Free Questions for SOA-C02 by dumpshq

Shared by Casey on 12-12-2023

For More Free Questions and Preparation Resources

Check the Links on Last Page

Question 1

Question Type: MultipleChoice

You need to update an existing AWS CloudFormation stack. If needed, a copy to the CloudFormation template is available in an Amazon SB bucket named cloudformation-bucket

1. Use the us-east-2 Region for all resources.

2. Unless specified below, use the default configuration settings.

3. update the Amazon EQ instance named Devinstance by making the following changes to the stack named 1700182:

a) Change the EC2 instance type to us-east-t2.nano.

b) Allow SSH to connect to the EC2 instance from the IP address range

192.168.100.0/30.

c) Replace the instance profile IAM role with IamRoleB.

4. Deploy the changes by updating the stack using the CFServiceR01e role.

5. Edit the stack options to prevent accidental deletion.

6. Using the output from the stack, enter the value of the ProdInstanceId in the text box below:

Options:

A- Explanation:

Here are the steps to update an existing AWS CloudFormation stack:

Log in to the AWS Management Console and navigate to the CloudFormation service in the us-east-2 Region.

Find the existing stack named 1700182 and click on it.

Click on the 'Update' button.

Choose 'Replace current template' and upload the updated CloudFormation template from the Amazon S3 bucket named 'cloudformation-bucket'

In the 'Parameter' section, update the EC2 instance type to us-east-t2.nano and add the IP address range 192.168.100.0/30 for SSH access.

Replace the instance profile IAM role with IamRoleB.

In the 'Capabilities' section, check the checkbox for 'IAM Resources'

Choose the role CFServiceR01e and click on 'Update Stack'

Wait for the stack to be updated.

Once the update is complete, navigate to the stack and click on the 'Stack options' button, and select 'Prevent updates to prevent accidental deletion'

To get the value of the ProdInstanceId , navigate to the 'Outputs' tab in the CloudFormation stack and find the key 'ProdInstanceId'. The value corresponding to it is the value that you need to enter in the text box below.

Note:

You can use AWS CloudFormation to update an existing stack.

You can use the AWS CloudFormation service role to deploy updates.

You can refer to the AWS CloudFormation documentation for more information on how to update and manage stacks: https://aws.amazon.com/cloudformation/

Answer:

A

Question 2

Question Type: MultipleChoice

A webpage is stored in an Amazon S3 bucket behind an Application Load Balancer (ALB). Configure the SS bucket to serve a static error page in the event of a failure at the primary site.

1. Use the us-east-2 Region for all resources.

2. Unless specified below, use the default configuration settings.

3. There is an existing hosted zone named lab-

751906329398-26023898.com that contains an A record with a simple routing policy that routes traffic to an existing ALB.

4. Configure the existing S3 bucket named lab-751906329398-26023898.com as a static hosted website using the object named index.html as the index document

5. For the index-html object, configure the S3 ACL to allow for public read access. Ensure public access to the S3 bucketjs allowed.

6. In Amazon Route 53, change the A record for domain lab-751906329398-26023898.com to a primary record for a failover routing policy. Configure the record so that it evaluates the health of the ALB to determine failover.

7. Create a new secondary failover alias record for the domain lab-751906329398-26023898.com that routes traffic to the existing 53 bucket.

Options:

A- Explanation:

Here are the steps to configure an Amazon S3 bucket to serve a static error page in the event of a failure at the primary site:

Log in to the AWS Management Console and navigate to the S3 service in the us-east-2 Region.

Find the existing S3 bucket named lab-751906329398-26023898.com and click on it.

In the 'Properties' tab, click on 'Static website hosting' and select 'Use this bucket to host a website'.

In 'Index Document' field, enter the name of the object that you want to use as the index document, in this case, 'index.html'

In the 'Permissions' tab, click on 'Block Public Access', and make sure that 'Block all public access' is turned OFF.

Click on 'Bucket Policy' and add the following policy to allow public read access:

{

'Version': '2012-10-17',

'Statement': [

{

'Sid': 'PublicReadGetObject',

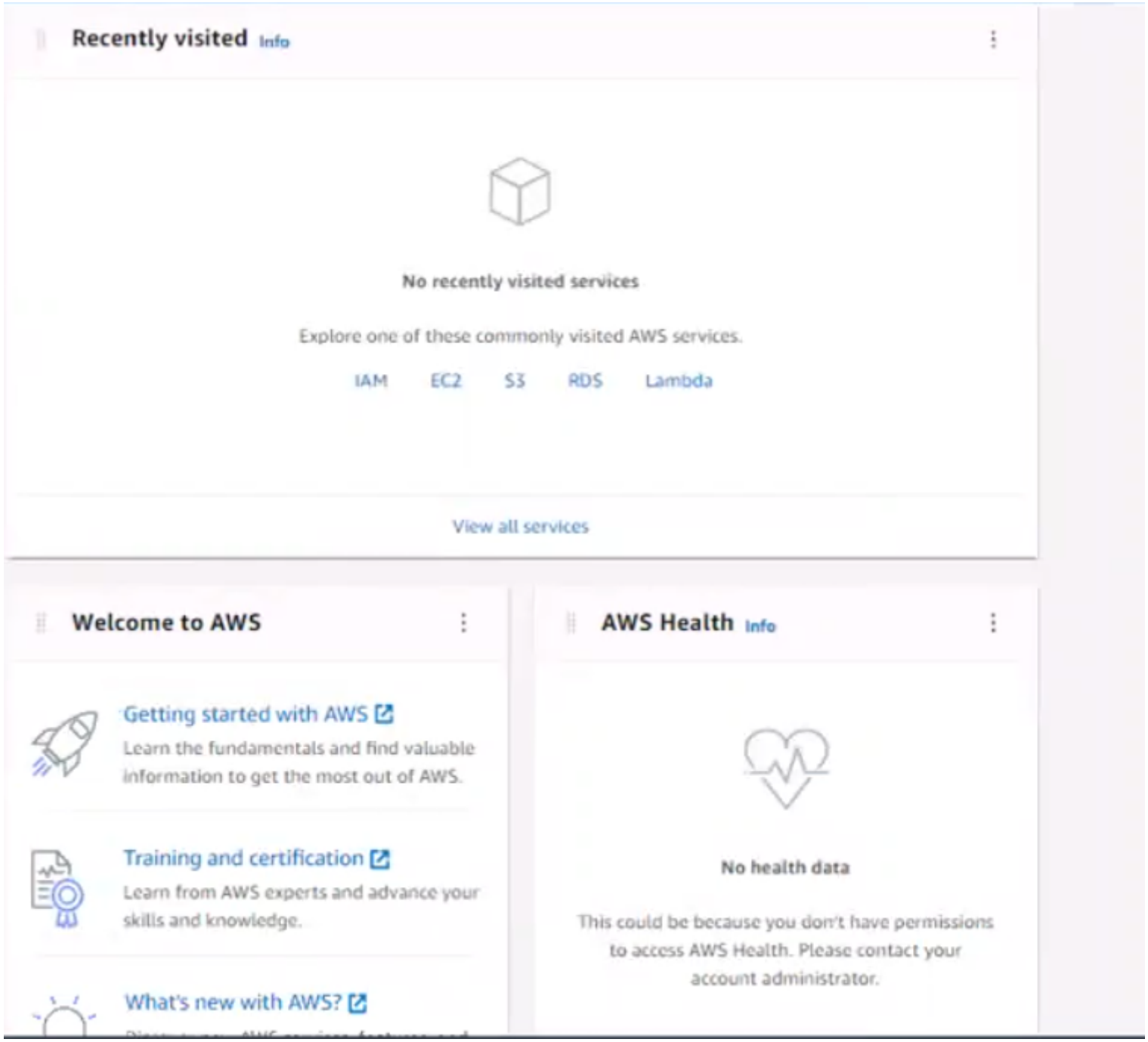
'Effect': 'Allow',

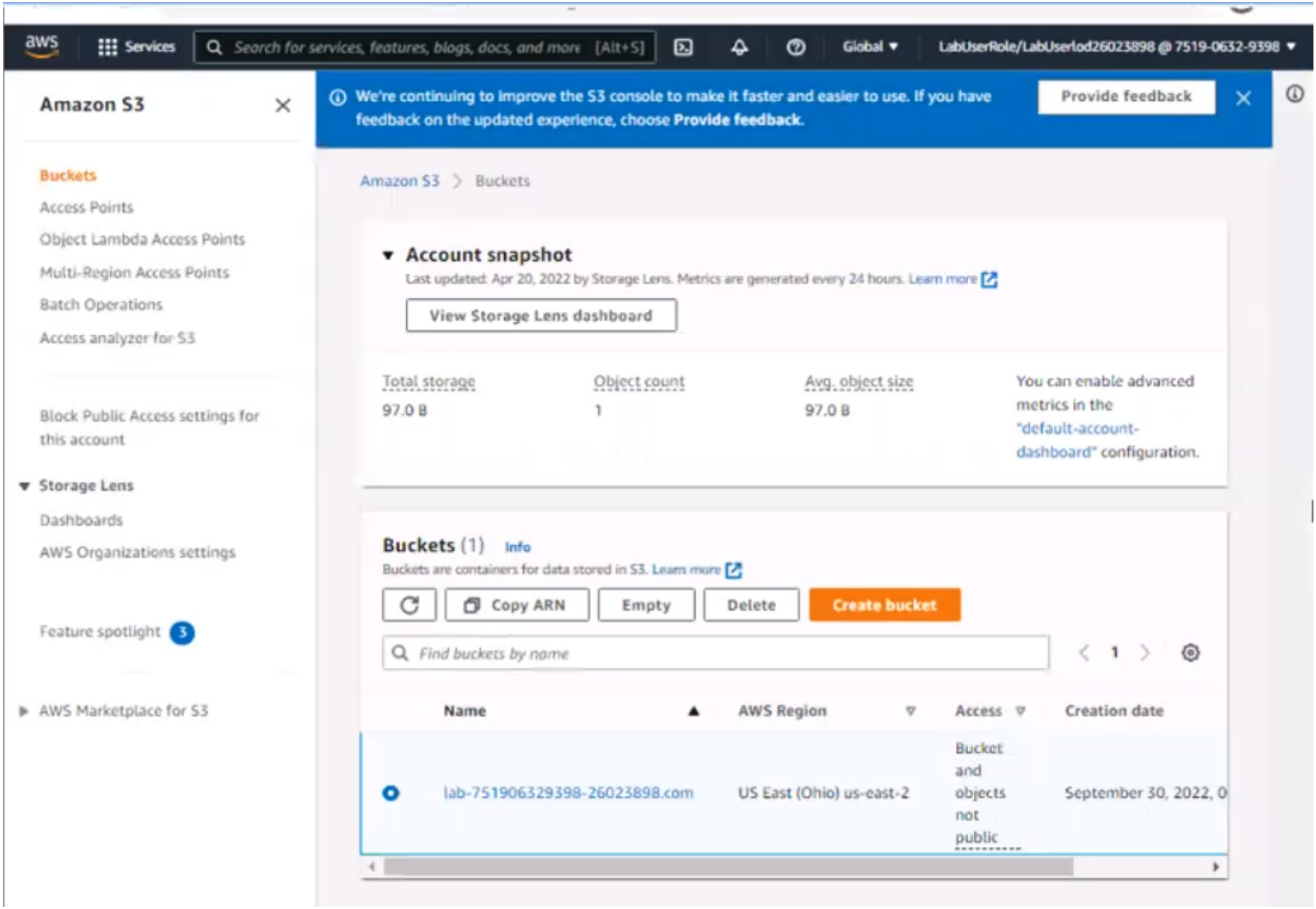
'Principal': '*',

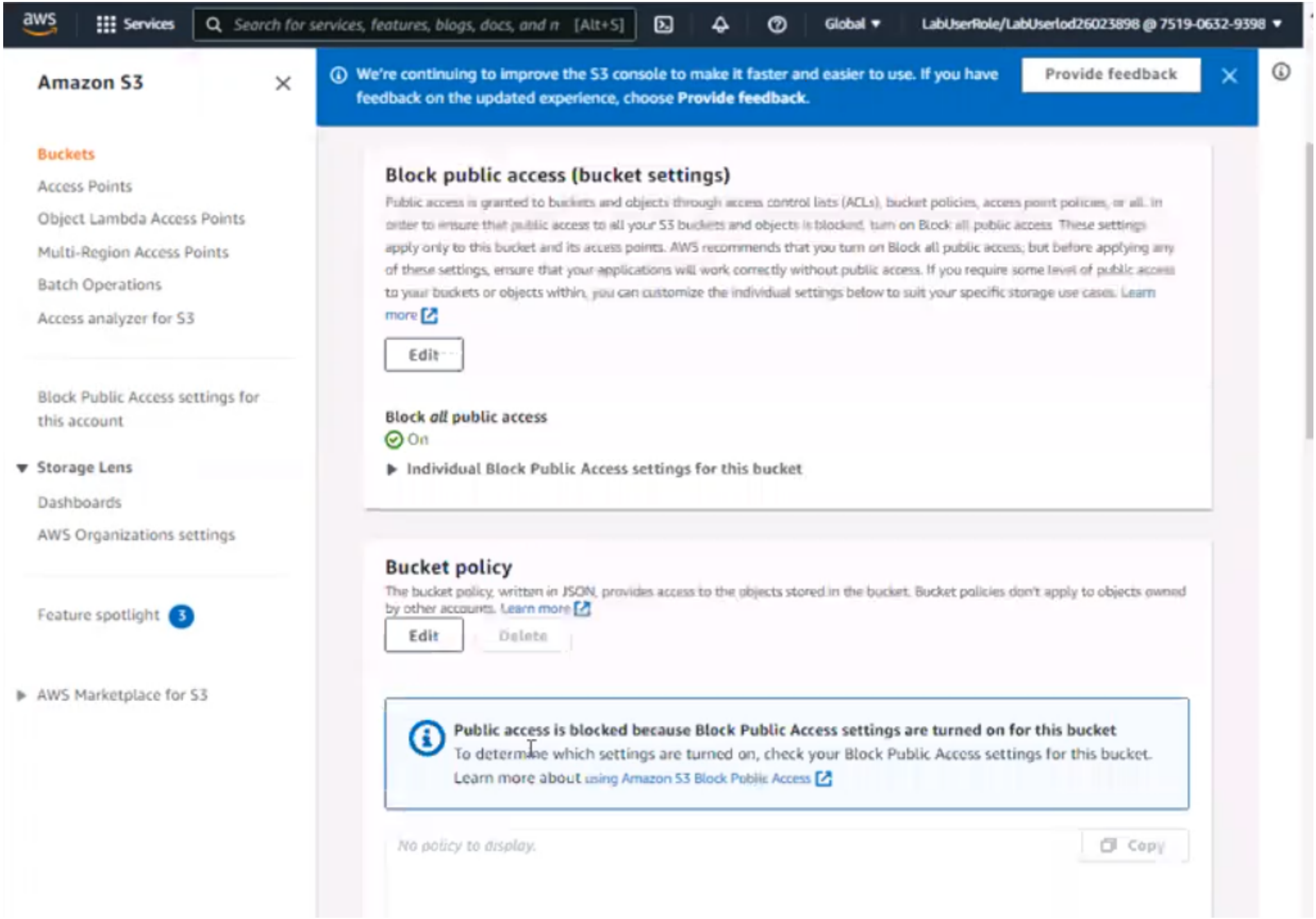
'Action': 's3:GetObject',

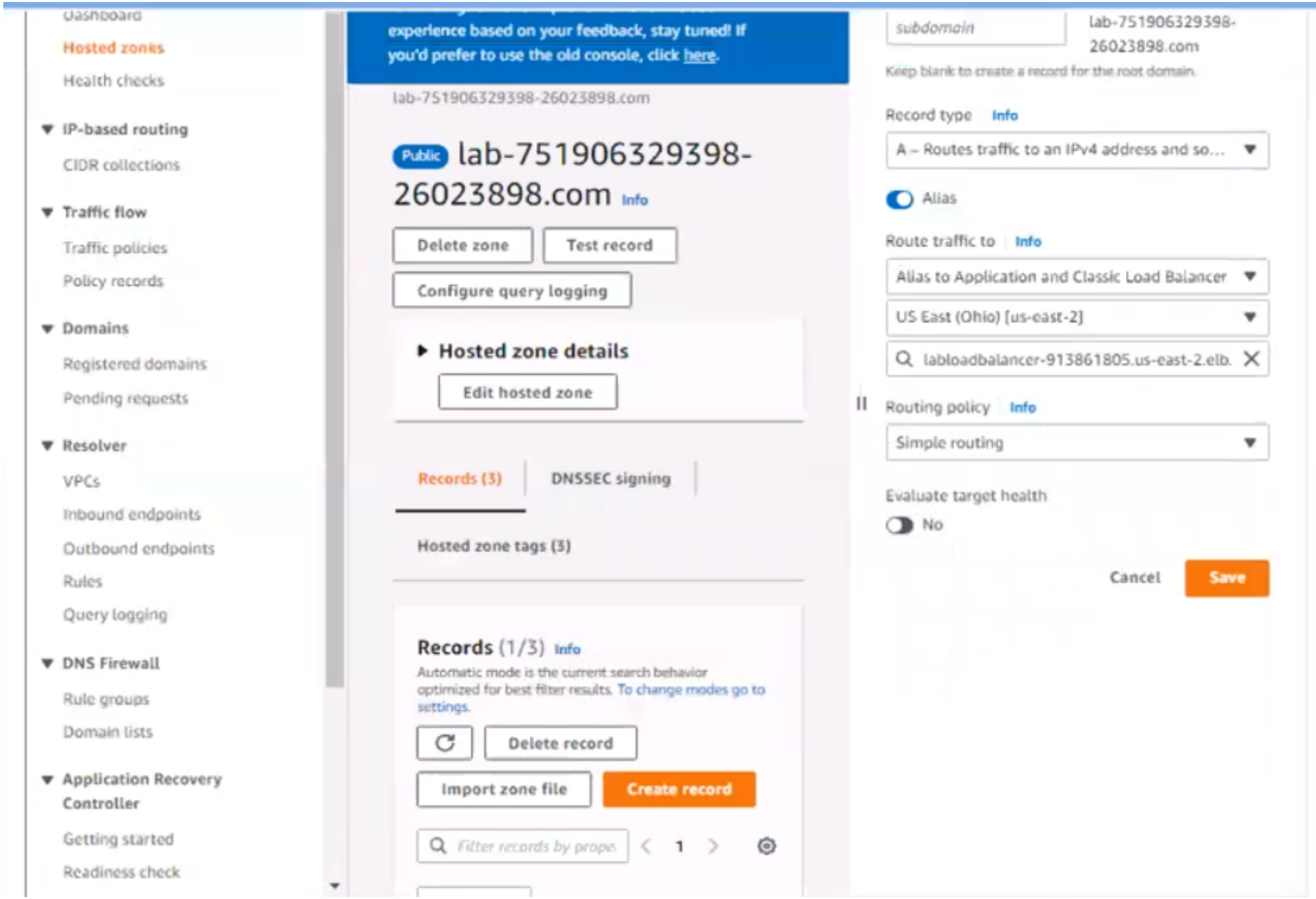
'Resource': 'arn:aws:s3:::lab-751906329398-26023898.com/*'

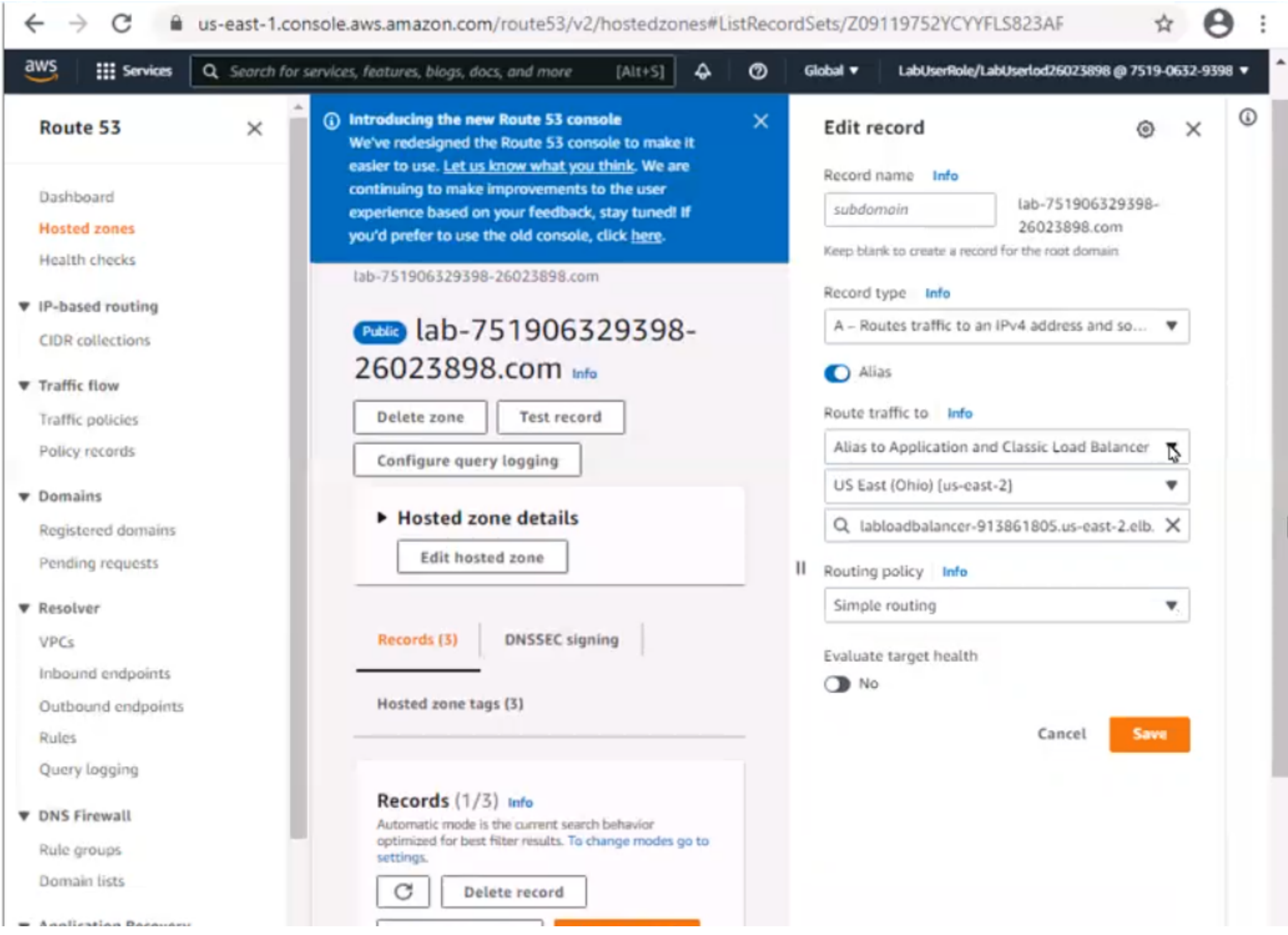
}
]
}
Now navigate to the Amazon Route 53 service, and find the existing hosted zone named lab-751906329398-26023898.com.
Click on the 'A record' and update the routing policy to 'Primary - Failover' and add the existing ALB as the primary record.
Click on 'Create Record' button and create a new secondary failover alias record for the domain lab-751906329398-26023898.com that routes traffic to the existing S3 bucket.
Now, when the primary site (ALB) goes down, traffic will be automatically routed to the S3 bucket serving the static error page.
Note:
You can use CloudWatch to monitor the health of your ALB.
You can use Amazon S3 to host a static website.
You can use Amazon Route 53 for routing traffic to different resources based on health checks.
You can refer to the AWS documentation for more information on how to configure and use these services:
https://aws.amazon.com/s3/
https://aws.amazon.com/route53/
https://aws.amazon.com/cloudwatch/

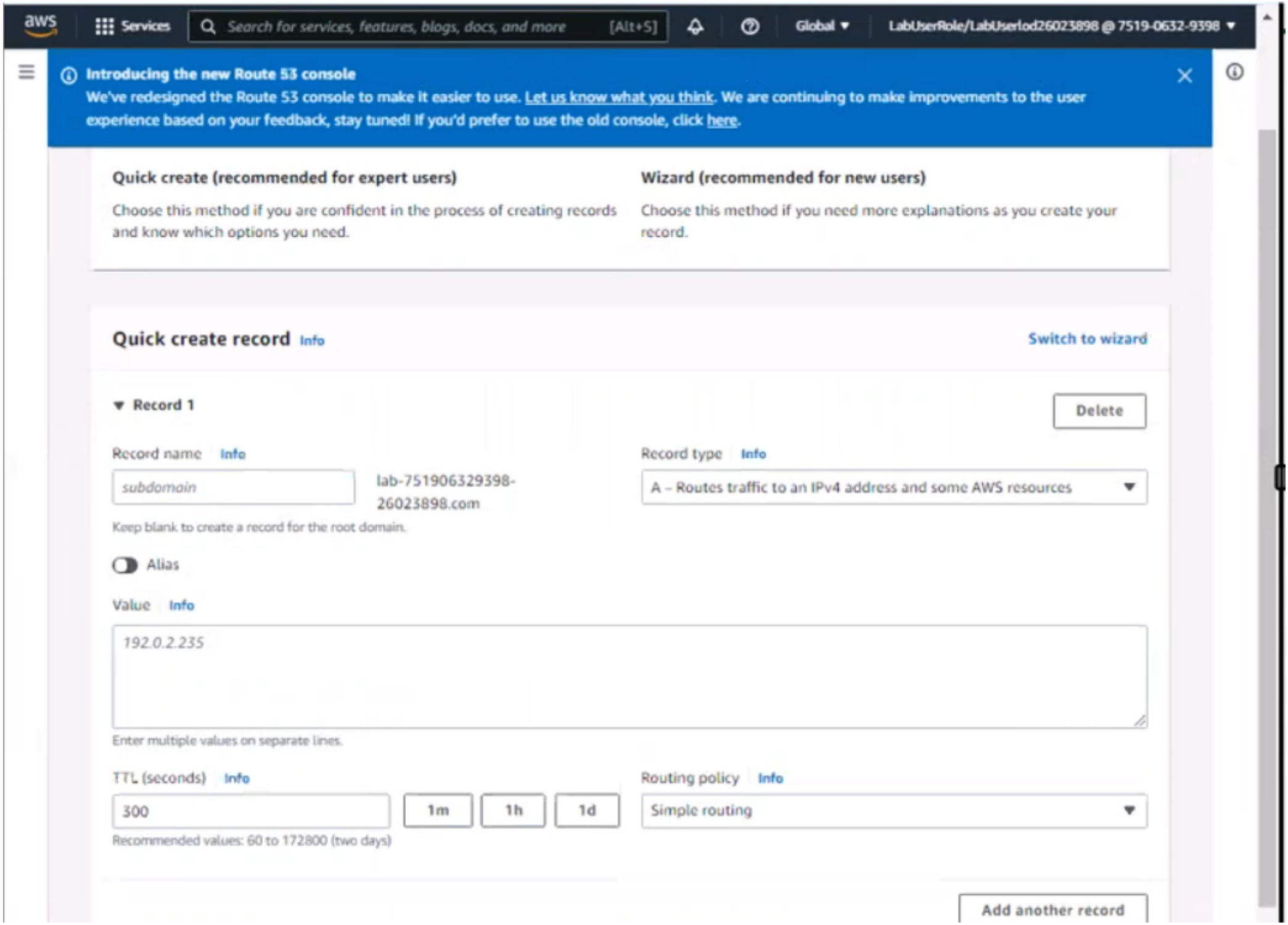

Recently visited Info
No recently visited services
Explore one of these commonly visited AWS services.
IAM EC2 S3 RDS Lambda
View all services
Welcome to AWS
Getting started with AWS
Learn the fundamentals and find valuable information to get the most out of AWS.
Training and certification
Learn from AWS experts and advance your skills and knowledge.
What's new with AWS?
AWS Health Info
No health data
This could be because you don't have permissions to access AWS Health. Please contact your account administrator.

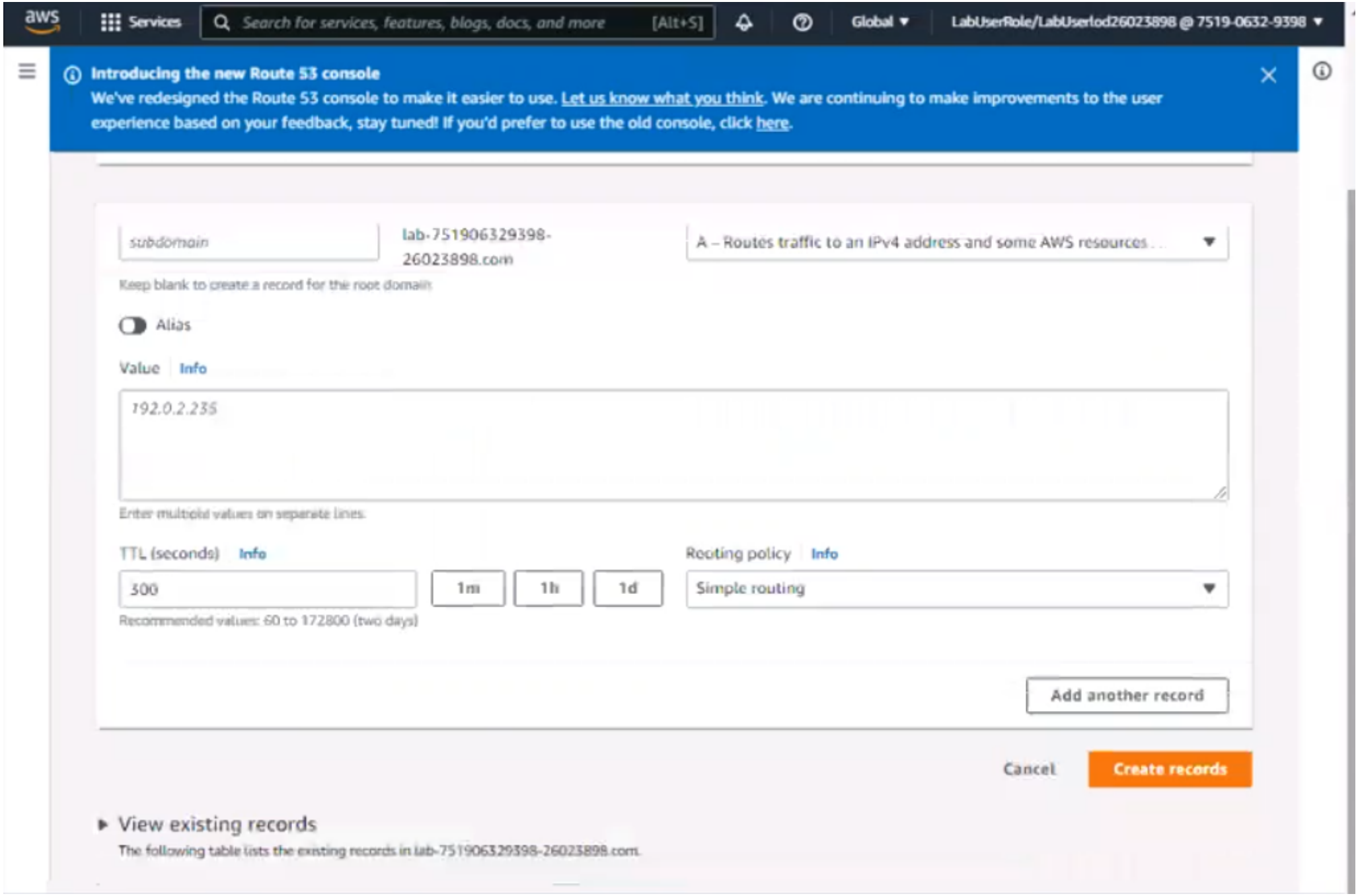

aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
LabUserRole/LabUserIod26023898 @ 7519-0632-9398
Amazon S3
We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.
Provide feedback
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Amazon S3 > Buckets
Account snapshot
Last updated: Apr 20, 2022 by Storage Lens. Metrics are generated every 24 hours. Learn more
View Storage Lens dashboard
Total storage
97.0 B
Object count
1
Avg. object size
97.0 B
You can enable advanced metrics in the "default-account-dashboard" configuration.
Buckets (1) Info
Buckets are containers for data stored in S3. Learn more
Copy ARN
Empty
Delete
Create bucket
Find buckets by name
1
Name
AWS Region
Access
Creation date
lab-751906329398-26023898.com
US East (Ohio) us-east-2
Bucket and objects not public
September 30, 2022, 0

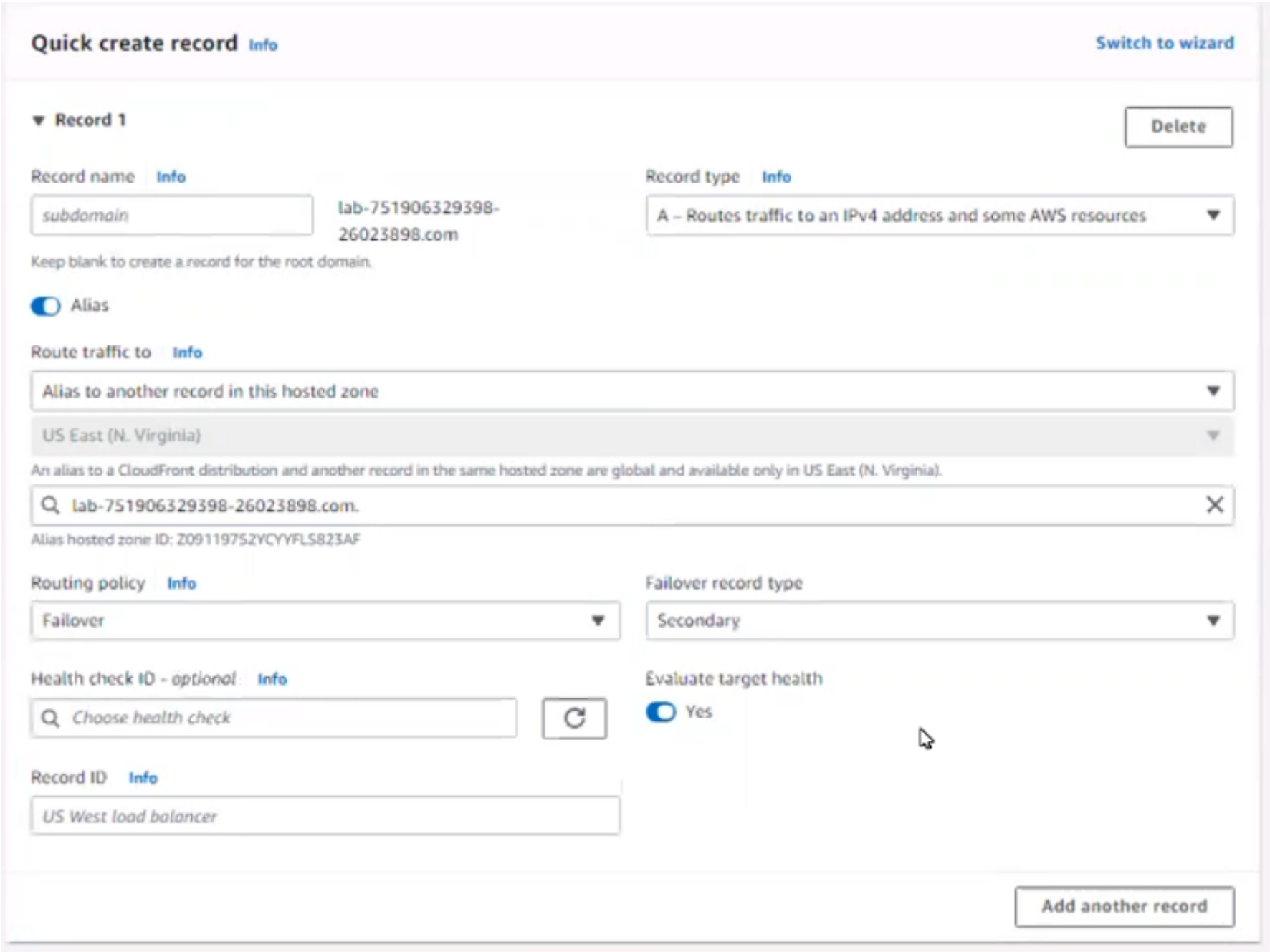

aws
Services
Search for services, features, blogs, docs, and n [Alt+S]
Global
LabUserRole/LabUserId26023898 @ 7519-0632-9398
Amazon S3
We're continuing to improve the S3 console to make it faster and easier to use. If you have feedback on the updated experience, choose Provide feedback.
Provide feedback
Buckets
Access Points
Object Lambda Access Points
Multi-Region Access Points
Batch Operations
Access analyzer for S3
Block Public Access settings for this account
Storage Lens
Dashboards
AWS Organizations settings
Feature spotlight 3
AWS Marketplace for S3
Block public access (bucket settings)
Public access is granted to buckets and objects through access control lists (ACLs), bucket policies, access point policies, or all. In order to ensure that public access to all your S3 buckets and objects is blocked, turn on Block all public access. These settings apply only to this bucket and its access points. AWS recommends that you turn on Block all public access, but before applying any of these settings, ensure that your applications will work correctly without public access. If you require some level of public access to your buckets or objects within, you can customize the individual settings below to suit your specific storage use cases. Learn more
Edit
Block all public access
On
Individual Block Public Access settings for this bucket
Bucket policy
The bucket policy, written in JSON, provides access to the objects stored in the bucket. Bucket policies don't apply to objects owned by other accounts. Learn more
Edit
Delete
Public access is blocked because Block Public Access settings are turned on for this bucket
To determine which settings are turned on, check your Block Public Access settings for this bucket.
Learn more about using Amazon S3 Block Public Access
No policy to display.
Copy


Dashboard
Hosted zones
Health checks
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
DNS Firewall
Rule groups
Domain lists
Application Recovery Controller
Getting started
Readiness check
experience based on your feedback, stay tuned! If you'd prefer to use the old console, click here.
lab-751906329398-26023898.com
Public lab-751906329398-26023898.com Info
Delete zone
Test record
Configure query logging
Hosted zone details
Edit hosted zone
Records (3)
DNSSEC signing
Hosted zone tags (3)
Records (1/3) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Delete record
Import zone file
Create record
Filter records by prope
1
subdomain
lab-751906329398-26023898.com
Keep blank to create a record for the root domain.
Record type Info
A – Routes traffic to an IPv4 address and so...
Alias
Route traffic to Info
Alias to Application and Classic Load Balancer
US East (Ohio) [us-east-2]
labloadbalancer-913861805.us-east-2.elb.
Routing policy Info
Simple routing
Evaluate target health
No
Cancel
Save


us-east-1.console.aws.amazon.com/route53/v2/hostedzones#ListRecordSets/Z09119752YCYYFLS823AF
aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
LabUserRole/LabUserId26023898 @ 7519-0632-9398
Route 53
Dashboard
Hosted zones
Health checks
IP-based routing
CIDR collections
Traffic flow
Traffic policies
Policy records
Domains
Registered domains
Pending requests
Resolver
VPCs
Inbound endpoints
Outbound endpoints
Rules
Query logging
DNS Firewall
Rule groups
Domain lists
Introducing the new Route 53 console
We've redesigned the Route 53 console to make it easier to use. Let us know what you think. We are continuing to make improvements to the user experience based on your feedback, stay tuned! If you'd prefer to use the old console, click here.
lab-751906329398-26023898.com
Public lab-751906329398-26023898.com Info
Delete zone
Test record
Configure query logging
Hosted zone details
Edit hosted zone
Records (3)
DNSSEC signing
Hosted zone tags (3)
Records (1/3) Info
Automatic mode is the current search behavior optimized for best filter results. To change modes go to settings.
Delete record
Edit record
Record name Info
subdomain
lab-751906329398-26023898.com
Keep blank to create a record for the root domain
Record type Info
A – Routes traffic to an IPv4 address and so...
Alias
Route traffic to Info
Alias to Application and Classic Load Balancer
US East (Ohio) [us-east-2]
labloadbalancer-913861805.us-east-2.elb.
Routing policy Info
Simple routing
Evaluate target health
No
Cancel
Save


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
LabUserRole/LabUserId26023898 @ 7519-0632-9398
Introducing the new Route 53 console
We've redesigned the Route 53 console to make it easier to use. Let us know what you think. We are continuing to make improvements to the user experience based on your feedback, stay tuned! If you'd prefer to use the old console, click here.
Quick create (recommended for expert users)
Choose this method if you are confident in the process of creating records and know which options you need.
Wizard (recommended for new users)
Choose this method if you need more explanations as you create your record.
Quick create record Info
Switch to wizard
Record 1
Delete
Record name Info
subdomain
lab-751906329398-26023898.com
Keep blank to create a record for the root domain.
Record type Info
A – Routes traffic to an IPv4 address and some AWS resources
Alias
Value Info
192.0.2.235
Enter multiple values on separate lines.
TTL (seconds) Info
300
1m
1h
1d
Recommended values: 60 to 172800 (two days)
Routing policy Info
Simple routing
Add another record


aws
Services
Search for services, features, blogs, docs, and more [Alt+S]
Global
LabUserRole/LabUserId26023898 @ 7519-0632-9398
Introducing the new Route 53 console
We've redesigned the Route 53 console to make it easier to use. Let us know what you think. We are continuing to make improvements to the user experience based on your feedback, stay tuned! If you'd prefer to use the old console, click here.
subdomain
lab-751906329398-26023898.com
A – Routes traffic to an IPv4 address and some AWS resources
Keep blank to create a record for the root domain.
Alias
Value Info
192.0.2.235
Enter multiple values on separate lines.
TTL (seconds) Info
300
1m
1h
1d
Recommended values: 60 to 172800 (two days)
Routing policy Info
Simple routing
Add another record
Cancel
Create records
View existing records
The following table lists the existing records in lab-751906329398-26023898.com.


Quick create record Info
Switch to wizard
Record 1
Delete
Record name Info
subdomain
lab-751906329398-26023898.com
Record type Info
A – Routes traffic to an IPv4 address and some AWS resources
Keep blank to create a record for the root domain.
Alias
Route traffic to Info
Alias to another record in this hosted zone
US East (N. Virginia)
An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).
lab-751906329398-26023898.com.
Alias hosted zone ID: Z09119752YCYYFLS823AF
Routing policy Info
Failover
Failover record type
Secondary
Health check ID - optional Info
Choose health check
Evaluate target health
Yes
Record ID Info
US West load balancer
Add another record

make improvements to the user experience based on your feedback, stay tuned! If you'd prefer to use the old console, click here.

Route 53 > Hosted zones > lab-751906329398-26023898.com > Create record

Record creation method

Quick create (recommended for expert users)

Choose this method if you are confident in the process of creating records and know which options you need.

Wizard (recommended for new users)

Choose this method if you need more explanations as you create your record.

Quick create record Info

Switch to wizard

Record 1

Delete

Record name Info

subdomain

lab-751906329398-26023898.com

Keep blank to create a record for the root domain.

Record type Info

A – Routes traffic to an IPv4 address and som...

Alias

Route traffic to Info

Alias to another record in this hosted zone

US East (N. Virginia)

An alias to a CloudFront distribution and another record in the same hosted zone are global and available only in US East (N. Virginia).

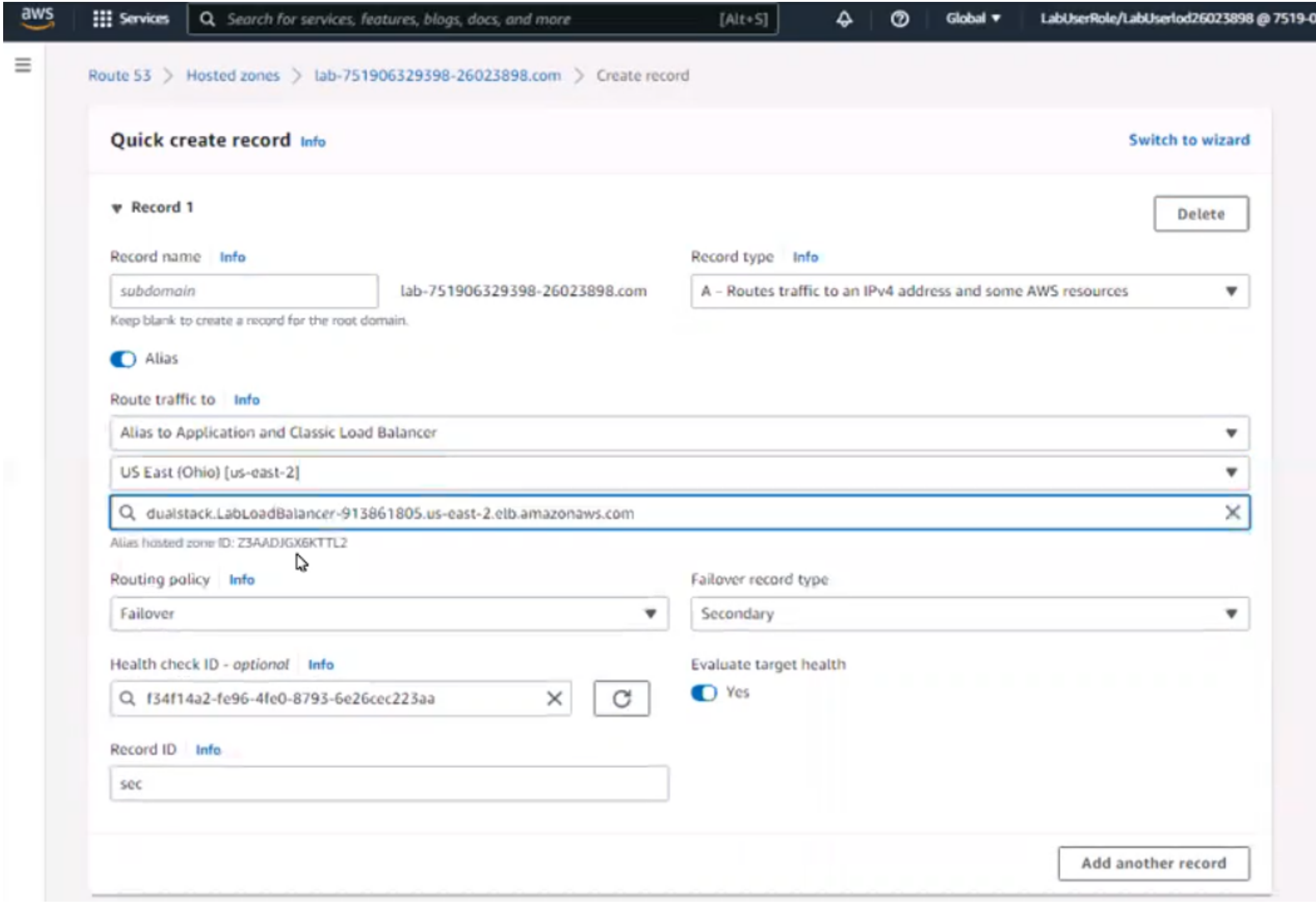
lab-751906329398-26023898.com.

Alias hosted zone ID: Z09119752YCYYFLS823AF

When you create records that have a routing policy other than simple, enter a value that uniquely identifies each record that has the same name and type. For example, you might assign a date/time stamp or a sequential counter.

Learn more

Working with records


aws
Services
Search for services, features, blogs, docs, and more
[Alt+S]
Global
LabUserRole/LabUserId26023898 @ 7519-0
Route 53 > Hosted zones > lab-751906329398-26023898.com > Create record
Quick create record Info
Switch to wizard
Record 1
Delete
Record name Info
subdomain
lab-751906329398-26023898.com
Keep blank to create a record for the root domain.
Record type Info
A – Routes traffic to an IPv4 address and some AWS resources
Alias
Route traffic to Info
Alias to Application and Classic Load Balancer
US East (Ohio) [us-east-2]
dualstack.LabLoadBalancer-913861805.us-east-2.elb.amazonaws.com
Alias hosted zone ID: Z3AADJGX6KTTL2
Routing policy Info
Failover
Failover record type
Secondary
Health check ID - optional Info
f34f14a2-fe96-4fe0-8793-6e26cec223aa
Evaluate target health
Yes
Record ID Info
sec
Add another record

Answer:

A

Question 3

Question Type: MultipleChoice

If your AWS Management Console browser does not show that you are logged in to an AWS account, close the browser and relaunch the

console by using the AWS Management Console shortcut from the VM desktop.

If the copy-paste functionality is not working in your environment, refer to the instructions file on the VM desktop and use Ctrl+C, Ctrl+V or Command-C , Command-V.

Configure Amazon EventBridge to meet the following requirements.

1. use the us-east-2 Region for all resources,

2. Unless specified below, use the default configuration settings.

3. Use your own resource naming unless a resource

name is specified below.

4. Ensure all Amazon EC2 events in the default event

bus are replayable for the past 90 days.

5. Create a rule named RunFunction to send the exact message every 1 5 minutes to an existing AWS Lambda function named LogEventFunction.

6. Create a rule named SpotWarning to send a notification to a new standard Amazon SNS topic named TopicEvents whenever an Amazon EC2

Spot Instance is interrupted. Do NOT create any topic subscriptions. The notification must match the following structure:

Input path:

```
{"instance":"$.detail.instance-id"}
```

Input Path:

{"instance" : "$.detail.instance-id"}

Input template:

" The EC2 Spot Instance has been on account.

Options:

A- Explanation:

Here are the steps to configure Amazon EventBridge to meet the above requirements:

Log in to the AWS Management Console by using the AWS Management Console shortcut from the VM desktop. Make sure that you are logged in to the desired AWS account.

Go to the EventBridge service in the us-east-2 Region.

In the EventBridge service, navigate to the 'Event buses' page.

Click on the 'Create event bus' button.

Give a name to your event bus, and select 'default' as the event source type.

Navigate to 'Rules' page and create a new rule named 'RunFunction'

In the 'Event pattern' section, select 'Schedule' as the event source and set the schedule to run every 15 minutes.

In the 'Actions' section, select 'Send to Lambda' and choose the existing AWS Lambda function named 'LogEventFunction'

Create another rule named 'SpotWarning'

In the 'Event pattern' section, select 'EC2' as the event source, and filter the events on 'EC2 Spot Instance interruption'

In the 'Actions' section, select 'Send to SNS topic' and create a new standard Amazon SNS topic named 'TopicEvents'

In the 'Input Transformer' section, set the Input Path to {"instance" : "$.detail.instance-id"} and Input template to "The EC2 Spot Instance <instance> has been interrupted on account.

Now all Amazon EC2 events in the default event bus will be replayable for past 90 days.

Note:

You can use the AWS Management Console, AWS CLI, or SDKs to create and manage EventBridge resources.

You can use CloudTrail event history to replay events from the past 90 days.

You can refer to the AWS EventBridge documentation for more information on how to configure and use the service: https://aws.amazon.com/eventbridge/

Answer:

A

Question 4

Question Type: MultipleChoice

A company needs to take an inventory of applications that are running on multiple Amazon EC2 instances. The company has configured users and roles with the appropriate permissions for AWS Systems Manager. An updated version of Systems Manager Agent has been installed and is running on every instance. While configuring an inventory collection, a SysOps administrator discovers that not all the instances in a single subnet are managed by Systems Manager.

What must the SysOps administrator do to fix this issue?

Options:

A- Ensure that all the EC2 instances have the correct tags for Systems Manager access.

B- Configure AWS Identity and Access Management Access Analyzer to determine and automatically remediate the issue.

C- Ensure that all the EC2 instances have an instance profile with Systems Manager access.

D- Configure Systems Manager to use an interface VPC endpoint.

Answer:

C

Explanation:

Ensuring that all the EC2 instances have an instance profile with Systems Manager access is the most effective way to fix this issue. Having an instance profile with Systems Manager access will allow the SysOps administrator to configure the inventory collection for all the instances in the subnet, regardless of whether or not they are managed by Systems Manager.

Topic 2, Simulation

Question 5

Question Type: **MultipleChoice**

A SysOps administrator creates two VPCs, VPC1 and VPC2, in a company's AWS account The SysOps administrator deploys a Linux Amazon EC2 instance in VPC1 and deploys an Amazon RDS for MySQL DB instance in VPC2. The DB instance is deployed in a private subnet. An application that runs on the EC2 instance needs to connect to the database.

What should the SysOps administrator do to give the EC2 instance the ability to connect to the database?

Options:

A- Enter the DB instance connection string into the VPC1 route table.

B- Configure VPC peering between the two VPCs.

C- Add the same IPv4 CIDR range for both VPCs.

D- Connect to the DB instance by using the DB instance's public IP address.

Answer:

B

Explanation:

VPC peering allows two VPCs to communicate with each other securely. By configuring VPC peering between the two VPCs, the SysOps administrator will be able to give the EC2 instance in VPC1 the ability to connect to the database in VPC2. Once the VPC peering is configured, the EC2 instance will be able to communicate with the database using the private IP address of the DB instance in the private subnet.

Question 6

Question Type: MultipleChoice

A company recently migrated its application to a VPC on AWS. An AWS Site-to-Site VPN connection connects the company's on-premises network to the VPC. The application retrieves customer data from another system that resides on premises. The application uses an on-premises DNS server to resolve domain records. After the migration, the application is not able to connect to the customer data because of name resolution errors.

Which solution will give the application the ability to resolve the internal domain names?

Options:

A- Launch EC2 instances in the VPC. On the EC2 instances, deploy a custom DNS forwarder that forwards all DNS requests to the on-premises DNS server. Create an Amazon Route 53 private hosted zone that uses the EC2 instances for name servers.

B- Create an Amazon Route 53 Resolver outbound endpoint. Configure the outbound endpoint to forward DNS queries against the on-premises domain to the on-premises DNS server.

C- Set up two AWS Direct Connect connections between the AWS environment and the on-premises network. Set up a link aggregation group (LAG) that includes the two connections. Change the VPC resolver address to point to the on-premises DNS server.

D- Create an Amazon Route 53 public hosted zone for the on-premises domain. Configure the network ACLs to forward DNS requests against the on-premises domain to the Route 53 public hosted zone.

Answer:

B

Explanation:

https://docs.aws.amazon.com/zh_tw/Route53/latest/DeveloperGuide/resolver-forwarding-outbound-queries.html

Question 7

Question Type: MultipleChoice

A company runs an application on Amazon EC2 instances. The EC2 instances are in an Auto Scaling group and run behind an Application Load Balancer (ALB). The application experiences errors when total requests exceed 100 requests per second. A SysOps administrator must collect information about total requests for a 2-week period to determine when requests exceeded this threshold.

What should the SysOps administrator do to collect this data?

Options:

A- Use the ALB's RequestCount metric. Configure a time range of 2 weeks and a period of 1 minute. Examine the chart to determine peak traffic times and volumes.

B- Use Amazon CloudWatch metric math to generate a sum of request counts for all the EC2 instances over a 2-week period. Sort by a 1-minute interval.

C- Create Amazon CloudWatch custom metrics on the EC2 launch configuration templates to create aggregated request metrics across all the EC2 instances.

D- Create an Amazon EventBridge (Amazon CloudWatch Events) rule. Configure an EC2 event matching pattern that creates a metric that is based on EC2 requests. Display the data in a graph.

Answer:

A

Explanation:

Using the ALB's RequestCount metric will allow the SysOps administrator to collect information about total requests for a 2-week period and determine when requests exceeded the threshold of 100 requests per second. Configuring a time range of 2 weeks and a period of 1 minute will ensure that the data can be accurately examined to determine peak traffic times and volumes.

Question 8

Question Type: MultipleChoice

A company's SysOps administrator regularly checks the AWS Personal Health Dashboard in each of the company's accounts. The accounts are part of an organization in AWS Organizations. The company recently added 10 more accounts to the organization. The

SysOps administrator must consolidate the alerts from each account's Personal Health Dashboard.

Which solution will meet this requirement with the LEAST amount of effort?

Options:

A- Enable organizational view in AWS Health.

B- Configure the Personal Health Dashboard in each account to forward events to a central AWS CloudTrail log.

C- Create an AWS Lambda function to query the AWS Health API and to write all events to an Amazon DynamoDB table.

D- Use the AWS Health API to write events to an Amazon DynamoDB table.

Answer:

A

Explanation:

Enabling the organizational view in AWS Health will allow the SysOps administrator to consolidate the alerts from each account's Personal Health Dashboard. It will also provide the administrator with a single view of all the accounts in the organization, allowing them to easily monitor the health of all the accounts in the organization.

Question 9

Question Type: MultipleChoice

A company's reporting job that used to run in 15 minutes is now taking an hour to run. An application generates the reports. The application runs on Amazon EC2 instances and extracts data from an Amazon RDS for MySQL database.

A SysOps administrator checks the Amazon CloudWatch dashboard for the RDS instance and notices that the Read IOPS metrics are high, even when the reports are not running. The SysOps administrator needs to improve the performance and the availability of the RDS instance.

Which solution will meet these requirements?

Options:

A- Configure an Amazon ElastiCache cluster in front of the RDS instance. Update the reporting job to query the ElastiCache cluster.

B- Deploy an RDS read replica. Update the reporting job to query the reader endpoint.

C- Create an Amazon CloudFront distribution. Set the RDS instance as the origin. Update the reporting job to query the CloudFront distribution.

D- Increase the size of the RDS instance.

Answer:

B

Explanation:

Using an RDS read replica will improve the performance and availability of the RDS instance by offloading read queries to the replica. This will also ensure that the reporting job completes in a timely manner and does not affect the performance of other queries that might be running on the RDS instance. Additionally, updating the reporting job to query the reader endpoint will ensure that all read queries are directed to the read replica.

Question 10

Question Type: MultipleChoice

A company recently purchased Savings Plans. The company wants to receive email notification when the company's utilization drops below 90% for a given day.

Which solution will meet this requirement?

Options:

A- Create an Amazon CloudWatch alarm to monitor the Savings Plan check in AWS Trusted Advisor. Configure an Amazon Simple

Queue Service (Amazon SQS) queue for email notification when the utilization drops below 90% for a given day.

B- Create an Amazon CloudWatch alarm to monitor the SavingsPlansUtilization metric under the AWS/SavingsPlans namespace in CloudWatch. Configure an Amazon Simple Queue Service (Amazon SQS) queue for email notification when the utilization drops below 90% for a given day.

C- Create a Savings Plans alert to monitor the daily utilization of the Savings Plans. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification when the utilization drops below 90% for a given day.

D- Use AWS Budgets to create a Savings Plans budget to track the daily utilization of the Savings Plans. Configure an Amazon Simple Notification Service (Amazon SNS) topic for email notification when the utilization drops below 90% for a given day.

Answer:

D

Explanation:

AWS Budgets can be used to create a Savings Plans budget and track the daily utilization of the company's Savings Plans. By creating a budget, it will trigger an action when the utilization drops below 90%, which in this case will be to send an email notification via an Amazon SNS topic. This will ensure that the company is notified when their Savings Plans utilization drops below 90%, allowing them to take action if necessary.