

Id	Name	Description
39320	Access a DynamoDB Table Securely from an AWS Lambda Function [Advanced]	In this Challenge Lab, you will deploy an AWS Lambda function that securely accesses an Amazon DynamoDB table. First, you will define an IAM role for your AWS Lambda function that grants it access to your DynamoDB table. Next, you will deploy your Lambda function with the IAM role assigned. Finally, you will test accessing your Lambda function via a function URL, to verify your Lambda function can access Amazon DynamoDB. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
39592	Add a PUT Method to an Amazon API Gateway [Advanced]	In this Challenge Lab, you will add a PUT method to an AWS Lambda API fronted by Amazon API Gateway that writes data to an Amazon DynamoDB database, test this change, and then promote it to a new testing environment. First, you will create a new Lambda function that can add data to a DynamoDB database. Next, you will add a route to an API Gateway that supports the HTTP PUT verb against this function. Then, you will verify that you can submit and store data successfully in DynamoDB by using the new cloudfunction endpoint. Then, you will create a new stage in API Gateway called test and promote your changes from dev to test. Then, you will add a new test API key and usage plan to API Gateway. Finally, you will verify you can call the endpoint successfully in test. Note: Once you begin the
30385	Automate Snapshots by Using DLM [Guided]	In this challenge, you will configure automated snapshots of the Elastic Block Store (EBS) volumes on your web servers. First, you will create tags for your volumes. Next, you will create an Amazon Data Lifecycle Manager (DLM) lifecycle policy that uses an hourly schedule, and then you will verify that a snapshot was created. Finally, you will replace the root volume on a web server by using a snapshot. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
21975	Build a Network by Using the VPC Wizard [Guided]	In this challenge, you will create a custom VPC with public and private subnets, and an Internet and NAT Gateway, and then you will associate route tables with the correct subnets. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21976	Build VPC Resources Manually [Guided]	In this challenge, you will create a custom VPC with public and private subnets, and an Internet and NAT Gateway. You will then associate route tables with the correct subnets. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
30595	Can You Automate Processes by Using AWS Services? [Advanced]	In this challenge, you will automate processes by using AWS services. First, enable AWS Config rules to verify compliance with allowed Amazon Elastic Cloud Compute (EC2) instance types and Amazon Simple Storage Service (S3) bucket encryption, and then enable AWS SM to support host management. Next, create an AWS CloudFormation stack that includes an Amazon Virtual Private Cloud (VPC), EC2 instances, and an S3 bucket, and then you will create an EventBridge rule that sends an email by using the Amazon Simple Notification Service (SNS) whenever a Systems Manager automation executes. Finally, check for compliance, and then you will add a remediation to the Config rules.
21792	Can You Automate the Build of EC2 Instances Behind an Elastic Load Balancer? [Advanced]	In this challenge, you will automate the creation of a highly available website that will load balance traffic across multiple web servers. First, you will create an IAM role, and then you will create two EC2 instances. Next, you will install a web server by using AWS System Manager Run Command. Finally, you will create a target group that contains the two EC2 instances, and then you will create an elastic load balancer that uses the target group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21977	Can You Build a Network Foundation in AWS? [Advanced]	In this challenge, you will create a custom VPC with public and private subnets, and an Internet and NAT Gateway. You will then associate route tables with the correct subnets. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21980	Can You Build a Website by Using an Amazon S3 Bucket? [Advanced]	In this challenge, you will create a static website by using an Amazon Simple Storage Service (Amazon S3) bucket. First, you will create an Amazon S3 bucket, and then you will configure version control for the bucket. Next, you will create a static website, and then you will configure public access for the bucket. Finally, you will enable transfer acceleration for the bucket, and then you will create a lifecycle rule that will archive old content automatically. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21793	Can You Configure a Resilient EC2 Server Farm? [Expert]	In this challenge, you will configure a web server farm that can scale to meet future demand. First, you will configure the supporting resources, and then you will create a custom Amazon Machine Image (AMI) based on an existing instance. Next, you will create a launch template, and then you will configure an Auto Scaling group. Finally, you will install a web server by using AWS System Manager Run Command, and then you will configure load balancing for the server farm. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
28710	Can You Configure a Resilient Website That Uses Monitoring and Automatic Remediation? [Expert]	In this challenge, you will build a web server that is monitored for memory usage and internal server errors. First, create and secure a new Amazon Elastic Cloud Compute instance that runs as a web server, and then you will connect to the instance by using EC2 Instance Connect. Next, configure the Amazon CloudWatch logs agent on the web server to monitor memory usage and HTTP access logs, and then you will use the custom memory metric to create a CloudWatch alarm that will trigger a restart of the instance. Finally, you will configure a log filter for internal server errors, and then you will create a CloudWatch alarm by using a custom log metric. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab before you start.
24445	Can You Configure an Auto Scaling Group and a Load Balancer? [Advanced]	In this challenge, you will configure a website that can scale from two to four load balanced instances based upon demand. First, you will create a target group, and then you will create an Application Load Balancer that uses the target group. Next, you will create a launch template, and then you will configure an Auto Scaling group that will scale out when the CPU load of the instances is 80 percent or higher. Finally, you will test the Auto Scaling group and the load balancer. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21786	Can You Create a Custom AMI Based on a New EC2 Instance? [Advanced]	In this challenge, you will create a web server template. First, you will create a key pair, and then you will create a security group. Next, you will create an EC2 instance that uses a user data script to install an Apache web server, and then you will add an additional EBS volume to store data. Finally, you will create an Amazon Machine Image (AMI) from the web server instance, and then you will test the new web server. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21789	Can You Create a Resilient System by Using a Launch Template and an Auto Scaling Group? [Advanced]	In this challenge, you will create a resilient set of servers that can be easily duplicated. First, you will create a key pair, and then you will create a security group. Next, you will create a new Amazon Machine Image (AMI) by using an existing instance, and then you will create a launch template. Finally, you will create an Auto Scaling group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
39630	Can You Create a Secure Serverless REST API in AWS? [Expert]	In this Challenge Lab, you will test your skills at creating a secure serverless REST API on AWS by using Amazon IAM, AWS Lambda, Amazon Dynamo DB, and Amazon API Gateway. First, you will create a DynamoDB table to store player score data for an online game, and then you will configure and upload an AWS Lambda function that reads and writes data to the DynamoDB table, using an AWS IAM role to authorize table access. Next, you will create an Amazon API Gateway that defines your AWS Lambda function as an integration. Finally, you will define an API key for the Amazon API Gateway REST API function and verify that you can call your API using the key.
19507	Can You Create a Website with Cross Region Replication and Logging? [Expert]	In this challenge, you will create a bucket for logs files, create a static website, and turn on version control and logging of files that are changed. You will then encrypt all content that is uploaded both in the website bucket and in the log bucket and replicate the website to another region. Finally, you will create a notification to email you when new content is put in the replication website bucket. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
27243	Can You Deploy an End-to-End Solution in AWS? [Expert]	In this challenge, you will configure a repeatable environment for a publicly available website by using the Amazon S3 and EC2 services. First, you will create a Virtual Private Cloud (VPC) environment for the EC2 instances. Next, you will create an Amazon S3 bucket that will hold the static web content for the website and create a custom EC2 launch template that includes the web server engine and an initial homepage for the website. Finally, you will deploy a web server based on the custom launch template and verify that the website is publicly available from the new EC2 instance. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
19460	Can You Design a Cloud Network by Using AWS? [Advanced]	In this challenge, you will verify your skills while creating a cloud network with both private and public subnets. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
33805	Can You Design a Database Solution? [Advanced]	In this Challenge Lab, you will configure a highly available MySQL database in an Amazon RDS DB instance to store data for a customer-facing website. First, create security groups to control access to the database servers, and then you will create subnet groups for the database servers in each region. Next, you will create a MySQL Amazon RDS DB instance, and then you will create an Amazon Elastic Compute Cloud (Amazon EC2) instance that runs a PHP website to connect to the database server. Finally, you will create a read replica of the database in another region for disaster recovery, then you will create a web server in the 2nd region to test access to the read replica.
21995	Can You Design an Elastic, Highly Available Architecture in AWS? [Advanced]	In this Challenge Lab, you will create a scalable and resilient website that contains a dashboard for monitoring. First, you will create security groups for a load balancer and an Auto Scaling group, and then you will create a launch template that you will use to create Amazon Elastic Cloud Compute (Amazon EC2) instances. Next, you will create an Auto Scaling group, and then you will attach the Auto Scaling group to a new Application Load Balancer. Finally, you will connect to the website through the load balancer, and then you will create a CloudWatch dashboard to monitor the load balancer. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or exit and then return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge
19506	Can You Enable Cross-Region Replication and Archiving? [Advanced]	In this challenge, you will create a bucket for logs files that replicates across regions into IA. You will then use a lifecycle policy in the new region to archive the files in Glacier after 30 days and deletes them after one year. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
24453	Can You Implement a Highly Available Website? [Expert]	In this challenge, you will configure, deploy a highly available, and secure website by using Amazon Web Services. First, you will establish a secure network environment by using a network access control list (ACL) and a security group, and then you will create an Amazon Elastic Compute Cloud (Amazon EC2) instance based on an existing instance, and then you will create a fleet of web servers running on an Amazon Elastic Compute Cloud (Amazon EC2) instance in a virtual private cloud (VPC) by using an Auto Scaling group. Finally, you will create an Application Load Balancer to use with the Auto Scaling group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21988	Can You Implement a Multi-Layer Security Model? [Advanced]	In this Challenge Lab, you need to implement a secure application within a VPC environment. The application will consist of 2 layers, a web server and an application server. You need to implement appropriate security measures using Network ACLs and Security Groups to protect both layers of the application. First, you will create security groups for the web and application layers. Next, you will create a network ACL for the subnets. Then, you will create EC2 instances for the web and application servers. Finally, you will test access to the application through the Network ACL and Security Groups. Note: Once you begin the challenge lab, you will not be able to pause, save, or return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before
27242	Can You Implement a Repeatable Compute Layer by Using EC2? [Advanced]	In this challenge, you will configure a repeatable AWS Elastic Compute Cloud (EC2) environment by using a custom launch template. First, you will launch a custom EC2 instance that contains a pre-installed web server, and then you will attach an Amazon Elastic Block Store (EBS) data disk. Next, you will create an Amazon Machine Image (AMI) based on an existing instance, and then you will create a launch template based upon the custom AMI. Finally, you will launch a new web server EC2 instance by using the custom launch template. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21996	Can You Implement an End-to-End Solution in AWS? [Expert]	In this Challenge Lab, you will create a scalable website that has a backend database and a dashboard for monitoring. First, you will create security groups and Network Access Control Lists (ACLs) to secure the network environment, and then you will create an Amazon RDS DB instance running MySQL. Next, you will create a launch template that you will use to create Amazon Elastic Cloud Compute (Amazon EC2) instances, and then you will create an Auto Scaling group and an Application Load Balancer. Next, you will configure the website to use the database, and then you will connect to the website through the load balancer. Finally, you will create a CloudWatch dashboard to monitor the load balancer and the RDS instance.
30301	Can You Implement Metrics, Alarms, and Filters? [Advanced]	In this challenge, you will configure CloudWatch logs for a website so that you will be notified when anyone attempts to access the admin page of the website. First, you will verify that the web server is running, and then you will connect to the console of the Elastic Cloud Compute (EC2) instance by using EC2 Instance Connect. Next, you will configure the CloudWatch logs agent on the web server, and then you will configure a log filter that will become a custom metric. Finally, you will use the custom metric to create a CloudWatch alarm, and then you will test the alarm. Note: Once you begin the challenge lab, you will not be able to pause, save, or return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
24452	Can You Implement Secure Access to a Service? [Advanced]	In this challenge, you will configure a web server that runs on an Amazon Elastic Compute Cloud (EC2) instance in a virtual private cloud (VPC). First, you will create a security group, and then you will configure a network access control list (ACL) that allows HTTP, HTTPS, and ICMP IPv4 traffic to reach the web server. Next, you will create an Amazon EC2 instance that runs a web server. Finally, you will test connectivity to the web server from the internet. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
28699	Can You Remediate Issues by Using Monitoring and Availability Metrics? [Advanced]	In this challenge, you will create a solution that will automatically start an Amazon Elastic Cloud Compute (Amazon EC2) instance when it stops. First, you will create a new Lambda execution role, and then you will create a Lambda function to start a specific EC2 instance. Next, you will create a new Amazon EventBridge rule to monitor the EC2 instance state and execute the Lambda function if the instance stops. Finally, you will test the rule by manually stopping the EC2 instance. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
24449	Can You Secure Access to an S3 Bucket? [Advanced]	In this challenge, you will create an Amazon S3 bucket to store static assets for a website, and then you will configure cross-region replication (CRR) to a new bucket. Next, you will enable public access to the bucket, and then you will create a user account for the web administrator. Next, you will create an Identity and Access Management (IAM) policy that provides full control of the bucket, and then you will create a new group. Finally, you will assign the IAM policy to the group, and then you will add the web administrator to the group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
19500	Can You Serve a Simple, Static Website with Amazon S3? [Advanced]	In this challenge, you will create an S3 bucket with version control to be a static website. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
19503	Can You Use Access Logging for Bucket Management and Monitoring? [Advanced]	In this challenge, you will create an S3 bucket to allow the distribution of files to the public. It will allow the upload and download of content but not the deletion, and setup logging of all activity in the bucket. The logs will be held in a separate S3 bucket. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
28696	Collect Metrics and Logs by Using the CloudWatch Agent [Guided]	In this challenge, you will configure the CloudWatch agent to collect metrics and logs for a website. First, you will verify that the web server is running, and then you will connect to the console of the Amazon Elastic Cloud Compute (Amazon EC2) instance by using EC2 Instance Connect. Next, you will configure the CloudWatch agent on the web server, and then you will create a custom metric and a log filter that you will use to test access to the database from the web server. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
21990	Configure a NoSQL Database by Using Amazon DynamoDB [Guided]	In this challenge lab, you will create an Amazon DynamoDB table that will be used to access data for a Python application. First, you will create a DynamoDB table, and then you will create an Identity and Access Management (IAM) policy to allow access to the DynamoDB table. Next, you will create an IAM role to allow access to the DynamoDB table, and then you will create an Amazon Elastic Compute Cloud (Amazon EC2) instance to run a Python application. Finally, you will install the Boto3 and pandas Python libraries in the AppServer instance, and then you will connect to the console of the Amazon EC2 instance to test access to the DynamoDB table from the Python application. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge
31519	Configure a Relational Database by Using Amazon RDS [Guided]	In this challenge lab, you will configure a MySQL database in an Amazon RDS DB instance to store data for a customer-facing website. First, you will create a security group to control access to the database server, and then you will create an Amazon RDS DB instance. Next, you will create an Amazon Elastic Compute Cloud (Amazon EC2) instance that runs a PHP website, and then you will install the MySQL command-line tools in the instance. Finally, you will create a table that contains data, and then you will test access to the database from the web server. Note: Once you begin the challenge lab, you will not be able to pause, save, or return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
24451	Configure a Security Group [Guided]	In this challenge, you will create a security group that will only allow specific traffic into a web server you are running. First, you will create a security group. Next, you will create an Amazon Elastic Compute Cloud (Amazon EC2) instance that uses the security group. Finally, you will test access to the web server through the security group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
30523	Configure an Amazon EventBridge Rule That Sends an Automated Email by Using the Simple Notification Service [Guided]	In this challenge, you will monitor an Amazon Elastic Compute Cloud (Amazon EC2) instance and generate an email if the instance is stopped. First, you will create a new Amazon Simple Notification Service (Amazon SNS) topic, and then you will create an email subscription. Next, you will create an Amazon EventBridge rule to monitor your EC2 instance for state changes. Finally, you will verify the EC2 instance, and then you will stop the instance that you received an email when the state changed. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
28708	Configure an Amazon EventBridge Rule That Triggers an Action [Guided]	In this challenge, you will configure an Amazon EventBridge rule that will send an email when an Amazon Elastic Cloud Compute (Amazon EC2) instance shuts down. First, verify that the EC2 instance is running, and then subscribe to an Amazon Simple Notification Service (Amazon SNS) topic. Next, create an Amazon EventBridge rule to monitor the status of the EC2 instance and generate a notification when the instance is stopped. Finally, simulate a failure of the EC2 instance, and then you will verify that you received an email notification. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
19502	Configure an Amazon S3 Notification [Guided]	In this Challenge Lab, you will configure an Amazon Simple Storage Service (S3) notification that will send an email when new content is uploaded to an S3 bucket. First, you will create a new S3 bucket, and then you will create a notification topic. Next, you will create a policy to allow your S3 bucket to use the notification, and then you then will create an event for your bucket to send a message to the topic. Finally, you will upload a file, and then you will verify that the notification is working. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or exit and then return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
21790	Configure an Elastic Load Balancer [Guided]	In this challenge, you will balance the traffic between multiple EC2 instances of an application. First, you will create a key pair, and then you will create a security group. Next, you will create two EC2 instances, and then you will create a target group. Finally, you will register the web servers with the target group, and then you will create an elastic load balancer that uses the target group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21978	Configure an S3 Bucket and Website [Guided]	In this challenge, you will create multiple S3 buckets, enable version control, server access logging, S3 encryption, public access, public website hosting, and will upload files to serve as a static website. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
28698	Configure an SNS Notification for a CloudWatch Alarm [Guided]	In this challenge, you will configure Amazon CloudWatch to generate an alarm and then send you a notification when 404 errors reach a specific level. First, create an Amazon Simple Notification Service (SNS) topic, and then create an email subscription for the topic. Next, create a CloudWatch metric and alarm for 404 errors on an Amazon Elastic Cloud Compute (Amazon EC2) instance, and then simulate errors on a website by attempting to connect to a nonexistent page. Finally, monitor the CloudWatch alarm until it is triggered, and then verify that you received a notification email. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure you have enough time to complete the challenge lab before you start.
30395	Configure AWS Auto Scaling [Guided]	In this challenge, you will configure Auto Scaling for your web servers. First, you will create a security group for a launch template, and then you will configure a launch template. Next, you will create an Elastic Load Balancer, and then you will create an Auto Scaling group. Finally, you will create a scheduled action for the Auto Scaling group. Note: Once you begin the challenge, you will not be able to pause, save, or exit and then return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
30769	Configure AWS Systems Manager Patch Manager [Guided]	In this challenge, you will configure patch management by using the Patch Manager capability in AWS Systems Manager. First, you will view the predefined baselines for managing patches, and then you will create new baselines for Windows Server and Amazon Linux systems. Next, you will organize Amazon Elastic Cloud Compute (Amazon EC2) instances into patch groups, and then you will scan for compliance. Finally, you will install any missing patches in the instances in the patch group, and then you will review the patch management dashboard and reporting information. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
19504	Configure Cross Region Replication for an S3 Bucket [Guided]	In this challenge, you will be setting up replication between two S3 buckets in different regions and using S3 IA for cost control. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21979	Configure Data Transfer and Storage Options for an S3 Bucket [Guided]	In this challenge, you will configure data transfer and storage options. First, you will create a new Amazon Simple Storage Service (S3) bucket. Next, you will enable transfer acceleration. Finally, you will classify stored files, and then you will configure file storage to use the most cost-effective storage tiers. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21427	Configure File Encryption and Access Logging [Guided]	In this challenge, you will configure a bucket to encrypt files at rest and log access to the bucket. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21992	Configure High Availability by Using an Elastic Load Balancer [Guided]	In this challenge lab, you will configure Elastic Load Balancing for two Amazon Elastic Compute Cloud (Amazon EC2) instances. First, you will create a security group for a load balancer, and then you will modify the security group for the web server. Next, you will configure two EC2 instances as web servers, and then you will create an IAM role to allow access to the EC2 instances. Finally, you will create a load balancer for the EC2 instances, and then you will test the load balancer. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
30604	Configure Maintenance Windows by Using AWS Systems Manager [Guided]	In this challenge, you will create maintenance windows in AWS Systems Manager to perform maintenance tasks on your AWS Elastic Cloud Compute (Amazon EC2) resources. First, you will create two new maintenance windows, and then you will register targets against the windows. Next, you will register a Run Command task on one of the windows, and then you will run a patch automation on the other window. Finally, you will verify that the Run Command task executed successfully. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
31179	Configure Security for an IAM User [Guided]	In this challenge, you will create an Identity and Access Management (IAM) user that has full administrator access. First, you will create an IAM user, and then you will create a user group. Next, you will assign a user to the group, and then you will attach a policy to the group. Finally, you will implement multi-factor authentication (MFA) for the root account. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
21982	Configure Storage by Using EBS [Guided]	In this challenge, you will configure storage by using Amazon Elastic Block Store (EBS) to create a volume that you can attach to an Amazon Elastic Compute Cloud (EC2) instance. First, you will create an EBS volume. Next, you will modify the EBS volume. Finally, you will attach the EBS volume to an EC2 instance. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21981	Connect to an EC2 Instance by Using RDP [Guided]	In this challenge, you will create a Windows Server virtual machine by using Amazon Elastic Compute Cloud (EC2). First, you will create a new key pair that you will use to decrypt the password for an EC2 instance. Next, you will create a security group to allow access to an EC2 instance, and then you will create an EC2 instance by using a Windows Server Amazon Machine Image (AMI). Finally, you will download an RDP file to your local computer, and then you will connect to the EC2 instance by using the RDP file. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.

28697	Create a CloudWatch Alarm [Guided]	In this challenge, you will configure Amazon CloudWatch to generate an alarm when CPU utilization reaches a specific level. First, you will create a CloudWatch alarm to monitor CPU utilization on an Amazon Elastic Cloud Compute (Amazon EC2) instance, and then you will connect to the console of the EC2 instance by using EC2 Instance Connect. Next, you will install a stress testing tool, and then you will run a stress test to simulate load. Finally, you will monitor the CloudWatch alarm until it is triggered. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
28705	Create a CloudWatch Dashboard [Guided]	In this challenge, you will configure a custom CloudWatch dashboard that will display multiple metrics on a single page. First, you will verify that the web servers are running behind a load balancer. Next, you will create a CloudWatch metric filter for memory usage on each web server. Finally, you will create a custom CloudWatch dashboard to display the memory, CPU, and load balancer metrics. Note: Once you begin the challenge, you will not be able to pause, save, or return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
21983	Create a Custom AMI by Using an Existing EC2 Instance [Guided]	In this challenge, you will create an Amazon Machine Image (AMI) to use as a web server template. First, you will create a key pair, and then you will create a security group. Next, you will create an AMI by using the web server instance. Finally, you will create an Amazon Elastic Cloud Compute (EC2) instance by using the custom AMI, and then you will test the new web server instance. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
27195	Create a Launch Template [Guided]	In this challenge, you will create a launch template, and then you will launch an Amazon Elastic Cloud Compute (Amazon EC2) instance from the template. First, you will configure a key pair, and then you will configure a security group. Next, you will create a launch template based on an Amazon Machine Image (AMI), and then you will launch an EC2 instance by using the template. Finally, you will establish an SSH terminal connection to the EC2 instance by using PuTTY. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
39620	Create a Production Deployment Environment in Amazon API Gateway [Advanced]	In this Challenge lab, you will take an AWS Lambda function fronted by Amazon API Gateway that is deployed for development and create a version to deploy to production. First, you will test the development version of your application to ensure it works. Next, you will use an AWS CloudFormation template to create a production version of your DynamoDB table, Lambda function, and associated IAM policies and roles. Next, you will add a stage variable to API Gateway that represents the correct Lambda function name for a stage. Next, you will change your API Gateway Lambda function integration to call the correct Lambda function based on the stage. Next, you will create a prod stage for API Gateway, along with an API key and API usage plan. Finally, you will deploy and call the prod version of y
21991	Create a Scalable Website That Uses an Elastic Load Balancer [Guided]	In this challenge lab, you will create a scalable and resilient website. First, you will create security groups for a load balancer and an Auto Scaling group. Next, you will create a launch template that you will use to create Amazon Elastic Cloud Compute (Amazon EC2) instances, and then you will create an Auto Scaling group. Finally, you will attach a new load balancer to the Auto Scaling group, and then you will connect to the website through the load balancer. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
39597	Create a Secure API Endpoint for a Lambda Function by Using Amazon API Gateway [Advanced]	In this Challenge Lab, you will create a secure Amazon API Gateway endpoint for an AWS Lambda function. First, you will create a new Amazon API Gateway for a REST API. Next, you will add an AWS Lambda integration to your Amazon API gateway, and then you will define a route and an HTTP GET request on your AWS Lambda function. Next, you will add an API key to your Amazon API Gateway to prevent unauthorized access. Finally, you will verify that you can authenticate to your Amazon API Gateway, and then you will retrieve data via your AWS Lambda function. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
39316	Create an Amazon DynamoDB Table [Advanced]	In this Challenge Lab, you will create an Amazon DynamoDB table that supports storing scores for an online game. First, you will create the Amazon DynamoDB table with the appropriate primary key and secondary attributes. Next, you will import sample data into the table from a file in Amazon S3. Finally, you will add a secondary index to support finding the current high score. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
21788	Create an Auto Scaling Group [Guided]	In this challenge, you will create an Auto Scaling group that will allow a set of servers to recover from a failure. You must have two virtual machines running at all times. First, you will create a key pair, and then you will create a security group. Next, you will create a launch configuration. Finally, you will create an Auto Scaling group, and then you will test the Auto Scaling group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21787	Create an EC2 Instance by Using a Launch Template [Guided]	You are a systems architect. You need to create a template that you can use to create Amazon Web Services (AWS) EC2 instances. The template must support version control. In this challenge, you will first create a key pair, and then you will create a console. Finally, you will test your REST API endpoint responds successfully to an HTTP GET request. Note: Once you begin the challenge, you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21785	Create an Instance by Using a Custom AMI [Guided]	In this challenge, you will replicate an existing web server. First, you will create a key pair, and then you will create an Amazon Machine Image (AMI) from an existing instance. Next, you will create an EC2 instance from the custom AMI, and then you will add a new volume. Finally, you will tag the Elastic Block Store (EBS) volumes on the new instance. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
19505	Create an Object Lifecycle Policy for Amazon S3 Documents [Guided]	In this challenge, you will change the storage class on files manually. Then you will setup a lifecycle policy to automatically maintain log files. The files will first be moved into S3 IA after 30 days, then to Glacier after 60 days, then deleted after one year. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21784	Create and Configure an EC2 Instance That Uses a User Data Script [Guided]	In this challenge, you will create an EC2 instance that contains an Apache web server. First, you will create a key pair to allow remote access to the server. Next, you will create a security group that allows SSH and HTTP traffic. Finally, you will create an EC2 instance that uses a user data script to install an Apache web server, and then you will test the web server. Note: Once you begin the challenge, you will not be able to pause, save, or exit and then return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
21243	Create Buckets, Versioning, and Permissions with Amazon S3 [Guided]	In the challenge, you will create an S3 Bucket that has version control enabled, upload a file, and then make the file publicly accessible. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
24444	Create EC2 Instances by Using Auto Scaling [Guided]	In this challenge, you will configure and deploy Elastic Compute Cloud (EC2) instances by using an Auto Scaling group. First, you will create a security group for a launch template, and then you will configure a launch template. Next, you will create an Auto Scaling group. Finally, you will test the Auto Scaling group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
28704	Create Metric Filters [Guided]	In this challenge, you will configure the Amazon CloudWatch agent to collect logs for a website so that you can monitor invalid access attempts. First, you will verify that the web server is running, and then you will connect to the console of the Amazon Elastic Cloud Compute (Amazon EC2) instance by using EC2 Instance Connect. Next, you will configure the CloudWatch agent on the web server. Finally, you will create a metric filter from the logs by using CloudWatch, and then you will review invalid access attempts by using a graph. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
39315	Deploy an AWS Lambda Function [Advanced]	In this Challenge Lab, you will deploy a REST API endpoint for AWS Lambda. First, you will create the Lambda function by using Python, and then you will package it into a ZIP file. Next, you will deploy it on AWS by using the AWS Management Console. Finally, you will test your REST API endpoint responds successfully to an HTTP GET request. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
19458	Design a VPC and Associated Subnets in AWS [Guided]	In this challenge, you will learn how to create a Virtual Private Cloud (VPC) and private subnets. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21987	Enable Network Security in AWS [Guided]	In this challenge, you will establish a secure network environment for an application service that will be hosted on AWS. First, you will enable the assignment of public IP addresses to a subnet in a virtual private cloud (VPC). Next, you will create a network access control list (ACL) for the public subnet, and then you will create a network ACL for the private subnet. Finally, you will create new Amazon Elastic Compute Cloud (Amazon EC2) instances that use the network ACLs, and then you will test access to the EC2 instances through the network ACLs. Note: Once you begin the challenge, you will not be able to pause, save, or return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
19459	Establish Internet and NAT Gateways [Guided]	In this challenge, you will create internet and NAT gateways and will create route tables to provide routing for your subnets. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
30773	Evaluate AWS Config Rules [Guided]	In this challenge, you will evaluate resources in your environment by using AWS managed rules and the AWS Config service. First, you will enable the AWS Config service, and then you will create a new Amazon Simple Storage Service (Amazon S3) bucket. Next, you will review the AWS Config resources. Finally, you will enable AWS managed rules to evaluate your resources. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
30532	Execute Commands and Automation Documents by Using the AWS Systems Manager Service [Guided]	In this challenge, you will configure AWS Systems Manager to manage the hosts for Amazon Elastic Cloud Computer (Amazon EC2) instances. First, you will create a new Amazon Simple Storage Service (Amazon S3) bucket, and then you will configure Systems Manager by using the Quick Start option. Next, you will verify that the EC2 instance is part of the managed fleet, and then you will review the built-in documents. Finally, you will run and verify command documents, and then you will run and verify automation documents. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
21973	Getting Started with Amazon Simple Storage Service (S3) [Getting Started]	In this Challenge Lab, you will create a highly available website using S3 buckets. You will also create an S3 bucket to allow users to upload files. This bucket will encrypt all files at test, log all activity in the bucket and send a notification when new content is uploaded to the bucket. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
24442	Getting Started with AWS Cloud Fundamentals [Getting Started]	In this lab, you will configure and deploy a highly available and secure website by using Amazon Web Services (AWS). First, you will configure network security for your environment, and then you will create and configure an Amazon Simple Storage Service (Amazon S3) bucket to store static assets. Next, you will create a fleet of EC2 instances by using an Auto Scaling group. Finally, you will integrate an Application Load Balancer into the Auto Scaling group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21783	Getting Started with AWS Elastic Compute Cloud [Getting Started]	In this lab, you will configure a scalable, load-balanced web server farm by using Amazon Web Services (AWS). First, you will configure an Amazon Elastic Compute Cloud (Amazon EC2) instance, and then you will create a custom Amazon Machine Image (AMI) based on the instance. Next, you will create a launch template, and then you will configure an Auto Scaling group. Finally, you will install a web server by using AWS System Manager Run Command, and then you will configure load balancing for the server farm. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
27199	Getting Started with AWS Secure Architecture Configuration [Getting Started]	In this lab, you will configure a secure Amazon Web Services (AWS) virtual private cloud (VPC) architecture for a web server. First, you will configure an AWS VPC environment following AWS best practices for security and reliability. Next, you will create an Auto Scaling Group that contains a load balancer to host multiple web servers in the VPC. Finally, you will test your environment to make sure that it is functioning. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21974	Getting Started with AWS Tech Essentials [Getting Started]	In this lab, you will configure an Amazon Web Services environment. First, you will create an Amazon Simple Storage Service (Amazon S3) bucket to host a publicly accessible website. Next, you will build a custom Virtual Private Cloud (VPC) that supports public and private workloads, and you will create a re-usable Amazon Elastic Compute Cloud (Amazon EC2) solution by using a custom AMI and a launch template. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
21241	Hosting a Static Website with Amazon S3 [Guided]	In this challenge, you will create and configure an Amazon S3 Bucket with version control to serve a static website. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
30382	Implement a Fault Tolerant File Service by Using EFS [Guided]	In this challenge, you will configure an Amazon Elastic File System (Amazon EFS) for your server infrastructure. First, you will create a file system, and then you will map a file share to a Linux bastion host. Next, you will map the EFS file system to the web servers, and then you will add files to the file share. Finally, you will configure the web servers to use the content in EFS, and then you will verify fault tolerance. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
26424	Implement a Network Access Control List [Guided]	In this challenge, you will create a secure network Access Control List (ACL) that will only allow specific traffic into a subnet. First, you will create a network ACL. Next, you will create an EC2 instance on the subnet that is associated with the network ACL. Finally, you will test access to the web server through the network ACL. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
31185	Implement a Security Monitoring Process [Guided]	In this challenge lab, you will implement a security monitoring process by using AWS CloudTrail. First, you will set up CloudTrail to track management events, and then you will configure a topic by using the Amazon Simple Notification Service (SNS). Next, you will configure monitoring for Amazon CloudWatch Logs by using a metric filter, and then you will configure an alarm for a log group. Finally, you will review the management events in the CloudTrail trail, and then you will review the CloudWatch alarms and graphs. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
31183	Implement an IAM Policy [Guided]	In this challenge lab, you will create an AWS Identity and Access Management (IAM) policy to manage an Amazon Simple Storage Service (Amazon S3) bucket. First, you will create an IAM policy, and then you will create a user group. Next, you will add a user account to the group, and then you will add an object to the bucket, and then you will attempt to delete both the object and the bucket. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
29780	Implement Caching in AWS by Using DAX [Guided]	In this challenge, you will implement caching for an application. First, you will deploy an Amazon DynamoDB Accelerator (DAX) cluster, and then you will configure an Identity and Access Management (IAM) role by using a policy. Next, you will launch an Amazon Elastic Cloud Compute (Amazon EC2) instance for your application, and then you will configure the EC2 instance. Finally, you will run the application, and then you will review the response times for the DAX cluster. Note: Once you begin the challenge, you will not be able to pause, save, or exit and then return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
24443	Implement Elastic Load Balancing Between EC2 Instances [Guided]	In this challenge, you will configure Elastic Load Balancing for two Amazon Elastic Compute Cloud (Amazon EC2) instances. First, you will configure two EC2 instances as web servers. Next, you will create a target group that includes the EC2 instances. Finally, you will create a load balancer for the EC2 instances. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
31188	Implement Encryption at Rest [Guided]	In this challenge lab, you will protect data in transit and at rest by using encryption. First, you will create an Amazon Key Management Service (KMS) key to manage the security of data at rest. Next, you will modify the key policy to allow the Amazon CloudTrail service to interact with KMS, and then you will create a CloudTrail trail that logs server-side encryption by using KMS. Finally, you will encrypt the data in an S3 bucket by using a KMS key. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
30248	Implement Health Checks by Using ELB and Route 53 [Guided]	In this challenge, you will configure health checks for your environment. First, you will create a target group for an Application Load Balancer, and then you will configure health checks for the target group. Next, you will create a listener that routes requests from the load balancer to the target group, and then you will configure health checks for your load balancer by using Route 53. Finally, you will configure an Amazon (SNS) topic to notify you when a failure occurs, and then you will monitor health checks while simulating a web server failure. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
24447	Implement Identity and Access Management [Guided]	In this challenge, you will create an Amazon Simple Storage Service (Amazon S3) bucket that will contain assets for a website that you will be hosting. The website must be accessible to a group of web administrators. First, you will create an Amazon S3 bucket to store the assets, and then you will create a user account for the web administrator. Next, you will create an Identity and Access Management (IAM) policy that provides full control of the bucket, and then you will create a new group. Finally, you will assign the IAM policy to the group, and then you will add the web administrator to the group. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
33394	Implement Protection for Data and Infrastructure [Guided]	In this Challenge Lab, you will protect data and other sensitive information in your AWS environment. First, you will create an Amazon Elastic Cloud Compute (Amazon EC2) key pair to provide a secure connection to an instance. Next, you will add the key to the AWS Systems Manager by using the AWS Management Console, and then you will upload a key to the Parameter Store by using the AWS Command Line Interface (CLI). Finally, you will store a set of access key credentials in the AWS Secrets Manager. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure you have enough time to complete the challenge lab before you start
30121	Implement Scaling for an Amazon RDS Instance [Guided]	In this challenge, you will implement scaling for an Amazon Relational Database Service (RDS) instance. First, you will create security groups, and then you will deploy a MySQL DB instance. Next, you will create an Amazon Elastic Cloud Compute (Amazon EC2) instance to act as a server, and then you will add data to the database. Finally, you will scale the RDS instance vertically and horizontally, and then you will verify that you can access the data. Note: Once you begin the challenge, you will not be able to pause, save, or exit and then return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
21985	Implement Security by Using an IAM Role [Guided]	In this challenge, you will create an Identity and Access Management (IAM) role that you will use to access an Amazon Simple Storage Service (Amazon S3) bucket from an Elastic Compute Cloud (EC2) instance. First, you will create an Amazon S3 bucket to store objects, and then you will create a role to provide access to the bucket from an EC2 instance. Next, you will create an IAM policy that provides full control of the bucket, and then you will assign the policy to the role. Finally, you will create a new EC2 instance that will use the role, and then you will sign in to the EC2 instance and test the role.
21986	Implement Security by Using Security Groups [Guided]	In this challenge, you will configure a web server that is accessible from the internet and an application server that is only accessible from the web server. First, you will create security groups to allow traffic into the web server and the application server. Next, you will create new Amazon Elastic Compute Cloud (Amazon EC2) instances that use the security groups. Finally, you will test access to the EC2 instances through the security groups. Note: Once you begin the challenge, you will not be able to pause, save, or return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
24446	Implement the Simple Storage Service [Guided]	In this challenge, you will configure a multi-region Simple Storage Service (S3) bucket that will store static website assets. First, you will create an S3 bucket, and then you will enable cross-region replication (CRR). Next, you will make the bucket public. Finally, you will add resources to the bucket, and then you will test access to the bucket. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
21791	Install a Web Server by Using AWS System Manager Run Command [Guided]	In this challenge, you will install Apache on multiple instances at the same time. First, you will create an IAM role for Run Command to use when accessing the server. Next, you will create two running instances, and then you will attach the role to the running instances. Finally, you will install Apache on multiple instances at one time. Note: Once you begin a challenge you will not be able to pause, save, or return to your progress. Please ensure you have set aside enough time to complete the challenge before you start.
29774	Manage AWS Logs by Using CloudTrail [Guided]	In this challenge, you will manage AWS logs by using CloudTrail. First, you will enable CloudTrail logging. Next, you will generate log entries. Finally, you will examine and download the logs, and then you will review the event history. Note: Once you begin the challenge, you will not be able to pause, save, or return to your challenge. Please ensure that you have set aside enough time to complete the challenge before you start.
32210	Migrate a Load Balanced Application by Using a Blue/Green and Canary Deployment Strategy [Guided]	In this challenge lab, you will migrate an app by using a blue/green and canary strategy. First, configure and test a blue app environment that uses two Amazon Elastic Cloud (Amazon EC2) instances, and then you will configure a parallel green app environment that uses two EC2 instances. Next, perform canary testing by using an Application Load Balancer, and then you will migrate fifty percent of the traffic to the green version. Finally, direct all traffic to the green EC2 instances and decommission the blue EC2 instances by using a CloudFormation change set. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
21994	Monitor Applications by Using CloudWatch [Guided]	In this challenge lab, you will monitor applications by using an Amazon CloudWatch dashboard. First, you will connect to the web servers that are running behind a load balancer. Next, you will create a CloudWatch metric filter for 404 errors on each web server, and then you will create a custom CloudWatch dashboard to display the memory, CPU, and load balancer metrics. Finally, you will test the dashboard by simulating activity. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
28709	Perform Automatic Remediation by Using an AWS Config Rule [Guided]	In this challenge, you will configure an AWS Config rule to ensure that public access to Amazon Simple Storage Service (Amazon S3) buckets is automatically disabled. First, you will create an Amazon Identity and Access Management (IAM) role for automation, and then you will create an S3 bucket that is noncompliant. Next, you will create an AWS Config rule to automatically remediate any noncompliant S3 buckets. Finally, you will test the AWS Config rule. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
30772	Provision and Maintain AWS Resources by Using CloudFormation [Guided]	In this challenge, you will provision and maintain AWS resources by using AWS CloudFormation. First, you will download a CloudFormation template, and then you will deploy a stack based on the template. Next, you will create a CloudFormation change set, and then you will execute the change set to create an Amazon Simple Storage Service (Amazon S3) bucket and an Amazon Elastic Cloud Compute (Amazon EC2) instance. Finally, you will detect changes to the EC2 instance by using CloudFormation drift detection, and then you will delete the CloudFormation stack. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.
39625	Secure Amazon API Gateway REST Methods by Using an Amazon Cognito User Pool [Advanced]	In this Challenge Lab, you will authorize end users to access your Amazon API Gateway REST API. First, you will create an Amazon Cognito user pool and an app client, and then you will create a new user in your Amazon Cognito user pool. Next, you will add your Amazon Cognito user pool as an authorizer for your Amazon API Gateway REST API. Finally, you will obtain a valid Amazon Cognito user JWT token, and then you will verify that you can call your Amazon API Gateway endpoints by using this token. Note: Once you begin the Challenge Lab, you will not be able to pause, save, or return to your Challenge Lab. Please ensure that you have set aside enough time to complete the Challenge Lab before you start.
28707	Troubleshoot an EC2 Instance by Using a CloudWatch Alarm [Guided]	In this challenge, you will configure CloudWatch to generate an alarm when memory usage reaches a specific level, and then automatically restart an Amazon Elastic Cloud Compute (Amazon EC2) instance. First, create a CloudWatch alarm for memory usage on an EC2 instance, and then you will connect to the console of the EC2 instance by using EC2 Instance Connect. Next, install a stress testing tool, and then run a stress test to simulate memory usage. Finally, monitor the CloudWatch alarm until it is triggered, and then you will verify that the EC2 instance restarts. Note: Once you begin the challenge lab, you will not be able to pause, save, or exit and then return to your challenge lab. Please ensure that you have set aside enough time to complete the challenge lab before you start.