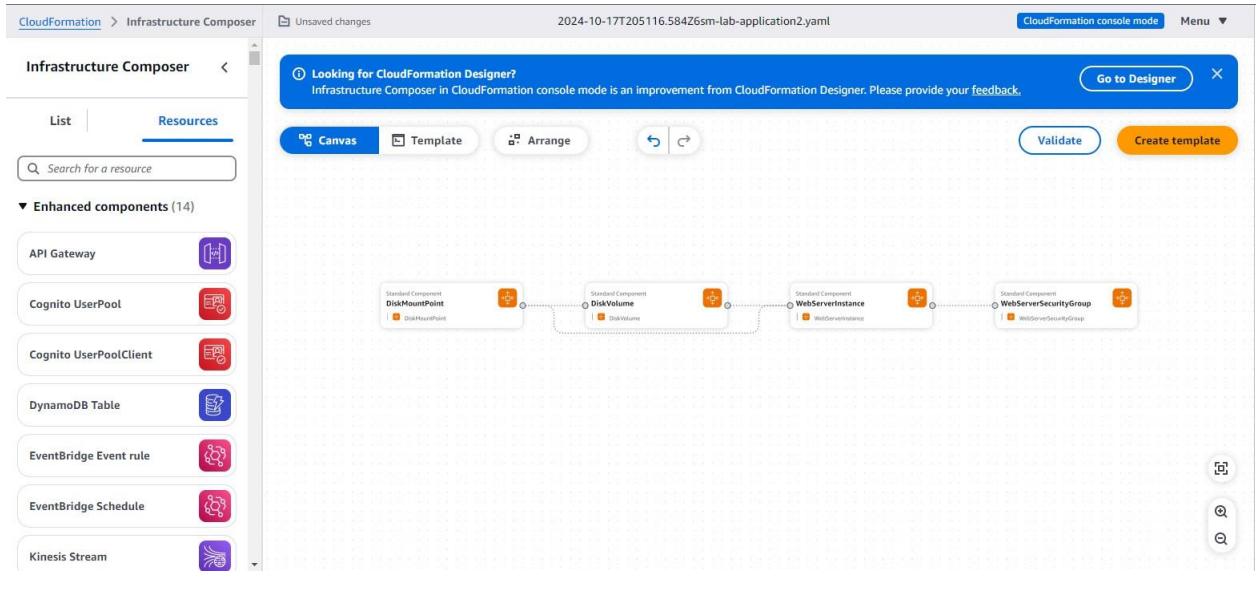
Sync from Git  
Sync a template from your Git repository.

Upload a template file

lab-application2.yaml X

JSON or YAML formatted file

S3 URL: <https://s3.us-east-1.amazonaws.com/cf-templates-8nx7zfmi2qg5-us-east-1/2024-10-17T213702.286Zj2c-lab-application2.yaml>



## Task 5: Deleting the Stack

1. **Delete the lab-application stack**, observing the deletion policy that creates a snapshot of the EBS volume before deletion.
2. **Verify the deletion process** in the Events tab and confirm that the EBS snapshot was created by checking the Snapshots section in the EC2 console.

## The Code

```
bash
Copy code
#!/bin/bash
```

```
# List resources that will be deleted from lab-application stack
echo "Listing resources that will be deleted with the lab-
application stack..."
aws cloudformation list-stack-resources \
--stack-name lab-application \
--query
```

```
'StackResourceSummaries[*].{ ResourceType: ResourceType, Logical  
ResourceId: Logical  
ResourceId, PhysicalResourceId: PhysicalResourceId }' \  
--output table  
  
# Confirm if the user wants to delete the lab-application stack  
read -p "Do you want to delete the lab-application stack?  
(yes/no): " delete_choice  
if [ "$delete_choice" == "yes" ];  
then # Delete lab-application  
stack  
echo "Deleting lab-application stack..."
```

```
aws cloudformation delete-stack --stack-name lab-application

# Wait for lab-application stack deletion to complete
echo "Waiting for lab-application stack deletion to complete..."
aws cloudformation wait stack-delete-complete --stack-name lab-
application echo "lab-application stack deleted successfully."
else
echo "Stack deletion
cancelled." fi
```

---

## The Output

```
bash
Copy code
Listing resources that will be deleted with the lab-application stack...
```

ListStackResources		
LogicalResourceId	PhysicalResourceId	ResourceType
DiskMountPoint	vol-0f61f40b4888fd2f1 i-	
031e8a3f8dd06be57	AWS::EC2::VolumeAttachment	
DiskVolume	vol-0f61f40b4888fd2f1	
AWS::EC2::Volume		
WebServerInstance	i-031e8a3f8dd06be57	
AWS::EC2::Instance		
WebServerSecurityGroup	sg-0156ab497929174c6	
AWS::EC2::SecurityGroup		

```
Do you want to delete the lab-application stack? (yes/no):
yes Deleting lab-application stack...
Waiting for lab-application stack deletion to
complete... lab-application stack deleted
successfully.
```

## Images for Task 5: Include screenshots of the following for Task 5:

The screenshot shows the AWS CloudFormation console. At the top, there's a navigation bar with 'Stacks (3)', a search bar, and a filter status dropdown set to 'Active'. Below the navigation is a table for the 'lab-application' stack, which was created on 2024-10-17 23:53:14 UTC+0300 and is currently in the 'DELETE\_IN\_PROGRESS' state.

The main view is titled 'lab-application' and shows the 'Resources' tab selected. It lists four resources:

Logical ID	Physical ID	Type	Status	Module
DiskMountPoint	vol-0e5915cb0cd1003b1jj-0d157901c900d9efa	AWS::EC2::VolumeAttachment	✓ DELETE_COMPLETE	-
DiskVolume	vol-0e5915cb0cd1003b1 [ ]	AWS::EC2::Volume	✓ DELETE_COMPLETE	-
WebServerInstance	i-0d157901c900d9efa [ ]	AWS::EC2::Instance	✓ DELETE_COMPLETE	-
WebServerSecurityGroup	sg-0def9734f9d383b82 [ ]	AWS::EC2::SecurityGroup	✓ DELETE_COMPLETE	-

Below this, there's a 'Snapshots (1)' section showing a single snapshot named 'Web Data'.

Name	Snapshot ID	Volume size	Description	Storage tier	Snapshot status	Started
Web Data	snap-0b29c195ca98b3f90	100 GiB	-	Standard	✓ Completed	2024/10/18 00:39 GMT+3

