NO.1 A company is tunning a website on Amazon EC2 instances thai are in an Auto Scaling group When the website traffic increases, additional instances lake several minutes to become available because ot a long-running user data script that installs software A SysOps administrator must decrease the time that is required (or new instances to become available Which action should the SysOps administrator take to meet this requirement?

A. Reduce the scaling thresholds so that instances are added before traffic increases

B. Purchase Reserved Instances to cover 100% of the maximum capacity of the Auto Scaling group

C. Update the Auto Scaling group to launch instances that have a storage optimized instance type

D. Use EC2 Image Builder to prepare an Amazon Machine Image (AMI) that has pre-installed software

Answer: D

Explanation:

automated way to update your image. Have a pipeline to update your image. When you boot from your AMI updates = scrits are already pre-installed, so no need to complete boot scripts in boot process. https://aws.amazon.com/image-builder/

NO.2 A company applies user-defined tags to resources that are associated with me company's AWS workloads Twenty days after applying the tags, the company notices that it cannot use re tags to filter views in the AWS Cost Explorer console.

What is the reason for this issue?

A. It lakes at least 30 days to be able to use tags to filter views in Cost Explorer.

B. The company has not activated the user-defined tags for cost allocation.

C. The company has not created an AWS Cost and Usage Report

D. The company has not created a usage budget in AWS Budgets

Answer: B

NO.3 A company is managing many accounts by using a single organization in AWS Organizations. The organization has all features enabled. The company wants to turn on AWS Config in all the accounts of the organization and in all AWS Regions.

What should a Sysops administrator do to meet these requirements in the MOST operationally efficient way?

A. Use AVVS CloudFormation StackSets to deploy stack instances that turn on AWS Config in all accounts and in all Regions.

B. Use AWS CloudFormation StackSets to deploy stack policies that turn on AWS Config in all accounts and in all Regions.

C. Use service control policies (SCPs) to configure AWS Config in all accounts and in all Regions.

D. Create a script that uses the AWS CLI to turn on AWS Config in all accounts in the organization. Run the script from the organization's management account.

Answer: C

NO.4 A company plans to launch a static website on its domain example com and subdomain www example.com using Amazon S3. How should the SysOps administrator meet this requirement?

A. Create one S3 bucket named example.com for both the domain and subdomain.

B. Create one S3 bucket with a wildcard named '.example.com tor both the domain and subdomain.

C. Create two S3 buckets named example.com and www.exdmpte.com. Configure the subdomain bucket to redirect requests to the domain bucket.
D. Create two S3 buckets named http//example.com and http//" exampte.com. Configure the wildcard (') bucket to redirect requests to the domain bucket.
Answer: C

NO.5 A company manages an application that uses Amazon ElastiCache for Redis with two extra-large nodes spread across two different Availability Zones. The company's IT team discovers that the ElastiCache for Redis cluster has 75% freeable memory. The application must maintain high availability.
What is the MOST cost-effective way to resize the cluster?
A. Decrease the number of nodes in the ElastiCache for Redis cluster from 2 to 1.
B. Deploy a new ElastiCache for Redis cluster that uses large node types. Migrate the data from the original cluster to the new cluster. After the process is complete, shut down the original duster.
C. Deploy a new ElastiCache for Redis cluster that uses large node types. Take a backup from the original cluster, and restore the backup in the new cluster. After the process is complete, shut down the original cluster.
D. Perform an online resizing for the ElastiCache for Redis cluster. Change the node types from extra-large nodes to large nodes.
Answer: D
Explanation:
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/scaling-redis-cluster-mode-enabled.html As demand on your clusters changes, you might decide to improve performance or reduce costs by changing the number of shards in your Redis (cluster mode enabled) cluster. We recommend using online horizontal scaling to do so, because it allows your cluster to continue serving requests during the scaling process.
https://docs.aws.amazon.com/AmazonElastiCache/latest/red-ug/redis-cluster-vertical-scaling-scaling-down.html

NO.6 A company is running production workloads that use a Multi-AZ deployment of an Amazon RDS for MySQL db.m6g.xlarge (general purpose) standard DB instance. Users report that they are frequently encountering a "too many connections" error. A SysOps administrator observes that the number of connections on the database is high.
The SysOps administrator needs to resolve this issue while keeping code changes to a minimum.
Which solution will meet these requirements MOST cost-effectively?
A. Modify the RDS for MySQL DB instance to a larger instance size.
B. Migrate the RDS for MySQL DB instance to Amazon DynamoDB.
C. Configure RDS Proxy. Modify the application configuration file to use the RDS Proxy endpoint.
D. Modify the RDS for MySQL DB instance to a memory optimized DB instance.
Answer: C
Explanation:
For the issue of "too many connections" on a MySQL database, using RDS Proxy offers a streamlined solution:
RDS Proxy Setup: RDS Proxy sits between your application and the database. It pools and efficiently

manages database connections, which reduces the number of direct connections to the database.
Connection Management: By handling connection pooling, RDS Proxy can help mitigate issues related to connection overhead and limits, such as the "too many connections" error, by allowing the database to serve more requests from a smaller and more stable number of connections.
Minimal Code Changes: Integrating RDS Proxy requires changes only to the database connection settings in the application's configuration files to point to the RDS Proxy endpoint instead of directly to the database. This minimizes the amount of code change needed and leverages RDS Proxy to handle connection scaling and management more efficiently.
This approach enhances database performance and scalability by efficiently managing connections without the need for significant application changes or database resizing.

NO.7 A company requires that all IAM user accounts that have not been used for 90 days or more must have their access keys and passwords immediately disabled A SysOps administrator must automate the process of disabling unused keys using the MOST operationally efficient method.
How should the SysOps administrator implement this solution?
A. Create an AWS Step Functions workflow to identify IAM users that have not been active for 90 days Run an AWS Lambda function when a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule is invoked to automatically remove the AWS access keys and passwords for these IAM users
B. Configure an AWS Config rule to identify IAM users that have not been active for 90 days Set up an automatic weekly batch process on an Amazon EC2 instance to disable the AWS access keys and passwords for these IAM users
C. Develop and run a Python script on an Amazon EC2 instance to programmatically identify IAM users that have not been active for 90 days Automatically delete these 1AM users
D. Set up an AWS Config managed rule to identify IAM users that have not been active for 90 days Set up an AWS Systems Manager automation runbook to disable the AWS access keys for these IAM users
Answer: D

NO.8 An organization with a large IT department has decided to migrate to AWS With different job functions in the IT department it is not desirable to give all users access to all AWS resources Currently the organization handles access via LDAP group membership What is the BEST method to allow access using current LDAP credentials?
A. Create an AWS Directory Service Simple AD Replicate the on-premises LDAP directory to Simple AD
B. Create a Lambda function to read LDAP groups and automate the creation of IAM users
C. Use AWS CloudFormation to create IAM roles Deploy Direct Connect to allow access to the on-premises LDAP server
D. Federate the LDAP directory with IAM using SAML Create different IAM roles to correspond to different LDAP groups to limit permissions
Answer: D

NO.9 A web application runs on Amazon EC2 instances behind an Application Load Balancer (ALB). The instances run in an Auto Scaling group across multiple Availability Zones. A SysOpe administrator notices that some of these EC2 instances show up as heathy in the Auto Scaling g-out but show up as

unhealthy in the ALB target group.
What is a possible reason for this issue?
A. Security groups ate rot allowing traffic between the ALB and the failing EC2 instances
B. The Auto Seating group health check is configured for EC2 status checks
C. The EC2 instances are failing to launch and failing EC2 status checks.
D. The target group health check is configured with an incorrect port or path
Answer: D

NO.10 An organization is running multiple applications for their customers. Each application is deployed by running a base AWS CloudFormation template that configures a new VPC. All applications are run in the same AWS account and AWS Region. A SysOps administrator has noticed that when trying to deploy the same AWS CloudFormation stack, it fails to deploy.
What is likely to be the problem?
A. The Amazon Machine image used is not available in that region.
B. The AWS CloudFormation template needs to be updated to the latest version.
C. The VPC configuration parameters have changed and must be updated in the template.
D. The account has reached the default limit for VPCs allowed.
Answer: D

NO.11 A SysOps administrator launches an Amazon EC2 Linux instance in a public subnet. When the instance is running, the SysOps administrator obtains the public IP address and attempts to remotely connect to the instance multiple times. However, the SysOps administrator always receives a timeout error.
Which action will allow the SysOps administrator to remotely connect to the instance?
A. Add a route table entry in the public subnet for the SysOps administrator's IP address.
B. Add an outbound network ACL rule to allow TCP port 22 for the SysOps administrator's IP address.
C. Modify the instance security group to allow inbound SSH traffic from the SysOps administrator's IP address.
D. Modify the instance security group to allow outbound SSH traffic to the SysOps administrator's IP address.
Answer: C

NO.12 A company has an Amazon RDS DB instance. The company wants to implement a caching service while maintaining high availability.
Which combination of actions will meet these requirements? (Choose two.)
A. Add Auto Discovery to the data store.
B. Create an Amazon ElastiCache for Memcached data store.
C. Create an Amazon ElastiCache for Redis data store.
D. Enable Multi-AZ for the data store.
E. Enable Multi-threading for the data store.
Answer: C,D
Explanation:
https://aws.amazon.com/elasticache/memcached/
https://aws.amazon.com/elasticache/redis/

NO.13 A company has an application that uses a scheduled AWS Lambda function to retrieve datasets from external sources over the internet. The function is not associated with a VPC. The company is modifying the application to store the information that the Lambda function retrieves on an Amazon RDS DB instance in a private subnet. The VPC has two public subnets and two private subnets.
A SysOps administrator must deploy a solution that allows the Lambda function to access the new database and continue to access the internet.
Which solution meets these requirements?
A. Create a new Lambda function with VPC access and an Elastic IP address. Attach the function to public subnets in two Availability Zones. Associate a security group with the Elastic IP address. Configure the security group outbound rules to allow Lambda to access the required resources.
B. Create a new Lambda function with VPC access and two public IP addresses. Attach the function to public subnets in the same Availability Zones that the database uses. Associate a security group with the function. Configure the security group inbound rules to allow Lambda to access the required resources.
C. Reconfigure the Lambda function for VPC access. Add NAT gateways to the public subnets in the VPAdd route table entries in the private subnets to route through the NAT gateways to the internet. Attach the function to the private subnets that support the database. Associate a security group with the function. Configure the security group outbound rules to allow Lambda to access the internet.
D. Reconfigure the Lambda function for VPC access. Attach the function to the private subnets. Add route table entries in the private subnets to route through the internet gateway to the internet. Associate a security group with the subnets. Configure the security group inbound rules to allow Lambda to access the required resources through the internet gateway.
Answer: C

NO.14 A company has a public website that recently experienced problems. Some links led to missing webpages, and other links rendered incorrect webpages. The application infrastructure was running properly, and all the provisioned resources were healthy. Application logs and dashboards did not show any errors, and no monitoring alarms were raised. Systems administrators were not aware of any problems until end users reported the issues.
The company needs to proactively monitor the website for such issues in the future and must implement a solution as soon as possible.
Which solution will meet these requirements with the LEAST operational overhead?
A. Rewrite the application to surface a custom error to the application log when issues occur. Automatically parse logs for errors. Create an Amazon CloudWatch alarm to provide alerts when issues are detected.
B. Create an AWS Lambda function to test the website. Configure the Lambda function to emit an Amazon CloudWatch custom metric when errors are detected. Configure a CloudWatch alarm to provide alerts when issues are detected.
C. Create an Amazon CloudWatch Synthetics canary. Use the CloudWatch Synthetics Recorder plugin to generate the script for the canary run. Configure the canary in line with requirements. Create an alarm to provide alerts when issues are detected.
Answer: A

NO.15 Application A runs on Amazon EC2 instances behind a Network Load Balancer (NLB). The EC2 instances are in an Auto Scaling group and are in the same subnet that is associated with the NLB. Other applications from an on-premises environment cannot communicate with Application A on port 8080.
To troubleshoot the issue, a SysOps administrator analyzes the flow logs. The flow logs include the following records:

```
2 123456789010 eni-1235b8ca123456789 192.168.0.13 172.31.16.139 59003 8080 1 4 336 1432917027 1432917142 ACCEPT OK
2 123456789010 eni-1235b8ca123456789 172.31.16.139 192.168.0.13 8080 59003 1 4 336 1432917094 1432917142 REJECT OK
```

What is the reason for the rejected traffic?
A. The security group of the EC2 instances has no Allow rule for the traffic from the NLB.
B. The security group of the NLB has no Allow rule for the traffic from the on-premises environment.
C. The ACL of the on-premises environment does not allow traffic to the AWS environment.
D. The network ACL that is associated with the subnet does not allow outbound traffic for the ephemeral port range.
Answer: A

NO.16 A SysOps administrator has created an AWS Service Catalog portfolio and has shared the portfolio with a second AWS account in the company. The second account is controlled by a different administrator.
Which action will the administrator of the second account be able to perform?
A. Add a product from the imported portfolio to a local portfolio.
B. Add new products to the imported portfolio.
C. Change the launch role for the products contained in the imported portfolio.
D. Customize the products in the imported portfolio.
Answer: A

NO.17 A Sysops administrator wants to share a copy of a production database with a migration account. The production database is hosted on an Amazon RDS DB instance and is encrypted at rest with an AWS Key Management Service (AWS KMS) key that has an alias of What must the Sysops administrator do to meet these requirements with the LEAST administrative overhead?
A. Take a snapshot of the RDS DB instance in the production account. Amend the KMS key policy of the production-rds-key KMS key to give access to the migration account's root user. Share the snapshot with the migration account.
B. Create an RDS read replica in the migration account. Configure the KMS key policy to replicate the production-rds-key KMS key to the migration account.
C. Take a snapshot of the RDS DB instance in the production account. Share the snapshot with the migration account. In the migration account, create a new KMS key that has an identical alias.
D. Use native database toolsets to export the RDS DB instance to Amazon S3. Create an S3 bucket and an S3 bucket policy for cross-account access between the production account and the migration account. Use native database toolsets to import the database from Amazon S3 to a new RDS DB instance.
Answer: A
Explanation:
To share an encrypted Amazon RDS DB instance snapshot across accounts, the least administrative overhead involves directly managing permissions on the AWS KMS key and sharing the snapshot.

Here's how to do it:
Take a Snapshot: Initiate a snapshot of your Amazon RDS DB instance in the production account. This captures the current state of the database.
Modify KMS Key Policy: Adjust the policy of the KMS key used for encryption (identified by the alias 'production-rds-key') to grant the kms:Decrypt permission to the migration account's root user. This step is crucial as it allows the migration account to use the same encryption key to decrypt the snapshot.
Share the Snapshot: Share the newly created snapshot with the migration account using the RDS console or AWS CLI. The migration account will now be able to see and use this snapshot to create a new RDS instance.
AWS Documentation Reference:
You can refer to the AWS documentation on sharing encrypted snapshots: Sharing Encrypted Snapshots.

NO.18 A company recently its server infrastructure to Amazon EC2 instances. The company wants to use Amazon CloudWatch metrics to track instance memory utilization and available disk space.
What should a SysOps administrator do to meet these requirements?
A. Configure CloudWatch from the AWS Management Console tor all the instances that require monitoring by CloudWatch. AWS automatically installs and configures the agents far the specified instances.
B. Install and configure the CloudWatch agent on all the instances. Attach an IAM role to allow the instances to write logs to CloudWatch.
C. Install and configure the CloudWatch agent on all the instances. Attach an IAM user to allow the instances to write logs to CloudWatch.
D. Install and configure the CloudWatch agent on all the instances. Attach the necessary security groups to allow the instances to write logs to CloudWatch
Answer: C

NO.19 A SysOps administrator must configure Amazon S3 to host a simple nonproduction webpage. The SysOps administrator has created an empty S3 bucket from the AWS Management Console. The S3 bucket has the default configuration in place.
Which combination of actions should the SysOps administrator take to complete this process? (Choose two.)
A. Configure the S3 bucket by using the "Redirect requests for an object" functionality to point to the bucket root URL.
B. Turn off the "Block all public access" setting. Allow public access by using a bucket ACL that contains <Permission>WEBSITE</Permission>.
C. Turn off the "Block all public access" setting. Allow public access by using a bucket ACL that allows access to the AuthenticatedUsers grantee.
D. Turn off the "Block all public access" setting. Set a bucket policy that allows "Principal": the s3:GetObject action.
E. Create an index.html document. Configure static website hosting, and upload the index document to the S3 bucket.
Answer: D,E
Explanation:

To host a static website on Amazon S3, the SysOps administrator needs to configure the bucket for public access and set up the static website hosting. Here's how to complete this process:
Turn off "Block all public access": Amazon S3 buckets have "Block all public access" settings enabled by default for security. Since the webpage needs to be accessible publicly, this setting must be disabled. This step is crucial to allow public read access to the web content.
Set a bucket policy: After disabling "Block all public access," set a bucket policy that explicitly allows public read access to the S3 bucket. This policy should allow the s3:GetObject action for everyone, which can be set by specifying "Principal": "*". This policy ensures that anyone can view the webpage but does not grant permissions to modify or delete the content.
Create an index.html document and configure static website hosting: The next step is to create an index.html file, which will serve as the entry point of the website. After creating this file, upload it to the bucket. Then, configure the bucket for static website hosting through the S3 management console. This setting enables the S3 bucket to serve the webpage directly from the index.html file.
Combining these actions, the S3 bucket will be properly configured to host and serve the static website with minimal operational overhead and maximum accessibility.

NO.20 A company wants to collect data from an application to use for analytics. For the first 90 days, the data will be infrequently accessed but must remain highly available. During this time, the company's analytics team requires access to the data in milliseconds. However, after 90 days, the company must retain the data for the long term at a lower cost. The retrieval time after 90 days must be less than 5 hours.
Which solution will meet these requirements MOST cost-effectively?
A. Store the data in S3 Standard-Infrequent Access (S3 Standard-IA) for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.
B. Store the data in S3 One Zone-Infrequent Access (S3 One Zone-IA) for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.
C. Store the data in S3 Standard for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Flexible Retrieval after 90 days.
D. Store the data in S3 Standard for the first 90 days. Set up an S3 Lifecycle rule to move the data to S3 Glacier Deep Archive after 90 days.
Answer: A
Explanation:
Glacier Deep Archive retrieval time more than 5 hours (it's 12 hours), so B&D out. S3 Standard IA is cheaper than S3 Standard. https://aws.amazon.com/tw/s3/pricing/

NO.21 A company runs a web application on three Amazon EC2 instances behind an Application Load Balancer (ALB). Web traffic increases significantly during the same 9-hour period every day and causes a decrease in the application's performance. A SysOps administrator must scale the application ahead of the changes in demand to accommodate the increased traffic.
Which solution will meet these requirements?
A. Create an Amazon CloudWatch alarm to monitor application latency. Configure an alarm action to increase the size of each EC2 instance if the latency threshold is reached.
B. Create an Amazon EventBridge rule to monitor application latency. Configure the rule to add an EC2 instance to the ALB if the latency threshold is reached
C. Deploy the application to an EC2 Auto Scaling group that uses a target tracking scaling policy.

Attach the ALB to the Auto Scaling group.

D. Deploy the application to an EC2 Auto Scaling group that uses a scheduled scaling policy. Attach the ALB to the Auto Scaling group.

Answer: D

Explanation:

For predictable, significant traffic increases during a specific time period every day:

EC2 Auto Scaling Group: Set up an Auto Scaling group for the EC2 instances running the web application. This group automatically adjusts the number of instances based on policies defined.

Scheduled Scaling Policy: Use a scheduled scaling policy to pre-emptively increase the number of instances before the expected increase in traffic each day. Scheduled scaling allows you to specify the scaling actions to occur at specific times, based on known or expected demand patterns.

Attach to ALB: Ensure the Auto Scaling group is attached to the Application Load Balancer, which will distribute incoming traffic across the dynamically adjusted pool of EC2 instances.

This approach ensures that the application scales up resources ahead of the expected load, maintaining performance and user experience without manual intervention.

NO.22 A SysOps administrator must analyze Amazon CloudWatch logs across 10 AWS Lambda functions for historical errors. The logs are in JSON format and are stored in Amazon S3. Errors sometimes do not appear in the same field, but all errors begin with the same string prefix.

What is the MOST operationally efficient way for the SysOps administrator to analyze the log files?

A. Use S3 Select to write a query to search for errors. Run the query across all log groups of interest.

B. Create an AWS Glue processing job to index the logs of interest. Run a query in Amazon Athena to search for errors.

C. Use Amazon CloudWatch Logs Insights to write a query to search for errors. Run the query across all log groups of interest.

D. Use Amazon CloudWatch Contributor Insights to create a rule. Apply the rule across all log groups of interest.

Answer: C

NO.23 A SysOps administrator is creating two AWS CloudFormation templates. The first template will create a VPC with associated resources, such as subnets, route tables, and an internet gateway. The second template will deploy application resources within the VPC that was created by the first template. The second template should refer to the resources created by the first template.

How can this be accomplished with the LEAST amount of administrative effort?

A. Add an export field to the outputs of the first template and import the values in the second template.

B. Create a custom resource that queries the stack created by the first template and retrieves the required values.

C. Create a mapping in the first template that is referenced by the second template.

D. Input the names of resources in the first template and refer to those names in the second template as a parameter.

Answer: A

Explanation:

https://docs.aws.amazon.com/AWSCloudFormation/latest/UserGuide/using-cfn-stack-exports.html

NO.24 A company has a simple web application that runs on a set of Amazon EC2 instances behind an Elastic Load Balancer in the eu-west-2 Region. Amazon Route 53 holds a DNS record for the application with a simple touting policy. Users from all over the world access the application through their web browsers.
The company needs to create additional copies of the application in the us-east-1 Region and in the ap-south-1 Region. The company must direct users to the Region that provides the fastest response times when the users load the application.
What should a SysOps administrator do to meet these requirements?
A. In each new Region, create a new Elastic Load Balancer and a new set of EC2 Instances to run a copy of the application. Transition to a geolocation routing policy.
B. In each new Region, create a copy of the application on new EC2 instances. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a latency routing policy.
C. In each new Region, create a copy of the application on new EC2 instances. Add these new EC2 instances to the Elastic Load Balancer in eu-west-2. Transition to a multivalue routing policy.
D. In each new Region, create a new Elastic Load Balancer and a new set of EC2 instances to run a copy of the application. Transition to a latency routing policy.
Answer: B

NO.25 A SysOps administrator receives an alert from Amazon GuardDuty about suspicious network activity on an Amazon EC2 instance. The GuardDuty finding lists a new external IP address as a traffic destination. The SysOps administrator does not recognize the external IP address. The SysOps administrator must block traffic to the external IP address that GuardDuty identified.
Which solution will meet this requirement?
A. Create a new security group to block traffic to the external IP address. Assign the new security group to the EC2 instance.
B. Use VPC flow logs with Amazon Athena to block traffic to the external IP address.
C. Create a network ACL. Add an outbound deny rule for traffic to the external IP address.
D. Create a new security group to block traffic to the external IP address. Assign the new security group to the entire VPC.
Answer: C
Explanation:
https://docs.aws.amazon.com/vpc/latest/userguide/vpc-network-acls.html

NO.26 A company has multiple Amazon EC2 instances that run a resource-intensive application in a development environment. A SysOps administrator is implementing a solution to stop these EC2 instances when they are not in use.
Which solution will meet this requirement?
A. Assess AWS CloudTrail logs to verify that there is no EC2 API activity. Invoke an AWS Lambda function to stop the EC2 instances.
B. Create an Amazon CloudWatch alarm to stop the EC2 instances when the average CPU utilization is lower than 5% for a 30-minute period.
C. Create an Amazon CloudWatch metric to stop the EC2 instances when the VolumeReadBytes metric is lower than 500 for a 30-minute period.
D. Use AWS Config to invoke an AWS Lambda function to stop the EC2 instances based on resource

configuration changes.

Answer: B

Explanation:

https://docs.aws.amazon.com/AmazonCloudWatch/latest/monitoring/UsingAlarmActions.html#AddingStopActions

NO.27 A company has a policy that requires all Amazon EC2 instances to have a specific set of tags. If an EC2 instance does not have the required tags, the noncompliant instance should be terminated. What is the MOST operationally efficient solution that meets these requirements?

A. Create an Amazon EventBridge (Amazon CloudWatch Events) rule to send all EC2 instance state changes to an AWS Lambda function to determine if each instance is compliant. Terminate any noncompliant instances.

B. Create an IAM policy that enforces all EC2 instance tag requirements. If the required tags are not in place for an instance, the policy will terminate noncompliant instance.

C. Create an AWS Lambda function to determine if each EC2 instance is compliant and terminate an instance if it is noncompliant. Schedule the Lambda function to invoke every 5 minutes.

D. Create an AWS Config rule to check if the required tags are present. If an EC2 instance is noncompliant, invoke an AWS Systems Manager Automation document to terminate the instance.

Answer: D

Explanation:

https://docs.aws.amazon.com/systems-manager/latest/userguide/systems-manager-automation.html

NO.28 A SysOps administrator is responsible for a legacy. CPU-heavy application The application can only be scaled vertically Currently, the application is deployed on a single t2 large Amazon EC2 instance The system is showing 90% CPU usage and significant performance latency after a few minutes What change should be made to alleviate the performance problem?

A. Change the Amazon EBS volume to Provisioned lOPs

B. Upgrade to a compute-optimized instance

C. Add additional t3. large instances to the application

D. Purchase Reserved Instances

Answer: B

NO.29 A company's SysOps administrator needs to change the AWS Support plan for one of the company's AWS accounts. The account has multi-factor authentication (MFA) activated, and the MFA device is lost.

What should the SysOps administrator do to sign in?

A. Sign in as a root user by using email and phone verification. Set up a new MFA device. Change the root user password.

B. Sign in as an 1AM user with administrator permissions. Resynchronize the MFA token by using the 1AM console.

C. Sign in as an 1AM user with administrator permissions. Reset the MFA device for the root user by adding a new device.

D. Use the forgot-password process to verify the email address. Set up a new password and MFA

device.
Answer: A

NO.30 A company has an internal web application that runs on Amazon EC2 instances behind an Application Load Balancer. The instances run in an Amazon EC2 Auto Scaling group in a single Availability Zone. A SysOps administrator must make the application highly available.
Which action should the SysOps administrator take to meet this requirement?
A. Increase the maximum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
B. Increase the minimum number of instances in the Auto Scaling group to meet the capacity that is required at peak usage.
C. Update the Auto Scaling group to launch new instances in a second Availability Zone in the same AWS Region.
D. Update the Auto Scaling group to launch new instances in an Availability Zone in a second AWS Region.
Answer: C

NO.31 A company updates its security policy to clarify cloud hosting arrangements for regulated workloads. Workloads that are identified as sensitive must run on hardware that is not shared with other customers or with other AWS accounts within the company.
Which solution will ensure compliance with this policy?
A. Deploy workloads only to Dedicated Hosts.
B. Deploy workloads only to Dedicated Instances.
C. Deploy workloads only to Reserved Instances.
D. Place all instances in a dedicated placement group.
Answer: A
Explanation:
Dedicated Hosts are physical servers that are dedicated to a single customer, ensuring that the customer's workloads are not shared with other customers or with other AWS accounts within the company. This will ensure that the company's security policy is followed and that sensitive workloads are running on hardware that is not shared with other customers or with other AWS accounts within the company.

NO.32 A company hosts a website on multiple Amazon EC2 instances that run in an Auto Scaling group. Users are reporting slow responses during peak times between
6 PM and 11 PM every weekend. A SysOps administrator must implement a solution to improve performance during these peak times.
What is the MOST operationally efficient solution that meets these requirements?
A. Create a scheduled Amazon EventBridge (Amazon CloudWatch Events) rule to invoke an AWS Lambda function to increase the desired capacity before peak times.
B. Configure a scheduled scaling action with a recurrence option to change the desired capacity before and after peak times.
C. Create a target tracking scaling policy to add more instances when memory utilization is above 70%.

D. Configure the cooldown period for the Auto Scaling group to modify desired capacity before and after peak times.

Answer: B

Explanation:

"Scheduled scaling helps you to set up your own scaling schedule according to predictable load changes. For example, let's say that every week the traffic to your web application starts to increase on Wednesday, remains high on Thursday, and starts to decrease on Friday. You can configure a schedule for Amazon EC2 Auto Scaling to increase capacity on Wednesday and decrease capacity on Friday." https://docs.aws.amazon.com/autoscaling/ec2/userguide/schedule_time.html

NO.33 A SysOps administrator is investigating why a user has been unable to use RDP to connect over the internet from their home computer to a bastion server running on an Amazon EC2 Windows instance.

Which of the following are possible causes of this issue? (Choose two.)

A. A network ACL associated with the bastion's subnet is blocking the network traffic.

B. The instance does not have a private IP address.

C. The route table associated with the bastion's subnet does not have a route to the internet gateway.

D. The security group for the instance does not have an inbound rule on port 22.

E. The security group for the instance does not have an outbound rule on port 3389.

Answer: A,C

NO.34 A company uses AWS Organizations to manage multiple AWS accounts. The company's SysOps team has been using a manual process to create and manage 1AM roles. The team requires an automated solution to create and manage the necessary 1AM roles for multiple AWS accounts.

What is the MOST operationally efficient solution that meets these requirements?

A. Create AWS CloudFormation templates. Reuse the templates to create the necessary 1AM roles in each of the AWS accounts.

B. Use AWS Directory Service with AWS Organizations to automatically associate the necessary 1AM roles with Microsoft Active Directory users.

C. Use AWS Resource Access Manager with AWS Organizations to deploy and manage shared resources across the AWS accounts.

D. Use AWS CloudFormation StackSets with AWS Organizations to deploy and manage 1AM roles for the AWS accounts.

Answer: D

NO.35 A SysOps administrator has set up a new Amazon EC2 instance as a web server in a public subnet. The instance uses HTTP port 80 and HTTPS port 443.

The SysOps administrator has confirmed internet connectivity by downloading operating system updates and software from public repositories. However, the SysOps administrator cannot access the instance from a web browser on the internet.

Which combination of steps should the SysOps administrator take to troubleshoot this issue? (Select THREE.)

A. Ensure that the inbound rules of the instance's security group allow traffic on ports 80 and 443.

B. Ensure that the outbound rules of the instance's security group allow traffic on ports 80 and 443.
C. Ensure that ephemeral ports 1024-65535 are allowed in the inbound rules of the network ACL that is associated with the instance's subnet.
D. Ensure that ephemeral ports 1024-65535 are allowed in the outbound rules of the network ACL that is associated with the instance's subnet.
E. Ensure that the filtering rules for any firewalls that are running on the instance allow inbound traffic on ports 80 and 443.
F. Ensure that AWS WAF is turned on for the instance and is blocking web traffic.
Answer: A,D,E
Explanation:
When troubleshooting inability to access an EC2 instance from the internet, you should:
A: Verify that the security group rules allow inbound HTTP and HTTPS traffic on ports 80 and 443. Security groups act as a virtual firewall to control the traffic to instances.
D: Check that outbound rules in the network ACL allow traffic for ephemeral ports 1024-65535. This is crucial for return traffic from web requests, which typically use these higher port numbers for responses.
E: Confirm that any software-based firewalls on the instance (such as Windows Firewall or iptables in Linux) are configured to allow inbound traffic on HTTP and HTTPS. These steps will ensure that the web server is correctly configured to receive and respond to web traffic from the internet. AWS provides guidelines on these configurations in their documentation on security groups EC2 Security Groups and network ACLs Network ACLs.